



# NetScaler Application Delivery Management 13.0

Machine translated content

## Disclaimer

このコンテンツの正式なバージョンは英語で提供されています。Cloud Software Group ドキュメントのコンテンツの一部は、お客様の利便性のみを目的として機械翻訳されています。Cloud Software Group は機械翻訳されたコンテンツを管理していないため、誤り、不正確な情報、不適切な用語が含まれる場合があります。英語の原文から他言語への翻訳について、精度、信頼性、適合性、正確性、またはお使用の Cloud Software Group 製品またはサービスと機械翻訳されたコンテンツとの整合性に関する保証、該当するライセンス契約書またはサービス利用規約、あるいは Cloud Software Group とのその他すべての契約に基づき提供される保証、および製品またはサービスのドキュメントとの一致に関する保証は、明示的か黙示的かを問わず、かかるドキュメントの機械翻訳された範囲には適用されないものとします。機械翻訳されたコンテンツの使用に起因する損害または問題について、Cloud Software Group は責任を負わないものとします。

## Contents

リリースノート	17
オンプレミスの <b>NetScaler ADM</b> を <b>Citrix Cloud</b> に移行する	19
よくある質問	27
トラブルシューティング	31
すべての方法記事	34
概要	38
機能とソリューション	39
アーキテクチャ	42
<b>NetScaler ADM</b> によるインスタンスの検出方法	43
ポーリングの概要	45
データガバナンス	52
ライセンス	57
システム要件	67
はじめに	80
展開	83
<b>NetScaler ADM</b> をインストールするための前提条件	84
<b>Citrix Hypervisor</b> での <b>NetScaler ADM</b>	86
<b>Microsoft Hyper-V</b> 上の <b>NetScaler ADM</b>	88
<b>VMware ESXi</b> 上の <b>NetScaler ADM</b>	95
<b>Kubernetes</b> クラスタ上の <b>NetScaler ADM</b>	100
<b>Linux KVM</b> サーバーでの <b>NetScaler ADM</b>	103
高可用性展開の構成	109
高可用性を実現するためのディザスタリカバリの構成	123

マルチサイト展開用にオンプレミスエージェントを構成する	132
<b>Kubernetes</b> クラスターに <b>ADM</b> エージェントをマイクロサービスとしてインストールする	139
<b>NetScaler ADM</b> 単一サーバー展開を高可用性展開に移行する	141
<b>NetScaler Insight Center</b> から <b>Citrix ADM</b> への移行	146
<b>NetScaler ADM</b> と <b>Citrix Director</b> の統合	148
追加のディスクを <b>NetScaler ADM</b> に接続する	149
構成	161
<b>Citrix ADM</b> へのインスタンスの追加	162
クラウドにデプロイされた <b>NetScaler ADC VPX</b> インスタンスを <b>NetScaler ADM</b> に追加する	173
仮想サーバーでのライセンスの管理および分析の有効化	175
<b>NTP</b> サーバーの構成	188
システム設定の構成	189
<b>NetScaler ADM</b> を <b>ServiceNow</b> インスタンスと統合する	193
エクスポートレポートのエクスポートまたはスケジュール設定	198
アップグレード	201
認証	207
<b>NetScaler ADM</b> で外部認証サーバーを構成する	210
<b>LDAP</b> 認証サーバーの追加	210
<b>RADIUS</b> 認証サーバーの追加	212
<b>TACACS</b> 認証サーバーの追加	214
<b>NetScaler ADM</b> ユーザー	215
認証サーバーグループの抽出	216
フォールバックおよび外部認証サーバーのカスケードを有効にする	217
アクセス制御	219

役割ベースのアクセス制御	219
アクセスポリシーの構成	222
グループの構成	226
役割の設定	236
ユーザーの構成	237
アプリケーション	239
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	241
アプリケーション管理	243
アプリケーションダッシュボードの概要	248
アプリケーションの表示	251
アプリケーションの詳細	252
アプリスコアコンポーネントを選択し、しきい値を設定します	257
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の詳細	260
<b>Web Insight</b> ダッシュボード	265
アプリケーション使用状況の分析	267
アプリダッシュボードのトラブルシューティング	276
アプリケーション分析のしきい値およびアラートの作成	284
インテリジェントなアプリケーション分析	286
インテリジェントアプリ分析の構成	286
アプリケーション分析用のパフォーマンス・インディケーター	287
応答時間	288
アクティブなサービス	289
平均 <b>CPU</b> 使用率	290
メモリ使用率	291

サービスフラップ	292
不安定なサーバー	293
セッションのビルダップ	295
セッションの再利用が低い	295
サージキューの蓄積	296
異常に大きい <b>HTTP</b> パケット	297
不適切な永続性タイプ	298
<b>TCP</b> 再構成キュー制限ヒット	299
<b>SSL</b> リアルタイムトラフィック	300
アプリケーションセキュリティダッシュボード	301
サービスグラフ	304
サービスグラフの設定	307
サービスグラフで詳細を表示	310
サービスグラフでのしきい値の設定	325
サービスの詳細の表示	327
問題のトラブルシューティングに関する進入の詳細の表示	330
分散トレース	335
サービスグラフで部分的なデータまたはデータがないかの診断詳細の表示	343
アプリケーションのサービスグラフ	345
サービスグラフ内のすべてのアプリケーションの全体的ビュー	352
<b>StyleBook</b>	361
<b>StyleBook</b> カテゴリー	363
<b>GitHub</b> リポジトリからの <b>StyleBook</b> のインポートと同期	372
デフォルトの <b>StyleBook</b> を使用する	374

<b>Web アプリケーションファイアウォール StyleBook</b>	<b>377</b>
<b>StyleBook</b> を使用して <b>WAF</b> と <b>BOT</b> プロファイルを作成する	<b>385</b>
すべてのデフォルト <b>StyleBook</b> を非表示にする	<b>386</b>
<b>StyleBooks</b> 構成ビルダーを使用した <b>NetScaler ADC</b> アプリケーション構成の移行	<b>388</b>
ビジネスアプリケーション <b>StyleBook</b>	<b>392</b>
<b>SSO Google Apps StyleBook</b>	<b>393</b>
<b>SSO Office 365 StyleBook</b>	<b>396</b>
<b>StyleBook</b> のための <b>Microsoft Skype for Business</b>	<b>405</b>
<b>Microsoft Exchange StyleBook</b>	<b>412</b>
<b>Microsoft SharePoint StyleBook</b>	<b>415</b>
<b>Microsoft ADFS proxy StyleBook</b>	<b>424</b>
<b>Oracle e-ビジネス StyleBook</b>	<b>442</b>
<b>Citrix StoreFront StyleBooks</b>	<b>444</b>
カスタム <b>StyleBook</b> の作成と使用	<b>447</b>
負分散仮想サーバーを作成する <b>StyleBook</b>	<b>449</b>
<b>StyleBook</b> による基本的な負分散構成の作成	<b>456</b>
複合 <b>StyleBook</b> の作成	<b>463</b>
カスタム <b>StyleBook</b> での <b>GUI</b> 属性の使用	<b>466</b>
カスタム <b>StyleBook</b> をインポートする	<b>467</b>
構成パックを作成および編集する	<b>472</b>
<b>NetScaler ADM</b> にファイルをアップロードする <b>StyleBook</b> を作成する	<b>482</b>
<b>SSL</b> 証明書と証明書キーファイルを <b>NetScaler ADM</b> にアップロードする <b>StyleBook</b> を作成する	<b>486</b>
<b>StyleBook</b> で定義された仮想サーバーでの分析の有効化とアラームの設定	<b>491</b>
インスタンスロール	<b>493</b>

<b>StyleBook</b> を作成して非 <b>CRUD</b> 操作を実行する	<b>501</b>
<b>StyleBook</b> の構成パックを別の <b>StyleBook</b> に移行する	<b>502</b>
<b>API</b> を使用して <b>StyleBook</b> から設定を作成する	<b>508</b>
<b>API</b> を使用して証明書とキーファイルをアップロードする設定を作成する	<b>516</b>
<b>API</b> を使用して任意のファイルタイプをアップロードする設定を作成する	<b>518</b>
<b>API</b> を使用してカスタム <b>StyleBook</b> をインポートする	<b>519</b>
<b>API</b> を使用してカスタム <b>StyleBook</b> をダウンロードする	<b>520</b>
<b>API</b> を使用してカスタム <b>StyleBook</b> を削除する	<b>521</b>
<b>StyleBook</b> の文法	<b>523</b>
<b>Header</b>	<b>525</b>
<b>StyleBook</b> のインポート	<b>526</b>
パラメーター	<b>527</b>
パラメーター-デフォルトソース構成	<b>540</b>
自動置換	<b>542</b>
コンポーネント	<b>547</b>
ヘルパーコンポーネント	<b>549</b>
オプションのプロパティ	<b>550</b>
プロパティ-デフォルトソース構成	<b>551</b>
ネストされたコンポーネント	<b>553</b>
条件構成	<b>554</b>
<b>repeat</b> 構造	<b>555</b>
繰り返し条件構成	<b>558</b>
ネストされた繰り返し	<b>558</b>
結果	<b>560</b>

パラメータ参照	561
親参照	562
コンポーネントのリファレンス	563
置換参照	564
変数参照	564
オペレーション	565
分析	567
アラーム	569
式	571
インプレース補間	576
組み込み関数	579
依存関係の検出	592
インスタンス管理	593
グローバルに分散したサイトの監視	596
タグを作成してインスタンスに割り当てる方法	601
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	604
<b>NetScaler ADC</b> インスタンスの管理パーティションの管理	606
<b>NetScaler ADC</b> の高可用性ペアの作成	611
<b>NetScaler ADC</b> インスタンスのバックアップと復元	615
セカンダリ <b>NetScaler ADC</b> インスタンスへのフェイルオーバーを強制する	622
セカンダリ <b>NetScaler ADC</b> インスタンスを強制的にセカンダリとして保持する	623
インスタンスグループの作成	624
<b>ADM</b> を使用して <b>SDX</b> 上の <b>ADC VPX</b> インスタンスのプロビジョニング	626
複数の <b>Citrix VPX</b> インスタンスの再検出	637



インスタンスの管理解除	637
インスタンスへのルートをトレースする	638
アップグレードアドバイザリ	639
セキュリティアドバイザリ	641
イベント	642
イベントダッシュボードの使用	642
イベントのイベント期間を設定する	644
イベントフィルタをスケジュールする	645
イベントに対して繰り返し電子メール通知を設定する	646
イベントを抑制する	648
イベントルールの作成	649
<b>NetScaler ADC</b> 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	664
イベントの概要の表示	665
イベントの重大度と <b>SNMP</b> トラップの詳細を表示します	666
<b>NetScaler ADC Syslog</b> メッセージの表示とエクスポート	668
<b>syslog</b> メッセージの抑制	672
インスタンスイベントのプルーニング設定の構成	674
<b>SSL</b> 証明書の管理	675
<b>SSL</b> ダッシュボードの使用	682
<b>SSL</b> 証明書の有効期限の通知を設定する	686
インストールされた証明書を更新する	688
<b>NetScaler ADC</b> インスタンスへの <b>SSL</b> 証明書のインストール	689
証明書署名要求 ( <b>CSR</b> ) の作成	691
<b>SSL</b> 証明書のリンクとリンク解除	694

エンタープライズポリシーの構成	694
<b>NetScaler ADC</b> インスタンスからの <b>SSL</b> 証明書のポーリング	695
<b>IP</b> アドレス管理 ( <b>IPAM</b> ) の構成	696
構成ジョブ	698
構成ジョブの作成	700
レコードアンドプレイを使用して構成ジョブを作成する	704
構成ジョブを使用して、 <b>1</b> つのインスタンスから複数のインスタンスに構成を複製する	708
構成ジョブでの変数の使用	712
修正コマンドからの構成ジョブの作成	717
ある <b>NetScaler ADC</b> インスタンスから別のインスタンスに実行および保存された構成を複製する	719
実行構成ジョブを再利用する	720
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	722
メンテナンス・ジョブを使用した <b>NetScaler ADC SDX</b> インスタンスのアップグレード	724
<b>Citrix SD-WAN WANOP</b> インスタンスの構成ジョブの作成	725
マスター構成テンプレートの使用	730
ジョブを使用して <b>NetScaler ADC</b> インスタンスをアップグレードする	736
構成テンプレートを使用した監査テンプレートの作成	744
設定ジョブで <b>SCP (put)</b> コマンドを使用する	746
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	749
構成ジョブでの構成監査テンプレートの再利用	750
構成テンプレートのインポートとエクスポート	754
メンテナンス・ジョブ	756
構成監査	767
監査テンプレートの作成	767

監査レポートを表示する	772
インスタンス間の設定変更の監査	777
ネットワーク構成に関する設定アドバイスを取得	781
<b>NetScaler ADC</b> インスタンスの構成監査をポーリングする	783
構成変更 <b>SNMP</b> トラップの構成監査差分を生成	785
ネットワーク機能	785
負荷分散エンティティのレポートを生成する	786
ネットワーク機能レポートのエクスポートまたはスケジュール設定	789
ネットワークレポート作成	792
<b>ADM</b> 監査ログを使用してインフラストラクチャの管理と監視	802
分析	805
ライセンス要件	807
ログストリームの概要	808
<b>URL</b> データ収集を無効にする	811
しきい値およびアラートの作成	812
適応しきい値の設定	813
データベースの永続性の構成	814
<b>Analytics</b> のセルフサービス診断	815
<b>Web Insight</b>	818
<b>Web Insight</b> に関する問題のトラブルシューティング	845
<b>HDX Insight</b>	849
<b>HDX Insight</b> データ収集の有効化	856
シングルホップモードで展開された <b>NetScaler Gateway</b> アプライアンスのデータ収集を有効にする	869
透過モードで展開された <b>NetScaler ADC</b> を監視するためのデータ収集を有効にする	871

ダブルホップモードで展開された <b>NetScaler Gateway</b> アプライアンスのデータ収集を有効にする	<b>874</b>
<b>LAN</b> ユーザーモードで展開された <b>NetScaler ADC</b> を監視するためのデータ収集を有効にする	<b>879</b>
<b>HDX Insight</b> のしきい値を作成してアラートを構成する	<b>882</b>
<b>HDX Insight</b> レポートと指標の表示	<b>886</b>
アクティブセッション	<b>888</b>
アクティブセッション	<b>889</b>
セッション	<b>903</b>
アクティブセッション	<b>905</b>
アクティブセッション	<b>911</b>
アクティブセッション	<b>913</b>
<b>Application</b> ビューのレポートとメトリック	<b>929</b>
セッション	<b>930</b>
アクティブセッション	<b>931</b>
デスクトップビューのレポートおよびメトリクス	<b>936</b>
アクティブセッション	<b>937</b>
アクティブセッション	<b>939</b>
ユーザービューのレポートとメトリック	<b>948</b>
アクティブセッション	<b>949</b>
アクティブセッション	<b>951</b>
インスタンスビューのレポートとメトリクス	<b>965</b>
ライセンスビューのレポートとメトリック	<b>972</b>
<b>HDX Insight</b> の問題のトラブルシューティング	<b>973</b>
<b>Gateway Insight</b>	<b>985</b>
<b>Gateway Insight</b> の問題のトラブルシューティング	<b>1003</b>

<b>Security Insight</b>	<b>1007</b>
ボット	<b>1029</b>
アプリケーションのセキュリティ違反の詳細を表示する	<b>1041</b>
<b>SSL Insight</b>	<b>1042</b>
<b>TCP Insight</b>	<b>1051</b>
<b>WAN Insight</b>	<b>1055</b>
<b>Video Insight</b>	<b>1058</b>
ネットワーク効率の表示	<b>1061</b>
最適化された <b>ABR</b> ビデオと最適化されていない <b>ABR</b> ビデオで使用するデータ量を比較する	<b>1062</b>
ストリーミングされる動画の種類とネットワークから消費されるデータ量の表示	<b>1064</b>
<b>ABR</b> ビデオの最適化と非最適化の再生時間を比較する	<b>1067</b>
最適化された <b>ABR</b> ビデオと最適化されていない <b>ABR</b> ビデオの帯域幅消費の比較	<b>1070</b>
<b>ABR</b> ビデオの再生の最適化数と非最適化数を比較する	<b>1071</b>
特定の時間枠のピークデータレートを表示する	<b>1074</b>
<b>SSL</b> フォワードプロキシ分析	<b>1077</b>
ダッシュボード	<b>1078</b>
使用例	<b>1084</b>
オーケストレーション	<b>1095</b>
<b>OpenStack: NetScaler ADC</b> インスタンスの統合	<b>1096</b>
前提条件	<b>1100</b>
<b>NetScaler ADM</b> および <b>OpenStack</b> での事前構成タスク	<b>1101</b>
<b>Horizon</b> を使用した <b>LBaaS V1</b> の設定	<b>1112</b>
コマンドラインを使用した <b>LBaaS V2</b> の設定	<b>1113</b>
レイヤ <b>7</b> コンテンツスイッチングの構成	<b>1118</b>

<b>OpenStack</b> での <b>NetScaler ADC VPX</b> インスタンスの手動 <b>Provisioning</b>	<b>1125</b>
<b>StyleBook</b> を使用した <b>OpenStack</b> での <b>NetScaler ADC VPX</b> インスタンスのプロビジョニング	<b>1127</b>
<b>VPX</b> チェックインとチェックアウトのライセンスおよび <b>OpenStack</b> 環境のプールライセンスのサポート	<b>1128</b>
管理パーティションの共有 <b>VLAN</b> サポート	<b>1131</b>
試用版ライセンスのワークフロー	<b>1133</b>
<b>OpenStack Heat</b> サービスとの統合	<b>1134</b>
サービスパッケージの分離ポリシー	<b>1140</b>
柔軟なポリシー・ベースのデバイス割り当て	<b>1143</b>
<b>NSX Manager: NetScaler ADC</b> インスタンスの手動 <b>Provisioning</b>	<b>1148</b>
<b>NSX Manager: NetScaler ADC</b> インスタンスの自動 <b>Provisioning</b>	<b>1165</b>
<b>Cisco ACI</b> ハイブリッドモードで <b>NetScaler ADM</b> を使用する <b>NetScaler ADC</b> オートメーション	<b>1175</b>
前提条件	<b>1178</b>
<b>Cisco APIC</b> および <b>NetScaler ADM</b> を使用して <b>NetScaler ADC</b> をハイブリッドモードで構成します	<b>1178</b>
<b>NetScaler ADM</b> を使用したアプリケーションの <b>StyleBook</b> の作成	<b>1179</b>
<b>NetScaler ADC</b> ハイブリッドモードデバイスパッケージを <b>Cisco APIC</b> にインポート	<b>1180</b>
<b>Cisco APIC</b> の <b>Device Manager</b> として <b>NetScaler ADM</b> を追加します	<b>1181</b>
<b>APIC</b> を使用して <b>Cisco ACI</b> にデバイスとして <b>NetScaler ADC</b> を追加します	<b>1185</b>
サービスグラフの作成とデプロイ	<b>1189</b>
<b>StyleBook</b> を使用して <b>NetScaler ADM</b> から <b>L4-L7</b> パラメータを構成する	<b>1199</b>
<b>APIC</b> からのエンドポイントイベントのアタッチとデタッチ	<b>1204</b>
<b>APIC</b> 障害レポート	<b>1204</b>
<b>NetScaler ADM</b> によって生成されたログ	<b>1205</b>
ハイブリッドモードデバイスパッケージによって生成されるログ	<b>1210</b>
<b>Cisco ACI</b> のクラウドオーケストレータモードの <b>NetScaler ADC</b> デバイスパッケージ	<b>1214</b>

<b>NetScaler ADM</b> で <b>Kubernetes</b> 入力構成を管理する	<b>1219</b>
<b>NetScaler ADC</b> プール容量	<b>1225</b>
<b>NetScaler ADC</b> プール容量を構成する	<b>1232</b>
<b>ADM</b> サーバーをプールされたライセンスサーバーとしてのみ構成する	<b>1239</b>
<b>NetScaler ADC VPX</b> の永続ライセンスを <b>NetScaler ADC</b> プール容量にアップグレードする	<b>1241</b>
<b>NetScaler ADC MPX</b> の永続ライセンスを <b>NetScaler ADC</b> プール容量にアップグレードする	<b>1247</b>
<b>NetScaler ADC SDX</b> で永続ライセンスを <b>NetScaler ADC</b> プール容量にアップグレードする	<b>1256</b>
クラスターモードの <b>NetScaler ADC</b> インスタンス上の <b>NetScaler ADC</b> プール容量	<b>1258</b>
サーバーヘルス監視	<b>1262</b>
問題が発生したときに予想される動作	<b>1263</b>
プール容量ライセンスの有効期限チェックの構成	<b>1265</b>
<b>NetScaler ADC VPX</b> および <b>BLX</b> ライセンスのチェックインとチェックアウト	<b>1266</b>
<b>NetScaler ADC</b> 仮想 <b>CPU</b> ライセンス	<b>1275</b>
<b>Citrix SD-WAN</b> インスタンスの管理	<b>1281</b>
<b>Citrix SD-WAN</b> インスタンスの追加	<b>1285</b>
マルチホップ展開のための <b>Citrix SD-WAN</b> 分析データの表示	<b>1289</b>
<b>Citrix SD-WAN WANOP</b> インスタンスのイベントレポートを表示する	<b>1293</b>
<b>Citrix SD-WAN WANOP</b> インスタンスのネットワークレポートの表示	<b>1293</b>
<b>Citrix SD-WAN WANOP</b> インスタンスのバックアップ	<b>1295</b>
<b>HAProxy</b> インスタンスの管理	<b>1303</b>
<b>HAProxy</b> インスタンスを <b>NetScaler ADM</b> に追加する	<b>1303</b>
<b>HAProxy</b> アプリのダッシュボード	<b>1306</b>
サードパーティライセンス	<b>1311</b>
<b>HAProxy</b> インスタンスのロールベースのアクセス制御	<b>1314</b>

<b>HAProxy</b> インスタンスの監視	<b>1314</b>
<b>HAProxy</b> インスタンスで構成されたフロントエンドの詳細を表示する	<b>1315</b>
<b>HAProxy</b> インスタンスで設定されたバックエンドの詳細を表示する	<b>1316</b>
<b>HAProxy</b> インスタンスで設定されたサーバーの詳細の表示	<b>1317</b>
フロントエンドまたはサーバーの数が最も多い <b>HAProxy</b> インスタンスを表示する	<b>1317</b>
<b>HAProxy</b> インスタンスを再起動する	<b>1319</b>
<b>HAProxy</b> インスタンスのバックアップと復元	<b>1319</b>
<b>HAProxy</b> 設定ファイルを編集します	<b>1321</b>
システム設定の管理	<b>1323</b>
システムバックアップの設定を構成する	<b>1328</b>
<b>NTP</b> サーバの構成	<b>1329</b>
<b>NetScaler Application Delivery Management (ADM)</b> のアップグレード	<b>1330</b>
<b>NetScaler ADM</b> パスワードをリセットする方法	<b>1331</b>
<b>NetScaler ADM</b> にアクセスするためのデュアル <b>NIC</b> の構成	<b>1339</b>
<b>syslog</b> パージ間隔の設定	<b>1341</b>
システムプルーニングとイベントプルーニングの設定	<b>1342</b>
デフォルト以外のユーザーのシェルアクセスを有効にする	<b>1344</b>
アクセスできない <b>NetScaler ADM</b> サーバーをリカバリする	<b>1345</b>
<b>NetScaler ADM</b> サーバーへのホスト名の割り当て	<b>1351</b>
<b>NetScaler ADM</b> サーバーのバックアップと復元	<b>1351</b>
監査情報の表示	<b>1355</b>
<b>SSL</b> 設定の構成	<b>1357</b>
<b>CPU</b> 、メモリ、ディスク使用率の監視	<b>1358</b>
通知設定の構成	<b>1359</b>



テクニカルサポートファイルを生成する	1363
暗号グループの構成	1365
<b>SNMP</b> トラップの宛先、マネージャコミュニティ、およびユーザーの作成	1366
システムアラームの設定と表示	1367
<b>API</b> プロキシサーバーとしての <b>NetScaler ADM</b>	1368
インフラストラクチャ分析を使用して問題を視覚化	1374
インフラストラクチャ分析でのインスタンスの詳細の表示	1398
<b>ADC</b> インスタンスの容量に関する問題の表示	1405
新しいインジケータによるインフラストラクチャ分析の強化	1408
よくある質問	1411

## リリースノート

February 6, 2024

NetScaler Application Delivery Management (ADM) 13.0 リリースノートでは、新機能、既存の機能の拡張、およびビルドの既知の問題について説明します。13.0 リリースのリリースノートには、次のセクションが含まれています。

- 新機能: ビルドでリリースされた既存の機能の新機能と機能強化。
- 既知の問題: ビルドに存在する問題とその回避策 (該当する場合)。
- 修正された問題: ビルドで対処された問題。

リリースノートの全文を表示するには、次のリンクをクリックしてください。

リリースノート	公開日	バージョン
<a href="#">Citrix ADM 13.0 リリースのビルド 92.18 のリリースノート</a>	公開日:2023 年 9 月 6 日	リリースノートのバージョン:1.0
<a href="#">Citrix ADM 13.0 リリースのビルド 91.12 のリリースノート</a>	公開日:2023 年 5 月 18 日	リリースノートのバージョン:1.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 90.7 のリリースノート</a>	公開日:2023 年 2 月 1 日	リリースノートのバージョン:1.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 89.7 のリリースノート</a>	公開日:2022 年 12 月 19 日	リリースノートのバージョン:1.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 88.12 のリリースノート</a>	公開日: 2022 年 10 月 20 日	リリースノートのバージョン:1.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 87.9 のリリースノート</a>	公開日:2023 年 2 月 6 日	リリースノートバージョン:2.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 86.17 のリリースノート</a>	公開日: 2022 年 6 月 20 日	リリースノートのバージョン:1.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 85.19 のリリースノート</a>	公開日: 2022 年 6 月 14 日	リリースノートのバージョン:1.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 84.10 のリリースノート</a>	公開日: 2021 年 12 月 14 日	リリースノートのバージョン:1.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 83.27 のリリースノート</a>	公開日: 2021 年 9 月 28 日	リリースノートのバージョン:1.0

リリースノート	公開日	バージョン
<a href="#">NetScaler ADM 13.0 リリースのビルド 82.41 のリリースノート</a>	公開日: 2021 年 6 月 9 日	リリースノートのバージョン:1.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 79.64 のリリースノート</a>	公開:2021 年 4 月 06 日	リリースノートのバージョン:1.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 76.29 のリリースノート</a>	公開:2021 年 2 月 19 日	リリースノートのバージョン:1.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 71.40 のリリースノート</a>	公開:2021 年 1 月 20 日	リリースノートバージョン:2.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 67.42 のリリースノート</a>	公開:2020 年 10 月 28 日	リリースノートバージョン:1.0。注:ビルド 67.42 はビルド 67.39 を置き換えます
<a href="#">NetScaler ADM 13.0 リリースのビルド 67.39 のリリースノート</a>	公開:2020 年 10 月 16 日	リリースノートバージョン:2.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 64.35 のリリースノート</a>	公開:2020 年 10 月 16 日	リリースノートバージョン:2.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 61.48 のリリースノート</a>	公開:2020 年 9 月 18 日	リリースノートバージョン:2.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 58.30 のリリースノート</a>	公開: 2020 年 6 月 10 日	リリースノートのバージョン:1.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 52.24 のリリースノート</a>	公開: 2020 年 3 月 26 日	リリースノートのバージョン:1.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 47.22 のリリースノート</a>	公開: 2019 年 12 月 10 日	リリースノートのバージョン:1.0
<a href="#">NetScaler ADM 13.0 リリースのビルド 41.28 のリリースノート</a>	公開: 2019 年 9 月 27 日 (ビルド 41.22 に代わるビルド 41.28)	リリースノートのバージョン:1.0

注

これらのリリースノートには、セキュリティ関連の修正は記載されていません。セキュリティに関する修正とアドバイスの一覧については、Citrix セキュリティ情報を参照してください。

## オンプレミスの **NetScaler ADM** を **Citrix Cloud** に移行する

February 6, 2024

オンプレミスの **NetScaler ADM 13.0 64.35** 以降のバージョンを **Citrix Cloud** に移行できます。ADM に 12.1 以前のバージョンがある場合は、まず **13.0 64.35** 以降にアップグレードしてから、Citrix Cloud に移行する必要があります。詳細については、「[アップグレード](#)」セクションを参照してください。

Citrix Cloud を介した ADM サービスでは、次のものを得ることができます。

- 最新機能のアップデートにより、約 2 週間ごとにリリースが速くなります。
- アプリケーションセキュリティ、ボット、パフォーマンス、使用状況に関する機械学習ベースの分析
- ピークおよびリーン期間の分析、アプリケーションセキュリティとボットの機械学習ベースの分析、アプリケーション CPU 分析など、現在 ADM サービスでのみサポートされているさまざまな機能。

移行を成功させるには、次のことを行う必要があります。

- Citrix Cloud アクセシビリティのために、オンプレミスの ADM でインターネット接続を確保する
- ADM サービスエージェントの設定
- Citrix Cloud からクライアントとシークレット CSV ファイルを取得する
- ADM サービスライセンスの検証
- スクリプトを使用して移行する

オンプレミスの ADM から ADM サービスに移行した後、オンプレミス ADM をもう一度続行する場合は、ロールバックスクリプトを使用できます。詳しくは、「[オンプレミス ADM へのロールバック](#)」を参照してください。

### **ADM** サービスエージェントの設定

NetScaler ADC インスタンスと NetScaler ADM 間の通信を有効にするには、エージェントを構成する必要があります。デフォルトでは、NetScaler ADM エージェントは最新のビルドに自動的にアップグレードされます。エージェントをアップグレードする特定の時刻を選択することもできます。詳しくは、「[Agent のアップグレード設定の構成](#)」を参照してください。

- 既存のオンプレミス ADM (スタンドアロンまたは HA ペア) にオンプレミスエージェントが設定されていない場合は、ADM サービス用に少なくとも 1 つのエージェントを構成する必要があります。
- 既存のオンプレミス ADM (スタンドアロンまたは HA ペア) がマルチサイト展開用のオンプレミスエージェントで構成されている場合は、ADM サービスに対して同じ数のエージェントを構成する必要があります。

エージェントの設定について詳しくは、「[はじめに](#)」セクションを参照してください。

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

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

1. citrix.cloud.com にログオンする
2. [ホーム] アイコンをクリックし、[ID とアクセス管理] を選択します。
3. 「API アクセス」タブで、セキュア・クライアント名を入力し、「クライアントの作成」をクリックします。
4. ID とシークレットが生成されます。[ダウンロード] をクリックし、オンプレミスの ADM に CSV ファイルを保存します。

たとえば、CSV ファイルを /var ディレクトリに保存します。

## ADM サービスライセンスの検証

ADM サービスのライセンスを取得する必要があります。

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

注:

VIP ライセンスが小さい場合、仮想サーバーはランダムに選択され、ADM サービスの VIP レベルの構成が失敗します。

- ライセンスサーバーとして ADM オンプレミス展開を使用する場合は、移行前にライセンスを ADM Service に再割り当てします。詳細については、「[ADM サーバーをプールされたライセンスサーバーとしてのみ構成する](#)」および「[\[ライセンスファイルを再割り当てする方法\]\(https://support.citrix.com/article/CTX115870\)](#)」を参照してください。
- オンプレミスの ADM でプールされたライセンスを使用している場合は、ADM サービスのプールライセンスを取得し、ライセンスを ADC インスタンスに割り当てる必要があります。詳細については、「[プールライセンスの構成](#)」を参照してください。次のサポートされている ADC バージョンでは、ADM からのライセンス割り当てを変更できます。
  - NetScaler ADC SDX: 13.0 74.11 またはそれ以降のバージョン。
  - NetScaler ADC VPX および MPX: 13.0 47.24 以降、12.1 58.14 またはそれ以降のバージョン、および 11.1 65.10 以降のバージョン。

スクリプトを使用して移行する

- ADM 82.x ビルドを使用すると、機能を選択して移行できます。

- ADM 76.x 以降のビルドでは、移行スクリプト (`servicemigrationtool.py` および `config_collect_onprem.py`) をビルドの一部として利用できます (`cd /mps/scripts`を参照)。
- 76.x より前のビルドの ADM の場合は、移行スクリプトをダウンロードし、オンプレミス ADM でスクリプトをコピーする必要があります。

注

移行中は、オンプレミスの ADM にインターネット接続があることを確認します。

1. SSH クライアントを使用して、オンプレミスの ADM にログインします。

注

ADM HA ペアの場合は、プライマリノードにログインします。

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

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

```
bash-3.2# cd /var
bash-3.2# pwd
/var
bash-3.2# ls -ltr secureclient.csv
-rw-r--r-- 1 root nobody 102 Dec 11 19:09 secureclient.csv
bash-3.2#
```

注

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

4. ADM **13.0 82.xx** バージョンでは、以下のコマンドを実行して移行を完了します。

- a) `cd /mps/scripts`
- b) `python servicemigrationtool.py <path of ClientID/Secret File in on-premises Citrix ADM VM>`

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

移行スクリプトを実行すると、ツールには次のオプションが表示されます。

```

-----
Checking For Pre-requisites before we start the Migration
-----

The no.of Agents in ADM Service are :1

VIP licenses available in ADM Service are: 2

No.of Vservers Licensed in ADM on-prem are: 72

All the vServers licensed in ADM on-prem will not be licensed in ADM Service since licenses available in service is less.
vServers will be licensed randomly. Do you want to continue ? [Y|N] y

User has started rerunning the migration.Providing the all options

-----
Citrix ADM on-prem to ADM Service Configuration Migration.
The following menu enables you to select the components to migrate.
Type the number of the component that you want to migrate, and then press Enter.
For example, type 1 if you want to migrate Management and Monitoring(M&M).
-----

1. Management and Monitoring(M&M).
2. Analytics.
3. Stylebooks.
4. PooledLicensing.
5. All.

Select an option from 1 to 5 [1]: 1

```

指定した選択肢に基づいて、その機能のみが ADM サービスに移行されます。

この例では、オプション 1 が選択されています。管理と監視 (M&M) の移行が完了し、次のメッセージが表示されます。

```

1. Management and Monitoring Module Migration to ADM Service is Complete.
-----

ADCs,SDXs and SDWANMPs Addition and their SNMP,SysLog Configurations to ADM Service are Successful. Tool will now disable System Features in ADM on-prem

Device_Events : ['SUCCESS']
Device_SSL_Cert : ['SUCCESS']
Device_SysLog : ['SUCCESS']
Device_Backup : ['SUCCESS']
AgentCluster : ['SUCCESS']
Device_Perf_Reporting : ['SUCCESS']
Device_Config_Audit : ['SUCCESS']
Emon_Scheduler : ['SUCCESS']

Disable Status of ADM System Features: {'Device_Events': "['SUCCESS']", 'Device_SSL_Cert': "['SUCCESS']", 'Device_SysLog': "['SUCCESS']", 'Device_Backup': "['SUCCESS']", 'AgentCluster': "['SUCCESS']", 'Device_Perf_Reporting': "['SUCCESS']", 'Device_Config_Audit': "['SUCCESS']", 'Emon_Scheduler': "['SUCCESS']"}
1628286958

ADM on-prem to ADM service Migration is Successfully Completed.
-----

ADM On-prem to ADM Service Configuration Migration is Complete.
Note: Please look out for failures and re-trigger the Tool after taking appropriate action.
-----

```

管理および監視 (M&M) 機能には次のものが含まれます。

- ADC インスタンス、タグ、インスタンスグループ、プロファイル、カスタムアプリ、設定ジョブ、SNMP、syslog 設定。
- サイト、IP ブロック、ネットワークレポート、分析しきい値、通知設定、データブルーニング設定。
- 監査テンプレート、ポーリング間隔、イベントルール、および設定を構成します。
- RBAC グループ、ロール、ポリシー

アナリティクス機能には以下が含まれます。

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

注:

- 管理と監視 (M&M) 機能は、他の機能 (2、3、または 4) を選択した場合でも、自動的に移行されます。
- 一度に指定できるフィーチャは 1 つだけです。
- フィーチャのマイグレーションが完了した後、他のフィーチャを後でマイグレートする場合、すでにマイグレートされたフィーチャはリストに表示されません。たとえば、**Analytics** 機能の移行を先に完了した場合、次回移行スクリプトを実行すると、**StyleBook**、プールライセンス、およびすべてのオプションのみが表示されます。

5. ADM **13.0 76.xx** バージョンの場合は、次のコマンドを実行して移行を完了します。

- a) `cd /mps/scripts`
- b) `python servicemigrationtool.py <path of ClientID/Secret File in on-premises Citrix ADM VM>`

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

6. 13.0 76.xx より前のバージョンの ADM の場合:

- a) 次の場所から移行スクリプトをダウンロードします。

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

The downloaded file comprises two bundle scripts, `servicemigrationtool_27.py` and `config_collect_onprem_27.py`.

- b) 2 つのスクリプトをオンプレミス ADM に保存します。たとえば、`/var` ディレクトリに保存します
- c) 以下のコマンドを実行して移行します。

- i. `cd /var`
- ii. `servicemigrationtool_27.py <path of ClientID/Secret File in on-premises ADM VM>`

たとえば、`python servicemigrationtool_27.py /var/secureclient.csv`

スクリプトを実行した後、前提条件を確認し、移行を続行します。スクリプトでは、最初にライセンスの可用性がチェックされます。次のメッセージは、オンプレミスライセンスよりも低い ADM サービスライセンスがある場合にのみ表示されます。



```

bash-3.2# python servicemigrationtool.py /var/baga.csv
Trying to Get the Customer Id...

The Customer Id: iaahfc73d8f4
ADM Service FQDN: baga.adm.cloud.com
The ADM on-prem IP: 10.106.150.37

Citrix ADM Deployed with No Agents

-----
Checking For Pre-requisites before we start the Migration
-----

The no.of Agents in ADM Service are :1

VIP licenses available in ADM Service are: 2
No.of Vservers Licensed in ADM on-prem are: 26

All the vServers licensed in ADM on-prem will not be licensed in ADM Service since licenses available in service is less.
vServers will be licensed randomly. Do you want to continue ? [Y|N] █
    
```

[Y]を選択すると、VIP にランダムにライセンスが付与され、移行が続行されます。[N]を選択すると、スクリプトは移行を停止します。

プールされたライセンスサーバでサポートされていない ADC インスタンスバージョンがある場合は、次のメッセージが表示されます。

```

-----
Changing of PooledLicense Server will be effective for below SDX/ADC versions
-----
For SDX Versions: 13.0 74.11 Onwards
For ADC Versions: 13.0 47.24 and Onwards
                  12.1 58.14 and Onwards
                  11.1 65.10 and Onwards
-----

The List of ADCs supported for Pooled License Server change are:
['10.106.150.73', '10.102.60.25']

The List of SDXs supported for Pooled License Server change are:
[]

The List of ADCs not supported for Pooled License Server change are:
[]

The List of SDXs not supported for Pooled License Server chagne are:
['10.102.103.238']

Migration will change the License Server to ADM Service Agent.
Do you want to change License Server in all the supported Pooled ADCs/SDXs ? [Y|N] n

Do you want to continue with rest of the migration ? [Y|N] █
    
```

[Y]を選択すると、ライセンスサーバーを変更して移行処理が続行されます。[N]を選択すると、移行の残りの部分に進むかどうかを尋ねるプロンプトが表示されます。[N]を選択すると、スクリプトは移行を停止します。

オンプレミスの構成によっては、移行が完了するまでのおおよその時間は数分から数時間です。移行が完了すると、

次のメッセージが表示されます。

```
-----  
ADM OnPrem to ADM Service Configuration Migration is Complete.  
Note: Please Look out for Failures and re-trigger the Tool after taking appropriate action.  
-----
```

すべての ADC および SD-WAN WANOP インスタンスと、それぞれの構成が ADM サービスに移行されると、移行は成功します。移行が成功すると、オンプレミスの NetScaler ADM は次のインスタンスイベントの処理を停止します。

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

### オンプレミス **ADM** にロールバックする

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

#### 前提条件

オンプレミスの ADM (ADM サービスへの移行前) が以下の場合:

- プールライセンスサーバーとして使用し、オンプレミスの ADM に必要なプール済みライセンスがあることを確認します。
- オンプレミスの ADM エージェントで構成され、エージェントが「UP」状態で使用可能であることを確認します。

#### ロールバックスクリプトを使う

##### 注

ロールバック後、Analytics、SNMP、プールされたライセンスの同じ構成 (移行前) がオンプレミス ADM で再び利用可能になります。移行後にこれらの構成に変更を加えた場合、その変更はオンプレミスの ADM には反映されません。

- **ADM 82.xx** 以降のビルドでは、ロールバックスクリプトはビルドの一部として使用でき、`/mps/scripts` からアクセスできます。

- **79.xx** より前のビルドの **ADM** では、82.x ビルドにアップグレードしてロールバックスクリプトを使用するか、ロールバックスクリプトをダウンロードしてオンプレミス ADM でスクリプトをコピーできます。

1. SSH クライアントを使用して、オンプレミスの ADM にログインします。
2. shell と入力して Enter キーを押すと、bash モードに切り替わります。
3. ADM **13.0 82.xx** ビルドでは、以下のコマンドを実行してロールバックを完了します。

a) `cd /mps/script`

b) `python rollback_to_onprem.py <path of ClientID/Secret File in ADM on-prem VM>`

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

ツールによってロールバック操作が開始され、続行するかどうかを確認するプロンプトが表示されます。

**Y** と入力して続行します。

```
bash-3.2# python rollback_to_onprem.py /var/tmp/baga_prod.csv
The Customer Id: iaahfc73d8f4
ADM Service FQDN: baga.adm.cloud.com
The ADM on-prem IP: 10.186.158.10
-----
On successful rollback operation, Instances will be removed from ADM Service. SNMP, Syslog, Analytics configurations and Pooled Licensing Server in Instances will point to on-prem ADM Server and reports will be shown in ADM on-prem.
-----
Do you want to proceed for roll back operation from ADM Service to ADM on-prem ? [Y|N] y
-----
```

ロールバックが完了すると、次のメッセージが表示されます。

```
=====Rollback Status Check=====
Removal of ADCs, SDXs, SDWANOPs and their respective Configurations from ADM Service are Successful.
Rollback operation from ADM Service to ADM on-prem is Successful
Enabling System features in ADM on-prem Server
Device Events : ['SUCCESS']
Device SSL Cert : ['SUCCESS']
Device Syslog : ['SUCCESS']
Device Backup : ['SUCCESS']
AgentCluster : ['SUCCESS']
Device Perf Reporting : ['SUCCESS']
Device Config Audit : ['SUCCESS']
Emon Scheduler : ['SUCCESS']
-----
Enable Status of ADM System Features: {'Device Events': ['SUCCESS'], 'Device SSL Cert': ['SUCCESS'], 'Device Syslog': ['SUCCESS'], 'Device Backup': ['SUCCESS'], 'AgentCluster': ['SUCCESS'], 'Device Perf Reporting': ['SUCCESS'], 'Device Config Audit': ['SUCCESS'], 'Emon Scheduler': ['SUCCESS']}
-----
ADM Service to ADM on-prem Rollback operation is Complete.
Note: Please look out for failures and re-trigger the Tool after taking appropriate action.
-----
bash-3.2#
```

4. 82.xx より前のビルドの ADM の場合:

a) ロールバックスクリプトを次の場所からダウンロードします。

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

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

i. `cd /mps/scripts`

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

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

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

i. `cd /var`

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

たとえば、`python rollback_to_onprem_27.py /var/secureclient.csv`

ツールによってロールバック操作が開始され、続行するかどうかを確認するプロンプトが表示されます。**Y**と入力して続行します。

## よくある質問

February 6, 2024

### ADM サービス

**ADM** サービスエージェントはオプションのオンプレミスの **NetScaler ADM** エージェントと似ていますか

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

### ADM サービスが選ばれる理由

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

- オンプレミスの NetScaler ADM よりも簡単なオンボーディングと低い所有コストを備えたクラウドベースの SaaS 製品。
- 最新機能のアップデートにより、約 2 週間ごとにリリースが速くなります。
- アプリケーションのセキュリティ、パフォーマンス、使用状況に関する機械学習ベースの分析。

- ピーク時およびリーク期間分析、機械学習ベースのアプリケーションセキュリティ分析、WAF とボットのアプリケーションセキュリティ分析、アプリケーション CPU 分析など、現在 ADM サービスでのみサポートされているさまざまな機能。

NetScaler ADM サービスの月間ウェビナーに参加して、最新の製品機能とソリューションについて理解することもできます。次のリンクを使用して、ウェビナーに登録してください。

<https://attendee.gotowebinar.com/register/4248811314610265355>

または

<https://attendee.gotowebinar.com/register/1601431406507289611>

オンプレミスの **NetScaler ADM** が HA ペアである場合、移行後はどうなりますか

すべての構成が Citrix Cloud に移動されます。ディザスタリカバリノードを構成する必要はありません。

何らかの理由でエージェントがダウンした場合はどうなりますか

エージェントが起動して稼働するまで、データが失われる可能性があります。ただし、マルチサイト展開用の ADM エージェントを構成して、エージェントのフェールオーバーがある場合に継続性を確保することもできます。詳しくは、「[ADM エージェントをマルチサイト展開用に構成する](#)」を参照してください。

インスタンスバックアップも移行されていますか

バックアップは移行には含まれません。

履歴データも移行されますか

履歴データは移行されません。オンプレミスの ADM からデータをエクスポートできます。

オンプレミスのライセンスも移行されていますか

なしオンプレミスのライセンスファイルは、ADM サービスには使用できません。ADM サービスのライセンスを取得する必要があります。詳しくは、「[ライセンス](#)」を参照してください。オンプレミスの ADM でプールライセンスを使用している場合は、ADM サービスのプールライセンスを取得し、インスタンスにライセンスを割り当てる必要があります。

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

次の機能は ADM サービスに移行できません。

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

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

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

移行後、インスタンスのライセンスを取得するか、アナリティクスを有効にする必要がありますか

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

## 移行ツール

移行スクリプトの実行後、エラーメッセージが表示されます。何が問題になりますか

失敗理由を含むログファイルが表示されます。適切な修正アクションを実行し、移行スクリプトを再度実行できます。一般に、移行スクリプトを実行する前に、次のことを確認してください。

- ADM サービスエージェントの設定
- ADM サービスライセンスの取得
- クライアントとセキュアな CSV ファイルを格納した正しいパスをコピーします

**ADC** インスタンスのバージョンは、プールされたライセンスの制限よりも低いバージョンです。ライセンスサーバーを変更するために「**Y**」オプションを選択するとどうなりますか

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

移行スクリプトが **ADC/SD-WAN WANOP** インスタンスに関する設定に失敗した場合はどうなりますか

ADC および SD-WAN WANOP インスタンスは、オンプレミスの ADM セットアップで引き続き動作します。提案された失敗した理由から必要なアクションを実行し、移行スクリプトを再実行できます。

**ADC** または **SD-WAN WANOP** インスタンスのいくつかが **ADM** サービスに移行できなかった場合はどうなりますか。移行スクリプトの再実行は役に立ちますか

はい。スクリプトを再実行すると、失敗したインスタンスのみが移行されます。5つのインスタンスのうち2つが移動に失敗したと仮定します。修正アクションを実行し、移行スクリプトを再実行すると、以前に正常に移動された3つのインスタンスに「デバイスが既に存在します」というメッセージが表示されます。また、以前に失敗した他の2つのインスタンスは正常に移行されます。

移行ステータスを確認するログファイルはありますか

はい、`/var/mps/log/` ディレクトリ内にログファイルが生成されます。python3.7 の ADM `servicemigrationtool.py.log` はログファイルとして持ち、Python 2.7 の ADM はログファイルとして持っています `servicemigrationtool_27.py.log`。

移行スクリプトの実行中にセッションが終了した場合はどうなりますか

移行スクリプトを再実行できます。新しいセッションでは、前回のセッションからすでに追加したインスタンスが「デバイスは既に存在します」と表示され、移行はさらに続行されます。

**ADM** サービスのライセンス数がオンプレミスの **NetScaler ADM** よりも少ない場合に、移行スクリプトが開始された場合はどうなりますか

移行スクリプトの実行後、提案が表示され、ライセンスに関する言及が小さくなり、続行または停止するよう求められます。より少ないライセンスで続行する場合、仮想サーバは使用可能なライセンスからランダムにライセンスされます。

オンプレミスの **NetScaler ADM** を **ADM** サービスエクスプレスアカウントに移行するとどうなりますか

ADM サービスの Express アカウントには、2つの仮想サーバーライセンス、2つの StyleBook 構成パック、2つの構成ジョブしかありません。オンプレミスの ADM にこれらの構成を超える構成があり、Express Account を使用して移行を開始する場合、スクリプトでは Express アカウントに適用可能な上記の構成 (2つの仮想サーバーライセンス、2つの StyleBook 構成パック、2つの構成ジョブ) のみを移行できます。

**Citrix Cloud** 招待ユーザー（**Citrix Cloud** アカウントを作成した管理者ユーザー以外）がオンプレミスの **ADM** セットアップを移行しようとした場合はどうなりますか

管理者は、移行スクリプトを実行することを推奨します。招待されたユーザーには管理者権限 (`adminExceptSystem_Group`) がありません。その結果、グループ、ロール、ポリシーの移行が失敗し、「ユーザーにはアクセス許可がありません」というメッセージが表示されます。

解決策として、管理者（Citrix Cloud アカウントを作成した）は、招待されたユーザーに関連付けられたグループを「`admin_group`」として変更できます。

### ロールバックスクリプト

ロールバックスクリプトがオンプレミスの **ADM HA** ペアで使用された場合はどうなりますか

オンプレミスの ADM HA ペアは、移行前に使用可能だったすべての構成で復元されます。

ロールバックスクリプトを使用した後、ディザスタリカバリノードはどうなりますか

ディザスタリカバリノードも、移行前にすべての構成でリストアされます。

### トラブルシューティング

February 6, 2024

移行スクリプトを初めて実行すると、前提条件をチェックし、移行を続行します。すべての前提条件が満たされている場合、移行はエラーなしで完了します。前提条件のいずれかが失敗すると、スクリプトは理由とともにエラーメッセージを表示します。エラーを修正したら、スクリプトを再度実行する必要があります。

#### 注

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

- 移行スクリプトを 1 回以上実行し、一部の構成が既に ADM サービスに移行されている場合があります。
- 移行スクリプトを実行する前に、ADM サービスで同じ設定を手動で作成した可能性があります。

次のエラーメッセージの一部を参照してください。



手動プロファイルが **ADM** サービスに追加されました

```
=====Profiles Addition to ADM Service=====

60.26 : FAILURE : Profile 60.26 already exists

The list of ADC profiles added to ADM Service are :
{'60.26': "['FAILURE']"}
```

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

**ADM** サービスに追加された **NetScaler ADC** デバイス

```
=====ADC Device Addition=====

10.106.150.53 : FAILURE : Error in contacting Citrix ADC, invalid credentials.
10.102.60.26 : FAILURE :Device with this IP address already exists.

The list of ADCs added to ADM Service are:

['10.102.60.26']
```

回避策: オンプレミスの ADM で、インスタンスのステータスを確認し、問題なくインスタンスにアクセスできるかどうかを確認します。問題が解決しない場合は、問題を修正し、移行スクリプトを再実行します。

**StyleBook** カスタムテンプレートを **ADM** サービスにインポートする

```
=====Stylebook custom templates Import to ADM Service=====

neustar.citrix.adc.stylebooks_5_0_appfw-signature : FAILURE : There is an existing StyleBook with same namespace, version and name.
neustar.citrix.adc.stylebooks_5_0_customer-template : FAILURE : There is an existing StyleBook with same namespace, version and name.

Custom stylebooks import status is: {'neustar.citrix.adc.stylebooks_5_0_appfw-signature': 'FAILURE', 'neustar.citrix.adc.stylebooks_5_0_customer-template': 'FAILURE'}
=====Stylebook repository Addition to ADM Service=====
```

回避策: このエラーメッセージは、移行済みの StyleBook の例です。このエラーは、移行スクリプトを実行する前に、NetScaler ADM サービスで同じ名前、バージョン、名前空間の StyleBook を手動で作成した場合にも表示されます。



## すべての方法記事

February 6, 2024

NetScaler Application Delivery Management (NetScaler ADM) 「ハウツー記事」は、NetScaler ADM の機能に関するシンプルで関連性が高く、実装が簡単な記事です。これらの記事には、インスタンス管理、アプリケーション管理、StyleBook、証明書管理、分析など、NetScaler ADM 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すると、各機能のハウツー記事の一覧が表示されます。

トピック				
インスタンス管理	イベントの管理	StyleBook	証明書管理	NetScaler ADM システム
アプリケーション管理	構成管理	認証	分析	ネットワーク機能

### インスタンス管理

[グローバルに分散したサイトを監視する方法](#)

[NetScaler ADC インスタンスの管理パーティションを管理する方法](#)

[NetScaler ADM にインスタンスを追加する方法](#)

[NetScaler ADM でインスタンスグループを作成する方法](#)

[NetScaler ADM でジオマップ用のサイトを構成する方法](#)

[NetScaler ADM を使用してセカンダリの NetScaler ADC インスタンスにフェイルオーバーを強制する方法](#)

[NetScaler ADM を使用してセカンダリの NetScaler ADC インスタンスを強制的にセカンダリのままにする方法](#)

[NetScaler ADM を使用してインスタンスをバックアップおよび復元する方法](#)

[NetScaler ADM ダッシュボードを使用して HAProxy インスタンスを監視する方法](#)

[HAProxy インスタンスに設定されているフロントエンドの詳細を表示する方法](#)

[HAProxy インスタンスに設定されているバックエンドの詳細を表示する方法](#)

[HAProxy インスタンスに設定されているサーバーの詳細を表示する方法](#)

[NetScaler ADM から HAProxy インスタンスを再起動する方法](#)

[NetScaler ADM を使用して HAProxy インスタンスをバックアップおよび復元する方法](#)

[NetScaler ADM を使用して HAProxy 構成ファイルを編集する方法](#)

[複数の NetScaler ADC VPX インスタンスを再検出する方法](#)

[NetScaler ADM で NetScaler ADC インスタンスとエンティティをポーリングする方法](#)

[NetScaler ADM でインスタンスを管理解除する方法](#)

[NetScaler ADM からインスタンスへのルートをトレースする方法](#)

## 構成管理

[NetScaler ADM で構成ジョブを作成する方法](#)

[設定ジョブで SCP \(put\) コマンドを使用する方法](#)

[NetScaler ADM を使用して NetScaler ADC SDX インスタンスをアップグレードする方法](#)

[NetScaler ADM の組み込みテンプレートを使用して作成されたジョブをスケジュールする方法](#)

[NetScaler ADM で組み込みテンプレートを使用して構成されたジョブを再スケジュールする方法](#)

[実行した設定ジョブを再利用する方法](#)

[NetScaler ADM を使用して NetScaler ADC インスタンスをアップグレードする方法](#)

[NetScaler ADM の構成ジョブで変数を使用する方法](#)

[NetScaler ADM で構成テンプレートを使用して監査テンプレートを作成する方法](#)

[NetScaler ADM の修正コマンドから構成ジョブを作成する方法](#)

[NetScaler ADM 上のある NetScaler ADC インスタンスから、実行中および保存した構成コマンドを別の NetScaler ADC インスタンスに複製する方法](#)

[NetScaler ADM で Citrix SD-WAN WO インスタンスの構成ジョブを作成する方法](#)

[レコードアンドプレイを使用して構成ジョブを作成する方法](#)

[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](#)

[NetScaler ADM でマスター構成テンプレートを使用する方法](#)

[NetScaler ADC インスタンスの構成監査をポーリングする方法](#)

[設定ジョブで構成監査テンプレートを再利用する方法](#)

[設定テンプレートをインポートおよびエクスポートする方法](#)

[ConfigChange SNMP トラップの設定監査差分を生成する方法](#)

## 証明書管理機能

[NetScaler ADM でエンタープライズポリシーを構成する方法](#)

[NetScaler ADM から NetScaler ADC インスタンスに SSL 証明書をインストールする方法](#)

[インストールした証明書を NetScaler ADM から更新する方法](#)

[NetScaler ADM を使用して SSL 証明書をリンクおよびリンク解除する方法](#)

[NetScaler ADM を使用して証明書署名リクエスト（CSR）を作成する方法](#)

[NetScaler ADM から SSL 証明書の有効期限の通知を設定する方法](#)

[NetScaler ADM で SSL ダッシュボードを使用する方法](#)

[NetScaler ADC インスタンスから SSL 証明書をポーリングする方法](#)

## アプリケーション管理

[Citrix ADM でアプリケーション定義を作成する方法](#)

## StyleBook

[StyleBook のさまざまなグループを表示する方法](#)

[独自の StyleBook を作成する方法](#)

[NetScaler ADM でユーザー定義の StyleBook を使用する方法](#)

[API を使用して StyleBook から構成を作成する方法](#)

[StyleBook で定義された仮想サーバーで分析を有効にしてアラームを構成する方法](#)

[NetScaler ADM にファイルをアップロードするための StyleBook を作成する方法](#)

[API を使用して任意のファイルタイプをアップロードする構成を作成する方法](#)

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

[API を使用して証明書とキーファイルをアップロードする構成を作成する方法](#)

[Microsoft Skype for Business StyleBook を企業で使う方法](#)

[企業で Microsoft Exchange StyleBook を使用する方法](#)

[企業で Microsoft SharePoint StyleBook を使用する方法](#)

## 分析

[インスタンスで分析を有効にする方法](#)

[適応型しきい値の設定方法](#)

[SLA 管理の設定方法](#)

[分析用データベース要約の設定方法](#)

[NetScaler ADM を使用してしきい値とアラートを作成する方法](#)

[NetScaler ADM からの分析用の URL データ収集を無効にする方法](#)

[ストリーミングされる動画の種類とネットワークから消費されるデータ量を表示する方法](#)

[特定の時間枠のピークデータレートを表示する方法](#)

[ネットワークの効率を表示する方法](#)

## イベントの管理

[NetScaler ADM でイベントのイベント経過時間を設定する方法](#)

[NetScaler ADM を使用してイベントフィルターをスケジュールする方法](#)

[NetScaler ADM からのイベントの繰り返し電子メール通知を設定する方法](#)

[NetScaler ADM を使用してイベントを抑制する方法](#)

[イベントダッシュボードを使用してイベントを監視する方法](#)

[NetScaler ADM でイベントルールを作成する方法](#)

[NetScaler ADC 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 ADM でイベントの概要を表示する方法](#)

[NetScaler ADM で SNMP トラップのイベントの重大度とスキューを表示する方法](#)

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

[NetScaler ADM でシステムログメッセージを非表示にする方法](#)

[インスタンスイベントのプルーニング設定を構成する方法](#)

## 認証

[外部認証サーバーのフォールバックとカスケードを有効にする方法](#)

[RADIUS 認証サーバーを追加する方法](#)

[LDAP 認証サーバーを追加する方法](#)

[TACACS 認証サーバを追加する方法](#)

[NetScaler ADM で認証サーバーグループを抽出する方法](#)

[フォールバックローカル認証を有効にする方法](#)

## NetScaler ADM システム

[NetScaler ADM をアップグレードする方法](#)

[NetScaler ADM パスワードをリセットする方法](#)

[NetScaler ADM のテクニカルサポートファイルを生成する方法](#)

[単一サーバー展開で NetScaler ADM サーバーをバックアップおよび復元する方法](#)

[高可用性ペアの NetScaler ADM 構成をバックアップおよび復元する方法](#)

[NetScaler ADM でデフォルト以外のユーザーのシェルアクセスを有効にする方法](#)

[NetScaler ADM で NTP サーバーを構成する方法](#)

[NetScaler ADM の SSL 設定を構成する方法](#)

[NetScaler ADM のシステムログ消去間隔を構成する方法](#)

[NetScaler ADM の監査情報を表示する方法](#)

[NetScaler ADM のシステム通知設定を構成する方法](#)

[NetScaler ADM の CPU、メモリ、およびディスクの使用状況を監視する方法](#)

[NetScaler ADM の暗号グループを構成する方法](#)

[NetScaler ADM で SNMP トラップ、マネージャー、ユーザーを作成する方法](#)

[NetScaler ADM サーバーにホスト名を割り当てる方法](#)

[NetScaler ADM のシステムプルーニング設定を構成する方法](#)

[NetScaler ADM を使用してシステムバックアップ設定を構成する方法](#)

[NetScaler ADM でシステムアラームを構成および表示する方法](#)

## ネットワーク機能

[負荷分散エンティティのレポートを生成する方法](#)

[ネットワーク機能レポートのエクスポートまたはスケジュール設定方法](#)

## 概要

February 6, 2024

NetScaler Application Delivery Management (ADM) は、管理者が企業全体にわたって可視化し、複数のインスタンスで実行する必要がある管理ジョブを自動化することにより、運用を簡素化する一元管理ソリューション

ンです。NetScaler ADC MPX、NetScaler ADC VPX、NetScaler ADC SDX、NetScaler ADC CPX、NetScaler Gateway、Citrix SD-WAN などのアプリケーションネットワーク製品を管理および監視できます。ADM を使用すると、単一の統合コンソールから、グローバルなアプリケーション配信インフラストラクチャ全体を管理、監視、トラブルシューティングできます。

ADM は、Citrix Hypervisor、VMware ESXi、Linux KVM 上で動作する仮想アプライアンスです。ADM は、Web アプリケーショントラフィックと仮想デスクトップトラフィックに関する次の詳細情報を収集することで、アプリケーションの可視性の課題を解決します。

- ユーザー・セッション・レベルの情報
- Web ページのパフォーマンスデータ
- データベース情報は、お客様のサイトの ADC インスタンスを介して流れ、実用的なレポートを提供します。

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

## 機能とソリューション

February 6, 2024

NetScaler Application Delivery Management (ADM) には次の機能があります。

### アプリケーションの分析と管理

#### アプリケーション・パフォーマンス分析

App Score は、アプリケーションがどの程度適切に機能しているかを定義する、システムのスコア評価のための製品です。これは、アプリケーションが応答性の点でうまく動作しているかどうか、脅威に対して脆弱ではなく、すべてのシステムが稼働しているかどうかを示しています。

#### アプリケーション・セキュリティ分析

App Security ダッシュボードには、アプリケーションのセキュリティの全体的な状態が表示されます。たとえば、セキュリティ違反、シグネチャ違反、脅威指数などの、セキュリティの主要な測定基準が表示されます。App Security ダッシュボードには、検出された ADC インスタンスに対する SYN 攻撃、スモールウィンドウ攻撃、DNS フラッド攻撃などの攻撃関連情報も表示されます。

### ネットワーク

#### インスタンス



Citrix ADC、Citrix Gateway、Citrix SD-WAN、および HAProxy インスタンスを管理できます。

### インスタンスグループ

次のようにインスタンスをグループ化できます。

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

### イベントの管理

ADC インスタンスの IP アドレスが ADM に追加されると、NITRO 呼び出しが ADM によって送信され、インスタンスがそのトラップまたはイベントを受信するためのトラップ宛先として暗黙的に追加されます。

イベントは、管理対象の ADC インスタンスでのイベントまたはエラーの発生を表します。

### 証明書管理

NetScaler ADM では、証明書管理のあらゆる側面が合理化されるようになりました。1つのコンソールから、使われていない、または期限切れが近い証明書のタブは閉じたまま、正しい発行者、キーの強度、および正しいアルゴリズムを確保する自動化されたポリシーを作成することができます。ADM の SSL ダッシュボードとその機能を使用するには、SSL 証明書とは何か、および ADM を使用して SSL 証明書を追跡する方法を理解する必要があります。

### 構成管理

NetScaler ADM では、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、システムのアップグレード、その他のメンテナンス作業など、構成タスクの実行に役立つ構成ジョブを作成できます。設定ジョブとテンプレートを使用すると、最も繰り返しの多い管理タスクを ADM の 1 つのタスクに簡略化できます。

### 構成監査

インスタンスの構成を監視して、異常を特定できます。

- 構成のアドバイス：構成の異常を特定できます。
- 監査テンプレート：特定の構成における変更を監視できます。

### ネットワークレポート作成

ADM の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

#### Web Insight

企業の Web アプリケーションを可視化し、アプリケーションを統合的かつリアルタイムで監視することで、IT 管理者が NetScaler ADC が提供するすべての Web アプリケーションを監視できるようにします。Web Insight は、ユーザーとサーバーの応答時間などの重要な情報を提供し、IT 組織がアプリケーションパフォーマンスを監視、改善できるようにします。

### HDX Insight

NetScaler ADC を通過する ICA トラフィックをエンドツーエンドで可視化します。管理者は、HDX Insight を通じて、リアルタイムのクライアントとネットワークの遅延測定基準、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。

### Gateway Insight

ユーザーのログイン時に発生したエラーを、アクセスモードにかかわらず視覚化します。あらゆる期間を対象にして、ログオンしたユーザーの一覧を、アクティブユーザーの数、アクティブセッションの数、ユーザー全体によって使用されたバイト数とライセンス数の情報と共に確認できます。

### Security Insight

単一ペインのソリューションを提供し、アプリケーションのセキュリティ状態にアクセスしたり、アプリケーションを保護する修正アクションを実施したりするうえで役立ちます。

### SSL Insight

SSL Insight は、セキュアな Web トランザクション (HTTPS) を可視化し、IT 管理者は、セキュアな Web トランザクションのリアルタイムおよび履歴の統合監視を提供することで、NetScaler ADC 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ます。

### TCP Insight

TCP Insight は、ADC インスタンスで使用される最適化手法と輻輳制御戦略 (またはアルゴリズム) のメトリックを監視して、データ送信時のネットワークの輻輳を回避するための、簡単にスケーラブルなソリューションを提供します。

### Video Insight

Video Insight 機能は、NetScaler ADC インスタンスが使用するビデオ最適化手法の指標を監視するための簡単にスケーラブルなソリューションを提供し、顧客体験と運用効率を向上させます。

### WAN Insight

WAN Insight 分析により、管理者はデータセンターとブランチの WAN 最適化アプライアンスの間を流れる高速化および高速化されていない WAN トラフィックを簡単に監視できます。また、WAN Insight は、ネットワーク上のクライアント、アプリケーション、ブランチを可視化して、ネットワークの問題を効果的にトラブルシューティングできるようにします。

### オーケストレーション

#### クラウドオーケストレーション

NetScaler ADC 製品と OpenStack クラウドオーケストレーションを統合できます。NetScaler ADM と OpenStack は互いの API を実装しているため、NetScaler ADC インスタンスの負荷分散機能 (LBaaS) を OpenStack クラウドオーケストレーションと統合できます。

## オーケストレーション

NetScaler ADM は、さまざまなベンダーの SDN コントローラと統合することにより、エンタープライズネットワークで SDN をサポートします。ADM は、VMware NSX Manager と Cisco Application Policy Infrastructure Controller (APIC) の両方をサポートしています。

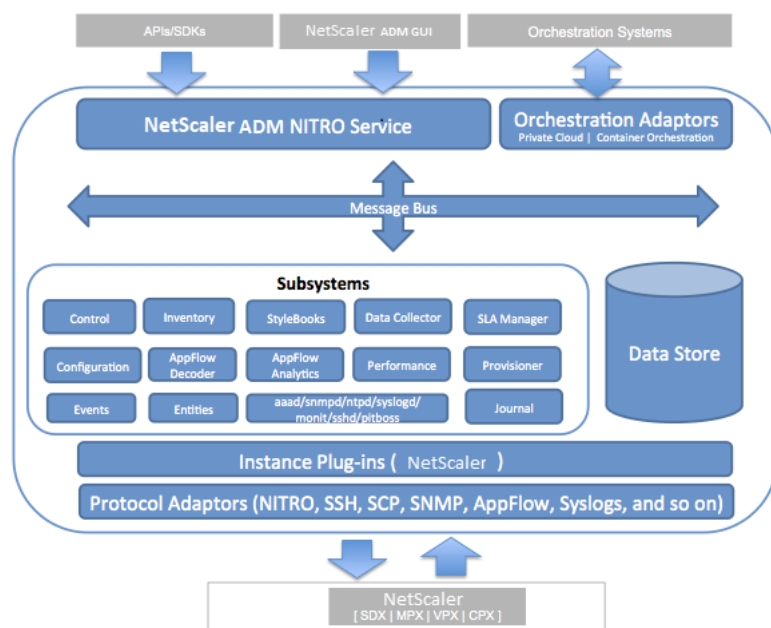
## アーキテクチャ

February 6, 2024

Citrix Application Delivery Management (ADM) データベースはサーバーと統合されており、サーバーはデータ収集や NITRO 呼び出しなどのすべての主要プロセスを管理します。サーバーは、そのデータストアに、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設定、証明書の詳細、インスタンスに設定されているエンティティなど、インスタンスの詳細のインベントリを格納します。単一サーバー展開は、処理するトラフィック量が少ない場合、またはデータを格納する期間が限られている場合に適しています。

現在、ADM は単一サーバーと高可用性という 2 種類のソフトウェア導入をサポートしています。

次の図は、ADM 内の異なるサブシステムと、ADM サーバーと管理対象インスタンス間の通信方法を示しています。



ADM の Service サブシステムは、ポート 80 および 443 を使用して、GUI または API から ADM 内のサブシステムに送信される HTTP 要求および応答を処理する Web サーバーとして機能します。これらの要求は、IPC (プロセス間通信) メカニズムを使用して、メッセージバス (メッセージ処理システム) を介してサブシステムに送信されます。要求は、情報の処理または適切なサブシステムへの送信を行うコントロールサブシステムに送信されます。その他のサブシステム (インベントリ、StyleBooks、データコレクタ、構成、AppFlow デコーダー、AppFlow Analytics、パ

パフォーマンス、イベント、エンティティ、SLA マネージャ、プロビジョニングツール、ジャーナルなど) には、特定の役割があります。

インスタンスプラグインは、ADM がサポートする各インスタンスタイプに固有の共有ライブラリです。情報は、NITRO 呼び出しを使用するか、SNMP、セキュアシェル (SSH)、またはセキュアコピー (SCP) プロトコルを介して ADM と管理対象インスタンスの間で転送されます。この情報は処理され、内部データベース (データストア) に格納されます。

## NetScaler ADM によるインスタンスの検出方法

February 6, 2024

インスタンスとは、NetScaler Application Delivery Management (ADM) から検出、管理、監視したい Citrix 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は、NetScaler ADM サーバーに追加する必要があります。次の Citrix アプライアンスと仮想アプライアンスを ADM に追加できます。

- NetScaler ADC インスタンス
  - Citrix MPX
  - Citrix VPX
  - Citrix SDX
  - Citrix CPX
  - Citrix BLX
- NetScaler Gateway インスタンス
- Citrix SD-WAN インスタンス

インスタンスは、NetScaler ADM サーバーの初回セットアップ時に追加することも、後で追加することもできます。

### 注

NetScaler ADM は、通信に ADC インスタンスの NetScaler ADC IP (NSIP) アドレスを使用します。ADM は、管理アクセスが有効になっているサブネット IP (SNIP) アドレスを持つ ADC インスタンスを検出することもできます。ADC インスタンスと ADM の間で開く必要のあるポートについては、「[ポート](#)」を参照してください。

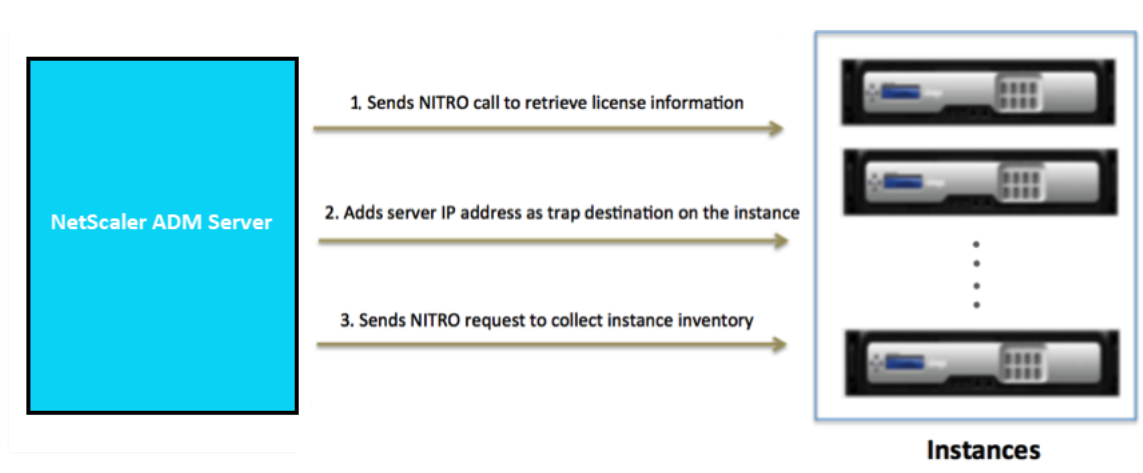
SNIP を使用して ADC HA ペアを追加する場合は、ADC HA ペアで独立ネットワーク構成 (INC) モードを有効にしてください。インスタンスの追加について詳しくは、「[インスタンスの追加](#)」を参照してください。

Citrix SD-WAN WO の場合、ADM はインスタンスの管理 IP アドレスを使用して通信します。

ADM に Citrix SD-WAN SE/PE インスタンスを追加することはできません。Citrix SD-WAN SE/PE アプリケーションで、ADM を AppFlow ow コレクタとして構成できます。

ADM サーバーにインスタンスを追加すると、サーバーはインスタンスのトラップ先として自身を暗黙的に追加し、インスタンスのインベントリを収集します。

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



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

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

Citrix SD-WAN WO インスタンスの場合、ADM はライセンス情報を使用してインスタンスを検出しません。インスタンスに NITRO リクエストを送信して、インスタンスタイプとバージョンを確認します。

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

#### 注

HTTP を使用すると、インスタンスにライセンスが設定されていない場合でも、すべてのインスタンスを ADM に追加できます。

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

この手順は、インスタンス上のトラップ先の数がトラップ先の上限值を超えると失敗します。インスタンスの上限は 20 です。

Citrix SD-WAN WO インスタンスの場合、ADM はその IP アドレスをインスタンスの SNMP マネージャーとして追加します。

3. ADM は、NITRO リクエストを送信して、インスタンスからインベントリを収集します。ホスト名、ソフトウェアバージョン、実行および保存された設定、証明書の詳細、インスタンスに設定されたエンティティなどのインスタンスの詳細を収集します。

この手順は、ネットワークまたはファイアウォールに関する問題があると失敗することがあります。

ADM にインスタンスを追加する方法については、[インスタンスの追加を参照してください](#)。

## ポーリングの概要

February 6, 2024

ポーリングは、Citrix Application Delivery Management (ADM) が Citrix ADC インスタンスから特定の情報を収集するプロセスです。世界中の組織に複数の NetScaler ADC インスタンスを構成している可能性があります。Citrix ADM を使用してインスタンスを監視するには、Citrix ADM は、すべての管理対象 ADC インスタンスから CPU 使用量、メモリ使用量、SSL 証明書、ライセンス機能、ライセンスタイプなどの特定の情報を収集する必要があります。ADM と管理対象インスタンスの間で発生するさまざまな種類のポーリングを次に示します。

- インスタンスポーリング
- インベントリのポーリング
- 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
- エンティティのポーリング

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

### **NetScaler ADM** が管理対象インスタンスおよびエンティティをポーリングする方法

NetScaler ADM は、デフォルトで定期的にポーリングを自動的に行います。NetScaler ADM では、いくつかのポーリングタイプのポーリング間隔を構成したり、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。

次の表は、ポーリングのタイプ、ポーリング間隔、使用されているプロトコルなどの詳細を示しています。

ポーリングタイプ	ポーリング間隔	ポーリングされた情報	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、ライセンスされた機能、モードなどのインベントリの詳細。	NITRO コールと SSH	いいえ
パフォーマンスデータ収集	5 分ごと (デフォルト)	ネットワークレポート情報	NITRO コール	いいえ
インスタンスバックアップポーリング	12 時間ごと (デフォルト)	管理されている ADC インスタンスの現在の状態のバックアップファイル	NITRO 呼び出し、SSH、および SCP。	はい。[ ネットワーク ] > [ インスタンス ] > [ **Citrix ADC ] に移動します。インスタンスを選択し、[ **Select Action ] リストから [ バックアップ/復元 ] をクリックします。
構成監査ポーリング	10 時間ごと (デフォルト)	ADC インスタンスで発生する構成変更 (実行中の構成と保存されている構成など)	SSH、SCP、および NITRO コール	はい。[ ネットワーク ] > [ 構成監査 ] に移動します。[ 構成監査 ] ページで、[ 設定 ] をクリックし、[ 構成監査ポーリング ] のポーリング間隔を構成します。

ポーリングタイプ	ポーリング間隔	ポーリングされた情報	使用プロトコル	ポーリング間隔の設定
SSL 証明書のポーリング	24 時間ごと (デフォルト)	NetScaler ADC 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	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直ちに NetScaler ADM に追加できます。これを行うには、[ ネットワーク ] > [ 構成の監査 ] に移動し、[ 今すぐポーリング ] をクリックします。[ <b>Poll Now</b> ] 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。はい。[ ネットワーク ] > [ <b>SSL</b> ダッシュボード ] に移動します。[ SSL ダッシュボード ] ページで、[ 設定 ] をクリックしてポーリング間隔を設定します。



ポーリングタイプ	ポーリング間隔	ポーリングされた情報	使用プロトコル	ポーリング間隔の設定
エンティティのポーリング	60 分ごと (デフォルト)	インスタンスに設定されているすべてのエンティティ。エンティティは、ADC インスタンスにアタッチされたポリシー、仮想サーバー、サービス、またはアクションのいずれかです。エンティティポーリングを有効にするには、 <a href="#">ADM 機能の有効化または無効化を参照してください</a> 。	NITRO 呼び出し	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直ちに NetScaler ADM に追加できます。これを行うには、[ネットワーク]>[SSL ダッシュボード]に移動し、[今すぐポーリング]をクリックします。[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。 はい。ただし、10 分未満に設定することはできません。設定するには、[ネットワーク]>[ネットワーク機能]に移動します。[ネットワーク機能] ページで、[設定]をクリックしてポーリング間隔を構成します。

ポーリングタイプ	ポーリング間隔	ポーリングされた情報	使用プロトコル	ポーリング間隔の設定
				エンティティを手動でポーリングし、インスタンスのすべてのエンティティを直ちに NetScaler ADM に追加できます。これを行うには、[ネットワーク]>[ネットワーク機能]に移動し、[今すぐポーリングする]をクリックします。[ <b>Poll Now</b> ] ページでは、ネットワーク内のすべてのインスタンスまたは選択したインスタンスをポーリングできます。

注:

ポーリングに加えて、管理対象 ADC インスタンスによって生成されたイベントは、インスタンスに送信された SNMP トラップを介して NetScaler ADM によって受信されます。たとえば、システム障害や構成の変更が発生したときにイベントが生成されます。

インスタンスのバックアップ中に、SSL ファイル、CA 証明書ファイル、ADC テンプレート、データベース情報などが NetScaler ADM にダウンロードされます。構成監査中は、ns.conf ファイルがダウンロードされてファイルシステムに格納されます。管理対象の NetScaler ADC 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 ADM が管理対象インスタンスで実行するさまざまなポーリング方法は次のとおりです。

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

### インスタンスのグローバルポーリング

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

### インスタンスの手動ポーリング

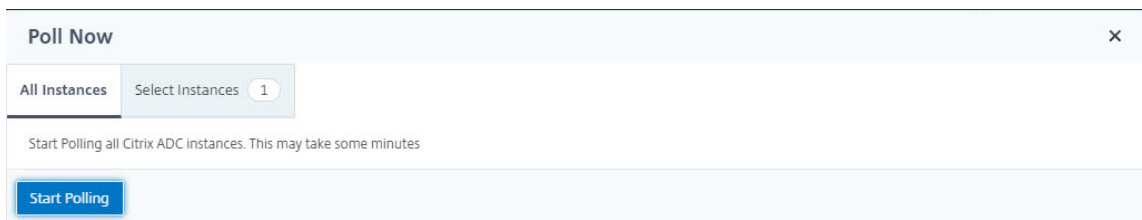
NetScaler ADM が多数のエントティティを管理している場合、ポーリングサイクルでレポートの生成に時間がかかり、画面が空白になったり、システムが以前のデータを表示したりする可能性があります。

NetScaler ADM には、自動ポーリングが行われない最小ポーリング間隔があります。新しい NetScaler ADC インスタンスを追加した場合、またはエントティティが更新された場合、NetScaler ADM は次のポーリングが行われるまで、新しいインスタンスまたはエントティティに加えられた更新を認識しません。また、さらに操作を行うために仮想 IP アドレスの一覧をすぐに取得する方法はありません。最短の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。手動でポーリングを実行して新しく追加されたインスタンスを検出することもできますが、これによって NetScaler ADC ネットワーク全体がポーリングされ、ネットワークに大きな負荷がかかります。NetScaler ADM では、ネットワーク全体をポーリングする代わりに、特定の時点で選択したインスタンスおよびエントティティのみをポーリングできるようになりました。

NetScaler ADM は、管理対象インスタンスを自動的にポーリングして、1 日の設定した時刻に情報を収集します。選択したポーリングにより、NetScaler ADM が選択したインスタンスにバインドされたエントティティの最新のステータスを表示するのに必要な更新時間を短縮できます。

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

1. NetScaler ADM で、[ ネットワーク ] > [ ネットワーク機能 ] に移動します。
2. [ ネットワーク機能 ] ページの右上隅にある [ 今すぐポーリングする ] をクリックします。
3. ポップアップページの「**Poll Now**」には、ネットワーク内のすべての NetScaler ADC 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を選択できます。
  - a) **All Instances** タブ- **Start Polling** をクリックしてすべてのインスタンスをポーリングします。
  - b) [ インスタンスを選択 ] タブ-リストからインスタンスを選択します。
4. [ ポーリングの開始 ] をクリックします。



Poll Now			
All Instances		Select Instances (14)	
Start Polling			
<input type="checkbox"/>	IP Address	Host Name	Instance State
<input checked="" type="checkbox"/>	10.106.150.55		● Up
<input checked="" type="checkbox"/>	10.102.205.34		● Up
<input checked="" type="checkbox"/>	10.102.29.200-TEST		● Up
<input checked="" type="checkbox"/>	10.102.29.160-10.102.29.165	NS	● Up
<input type="checkbox"/>	10.102.205.34-partition_10.102.205.34_admin_232232		● Up
<input type="checkbox"/>	10.102.205.27		● Up
<input type="checkbox"/>	10.102.29.200		● Up
<input type="checkbox"/>	10.106.118.120		● Up
<input type="checkbox"/>	10.102.205.27-p1		● Up

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

### エンティティの手動ポーリング

Citrix ADM では、特定のインスタンスにバインドされているいくつか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のステータスを知ることができます。このような場合、更新された 1 つのエンティティのステータスを知るために、インスタンス全体をポーリングする必要はありません。エンティティを選択してポーリングすると、NetScaler ADM はそのエンティティのみをポーリングし、NetScaler ADM GUI でステータスを更新します。

仮想サーバーがダウンしてい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状態が 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、正しい状態がすぐに GUI に表示されるようにしたい場合があります。

サービス、サービスグループ、負荷分散仮想サーバー、キャッシュ削減仮想サーバー、コンテンツスイッチング仮想サーバー、認証仮想サーバー、VPN 仮想サーバー、GSLB 仮想サーバー、およびアプリケーションサーバーをポーリングして、ステータスの更新を確認できるようになりました。

#### 注

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

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

例として、このタスクは負荷分散仮想サーバーのポーリングに役立ちます。同様に、他のネットワーク機能エンティティもポーリングできます。

1. Citrix ADM で、[ネットワーク] > [ネットワーク機能] > [負荷分散] > [仮想サーバー] に移動します。
2. 状態が DOWN と表示されている仮想サーバを選択し、[ **Poll Now** ] をクリックします。これで、仮想サーバーのステータスが UP に変わります。

Instance	Host Name	Name	Protocol	State	Effective State	Last State Change	
<input checked="" type="checkbox"/>	10.102.29.60	-NA-	asd234	HTTP	● Down	● DOWN	22 days, 02h : 53m
<input type="checkbox"/>	10.102.29.60	-NA-	asd229	HTTP	● Up	● Up	22 days, 02h : 53m
<input type="checkbox"/>	10.102.29.60	-NA-	asd11	HTTP	● Up	● Up	22 days, 02h : 53m
<input type="checkbox"/>	10.102.29.60	-NA-	asd165	HTTP	● Up	● Up	22 days, 02h : 53m
<input type="checkbox"/>	10.102.29.60	-NA-	asd158	HTTP	● Up	● Up	22 days, 02h : 53m
<input type="checkbox"/>	10.102.29.60	-NA-	sharepoint-application-test-audio-management-lb	HTTP	● Up	● Up	22 days, 02h : 53m
<input type="checkbox"/>	10.106.43.12	-NA-	lbv_test_entity_144.122.201.24	HTTP	● Up	● Up	03h : 04m : 31s
<input type="checkbox"/>	10.102.29.60	-NA-	asd178	HTTP	● Up	● Up	22 days, 02h : 53m
<input type="checkbox"/>	10.106.43.12	-NA-	lbv_test_entity_144.122.200.19	HTTP	● Down	● DOWN	03h : 04m : 31s
<input type="checkbox"/>	10.102.29.60	-NA-	asd82	HTTP	● Down	● DOWN	22 days, 02h : 53m

## データガバナンス

February 6, 2024

Citrix は、Citrix アプリケーションデリバリー管理 (ADM) 展開に関する統計情報を収集して、展開の使用状況と規模を把握します。統計には、オンプレミスの ADM 導入の状態、ステータス、および使用パターンが含まれます。この統計は、Citrix が ADM 展開上の問題をプロアクティブにトラブルシューティングするのに役立ちます。

- **Citrix Cloud** で顧客 ID を作成 -ADM の状態、ステータス、およびその他の指標に関する重要な統計情報を ADM オンプレミス展開から Citrix Cloud アカウントに送信します。

顧客 ID を作成した後、「クラウド接続」は、Citrix Cloud アカウントを作成して、オンプレミスと ADM サービスの間の接続を確立します。「顧客 ID の設定」を参照してください。

- メンテナンス・スクリプトの設定 -データベースを最適化します。データベースを最適化すると、テーブルの作成や列の変更などが行われる場合があります。メンテナンススクリプトの設定には、同じ「Cloud Connect」機能が使用されます。メンテナンススクリプトを使用したデータベースの最適化を参照してください。
- カスタマーユーザーエクスペリエンス向上プログラム (**CUXIP**) -このプログラムはデフォルトで有効になっています。Citrix ADM から使用状況データを収集します。このデータにより、ガイド付きワークフロー、検索記事、製品通知、フィードバック、アンケートなどを通じて ADM エクスペリエンスを最適化できます。「カスタマーユーザーエクスペリエンス向上プログラム」を参照してください。

## カスタマー ID の設定

Citrix Application Delivery Management (ADM) では、情報へのアクセスを開始する前に、ADM GUI で自分自身を認証する必要があります。ADM で自分自身を認証する前に、Citrix Cloud サービスに登録する必要があります。ADM GUI で Citrix Cloud ユーザー資格情報を指定します。詳しくは、「[Citrix Cloud へのサインアップ](#)」を参照してください。

NetScaler ADM で認証する方法はさまざまです。次のセクションでは、ADM の新規ユーザまたは既存のユーザである場合のワークフローについて説明します。

### ワークフロー 1-新規ユーザーの場合

1. 選択した Hypervisor への NetScaler ADM のインストールを完了します。
2. 必要な IP アドレスをさまざまに設定します。
3. Web ブラウザで、NetScaler ADM の IP アドレスを入力します。
4. **[User Name]** と **[Password]** の各フィールドに管理者の資格情報を入力します。  
  
[顧客 ID の設定] ページが開きます。このページでは、Citrix Cloud の資格情報を使用して自分自身を識別する必要があります。  
  
Citrix Cloud でアカウントを作成していない場合は、[\[Citrix Cloud\]](#) をクリックして登録します。
5. [認証] をクリックし、Citrix Cloud への登録に使用したメールアドレスを入力します。
6. [テレメトリ用データの共有に同意します] の横にあるチェックボックスを選択し、[送信] をクリックします。

### ワークフロー 2-既存のユーザーが最新の ADM バージョンにアップグレードする場合

1. Citrix ADM を最新バージョンにアップグレードした後、Web ブラウザで Citrix ADM IP アドレスを入力します。
2. **[User Name]** と **[Password]** の各フィールドに管理者の資格情報を入力します。
3. [顧客 ID の設定] ページが開きます。このページでは、Citrix Cloud の資格情報を使用して自分自身を識別する必要があります。  
  
Citrix Cloud でアカウントを作成していない場合は、[\[Citrix Cloud\]](#) をクリックして登録します。
4. [認証] をクリックし、Citrix Cloud への登録に使用したメールアドレスを入力します。
5. [テレメトリ用にデータを共有することに同意します] の横にあるチェックボックスをオンにし、[送信] をクリックします。

既存のユーザーとして、次の 2 つの方法のいずれかを使用して、後で ADM で ID を設定することもできます。

- [システム] > [システム管理] に移動し、[認証] をクリックします。
- ADM GUI の右上にある雲マークをクリックします。  
認証に成功すると、X は緑色のチェックマークに変わります。

#### 注:

次のドメインがホワイトリストに登録されていることを確認してください。

- \*.citrixnetworkapi.net
- \*.blob.core.windows.net

お客様のデータを NetScaler ADM にアップロードし、NetScaler ADM の機能を使用することにより、お客様は、Citrix 製品およびサービスに関する技術情報、ユーザー情報、または関連情報を Citrix が収集、保存、送信、保守、処理、および使用することに同意するものとします。

Citrix が受け取った情報は、常に [Citrix.com のプライバシーポリシー](#) に従って取り扱われます。

## 診断とデータ収集

Citrix ADM は、顧客 ID を使用して次のテレメトリを収集します。

- **ADM** で実行されるアクション:
  - Citrix ADM UI/API インターフェイスを使用して実行されるアクション。
  - Citrix ADM SDK インターフェイスを使用して実行されるアクション。
  - 1 日の操作数。この数には、API または UI からの GET 以外のリクエストが含まれます。
  - ADM によって行われた ADC アップグレードの数。
- **Citrix ADM** ライセンス情報: 資格のある仮想サーバーの数。
- 主な統計情報:
  - イベントルールの総数。
  - ユーザー定義 StyleBook の総数とユーザー定義 StyleBook。
  - 管理対象アプリケーションとカスタムアプリケーションの数。
  - 登録エージェントの数。
  - Citrix ADC 全体の全体的なスループット (Rx+Tx)。
  - 管理対象インスタンスの数。この数には管理パーティションも含まれます。
  - Citrix ADM SaaS を使用している管理者の数。
- **Citrix ADM** のジオロケーション
  - 展開情報: この情報には、高可用性、障害復旧、ADM エージェントなどの展開タイプが含まれます。

## なぜデータが収集されるのですか

収集されたテレメトリデータは次のことに役立ちます。

- Citrix ADM の正しいサイジングと展開を推奨します。
- ADM オンプレミス導入の問題を積極的にトラブルシューティングします。

### このデータを使用できるのは誰ですか？

収集された情報の唯一の所有者は Citrix です。Citrix は、お客様が自発的に提供した情報にアクセスしたり、収集したりします。この情報を第三者に販売または貸与することはありません。当社は、お客様のリクエストに応えるために必要な場合を除き、お客様の情報を組織外の第三者と共有することはありません。例: 注文を発送したり、問題を積極的に解決したりするため。

### お客様のデータをどのくらいの期間保管しますか

通常、ユーザーが当社のサービスを使用するまで、個人/使用状況データを保存します。あるいは、そうする別の目的があります。その後、法律で義務付けられているか許可されているか、内部報告や調整の目的で必要であるかぎり、データは保存されなくなります。

すべてのテレメトリデータは、13 か月または 396 日以内の期間保存されます。

### メンテナンススクリプトを使用したデータベースの最適化

メンテナンススクリプトは、ADM オンプレミス環境におけるデータベース関連の問題を解決するために使用されます。ADM ソフトウェアは、データベース保守スクリプトを ADM サービスから自動的にダウンロードし、データベース関連の問題を迅速に解決します。以前は、これらの問題は、スクリプトを手動で実行することで解決されました。

この機能を使用すると、ADM オンプレミス展開は、ADM Service からデータベースのメンテナンススクリプトを定期的にダウンロードします。そのためには、必ずカスタマー ID を設定してください。

メンテナンススクリプトは毎日および毎週実行されます。また、スクリプトでテーブルを作成したり、カラムを追加または削除したりして、データベースのパフォーマンスを向上させることもできます。

### カスタマー・ユーザー・エクスペリエンス向上プログラム

Citrix システムズの目的は、ユーザーに魅力的な製品体験を提供することです。カスタマーユーザーエクスペリエンス向上プログラム (**CUXIP**) では、**Pendo** を使用して検索記事やアプリ内ガイドなどを提供することで、一般的でありながら詳細なタスクをユーザーに案内しています。また、ユーザーが最近のすべての発表に遅れないように支援します。

### CUXIP ではどのような使用データが収集されますか？

使用状況データはすべてユーザーアクションに関するものです。イベントレベルのデータとも呼ばれる使用データには、ユーザーがウェブサイト上で訪問したページから特定の機能のクリック数まで、あらゆるものが含まれます。使用状況データは、ユーザーがアプリケーション内でどのように移動するかに関する貴重な情報です。このデータにより、ユーザーエクスペリエンスを最適化できます。

当社が収集する使用データの一部は次のとおりです。



- ページビューの詳細、各ページに費やされた時間。
- 訪問者 ID は、ページ上のユニークビジター数を識別するのに役立つ一意の匿名化された識別子です。
- アンケートの統計情報—スコア、ビュー、投稿数など。

### **CUXIP** はどのように役立ちますか

使用状況データを使用して、ADM の使い勝手を向上させます。以下は、お客様のユーザーエクスペリエンスを向上させることを意図しているいくつかの方法です。

- アプリ内のガイド付きワークフローと関連記事の検索機能。
- アプリ内からアンケートに参加して、製品の改善に役立ててください。
- 最近のお知らせやその他の通知について最新情報を入手してください。
- 製品チームに質問やフィードバックを投稿してください。

### **CUXIP** はどのように機能しますか?

Citrix ADM アプライアンスは内部ネットワークに配置できます。CUXIP のガイド付きアシスタンスを利用するには、ブラウザがインターネット接続されている必要があります。

### **ADM** で **CUXIP** を無効にするにはどうすればよいですか?

CUXIP を無効にするには、ADM GUI で次の手順を実行します。

1. **[System] > [System Administration]** の順に選択します。
2. **[CUXIP 設定]** で、CUXIP を無効にします。

### プライバシーポリシーの変更

プライバシーポリシーは随時更新される場合があります。このページに新しいプライバシーポリシーを掲載することにより、変更を通知します。変更が有効になる前に、電子メールまたはサービス上の目立つように通知し、このプライバシーポリシーの上部にある「発効日」を更新します。

変更がないか定期的に本プライバシーポリシーを確認することをお勧めします。本プライバシーポリシーの変更は、[Citrix プライバシーポリシーのページ](#)に掲載された時点で有効となります。

### 参照ドキュメント

Citrix のプライバシーポリシー: <https://www.citrix.com/about/legal/privacy/>

## ライセンス

February 6, 2024

NetScaler Application Delivery Management (ADM) では、NetScaler ADC インスタンスが <https> プロトコルで検出された場合、インスタンスを管理および監視するために、認証済みの NetScaler ADC ライセンスが必要です。

ライセンスがないインスタンスとエンティティを数に限りなく管理し、監視することができます。ただし、ライセンスを適用しなくても、アプリダッシュボードで検出された 30 のアプリケーションを管理し、30 台の仮想サーバーの分析データを表示することしかできません。検出されたアプリケーションが 30 台または仮想サーバーが 30 台を超える場合は、ライセンスを購入して適用する必要があります。

	NetScaler ADM 機能	[無料] 仮想サーバーの数に関係なく、Citrix ADM ライセンスは必要ありません	30 台以上の仮想サーバーには NetScaler ADM ライセンスが必要	NetScaler ADC ライセンス要件
分析	Web Insight	いいえ	はい	該当なし
	HDX Insight*	いいえ	はい	詳細 (レポート作成時間 1 時間以内) プレミアム (レポート作成時間 = 無制限)
	Security Insight	いいえ	はい	プレミアム (または) アドバンスド (App Firewall) ライセンス
	SSL Insight	いいえ	はい	該当なし
	Gateway Insight	いいえ	はい	詳細 (レポート作成時間 1 時間以内) プレミアム (レポート作成時間 = 無制限)
	TCP Insight	いいえ	はい	該当なし
	Video Insight	いいえ	はい	プレミアム (Citrix T 1000 シリーズ、VPX-T)

	NetScaler ADM 機能	[無料] 仮想サーバーの数に関係なく、Citrix ADM ライセンスは必要ありません	30 台以上の仮想サーバーには NetScaler ADM ライセンスが必要	NetScaler ADC ライセンス要件
	WAN Insight	いいえ	該当なし	Citrix SD-WAN インスタンス最適化エディション (WANOP) を使用する
アプリケーション	アプリケーション統計情報 (アプリダッシュボード、アプリセキュリティダッシュボード)	いいえ	はい	アプリダッシュボードとアプリセキュリティダッシュボードの NetScaler ADC Web App Firewall 関連情報には、Premium (または) App ファイアウォールのライセンスが必要です。
	StyleBook	はい	いいえ	該当なし
ネットワーク	ライセンスサーバー	はい	いいえ	該当なし
	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	はい	いいえ	該当なし
	イベント管理および syslog	はい	いいえ	該当なし
	構成ジョブ、構成監査、構成アドバイス	はい	いいえ	該当なし
	ネットワークレポート (インスタンスレベル)	はい	いいえ	該当なし

NetScaler ADM 機能	[無料] 仮想サーバーの数に関係なく、Citrix ADM ライセンスは必要ありません	30 台以上の仮想サーバーには NetScaler ADM ライセンスが必要	NetScaler ADC ライセンス要件
ネットワークレポート (仮想サーバーレベル)	はい	いいえ	該当なし
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、サーバーの可視性と管理)	はい	いいえ	該当なし
SSL 証明書管理、監視、ダッシュボード (インスタンスレベル)	はい	いいえ	該当なし
SSL 証明書ダッシュボード (仮想サーバーレベル)	はい	いいえ	該当なし
システム			
RBAC および外部認証 (インスタンスレベル)	はい	いいえ	該当なし
RBAC および外部認証	はい	いいえ	該当なし
オーケストレーション			
オープンスタック・インテグレーション	はい	いいえ	該当なし
VMware NSX インテグレーション	はい	いいえ	該当なし
Cisco APIC 統合	はい	いいえ	該当なし
コンテナ統合	はい	いいえ	該当なし
サードパーティ製ロードバランサー			

NetScaler ADM 機能	[無料] 仮想サーバーの数に関係なく、Citrix ADM ライセンスは必要ありません	30 台以上の仮想サーバーには NetScaler ADM ライセンスが必要	NetScaler ADC ライセンス要件
HAProxy: ホスト/インスタンス/バックエンド/サーバー/フロントエンドの可視性、設定のダウンロードまたはアップロード、およびアプライアンスの再起動。	はい	いいえ	該当なし
アプリダッシュボード	いいえ	はい (別途ライセンスが必要)	該当なし

\*Citrix Director を NetScaler ADM サポートと統合するには、Citrix Director にプレミアムライセンスが必要です。

より多くの仮想サーバーのライセンスは、10 個の仮想サーバーパックで提供されます。NetScaler ADM GUI を使用して、有効なライセンスを取得し、NetScaler ADM サーバーにライセンスを追加できます。

## 高可用性

NetScaler ADM サーバーには、VIP、CICO、およびプール容量ライセンスを含めることができます。ライセンスが ADM サーバに対して発行されると、ライセンスはサーバーのホスト ID にバインドされます。また、別の ADM サーバへのライセンスの割り当ては制限されます。

ADM 高可用性ペアをライセンスサーバとして設定する場合、プライマリサーバとセカンダリサーバに同じライセンスファイルが必要です。したがって、ADM の高可用性展開では、NetScaler ADM は両方のサーバーに同じライセンスファイルを割り当てることをサポートします。

### 注

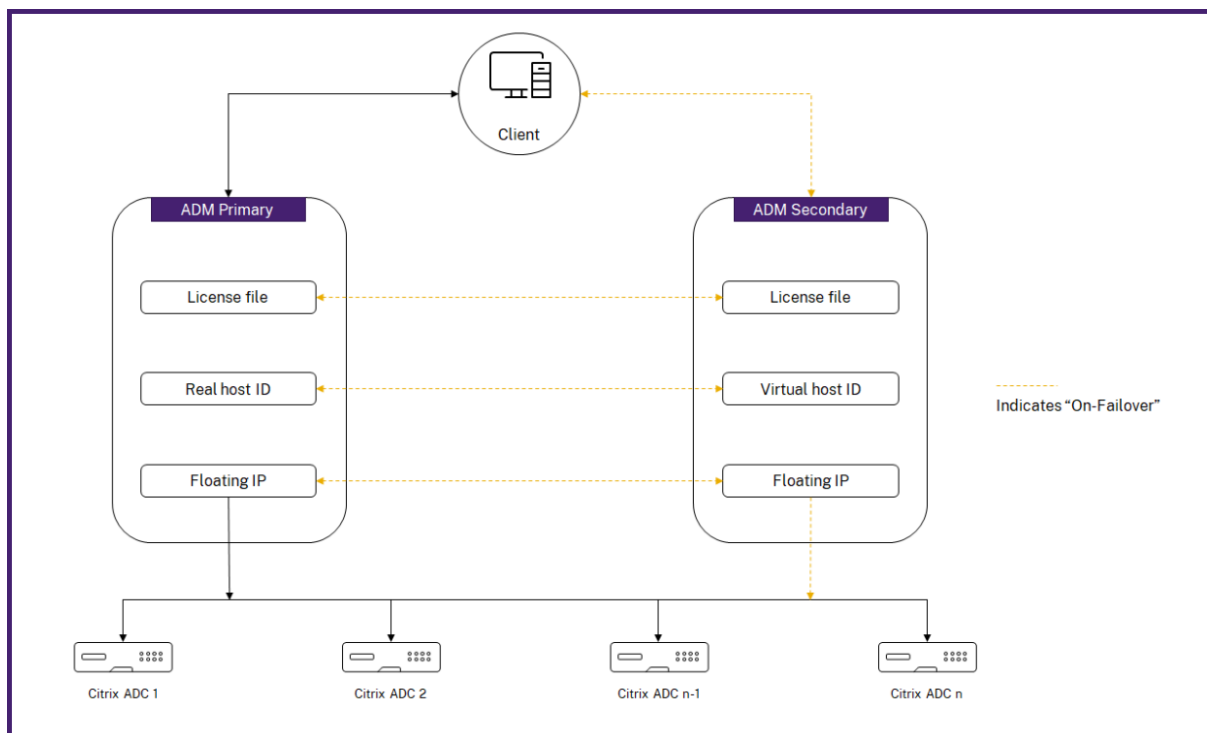
- NetScaler ADM 12.1.49.x 以前のリリースをインストールしている場合、セカンダリノードでライセンスを維持するために 30 日間の猶予期間があります。猶予期間の後、Citrix に連絡して元のライセンスを再ホストする必要があります。
- 12.1.50.x 以降のリリースでは、NetScaler ADM ライセンスは自動的にセカンダリノードに同期されません。

- プールされたライセンスは、12.1.50.x 以降のリリースからセカンダリノードに自動的に同期されます。

### ADM の高可用性ノード間でライセンスはどのように同期されますか

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

- 実際のホスト ID -この ID は、ADM サーバの MAC アドレスから生成されます。各 ADM スタンドアロン配置には、一意のホスト ID があります。
- 仮想ホスト ID : この ID は、高可用性の導入時に自動的に生成されます。ADM プライマリサーバの実際のホスト ID は、セカンダリサーバの仮想ホスト ID として使用されます。この ID は暗号化された形式で ADM データベースに格納され、この ID への変更は制限されます。仮想ホスト ID は、実際のホスト ID よりも優先されます。



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

1. ノード 1 で使用可能なライセンスファイルは、ノード 2 に同期されます。
2. ノード 1 の新しいライセンスファイルは、Node-2 に定期的に同期されます。
3. ADM は、ライセンス容量が 2 倍になるのを防ぐため、ライセンスサーバがノード 1 でのみ動作することを保証します。

4. NetScaler ADC インスタンスは、フローティング IP アドレスを使用してノード 1 からライセンスをチェックアウトします。

ライセンスは ADC インスタンスにロックされます。NetScaler ADM HA からライセンスをチェックアウトするには、インスタンスに特定のアプライアンスの IP アドレスが必要です。プライマリサーバーでライセンスを適用すると、そのライセンスが担当し、それ以降のすべてのライセンスがそのインスタンスに適用されます。ライセンスを削除できるのは、ライセンスをインストールしたサーバだけです。

### オーケストレーション

Orchestration モジュールは、ライセンス管理から独立しており、常に使用できます。

### 仮想サーバーライセンスをアップグレードする

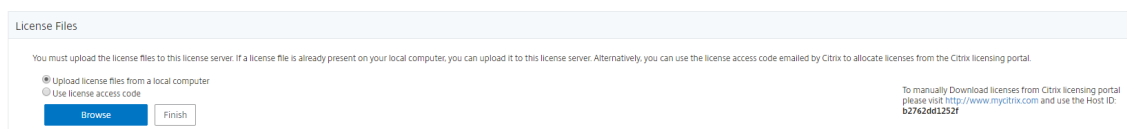
NetScaler ADM でライセンスをアップグレードして、NetScaler ADC アプライアンスでホストされているより多くの仮想サーバーを監視および管理できます。

アプライアンスライセンスをアップグレードするには:

1. 管理者の資格情報を使用して NetScaler ADM にログオンします。
2. [ネットワーク]>[ライセンス]>[設定] に移動します。
3. 詳細ペインで [ライセンスファイル] に移動し、次のオプションのいずれかを選択します。
  - ローカルコンピュータからライセンスファイルをアップロードします。ローカルコンピュータに既にライセンスが存在する場合は、「ブラウズ」をクリックし、ライセンスの割り当てに使用するライセンスファイル (.lic) を選択します。「完了」をクリックします。
  - ライセンスアクティベーションコードを使用します。Citrix は、購入したライセンスのライセンスアクセスコードを電子メールで送信します。テキストボックスにライセンスアクセスコードを入力し、[ **Get Licenses** ] をクリックします。

#### 注

このオプションを選択する場合は、NetScaler ADM がインターネットに接続されていないか、プロキシサーバーが使用可能である必要があります。



4. [ライセンス設定] ページからいつでもライセンスを追加できます。

License Files			
The following license files are present on this server. Select <b>Add New License</b> to upload more licenses. To delete a license, select the license and click <b>Delete</b> .			
<input type="button" value="Add New License"/> <input type="button" value="Apply Licenses"/> <input type="button" value="Delete"/> <input type="button" value="Download"/>			
<input type="checkbox"/>	Name	Last Modified	Size
<input type="checkbox"/>	CNS_VIPE_100CCS_RetailS_LaterSA.lic	2016-06-27 14:09:44	1.06 KB
<input type="checkbox"/>	CNS_VIPE_500CCS_RetailS.lic	2016-06-27 14:09:44	1.06 KB

## 確認

Citrix ADM にインストールされているライセンスを確認するには、[システム] > [ライセンスと分析] に移動します。

Licenses / System Licenses

System Licenses	
Allowed Virtual Servers 530	Total Managed Virtual Servers 169

## 仮想サーバの管理

NetScaler ADM を使用して管理および監視する仮想サーバーまたはサードパーティ仮想サーバーを選択できます。

### 注意事項

- デフォルトでは、NetScaler ADM は、仮想サーバーのポーリングサイクルごとに仮想サーバーのライセンスをランダムに自動的に付与します。
- NetScaler ADM で検出された仮想サーバーの総数が、インストールされている仮想サーバーライセンスの数よりも少ない場合、NetScaler ADM はデフォルトですべての仮想サーバーのライセンスを取得します。

仮想サーバーを手動で選択するかライセンスの割り当て対象を一部の仮想サーバーのみに制限するには、まず仮想サーバーへの自動ライセンス割り当てを無効化してから、管理する仮想サーバーを選択する必要があります。

### 仮想サーバーの自動ライセンス認証を無効にする

- [システム] > [ライセンスと分析] に移動します。

ダッシュボードには、使用可能な仮想サーバライセンス、管理対象仮想サーバ、および仮想サーバタイプ、およびライセンスの有効期限情報が表示されます。



2. 仮想サーバーライセンスの割り当てで、自動ライセンス仮想サーバーを無効にし、アドレス指定できない仮想サーバーを自動選択します。

### Virtual Server License Summary

Total Licensed	5
<div style="background-color: #00a651; height: 10px; width: 100%; margin-bottom: 2px;"></div> Load Balancing	5
<div style="background-color: #a6a6a6; height: 10px; width: 0%; margin-bottom: 2px;"></div> Content Switching	0
<div style="background-color: #a6a6a6; height: 10px; width: 0%; margin-bottom: 2px;"></div> Cache Redirection	0
<div style="background-color: #a6a6a6; height: 10px; width: 0%; margin-bottom: 2px;"></div> Authentication	0
<div style="background-color: #a6a6a6; height: 10px; width: 0%; margin-bottom: 2px;"></div> GSLB	0
<div style="background-color: #a6a6a6; height: 10px; width: 0%; margin-bottom: 2px;"></div> Citrix Gateway	0

Auto-select Virtual Servers  ON ⓘ

Auto-select non addressable Virtual Servers  ON ⓘ

[View All Virtual Servers](#)

#### ライセンスを取得するサードパーティ仮想サーバーの選択

1. [システム] > [ライセンスと分析] に移動します。  
 ダッシュボードには、使用可能な仮想サーバライセンス、管理対象仮想サーバ、および仮想サーバタイプ、およびライセンスの有効期限情報が表示されます。
2. [サードパーティ仮想サーバーの概要] で、[サードパーティ仮想サーバーの自動選択] を無効にします。

### Third Party Virtual Server Summary

Total Licensed	0
<div style="background-color: #00a651; height: 10px; width: 100%; margin-bottom: 2px;"></div> HAProxy Frontend	0

Auto-select Third Party Virtual Servers  OFF

[Configure License](#)

## 仮想サーバライセンスを手動で適用する

個々の仮想サーバにライセンスを手動で適用できます。

1. [仮想サーバライセンスの割り当て] で、[ライセンスの構成] を選択します。  
[すべての仮想サーバ] ページが表示されます。
2. プロパティを使用して、ライセンスされていない仮想サーバをフィルタリングします。 **Licensed: No**。
3. ライセンスを取得する仮想サーバを選択します。
4. [ライセンス] をクリックします。

## ポリシーベースの仮想サーバライセンスを構成する

仮想サーバにライセンスを適用するポリシーを設定できます。このポリシーは、自動ライセンスを取得する仮想サーバの数を制御します。また、選択したインスタンスの仮想サーバにのみライセンスが適用されます。

[ポリシーの編集] をクリックすると、次の項目を指定できます：

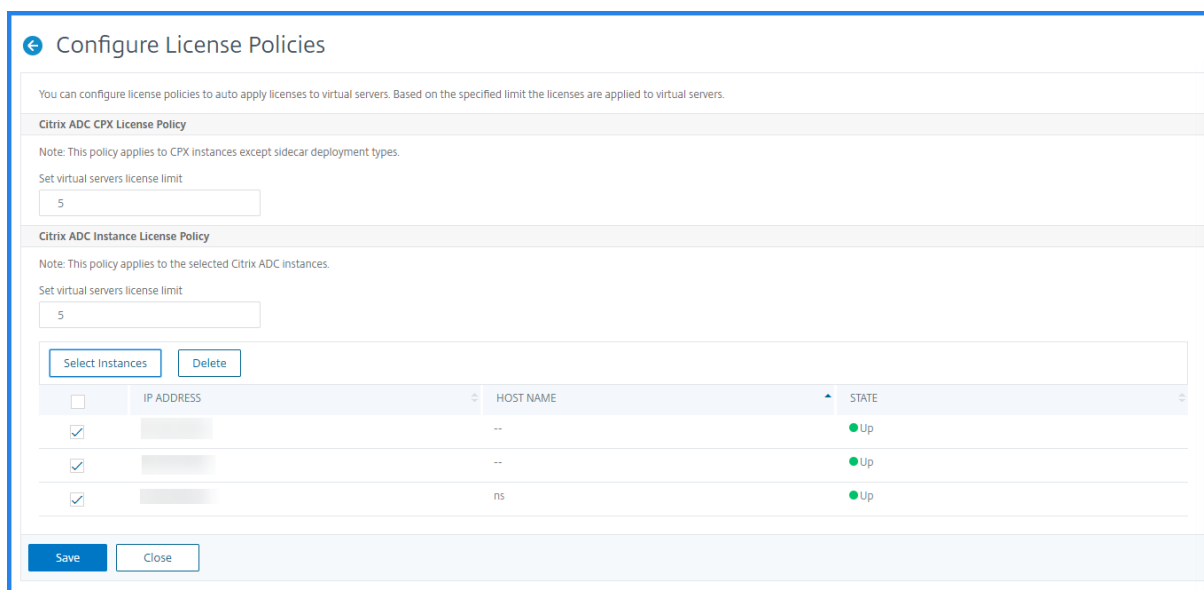
- CPX インスタンスに仮想サーバの制限を個別に設定して、ライセンスを適用します。ADM は、指定された制限まで CPX インスタンス上の仮想サーバにライセンスを適用します。

### 重要

：この制限は、サイドカーデプロイタイプを除く CPX インスタンスに適用されます。

サイドカーデプロイメントタイプの CPX インスタンスを表示するには、**License Type: Freely Managed** プロパティを使用して仮想サーバをフィルター処理します。

- ライセンスを適用するために、選択した ADC インスタンス (MPX/VPX/BLX) に仮想サーバの制限を設定します。ADM は、指定された制限まで ADC インスタンス上の仮想サーバにライセンスを適用します。
- 仮想サーバライセンスを適用する優先 ADC インスタンスを選択します。したがって、ADM は、選択したインスタンスの仮想サーバにのみライセンスを適用できます。



### ライセンスされた仮想サーバの表示

ライセンスが仮想サーバに適用されると、ライセンスされた仮想サーバまたはサードパーティの仮想サーバを **Licensing & Analytics** ページから表示できます。ライセンスされた仮想サーバを表示するには、以下を実行してください。

1. [システム] > [ライセンスと分析] に移動します。
2. 仮想サーバライセンスの 概要の [ライセンス合計] セクションで、仮想サーバタイプをクリックします。

### アドレス指定できない仮想サーバの自動ライセンスサポートを構成する

デフォルトでは、NetScaler ADM は、アドレス指定できない仮想サーバにライセンスを自動的に適用しません。アドレス指定不可の仮想サーバをライセンスする場合は、自動ライセンスオプションを無効にし、アドレス指定不可の仮想サーバを手動で選択する必要があります。これにより、ライセンスを適用するときに、アドレス指定不可能なサーバを最初に手動で選択する手間が増えます。また、ネットワークに追加されるたびに、アドレス指定不可能な新しい仮想サーバを手動で選択する必要があります。

NetScaler ADM には、NetScaler ADM の [仮想サーバライセンスの割り当て] のオプションがあります。アドレス指定不可仮想サーバの自動選択 オプションを有効にすると、アドレス指定不可仮想サーバのライセンスを自動的に適用します。

#### 注

- NetScaler ADM は、デフォルトでは、アドレス指定不可能な仮想サーバをライセンス用に自動的に選択しません。

- アプリケーション分析 (App Dashboard) は、ライセンスされたアドレス指定不可能な仮想サーバーで現在サポートされている唯一の分析です。

### 仮想サーバーライセンスの有効期限チェック

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

ライセンスのステータスを表示するには、次の手順に従います。

1. [ネットワーク]>[ライセンス]>[システムライセンス]に移動します。
2. [ライセンスの有効期限情報] セクションでは、有効期限が切れる予定のライセンスの詳細を確認できます。
  - **機能:** 有効期限が切れるライセンスのタイプ。
  - **数:** 影響を受ける仮想サーバーまたはインスタンスの数。
  - **Days to expiry:** 有効期限までに残されている日数。

ライセンスの通知設定を構成するには:

1. [ネットワーク]>[ライセンス]>[設定]に移動します。
2. [通知設定] セクションで、鉛筆アイコンをクリックし、パラメータを編集します。
  - **電子メールプロファイル:** ライセンスがしきい値に達したとき、または期限切れになったときに通知を送信するための電子メールプロファイルまたは配布リスト。
  - **SMS (テキストメッセージ):** ライセンスがしきい値に達したとき、または期限切れになったときに通知を送信するための SMS プロファイルまたは配布リスト。
  - **Slack -Slack** プロファイルの詳細を指定します。
  - **PagerDuty アラート -PagerDuty** プロファイルを指定します PagerDuty ポータルで構成された通知設定に基づいて、証明書の有効期限が近づくと通知が送信されます。
  - **通知する:** メールまたは **SMS** で管理者に通知するプールライセンスの割合を設定します。
  - **License Expiry Threshold:** [Alert Threshold] で設定した数のライセンスが期限切れになるまでの日数。
  - **ライセンスの有効期限:** 有効期限までの残り日数。

### システム要件

February 6, 2024

NetScaler Application Delivery Management (ADM) をインストールする前に、ソフトウェア要件、ブラウザ一要件、ポート情報、ライセンス情報、および制限について理解しておく必要があります。

## NetScaler ADM の要件

コンポーネント	条件
RAM	32 GB
仮想 CPU	8 基の CPU
記憶域	<p>注: Citrix ADM 展開では、ソリッドステートドライブ (SSD) テクノロジを使用することをお勧めします。</p> <p>必要なデフォルトのストレージ容量は 120 GB です。実際のストレージ要件は、NetScaler ADM のサイズ設定の見積もりによって異なります。[Citrix ADM HA 導入ガイドの「最大制限」セクション (7 ページ) に記載されている <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/adc/Citrix_ADM_HA_Deployment_Guide.pdf">サイジング計算ツール</a> を使用](<a href="https://www.citrix.com/content/dam/citrix/en_us/documents/adc/Citrix_ADM_HA_Deployment_Guide.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/adc/Citrix_ADM_HA_Deployment_Guide.pdf</a>) してください。このガイドは、<a href="#">ダウンロードサイトの [NetScaler MAS リリース 12.1] &gt; [以前のバージョン]</a> から入手できます。注: 展開ガイドとサイジング計算ツールにアクセスするには、Citrix アカウントが必要です。</p> <p>NetScaler ADM ストレージ要件が 120GB を超える場合は、追加のディスクを接続する必要があります。追加できるディスクは 1 つだけです。</p> <p>初期展開の時点で、記憶域を見積もり、追加のディスクを接続することをお勧めします。</p> <p>詳しくは、「<a href="#">NetScaler ADM に追加のディスクを接続する方法</a>」を参照してください。</p>
仮想ネットワークインターフェイス	1
スループット	1Gbps または 100Mbps

### 注

NetScaler ADM は AMD チップセットではサポートされていません。

## NetScaler ADM オンプレミスエージェントの要件

コンポーネント	条件
RAM	32 GB
仮想 CPU	8 基の CPU
記憶域	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	1Gbps

注

NetScaler ADM エージェントは、AMD チップセットではサポートされていません。

### NetScaler ADM 機能に必要な最低限の NetScaler ADC バージョン

重要

NetScaler ADM のバージョンとビルドは、NetScaler ADC のバージョンおよび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 ADM 12.1 ビルド 50.39 をインストールしている場合は、NetScaler ADC 12.1 ビルド 50.28/50.31 以前がインストールされていることを確認します。

NetScaler ADM 機能	NetScaler ADC ソフトウェアのバージョン
StyleBook	10.5 以降
OpenStack/CloudStack のサポート	11.0 以降 (パーティションが必要な場合) 11.1 以降 (共有仮想 LAN 上のパーティションが必要な場合)
NSX のサポート	11.1 Build 47.14 以降 (VPX)
Mesos/Marathon のサポート	10.5 以降
バックアップ/復元	NetScaler ADC、10.1 以降の場合 Citrix SDX の場合、11.0 以降
ジョブを使用した監視/レポート作成および構成	10.1 以降
分析機能	
Web Insight	10.5 以降
HDX Insight	10.1 以降
Security Insight	11.0.65.31 以降

NetScaler ADM 機能	NetScaler ADC ソフトウェアのバージョン
Gateway Insight	11.0.65.31 以降
Cache Insight	10.5 以降 *
SSL Insight	12.0 以降

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

### Citrix SD-WAN インスタンス管理の要件

#### Citrix SD-WAN プラットフォームのエディション/バージョンと NetScaler ADM 機能の相互運用性マトリックス

プラットフォーム・ Edition	Citrix SD-WAN WANOP	Citrix SD-WAN SE	Citrix SD-WAN PE
検出中	はい	はい	はい
構成	はい	いいえ	いいえ
監視	はい	いいえ	いいえ
レポート (ネットワークレ ポート)	はい	いいえ	いいえ
イベント管理	はい	いいえ	いいえ
<b>HDX Insight</b>	はい	いいえ	いいえ
<b>WAN Insight</b>	はい	いいえ	いいえ
<b>HDX Insight</b> (マルチホ ップ展開)	はい	はい	いいえ

### Citrix SD-WAN インスタンスでサポートされるシンククライアント

NetScaler ADM は、Citrix SD-WAN 展開を監視するために、次のシンククライアントをサポートしています。

- Dell Wyse WTOS モデル R10L Rx0L シンククライアント
- NComputing N400
- Dell Wyse WTOS Model CX0 C00X Xenith
- Dell Wyse WTOS Model TXO T00X Xenith2

- Dell Wyse WTOS Model CX0 C10LE
- Dell Wyse WTOS モデル R00LX Rx0L HDX シンククライアント
- Dell Wyse 拡張 SUSE Linux エンタープライズ、モデル Dx0D、D50D
- Dell Wyse ZX0 Z90D7 (WES7) シンククライアント

## NetScaler ADM 分析の要件

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

---

NetScaler ADM 機能	Citrix Virtual Apps and Desktops バージョン
HDX Insight	Citrix Virtual Apps and Desktops 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 としてブランド化されています）は、NetScaler ADC インスタンスで使用できる必要があります。NetScaler ADM では、スタンドアロンの Access Gateway Standard アプライアンスはサポートされません。

NetScaler ADM では、Citrix Virtual Apps または Citrix Virtual Desktops で公開され Citrix Receiver から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、Receiver がインストールされているオペレーティングシステムの制約を受けます。現在、NetScaler ADC は、iOS または Android オペレーティングシステム上で動作する Citrix Receiver を介してアクセスされるアプリケーションやデスクトップの ICA トラフィックを解析しません。

### HDX Insight でサポートされているシンククライアント

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



**HDX** インサイトには **NetScaler ADC** インスタンスライセンスが必要

NetScaler ADM for HDX Insight によって収集されるデータは、監視対象の NetScaler ADC インスタンスのバージョンとライセンスによって異なります。HDX Insight レポートは、リリース 10.5 以降を実行している NetScaler ADC Premium および Advanced アプライアンスのみに表示されます。

NetScaler ADC ライセンス/期間	5 分	1 時間	1 日	1 週間	1 か月超
Standard	いいえ	いいえ	いいえ	いいえ	いいえ
詳細設定	はい	はい	いいえ	いいえ	いいえ
Premium	はい	はい	はい	はい	はい

サポートされるハイパーバイザー

次の表は、NetScaler ADM でサポートされているハイパーバイザーの一覧です。

ハイパーバイザー	バージョン
Citrix Hypervisor	7.1 と 7.4
VMware ESX	6.0、6.5、6.7、および 7.0
Microsoft Hyper-V	2012 R2 および 2016
汎用 KVM	RHEL 7.4 and Ubuntu 16.04

サポートされているオペレーティングシステムとレシーバのバージョン

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

オペレーティングシステム	Receiver のバージョン
Windows	4.0 Standard Edition
Linux	13.0.265571 およびそれ以降
Mac	11.8、Build 238301 以降
HTML5	1.5*

---

オペレーティングシステム	Receiver のバージョン
Chrome アプリ	1.5*

---

\* Citrix CloudBridge (Citrix SD-WAN WANOP) リリース 7.4 以降に適用されます。

### サポートされているブラウザ

次の表は、NetScaler ADM でサポートされている Web ブラウザーの一覧です。

---

ウェブブラウザ	バージョン
Microsoft Edge	79 以降
Google Chrome	51 以降
Safari	10 以降
Mozilla Firefox	52 以降

---

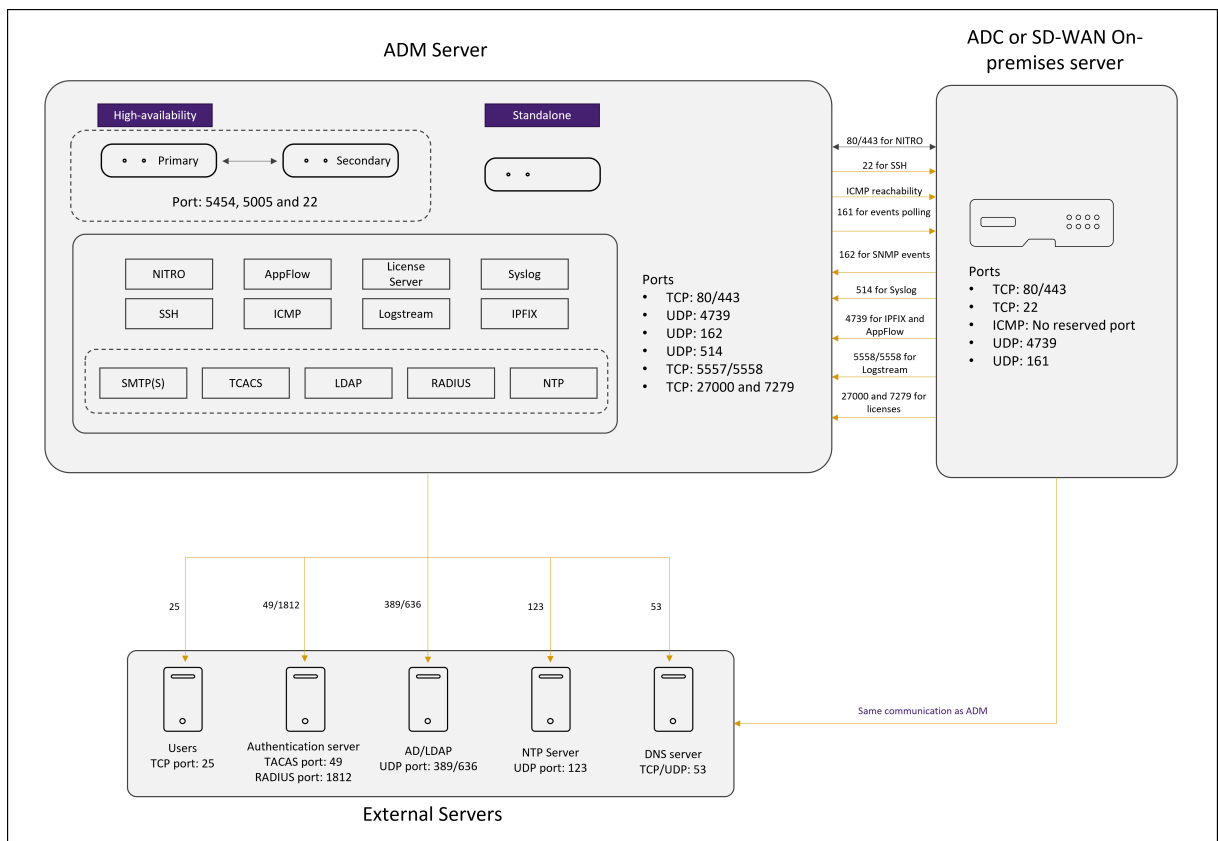
### サポートされるポート

NetScaler ADM は、NetScaler ADC IP (NSIP と呼ばれる) アドレスを使用して NetScaler ADC と通信します。ADM エージェントは、ADC インスタンスと ADM または SD-WAN インスタンスと ADM の間の中間として使用できます。これらのサーバーとの通信を確立するには、必要なポートを開きます。

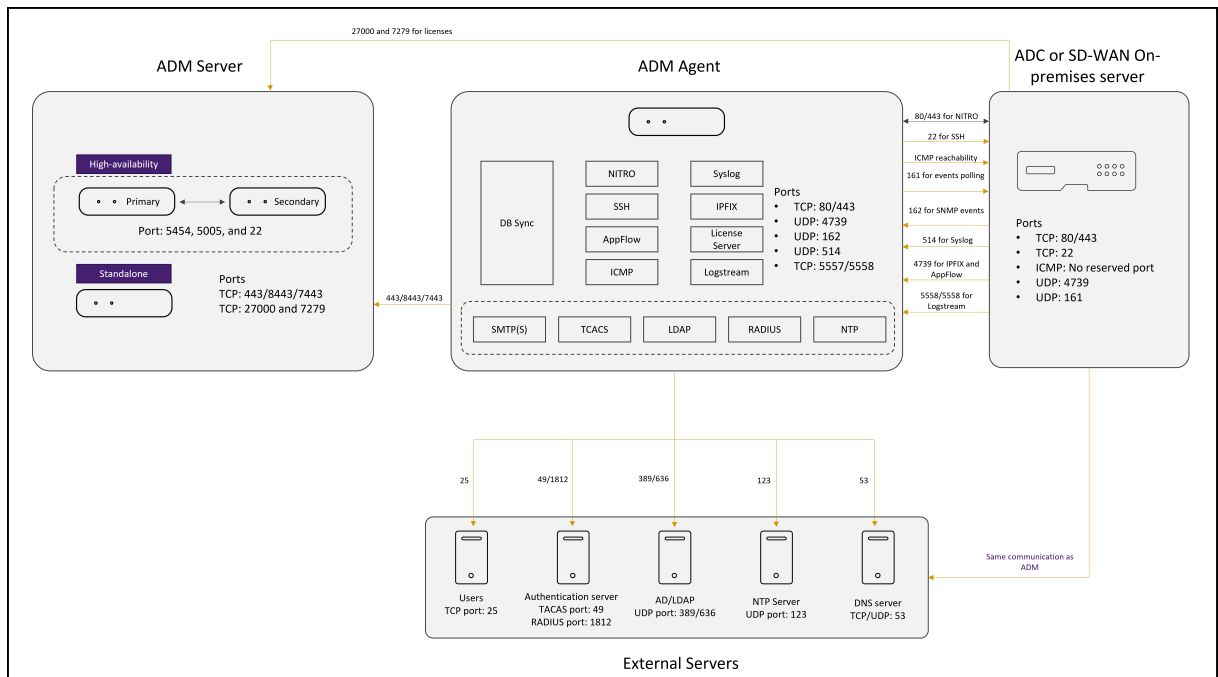
#### 注

Citrix ADC を高可用性モードで構成した場合、Citrix ADM は Citrix ADC サブネット IP (管理 SNIP) アドレスを使用して Citrix ADC と通信します。SNIP を使用して NetScaler ADM と通信する場合、必要なポートは同じままです。

エージェントレス展開のネットワークポート図:



**ADM エージェントを含む展開のネットワークポート図:**



次の項では、必要なポートとその目的について説明します。

- ADM サーバ

- ADM エージェント
- ADC または SD-WAN インスタンス
- 外部サーバ

### ADM サーバのポート

この表は、ADM サーバで開く必要のある必須ポートを示しています。

ポート	種類	詳細	コミュニケーションの方向
5454 と 22	TCP	高可用性モードの NetScaler ADM ノード間の通信およびデータベース同期用のデフォルトポート。	NetScaler ADM プライマリノードから NetScaler ADM セカンダリノードへ
443/8443/7443	TCP	NetScaler ADM エージェントと NetScaler ADM 間の通信用のポート。	NetScaler ADM エージェントが NetScaler ADM との通信を開始します。次に、Citrix ADM とエージェントは相互に対話します。

ADM および ADC インスタンスが通信にエージェントを使用していない場合は、必ず ADM サーバで次のポートを開きます。

ポート	種類	詳細	コミュニケーションの方向
80/443	TCP	NetScaler ADM から NetScaler ADC または Citrix SD-WAN インスタンスへの NITRO 通信用。	NetScaler ADM エージェントから NetScaler ADC に、NetScaler ADC から NetScaler ADM エージェントへの Citrix
4739	UDP	NetScaler ADC または Citrix SD-WAN インスタンスから NetScaler ADM への AppFlow ow 通信の場合。	NetScaler ADC または Citrix SD-WAN から NetScaler ADM エージェントへ

ポート	種類	詳細	コミュニケーションの方向
162	UDP	NetScaler ADC インスタンスから NetScaler ADM に SNMP イベントを受信する。	NetScaler ADC から NetScaler ADM エージェントへ
514	UDP	NetScaler ADC または Citrix SD-WAN インスタンスから NetScaler ADM への syslog メッセージを受信する。	NetScaler ADC または Citrix SD-WAN から NetScaler ADM エージェントへ
5557/5558	TCP	Citrix ADC から Citrix ADM へのログストリーム通信 (Security Insight、Web Insight、HDX Insight 用)。	NetScaler ADC から NetScaler ADM へ
5005	TCP	HA ノード間でハートビートを交換するためのポート。	NetScaler ADM プライマリノードからセカンダリノードへ。NetScaler ADM セカンダリノードからプライマリノードへ。

#### ADM エージェントのポート

この表は、ADM エージェント上で開く必要がある必須ポートを示しています。

ポート	種類	詳細	コミュニケーションの方向
80/443	TCP	NetScaler ADM から NetScaler ADC または Citrix SD-WAN インスタンスへの NITRO 通信用。	NetScaler ADM エージェントから NetScaler ADC に、NetScaler ADC から NetScaler ADM エージェントへの Citrix
4739	UDP	NetScaler ADC または Citrix SD-WAN インスタンスから NetScaler ADM への AppFlow ow 通信の場合。	NetScaler ADC または Citrix SD-WAN から NetScaler ADM エージェントへ

ポート	種類	詳細	コミュニケーションの方向
162	UDP	NetScaler ADC インスタンスから NetScaler ADM に SNMP イベントを受信する。	NetScaler ADC から NetScaler ADM エージェントへ
514	UDP	NetScaler ADC または Citrix SD-WAN インスタンスから NetScaler ADM への syslog メッセージを受信する。	NetScaler ADC または Citrix SD-WAN から NetScaler ADM エージェントへ
5557/5558	TCP	Citrix ADC から Citrix ADM へのログストリーム通信 (Security Insight、Web Insight、HDX Insight 用)。	NetScaler ADC から NetScaler ADM へ

#### ADC および SD-WAN インスタンス用のポート

次の表では、NetScaler ADC および SD-WAN インスタンスで開く必要がある必須ポートについて説明します。

ポート	種類	詳細	コミュニケーションの方向
80/443	TCP	NetScaler ADM から NetScaler ADC または Citrix SD-WAN インスタンスへの NITRO 通信用です。443。高可用性モードの NetScaler ADM サーバー間の NITRO 通信用。	NetScaler ADM から NetScaler ADC へ、NetScaler ADC から NetScaler ADM へ

ポート	種類	詳細	コミュニケーションの方向
22	TCP	NetScaler ADM から NetScaler ADC または Citrix SD-WAN インスタンスへの SSH 通信用です。高可用性モードで展開された NetScaler ADM サーバー間の同期用。また、このポートは、ADM エージェントと NetScaler ADC 間の SSH 通信に必要です。	NetScaler ADM から NetScaler ADC へ。または、NetScaler ADC への NetScaler ADM エージェント。
予約されているポートなし	ICMP	高可用性モードで展開された NetScaler ADM と NetScaler ADC インスタンス、SD WAN インスタンス、またはセカンダリ NetScaler ADM サーバー間のネットワーク到達可能性を検出するため。	NetScaler ADM から NetScaler ADC へ
161	UDP	ADC インスタンスからイベントをポーリングする。	NetScaler ADM から NetScaler ADC へ

注:

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

外部サーバーのポート

次の表では、外部サーバで開く必要がある必須ポートについて説明します。

ポート	種類	詳細	コミュニケーションの方向
25	TCP	NetScaler ADM からユーザーに SMTP 通知を送信する場合。	ユーザーへの NetScaler ADM。
389/636	TCP	認証プロトコルのデフォルトポートです。NetScaler ADM と LDAP 外部認証サーバー間の通信用。	NetScaler ADM から LDAP 外部認証サーバーへ

ポート	種類	詳細	コミュニケーションの方向
123	UDP	のデフォルト NTP サーバポート。複数のタイムゾーンと同期しています。	NTP サーバへの NetScaler ADM
1812	RADIUS	認証プロトコルのデフォルトポートです。NetScaler ADM と RADIUS 外部認証サーバー間の通信用。	NetScaler ADM から RADIUS 外部認証サーバーへ
49	TACACS	認証プロトコルのデフォルトポートです。NetScaler ADM と TACACS 外部認証サーバー間の通信用。	NetScaler ADM から TACACS 外部認証サーバーへ

#### 制限事項

NetScaler ADM 12.1 以降では、次の機能が IPv6 形式の IP アドレスをサポートします。

1. NetScaler ADM GUI の管理アクセス
2. NetScaler ADC の管理アクセス
3. 登録とインベントリ
4. ネットワークダッシュボード
5. SSL ダッシュボード
6. 構成ジョブ
7. 構成監査
8. ネットワーク機能
9. ネットワークレポート
10. ADC インスタンスのバックアップと復元
11. NetScaler からの SNMP イベント

次の機能は IPv6 をサポートしていません。

1. 高可用性フローティング IP
2. IPv6 をサポートする ADC から受信した syslog
3. IPv6 をサポートする ADC 上の StyleBook
4. 分析



## 5. プールライセンス

### はじめに

February 6, 2024

このドキュメントでは、初めて NetScaler Application Delivery Management (ADM) の展開と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 (Citrix SD-WAN WO、NetScaler Gateway など) と HAProxy などのサードパーティデバイスを管理するネットワーク管理者およびアプリケーション管理者を対象としています。NetScaler ADM を使用して管理するデバイスの種類に関係なく、このドキュメントの手順に従います。

NetScaler ADM の既存ユーザーの場合は、[サーバーを最新リリースの Citrix \[ADM にアップグレードする前に\]\(/ja-jp/netscaler-application-delivery-management-software/13/upgrade.html\)](#)、リリースノート、システム要件、およびライセンスの詳細を確認することをお勧めします。

#### 手順 1-システム要件を確認する

NetScaler ADM をデータセンターに導入する前に、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、および制限を確認してください。

- **ライセンス情報。** ライセンスがないインスタンスとエンティティを数に限りなく管理し、監視することができます。ただし、ライセンスを適用せずに管理できるのは、検出された 30 個のアプリのみで、分析情報を表示できるのは 2 つの仮想サーバーのみです。30 を超えるアプリを管理したり、3 つ以上の仮想サーバーの分析を表示したりするには、適切なライセンスを購入する必要があります。[詳細情報。](#)
- **オペレーティングシステムと受信機の要件。** この情報をレビューして、サポートされるオペレーティングシステムに対する正しい Receiver のバージョンをお持ちであることを確認してください。[詳細情報。](#)
- **ブラウザの要件。** NetScaler ADM GUI にアクセスするには、必要なブラウザと正しいバージョンがインストールされていることを確認する必要があります。[詳細情報。](#)
- **ポート。** NetScaler ADM が NetScaler ADC または SD-WAN インスタンス、または NetScaler ADC インスタンスと SD-WAN インスタンスの両方と通信するために必要なポートが開いていることを確認します。[詳細情報。](#)
- **NetScaler ADC インスタンスの要件。** さまざまな NetScaler ADM 機能が、さまざまな NetScaler ADC ソフトウェアバージョンでサポートされています。この情報を確認して、NetScaler ADC インスタンスを正しいバージョンにアップグレードしていることを確認します。[詳細情報。](#)
- **Citrix SD-WAN インスタンスの要件。** この情報を確認して、Citrix SD-WAN インスタンスを正しいバージョンにアップグレードし、正しいプラットフォームエディションがあることを確認します。[詳細情報。](#)

## 手順 2-NetScaler ADM を展開する

アプリケーションとネットワークインフラストラクチャを管理および監視するには、まずいずれかのハイパーバイザーに NetScaler ADM をインストールする必要があります。NetScaler ADM は、単一のサーバーとして、または高可用性モードで展開できます。NetScaler ADC Insight Center を使用している場合は、NetScaler ADM に移行して、分析機能に加えて、管理、監視、オーケストレーション、およびアプリケーション管理機能を利用できます。

- 単一サーバーの導入。NetScaler ADM 単一サーバー展開では、データベースがサーバーと統合され、単一のサーバーがすべてのトラフィックを処理します。NetScaler ADM Citrix Hypervisor、VMware ESXi、Microsoft Hyper-V、Linux KVM とともに展開できる。参照：
  - [Citrix Hypervisor を使用した NetScaler ADM](#)
  - [Microsoft Hyper-V を搭載した NetScaler ADM](#)
  - [VMware ESXi を使用した NetScaler ADM](#)
  - [Linux KVM サーバーを使用した NetScaler ADM](#)
- 高可用性導入。2 台の NetScaler ADM サーバーの高可用性展開 (HA) により、中断のない操作が可能になります。高可用性設定では、両方の NetScaler ADM ノードを同じソフトウェアバージョンとビルドを使用して同じサブネット上にアクティブ/パッシブモードで展開し、同じ構成にする必要があります。高可用性展開では、NetScaler ADM プライマリノードでフローティング IP アドレスを構成できるため、NetScaler ADC ロードバランサを別途用意する必要がなくなります。詳細については、「[高可用性展開での構成](#)」をご参照ください。

## ステップ 3-NetScaler ADM にインスタンスを追加する

インスタンスとは、NetScaler ADM から検出、管理、監視したい Citrix アプライアンス、仮想アプライアンス、またはサードパーティのデバイスです。これらのインスタンスを管理および監視するには、NetScaler ADM サーバーにインスタンスを追加する必要があります。NetScaler ADM には、次のインスタンスを追加できます。

- Citrix ADC
  - NetScaler ADC MPX
  - NetScaler ADC VPX
  - NetScaler ADC SDX
  - NetScaler ADC CPX
  - NetScaler Gateway
  - Citrix SD-WAN
- HAProxy

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

[詳しい情報](#)

#### ステップ 4-仮想サーバーでの分析を有効にする

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

[詳しい情報](#)

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

NetScaler ADM でネットワークタイムプロトコル (NTP) サーバーを構成して、その時計を NTP サーバーと同期させる必要があります。NTP サーバーを構成すると、NetScaler ADM クロックは、ネットワーク上の他のサーバーと同じ日付と時刻の設定になります。

[詳しい情報](#)

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

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

- システムアラームを設定します。システムアラームを設定して、システムの重大な問題または重大な問題を認識していることを確認します。たとえば、CPU 使用率が高い場合や、サーバーへのログインに複数回失敗した場合に、管理者に通知が送信されるようにします。
- システム通知を設定します。さまざまなシステム関連機能について、ユーザーのグループを選択するために通知を送信できます。NetScaler ADM で通知サーバーを設定し、電子メールおよびショートメッセージサービス (SMS) Gateway サーバーを構成して、ユーザーに電子メールおよびテキスト通知を送信できます。これによりユーザーログインやシステムの再起動などの、システムレベルのアクティビティが管理者に通知されます。
- システム削除設定を構成します。NetScaler ADM サーバーのデータベースに保存されるレポートデータの量を制限するために、NetScaler ADM がネットワークレポートデータ、イベント、監査ログ、およびタスクログを保持する間隔を指定できます。デフォルトでは、これらのデータは 24 時間ごとに (00:00 の時刻に) 削除されます。
- システムバックアップの設定を構成します。NetScaler ADM は、毎日 00:30 にシステムを自動的にバックアップします。デフォルトでは、3 つのバックアップファイルが保存されます。それ以上の数のシステムのバックアップを保持する必要があるかもしれません。

- インスタンスのバックアップ設定を構成します。NetScaler ADC インスタンスの現在の状態をバックアップする場合、インスタンスが不安定になった場合に備えて、バックアップファイルを使用して安定性を回復できます。アップグレードを実行する前にこれを行うことは特に重要です。デフォルトでは、12 時間ごとにバックアップされて、3 つのバックアップファイルがシステムに保持されます。
- インスタンスイベントブリーニング設定を構成します。NetScaler ADM サーバーのデータベースに保存されるイベントメッセージデータの量を制限するために、NetScaler ADM がネットワークレポートデータ、イベント、監査ログ、およびタスクログを保持する間隔を指定できます。デフォルトでは、これらのデータは 24 時間ごとに（00:00 の時刻に）削除されます。
- インスタンスの **Syslog** 消去設定を行います。データベースに保存される Syslog データの量を制限するために、Syslog データをパージする間隔を指定できます。次の syslog データを NetScaler ADM から削除するまでの日数を指定できます。
  - 汎用 Syslog データ
  - AppFirewall データ
  - NetScaler Gateway のデータ。

[詳しい情報](#)

### 次の操作

NetScaler ADM を展開してセットアップしたら、インスタンスとアプリケーションの管理と監視を開始できます。

**NetScaler ADC** インスタンスとアプリケーションの管理。NetScaler ADM のすべての機能は、NetScaler ADC インスタンスでサポートされています。いずれの機能も使用を開始できます。

**Citrix ADC SD-WAN** インスタンスの管理 SD-WAN WO インスタンスでは、すべての NetScaler ADM 機能がサポートされているわけではありません。たとえば、証明書の管理や構成の監査はサポートされていません。サポートされている機能とその使用方法については、「[Citrix ADM を使用した Citrix SD-WAN WO の管理](#)」を参照してください。

**HAProxy** インスタンスおよびアプリケーションの管理。HAProxy デプロイメントで構成されたフロントエンド、バックエンド、サーバーを監視できます。また、アプリケーション管理機能を使用して、NetScaler ADM によって監視されるフロントエンドのリアルタイム統計を監視することもできます。HAProxy でサポートされている機能とその使用方法については、「[NetScaler ADM を使用した HAProxy インスタンスの管理と監視](#)」を参照してください。

### 展開

February 6, 2024

NetScaler ADM を使用してアプリケーションとネットワークインフラストラクチャを管理および監視する前に、まずハイパーバイザーの 1 つまたは Kubernetes クラスターにインストールする必要があります。NetScaler ADM をハイパーバイザーに展開する場合は、単一サーバーとして、または高可用性モードで展開できます。高可用性モードは Kubernetes クラスターには適用されません。NetScaler Insight Center を使用している場合は、NetScaler ADM に移行して、分析機能に加えて、管理、監視、オーケストレーション、およびアプリケーション管理機能を利用できます。

- 単一サーバーの導入: ハイパーバイザーに展開されたスタンドアロンの ADM の場合、データベースはサーバーと統合され、1 つのサーバーがすべてのトラフィックを処理します。NetScaler ADM Citrix Hypervisor、VMware ESXi、Microsoft Hyper-V、Linux KVM とともに展開できる。参照:
  - [Citrix Hypervisor での NetScaler ADM](#)
  - [Microsoft Hyper-V 上の NetScaler ADM](#)
  - [VMware ESXi 上の NetScaler ADM](#)
  - [Linux KVM サーバーでの NetScaler ADM](#)
  - [Kubernetes クラスター上の NetScaler ADM](#)
- 高可用性 (HA) 展開: 2 台の NetScaler ADM サーバーの高可用性展開では、運用が中断されることはありません。高可用性セットアップでは、両方の NetScaler ADM ノードをアクティブ/パッシブモードで、同じサブネット上に同じソフトウェアバージョンとビルドを使用して展開し、同じ構成にする必要があります。高可用性展開では、NetScaler ADM プライマリノードでフローティング IP アドレスを構成できるため、個別の NetScaler ADC ロードバランサーが不要になります。「[高可用性展開での構成](#)」を参照してください。

注:

高可用性は、Kubernetes クラスターにデプロイされた ADM には適用されません。

- **NetScaler Insight Center から NetScaler ADM への移行:** NetScaler Insight Center の導入環境を、既存の構成、設定、またはデータを失うことなく NetScaler ADM に移行できます。NetScaler ADM を使用すると、NetScaler ADC および Citrix SD-WAN インスタンスによって生成されたさまざまな分析を表示できるだけでなく、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単一の統合コンソールから管理、監視、トラブルシューティングすることもできます。「[NetScaler Insight Center から NetScaler ADM への移行](#)」を参照してください。
- **NetScaler ADM と Director の統合:** Director は NetScaler ADM と統合し、ネットワーク分析とパフォーマンス管理を行います。[NetScaler ADM と Director の統合を参照してください](#)。

## NetScaler ADM をインストールするための前提条件

February 6, 2024

Microsoft HyperV、VMware ESXi、Linux KVM、

および Citrix Hypervisor プラットフォーム用の Citrix Application Delivery Management (ADM) を仮想アプリケーションとしてダウンロードしてインストールできます。

NetScaler ADM をインストールする前に、ソフトウェア要件、ブラウザの要件、ポート

情報、ライセンス情報、およびこれらすべてのプラットフォームに関する制限事項を理解しておく必要があります。

特定のプラットフォーム要件と Citrix ADM をインストールする詳細な手順については、以下のトピックを参照してください。

- [Citrix Hypervisor を使用した NetScaler ADM](#)
- [Citrix ADM とマイクロソフト HyperV](#)
- [VMware ESXi を使用した NetScaler ADM](#)
- [Linux KVM サーバーを使用した NetScaler ADM](#)

### Citrix ADM の一般的な要件

コンポーネント	条件
RAM	32 GB
仮想 CPU	8 基の CPU
記憶域	<p>Citrix ADM の展開にはソリッドステートドライブ (SSD) テクノロジーを使用することをお勧めします。必要なデフォルトのストレージ容量は 120 GB です。実際のストレージ要件は、NetScaler ADM のサイズ設定の見積もりによって異なります。[Citrix ADM HA 導入ガイドの「最大制限」セクション (7 ページ) に記載されている <a href="#">サイジング計算ツール</a> を使用] (<a href="https://www.citrix.com/content/dam/citrix/en_us/documents/adc/Citrix_ADM_HA_Deployment_Guide.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/adc/Citrix_ADM_HA_Deployment_Guide.pdf</a>) してください。このガイドは、<a href="#">ダウンロードサイトの [NetScaler MAS リリース 12.1] &gt; [以前のバージョン]</a> から入手できます。注: 展開ガイドとサイジング計算ツールにアクセスするには、Citrix アカウントが必要です</p> <p>NetScaler ADM ストレージ要件が 120 GB を超える場合は、追加のディスクを接続する必要があります。最初の展開時には、ストレージを見積もり、追加のディスクを接続することをお勧めします。追加できるディスクは 1 つだけです。</p>

コンポーネント	条件
	詳しくは、「 <a href="#">NetScaler ADM に追加のディスクを接続する方法</a> 」を参照してください。
仮想ネットワークインターフェイス	1
スループット	1Gbps

---

注:

NetScaler ADM VHD はローカルストレージでホストすることをお勧めします。SAN 内のストレージデバイスでホストされている場合、NetScaler ADM が期待どおりに動作しないことがあります。そのため、SAN への ADM の導入はサポートされていません。

## Citrix Hypervisor での NetScaler ADM

February 6, 2024

NetScaler ADM を Citrix Hypervisor (旧 XenServer) にインストールするには、まず NetScaler ADM .xva イメージファイルをローカルコンピュータにダウンロードする必要があります。Citrix ADM のインストールを実行するには、Citrix XenCenter を使用する必要があります。

注:

Citrix ADM は XenMotion をサポートしていません。

### 前提条件

Citrix ADM をインストールする前に、次の要件が満たされていることを確認してください:

- Citrix Hypervisor バージョン 7.1 以降が、最小要件を満たすハードウェアにインストールされます。
- 最小要件を満たす管理用のワークステーションに XenCenter がインストールされている。Citrix ADM を Citrix Hypervisor にインストールするには、XenCenter を使用する必要があります。
- Citrix ADM .XVA イメージファイルをダウンロードしました。

### XenCenter のシステム要件

XenCenter は、Windows のクライアントアプリケーションです。Citrix Hypervisor ホストと同じマシン上で実行することはできません。次の表は、最小システム要件を示しています。

コンポーネント	条件
オペレーティングシステム	Windows 7、Windows Server 2003、または Windows 10
.NET Framework	バージョン 2.0 以降
CPU	750 MHz (MHz)、推奨:1 ギガヘルツ (GHz) またはそれより高速
RAM	1GB。推奨: 2GB
NIC	100Mbps 以上の NIC

## Citrix Application Delivery Management のインストール

1. XVA イメージファイルを Citrix Hypervisor にインポートし、[コンソール] タブで初期ネットワーク構成オプションを構成します。

```

Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
-----
 1. Citrix ADM Host Name [ADMHA1]:
 2. Citrix ADM IPv4 address [10.102.29.52]:
 3. Netmask [255.255.255.0]:
 4. Gateway IPv4 address [10.102.29.11]:
 5. DNS IPv4 Address [127.0.0.2]:
 6. Cancel and quit.
 7. Save and quit.
-----
Select a menu item from 1 to 7 [7]:

```

2. 必要な IP アドレスを指定したら、構成設定を保存します。
3. プロンプトが表示されたら、nsrecover/nsroot 認証情報を使用してログオンします。

```

login: nsrecover
Password:
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
    The Regents of the University of California. All rights reserved.
bash-3.2#

```

### 注

ログオン後、初期ネットワーク構成を更新する場合は、`networkconfig`を入力し、構成を更新し、構成を保存します。

4. シェルプロンプトで次のコマンドを入力して、展開スクリプトを実行します。`/mps/deployment_type.py`



```
bash-3.2# deployment_type.py
-----
Citrix ADM Deployment Configuration.
```

5. 展開の種類として **NetScaler ADM** サーバーを選択します。デフォルトでは、オプションを選択しない場合は、サーバーとして展開されます。

```
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-----
1. Citrix ADM Server.
2. Remote Disaster Recovery Node.
3. Cancel and exit.
Select an option from 1 to 3 [3]: 
```

6. NetScaler ADM をスタンドアロン展開として展開するには、「はい」と入力します。
7. 「はい」と入力して、NetScaler ADM サーバーを再起動します。

注

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

## 確認

サーバーをインストールしたら、Web ブラウザーで NetScaler ADM サーバーの IP アドレスを入力して GUI にアクセスできます。サーバーにログオンするためのデフォルトの管理者資格情報は nsroot/nsroot です。

ブラウザに NetScaler ADM 構成ユーティリティが表示されます。

## Microsoft Hyper-V 上の NetScaler ADM

February 6, 2024

Microsoft Hyper-V に NetScaler ADM をインストールするには、まず NetScaler ADM イメージファイルをローカルコンピュータにダウンロードする必要があります。また、システムにハードウェア仮想化拡張機能があることを確認し、CPU 仮想化拡張機能が使用可能であることを確認してください。

### 前提条件

Citrix ADM 仮想アプライアンスをインストールする前に、次の要件が満たされていることを確認してください。

- 最小要件を満たすハードウェアに Microsoft Hyper-V Version 6.2 以降がインストールされている。
- 最小システム要件を満たす管理用のワークステーションに Microsoft Hyper-V マネージャーがインストールされている。
- Citrix ADM イメージファイルをダウンロードしました。

### Microsoft Hyper-V のシステム要件

Microsoft Hyper-V は、Windows クライアントアプリケーションです。次の表は、最小システム要件を示しています。

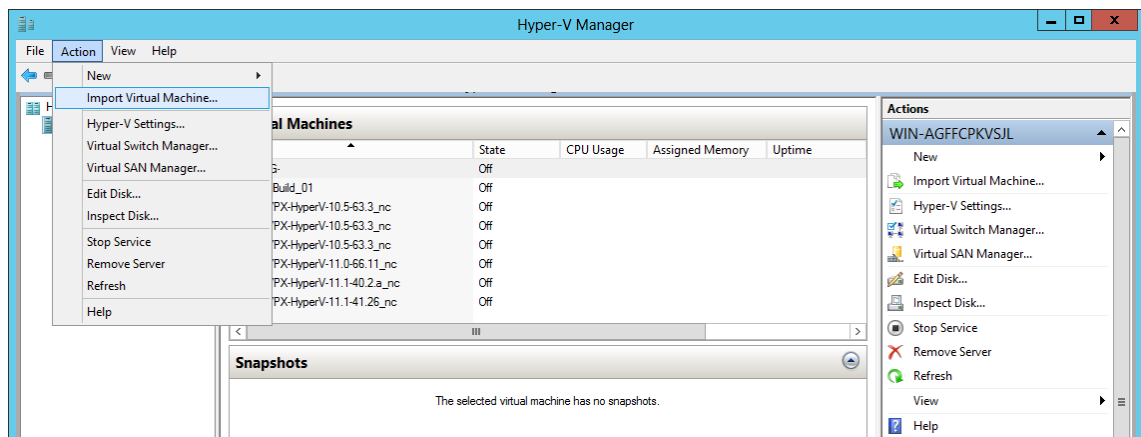
コンポーネント	条件
オペレーティングシステム	Windows Server 2012 R2
.NET Framework	バージョン 2.0 以降
CPU	750 MHz (MHz)、推奨:1 ギガヘルツ (GHz) またはそれより高速
RAM	1GB。推奨: 2GB
NIC	100Mbps 以上の NIC

### NetScaler Application Delivery Management インストール

インストールできる Citrix ADM サーバーの数は、Hyper-V サーバーで使用可能なメモリによって異なります。

**NetScaler ADM** をインストールするには:

1. ワークステーションで Hyper-V マネージャークライアントを起動します。
2. [操作] メニューの [仮想マシンのインポート] を選択します。

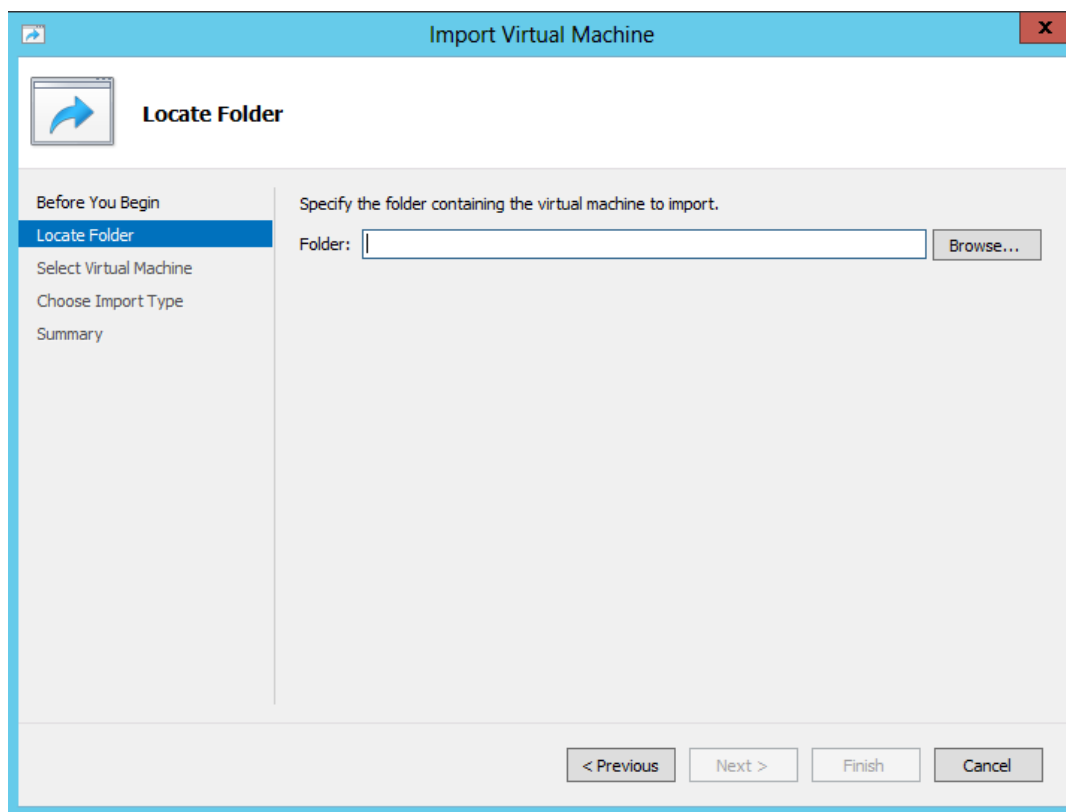


3. Hyper-V イメージをインポートし、次の操作を行います。

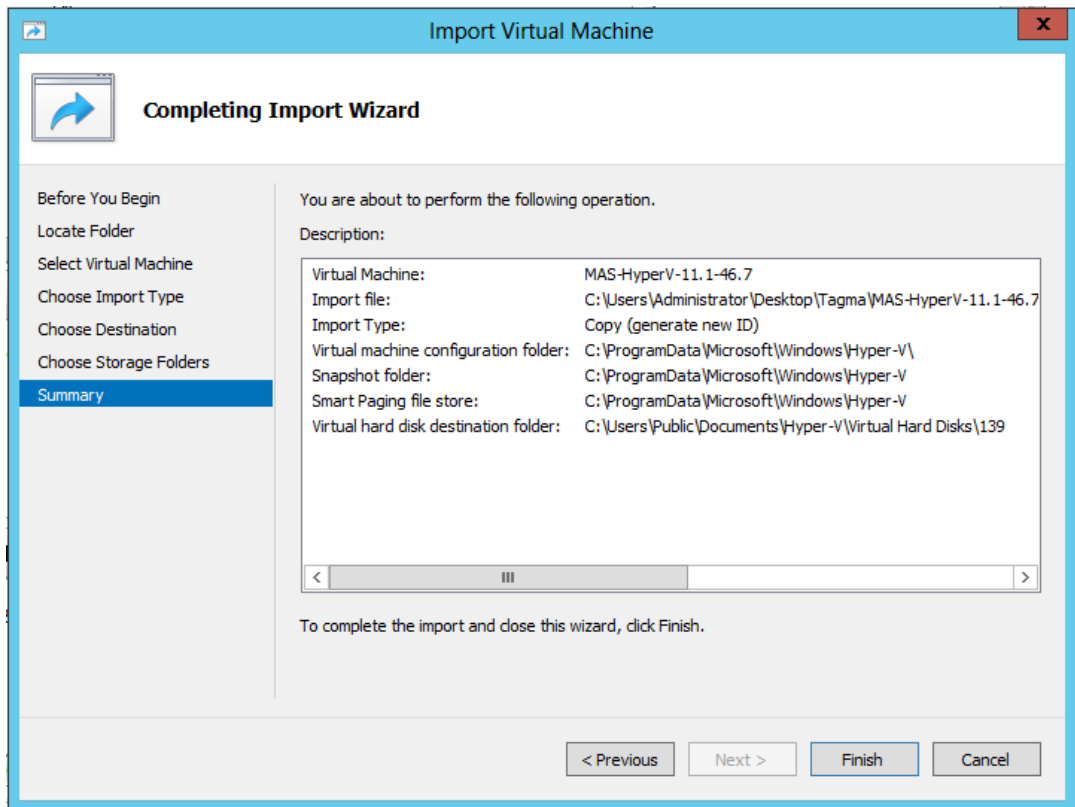
- a) [仮想マシンのインポート] ダイアログボックスの [フォルダーの検索] セクションで、Citrix ADM Hyper-V イメージを保存したフォルダーを参照し、フォルダーを選択して [次へ] をクリックします。
- b) [Select virtual machine] セクションで、該当する仮想マシン名を選択します。
- c) [**Choose Import Type**] セクションで、[Copy the virtual machine (create a new unique ID)] オプションを選択し、[Next] をクリックします。
- d) [**Choose Destination**] セクションで、仮想マシンファイルを格納するフォルダーを指定します。

注

デフォルトでは、仮想マシンファイルは、ローカルホストのデフォルトの Hyper-V フォルダーにインポートされます。

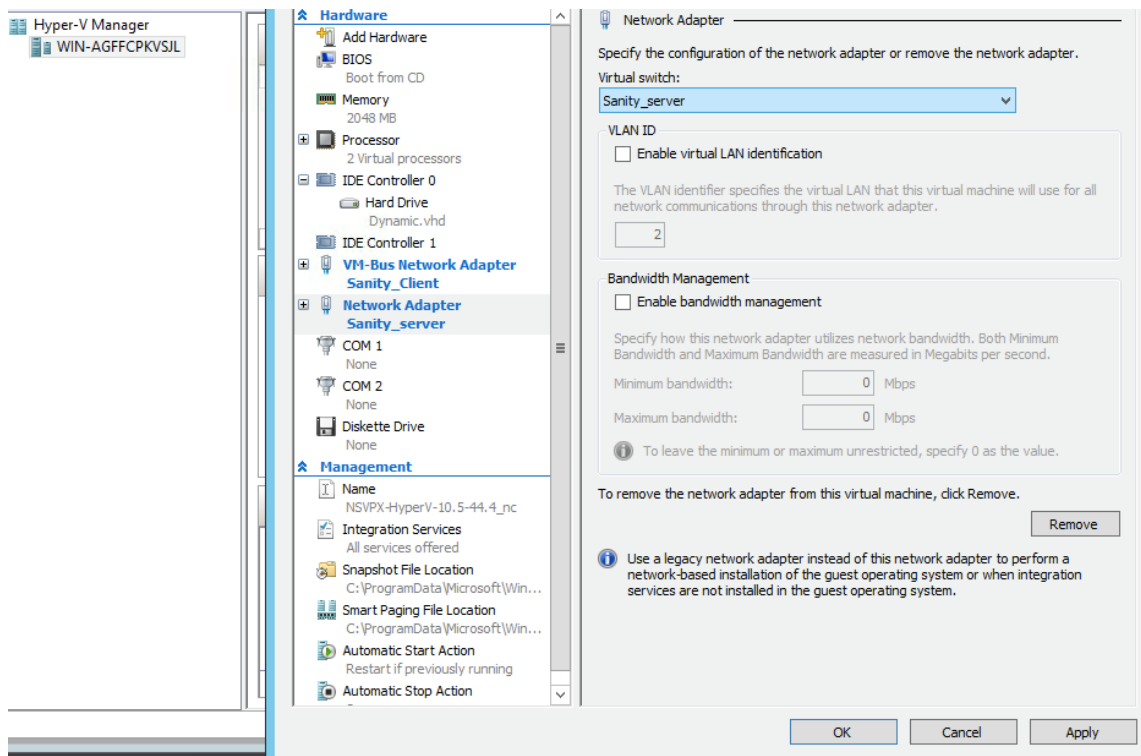


- e) [**Choose Storage Folders**] セクションで、仮想ハードディスクを保存する場所を選択し、[**Next**] をクリックします。
- f) 概要を示すペインで仮想マシンの情報を確認したら、[**Finish**] をクリックします。



Citrix ADM Hyper-V イメージが右側のペインに表示されます。

4. NetScaler ADM Hyper-V イメージを右クリックし、[ 設定 ] をクリックします。
5. 表示されるダイアログボックスの左側のペインで [ ハードウェア ] > [ **VM\_Bus Network Adaptor** ] に移動し、右側のペインの [ ネットワーク ] リストから適切なネットワークを選択します。



6. [適用] をクリックしてから、[OK] をクリックします。
7. Citrix ADM Hyper-V イメージを右クリックして、「接続」をクリックします。
8. 「コンソール」 ウィンドウで、「開始」 ボタンをクリックします。
9. 初期ネットワーク設定オプションを設定します。

```
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([ ]).
Selecting the listed number allows the address to be changed.
-----
 1. Citrix ADM Host Name [ADMHA1]:
 2. Citrix ADM IPv4 address [10.102.29.52]:
 3. Netmask [255.255.255.0]:
 4. Gateway IPv4 address [10.102.29.1]:
 5. DNS IPv4 Address [127.0.0.2]:
 6. Cancel and quit.
 7. Save and quit.

Select a menu item from 1 to 7 [7]:
```

10. 必要な IP アドレスを指定したら、構成設定を保存します。
11. プロンプトが表示されたら、nsrecover/nsroot 認証情報を使用してログオンします。

```
login: nsrecover
Password:
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

bash-3.2#
```

## 注

ログオン後、初期ネットワーク構成を更新する場合は、`networkconfig`を入力し、構成を更新し、構成を保存します。

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

```
1 deployment_type.py
2 <!--NeedCopy-->
```

```
bash-3.2# deployment_type.py
```

```
-----
Citrix ADM Deployment Configuration.
```

13. 展開の種類として **NetScaler ADM** サーバーを選択します。デフォルトでは、オプションを選択しない場合は、サーバーとして展開されます。

```
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-----
```

- ```
1. Citrix ADM Server.
2. Remote Disaster Recovery Node.
3. Cancel and exit.
```

```
Select an option from 1 to 3 [3]: 
```

14. Citrix ADM を スタンドアロン環境として展開するには、「はい」と入力します。

15. 「はい」と入力して、NetScaler ADM サーバーを再起動します。

## 注

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

## 確認

サーバーのインストール後、ブラウザのアドレスバーに NetScaler ADM サーバーの IP アドレスを入力して、GUI にアクセスできます。サーバーにログオンするためのデフォルトの管理者資格情報は `nsroot/nsroot` です。

ブラウザに NetScaler ADM 構成ユーティリティが表示されます。

## VMware ESXi 上の NetScaler ADM

February 6, 2024

VMware ESXi に NetScaler ADM 仮想アプライアンスをインストールするには、VMware vSphere クライアントを使用します。

### 前提条件

仮想アプライアンスのインストールを開始する前に、次の必要条件を確認します。

- サポートされている VMware ESXi バージョン (6.0、6.5、6.7、および 7.0) をインストールします。
- 最小システム要件を満たす管理用のワークステーションに VMware Client をインストールします。
- NetScaler ADM セットアップファイルをダウンロードします。

#### 注

VMotion は、**NetScaler ADM 13.0** ビルド **47.22** 以降でのみサポートされています。vSphere の高可用性や vSphere DRS セットアップなど、ESXi ハイパーバイザーにデプロイされた ADM サーバの移行をスケジュールして自動化できます。

### NetScaler ADM をインストールするには

#### 注

手順とスクリーンキャプチャは、VMware ESXi バージョン 6.0 に基づいています。GUI は他の ESXi バージョンでは異なる場合があります。VMXNET3 アダプタ搭載の VMware ESXi バージョン 7.0.1c ビルド番号 17325551 は、**NetScaler ADM 13.0 71.40** 以降でサポートされています。バージョン固有の手順については、VMware のドキュメントを参照してください。

1. ワークステーション上で VMware vSphere Client を起動します。
2. [IP アドレス/名前] テキストボックスに、接続する VMware ESXi サーバの IP アドレスを入力します。
3. [User Name] と [Password] の各テキストボックスに管理者資格情報を入力してから、[Login] をクリックします。
4. [File] メニューの [Deploy OVF Template] を選択します。
5. [OVF テンプレートのデプロイ] ダイアログボックスの [ファイルまたは URL からのデプロイ] で、.ovf ファイルを選択し、[次へ] をクリックします。



注

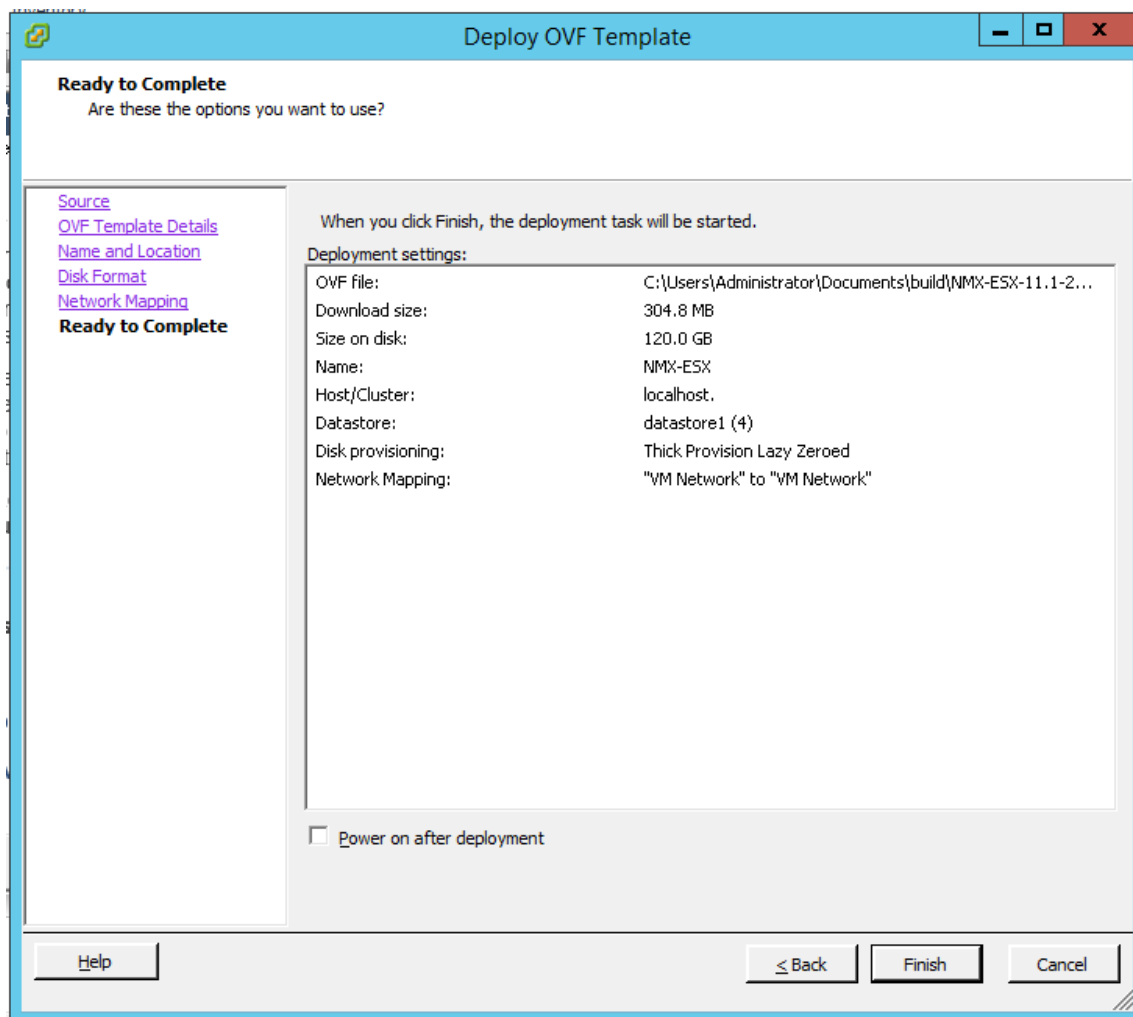
警告メッセージに次のテキストが表示される場合: オペレーティングシステム識別子は選択したホストでサポートされていません、VMware サーバが FreeBSD オペレーティングシステムをサポートしているかどうかを確認します。[はい] をクリックします。

6. [ **OVF** テンプレートの詳細] ページで、[ 次へ] をクリックします。
7. NetScaler ADM 仮想アプライアンスの名前を入力し、[ 次へ] をクリックします。
8. [Disk Format] で [Thin provisioned format] または [Thick provisioned format] を選択し、ディスク形式を指定します。

注

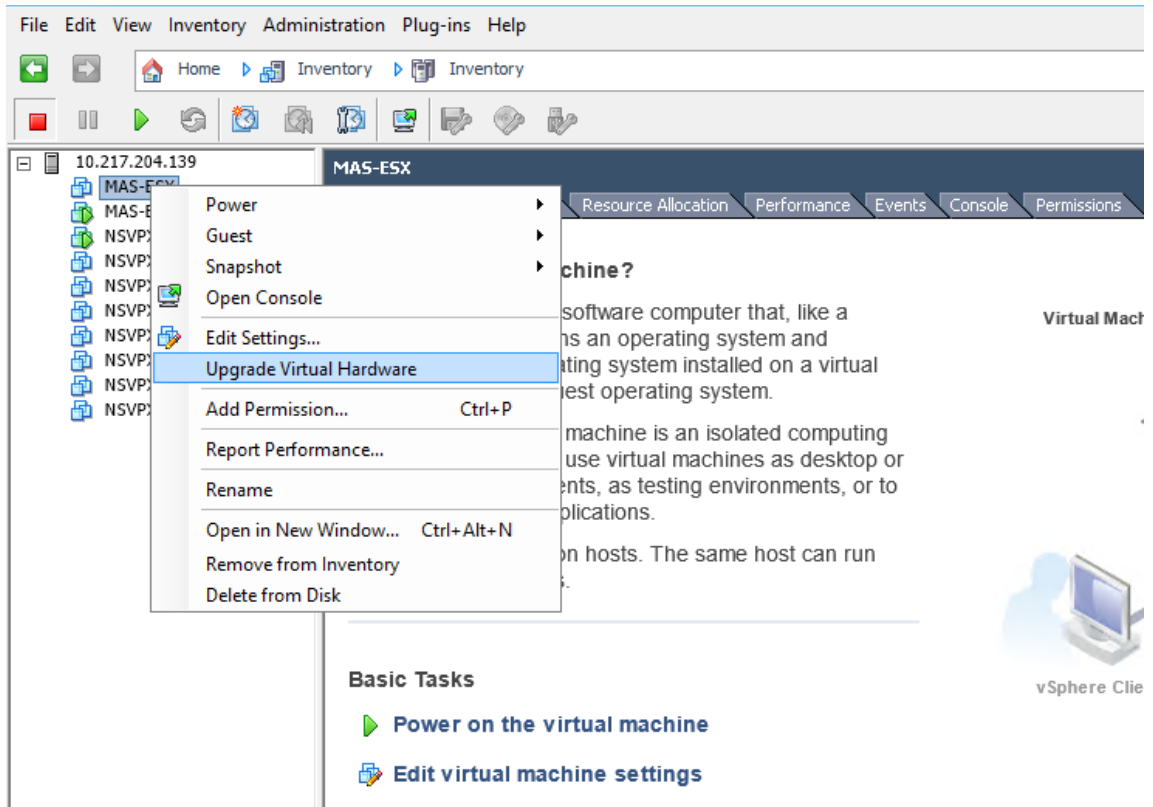
Citrix では、シックプロビジョニング形式を選択することをお勧めします。

9. [完了] をクリックして、インストールプロセスを開始します。

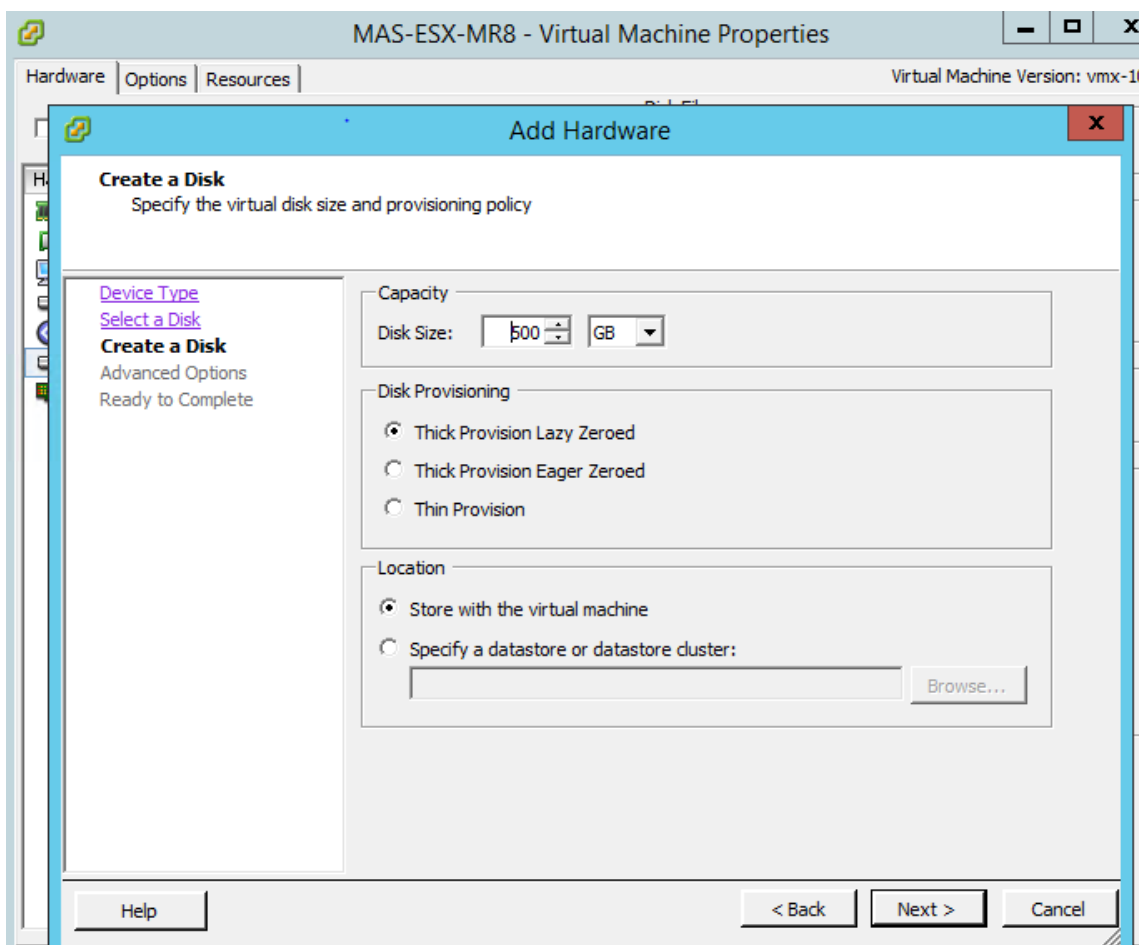


10. これで、NetScaler ADM 仮想アプライアンスを起動する準備ができました。

- ナビゲーションペインで、インストールした仮想アプライアンスを選択します。[インベントリ]メニューから、仮想マシンを右クリックし、[仮想ハードウェアのアップグレード]をクリックします。[仮想マシンの確認]ダイアログボックスで、[はい]をクリックします。



- [インベントリ]メニューで、[仮想マシン]をクリックし、[設定の編集]をクリックします。
- [仮想マシンのプロパティ]ダイアログボックスの[ハードウェア]タブで[メモリ]をクリックし、右側のペインで[メモリサイズ]に32 GBを指定します。
- [CPU]をクリックし、右側のペインでCPUを8と指定します。[OK]をクリックします。
- 要件に応じて余分なディスクを追加します。



16. ナビゲーションペインで、インストールした仮想アプライアンスを選択します。[インベントリ]メニューから、[仮想マシン]、[パワー]、[パワーオン]の順にクリックします。
17. [コンソール] タブをクリックして、NetScaler ADM の初期ネットワーク構成オプションを表示します。

```

Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([ ]).
Selecting the listed number allows the address to be changed.
-----
1. Citrix ADM Host Name [ADMHA1]:
2. Citrix ADM IPv4 address [10.102.29.52]:
3. Netmask [255.255.255.0]:
4. Gateway IPv4 address [10.102.29.1]:
5. DNS IPv4 Address [127.0.0.2]:
6. Cancel and quit.
7. Save and quit.

Select a menu item from 1 to 7 [7]:
    
```

18. 必要な IP アドレスを指定したら、構成設定を保存します。
19. プロンプトが表示されたら、nsrecover/nsroot 認証情報を使用してログオンします。

```
login: nsrecover
Password:
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

bash-3.2#
```

## 注

ログオン後、初期ネットワーク構成を更新する場合は、`networkconfig`を入力し、構成を更新し、構成を保存します。

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

```
1 deployment_type.py
2 <!--NeedCopy-->
```

```
bash-3.2# deployment_type.py
-----
Citrix ADM Deployment Configuration.
```

21. 展開の種類として **NetScaler ADM** サーバーを選択します。デフォルトでは、オプションを選択しない場合は、サーバーとして展開されます。

```
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-----

1. Citrix ADM Server.
2. Remote Disaster Recovery Node.
3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

22. NetScaler ADM をスタンドアロン展開として展開するには、「はい」と入力します。

23. 「はい」と入力して、NetScaler ADM サーバーを再起動します。

## 注

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

## 確認

サーバーをインストールしたら、ブラウザに NetScaler ADM サーバーの IP アドレスを入力して GUI にアクセスできます。サーバーにログオンするためのデフォルトの管理者資格情報は `nsroot/nsroot` です。

ブラウザに NetScaler ADM 構成ユーティリティが表示されます。

注:

VMware ESXi では ADM のインストールに通常約 10 分かかりますが、システムによってはさらに時間がかかる場合があります。

## Kubernetes クラスタ上の NetScaler ADM

February 6, 2024

NetScaler ADM 仮想アプライアンスを Kubernetes クラスタにインストールする前に、前提条件のセクションをお読みください。

### 前提条件

ADM をインストールする前に、次の前提条件が満たされていることを確認します。

### Kubernetes クラスタ

- Kubernetes クラスタは、以下のバージョン以上である必要があります:
  - サーバーバージョン v1.13
  - クライアントバージョン v1.13

`kubectl version` コマンドを入力してバージョンを確認します。

- クラスタにインストールされる Helm アプリケーションは、以下のバージョン以上である必要があります。
  - サーバーバージョン v2.12.1
  - クライアントバージョン v2.12.0

`helm version` コマンドを使用してバージョンを確認します。

- Kubernetes cluster CNI (Container Network Interface) は Calico バージョン v3.1.3 以上でなければならない。
- クラスタ内のすべての下位ノードに NFS クライアントをインストールする必要があります。これは、ADM アプリケーションがネットワークファイルサーバにマウントされたボリューム上のデータと構成を保持するためです。Ubuntu ベースの下位に NFS クライアントをインストールするには、次のコマンドを入力します。

```
apt-get update
```

```
apt install nfs-common
```

- ADM アプリケーションでは、クラスタ全体で 32 GB のメモリと 8 つの vCPU、NFS では 120 GB の領域が必要です。

## NFS 共有

ADM アプリケーションには、設定、証明書、イメージなどのデータを保存するための永続ボリュームが必要です。このためには、ADM には NFS マウントが必要です。このアプリケーションには、共有ネットワークマウントの 2 つのフォルダが必要です。

- 1 つは証明書、イメージなどのファイルを保存するためのものです。
- データベース用のもう一つ

注:

SSD を備えた NFS を使用することをお勧めします。

これら 2 つのフォルダは、異なるものでも同じでもかまいません。両方のフォルダーに 777 のアクセス許可が必要です。最初のフォルダには 10 GB 以上の空き容量が必要です。2 つ目のフォルダーのサイズは、データベース内で永続的にする必要のあるデータの量によって異なります。最小サイズは 100 GB です。

本番環境では、本番グレードの NFS ソリューションを使用することをお勧めします。

## NetScaler ADC アプライアンス

NetScaler ADC アプライアンスは入力デバイスとして必要です。ADC は、必要なアプリケーションサービスを Kubernetes

クラスターの外部で使用できるようにします。NetScaler ADC アプライアンスは Kubernetes クラスターの外部にあり、ADC からワーカーノードに到達できる必要があります。次の手順を実行します:

- ADC で SNIP を設定します。ADC はこの SNIP を使用して Kubernetes クラスターのワーカーノードに到達します。
- 必要なアプリケーションサービスを Kubernetes クラスター外で利用できるようにするために、仮想サーバの IP アドレスとして使用する空き IP アドレスを特定します。

## Kubernetes クラスターに ADM をインストールする

Kubernetes クラスターに ADM アプライアンスをインストールするには、次の手順に従います。

1. [Citrix ダウンロードサイトに移動し](#)、Kubernetes 用 NetScaler ADM Helm チャートのファイルをダウンロードします。
2. ダウンロードした Helm チャート tarball を Kubernetes クラスターのメインノードの /var ディレクトリに抽出します。
3. `values.yaml` ディレクトリの下に `/var/citrixadm` ファイルを開きます。
4. ファイルの `dbpasswd` フィールドに、データベースのパスワードを入力します。

5. 次の値を変更します。ADM アプリケーションは、これらの値を使用して、サービスが外部に公開されるように NetScaler ADC アプライアンスを構成します。

- **ingressIP**: アプリケーションにアクセスするために NetScaler ADC で構成された仮想 IP。
- **applicationID**: NetScaler ADC アプライアンス上の入力構成とその他の構成を区別するための一意の ID。
- **ingressADCIP**: NetScaler ADC IP アドレス (NSIP)。ADM アプリケーションの入力として使用されます。
- **ingressADCUsername**: NetScaler ADC アプライアンスにアクセスするためのユーザー名。このユーザーは書き込み権限を持っている必要があります。
- **ingressADCPasswd**: ユーザー名のパスワード。

```
# ingressIP is the Virtual IP configured in the Citrix ADC for accessing the application
ingressIP: "xx.xx.xx.xx"

# coreDumpFilePath is the directory on slave nodes of the cluster which will be used to store core dumps files in case
application runs into faulty state
# this setting is optional
# Admin needs to create this directory on each of the slave nodes and then run the command: "echo <coreDumpFilePath_value>/
core.%h.%e.%p > /proc/sys/kernel/core_pattern"
coreDumpFilePath: "/var/mps/cores"

# applicationID is the identifier for ingress configuration
applicationID: "citrixadm"

# ingressADCIP is the NSIP of the northbound ADC used to expose the ADM application to the outside world
ingressADCIP: "xx.xx.xx.xx"

# ingressADCUsername is the username of the northbound ADC
ingressADCUsername: "nsroot"

# ingressADCPasswd is the password for above username
ingressADCPasswd: "nsroot"
```

6. [ストレージ] セクションで次の値を変更します。これらの値は、ADM アプリケーションが必要とするファイルの保存に必要な永続性を指定します。

- **nfsServer**: NFS サーバのホスト名または IP アドレス
- **path**: アプリケーションファイルを保存するフォルダのパスをマウントします。
- **size**: 少なくとも 10 GB。

注

この値の単位は Gi です。たとえば、10Gi、20Gi などです。

7. **pg-datastore** 下のストレージセクションに移動し、次の値を変更します。これらの値は、データベースの作成に使用される永続性を指定します。

- **nsfServer**: NFS サーバーのホスト名または IP アドレス。
- **size**: データストアに使用されるフォルダのパスをマウントします。
- **path**: 少なくとも 100 GB。

注

この値の単位は Gi です。例えば、100Gi、200Gi。

8. メインノードの `/var/citrix` ディレクトリに移動し、次のコマンドを実行して ADM アプリケーションをインストールします。

```
helm install -n citrixadm --namespace <name> ./citrixadm
```

注

この helm コマンドは helm バージョン 3.x ではサポートされていません。

このコマンドは、必要な Pod をクラスターにインストールします。名前空間引数はオプションです。名前空間が指定されていない場合、Helm は ADM をデフォルトの名前空間にインストールします。管理を容易にするために、ADM を別の名前空間にインストールします。

9. ブラウザを開き、認証情報として `nsroot/nsroot` を使用し `http://< virtual server IP address >` を入力して ADM にログインします。セキュアなアクセスタイプの場合 `https://< virtual server IP address >`。

注

デプロイ中、ADM アプリケーションはデータストアにテーブルを作成しますが、これにはしばらく時間がかかります。Kubernetes が ADM アプリケーションのさまざまな Pod に割り当てたリソースによっては、サービスが起動するまでに 5 ~15 分かかることがあります。

## Linux KVM サーバーでの NetScaler ADM

February 6, 2024

NetScaler Application Delivery Management (ADM) をプロビジョニングできる仮想化プラットフォームには、Linux-KVM があります。

Linux-KVM に NetScaler ADM をインストールする前に、システムにハードウェア仮想化拡張機能があることを確認し、CPU 仮想化拡張機能が使用可能であることを確認します。ハイパーバイザーで `virsh` (仮想マシンを管理するためのコマンドラインツール) が使用できることを確認します。

管理者の資格情報を使用して Citrix.com の Web サイトにログオンし、最新の NetScaler ADM セットアップファイルにアクセスし、コンピュータにダウンロードします。次に、Citrix ADM を Linux-KVM プラットフォームにインストールし、ネットワーク用に構成します。

### 前提条件

Citrix ADM 仮想アプライアンスをインストールする前に、Linux-KVM バージョン 3.6.11-4 以降が最小要件を満たすハードウェアにインストールされていることを確認してください。



ハードウェア要件

| コンポーネント   | 条件                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU       | <p>インテル VT-X プロセッサに含まれているハードウェア仮想化機能を備えた 64 ビット x86 プロセッサ。ホスト Linux-KVM に 2 つ以上の CPU コアを指定します。</p> <p>注: CPU が Linux ホストをサポートしているかどうかをテストするには、ホスト Linux シェルプロンプトで次のコマンドを入力します。<br/> <code>*. egrep '^flags .\* ( vmx   svm )' /proc/cpuinfo</code>*<br/>                     拡張機能の BIOS 設定が無効になっている場合は、BIOS で有効にする必要があります。プロセッサ速度に関する具体的な推奨はありませんが、速度が速いほど、NetScaler ADM パフォーマンスが向上します。</p> |
| メモリ (RAM) | <p>ホスト Linux カーネルに対して 4GB 以上。VM により必要とされる追加メモリを追加します。</p>                                                                                                                                                                                                                                                                                                                                   |
| ハード ディスク  | <p>ホスト Linux カーネルおよび VM 要件の領域を計算します。1 つの Citrix ADM 仮想マシンには 120 GB のディスク容量が必要です。</p>                                                                                                                                                                                                                                                                                                        |

注

指定されたメモリとハードディスクの要件は、ホスト上で他の仮想マシンが実行されていないことを考慮して、Citrix ADM を OpenStack プラットフォームにデプロイするためのものです。OpenStack のハードウェア要件は、OpenStack で実行される仮想マシンの数によって異なります。

ソフトウェア要件

Citrix では、より最新のカーネルを推奨しています (64 ビット版の 3.6.11-4 カーネルまたはそれ以降など)。

ネットワークの要件 NetScaler ADM は、VirtIO 準仮想化ネットワークインターフェイスを 1 つだけサポートします。NetScaler ADM と Linux-KVM が通信できるように、このインターフェイスを Linux-KVM ホストの管理ネットワークに接続してください。

**NetScaler ADM** セットアップファイルのダウンロード

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

1. Web ブラウザーを開き、アドレスバーに「[www.citrix.com](http://www.citrix.com)」と入力します。

2. [サインイン] オプションにカーソルを合わせ、[My Account] をクリックし、Citrix の資格情報を入力して、[サインイン] をもう一度クリックします。
3. [ダウンロード] セクションに移動します。
4. ダウンロードリストから、「Citrix Application Delivery Management」を選択します。
5. [NetScaler Application Delivery Management] ページで、リリースを選択します。たとえば、リリース **13.0** を選択します。
6. [製品][ソフトウェア] をクリックして展開し、最新のビルドをクリックします。たとえば、**NetScaler MAS** リリース（機能フェーズ）**13.0** ビルド **36.27** を選択します。  
選択したビルドページが表示されます。
7. [ダウンロードするジャンプ] リストで、[KVM 用の NetScaler MAS イメージ、13.0 ビルド xx.xx] を選択します。
8. [Download File] をクリックし、EULA を受け入れ、圧縮イメージファイルをローカルマシン上の任意のフォルダにダウンロードします。

## Linux-KVM で NetScaler Application Delivery Management をインストール

1. SSH を使用して、KVM ホストにログオンします。
2. CLI プロンプトで、いずれかのファイル転送プログラムを使用して、イメージをサーバーのフォルダーにコピーします。
3. ダウンロードしたイメージを保存したディレクトリに移動します。
4. コマンドラインで次の手順を実行します。
  - a) ディレクトリ内のファイルの一覧を表示して、イメージファイルが存在することを確認します。
  - b) tar コマンドを使用して、Citrix Application Delivery Management イメージファイルを解凍します。解凍したパッケージには、次のコンポーネントが含まれています。
    - i. Citrix ADM 属性を指定するドメイン XML ファイル
    - ii. ドメインディスクイメージのチェックサムが記述されたテキストファイル
    - iii. ドメインディスクイメージ

```
1 tar -xvfz MAS-KVM.tgz
2 MAS-KVM.xml
3 MAS-KVM.qcow2
4 checksum.txt
5 <!--NeedCopy-->
```

```

root@ubuntu:~/mas-build#
root@ubuntu:~/mas-build# tar xvfz MAS-KVM-11.1-50.10.tgz
MAS-KVM.xml
checksum.txt
MAS-KVM-11.1-50.10.qcow2
root@ubuntu:~/mas-build# █

```

iv. バックアップオプションとして、MAS-KVM.xml のコピーを MAS1-KVM.xml という名前で作成します。vi エディターを使用して、MAS1-KVM.xml ファイルを開きます。

v. MAS1-KVM.xml で、次のネットワーク属性を編集します。

A. `name` -名前を指定します。

B. `mac` -MAC アドレスを指定します。

C. `source file` -ディスクイメージの絶対ソースパスを指定します。ファイルパスは絶対パスである必要があります。

注

ドメイン名と MAC アドレスは一意である必要があります。

D. `mode` -モードを指定します。

E. `model type` -VirtIO に設定します。

F. `source dev` -インターフェイスを指定します。

```

1 <name> MAS1-KVM</name>
2 <mac address='52:54:00:29:74:b3' />
3 <source file='/var/ MAS-KVM.qcow2' />
4 <source dev='eth0' mode='bridge' />
5 <model type='virtio' />
6 <!--NeedCopy-->

```

vi. 次のコマンドを使用して、MAS1-KVM.xml ファイルの仮想マシンの属性を定義します。`virsh define \<FileName\>.xml`

```

1 virsh define MAS-KVM.xml
2 Domain MAS defined from MAS-KVM.xml
3 <!--NeedCopy-->

```

```

root@ubuntu:~/mas-build# virsh define MAS-KVM.xml
Domain MAS defined from MAS-KVM.xml
root@ubuntu:~/mas-build# █

```

vii. 次のコマンドを入力して、NetScaler ADM を起動します。`virsh start \[ \<DomainName\> | \<DomainUUID\> \]`

```
1 virsh start MAS
2 Domain MAS started
3 <!--NeedCopy-->
```

```
root@ubuntu:/home/mas-build# virsh start MAS
Domain MAS started

root@ubuntu:/home/mas-build# █
```

- viii. 次のコマンドを使用して、NetScaler ADM 仮想マシンに接続できます。 `virsh console` `\<DomainName\>`

```
1 virsh console MAS
2 Connected to domain MAS
3 Escape character is ^]
4 <!--NeedCopy-->
```

```
root@ubuntu:/home/mas-build# virsh console MAS
Connected to domain MAS
Escape character is ^]
█
```

## CitrixApplication Delivery Management の構成

### 注

Linux KVM ホストによっては、複数の CPU が使用されていると、FreeBSD ゲストが正常に再起動しない場合があります。Citrix ADM 仮想アプライアンスを再起動すると、Citrix ADM CLI と GUI が応答しなくなります。詳細については、<https://bugs.launchpad.net/qemu/+bug/1329956> を参照してください。

NetScaler ADM 仮想アプライアンスの再起動時に NetScaler ADM CLI と GUI が応答しなくなるのを避けるには、KVM ホスト上のすべての仮想マシンをシャットダウンし、KVM ホストで次の操作を実行します。

1. 次のコマンドを使用して、`kvm_intel` モジュールを削除します。  
`rmmod kvm\*_intel`
2. 次のコマンドを使用して **APICv** を無効にし、`kvm_intel` モジュールをリロードします。  
`modprobe kvm\*_intel enable\*_apicv=N`
3. KVM ホスト上で仮想マシンを起動します。

NetScaler ADM をインストールした後、サービスが利用可能になるまで約 10 分ほどかかります。その後、NetScaler ADM にログオンします。

1. コマンドラインで、システム管理者のデフォルトの資格情報を使用してシステムにログオンします。

- ユーザー名: `nsroot`
- パスワード: `nsroot`

注

初めてログオンしたら、管理パスワードを変更します。管理パスワードを変更したら、ネットワークで機能するように MAS を構成します。パスワードは、NetScaler ADM ユーザーインターフェイスから変更できます。Citrix ADM ホームページから、[システム] > [ユーザー管理] > [ユーザー] に移動します。ユーザーを選択して **[Edit]** をクリックし、[Password] フィールドでパスワードを更新します。

2. プロンプトで、「`shell`」と入力します。
3. 「**networkconfig**」と入力して、Citrix ADM の初期ネットワーク構成メニューに入ります。管理 IP アドレスを構成します。
4. Citrix ADM の初期ネットワーク構成を完了するには、プロンプトに従います。コンソールには、Citrix ADM の次のパラメータを設定するための Citrix ADM 初期ネットワーク構成オプションが表示されます。ホスト名は、デフォルトで設定されています。
  - a) **2** を入力して Citrix ADM IPv4 アドレスを更新します-Citrix ADM にアクセスする管理 IP アドレス
  - b) 「**3**」を入力してネットマスク-管理 IP アドレスに関連付けられたサブネットマスクを更新します。
  - c) ゲートウェイ **IPv4** アドレス (Citrix ADM の管理 IP アドレスのサブネットのデフォルトゲートウェイ IP アドレス) を更新するには、**4** を入力します
  - d) 保存して終了するには **7** を入力します。設定の変更を保存し、システムを終了します。

```

Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
-----
 1. Citrix ADM Host Name [ADMHA1]:
 2. Citrix ADM IPv4 address [10.102.29.52]:
 3. Netmask [255.255.255.0]:
 4. Gateway IPv4 address [10.102.29.1]:
 5. DNS IPv4 Address [127.0.0.2]:
 6. Cancel and quit.
 7. Save and quit.
Select a menu item from 1 to 7 [7]:
    
```

5. シェルプロンプトで次のコマンドを入力して、展開スクリプトを実行します。 `deployment_type.py`
6. 表示される展開画面で、展開の種類を **NetScaler ADM** サーバーとして選択します。

```
-----  
Citrix ADM Deployment Configuration.  
The following menu enables you to select the components of your Citrix ADM deployment.  
Type the number of the component that you want to deploy, and then press Enter.  
For example, type 1 if you want to install as Citrix ADM Server.  
-----  
  
1. Citrix ADM Server.  
2. Remote Disaster Recovery Node.  
3. Cancel and exit.  
  
Select an option from 1 to 3 [3]: 
```

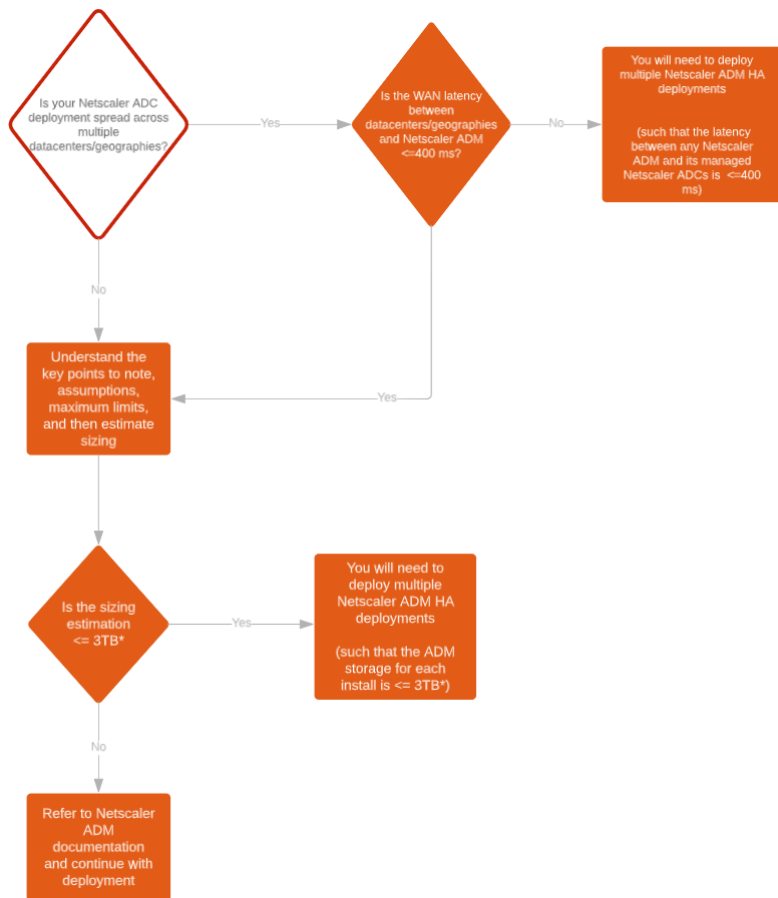
7. NetScaler ADM をスタンドアロン展開として展開するには、「**Yes**」と入力します。
8. 「はい」と入力して Citrix ADM サーバーを再起動します。
9. Citrix ADM サーバーを再起動したら、コマンドラインまたは GUI を使用してデフォルトの管理者資格情報を `nsroot/nsroot` として使用して Citrix ADM にログオンします。  
  
ブラウザのアドレスバーに Citrix ADM サーバーの IP アドレスを入力することで、後で Citrix ADM にアクセスできます。サーバにログオンするためのデフォルトの管理者認証情報は `nsroot/nsroot` です。

## 高可用性展開の構成

February 6, 2024

高可用性 (HA) とは、サービスを中断することなくユーザーが常に利用できるシステムを指します。高可用性セットアップは、システムのダウンタイム、ネットワークまたはアプリケーションの障害時に不可欠であり、どの企業にとっても重要な要件です。同じ構成のアクティブ/パッシブモードの 2 つの Citrix ADM ノードを高可用性展開することで、運用が中断されることはありません。

導入シナリオ



注

単一の NetScaler ADM HA 展開での検証済みの最大ストレージ制限は 3TB です。詳細については、『[導入ガイド](#)』を参照してください。

重要

**HTTPS** を使用して **Citrix ADM 12.1** ビルド **48.18** 以降のバージョンにアクセスするには:

Citrix ADM を高可用性モードで負荷分散するように Citrix ADC インスタンスを構成している場合は、まず Citrix ADC インスタンスを削除します。次に、高可用性モードで Citrix ADM にアクセスするためのフローティング IP アドレスを構成します。

Citrix ADM での高可用性展開の利点は次のとおりです:

- プライマリノードとセカンダリノード間のハートビートを監視するメカニズムが改善されました。
- 論理的な双方向レプリケーションの代わりに、データベースの物理ストリーミングレプリケーションを行います。

- プライマリノードにフローティング IP アドレスを構成できるため、個別の Citrix ADC ロードバランサーが不要になります。
- フローティング IP アドレスを使用して Citrix ADM ユーザーインターフェイスに簡単にアクセスできます。
- NetScaler ADM ユーザーインターフェイスは、プライマリノードでのみ提供されます。1 次ノードを使用することで、2 次ノードにアクセスして変更を行うリスクを排除できます。
- フローティング IP アドレスを設定するとフェイルオーバーの状況に対処でき、インスタンスを再設定する必要はありません。
- スプリットブレインの状況を検出して処理する機能が組み込まれています。

次の表は、高可用性導入で使用される用語をまとめたものです。

| 利用規約            | 説明                                                                                                                                                                                                                                   |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| プライマリノード        | 高可用性デプロイメントに登録された最初のノード。                                                                                                                                                                                                             |
| 2 次ノード          | 2 番目のノードが高可用性デプロイメントに登録されました。                                                                                                                                                                                                        |
| ハートビート          | 高可用性セットアップでプライマリノードとセカンダリノード間でメッセージを交換するために使用されるメカニズム。メッセージは、個々のノード上のアプリケーションのステータスとヘルスを決定します。                                                                                                                                       |
| フローティング IP アドレス | フローティング IP は、同じサブネット内のあるノードから別のノードに即座に移動できる IP アドレスです。内部的には、プライマリノードのネットワークインターフェースのエイリアスとして設定されます。フェイルオーバーが発生すると、フローティング IP アドレスは古いプライマリから新しいプライマリにシームレスに移動されます。これは、クライアントが 1 つの IP アドレスを使用して高可用性ノードと通信できるようにするため、高可用性セットアップに役立ちます。 |

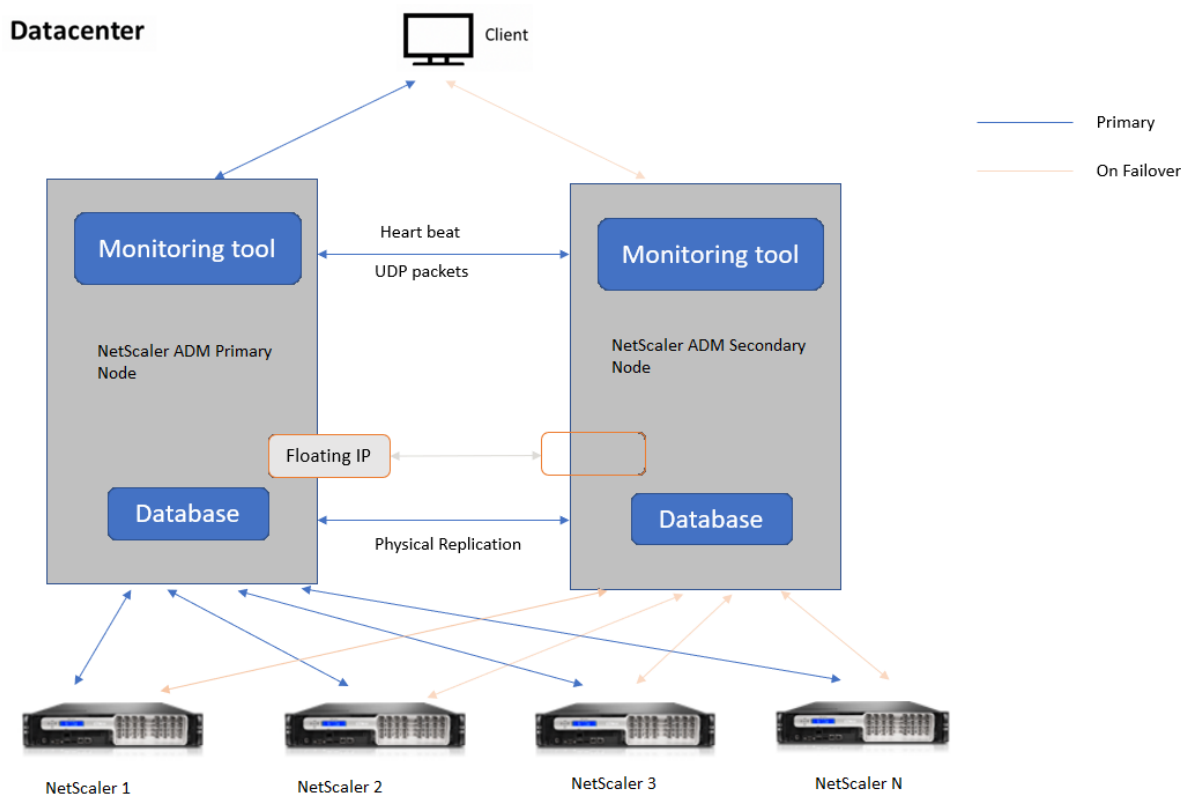
(注)

ポートとプロトコルの詳細については、「[ポート](#)」を参照してください。

## 高可用性アーキテクチャのコンポーネント

次の図は、高可用性モードで展開された 2 つの NetScaler ADM ノードのアーキテクチャを示しています。





高可用性展開では、一方の NetScaler ADM ノードがプライマリノード（MAS 1）として構成され、もう一方はセカンダリノード（MAS 2）として構成されます。何らかの理由でプライマリノードがダウンした場合、セカンダリノードが新しいプライマリノードとして引き継がれます。

## 監視ツール

監視ツールは、フェイルオーバー状況の監視、警告、処理に使用される内部プロセスです。ツールはアクティブで、各ノードで高可用性で実行されています。サブシステムの起動、両方のノードでのデータベースの起動、フェイルオーバーの有無のプライマリノードまたはセカンダリノードの決定などを行います。

## プライマリノード

プライマリノードは接続を受け入れ、インスタンスを管理します。AppFlow、SNMP、ログストリーム、syslog などのすべてのプロセスはプライマリノードによって管理されます。Citrix ADM ユーザーインターフェイスへのアクセスは、プライマリノードで利用できます。フローティング IP アドレスはプライマリノードで設定されます。

## 2次ノード

セカンダリノードは、プライマリノードから送信されたハートビートメッセージを聞きます。セカンダリノードのデータベースは読み取り/レプリカモードのみです。セカンダリノードではどのプロセスもアクティブではなく、セカン

ダリノードでは Citrix ADM ユーザーインターフェイスにアクセスできません。

### 物理ストリーミングレプリケーション

プライマリノードとセカンダリノードは、ハートビートメカニズムを介して同期します。データベースの物理ストリーミングレプリケーションでは、セカンダリノードはリードレプリカモードで起動します。セカンダリノードは、プライマリノードから受信したハートビートメッセージを聞きます。セカンダリノードが 180 秒間ハートビートを受信しない場合、プライマリノードはダウンしていると見なされます。次に、セカンダリノードがプライマリノードを引き継ぎます。

### ハートビートメッセージ

ハートビートメッセージは、プライマリノードとセカンダリノード間で送受信されるユーザーデータグラムパケット (UDP) です。Citrix ADM とデータベースのすべてのサブシステムを監視して、ノードの状態、状態、プロセスなどに関する情報を交換します。情報は、高可用性ノード間で毎秒共有されます。フェイルオーバーまたは高可用性状態の中断が発生した場合、通知はアラートとして管理者に送信されます。

### フローティング IP アドレス

フローティング IP アドレスは、高可用性セットアップのプライマリノードに関連付けられます。これはプライマリノードの IP アドレスに与えられるエイリアスで、クライアントはこれを使用してプライマリノードの Citrix ADM に接続できます。フローティング IP アドレスはプライマリノードで設定されるため、フェイルオーバーの場合にインスタンスを再構成する必要はありません。インスタンスは同じ IP アドレスに再接続して新しいプライマリにアクセスします。

### 注意すべき重要なポイント

- 高可用性設定では、両方の Citrix ADM ノードがアクティブ/パッシブモードで展開されます。これらは同じサブネット上にあり、同じソフトウェアバージョンとビルドを使用し、同じ構成でなければなりません。
- フローティング IP アドレス:
  - フローティング IP アドレスはプライマリノードで設定されます。
  - フェイルオーバーが発生した場合、インスタンスを再構成する必要はありません。
  - プライマリノードの IP アドレスまたはフローティング IP アドレスを使用して、ユーザーインターフェイスから高可用性ノードにアクセスできます。

#### 注

Citrix では、ユーザーインターフェイスへのアクセスにはフローティング IP アドレスを使用する

ことをお勧めします。

- データベース：
  - 高可用性セットアップでは、すべての構成ファイルが 1 分間隔でプライマリノードからセカンダリノードに自動的に同期されます。
  - データベースの同期は、データベースを物理的に複製することによって即座に行われます。
  - セカンダリノードのデータベースはリードレプリカモードです。

- NetScaler ADM アップグレード：

- 内部プロセスは、Citrix ADM を以前のバージョンから暗黙的にアップグレードします。

注

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

- UDP のデフォルトポート 5005 は、ハートビートを送信するノードとメッセージを受信するノードの両方で使用できます。

- MAC

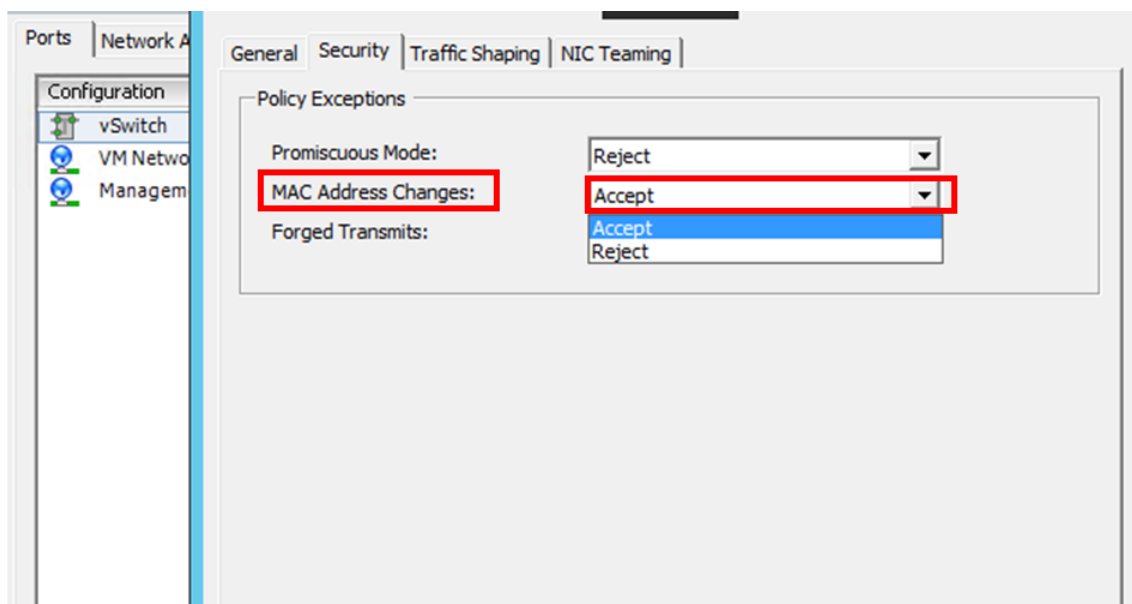
アドレスハイパーバイザーの「MAC アドレス変更」オプションの設定は、仮想マシンが受信するトラフィックに影響します。仮想スイッチで MAC アドレスの変更を有効にして、フェールオーバー後にフローティング IP アドレスが新しいプライマリノードにシームレスに移動できるようにします。

たとえば、Citrix ADM を VMware ESXi の高可用性環境にデプロイする場合は、MAC アドレスの変更を受け入れるようにしてください。ESXi では、アクティブ MAC アドレスを初期 MAC アドレス以外に変更する要求が許可されるようになりました。

注：

ESXi バージョン 6.7 にデプロイされた Citrix ADM では、**MAC** アドレス変更オプションも拒否に設定できます。フェールオーバー後、トラフィックは **MAC Address Changes** の設定に関係なく、新しいプライマリノードにシームレスに流れます。したがって、MAC アドレスの変更を受け入れることは必須ではありません。

NetScaler ADM が 6.7 より低いバージョンの ESXi に展開されている場合は、**[MAC アドレスの変更]** オプションが **[承認のみ]** に設定されていることを確認します。



#### 前提条件

Citrix ADM ノードの高可用性を設定する前に、次の前提条件に注意してください：

- Citrix ADM 高可用性デプロイメントは、Citrix ADM バージョン 12.0 ビルド 51.24 からサポートされています。
- Citrix Application Delivery Management イメージファイル (.xva) を Citrix のダウンロードサイトからダウンロードします。 <https://www.citrix.com/downloads/>

Citrix では、スケジューリング動作とネットワーク遅延を改善するために、(仮想マシンのプロパティで) CPU 優先度を最高レベルに設定することを推奨しています。

次の表は、仮想コンピューティングリソースの最小要件を示しています。

| コンポーネント | 条件              |
|---------|-----------------|
| RAM     | <b>32 GB</b>    |
| 仮想 CPU  | <b>8 基の CPU</b> |

| コンポーネント           | 条件                                                                                                                                                                                                                                                                                                           |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 記憶域               | Citrix ADM 展開では、ソリッドステートドライブ (SSD) テクノロジを使用することをお勧めします。デフォルト値は 120GB です。実際のストレージ要件は、NetScaler ADM のサイズ設定の見積もりによって異なります。Citrix ADM ストレージ要件が 120 GB を超える場合は、追加のディスクを接続する必要があります。<br>注: 追加できるディスクは 1 つだけです。初期展開の時点で、記憶域を見積もり、追加のディスクを接続することをお勧めします。詳しくは、「 <a href="#">Citrix ADM に追加ディスクを接続する方法</a> 」を参照してください。 |
| 仮想ネットワークインターフェイス  | 1                                                                                                                                                                                                                                                                                                            |
| スループット            | 1Gbps または 100Mbps                                                                                                                                                                                                                                                                                            |
| ハイパーバイザー          | バージョン                                                                                                                                                                                                                                                                                                        |
| Citrix Hypervisor | 6.2 と 6.5                                                                                                                                                                                                                                                                                                    |
| VMware ESXi       | 5.5 と 6.0                                                                                                                                                                                                                                                                                                    |
| Microsoft Hyper-V | 2012 R2                                                                                                                                                                                                                                                                                                      |
| Linux KVM         | Ubuntu と Fedora                                                                                                                                                                                                                                                                                              |

### Citrix ADM を高可用性モードでセットアップするには

1. 最初のサーバー (プライマリノード) を登録してデプロイします。
2. 2 番目のサーバー (2 次ノード) を登録してデプロイします。
3. 高可用性セットアップ用にプライマリノードとセカンダリノードをデプロイします。

### 最初のサーバー (プライマリノード) を登録してデプロイする

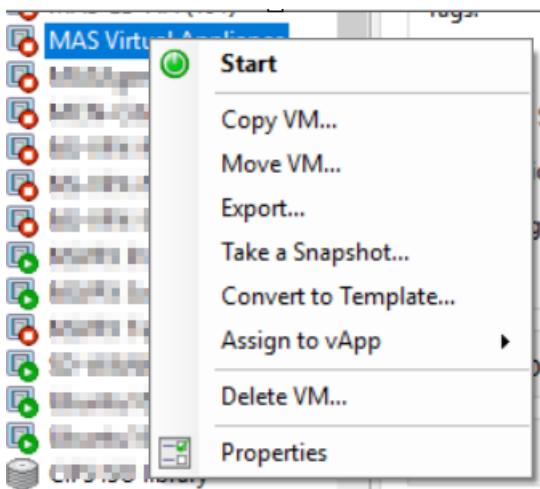
最初のノードを登録するには:

1. Citrix のダウンロードサイトからダウンロードした.xva イメージファイルを使用して、ハイパーバイザーにインポートします。

注:

.xva イメージファイルをインポートして開始するまでに数分かかる場合があります。画面下部にステータスが表示されます。

2. インポートが成功したら、右クリックして [開始] をクリックします。



3. [コンソール] タブから、初期ネットワーク構成で Citrix ADM を構成します。

```

Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([ ]).
Selecting the listed number allows the address to be changed.
-----
 1. Citrix ADM Host Name [ADMHA1]:
 2. Citrix ADM IPv4 address [10.102.29.52]:
 3. Netmask [255.255.255.0]:
 4. Gateway IPv4 address [10.102.29.1]:
 5. DNS IPv4 Address [127.0.0.2]:
 6. Cancel and quit.
 7. Save and quit.
-----
Select a menu item from 1 to 7 [7]:
    
```

4. 初期ネットワーク設定が完了すると、ログインのプロンプトが表示されます。次の認証情報(*nsrecover/nsroot*)を使用してログオンします。

注

ログオン後、初期ネットワーク構成を更新する場合は、`networkconfig`を入力し、構成を更新し、構成を保存します。

5. プライマリノードをデプロイするには、`/mps/deployment_type.py` と入力します。Citrix ADM 展開構成メニューが表示されます。

```
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-----

1. Citrix ADM Server.
2. Remote Disaster Recovery Node.
3. Cancel and exit.

Select an option from 1 to 3 [3]: 
```

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

```
bash-3.2# /mps/deployment_type.py
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-----

1. Citrix ADM Server.
2. Remote Disaster Recovery Node.
3. Cancel and exit.

Select an option from 1 to 3 [3]: 
```

7. コンソールで、NetScaler ADM スタンドアロン展開を選択するように求められます。**No** と入力して、展開を高可用性として確認します。

```
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-----

1. Citrix ADM Server.
2. Remote Disaster Recovery Node.
3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
Citrix ADM Standalone deployment [yes/no]:no
```

8. コンソールに、最初のサーバ・ノードを選択するように求められます。**Yes** と入力して、ノードを最初のノードとして確認します。

```
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-----

1. Citrix ADM Server.
2. Remote Disaster Recovery Node.
3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
Citrix ADM Standalone deployment [yes/no]:no
First Server Node for Citrix ADM [yes/no]:yes
```

9. コンソールに、システムの再起動を求めるメッセージが表示されます。「Yes」と入力して再起動します。

```
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-----

1. Citrix ADM Server.
2. Remote Disaster Recovery Node.
3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
Citrix ADM Standalone deployment [yes/no]:no
First Server Node for Citrix ADM [yes/no]:yes
Restart the system for the configuration to take effect. Do you want to restart?
[yes/no]:yes
```

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

## 2 台目のサーバー (2 次ノード) を登録してデプロイします

1. **Citrix** のダウンロードサイトからダウンロードした **.xva** イメージファイルを使用して、ハイパーバイザーにインポートします。
2. [コンソール] タブから、次の図に示す初期ネットワーク構成で Citrix ADM を構成します。
3. 初期ネットワーク設定が完了すると、システムはログインを要求します。次の認証情報 (*nsrecover/nsroot*) を使用してログオンします。



## 注

ログオン後、初期ネットワーク構成を更新する場合は、`networkconfig`を入力し、構成を更新し、構成を保存します。

4. セカンダリノードをデプロイするには、`/mps/deployment_type.py` と入力します。Citrix ADM 展開構成メニューが表示されます。
5. **1** を選択して Citrix ADM サーバーをセカンダリノードとして登録します。
6. コンソールでは、Citrix ADM をスタンドアロン展開として選択するよう求められます。**No** と入力して、展開を高可用性として確認します。
7. コンソールでは、最初のサーバーノードを選択するよう求められます。**No** を入力して、ノードを 2 番目のサーバとして確認します。

```
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-----

1. Citrix ADM Server.
2. Remote Disaster Recovery Node.
3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
Citrix ADM Standalone deployment [yes/no]:no
First Server Node for Citrix ADM [yes/no]:no
```

8. コンソールでは、プライマリノードの IP アドレスとパスワードを入力するよう求められます。

```
-----

1. Citrix ADM Server.
2. Remote Disaster Recovery Node.
3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
Citrix ADM Standalone deployment [yes/no]:no
First Server Node for Citrix ADM [yes/no]:no

-----

Server node Configuration. This menu allows you to specify server ip address and password.
Enter 0 anytime for cancel and quit.
-----

Enter Citrix ADM IP Address:10.102.29.52
Enter password for Citrix ADM:
```

9. コンソールに、フローティング IP アドレスの入力を求めるプロンプトが表示されます。

```

-----
 1. Citrix ADM Server.
 2. Remote Disaster Recovery Node.
 3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
Citrix ADM Standalone deployment [yes/no]:no
First Server Node for Citrix ADM [yes/no]:no

-----
          Server node Configuration. This menu allows you to specify server ip
address and password.
          Enter 0 anytime for cancel and quit.
-----

Enter Citrix ADM IP Address:10.102.29.52
Enter password for Citrix ADM:
Enter Floating IP address:10.102.29.97

```

10. コンソールに、システムの再起動を求めるメッセージが表示されます。「Yes」と入力して再起動します。

注

- ノードの高可用性導入には、フローティング IP アドレスが必須です。
- 設定に問題がある場合、システムはエラーメッセージを表示します。
- システムが再起動し、設定が有効になるまでに数分かかります。

### プライマリノードとセカンダリノードを高可用性ペアとしてデプロイ

登録後、プライマリノードとセカンダリノードの両方が Citrix ADM ユーザーインターフェイスに表示されます。これらのノードを高可用性ペアにデプロイします。

注

- ノードを高可用性ペアにデプロイする前に、初期ネットワーク構成後にセカンダリノードの再起動が完了していることを確認してください。
- 高可用性展開が完了したら、フローティング IP アドレスを使用して Citrix ADM ユーザーインターフェイスにアクセスします。

ノードを高可用性ペアとしてデプロイするには:

1. Web ブラウザーを開き、最初の Citrix ADM サーバーノードの IP アドレスを入力します。
2. 「ユーザー名」フィールドと「パスワード」フィールドに、管理者の資格情報を入力します。
3. ホームページの「はじめに」をクリックします。

4. 展開の種類として、[高可用性モードで展開された **2** つのサーバー] を選択し、[次へ] をクリックします。
5. [配置] ページで、[配置] をクリックします。
6. 確認メッセージが表示されます。[はい] をクリックします。

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

注

これで、Floating IP アドレスの使用を開始できます。

7. 管理者資格情報を使用して Citrix ADM にログオンし、ホームページで「はじめに」をクリックし、オプションで次の操作を行います：
  - a) NetScaler ADC インスタンスの追加
  - b) カスタマー ID の設定

注

[スキップ] をクリックして後で完了し、[完了] をクリックすることもできます。

8. [システム] > [配置] に移動して、配置を検証します。

詳細については、「[よく寄せられる質問](#)」を参照してください。

## 高可用性の無効化

Citrix ADM 高可用性ペアで高可用性を無効にして、ノードをスタンドアロンの Citrix ADM サーバーに変換できます。

注

プライマリノードからの高可用性を無効にします。

高可用性を無効にするには：

1. Web ブラウザーで、Citrix ADM サーバーのプライマリノードの IP アドレスを入力します。
2. [ユーザー名] フィールドと [パスワード] フィールドに、管理者の資格情報を入力します。
3. [システム] タブで、[展開] に移動し、[高可用性の解除] をクリックします。

ダイアログボックスが表示されます。[はい] をクリックすると、高可用性デプロイが中断されます。

## 高可用性を再デプロイ

スタンドアロンデプロイで高可用性を無効にした後は、再び高可用性モードに再デプロイできます。高可用性の再デプロイは、高可用性を初めてデプロイする場合と同様です。詳細については、「[プライマリノードとセカンダリノードを高可用性ペアとしてデプロイする](#)」を参照してください。

## 高可用性フェイルオーバーのシナリオ

フェイルオーバーが実行されるのは、次のいずれかの状態が検出された場合です。

- ノード障害: プライマリノードがダウンし、プライマリノードからハートビートが 180 秒間検出されません。
- アプリケーションの正常性障害: プライマリノードが稼働していますが、NetScaler ADM プロセスの 1 つが停止しています。

## スプリットブレインシナリオ

ネットワークリンクのダウンタイムが原因で両方のノード間で通信が切断された場合は、次のようになります。

- プライマリノードは引き続きプライマリとして動作します
- ハートビートを受信できなかったため、セカンダリノードがプライマリノードを引き継ぎます
- 両方のノードが個別のデータベースインスタンスを実行します

たとえば、企業では、2 つの Citrix ADM ノードがプライマリとセカンダリとして展開されています。ネットワークリンクのダウンタイムが発生する可能性があるため、2 つの Citrix ADM ノード間の通信は完全に切断されます。180 秒以上ハートビートの交換が行われなため、どちらのノードも自身をプライマリノードと見なします。両方のノードは、アクティブなノードとして機能し、データベースの独自のインスタンスを実行します。

Citrix ADM 12.1 以降のリリースでは、このスプリットブレインの状況は、ネットワークリンクとハートビートが復元された後に正常に処理されます。高可用性同期は自動的に復元されます。回復時間は、ノード間のリンクのデータと速度によって異なります。

### 注

スプリットブレイン状態では、古いプライマリノードで発生した変更は、高可用性で再結合されたときに新しいプライマリノードにリセットされます。スプリットブレイン中に新しいプライマリノードで発生した変更はそのまま残ります。

## 高可用性を実現するためのディザスタリカバリの構成

February 6, 2024

災害（さいがん）とは、自然の災害、または人為的な出来事によって引き起こされる事業機能の突然の混乱である。災害はデータセンターの運用に影響を及ぼします。その後、災害現場で失われたリソースとデータを完全に再構築して復元する必要があります。データ消失やデータセンターのダウンタイムは重要であり、ビジネス継続性が低下します。

NetScaler ADM ディザスタリカバリ (DR) 機能は、高可用性モードで展開された NetScaler ADM 完全なシステムバックアップとリカバリ機能を提供します。リカバリ時には、証明書、構成ファイル、およびデータベースの完全なバックアップがリカバリサイトで使用できます。

次の表では、Citrix ADM で障害復旧を構成する際に使用される用語について説明します。

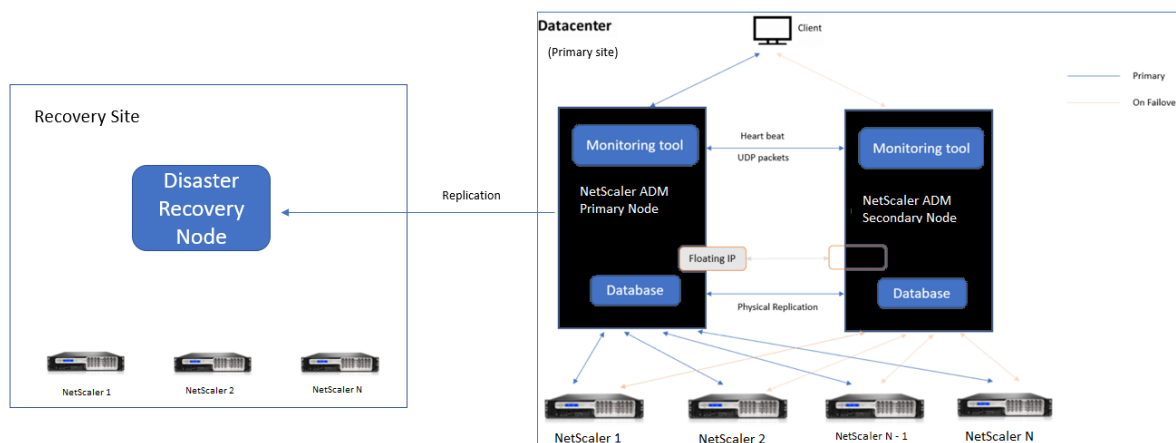
| 利用規約                 | 説明                                                                                                    |
|----------------------|-------------------------------------------------------------------------------------------------------|
| プライマリサイト (データセンター A) | プライマリサイトには、高可用性モードで展開された NetScaler ADM ノードがあります。                                                      |
| リカバリサイト (データセンター B)  | リカバリ・サイトには、スタンドアロン・モードで展開された災害復旧ノードがあります。このノードは読み取り専用モードで、プライマリサイトがダウンするまで動作しません。                     |
| 災害復旧ノード              | リカバリ・ノードは、リカバリ・サイトにデプロイされたスタンドアロン・ノードです。このノードは、プライマリ・サイトで災害が発生し、それが機能しない場合に備えて、新しいプライマリに対して動作可能になります。 |

注: プライマリサイトと DR サイトは、ポート 5454 と 22 を介して相互に通信します。これらのポートはデフォルトで有効になっています。  
 ポートとプロトコルの詳細については、「[ポート](#)」を参照してください。

### ディザスタリカバリのワークフロー

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

#### 災害発生前の初期設定



この図は、ディザスタ前のディザスタリカバリ設定を示しています。

プライマリサイトには、高可用性モードで展開された NetScaler ADM ノードがあります。詳しくは、「[高可用性展開](#)」を参照してください。

リカバリサイトには、スタンドアロンの NetScaler ADM 災害復旧ノードがリモートで展開されています。災害復旧ノードは読み取り専用モードであり、プライマリノードからデータを受信してデータバックアップを作成します。リカバリサイトの Citrix ADC インスタンスも検出されますが、それらを通過するトラフィックはありません。バックアッププロセス中、すべてのデータ、ファイル、および構成は、プライマリノードからディザスタリカバリノードに複製されます。

### 前提条件

障害回復ノードをセットアップする前に、次の前提条件に注意してください：

- 障害回復設定を有効にするには、プライマリサイトの Citrix ADM ノードが高可用性モードで構成されている必要があります。
- プライマリサイトでの Citrix ADM スタンドアロン展開は、障害回復機能をサポートしていません。
- Citrix ADM HA ペア（プライマリサイト内）とスタンドアロンノード（DR サイト内）のソフトウェアバージョン、ビルド、構成は同じである必要があります。

Citrix では、スケジューリング動作とネットワーク遅延を改善するために、（仮想マシンのプロパティで）CPU 優先度を最高レベルに設定することを推奨しています。

次の表は、ディザスタリカバリノードを設定するための最小要件を示しています。

| コンポーネント          | 条件                                                                                                                                                                                                                                                                                                                      |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RAM              | 32 GB                                                                                                                                                                                                                                                                                                                   |
| 仮想 CPU           | 8 基の CPU                                                                                                                                                                                                                                                                                                                |
| 記憶域              | NetScaler ADM 展開では、ソリッドステートドライブ (SSD) テクノロジーを使用することをお勧めします。デフォルト値は 120GB です。実際のストレージ要件は、NetScaler ADM のサイズ設定の見積もりによって異なります。Citrix ADM ストレージ要件が 120 GB を超える場合は、追加のディスクを接続する必要があります。<br>注: 追加できるディスクは 1 つだけです。初期展開時には、ストレージを見積もり、より多くのディスクを接続することをお勧めします。詳しくは、「 <a href="#">NetScaler ADM に追加のディスクを接続する方法</a> 」を参照してください。 |
| 仮想ネットワークインターフェイス | 1                                                                                                                                                                                                                                                                                                                       |

| コンポーネント           | 条件                |
|-------------------|-------------------|
| スループット            | 1Gbps または 100Mbps |
| ハイパーバイザー          | バージョン             |
| Citrix Hypervisor | 6.2 と 6.5         |
| VMware ESXi       | 5.5 と 6.0         |
| Microsoft Hyper-V | 2012 R2           |
| Linux KVM         | Ubuntu と Fedora   |

---

### 初めてのディザスタリカバリのセットアップ

- 高可用性モードで NetScaler ADM を展開する
- NetScaler ADM 障害回復ノードを展開して登録する
- ユーザーインターフェイスからディザスタリカバリ設定を有効または無効にする

### 高可用性モードで **NetScaler ADM** を展開する

ディザスタリカバリ設定を設定するには、NetScaler ADM が高可用性モードで展開されていることを確認します。NetScaler ADM を高可用性で展開する方法については、「[高可用性展開](#)」を参照してください。

#### 注

- 高可用性モードでデプロイされた Citrix ADM は、Citrix ADM リリースバージョン 13.0 にアップグレードする必要があります。
- 障害復旧ノードをプライマリノードに登録するには、**Floating IP** アドレスが必須です。

### DR コンソールを使用して **Citrix ADM** 災害復旧ノードを展開して登録する

NetScaler ADM 災害復旧ノードを登録するには:

1. Citrix のダウンロードサイトから、**.xva** イメージファイルをダウンロードし、ハイパーバイザーにインポートします。
2. [コンソール] タブから、初期ネットワーク構成で Citrix ADM を構成します。

#### 注

災害復旧ノードは、別のサブネット上に配置できます。

```

-----
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
-----

  1. Citrix ADM Host Name [DR]:
  2. Citrix ADM IPv4 address [10.102.29.53]:
  3. Netmask [255.255.255.0]:
  4. Gateway IPv4 address [10.102.29.1]:
  5. DNS IPv4 Address [127.0.0.2]:
  6. Cancel and quit.
  7. Save and quit.

Select a menu item from 1 to 7 [7]: █

```

- 初期ネットワーク設定が完了すると、ログインのプロンプトが表示されます。次の認証情報を使用してログインします—nsrecover/nsroot.

**重要**

:登録中に DR ノードの認証情報 (nsrecover/nsroot) を変更しないでください。DR ノードが正  
常に登録されたら、DR ノードの認証情報を変更できます。

- 災害復旧ノードを展開するには、**/mps/deployment\_type.py** と入力し、Enter キーを押します。Citrix ADM 展開構成メニューが表示されます。

```

bash-3.2# /mps/deployment_type.py
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-----

  1. Citrix ADM Server.
  2. Remote Disaster Recovery Node.
  3. Cancel and exit.

Select an option from 1 to 3 [3]: █

```

- 災害復旧ノードを登録するには、**[ 2 ]** を選択します。



```
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-----
-----
1. Citrix ADM Server.
2. Remote Disaster Recovery Node.
3. Cancel and exit.

Select an option from 1 to 3 [3]: 2
Selected Option      2. Remote Disaster Recovery Node.
```

6. コンソールは、高可用性ノードの Floating IP アドレスとパスワードを要求します。
7. Floating IP アドレスとパスワードを入力して、障害復旧ノードをプライマリノードに登録します。

```
-----
Backup node Configuration.

Specify the IP address and the password of the Citrix ADM server.
Type 0 anytime to cancel and quit.
-----
Enter Citrix ADM Floating IP Address:10.102.29.97
Enter password for Citrix ADM:█
```

これで、災害復旧ノードが正常に登録されました。

```
Stopping appd
Stopping nsulfd
Stopped nsulfd
Stopped appd
waiting for server to shut down... done
server stopped
-----
Backup node Registration successful.
```

注：  
災害復旧ノードには GUI がありません。

8. DR ノードのパスワードを変更する場合は、次のスクリプトを実行します。

```
1 /mps/change_freebsd_password.sh <username> <password>
2 <!--NeedCopy-->
```

### NetScaler ADM GUI を使用して災害復旧ノードを展開する

DR コンソールを使用して災害復旧ノードが正常に登録されたら、Citrix ADM GUI から DR ノードを展開します。この手順により、Citrix ADM プライマリサイトからの障害回復設定が有効になります。

1. [システム] > [システム管理] > [障害回復の設定] に移動します。
2. 「障害回復」 ページで、「DR ノードのデプロイ」を選択します。

3. 確認ダイアログが表示されます。[Yes] をクリックして続行します。

注

システムバックアップにかかる時間は、データサイズと WAN リンク速度によって異なります。

Citrix ADM GUI で DR ノードを正常に展開すると、DR ノードのデータベースの状態、メモリ、CPU、およびディスク使用量を監視できます。

ディザスタリカバリ設定を無効にするには、「DR ノードを削除」を選択します。確認ダイアログが表示されます。[はい] をクリックして続行します。

DR ノードを再度有効にするには、高可用性ペアの DR ノードを再設定します：

1. Hypervisor または SSH コンソールを使用して DR ノードにログオンします。
2. DR コンソールを使用して NetScaler ADM 障害回復ノードを展開および登録する手順に従って、DR ノードを構成します。
3. NetScaler ADM GUI を使用してディザスタリカバリノードを展開します。

詳細については、[FAQ](#)を参照してください。

重要

- プライマリサイトで災害が発生したことを検出するのは、管理者の責任です。
- 災害復旧ワークフローは、プライマリサイトがダウンした後、管理者が手動で開始します。
- 管理者は、リカバリサイトのディザスタリカバリノードでリカバリスクリプトを実行して、プロセスを手動で開始する必要があります。
- プライマリサイトの HA ペアをアップグレードする場合は、DR サイトのスタンドアロンノードも手動でアップグレードする必要があります。

### 災害後のワークフロー

障害発生後にプライマリサイトがダウンした場合は、災害復旧ワークフローを次のように開始する必要があります。

1. 管理者は、プライマリ・サイトが障害に見舞われ、そのサイトが稼働していないことを確認しました。
2. 管理者がリカバリプロセスを開始します。
3. 管理者は、(リカバリサイトで) 要件に基づいて、障害復旧ノードで次のいずれかのリカバリスクリプトを手動で実行する必要があります。
  - DR ノードでの SNMP、Syslog、および分析の把握：

```
1 /mps/scripts/pgsql/pgsql_restore_remote_backup.sh
2
3 <!--NeedCopy-->
```

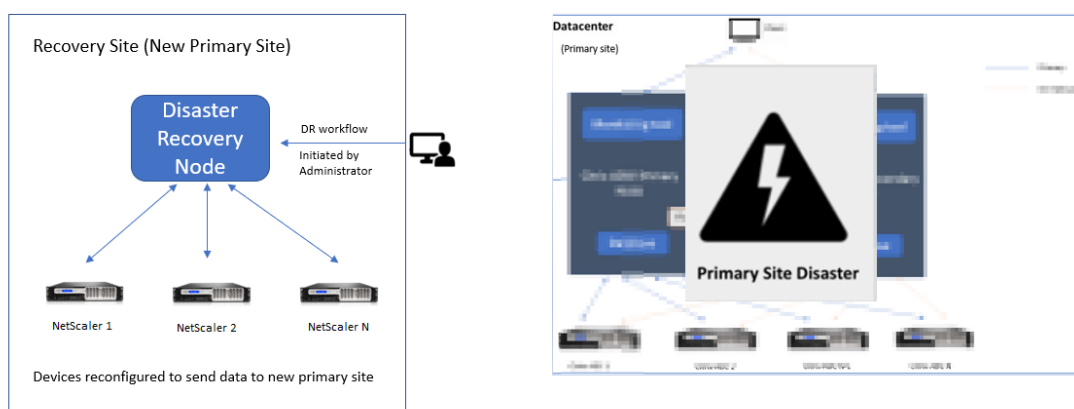
- DR ノードをライセンスサーバとしても設定します:

```

1 /mps/scripts/pgsql/pgsql_restore_remote_backup.sh -reconfig-
  ls <IP-address-of-the-primary-site>
2
3 <!--NeedCopy-->
    
```

4. 内部的には、NetScaler ADC インスタンスは、新しいプライマリサイトになった災害復旧ノードにデータを送信するように自動的に再構成されます。

次の図は、プライマリサイトに障害が発生した後の災害復旧ワークフローを示しています。



注:

DR サイトでスクリプトを開始すると、DR サイトが新しいプライマリサイトになります。また、DR ユーザーインターフェイスにアクセスすることもできます。

## 災害復旧後

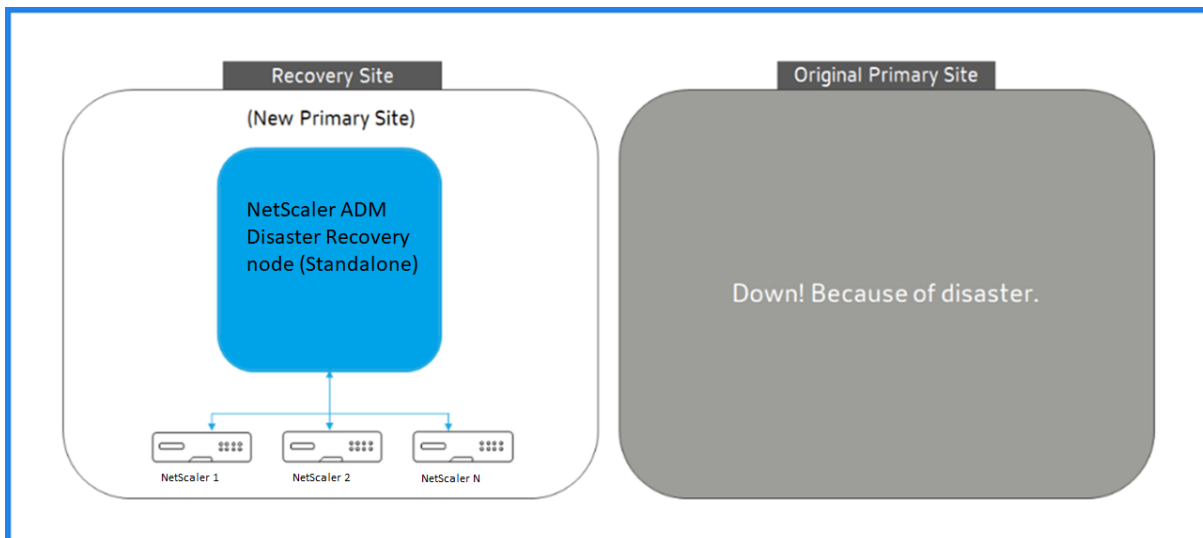
災害が発生し、管理者がリカバリ・スクリプトを開始すると、DR サイトが新しいプライマリ・サイトになります。後で構成を元のサイトに戻す場合は、「構成を元のプライマリサイトに戻す」を参照してください。

### 重要

- Citrix ADM 12.1.49.x 以前のリリースをインストールしている場合、Citrix ADM (DR サイト) で元のライセンスを再ホストするよう Citrix に連絡するまでの 30 日間の猶予期間があります。
- 12.1.50.x 以降のリリースでは、Citrix ADM ライセンスは自動的に DR サイトと同期されます (ライセンスについて Citrix に問い合わせる必要はありません)。
- DR サイトのプールライセンスは 12.1.50.x 以降のリリースでサポートされています。インスタンスにプールされたライセンスを適用している場合は、DR サイトにインスタンスを手動で再構成します。

## 構成を元のプライマリサイトに戻す

障害発生後、設定されたディザスタリカバリ (DR) ノードが新しいプライマリサイトになり、クライアントトラフィックはこのノードを経由します。



詳細については、「災害後のワークフロー」を参照してください。

元のプライマリサイトが災害から解放され、すべての操作をプライマリサイトに移動する場合は、DR ノードからの構成と一致するように元のプライマリサイトを再構成します。

開始する前に、プライマリサイトと DR サイトの両方がアクティブであることを確認します。

DR サイトから元のプライマリサイトへの変更を元に戻すには、次の手順を実行します。

1. 元のプライマリサイトにログインし、次のコマンドを実行します。

```
1 nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
  password> -L <primary-node-password> &
2 <!--NeedCopy-->
```

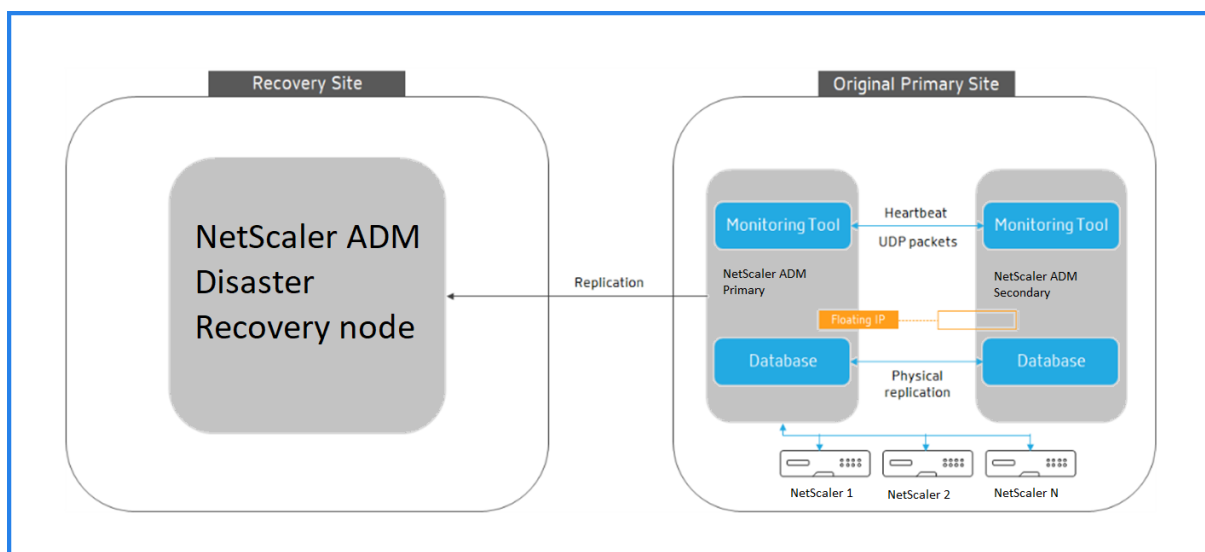
このコマンドは、プライマリサイトに Syslog、SNMP、Analytics のみを設定します。

プライマリサイトを ADC インスタンスのプールライセンスサーバーとして構成する場合は、次のコマンドを実行します。

```
1 nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
  password> -L <primary-node-password> -O yes &
2 <!--NeedCopy-->
```

-O コマンドは、DR サイトの IP アドレスを取得し、プライマリサイトをプールライセンスサーバーとして再構成します。

2. DR サイトを再構成します。ディザスタリカバリのセットアップを展開するを参照してください。



DR サイトから元のプライマリサイトに構成を正常に元に戻すと、クライアントトラフィックは NetScaler ADM プライマリノードを通過します。

## マルチサイト展開用にオンプレミスエージェントを構成する

February 6, 2024

以前のバージョンの NetScaler ADM では、リモートデータセンターに展開された NetScaler ADC インスタンスは、プライマリデータセンターで実行されている NetScaler ADM から管理および監視できます。NetScaler ADC インスタンスは、プライマリ NetScaler ADM に直接データを送信し、その結果、WAN 帯域幅を消費しました。また、分析データの処理には、プライマリ NetScaler ADM CPU とメモリリソースが使用されます。

データセンターを世界中に配置できます。エージェントは、次のシナリオで重要な役割を果たします。

- リモートデータセンターにエージェントをインストールして、WAN 帯域幅の消費量を削減する。
- データ処理のためにトラフィックをプライマリ NetScaler ADM に直接送信するインスタンスの数を制限する。

### 注

- リモートデータセンターにインスタンス用のエージェントをインストールすることは推奨されますが、必須ではありません。必要に応じて、ユーザーは NetScaler ADC インスタンスをプライマリ NetScaler ADM に直接追加できます。
- 1 つ以上のリモートデータセンターにエージェントをインストールした場合、エージェントとプライマリサイト間の通信は Floating IP アドレスを経由します。詳細については、[port](#) を参照してください。
- エージェントをインストールして、1 つ以上のリモートデータセンターのインスタンスにプールされたラ

ライセンスを適用できます。このシナリオでは、プライマリサイトと1つまたは複数のリモートデータセンター間の通信はフローティング IP アドレスを介して行われます。

NetScaler ADM 12.1 以降では、インスタンスをエージェントで構成して、別のデータセンターにあるプライマリ NetScaler ADM と通信できます。

エージェントは、プライマリ NetScaler ADM と、異なるデータセンターで検出されたインスタンスの間の仲介者として動作します。エージェントをインストールする利点は次のとおりです。

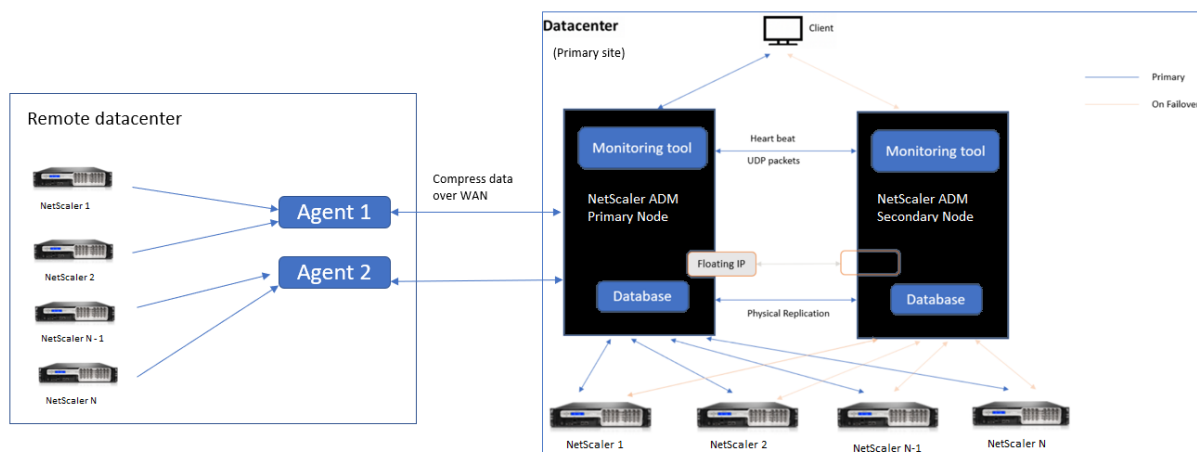
- インスタンスはエージェントに対して構成され、未処理のデータがプライマリ NetScaler ADM ではなくエージェントに直接送信されます。エージェントは第 1 レベルのデータ処理を行い、処理されたデータを圧縮形式でプライマリ NetScaler ADM に送信して格納します。
- エージェントとインスタンスは同じデータセンター内に配置されるため、データ処理が高速化されます。
- エージェントをクラスタリングすると、エージェントのフェイルオーバー時に NetScaler ADC インスタンスが再配布されます。サイト内の 1 つのエージェントに障害が発生すると、NetScaler ADC イ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。

### 注

サイトごとにインストールされるエージェントの数は、処理されるトラフィックによって異なります。

## アーキテクチャ

次の図は、2つのデータセンターにおける NetScaler ADC インスタンスと、マルチサイトエージェントベースのアーキテクチャを使用した NetScaler ADM の高可用性展開を示しています。



プライマリサイトには、高可用性構成で展開された NetScaler ADM ノードがあります。プライマリサイトの NetScaler ADC インスタンスは、NetScaler ADM に直接登録されます。

セカンダリサイトでは、エージェントがプライマリサイトの NetScaler ADM サーバーに展開され、登録されます。これらのエージェントはクラスタ内で動作し、エージェントのフェイルオーバーが発生した場合にトラフィックの継続的なフローを処理します。セカンダリサイトの NetScaler ADC インスタンスは、そのサイト内のエージェントを

介してプライマリ NetScaler ADM サーバーに登録されます。インスタンスは、プライマリ NetScaler ADM ではなく、エージェントにデータを直接送信します。エージェントは、インスタンスから受信したデータを処理し、圧縮形式でプライマリ NetScaler ADM に送信します。エージェントは安全なチャンネルを介して NetScaler ADM サーバーと通信し、チャンネルを介して送信されるデータは帯域幅の効率化のために圧縮されます。

### 開始

- エージェントをデータセンターにインストールする
  - エージェントを登録する
  - エージェントをサイトに接続する
- NetScaler ADC インスタンスの追加
  - 新しいインスタンスを追加する
  - 既存のインスタンスを更新する

### エージェントをデータセンターにインストールする

エージェントをインストールして構成して、プライマリ NetScaler ADM と他のデータセンターで管理対象の NetScaler ADC インスタンス間の通信を有効にできます。

エンタープライズデータセンターの次のハイパーバイザーにエージェントをインストールできます。

- Citrix Hypervisor
- VMware ESXi
- Microsoft Hyper-V
- Linux KVM サーバー

### 注

マルチサイト展開用のオンプレミスエージェントは、NetScaler ADM 高可用性展開でのみサポートされます。

エージェントのインストールを開始する前に、Hypervisor が各エージェントに提供する必要のある仮想コンピューティングリソースがあることを確認してください。

---

| コンポーネント | 条件       |
|---------|----------|
| RAM     | 32 GB    |
| 仮想 CPU  | 8 基の CPU |

| コンポーネント           | 条件    |
|-------------------|-------|
| 記憶域               | 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            | 1Gbps |

#### ポート

通信のために、エージェントと NetScaler ADM オンプレミスサーバーの間で次のポートを開く必要があります。

| 種類  | ポート             | 詳細                                            | コミュニケーションの方向                              |
|-----|-----------------|-----------------------------------------------|-------------------------------------------|
| TCP | 8443, 7443, 443 | エージェントと NetScaler ADM オンプレミスサーバー間の送信および受信通信用。 | NetScaler ADM エージェントから NetScaler ADM への接続 |

エージェントと NetScaler ADC インスタンスの間で次のポートが開いている必要があります。

|種類|ポート|詳細|コミュニケーションの方向|

|---|---|---|---|

|TCP|80|エージェントと NetScaler ADC または Citrix SD-WAN インスタンス間の NITRO 通信用。|NetScaler ADM から NetScaler ADC へ、NetScaler ADC から NetScaler ADM へ|

|TCP|22|エージェントと NetScaler ADC または Citrix SD-WAN インスタンス間の SSH 通信用。高可用性モードで展開された NetScaler ADM サーバー間の同期用。|NetScaler ADM から NetScaler ADC に、NetScaler ADM エージェントは NetScaler ADC に|

|UDP|4739|エージェントと NetScaler ADC または Citrix SD-WAN インスタンス間の AppFlow ow 通信用。|NetScaler ADC または Citrix SD-WAN から NetScaler ADM へ|

|ICMP|予約ポートなし|NetScaler ADM と NetScaler ADC インスタンス、SD WAN インスタンス、または高可用性モードで展開されたセカンダリ NetScaler ADM サーバー間のネットワーク到達可能性を検出するには。|

|UDP|161、162|NetScaler ADC インスタンスからエージェントに SNMP イベントを受信するには。|ポート 161-NetScaler ADM から NetScaler ADC|

|||ポート 162-NetScaler ADC から NetScaler ADM へ|UDP

|514|NetScaler ADC または Citrix SD-WAN インスタンスからエージェントへの syslog メッセージを受信するには。|NetScaler ADC または Citrix SD-WAN から Citrix

ADM||TCP|5557|エージェントと NetScaler ADC インスタンス間のログストリーム通信用。|Citrix ADC から NetScaler ADM|



エージェントを登録する

1. Citrix ダウンロードサイトからダウンロードしたエージェントイメージファイルを使用して、ハイパーバイザーにインポートします。<Version.no\> エージェントイメージファイルの命名パターンは、**MASAGENT-\<HYPERVISOR\>**です。例: **MASAGENT-XEN-13.0-xy.xva**
2. [コンソール] タブから、初期ネットワーク構成で Citrix ADM を構成します。
3. NetScaler ADM ホスト名、IPv4 アドレス、およびゲートウェイの IPv4 アドレスを入力します。オプション 7 を選択して、設定を保存して終了します。

```
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
-----
1. Citrix ADM Host Name [ADMAGENT]:
2. Citrix ADM IPv4 address [10.102.29.214]:
3. Netmask [255.255.255.0]:
4. Gateway IPv4 address [10.102.29.1]:
5. DNS IPv4 Address [127.0.0.2]:
6. Cancel and quit.
7. Save and quit.
-----
Select a menu item from 1 to 7 [7]: 7
```

4. 登録が成功すると、コンソールはログオンを要求します。資格情報として *nsrecover/nsroot* を使用します。
5. エージェントを登録するには、**/mps/register\_agent\_onprem.py** と入力します。Citrix ADM エージェント登録資格情報は、次の図のように表示されます。
6. NetScaler ADM フローティング IP アドレスとユーザー資格情報を入力します。

```
bash-3.2# /mps/register_agent_onprem.py
-----
Citrix ADM Agent Registration with Citrix ADM On-Prem Server. This menu allows you to specify Citrix ADM Server IP Address and admin credentials.
If Citrix ADM is deployed in HA mode, it is advisable to register with Citrix ADM floating IP Address.
-----
Enter IP Address or URL:10.102.29.211
Enter User Name:nsroot
Enter Password:
-----
Trying to register this agent with Citrix ADM 10.102.29.211
Dec 3 18:07:52 <auth.notice> ns date: date set by nsrecover
-----
Citrix ADM Agent Registration successful.
-----
```

登録が成功すると、エージェントは再起動してインストールプロセスを完了します。

エージェントが再起動したら、NetScaler ADM GUI にアクセスし、メインメニューから [ネットワーク] > [エージェント] ページに移動してエージェントの状態を確認します。新しく追加されたエージェントは **Up** 状態になります。

### 注

NetScaler ADM はエージェントのバージョンを表示し、エージェントが最新バージョンであるかどうかを確認します。ダウンロードアイコンは、エージェントが最新バージョンではなく、アップグレードが必要であることを示します。エージェントのバージョンを NetScaler ADM バージョンにアップグレードすることをお勧めします。

### エージェントをサイトに接続する

1. エージェントを選択し、「サイトを接続」をクリックします。
2. [サイトの添付] ページで、リストからサイトを選択するか、プラス (+) ボタンを使用してサイトを作成します。
3. 「保存」をクリックします。

### 注

- デフォルトでは、新しく登録されたすべてのエージェントがデフォルトのデータセンターに追加されます。
- エージェントを正しいサイトに関連付けることが重要です。エージェントに障害が発生した場合、エージェントに割り当てられた NetScaler ADC インスタンスは、同じサイト内の他の機能しているエージェントに自動的に切り替わります。

### エージェントアクション

[ネットワーク] > [エージェント] > [アクションの選択] で、エージェントにさまざまなアクションを適用できます。

[アクションの選択] では、次の機能を使用できます。

新しい証明書をインストールする: セキュリティ要件を満たすために別のエージェント証明書が必要な場合は、証明書を追加できます。

デフォルトのパスワードを変更する: インフラストラクチャのセキュリティを確保するために、エージェントのデフォルトのパスワードを変更します。

テクニカルサポートファイルを生成する: 選択した NetScaler ADM 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、Citrix テクニカルサポートに送信して、調査とトラブルシューティングを行うことができます。

### NetScaler ADC インスタンスの追加

インスタンスは、エージェントを介して NetScaler ADM から検出、管理、監視する Citrix アプライアンスまたは仮想アプライアンスです。次の Citrix アプライアンスおよび仮想アプライアンスを NetScaler ADM またはエージェントに追加できます。

- NetScaler ADC MPX
- NetScaler ADC VPX
- NetScaler ADC SDX
- NetScaler ADC CPX
- NetScaler Gateway
- Citrix の SSL 転送プロキシ
- Citrix SD-WAN WO

詳しくは、「[NetScaler ADM へのインスタンスの追加](#)」を参照してください。

既存のインスタンスをエージェントにアタッチする

プライマリ NetScaler ADM にインスタンスがすでに追加されている場合は、エージェントを編集してエージェントにアタッチできます。

1. [ネットワーク] > [インスタンス] に移動し、インスタンスタイプを選択します。たとえば、NetScaler ADC などです。
2. [Edit] をクリックして、既存のインスタンスを編集します。
3. エージェントをクリックして選択します。
4. [Agent] ページで、インスタンスを関連付けるエージェントを選択し、[OK] をクリックします。

注:

インスタンスを関連付ける サイト を選択してください。

インスタンスの **GUI** にアクセスしてイベントを検証する

インスタンスが追加され、エージェントが設定されたら、インスタンスの GUI にアクセスして、トラップ宛先が設定されているかどうかを確認します。

Citrix ADM で、[ネットワーク] > [インスタンス] に移動します。[インスタンス] で、アクセスするインスタンスのタイプ (NetScaler ADC VPX など) を選択し、特定のインスタンスの IP アドレスをクリックします。

選択したインスタンスの GUI がポップアップウィンドウに表示されます。

デフォルトでは、エージェントはインスタンスのトラップ送信先として設定されます。確認するには、インスタンスの GUI にログオンし、トラップの送信先を確認します。

重要

リモートデータセンターに NetScaler ADC インスタンス用のエージェントを追加することをお勧めしますが、

必須ではありません。

インスタンスをプライマリ MAS に直接追加する場合は、インスタンスの追加中にエージェント を選択しないでください。

## NetScaler ADM エージェントのフェイルオーバー

エージェントのフェイルオーバーは、2 つ以上の登録済みエージェントがあるサイトで発生する可能性があります。サイトでエージェントが非アクティブ (DOWN 状態) になると、NetScaler ADM は非アクティブなエージェントの ADC インスタンスを他のアクティブなエージェントと再配布します。

### 重要

- アカウントでエージェントフェイルオーバー機能が有効になっていることを確認します。この機能を有効にするには、[ADM 機能の有効化または無効化を参照してください](#)。
- エージェントがスクリプトを実行している場合は、サイト内のすべてのエージェントにスクリプトが存在することを確認します。したがって、変更されたエージェントは、エージェントのフェイルオーバー後にスクリプトを実行できます。

ADM GUI でサイトをエージェントにアタッチする方法については、エージェントをサイトにアタッチするを参照してください。

エージェントのフェイルオーバーを実現するには、NetScaler ADM エージェントを 1 つずつ選択し、同じサイトに接続します。

たとえば、バンガロールのサイトで、10.106.1xx.2x と 10.106.1xx.3x の 2 つのエージェントが接続され、動作しているとします。1 つのエージェントが非アクティブになると、NetScaler ADM はエージェントを検出し、その状態を down と表示します。

NetScaler ADM エージェントがサイトで非アクティブ (DOWN 状態) になると、NetScaler ADM はエージェントがアクティブ (UP 状態) になるまで 5 分間待機します。エージェントが非アクティブのままである場合、NetScaler ADM は、同じサイト内の利用可能なエージェント間でインスタンスを自動的に再配布します。

NetScaler ADM では、30 分ごとにインスタンスの再配布がトリガーされ、サイト内のアクティブなエージェント間で負荷が分散されます。

## Kubernetes クラスタに ADM エージェントをマイクロサービスとしてインストールする

February 6, 2024

NetScaler ADM エージェントをマイクロサービスとして展開すると、NetScaler ADC CPX の管理に役立ちます。このドキュメントで説明する手順は、NetScaler ADM クラスタと Kubernetes クラスタが別のネットワーク上で構成されている場合에만適用されます。このシナリオでは、Kubernetes クラスターがホストされているマイクロサービスとして ADM エージェントを構成できます。

注

[オンプレミスエージェントを設定し](#)、Kubernetes クラスターがホストされているネットワークにエージェントを登録することもできます。

## 開始

1. NetScaler ADM で、[ネットワーク] > [エージェント] に移動します。
2. [アクションの選択] リストから、[エージェントマイクロサービスのダウンロード] オプションを選択します。
3. [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 クラスタ内のエージェントのサービスを定義し、このエージェントを同じクラスタ内の他のエージェントと区別するための文字列 ID。
  - b) 「パスワード」 —エージェントを介して CPX から ADM へのオンボードにこのパスワードを使用するように、CPX 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。

注

デフォルトのパスワード (`nsroot`) を使用しないでください。

- d) [**Yaml** ファイルをダウンロード] をクリックします。

## Kubernetes クラスタに NetScaler ADM エージェントをインストールする

Kubernetes メインノードで以下を実行します。

1. ダウンロードした YAML ファイルを保存します
2. 次のコマンドを実行します：

```
kubectl create -f <yaml file>
```

例: `kubectl create -f testing.yaml`

エージェントが正常に作成されました。

```
root@msd-micro-01:~# kubectl create -f testing.yaml
deployment.apps/testing created
service/testing created
secret/testing created
configmap/testing created
root@msd-micro-01:~#
```

NetScaler ADM で、[ネットワーク] > [エージェント] の順に選択し、エージェントの状態を確認します。

サービスグラフの使用を開始するための詳細については、「[サービスグラフの設定](#)」を参照してください。

## NetScaler ADM 単一サーバー展開を高可用性展開に移行する

February 6, 2024

Citrix ADM 単一サーバーを、2 台の Citrix ADM サーバーからなる高可用性展開にアップグレードできます。Citrix ADM サーバーの高可用性ペアはアクティブ/パッシブモードで、両方のサーバーの構成は同じです。このタイプのアクティブ/パッシブ展開では、一方の Citrix ADM サーバーがプライマリノードとして構成され、もう一方がセカンダリノードとして構成されます。何らかの理由でプライマリノードがダウンした場合、セカンダリノードが引き継ぎます。

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

Citrix ADM 単一サーバーを高可用性モードに移行するには、次の手順が必要です：

1. 既存のサーバーノードを変更します
2. 2 台目のサーバーノードをプロビジョニングします
3. HA モードで 2 つのノードを展開します
4. 高可用性ペアの設定

### 既存の Citrix ADM サーバーノードを変更します

Citrix ADM を単一サーバーから高可用性モードに移行するには、サーバーノードの初期展開タイプを高可用性モードに変更する必要があります。

1. ワークステーションまたはラップトップで、既存の Citrix ADM サーバーノードのコンソールを開きます。たとえば、IP アドレスが 10.106.171.17 の Citrix ADM をスタンドアロンサーバーとしてデプロイしたとします。

2. NetScaler ADM にログオンします。デフォルトのクレデンシャルは `nsroot` および `nsroot` です。
3. シェルプロンプトで `/mps/deployment_type.py` と入力し、**Enter** キーを押します。
4. 展開タイプを Citrix ADM サーバーとして選択します。デフォルトでは、オプションを選択しない場合は、サーバーとして展開されます。

```
bash-3.2# /mps/deployment_type.py
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-----

  1. Citrix ADM Server.
  2. Remote Disaster Recovery Node.
  3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

5. デプロイメントコンソールで、サーバーデプロイメントを選択するよう求められます（スタンドアロンとして）。**「No」** と入力して、展開を高可用性ペアとして確認します。
6. (最初のサーバーノード) を選択するかどうかを尋ねるメッセージがコンソールに表示されます。**「Yes」** と入力して、ノードを最初のサーバーノードとして確定します。
7. サーバーを再起動するかどうかを尋ねるメッセージがコンソールに表示されます。
8. **「Yes」** と入力して再起動します。

```
Selected Option      1. Citrix ADM Server.
Citrix ADM Standalone deployment [yes/no]:no
First Server Node for Citrix ADM [yes/no]:yes
Restart the system for the configuration to take effect. Do you want to restart?
[yes/no]:yes
```

## 2 番目のサーバ・ノードのプロビジョニング

ハイパーバイザー上に 2 台目のサーバーをプロビジョニングする必要があります。1 台目のサーバーのインストールに使用したものと同一イメージファイルを使用するか、同じバージョンのイメージファイルを Citrix のダウンロードサイトから取得します。

1. イメージファイルを Hypervisor にインポートし、[Console] タブから、次の画面の説明に従って初期ネットワーク構成オプションを設定します:

```

Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
-----
 1. Citrix ADM Host Name [CitrixADM]:
 2. Citrix ADM IPv4 address [10.102.29.211]:
 3. Netmask [255.255.255.0]:
 4. Gateway IPv4 address [10.102.29.1]:
 5. DNS IPv4 Address [127.0.0.2]:
 6. Cancel and quit.
 7. Save and quit.

Select a menu item from 1 to 7 [7]: █

```

2. 必要な IP アドレスを指定した後、シェルプロンプトで `/mps/deployment_type.py` と入力し、Enter キーを押します。
3. 展開タイプを **Citrix ADM** サーバーとして選択します。
4. デプロイメントコンソールで、サーバーデプロイメントを選択するよう求められます（スタンドアロンとして）。「**No**」と入力して、展開を高可用性ペアとして確認します。

```

bash-3.2# /mps/deployment_type.py
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-----
 1. Citrix ADM Server.
 2. Remote Disaster Recovery Node.
 3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
Citrix ADM Standalone deployment [yes/no]:no

```

5. (最初のサーバーノード) を選択するかどうかを尋ねるメッセージがコンソールに表示されます。「**No**」と入力して、ノードを 2 番目のサーバ・ノードとして確認します。



```

-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-----

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
Citrix ADM Standalone deployment [yes/no]:no
First Server Node for Citrix ADM [yes/no]:no
    
```

6. 最初のサーバの IP アドレスとパスワードを入力します。

```

-----

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
Citrix ADM Standalone deployment [yes/no]:no
First Server Node for Citrix ADM [yes/no]:no

-----

Server node Configuration. This menu allows you to specify server ip
address and password.
Enter 0 anytime for cancel and quit.
-----

Enter Citrix ADM IP Address:10.102.29.52
Enter password for Citrix ADM:
    
```

7. 最初のノードのフローティング IP アドレスを入力します。

```
-----
1. Citrix ADM Server.
2. Remote Disaster Recovery Node.
3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
Citrix ADM Standalone deployment [yes/no]:no
First Server Node for Citrix ADM [yes/no]:no

-----
Server node Configuration. This menu allows you to specify server ip
address and password.
Enter 0 anytime for cancel and quit.
-----

Enter Citrix ADM IP Address:10.102.29.52
Enter password for Citrix ADM:
Enter Floating IP address:10.102.29.97
```

8. コンソールに、システムの再起動を求めるメッセージが表示されます。「Yes」と入力して再起動します。

## 2 台のサーバーを高可用性モードでデプロイします

2つのサーバーノードを高可用性ペアとしてインストールするには、既存の Citrix ADM サーバーノードの GUI からこれらのノードを展開する必要があります。2 台のサーバー間の内部通信は、2 つのサーバーノードを展開した時点で開始されます。

### 重要

: 高可用性ノードをデプロイする前に、必ずデフォルトのパスワードを変更してください。

1. Web ブラウザで、既存の NetScaler ADM サーバーノードの IP アドレスを入力します。
2. [User Name] と [Password] の各フィールドに管理者の資格情報を入力します。
3. [システム] タブで、[配置] に移動し、[\*\* 配置 \*\*] をクリックします。
4. 確認のメッセージが表示されます。[はい] をクリックします。

### 注

Citrix ADM を高可用性で展開すると、プライマリノードまたはフローティング IP アドレスにアクセスできます。12.1 リリース以降では、セカンダリノードにアクセスできません。

5. 2 番目のサーバノードの設定時に Floating IP を入力しましたが、システムページで FIP を更新することもできます。[HA 設定] > [高可用性モード用のフローティング IP アドレスの設定] をクリックします。前に設定したフローティング IP アドレスを表示できます。新しい IP アドレスを入力して [OK] をクリックします。

## NetScaler Insight Center から Citrix ADM への移行

February 6, 2024

既存の構成、設定、またはデータを失うことなく、NetScaler Insight Center 展開を NetScaler ADM に移行できるようになりました。Citrix ADM を使用すると、アプリケーションに関連する Citrix ADC インスタンスによって生成されたさまざまな分析を表示できるだけでなく、単一の統合コンソールからグローバルなアプリケーション配信インフラストラクチャ全体を管理、監視、トラブルシューティングすることもできます。

### 注

現在のところ、移行は、NetScaler Insight Center スタンドアロンインスタンスでのみサポートされています。

### 前提条件

NetScaler Insight Center 仮想アプライアンスを Citrix ADM に移行する前に、次の要件が満たされていることを確認してください。

- NetScaler Insight Center 11.1 Build 47.14 以降がインストールされている。
- NetScaler ADM 12.0 ビルド 57.24.tgz イメージファイルをダウンロードしました。

### 注:

NetScaler ADM 12.0 ビルド 57.24 をインストールし、最新の NetScaler ADM 13.0 ビルドにアップグレードする必要があります。詳しくは、「[アップグレード](#)」を参照してください。

- NetScaler ADM 13.0 の最新のビルド.tgz イメージファイルをダウンロードしました。

### ハードウェア要件

| コンポーネント | 条件       |
|---------|----------|
| RAM     | 32 GB    |
| 仮想 CPU  | 8 基の CPU |
| 記憶域     | 120 GB   |

注: 優れたパフォーマンスのためには、**500GB** を使用することをお勧めします。また、Citrix ADM の展開にはソリッドステートドライブ (SSD) テクノロジーを使用することをお勧めします。

---

| コンポーネント           | 条件                |
|-------------------|-------------------|
| 仮想ネットワーク インターフェイス | 1                 |
| スループット            | 1Gbps または 100Mbps |
| ハイパーバイザー要件        |                   |
| Citrix Hypervisor | 6.2, 6.5          |
| VMware ESX        | 5.5, 6.0          |
| Microsoft Hyper-V | 2012 R2           |
| Linux - KVM       | Ubuntu、Fedora     |

---

## インストール手順

**NetScaler Insight Center** を **NetScaler ADM** に移行するには:

1. NetScaler Insight Center シェルプロンプトにログオンします。
2. NetScaler ADM 12.0 ビルド 57.24 を `/var/mps/mps_images` フォルダーにダウンロードします。
3. `tar -zxvf build-mas-12.0-57.24.tgz` コマンドを使用して、**TGZ** ファイルを解凍します。

```
bash-3.2# tar -zxvf build-mas-12.0.57.24.tgz
```

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

```
bash-3.2# ./installmas
```

5. NetScaler ADM 12.0 ビルド 57.24 をインストールした後、上記の手順を実行して、最新の NetScaler ADM 13.0 ビルドにアップグレードする必要があります。

移行後、NetScaler Insight Center インベントリで検出されたすべての Citrix ADC インスタンスが、Citrix ADM の [ネットワーク] > [インスタンス] セクションに表示されます。ただし、最初は、検出されたアプライアンスでホストされている仮想サーバーを手動でポーリングする必要があります。

### 注

Citrix ADM では、デフォルトでは、検出された Citrix ADC インスタンス内で作成された 2 つの仮想サーバーを管理および監視するためのライセンスコストはかかりません。3 つ以上の仮想サーバーを監視および管理す

るには、必要な NetScaler ADM ライセンスをインストールします。詳しくは、「[NetScaler ADM ライセンス](#)」を参照してください。

## NetScaler ADM と Citrix Director の統合

February 6, 2024

Director は NetScaler ADM と統合してネットワーク分析とパフォーマンス管理を行います。

- ネットワーク分析では、NetScaler ADM から HDX Insight レポートを取得し、ネットワークのアプリケーションとデスクトップビューを提供します。この機能を通じて、Director は展開における ICA トラフィックの詳細な分析ビューを提供します。
- パフォーマンス管理機能により、履歴保持および傾向に関するレポートを生成できます。データの履歴保持とリアルタイム評価により、管理者はサーバーのキャパシティとヘルスに関する傾向レポートを作成できます。

NetScaler ADM を Director と統合すると、HDX Insight レポートから Director に次の情報が表示されます。

- [Trends] ページの [Network] タブには、展開におけるアプリケーション、デスクトップ、ユーザーに対する遅延と帯域幅の影響の情報が表示されます。
- [ユーザーの詳細] ページには、特定のユーザーセッションに特化した遅延と帯域幅情報が表示されます。

### 前提条件

#### HDX Insight から NetScaler ADM への移行のハードウェア要件

| コンポーネント           | 条件                                                               |
|-------------------|------------------------------------------------------------------|
| RAM               | 32 GB                                                            |
| 仮想 CPU            | 8                                                                |
| 記憶域               | 500GB。NetScaler ADM 展開では、ソリッドステートドライブ (SSD) テクノロジを使用することをお勧めします。 |
| 仮想ネットワーク インターフェイス | 1                                                                |
| スループット            | 1Gbps または 100Mbps                                                |

### ソフトウェア要件

NetScaler ADM 仮想アプライアンスに移行する前に、次の要件が満たされていることを確認します。

- Director Version 1811 がインストールされている。
- NetScaler HDX Insight Version 10.1 以降がインストールされている。
- HDX Insight と NetScaler ADM は Citrix VDA バージョン 7.0 以降をサポートしています
- Citrix Workspace は、Citrix Virtual Apps and Desktops バージョン 7.0 以降でサポートされています
- MAC Citrix Receiver for Mac Version 11.8 以降および Windows Citrix Receiver for Windows 14.0 以降が有効であり、正確な ICA RTT の測定基準を表示できる。
- NetScaler ADM バージョン 11.0 以降がインストールされます。NetScaler ADM のインストール方法の詳細については、「NetScaler ADM の展開」を参照してください。

### 制限事項

- この機能は、組織のライセンスおよび管理者権限によっては使用できない場合があります。
- ICA セッション RTT (Round Trip Time: 往復時間) のデータは、Citrix Receiver for Windows 3.4 以降および Citrix Receiver for Mac 11.8 以降の場合、正確に表示されます。これらのバージョンよりも前のバージョンの Receiver については、正確なデータが表示されません。
- [Trends] ビューでは、7 よりも前のバージョンの VDA に対しては HDX 接続のログオンデータが収集されません。以前のバージョンの VDA については、グラフのデータが 0 として表示されます。
- 500GB 未満の記憶域の外部ハードディスクが既に存在する展開に対して、追加ハードディスクは設定できません。

### 注

- Director の詳細と、NetScaler ADM を Director と統合する手順については、<https://docs.citrix.com/en-us/xenapp-and-xendesktop/7-15-ltsr/director/hdx-insight.html>を参照してください。
- HDX Insight の詳細については、<http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director/hdx-insight.html>を参照してください。

### 追加のディスクを **NetScaler ADM** に接続する

February 6, 2024

NetScaler Application Delivery Management (ADM) ストレージ要件は、NetScaler ADM のサイズ推定に基づいて決定されます。デフォルトでは、NetScaler ADM は 120GB のストレージ容量を提供します。データの格納に 120 GB を超える必要がある場合は、追加のディスクを接続できます。

注

- NetScaler ADM 初期展開時に、ストレージ要件を見積もり、追加のディスクをサーバーに接続します。
- NetScaler ADM 単一サーバー展開では、デフォルトのディスクに加えて、サーバーに接続できるディスクは 1 つだけです。
- NetScaler ADM 高可用性展開の場合は、各ノードに追加のディスクを接続する必要があります。両方のディスクのサイズは同じである必要があります。
- 以前より容量の低い外部ディスクを接続していた場合は、新しいディスクを接続する前にディスクを取り外す必要があります。
- 2 テラバイトを超える容量の追加のディスクを接続できます。必要に応じて、ディスクのサイズも 2 テラバイト未満にすることができます。
- NetScaler ADM 展開では、ソリッドステートドライブ (SSD) テクノロジーを使用することをお勧めします。

このドキュメントでは、追加の新しいディスクの接続、パーティションの作成、および追加ディスクのサイズ変更に関する次のシナリオについて説明します：

1. 新しい余分なディスクを取り付ける
2. ディスクパーティション化ツールの起動
3. 新しい余分なディスクにパーティションを作成する
4. 既存の余分なディスクのサイズを変更する
5. 追加ディスク上のパーティションを削除する

### スタンドアロンの **NetScaler ADM** に追加ディスクを接続する

仮想マシンにディスクをアタッチするには、次の手順を実行します。

1. NetScaler ADM 仮想マシンをシャットダウンします。
2. Hypervisor で、必要なディスクサイズの追加のディスクを NetScaler ADM 仮想マシンに接続します。

新しく接続された大きなディスクには、データベースデータと NetScaler ADM ログファイルが格納されます。コアファイル、オペレーティングシステムログファイルなどの保存には、既存の 120 ギガバイトのデフォルトディスクが使用されます。

3. NetScaler ADM 仮想マシンを起動します。

## NetScaler ADM ディスクパーティションツール

NetScaler ADM では、新しいコマンドラインツールである **NetScaler ADM** ディスクパーティションツールが提供されるようになりました。このツールの機能については、次のように詳しく説明します。

1. このツールを使用すると、新しく追加した余分なディスクにパーティションを作成できます。
2. このツールを使用して、既存の余分なディスクのサイズを変更することもできます。しかし、既存の外部ディスクは 2 テラバイトを超えてはいけません。

### 注

- データを失わずに 2 テラバイトを超える既存のディスクのサイズを変更することはできません。これは、プラットフォームの既知の制限によるものです。
- 2 テラバイトを超えるストレージ容量を作成するには、既存のパーティションを削除し、この新しいツールを使用してパーティションを作成する必要があります。

3. この新しいツールを使用すると、ディスク上で任意のパーティションアクションを明示的に実行できます。このツールを使用すると、ディスクと関連データを明確に可視化して制御できます。

### 注:

このツールは、NetScaler ADM サーバーに接続した追加ディスクでのみ使用できます。このツールを使用してプライマリ (デフォルト) の 120 ギガバイトディスクにパーティションを作成することはできません。

## ディスクパーティションツールを起動する

1. PuTTY などの SSH クライアントを使用して、NetScaler ADM への SSH 接続を開きます。
2. 管理者の資格情報を使用して Citrix ADM にログインします。
3. シェルプロンプトに切り替えて、次のように入力します。

```
1 /mps/DiskPartitionTool.py
2 <!--NeedCopy-->
```

```
bash-3.2# /mps/DiskPartitionTool.py
-----
MAS/SVM Disk Partition Tool (DPT) 1.0
-----
Welcome to MAS/SVM DPT! Type 'help' or '?' to view a list of commands.
(dpt):
```



## 注

高可用性展開の NetScaler ADM では、ディスクをそれぞれの仮想マシンに接続した後、両方のノードでツールを起動し、パーティションを作成またはサイズ変更する必要があります。

## 新しい追加ディスクにパーティションを作成する

**create** コマンドは、新しいセカンダリディスクが追加されるたびにパーティションを作成するために使用されます。このコマンドを使用して、「remove」コマンドを使用して既存のパーティションを削除した後、既存のセカンダリディスクにパーティションを作成することもできます。

```
(dpt): ?create
Creates a new partition on the attached disk. A swap partition of size 32GB is also created automatically.

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

## 注:

ディスクパーティションツールを使用してパーティションを作成する場合、2 テラバイトのサイズ制限はありません。このツールでは、2 テラバイトを超えるパーティションを作成できます。ディスクのパーティションを作成すると、サイズが 32 GB のスワップパーティションが自動的に追加されます。プライマリパーティションは、ディスク上の残りのすべての領域を使用します。

コマンドが実行されると、GUID パーティションテーブル (GPT) パーティションスキームが作成されます。また、残りの領域を使用するために 32 GB の swap パーティションとデータパーティションが作成されます。その後、プライマリパーティションに新しいファイルシステムが作成されます。

## 注:

このプロセスには数秒かかることがあり、プロセスを中断しないでください。

```
(dpt): create
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
Are you sure you want to continue (Y/N): y

Creating GPT partition scheme...
da1 created

Creating partition 1 using (456287933) blocks. Leaving aside 32G for swap...
da1p1 added

Creating partition 2 for swap using remaining 32G...
da1p2 added

Formatting the new partition. This may take some time (~20 seconds). Please be patient and don't interrupt the process...
```

create コマンドが完了すると、仮想マシンが自動的に再起動され、新しいパーティションがマウントされます。

```

Create Done.
VM has to be rebooted for the new partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY

```

再起動後、新しいパーティションは /var/mps にマウントされます。

```

bash-3.2# df -k
Filesystem 1024-blocks    Used    Avail Capacity  Mounted on
/dev/md0      456046    374346    72580     84%    /
devfs          1          1         0    100%    /dev
procfs         4          4         0    100%    /proc
fdescfs        1          1         0    100%    /dev/fd
/dev/da0s1a   1623950    284466   1209568    19%    /flash
/dev/da0s1e  116073918  2812298 103975708     3%    /var
/dev/da1p1   495168802    43854  455511444     0%    /var/mps

```

追加された swap パーティションは、「create」コマンドの出力にスワップ領域として表示されます。

```

CPU:  0.0% user,  0.0% nice,  0.0% system,  0.7% interrupt, 99.3% idle
Mem:  89M Active, 21M Inact, 123M Wired, 16M Cache, 74M Buf, 6965M Free
Swap: 37G Total, 37G Free

```

#### 注

パーティションを作成すると、このツールによって仮想マシンが再起動されます。

既存の追加ディスク内のパーティションのサイズを変更する

**resize** コマンドを使用して、アタッチされている (セカンダリ) ディスクのサイズを変更できます。master boot record (MBR) または GPT スキームを持つディスクのサイズを変更できます。ディスクのサイズは、2 テラバイト未満から最大 2 テラバイトにする必要があります。

#### 注

- 「resize」コマンドは、既存のデータを失うことなく機能するように設計されています。ただし、サイズ変更を試みる前に、このディスク内の重要なデータを外部ストレージにバックアップすることを Citrix ではお勧めします。データバックアップは、サイズ変更操作中にディスクデータが破損する可能性がある場合に役立ちます。
- パーティションのサイズ変更中は、ディスク領域を 100 GB ずつ増やしてください。このような増分増加

により、より頻繁にサイズを変更する必要がなくなります。

```
(dpt): ?resize
Resizes existing partition on attached disk to utilize all space available. Pre-conditions are:
1. Secondary disk exists and capacity of disk < 2TB
2. A single partition exists on secondary disk and there is atleast 100GB to gain by resizing

*****
*** WARNING !! ***
*****

Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

「resize」コマンドは、すべての前提条件をチェックし、すべての前提条件が満たされているかどうか、およびサイズ変更へ同意した後に続行します。これにより、NetScaler ADM サブシステム、PostgreSQL DB プロセス、および NetScaler ADM モニタープロセスなど、ディスクにアクセスするプロセスが停止されます。プロセスが停止すると、ディスクはアンマウントされ、サイズ変更の準備をします。サイズ変更は、使用可能な領域全体を占有するようにパーティションを拡張し、ファイルシステムを拡張することによって行われます。スワップパーティションがディスク上に存在する場合、サイズ変更後に削除され、ディスクの最後に再作成されます。スワップパーティションについては、このドキュメントの「**Create command**」セクションで説明しています。

(注

) 「ファイルシステムの拡大」プロセスでは、完了までに多少時間がかかる場合があります、プロセスの進行中にプロセスを中断しないように注意してください。パーティションのサイズを変更した後、ツールによって仮想マシンが再起動されます。

```
(dpt): resize

*****
*** WARNING !! ***
*****

Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to resize (Y/N): y
```

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to resize existing partition.
Disabling swap on partition: /dev/da1p2
Deleting swap partition: da1p2
Resizing partition da1p1...
da1p1 resized

Adding a swap partition da1p2...
da1p2 added

Formatting the newly added portions of the partition. This may take some time (~10 seconds). Please be patient and don't interrupt the process...
```

サイズ変更プロセスのすべての中間手順 (アプリケーションの停止、ディスクのサイズ変更、ファイルシステムの拡大) がコンソールに表示されます。プロセスが完了すると、次のメッセージが表示されます。

```

Resize Done.
VM has to be rebooted for the resized partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
    
```

再起動後、” df” コマンドを使用してサイズの増加を観察することができます。サイズを大きくした後の前後の詳細は次のとおりです。

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> bash-3.2# df -k Filesystem 1024-blocks  Used    Avail Capacity  Mounted on /dev/md0    456046  374864  72062   84%          / devfs      1        1        0   100%        /dev procfs     4        4        0   100%        /proc fdescfs    1        1        0   100%        /dev/fd /dev/da0s1a 1623950  284468  1209566 19%         /flash /dev/da0s1e 116073918 1662048 105125958 2%         /var /dev/dais1a 152329216 3082226 137060654 2%         /var/mps             </pre> | <pre> bash-3.2# df -k Filesystem 1024-blocks  Used    Avail Capacity  Mounted on /dev/md0    456046  374838  72088   84%          / devfs      1        1        0   100%        /dev procfs     4        4        0   100%        /proc fdescfs    1        1        0   100%        /dev/fd /dev/da0s1a 1623950  284468  1209566 19%         /flash /dev/da0s1e 116073918 1666800 105121206 2%         /var /dev/dais1a 304651668 3137954 277141582 1%         /var/mps             </pre> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### 追加のディスクのパーティションを削除します

セカンダリディスク上の既存のパーティションのサイズは、最大 2 テラバイトまで変更できます。これは、パーティションの既知の制限によるものです。2 テラバイトを超えるディスクが必要な場合は、新しいディスクを接続し、ディスクパーティションツールを使用してパーティションを作成します。remove コマンドを使用して既存のパーティションを削除し、パーティションを作成することもできます。

**注:**

既存のパーティションを削除すると、既存のデータはすべて削除されます。したがって、このコマンドを使用する前に、重要なデータを外部ストレージにバックアップする必要があります。

```

(dpt): ?remove
Removes existing partition from attached disk.

*****
*** WARNING !! ***
*****

All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
    
```

「remove」コマンドを実行すると、確認が要求され、確認されると、セカンダリディスクを使用するすべてのプロセス（ADM サブシステム、PostgreSQL プロセス、ADM モニターなど）が停止します。swap パーティションが存在し、そのパーティションで swap が有効になっている場合、swap は無効になります。

```
(dpt): remove
*****
*** WARNING !! ***
*****
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
Are you sure you want to continue (Y/N): y
```

「y」と入力すると、ディスクがアンマウントされ、ディスク上のすべてのパーティションが削除されます。

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to remove existing partitions.
Disabling swap on partition: /dev/da1p2
Removing all partitions from: da1
Remove Done.
Rebooting VM now...
```

#### 注

パーティションを削除すると、仮想マシンが再起動されます。

#### 仮想マシンの再起動

パーティションの作成、サイズ変更、またはスワップファイルの作成時に、仮想マシンを再起動します。変更は再起動後にのみ有効になります。この目的のために、ツールに再起動コマンドが用意されています。

```
(dpt): ?reboot
Reboot the VM. Note: VM has to be rebooted after new partition is created, existing one is resized or swap file is created.
The VM is rebooted automatically after these operations. If the automatic reboot does not happen, then this command can be used to reboot the VM.
```

確認を求められ、確認されると、すべてのプロセス（ADM サブシステム、PostgreSQL プロセス、ADM モニターなど）が停止します。仮想マシンが再起動されます。

```
(dpt): reboot
Are you sure you want to reboot the VM (Y/N): y

Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

## ディスクデータのバックアップファイルを作成する

パーティションのサイズ変更または削除を行う前に、NetScaler ADM データをバックアップする手順を次に示します。

## 注:

バックアップファイルを作成するにはディスク容量が必要です。バックアップコマンドを実行する前に、十分な空きディスク領域（50% 以上）があることを確認することをお勧めします。

## 1. ADM を停止します。

```
1 /mps/masd stop
2 <!--NeedCopy-->
```

## 2. PostgreSQL を停止します。

```
1 su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh
2 <!--NeedCopy-->
```

## 3. ADM モニタを停止します。

```
1 /mps/scripts/stop_mas_monit.sh
2 <!--NeedCopy-->
```

## 4. tarball を作成します。

```
1 cd /var
2 tar cvfz /var/mps/mps_backup.tgz mps
3 <!--NeedCopy-->
```

## 注:

バックアップするデータのサイズに応じて、操作に時間がかかります。

## 5. チェックサムを生成します。

```
1 md5 /var/mps/mps_backup.tgz > /var/mps/mps_backup_checksum
2 <!--NeedCopy-->
```

## 6. tarball ファイルとチェックサムファイルをリモートサーバにコピーします。

7. コピーした tarball の正確性を検証します。転送されたファイルのチェックサムを生成し、ソースチェックサムと比較します。

## 8. ADM 仮想マシンから tarball を削除します。

```
1 cd /var/mps/
2 rm mps_backup.tgz mps_backup_checksum
3 <!--NeedCopy-->
```

## 追加コマンド

ツールでは、前述のコマンドの他に、次のコマンドも使用できます。

## 【ヘルプ】コマンド:

サポートされているコマンドの一覧を表示するには、**help** または **?** を押して Enter キーを押します。各コマンドのヘルプを表示するには、**[help]** または **[?]** を押します。**\*\*** に続けてコマンド名を入力し **\*\***、Enter キーを押します。

```
(dpt): help
DPT Commands
-----
create  create_swapfile  exit  help  info  reboot  remove  resize
(dpt):
```

## 情報コマンド:

**info** コマンドは、接続されているセカンダリディスクが存在する場合、そのディスクに関する情報を提供します。このコマンドは、デバイス名、パーティション構成、人間が読める形式のサイズ、およびディスクブロック数を提供します。スキームは MBR または GPT です。MBR スキームとは、以前のバージョンの NetScaler ADM バージョンを使用してディスクがパーティション分割されたことを意味します。MBR/GPT ベースのパーティションはサイズ変更できますが、2 テラバイトを超えることはできません。GPT パーティションスキームとは、NetScaler ADM 12.1 以降を使用してディスクがパーティション分割されたことを意味します。

## 注:

GPT パーティションは、作成時に 2 テラバイトを超える場合があります。ただし、小さいサイズのディスクを作成した後は、ディスクのサイズを 2 テラバイトを超えるサイズに変更することはできません。これは、プラットフォームの既知の制限です。

```
(dpt): ?info
Provides information about attached disk (if found).
(dpt): info
-----
Disk: da1
Scheme: MBR
Size: (150G)
Blocks: 314572737
-----
(dpt):
```

スワップファイル作成コマンド:

NetScaler ADM のプライマリディスクのデフォルトのスワップパーティションは 4 GB であるため、デフォルトのスワップ領域は 4 GB です。NetScaler ADM のデフォルトのメモリ構成 (2 GB) では、このスワップ領域で十分です。ただし、より高いメモリ構成で NetScaler ADM を実行する場合は、ディスクにより多くのスワップ領域を割り当てる必要があります。

注:

スワップパーティションは通常、オペレーティングシステムのインストール中にハードディスクドライブ (HDD) 上に作成される専用パーティションです。このようなパーティションは、スワップスペースとも呼ばれます。スワップパーティションは、追加のメインメモリをシミュレートする仮想メモリに使用されます。

以前のバージョンの NetScaler ADM で追加されたセカンダリディスクには、デフォルトでスワップパーティションが作成されません。「create\_swapfile」コマンドは、スワップパーティションを持たない古いバージョンの NetScaler ADM を使用して作成されたセカンダリディスクを対象としています。このコマンドでは、次の項目がチェックされます。

- セカンダリディスクの存在
- マウント中のディスク
- ディスクのサイズ (500 GB 以上)
- スワップファイルの存在

「create\_swapfile」コマンドは、メモリが 16 GB 以上の場合にのみ有効で、メモリが不足しているときには使用できません。したがって、このコマンドはスワップファイルの作成を続行する前にメモリをチェックします。

```
(dpt): ?create_swapfile
Creates a 32GB swap file on the secondary disk. Pre-conditions are:
1. Secondary disk exists
2. Secondary disk is partitioned and mounted
3. Capacity of disk >= 500GB
4. Swap file is not already found
5. RAM size >= 16GB

Creating swapfile is a time consuming operation and can take ~5 minutes to complete. Once started the operation should not be interrupted.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

すべての条件が満たされ、ユーザーが続行に同意すると、32 GB のスワップファイルがセカンダリディスクに作成されます。スワップファイルの作成プロセスには数分かかるため、処理中に中断しないように注意してください。正常に完了すると、スワップファイルが有効になるために再起動が行われます。

```
Creating swapfile. This may take some time (~5 mins). Please be patient and don't interrupt the process...
32768+0 records in
32768+0 records out
34359738368 bytes transferred in 724.061475 secs (47454173 bytes/sec)

Changing permissions for created swapfile...

Create (swapfile) Done.
VM has to be rebooted for the newly created swapfile to take effect.
```

再起動後、top コマンドを使用して swap の増加を観察できます。



```
CPU: 1.7% user, 0.0% nice, 0.8% system, 0.2% interrupt, 97.4% idle
Mem: 1847M Active, 506M Inact, 382M Wired, 4684K Cache, 199M Buf, 4473M Free
Swap: 4198M Total, 4198M Free
```

```
CPU: 42.0% user, 0.0% nice, 7.6% system, 5.0% interrupt, 45.3% idle
Mem: 1805M Active, 423M Inact, 393M Wired, 4792K Cache, 199M Buf, 4587M Free
Swap: 36G Total, 36G Free
```

終了コマンド:

ツールを終了するには、`exit` と入力して Enter キーを押します。

```
(dpt): exit
bash-3.2#
```

高可用性で展開された **NetScaler ADM** に追加ディスクを接続する

ここでは、セカンダリディスクなしで高可用性セットアップで NetScaler ADM サーバーのペアを構成したシナリオを考えてみましょう。また、2 つ以上の NetScaler ADC インスタンスを追加し、すべてのプロセスが実行されていることを確認したとします。この設定では、セカンダリディスクを仮想マシンに追加できます。高可用性セットアップでは、次のタスクで説明するように、両方のノードにディスクを追加する必要があります。

1. NetScaler ADM ノード名は「`adm_primary`」および「`adm_secondary`」であると仮定します。
2. まず、`ADM_Secondary` でパーティションツールを実行してから、セカンダリディスクを追加します。ディスクが追加されると、仮想マシンが再起動します。
3. 再起動後、`ADM_SECONDARY` をシャットダウンします。
4. 次に、`ADM_Primary` でパーティションツールを実行し、セカンダリディスクを追加します。ディスクが追加されると、仮想マシンが再起動します。  
  
両方のノードに、同じ容量のディスクを追加してください。たとえば、500 GB の容量のディスクをプライマリノードに追加する場合、500 GB の容量のディスクをセカンダリノードにも追加します。
5. `ADM_Primary` が再起動したら、そのノードがプライマリノードであることを確認します。
6. ここで、`adm_secondary` ノードを起動します。セカンダリノードとして起動し、データベースが同期されていることを確認します。
7. すべてのデータがまだ存在することを確認します。

両方のノードの **RAM** 容量を増やすには、次の手順を実行します。

1. `ADM_Secondary` をシャットダウンし、必要に応じて RAM サイズを増やします。ノードを再起動しないでください。
2. `ADM_Primary` をシャットダウンし、必要に応じて RAM サイズを増やします。  
  
両方のノードで RAM サイズを均等に増やしてください。たとえば、プライマリノードの RAM サイズを 16 GB に増やす場合は、セカンダリノードでも同じようにします。

3. ADM\_Primary を再起動します。
4. ADM\_Primary が再起動したら、そのノードがプライマリノードであることを確認します。
5. ここで、adm\_secondary ノードを起動します。再起動後、セカンダリとして起動し、DB 同期が機能していることを確認します。
6. ここで、すべてのデータがまだ存在していることを確認します。

(注)

セカンダリディスクを追加すると、プライマリノードが起動するまでに多少時間がかかります。また、セカンダリディスクを両方のノードに追加して RAM 容量を増やすプロセス全体で、しばらくの間、両方のノードがダウンする必要があります。このメンテナンス作業を計画する際には、このダウンタイムを考慮してください。

## 構成

February 6, 2024

NetScaler ADM サーバーには、GUI を使用してのみアクセスできます。インスタンスの追加、インスタンスとアプリケーションの管理、監視、分析の表示、NetScaler ADM サーバーの設定を行うには、GUI にアクセスする必要があります。

構成ユーティリティとダッシュボードにアクセスするには、サポートされている Web ブラウザーがワークステーションにインストールされている必要があります。

次のブラウザーがサポートされています。

---

| ウェブブラウザ           | バージョン             |
|-------------------|-------------------|
| Internet Explorer | 11.0 以降           |
| Google Chrome     | Chrome 19 以降      |
| Safari            | Safari 5.1.1 以降   |
| Mozilla Firefox   | Firefox 3.6.25 以降 |

---

**NetScaler ADM GUI** にアクセスするには:

管理者の資格情報を使用して NetScaler ADM にログオンします。

NetScaler ADM にログオンした後、次の手順を実行して作業を開始する必要があります。

- [NetScaler ADM にインスタンスを追加します](#)。これらのインスタンスを管理および監視する場合は、Citrix ADM サーバーにインスタンスを追加する必要があります。

- **仮想サーバーで分析を有効にします。** アプリケーショントラフィックフローの分析データを表示するには、特定のアプリケーションのトラフィックを受け取る仮想サーバーの分析機能を有効化する必要があります。
- **NetScaler ADM で NTP サーバーを構成します。** Citrix ADM でネットワークタイムプロトコル (NTP) サーバーを構成して、その時計を NTP サーバーと同期する必要があります。
- **NetScaler ADM のパフォーマンスを最適化するためのシステム設定を構成します。** NetScaler ADM を使用してインスタンスとアプリケーションの管理と監視を開始する前に、NetScaler ADM サーバーのパフォーマンスを最適化するためのいくつかのシステム設定を構成することをお勧めします。

## Citrix ADM へのインスタンスの追加

February 6, 2024

インスタンスは、NetScaler ADM から検出、管理、監視する Citrix 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は、NetScaler ADM サーバーにインスタンスを追加する必要があります。以下の Citrix アプライアンスと仮想アプライアンスを NetScaler ADM に追加できます。

- NetScaler ADC MPX
- NetScaler ADC VPX
- NetScaler ADC SDX
- NetScaler ADC CPX
- NetScaler ADC BLX
- NetScaler Gateway
- Citrix SD-WAN

インスタンスは、NetScaler ADM サーバーの初回セットアップ時に追加することも、後で追加することもできます。次に、NetScaler ADM がインスタンスにアクセスするために使用できるインスタンスプロファイルを指定する必要があります。

### 注

- NetScaler ADM は、通信に NetScaler ADC インスタンスの NetScaler IP (NSIP) アドレスを使用します。NetScaler ADC インスタンスと NetScaler ADM の間で開く必要のあるポートについては、「[ポート](#)」を参照してください。
- Citrix SD-WAN WO および Citrix SD-WAN EE インスタンスの場合、NetScaler ADM はインスタンスの管理 IP アドレスを使用して通信します。

- NetScaler ADM がインスタンスを検出する方法については、「[インスタンスの検出](#)」を参照してください。

## NetScaler ADC プロファイルの作成方法

NetScaler ADC プロファイルには、NetScaler ADM に追加するインスタンスのユーザー名、パスワード、通信ポート、認証タイプが含まれます。インスタンスの種類ごとにデフォルトのプロファイルが用意されています。たとえば、**nsroot** は NetScaler ADC インスタンスのデフォルトのプロファイルです。デフォルトのプロファイルは、デフォルトの NetScaler ADC 管理者の資格情報を使用して定義されます。インスタンスのデフォルトの管理者資格情報を変更した場合は、それらのインスタンスのカスタムの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、または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 ADC プロファイルは、[インスタンス] ページから、またはインスタンスの追加または変更時に作成できます。

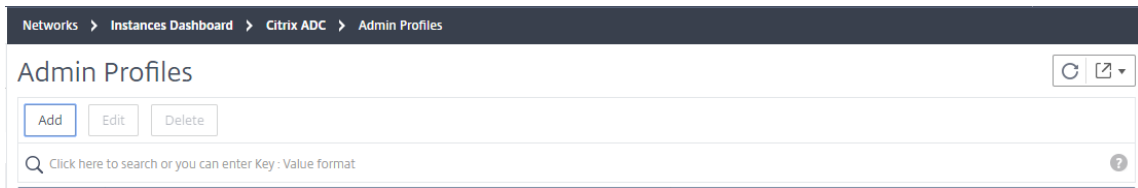
注:

インスタンスプロファイルの作成には、必ずスーパー管理者アカウントを使用してください。

[インスタンス] ページから **NetScaler ADC** プロファイルを作成するには:

1. [ネットワーク] > [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 ADC などです。
3. [NetScaler ADC] ページの [アクションの選択] で、[プロファイル] を選択します。

4. [管理プロファイル] ページで、[追加] を選択します。



5. **NetScaler ADC** プロファイルの作成ページで、次の操作を行います。

## ← Create Citrix ADC Profile

Profile Name\*  ✘ Please enter value

User Name\*

Password\*

SSH Port

Note: HTTP port and HTTPS port are configurable for CPX only.

HTTP Port

HTTPS Port

Use global settings for Citrix ADC communication

▼ SNMP

Version  
 v2  v3

Community\*

▼ Timeout Settings

Waiting Time for sending the request from Application Delivery Management to Citrix ADC after successful reboot.

Timeout (in Seconds)

- a) プロファイル名: NetScaler ADC 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 ADC インスタンスにログオンするユーザー名を指定します。
- c) パスワード: NetScaler ADC インスタンスにログオンするためのパスワードを指定します。

d) **SSH** ポート:NetScaler ADM と NetScaler ADC インスタンス間の SSH 通信用のポートを指定します。

e) **HTTP** ポート:NetScaler ADM と NetScaler ADC インスタンス間の HTTP 通信用の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 ADC CPX インスタンスで構成したデフォルト以外またはカスタマイズされた HTTP ポートを指定することもできます。カスタマイズされた HTTP ポートは、NetScaler ADM と NetScaler ADC CPX 間の通信にのみ使用できます。

f) **HTTPS** ポート:NetScaler ADM と NetScaler ADC インスタンス間の HTTPS 通信用の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 ADC CPX インスタンスで構成したデフォルト以外またはカスタマイズされた HTTPS ポートを指定することもできます。カスタマイズされた HTTPS ポートは、NetScaler ADM と NetScaler ADC CPX の間の通信にのみ使用できます。

g) **NetScaler ADC** 通信にグローバル設定を使用する: NetScaler ADM と NetScaler ADC 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 を選択します。

h) **SNMP** バージョン: **SNMPv2** または **SNMPv3** のいずれかを選択し、次の操作を行います。

i. SNMPv2 を選択する場合は、認証用のコミュニティ名を指定します。

ii. SNMPv3 を選択する場合は、\*\* 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、[\*\* 認証の種類] と [\*\* プライバシーの種類 \*\*] を選択します。

▼ SNMP

Version

v2    v3

Security Name\*

Security Level\*

AuthPriv ▼

Authentication Type\*

MD5 ▼

Authentication Password\*

Privacy Type\*

DES ▼

Privacy Password\*

注

NetScaler ADC 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 ADM が NetScaler ADC インスタンスに接続要求を送信する前に待機する必要がある時間を指定します。
- j) [作成] を選択します。

### ADC インスタンスを **NetScaler ADM** に追加する

インスタンスは、NetScaler ADM サーバーの初回セットアップ時に追加することも、後で追加することもできます。

インスタンスを追加するには、各 NetScaler ADC インスタンスのホスト名または IP アドレス、または IP アドレスの範囲を指定する必要があります。

SD-WAN インスタンスの場合、各インスタンスの IP アドレス、または IP アドレスの範囲を指定する必要があります。NetScaler ADM は、Citrix SD-WAN WO エディションと Citrix SD-WAN PE エディションのみをサポートすることに注意してください。

## 注

- クラスターで構成された NetScaler ADC インスタンスを追加するには、クラスターの IP アドレスまたはクラスター設定の個々のノードのいずれかを指定する必要があります。ただし、NetScaler ADM では、クラスターはクラスター IP アドレスだけで表されます。
- 高可用性ペアとして設定された NetScaler ADC インスタンスの場合、一方のインスタンスを追加すると、そのペアのもう一方のインスタンスが自動的に追加されます。

2 つの Citrix ADM サーバーが高可用性モードでセットアップされている場合、インスタンスが追加されると、トラフィックソースは ADM フローティング IP アドレスを経由します。

オンプレミスエージェントを使用して設定されたリモートデータからインスタンスを追加すると、トラフィックソースは ADM エージェントを経由します。

**NetScaler ADM** にインスタンスを追加するには：

1. 管理者の資格情報を使用して NetScaler ADM にログインします。
2. [ネットワーク]>[インスタンス]>[Citrix ADC] に移動します。追加するインスタンスのタイプ (NetScaler ADC VPX など) を選択し、[追加] をクリックします。

|  | IP Address    | Host Name | Instance State | Rx (Mbps) | Tx (Mbps) | HTTP Req/s | CPU Usage (%) |
|--|---------------|-----------|----------------|-----------|-----------|------------|---------------|
|  | 10.102.29.60  | --        | ● Up           | 0         | 0         | 0          | 1.7           |
|  | 10.102.29.200 | --        | ● Up           | 0         | 0         | 0          | 3.9           |

3. 次のいずれかのオプションを選択します：

- デバイス **IP** アドレスの入力-NetScaler ADC インスタンスの場合は、各インスタンスのホスト名または IP アドレス、または IP アドレスの範囲を指定します。

SNIP を使用して ADC HA ペアを検出する場合は、独立ネットワーク構成 (INC) モードが有効になっていることを確認してください。また、SNIP アドレスを次の形式で指定します。

```
1 <SNIP of primary instance>#<SNIP of secondary instance>
2 <!--NeedCopy-->
```

たとえば、10.10.10.11#10.10.10.12

SD-WAN インスタンスの場合、各インスタンスの IP アドレス、または IP アドレスの範囲を指定する必要があります。



- **Import from file** - ローカルシステムから、追加するすべてのインスタンスの IP アドレスを含むテキストファイルをアップロードします。
4. 「プロファイル名」から、適切なインスタンスプロファイルを選択するか、「+」アイコンをクリックして新しいプロファイルを作成します。
  5. サイトから、インスタンスを追加する場所を選択するか、+ アイコンをクリックして新しい場所を作成します。
  6. 「OK」をクリックして、NetScaler ADM にインスタンスを追加するプロセスを開始します。

注

インスタンスを再検出する場合は、[ネットワーク]>[インスタンス]>[NetScaler ADC]に移動します。インスタンスタイプ (VPX など) を選択し、再検出するインスタンスを選択し、[アクションの選択] リストから [再検出] をクリックします。

### ADC CPX インスタンスを NetScaler ADM に追加する

NetScaler ADM は、CPX 機能の改善をサポートするように拡張されました。NetScaler ADC CPX インスタンスは、CPX の IP アドレスをデバイスプロファイルとともに提供することにより、NetScaler ADM に追加されるようになりました。CPX インスタンスの追加プロセスは、ADM で VPX や MPX などの他の ADC タイプを追加する方法と似ています。また、ADM における CPX の登録が強化されました。CPX が起動すると、NetScaler ADM は自動的に CPX インスタンスを検出して登録します。CPX インスタンスは、Docker ホストを介して検出されなくなりました。

1. [ネットワーク]>[インスタンス]>[NetScaler ADC]に移動し、[CPX] タブをクリックします。
2. [Add] をクリックして、NetScaler ADM に新しい CPX インスタンスを追加します。
3. [NetScaler ADC CPX の追加] ページが開きます。次のパラメーターの値を入力します：
  - a) CPX インスタンスの到達可能な IP アドレス、または CPX インスタンスがホストされている Docker コンテナの IP アドレスのいずれかを指定することにより、CPX インスタンスを追加できます。
  - b) CPX インスタンスのプロファイルを選択します。
  - c) インスタンスを展開するサイトを選択します。
  - d) エージェントを選択します。
  - e) オプションとして、キーと値のペアをインスタンスに入力できます。キーと値のペアを追加すると、後でインスタンスを簡単に検索できます。

## ← Add Citrix ADC CPX

Enter Device IP Address     Import from file

Enter one or more hostnames, IP addresses , and/or a range of IP addresses (for example, 10.102.40.30-10.102.40.45) using a comma separator.

Routable IP/ Docker IP\*

?

Profile Name\*

Site\*

Agent

>

Tags

+

### 注

NetScaler ADC CPX インスタンスの場合、CPX インスタンスプロファイルを作成するときに、ホストの **HTTP**、**HTTPS**、**SSH**、および **SNMP** ポートの詳細を指定する必要があります。ホストが公開したポートの範囲を [ 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。

4. **[OK]** をクリックします。

## NetScaler ADM にスタンドアロンの NetScaler ADC BLX インスタンスを追加する

スタンドアロンの NetScaler ADC BLX インスタンスは、専用ホスト Linux サーバー上で実行される単一のインスタンスです。

1. [ ネットワーク ] > [ インスタンス ] > [ \*\*Citrix ADC\*\* ] に移動します。
2. [ **BLX** ] タブで、[ 追加 ] をクリックします。
3. [ インスタンスタイプ ] リストから [ スタンドアロン ] オプションを選択します。
4. **IP** アドレスフィールドに、BLX インスタンスの IP アドレスを指定します。
5. ホスト **IP** アドレスフィールドに、BLX インスタンスがホストされている Linux サーバーの IP アドレスを指定します。
6. プロファイル名リストで、BLX インスタンスの適切なプロファイルを選択するか、プロファイルを作成します。  
プロファイルを作成するには、[ 追加 ] をクリックします。

**重要**

: プロファイルで 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。

7. サイトリストで、インスタンスを追加するサイトを選択します。

サイトを追加する場合は、[追加] をクリックします。

8. エージェントリストで、インスタンスを関連付ける NetScaler ADM エージェントを選択します。

NetScaler ADM にエージェントが 1 つしか構成されていない場合、そのエージェントはデフォルトで選択されます。

9. [OK] をクリックします。

## ← Add Citrix ADC BLX

**Instance Type\***

Standalone ▼ ⓘ

**IP Address\***

10.10.10.10 ⓘ

**Host IP Address\***

10.10.10.20 ⓘ

**Profile Name\***

blx\_nsroot\_profile ▼ Add Edit

**Site\***

ad ▼ Add Edit

**Agent**

× >

**Tags**

Key Value +

OK Close

## NetScaler ADM に高可用性の NetScaler ADC BLX インスタンスを追加

異なるホスト Linux サーバーで実行される高可用性 NetScaler ADC BLX インスタンス。Linux サーバーは複数の BLX インスタンスをホストできません。

1. [ **BLX** ] タブで、[ 追加 ] をクリックします。
2. [ インスタンスタイプ ] リストから [ 高可用性 ] オプションを選択します。
3. **IP** アドレスフィールドに、BLX インスタンスの IP アドレスを指定します。
4. ホスト **IP** アドレスフィールドに、BLX インスタンスがホストされている Linux サーバーの IP アドレスを指定します。
5. 「ピア **IP** アドレス」フィールドに、ピア BLX インスタンスの IP アドレスを指定します。
6. 「ピアホスト **IP** アドレス」フィールドに、ピア BLX インスタンスがホストされている Linux サーバーの IP アドレスを指定します。
7. プロファイル名リストで、BLX インスタンスの適切なプロファイルを選択するか、プロファイルを作成します。  
プロファイルを作成するには、[ 追加 ] をクリックします。

**重要**

: プロファイルで 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。

8. サイトリストで、インスタンスを追加するサイトを選択します。  
サイトを追加する場合は、[ 追加 ] をクリックします。
9. エージェントリストで、インスタンスに関連付ける NetScaler ADM エージェントを選択します。  
NetScaler ADM にエージェントが 1 つしか構成されていない場合、そのエージェントはデフォルトで選択されます。
10. [ **OK** ] をクリックします。

## ← Add Citrix ADC BLX

**Instance Type\***  
 ⓘ

**IP Address\***  
 ⓘ

**Host IP Address\***  
 ⓘ

**Peer IP Address\***  
 ⓘ

**Peer Host IP Address\***  
 ⓘ

**Profile Name\***  
 ⓘ

**Site\***  
 ⓘ

**Agent**  
 ⓘ

**Tags**

| Key                              | Value                              |
|----------------------------------|------------------------------------|
| <input type="text" value="Key"/> | <input type="text" value="Value"/> |

+

### NetScaler ADM からインスタンス GUI にアクセスする

1. [ ネットワーク ] > [ インスタンス ] > [ NetScaler ADC ] に移動します。
2. アクセスするインスタンスのタイプ (VPX、MPX、CPX、SDX、BLX など) を選択します。
3. 必要な NetScaler ADC IP アドレスまたはホスト名をクリックします。

The screenshot shows the Citrix ADC management interface. At the top, there is a breadcrumb trail: Networks > Instances Dashboard > Citrix ADC. Below this, the title 'Citrix ADC' is displayed. A navigation bar contains buttons for 'Add', 'Edit', 'Remove', 'Dashboard', 'Tags', 'Partitions', 'Provision', and 'Select Action'. A search bar is present with the text 'Click here to search or you can enter Key : Value format'. Below the search bar is a table with the following columns: IP ADDRESS, HOST NAME, INSTANCE STATE, RX (MBPS), TX (MBPS), HTTP REQ/S, and AGENT. The table contains six rows of data.

| <input type="checkbox"/> | IP ADDRESS                      | HOST NAME | INSTANCE STATE   | RX (MBPS) | TX (MBPS) | HTTP REQ/S | AGENT               |
|--------------------------|---------------------------------|-----------|------------------|-----------|-----------|------------|---------------------|
| <input type="checkbox"/> | 10.106.171.67                   | --        | ● Up             | 0         | 0         | 0          | --                  |
| <input type="checkbox"/> | 10.106.154.10                   | NS        | ● Out of Service | 0         | 0         | 0          | --                  |
| <input type="checkbox"/> | 10.106.136.175 - 10.106.136.176 | ns1       | ● Down           | 0         | 0         | 0          | --                  |
| <input type="checkbox"/> | 10.106.136.62                   | --        | ● Up             | 0         | 0         | 0          | --                  |
| <input type="checkbox"/> | 10.106.136.43                   | --        | ● Down           | 0         | 0         | 0          | ns (10.102.103.247) |

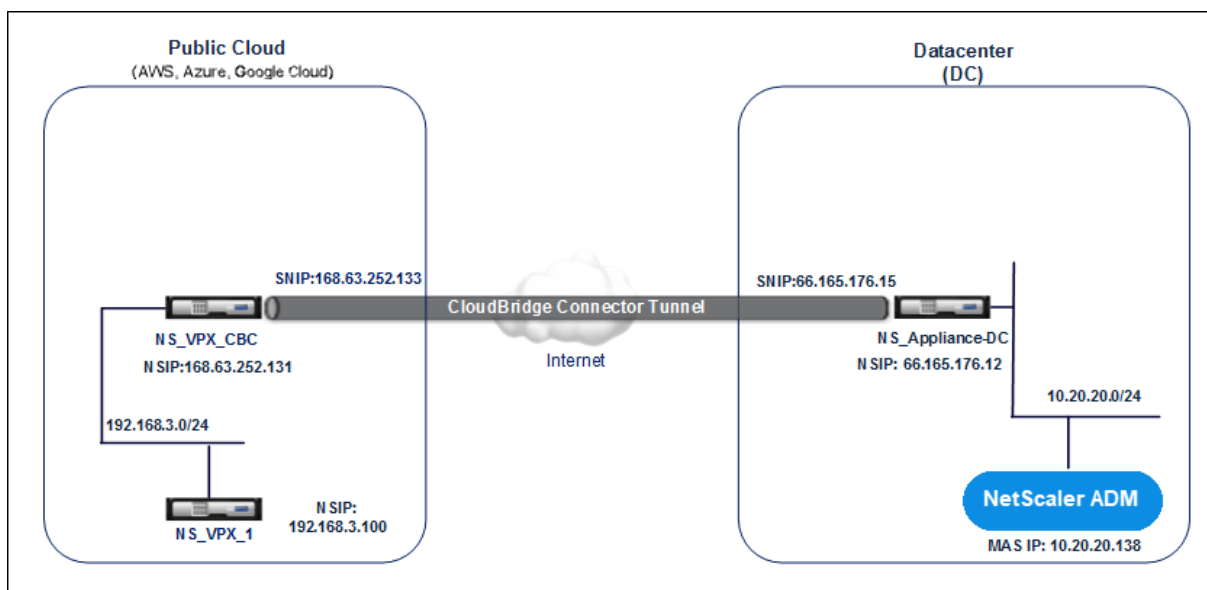
選択したインスタンスの GUI がポップアップウィンドウに表示されます。

## クラウドにデプロイされた **NetScaler ADC VPX** インスタンスを **NetScaler ADM** に追加する

February 6, 2024

Citrix ADM を使用して、Amazon Web Services (AWS) や Microsoft Azure などのパブリッククラウドにデプロイされた Citrix ADC VPX インスタンスを管理および監視できます。パブリッククラウドに展開されている NetScaler ADM と NetScaler ADC VPX インスタンスの間にレイヤー 3 接続を確立する必要があります。レイヤー 3 接続を確立するには、Citrix CloudBridge Connector、Citrix SD-WAN、AWS への直接接続、Azure の VPN、または Equinix などのサードパーティ製のコネクタなどのソリューションを使用できます。

次のトポロジ例では、NetScaler ADM とクラウドにデプロイされた NetScaler ADC VPX インスタンス間のレイヤー 3 接続に Citrix CloudBridge Connector を使用しています。



Citrix CloudBridge Connector トンネルは、データセンター DC 内の NetScaler ADC アプライアンス NS\_Appliance-DC と、パブリッククラウドの NetScaler ADC 仮想アプライアンス (VPX) NS\_VPX\_CBC の間にセットアップされます。NS\_Appliance-DC および NS\_VPX\_CBC を使用すると、NetScaler ADM とパブリッククラウドにデプロイされた NetScaler ADC VPX インスタンス NS\_VPX\_1 との間の通信が可能になります。通信が確立されると、NetScaler ADM で NS\_VPX\_1 を検出できるようになります。

このトポロジを設定するには:

1. パブリッククラウドで NetScaler ADC VPX インスタンスをインストール、構成、および起動します。
  - 手順については、「[NetScaler ADC VPX を AWS にインストールする](#)」を参照してください。
  - 手順については、「[NetScaler ADC VPX を Microsoft Azure にインストールする](#)」を参照してください。
2. データセンターの仮想化プラットフォーム上で NetScaler ADC 物理アプライアンスを展開して構成するか、NetScaler ADC 仮想アプライアンス (VPX) をプロビジョニングして構成します。
  - 手順については、「[Citrix Hypervisor に NetScaler ADC VPX インスタンスをインストールする](#)」を参照してください。
  - 手順については、[VMware ESXi への Citrix 仮想アプライアンスのインストール](#)を参照してください。
  - 手順については、[Microsoft Hyper-V に NetScaler ADC 仮想アプライアンスをインストールする](#)を参照してください。
3. データセンターとパブリッククラウドの間に Citrix CloudBridge Connector を構成します。手順については、「[Citrix CloudBridge Connector の構成](#)」を参照してください。
4. NetScaler ADM とクラウドにデプロイされた NetScaler ADC VPX インスタンス間の接続を確立するための静的ルートを次のように構成します。

- a) NetScaler ADM にログオンします。
- b) [システム] > [静的ルート] に移動し、[追加] をクリックします。

## ← Create Static Route

Configure the static route for establishing connection between NetScaler MAS and the NetScaler VPX instances deployed on the cloud.

Network Address

 ?

Netmask

Gateway

- c) [ネットワークアドレス] フィールドに、NetScaler ADM からコネクタを経由する静的ルートを確認するネットワークのアドレスを入力します。
  - d) [ **Netmask** ] フィールドに、ネットワークのネットマスクを入力します。
  - e) 「ゲートウェイ」フィールドに、ゲートウェイのアドレスを入力します。
5. パブリッククラウド内の NetScaler ADC VPX インスタンスの IP アドレスの範囲を指定して、NetScaler ADC VPX クラウドインスタンスを Citrix ADNetScaler ADM に追加します。詳細な手順については、[「NetScaler ADM にインスタンスを追加する」](#)を参照してください。

## 仮想サーバーでのライセンスの管理および分析の有効化

February 6, 2024

### 注

- 分析を有効にする以下の情報と手順は、Citrix **ADM** バージョンが **13.0 build 41.x** 以降の場合にのみ適用されます。NetScaler ADM のバージョンが **13.0** ビルド **36.27** より前の場合は、「分析の有効化」を参照してください。
- デフォルトでは、[自動ライセンス仮想サーバ] オプションは有効になっています。仮想サーバのライセンスを取得するのに十分なライセンスがあることを確認する必要があります。ライセンスが制限されていて、要件に基づいて選択した仮想サーバのみにライセンスを付与する場合は、[自動ライセンス仮想サーバ] オプションを無効にします。[システム] > [ライセンスと分析] に移動し、[\*\* 仮想サーバーライセンスの割り当て] の [自動ライセンス仮想サーバー \*\*] オプションを無効にします。



分析を有効にするプロセスが簡素化されます。これで、仮想サーバーのライセンスを取得し、単一のワークフローで分析を有効にできます。

[システム] > [ライセンスと分析] に移動して、次の操作を行います。

- 仮想サーバライセンスの概要を表示する
- 仮想サーバー分析の概要の表示

[ライセンスの設定] または [分析の設定] をクリックすると、[すべての仮想サーバー] ページが表示されます。

| NAME                                                             | IP ADDRESS   | STATE | LICENSED | ANALYTICS STATUS              | TYPE           |
|------------------------------------------------------------------|--------------|-------|----------|-------------------------------|----------------|
| O365 STS 601 ADFS Load Balancing Virtual Server                  | 10.3.22.120  | Down  | Yes      | DISABLED                      | Load Balancing |
| V_DC1_v_http_42                                                  | 10.20.202.42 | Down  | Yes      | Web Insight, Security Insight | Load Balancing |
| Federated Identity 601 Prod 636 Load Balancing Virtual Server    | 10.3.22.194  | Down  | Yes      | DISABLED                      | Load Balancing |
| V_DC1_v_ssl_19                                                   | 10.20.202.19 | Down  | Yes      | Web Insight, Security Insight | Load Balancing |
| Dimensions Hyperspace Web Load Balancing Virtual Server          | 10.3.22.115  | Down  | Yes      | DISABLED                      | Load Balancing |
| Dimensions InterConnect Prod 80 Load Balancing Virtual Server    | 10.3.22.117  | Down  | Yes      | DISABLED                      | Load Balancing |
| LDAP Internal 389 Load Balancing Virtual Server                  | 10.3.22.118  | Down  | Yes      | DISABLED                      | Load Balancing |
| Dimensions EPCS Prod Load Balancing Virtual Server               | 10.3.22.119  | Down  | Yes      | Web Insight, Security Insight | Load Balancing |
| Dimensions InterConnect Prod 18002 Load Balancing Virtual Server | 10.3.22.117  | Down  | Yes      | Web Insight, Security Insight | Load Balancing |
| V_DC1_v_ssl_5                                                    | 10.20.202.5  | Down  | Yes      | Web Insight, Security Insight | Load Balancing |
| V_DC1_v_http_5                                                   | 10.20.202.5  | Down  | Yes      | Web Insight, Security Insight | Load Balancing |

[すべての仮想サーバー] ページでは、次の操作を実行できます。

- ライセンスのない仮想サーバーにライセンスを適用
- ライセンスされた仮想サーバーのライセンスを削除
- ライセンスされた仮想サーバーで分析を有効にする
- 分析の編集
- 分析を無効にする

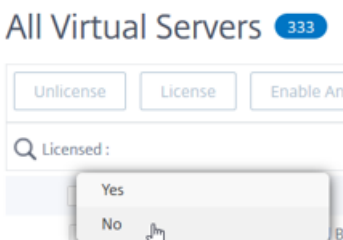
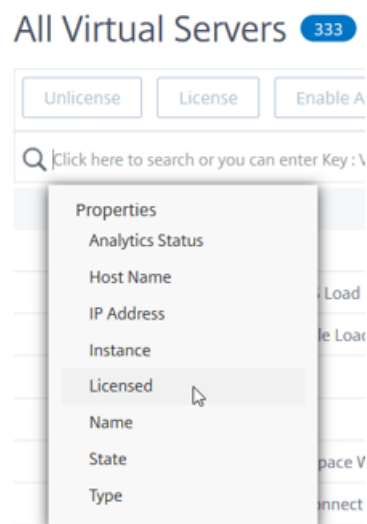
注

分析を有効にするためにサポートされている仮想サーバーは、負荷分散、コンテンツスイッチング、および NetScaler Gateway です。

仮想サーバでのライセンスの管理

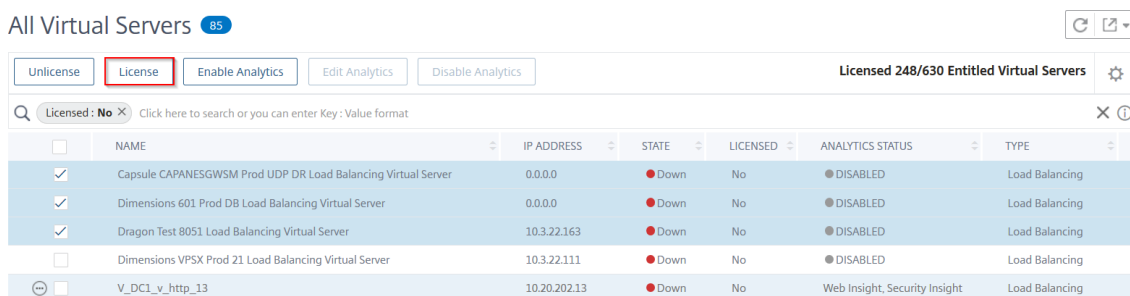
仮想サーバーのライセンスを取得するには、「すべての仮想サーバー」ページから：

1. 検索バーをクリックして [ライセンス済み] を選択し、[いいえ] を選択します。



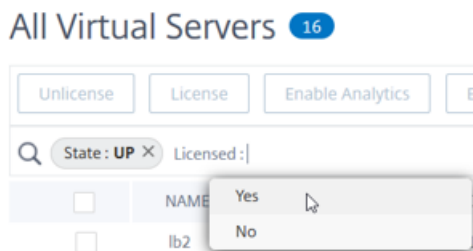
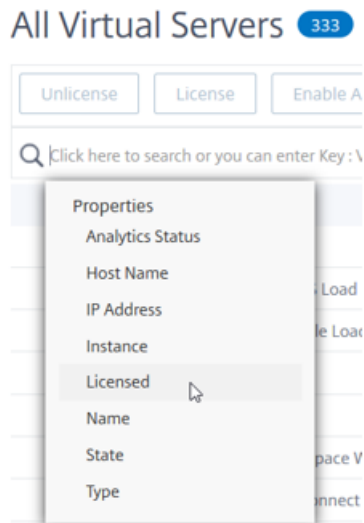
フィルタが適用され、ライセンスされていない仮想サーバのみが表示されます。

2. 仮想サーバーを選択し、[ライセンス] をクリックします。

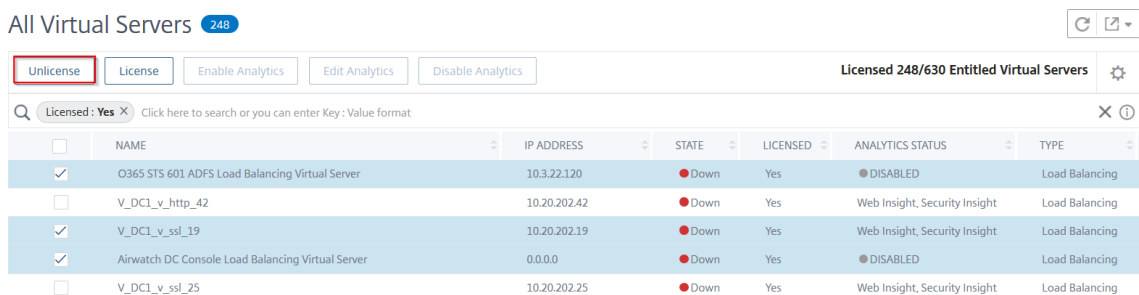


仮想サーバーのライセンスを解除するには、「すべての仮想サーバー」ページから：

1. 検索バーをクリックし、[ライセンス]を選択し、[はい]を選択します。



2. 仮想サーバーを選択し、[ライセンスの解除]をクリックします。



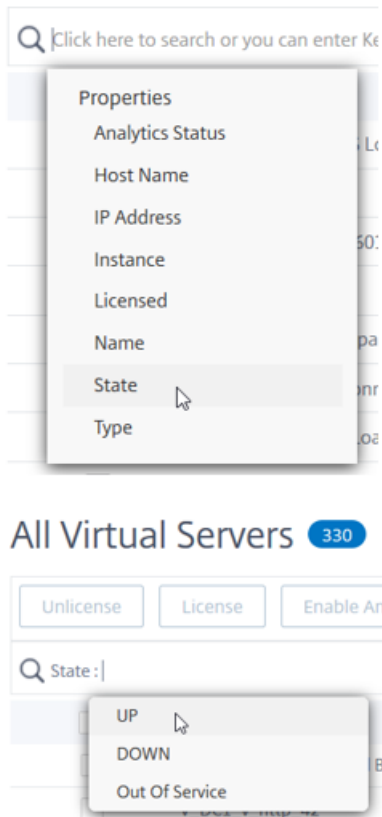
## 分析を有効にする

仮想サーバーの分析を有効にするための前提条件は次のとおりです。

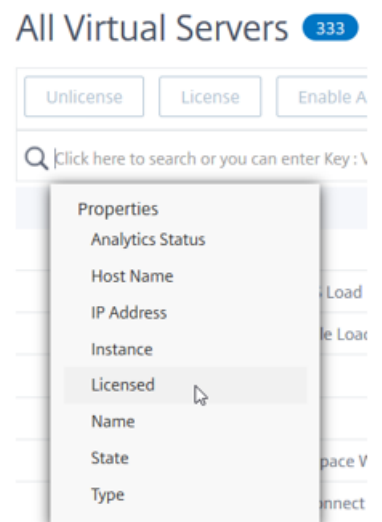
- 仮想サーバのライセンスが付与されていることを確認する
- 分析ステータスが無効になっていることを確認します
- 仮想サーバのステータスが **UP** であることを確認します。

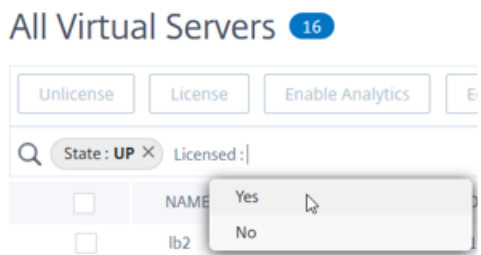
結果をフィルタリングして、前提条件に記載されている仮想サーバーを特定できます。

1. 検索バーをクリックして [ **State** ] を選択し、次に [ **UP** ] を選択します。

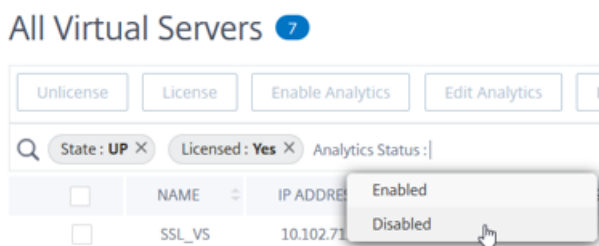
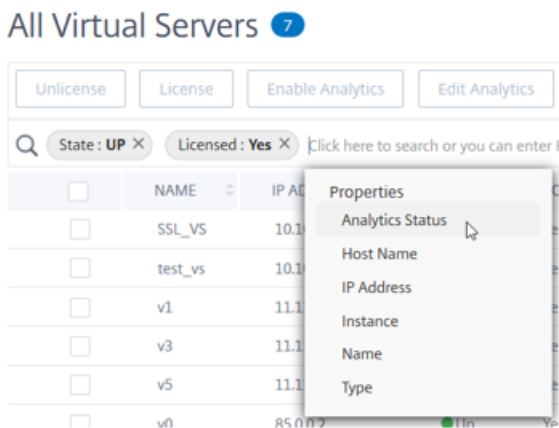


2. 検索バーをクリックして [ ライセンス ] を選択し、[ はい ] を選択します。

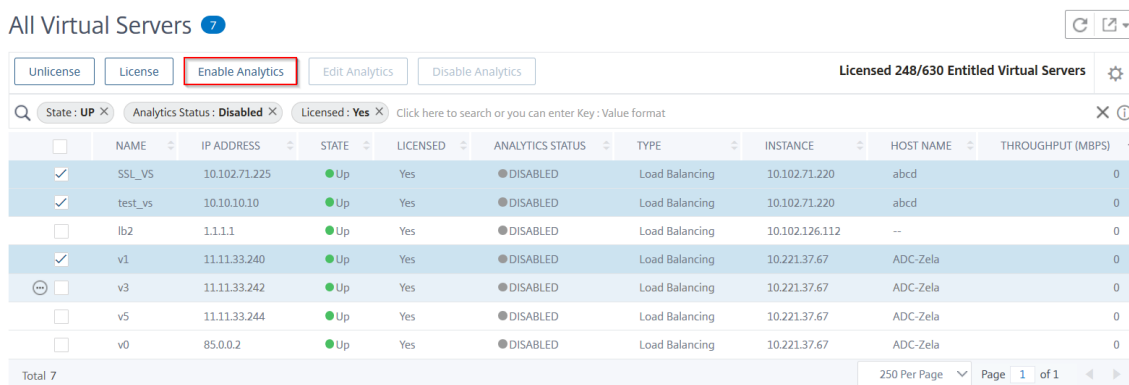




3. 検索バーをクリックし、[ **Analytics** ステータス]、[ 無効 ] の順に選択します。



4. フィルターを適用したら、仮想サーバーを選択し、「**Analytics** を有効にする」をクリックします。



注

または、特定のインスタンスの分析を有効にすることもできます。

- 1 1. [ \*\*ネットワーク\*\* ] > [ \*\*インスタンス\*\* ] > [ \*\*Citrix ADC\*\* ] に移動し、インスタンスタイプを選択します。たとえば、VPX です。
- 2
- 3 1. インスタンスを選択し、\*\*「アクションの選択」リストから「\*\*\*\*Analytics の設定\*\*」を選択します
- 4 1. 「仮想サーバーでの分析の設定」ページで、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。

5. 「アナリティクスを有効にする」ウィンドウで:

- a) インサイトタイプ (Web Insight または Security Insight) を選択します。
- b) **Logstream** をトランスポートモードとして選択

注

NetScaler ADC 12.0 以前の場合、**IPFIX** はトランスポートモードのデフォルトのオプションです。NetScaler ADC 12.0 以降では、トランスポートモードとして [ログストリーム] または [**IPFIX**] を選択できます。

IPFIX とログストリームの詳細については、「ログストリームの概要」を参照してください。

c) [ インスタンスレベルオプション ] で以下を実行します

- [ **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。
- **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。

d) 式はデフォルトで true です

e) [**OK**] をクリックします

## Enable Analytics ✕

**Selected Virtual Server - Load Balancing: 3**

Web Insight

Security Insight

▼ Advanced Options

Transport Mode

Logstream  IPFIX

Instance level options

Enable HTTP X-Forwarded-For

Citrix Gateway

▼ Expression Configuration

Select expression for Load Balancing/Content Switching

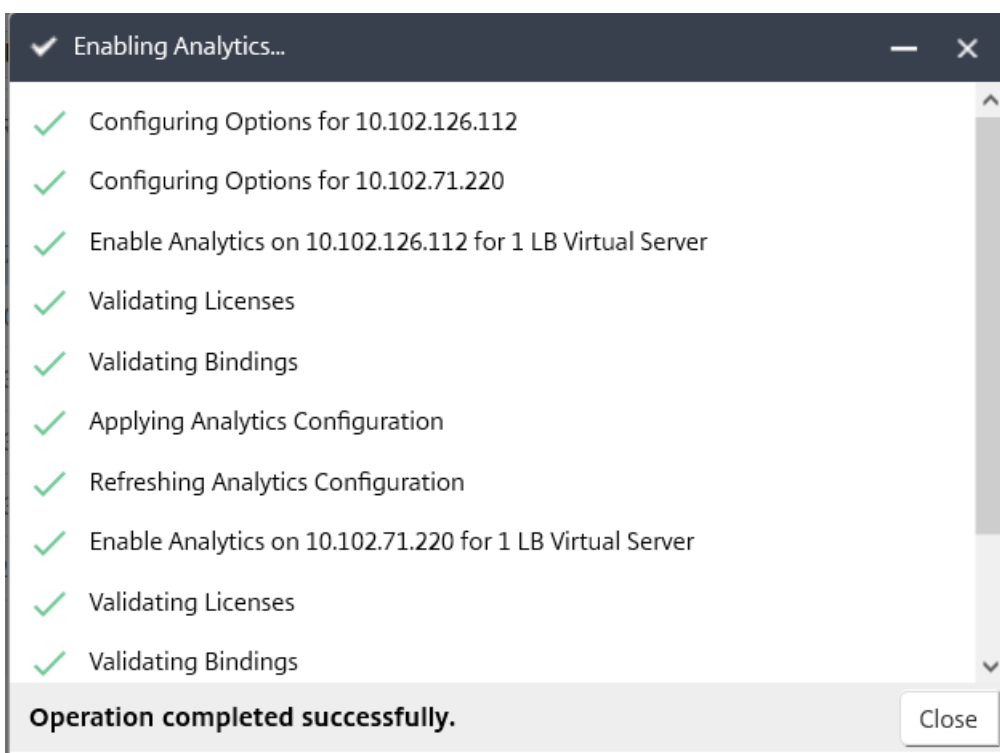
Select Expression

Edit Expression

## 注

- ライセンスされていない仮想サーバーを選択すると、NetScaler ADM はまずそれらの仮想サーバーのライセンスを取得し、次に分析を有効にします。
- 管理パーティションでは、**Web Insight** のみがサポートされます
- キャッシュリダイレクト、認証、GSLB などの仮想サーバーでは、分析を有効にすることはできません。エラーメッセージが表示されます。

[OK] をクリックすると、NetScaler ADM は選択した仮想サーバー上で分析を有効にするために処理します。



注

Citrix ADM では、ログストリームに Citrix ADC SNIP を使用し、IPFIX には NSIP を使用します。Citrix ADM エージェントと Citrix ADC 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、次のポートを開いて、Citrix ADM が AppFlow トラフィックを収集できるようにしてください。

| 転送モード     | 接続元 IP | 種類  | ポート  |
|-----------|--------|-----|------|
| IPFIX     | NSIP   | UDP | 4739 |
| Logstream | SNIP   | TCP | 5557 |

分析の編集

仮想サーバー上のアナリティクスを編集するには:

1. 仮想サーバの選択

注

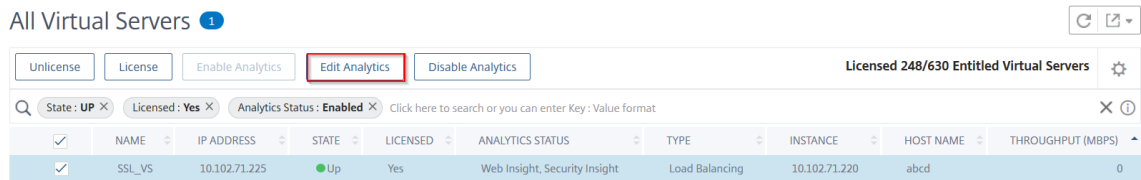
または、特定のインスタンスの分析を編集することもできます。

- 1 1. [ \*\*ネットワーク\*\* ] > [ \*\*インスタンス\*\* ] > [ \*\*Citrix ADC\*\* ] に移動し、インスタンスタイプを選択します。たとえば、VPX です。



- 2
- 3 1. インスタンスを選択して [ **\*\*Analytics を編集\*\*** ] をクリックします。

2. 「アナリティクスの編集」をクリック



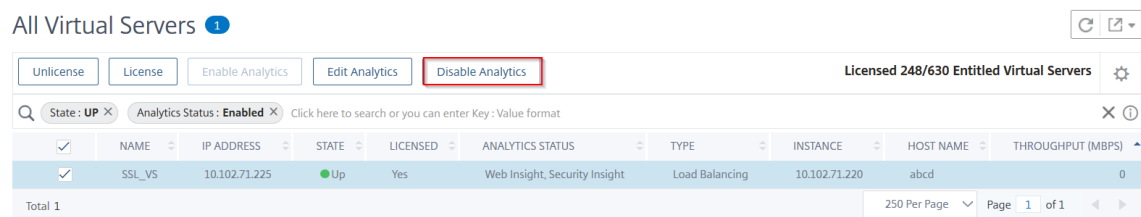
3. **Analytics** 設定の編集ウィンドウで、適用するパラメータを編集します。

4. [OK] をクリックします。

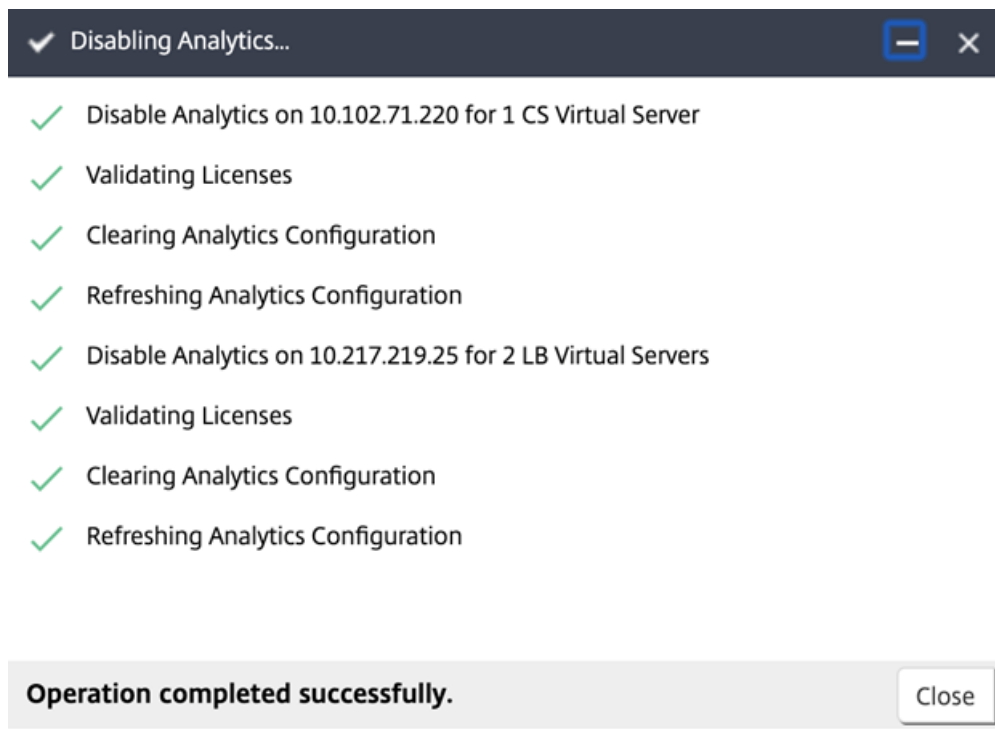
分析を無効にする

選択した仮想サーバーの分析を無効にするには:

1. 仮想サーバの選択
2. 分析を無効化をクリック



NetScaler ADM は、選択した仮想サーバーの分析を無効にします。



次の表では、IPFIX および Logstream をトランスポートモードとしてサポートする NetScaler ADM 機能を説明します。

| 機能               | IPFIX | Logstream |
|------------------|-------|-----------|
| Web Insight      | •     | •         |
| Security Insight | •     | •         |
| Gateway Insight  | •     | •         |
| HDX Insight      | •     | •         |
| SSL Insight      | 未サポート | •         |
| CR Insight       | •     | •         |
| IP レピュテーション      | •     | •         |
| AppFirewall      | •     | •         |
| クライアント側の測定       | •     | •         |
| Syslog/Auditlog  | •     | •         |

以前のビルドの仮想サーバーでの分析を有効にする

**Citrix ADM 13.0** ビルド **36.27** の仮想サーバーで分析を有効にするには:

1. [ネットワーク]>[インスタンス]>[**Citrix ADC**]に移動し、分析を有効にする Citrix ADC インスタンスを選択します。
2. インスタンスのリストから、インスタンスを選択します。
3. 「アクションの選択」リストから、「**Analytics** の設定」を選択します。
4. 「アプリケーションリスト」で、仮想サーバーを選択し、「**AppFlow** を有効にする」をクリックします。
5. 「**AppFlow** を有効にする」フィールドに「true」と入力し、有効にする分析に基づいて、「Security Insight」または「Web Insight」、あるいはその両方を選択します。

### Enable AppFlow

**Select Expression**

Load Balancing

▼

true

**Transport Mode**  IPFIX  Logstream

Web Insight

Client Side Measurement

Security Insight

If there is a firewall between Citrix ADM and the Citrix ADC instance, please make sure the UDP port 4739 is open. This is to allow ADM to collect AppFlow traffic. SSL Insight will not be available if IPFIX Transport mode is used.

OK

Cancel

注

Citrix ADM では、ログストリームに Citrix ADC SNIP を使用し、IPFIX には NSIP を使用します。NetScaler ADM と NetScaler ADC 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、次のポートを開いて NetScaler ADM が AppFlow トラフィックを収集できるようにします。

| 転送モード     | 接続元 IP | 種類  | ポート  |
|-----------|--------|-----|------|
| IPFIX     | NSIP   | UDP | 4739 |
| Logstream | SNIP   | TCP | 5557 |

- HDX Insight および Gateway Insight では、[AppFlow を有効にする]をクリックしながら[NetScaler ADC インスタンスに構成された VPN 仮想サーバー] を選択し、それに応じてプロトコルの [ICA] または [HTTP] チェックボックスをオンにする必要があります。

### Enable AppFlow

Select Expression \*

VPN

Transport Mode  IPFIX  Logstream  ICA

TCP

HTTP

If the AppFlow for a virtual server is enabled on more than one NetScaler Management and Analytics System appliance, then the appliance on which the AppFlow is enabled most recently has the highest priority for collecting the information.

OK

Cancel

- TCP Insight の場合は、[システム] > [分析設定] > [機能の構成] に移動し、[ **TCP Insight** を有効にする] を選択します。
- Video Insight の場合は、NetScaler ADC アプライアンスで構成を変更する必要があります。ビデオインサイトの分析を有効にする方法については、[Video Insight](#) を参照してください。
- WAN Insight の場合：
  - [インフラストラクチャ] > [インスタンス] > [**Citrix SD-WAN WO**] に移動し、データセンターの WAN 最適化アプライアンスを選択します。
  - [アクション] リストから [インサイトの有効化] を選択します。
  - 必要に応じて以下のパラメーターを選択します。
    - \* HDX Insight の地情報データ収集: クライアントの IP アドレスを Google Geo API と共有します。
    - \* AppFlow: WAN 最適化インスタンスからのデータの収集を開始します。
      - ・ TCP と WANOpt: TCP と WanOpt のインサイトレポートを提供します。
      - ・ HDX: HDX Insight レポートを提供します。
      - ・ HDX 用の TCP のみ: HDXInsight レポートにのみ TCP を提供します。

Citrix ADM で検出された Citrix ADC インスタンスで AppFlow を有効にしているときに、AppFlow トランスポートモードを **IPFIX** またはログストリームに選択できます。IPFIX とログストリームの詳細については、「ログストリームの概要」を参照してください。

次の表では、IPFIX および Logstream をトランスポートモードとしてサポートする NetScaler ADM 機能を説明します。

| 機能               | IPFIX | Logstream |
|------------------|-------|-----------|
| Web Insight      | •     | •         |
| Security Insight | •     | •         |
| Gateway Insight  | •     | •         |
| HDX Insight      | •     | •         |
| SSL Insight      | 未サポート | •         |
| CR Insight       | •     | •         |
| IP レピュテーション      | •     | •         |
| AppFirewall      | •     | •         |
| クライアント側の測定       | •     | •         |
| Syslog/Auditlog  | •     | •         |

また、Citrix ADM の「Web Insight を有効にする」オプションを使用して、Web Insight トラフィックの処理を有効または無効にすることもできます。Web Insight トラフィックを監視しない場合は、このオプションを無効にすることができます。NetScaler ADM は、管理対象インスタンスの仮想サーバーからの Web Insight トラフィックを処理しません。

## NTP サーバーの構成

February 6, 2024

Citrix ADM でネットワークタイムプロトコル (NTP) サーバーを構成して、その時計を NTP サーバーと同期させることができます。NTP サーバーを構成すると、NetScaler ADM クロックは、ネットワーク上の他のサーバーと同じ日付と時刻の設定になります。

**Citrix ADM** で NTP サーバーを構成するには:

1. ADM GUI から、[システム] > [管理] に移動します。[システム管理] ページの [ネットワーク構成] で、[NTP サーバー] をクリックします。次に、[追加] をクリックします。

2. **[Create NTP Server]** ページで、次の詳細情報を入力します。

- **Server Name/IP Address** -NTP サーバーのドメイン名と IP アドレスを入力します。ここで入力したドメイン名と IP アドレスは、NTP サーバーを追加した後は変更できません。
- **Minimum Poll Interval** -NTP メッセージの送信間隔の最小値を秒数（2 のべき乗）で指定します。たとえば、最小ポーリング間隔を 64 秒にする場合、64 は 2 の 6 乗であるため、「6」と入力します。
- **Maximum Poll Interval** -NTP メッセージの送信間隔の最大値を秒数（2 のべき乗）で指定します。たとえば、最大ポーリング間隔を 256 秒にする場合、256 は 2 の 8 乗であるため、「8」と入力します。
- **Key Identifier** - NTP サーバーとの対称キー認証に使用するキー識別子を入力します。Autokey を選択する場合は、キー識別子を追加しないでください。
- **Autokey** - NTP サーバーとの公開キー認証を使用する場合は、**[Autokey]** を選択します。キー識別子を追加する場合は、Autokey を選択しないでください。
- **Preferred** -この NTP サーバーをクロック同期の優先サーバーとして指定する場合に、このオプションを選択します。2 台以上のサーバーを構成する場合のみ適用されます。

3. **[作成]** をクリックします。

**NetScaler ADM** で **NTP** 同期を有効にするには：

1. **[System]** > **[NTP Servers]** の順に選択します。
2. **[NTP 同期化]** をクリックし、**[NTP 同期を有効にする]** チェックボックスをオンにします。
3. **[OK]** をクリックします。

## システム設定の構成

February 6, 2024

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

### システムアラームの設定

システムアラームを設定して、システムの重大な問題または重大な問題を認識していることを確認します。たとえば、CPU 使用率が高い場合や、サーバーへのログインに複数回失敗した場合に、管理者に通知が送信されるようにします。cpuUsageHigh や memoryUsageHigh などの一部のアラームカテゴリでは、しきい値を設定してそれぞれの重要度（Critical や Major など）を定義できます。inventoryFailed や loginFailure などのカテゴリについては、重要度のみを定義できます。アラームカテゴリ（MemoryUsageHigh など）のしきい値を超えた場合、またはアラ

ームカテゴリに対応するイベント (LoginFailure など) が発生した場合、メッセージがシステムに記録され、そのメッセージを syslog メッセージとして表示できます。

システムアラームを設定するには、次の手順を実行します。

1. [システム] > [SNMP] に移動し、右上隅の [アラーム] タブをクリックします。
2. 設定するアラームを選択し、[Edit] をクリックします。
3. [Configure Alarm] ページで、アラームの重大度を選択し、[Threshold] を設定します。
4. しきい値を超えたアラーム、またはイベントが発生したアラームを表示するには、[システム] > [監査] に移動し、[Syslog メッセージ] をクリックします。

### システム通知の設定

さまざまなシステム関連機能について、ユーザーのグループを選択するために通知を送信できます。NetScaler ADM で通知サーバーを設定し、電子メールおよびショートメッセージサービス (SMS) Gateway サーバーを構成して、ユーザーに電子メールおよびテキスト通知を送信できます。通知を設定すると、ユーザーログインやシステム再起動など、システムレベルのアクティビティが確実に通知されます。

システム通知を構成するには、次の手順に従います。

1. [システム] > [管理] に移動します。[システム管理] ページの [イベント通知] で、[イベントの通知とダイジェストの構成] > [イベント通知] をクリックします。
2. [システム通知設定の構成] ページで、NetScaler ADM によって生成されるイベントのカテゴリまたはカテゴリを選択します。
3. 次に、メールサーバーまたは SMS サーバーを、メールまたは SMS、あるいはその両方を使用して通知を受信するように構成します。

### システム削除設定の構成

NetScaler ADM サーバーのデータベースに保存されるレポートデータの量を制限するために、NetScaler ADM がネットワークレポートデータ、イベント、監査ログ、およびタスクログを保持する間隔を指定できます。デフォルトでは、これらのデータは 24 時間ごとに (00:00 の時刻に) 削除されます。

システムプルーニング設定を構成するには:

1. [System] > [System Administration] の順に選択します。[データのプルーニング] で、[システムとインスタンスのデータのプルーニング] をクリックします。
2. システムページで、データを保持する日数を指定し、「保存」をクリックします。

## インスタンスの **Syslog** プルーニング設定の設定

データベースに保存される Syslog データの量を制限するために、Syslog データをパージする間隔を指定できます。NetScaler ADM から汎用 syslog データが削除されるまでの日数を指定できます。

インスタンスの **Syslog** 消去設定を構成するには:

1. [システム] > [管理] > [データプルーニング] に移動します。
2. [システムとインスタンスのデータプルーニング] > [インスタンス **Syslog**] をクリックします。
3. インスタンスの **Syslog** プルーニング設定ページで、「**Syslog** 汎用データの保持」フィールドに 1 日から 180 日までの日数を指定します。
4. [保存] をクリックします。

## インスタンスイベントプルーニング設定の構成

NetScaler ADM サーバーのデータベースに保存されるイベントメッセージデータの量を制限するために、NetScaler ADM がネットワークレポートデータ、イベント、監査ログ、およびタスクログを保持する間隔を指定できます。デフォルトでは、これらのデータは 24 時間ごとに (00:00 の時刻に) 削除されます。

インスタンスイベントプルーニング設定を構成するには:

1. [システム] > [管理] に移動します。
2. [システム管理] ページの [データプルーニング] で、[システムとインスタンスのデータプルーニング] をクリックします。
3. 「データプルーニング」ページで、「インスタンスイベント」をクリックします。
4. [保持するデータ (日数)] フィールドに、Citrix ADM サーバーにデータを保持する時間間隔を日単位で入力し、[保存] をクリックします。

## システムバックアップの設定を構成する

NetScaler ADM は、毎日 00:30 にシステムを自動的にバックアップします。デフォルトでは、3 つのバックアップファイルが保存されます。それ以上の数のシステムのバックアップを保持する必要があるかもしれません。バックアップファイルを暗号化できるほか、バックアップを外部サーバーに保存することを選択できます。

システムバックアップの設定を構成するには、次の手順で行います。

1. [システム] > [管理] に移動します。
2. [バックアップ] で、[システムとインスタンスのバックアップの設定] をクリックします。
3. [システム] をクリックし、[システムバックアップ設定の構成] ページで必要な値を指定します。



## インスタンスのバックアップ設定の構成

Citrix ADC インスタンスの現在の状態をバックアップすると、インスタンスが不安定になった場合にバックアップファイルを使用して安定性を回復できます。アップグレードを実行する前にこれを行うことは特に重要です。デフォルトでは、12 時間ごとにバックアップされて、3 つのバックアップファイルがシステムに保持されます。

インスタンスのバックアップ設定を構成するには：

1. [システム] > [管理] に移動します。
2. [バックアップ] で、[システムとインスタンスのバックアップの設定] をクリックします。
3. [\*\* インスタンスのバックアップ設定の設定 \*\*] の [インスタンス] をクリックし、必要な値を指定します。

## ADM 機能の有効化または無効化

管理者は、[システム] > [管理] > [設定可能な機能] ページで次の機能を有効または無効にできます。

- エージェントのフェイルオーバー：エージェントのフェイルオーバーは、複数のアクティブなエージェントがあるサイトで実行できます。サイト内でエージェントが非アクティブ（DOWN 状態）になると、NetScaler ADM サービスは、非アクティブなエージェントの ADC インスタンスを他のアクティブなエージェントに再配布します。詳細については、「[オンプレミスエージェントをマルチサイト展開用に構成する](#)」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-エンティティは、ADC インスタンスにアタッチされたポリシー、仮想サーバ、サービス、またはアクションのいずれかです。デフォルトでは、NetScaler ADM は 60 分ごとに構成済みのネットワーク機能エンティティを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。
- インスタンスのバックアップ -NetScaler ADC インスタンスの現在の状態をバックアップし、後でバックアップしたファイルを使用して ADC インスタンスを同じ状態に復元します。詳しくは、「[NetScaler ADC インスタンスのバックアップと復元](#)」を参照してください。
- インスタンス構成の監査 -管理対象の NetScaler ADC インスタンスの構成変更を監視し、構成エラーのトラブルシューティングを行い、未保存の構成を復元します。詳しくは、「[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 NetScaler ADC インスタンスでのイベントまたはエラーの発生を表します。Citrix ADM で受信したイベントは [イベントの概要] ページ（[ネットワーク] > [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（[ネットワーク] > [イベント] > [イベントメッセージ]）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用。詳細については、「[ネットワークレポート](#)」を参照してください。

- インスタンス **SSL** 証明書 -NetScaler ADM では、管理対象のすべての NetScaler ADC インスタンスにインストールされた SSL 証明書を一元的に表示できます。詳細については、「[SSL ダッシュボード](#)」を参照してください。
- インスタンス **Syslog** -すべての syslog メッセージを Citrix ADNetScaler ADM 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は、NetScaler ADC インスタンスで生成された syslog イベントを監視できます。

機能を有効にするには、次の手順を実行します。

1. 有効にする機能を一覧から選択します。
2. [有効にする] をクリックします。

重要:

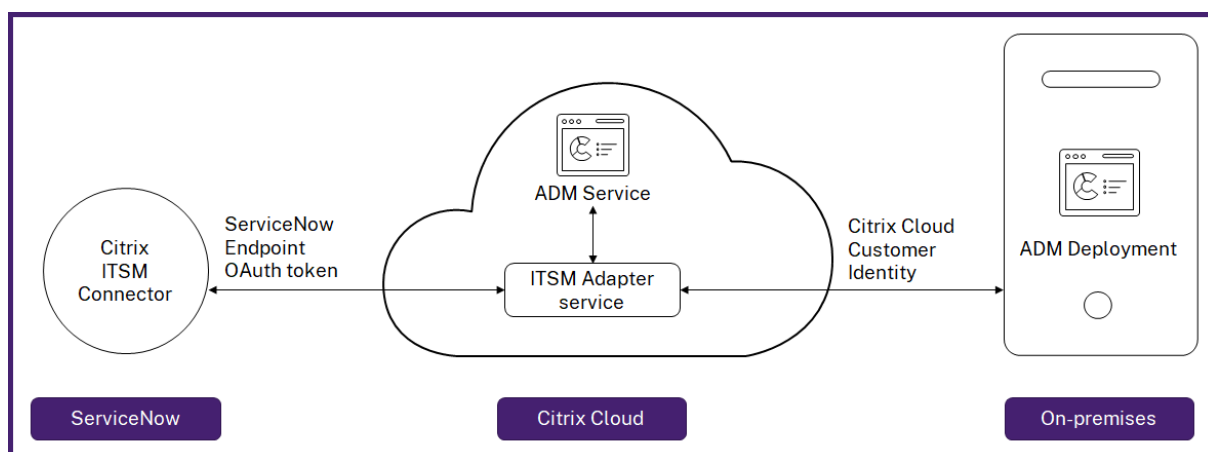
機能が無効になっている場合、ユーザーはその機能に関連付けられた操作を実行できません。

## NetScaler ADM を ServiceNow インスタンスと統合する

February 6, 2024

NetScaler ADC および ADM イベントの ServiceNow 通知を有効にする場合は、NetScaler ADM を ServiceNow インスタンスと統合します。この統合では、Citrix ITSM コネクタを使用して NetScaler ADM と ServiceNow インスタンス間の通信を行います。

ServiceNow と ADM の統合では、トークンベースの認証に ITSM アダプタサービスを使用します。そのために、ServiceNow にエンドポイントインスタンスが作成されます。詳細については、「[ITSM アダプタの仕組み](#)」を参照してください。



ADM オンプレミス展開を ITSM アダプタに接続するには、必ず顧客 ID を設定してください。詳細については、「[顧客 ID の設定](#)」を参照してください。

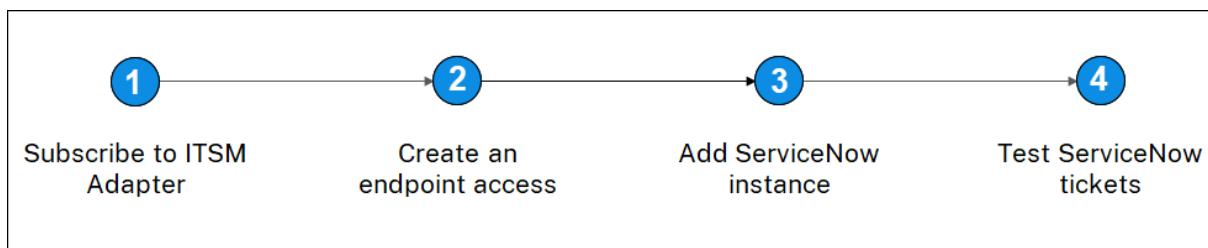
## 前提条件

ADM と ServiceNow を統合する前に、次のことを確認してください。

1. [Citrix Cloud にサインアップ](#)します。Citrix Cloud 管理者を管理するためのアクセス権があることを確認してください。詳しくは、「[Citrix Cloud 管理者の管理](#)」を参照してください。

## ADM を ServiceNow と統合するにはどうすればいいですか

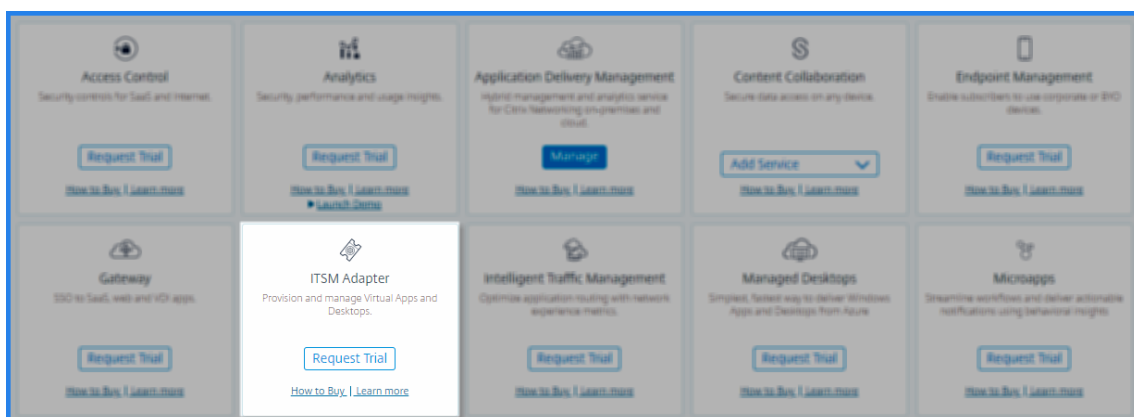
ITSM コネクタを使用して NetScaler ADM と ServiceNow を統合するには、次の手順を実行します。



1. Citrix Cloud で ITSM アダプターサービスにサブスクライブします。
2. ServiceNow インスタンスにエンドポイントアクセスを作成します。
3. ServiceNow インスタンスを追加します。
4. ServiceNow チケットの自動生成を ADM でテストします。

### ステップ 1-Citrix Cloud で ITSM アダプターサービスにサブスクライブする

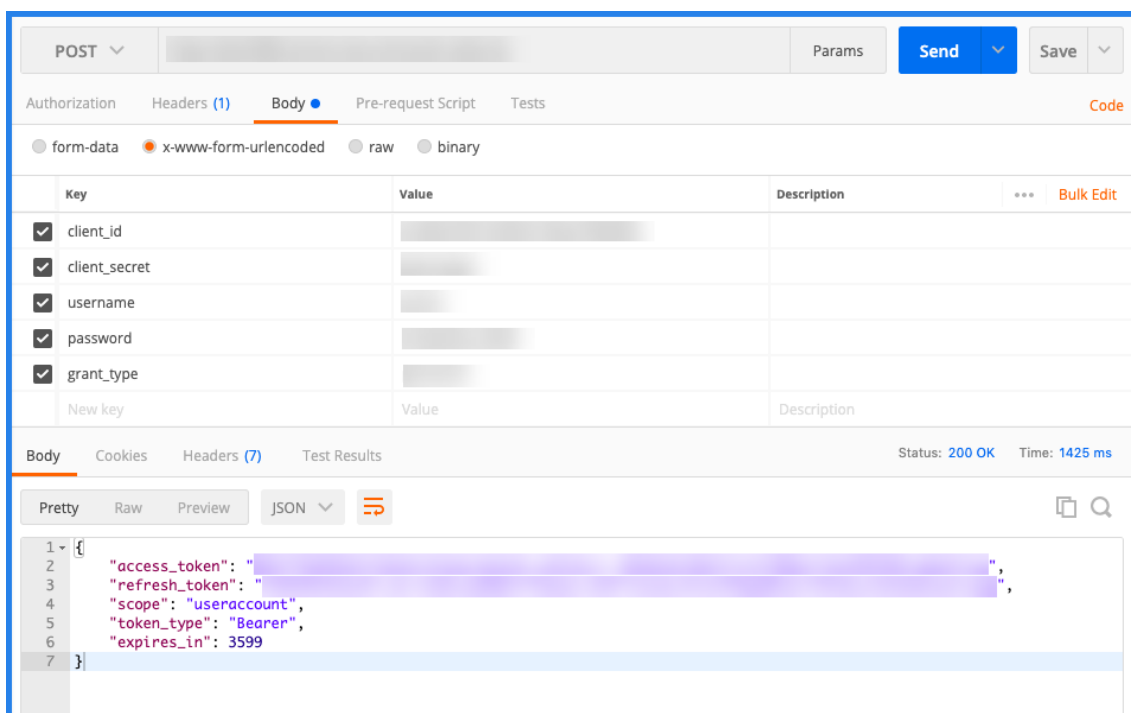
1. [ **ITSM アダプタ** ] タイルで、[ 試用版の要求 ] をクリックします。



2. [ **ID アクセスと管理** ] > [ **API アクセス** ] に移動し、クライアント **ID** とクライアントシークレットの情報をメモします。

## ステップ 2-ServiceNow インスタンスでエンドポイントアクセスを作成する

1. 管理者の認証情報を使用して ServiceNow インスタンスにログインします。
2. ServiceNow ストアに移動します。 **Citrix ITSM** コネクタをダウンロードしてインストールします。
3. **Citrix ITSM** コネクタペインで、**[\*\* ホーム]** を選択し、**[認証]** をクリックします。 **\*\*Citrix Cloud** からメモしたクライアント ID とシークレットを入力します。
4. 接続をテストします。
5. 構成を保存します。 ServiceNow から、接続がアクティブであることを示す確認メッセージが表示されます。
6. ServiceNow インスタンスにアクセスするためのエンドポイントを作成します。 [クライアントがインスタンスにアクセスするためのエンドポイントを作成する](#) を参照してください。
7. クライアント ID とクライアントシークレットを使用して、アクセストークンとリフレッシュトークンを取得します。 [OAuth トークンを参照してください](#)。



## ステップ 3-ServiceNow インスタンスを追加する

1. [管理] タブで、[ServiceNow インスタンスの追加] を選択します。
2. インスタンス名、クライアント **ID**、クライアントシークレット **\*\***、**\*\*** 更新トークン、およびアクセストークンを指定します。
3. [テスト] をクリックします。

ServiceNow インスタンスが ITSM アダプタサービスに接続されました。

4. 接続が正常にテストされたら、[保存] をクリックして ServiceNow インスタンスを追加します。

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

1. NetScaler ADM にログインします。
2. [アカウント] > [通知] に移動し、[ **ServiceNow** ] を選択します。
3. リストから ServiceNow プロファイルを選択します。
4. 「テスト」 をクリックして ServiceNow チケットを自動生成し、構成を確認します。

NetScaler ADM GUI で ServiceNow チケットを表示する場合は、[ **ServiceNow** チケット ] を選択します。

#### ADM で **ServiceNow** 通知を設定する

ServiceNow インスタンスが ITSM アダプタに登録されると、NetScaler ADM GUI で次のイベントに対する ServiceNow 通知を設定できます。

**重要:**

この機能は、ServiceNow クラウドでサポートされています。

- **NetScaler ADC イベント:** NetScaler ADM は、選択した管理対象 NetScaler ADC インスタンスから、選択した一連の NetScaler ADC イベントの ServiceNow インシデントを生成できます。

管理対象インスタンスから NetScaler ADC イベントの ServiceNow 通知を送信するには、イベントルールを構成し、ルールのアクションを「**ServiceNow 通知の送信**」として割り当てる必要があります。

[ネットワーク]>[イベント]>[ルール]に移動して、ADM で イベントルールを作成します。詳しくは、[ServiceNow 通知の送信を参照してください](#)。

- **アプリケーション分析:** NetScaler ADM は、指定されたしきい値に違反するアプリケーションに対して ServiceNow インシデントを生成できます。

**Configure Rule**

For more information about each metric, see [documentation](#).

| Metric*   | Comparator* | Value* |
|-----------|-------------|--------|
| App Score | <           | 90     |

**Notification Settings**

- Enable Threshold
- Notify through Email
- Notify through Slack
- Notify through ServiceNow

Citrix\_Workspace\_SN [Test]

[Create] [Close]

この例では、アプリケーションの App スコアが 90 未満になると ServiceNow インシデントが生成されます。

- **SSL 証明書と ADM ライセンスイベント:** NetScaler ADM は、SSL 証明書の有効期限および ADM ライセンス有効期限イベントの ServiceNow インシデントを生成できます。

SSL 証明書の有効期限切れに関する ServiceNow 通知を送信するには、[SSL 証明書の有効期限を参照してください](#)。

ADM ライセンスの有効期限切れに関する ServiceNow 通知を送信するには、「[NetScaler ADM ライセンスの有効期限](#)」を参照してください。

## エクスポートレポートのエクスポートまたはスケジュール設定

February 6, 2024

NetScaler ADM では、選択した NetScaler ADM 機能の包括的なレポートをエクスポートできます。このレポートには、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が表示されます。

NetScaler ADM は、個別の ADM 機能の下に機能固有のスケジュールエクスポートレポートを表示します。これらのレポートは表示、編集、削除できます。たとえば、NetScaler ADC インスタンスのエクスポートレポートを表示するには、[ネットワーク] > [インスタンス] > [**NetScaler ADC**] の順に選択し、[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。

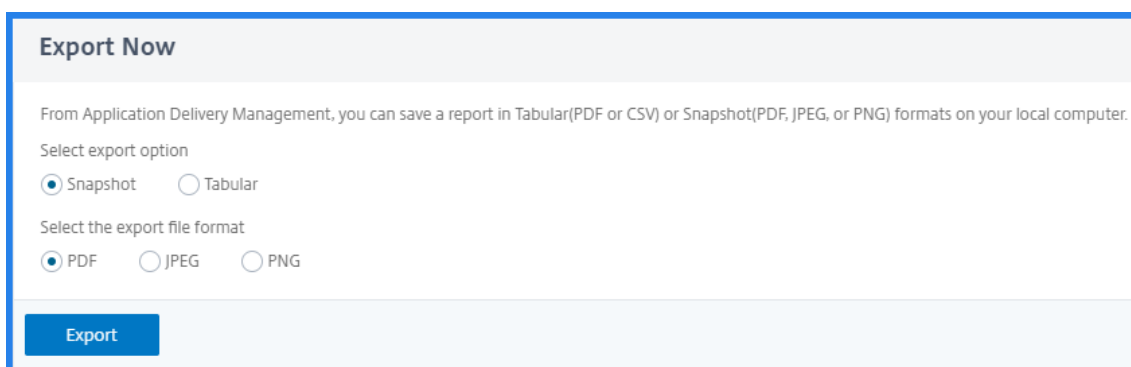
- レポートをローカルコンピュータにエクスポートする
- エクスポートレポートのスケジュール設定
- 定期エクスポートレポートを表示、編集、または削除する

### レポートのエクスポート

レポートを ADM からローカルコンピュータにエクスポートするには、次の手順に従います。

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。

- 
- 



4. ローカルコンピュータにレポートを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

エクスポートレポートを定期的にスケジュールするには、繰り返しの間隔を指定します。NetScaler ADM は、エクスポートされたレポートを設定済みのメールまたはスラックプロファイルに送信します。

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. 「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的に入力されます。ただし、意味のあるタイトルで書き換えることができます。
  - エクスポートオプション -スナップショットまたは表形式で ADM レポートを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
  - [形式]-構成済みの電子メールまたは Slack のプロファイルに関するレポートを受信するファイル形式を選択します。
  - [繰り返し]-リストから [毎日]、[毎週]、または [毎月] を選択します。
  - 説明 -レポートに意味のある説明を指定します。
  - エクスポート時間 -レポートをエクスポートする時刻を指定します。
  - 電子メール - 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. [**Schedule**] をクリックします。



### Schedule Export

You can schedule the export of the reports to specified email addresses at various intervals.

Subject\*

Select export option

Snapshot     Tabular

Select the export file format

PDF     CSV

Recurrence\*

Description

commandcenter.event\_time\_zone\_note\_svc

Export Time\*

How many data records do you want to export?\*

Email

Email Distribution List\*






Slack

### 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、以下を実行します。

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。  
 レポートのエクスポートページには、機能固有のエクスポートレポートがすべて表示されます。
2. 編集するレポートを選択し、**【編集】**をクリックします。

## アップグレード

February 6, 2024

NetScaler ADM の各リリースでは、機能が強化された新機能および更新された機能が提供されます。NetScaler ADM を最新リリースにアップグレードして、新機能とバグ修正を利用することをお勧めします。[すべてのリリース発表に付随するリリースノートには](#)、拡張機能、既知の問題点、およびバグ修正の包括的なリストが含まれています。また、アップグレードを開始する前に、ライセンスフレームワークと使用できるライセンスの種類を理解することも重要です。NetScaler ADM のライセンス情報については、「[ライセンス](#)」を参照してください。

アップグレードパスの情報は、『[Citrix アップグレードガイド](#)』にも記載されています。

### アップグレードの前に

Citrix ADM ダウンロードページからアップグレードパッケージをダウンロードし、この記事の指示に従ってシステムを最新の 13.0 ビルドにアップグレードします。アップグレードプロセスが開始されると、ADM が再起動し、アップグレードが完了すると、既存の接続が終了して再接続されます。既存の構成は保持されますが、アップグレードが正常に完了するまで NetScaler ADM はデータを処理しません。

#### 重要

NetScaler ADM のバージョンとビルドは、NetScaler ADC のバージョンおよび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 ADM 12.1 ビルド 50.39 をインストールしている場合は、NetScaler ADC 12.1 ビルド 50.28/50.31 以前がインストールされていることを確認します。

### 13.0 にアップグレードする前に注意すべき点:

- バージョン 11.1 またはバージョン 12.0 56.x および以前のビルドからアップグレードする場合は、次の手順を実行します。
  - 既存のバージョンから 12.0 ビルド 57.24 にアップグレードします。
  - バージョン 12.1 の最新ビルドにアップグレードします。
  - バージョン 13.0 にアップグレードします。
- 12.0 ビルド 57.24 以降からアップグレードする場合は、まず 12.1 にアップグレードしてから 13.0 にアップグレードします。
- 12.1 からアップグレードする場合は、13.0 に直接アップグレードできます。
- 13.0 67.xx 以降にアップグレードする場合は、まず 13.0 64.xx にアップグレードしてから 13.0 67.xx 以降にアップグレードし、ユーザーエクスペリエンスを向上させます。

### 13.0 67.xx 以降にアップグレードする前に注意すべき重要なポイント

ADM ソフトウェアをバージョン 13.0 67.xx 以降にアップグレードすると、ADM データベースも移行されます。このデータ移行は、ADM が PostgreSQL バージョン 10.11 を使用しているために発生します。

#### 注

ADM ソフトウェアのダウングレードはサポートされていません。ダウングレードを試みないでください。

#### 推奨される注意事項:

- 13.0 67.xx 以降にアップグレードする場合は、NetScaler ADM サーバーのスナップショットを作成します。
- アップグレードする前に、NetScaler ADM サーバーをバックアップしてください。
- アップグレード後、NetScaler ADM サーバーと管理対象インスタンス間の接続の再確立が必要になる場合があります。「続行すると接続に失敗する可能性がある」という旨を警告する確認メッセージが表示されます。
- 高可用性セットアップの NetScaler ADM サーバーでは、アップグレード時にどちらのノードでも構成を変更しないでください。

#### 警告

アップグレード処理が正常に完了するまでブラウザを更新しないでください。アップグレードが完了するまでのおおよその時間を GUI で確認します。

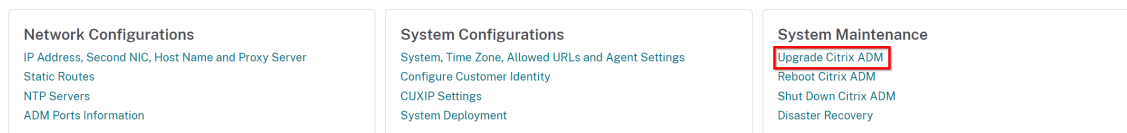
- アップグレード後、アクティブノードは高可用性ペアで変更できます。

### 単一の NetScaler ADM サーバーをアップグレード

単一の NetScaler ADM サーバーをアップグレードするには:

1. 管理者の資格情報を使用して NetScaler ADM にログインします。
2. [システム] > [システム管理] に移動します。システム管理の小見出しの下で、「NetScaler ADM のアップグレード」をクリックします。

#### System Administration



3. **NetScaler ADM をアップグレードする** ページで、[アップグレードに成功したらソフトウェアイメージをクリーンアップする] チェックボックスをオンにして、アップグレード後にイメージファイルを削除します。このオプションを選択すると、アップグレード時に NetScaler ADM イメージファイルが自動的に削除されます。

注

このオプションはデフォルトで選択されています。アップグレードプロセスを開始する前にこのチェックボックスをオンにしない場合は、イメージを手動で削除する必要があります。

## ← Upgrade Citrix ADM

Software Image\*

Choose File
▼

Clean software image on successful upgrade

OK
Close

- その後、[ローカル]（ローカル マシン）または [アプライアンス] を選択して、新しいイメージファイルをアップロードできます。ビルドファイルは、NetScaler ADM 仮想アプライアンス上に存在する必要があります。

## ← Upgrade Citrix ADM

Software Image\*

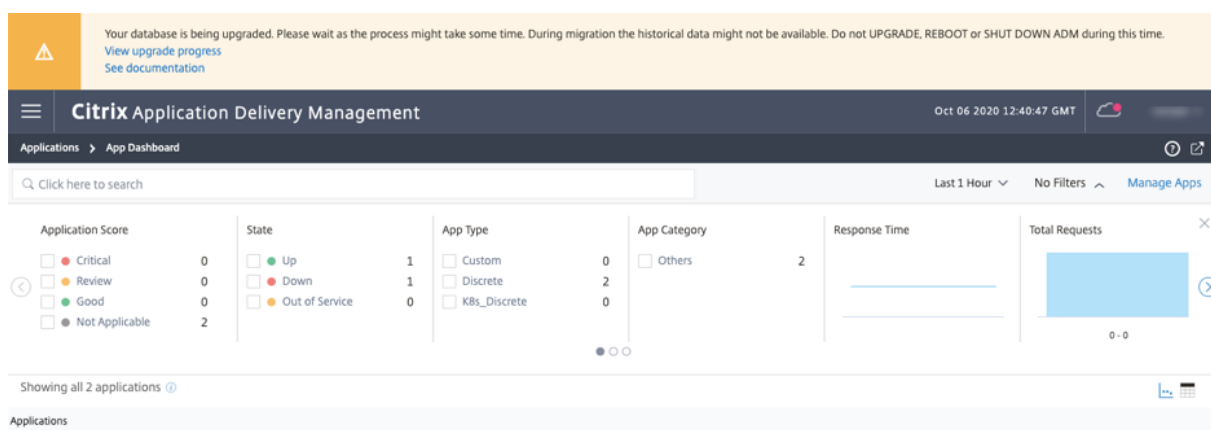
Choose File
▼
build-mas-■■■■■■■■■■.tgz
?

Clean software image on successful upgrade

OK
Close

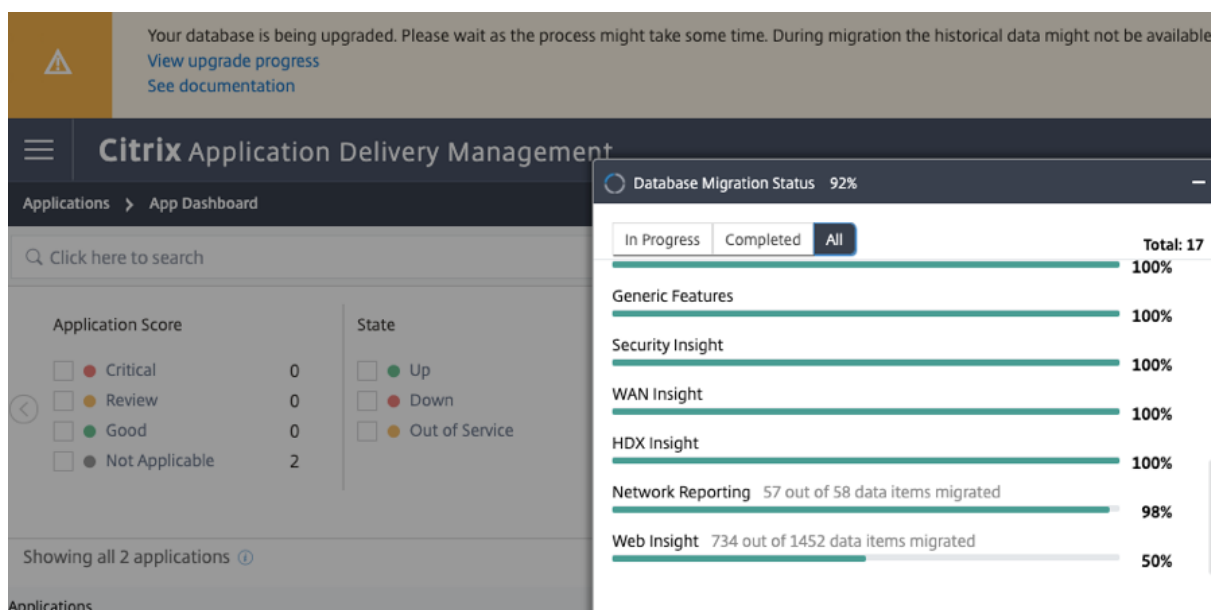
- [OK] をクリックします。  
[確認] ダイアログボックスが表示されます。[はい] をクリックします。  
アップグレードプロセスが開始されます。

設定を移行したら、ADM GUI にログオンできます。ログオンすると、履歴データはバックグラウンドで移行を開始しますが、ADM で作業を続行できます。



履歴データの移行中に、古いデータの一部が使用できない場合があります。データベースの移行にかかる時間は、データのサイズとテーブル数によって異なります。

ADM GUI を使用してデータベースの移行を監視できます。[アップグレードの進行状況の表示] をクリックすると、[データベース移行ステータス] が表示されます。



## データベース移行に関する問題のトラブルシューティング

13.0 67.xx 以降へのアップグレードプロセス中に、Web Insight 履歴データの移行が滞っているように見えることがあります。このような場合、データ移行の詳細を確認するには、次の手順を実行します。

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

```

1      cat /var/mps/log/db_upgrade/web_insight_mapping_migration_status
2
3      <!--NeedCopy-->
    
```

出力の例を次に示します

```
1 bash-3.2# cat /var/mps/log/db_upgrade/  
    web_insight_mapping_migration_status  
2 Tue Oct 6 07:41:55 GMT 2020  
3 157 out of 127346 done in 54 seconds  
4 File  
5 /var/mps/db_upgrade/hist_table_mig_data/Web_Insight/  
    af_app_client_server_resp_second_l3p_d7_dump  
6 bash-3.2#  
7  
8 <!--NeedCopy-->
```

この例では、`af_app_client_server_resp_second_l3p_d7` はアップグレード中のエントリです。また、127,346 のうち 157 エントリが 54 秒で移行されます。

## 12.1 リリースから 13.0 リリースへの高可用性ペアのアップグレード

高可用性モードの NetScaler ADM サーバーの場合、アクティブノードまたはフローティング IP アドレスにアクセスしてアップグレードできます。いずれかのサーバーでアップグレードプロセスを開始すると、両方の NetScaler ADM サーバーが自動的に最新のビルドにアップグレードされます。

### 注

12.0 以前のリリースから高可用性ペアをアップグレードする場合は、「[NetScaler ADM 12.1 のアップグレード](#)」を参照してください。

## NetScaler ADM ディザスタリカバリ展開のアップグレード

NetScaler ADM ディザスタリカバリ展開のアップグレードは、次の 2 ステップのプロセスです。

- プライマリサイトの高可用性モードで構成された NetScaler ADM ノードをアップグレードします。後で災害復旧ノードをアップグレードする必要があります。
- 障害復旧ノードをアップグレードする前に、高可用性で展開されている NetScaler ADM サーバーをアップグレードしていることを確認してください。

## NetScaler ADM 障害回復ノードをアップグレードする

1. Citrix ダウンロードサイトから NetScaler ADM アップグレードイメージファイルをダウンロードします。
2. `nsrecover` 認証情報を使用して、このファイルをディザスタリカバリノードにアップロードします。
3. `nsrecover` 認証情報を使用してディザスタリカバリノードにログインします。

4. イメージファイルを配置したフォルダに移動し、ファイルを解凍します。

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Wed May 15 05:27:10 2019 from 10.252.241.103
bash-3.2# cd /var/mps/mps_images
bash-3.2# tar xvfz build-mas-13.0-36.25.tgz
```

5. 次のスクリプトを実行します。

```
./installmas
```

```
bash-3.2# ./installmas
```

オンプレミスエージェントをマルチサイト展開用にアップグレードする

NetScaler ADM エージェント展開のアップグレードは3段階のプロセスです。

オンプレミスエージェントをアップグレードする前に、次のタスクを完了していることを確認してください。

1. 高可用性で展開されている NetScaler ADM サーバーをアップグレードします。
2. NetScaler ADM 障害回復ノードをアップグレードします。

詳しくは、「NetScaler ADM ディザスタリカバリ展開のアップグレード」を参照してください。

オンプレミスエージェントのアップグレード

1. Citrix ダウンロードサイトから NetScaler ADM エージェントのアップグレードイメージファイルをダウンロードします。
2. `nsrecover` 認証情報を使用して、このファイルをエージェントノードにアップロードします。
3. 正しいエージェントアップグレードイメージをダウンロードしてください。次に、画像ファイル名形式の例を示します。

```
build-masagent-13.0-48.18.tgz
```

4. `nsrecover` 資格情報を使用してオンプレミスエージェントにログオンします。
5. イメージファイルを配置したフォルダに移動し、ファイルを解凍します。

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 30 08:50:48 2018 from 10.252.241.37
bash-3.2# cd /var/mps/mps_images/
bash-3.2# tar zxvf build-masagent-12.1-502.109.tgz
```

6. 次のスクリプトを実行します。

```
./installmasagent
```

```
bash-3.2# ./installmasagent
```

## NetScaler ADM サーバーにディスクを追加する

NetScaler ADM ストレージ要件がデフォルトのディスク容量 (120 GB) を超える場合は、追加のディスクを接続できます。単一サーバーおよび高可用性環境の両方で、より多くのディスクを接続できます。

NetScaler ADM をリリースバージョン 12.1~13.0 からアップグレードしても、以前のバージョンの追加ディスクに作成したパーティションは変わりません。パーティションは削除されず、サイズも変更されません。

ディスクを追加する手順は、アップグレードしたビルドでも変わりません。NetScaler ADM の新しいディスクパーティション作成ツールを使用して、新しく追加したディスクにパーティションを作成できるようになりました。このツールを使用して、既存のより多くのディスク内のパーティションのサイズを変更することもできます。[追加のディスクを接続する方法と新しいディスクパーティション分割ツールを使用する方法](#)について詳しくは、「[NetScaler ADM に追加のディスクを接続する方法](#)」を参照してください。

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

NetScaler ADM 12.1 ビルド 49.23 以降、OpenStack オーケストレーションワークフローのアーキテクチャが更新されました。ワークフローでは、NetScaler ADM StyleBook を使用して NetScaler ADC インスタンスを構成できるようになりました。バージョン 12.0 または 12.1 ビルド 48.18 から NetScaler ADM 13.0 にアップグレードする場合は、次の移行スクリプトを実行する必要があります。

```
1 /mps/scripts/migration_scripts/migrate_configurations.py
2 <!--NeedCopy-->
```

os-cs-lb-mon StyleBook と移行スクリプトについて詳しくは、「[StyleBook を使用した OpenStack での NetScaler ADC VPX インスタンスのプロビジョニング](#)」を参照してください。

## 認証

February 6, 2024

ユーザーは、Citrix ADM による内部認証、認証サーバーによる外部認証、またはその両方で認証できます。ローカル認証を使用する場合、ユーザーは NetScaler ADM セキュリティデータベースに存在する必要があります。ユーザーが外部で認証される場合、選択した認証プロトコルに応じて、ユーザーの「外部名」が認証サーバーに登録されている外部ユーザー ID と一致する必要があります。



NetScaler ADM は、RADIUS、LDAP、および TACACS サーバーによる外部認証をサポートしています。この統合サポートは、システムにアクセスしているすべてのローカルおよび外部の認証、認可、およびアカウントिंगサーバユーザを認証および認可するための共通のインターフェイスを提供します。NetScaler ADM では、システムとの通信に使用する実際のプロトコルに関係なく、ユーザーを認証できます。外部認証用に構成された Citrix ADM 実装にユーザーがアクセスしようとする、要求されたアプリケーションサーバーは、認証のためにユーザー名とパスワードを RADIUS、LDAP、または TACACS サーバーに送信します。認証が成功すると、ユーザーには Citrix ADM へのアクセス権が付与されます。

#### 外部認証サーバ

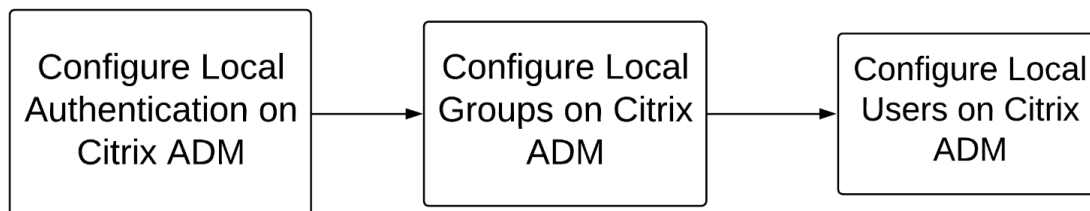
NetScaler ADM は、すべての認証、承認、および監査サービス要求をリモート RADIUS、LDAP、または TACACS サーバーに送信します。リモート認証、承認、および監査サーバーは、要求を受信し、要求を検証し、NetScaler ADM に応答を送信します。認証にリモート RADIUS、TACACS、または LDAP サーバーを使用するように構成すると、NetScaler ADM は RADIUS、TACACS、または LDAP クライアントになります。これらのいずれの構成でも、認証記録はリモートホストサーバーのデータベースに格納されます。アカウント名、割り当てられたアクセス許可、および時間アカウントングレコードは、各ユーザーの認証、承認、および監査サーバーにも格納されます。

また、NetScaler ADM の内部データベースを使用して、ユーザーをローカルで認証することもできます。ユーザーとそのパスワード、およびデフォルトの役割のエントリをデータベースに作成します。特定のタイプの認証の認証順序を選択することもできます。サーバーグループ内のサーバーの一覧は、順番付きの一覧です。一覧の 1 番目のサーバーが使用できる場合は常にこのサーバーが使用され、使用できない場合は一覧の 2 番目のサーバーが使用されます。認証サーバ、認可、監査サーバの設定済みリストへのフォールバック認証バックアップとして、内部データベースを含めるようにサーバを設定できます。

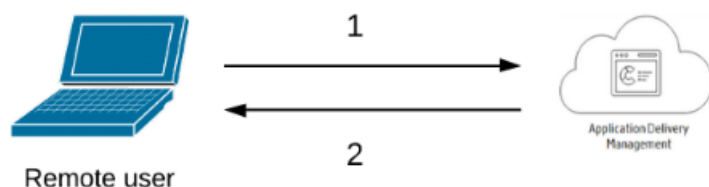
#### NetScaler ADM でユーザーを認証する

NetScaler ADM でユーザーを認証するには、次の 2 つの方法があります。

- Citrix ADM で構成されたローカルユーザー



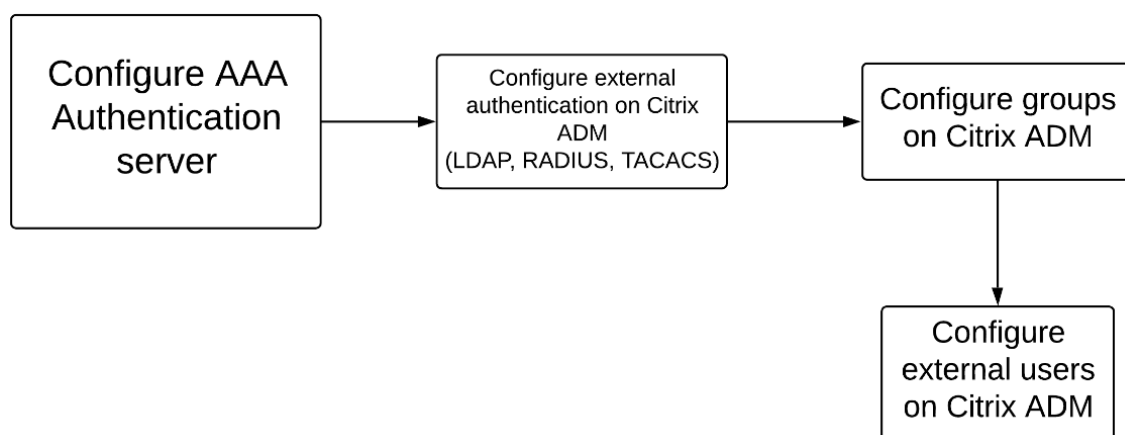
設定後、ローカルサーバでのユーザー認証のワークフローを次に示します。



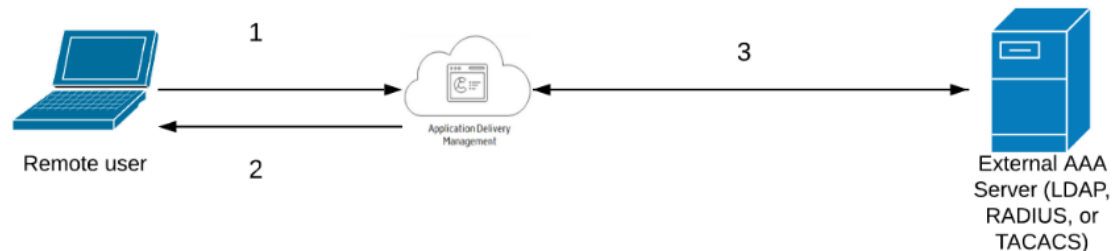
**1**—ユーザーは Citrix ADM にログオンします

**2**—Citrix ADM は、ユーザーに認証用の資格情報の入力を促し、資格情報が ADM データベースで一致するかどうかを確認します。

- 外部認証サーバーの使用



構成後、外部認証、承認、および監査サーバーでのユーザー認証のワークフローを次に示します。



**1**—ユーザーは Citrix ADM に接続します

**2**—NetScaler ADM がユーザーに資格情報の入力を求めます

**3** -NetScaler ADM は、外部認証、承認、および監査サーバーを使用してユーザーの資格情報を検証します。検証が成功すると、ユーザーは引き続きログオンできます。

## NetScaler ADM で外部認証サーバーを構成する

February 6, 2024

LDAP、RADIUS、または TACACS サーバーを構成したら、これらのサーバーを NetScaler ADM に追加できます。

### LDAP 認証サーバーの追加

February 6, 2024

LDAP プロトコルを RADIUS および TACAS 認証サーバと統合すると、ADM を使用して、分散ディレクトリからユーザーレディンシャルを検索および認証できます。

1. [システム] > [認証] に移動します。
2. [LDAP] タブを選択し、[追加] をクリックします。
3. 「LDAP サーバーの作成」 ページで、次のパラメータを指定します。
  - a) 名前—LDAP サーバー名を指定します。
  - b) サーバー名/IP アドレス—LDAP IP アドレスまたはサーバー名を指定します。
  - c) セキュリティタイプ—システムと LDAP サーバー間で必要な通信のタイプ。一覧から選択します。プレーンテキスト通信が不十分な場合は、トランスポート層セキュリティ (TLS) または SSL を選択して暗号化通信を選択できます。
  - d) ポート—デフォルトでは、ポート 389 が PLAINTEXT に使用されます。SSL/TLS にはポート 636 を指定することもできます。
  - e) サーバーの種類—LDAP サーバーの種類として Active Directory (AD) または NDS (ノベルディレクトリサービス) を選択します。
  - f) タイムアウト (秒) —Citrix ADM システムが LDAP サーバーからの応答を待つ時間 (秒単位)
  - g) LDAP ホスト名—「LDAP 証明書の検証」 チェックボックスを選択し、証明書に入力するホスト名を指定します。

[認証] オプションをオフにして、SSH 公開キーを指定します。キーベースの認証では、LDAP サーバーのユーザーオブジェクトに保存されている公開鍵のリストを SSH 経由で取得できるようになりました。

[接続設定] で、次のパラメータを指定します。

- i. ベース **DN**—検索を開始する LDAP サーバーのベースノード
- ii. 管理者バインド **DN**—LDAP サーバーにバインドするユーザー名。たとえば、admin@aaa.local。
- iii. バインド **DN** パスワード—認証用のパスワードを入力するには、このオプションを選択します
- iv. パスワードの変更を有効にする—パスワードの変更を有効にするには、このオプションを選択します

[その他の設定] で、次のパラメータを指定します。

- i. サーバーログオン名属性—システムが外部 LDAP サーバーまたは Active Directory にクエリを実行するために使用する名前属性。リストから **samAccountname** を選択します。
- ii. 「検索フィルタ」—LDAP サーバーで構成された検索フィルタに従って、2 要素認証用に外部ユーザーを設定します。たとえば、ldaploginame samaccount を指定した vpnallowed=true、ユーザーが指定したユーザー名 bob を指定すると、LDAP 検索文字列が返されます: &(vpnallowed=true)(samaccount=bob)。

注

デフォルトでは、検索フィルタの値は角かっこで囲まれています。

- iii. 「グループ属性」—リストから「MemberOf」を選択します。
- iv. サブ属性名—LDAP サーバーからグループを抽出するためのサブ属性名。
- v. デフォルト認証グループ—抽出されたグループに加えて、認証が成功したときに選択されるデフォルトグループ。

4. [作成] をクリックします。

LDAP サーバーが設定されました。

### 注

ユーザーが Active Directory グループメンバーである場合、NetScaler ADM 上のグループとユーザーの名前は、同じ Active Directory グループメンバーの名前である必要があります。

## RADIUS 認証サーバーの追加

February 6, 2024

1. [システム] > [認証] に移動します。
2. [RADIUS] タブを選択し、[追加] をクリックします。

「RADIUS サーバーの作成」ページで、次のパラメータを指定します。

- a) 名前—RADIUS サーバー名を指定します。
- b) サーバー名/IP アドレス—RADIUS サーバーの IP アドレスを指定します
- c) ポート—RADIUS サーバがホストされているポート番号を指定します。既定のポートは 1812 です。
- d) タイムアウト (秒) —Citrix ADM システムが RADIUS サーバーからの応答を待つ時間 (秒単位)
- e) シークレットキー—認証用の RADIUS シークレットキーを指定します。
- f) シークレットキーの確認—確認のため、キーをもう一度指定してください

## ← Create RADIUS Server

|                           |                                             |
|---------------------------|---------------------------------------------|
| Name*                     | <input type="text" value="RADIUS for ADM"/> |
| Server Name / IP Address* | <input type="text" value="10.102.29.394"/>  |
| Port*                     | <input type="text" value="1812"/>           |
| Time-out (seconds)*       | <input type="text" value="3"/>              |
| Secret Key*               | <input type="password" value="•••••"/>      |
| Confirm Secret Key*       | <input type="password" value="•••••"/> ⓘ    |

「詳細」で、次のパラメータを指定します。

- i. **NAS ID** – 識別子を RADIUS サーバに送信する ID を指定します
- ii. **グループベンダー ID** – RADIUS グループ抽出を使用するベンダー ID を指定します
- iii. **グループプレフィックス** -RADIUS グループ抽出用の RADIUS 属性内のグループ名の前に置く文字列
- iv. **グループ属性タイプ**–RADIUS グループ抽出の属性タイプを指定します
- v. **グループセパレーター**–RADIUS グループ抽出用の RADIUS 属性内のグループ名を区切る文字列
- vi. **IP アドレスベンダー識別子**–RADIUS のベンダー ID はイントラネット IP を示します。値が 0 の場合、属性がベンダーでエンコードされていないことを示します。
- vii. **パスワードベンダー識別子**–ユーザーパスワードを抽出するための RADIUS 応答内のベンダー ID パスワード
- viii. **IP アドレス属性タイプ**–RADIUS が応答するリモート IP アドレス属性
- ix. **パスワード属性タイプ**: RADIUS が応答するためのパスワード属性
- x. **パスワードエンコーディング**–リストから pap、chap、mschapv1、または mschapv2 を選択します。これは、システムから RADIUS サーバに送信される RADIUS パケットでパスワードをエンコードする方法を示しています。

- xi. デフォルト認証グループ抽出されたグループに加えて認証が成功したときに選択されるデフォルトグループ

アプライアンスに監査情報を RADIUS サーバに記録させたい場合は、「アカウントティング」を選択します。

3. [作成] をクリックします。

これで、RADIUS サーバが設定されました。

## TACACS 認証サーバーの追加

February 6, 2024

1. [システム] > [認証] に移動します。
2. [TACACS] タブを選択し、[追加] をクリックします。
3. TACACS の作成ページで、次のパラメータを指定します。

- a) 名前—TACACS サーバ名を指定します。
- b) IP アドレス—TACACS の IP アドレスを指定します。
- c) ポート—TACACS サーバがホストされているポート番号を指定します。デフォルトポートは 49 です
- d) タイムアウト (秒) —Citrix ADM システムが LDAP サーバからの応答を待つ時間 (秒単位)
- e) TACACS キー—認証用の TACACS キーを指定します
- f) TACACS キーの確認—確認のため、TACACS キーをもう一度指定してください
- g) グループ属性名—グループ名を指定します。

アプライアンスに監査情報を TACACS サーバに記録させたい場合は、「アカウントティング」を選択します。

4. [作成] をクリックします。

## ← Create TACACS Server

|                                                  |                                                    |
|--------------------------------------------------|----------------------------------------------------|
| Name*                                            | <input type="text" value="TACACS for ADM"/>        |
| IP Address*                                      | <input type="text" value="10 . 102 . 29 . 216"/> ⓘ |
| Port*                                            | <input type="text" value="49"/>                    |
| Time-out (seconds)*                              | <input type="text" value="3"/>                     |
| TACACS Key*                                      | <input type="password" value="•••••"/> ⓘ           |
| Confirm TACACS Key*                              | <input type="password" value="•••••"/>             |
| Group Attribute Name                             | <input type="text" value="defaultgroup"/>          |
| <input checked="" type="checkbox"/> Accounting ⓘ |                                                    |

### NetScaler ADM ユーザー

February 6, 2024

NetScaler ADM でローカルにユーザーアカウントを作成して、認証サーバーのユーザーを補完することができます。たとえば、社外のコンサルタントや来訪者などの一時的なユーザー用のアカウントを、認証サーバー上ではなく Access Gateway 上にローカルに作成します。

ユーザーの構成について詳しくは、「[ユーザーの構成](#)」を参照してください。



注

ユーザーが Active Directory を使用している場合は、Citrix ADM のグループ名が外部サーバーの Active Directory グループのグループ名と同じであることを確認してください。

### Citrix ADM のユーザーグループ

NetScaler ADM では、グループを作成してユーザーをグループに追加することで、ユーザーを認証および承認できます。グループには「管理者」または「読み取り専用」の権限があり、そのグループのすべてのユーザーに同じ権限が与えられます。

Citrix ADM の場合:

- グループは、同様の権限を持つユーザーの集まりとして定義されます
- グループには 1 つまたは複数の役割を設定できます。
- ユーザーは、割り当てられた権限に基づいてアクセスできるエンティティとして定義されます。
- ユーザーは 1 つ以上のグループに所属できます。

NetScaler ADM でローカルグループを作成し、グループ内のユーザーに対してローカル認証を使用できます。認証に外部サーバーを使用している場合は、内部ネットワークの認証サーバーで構成されたグループと一致するように Citrix ADM 上のグループを構成します。ユーザーがログオンして認証されると、グループ名が認証サーバー上のグループと一致すると、ユーザーは NetScaler ADM でそのグループの設定を継承します。

ローカル認証を使用している場合は、ユーザーを作成し、Citrix ADM で構成されたグループに追加します。ユーザーはこれらのグループの設定を継承します。

グループの設定とグループ権限の割り当てについては、「[グループの構成](#)」を参照してください。

### 認証サーバーグループの抽出

February 6, 2024

注

TACACS サーバーの抽出は **Citrix ADM13.0** でサポートされています。

Citrix ADM を使用すると、次のことが可能になります。

- 外部認証サーバーでユーザーが所属するグループのリストを抽出します。
- 外部サーバで設定されたグループと一致するグループ設定に、これらのグループを割り当てます。

利点:

- 外部サーバーで管理されるため、NetScaler ADM でユーザーを作成する必要はありません。
- NetScaler ADM は、特定のロードバランサー仮想サーバーおよびシステム上の特定のアプリケーションにアクセスするためのグループ権限を割り当てることによって、ユーザーの認証を実行します。

### フォールバックおよび外部認証サーバーのカスケードを有効にする

February 6, 2024

フォールバックオプションを使用すると、外部サーバーの認証が失敗した場合にローカル認証を引き継ぐことができます。Citrix ADM と外部認証サーバーの両方で構成されたユーザーは、構成済みの外部認証サーバーがダウンしているか、アクセスできない場合でも、Citrix ADM にログオンできます。フォールバック認証を確実に機能させるには:

- 外部サーバーがダウンしているかアクセスできない場合、NSroot 以外のユーザーは Citrix ADM にアクセスできる必要があります
- 少なくとも 1 つの外部サーバーを追加する必要があります

Citrix ADM は、ローカル認証に加えて、認証、承認、アカウントिंग (AAA) プロトコル (LDAP、RADIUS、TACACS) の統合システムもサポートしています。この統合サポートにより、システムにアクセスするすべてのユーザーと外部 AAA クライアントを認証および承認するための共通インターフェイスが提供されます。

NetScaler ADM は、システムと通信する実際のプロトコルに関係なく、ユーザーを認証できます。

外部認証サーバーをカスケードすることにより、外部ユーザーの認証と承認において、エラーのない継続的なプロセスを実現します。最初の認証サーバーで認証が失敗した場合、NetScaler ADM は 2 番目の外部認証サーバーを使用してユーザーを認証しようとします。カスケード認証を有効にするには、Citrix ADM に外部認証サーバーを追加する必要があります。サポートされている外部認証サーバー (RADIUS、LDAP、TACACS) であれば、いずれの種類でも追加できます。

たとえば、4 つの外部認証サーバを追加し、2 つの RADIUS サーバ、1 つの LDAP サーバ、1 つの TACACS サーバを設定とします。Citrix ADM は、構成に基づいて外部サーバーとの認証を試みます。このシナリオ例では、Citrix ADM は次のことを試みます。

- 最初の RADIUS サーバに接続
- 1 台目の RADIUS サーバで認証に失敗した場合は、2 番目の RADIUS サーバに接続する
- 両方の RADIUS サーバで認証に失敗した場合は、LDAP サーバに接続する
- RADIUS サーバと LDAP サーバの両方で認証に失敗した場合は、TACACS サーバに接続します。

注

NetScaler ADM では、最大 32 台の外部認証サーバーを構成できます。

#### フォールバックと外部サーバーのカスケード構成

1. [システム] > [認証] に移動します。
2. [認証] ページで、[設定] をクリックします。
3. 「認証設定」 ページで、「サーバータイプ」 リストから「**EXTERNAL**」を選択します (カスケード接続できるのは外部サーバーのみです)。
4. 「挿入」 をクリックし、「外部サーバー」 ページで、カスケードする認証サーバーを 1 つまたは複数選択します。
5. 外部認証が失敗した場合にローカル認証を引き継ぐようにするには、「フォールバックローカル認証を有効にする」 チェックボックスを選択します。
6. 外部ユーザーグループ情報をシステム監査ログに取り込む場合は、「外部グループ情報を記録する」 チェックボックスを選択します。
7. [OK] をクリックしてページを閉じます。

選択したサーバーが [外部サーバー] に表示されます。

## ← Authentication Configuration

The appliance can authenticate users with local user accounts or by using an external authentication server.

Server Type\*

EXTERNAL

External Servers

| <input type="checkbox"/>            | Server Type | Server Name |
|-------------------------------------|-------------|-------------|
| <input checked="" type="checkbox"/> | RADIUS      | RADIUS R1   |
| <input checked="" type="checkbox"/> | RADIUS      | RADIUS R2   |

Enable fallback local authentication

サーバー名の横にあるアイコンを操作し、サーバーを一覧中で上下に移動して、認証の順番を指定することもできます。

## アクセス制御

February 6, 2024

認証とは、利用者が本人であることを確認するプロセスです。認証を行うには、認証メカニズムによる問い合わせが可能なアカウントがシステム内で既に作成されているか、最初の認証プロセスの一部としてアカウントが作成されている必要があります。NetScaler Application Delivery Management (ADM) は、ローカルユーザーと外部ユーザーの両方を認証する方法を提供します。ローカルユーザーは内部で認証されますが、Citrix ADM は RADIUS、LDAP、および TACACS プロトコルによる外部認証をサポートします。外部認証用に構成された NetScaler ADM にユーザーがアクセスしようとする、要求されたアプリケーションサーバーは認証のために RADIUS、LDAP、または TACACS サーバーにユーザー名とパスワードを送信します。認証されると、必要なプロトコルを使用して Citrix ADM 上のユーザーを識別します。

アクセス制御とは、特定のリソースに対して必要なセキュリティを適用するプロセスです。このセキュリティ技術は、コンピューターのシステム環境でリソースを表示または使用できるユーザーを制限するために使用できます。アクセス制御は、コンピューターシステムの正規ユーザーが実行できるアクションや操作を制限することを目的とします。アクセス制御は、ユーザーが直接実行できる操作と、ユーザーの代わりに実行できるプログラムを制限します。このようにアクセス制御は、セキュリティ違反につながる可能性のあるアクティビティを防止しようとしています。アクセス制御では、参照モニターを通じてアクセス制御が適用される前に、ユーザー認証が正常に検証されていることが前提になっています。Citrix ADM では、きめ細かな役割ベースのアクセス制御 (RBAC) が可能であり、管理者は企業内の個々のユーザーの役割に基づいてユーザーにアクセス権限を与えることができます。Citrix ADM の RBAC は、アクセスポリシー、ロール、グループ、およびユーザーを作成することによって実現されます。

## 役割ベースのアクセス制御

February 6, 2024

Citrix ADM には、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、きめ細かな役割ベースのアクセス制御 (RBAC) が用意されています。ここでは、アクセスとはファイルの表示、作成、変更、削除などの特定のタスクを実行する能力のことです。役割は、社内でのユーザーの権限と責任に従って定義されます。たとえば、1人のユーザーがすべてのネットワーク操作の実行を許可し、別のユーザーがアプリケーションのトラフィックフローを監視し、設定テンプレートの作成を支援することができます。

役割はポリシーで決定されます。ポリシーを作成した後に役割を作成し、各役割を 1 つまたは複数のポリシーにバインドし、役割をユーザーに割り当てます。役割は、ユーザーのグループに割り当ててもできます。

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複数のユーザーを 1 つのグループに割り当てることができます。ロールは、特定の条件に基づいてユーザーまたはグループに付与される ID です。NetScaler ADM では、役割とポリシーの作成は NetScaler ADC RBAC 機能に固有です。役割

とポリシーは、企業のニーズが進展するにつれて簡単に作成、変更、または終了できます。各ユーザーの権限を個別に更新する必要はありません。

役割は機能ベースまたはリソースベースにすることができます。たとえば、SSL/セキュリティ管理者とアプリケーション管理者を考えてみましょう。SSL/セキュリティ管理者は、SSL 証明書の管理および監視機能への完全なアクセス権を持ってい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、スコープ内のリソースにのみアクセスできる必要があります。

例:

ADC グループ長であるクリスは、組織内の NetScaler ADM スーパー管理者です。Chris 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の David は、SSL 証明書の管理と監視のための完全なアクセス権を持っているだけでなく、システム管理操作のための読み取り専用アクセス権を持っている必要があります。

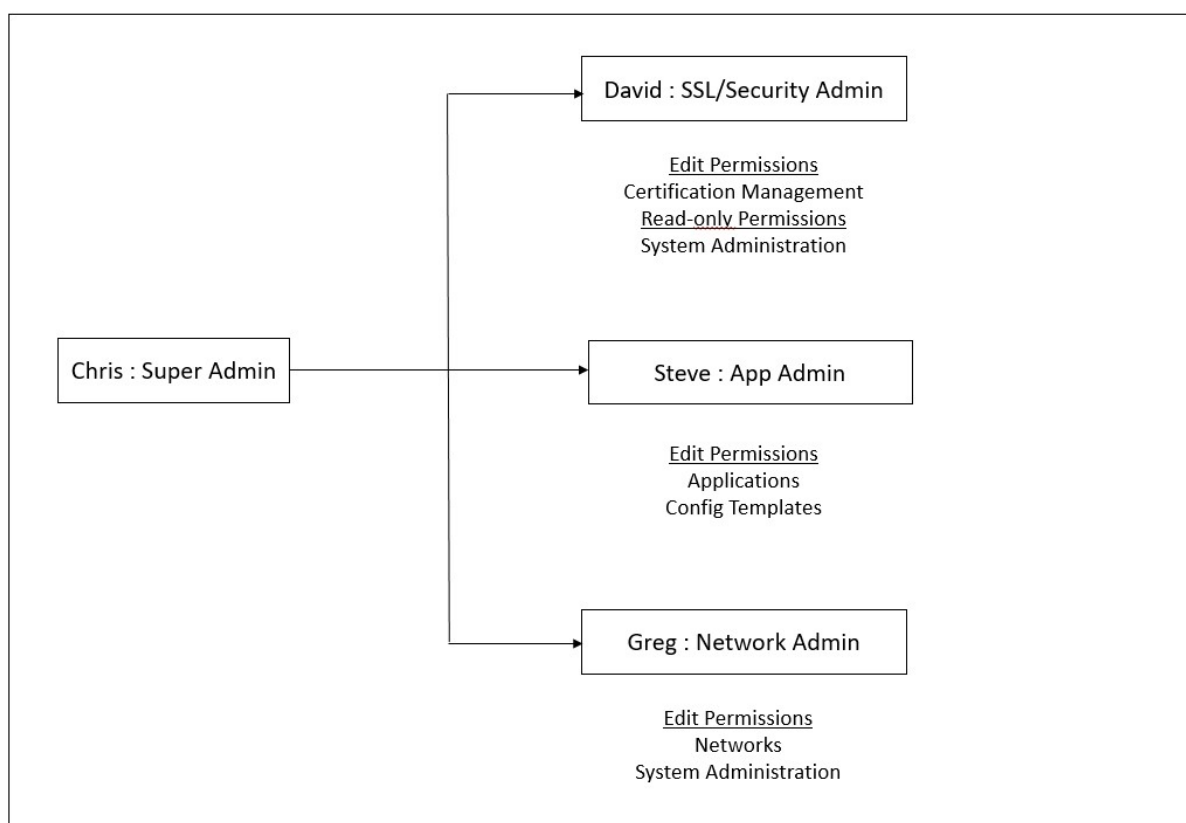
アプリケーション管理者のスティーブは、特定のアプリケーションと特定の構成テンプレートのみへのアクセスが必要です。

ネットワーク管理者のグレッグは、システムとネットワーク管理へのアクセスが必要です。

また、Chris は、ローカルまたは外部であるかどうかにかかわらず、すべてのユーザーに対して RBAC を提供する必要があります。

NetScaler ADM ユーザーは、ローカルで認証することも、外部サーバー (RADIUS/LDAP/TACACS) を使用して認証することもできます。RBAC 設定は、採用される認証方法に関わらずすべてのユーザーに適用可能でなければなりません。

下図に、各種の管理者とほかのユーザーが持つ権限と社内での役割を示します。



### 制限事項

RBAC は、以下の Citrix ADM 機能については完全にはサポートされていません。

- **Analytics** -RBAC は、分析モジュールでは完全にサポートされていません。RBAC のサポートはインスタンスレベルに限定されており、Web Insight、SSL Insight、Gateway Insight、HDX Insight、および Security Insight の分析モジュールのアプリケーションレベルには適用できません。たとえば、以下のようなものです。

#### 例 1: インスタンスベースの RBAC (サポート)

RBAC はインスタンスレベルでサポートされているため、いくつかのインスタンスを割り当てられた管理者は、**Web Insight >Instance** でそれらのインスタンスのみを表示でき \*\*、\*\***Web Insight > Applications** で対応する仮想サーバーのみを見ることができます。

#### 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ている管理者は、[ **Web Insight** ] > [アプリケーション] ですべての仮想サーバーを表示できますが、**RBAC** はアプリケーションレベルではサポートされていないため、アクセスできません。

- **StyleBook** –RBAC は StyleBook では完全にはサポートされていません。

- NetScaler ADM では、StyleBooks と構成パックは別個のリソースとみなされます。StyleBook と構成パックには、表示、編集、またはその両方のアクセス権を、別々に、または同時に提供することができます。構成パックに対する表示権限または編集権限により、ユーザーは StyleBooks を暗黙的に表示できます。これは、構成パックの詳細を取得したり、構成パックを作成したりするのに不可欠です。
  - 特定の StyleBook または構成パックに対するアクセス権がサポートされていない  
例: インスタンスに構成パックがすでに存在する場合、ユーザーは対象の NetScaler ADC インスタンスへのアクセス権がない場合でも、ターゲット NetScaler ADC インスタンスの構成を変更できます。
- オーケストレーション-RBAC はオーケストレーションではサポートされていません。

## アクセスポリシーの構成

February 6, 2024

アクセスポリシーでは、権限が定義されます。ポリシーは、1人のユーザーや1つのグループ、または複数のユーザーやグループに適用できます。Citrix Application Delivery Management (ADM) には、4つの定義済みアクセスポリシーがあります。

1. 管理ポリシー。Citrix ADM のすべての機能へのアクセスを許可します。ユーザーには表示権限と編集権限があり、すべての NetScaler ADM コンテンツを表示でき、すべての編集操作を実行できます。つまり、ユーザーはリソースに対して追加、変更、削除の操作を実行できます。
2. 読み取り専用ポリシー。読み取り専用権限を付与します。ユーザーは Citrix ADM のすべてのコンテンツを表示できますが、操作を実行する権限はありません。
3. アプリ管理ポリシー。NetScaler ADM 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ているユーザーは、カスタムアプリケーションを追加、変更、削除できるほか、サービス、サービスグループ、および各種仮想サーバー（コンテンツスイッチ、キャッシュリダイレクト、および HAProxy 仮想サーバーなど）を有効または無効にできます。
4. アプリ読み取り専用ポリシー。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ている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、および無効化の操作は実行できません。

注: 定義済みのポリシーは編集できません。

また、ユーザーは独自の（ユーザー定義の）ポリシーを作成できます。

ユーザー定義のアクセスポリシーを作成するには、次の手順を実行します。

1. Citrix ADM で、[システム] > [ユーザー管理] > [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. 「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。

[アクセス許可] セクションには、NetScaler ADM のすべての機能が一覧表示され、読み取り専用、有効/無効化、または編集アクセス権を指定するためのオプションが表示されます。

4. [+] アイコンをクリックして、各機能グループを複数の機能に展開します。

a) 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:** このオプションにより、ユーザーは NetScaler ADM で機能を表示できます。
- **有効化/無効化:** このオプションは、NetScaler ADM での操作を有効または無効にするネットワーク機能でのみ使用できます。ユーザーは、この機能を有効または無効にすることができます。また、ユーザーは「今すぐ投票」アクションを実行することもできます。

ユーザーに「有効/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フルアクセスを許可します。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 を展開すると、より多くの設定オプションが表示されます。

次の図では、負荷分散機能の構成オプションに異なる権限があります:



Permissions

- All
  - Applications
  - Networks
    - Infrastructure Analytics
    - Instances Dashboard
    - Network Functions
      - Load Balancing
        - Virtual Servers
          - View  Enable - Disable  Edit
        - Services
          - View  Enable - Disable  Edit
        - Service Groups
          - View  Enable - Disable  Edit
        - Servers
      - Content Switching
      - Cache Redirection
      - Authentication
      - GSLB
        - Virtual Server
          - View  Enable - Disable  Edit
        - Services
        - Domains
        - Service Groups
      - HAProxy
      - Citrix Gateway
      - Auditing
      - Settings
    - Instances
    - Autoscale Groups
    - Sites and IP Blocks
    - Instance Groups
    - Agents
    - License Management
    - Events
    - Certificate Management
    - Configuration
    - Configuration Audit
    - Domain Names
    - Network Reporting
    - API
  - Analytics
  - Orchestration
  - System

仮想サーバ機能に対する表示権限は、ユーザーに付与されます。ユーザーは、NetScaler ADM で負荷分散仮想サーバーを表示できます。仮想サーバーを表示するには、[ネットワーク]>[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。

サービス機能の有効化/無効化権限は、ユーザーに付与されます。この権限は閲覧権限も付与します。ユーザーは、負荷分散仮想サーバーにバインドされたサービスを有効または無効にすることができます。また、ユーザーはサービスに対して [ **Poll Now** ] 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、[ネットワーク]>[\*\* 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 **Enable-Disable** アクセス許可を持っている場合、次のページで、サービスの有効化/無効化アクションが制限されます。

- a) [ネットワーク]>[ネットワーク機能]に移動します。
- b) 仮想サーバを選択し、[構成]をクリックします。
- 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。  
このページには、「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の編集権限がユーザーに付与されます。この権限は、\*\* 表示権限と有効化/無効化権限が付与されている場所でのフルアクセスを許可します \*\*。ユーザーは、負荷分散仮想サーバーにバインドされているサービスグループを変更できます。サービスグループを編集するには、[\*\* ネットワーク]>[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。

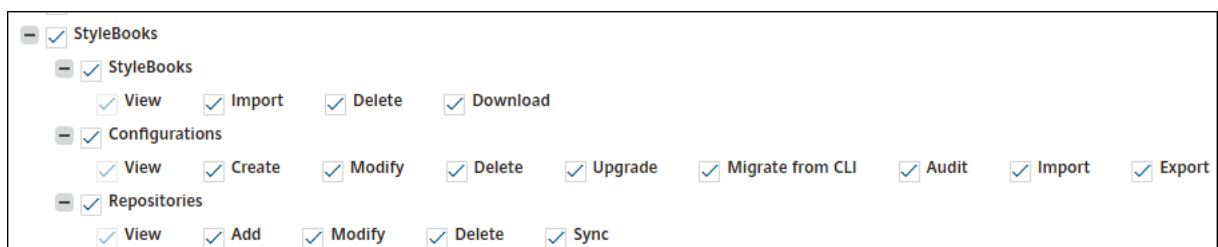
5. [作成] をクリックします。

### ユーザーに **StyleBook** パーミッションを付与する

アクセスポリシーを作成して、StyleBook のインポート、削除、ダウンロードなどの権限を付与できます。

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。



## グループの構成

February 6, 2024

NetScaler ADM では、グループには機能レベルとリソースレベルのアクセス権の両方があります。たとえば、あるユーザーグループは選択した NetScaler ADC インスタンスのみにアクセスし、別のグループには選択した少数のアプリケーションのみにアクセスできるなどです。

グループを作成するときに、グループにロールを割り当てたり、グループへのアプリケーションレベルのアクセスを提供したり、ユーザーをグループに割り当てることができます。NetScaler ADM では、そのグループのすべてのユーザーに、同じアクセス権が割り当てられます。

NetScaler ADM では、ネットワーク機能エンティティの個々のレベルでユーザーアクセスを管理できます。特定の権限をエンティティレベルでユーザーまたはグループに動的に割り当てることができます。

NetScaler ADM は、仮想サーバー、サービス、サービスグループ、およびサーバーをネットワーク機能エンティティとして扱います。

- 仮想サーバー (アプリケーション) -負荷分散 (lb)、GSLB、コンテキストスイッチング (CS)、キャッシュリダイレクト (CR)、認証 (Auth)、Citrix Gateway (VPN)
- サービス -負荷分散と GSLB サービス
- サービスグループ -負荷分散と GSLB サービスグループ
- サーバ -負荷分散サーバ


### ユーザーグループの作成


1. NetScaler ADM で、[システム] > [ユーザー管理] > [グループ] に移動します。
2. [追加] をクリックします。  
「システムグループの作成」ページが表示されます。
3. [グループ名] フィールドに、グループの名前を入力します。
4. 「グループの説明」フィールドに、グループの説明を入力します。グループについてわかりやすい説明をしておくと、後でグループの役割と機能をよりよく理解するのに役立ちます。
5. [ロール] セクションで、1 つ以上のロールを [構成済み] リストに追加または移動します。


注:

[使用可能] ボックスの一覧で、[新規] または [編集] をクリックし、ロールを作成または変更することができます。または、[\*\* システム] > [ユーザー管理] > [ユーザー] に移動し、ユーザーを作成または変更することもできます。 \*\*

## ← Create System Group

 **Group Settings**

 Authorization Settings

 Assign Users

Group Name\*  
 ?

Group Description  
 ?

Roles\*

**Available (3)**  [Select All](#)

|             |   |
|-------------|---|
| appReadOnly | + |
| appAdmin    | + |
| readonly    | + |

New | Edit

**Configured (1)**  [Remove All](#)


|       |   |
|-------|---|
| admin | - |
|-------|---|


Configure User Session Timeout


6. [次へ] をクリックします。「認証設定」タブでは、次のリソースの認証設定を指定できます。

- Autoscale グループ
- インスタンス
- アプリケーション
- 構成テンプレート
- StyleBook
- コンフィグパック
- ドメイン名

## ← Create System Group

 Group Settings

 Authorization Settings

 Assign Users

All AutoScale Groups

All Instances

Choose Applications\*

All Applications
▼

All Configuration templates

All StyleBooks

All Domain Names

Cancel

← Back

Create Group →

ユーザーがアクセスできる特定のリソースをカテゴリから選択したい場合があります。

### Autoscale グループ:

ユーザーが表示または管理できる特定の Autoscale e グループを選択する場合は、次の手順を実行してください。

- a) 「すべての **AutoScale** グループ」チェックボックスをオフにし、「**AutoScale** グループを追加」をクリックします。
- b) リストから必要な Autoscale グループを選択し、「**OK**」をクリックします。

### インスタンス:

ユーザーが表示または管理できる特定のインスタンスを選択するには、次の手順を実行します。

- a) [すべてのインスタンス] チェックボックスをオフにし、[インスタンスを選択] 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。

All Instances

Select Instances

Delete

| ■                        | IP Address    | Name | State |
|--------------------------|---------------|------|-------|
| <input type="checkbox"/> | 10.106.136.53 |      | ● Up  |
| <input type="checkbox"/> | 10.102.102.83 |      | ● Up  |

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アクセス権をユーザーに付与できます。

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。なぜなら、アプリケーションはインスタンスから独立しているため、ユーザーにアクセス権が付与されているからです。

アプリケーションへのアクセスをユーザーに許可すると、そのユーザーは、インスタンスの選択に関係なく、そのアプリケーションにのみアクセスできます。

このリストには次のオプションがあります。

- **すべてのアプリケーション:** このオプションはデフォルトで選択されています。NetScaler ADM に存在するすべてのアプリケーションを追加します。
- **選択したインスタンスのすべてのアプリケーション:** このオプションは、「すべてのインスタンス」カテゴリからインスタンスを選択した場合にのみ表示されます。選択したインスタンスに存在するすべてのアプリケーションを追加します。
- **特定のアプリケーション:** このオプションでは、ユーザーにアクセスさせたい必須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:** このオプションでは、特定のタイプ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。

「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、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が承認されます。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、Citrix ADM は選択したアプリケーションにバインドされているすべてのエンティティを承認します。

注記

バインドされたエンティティを承認する場合は、エンティティタイプを 1 つだけ選択してください。

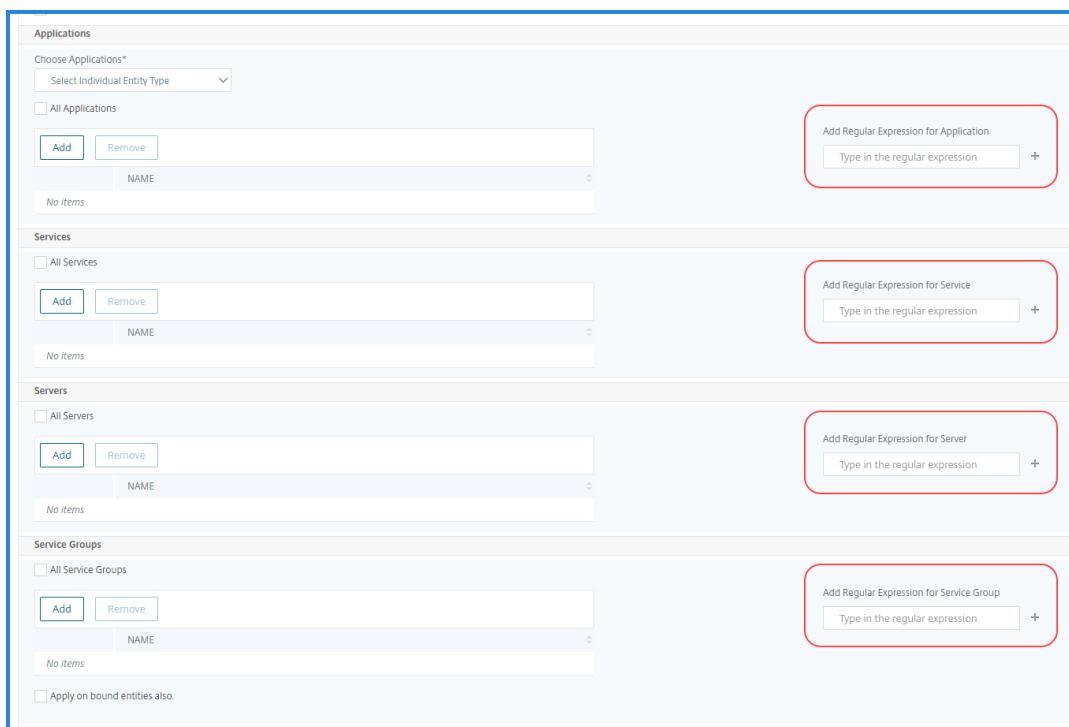
正規表現を使用して、グループの正規表現基準を満たすネットワーク関数エンティティを検索して追加できます。指定された正規表現は NetScaler ADM に保持されます。正規表現を追加するには、次の手順を実行します。

- a) 「正規表現を追加」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。

次の図は、「特定のアプリケーション」オプションを選択した場合に、正規表現を使用してアプリケーションを追加する方法を示しています。



次の図は、[ 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場合に、正規表現を使用してネットワーク関数エンティティを追加する方法を示しています。



正規表現をさらに追加するには、+ アイコンをクリックします。

注:

正規表現は、サーバーエンティティタイプのサーバー名にのみ一致し、サーバーの IP アドレスとは一致しません。

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。

正規表現はシステムに保存され、認証範囲を更新します。新しいエンティティがエンティティタイプの正規表現と一致すると、NetScaler ADM は認証範囲を新しいエンティティに更新します。

設定テンプレート:

ユーザーが表示または管理できる特定の設定テンプレートを選択するには、次の手順を実行します。

- a) [ すべての構成テンプレート] チェックボックスをオフにし、[ 構成テンプレートを追加] をクリックします。

- b) リストから目的のテンプレートを選択し、[ **OK** ] をクリックします。

### StyleBook:

ユーザーが表示または管理できる特定の StyleBook を選択するには、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て、「グループに **StyleBook** を追加」をクリックします。StyleBook を個別に選択することも、フィルタクエリを指定して StyleBook を承認することもできます。

個々の StyleBook を選択する場合は、「個別 StyleBook」ペインから **StyleBook** を選択し、「選択内容の保存」をクリックします。

クエリを使用して StyleBook を検索する場合は、[ カスタムフィルタ ] ペインを選択します。クエリは、**name**、**namespace** および **version** をキーとするキーと値のペアの文字列です。

正規表現を値として使用して、グループの正規表現条件を満たす StyleBook を検索して追加することもできます。StyleBooks を検索するカスタムフィルタクエリは、**And**と**Or**の両方をサポートしています。

例:

```
1 name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
  version=1.0
2 <!--NeedCopy-->
```

このクエリは、次の条件を満たす StyleBook をリストします。

- StyleBook 名は **lb-mon** または **lb** のいずれかです。
- StyleBook の名前空間は **com.citrix.adc.stylebooks** です。
- StyleBook 版は **1.0** です。

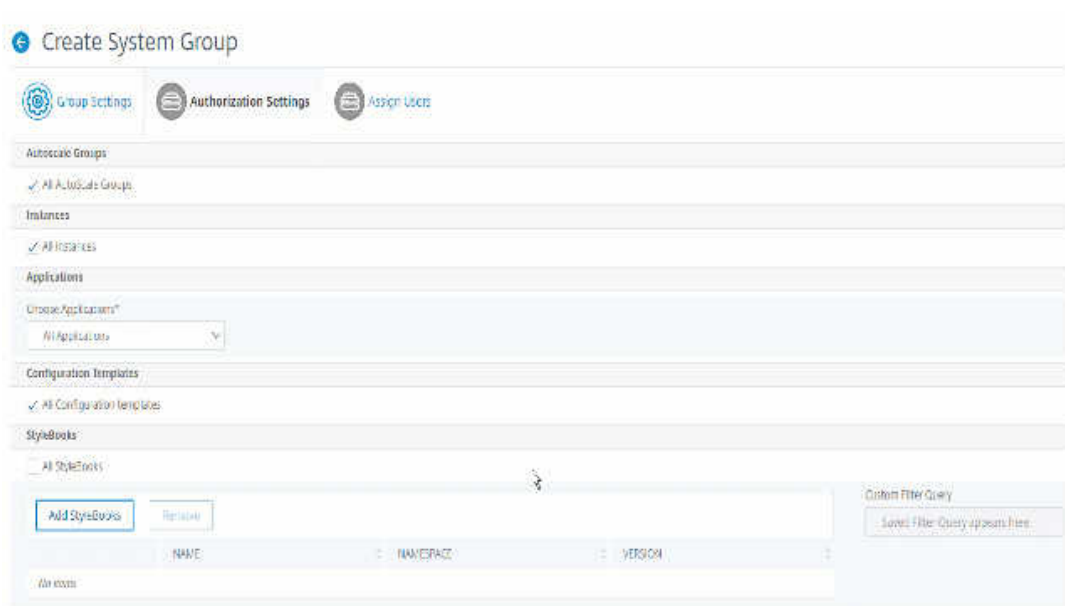
キー式に定義された値式の間で **Or** 演算を使用します。

例:

- **name=lb-mon|lb** クエリは有効です。これは、名前 **lb-mon** または **lb** のいずれかを持つ StyleBooks を返します。
- **name=lb-mon | version=1.0** クエリは無効です。

**Enter** を押して検索結果を表示し、[ クエリーの保存 ] をクリックします。





保存されたクエリが [カスタムフィルタクエリ] に表示されます。保存されたクエリに基づいて、ADM はそれらの StyleBook へのユーザーアクセスを提供します。

- b) リストから必要な StyleBook を選択し、「OK」をクリックします。

グループを作成し、そのグループにユーザーを追加するときに、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、依存するすべての StyleBook も選択されます。

コンフィグパック:

**Configpacks** で、次のいずれかのオプションを選択します。

- 
- 選択した **StyleBook** のすべての構成: このオプションでは、選択した StyleBook のすべての構成パックが追加されます。
- 特定の構成: このオプションでは、必要な構成パックを追加できます。

グループを作成し、そのグループにユーザーを追加するときに、必要な構成パックを選択できます。

ドメイン名:

ユーザーが表示または管理できる特定のドメイン名を選択するには、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、[ドメイン名を追加] 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。

7. [**Create Group**] をクリックします。

8. 「ユーザーの割り当て」セクションで、「使用可能」リストからユーザーを選択し、「構成済み」リストにユーザーを追加します。

注:

「新規」をクリックしてユーザーを追加することもできます。

## ← Create System Group

9. [完了] をクリックします。

### 複数のネットワーク機能エンティティにわたるユーザーアクセスを管理

管理者は、Citrix ADM のネットワーク機能エンティティの個々のレベルでユーザーアクセスを管理できます。また、正規表現フィルターを使用して、エンティティレベルで特定の権限をユーザーまたはグループに動的に割り当てることができます。

このドキュメントでは、エンティティレベルでユーザー権限を定義する方法について説明します。

開始する前に、グループを作成します。詳しくは、「NetScaler ADM でのグループの構成」を参照してください。

#### 使用シナリオ:

1 つ以上のアプリケーション (仮想サーバー) が同じサーバーでホストされているシナリオを考えてみましょう。スーパー管理者 (George) は、Steve (アプリケーション管理者) にホスティングサーバーではなく App1 にのみアクセス権を付与したいと考えています。

次の表は、サーバー A がアプリケーション App-1 と App-2 をホストするこの環境を示しています。

| ホストサーバー | アプリケーション (仮想サーバー) | サービス          | サービスグループ            |
|---------|-------------------|---------------|---------------------|
| サーバー A  | App1              | App-service-1 | App-service-group-1 |
| サーバー A  | App2              | App-service-2 | App-service-group-2 |

注:

Citrix ADM は、仮想サーバー、サービス、サービスグループ、およびサーバーをネットワーク機能エンティティとして扱います。エンティティタイプの仮想サーバーはアプリケーションと呼ばれます。

ネットワーク機能エンティティにユーザー権限を割り当てるために、George はユーザー権限を次のように定義します。

1. [アカウント] > [ユーザー管理] > [グループ] に移動し、グループを追加します。
2. 「認証設定」 タブで、「アプリケーションを選択」を選択します。
3. 「個々のエンティティタイプを選択」を選択します。
4. 「すべてのアプリケーション」 エンティティタイプを選択し、使用可能なリストから App-1 エンティティを追加します。
5. [Create Group] をクリックします。
6. 「ユーザーの割り当て」 で、権限を必要とするユーザーを選択します。このシナリオでは、George は Steve のユーザープロファイルを選択します。
7. [完了] をクリックします。

この認証設定では、Steve は App-1 のみを管理でき、他のネットワーク機能エンティティは管理できません。

注:

「バインドされたエンティティにも適用」 オプションがオフになっていることを確認してください。それ以外の場合、Citrix ADM は App-1 にバインドされているすべてのネットワーク機能エンティティへのアクセスを許可します。その結果、ホスティングサーバーへのアクセスも許可されます。

スーパー管理者は、エンティティタイプごとに正規表現 (regex) を指定できます。正規表現はシステムに保存され、ユーザー認証範囲を更新します。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と一致すると、Citrix ADM はユーザーに特定のネットワーク機能エンティティへのアクセスを動的に許可できます。

ユーザー権限を動的に付与するために、特権管理者は [権限設定] タブに正規表現を追加できます。

このシナリオでは、George が Applications App\* エンティティタイプの正規表現を追加すると、正規表現条件に一致するアプリケーションがリストに表示されます。この認証設定により、Steve は App\* 正規表現に一致するすべてのアプリケーションにアクセスできます。ただし、彼のアクセスはアプリケーションのみに制限され、ホストされたサーバーには制限されません。

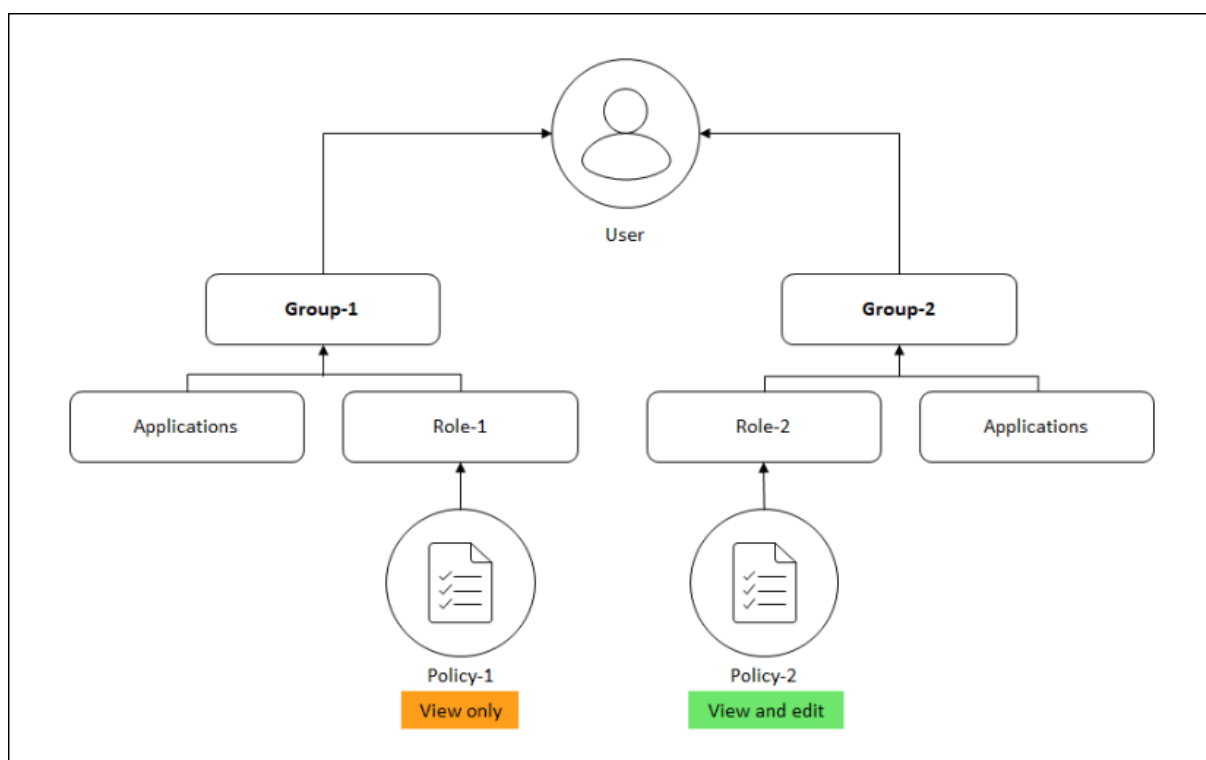
### 承認スコープに基づくユーザーアクセスの変更方法

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プされます。

この場合、ADM は特定の認証範囲に応じてユーザーにアプリケーションへのアクセスを許可します。

ポリシー 1 とポリシー 2 の 2 つのポリシーを持つグループに割り当てられているユーザを考えてみましょう。

- **Policy-1** –アプリケーションへのアクセス権限のみを表示します。
- **ポリシー-2** –アプリケーションへのアクセス権を表示および編集します。



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 アプリケーションに対する編集アクセスは、Group-1 認可スコープにはないため、制限されます。

### NetScaler ADM を 12.0 以降のリリースにアップグレードするときの RBAC のマッピング

Citrix ADM 12.0 から 13.0 にアップグレードすると、グループの作成時に「読み取り/書き込み」または「読み取り」権限を提供するオプションが表示されません。これらの権限は「役割」と「アクセスポリシー」に置き換えられており、より柔軟に役割ベースの権限をユーザーに提供できます。次の表は、リリース 12.0 の権限がリリース 13.0 にどのようにマップされるかを示しています。

| 12.0             | アプリケーションのみ許可 | 13.0        |
|------------------|--------------|-------------|
| admin read-write | False        | admin       |
| admin read-write | True         | appAdmin    |
| admin read-only  | False        | readonly    |
| admin read-only  | 真            | appReadonly |

## 役割の設定

February 6, 2024

Citrix Application Delivery Management (ADM) 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。ポリシーと役割には、1 対 1、1 対多、多対多の関係を定義できます。1 つの役割を複数のポリシーにバインドすることも、複数の役割を 1 つのポリシーにバインドすることもできます。

たとえば、ある機能のアクセス権を定義するポリシーと別の機能のアクセス権を定義する別のポリシーの 2 つのポリシーに、1 つの役割をバインドできます。一方のポリシーでは、Citrix ADM に Citrix ADC インスタンスを追加する権限を付与し、もう一方のポリシーでは StyleBook を作成して展開し、Citrix ADC 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。

複数のポリシーで 1 つの機能に編集権限と読み取り専用権限を定義する場合、編集権限が優先されます。

Citrix ADM には、次の 4 つの定義済みロールがあります。

- 管理者。すべての NetScaler ADM 機能にアクセスできます。（この役割は adminpolicy にバインドされています）。
- 読み取り専用。読み取り専用アクセスが設定されています（この役割は readonlypolicy にバインドされています）。
- **appAdmin**。NetScaler ADM アプリケーション機能にのみ管理者権限が付与されます。（この役割は appAdminPolicy にバインドされています）。
- **appReadonly**。アプリケーション機能に対する読み取り専用アクセス権が設定されています（この役割は appReadOnlyPolicy にバインドされています）。

注: 定義済みのロールは編集できません。

また、独自の（ユーザー定義の）役割を作成することもできます。

ロールを作成してポリシーを割り当てるには、次の手順に従います。

1. Citrix ADM で、[システム] > [ユーザー管理] > [ロール] に移動します。
2. [追加] をクリックします。
3. 「ロール名」フィールドにロールの名前を入力し、「ロールの説明」フィールドに説明を入力します (オプション)。
4. 「ポリシー」セクションで、**1** つ以上のポリシーを設定済みリストに追加または移動します。

## ← Create Roles

Role Name\*  
example-external-auth-role

Role Description  
External TACACS Authentication

Policies\*

Available (3) Search Select All

- appAdminPolicy +
- readonlypolicy +
- appReadOnlyPolicy +

New | Edit

Configured (1) Search Remove All

- adminpolicy -

Create Close

5. [作成] をクリックします。

## ユーザーの構成

February 6, 2024

デフォルトでは、Citrix Application Delivery Management (ADM) には 1 人のユーザーがいます。

nsroot - ルートユーザー (nsroot) は、アプライアンスに対するすべての管理権限を持ちます。nsroot ユーザーは Citrix ADM のスーパー管理者です。

ユーザーは、アカウントを構成することで追加できます。Citrix ADM に新しいユーザーを追加するときは、適切なグループ、役割、およびポリシーを割り当てることによってそのユーザーの権限を定義できます。

ユーザーをグループに割り当てて、グループを複数の役割にバインドすることができます。ユーザー、グループ、役割、およびアクセスポリシーの間には、1対1、1対多、多対多の関係を定義できます。複数のデスクトップを単一のユーザーに割り当てることができます。グループには複数の役割を設定することも、複数のグループに同一の役割を設定することもできます。

**NetScaler ADM** でユーザーを構成するには:

1. NetScaler ADM で、[システム] > [ユーザー管理] > [ユーザー] に移動します。
2. [追加] をクリックします。
3. 次の詳細情報を入力します:
  - a) ユーザー名。ユーザーの名前
  - b) パスワード。ユーザーが Citrix ADM にログオンするときに使用するパスワード
4. 必要に応じて、「外部認証を有効にする」を選択して、外部認証サーバーを介してユーザーを認証できるようにします。
5. グループを作成していて、ユーザーをグループに割り当てたい場合は、「グループ」セクションで、**1**つ以上のグループを「使用可能」リストから「構成済み」リストに移動します。

## ← Create System User

User Name\*  
 ?

Password\*  
 ?

Confirm Password\*  
 ?

Enable External Authentication ?  
 Configure User Session Timeout ?

Groups\*

**Available (3)** [Select All](#)

|            |   |
|------------|---|
| NSMASUser1 | + |
| read_only  | + |
| owner      | + |

▶

◀

**Configured (1)** [Remove All](#)

|             |   |
|-------------|---|
| NSMASUser11 | - |
|-------------|---|

6. [作成] をクリックします。

## アプリケーション

February 6, 2024

NetScaler ADM のアプリケーション分析および管理機能により、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。

- スコアをチェックし、アプリケーションの全体的なパフォーマンスを分析します
- サーバーまたはクライアントで引き続き発生する問題がないか確認してください
- アプリケーショントラフィックフローの異常を検出し、是正措置を取る

注

アプリケーションとは、インスタンス（NetScaler ADC）で構成された 1 つ以上の仮想サーバーを指し



ます。

1 時間、1 日、1 週間、1 か月などの期間にわたってアプリケーションを監視できます。

### 前提条件

- NetScaler ADM に NetScaler ADC インスタンスを追加したことを確認してください
- NetScaler ADC インスタンスの有効なライセンスがあることを確認してください。詳細については、「[ライセンス](#)」を参照してください。
- 仮想サーバのライセンスを適用していることを確認します。詳しくは、「[仮想サーバーでのライセンスの管理](#)」を参照してください。

### アプリケーションの概要

アプリケーションには、次のものがあります。

- ディスクリットアプリケーション
- 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)

### ディスクリットアプリケーション

ライセンスが付与されているすべての仮想サーバは、個別のアプリケーションと呼ばれます。

### カスタムアプリケーション

1 つのカテゴリの仮想サーバは、カスタムアプリケーションと呼ばれます。管理者は、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、ダッシュボードからアプリケーションを管理および監視できます。1 つのカテゴリに分類されている特定のアプリケーションを簡単に監視できます。

たとえば、データセンター 1 のカテゴリを作成し、その ADC インスタンスを追加できます。カテゴリを定義してデータセンター 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別のカテゴリでアプリケーションダッシュボードが表示されます。

### 注意事項

- カスタムアプリケーションに追加された個別アプリケーションは、個別のアプリケーションから削除されます。
- どのカテゴリにも追加されていないアプリケーションは、すべて「その他」として利用できます。

- デフォルトでは、NetScaler ADM では最大 2 つのアプリケーションのライセンスを追加できます。ライセンスに応じて、監視するアプリケーションのライセンスを選択して適用できます。

### マイクロサービスアプリケーション

Kubernetes クラスタでは、NetScaler ADC MPX（ハードウェア）、NetScaler ADC VPX（仮想化）、および NetScaler ADC CPX（コンテナ化）用の Ingress Controller を提供します。詳しくは、「[Citrix Ingress Controller](#)」を参照してください。

NetScaler ADC CPX インスタンスを使用して構成される個別の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

February 6, 2024

Citrix ADM では、アプリケーションページからアプリケーションを管理し、ダッシュボードページからアプリケーションの詳細を表示できます。

#### アプリケーション管理

アプリケーションページでは、すべてのカスタム・アプリケーションおよび個別のアプリケーションを表示できます。

| APP NAME                            | AVAILABILITY | TYPE     | CATEGORY | # VIRTUAL SERVERS/STATE | # SERVICES/STATE | # SERVERS/STATE | ACTIONS |
|-------------------------------------|--------------|----------|----------|-------------------------|------------------|-----------------|---------|
| SFB-sfb-fe-calladmissioncontrol...  | Down         | Discrete | Others   | 1 0 0 1 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |
| SFB-sfb-fe-calladmissioncontrol...  | Down         | Discrete | Others   | 1 0 0 1 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |
| SFB-sfb-fe-sip-callpark-lb_10.10... | Down         | Discrete | Others   | 1 0 0 1 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |
| SFB-sfb-fe-sip-confannounce-lb...   | Down         | Discrete | Others   | 1 0 0 1 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |

[アプリケーション] ページでは、管理者として次の操作を実行できます。

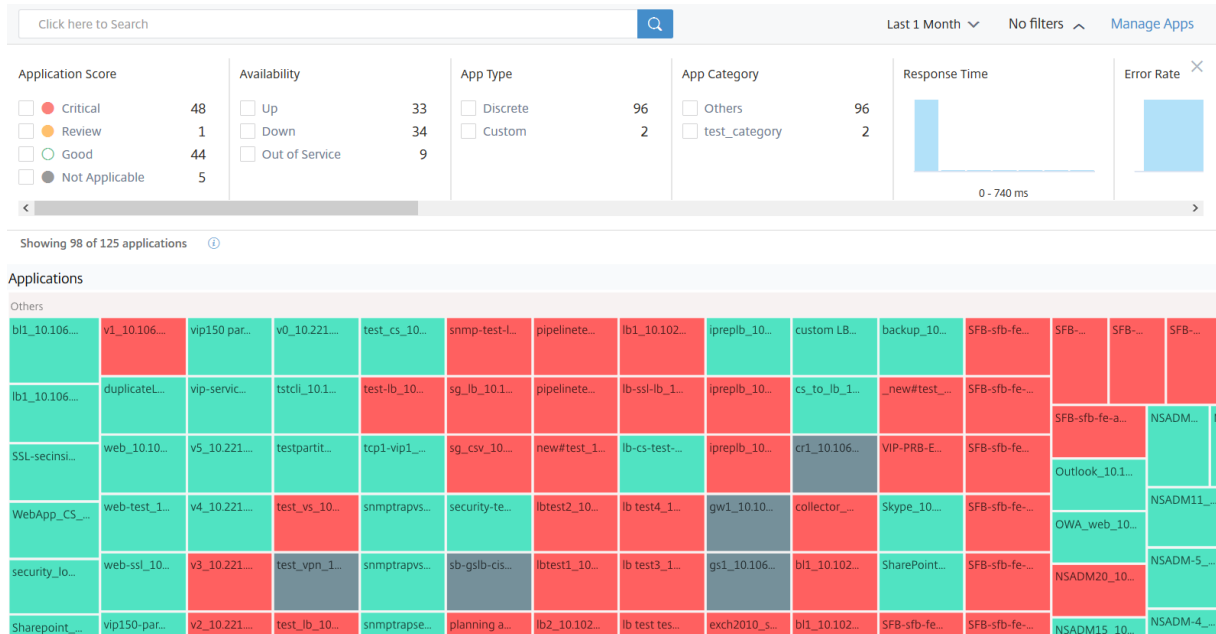
- アプリケーションの追加
- アプリケーション名、アプリケーションタイプ、アプリケーションカテゴリ、関連する仮想サーバー、関連するサービスなどのアプリケーションの詳細を表示します。
- カスタムアプリケーションの編集または削除

アプリケーションを追加、編集、または削除すると、その詳細が [アプリケーション] ページにすぐに反映されます。

詳しくは、「[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] に移動すると、アプリケーションのリストが表形式またはグラフ形式で表示されます。



すべてのアプリケーションは、アプリケーションがデータの入力を開始した後にのみダッシュボードに表示されます。ダッシュボードからアプリケーションをクリックして、アプリケーションのパフォーマンスの詳細情報を表示します。詳しくは、「[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、「[App Dashboard のトラブルシューティング](#)」でトラブルシューティングの手順を実行してください。

### 以前のダッシュボードと比較した新しいダッシュボードの動作の更新

- カスタムアプリケーションを追加または編集した後、アプリケーションがダッシュボードに反映されるまでに数分かかる場合があります。
- カスタムアプリケーションを削除しても、ADM が分析データを取得するまで（最長で 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引き続き表示されます。

2020 年 1 月 2 日にアプリケーションを作成し、2020 年 1 月 4 日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。このシナリオの内容は以下のとおりです。

- 過去 1 日、1 週間、1 か月の期間を選択すると、2020 年 1 月 4 日に削除されたアプリケーションが引き続きダッシュボードに表示されます。
- 過去 1 週間と 1 か月の期間を選択すると、2020 年 1 月 5 日に削除されたアプリケーションが引き続きダッシュボードに表示されます。

- 期間がアプリ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、2020年1月6日(過去1日間)、2020年1月12日(過去1週間)、および2020年2月5日以降(過去1か月間)に削除されたアプリケーションはダッシュボードに表示されません。

注

アプリケーションを追加した後、関連する NetScaler ADC インスタンスが停止している、サービスが停止している、または一時的なネットワーク障害のためにアクセスできない場合:

-ADC インスタンスに関連するアプリケーションは、アプリケーションページにのみ表示され、ダッシュボードには表示されません。

-アプリケーションは、ADC インスタンスが起動して実行されると、ダッシュボードに表示されます。

## アプリケーション管理

February 6, 2024

ダッシュボードから、「**Manage Apps**」をクリックしてアプリケーションの詳細を表示し、カスタムアプリケーションを追加、編集、または削除します。

### アプリケーション詳細の表示

| Manage Applications                               |       |          |          |                       |                |                      |               |                                 |
|---------------------------------------------------|-------|----------|----------|-----------------------|----------------|----------------------|---------------|---------------------------------|
| <input type="text" value="Click here to search"/> |       |          |          |                       |                |                      |               | <a href="#">New Application</a> |
| APP NAME                                          | STATE | TYPE     | CATEGORY | VIRTUAL SERVERS/STATE | SERVICES/STATE | SERVICE GROUPS/STATE | SERVERS/STATE | ACTION                          |
| uslb_10.106.197.167_lb                            | ● Up  | Discrete | Others   | 1 ● 1 ● 0 ● 0         | 1 ● 1 ● 0 ● 0  | 0 ● 0 ● 0 ● 0        | 1 ● 1 ● 0     |                                 |
| mylb_10.106.197.167_lb                            | ● Up  | Discrete | Others   | 1 ● 1 ● 0 ● 0         | 1 ● 1 ● 0 ● 0  | 0 ● 0 ● 0 ● 0        | 1 ● 1 ● 0     |                                 |

- アプリケーション名—アプリケーション名を示します。
- 可用性—稼働中 **\*\***、停止中、一部稼働中 **\*\***、サービス停止、**\*\*** サービス停止、**NA** など、アプリケーションの現在の可用性を示します **\*\***
  - **Up** : アプリケーションに関連づけられているすべての仮想サーバが Up です。
  - 停止—アプリケーションに関連するすべての仮想サーバが停止しています
  - **Partially Up** : アプリケーションに関連づけられている 1 つの仮想サーバがダウンしているか、サービスが停止している
  - **Out of Service** —アプリケーションに関連するすべての仮想サーバがアウトオブサービスです

- **NA** –アプリケーション用の仮想サーバは設定されていません

- タイプ—アプリケーションがカスタムとディスクリートのどちらに属しているかを示します
- 「カテゴリ」 (Category) —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/状態—設定されている仮想サーバの総数とすべての仮想サーバの現在の状態を示します。マウスポインターを合わせると、仮想サーバの合計、仮想サーバの種類、仮想サーバのステータスなどの詳細が表示されます。

| APP NAME                     | AVAILABILITY   | TYPE     | CATEGORY | # VIRTUAL SERVERS/STATE | # SERVICES/STATE | # SERVERS/STATE | ACTIONS |
|------------------------------|----------------|----------|----------|-------------------------|------------------|-----------------|---------|
| VIP-PRB-EPC-gpsCarLinkMPL... | Out of Service | Discrete | Others   | 1 0 0 1 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |
| SSUxServer_10.106.150.52_B   | Out of Service | Discrete | Others   | 1 0 0 1 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |
| gs1_10.106.150.52_ogn        | Down           | Discrete | Others   | 1 0 0 1 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |
| gs1_10.106.150.52_galb       | Down           | Discrete | Others   | 1 0 0 1 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |
| group-85-85                  | Down           | Custom   | test-cat | 5 0 0 1 0 0             | 0 0 0 1 0 0      | 0 0 0 0         |         |
| 85-8_10.106.43.7_B           | Down           | Discrete | Others   | 1 0 0 1 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |
| CSW2_10.106.150.52_cs        | Up             | Discrete | Others   | 1 1 0 0 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |
| Bwt1_10.106.181.230_B        | Up             | Discrete | Others   | 1 1 0 0 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |
| Test3_10.106.43.7_B          | Up             | Discrete | Others   | 1 1 0 0 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |
| custom-app-58test            | NA             | Custom   | test-cat | 0 0 0 0 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |
| test-85-jayb-8_10.106.43.7_B | Down           | Discrete | Others   | 1 0 0 1 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |
| test-87_10.106.43.7_B        | Down           | Discrete | Others   | 1 0 0 1 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |
| test-86_10.106.43.7_B        | Down           | Discrete | Others   | 1 0 0 1 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |
| Custom App                   | Partially up   | Custom   | test-cat | 0 0 0 0 0 0             | 0 0 0 0 0 0      | 0 0 0 0         |         |
| Custom App 1                 | Partially up   | Custom   | test-cat | 8 0 4 1 0 3             | 0 0 0 0 0 0      | 0 0 0 0         |         |

- **services/state** —すべてのサービスの構成済みサービスの合計と現在のステータスを示します。
- **Service Goups/state** : 設定されているサービスグループの合計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/状態: アプリケーション用に構成されたサーバの合計と、すべてのサーバの現在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. 「新規アプリケーション」をクリックして、新しい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。

## ← Define Application

Name\*

Category\*

 >

Select Existing Applications

Define Selection Criteria

Create a new application from a StyleBook

**Applications**

|          | Name |
|----------|------|
| No items |      |

注:

「アプリケーション」をクリックし、「新規アプリケーション」を選択して新しいアプリケーションを追加することもできます。

2. 次のパラメーターを設定します。

| フィールド | 説明                                                                                                                                                                 |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前    | カスタムアプリケーションの名前。たとえば、LB_TEST などです。                                                                                                                                 |
| カテゴリ  | <p>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、アプリケーションカテゴリページが表示されます。カテゴリを選択し、[ 選択 ] をクリックします。カテゴリを追加するには</p> <ol style="list-style-type: none"> <li>[ 追加 ] をクリックします</li> </ol> |

| フィールド                                                     | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>既存のアプリケーションの選択</p> <p>[アプリケーションを追加]</p> <p>選択条件の定義</p> | <p>a) 任意の名前を入力します。</p> <p>3. [作成] をクリックします</p> <p>NetScaler ADC 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。</p> <p>インスタンスに設定されているすべての仮想サーバーを表示します。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。</p> <p>仮想サーバーの範囲、または元のサーバー/サービスの IP アドレスの範囲でアプリケーションを定義するオプション。</p> <ul style="list-style-type: none"> <li>• サーバー。サーバーまたはサービスの IP アドレス、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を指定します。1 つの IP アドレスか IP アドレスの範囲、またはコンマ区切りでそれらを組み合わせて入力できます。たとえば、「10.102.29.20, 10.102.43.10-60, 10.216.43.45」と入力します。</li> <li>• 仮想サーバー。仮想サーバーの 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 アドレスか IP アドレスの範囲、またはコンマ区切りによるそれらの組み合わせで入力できます。たとえば、「10.102.29.20, 10.102.43.10-60, 10.216.43.45」と入力します。</li> </ul> |
| <p>StyleBook から新しいアプリケーションを作成する</p>                       | <p>StyleBook を使用してアプリケーションを作成できます。詳しくは、「StyleBook を使用したアプリケーションの作成」を参照してください。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

3. **[OK]** をクリックします。

注:

現在、Application Dashboard では、負荷分散とコンテンツスイッチング仮想サーバーのみがサポートされています。

これで、アプリケーションダッシュボードがカテゴリとともに表示され、すべてのアプリケーションが下にグ

ループ化されます。

カスタムアプリケーションの「**StyleBook** から新しいアプリケーションを作成する」オプションを選択した場合は、Citrix ADM がライセンス対象として仮想サーバーを自動選択できるようにする必要があります。仮想サーバの自動選択を有効にするには、次の手順で行います。

- a) [システム] > [ライセンスと分析] に移動します。
- b) [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 [アドレス指定できない仮想サーバーの自動選択] をクリックして有効にします。

## StyleBook を使用してアプリケーションを作成する

StyleBook を使用してアプリケーションを作成するには:

1. Citrix ADM で、[アプリケーション] > [ダッシュボード] に移動し、[カスタムアプリケーションの定義] をクリックしてカスタムアプリケーションを作成します。
2. 「アプリケーションの定義」ページの「名前」フィールドにアプリケーションの名前を入力します。
3. [カテゴリ] セクションからアプリケーションカテゴリを選択します。NetScaler ADM では、ユーザー定義のアプリケーションをグループ化するカテゴリを定義できます。必要に応じて、さらにカテゴリを追加することもできます。
4. 「**StyleBook** から新規アプリケーションを作成」をクリックして選択し、「**OK**」をクリックします。  
「StyleBook の選択」ページが表示されます。このページには、NetScaler ADM で使用できるデフォルトの StyleBook がすべて含まれています。
5. StyleBook を選択します。  
「構成の詳細」ページが表示されます。
6. StyleBook のすべてのパラメーターの値を入力します。また、[View Definition] をクリックして、使用する前に StyleBook の構成を表示することもできます。  
詳しくは、「[デフォルトの StyleBook を使用する](#)」を参照してください。
7. [作成] をクリックします。

[ **Dry Run** ] をクリックして、選択した NetScaler ADC インスタンスで NetScaler ADM が作成しようとする構成を確認することもできます。このオプションは、設定の最終チェックを確認するためのテスト用です。ドライランオプションが成功した場合でも、さまざまな理由（IP の競合、インスタンスにアクセスできないなど）により、選択した NetScaler ADC での実際の構成が失敗する可能性があります。

## アプリケーションを編集または削除する

アプリケーションページから、カスタムアプリケーションを編集または削除できます。アプリケーションを編集するには [編集] ボタンをクリックし、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のエクスポート

NetScaler ADM では、現在のアプリケーションダッシュボードのスナップショットを取得し、レポートとしてエクスポートできます。頻繁な間隔で、アプリ管理者はこれらのレポートを使用して、アプリの使用状況やパフォーマンス上のペナルティについて更新する必要があります。

この機能により、管理者はこのデータを.png、.jpeg、または.pdf レポートとして抽出できます。

注:

NetScaler ADM の他のレポートエクスポートオプションとは異なり、アプリダッシュボードとセキュリティダッシュボードのレポートは.pdf または.png ファイルとしてのみエクスポートできます。.csv 形式は現在サポートされていません。

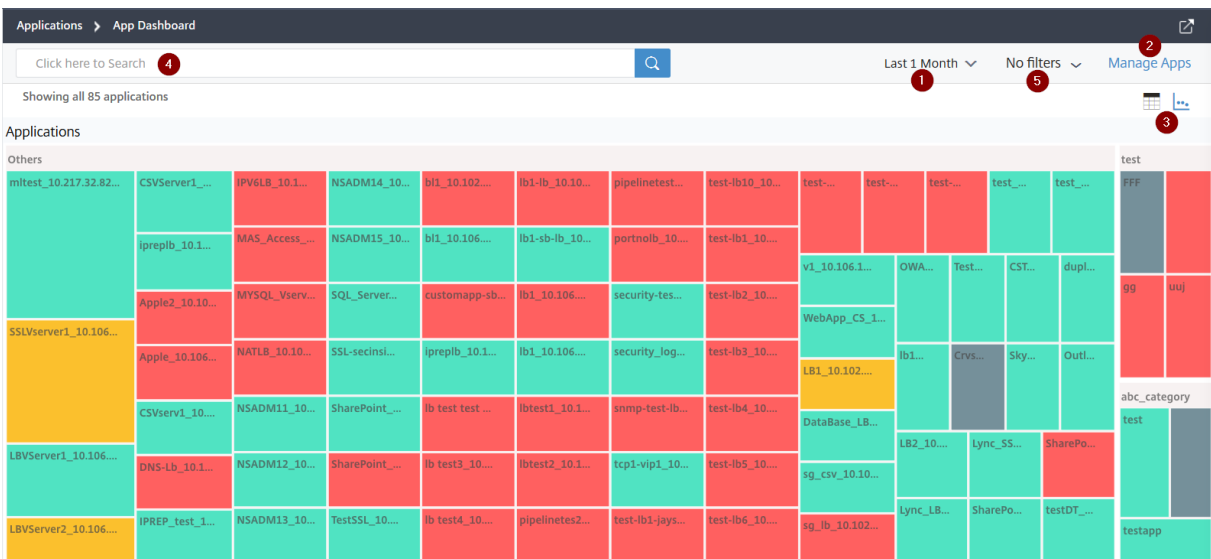
レポートがシステムにダウンロードされます。アプリダッシュボードとアプリセキュリティダッシュボードページから、第 2 レベルのページに移動してレポートとしてエクスポートすることもできます。現在、一度に 1 つのアプリケーションのレポートしかダウンロードできません。

## アプリケーションダッシュボードの概要

February 6, 2024

アプリケーションダッシュボードには、「その他」の下に個別のアプリケーションが表示され、それぞれのカテゴリにグループ化されたカスタムアプリケーションが表示されます。

アプリケーション > ダッシュボードに移動して、アプリダッシュボードを表示します。



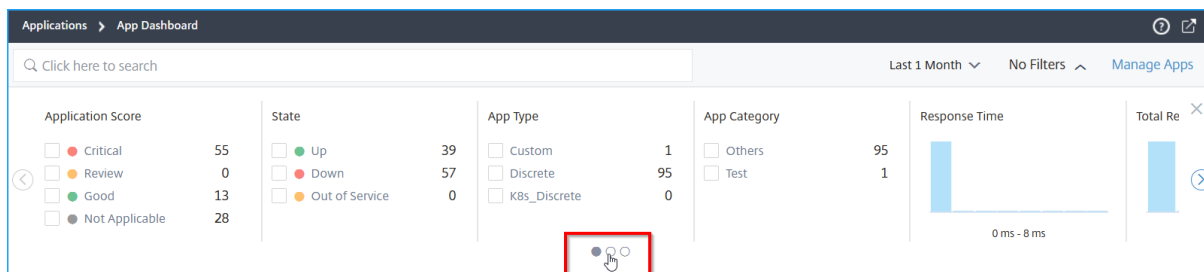
1 — 1 時間、1 日、1 週間、1 か月など、選択した期間のアプリケーションの詳細を表示します。

2 –アプリケーションの管理と新しいアプリケーションの追加が可能

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。クリックすると詳細が表示されます。



カーouselスライダーを選択すると、すべてのオプションに簡単にアクセスできます。

次の操作を実行できます：

- 選択すると、スコアに基づいてアプリケーションが表示されます。
  - 重要—アプリケーションスコアは 0~40 未満
  - 公平—応募スコアは 40~75 未満
  - 良い—アプリケーションのスコアが 75 を超えている
  - 該当なし—アプリケーション用の仮想サーバは設定されていません

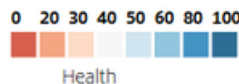
次の表は、以前のアプリスコアと現在のアプリスコアの違いを示しています。

アプリケーションスコア (クリティカル、レビュー、良好、該当なし)

アプリスコア (以前の表示と色の凡例)

スコアは、アプリケーションの現在のすべての問題のペナルティスコアを **100** 引いたものとして計算されます。アプリケーションは、赤 (重要)、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。

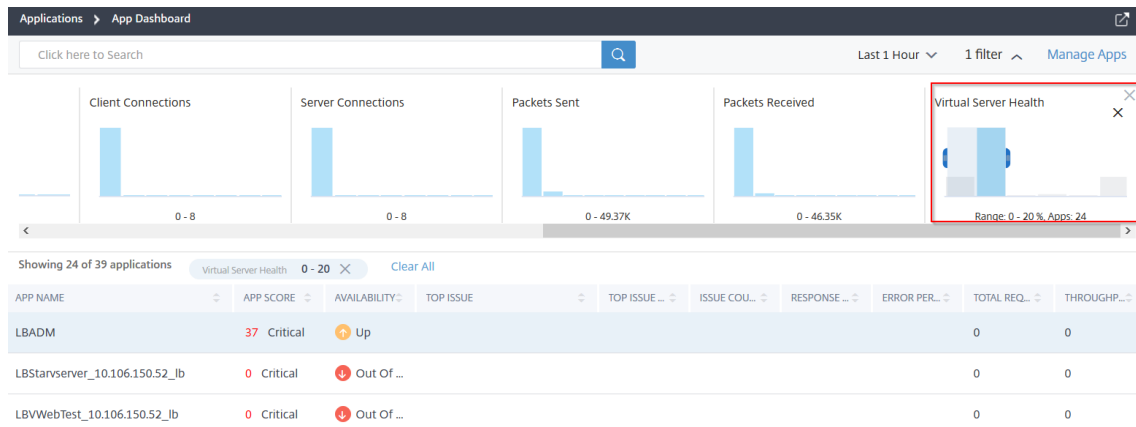
スコアは **100** として計算されます- (アプリサーバーリソース +**NetScaler ADC** システムリソース) アプリケーションは色の凡例で表示されます。



- 「Up」、「Down」、「Out of Service」などのアプリケーションのステータスに基づいてアプリケーションを表示するために選択します。
- 選択すると、「Discrete」や「Custom」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が表示されます。
- 選択すると、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が表示されます

- ヒストグラムをドラッグしてフィルターを適用し、アプリケーションを表示します。

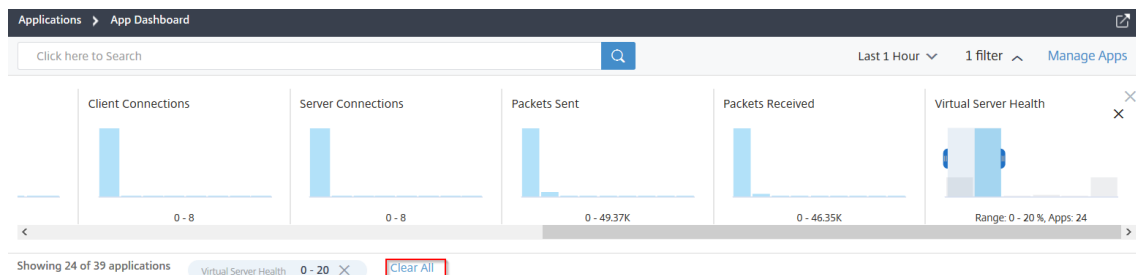
たとえば、仮想サーバーの状態が 0 ~ 20 のアプリケーションを表示する場合は、仮想サーバーの状態ヒストグラムをドラッグして結果をフィルタリングします。



## 注

ヒストグラムをクリックして、関連するアプリケーションを表示することもできます。

適用されている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。



フィルタを適用できるアプリケーションの概要を次に示します。

- 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
- エラー率—アプリケーションの 5xx エラーの平均エラー率を表示するヒストグラム
- リクエスト総数—アプリケーションが受け取ったリクエストの総数を表示するヒストグラム
- スループット—アプリケーションによって処理された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
- **Data Volume** —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。データ量は、アプリケーションの合計要求バイト数と応答バイト数で計算されます。
- クライアント接続—アプリケーションによって確立された平均クライアント接続を表示するヒストグラム
- サーバー接続—アプリケーションによって確立された平均サーバー接続を表示するヒストグラム

- 送信パケット数—アプリケーションによって送信された合計パケット数を表示するヒストグラム
- 受信パケット—アプリケーションが受信したパケットの合計を表示するヒストグラム
- 仮想サーバーの健全性—スコア範囲 0% ~100% のアプリケーションの合計を表示するヒストグラム。仮想サーバーの状態は、アプリケーションに関連するアクティブなサービスの (%) です。たとえば、仮想サーバに 2 つのサービスが設定されていて、そのうちの 1 つがダウンしている場合、スコアは 50% です。

検索バーを使用して結果を検索およびフィルタする

検索バーにマウスポインタを置き、カテゴリを選択して検索を絞り込むことができます。

## アプリケーションの表示

February 6, 2024

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。

Showing 98 of 125 applications ⓘ

| APP NAME                 | APP SCORE | AVAILABILITY | APP TYPE | APP CATEG. | TOP ISSUE | TOP ISSUE CATEGORY                        | ISSUE COUL. | RESPONSE | ERROR PER. | TOTAL REQ. | THROUGHPUT | DATA VOLL. |         |
|--------------------------|-----------|--------------|----------|------------|-----------|-------------------------------------------|-------------|----------|------------|------------|------------|------------|---------|
| web_10.107.98.70_lb      | 85        | Good         | Up       | Discrete   | Others    | Active Services<br>Last Monday at 1:00 AM | Performance | 1        | 0          | 0%         | 0          | 0          | 0 Bytes |
| web-test_10.107.98.70_lb | 85        | Good         | Up       | Discrete   | Others    | Active Services<br>Last Monday at 1:00 AM | Performance | 1        | 0          | 0%         | 0          | 0          | 0 Bytes |
| web-ssl_10.107.98.70_lb  | 85        | Good         | Up       | Discrete   | Others    | Active Services<br>Last Monday at 1:00 AM | Performance | 1        | 0          | 0%         | 0          | 0          | 0 Bytes |

ダッシュボードには、次のアプリケーション詳細が表示されます。

- アプリケーション名—アプリケーション名を示します。
- アプリスコア—アプリケーションのスコアと、「\*\* 重要」、「良好」、「普通」、「該当なし」などのステータスを示します \*\*
- 可用性—稼働中 \*\*、停止中、一部稼働中 \*\*、サービス停止、\*\* サービス停止、**NA** など、アプリケーションの現在の可用性を示します \*\*
  - **Up** : アプリケーションに関連づけられているすべての仮想サーバが Up です。
  - 停止—アプリケーションに関連するすべての仮想サーバが停止しています。
  - **Partially Up** —アプリケーションに関連づけられている仮想サーバの 1 つがダウンしているか、サービス停止状態です。
  - **Out of Service** —アプリケーションに関連するすべての仮想サーバがアウトオブサービスです。
  - **NA** —アプリケーションに対して仮想サーバが設定されていません。

- 最上位の問題—アプリケーションでエラー数が最も多い問題を示します
- 最重要課題カテゴリ—課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応答までの平均応答時間を示します
- エラーパーセンテージ—アプリケーションの 5xx エラーの合計エラーパーセンテージを示します

注

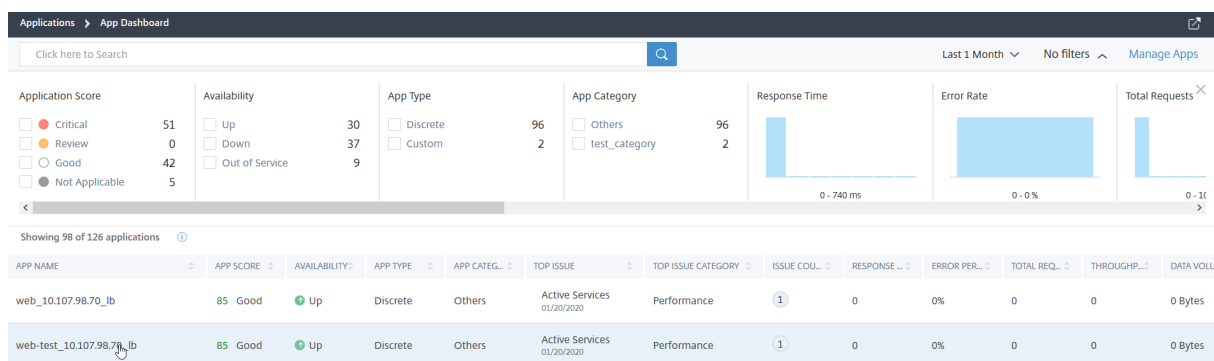
5xx エラーパーセンテージメトリックは、**Citrix ADC 13.0** 以降の場合にのみ表示されます。以前のバージョンでは、値は **0** と表示されます。

- リクエスト総数—アプリケーションが受け取ったリクエストの合計を示します
- 「スループット」—アプリケーションのネットワークスループットの合計を示します。スループットは、仮想サーバーの要件バイト/秒 + レスバイト/秒で計算されます
- データ量—アプリケーションによって処理されたデータの合計を示します
- 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的なクライアント接続を示します
- 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を示します。

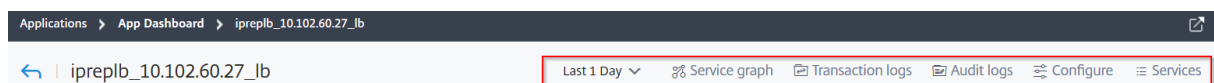
## アプリケーションの詳細

February 6, 2024

ダッシュボードのアプリケーションをクリックしてドリルダウンすると、詳細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。

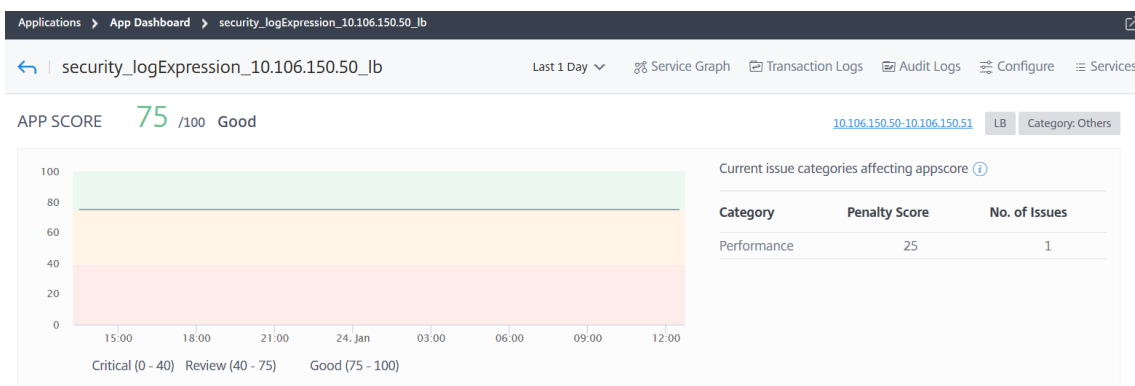


アプリケーションの詳細ページから:

- リストから期間を選択すると、特定の期間の詳細が表示されます。
- 「サービス・グラフ」をクリックして、選択したアプリケーションのサービス・グラフを表示します。詳細については、「[アプリケーション用サービスグラフ](#)」を参照してください。
- 「トランザクション・ログ」をクリックして、5xx エラーの詳細なトランザクションを表示します。
- [ 監査ログ ] をクリックして、監査ログの詳細情報を表示します。
- [ **Configure** ] をクリックして、アプリケーションのサービスおよびサービスグループ設定を表示または編集します。
- [ サービス ] をクリックして、アプリケーションにバインドされたサービスを表示します。

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。最終的なスコアは、ペナルティ合計を差し引いた **100** として計算されます。



このダッシュボードでは、アプリのスコアに影響している現在の問題を表示することもできます。[懸案事項]で懸案の詳細を表示できます。

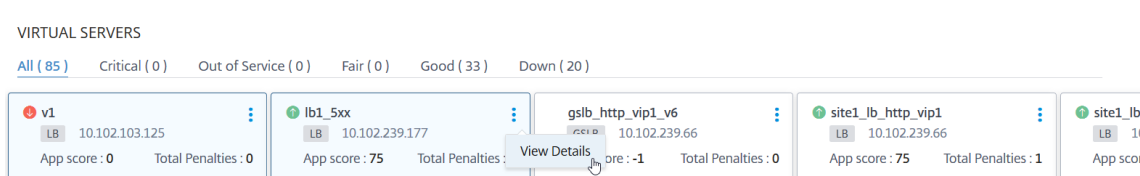
- 仮想サーバー—

注

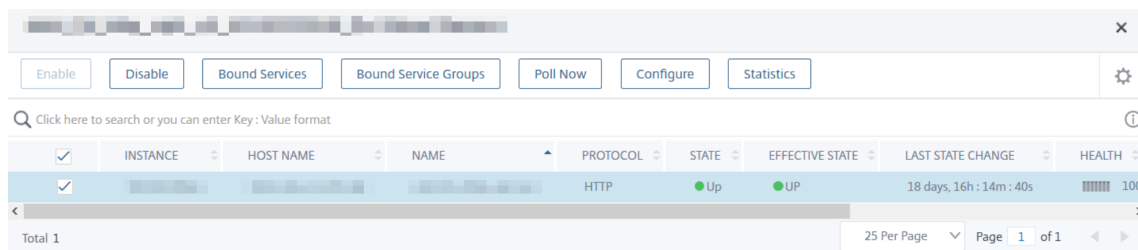
仮想サーバーセクションは、カスタムアプリケーションでのみ表示されます。個別のアプリケーションの場合は、**IP** アドレスをクリックすると仮想サーバーの詳細が表示されます。

APP SCORE **100** /100 Good [10.106.154.192](#) LB Category: Others

カスタムアプリケーションに関連付けられているすべての仮想サーバーを表示します



「詳細を表示」をクリックして、仮想サーバーの設定を表示および管理します。

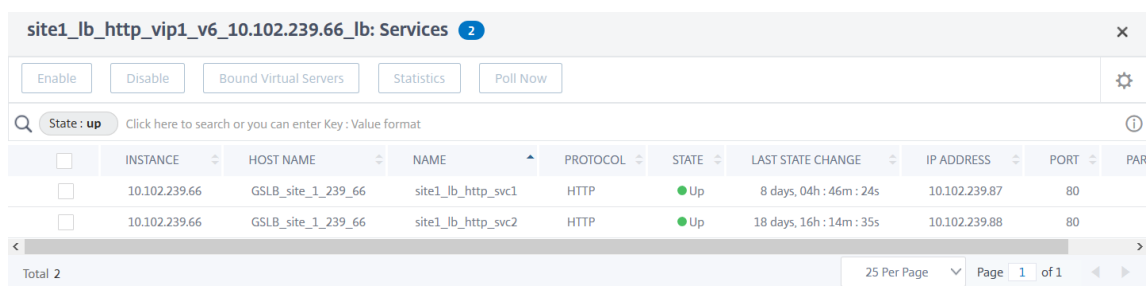


- すべてのサービス–アプリケーションにバインドされているサービス

## ALL SERVICES GROUPS

| Group name | Group state | Service States                 |
|------------|-------------|--------------------------------|
| [Redacted] | ENABLED     | 1 Up  0 Out of Service  0 Down |

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



- 主要メトリック–アプリケーションの応答時間、エラー率、1秒あたりのリクエスト数、スループット、合計接続数、データボリュームなどのアプリケーション・メトリックの詳細。SSL 関連アプリケーションの場合、セッションヒット、暗号化されたバイトレート、復号化されたバイトレート **\*\***、**\*\*** 新規作成された **SSL** セッションなどのメトリックの詳細が表示されます。

注

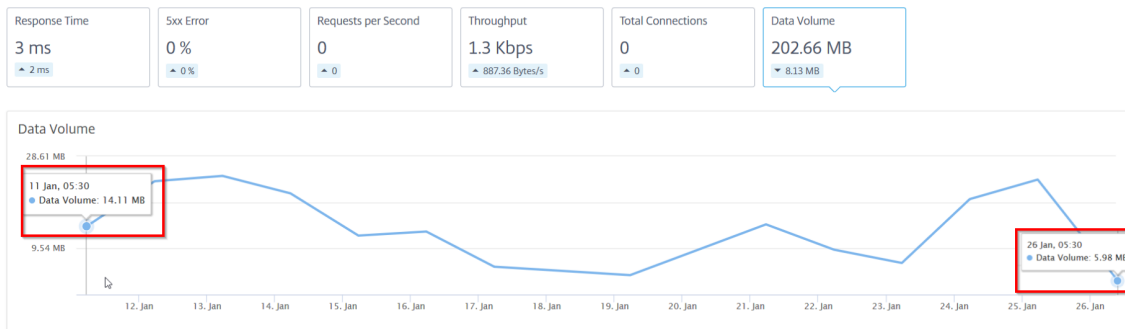
5xx エラーパーセンテージメトリックは、**Citrix ADC 13.0** 以降の場合にのみ表示されます。以前のバージョンでは、値は **0** と表示されます。

各指標で、選択した期間の平均値と差値を表示できます。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。

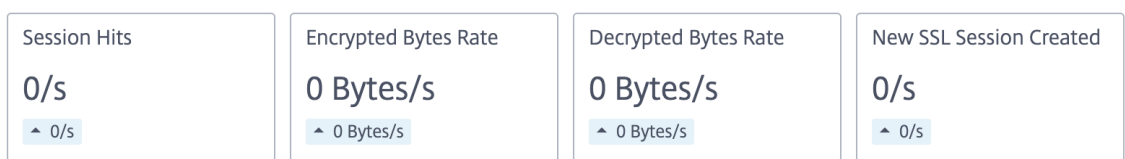
選択した期間について、次のインスタンスメトリックスをグラフ形式で表示できます。

次の図は、データボリュームの例で、選択した期間は 1 か月です。202.66 MB は 1 か月間のデータ量の合計で、8.13 MB という値は差額です。グラフでは、最初の値は 14.11 で、最後の値は 5.98 です。差の値は  $14.11 - 5.98 = 8.13$  MB です。

KEY METRICS



SSL 関連アプリケーションの場合は、次のその他のメトリックスを表示できます。



- [問題] —選択したアプリケーションに適用可能な問題。次の問題とそのカテゴリを表示できます。

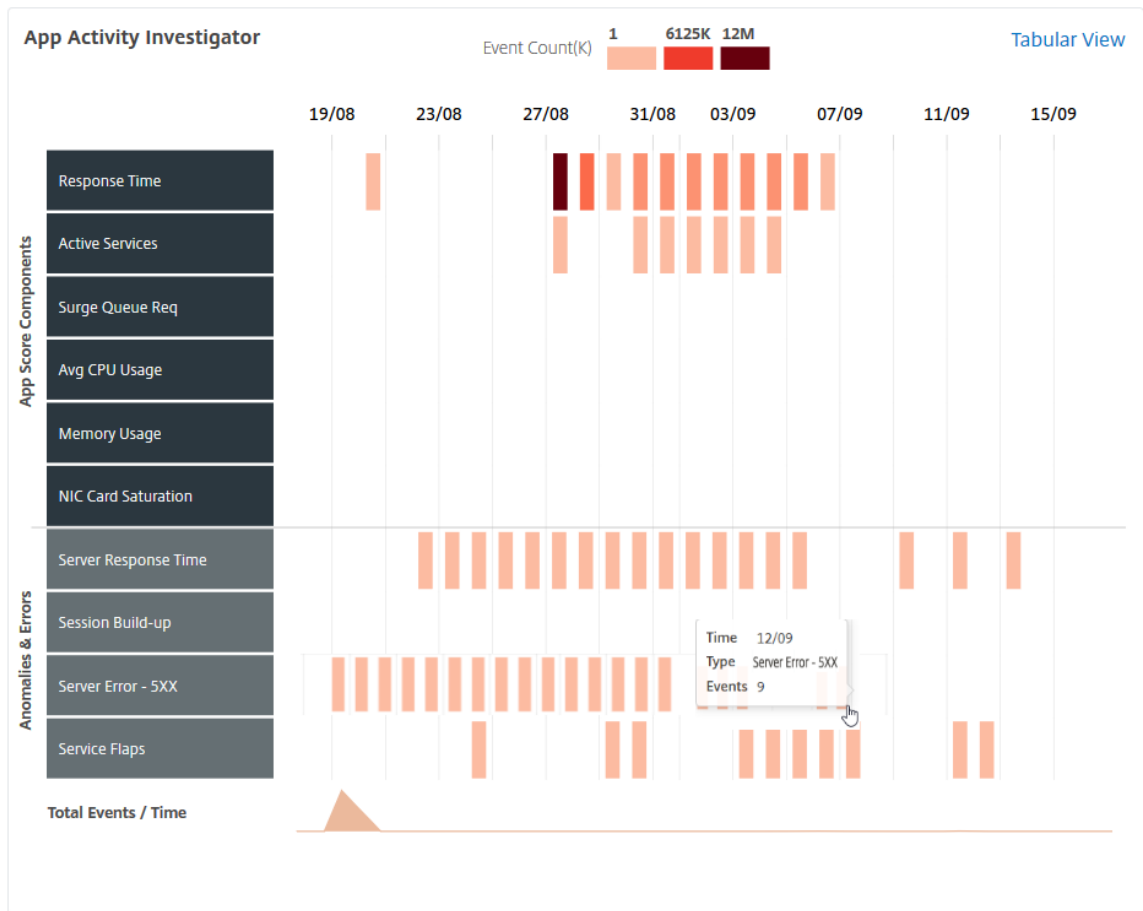
| パフォーマンス          | インスタンスヘルス  | 構成               | システムリソース   |
|------------------|------------|------------------|------------|
| 応答時間             | 平均 CPU 使用率 | 不安定なサーバー         | 不適切な永続性タイプ |
| アクティブなサービス       | メモリ使用率     | 異常に大きい HTTP パケット | NIC カードの飽和 |
| セッションの再利用が低い     |            | TCP 再構成キュー制限ヒット  |            |
| サージキューのビルダップ     |            |                  |            |
| SSL リアルタイムトラフィック |            |                  |            |
| セッションのビルダップ      |            |                  |            |
| 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、推奨アクション、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指標](#)」を参照してください。

次の画像は、App Activity Investigator のページの以前のビューです：





**Activity Investigator** ページで表示できるカテゴリとともに、すべての問題を [問題] セクションに表示できるようにになりました。

ISSUES

Current (1) All (3)

|                                                    |      |
|----------------------------------------------------|------|
| Response Time<br>Performance<br>Today at 5:30 AM   | 40   |
| Active Services<br>Performance<br>Today at 5:30 AM | 3.9K |
| Memory Usage<br>Instance Health<br>01/06/2020      | 4    |

**Medium Response Time**

Detects events when application response time to respond for client requests deviates from the configured threshold.

**What Happened**  
App response time for v1 has breached the configured threshold of 500ms.

No. of occurrences: 40      Last occurred: Today at 5:30 AM

**Details**

| TIME            | NO OF OCCURRENCES | SEVERITY | DETECTION MSG                                                                  |
|-----------------|-------------------|----------|--------------------------------------------------------------------------------|
| Jan 23 - Jan 24 | 2                 | MEDIUM   | The response time for 37 transactions has exceeded the configured value 500ms. |
| Jan 22 - Jan 23 | 5                 | MEDIUM   | The response time for 37 transactions has exceeded the configured value 500ms. |

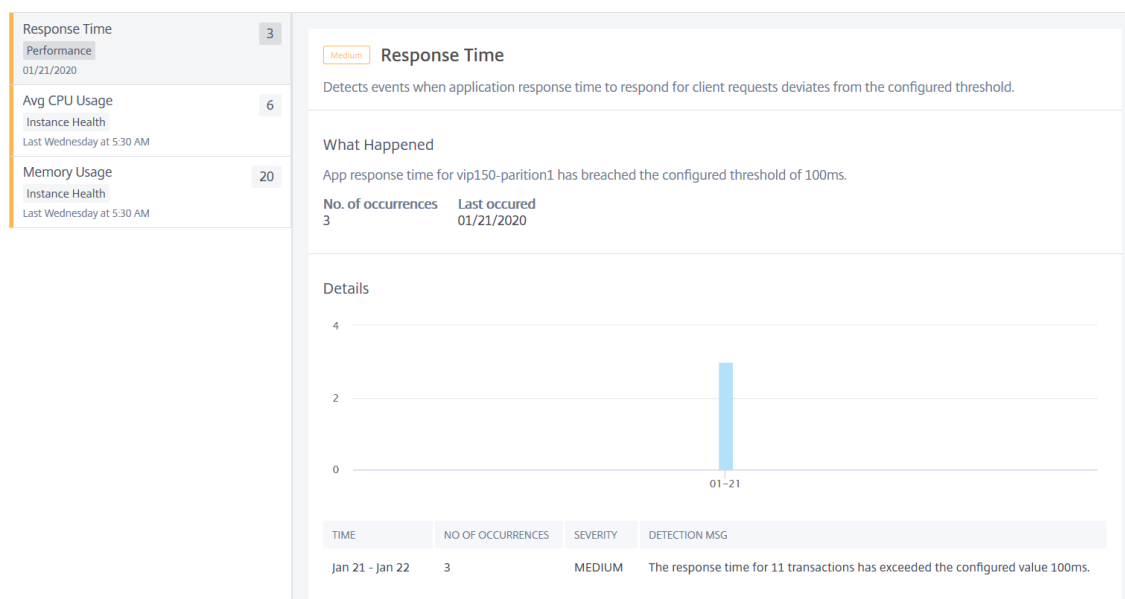
- 現在のタブに表示される問題は、選択した期間のアプリケーションの問題を示しています。
- 「すべて」タブに表示される問題は、アプリケーションの問題の合計を示しています。

次の例は、1日間のアプリケーションの問題です。「**Current**」タブには、アプリのスコアに影響する現在の問題がないことが表示されます。

[すべて]タブには、1日間に検出された問題の総数が表示されます。

ISSUES

Current (0) All (3)



## アプリスコアコンポーネントを選択し、しきい値を設定します

February 6, 2024

アプリダッシュボードでは、管理者は、コンポーネントを選択し、アプリスコア計算のしきい値を構成することができます。アプリスコアは、次の定義を定義するスコアリングシステムです。

- アプリケーションがどれくらいうまく実行されているか
- アプリケーションが応答性の点でうまく動作しているかどうか

[アプリケーション] > [ダッシュボード] に移動し、[設定] アイコンを選択します。

[アプリスコアの構成] ページで、コンポーネントを選択し、しきい値を構成して、最終的なアプリスコアを決定できます。

### Configure App Score

Configure the contributing factors and their thresholds to calculate the App Score values

- ADC Memory Usage ⓘ
  - Low Memory Threshold (%)
  - High Memory Threshold (%)
- Surge Queue Build-up ⓘ
  - Lower Surge Queue Threshold
  - Higher Surge Queue Threshold
- ADC CPU Usage ⓘ
  - Low CPU Threshold (%)
  - High CPU Threshold (%)
- Response Time ⓘ
  - Response Time (ms)
- App CPU Usage ⓘ
  - Low App CPU Threshold (%)
  - High App CPU Threshold (%)
- Active Services ⓘ
  - Active Services Threshold (%)
- Improper Persistence Type ⓘ
- Server Error 5xx ⓘ
- Unusually Large HTTP Packets ⓘ
- SSL Real Time Traffic ⓘ
- SSL Session Build-up ⓘ
- Low Session Reuse ⓘ
- NIC Card Saturation ⓘ
- TCP Reassemble Queue Limit Hits ⓘ

アプリスコアの計算は、次のコンポーネントに基づいています。

| アプリスコアコンポーネント    | ユーザが設定したしきい値 | 説明                                                                                   |
|------------------|--------------|--------------------------------------------------------------------------------------|
| ADC メモリ使用量       | はい           | NetScaler ADC インスタンスの合計メモリ使用量の低しきい値と上限しきい値                                           |
| 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要求の合計の下限および上限しきい値。                                              |
| ADC の CPU 使用率    | はい           | NetScaler ADC インスタンスの CPU 使用率の合計の下限および上限しきい値。                                        |
| 応答時間             | はい           | 要求パケットの送信から、仮想サーバ上で構成されたサービスからの最初の応答パケットを受信するまでの時間間隔。                                |
| アプリの CPU 使用率     | はい           | アプリケーションによる CPU 使用率の合計（低）および上限しきい値。                                                  |
| アクティブなサービス       | はい           | 仮想サーバにバインドされているアクティブでなければならないサービスのパーセンテージのしきい値。                                      |
| 不適切な永続性タイプ       | いいえ          | 仮想サーバでの永続性の使用率が低いかどうかを示します。                                                          |
| サーバーエラー (5xx)    | いいえ          | Web サーバが 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 ADC インスタンスで構成された値を超えた場合の発生を示します。               |
| 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 セッションのビルド    | いいえ          | 一定期間にわたるセッションのビルドアップを示します。これにより、NetScaler ADC インスタンスでこれらのセッションに大量のメモリが保持される可能性があります。 |

| アプリスコアコンポーネント   | ユーザが設定したしきい値 | 説明                                                      |
|-----------------|--------------|---------------------------------------------------------|
| セッションの再利用率が低い   | いいえ          | NetScaler ADC インスタンスによって再使用されるセッションの数が実際の数が多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廃棄されたパケットの合計を示します。                          |
| TCP 再構成キュー制限ヒット | いいえ          | TCP 接続上の順序外パケットが、設定された順序外パケットキューサイズを超えているかどうかを示します。     |

デフォルトでは、すべてのコンポーネントが有効です。いずれかのコンポーネントを無効にすると、NetScaler ADM は選択し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。

注

[アナリティクス] > [設定] に移動して [アプリスコアの構成] をクリックして、引き続きしきい値を構成することもできます。

## マイクロサービスアプリケーションのアプリケーションの詳細

February 6, 2024

ダッシュボードからマイクロサービスアプリケーションをクリックして、詳細情報をドリルダウンします。

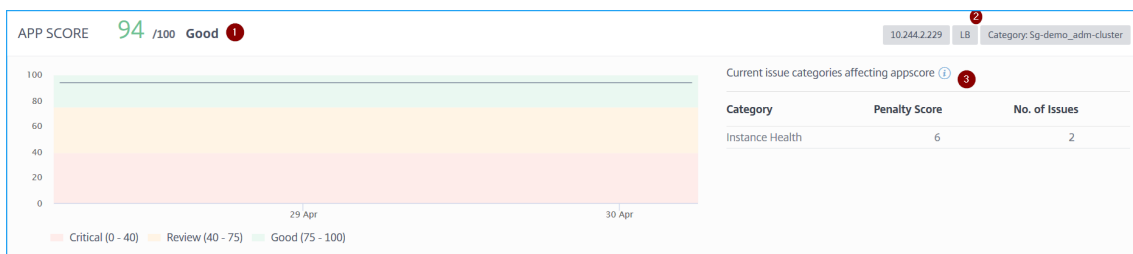
選択したアプリケーションページが表示されます。

アプリケーションの詳細ページから:

- リストから期間を選択すると、特定の期間の詳細が表示されます。
- 「サービス・グラフ」をクリックして、選択したアプリケーションのサービス・グラフを表示します。詳細については、「[アプリケーション用サービスグラフ](#)」を参照してください。
- [ [Transaction Logs](#) ] をクリックすると、選択したアプリケーションの詳細なトランザクションが表示されます。
- [ [監査ログ](#) ] をクリックして、監査ログの詳細情報を表示します。

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。また、現在のアプリケーションの問題も表示できます。これは、問題のカテゴリに基づいて適用可能なペナルティスコアと呼ばれます。最終的なスコアは、ペナルティ合計を差し引いた **100** として計算されます。



**1**—現在のアプリのスコアを示します。

**2**—CPX IP アドレス、負荷分散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、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する問題を示します

このダッシュボードでは、アプリのスコアに影響している現在の問題を表示することもできます。[懸案事項]で懸案の詳細を表示できます。

- **K8S** サービスの詳細

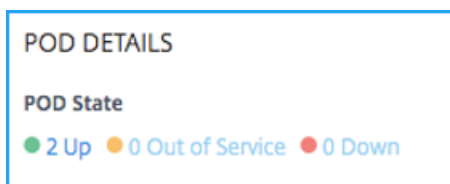
次の詳細を表示できます。

| K8s SERVICE DETAILS |              |           |                                                                          |
|---------------------|--------------|-----------|--------------------------------------------------------------------------|
| Service Name        | Cluster Name | Namespace | Service Labels                                                           |
| tea-beverage        | cluster      | sg-demo   | app: dev-test, service.kubernetes.io/headless: , environment: production |

- [サービス名]—サービス名
- クラスター名—サービスがホストされているクラスター名
- **Namespace**—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

- ポッドの詳細

ポッドは、Kubernetes クラスターでホストされるコンテナのグループです。Pod 内では、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 は IP アドレスに関連付けられています。



ポッドの状態をクリックして詳細を表示します

The screenshot shows the NetScaler ADM interface for a cluster named 'tea-beverage\_sg-demo\_adm-cluster'. The main table displays Pod information:

| POD IP ADDRESS | HOST NAME                    | INSTANCE     | POD STATE |
|----------------|------------------------------|--------------|-----------|
| 10.244.1.157   | cpx-ingress-577bfd945b-f6hlc | 10.244.2.229 | UP        |
| 10.244.2.211   | cpx-ingress-577bfd945b-f6hlc | 10.244.2.229 | UP        |

Summary: Total 2 pods. Pod State: 2 Up, 0 Out of Service, 0 Down. Key Metrics: Response Time 0, 5xx Error 0%.

- ポッド **IP** アドレス—ポッドの IP アドレスを表します。
  - ホスト名—ポッドに割り当てられたホスト名を示します
  - インスタンス—NetScaler ADC CPX の IP アドレスを表します
  - **POD** の状態—Pod の現在の状態を示します
- キー・メトリック—レスポンス時間、**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、データボリュームなどの主要なメトリックの詳細が表示されます。

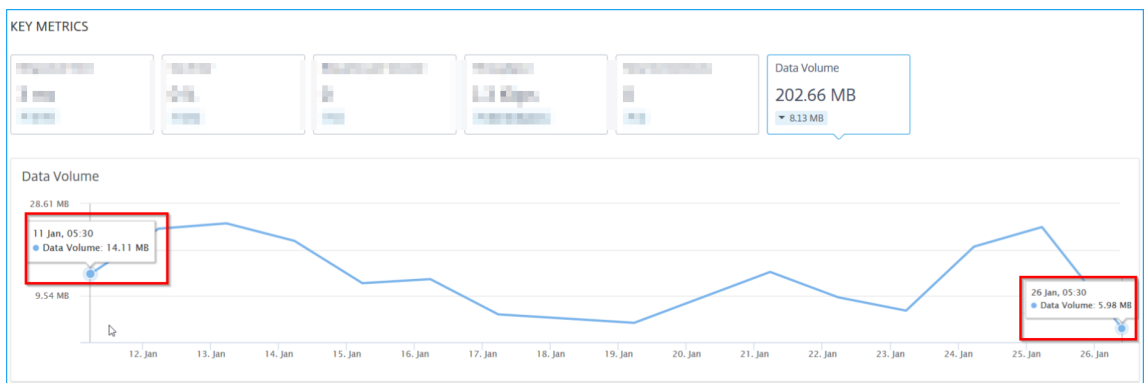
各指標で、選択した期間の平均値と差値を表示できます。差分値は、選択した期間の最初の値から最後の値を引いたものとして計算されます。

選択した期間について、次のインスタンスメトリックスをグラフ形式で表示できます。

The screenshot shows the 'KEY METRICS' section with the following data:

| Response Time | 5xx Error | Requests per Second | Throughput | Client Connections | Server Connections | Data Volume |
|---------------|-----------|---------------------|------------|--------------------|--------------------|-------------|
| 0             | 0%        | 15.3                | 6.5 Kbps   | 0                  | 0                  | 0 Bytes     |

次の図は、データボリュームの例で、選択した期間は 1 か月です。202.66 MB は 1 か月間のデータ量の合計で、8.13 MB という値は差額です。グラフでは、最初の値は 14.11 で、最後の値は 5.98 です。差の値は  $14.11 - 5.98 = 8.13$  MB です。



- [問題] – 選択したアプリケーションに適用可能な問題。次の問題とそのカテゴリを表示できます。

| パフォーマンス          | インスタンスヘルス  | 構成               | システムリソース   |
|------------------|------------|------------------|------------|
| 応答時間             | 平均 CPU 使用率 | 高い 5xx レスポンス     | 不適切な永続性タイプ |
| セッションの再利用が低い     | メモリ使用率     | 異常に大きい HTTP パケット | NIC カードの飽和 |
| サージキューのビルダップ     |            | TCP 再構成キュー制限ヒット  |            |
| SSL リアルタイムトラフィック |            |                  |            |

各問題をクリックすると、次の情報が表示されます。

- 総発生数
- 問題のトラブルシューティングに推奨される処置
- 時間、サービス名、発生回数の合計、重大度、検出メッセージなどの問題の詳細



ISSUES

Current (1) All (3)

|                                                    |      |
|----------------------------------------------------|------|
| Response Time<br>Performance<br>Today at 5:30 AM   | 40   |
| Active Services<br>Performance<br>Today at 5:30 AM | 3.9K |
| Memory Usage<br>Instance Health<br>01/06/2020      | 4    |

**Medium Response Time**

Detects events when application response time to respond for client requests deviates from the configured threshold.

**What Happened**  
App response time for v1 has breached the configured threshold of 500ms.

**No. of occurrences** 40      **Last occurred** Today at 5:30 AM

**Details**

| TIME            | NO OF OCCURRENCES | SEVERITY | DETECTION MSG                                                                  |
|-----------------|-------------------|----------|--------------------------------------------------------------------------------|
| Jan 23 - Jan 24 | 2                 | MEDIUM   | The response time for 37 transactions has exceeded the configured value 500ms. |
| Jan 22 - Jan 23 | 5                 | MEDIUM   | The response time for 37 transactions has exceeded the configured value 500ms. |

- \* 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示しています。
- \* 「すべて」タブに表示される問題は、アプリケーションの問題の合計を示しています。

次の例は、1日間のアプリケーションの問題です。「**Current**」タブには、アプリのスコアに影響する現在の問題がないことが表示されます。

[すべて]タブには、1日間に検出された問題の総数が表示されます。

ISSUES

Current (0) All (3)

|                                                               |    |
|---------------------------------------------------------------|----|
| Response Time<br>Performance<br>01/21/2020                    | 3  |
| Avg CPU Usage<br>Instance Health<br>Last Wednesday at 5:30 AM | 6  |
| Memory Usage<br>Instance Health<br>Last Wednesday at 5:30 AM  | 20 |

**Medium Response Time**

Detects events when application response time to respond for client requests deviates from the configured threshold.

**What Happened**  
App response time for vip150-partition1 has breached the configured threshold of 100ms.

**No. of occurrences** 3      **Last occurred** 01/21/2020

**Details**

| TIME            | NO OF OCCURRENCES | SEVERITY | DETECTION MSG                                                                  |
|-----------------|-------------------|----------|--------------------------------------------------------------------------------|
| Jan 21 - Jan 22 | 3                 | MEDIUM   | The response time for 11 transactions has exceeded the configured value 100ms. |

## Web Insight ダッシュボード

February 6, 2024

改良された Web Insight 機能が拡張され、Web アプリケーション、クライアント、NetScaler ADC インスタンスの詳細なメトリックを可視化できます。この改善された Web Insight により、パフォーマンスと使用率の視点からアプリケーション全体を評価し、視覚化することができます。管理者は、次の対象 Web Insight を表示できます。

- アプリケーション。[ [アプリケーション](#) ] > [ [ダッシュボード](#) ] に移動し、アプリケーションをクリックし、[ **Web Insight** ] タブを選択して詳細なメトリックスを表示します。詳細については、「[アプリケーション使用状況分析](#)」を参照してください。
- すべてのアプリケーション。[ [アプリケーション](#) ] > [ **Web Insight** ] に移動し、各タブ ([ [アプリケーション](#) ]、[ [クライアント](#) ]、[ [インスタンス](#) ]) をクリックして、次のメトリックを表示します。

| アプリケーション    | クライアント       | インスタンス                    |
|-------------|--------------|---------------------------|
| アプリケーション    | クライアント       | インスタンス・メトリック              |
| サーバー        | 地理的場所        | アプリケーション                  |
| ドメイン        | HTTP 要求メソッド  | ドメイン                      |
| 地理的場所       | HTTP 応答の状態   | URL                       |
| URL         | URL          | HTTP 要求メソッド               |
| HTTP 要求メソッド | オペレーティングシステム | HTTP 応答の状態                |
| HTTP 応答の状態  | Web ブラウザー    | クライアント                    |
| SSL エラー     | SSL エラー      | サーバー                      |
| SSL の使用状況   | SSL の使用状況    | オペレーティングシステム<br>Web ブラウザー |

Applications Clients Instances
Last 1 Month

---

### Applications

Top apps with high bandwidth and response time

Requests | Bandwidth | Response Time

| APPLICATION              | BANDWIDTH (AVG) | RESPONSE TIME (AVG) | REQUESTS |
|--------------------------|-----------------|---------------------|----------|
| fb_114                   | 9.15 MB         | 923 ms              | 14.9K    |
| SSL_VS                   | 0 Bytes         | <1 ms               | 121      |
| test_vs_ssl              | 0 Bytes         | <1 ms               | 121      |
| k8s-10.244.2.112_80_http | 55.07 KB        | 20 ms               | 81       |
| vpn_gw                   | 0 Bytes         | <1 ms               | 12       |

[See more](#)

### Servers

Unique servers accessing the application

Requests | Server Network Latency | Server Response Time | Bandwidth

| SERVER         | SERVER NETWORK LATENCY (L) | REQUESTS |
|----------------|----------------------------|----------|
| 10.102.103.113 | 921 ms                     | 14.9K    |
| 10.102.71.225  | <1 ms                      | 121      |
| 10.102.71.226  | <1 ms                      | 121      |
| 10.244.1.95    | <1 ms                      | 23       |
| 10.102.71.228  | <1 ms                      | 12       |

[See more](#)

### Domains

Top domains

Requests | Bandwidth | Response Time

| DOMAIN                     | BANDWIDTH (AVG) | REQUESTS |
|----------------------------|-----------------|----------|
| 10.102.103.99              | 8.51 MB         | 14.4K    |
| --NA--                     | 513.6 KB        | 453      |
| 10.102.103.99:80           | 62.67 KB        | 52       |
| netflix-frontend-service   | 14.82 KB        | 23       |
| recommendation-engine s... | 8.75 KB         | 12       |

[See more](#)

### Geo Locations


Locations from where the clients/users are accessing the applications

Total Locations: 1 | Response Time: 20.51 s (max) | Bandwidth: 16.56 MB (total) | Requests: 15.3K (total)

Requests | Response Time | Bandwidth

| LOCATION | RESPONSE TIME | BANDWIDTH | REQUESTS |
|----------|---------------|-----------|----------|
| *        | 95 ms         | 16.56 MB  | 15.3K    |

[See more](#)



### URLs

Top urls with high load time and render time

Total Urls: 5.7K | Load Time: <1 ms (max) | Render Time: <1 ms (max)

Requests | Load Time | Render Time

| URL                          | LOAD TIME (AVG) | RENDER TIME (AVG) | REQUESTS |
|------------------------------|-----------------|-------------------|----------|
| /                            | <1 ms           | <1 ms             | 446      |
| /console/login/LoginForm.jsp | <1 ms           | <1 ms             | 139      |
| /index.php                   | <1 ms           | <1 ms             | 116      |
| /q?w_38jg_...html            | <1 ms           | <1 ms             | 96       |
| /admin_u/mas/ent/login.html  | <1 ms           | <1 ms             | 79       |

[See more](#)

### HTTP Request Methods

Indicates HTTP request methods used to access the applications

| REQUEST METHODS | BANDWIDTH | NO. OF OCCURRENCES |
|-----------------|-----------|--------------------|
| GET             | 8.65 MB   | 14.5K              |
| POST            | 459.6 KB  | 368                |
| Unknown         | 35.85 KB  | 324                |
| HEAD            | 17.1 KB   | 39                 |
| OPTIONS         | 35.1 KB   | 18                 |

[See more](#)

### HTTP Response Status

Indicates if a specific HTTP request has been successfully completed

| RESPONSE STATUS | RESPONSE STATUS REASON | NO. OF OCCURRENCES |
|-----------------|------------------------|--------------------|
| 404             | Not Found              | 12.2K              |
| 401             | Unauthorized           | 2.2K               |
| 302             | Found                  | 337                |
| 0               | Unknown                | 254                |
| 200             | OK                     | 152                |

[See more](#)

### SSL Errors

SSL failure on frontend and backend

Total Errors: 254 | Frontend Errors: 254 | Backend Errors: 0

Frontend | Backend

| SSL FAILURE TYPE   | NO. OF OCCURRENCES |
|--------------------|--------------------|
| HANDSHAKE FAILURE  | 152                |
| PROTOCOL VERSION   | 54                 |
| CLIENTAUTH FAILURE | 18                 |
| NA                 | 18                 |
| ILLEGAL PARAMETER  | 6                  |


[See more](#)

### SSL Usage

SSL usage by certificates, protocols, ciphers negotiated and key strength

Certificates: 0 | Protocols: 0 | Ciphers: 0 | Key Strength: 0

Certificates | Protocols | Ciphers | Key Strength

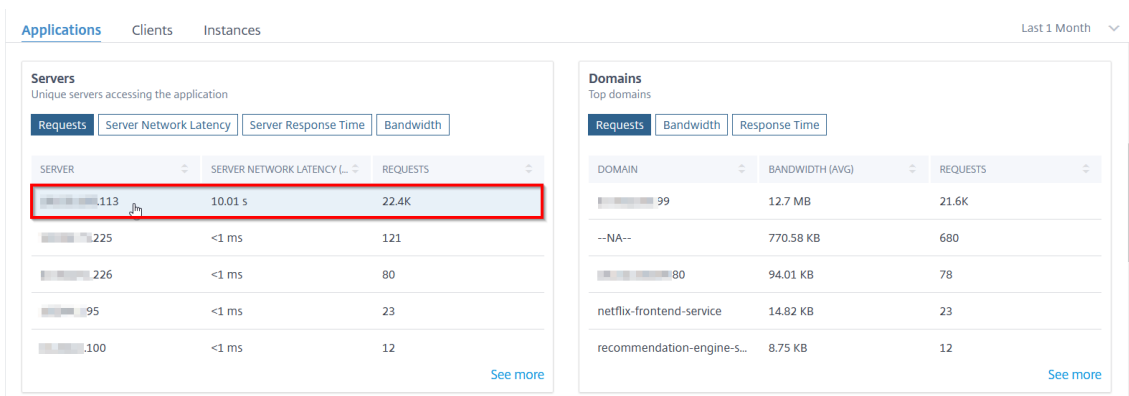


No data available.

各指標で、上位 5 つの結果を表示できます。をクリックしてさらにドリルダウンして、問題を分析し、トラブルシューティングアクションを迅速に行うことができます。

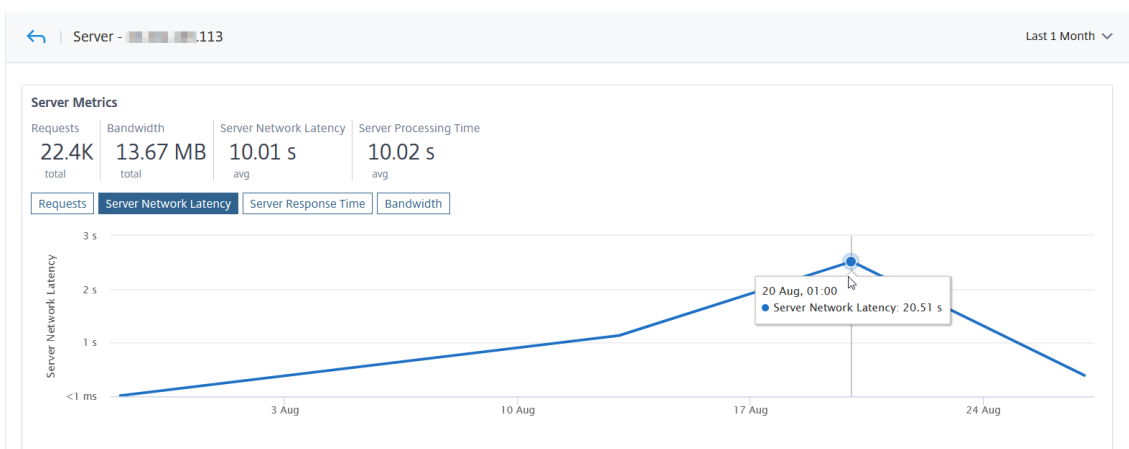
たとえば、1 か月間のサーバーネットワーク遅延を分析し、運用環境をスケールアップするかスケールダウンするかを決定するとします。これを分析するには：

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] まで下にスクロールし、サーバーをクリックします。



選択したサーバーのメトリックの詳細が表示されます。

2. [サーバーネットワーク遅延] タブを選択して、遅延を分析します。



平均レイテンシーは 10.01 秒を示し、グラフから、過去 1 か月のサーバーネットワークのレイテンシーが高いと思われることを分析できます。管理者は、本番環境のスケールアップを決定できます。

Web Insight のユースケースの詳細については、[Web Insight](#)を参照してください。

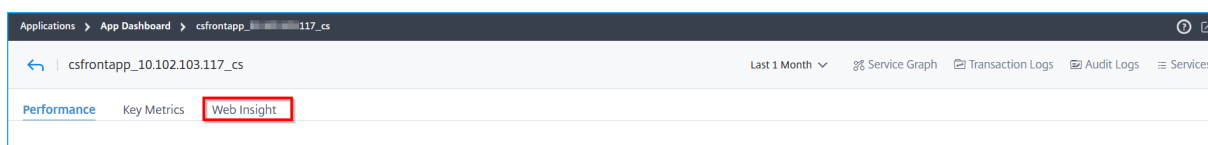
## アプリケーション使用状況の分析

February 6, 2024

アプリケーション所有者は、パフォーマンスと使用の観点からアプリケーション全体を評価し、視覚化する能力を持っている必要があります。

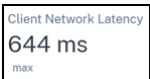

即興の **App Dashboard** を使用すると、すべてのアプリケーションパフォーマンスと使用状況メトリクスをまとめて表示できます。既存のアプリケーション・パフォーマンス・メトリックとともに、アプリケーションをクリックすると、「**Web Insight**」タブにメトリックの詳細が表示されます。

- アプリケーションの使用状況を理解します。
- パフォーマンスの偏差と使用状況の指標を関連付けます。



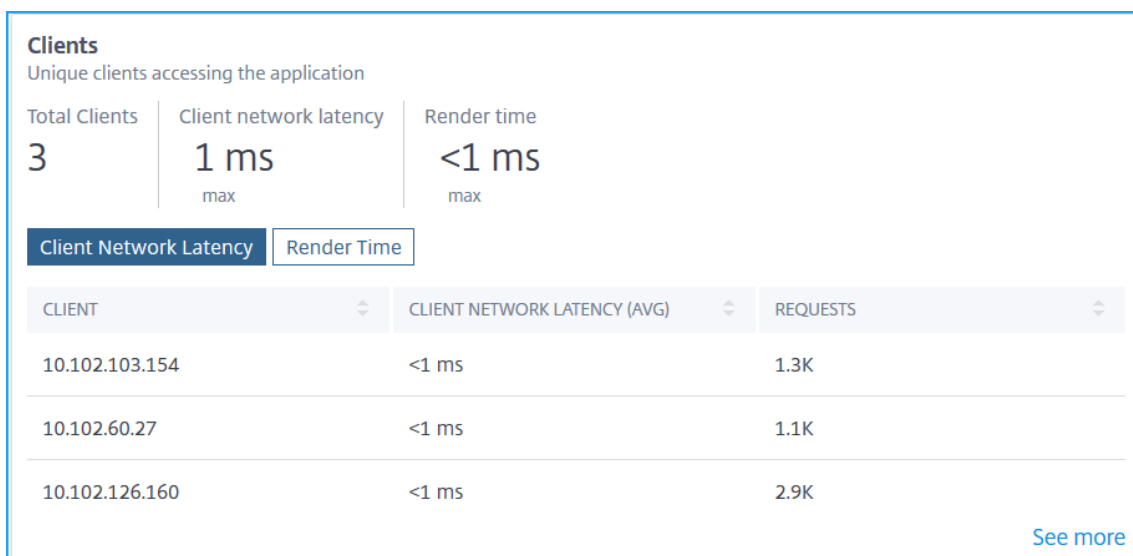
### 注

各メトリックについて、最大値と合計値を示すオプションを表示できます。例：

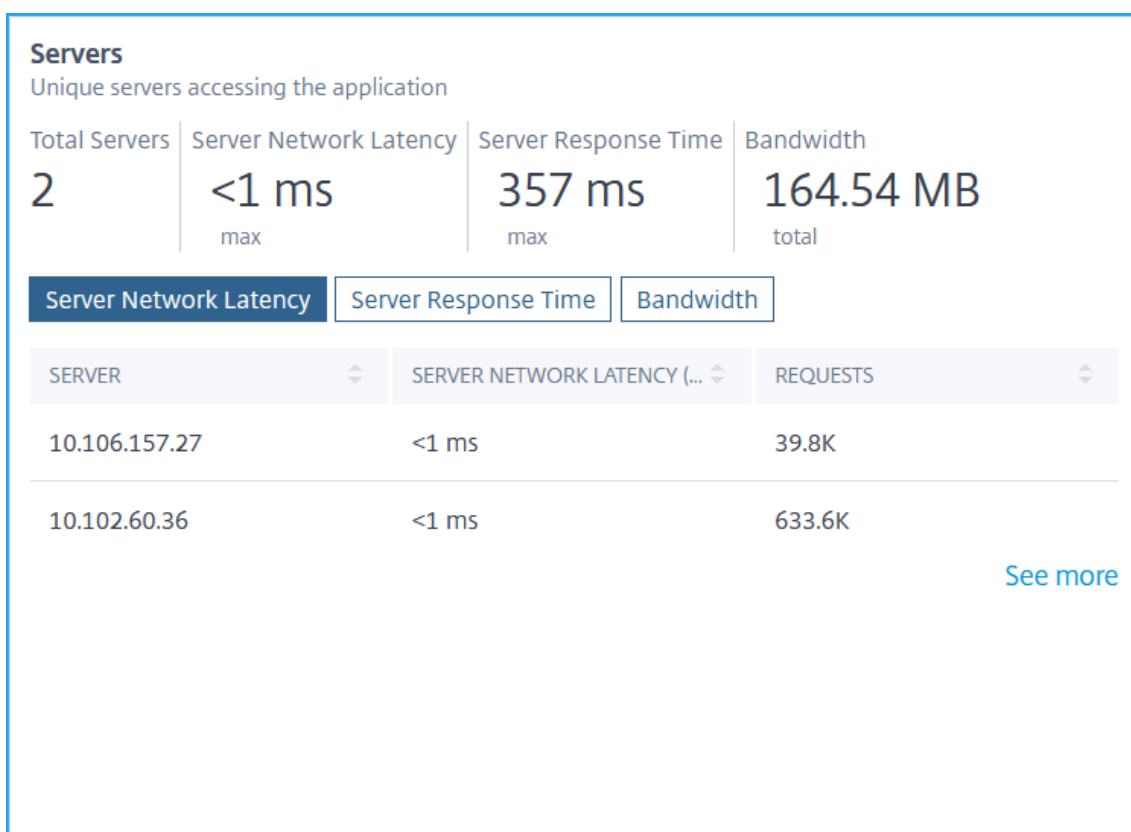
-  - 選択した期間における最大クライアント・ネットワーク・レイテンシークライアント 1 = 30 ミリ秒、クライアント 2 = 15 ミリ秒、クライアント 3 = 3 ミリ秒のネットワーク遅延があるとした場合。このシナリオでは、クライアントネットワーク遅延は 30 ミリ秒と表示されます。
- 。クライアント 1 = 30 MB、クライアント 2 = 45 MB、クライアント 3 = 40 MB の帯域幅消費があるとした場合。このシナリオでは、帯域幅が表示されます (30 MB + 45 MB + 40 MB) = 115 MB。

[使用状況] タブに表示できる Web Insight メトリックスを次に示します。

- 「クライアント」 - アプリケーションにアクセスするクライアントのインサイトを表示します。



- 「合計クライアント」 - アプリケーションにアクセスしているクライアントの合計が表示されます。
- [クライアントネットワーク遅延]: クライアントから NetScaler ADC 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、次の項目を表示します。
  - \* 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です。
  - \* [Requests] - クライアントからのリクエストの合計です。
- 「レンダリング時間」 (Render Time) - サーバーの応答をレンダリングするのに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、次の項目を表示します。
  - \* 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。
  - \* [Requests] - クライアントからのリクエストの合計です。
- サーバー - アプリケーションにアクセスするサーバーのインサイトを表示します。



- **[Total Servers]**: アプリケーションにアクセスしているサーバの合計が表示されます。
- 「サーバーのネットワーク遅延」-サーバーから NetScaler ADC へのネットワーク遅延を表示します。[サーバーネットワーク遅延] タブをクリックして、次の項目を表示します。
  - \* 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です。
  - \* [要求] -サーバーからのリクエストの合計です。
- 「サーバー応答時間」-サーバーが要求に回答するのに要した時間を表示します。[サーバー応答時間] タブをクリックして、次の項目を表示します。
  - \* サーバー-サーバーの IP アドレス。
  - \* 応答時間 (平均): サーバからの平均応答時間。
  - \* [要求] -サーバーからのリクエストの合計です。
- **[Bandwidth]**: サーバによって消費された合計帯域幅を表示します。[帯域幅] タブをクリックして、次の項目を表示します。
  - \* サーバー-サーバーの IP アドレス。
  - \* 帯域幅: サーバから消費された合計帯域幅。

\* [要求] –サーバーからのリクエストの合計です。

- 地理的場所—特定の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のインサイトを表示します。

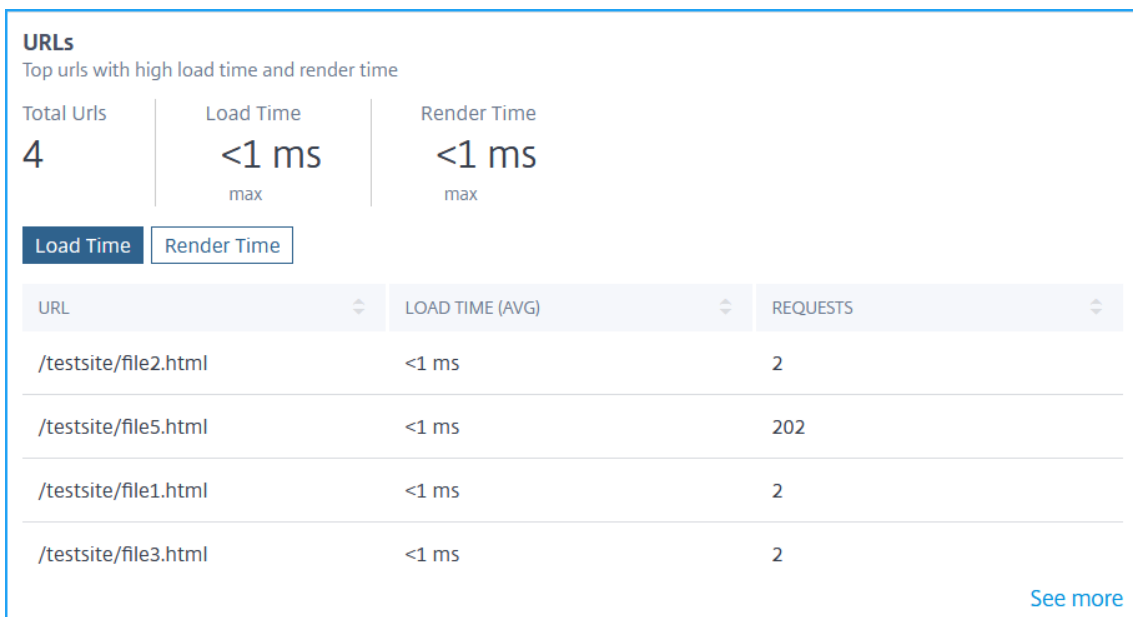


- ロケーションの合計—アプリケーションにアクセスしているクライアントのロケーションの合計数を表示します。
- [応答時間]: クライアントの場所からの応答時間を表示します。
- 帯域幅—すべての場所でクライアントが消費した合計帯域幅を表示します。
- [Requests]: すべてのクライアントロケーションからの要求の合計を表示します。

各タブをクリックすると、次の項目が表示されます。

- \* 「場所」—場所の名前。
- \* [応答時間]: クライアントの場所からの平均応答時間。
- \* **Bandwidth**: クライアントのロケーションから消費される帯域幅。
- \* [Requests] —クライアントロケーションからのリクエストの合計です。

- 「URL」—負荷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。





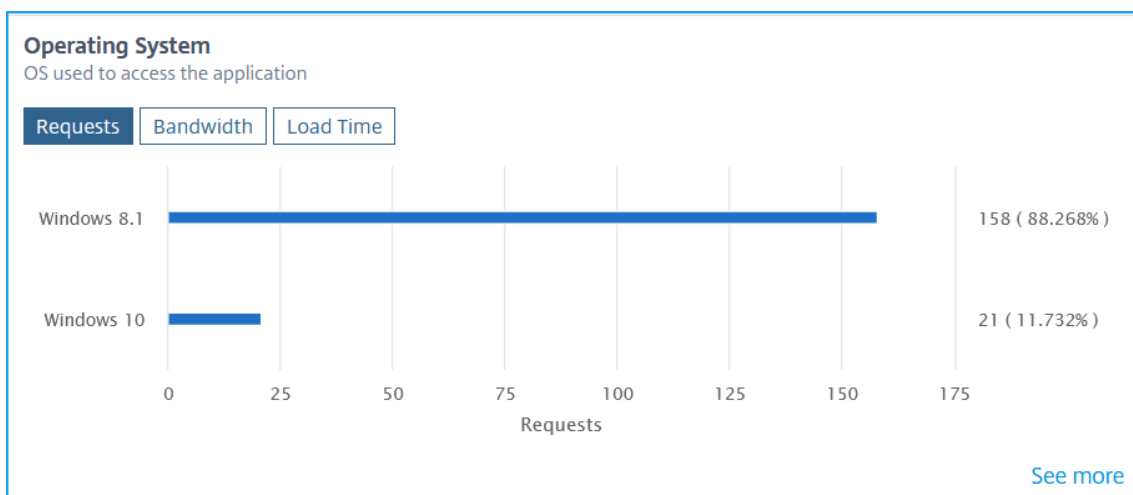
- 「合計 **URL**」 -合計 URL を表示します。
- 「ロード時間」-URL のロードにかかった時間を表示します。[ ロード時間] タブをクリックして、次の項目を表示します。
  - \* 「**URL**」 -URL 名。
  - \* 読み込み時間 (平均) -URL の読み込みにかかった平均時間。
  - \* リクエスト-URL からのリクエストの合計です。
- 「レンダリング時間」 (Render Time)-URL のレンダリングおよび表示にかかった時間を表示します。[ レンダリング時間] タブをクリックして、次の項目を表示します。
  - \* 「**URL**」 -URL 名。
  - \* レンダリング時間 (平均) -URL のレンダリングにかかった平均時間。
  - \* リクエスト-URL からのリクエストの合計です。
- 「**HTTP** 応答ステータス」 -完了した HTTP リクエストのインサイトを表示します。

**HTTP Response Status**  
Indicates if a specific HTTP request has been successfully completed

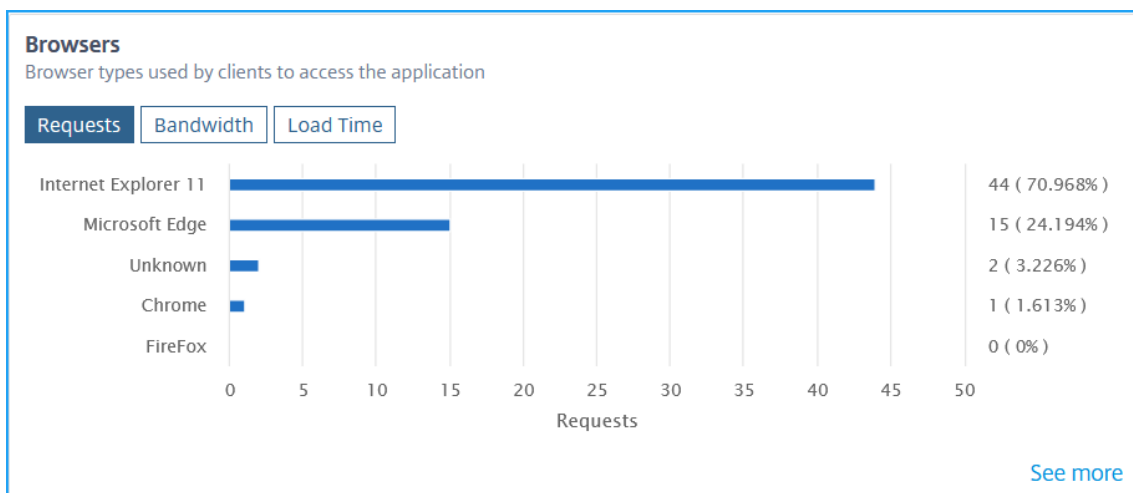
| RESPONSE STATUS | RESPONSE STATUS REASON | NO. OF OCCURENCES |
|-----------------|------------------------|-------------------|
| 200             | OK                     | 202               |
| 500             | Internal Server Error  | 6                 |

[See more](#)

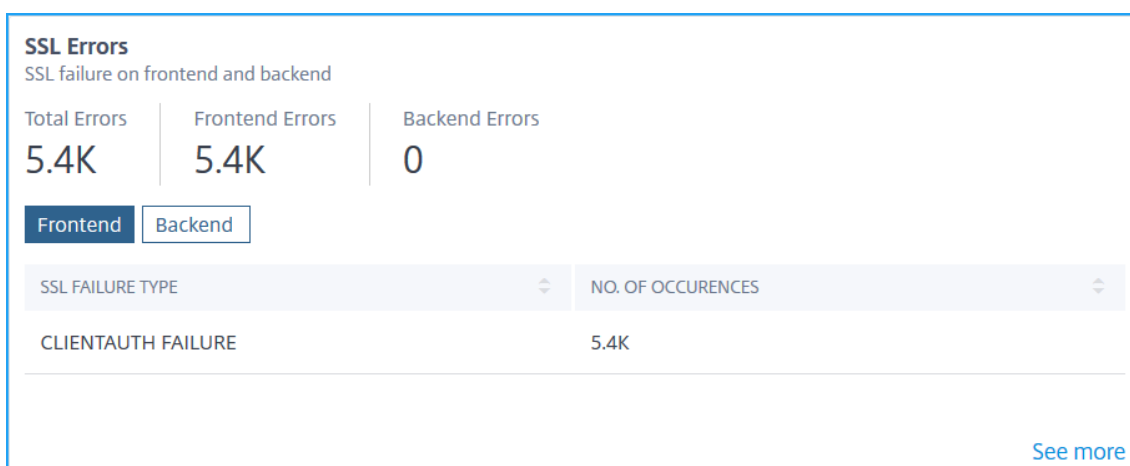
- [応答ステータス]: 2xx、4xx、5xx などの応答コードを表示します。
- 「応答ステータスの理由」 -内部サーバーエラー、見つからないなどの応答理由を表示します。
- 「オカレンスの数」-オカレンスの合計数を表示します。
- オペレーティングシステム-アプリケーションにアクセスする OS のインサイトを表示します。



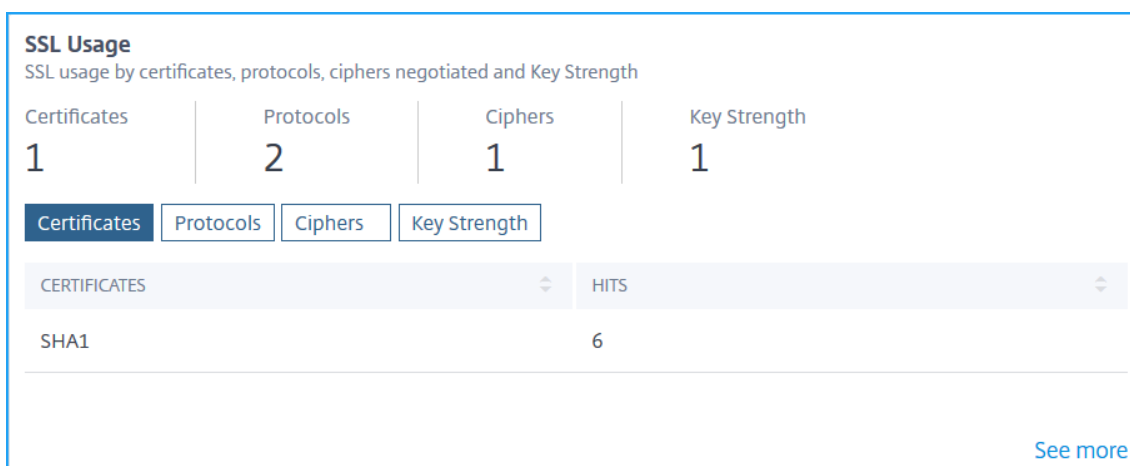
- 「**Requests**」 - 各オペレーティングシステムからのリクエストの合計を表示します。
  - [**Bandwidth**]: 各オペレーティングシステムによって消費された合計帯域幅を表示します。
  - 「ロード時間」 - 各オペレーティングシステムからサーバーからロードされた合計時間が表示されます。
- 「ブラウザ」 - アプリケーションにアクセスするためにクライアントが使用するブラウザの種類に関するインサイトが表示されます。



- 「要求」 - 各ブラウザからのリクエストの合計を表示します。
  - [**Bandwidth**]: 各ブラウザによって消費された合計帯域幅が表示されます。
  - 「読み込み時間」 - ブラウザーがサーバーからロードされるまでに要した合計時間を表示します。
- [**SSL エラー**] - フロントエンドサーバーとバックエンドサーバーからの SSL エラーに関するインサイトを表示します。



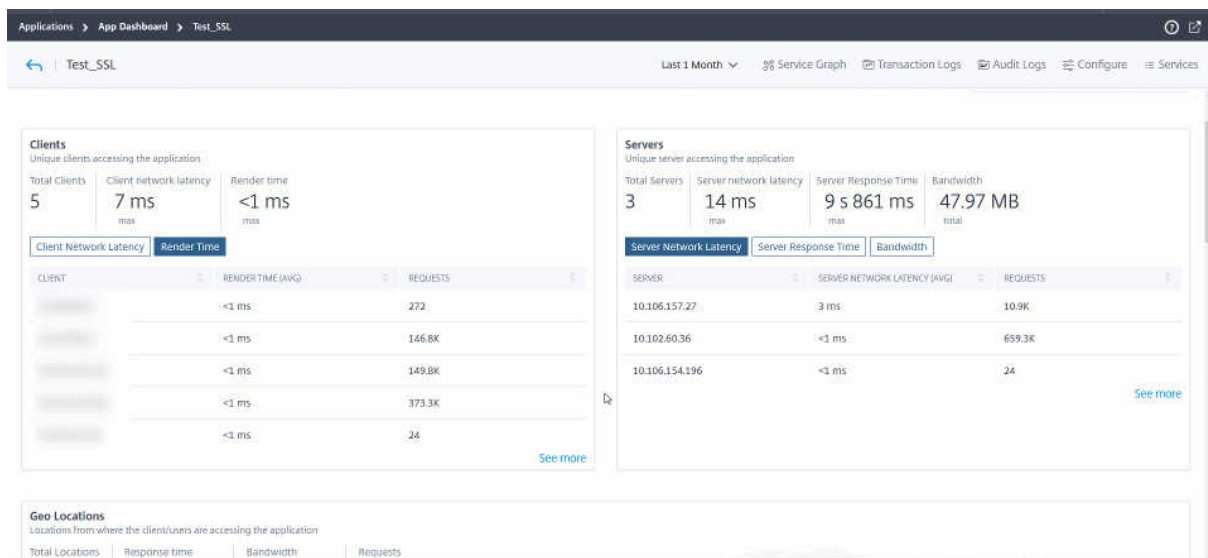
- 「エラーの合計」 - SSL エラー発生の合計を表示します。
  - 「フロントエンド」 - フロントエンドサーバーからの SSL エラーの合計を表示します。[フロントエンド] タブをクリックして、SSL エラータイプと合計発生回数を表示します。
  - バックエンド: バックエンドサーバからの SSL エラーの合計を表示します。[バックエンド] タブをクリックして、SSL エラータイプと発生の合計を表示します。
- **[SSL 使用状況]** - SSL 証明書、プロトコル、暗号、キー強度などの SSL 使用状況に関するインサイトを表示します。



- 「証明書」 - SSL 証明書の合計を表示します。[ **Certificates** ] タブをクリックして、証明書の名前と合計ヒット数を表示します。
- [**Protocols**]: SSL プロトコルの合計を表示します。[ **Protocols** ] 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」 - 暗号の合計を表示します。[ **Ciphers** ] 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 証明書で使用されるキーの強度の合計を表示します。[ キー強度 ] タブをクリックして、各キー強度とヒット数の合計の詳細を表示します。

メトリックスの詳細をグラフ形式で表示

各指標について、[詳細を表示] オプションをクリックすると、詳細をグラフィカル形式で表示できます。詳細をグラフィカル形式で表示するには、[>] をクリックします。



[詳細を表示] オプションをクリックした後、各メトリックについて表示できる詳細を次に示します。

| インサイト名 | メトリックス | 説明 |

|---|---|---|

|\*\* クライアント \*\*| クライアント | クライアントリストを示します |

|| レンダリング時間 (平均)| クライアントがサーバの応答をレンダリングするのにかかった平均時間を示します |

|| クライアントネットワーク遅延 (AVG) | クライアントから NetScaler ADC インスタンスまでの平均ネットワーク遅延を示します。 |

|| リクエスト | クライアントからのリクエストの合計を示します。 |

|\*\* サーバー \*\*| サーバー | サーバーリストを示します |

|| サーバー処理時間 (平均)| サーバーが要求を処理するのに要した平均時間を示します |

|| サーバーネットワーク遅延 (AVG) | サーバーから NetScaler ADC インスタンスまでの平均ネットワーク待ち時間を示します |

|| ヒット数 | サーバーが受信した総ヒット数を示します |

|\*\* 地理的位置 \*\*| 所在地 | クライアントの場所を示します |

|| 応答時間 | クライアントの場所からの合計応答時間を示します |

|| 帯域幅 | ロケーションから消費された合計帯域幅を示します。 |

|| リクエスト | ロケーションからのリクエストの合計を示します |

|\*\*URL\*\* | レンダリング時間 (平均) | サーバーからページをロードするのに要した平均時間を示します |

|| ロード時間 (平均)| URL のレンダリングと表示に要した平均時間を示します |

|| ヒット数 | URL からの総ヒット数を示します |

|\*\*HTTP 応答の状態 \*\*| 名前 | 「OK」、「見つかりません」、「内部サーバーエラー」などの応答ステータス名を表します。 |

|| 回答状況 | サーバから受信した応答ステータスコード (200、400、500 など) を示します。 | |
|| ヒット数 | レスポンスコードからの総ヒット数を示します。 |  
|| 帯域幅 | 消費された総帯域幅を示します |  
|| \*\* オペレーティングシステム \*\* | オペレーティングシステム |Windows、MAC などのオペレーティングシステム名を示します。 |  
|| ロード時間 | オペレーティングシステムがサーバーからロードされるまでに要し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リクエストの合計を示します |  
|| \*\*Web ブラウザー \*\* |Web ブラウザー |Mozilla Firefox や Chrome などのブラウザ名を表します |  
|| ロード時間 | ブラウザがサーバーからロードするのに要し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総帯域幅を示します |  
|| 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 |  
|| オカレンス |SSL エラーの総発生回数を示します。 |  
|| **SSL** 使用法 | プロトコル名とバージョン (TLS、SSL など) を示します |  
|| ヒット | プロトコルからの総ヒット数を示します |

Web Insight のユースケースの詳細については、「[Web Insight](#)」を参照してください。

## アプリダッシュボードのトラブルシューティング

February 6, 2024

アプリケーション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ケーションの基本構成の詳細がすぐに表示されます。アプリスコア、主要指標、問題などのアプリケーション分析の詳細が、数分 (約 10 ~ 15 分) 以内に読み込まれます。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 ADC インスタンスからのメトリクスデータフロー (AppFlow コレクターまたはアナリティクスプロファイル) 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の詳細については、このドキュメントを参照してください。

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。

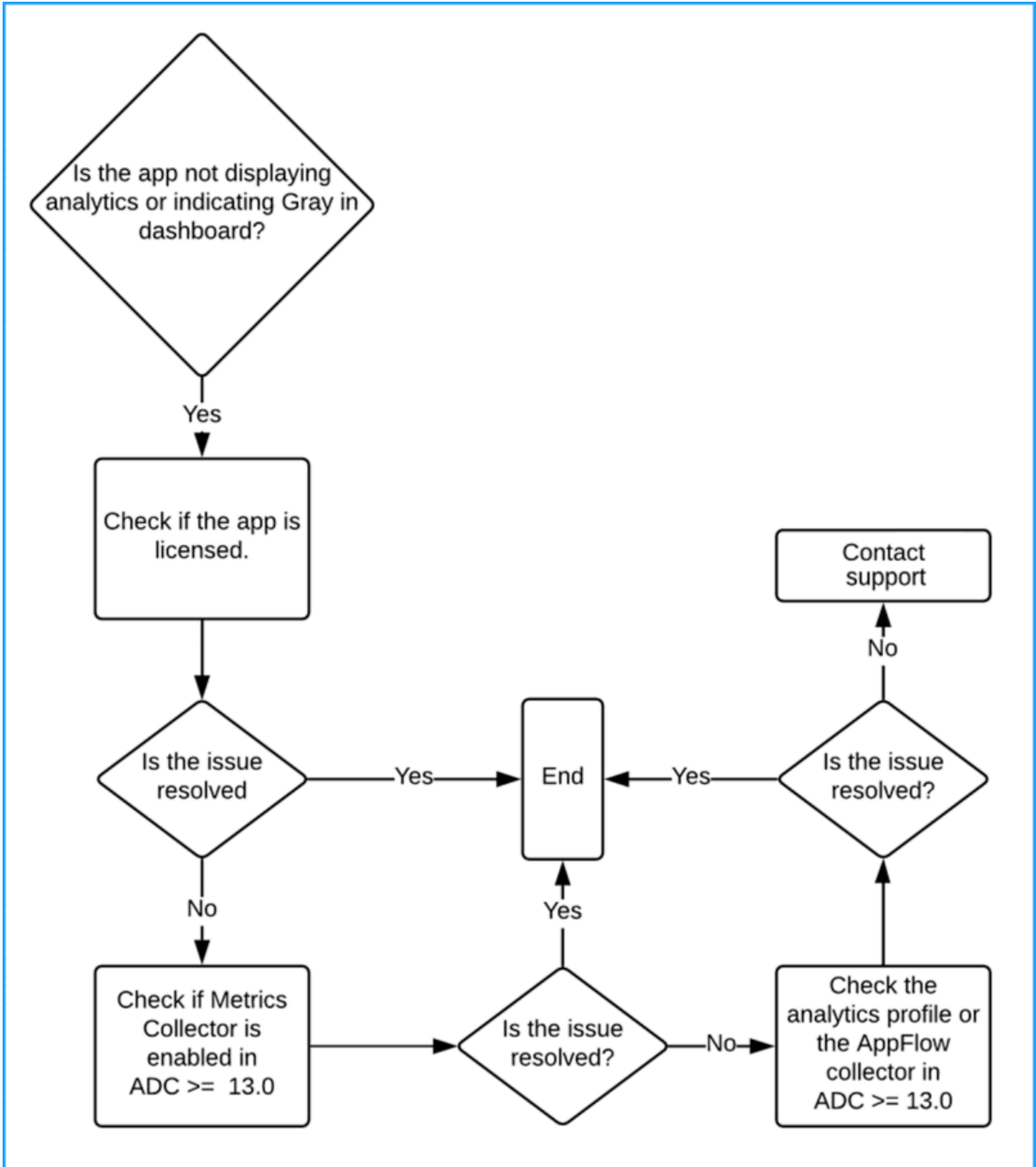
- アプリケーションをクリックすると、指定した期間 (10 ~ 15 分) の後でも、選択したアプリケーションの分析に必要なデータが表示されません。
- CS または LB アプリケーションは、アプリケーションダッシュボードで常に灰色 (適用不可ステータス) を示します。

### 注

この文書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

バにのみ適用されます。

トラブルシューティングのシナリオ



アプリケーションはライセンス供与されています

アプリケーションがライセンスされているかどうかを確認する必要があります。

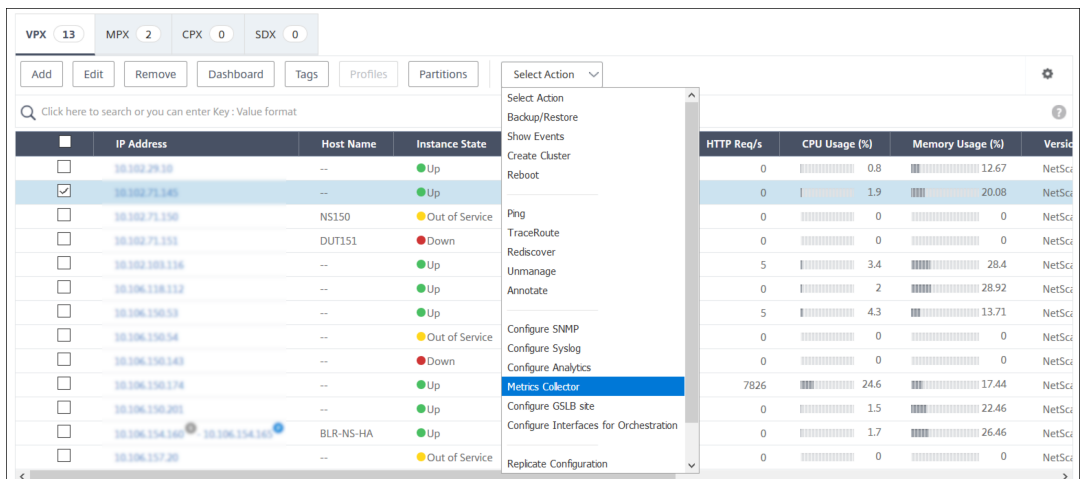
- **ADM** サービス - [アカウント] > [サブスクリプション] に移動し、[仮想サーバーライセンスの概要] でアプリケーションがライセンスされているかどうかを確認します。アプリケーションにライセンスが付与されていない場合は、「[ライセンスの管理と仮想サーバーでの分析の有効化](#)」を参照して、仮想サーバーにライセンスを付与します。
- **ADM** オンプレム - [システム] > [ライセンス & 分析] に移動し、[仮想サーバーライセンスの概要] でアプリケーションがライセンスされているかどうかを確認します。アプリケーションにライセンスが付与されていない場合は、「[ライセ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、仮想サーバーにライセンスを付与します。

メトリクスコレクタが有効です

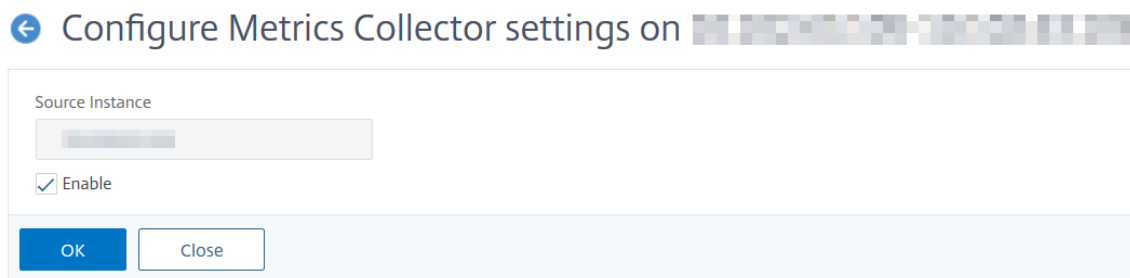
NetScaler ADC インスタンスでメトリクスコレクタが有効になっているかどうかを確認する必要があります。

NetScaler ADC バージョン 13.0 以降では、ADC インスタンスが ADM に正常に追加されると、メトリックコレクターがデフォルトで有効になります。メトリック・コレクタが有効になっているかどうかを確認するには、次の手順に従います。

1. [ネットワーク] > [インスタンス] に移動します。[インスタンス] で、インスタンスの種類 (NetScaler ADC VPX など) を選択します。
2. NetScaler ADC インスタンスを選択します。
  - a) 「アクションの選択」リストから、「メトリック・コレクター」を選択します。



3. 「メトリック・コレクタ設定の構成」ページで、「有効」オプションが選択されていることを確認します。そうでない場合は、「有効」オプションを選択し、「OK」をクリックします。



メトリック・コレクタを有効にした後でデータを表示できない場合は、次のことを検証します。

- **47.x** ビルドより前の **CitrixADC** インスタンスバージョン **13.0** の AppFlow コレクター。
- Citrix ADC インスタンスビルド **47.x** 以降の分析プロファイル。

### NetScaler ADC インスタンスの以前のビルド

NetScaler ADC の場合:

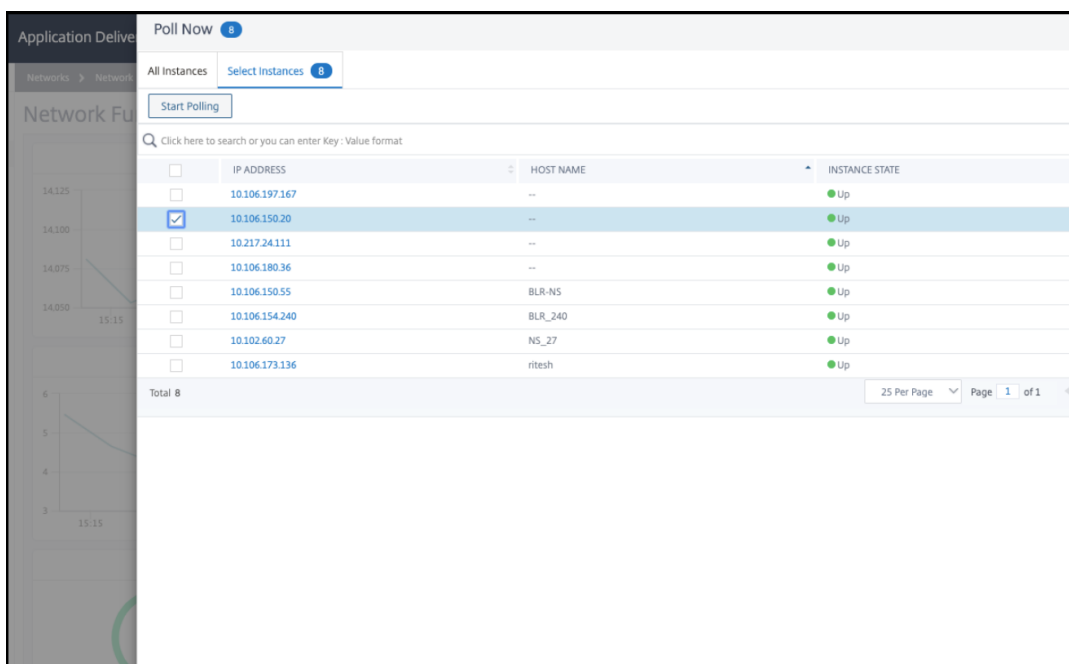
1. 次のコマンドを実行して、コレクタが起動し、ポート 5563 で実行されていることを確認します。

```
sh appflow collector af_collector_rest_<adm_receiver_ip>
```

```
> sh appflow collector af_collector_rest_10.102.103.114
1) Name: af_collector_rest_10.102.103.114
IPv4 address: 10.102.103.114
Port: 5563
Netprofile:
Transport: rest
State: UP
Done
```

2. 使用可能なコレクタがない場合は、NetScaler ADM でインスタンスの手動ポーリングを実行します。
  - a) [ネットワーク] > [ネットワーク機能] > [今すぐ投票] に移動します
  - b) インスタンスを選択し、[ **Start Polling** ] をクリックします。





ポーリングに失敗した場合は、ADM から ADC インスタンスを削除してから、もう一度 ADC インスタンスを追加します。ADC インスタンスを追加すると、コレクタは ADC に追加されます。

コレクタに「Down」ステータスが表示されている場合：

1. SNIP が構成されているかどうかを確認します。

```
> sh ip | grep SNIP
2) 10.106.150.34 0 SNIP Active Enabled Enabled NA Enabled
```

SNIP が構成されていない場合は、SNIP を構成する必要があります。詳細については、「[SNIP の構成](#)」を参照してください。

2. ADC インスタンスが ADM に到達可能であることを確認してください。

ping テストを実行することで検証できます。ping -S <SNIP> <adm\_receiver\_ip>を実行します

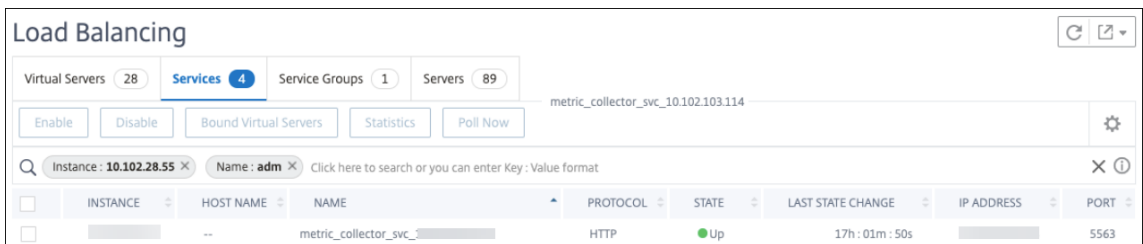
```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

### NetScaler ADC インスタンスは後でビルド

NetScaler ADM で、メトリクスコレクタサービスが使用可能であることを確認します。

1. [ネットワーク] > [ネットワーク機能] > [負荷分散] > [サービス] に移動します。
2. 検索バーで、[インスタンス:(IP アドレス)] と [名前:ADM] でフィルタリングします。
3. `adm_metric_collector_svc_<adm_receiver ip>` が使用可能かどうか確認します。IP アドレスは、ADM 管理 IP またはエージェント IP のいずれかになります。

このサービスが **UP** ステータスで、ポート 5563 で実行されていることを確認します。



それでもデータを表示できない場合は、コレクタサービスが NetScaler ADC 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ます。

1. NetScaler ADC にログオンする
2. 次のコマンドを実行します:

```
sh analytics profile ns_analytics_time_series_profile
```

```
> sh analytics profile ns_analytics_time_series_profile
1) Name: ns_analytics_time_series_profile
   Collector: adm_metric_collector_svc_10.102.103.114
   Profile-type: timeseries
      Output Mode: avro
      Metrics: ENABLED
      Events: ENABLED
      Auditlog: DISABLED
      Reference Count: 0
Done
```

コレクタに「**Down**」ステータスが表示されている場合:

1. SNIP が構成されているかどうかを確認します。

```
> sh ip | grep SNIP
2) 10.106.150.34 0 SNIP Active Enabled Enabled NA Enabled
```

SNIP が構成されていない場合は、SNIP を構成する必要があります。詳細については、「[SNIP の構成](#)」を参照してください。

2. ADC インスタンスが ADM に到達可能であることを確認してください。

ping テストを実行することで検証できます。ping -S <SNIP> <adm\_receiver\_ip>を実行します

```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

3. Telnet を介したトラフィック接続がサービスを接続できることを確認します。

```
root@ns# telnet 10.102.103.114 5563
Trying 10.102.103.114...
Connected to 10.102.103.114.
Escape character is '^]'.
^]
telnet> q
Connection closed.
```

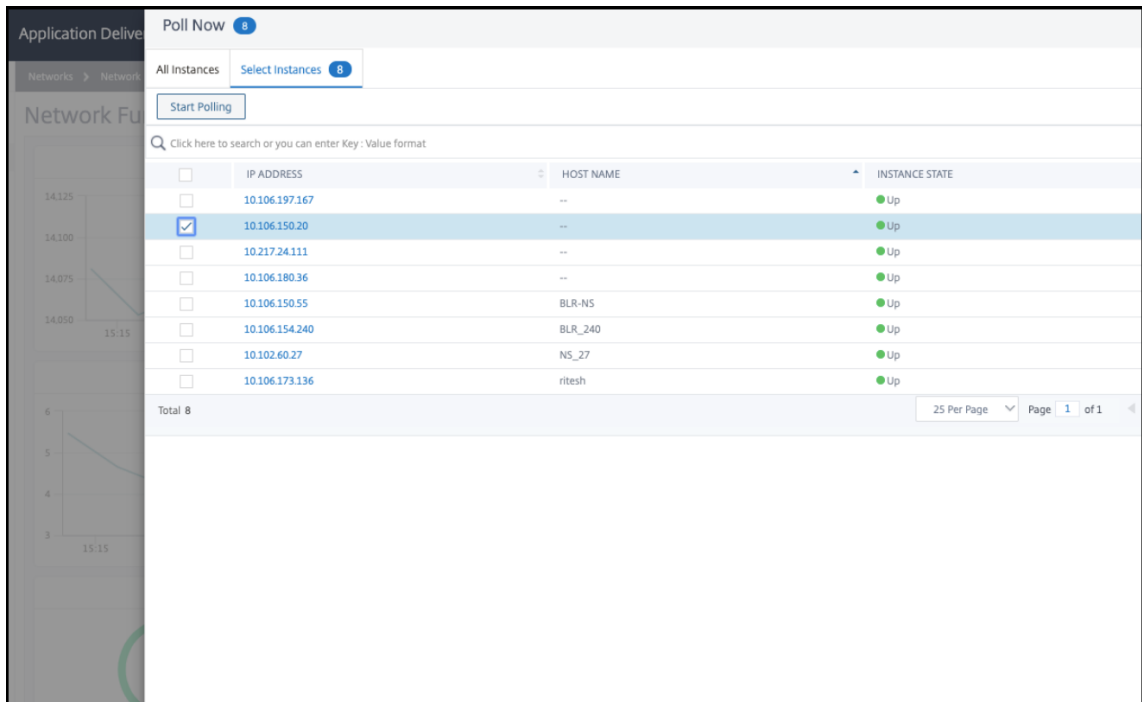
telnet がサービスに接続できる場合は、ファイアウォールが存在し、メトリックデータフローをブロックしています。ファイアウォールブロックの問題を解決する必要があります。

NetScaler ADC で時系列分析プロファイルにコレクタサービスがバインドされていない場合、コレクタは空白として表示されます。

```
> sh analytics profile ns_analytics_time_series_profile
1) Name: ns_analytics_time_series_profile
Collector:
Profile-type: timeseries
  Output Mode: avro
  Metrics: ENABLED
  Events: ENABLED
  Auditlog: DISABLED
Reference Count: 0
Done
```

NetScaler ADM でインスタンスの手動ポーリングを実行する必要があります。

1. [ ネットワーク ] > [ ネットワーク機能 ] > [ 今すぐ投票 ] に移動します
2. インスタンスを選択し、[ **Start Polling** ] をクリックします。



ポーリングが失敗した場合は、次のコマンドを使用して、NetScaler ADC インスタンスでコレクタ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。

```
> add service adm_metric_collector_svc_10.102.103.114 10.102.103.114 HTTP 5563
Done
> unset analyticsprofile ns_analytics_time_series_profile -collectors
Done
> set analytics profile ns_analytics_time_series_profile -collectors adm_metric_collector_svc_10.102.103.114 -metrics enabled -events enabled
Done
> sh analytics profile ns_analytics_time_series_profile
1) Name: ns_analytics_time_series_profile
   Collector: adm_metric_collector_svc_10.102.103.114
   Profile-type: timeseries
     Output Mode: avro
     Metrics: ENABLED
     Events: ENABLED
     Auditlog: DISABLED
     Reference Count: 0
Done
```

上記のトラブルシューティング手順をすべて実行しても問題が解決しない場合は、**Citrix** サポートにお問い合わせください。

ださい。

## アプリケーション分析のしきい値およびアラートの作成

February 6, 2024

Citrix ADM のアプリケーション分析により、Citrix ADC インスタンスを通過するさまざまなタイプのトラフィックを監視できます。Citrix ADM では、次のカウンターにしきい値を設定して、トラフィックとアプリのスコアを監視できます。

CPU、メモリ、NIC 破棄および応答時間のしきい値を設定し、アプリスコアを監視できます。

**NetScaler ADM** でアプリのスコアを構成するには：

1. Citrix ADM で、[アナリティクス] > [設定] に移動します。
2. [設定] ページで、[アプリスコアの構成] をクリックします。
3. [アプリスコアの構成] ページで、次のパラメータの値を入力します。
  - a) **CPU** しきい値が低い。Citrix ADC インスタンスの合計 CPU 使用量の下限値。
  - b) **CPU** のしきい値が高い。Citrix ADC インスタンスの合計 CPU 使用率の上限値。
  - c) メモリしきい値が低い。Citrix ADC インスタンスの合計メモリ使用量の下限値。
  - d) メモリしきい値が高い。Citrix ADC インスタンスの合計メモリ使用量の上限値。
  - e) **NIC** が低いと **SLA** が破棄されます。インターフェイスによって廃棄されるパケットの下限しきい値。
  - f) **NIC** が高いと **SLA** が破棄されます。インターフェイスによって廃棄されるパケットのしきい値が高いほど。
  - g) 応答時間。要求パケットの送信から、仮想サーバ上で構成されたサービスからの最初の応答パケットを受信するまでの時間間隔。Citrix ADM で設定されているデフォルト値は 500 ミリ秒です。
  - h) アクティブサービスのしきい値。仮想サーバにバインドされているアクティブでなければならないサービスのパーセンテージのしきい値。

## ← Configure App Score

Configure the below settings to calculate the App Score values

Low CPU Threshold (%)

High CPU Threshold (%)

Low Memory Threshold (%)

High Memory Threshold (%)

Low NIC Discards

High NIC Discards

Server Response Time (ms)

Active Services Threshold (%)

4. **[OK]** をクリックします。

## インテリジェントなアプリケーション分析

February 6, 2024

Intelligent App Analytics では、機械学習とルールベースのアルゴリズムを使用して、アプリケーションのパフォーマンスの問題を特定できます。NetScaler ADM インテリジェントアプリ分析機能:

- NetScaler ADC インスタンスを介して配信されるアプリケーションの監視とトラブルシューティングのための簡単でスケーラブルなソリューションを提供します。
- あらゆるレベルのアプリケーションを監視して、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改善します。

通常の展開では、数千台のサーバーがユーザーのデータニーズに対応します。これらのサーバーに送信されるトラフィックは、負荷分散され、NetScaler ADC アプライアンスに構成された仮想サーバーによって監視されます。各仮想サーバーは、これらの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ます。このような展開では、インテリジェント App Analytics 機能によって次のことが実現されます。

- システム停止やその他のイベント発生時の監視、管理、意思決定
- アプリケーション用に設定された仮想サーバーとサービスを監視します
- 仮想サーバおよびサービスに関する重要な情報を表示します。これにより、アプリケーションの最適なパフォーマンスを実現するために必要な構成を変更できます。

組織のサーバーファームをスケールアップすると、サーバー上で受信される大量のトラフィックに関連する問題を追跡し、必要なトラブルシューティングに絞込み込むことが難しくなります。

アプリケーションが実行されていて大量のトラフィックを受信している場合、さまざまな問題が発生する可能性があります。アプリケーション分析のパフォーマンス・インディケータを表示するには、「アプリケーション」>「ダッシュボード」に移動してアプリケーションを選択し、「問題」セクションで 問題 を表示します。

## インテリジェントアプリ分析の構成

February 6, 2024

インテリジェントアプリ分析機能は、**Citrix ADC 12.1.50.x** 以降でのみサポートされています。メトリックコレクターは **Citrix** ADC カウンターデータを NetScaler ADM にプッシュし、アプリケーションの問題の検出に使用されます。インテリジェントアプリ分析機能を使用するには、各 NetScaler ADC インスタンスでメトリクスコレクターを構成する必要があります。デフォルトでは、NetScaler ADM にインスタンスを追加している間、メトリックコレクターは **Citrix** ADC で有効になります。

メトリクスコレクターが有効になっているかどうかを確認するには:

1. [ネットワーク] > [\*\* インスタンス] > [\*\*Citrix ADC] に移動し、監視するインスタンスのタイプ (Citrix ADC VPX など) を選択します。
2. NetScaler ADC インスタンスを選択します。
3. 「アクションの選択」 リストから、「メトリック・コレクター」を選択します。

The screenshot shows the NetScaler ADC management console. At the top, there are tabs for VPX (13), MPX (2), CPX (0), and SDX (0). Below the tabs are buttons for Add, Edit, Remove, Dashboard, Tags, Profiles, and Partitions. A search bar is present with the text 'Click here to search or you can enter Key: Value format'. The main area displays a table of instances with columns for IP Address, Host Name, Instance State, HTTP Req/s, CPU Usage (%), Memory Usage (%), and Version. A context menu is open over the table, listing various actions such as Show Events, Create Cluster, Reboot, Ping, TraceRoute, Rediscover, Unmanage, Annotate, Configure SNMP, Configure Syslog, Configure Analytics, **Metrics Collector** (highlighted), Configure GSLB site, Configure Interfaces for Orchestration, and Replicate Configuration.

4. メトリックコレクターの設定ページでは、「有効にする」オプションがデフォルトで選択されています。このオプションが選択されていない場合は、必ず「有効にする」オプションを選択し、「OK」をクリックしてください。

← Configure Metrics Collector settings on [blurred text]

Source Instance

[blurred text]

Enable

OK Close

注

サーバーエラーとその詳細な **Web** トランザクションの異常を表示するには、[仮想サーバーで分析を有効にする必要があります](#)。

## アプリケーション分析用のパフォーマンス・インディケーター

February 6, 2024

パフォーマンス指標と、NetScaler ADC Web アプリケーションで発生するカテゴリを表示できます。これらの指標を表示するには、ADC インスタンスで **Analytics and Metrics Collector** を有効にする必要があります。



分析およびメトリック・コレクターを有効にした後、「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を選択し、「問題」セクションまでスクロールダウンすると、次のインジケータを表示できます：

- 応答時間
- アクティブなサービス
- 平均 CPU 使用率
- メモリ使用率
- NIC カードの飽和
- サービスフラップ
- セッションの再利用が低い
- 不適切な永続性タイプ
- 不安定なサーバー (5xx)
- SSL リアルタイムトラフィック
- 異常に大きい HTTP パケット
- TCP 再構成キュー制限ヒット
- サージキューの蓄積

### 応答時間

February 6, 2024

この問題は、クライアントのリクエストに回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外れることを検出します。「応答時間」タブをクリックすると、問題の詳細が表示されます。

ISSUES

Current (0) All (3)

The screenshot displays the 'ISSUES' section with a list of metrics on the left and a detailed view of a 'Response Time' issue on the right. The 'Response Time' issue is highlighted with a red box in the list. The detailed view shows a 'Medium' severity issue that detects events when application response time deviates from a configured threshold. It includes a 'What Happened' section stating that the app response time for vip150-parition1 has breached the 100ms threshold. A bar chart shows 3 occurrences on 01-21. A table below the chart provides the following data:

| TIME            | NO OF OCCURRENCES | SEVERITY | DETECTION MSG                                                                  |
|-----------------|-------------------|----------|--------------------------------------------------------------------------------|
| Jan 21 - Jan 22 | 3                 | MEDIUM   | The response time for 11 transactions has exceeded the configured value 100ms. |

[詳細] では、次の項目を表示できます：

- 選択した時間のイベントの合計を示すグラフ。クリックしてフィルターを適用し、詳細を表示します
- 問題が発生したとき
- 選択した時間の合計出現回数
- 「低」、「中」、「高」などの問題の重大度
- 設定されたしきい値を超え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

February 6, 2024

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、設定されているしきい値を下回ったことを検出します。アクティブサービスタブをクリックすると、問題の詳細が表示されます。

## ISSUES

Current (1) All (1)

Active Services Performance 9  
Last Wednesday at 5:30 AM

Medium

### Active Services

Detects events when % of active services bound to the virtual server is lesser than the configured value.

---

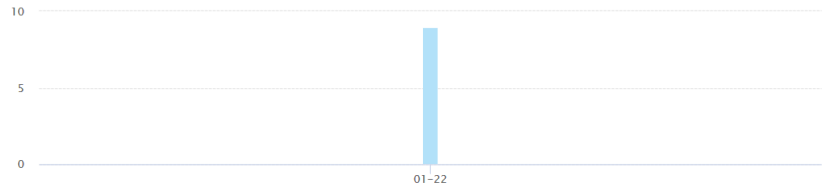
**What Happened**

Percentage active services up for has breached the configured threshold of 100%.

|                           |                           |
|---------------------------|---------------------------|
| <b>No. of occurrences</b> | <b>Last occurred</b>      |
| 9                         | Last Wednesday at 5:30 AM |

---

**Details**



| TIME            | NO OF OCCURRENCES | SEVERITY | DETECTION MSG                                                                               |
|-----------------|-------------------|----------|---------------------------------------------------------------------------------------------|
| Jan 22 - Jan 23 | 9                 | MEDIUM   | The current active session 0% for the application is lesser than the configured value 100%. |

[詳細] では、次の項目を表示できます：

- 選択した期間のイベントの合計を示すグラフ。クリックしてフィルターを適用し、詳細を表示します
- 問題が発生したとき
- 選択した期間の合計発生回数
- 「低」、「中」、「高」などの問題の重大度
- アクティブなサービスセッションの割合、および設定されたしきい値を示す検出メッセージ

## 平均 CPU 使用率

February 6, 2024

この問題は、このアプリケーションの ADC CPU 使用率が設定されたしきい値を超えることを検出します。平均 CPU 使用率タブをクリックすると、問題の詳細が表示されます。

ISSUES

Current (0) [All \(3\)](#)

**Response Time** 3

Performance  
Last Tuesday at 5:30 AM

**Avg CPU Usage** 6

Instance Health  
Last Wednesday at 5:30 AM

**Memory Usage** 20

Instance Health  
Last Wednesday at 5:30 AM

**Medium Avg CPU Usage**

Detects events when average CPU usage for the ADC deployed for this application is higher than the configured threshold.

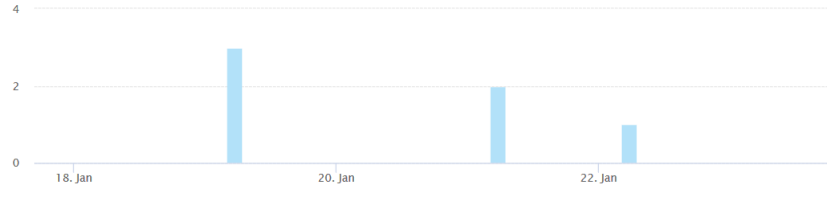
---

**What Happened**

No. of occurrences: 6      Last occurred: Last Wednesday at 5:30 AM

---

**Details**



| TIME            | NO OF OCCURRENCES | SEVERITY | DETECTION MSG                                                             |
|-----------------|-------------------|----------|---------------------------------------------------------------------------|
| Jan 22 - Jan 23 | 1                 | MEDIUM   | The ADC average CPU usage 6.9% has exceeded the configured threshold 5%.  |
| Jan 21 - Jan 22 | 2                 | MEDIUM   | The ADC average CPU usage 6.9% has exceeded the configured threshold 5%.  |
| Jan 19 - Jan 20 | 3                 | MEDIUM   | The ADC average CPU usage 13.3% has exceeded the configured threshold 5%. |

[詳細] では、次の項目を表示できます：

- 選択した期間のイベントの合計を示すグラフ。クリックしてフィルターを適用し、詳細を表示します
- 問題が発生したとき
- 選択した期間の合計発生回数
- 「低」、「中」、「高」などの問題の重大度
- ADC 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

February 6, 2024

この問題は、このアプリケーションの ADC メモリ使用量が設定されたしきい値を超えることを検出します。メモリ使用量タブをクリックすると、問題の詳細が表示されます。

ISSUES

Current ( 0 ) All ( 3 )

**Memory Usage**  
 Detects events when average memory usage for the ADC deployed for this application is higher than the configured threshold.

**What Happened**  
 No. of occurrences: 20  
 Last occurred: Last Wednesday at 5:30 AM

**Details**

| TIME            | NO OF OCCURRENCES | SEVERITY | DETECTION MSG                                                          |
|-----------------|-------------------|----------|------------------------------------------------------------------------|
| Jan 22 - Jan 23 | 1                 | MEDIUM   | The ADC memory usage 42.08% has exceeded the configured threshold 10%. |
| Jan 21 - Jan 22 | 2                 | MEDIUM   | The ADC memory usage 42.02% has exceeded the configured threshold 10%. |

[詳細] では、次の項目を表示できます：

- 選択した期間のイベントの合計を示すグラフ。クリックしてフィルターを適用し、詳細を表示します
- 問題が発生したとき
- 選択した期間の合計発生回数
- 「低」、「中」、「高」などの問題の重大度
- ADC 平均メモリ使用率 (%) と設定されたしきい値を示す検出メッセージ

サービスフラップ

February 6, 2024

ネットワーク管理者は、アプリケーションの可用性を最適化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ある場合、アプリケーションサーバーのステータスと可用性が全体的なパフォーマンスに影響を与える可能性があります。

サービスフラップイベントを使用すると、問題のあるアプリケーションを特定できます。サービスフラップイベントは次のような場合にも役立ちます。

- 特定の期間、どのサービスがダウン状態になっているかを把握する
- 特定の期間に稼働中または停止状態になっているサービスの数を把握できます。

サービスフラップタブをクリックすると、サービスフラップの詳細が表示されます。

ISSUES

Current (0) All (6)

|                                                         |      |
|---------------------------------------------------------|------|
| Response Time<br>Performance<br>Yesterday at 5:30 AM    | 133  |
| Active Services<br>Performance<br>01/16/2020            | 9.5K |
| Service Flaps<br>Performance<br>Last Sunday at 5:30 AM  | 15   |
| SSL Real Time Traffic<br>Performance<br>01/15/2020      | 2.2K |
| Unusually large HTTP packets<br>Config<br>01/14/2020    | 52   |
| TCP reassemble queue limit hits<br>Config<br>01/15/2020 | 4.3K |

**Service Flaps**

Service Flaps events help to understand which services are in UP or DOWN state for a specific duration.

**What Happened**

No. of occurrences: 15      Last occurred: Last Sunday at 5:30 AM

**Details**

| TIME            | SERVICE/SERVICE GROUP | SERVICE IP ADDRESS | STATE |
|-----------------|-----------------------|--------------------|-------|
| Jan 19 - Jan 20 | service1              | 10.102.103.116     | UP    |
| Jan 19 - Jan 20 | service1              | 10.102.103.116     | DOWN  |
| Jan 15 - Jan 16 | service1              | 10.102.103.116     | UP    |
| Jan 15 - Jan 16 | service1              | 10.102.103.116     | DOWN  |
| Jan 14 - Jan 15 | service1              | 10.102.103.116     | UP    |
| Jan 14 - Jan 15 | service1              | 10.102.103.116     | DOWN  |
| Jan 13 - Jan 14 | service1              | 10.102.103.116     | DOWN  |
| Jan 13 - Jan 14 | service1              | 10.102.103.116     | UP    |
| Jan 13 - Jan 14 | service1              | 10.102.103.116     | DOWN  |
| Jan 12 - Jan 13 | service1              | 10.102.103.116     | DOWN  |

Showing 1 - 10 of 15 items      Page 1 of 2

発生回数や前回発生時刻などの詳細を表示できます。

[詳細] では、次の項目を表示できます。

- サービスフラップ異常が発生した時間
- サービス/サービスグループ名
- サービス IP アドレス
- 現在のサービス状態

## 不安定なサーバー

February 6, 2024

シナリオによっては、無効なリクエスト、一時的な過負荷、またはサーバーの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、ウェブサーバーがステータスコードを返すことがあります。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とともに表示されます。例：

- **502 Bad Gateway**  
サーバーがゲートウェイまたはプロキシとして機能していて、上流のサーバーから無効な応答を受信しました。
- **503 サービス利用不可**サーバーは現在利用できません  
。サーバーは過負荷またはメンテナンスのためにダウンしている可能性があります。
- **504 ゲートウェイのタイムアウト**サーバーはゲートウェイまたはプロキシとして機能しており、上流の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。ウェブページをアップして利用できるようにするために、ウェブサーバには是正措置を実施しなければならない場合があります。

不安定なサーバーインジケータを使用すると、これらの障害を確認し、問題を解決するための是正措置を決定し、クライアントのリクエストが処理され、ウェブページが常に利用可能であることを確認できます。

不安定なサーバタブを選択すると、問題の詳細が表示されます。

ALL ISSUES

| TIME            | SERVICE/SERVICE GROUP | NO OF OCCURRENCES | SEVERITY | DETECTION MSG                                         |
|-----------------|-----------------------|-------------------|----------|-------------------------------------------------------|
| Dec 11 - Dec 12 | svc8081               | 810               | HIGH     | 100% of the responses from this server are 5xx errors |
| Dec 10 - Dec 11 | svc8081               | 126               | HIGH     | 100% of the responses from this server are 5xx errors |

問題のトラブルシューティングに 推奨される対処 方法は次のとおりです。

- 5xx エラーで応答するサーバーに適したパラメーターを使用して L7 モニターを設定します。モニターは、サービスの状態を追跡するエンティティです。アプライアンスは、各サービスにバインドされたモニターを使用してサーバーを定期的にプローブします。サーバーが指定された応答タイムアウト内に応答せず、指定されたプローブが失敗した場合、サービスはダウンとマークされます。次に、アプライアンスは残りのサービス間で負荷分散を実行します。モニターの構成について詳しくは、「[カスタムモニター](#)」を参照してください。
- サーバーのトラブルシューティング

[詳細] では、次の項目を表示できます。

- 不安定なサーバー異常が発生した時間
- サービス/サービスグループ名
- 総発生数
- 異常の重大度（高、低、中など）
- 5xx エラーを報告する本サービスからの応答の% を示す検出メッセージ

サーバーエラー 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。

## セッションのビルダップ

February 6, 2024

セキュリティで保護されたすべてのトランザクションについて、NetScaler ADC は最初のトランザクションに対して SSL オフロード処理を実行し、セッションの再利用構成に基づいて **SSL** セッションを保存します。

トラフィックレートによっては、一定期間にわたってセッションが蓄積され、Citrix ADC でこれらのセッションによって大量のメモリが滞留する可能性があります。

セッションのビルドアップイベントは、管理者に警告し、このイベントを解決するための推奨アクションを提供します。「セッションビルドアップ」タブをクリックすると、問題の詳細が表示されます

[詳細] では、次の項目を表示できます：

- セッションのビルドアップ異常が発生した時間
- 仮想サーバー名
- 異常の重大度（高、低、中など）
- 仮想サーバーで **X** 個の SSL セッションが使用可能で、現在、設定されているタイムアウトセッション内で 1 秒あたり **Y** 回の SSL ハンドシェイクが行われていることを示すメッセージ。

この異常を修正するための推奨アクションは、セッションのタイムアウトを減らすか、セッションの再利用を無効にすることです。詳細については、「[セッションタイムアウト](#)」を参照してください。

## セッションの再利用が低い

February 6, 2024

NetScaler ADC 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により、SSL トランザクションを処理します。サーバーから応答を受信すると、NetScaler ADC インスタンスはクライアントとの安全なトランザクションを完了します。キャッシュされたセッションパラメータを使用して、NetScaler ADC インスタンスは、連続した要求に対して SSL ハンドシェイク処理を完了します。

これらのセッションが再利用されない場合は、NetScaler ADC インスタンスのオーバーヘッドになります。**Low Session Reuse** インジケータを使用すると、実際に再利用されているセッション数が少ないかどうかを確認できます。

「低セッション再利用」タブをクリックすると、問題の詳細が表示されます。



ALL ISSUES

|                                                        |       |
|--------------------------------------------------------|-------|
| Response Time<br>Performance<br>Today at 5:30 AM       | 7.2K  |
| Surge Queue Buildup<br>Config<br>Today at 5:30 AM      | 30.1K |
| Service Flaps<br>Performance<br>Last Monday at 5:30 AM | 1     |
| Low Session Reuse<br>Performance<br>Today at 5:30 AM   | 97.3K |
| ServerError 5xx<br>Config<br>Today at 5:30 AM          | 27.3K |

**Low Session Reuse** Medium

SSL session reuse helps optimize performance by providing clients the opportunity to reuse cached session parameters. However, if sessions are not reused, they become an overhead for the ADC instance. This indicator detects conditions, where the actual number of sessions being reused is less.

---

**What Happened**

|                           |                      |
|---------------------------|----------------------|
| <b>No. of occurrences</b> | <b>Last occurred</b> |
| 97.3K                     | Today at 5:30 AM     |

---

**Recommended Actions**

- Disable session reuse or reduce the session idle timeout for better performance.

---

**Details**

[App](#) 23

| TIME            | NO OF OCCURRENCES | SEVERITY | DETECTION MSG                                     |
|-----------------|-------------------|----------|---------------------------------------------------|
| Dec 12 - Dec 13 | 3                 | HIGH     | Only -0.00 % of sessions created are being reused |
| Dec 12 - Dec 13 | 764               | HIGH     | Only 0.00 % of sessions created are being reused  |
| Dec 11 - Dec 12 | 27                | HIGH     | Only -0.00 % of sessions created are being reused |

問題のトラブルシューティングに 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、セッションのタイムアウトを減らすことです。詳しくは、「[セッション再利用](#)」を参照してください。

[詳細] では、次の項目を表示できます：

- セッション再利用率が低いアプリケーションの総数
- セッション再利用率の異常が発生した時間
- 総発生数
- 異常の重大度（高、低、中など）
- 設定済みセッションの%のみが再利用されていることを示す検出メッセージ

### サージキューの蓄積

February 6, 2024

サーバーが要求の急増を受け取ると、サーバーはクライアントに応答するのが遅くなります。多くの場合、オーバーロードにより、クライアントはエラーページを受信します。仮想サーバーには、受信要求を処理するために十分なバックエンドサーバーを構成する必要があります。

サージキューのビルドアップ インジケータを使用すると、サージキューのビルドアップがある仮想サーバーを表示できます。**Surge Queue Buildup** タブをクリックすると、問題の詳細が表示されます。

## ISSUES

Current (0) All (3)

|                                                      |      |
|------------------------------------------------------|------|
| Response Time<br>Performance<br>11/23/2019           | 3    |
| Surge Queue Buildup<br>Performance<br>11/23/2019     | 1.3K |
| Unusually large HTTP packets<br>Config<br>12/12/2019 | 51   |

**Surge Queue Buildup**  
Medium  
 Detects virtual servers that are underprovisioned by checking for frequent build up of surgequeue. A virtual server needs to have enough of backend servers configured to handle all the requests that are arriving. When servers are out of capacity, the requests are queued until the servers respond, which result in latency.

**What Happened**  
 No. of occurrences: 1.3K  
 Last occurred: 11/23/2019

**Recommended Actions**  
 Increase maxclient configured for the application, or increase the number of backend servers serving the application.

**Details**

| TIME            | NO OF OCCURRENCES | SEVERITY | DETECTION MSG                                             |
|-----------------|-------------------|----------|-----------------------------------------------------------|
| Nov 23 - Nov 24 | 1.3K              | HIGH     | SurgeQueue buildup has been observed at vserversbase_lb1* |

問題のトラブルシューティングに推奨される対処方法は次のとおりです。

- クライアント接続の制限数を増やします。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。
- アプリケーション要求を処理するためにバックエンドサーバーを増やす

[詳細] では、次の項目を表示できます：

- サージキューの蓄積異常が発生した時間
- 総発生数
- 異常の重大度（高、低、中など）
- 仮想サーバ上のサージキューの蓄積を示す検出メッセージ

## 異常に大きい HTTP パケット

February 6, 2024

HTTP トランザクションは、クライアントとサーバー間の要求応答メッセージを使用します。要求メッセージと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。仮想サーバー、サービス、またはサービスグループで HTTP ヘッダーの長さを設定して、4xx エラーを回避できます。

HTTP 要求/応答がヘッダーの最大長を超えると、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を使用すると、HTTP ヘッダーサイズが設定値を超えた HTTP メッセージの発生状況を確認できます。

「異常に大きい **HTTP** パケット」タブをクリックすると、問題の詳細が表示されます。

ISSUES

Current (0) [All \(3\)](#)

- Response Time Performance 3  
11/23/2019
- Surge Queue Buildup Performance 1.3K  
11/23/2019
- Unusually large HTTP packets Config 51  
12/12/2019

**High** Unusually large HTTP packets

Detects the presence of HTTP messages with HTTP header size larger than the configured HTTP profile limit for vserver, service, or service group. This indicator suggests a probable attack or an incorrect header length is configured.

**What Happened**

No. of occurrences: 51    Last occurred: 12/12/2019

**Recommended Actions**

- Review your traffic to determine if the header sizes are genuine.  If genuine then update maxHeaderLen value on the HTTP profile to accommodate those packets.
- If it is not genuine then blacklist the source to avoid attacks.

**Details**

[App \(2\)](#)    [Services \(1\)](#)

| TIME            | NO OF OCCURRENCES | SEVERITY | DETECTION MSG                                                                                                                                         |
|-----------------|-------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dec 12 - Dec 13 | 1                 | HIGH     | HTTP Request/Response exceeds the configured maximum header length. Current config settings are: HTTP profile: nshttp_default_profile maxhdrlen: 5000 |
| Nov 22 - Nov 23 | 25                | HIGH     | HTTP Request/Response exceeds the configured maximum header length.                                                                                   |

問題のトラブルシューティングに 推奨される対処 方法は次のとおりです。

- トラフィックを確認して、ヘッダーサイズが本物かどうかを判断します。ヘッダーサイズが正規の場合は、HTTP プロファイルの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。
- ヘッダーのサイズが正規でない場合は、攻撃を回避するためにソースを一覧表示します。

[詳細] では、次の項目を表示できます：

- 異常発生した時間
- 総発生数
- 異常の重大度（高、低、中など）
- 仮想サーバ、サーバ、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

## 不適切な永続性タイプ

February 6, 2024

仮想サーバーにより実行されるサービスへの接続を維持したい場合（電子商取引で使用される接続など）は、その仮想サーバーに対してパーシステンスを構成する必要があります。その後、アプライアンスは最初のサーバー選択に設定された負荷分散方法を使用しますが、それ以降のすべての要求は同じクライアントからの同じサーバーに転送します。

永続性は、既存のセッションが後続のリクエストを処理するために再利用される場合に有効です。持続性セッションの再利用が少ない場合、ADC で作成されるセッションはオーバーヘッドに過ぎません。

**Improper Persistence Type** インジケータを使用すると、仮想サーバーでのパーシスタンスの使用率が低いかどうかを判断できます。「不適切な持続性タイプ」タブをクリックして、問題の詳細を表示します。

ISSUES

Current (3) All (3)

**Improper Persistence Type**

Persistence is effective when existing sessions are reused to serve subsequent requests. If persistence session reuse is low indicates, sessions created are just an overhead on ADC. The indicator detects if there is very low reuse of persistence sessions.

**What Happened**

| No. of occurrences | Last occurred    |
|--------------------|------------------|
| 12                 | Today at 3:46 PM |

**Recommended Actions**

- Check the persistence type or disable Persistence.

**Details**

| TIME                     | NO OF OCCURRENCES | SEVERITY | DETECTION MSG                                                                                                                                         |
|--------------------------|-------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jan 28 3:46 pm - 3:47 pm | 1                 | HIGH     | lb virtual server : lb_111 with ip: 10.106.177.122 is having low use of persistence Sessions.About 99.95% of persistence sessions are getting unused. |
| Jan 28 3:45 pm - 3:46 pm | 1                 | HIGH     | lb virtual server : lb_111 with ip: 10.106.177.122 is having low use of persistence Sessions.About 100.0% of persistence sessions are getting unused. |

問題のトラブルシューティングに 推奨されるアクション は、永続性タイプを確認するか、永続性を無効化することで。詳細については、「[パーシスタンス設定](#)」を参照してください。

[詳細] では、次の項目を表示できます：

- 異常発生した時間
- 総発生数
- 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

## TCP 再構成キュー制限ヒット

February 6, 2024

TCP は、OOO パケットを TCP 通信に保持するために、アウトオブオーダーキューを維持します。この設定は、パケットをランタイムメモリに保持する必要がある場合にキューサイズが長くなると、NetScaler ADC メモリに影響します。

このキューサイズは、ネットワークおよび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する必要があります。

**TCP** 再構成キュー制限ヒット インジケータを使用すると、TCP 接続上のアウトオブオーダーパケットが、設定されたアウトオブオーダー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。

**TCP** リアセンブルキュー制限ヒット数タブをクリックすると、問題の詳細が表示されます。

Current (2) All (3)

Active Services 54

Performance  
Today at 2:44 PM

High TCP reassemble queue limit hits

Detects reassembly queue flushes because out-of-order packets exceeded the configured limit. This indicator suggests a probable attack, and ADC handles the attack by dropping the erroneous packets.

TCP reassemble queue limit ... 9

Config  
Today at 2:44 PM

**What Happened**

No. of occurrences: 9      Last occurred: Today at 2:44 PM

**Recommended Actions**

- Review your traffic to determine if this is an attack.
- If it is not an attack but a temporary network glitch, no action is required.

- If it is an attack, blacklist the sources.
- If it is an expected network behaviour, update the oooQSize value on TCP profile to avoid packet drops and latency.

**Details**

App (0)    [Services \(9\)](#)

| TIME                     | SERVICE/SERVICE GROUP | NO OF OCCURRENCES | SEVERITY | DETECTION MSG                                                                                             |
|--------------------------|-----------------------|-------------------|----------|-----------------------------------------------------------------------------------------------------------|
| Jan 14 2:44 pm - 2:45 pm | service1              | 1                 | HIGH     | Number of Out-of-Order packets on a TCP connection exceeds the configured out of order packet queue size. |

問題のトラブルシューティングに 推奨される対処 方法は次のとおりです。

- トラフィックを確認し、攻撃の場合は送信元をブロックリストします。
- この動作が予想されるネットワーク動作である場合は、TCP プロファイルの **out-of-order packets size** 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グリッチであれば、それ以上の操作は必要ありません

[詳細] では、次の項目を表示できます：

- 異常発生した時間
- 総発生数
- 異常の重大度（低、中、高など）
- 現在の TCP プロファイルと oooQSize 設定を示す検出メッセージ

## SSL リアルタイムトラフィック

February 6, 2024

NetScaler ADC 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、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

リアルタイムトラフィックインジケータは、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識別し、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すると、問題の詳細が表示されます。

ISSUES

Current (0) All (6)

|                                        |      |
|----------------------------------------|------|
| Response Time Performance              | 133  |
| Active Services Performance            | 9.5K |
| Service Flaps Performance              | 15   |
| SSL Real Time Traffic Performance      | 2.2K |
| Unusually large HTTP packets Config    | 52   |
| TCP reassemble queue limit hits Config | 4.3K |

**SSL Real Time Traffic**

This indicator analyzes SSL traffic to identify real time traffic and suggests optimal configuration settings for improving latency.

**What Happened**

No. of occurrences: 2.2K      Last occurred: 01/15/2020

**Recommended Actions**

- Improve network latency by tuning sslTriggerTimeout, encryptTriggerPKCount and pushEncTrigger parameters on the vsener entity.

**Details**

| TIME            | NO OF OCCURRENCES | SERVICE/SERVICE GROUP | SEVERITY | DETECTION MSG                                                      |
|-----------------|-------------------|-----------------------|----------|--------------------------------------------------------------------|
| Jan 15 - Jan 16 | 1K                | service1              | MEDIUM   | The application is sending small records of average size (1 bytes) |
| Jan 14 - Jan 15 | 1.2K              | service1              | MEDIUM   | The application is sending small records of average size (1 bytes) |

この問題をトラブルシューティングするための推奨処置は、SSL パラメータを更新してネットワークの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、次の項目を表示できます：

- 異常発生した時間
- サービス/サービスグループ名
- 異常の重大度（低、中、高など）
- アプリケーションの現在の設定を含む検出メッセージ

## アプリケーションセキュリティダッシュボード

February 6, 2024

**App Security** ダッシュボードには、検出済みまたはライセンス済みアプリケーションのセキュリティメトリックの概要が表示されます。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/ライセンスされたアプリケーションのセキュリティ攻撃情報が表示されます。

アプリの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、次の操作を行います。

- [アプリケーション] > [アプリセキュリティダッシュボード] に移動します。
- [Instance] リストからインスタンスの IP アドレスを選択します。

このレポートには、アプリケーション別に次の情報が含まれています。

- 脅威インデックス。アプリケーションに対する攻撃の重要度を示す 1 桁の評価システム。アプリケーションに対する攻撃の重大度が高いほど、そのアプリケーションの脅威指数は大きくなります。値の範囲は 1 ~7 です。

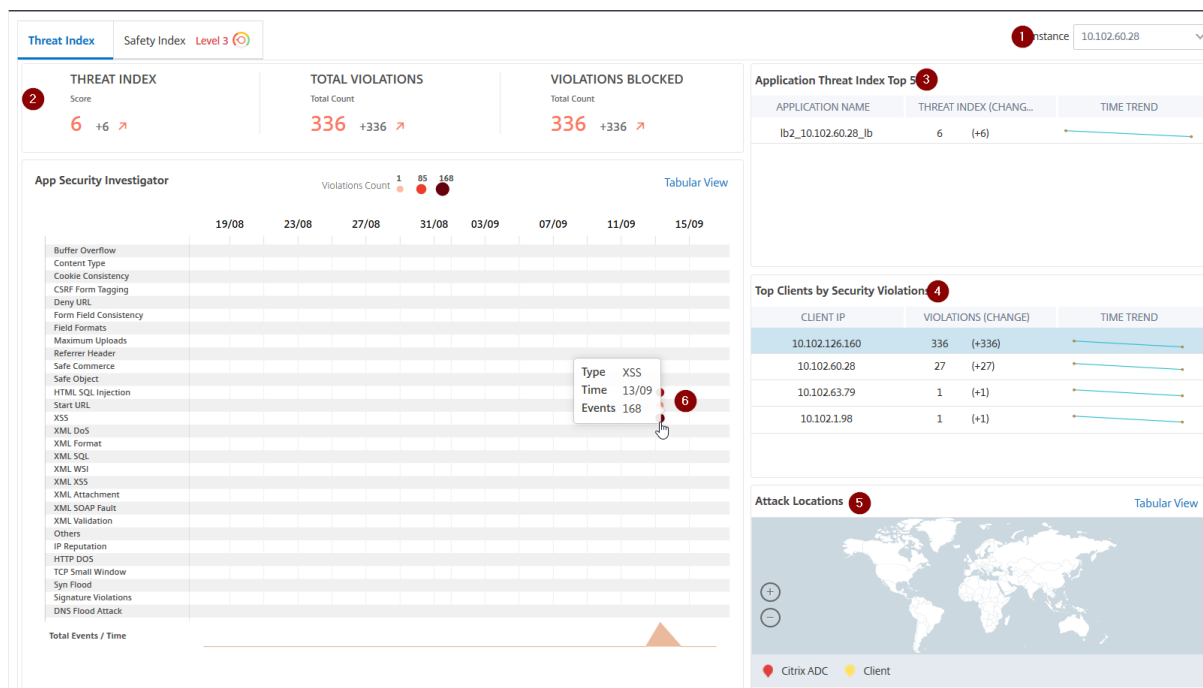
脅威指数は攻撃情報に基づいています。違反タイプ、攻撃カテゴリ、場所、クライアントの詳細などの攻撃関連情報から、アプリケーションへの攻撃に関する洞察が得られます。違反情報は、違反または攻撃が発生した場合にのみ NetScaler ADM に送信されます。侵害や脆弱性が多いと、脅威指数の値が高くなります。

- 安全指数。外部から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 ADC インスタンスをどのように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小さいほど、安全性指数は高くなります。値の範囲は 1 ~7 です。

安全指標では、アプリケーションファイアウォール構成と NetScaler ADC システムセキュリティ構成の両方が考慮されます。高い安全性指数値を得るためには、両方の構成を堅牢にする必要があります。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行われていて、`nsroot` ユーザーの強力なパスワードなどの NetScaler ADC システムの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指数の値が割り当てられます。

App Security Investigator で報告された不一致を確認できます。

### 脅威インデックスの詳細



1-詳細を表示できる NetScaler ADC インスタンスの IP アドレスが表示されます。

2-脅威インデックスのスコア、発生した違反の総数、ブロックされた違反の合計数などの詳細を表示します。

3 -選択したインスタンスの仮想サーバーを表示します。

4 -クライアントに基づいてセキュリティ違反を表示します。App Security Investigator のグラフは、クライアントごとに表示されます。各クライアント IP をクリックすると、結果を表示できます。

5 -違反をマップビューと表形式で表示します。

6 -違反の詳細を表示します。グラフ上にマウスポインタを置くと、違反の種類、攻撃時間、合計イベントなどの詳細が表示されます。

バブルグラフをクリックすると、詳細が [ アプリセキュリティ違反の詳細] ページに表示されます。たとえば、クロスサイトスクリプティング (クロスサイトスクリプト) 違反の詳細をさらに表示する場合は、**App Security Investigator** で **XSS** に設定されたグラフをクリックします。

[ アプリのセキュリティ違反の詳細] には、攻撃時間、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。

| ATTACK TIME                       | CLIENT IP      | SECURITY CHECK VIOLATION | SEVERITY | VIOLATION CATEGORY | ATTACK CATEGORY      | ACTION TAKEN | URL                                                       |
|-----------------------------------|----------------|--------------------------|----------|--------------------|----------------------|--------------|-----------------------------------------------------------|
| Sep 12 06:30 AM - Jan 01 05:29 AM | 10.102.126.160 | XSS                      | Critical | XSS                | Cross-site Scripting | Blocked      | http://10.102.60.238/xss_sql/login.php?username1=onload   |
| Sep 12 06:30 AM - Jan 01 05:29 AM | 10.102.126.160 | XSS                      | Critical | XSS                | Cross-site Scripting | Blocked      | http://10.102.60.238/xss_sql/login.php?password2=<alert>  |
| Sep 12 06:30 AM - Jan 01 05:29 AM | 10.102.126.160 | XSS                      | Critical | XSS                | Cross-site Scripting | Blocked      | http://10.102.60.238/xss_sql/login.php?password1=<javascr |
| Sep 12 06:30 AM - Jan 01 05:29 AM | 10.102.126.160 | XSS                      | Critical | XSS                | Cross-site Scripting | Blocked      | http://10.102.60.238/xss_sql/login.php?password1=<alert>  |
| Sep 12 06:30 AM - Jan 01 05:29 AM | 10.102.126.160 | XSS                      | Critical | XSS                | Cross-site Scripting | Blocked      | http://10.102.60.238/xss_sql/login.php?username1=<script> |
| Sep 12 06:30 AM - Jan 01 05:29 AM | 10.102.126.160 | XSS                      | Critical | XSS                | Cross-site Scripting | Blocked      | http://10.102.60.238/xss_sql/login.php?username2=<script> |
| Sep 12 06:30 AM - Jan 01 05:29 AM | 10.102.126.160 | XSS                      | Critical | XSS                | Cross-site Scripting | Blocked      | http://10.102.60.238/xss_sql/login.php?password2=<javascr |
| Sep 12 06:30 AM - Jan 01 05:29 AM | 10.102.126.160 | XSS                      | Critical | XSS                | Cross-site Scripting | Blocked      | http://10.102.60.238/xss_sql/login.php?username2=onload   |

Total 8      25 Per Page      Page 1 of 1

[ 設定] オプションをクリックして、表示させるオプションを選択することもできます。

### 安全指数の詳細

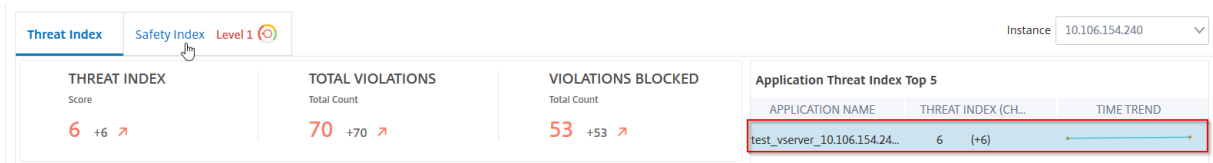
アプリケーションの脅威への露出度を確認したら、そのアプリケーションに設定されているセキュリティ構成と欠落しているセキュリティ構成を確認します。この情報は、アプリケーション安全性指数の概要をドリルダウンして取得できます。

安全性指数概要には、次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。

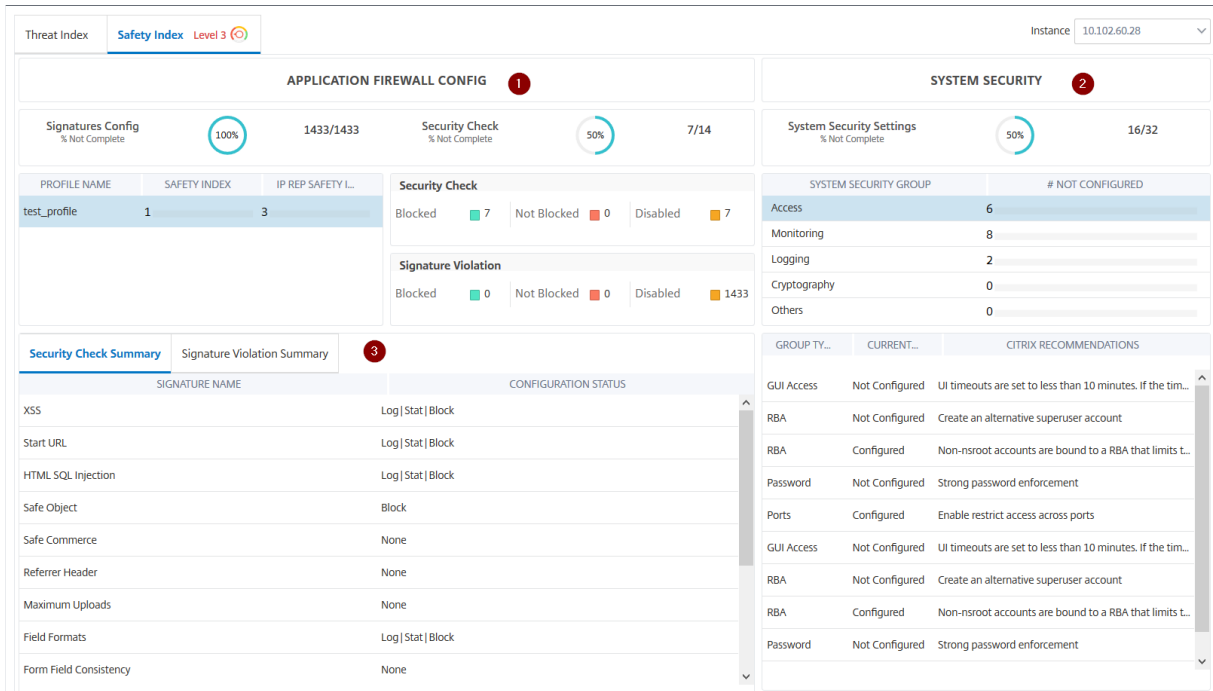
- アプリケーションファイアウォールの設定。構成されていないシグネチャおよびセキュリティエンティティの数を表示します。
- **NetScaler ADM** システムセキュリティ構成されていないシステムセキュリティ設定の数を表示します。

安全指数の詳細を表示するには、仮想サーバーまたはアプリケーションを選択し、[ 安全指数] タブをクリックします。





詳細が表示されます。



1 -アプリケーションファイアウォールの設定の詳細情報を表示します。

2 -システムセキュリティの詳細情報を表示します。各セキュリティグループをクリックすると、現在のステータスとCitrixの推奨事項の詳細が表示されます。

3 -セキュリティチェックと署名違反のサマリーを表示します。

仮想サーバーのセキュリティインサイトを有効にし、[ **\*\*Analytics** ] > [ [Security Insight](#) ] に移動して、脅威環境のサマリーを表示することもできます。\*\* 安全性指数のユースケースについて詳しくは、[セキュリティインサイトを参照してください](#)。

## サービスグラフ

February 6, 2024

NetScaler ADM サービスグラフ機能を使用すると、すべてのサービスをグラフィカルに監視できます。この機能では、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。次のサービスグラフを表示できます。

- すべての NetScaler ADC インスタンスで構成されたアプリケーション

- Kubernetes アプリケーション
- 3 層の Web アプリケーション

すべての **NetScaler ADC** インスタンスにおけるアプリケーションのサービスグラフ

グローバルサービスグラフ機能を使用すると、[clients to infrastructure to application](#)ビューの全体的な視覚化を取得できます。この単一ペインのサービスグラフビューでは、管理者として、次の操作を実行できます。

- ユーザーが特定のアプリケーション (3 層の Web アプリとマイクロサービスアプリ) にアクセスしているリージョンを理解する
- クライアント要求が処理されたというインフラストラクチャ (NetScaler ADC インスタンス) ビューの視覚化
- 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から発生しているかどうかを把握
- さらにドリルダウンして、問題のトラブルシューティングを行います。

「アプリケーション」>「サービスグラフ」の順に選択し、「グローバル」タブをクリックして以下を表示します。

- クライアントからバックエンドサーバに接続されたすべてのアプリケーションのエンドツーエンドの詳細
- 各データセンターに接続されているすべての NetScaler ADC インスタンス

注

GSLB アプリがある場合にのみ、データセンターを表示できます。

- クライアントのメトリック情報
- NetScaler ADC メトリックス情報
- 個別のアプリケーション、カスタムアプリケーション、および個別のマイクロサービスアプリケーションを持つすべての NetScaler ADC インスタンス
- カスタムアプリ、個別アプリ、マイクロサービスアプリに属する上位 4 つの低スコアアプリケーション
- 上位 4 台の低スコア仮想サーバのメトリック情報
- クリティカル、レビュー、良い、適用できないなどのアプリケーション (個別のアプリ、カスタムアプリ、マイクロサービスアプリ) のステータス。

詳細については、「[Service Graph でのアプリケーションの全体表示](#)」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

[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]タブをクリックして以下を表示します。

- エンド・ツー・エンドのアプリケーション全体のパフォーマンスを確保
- アプリケーションのさまざまなコンポーネントの相互依存によって生じるボトルネックを特定
- 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洞察を集める
- 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
- HTTP、TCP、SSL メトリックの分析

NetScaler ADM でこれらのメトリックを視覚化することで、問題の根本原因を分析し、必要なトラブルシューティングアクションを迅速に行うことができます。サービスグラフは、アプリケーションをさまざまなコンポーネントサービスに表示します。Kubernetes クラスター内で実行され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。はじめに、「[サービスグラフの設定](#)」をご参照ください。

### 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** アプリケーション] タブをクリックして以下を表示します。

- アプリケーションの構成方法の詳細（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）  
GSLB アプリケーションの場合は、データセンター、ADC インスタンス、CS、および LB 仮想サーバーを表示できます。
- クライアントからサービスへのエンド・ツー・エンドのトランザクション
- クライアントがアプリケーションにアクセスしている場所
- クライアント要求が処理されるデータセンターの名前と、関連するデータセンター NetScaler ADC 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、仮想サーバーのメトリックの詳細
- エラーがクライアントまたはサービスからのものである場合
- 「緊急」、「レビュー」、「良好」などのサービスステータス。NetScaler ADM 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を表示します。
  - 重大 (赤) -平均サービス応答時間が 200 ミリ秒を超え、エラーカウントが 0 より大きいことを示します。
  - **Review** (オレンジ) -平均サービス応答時間が 200 ミリ秒を超えるか、エラーカウントが 0 より大きいことを示します。
  - 良好 (緑) -エラーがなく、平均サービス応答時間が 200 ミリ秒未満であることを示します

- **Critical**、**Review**、**Good** などのクライアントのステータス。NetScaler ADM は、クライアントネットワークの遅延とエラー数に基づいてクライアントのステータスを表示します。
  - **Critical (赤)**-平均クライアントネットワーク遅延が 200 ミリ秒を超え、エラーカウントが 0 より大きいことを示します
  - **Review (オレンジ)** -平均クライアントネットワーク遅延が 200 ミリ秒を超えるか、エラーカウントが 0 より大きいことを示します。
  - **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が 200 ミリ秒未満であることを示します。
- クリティカル、レビュー、良好 (**Good**) などの仮想サーバのステータス。NetScaler ADM は、アプリのスコアに基づいて仮想サーバのステータスを表示します。
  - **クリティカル (赤)** -アプリのスコアが 40 未満になったことを示します
  - **Review (オレンジ)** -アプリのスコアが 40~75 の間であることを示します
  - **Good (緑)** -アプリのスコアが 75 を超えることを示します。

注意事項:

- 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バインドされた仮想サーバがない場合、そのアプリケーションのサービスグラフに詳細は表示されません。
- 仮想サーバと Web アプリケーションの間でアクティブなトランザクションが発生した場合にのみ、サービスグラフでクライアントとサービスのメトリックを表示できます。
- 仮想サーバとウェブアプリケーションの間で利用可能なアクティブなトランザクションがない場合は、負荷分散、コンテンツスイッチング、GSLB 仮想サーバ、サービスなどの構成データに基づいてサービスグラフでのみ詳細を表示できます。
- アプリケーション構成に変更が加えられた場合、サービスグラフに反映されるまで 10 分かかることがあります。

詳細については、「[アプリケーション用サービスグラフ](#)」を参照してください。

## サービスグラフの設定

February 6, 2024

ソフトウェア要件

|                        |                  | コンテナネットワークイン             | NetScaler           | NetScaler                  |
|------------------------|------------------|--------------------------|---------------------|----------------------------|
| Kubernetes ディストリビューション | Kubernetes バージョン | ターフェイス (CNI)             | CPX バージョン           | CIC バージョン                  |
| オープンソース                | v1.16.3          | Flannel、Calico または Canal | 13.0–41.28 以降       | 1.5.25 以降                  |
|                        |                  |                          | NetScaler ADM バージョン | NetScaler ADM エージェントのバージョン |
|                        |                  |                          | 13.0–47.22 以降       | 13.0–47.22 以降              |

Kubernetes クラスタにはさまざまなデプロイメントトポロジを設定できます。サービスグラフでサポートされるトポロジを次の表に示します。

| トポロジ              | サービスグラフでサポート                    |
|-------------------|---------------------------------|
| シングルティア入力または統合入力  | はい                              |
| デュアルティア           | はい                              |
| Cloud             | 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 |
| サービスマッシュライト       | はい                              |
| サービスマッシュ          | はい                              |
| ロードバランサーの種類のサービス  | いいえ                             |
| NodePort タイプのサービス | いいえ                             |

NetScaler ADM でのサービスグラフの設定を完了するには、Kubernetes クラスタ用に構成したトポロジの種類をクリックし、上記の手順を完了します。

- 単一層または統合入力トポロジ
- デュアルティアまたはサービスマッシュ Lite トポロジ
- サービスマッシュトポロジ

注

2層トポロジとサービスマッシュ Lite トポロジ用のサービスグラフを設定する手順は同じです。

はじめに

次のシナリオを使用して、サービスグラフを表示できます。

- 同じネットワーク上にある NetScaler ADM と Kubernetes クラスタ（たとえば、同じ Citrix Hypervisor でホストされている NetScaler ADM と Kubernetes クラスタ）。
- NetScaler ADM および Kubernetes クラスタが別のネットワーク上にインストールされている。このシナリオでは、[オンプレミスエージェントを設定し](#)、Kubernetes クラスタがホストされているネットワークにエージェントを登録する必要があります。

#### 単一層または統合入力トポロジ

以下を用意してください：

- 単一層またはユニファイド入力トポロジで Kubernetes クラスタを構成しました。
- [VPX、MPX、SDX、BLX インスタンスを Citrix ADM に追加し](#)、**Web Insight** を有効にしました。
- NetScaler ADM に [Kubernetes クラスタが追加されました](#)。

#### デュアルティアまたはサービスメッシュ **Lite** トポロジ

以下を用意してください：

- サポートされているトポロジのいずれかで Kubernetes クラスタを構成しました。
- NetScaler ADM と NetScaler ADC CPX 間の通信を有効にするために、Citrix [ADM で静的ルートを構成しました](#)。

注

NetScaler ADM を同じクラスターに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デプロイファイルを [ダウンロード](#) しました。
- CPX YAML ファイルに [必須パラメータ](#) を追加して、CPX を Citrix ADM に正常に登録できるようにしました。
- [VPX、MPX、SDX、または BLX インスタンスを Citrix ADM に追加](#) しました。
- NetScaler ADM に [Kubernetes クラスタが追加されました](#)。
- [サンプルマイクロサービスアプリケーションをデプロイ](#) しました。
- NetScaler ADC CPX を展開し、[CPX を ADM に登録](#) しました（2 層アーキテクチャにのみ適用）
- [仮想サーバの自動選択を有効](#) にして、仮想サーバのライセンスを取得しました。
- Citrix ADM エージェントが HTTP および TCP トランザクションを取得するために、[Web トランザクションと TCP トランザクションの設定](#) を「すべて」に有効にしました。
- [トラフィックをマイクロサービスに送信](#) しました。

### サービスマッシュアップポロジ

以下を用意してください:

- 次のいずれかのサービスマッシュアップポロジで Kubernetes クラスターバージョン1.14.0を構成しました。
  - Istio のサイドカープロキシとしての NetScaler ADC CPX
  - Istio の入力ゲートウェイとしての NetScaler ADC

詳しくは、「[NetScaler ADC Istio アダプターの展開アーキテクチャ](#)」を参照してください。

- `admissionregistration.k8s.io/v1beta1` API を有効にしました。API を確認するには、以下を使用します。

```
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` をインストールしました。
- Helm バージョン `3.x` をインストールしました。
- NetScaler ADM と NetScaler ADC CPX 間の通信を有効にするために、Citrix ADM で静的ルートを構成しました。

注

NetScaler ADM エージェントを同じクラスターに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。

- サービスマッシュアップポロジデータを取り込むために必要なパラメータを設定しました。
- サンプルアプリケーションをデプロイしました。
- NetScaler ADM に Kubernetes クラスターが追加されました。
- 仮想サーバの自動選択を有効にして、仮想サーバのライセンスを取得しました。
- Citrix ADM エージェントが HTTP および TCP トランザクションを取得するために、Web トランザクションと TCP トランザクションの設定を「すべて」に有効にしました。
- トラフィックをマイクロサービスに送信しました。

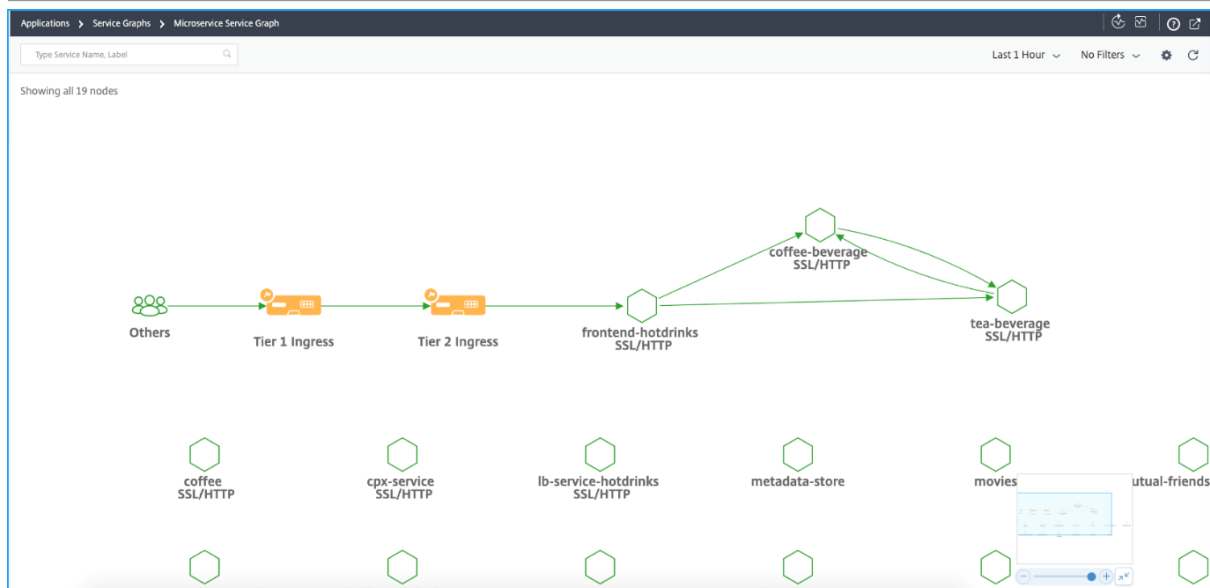
### サービスグラフで詳細を表示

February 6, 2024

NetScaler ADM で、[アプリケーション] > [サービスグラフ] > [Kubernetes サービスグラフ] の順に選択し、リストから時間を選択してサービスグラフの詳細を表示します。

## 2 階層/サービスマッシュ Lite トポロジ

シングルテ



- 階層 **1** の入力—Kubernetes クラスタ内の CitrixIngress Controller は、Kubernetes クラスタ外の NetScaler ADC インスタンス (VPX/MPX/SDX/BLX) を構成します。
- 階層 **2** の入力—Kubernetes クラスタ内の NetScaler ADC CPX インスタンスとともにサイドカーとして動作する CitrixIngress Controller です。
- **[Ingress]**: 他のすべての配置トポロジを表示します。



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のネットワークマップ
- 2 -特定の期間のヒット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 -期間を選択するタイムリスト
- 5 -フィルターを適用してサービスを表示する
- 6 -設定アイコン
- 7 -ズームインおよびズームアウト
- 8 -グラフビューまたは表形式ビュー

選択した期間に基づいて、サービスグラフを表示できます。

サービスアイコン

説明



エッジの幅は、ヒット数を示します。エッジの幅が大きいくほど、ヒット数が増えることを示します。



警告アイコンが付いたサービスは、サービスにエラーがあることを示します。

サービスアイコン

説明



ストップウォッチアイコンが付いたサービスは、サービスにレイテンシーまたは応答時間の問題があることを示します。

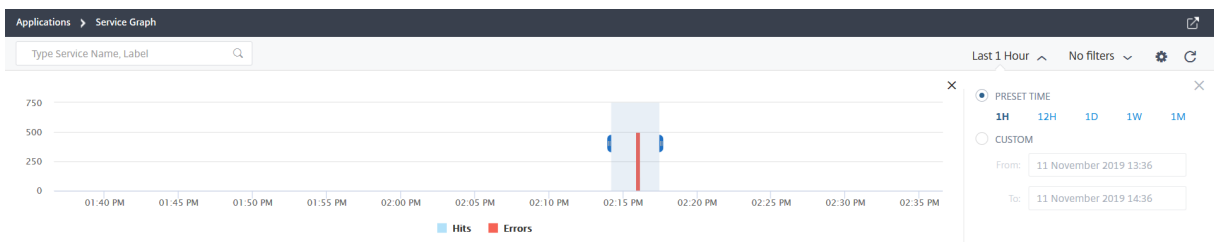


ストップウォッチと警告アイコンの両方があるサービスは、サービスにエラーと遅延/応答時間の問題の両方があることを示します。

注:

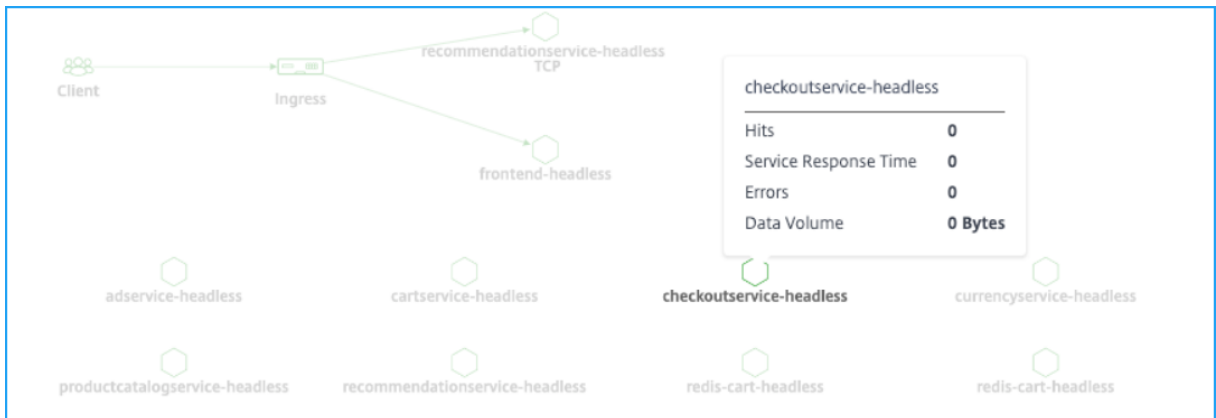
サービスに警告アイコンまたはストップウォッチアイコンがない場合は、そのサービスに Hits の異常またはしきい値違反があることを示します。

選択した期間に基づいて、サービスグラフを表示できます。グラフからヒットを示す期間を選択し、さらにドリルダウンして追加情報を表示します。

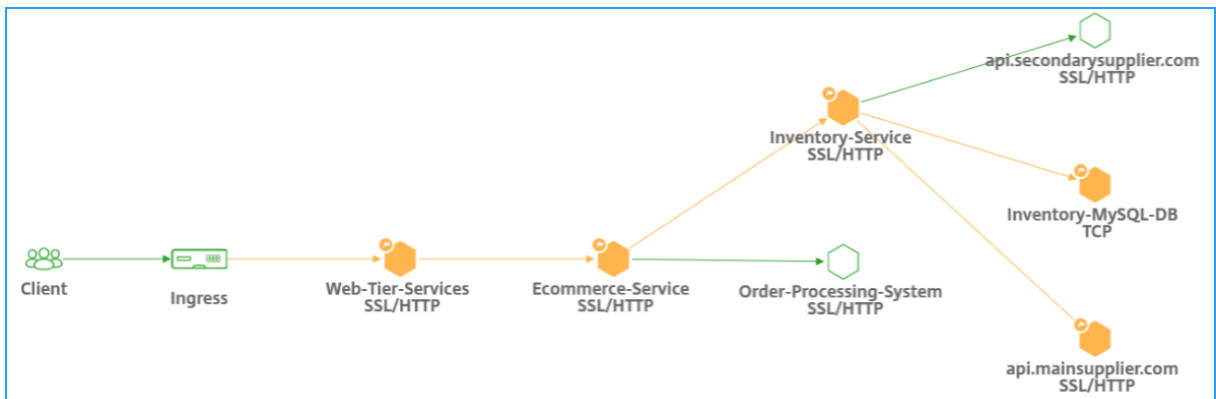


注

NetScaler ADM でアクティブなトランザクションが受信されない場合は、NetScaler ADC インスタンスによって負荷分散されたサービスのみを表示できます。サービスの上にマウスポインタを置くと、すべてのメトリックが 0 として表示されます。

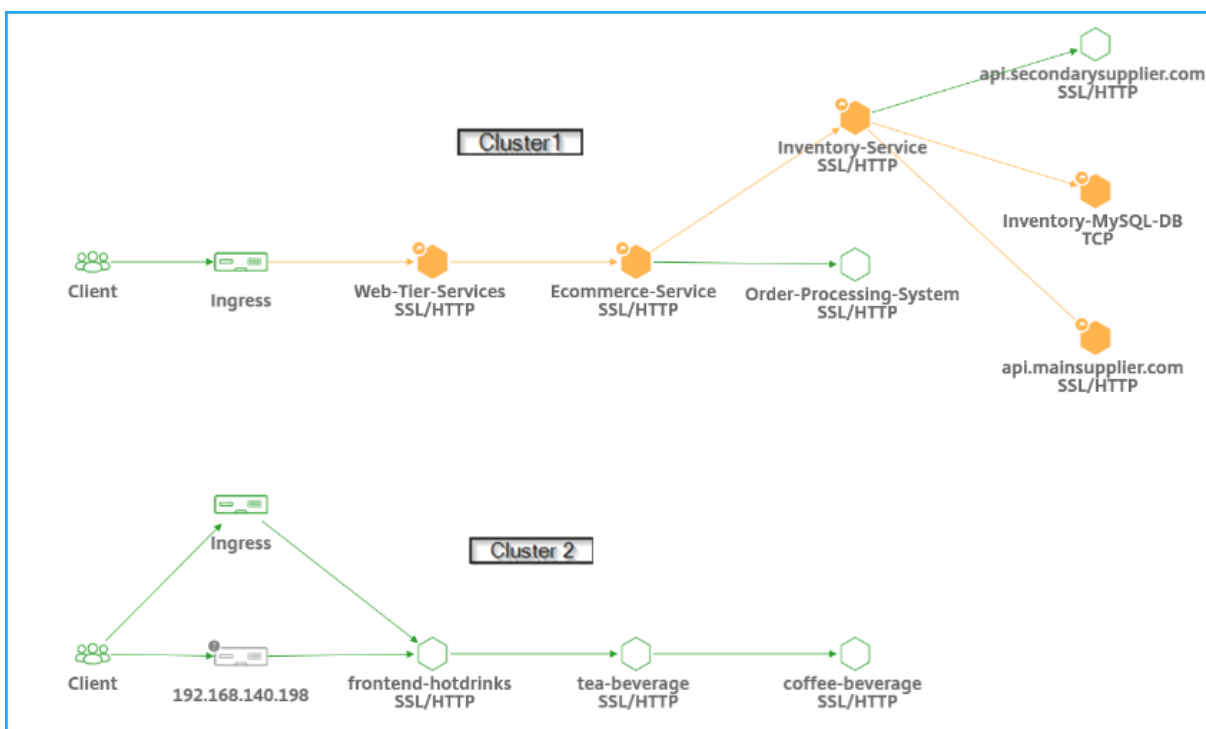


サービスグラフは、サービスが使用するプロトコルとともに表示されます。次の図に示すように、Kubernetes クラスタで次のサービスが実行されているとします。



注

オーケストレーション > **Kubernetes** > **Clusters** で複数のクラスターを追加した場合は、各クラスターに関連付けられたサービスを表示できます。



サービスの次のステータスを表示できます。

- **重大 (赤)** -平均サービス応答時間が 200 ミリ秒を超え、エラーカウントが 0 より大きいことを示します。
- **Review (オレンジ)** -平均サービス応答時間が 200 ミリ秒を超えるか、エラーカウントが 0 より大きいことを示します。
- **良好 (緑)** -エラーがなく、平均サービス応答時間が 200 ミリ秒未満であることを示します

サービスで使用されるプロトコルを識別するための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 SSL over HTTP プロトコルを使用していることを示します。
- **SSL、TCP** –サービスが SSL over TCP プロトコルを使用していることを示します。

注

プロトコルのないサービスは、サービスが 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た主要なメトリックの傾向の表示

表形式ビューを使用すると、次の項目を確認できます。

- サービスの主なメトリック
- ソースサービスと宛先サービス間の主要なメトリック

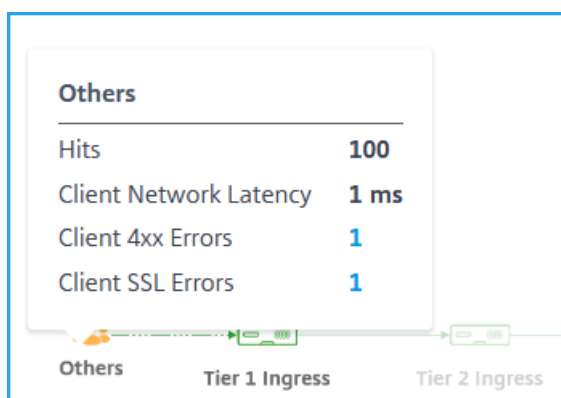
| Service               | Service To Service | STATUS   | HITS    | RESPONSE TIME (P99) | ERRORS | DATA VOLUME |
|-----------------------|--------------------|----------|---------|---------------------|--------|-------------|
| netflix-frontend      |                    | Good     | 476.9 K | 167 ms              | 0      | 315 MB      |
| recommendation-engine |                    | Critical | 272.5 K | 141 ms              | 68.1 K | 229 MB      |
| telemetry-store       |                    | Review   | 272.5 K | 14 ms               | 68.1 K | 226 MB      |
| metadata-store        |                    | Review   | 204.4 K | 33 ms               | 0      | 169 MB      |
| tv-shows              |                    | Review   | 136.3 K | 84 ms               | 0      | 108 MB      |

管理者は、これらの主要なメトリックを使用して、選択した期間におけるゴールデンシグナルの傾向を分析できます。

### クライアントメトリックの表示

クライアントがサービスにアクセスしている場所を表示できます。管理者は、クライアントメトリックスを視覚化し、クライアントから発生する問題を分析できます。

クライアントリージョンにマウスポインタを合わせると、メトリックスが表示されます。



- **Hits** -クライアントが受信したヒット数の合計を示します。
- **クライアントネットワーク待ち時間** -平均クライアントネットワーク遅延を示します。
- **クライアント 4xx エラー** -クライアントの 4xx エラーの合計を示します。
- **クライアント SSL エラー** -クライアントの SSL エラーの合計を示します。

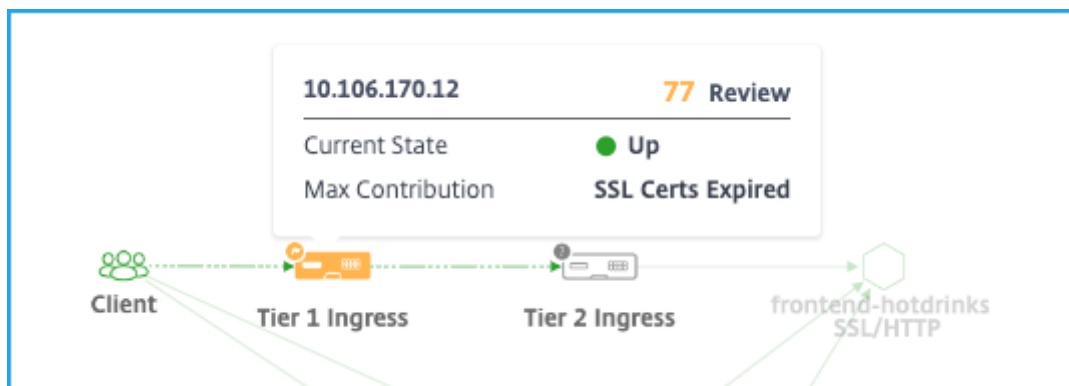
**NetScaler ADM の IP ブロック** -クライアントがパブリック IP アドレスを使用している場合、NetScaler ADM はクライアントの場所を認識できます。NetScaler ADM には組み込みの場所 CSV ファイルがあり、これはクライアントの IP アドレス範囲に基づいて場所と一致します。

NetScaler ADM は、IP アドレスが NetScaler ADM サーバーに追加される場合のみ、プライベート IP アドレスを使用して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 ADM は、トラフィックがこのクライアントの都市 A から発信されていることを認識します。

詳細については、「[プライベート IP ブロックを作成する](#)」を参照してください。

## 入力メトリックの表示

Kubernetes クラスタで使用されている入力のタイプを表示できます。



- NetScaler ADC IP アドレスとそのスコア
- 現在の状態: NetScaler ADC インスタンスが稼働中、停止中、または状態外のいずれであるかを示す
- [最大コントリビューション] – インスタンススコアに影響している問題を示します。

単一層トポロジでは、単一の **Ingress** だけを表示できます。

[**Ingress**] をクリックして、さらにドリルダウンして詳細を表示します。詳細については、「[イングレス詳細の表示](#)」を参照してください。

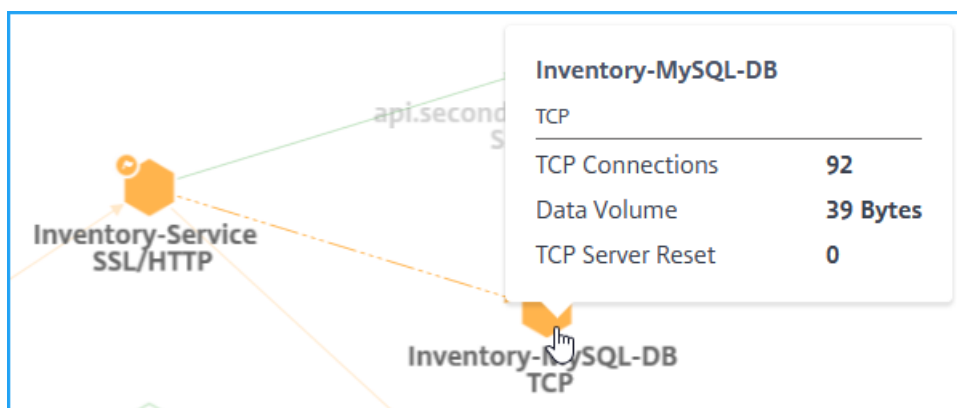
## TCP および SSL メトリックの表示

TCP メトリックと SSL メトリックを使用すると、次のことができます。

- サービス間の TCP 接続の詳細を表示する
- TCP 関連の問題が送信元サービスにあるのか、宛先サービスにあるのかを判断します
- SSL エラーが送信元または宛先サービスのどちらからのものかを表示する
- SSL サービスが使用する SSL プロトコルのバージョンの表示

### TCP メトリクス

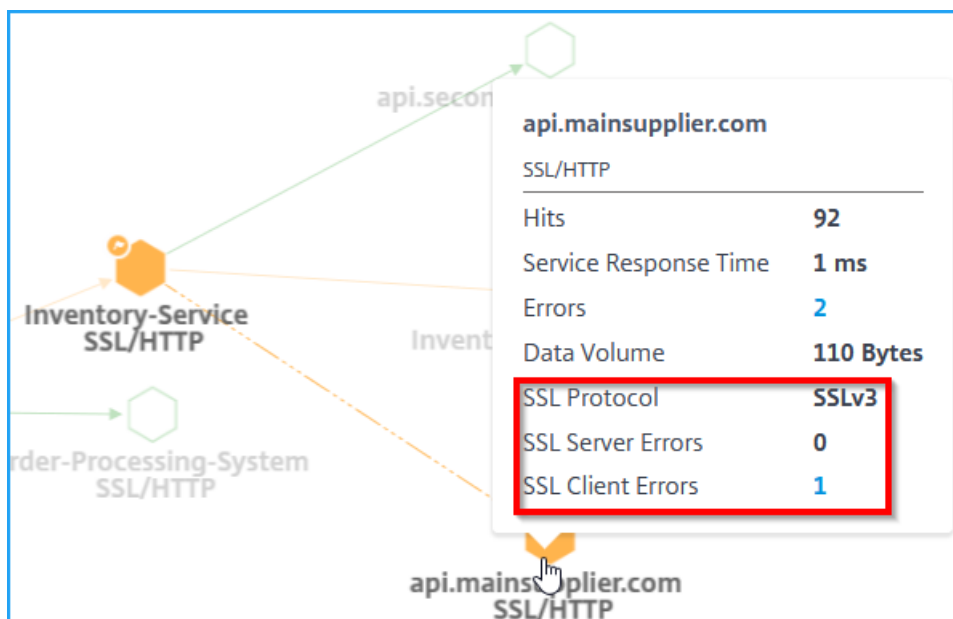
TCP サービスまたは関連する受信サービスの上にマウスポインターを置くと、TCP メトリックが表示されます。



- **TCP** 接続—サービス間で確立された接続の総数
- データ量—サービスによって処理されたデータの総数
- **TCP** サーバーリセット—サーバーから開始された TCP リセットの合計数

### 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置くと、SSL メトリックが表示されます。



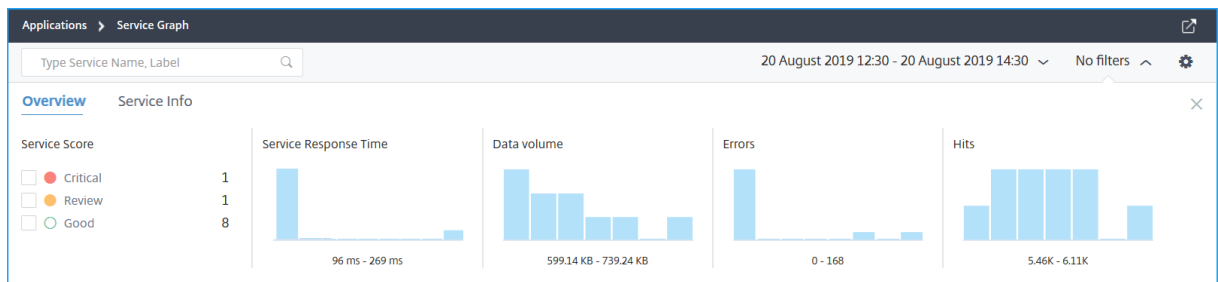
- **SSL** サーバーエラー—サーバーで発生した SSL エラーの合計数を示します。(たとえば、SSL 証明書が不明な場合)
- **SSL** プロトコル—サービスが使用する SSL プロトコルのバージョンを示します。
- **SSL** クライアントエラー—クライアントで発生した SSL エラーの合計数を示します。(SSL クライアント認証エラーなど)

## サービスの詳細の表示

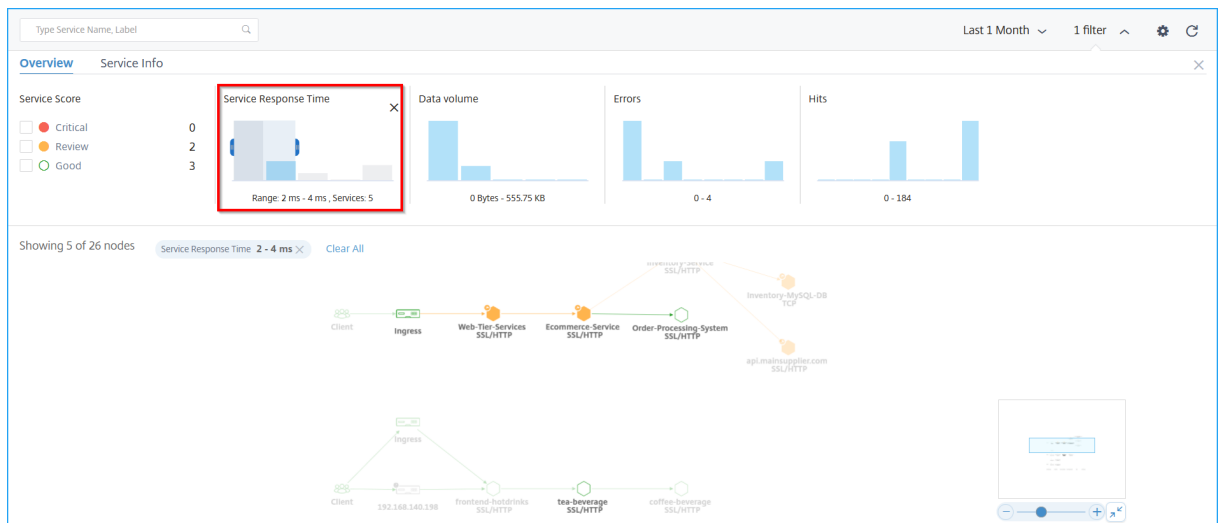
サービスをクリックし、[ **View Details** ] を選択して、サービスの詳細を表示します。詳細については、「サービスの詳細を表示する」を参照してください。

## フィルタの適用

フィルターを適用して特定のサービス情報を表示できます。フィルターオプションを表示するには、[ フィルターリストなし ] をクリックします。



たとえば、遅延が 150 ミリ秒未満のサービスを表示するには、[ サービス応答時間 ] の下の棒グラフをクリックして結果を表示します。



[ サービス情報 ] をクリックして、次のフィルタを選択して適用します。

- [ **Cluster** ]: 選択した 1 つ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が表示されます。
- [ **Namespace** ]: 選択したネームスペースに適用可能なすべてのサービスが表示されます。

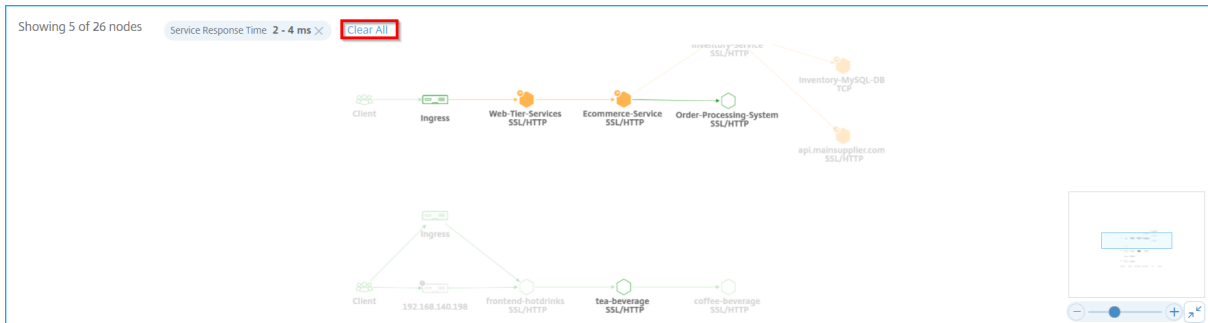
| Cluster Name                          | Namespace                                     | app                                           | tier                              | role                            |
|---------------------------------------|-----------------------------------------------|-----------------------------------------------|-----------------------------------|---------------------------------|
| <input type="checkbox"/> Test_Cluster | <input type="checkbox"/> sg-demo              | <input type="checkbox"/> Others               | <input type="checkbox"/> Others   | <input type="checkbox"/> Others |
| <input type="checkbox"/> cluster-2    | <input type="checkbox"/> default              | <input type="checkbox"/> redis                | <input type="checkbox"/> backend  | <input type="checkbox"/> master |
| <input type="checkbox"/> shopping-app | <input type="checkbox"/> sg-onprem-masvc      | <input type="checkbox"/> lb-service-hotdrinks | <input type="checkbox"/> frontend | <input type="checkbox"/> slave  |
| <input type="checkbox"/> NA           | <input type="checkbox"/> sg-onprem-masvc-s... | <input type="checkbox"/> guestbook            |                                   |                                 |
|                                       | <a href="#">+ 4 more</a>                      | <a href="#">+ 13 more</a>                     |                                   |                                 |
|                                       | 70                                            | 57                                            | 98                                | 142                             |
|                                       | 49                                            | 44                                            | 16                                | 16                              |
|                                       | 45                                            | 19                                            | 9                                 | 8                               |
|                                       | 2                                             | 19                                            | 8                                 | 8                               |



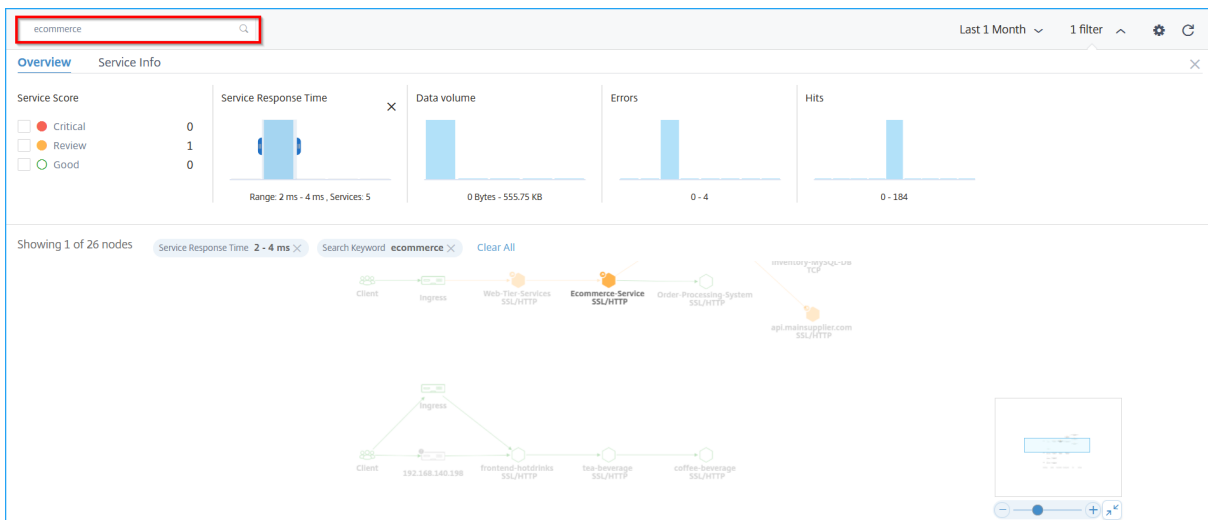
注

Kubernetes サービス定義 YAML でサービスに対して構成されたラベルによっては、より多くのフィルターオプションを表示することもできます。

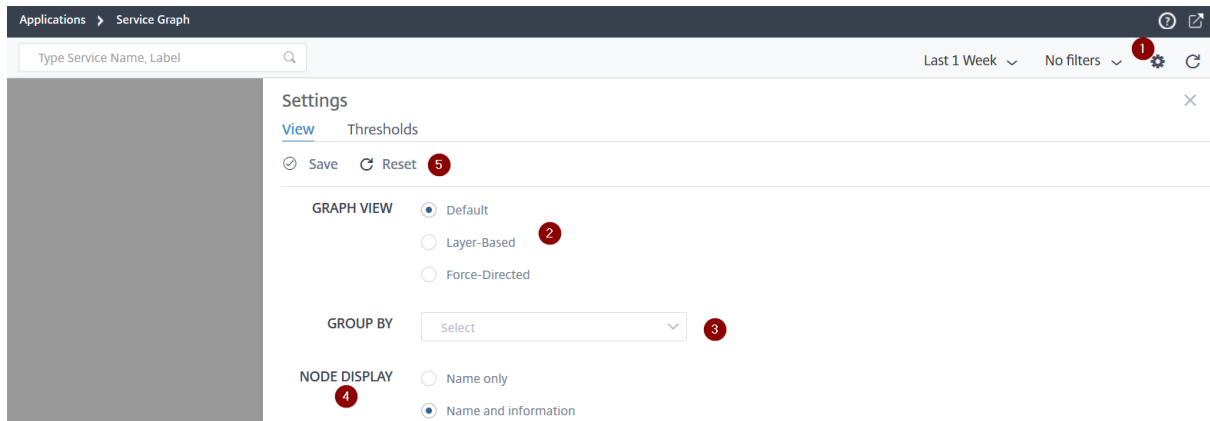
すべてのフィルタをクリアするには、[すべてクリア]をクリックします。



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て、結果をサービスグラフに表示することもできます。



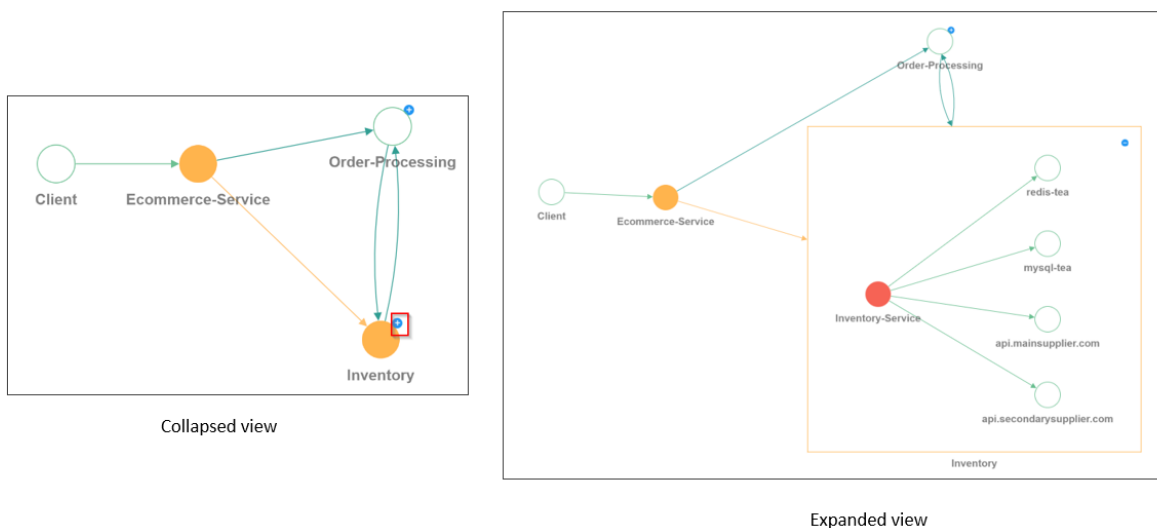
設定オプションを使用する



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、または強制指向のビューとして表示するオプション

3 –リストからオプションを選択すると、カテゴリに基づいてサービスが表示されます。リストからカテゴリを選択したら、グラフの [ + ] をクリックしてすべてのサービスを表示します



4 : サービスの表示方法に関するオプションを選択できます。

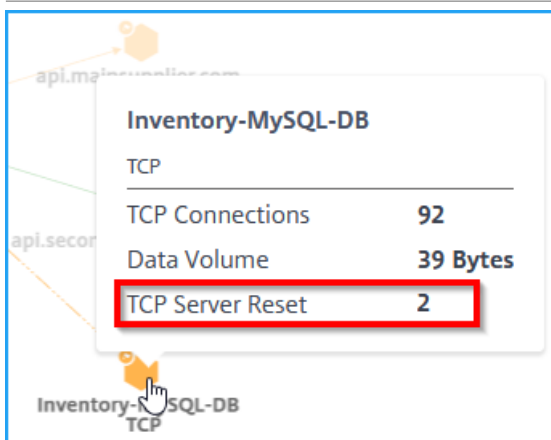
5 -設定を保存するか、デフォルトにリセットするオプション。

エラーを分析

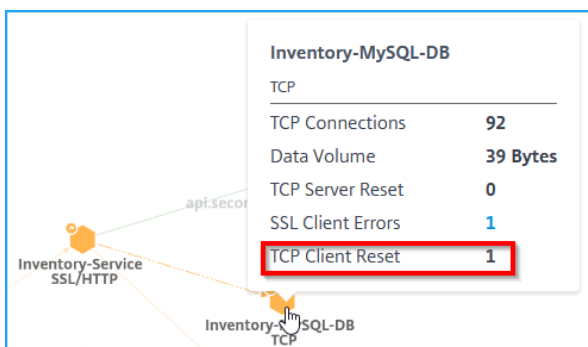
エラーを示すサービスにマウスポインターを置きます。

エラー

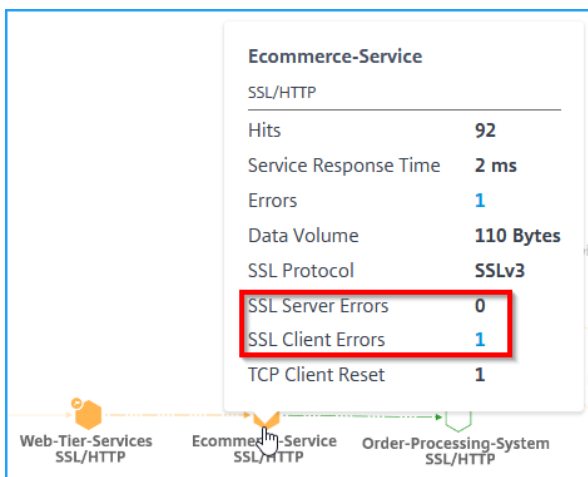
説明



**TCP** サーバリセットは、サーバーから開始された TCP リセットの合計数を示します。



**TCP** クライアントリセットは、クライアントによって開始された TCP リセットの合計数を示します。



SSL クライアントエラーは、クライアントからの SSL エラーの合計数を示します。(SSL クライアント認証エラーなど)。  
 SSL サーバーエラーは、サーバーで発生した SSL エラーの合計数を示します。(たとえば、SSL 証明書が不明な場合)

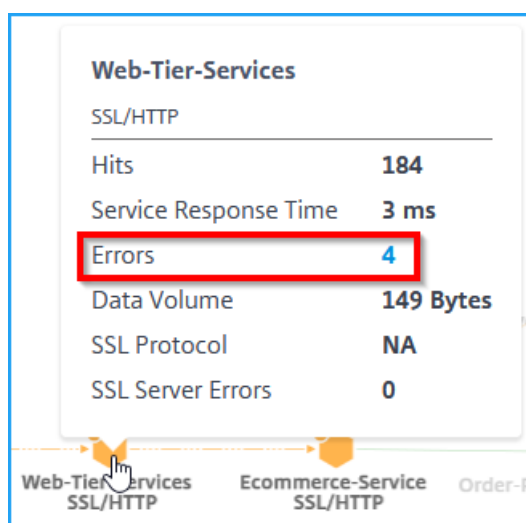
注

- クライアントエラー数が **1** 以上の場合、クライアントエラー数は (プロトコルタイプに関係なく) どのサービスでも表示されます。
- どのサービスについてもクライアントエラー数が表示されるため、エラーはクライアント側からのものであることが分かります。

### HTTP トランザクションの詳細を表示する

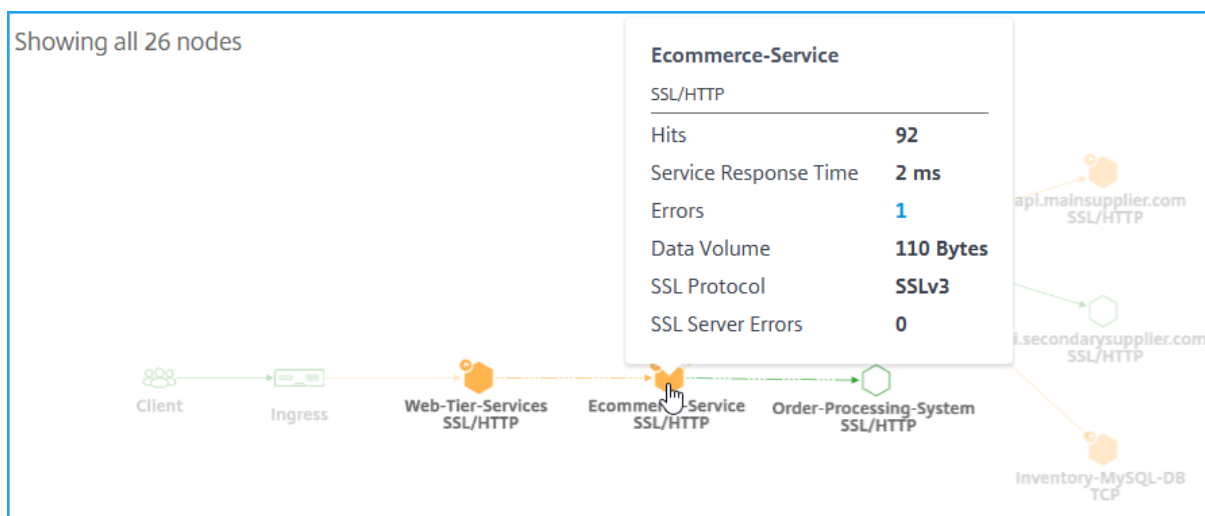
注

エラーを表示するには、誤ったサービスの上にマウスポインタを置いて、問題数をクリックします。

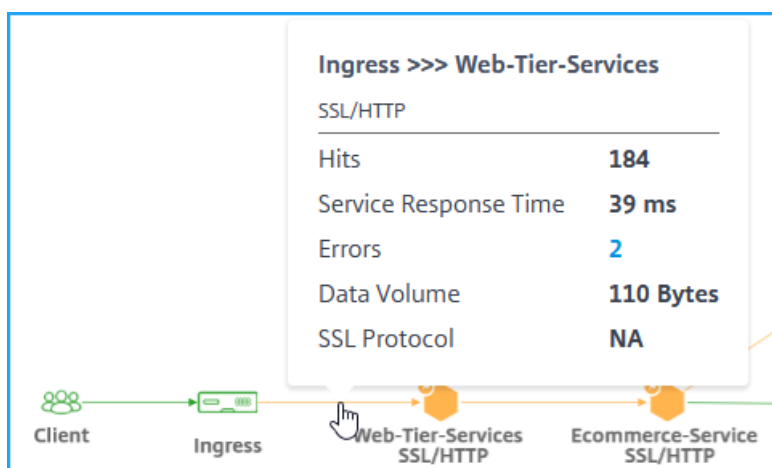


この図に示されている例では、コンポーネントサービスの通信方法を示すアプリケーションのエンドツーエンドのネットワークマップを表示できます。

E コマースサービスにマウスポインターを合わせると、E \*\* コマースサービスのメトリックの詳細が表示されます \*\*。



NetScaler ADM では、Ingress とサービス間のトランザクションの詳細を表示することもできます。マウスポインターにカーソルを合わせると、Ingress とサービスの間の合計エラー数や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—最初のバイトまでの時間 (TTFB) でサービスが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 などのエラーの合計を示します。

「データボリューム」—サービスによって処理されるデータの合計量を示します。

「SSL プロトコル」—SSL プロトコルのバージョンを示します。

[ Ingress ] と [ service ] の間の矢印をクリックして、詳細なトランザクションを表示します。

詳細については、「[Web トランザクションの分析を表示する](#)」を参照してください。

## サービスグラフでのしきい値の設定

February 6, 2024

管理者として、Kubernetes サービスのしきい値を設定できます。NetScaler ADM では、サービスの応答時間とエラー数に基づいて、サービスの状態（重大、レビュー、および良好）が表示されます。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

デフォルトしきい値は削除できません。

新しいしきい値を設定するには、次の手順を実行します。

サービスグラフ内:

1. 設定アイコンをクリックし、[しきい値] タブを選択します。
2. 新しいしきい値をクリックして新しいしきい値を設定します。

The screenshot shows the 'Settings' page with the 'Thresholds' tab selected. A notification banner at the top explains that service statuses are determined by factor thresholds. Below the banner, there is a 'Default Thresholds' section. On the right side of this section, a blue button labeled 'New Threshold' is highlighted with a red rectangular box. The main content area shows a table with the following data:

| Default Thresholds         |              |
|----------------------------|--------------|
| Name                       | Applied to   |
| Default Thresholds         | All Services |
| Thresholds                 |              |
| High Service Response Time | 200 ms       |
| High Errors                | 0            |

「新規しきい値」ページが表示されます。

3. 次のパラメータを設定します。
  - a) 「名前」 — しきい値の名前を指定します。
  - b) 「マイクロサービス」で、しきい値を適用するサービスを選択します。
  - c) 「しきい値」で、「応答時間が長く、エラーが多い」には「シングル」または「ダブル」を選択します。
  - d) しきい値を指定します。

注

ダブルしきい値を選択する場合は、次の点を確認してください。

- しきい値 1 の値は、しきい値 2 の値よりも小さいです。たとえば、しきい値 1 を 250 ミリ秒に設定する場合、しきい値 2 は 251 ミリ秒以上にする必要があります。
- しきい値 1 の値は、しきい値 2 と同じにはできません。

4. [保存] をクリックします。

Settings

← New Threshold

---

Name \*

Microservices

Apply to  Services

Select Remove

| <input type="checkbox"/> | MICROSERVICE NAME | NAMESPACE | CLUSTER |
|--------------------------|-------------------|-----------|---------|
| No rows found            |                   |           |         |

Thresholds

|                            |                                |                         |
|----------------------------|--------------------------------|-------------------------|
| Type ⓘ                     | Threshold 1                    | Threshold 2             |
| High Service Response Time | Double <input type="text"/> ms | <input type="text"/> ms |
| High Errors                | Single <input type="text"/>    |                         |

Save Cancel

しきい値は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表示できます。

単一しきい値

単一のしきい値を構成すると、NetScaler ADM:

- 現在の値と設定されたしきい値を比較します
- 超過したしきい値を基にペナルティ合計を計算します
- ペナルティ計算に基づくサービススコアとサービスステータスを表示します。

## 二重しきい値

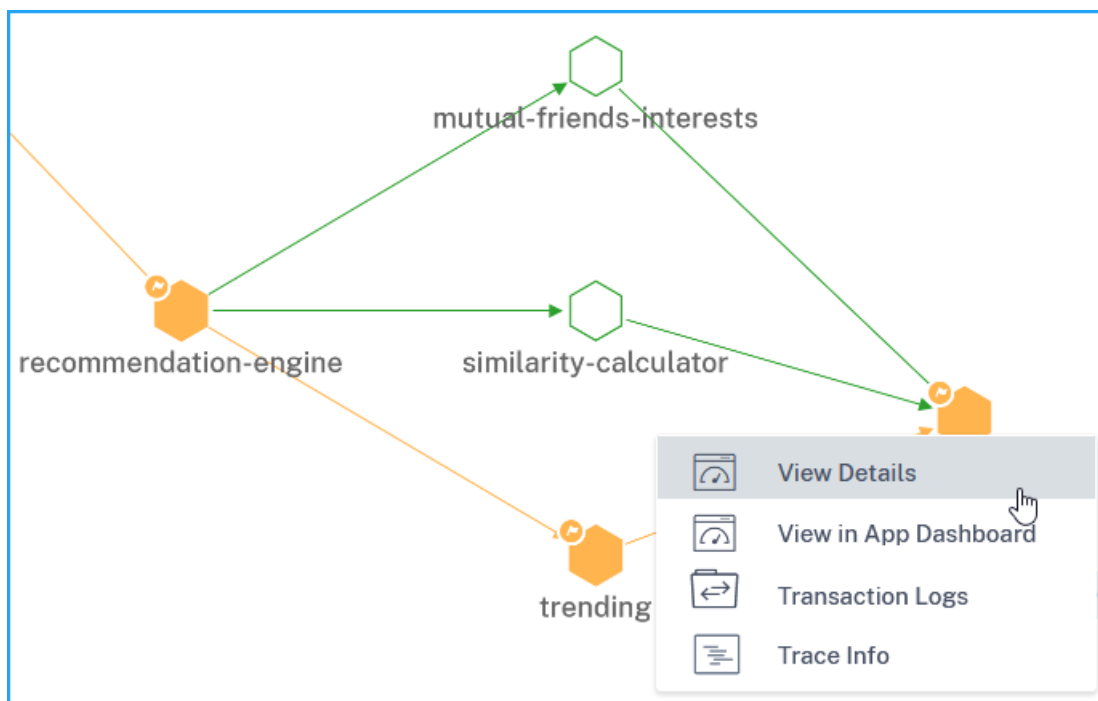
二重しきい値を構成すると、NetScaler ADM:

- 現在の値と設定されたしきい値を比較します
- 現在の値が次の値であるかどうかを調べます。
  - しきい値 1 より小さい
  - しきい値 1 としきい値 2 の間
  - しきい値 2 より大きい
- 超過したしきい値を基にペナルティ合計を計算します
- ペナルティ計算に基づくサービススコアとサービスステータスを表示します。

## サービスの詳細の表示

February 6, 2024

サービスをクリックし、[詳細の表示] を選択します。

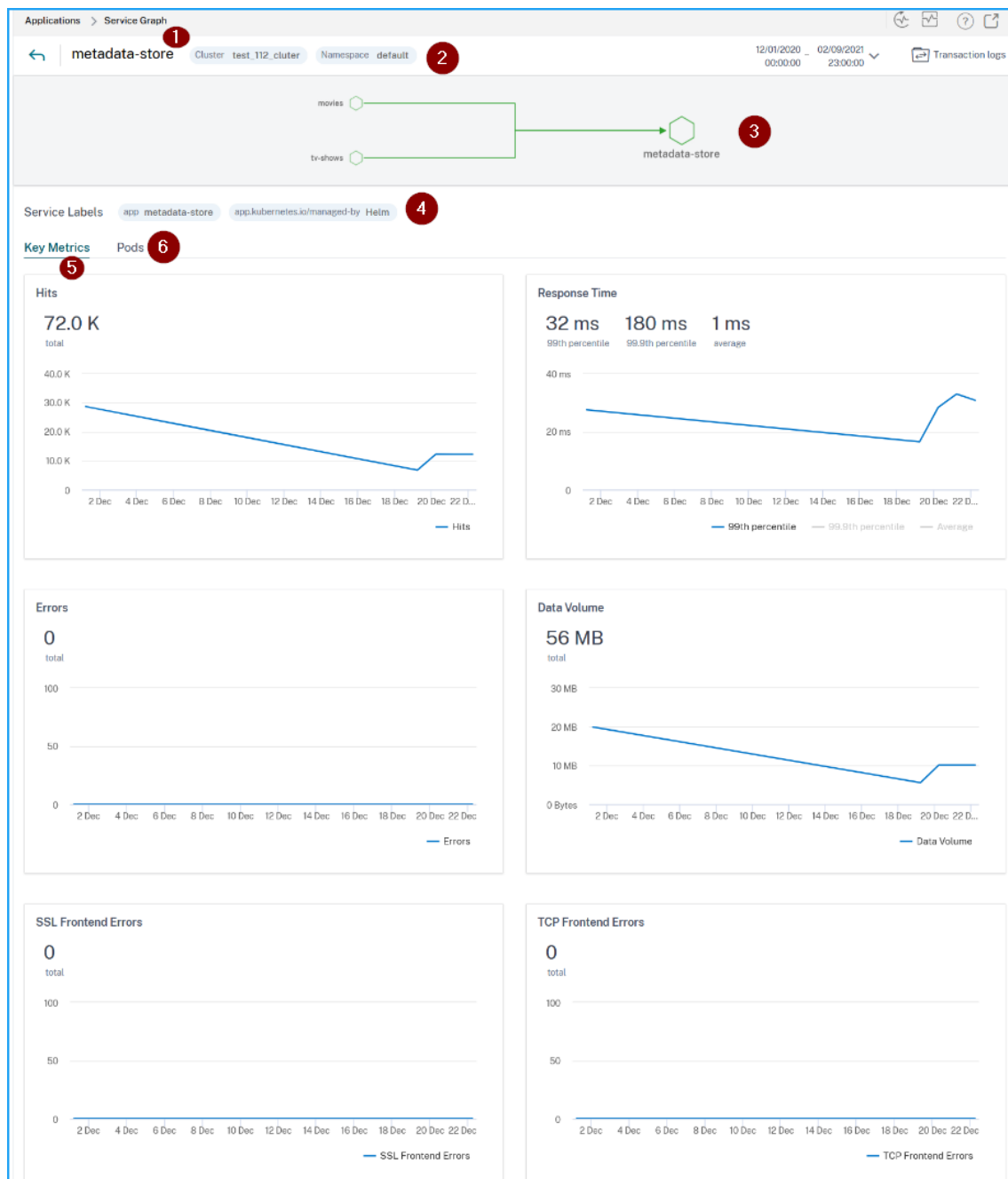


サービスの詳細ページでは、次の項目を表示できます。

- サービスがホストされているクラスター名 (1)



- サービスの名前空間とサービスラベル (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着信および発信サービス (3)
- ヒット、レスポンス時間、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 (5) などのグラフ形式のサービスキーメトリック。
- サービスに関連付けられたバックエンド Pod (6)。



これらの主要な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。

レスポンス時間メトリックでは、次の項目を表示できます。

- **99** パーセンタイル： 選択した期間の要求の 99% が 32 ミリ秒未満であることを示します（画像例による）。
- **Average**： 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—サービスからの応答時間が最も高いことを示します

### メトリックスの詳細

| メトリックス         | 説明                                                     |
|----------------|--------------------------------------------------------|
| ヒット数           | サービスによって受信されたリクエストの総数                                  |
| エラー            | サービスからの HTTP エラーの合計                                    |
| サービス応答時間       | 最初のバイトまでの時間（TTFB）の応答にサービスから要した平均応答時間。                  |
| データ量           | サービスによって処理された合計データ量                                    |
| 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：<br>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。<br>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：<br>TCP サーバのリセット            |
| TCP フロントエンドエラー | サービスからの TCP フロントエンドエラーの合計。<br>例:TCP クライアントのリセット        |

### バックエンドポッドの詳細を表示する

[ **Pods** ] タブをクリックして、サービスに関連付けられたバックエンド Pod を表示します。

The screenshot shows the configuration page for the 'telemetry-store' service in the NetScaler GUI. At the top, there are tabs for 'mutual-friends-interests', 'similarity-calculator', and 'trending', all pointing to the 'telemetry-store' service. Below this, the 'Service Labels' section shows 'app telemetry-store'. Under 'Key Metrics', the 'Pods' tab is highlighted with a red box. A 'Poll Now' button is visible on the right. The main content area displays a table with the following data:

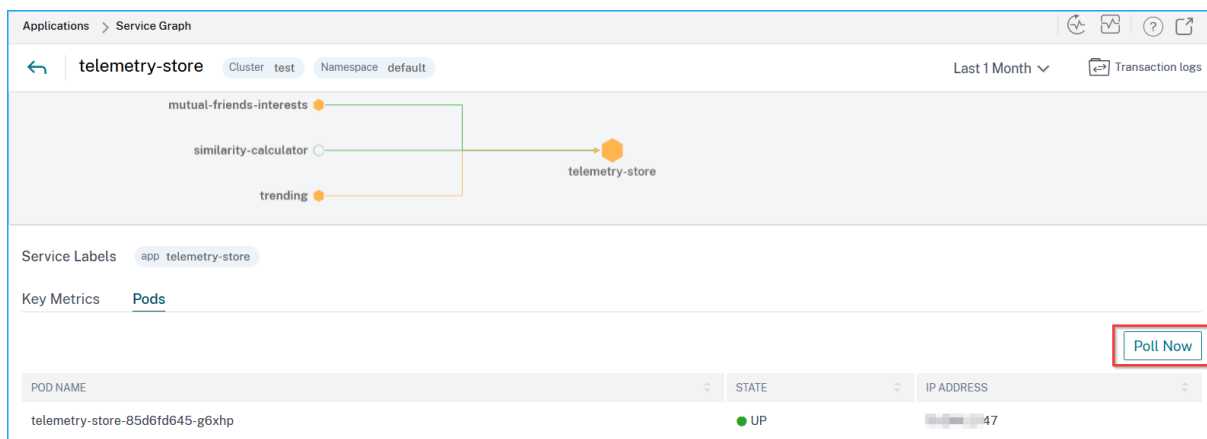
| POD NAME                        | STATE | IP ADDRESS |
|---------------------------------|-------|------------|
| telemetry-store-85d6fd645-g6xhp | ● UP  | 10.10.10.7 |

- ポッド名—ポッド名を示します

- **Status** –Pod が実行中 (UP) かそうでないか (DOWN) を示します。
- **IP アドレス**–ポッドの IP アドレスを表します。

[今すぐ投票] オプションを使用して **Pod** のステータスを取得します

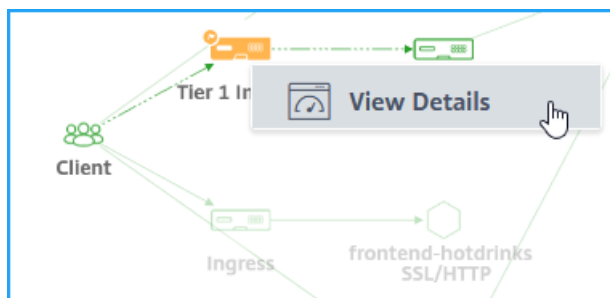
[ **Poll Now** ] オプションは、クラスターから最新の Pod ステータスを取得します。



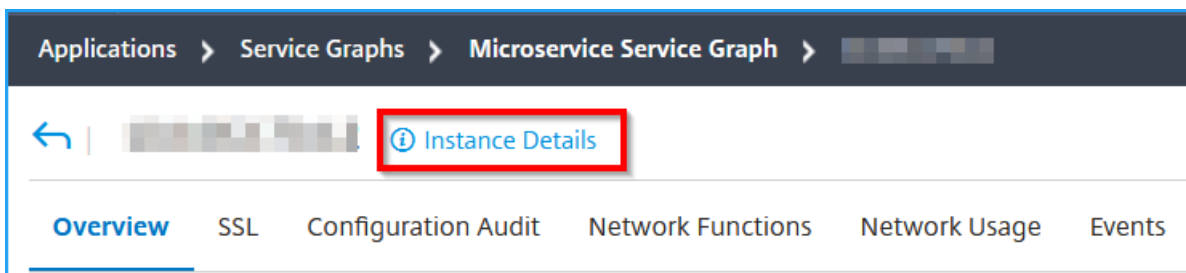
問題のトラブルシューティングに関する進入の詳細の表示

February 6, 2024

サービスグラフで、入力をクリックし、[詳細の表示] を選択して、Kubernetes クラスター用に構成されている NetScaler ADC インスタンスの詳細を視覚化します。



[ インスタンスの詳細 ] をクリックして詳細を表示します。



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。

| [redacted] - Details  |                                         |                       |                                     |
|-----------------------|-----------------------------------------|-----------------------|-------------------------------------|
| <b>Information</b>    |                                         |                       |                                     |
| HOST NAME             | [redacted]                              | MODEL ID              | 2000                                |
| SYSTEM IP ADDRESS     | [redacted]                              | SYSTEM CUSTOM ID      | Default                             |
| SYSTEM NAME           | NetScaler                               | PACKET ENGINES        | 1                                   |
| TYPE                  | NetScaler CPX                           | SSL CARDS             | 0                                   |
| HA MASTER STATE       | Primary                                 | CPU                   | 3501MHZ                             |
| NODE STATE            | <span style="color: green;">↑</span> Up | VERSION               | NS13.1: Build 49.13.nc              |
| PEER IP ADDRESS       | --                                      | HARDWARE VERSION      | ADC CPX                             |
| SECONDARY NODE STATUS | --                                      | LOM VERSION           | -NA-                                |
| HA SYNC STATUS        | ENABLED                                 | HOST ID               | nscpx-netscal                       |
| SYSTEM SERVICES       | 72                                      | SERIAL NUMBER         | -ingress-controller-[redacted]-     |
| NETMASK               | [redacted]                              | ENCODED SERIAL NUMBER | -ingress-controller-[redacted]-     |
| GATEWAY               | [redacted]                              | NetScaler ADC UUID    | a48d554d-9082-4899-bb59-c[redacted] |
| ADMIN PROFILE         | 10.128.3.202_cpx_profile                | LOCATION              | POP (default)                       |
| HEALTH                | --                                      | CONTACT PERSON        | WebMaster (default)                 |
| MAINTENANCE TYPE      | --                                      | MAINTENANCE END DATE  | 0                                   |
| UPTIME                | --                                      |                       |                                     |
| DESCRIPTION           | --                                      |                       |                                     |

- 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。[ライセンス機能] をクリックすると、ライセンスされている機能が表示されます。

### Features

All features are licensed except the following:

| License Type        | Advanced | Licensing Mode       | Pooled |
|---------------------|----------|----------------------|--------|
| Model ID            | 2000     | Web Interface        | ×      |
| Integrated Caching  | ×        | Application Firewall | ×      |
| CloudBridge         | ×        | Priority Queuing     | ×      |
| Sure Connect        | ×        | DoS Protection       | ×      |
| Content Accelerator | ×        | vPath                | ×      |
| RISE                | ×        | Reputation           | ×      |
| Delta Compression   | ×        | URL Filtering        | ×      |
| Video Optimization  | ×        |                      |        |

[Licensed Features >](#)

- 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。「有効化されたモードを表示」をクリックすると、インスタンスで有効になっているモードが表示されます。

### Modes

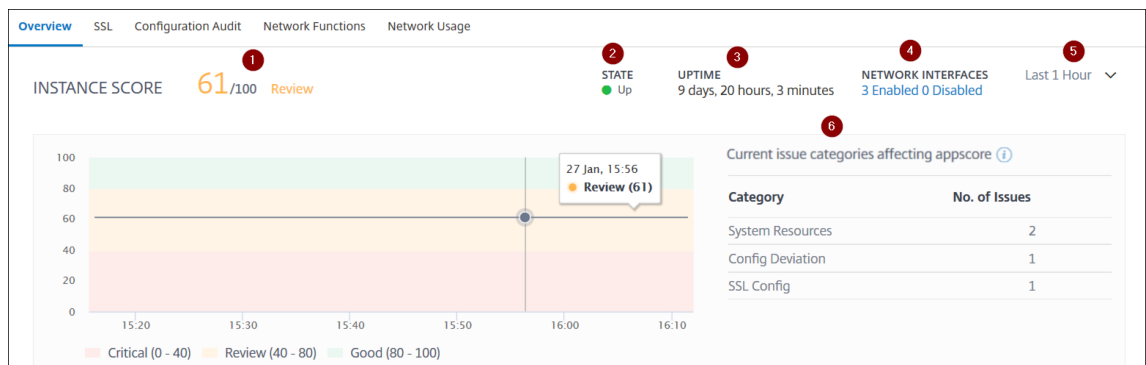
All modes are enabled except the following:

|                              |   |                                 |   |
|------------------------------|---|---------------------------------|---|
| Bridge BPDUs                 | × | Client side Keep Alive          | × |
| Direct Route Advertisement   | × | IPv6 Direct Route Advertisement | × |
| Intranet Route Advertisement | × | Layer 2 Mode                    | × |
| MAC based forwarding         | × | Media Classification            | × |
| RISE APBR                    | × | RISE RHI                        | × |
| Static Route Advertisement   | × | IPv6 Static Route Advertisement | × |
| TCP Buffering                | × | Use Source IP                   | × |
| Unified Logging Format       | × |                                 |   |

[View Enabled Modes ▾](#)

インスタンスダッシュボードにはインスタンスの概要が表示され、次の詳細を確認できます。

- インスタンススコア

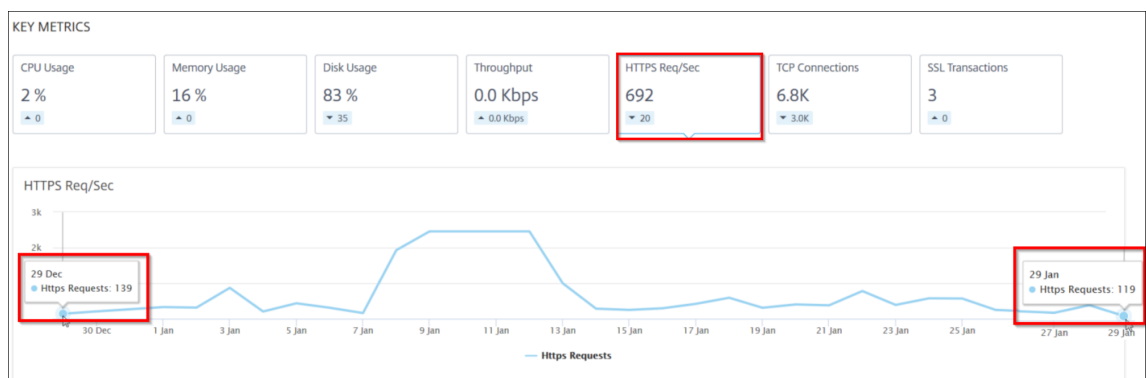


- 1—選択した期間における現在の NetScaler ADC インスタンスのスコアを示します。最終スコアは、**100** から合計ペナルティを引いたものとして計算されます。グラフには、選択した期間のスコア範囲が表示されます。
- 2： NetScaler ADC インスタンスの現在のステータス（[アップ]、[停止]、[サービス外] など）を示します。
- 3—NetScaler ADC インスタンスが起動して実行されている期間を示します。
- 4—インスタンスで有効化されているネットワークインタフェースと無効化されているネットワークインタフェースの合計数を示します。クリックすると、ネットワークインターフェ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—インスタンスの詳細を表示する期間をリストから選択します。
- 6—ADC インスタンスの全問題と問題カテゴリを表示します。

• 主要指標

各タブをクリックすると、詳細が表示されます。各指標で、選択した時間の平均値と差分値を表示できます。

次の図は、HTTPS 要求/秒の例で、選択した期間は過去 1 か月間です。値 **692** は過去 1 か月の平均 HTTPS 要求/秒で、値 **20** は差の値です。グラフでは、最初の値は **139**、最後の値は **119** です。差の値は **139 – 119 = 20** です。



選択した期間について、次のインスタンスメトリックスをグラフ形式で表示できます。

- **CPU 使用率**—選択した期間におけるインスタンスの平均 CPU%（パケット CPU と管理 CPU の両方で表示）。
- **Memory Usage**—選択した期間におけるインスタンスの平均メモリ使用率（%）。

- ディスク使用量—選択した期間におけるインスタンスの平均ディスク容量 (%)。
- スループット—選択した期間にインスタンスが処理した平均ネットワークスループットです。
- **HTTPS** リクエスト/秒—選択した期間にインスタンスが受信した HTTPS リクエストの平均。
- **TCP** 接続—選択した期間にクライアントとサーバーによって確立された TCP 接続の平均値。
- **SSL** トランザクション—選択した期間にインスタンスが処理した SSL トランザクションの平均です。

• 問題点

NetScaler ADC インスタンスで発生する次の問題を確認できます。

| 問題カテゴリ   | 説明                                                         | 問題                                                                                                                                                                                                  |
|----------|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| システムリソース | CPU、メモリ、ディスク使用率など、NetScaler ADC 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。 | <ul style="list-style-type: none"> <li>- 高い CPU 使用率</li> <li>- 高いメモリ使用量</li> <li>- 高いディスク使用量</li> <li>- SSL カード障害</li> <li>- 停電</li> <li>- ディスクエラー</li> <li>- フラッシュエラー</li> <li>- NIC 廃棄</li> </ul> |
| SSL 設定   | NetScaler ADC インスタンスの SSL 構成に関連するすべての問題を表示します。             | <ul style="list-style-type: none"> <li>-SSL 証明書の有効期限切れ</li> <li>- 推奨されない発行者</li> <li>- 推奨されないアルゴリズム</li> <li>- 推奨キーストレンクスではありません</li> </ul>                                                         |
| 設定偏差     | NetScaler ADC 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。          | <ul style="list-style-type: none"> <li>-構成ドリフト</li> <li>- 実行とテンプレート</li> </ul>                                                                                                                      |

| 問題カテゴリ | 説明                                                                                                                     | 問題                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| 容量の問題  | ADC 容量の問題を表示します。ADM は、ADC インスタンスから 5 分ごとにこれらのイベントをポーリングし、パケットドロップまたはレート制限カウンタが存在する場合は、その増加を表示します。問題は、次の容量パラメータに分類されます。 | - スループット制限に達しました                                              |
| 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、「 <a href="#">新しい指標によるインフラストラクチャ分析の強化</a> 」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に次のエラーが発生したとします。

| CERTIFICATE NAME      | DAYS TO EXPIRY    | STATUS | DOMAIN         | SIGNATURE          | ISSUER         |
|-----------------------|-------------------|--------|----------------|--------------------|----------------|
| ns-server-certificate | 15 years 306 days | Valid  | default UZEKYL | sha256WithRSAEn... | default UZEKYL |

- [ **Current** ] タブには、インスタンススコアに影響している現在の ADC 運用上の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ストラクチャの問題が表示されます。

## 分散トレース

February 6, 2024



サービスグラフでは、ディストリビューティッド（分散）トレーシングビューを使用して次のことができます。

- サービス全体のパフォーマンスを分析します。
- 選択したサービスとその相互依存サービス間の通信フローを視覚化します。
- エラーを示すサービスを特定し、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相互依存サービス間のトランザクションの詳細を表示します。

#### 前提条件

サービスのトレース情報を表示するには、次の操作を行う必要があります。

- East-West トラフィックを送信する間、アプリケーションが次のトレースヘッダーを保持していることを確認します。

- `x-request-id`
- `x-b3-traceid`
- `x-b3-spanid`
- `x-b3-parentspanid`
- `x-b3-sampled`
- `x-b3-flags`
- `x-ot-span-context`

- **1.7.23** より前の **CIC** ビルドの場合、`CPX NS_DISTRIBUTED_TRACING` YAML ファイルをおよび値として更新します `yes`

```
1  apiVersion: apps/v1
2  kind: Deployment
3  metadata:
4    name: cpx-ingress
5  spec:
6    selector:
7      matchLabels:
8        app: cpx-ingress
9    replicas: 1
10   template:
11     metadata:
12       name: cpx-ingress
13     labels:
14       app: cpx-ingress
15     annotations:
16     spec:
17       serviceAccountName: cpx-ingress-k8s-role
18     containers:
19     - name: cpx-ingress
20       image: "quay.io/citrix/citrix-k8s-cpx-ingress:13.0-47.103"
21       securityContext:
22         privileged: true
23       env:
24         - name: "EULA"
25           value: "yes"
26         - name: "KUBERNETES_TASK_ID"
27           value: ""
28         - name: "NS_MGMT_SERVER"
29           value: "192.168.0.1"
30         - name: "NS_MGMT_FINGER_PRINT"
31           value: "12:12:AB:CD:EA:72:E3:10:47:CD:AF:AG:C3:B7:82:60:97:30:E2:5D"
32         - name: "NS_HTTP_PORT"
33           value: "9000"
34         - name: "NS_HTTPS_PORT"
35           value: "9443"
36         - name: "LOGSTREAM_COLLECTOR_IP"
37           value: "192.168.0.1"
38     imagePullPolicy: Always
```

- **1.7.23** 以降の **CIC** ビルドでは、ConfigMap を使用する必要があります。

ConfigMaps を使用すると、Pod から設定を分離し、ワークロードを移植することができます。ConfigMaps を使用すると、ワークロード構成を簡単に変更および管理でき、構成データを Pod 仕様にハードコードする必要性を軽減できます。

ConfigMap サポートでは、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 Pod を再起動する必要はありません。詳細については、[Ingress コントローラーに対する ConfigMap のサポートを参照してください](#)。

ConfigMap を使用すると、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。構成マップを使用するには、次の手順に従います。

1. 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り、監査ログ、イベント、トランザクションなどのその他の変数が無効になっています。

```
1  apiVersion: v1
2  kind: ConfigMap
3  metadata:
4    name: cic-configmap
5    namespace: default
6  data:
7    LOGLEVEL: 'debug'
8    NS_PROTOCOL: 'http'
9    NS_PORT: '80'
```

```

10  NS_HTTP2_SERVER_SIDE: 'ON'
11  NS_ANALYTICS_CONFIG:
12    distributed_tracing:
13      enable: 'true'
14      samplingrate: 100
15    endpoint:
16      server: <ADM-AgentIP> / <ADM-AppserverIP>
17    timeseries:
18      port: 5563
19    metrics:
20      enable: 'true'
21      mode: 'avro'
22    auditlogs:
23      enable: 'false'
24    events:
25      enable: 'false'
26    transactions:
27      enable: 'false'
28      port: 5557
29  <!--NeedCopy-->

```

## 注

0 から 100 まで `Samplingrate` の値を指定できます。NetScaler ADM には、上記のトレースランザクション数が表示されます。

2. 以下を使用して ConfigMap を展開します。

```
kubectl create -f <configmap-yaml>.yaml
```

3. CPX YAML ファイルを編集し、`envFrom` または `args` を使用して次の引数を指定します。

```

1  envFrom:
2    - configMapRef:
3      name: cic-configmap
4  <!--NeedCopy-->

```

または

```

args:
- --configmap
  default/cic-configmap

```

4. 任意の変数の値を変更する場合は、ConfigMap で値を編集します。この例では、他のすべての変数を **false** から **true** に変更しています。

```

1  apiVersion: v1
2  kind: ConfigMap
3  metadata:
4    name: cic-configmap
5    namespace: default

```

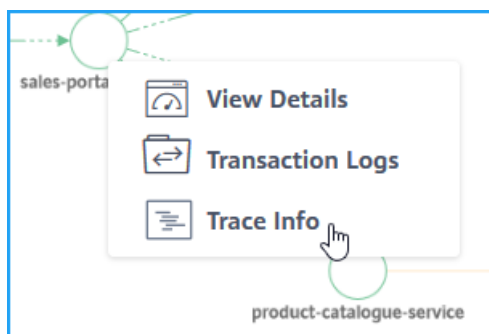
```
6 data:
7   LOGLEVEL: 'debug'
8   NS_PROTOCOL: 'http'
9   NS_PORT: '80'
10  NS_HTTP2_SERVER_SIDE: 'ON'
11  NS_ANALYTICS_CONFIG:
12    distributed_tracing:
13      enable: 'true'
14      samplingrate: 100
15    endpoint:
16      server: <ADM-AgentIP> / <ADM-AppserverIP>
17    timeseries:
18      port: 5563
19    metrics:
20      enable: 'true'
21      mode: 'avro'
22    auditlogs:
23      enable: 'true'
24    events:
25      enable: 'true'
26    transactions:
27      enable: 'true'
28      port: 5557
29  <!--NeedCopy-->
```

5. 次のコマンドを使用して ConfigMap を再適用します。

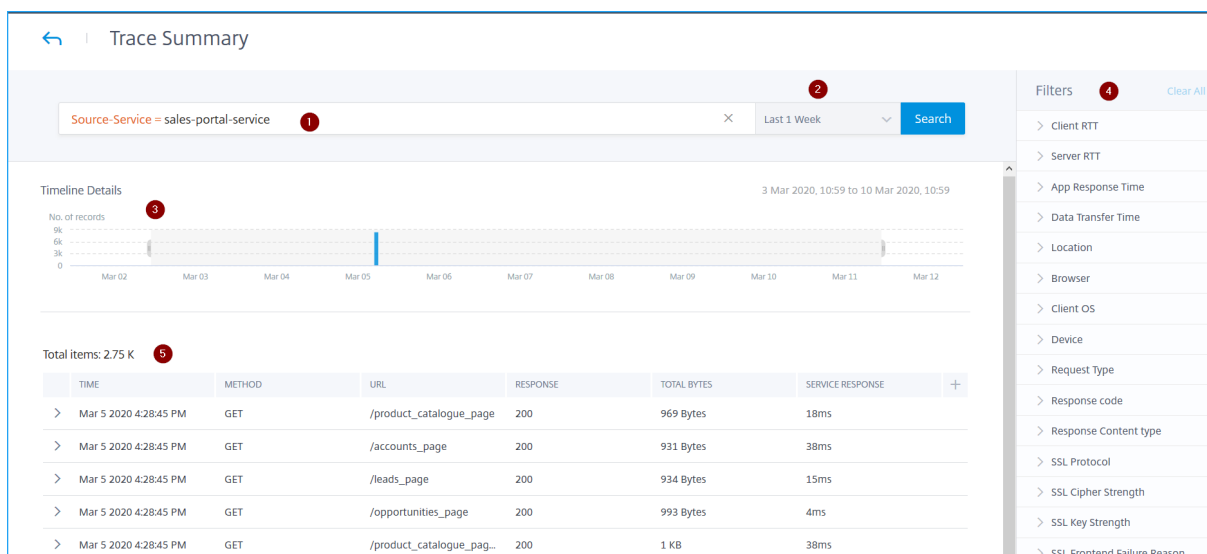
```
kubectl apply -f <yaml-file>.yaml
```

#### サービストレースの詳細の表示

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。



選択したサービスの「トレースの概要」ページが表示されます。



トレースの概要には以下が表示されます。

- 提案と演算子を使用したトランザクションを検索できる拡張検索 (1)。詳細については、「[アドバンスサーチ](#)」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 (2) などの期間を選択できる期間リスト。
- 特定の期間の結果をドラッグして選択して表示できる「タイムラインの詳細」グラフ (3)。
- 各指標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)。

### 取引の詳細を表示

トランザクションをクリックしてドリルダウンすると、詳細情報が表示されます。選択したサービスについて、次のようなトランザクションの詳細を表示できます。

- 開始日時
- 終了時間
- SSL メトリック
- 相互に依存するサービスとの通信 (各サービスでのエラーと応答時間を含む)

次の例は、`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。

The screenshot shows the NetScaler AD Management interface. On the left, under 'sales-portal-service', the following details are listed:

- Start Time: 5 Mar 2020 16:22:41
- End Time: 5 Mar 2020 16:23:05
- SSL Protocol: NA
- SSL Cipher Strength: NA
- SSL Key Strength: NA
- SSL Key Hash: NA
- SSL Frontend Failure: NA

On the right, under 'Services Inside Trace', the following summary is shown:

- Number of Services: 3
- Number of Spans: 3
- catalogue-store-service: 1 Error, 4 ms (6%)
- product-catalogue-service: 0 Errors, 23 ms (32%)
- sales-portal-service: 0 Errors, 44 ms (61%)

A red box highlights the 'See Trace Details' button. At the bottom, it indicates 'Showing 21 - 30 of 2760 items' and 'Page 3 of 276'.

「トレースの詳細」ページが表示されます。

The screenshot shows a detailed trace for 'sales-portal-service: HTTP GET /product\_catalog...'. The trace starts at 5 Mar 2020 16:22:41 and has a duration of 44 ms. It shows three services and three total spans. A timeline at the top indicates the duration of each span: sales-portal-service (44 ms), product-catalogue-service (23 ms), and catalogue-store... (4 ms). A red circle '1' is placed above the 'Services: 3' and 'Total Spans: 3' information. A red circle '2' is placed above the 'product-catalogue-service' span. A red circle '3' is placed above the 'Ingress' section.

The 'Ingress' section for 'sales-portal-service' shows the following details:

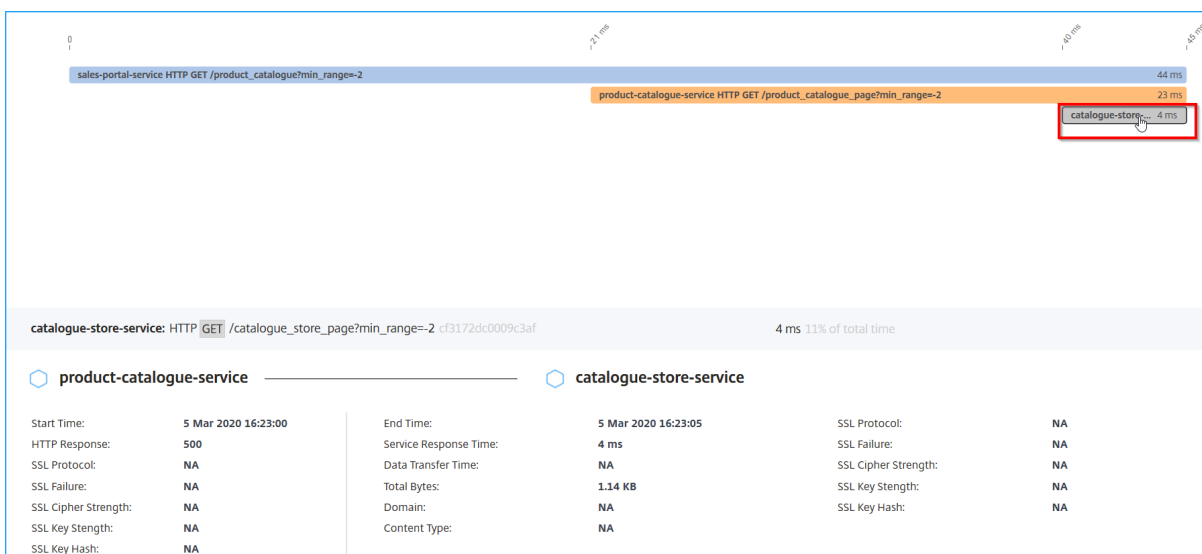
- Start Time: 5 Mar 2020 16:22:20
- End Time: 5 Mar 2020 16:23:05
- HTTP Response: 200
- Service Response Time: 44 ms
- SSL Protocol: NA
- SSL Failure: NA
- SSL Cipher Strength: NA
- SSL Key Strength: NA
- SSL Key Hash: NA
- Total Bytes: 1 KB
- Domain: NA
- Content Type: NA
- SSL Protocol: NA
- SSL Failure: NA
- SSL Cipher Strength: NA
- SSL Key Strength: NA
- SSL Key Hash: NA

1 —トランザクションの開始時間、応答時間、合計サービス、合計スパンが表示されます。

2 —相互依存サービスと通信した、選択し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すると、詳細が表示されます。

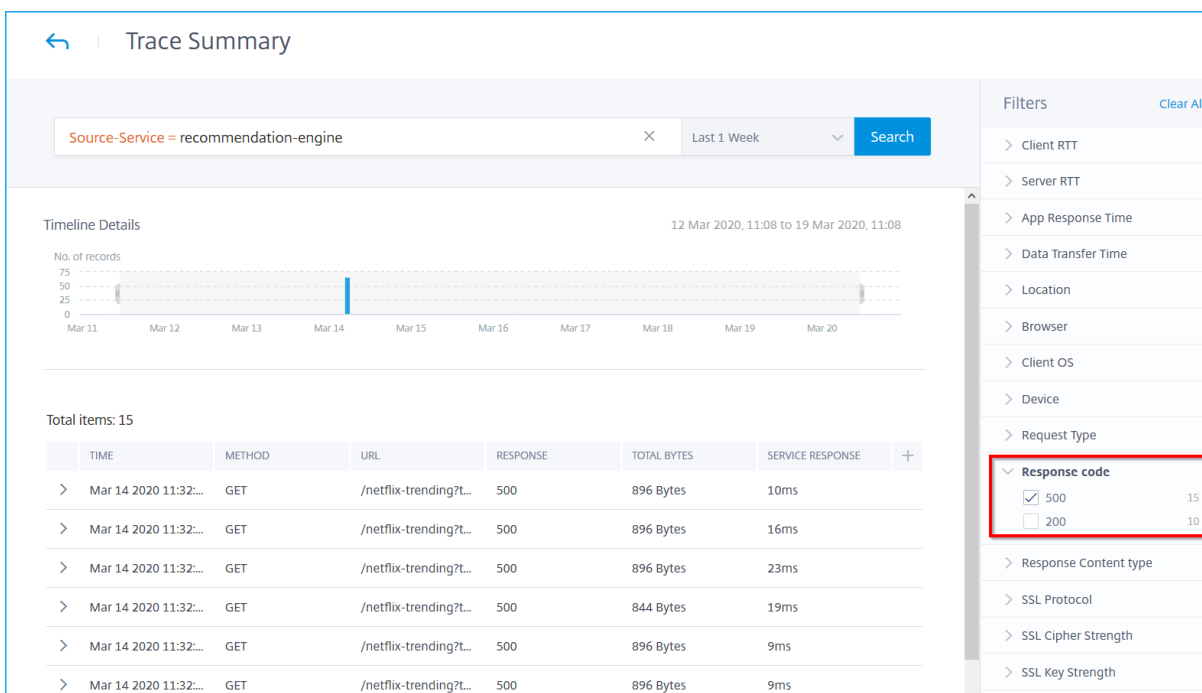
3 —各サービスのトランザクションの詳細を表示します。

例の画像によると、`catalogue-store-service`はエラーを示しています。`catalogue-store-service`のご利用可能な取引をクリックしてください。



product-catalogue-serviceとcatalogue-store-serviceのトランザクションの詳細には、HTTP 応答が 500 と表示されています。これらの詳細により、管理者はエラーのあるサービスを分析し、product-catalogue-serviceを解決策としてトラブルシューティングを行うことができます。

フィルターパネルの各指標からオプションを選択して、結果を絞り込むこともできます。たとえば、5xx トランザクションをすべて表示するには、[レスポンスコード] をクリックして [500] を選択します。



- クライアント **RTT**: クライアントからパケットが送信されるまでの時間。
- サーバー **RTT**: パケットがサーバーから送信されるまでの時間。
- アプリ応答時間: アプリケーションの平均応答時間

- データ転送時間: サービスとの間で送受信されるデータ転送のサイズと速度。
- 場所: クライアントの場所
- ブラウザ: クライアントが使用するブラウザタイプ。例: Chrome、Firefox。
- クライアント **OS**: ブラウザからのユーザエージェントの詳細に基づくクライアント OS。
- デバイス: ブラウザからのユーザ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。
- 要求タイプ: 取引要求タイプ。例: GET。
- 応答コード: サーバーから受信した応答コード。たとえば、501、404、200 などです。
- 応答コンテンツタイプ: トランザクションコンテンツタイプ。クライアント要求が text/html の場合、サーバーからの応答は 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 プロトコルのバージョン。例: SSLv3。
- **SSL** 暗号強度: 高、中、低などの SSL 証明書の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。キーの長さは、SSL アルゴリズムのセキュリティを定義します。例: 2048
- **SSL** フロントエンドの失敗理由: フロントエンド SSL ハンドシェイクのエラーメッセージ。例: SSL CLIENTAUTH FAILURE

## サービスグラフで部分的なデータまたはデータがないかの診断詳細の表示

February 6, 2024

[必要なサービスグラフ構成を完了し](#)、NetScaler ADM に Kubernetes クラスターを追加すると、サービスグラフにデータが入力され始めます。状況によっては、サービスグラフに部分的なデータが表示されているか、データが表示されないことがあります。サービスグラフに部分的なデータまたはデータがない理由のいくつかは、次のとおりです。

- スタティックルートが設定されていません
- Kubernetes クラスターのステータスが停止しています
- CPX 登録が失敗しました
- CPX 仮想サーバにはライセンスがありません
- サービスグラフがすべてのデータをロードできないように、必要な分析構成が設定されていません

管理者として、サービスグラフに部分的なデータが表示されている場合やデータがない場合に、その理由を分析することが困難な場合があります。サービスグラフページの診断情報を使用すると、データの一部またはデータがない問題のトラブルシューティングに必要な理由と必要なアクションを確認できます。



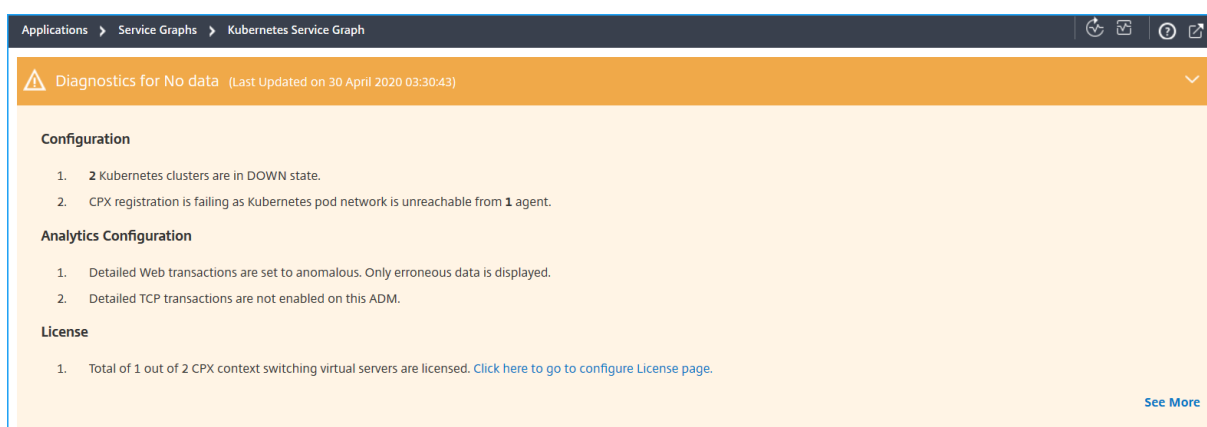
NetScaler ADM で、[アプリケーション] > [サービスグラフ] の順に選択し、[マイクロサービス] タブをクリックします。

### 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は、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原因を確認できます。次の図は、サービスグラフにデータがない場合の例です。



問題の詳細を表示するには、[詳細を表示] をクリックします。

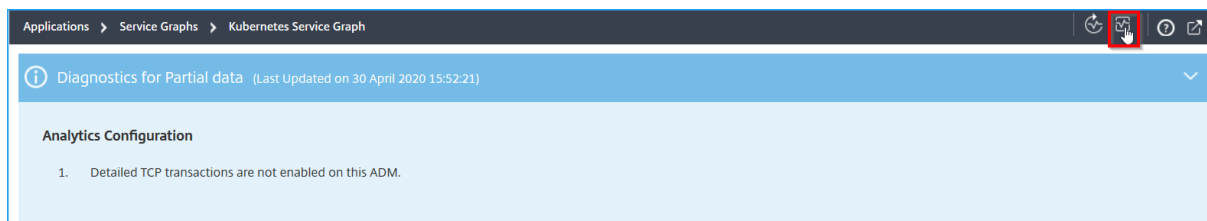
| Diagnostics Details 6   |                                                                                               |                                                                                 |
|-------------------------|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| ISSUE TYPE              | MESSAGE                                                                                       | ACTION                                                                          |
| Analytics Configuration | Detailed Web transactions are set to anomalous. Only erroneous data is displayed.             | Set Detailed Web transactions to all in Analytics > Settings > Enable features  |
| Analytics Configuration | Detailed TCP transactions are not enabled                                                     | Set Detailed TCP transactions to all in Analytics > Settings > Enable features. |
| Configuration           | Unable to get valid response from Agent                                                       | Check Agent status.                                                             |
| Configuration           | Unable to get valid response from Agent                                                       | Check Agent status.                                                             |
| Configuration           | Registration of CPX has failed due to Agent [redacted], not able to reach cluster pod network | Please add routes on Agent [redacted] so that pod network on cluster c          |
| License                 | Total of 1 out of 2 CPX context switching virtual servers are licensed                        | Please go to System Licenses to license virtual servers                         |

- [問題の種類] –構成、分析設定、またはライセンスから発生する問題を示します。
- 「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を行うために実行する必要があるアクションを示します。

### 部分データの診断

サービスグラフが部分的なデータだけで表示される場合は、[ **Show Diagnostics** ] 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。

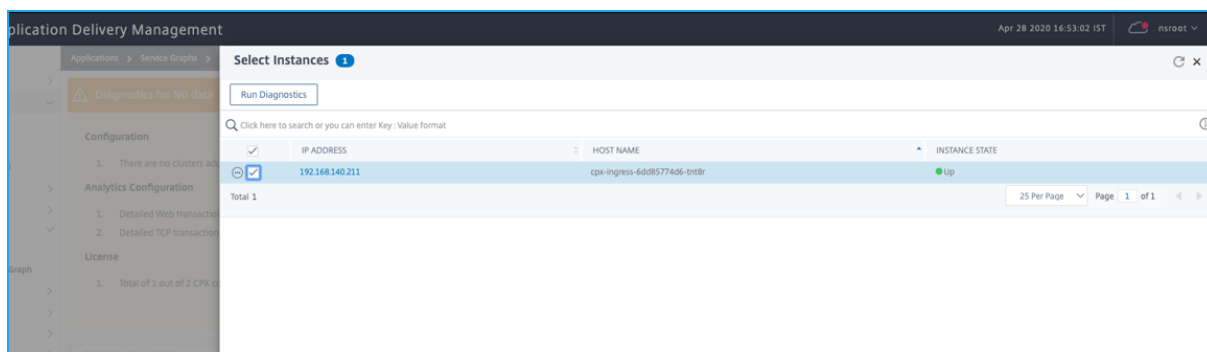


この例では、[分析]>[設定]に移動して[TCP トランザクション設定]を[すべて]に設定する必要があります。

### トラブルシューティング

管理者は、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、これらの問題のトラブルシューティングを試みることができます。トラブルシューティング後、NetScaler ADM は定期的な診断チェックを定期的に自動的に実行します。診断チェックが完了すると、サービスグラフ内のデータの一部またはデータがない問題が解決されます。

[診断の実行]をクリックし、**CPX** インスタンスを選択し、[診断の実行]をクリックすることもできます。



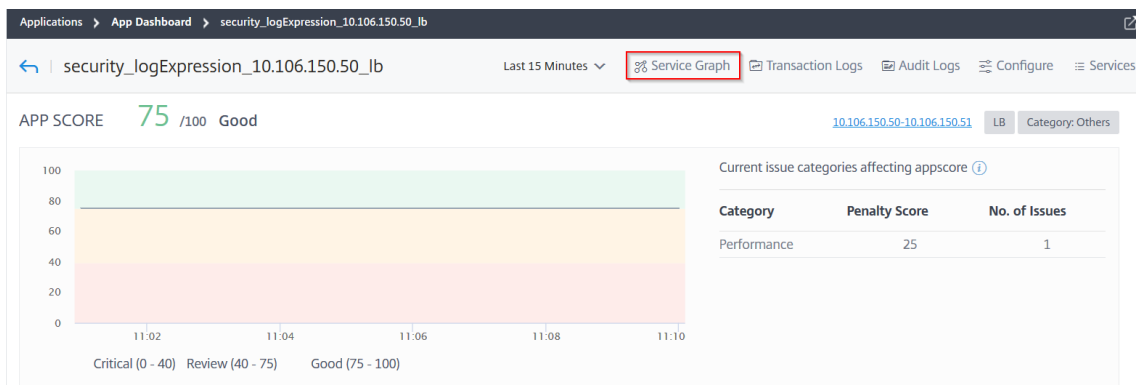
トラブルシューティングシナリオの詳細については、[FAQ](#)を参照してください。

### アプリケーションのサービスグラフ

February 6, 2024

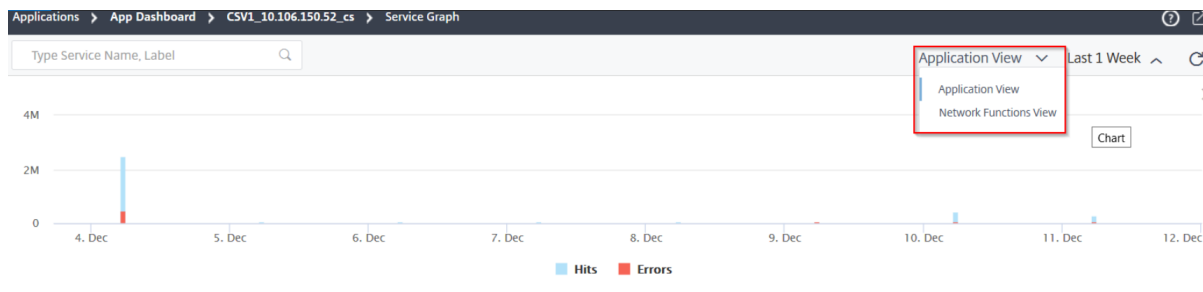
アプリケーションのサービス・グラフを表示するには、次の手順に従います。

1. [アプリケーション]>[ダッシュボード]に移動します。
2. 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、[サービスグラフ]をクリックします。

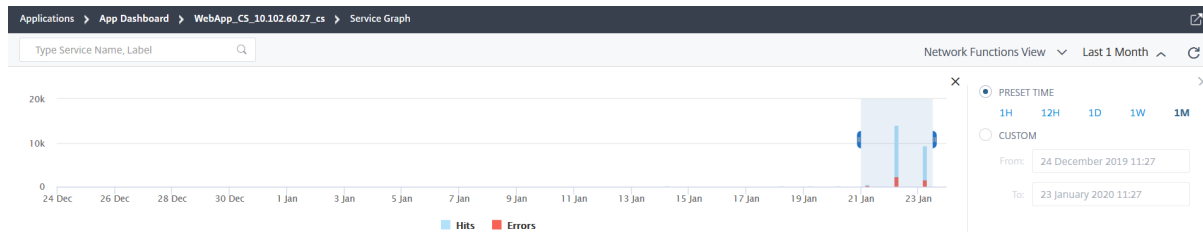


選択したアプリケーションのサービスグラフページが表示されます。

サービスグラフは、\*\* 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表示できます\*\*。

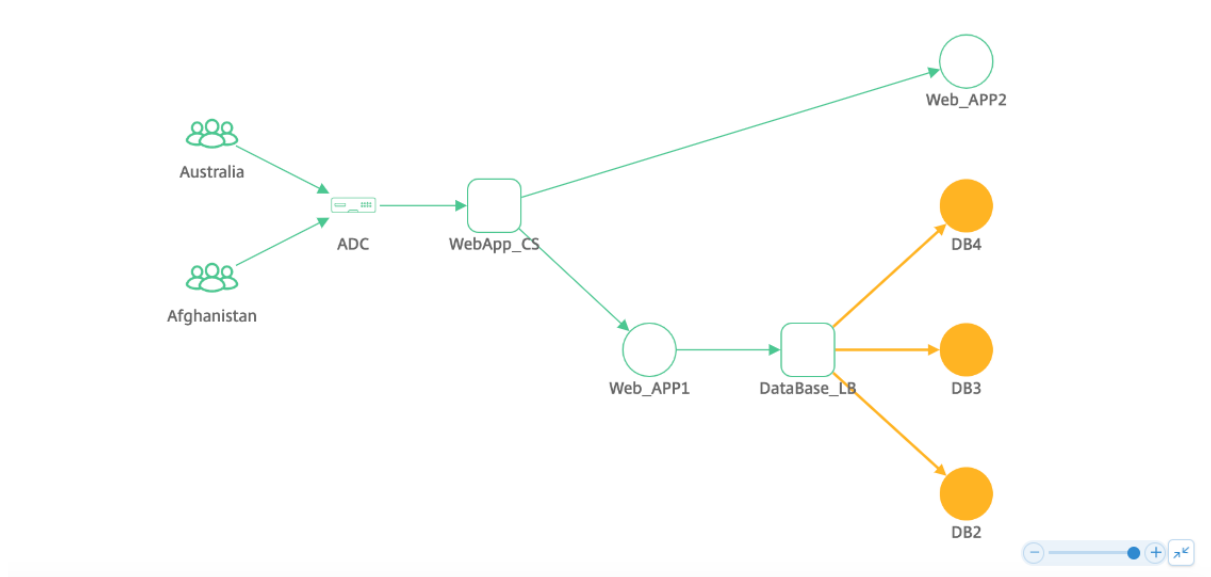


ヒットとエラーをドラッグして選択し、結果を変更することもできます。



## アプリケーションビュー

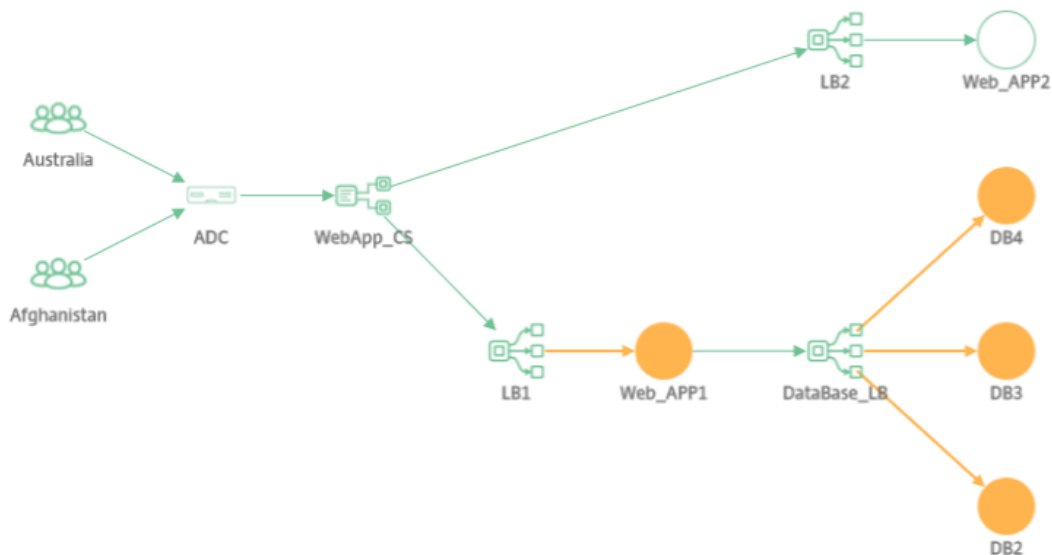
アプリケーション構成の概要を表示します。このビューでは、クライアント、ADC、Web アプリケーション間の通信を視覚化できます。



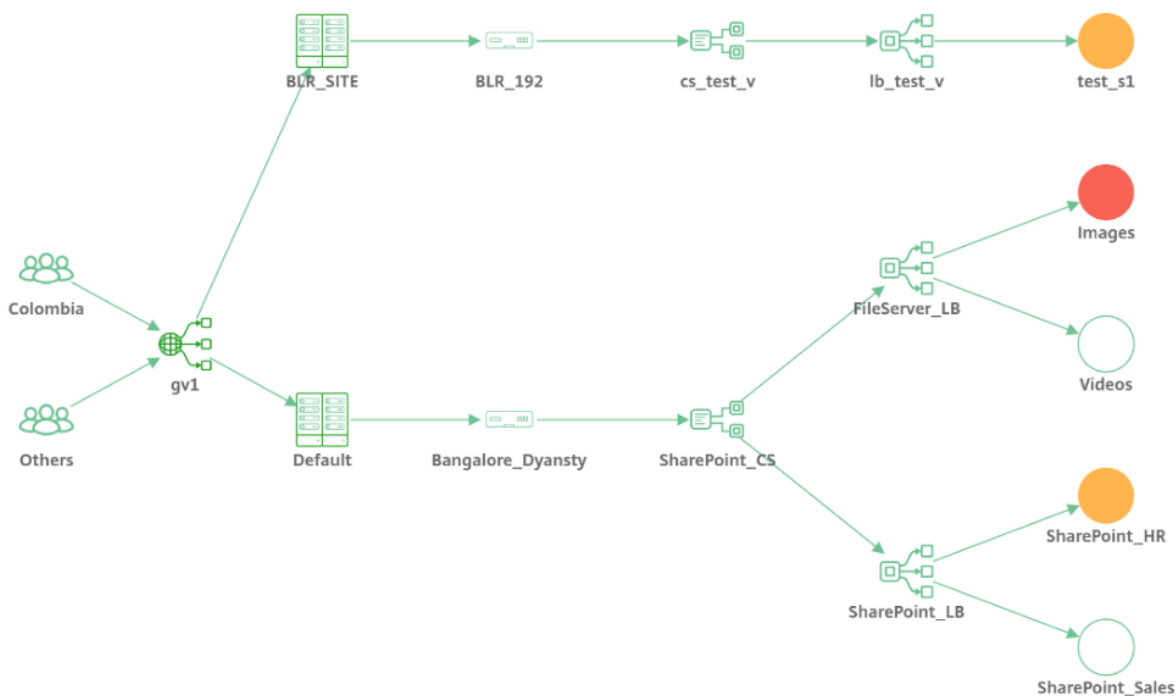
### ネットワーク機能ビュー

アプリケーションに関連付けられている仮想サーバーを表示します。このビューでは、ADC が以下と通信しているかどうかを視覚化できます。

- アプリケーションにアクセスするためのコンテンツスイッチング仮想サーバー
- アプリケーションにアクセスするための負荷分散仮想サーバー
- アプリケーションにアクセスするためのコンテンツスイッチング仮想サーバーと負荷分散仮想サーバーの両方



GSLB アプリケーションの場合、詳細がデータセンターと NetScaler ADC とともに表示されます。

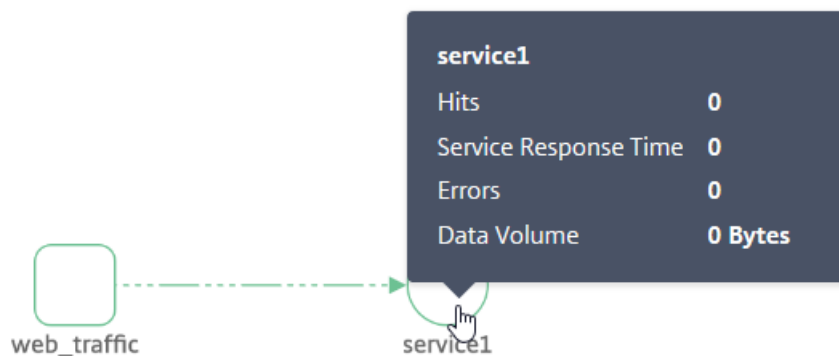


アクティブなトランザクションがないサービスグラフビュー

ADCとWebアプリケーションの間でアクティブなトランザクションが発生しない場合、サービスグラフにはアプリケーションの基本構成のみが表示されます(クライアントとADCは表示されません)。



サービスまたは仮想サーバーにマウスポインターを置くと、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と表示されます。

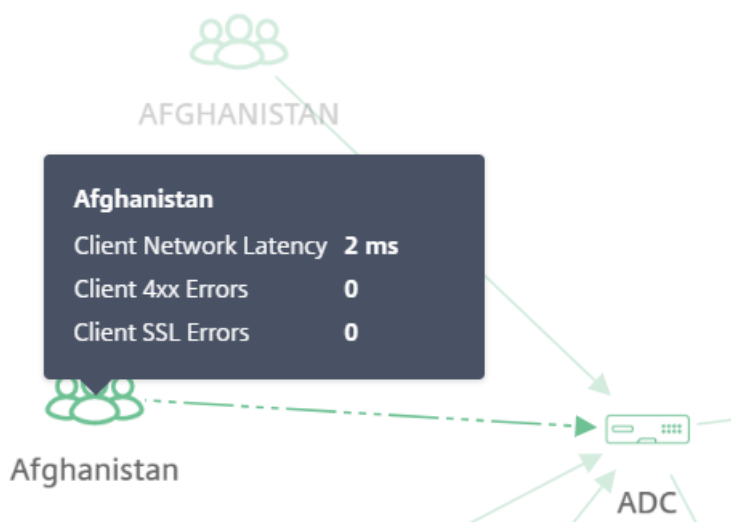


## 指標の分析

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が表示されます。

### クライアント・メトリック

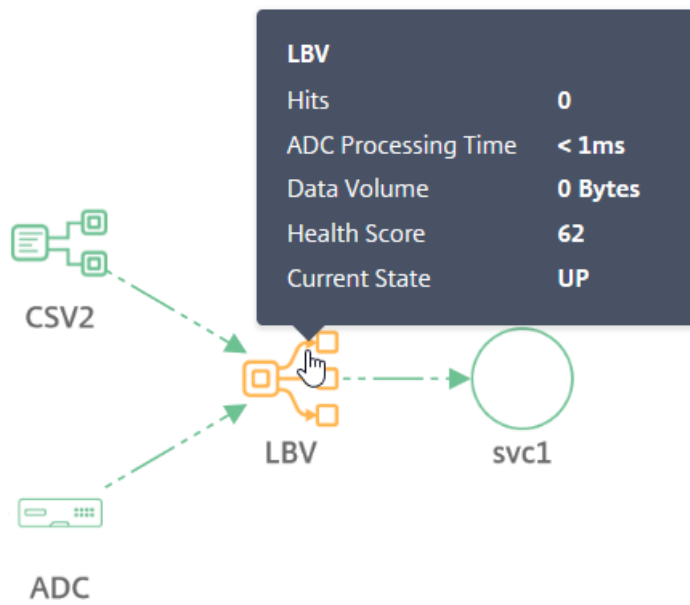
クライアントにマウスポインターを置くと、クライアントメトリックが表示されます。



- クライアントネットワーク遅延—クライアントからのネットワーク遅延を示します。
- クライアント **4xx** エラー—クライアントから発生した 4xx エラーの合計数を示します。
- クライアント **SSL** エラー—クライアントからの SSL エラーの総数を示します。

### ネットワーク機能メトリック

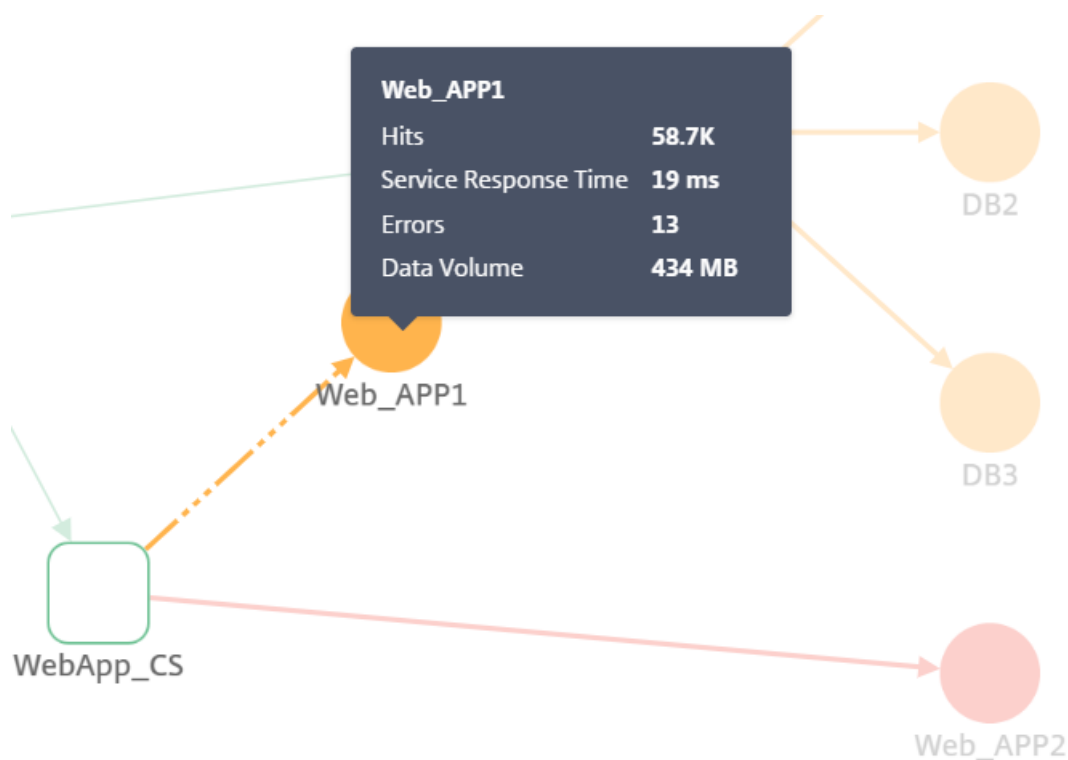
負荷分散サービスまたはコンテンツスイッチングサービスにマウスポインターを置くと、メトリックの詳細が表示されます。



- **Hits** —仮想サーバーが受信したヒットの合計数を示します。
- **ADC 処理時間**—ADC インスタンスごとの平均処理時間を示します
- **Data Volume** : 仮想サーバによって処理された合計データ量を示します。
- **ヘルススコア**—アプリのスコアを示します
- **Current state** : 仮想サーバの現在のステータスを示します。

#### サービスメトリック

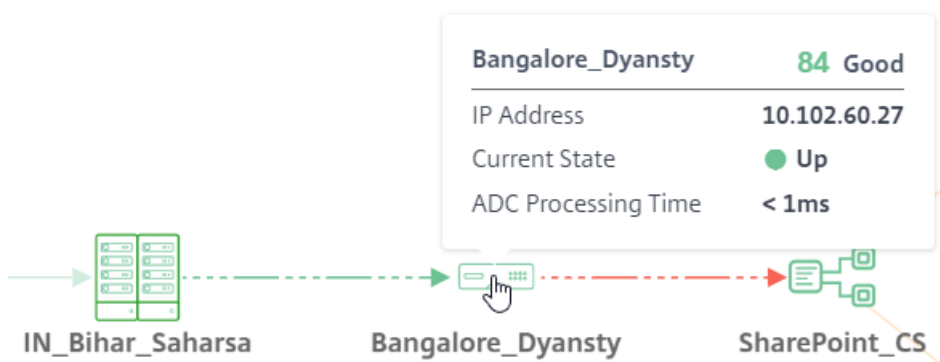
サービス (ウェブアプリケーション) にマウスポインターを置くと、メトリックが表示されます



- 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合計を示します

### NetScaler ADC メトリクス (GSLB アプリケーションのみ)

ADC にマウスポインターを置くと、メトリックが表示されます。



- ホスト名と現在の ADC スコアを表示します。スコアは、NetScaler ADC 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。



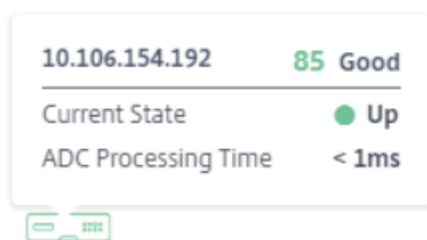
- **IP** アドレス—NetScaler ADC IP アドレスを示します。
- 現在の状態—NetScaler ADC のステータス（稼働中、停止中、サービス停止など）を示します
- **ADC** 処理時間—ADC インスタンスによる平均処理時間を示します

注

NetScaler ADC 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 ADC IP アドレスが表示されます。

-メトリックでは、NetScaler ADC IP アドレス情報は表示されません。

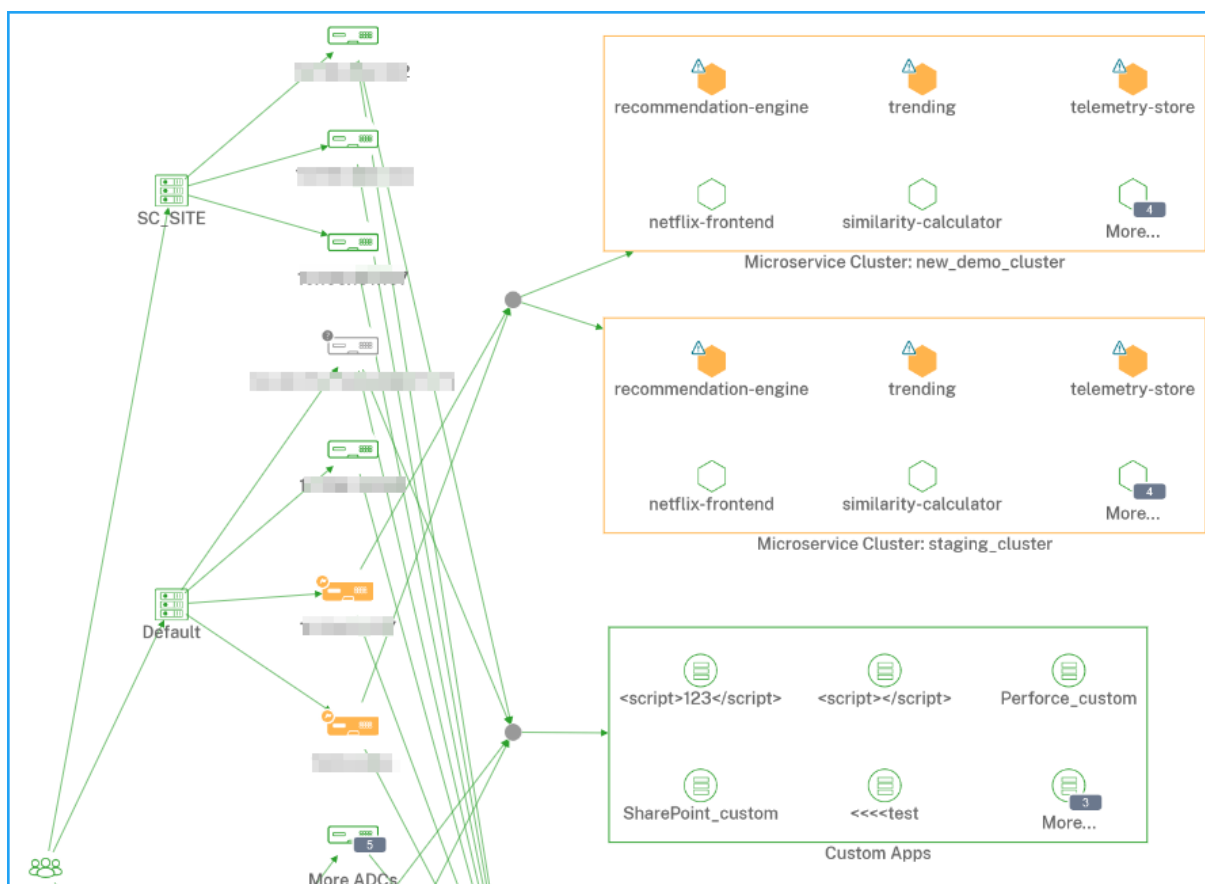


10.106.154.192

サービスグラフ内のすべてのアプリケーションの全体的ビュー

February 6, 2024

[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。



サービスグラフには、選択した期間の次の情報が表示されます。

- 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 ADC 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 ADC インスタンスからの個別のアプリケーションの合計

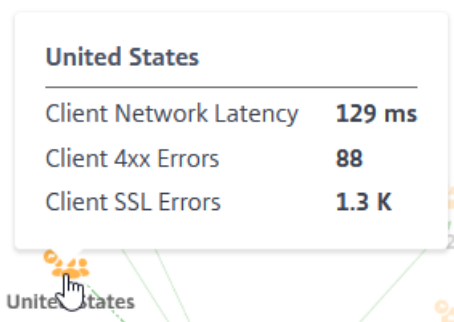
注

NetScaler ADC インスタンスに個別のアプリケーションがない場合、NetScaler ADC インスタンスから個別の仮想サーバーに向かう矢印端は表示されません。

- すべての NetScaler ADC インスタンスからのカスタムアプリケーションの合計
- NetScaler ADC CPX インスタンスからのマイクロサービスアプリケーションの合計

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ポインタを合わせると、メトリックスが表示されます。

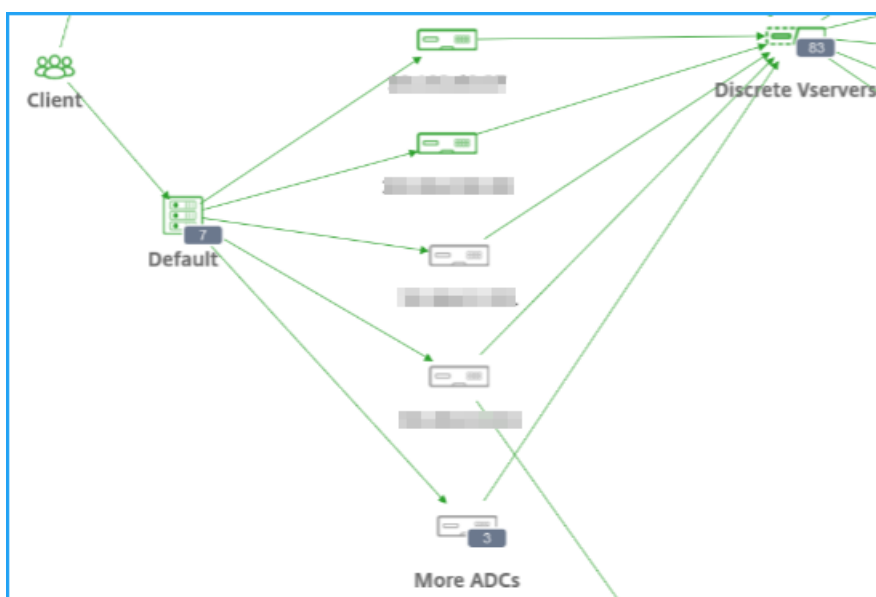


- クライアントネットワーク待ち時間 -平均クライアントネットワーク遅延を示します。
- クライアント **4xx** エラー -クライアントの 4xx エラーの合計を示します。
- クライアント **SSL** エラー -クライアントの SSL エラーの合計を示します。

### NetScaler ADC の詳細を表示する

サービスグラフでは、次の項目を表示できます。

- NetScaler ADC インスタンスの合計でグループ化されたデータセンター
- 各データセンターの上位 4 つの低スコアの NetScaler ADC インスタンスのみ



[その他の **ADC**] をクリックして、それぞれのステータス (クリティカル、レビュー、良好および該当なし) タブを選択して、すべての NetScaler ADC インスタンスを表示します。

| HOST NAME | IP ADDRESS | SCORE | INSTANCE STATE | MAX CONTI |
|-----------|------------|-------|----------------|-----------|
| NS_27     |            | 82    | Good Up        | Not Recor |
| --        |            | 85    | Good Up        | Not Recor |

NetScaler ADC インスタンスにマウスポインタを置いて、メトリックを表示します。

**10.102.103.117** 79 Review  
 Host Name **AWS-ADC3**  
 Current State ● Up  
 Top Issue **High Disk Usage**

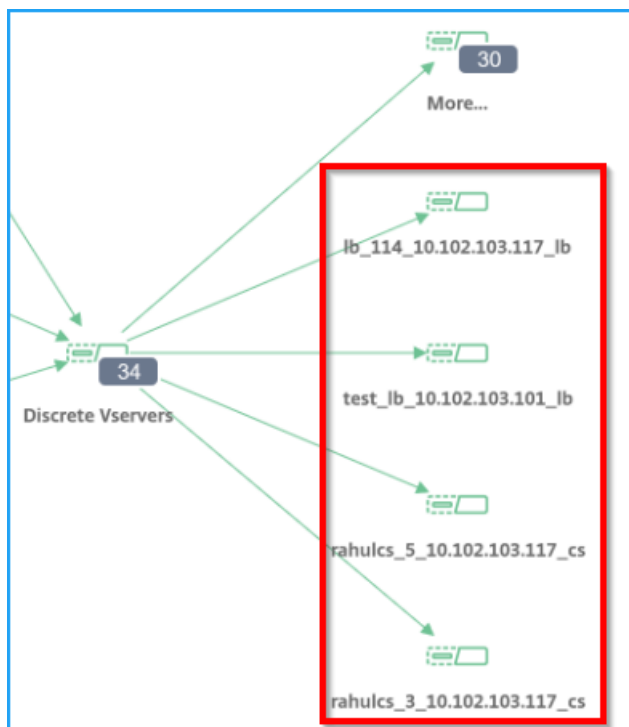
以下を表示できます：

- NetScaler ADC インスタンスの IP アドレスとスコア
- ホスト名—NetScaler ADC 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 ADC インスタンスの現在のステータス（稼働中、停止、アウトオブサービスなど）を示します。
- 上位の問題—現在の NetScaler ADC スコアに影響する上位の問題を示します

**NetScaler ADC** インスタンスをクリックして、インスタンスのスコア、主要メトリック、および ADC インスタンスに関連付けられた問題などのインスタンスの詳細を表示します。詳細については、「[インフラストラクチャ分析](#)」の「[インスタンスの詳細の表示](#)」を参照してください。

ディスクリートアプリケーションの表示

サービス・グラフには、上位4つの低スコアディスクリートアプリケーションが表示されます。



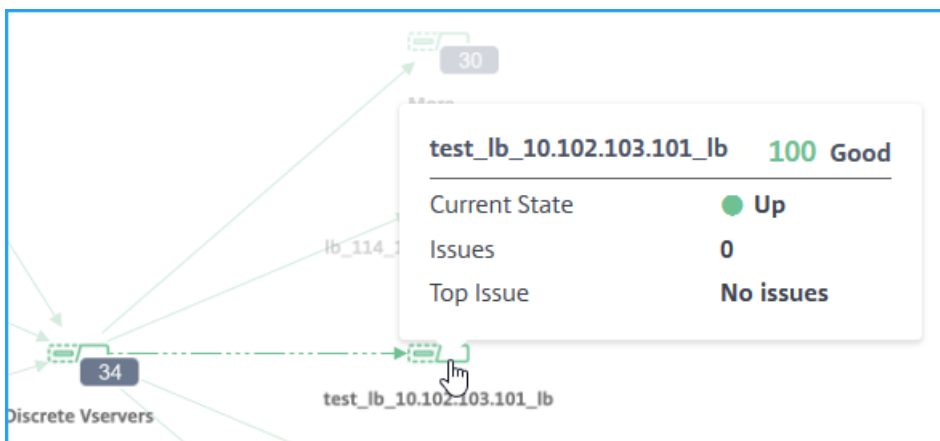
次の個別のアプリケーションがあるとします。

| アプリ名  | Citrix ADC     | App Score   | アプリのステータス |
|-------|----------------|-------------|-----------|
| App1  | 10.102.29.50   | 35 (クリティカル) | アップ       |
| App2  | 10.102.29.90   | 100 (いいね)   | ダウン       |
| アプリ 3 | 10.102.32.40   | 49 (レビュー)   | アップ       |
| アプリ 4 | 10.102.113.208 | 92 (いいね)    | ダウン       |
| アプリ 5 | 10.102.25.25   | 86 (いいね)    | アップ       |
| アプリ 6 | 10.102.29.41   | 77 (よい)     | アップ       |
| アプリ 7 | 10.102.29.102  | 41 (レビュー)   | アップ       |

このシナリオでは、サービスグラフの上位4つの低スコアアプリケーションとして App1、App3、App6、およびアプリケーション7を表示できます。

同様に、カスタムアプリケーションとマイクロサービスアプリケーションの上位4つの低スコアアプリケーションを表示することもできます。

サービスの上にマウスポインタを置くと、メトリックス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（Up、Down）を示します。
- **Issues** –アプリケーションに適用可能な問題の合計を示します。
- **Top Issue**：アプリケーション全体のスコアに影響する上位の問題を示します。

[詳細] をクリックして、すべての個別のアプリケーションを表示します。次の図に示すように、「離散仮想サーバー」ページが表示されます。

The screenshot shows the 'Discrete Vservers' page with a summary of application health and a table of application details.

Summary:

- Total: 28
- Critical: 13
- Review: 0
- Good: 13
- Not Applicable: 2

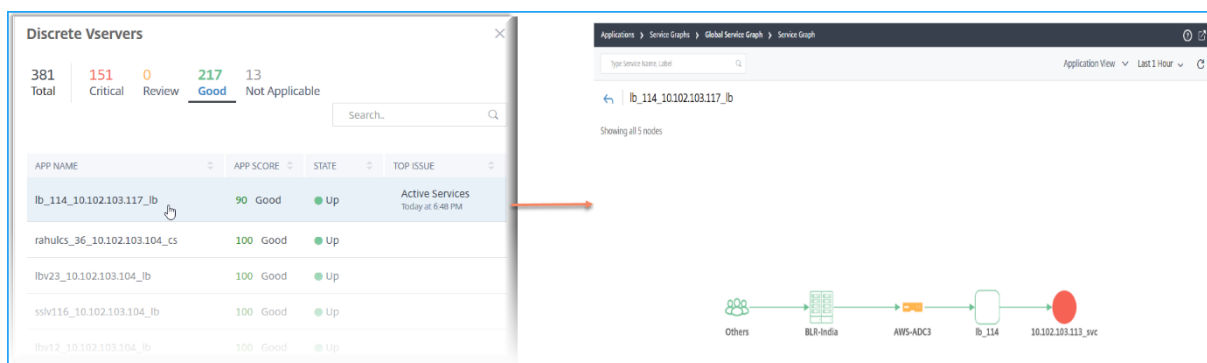
| APP NAME                      | APP SCORE | STATE | TOP ISSUE                        |
|-------------------------------|-----------|-------|----------------------------------|
| lb_114_10.102.103.117_lb      | 90        | Good  | Active Services Today at 1:38 PM |
| cs_7_10.102.103.117_cs        | 100       | Good  | Up                               |
| lb_ATO_10.102.103.101_lb      | 100       | Good  | Up                               |
| cs_2_10.102.103.117_cs        | 100       | Good  | Up                               |
| csfrontapp_10.102.103.117_cs  | 100       | Good  | Up                               |
| cs_1_10.102.103.117_cs        | 100       | Good  | Up                               |
| test_lb_10.102.103.101_lb     | 100       | Good  | Up                               |
| vs1_10.102.103.117_lb         | 100       | Good  | Up                               |
| test_lb_101_10.102.103.101_lb | 100       | Good  | Up                               |

仮想サーバは、ステータスに応じて表示されます。

- 合計—ディスクリットアプリケーションの合計
- クリティカル—アプリのスコアは 0 から 40 以下です

- レビュー—アプリのスコアは 40 から 75 未満です
- 良かった—アプリのスコアは > 75
- 該当なし—アプリは仮想サーバーにバインドされていません

各タブをクリックすると、仮想サーバを表示できます。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。



詳細については、「[アプリケーションの Service Graph](#)」を参照してください。

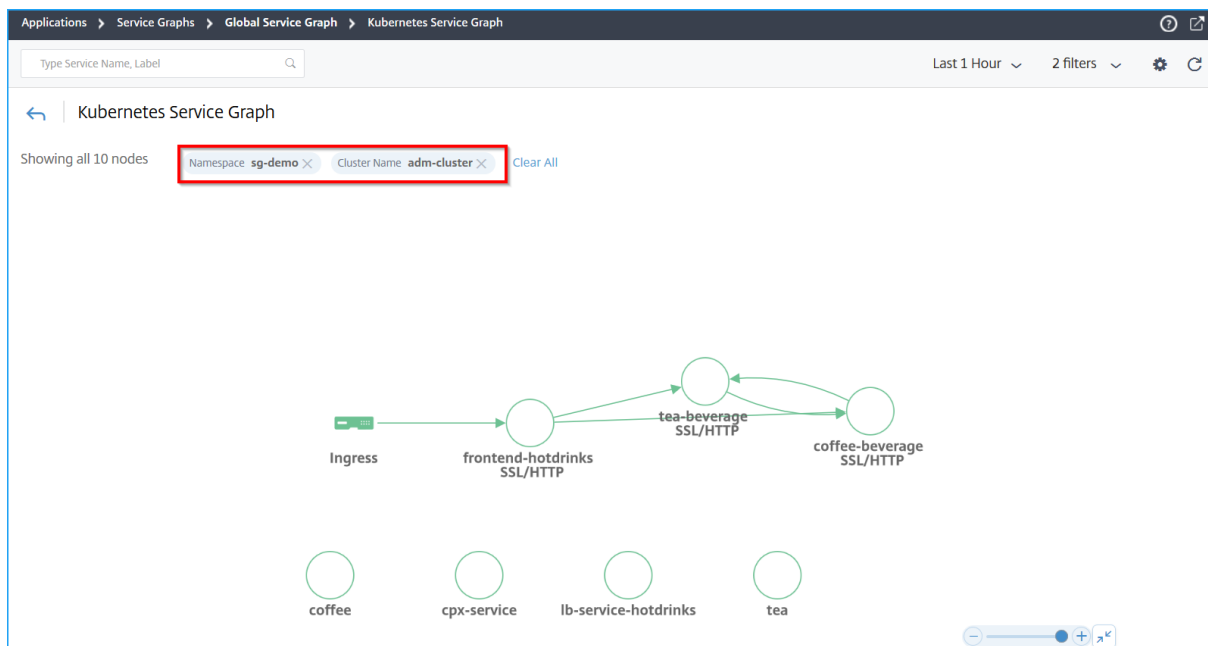
## マイクロサービスアプリケーションの表示

サービスグラフには、Kubernetes クラスターに属するすべてのマイクロサービスアプリケーションも表示されます。サービスの上にマウスポインタを置くと、メトリックスの詳細が表示されます。

以下を表示できます：

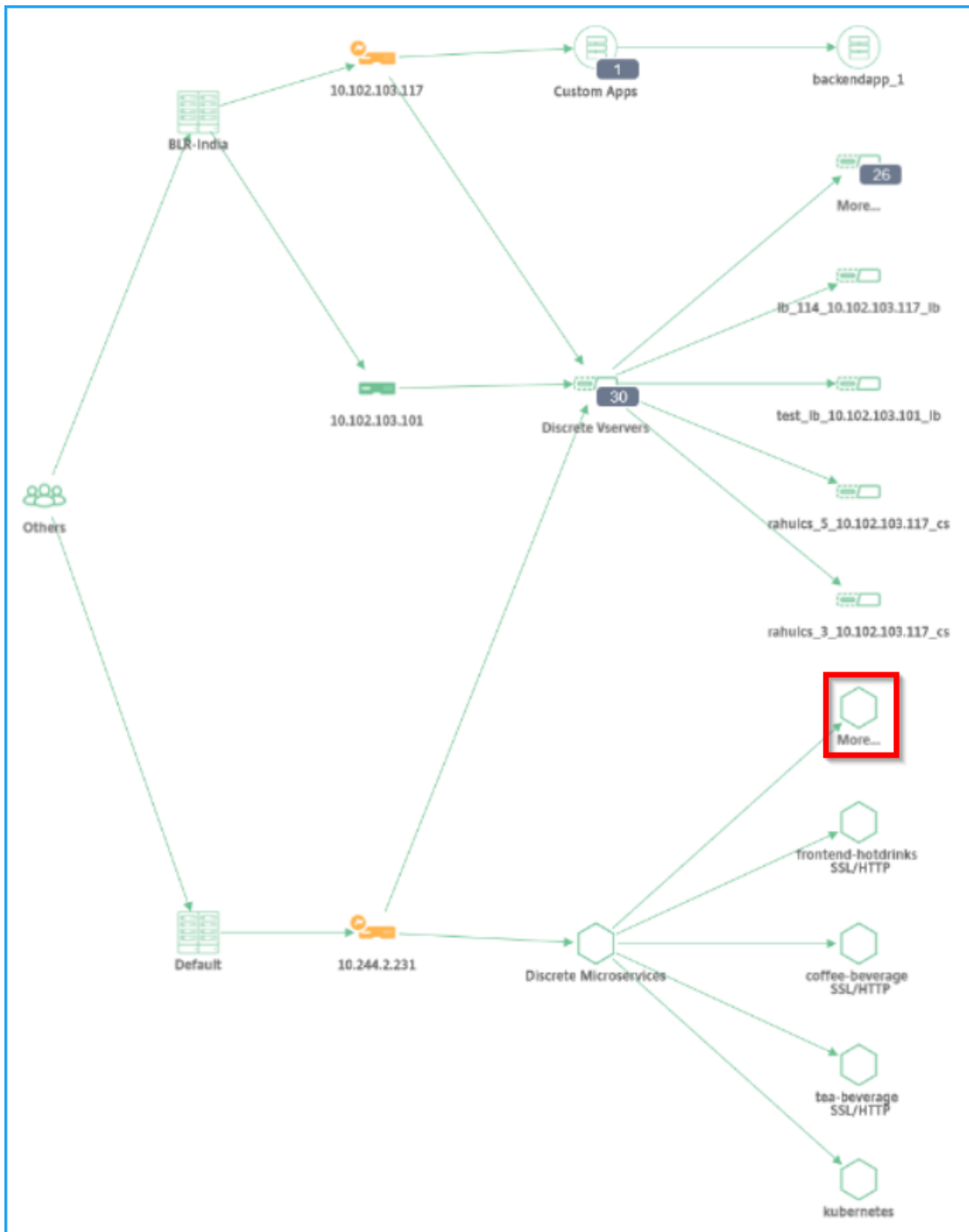
- サービス名
- SSL、HTTP、TCP、SSL over HTTP、SSL などのサービスで使用されるプロトコル
- **Hits** —サービスによって受信されたヒットの総数
- サービス応答時間—サービスから取得した平均応答時間。  
(応答時間 = クライアント RTT + 要求の最後のバイト—要求の最初のバイト)
- エラー—4xx、5xx などのエラーの総数
- **Data Volume** —サービスによって処理されるデータの総量
- 名前空間—サービスの名前空間
- クラスター名—サービスがホストされているクラスター名
- **SSL** サーバーエラー—サービスからの SSL エラーの合計

サービスををクリックすると、選択したサービスの Kubernetes サービスグラフが、適用されたサービス名前空間とクラスター名フィルターと共に表示されます。



[詳細] をクリックして、すべてのサービスを持つ Kubernetes サービスグラフを表示します。Kubernetes サービスグラフについて詳しくは、[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](#)。





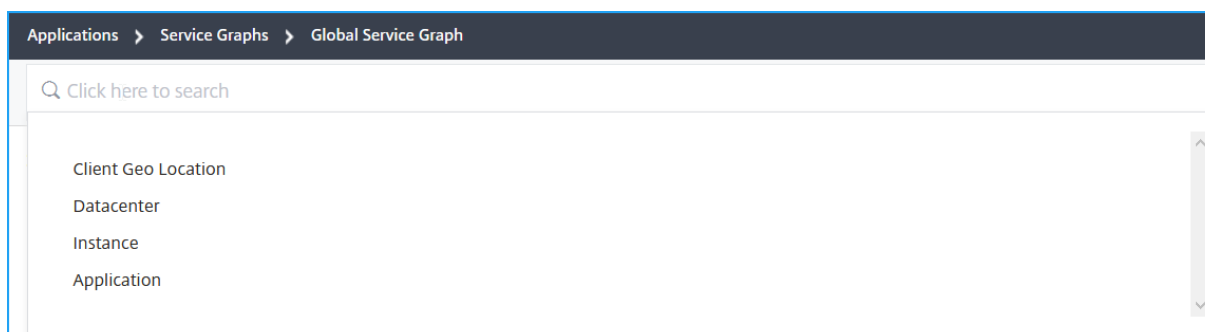
### 結果をフィルタする検索バー

検索バーを使用して結果をフィルタリングできます。管理者は、次の条件を満たす場合に、この検索バーを使用して、特定のインスタンス/クライアント/アプリケーション/データセンターにすばやく絞り込むことができます。

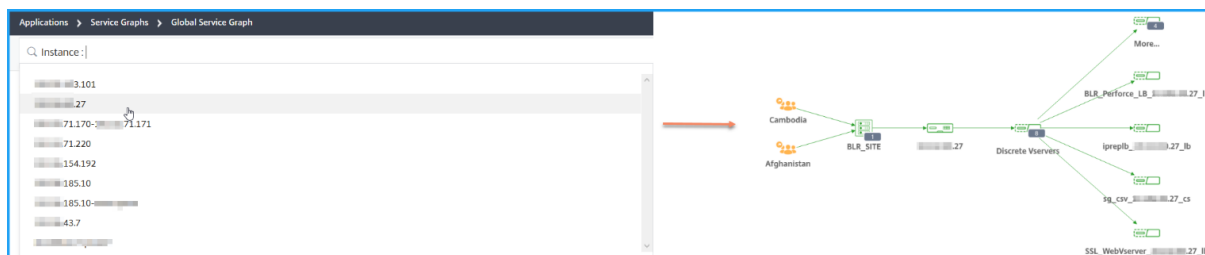
- 多数のデータセンターを持つ大企業

- データセンターごとに多数の NetScaler ADC インスタンスを構成しました
- 各 NetScaler ADC インスタンス経由で展開またはアクセスされる多数のアプリケーションを構成
- 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を置き、フィルタを作成するカテゴリを選択します。



たとえば、特定の ADC インスタンスを表示する場合は、検索バーから [ **Instance** ] 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の関連アプリケーション、データセンター、クライアントの場所が表示されます。



## StyleBook

February 6, 2024

StyleBook は、アプリケーションの複雑な NetScaler ADC 構成の管理作業を簡素化します。StyleBook は、NetScaler ADC 構成の作成と管理に使用できるテンプレートです。NetScaler ADC の特定の機能を構成するための StyleBook を作成することも、Microsoft Exchange や Lync などのエンタープライズアプリケーション展開用の構成を作成するように StyleBook を設計することもできます。

StyleBook は DevOps チームによって実践されているコードとしてのインフラストラクチャの原則によく適しています。コードとしてのインフラストラクチャの構成は宣言的でバージョン管理されるものです。構成は繰り返され全体として展開されるものでもあります。StyleBooks には以下の利点があります。

- 宣言: **StyleBook** は、命令構文ではなく宣言構文で書かれています。Stylebook では、特定の NetScaler ADC インスタンスで実現する手順ではなく、構成の結果や「望ましい状態」の説明に集中できます。Citrix

Application Delivery Management (ADM) は、Citrix ADC 上の既存の状態と指定した目的の状態との差分を計算し、インフラストラクチャに必要な編集を行います。StyleBook は YAML で記述された宣言構文を使用するため、StyleBook のコンポーネントは任意の順序で指定でき、NetScaler ADM は計算された依存関係に基づいて正しい順序を決定します。

- **アトミック:StyleBooks** を使用して構成をデプロイすると、フル構成レーションがデプロイされるか、何もデプロイされないかで、インフラストラクチャー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 と一意に区別できる名前、名前空間、バージョン番号があります。この特徴を保つために、StyleBook を変更した場合はそのバージョン番号（またはその名前または名前空間）を更新する必要があります。バージョンの更新では、同じ StyleBook の複数のバージョンを維持することもできます。
- **コンポーザブル:StyleBook** を定義すると、その StyleBook をユニットとして使用して他の StyleBook を作成できます。共通の構成パターンの繰り返しを避けることができます。また、社内の標準の構成ブロックを確立することもできます。StyleBook はバージョン管理され、既存の StyleBook を変更すると新しい StyleBook になるため、依存する StyleBook が意図せずに壊されることはありません。
- **アプリ中心:StyleBooks** を使用して、アプリケーション全体の NetScaler ADC 構成を定義できます。アプリケーションの構成はパラメーターを使用することで抽象化できます。そのため、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ーを入力するだけのシンプルなインターフェイスを使用して複雑な Citrix ADC 構成を作成できます。StyleBooks から作成された構成は、インフラストラクチャに関連付けられていません。したがって、1 つの構成を 1 つまたは複数の Citrix ADC 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 ADM は、NetScaler ADM GUI を使用して構成を行うときに、StyleBook のパラメーターを入力するために使用する UI フォームを自動生成します。StyleBook の作成者が新しい 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 主導**: すべての構成操作は、NetScaler ADM GUI または REST API を使用してサポートされます。API は、同期モードまたは非同期モードで使用できます。StyleBook の API では、構成タスクに加えて、実行時に StyleBook のスキーマ（パラメーターの説明）を見つけることもできます。

1 つの StyleBook を使用して複数の構成を作成できます。各構成は構成パックとして保存されます。たとえば、通常の HTTP 負荷分散アプリケーションの構成を定義する StyleBook があるとします。負荷分散エンティティの値を使用して構成を作成し、Citrix ADC インスタンスで実行できます。この構成は構成パックとして保存されます。同じ StyleBook を使用して異なる値を持つ別の構成を作成し、同じまたは別の Citrix ADC インスタンスで実行できます。この構成には、新しい構成パックが作成されます。構成パックは、Citrix ADM と、構成が実行される Citrix ADC インスタンスの両方に保存されます。

NetScaler ADM に同梱されているデフォルトの StyleBook を使用して展開用の構成を作成するか、独自の StyleBook を設計して NetScaler ADM にインポートすることができます。StyleBooks を使用して、NetScaler ADM GUI または API を使用して構成を作成できます。

このドキュメントでは、次の内容について説明します。

- [StyleBook の閲覧方法](#)
- [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](#)
- [StyleBook の API](#)
- [StyleBook の文法](#)

## StyleBook カテゴリー

February 6, 2024

Citrix Application Delivery Management (ADM) には、2つの StyleBook カテゴリーがあります。これらは、デフォルトの StyleBooks とカスタム StyleBook です。デフォルトでもカスタムでも、StyleBook はパブリックまたはプライベートの StyleBook です。NetScaler ADM では、システムに存在する StyleBook の種類や表示状態に関係なく、すべての StyleBook を表示できます。また、StyleBook 同士がどのように接続されているかをグラフィカルに表示することもできます。

このドキュメントでは、StyleBook のさまざまなタイプについて説明します。また、NetScaler ADM から StyleBooks に対して実行できる以下のアクションについても説明します。

- カスタム StyleBook をダウンロードして修正するか、既存の StyleBook に基づいて StyleBook を作成します。
- ADM のデフォルトの StyleBook を非表示にします。
- NetScaler ADM からカスタム StyleBook を削除します。
- StyleBooks にタグを追加します。

### デフォルトおよびカスタム **StyleBook**

- デフォルトの **StyleBook** は、NetScaler ADM に同梱されている StyleBook で、NetScaler ADC インスタンスに展開できる構成を作成できます。デフォルトの StyleBooks は削除できませんが、ADM GUI からは非表示にできます。
- カスタム **StyleBook** は、NetScaler ADM にインポートした独自の StyleBook です。

デフォルトの StyleBook とカスタム StyleBook はどちらもパブリックまたはプライベートにすることができます。

### パブリックおよびプライベートの **StyleBook**

構成パックを作成できる StyleBooks は、パブリック StyleBooks に分類できます。つまり、これらはすべて、NetScaler ADM GUI および API から構成を作成するために直接使用することができます。

しかし、一部の StyleBook は、他の StyleBook のビルディングブロックとして使用されます。そのような **StyleBook** はプライベートとしてマークされます。プライベート StyleBook は、NetScaler ADM GUI から構成パックを直接作成することはできません。ただし、NetScaler ADM でこれらの StyleBook を表示および表示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。NetScaler ADM API を使用して構成パックを作成するために、プライベート StyleBooks を使用できます。

プライベートとしてマークされた **StyleBook** の例

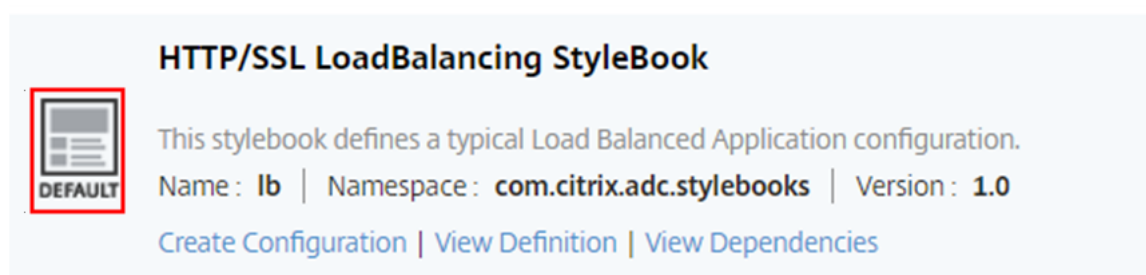
```
1 name: basic-lb-config
2 namespace: com.example.stylebooks
3 version: "0.1"
4 display-name: Load Balancing Configuration
5 description: |
6     This StyleBook defines a simple load balancing configuration and is
7     a building block to build other load balancing configurations.
8 schema-version: "1.0"
9 private: true
10 <!--NeedCopy-->
```

## StyleBook を見る


NetScaler ADM では、StyleBook の数がデフォルトとプライベートの両方で増加しています。アクセスしたい特定の StyleBook を検索することもできます。また、両方のタイプの StyleBook を別々に表示することもできます。

NetScaler ADM で、[アプリケーション] > [**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 のパネルには、次のアイコンがあります。



**HTTP/SSL LoadBalancing StyleBook**


 This stylebook defines a typical Load Balanced Application configuration.

Name: lb | Namespace: com.citrix.adc.stylebooks | Version: 1.0

[Create Configuration](#) | [View Definition](#) | [View Dependencies](#)

デフォルトのプライベート StyleBook には、プライベート StyleBook として宣言するアイコンがあります。

**lbvserver-params**




This stylebook defines the parameters for a load balancing virtual server.  
 Name: **lbvserver-params** | Namespace: **com.citrix.adc.commonotypes** | Version: **1.0**  
[View Definition](#) | [View Dependencies](#)

プライベート StyleBook の定義と依存関係を表示できますが、GUI を使用してプライベート StyleBook から構成パックを作成することはできません。プライベート StyleBook の主な目的は、別の StyleBook のビルディングブロックとして使用することです。Building-blocks-StyleBooks を使用すると、一般的な構成パターンの再利用を促進します。

カスタムパブリック StyleBook には、次の図に示すように別のアイコンが表示されます。


**Enable Netscaler features** | Citrix ADC Versions Supported : **10.5, 11.0, 11.1, 12.0 and 12.1**



This shows how to enable Netscaler features  
 Name: **EnableFeatures** | Namespace: **com.example.stylebooks** | Version: **0.1**  
[Create Configuration](#) | [View Definition](#) | [View Dependencies](#) | [Download](#) | [Delete](#)

カスタムプライベート StyleBook は次のアイコンで表示されますが、

**certificate**




This stylebook defines a typical ssl certificate type.  
 Name: **certificate** | Namespace: **com.citrix.adc.commonotypes** | Version: **1.1**  
[View Definition](#) | [View Dependencies](#) | [Download](#) | [Delete](#)

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表示されます。StyleBook には、すべて、パブリック、またはプライベートの 3 つのオプションがあります。オプションの 1 つをクリックします。

StyleBooks |  🔄 Public ▼ ⚙️


🔍 [Click here to search or you can enter Key : Value format](#)

**Enable Netscaler features** | Citrix ADC Versions Supported : 10.5, 11.0, 11.1, 12.0 and 12.1




This shows how to enable Netscaler features  
 Name: **EnableFeatures** | Namespace: **com.example.stylebooks** | Version: **0.1**  
[Create Configuration](#) | [View Definition](#) | [View Dependencies](#) | [Download](#) | [Delete](#)

**HTTP/SSL LoadBalancing StyleBook** | Citrix ADC Versions Supported : 10.5, 11.0, 11.1, 12.0 and 12.1



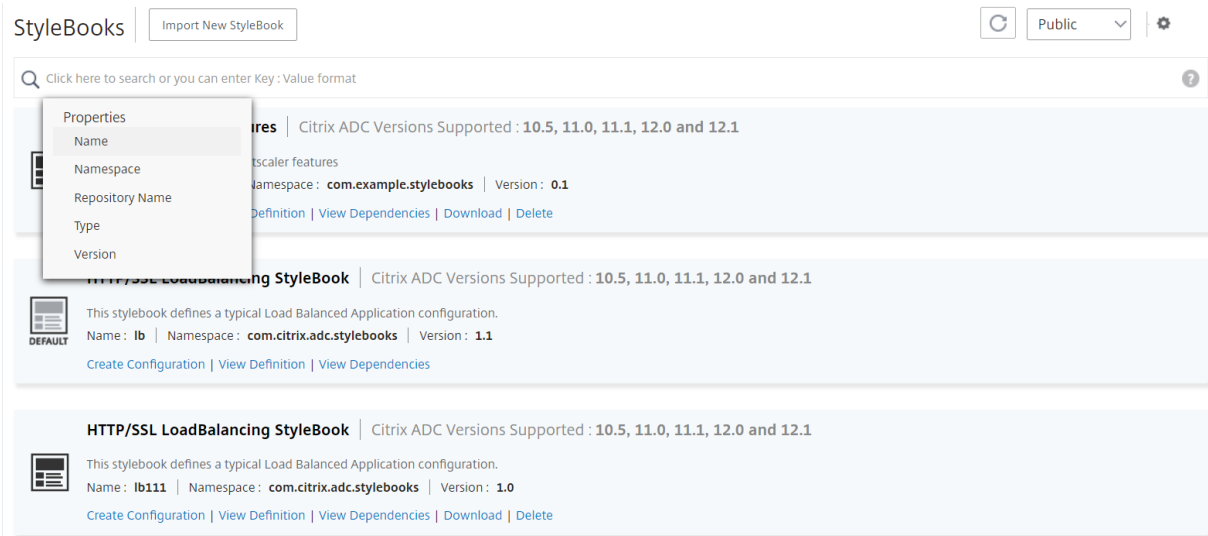
This stylebook defines a typical Load Balanced Application configuration.  
 Name: **lb** | Namespace: **com.citrix.adc.stylebooks** | Version: **1.1**  
[Create Configuration](#) | [View Definition](#) | [View Dependencies](#)

**HTTP/SSL LoadBalancing StyleBook** | Citrix ADC Versions Supported : 10.5, 11.0, 11.1, 12.0 and 12.1



This stylebook defines a typical Load Balanced Application configuration.  
 Name: **lb111** | Namespace: **com.citrix.adc.stylebooks** | Version: **1.0**  
[Create Configuration](#) | [View Definition](#) | [View Dependencies](#) | [Download](#) | [Delete](#)

検索アイコンをクリックして、特定の StyleBook を検索することもできます。名前、名前空間、バージョン属性、またはこれらのオプションの組み合わせで検索できます。検索操作では、大文字と小文字は区別されません。

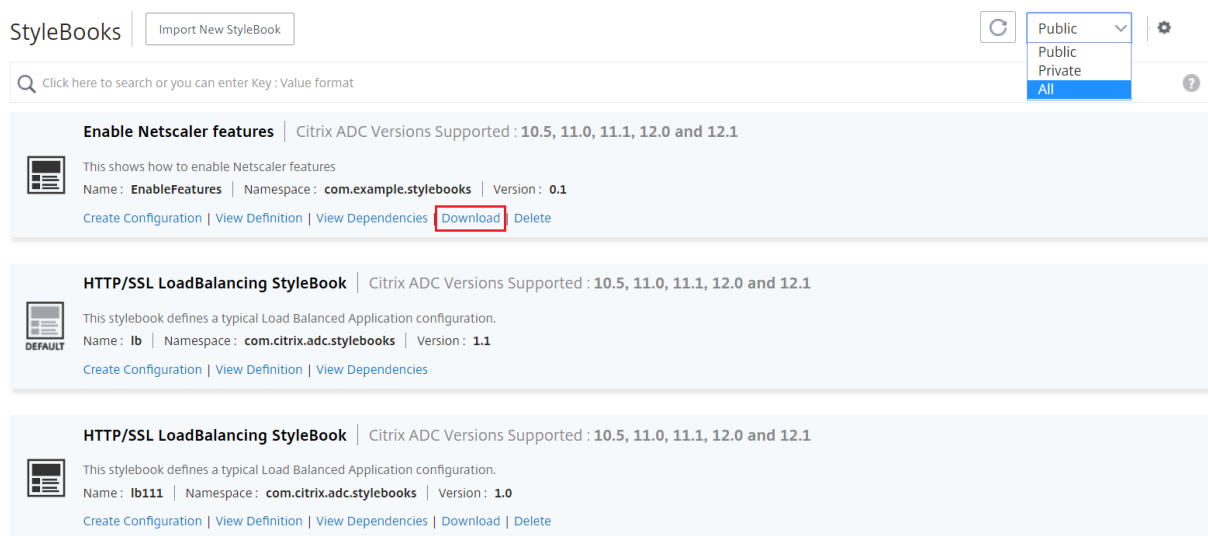


## カスタム StyleBook をダウンロードする

NetScaler ADM からカスタム StyleBook をダウンロードするには、[アプリケーション] > [StyleBooks] > [構成] に移動します。右側のパネルに表示される StyleBook のリストで、カスタム定義の StyleBook をダウンロードするオプションをオンにします。[Download] をクリックします。StyleBook に依存するカスタム StyleBook がある場合は、ダウンロードしたバンドルに依存する StyleBook を含めることができます。

注:

公開または非公開としてマークされているカスタム StyleBook をダウンロードできます。



注:

NetScaler ADM デフォルトの StyleBook をダウンロードすることはできません。それらの定義と依存関係を表示できます。これを行うには、StyleBook パネルの「表示定義」および「依存関係の表示」リンクをクリックします。

### 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。NetScaler ADM から StyleBook を削除するかどうかを確認するポップアップウィンドウが表示されます。StyleBook で他のカスタム StyleBook が使用されている場合は、チェックボックスをオンにしてその StyleBook を削除できます。

StyleBooks | Import New StyleBook

Public | Public | Private | All

Click here to search or you can enter Key: Value format

**Enable Netscaler features** | Citrix ADC Versions Supported : 10.5, 11.0, 11.1, 12.0 and 12.1

This shows how to enable Netscaler features

Name : EnableFeatures | Namespace : com.example.stylebooks | Version : 0.1

Create Configuration | View Definition | View Dependencies | Download | Delete

**HTTP/SSL LoadBalancing StyleBook** | Citrix ADC Versions Supported : 10.5, 11.0, 11.1, 12.0 and 12.1

This stylebook defines a typical Load Balanced Application configuration.

Name : lb | Namespace : com.citrix.adc.stylebooks | Version : 1.1

Create Configuration | View Definition | View Dependencies

**HTTP/SSL LoadBalancing StyleBook** | Citrix ADC Versions Supported : 10.5, 11.0, 11.1, 12.0 and 12.1

This stylebook defines a typical Load Balanced Application configuration.

Name : lb111 | Namespace : com.citrix.adc.stylebooks | Version : 1.0

Create Configuration | View Definition | View Dependencies | Download | Delete

注:

NetScaler ADM 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。そうしないと、既存の StyleBook が壊れます。

### StyleBook の依存関係を表示する

StyleBook の重要かつ便利な特徴の 1 つは、別の StyleBook の構築ブロックとして使用できる点です。StyleBook を別の StyleBook にインポートできます。インポートされた StyleBook は型として宣言され、2 番目の StyleBook のコンポーネントまたはパラメータで使用されます。NetScaler ADM で既存のデフォルトの StyleBook を調べて、1 つの StyleBook を別の StyleBook の上に構築する方法を学ぶことができます。

NetScaler ADM では、StyleBook の相互接続方法をグラフィカルに表示できます。この表現は、他の StyleBook をビルディングブロックとして使用して構築された複雑な StyleBook に特に便利です。ディペンデンスグラフを見ると、複数の StyleBook 間の関係や依存関係を確認できます。



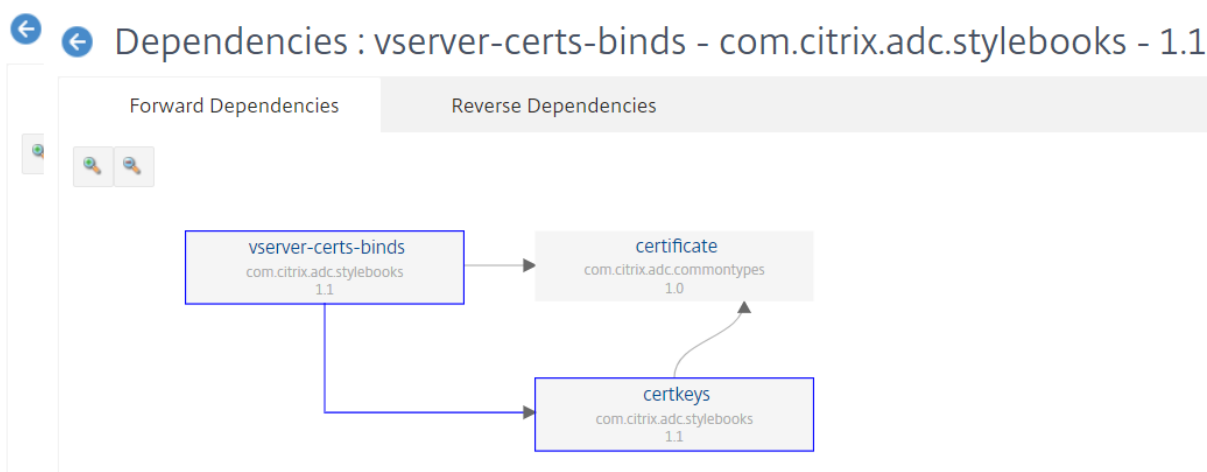
他の StyleBook で使用されている StyleBook は、既存の StyleBook が壊れるため、システムから削除することはできません。ディペンデンシーグラフ表示を使用して、StyleBook の削除を妨げている StyleBook を特定できます。

### StyleBook の依存関係を表示するには

NetScaler ADM で、[アプリケーション] > [StyleBook] に移動します。[StyleBook] ページには、Citrix ADM で使用可能なすべての StyleBook が表示されます。下にスクロールして、StyleBook を見つけます。**StyleBook** タイルには、構成の作成、StyleBook の定義の表示、StyleBook の依存関係の表示へのリンクが表示されます。[依存関係の表示] をクリックします。

### フォワード依存関係

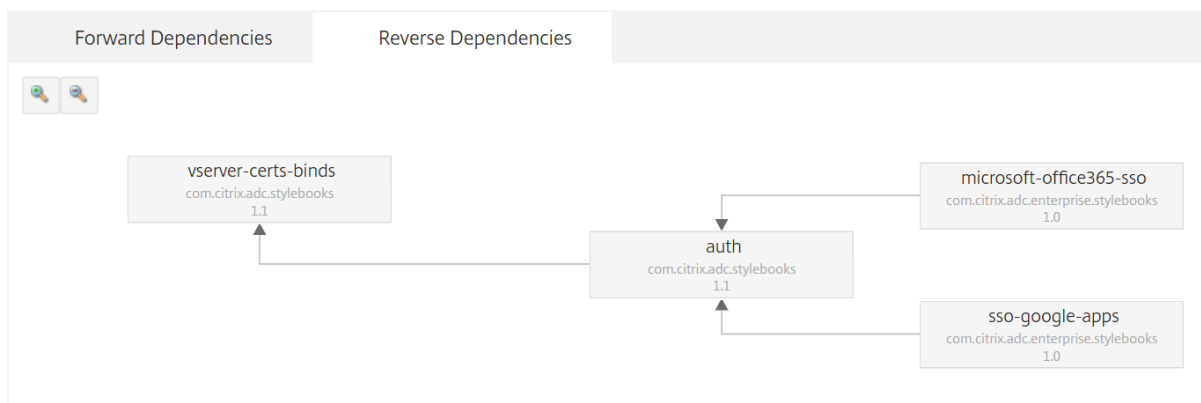
前方依存関係タブでは、StyleBook が使用しているさまざまなデフォルトの StyleBook を表示できます。矢印に従って、StyleBook が使用している StyleBook を見つけてください。矢印の 1 つにマウスを合わせると、矢印と相互に接続されている StyleBook が強調表示されます。StyleBook の名前をクリックして、その StyleBook の定義を表示することもできます。



### 逆依存関係

「逆依存関係」タブでは、StyleBook を使用している StyleBook をグラフィカルに表示できます。矢印に従えば、表示内のすべての StyleBook が StyleBook の方向を指していることがわかります。StyleBook が直接使用している場合や、StyleBook が別の StyleBook を介して StyleBook を使用している場合があります。

## Dependencies : vserver-certs-binds - com.citrix.adc.stylebooks - 1.1



### 構成パックに対する **ADC** 構成の監査

StyleBook 構成パックで行った変更を、現在の ADC 構成と比較できます。この比較では、次の操作を実行できます：

- StyleBook 構成パックと ADC 構成間の構成ドリフトを検出します。
- ADC 上で変更または削除されたオブジェクトで、構成パックによって加えられた変更を反映していないオブジェクトを特定します。

構成パックの変更と ADC の設定を比較するには、次の手順に従います。

1. 「アプリケーション」 > 「**StyleBook**」 > 「構成」に移動します。
2. 「構成監査」をクリックします。

「構成の監査」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。

**Configuration Audit** X

Modified Deleted

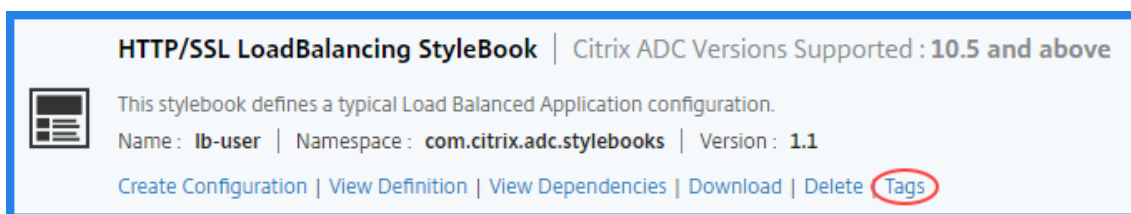
|                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Objects Created on Instance : ██████████   Count : 3</p> <ul style="list-style-type: none"> <li>▶ Type : servicegroup</li> <li>▶ Type : lbvserver_servicegroup_binding</li> <li>▶ Type : lbvserver                             <ul style="list-style-type: none"> <li>name : lb-mon1-lb</li> <li>servicetype : HTTP</li> <li>ipv46 : 65.54.43.32</li> <li>port : 80</li> </ul> </li> </ul> | <p>Objects Audited on Instance : ██████████   Count : 3</p> <ul style="list-style-type: none"> <li>▶ Type : servicegroup</li> <li>▶ Type : lbvserver_servicegroup_binding</li> <li>▶ Type : lbvserver                             <ul style="list-style-type: none"> <li>name : lb-mon1-lb</li> <li>servicetype : HTTP</li> <li>ipv46 : 10.20.30.40</li> <li>port : 80</li> </ul> </li> </ul> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## StyleBook のタグを作成する

NetScaler ADM では、任意の StyleBook にタグを追加できます。タグは、異なる条件を使用して StyleBook をグループ化できるキーと値のペアです。これらのタグは、NetScaler ADM で StyleBook を検索またはフィルタリングするときに使用できます。

StyleBook にタグを追加するには:

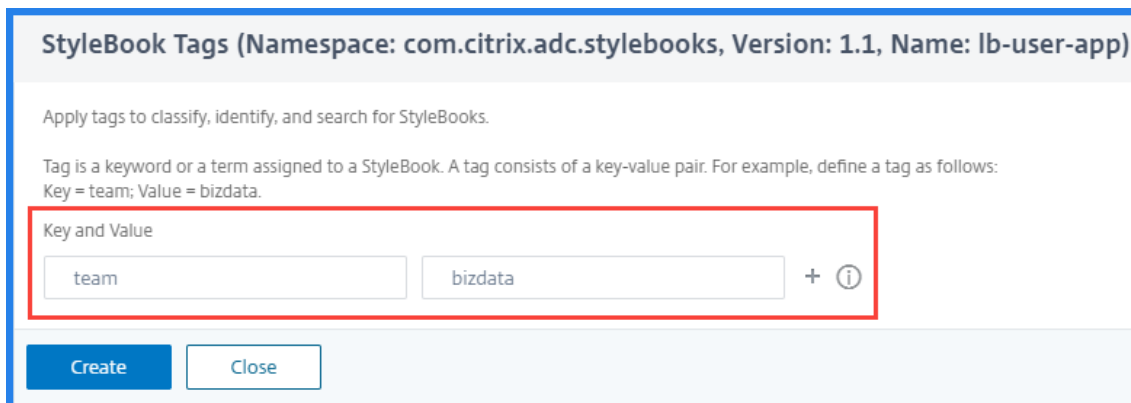
1. 「アプリケーション」 > 「StyleBook」 に移動します。
2. **StyleBook** で、タグを追加するタグを選択します。



すべてのタイプの StyleBook にタグを追加できます。

3. StyleBook をフィルタリングするのに役立つ、必要な キーと値の 情報を指定します。

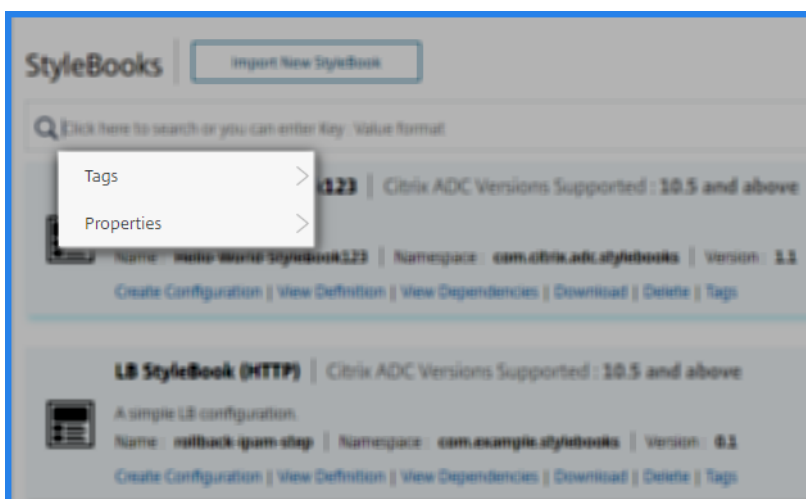
たとえば、キー = チームと値 = BizData



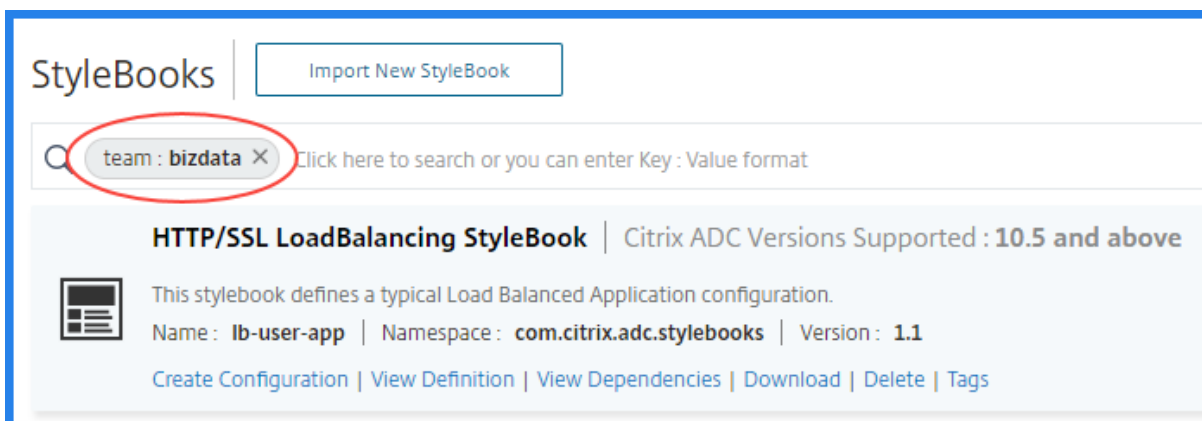
タグを追加するには、[+] をクリックします。

4. [作成] をクリックします。

タグを使用して StyleBooks をフィルタするには、検索バーで [タグ] をクリックし、リストからキーと値を選択します。指定したタグに一致する StyleBooks が表示されます。



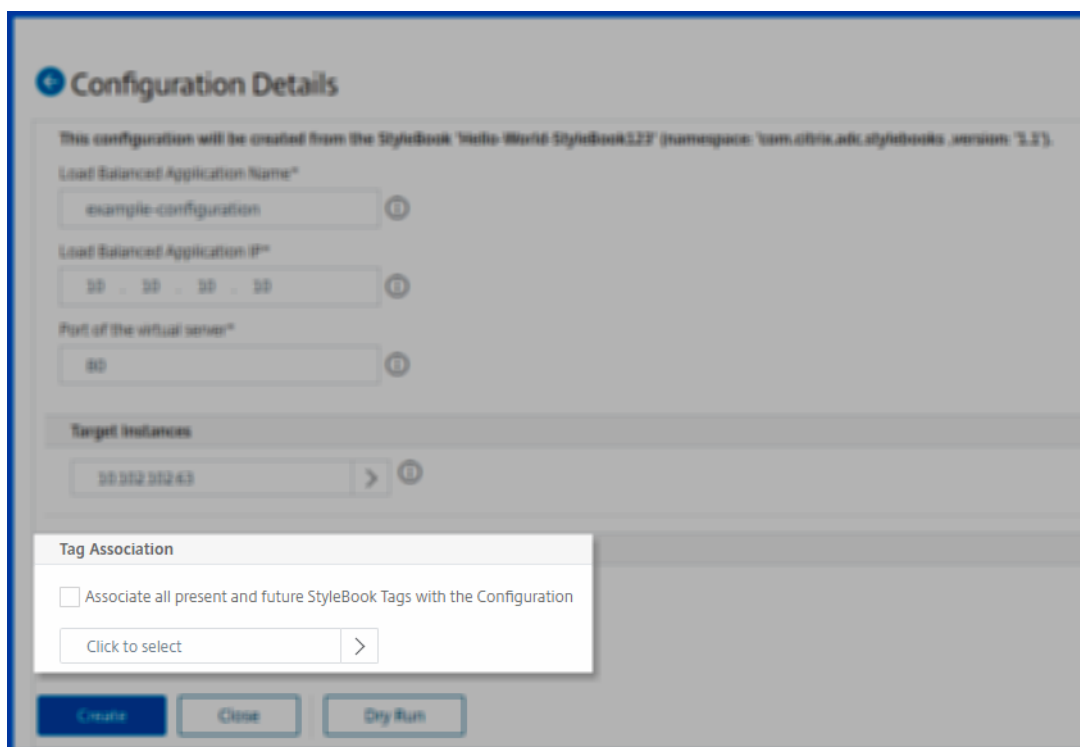
次に、key=teamおよびvalue=bizdataというタグを持つ StyleBooks を検索する例を示します。



StyleBook タグを構成パックに関連付けることができます。そのため、StyleBook タグ自体を使用して構成パックを検索できます。

構成パックを作成するときは、[ タグの関連付け ] セクションで次のいずれかのオプションを使用します：

- 現在および将来のすべての **StyleBook** タグを構成に関連付ける—このオプションは、すべての StyleBook タグを構成パックに関連付けます。また、今後 StyleBooks に追加する可能性のある新しいタグを必ず関連付けます。
- 「タグの選択」 -このオプションは、選択した StyleBook のタグを表示します。必要な StyleBook タグを選択し、構成パックに関連付けることができます。



## GitHub リポジトリからの **StyleBook** のインポートと同期

February 6, 2024

開発に CI/CD プロセスを使用しているシナリオを考えてみましょう。または、すべてのアプリケーションソースコードとデプロイオブジェクトを GitHub で管理しているシナリオ。

GitHub リポジトリでは、Citrix ADC 構成をデプロイしてこれらの StyleBook を管理するための StyleBook を複数作成している場合があります。これらの StyleBook は、Citrix のアプリケーションおよびデリバリー管理 (ADM) にも必要です。これで、これらの StyleBook を Citrix ADM に直接インポートできます。GitHub から手動でコピーして Citrix ADM にアップロードしたり、ADM と GitHub の両方でファイルを手動で同期したりする必要はありません。

GitHub リポジトリを表すリポジトリを NetScaler ADM で定義できるようになりました。GitHub リポジトリの URL と、GitHub で作成したユーザ名とパスワード (または API トークン) を入力します。つまり、GitHub で有効なアカウントを持つ権限のあるユーザーのみが StyleBook をインポートおよび同期できます。

リポジトリを作成したら、NetScaler ADM を GitHub リポジトリと同期できます。Citrix ADM は GitHub に接続し、そのリポジトリにある StyleBook をインポートします。次に、ADM は StyleBook を検証し、Citrix ADM の StyleBook のリストに追加します。検証に失敗した場合、StyleBook は NetScaler ADM に追加されません。エラーを修正し、更新されたバージョンを GitHub リポジトリにコミットします。その後、それらをインポートするか、NetScaler ADM に再度同期してみてください。

注

- StyleBooks ファイルは、GitHub リポジトリのどのブランチからでもインポートおよび同期できます。
- 依存関係にある StyleBook が関連付けられている StyleBook をインポートして同期することもできます。
- GitHub リポジトリからの StyleBooks の同期は、NetScaler ADM GUI または API から手動で開始する必要があります。つまり、現在、StyleBook のインポートと同期は、GitHub コミットアクティビティに基づいて自動的に行われません。

### リポジトリを追加し、**GitHub** リポジトリから **StyleBook** をインポートする

開始する前に、GitHub に有効なアカウントがあることを確認してください。

StyleBook ファイルは、GitHub リポジトリ内の任意のフォルダーから ADM にインポートできます。

1. Citrix ADM で、[アプリケーション] > [**StyleBook**] > [リポジトリ] に移動します。
2. [追加] をクリックします。「リポジトリの追加」ウィンドウで、次のパラメータを入力します。
  - 名前。リポジトリの名前を入力します。この名前は、GitHub のリポジトリ名と同じでもかまいません。
  - リポジトリの **URL**。GitHub リポジトリの URL を入力します。
  - ユーザー名とパスワード。GitHub アカウントにアクセスするためのユーザー名とパスワードを入力します。

注:

パスワードの代わりに API トークンを指定することもできます。HTTPS 経由で GitHub のパスワードの代わりに API トークンを使用できます。GitHub リポジトリの API トークンを作成する方法については、[個人アクセストークンの作成に関するGitHub ドキュメント](#)を参照してください。

3. [作成] をクリックします。

### ← Add Repository

Add GitHub repository details

Name\*

Repository URL\*

User Name\*

Password  API Token

Password\*

リポジトリは NetScaler ADM で作成されます。

4. **StyleBook** をインポートまたは同期するには、リポジトリページでリポジトリを選択し、「同期」をクリックします。

ここで使用できるその他のアクションは次のとおりです。

- **編集**。リポジトリの URL、ユーザー名、パスワード (または API トークン) を編集できます。
- **【削除】**。リポジトリを、その GitHub リポジトリから以前にインポートされた Citrix ADM に存在するすべての StyleBook とともに削除できます。

注:

ConfigPack が関連付けられている StyleBook がある場合は、NetScaler ADM からリポジトリを削除できません。まず、これらの StyleBook のすべての構成パックを削除します。後で NetScaler ADM からリポジトリを削除して、そのリポジトリから StyleBooks をクリーンアップできます。

- **リセット**。Citrix ADM からリポジトリエントリを実際に削除しなくても、そのリポジトリから同期された Citrix ADM 内のすべての StyleBook を削除できます。
- **ファイルを一覧表示**します。NetScaler ADM に存在する、GitHub リポジトリからのすべての StyleBook のリストが表示されます。

デフォルトの **StyleBook** を使用する

February 6, 2024

デフォルトの StyleBook のセットは、NetScaler Application Delivery Management (ADM) に付属しています。デフォルトの StyleBook を使用する場合は、StyleBook でパラメータの値を指定し、構成を実行する NetScaler ADC インスタンスの IP アドレスを選択する必要があります。構成を送信すると、NetScaler ADM は指定したパラメーター値を検証し、構成のグラフを作成し、NetScaler ADC 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。

デフォルトの **StyleBook** から設定を作成するには

1. アプリケーション > 構成 > **StyleBooks** に移動します。StyleBook ページには、NetScaler ADM のすべての StyleBook が表示されます。このリストには、デフォルトとカスタムの StyleBook の両方が含まれています。検索フィールドに StyleBook の名前を入力し、Enter キーを押します。それ以外の場合は、リストを下にスクロールして StyleBook を見つけることができます。
2. 「構成を作成」をクリックします。パラメータに必要な値を指定します。

The screenshot shows a configuration form with the following sections:

- Basic Settings:**
  - Load Balanced Application Name\*: lb-app
  - Load Balanced App Virtual IP address\*: 192 . 128 . 29 . 41
  - Load Balanced App Virtual Port: 80
  - Load Balanced App Protocol\*: HTTP
- Advanced Load Balancer Settings:**
  - Application Servers IP Addresses: 10 . 102 . 29 . 52, 10 . 102 . 29 . 53
  - Application Servers FQDN names: example.app.com
  - Application Server Port\*: 80
  - Application Server Protocol\*: HTTP
- Advanced Application Server Settings:**
  - SSL Certificate Settings: (Empty table with columns: Certificate Name, CertKey Format, Certificate Key Name, Private Key Password)
  - Target Instances: (Click to select button)
  - Dry Run: (Unchecked checkbox)
- Buttons:** Create, Close

3. [ターゲットインスタンス] で、構成を実行する NetScaler ADC インスタンスの IP アドレスをクリックして選択



します。この設定を複数のインスタンスで実行する場合は、「+」をクリックしてさらにインスタンスを追加します。

**Citrix ADM** > [システム] > [システム設定の変更] > [システム設定の変更 \*\*] で [インスタンスログイン \*\* の認証情報を確認する] オプションが有効になっている場合、選択した Citrix ADC インスタンスで構成を実行すると、Citrix ADC インスタンスの認証情報の入力を求められます。それ以外の場合、NetScaler ADM はインスタンスプロファイルに格納されているインスタンス認証情報を使用してインスタンスにログインします。

## ← Modify System Settings

Communication with instance(s)\*

http

- Secure Access Only
- Enable Session Timeout
- Allow Basic Authentication
- Enable nsrecover Login
- Enable Certificate Download
- Enable Shell access for non-nsroot User
- Prompt Credentials for Instance Login

OK Close

NetScaler ADC インスタンスで実行する前に構成をテストまたは検証する場合は、[ドライラン] を選択し、[作成] をクリックします。構成が有効の場合は、指定した値に基づいて作成されたオブジェクトが表示されます。

**Objects** ×

---

**Objects Added on Instance : 10.102.29.140**

---

**Type : server**  
 domain : example.app.com  
 name : example.app.com-server

---

**Type : service**  
 name : example.app.com-service  
 port : 80  
 servername : example.app.com-server  
 servicetype : HTTP

---

**Type : lbserver**  
 appflowlog : ENABLED  
 authentication : OFF  
 authn401 : OFF  
 downstateflush : ENABLED  
 ipv46 : 192.128.29.41  
 lbmethod : LEASTCONNECTION  
 name : lb-app-lb  
 port : 80  
 servicetype : HTTP

---

**Type : servicegroup**  
 cjp : DISABLED  
 cka : NO  
 cmp : NO  
 downstateflush : DISABLED  
 servicegroupname : lb-app-svcgrp  
 servicetype : HTTP  
 sp : OFF  
 state : ENABLED  
 tcpb : NO  
 useproxyport : NO

4. [ドライラン] チェックボックスをオフにし、[作成] をクリックして構成を作成し、NetScaler ADC インスタンスで構成を実行します。作成した StyleBook 構成は、以下に示すように構成のリストに表示されます。

**注**

更新アイコンをクリックして、NetScaler ADM で最近検出された NetScaler ADC 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 ADM を使用して、この構成パックを調査、更新、または削除できるようになりました。

## Web アプリケーションファイアウォール StyleBook

February 6, 2024

Citrix Web App Firewall wall は、Web アプリケーションファイアウォール (WAF) で、アプリケーション層およびゼロデイ脅威を含む既知の攻撃と未知の攻撃の両方から Web アプリケーションとサイトを保護します。

NetScaler ADM は、NetScaler ADC 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 を提供します。

### アプリケーションファイアウォール構成の展開

以下のタスクは、ビジネスネットワーク内の NetScaler ADC インスタンスで、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負荷分散構成を展開するのに役立ちます。

アプリケーション・ファイアウォール設定を使用して **LB** 構成を作成するには、次の手順に従います。

1. NetScaler ADM で、[アプリケーション] > [構成] > [**StyleBook**] に移動します。[StyleBook] ページには、Citrix ADM で使用可能なすべての StyleBook が表示されます。下にスクロールして、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使用した HTTP/SSL 負荷分散 StyleBook を見つけます。StyleBook は、`lb-appfw` という名前を入力して検索することもできます。[構成を作成] 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ます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。

2. 次のパラメーターの値を入力します：

- 負荷分散されたアプリケーション名。ネットワークに展開するアプリケーションファイアウォールを使用した負荷分散設定の名前。
- 負荷分散されたアプリケーションの仮想 **IP** アドレス。NetScaler ADC 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。
- 負荷分散されたアプリケーション仮想ポート。負荷分散されたアプリケーションにアクセスする際にユーザーが使用する TCP ポート。
- 負荷分散された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。

Load Balanced Application Name\*

Load Balanced App Virtual IP address\*

Load Balanced App Virtual Port

Load Balanced App Protocol\*

Advanced Load Balancer Settings

Application Server Protocol\*

3. オプションとして、ロードバランサーの詳細設定を有効にして構成できます。

Advanced Load Balancer Settings

Advanced load balancer settings

Load Balanced App Client Timeout

Load Balanced App Persistence Timeout

Load Balanced App HTTP header

Load Balanced App URL Redirect

Load Balanced App Threshold Type

Load Balanced App Threshold

4. オプションで、負荷分散仮想サーバのトラフィックを認証するための認証サーバを設定することもできます。

Authentication Parameters

Parameters related to enabling authentication on this virtual IP

Enable Authentication

FQDN of Auth VServer

Name of Auth VServer

Enable HTTP 401 Auth

5. [サーバー IP とポート] セクションの [+] をクリックして、アプリケーションサーバーと、それらにアクセス可能なポートを作成します。

Application Server IP Address\*

Application Server Port

Weight

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。

Application Server Domain Name\*

Application Server Port

7. SSL 証明書の詳細を指定することもできます。

Certificate Name\*

  
Certificate File\* test\_cert.pem  
CertKey Format\*  
Certificate Key Name  
Certificate Key File test\_cert\_key.pem  
Private Key Password  
 Advanced Certificate Settings

8. ターゲット NetScaler ADC インスタンスでモニターを作成することもできます。

Monitor Name\*

  
Monitor Type\*  
Destination IP  
Destination Port  
HTTP Request  
Send String

9. 仮想サーバでアプリケーションファイアウォールを設定するには、WAF 設定を有効にします。

その VIP 上のすべてのトラフィックにアプリケーションファイアウォール設定を適用する場合は、アプリケ

アプリケーションファイアウォールポリシールールが true であることを確認します。それ以外の場合は、NetScaler ADC ポリシールールを指定して、アプリケーションファイアウォール設定を適用する要求のサブセットを選択します。次に、適用する必要があるプロファイルのタイプ (HTML または XML) を選択します。

10. オプションで、アプリケーションファイアウォールの [プロファイル設定] チェックボックスをオンにして、アプリケーションファイアウォールプロファイルの詳細設定を構成できます。
11. 必要に応じて、アプリケーションファイアウォール署名を構成する場合は、仮想サーバーを展開する NetScaler ADC インスタンス上に作成される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、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を構成することもできます。

アプリケーションファイアウォールと構成設定の詳細については、「アプリケーションファイアウォール」を参照してください。

13. [ターゲットインスタンス] セクションで、アプリケーションファイアウォールで負荷分散仮想サーバーを展開する NetScaler ADC インスタンスを選択します。

注:

更新アイコンをクリックして、NetScaler ADM で最近検出された NetScaler ADC 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一覧に追加することもできます。

14. **IP** レピュテーションチェックを有効にして、不要な要求を送信している IP アドレスを特定することもできます。IP レピュテーションリストを使用すると、不正なレピュテーションを持つ IP からの要求をプリエンプティブに拒否できます。
15. 「作成」をクリックして、選択した Citrix ADC インスタンスで構成を作成します。

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、Dry Run を選択して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ことを推奨します。

構成が正常に作成されると、StyleBook は必要な負荷分散仮想サーバー、アプリケーションサーバー、サービス、サービスグループ、アプリケーションファイアウォールラベル、アプリケーションファイアウォールポリシーを作成し、負荷分散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るオブジェクトを示しています。



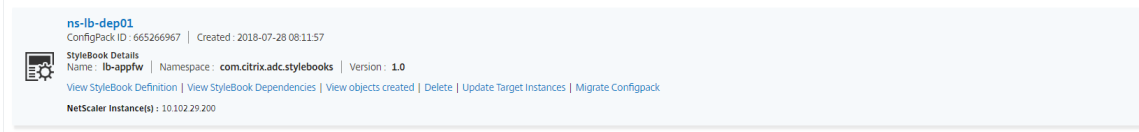
**Objects created ( 13 )** ✕

✓ The ConfigPack ' (ID: 665266967) using the StyleBook 'lb-appfw' (namespace: 'com.citrix.adc.stylebooks', version: '1.0') has been successfully created. ✕

**Instance : 10.102.29.200 | Count : 13**

|                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Type : lbserver</b><br/>                     ip46 : 10.10.10.1<br/>                     name : ns-lb-dep01-lb<br/>                     port : 80<br/>                     servicetype : HTTP</p>                                                                                                                                                                                                                                                    |
| <p><b>Type : servicegroup</b><br/>                     servicegroupname : ns-lb-dep01-svcgrp<br/>                     servicetype : HTTP</p>                                                                                                                                                                                                                                                                                                              |
| <p><b>Type : lbserver_servicegroup_binding</b><br/>                     name : ns-lb-dep01-lb<br/>                     servicegroupname : ns-lb-dep01-svcgrp</p>                                                                                                                                                                                                                                                                                          |
| <p><b>Type : server</b><br/>                     ipaddress : 10.10.10.2<br/>                     name : 10.10.10.2</p>                                                                                                                                                                                                                                                                                                                                    |
| <p><b>Type : servicegroup_servicegroupmember_binding</b><br/>                     ip : 10.10.10.2<br/>                     port : 80<br/>                     servicegroupname : ns-lb-dep01-svcgrp</p>                                                                                                                                                                                                                                                   |
| <p><b>Type : server</b><br/>                     domain : AppServer.newdomain.com<br/>                     name : AppServer.newdomain.com-server</p>                                                                                                                                                                                                                                                                                                      |
| <p><b>Type : service</b><br/>                     name : AppServer.newdomain.com-service<br/>                     port : 80<br/>                     servername : AppServer.newdomain.com-server<br/>                     servicetype : HTTP</p>                                                                                                                                                                                                          |
| <p><b>Type : lbserver_service_binding</b><br/>                     name : ns-lb-dep01-lb<br/>                     servicename : AppServer.newdomain.com-service</p>                                                                                                                                                                                                                                                                                       |
| <p><b>Type : nsfeature</b><br/>                     Meta Properties<br/>                     action : enable<br/>                     feature : appfw</p>                                                                                                                                                                                                                                                                                                 |
| <p><b>Type : appfwpolicylabel</b><br/>                     labelname : ns-lb-dep01-appfwpolicylabel<br/>                     policylabeltype : HTTP_REQ</p>                                                                                                                                                                                                                                                                                               |
| <p><b>Type : appfwpolicy</b><br/>                     name : ns-lb-dep01-iprep-appfw-policy<br/>                     profilename : APPFW_BLOCK<br/>                     rule : CLIENTIPSRC.IPREP_IS_MALICIOUS</p>                                                                                                                                                                                                                                         |
| <p><b>Type : appfwpolicylabel_appfwpolicy_binding</b><br/>                     gotopriorityexpression : END<br/>                     labelname : ns-lb-dep01-appfwpolicylabel<br/>                     policyname : ns-lb-dep01-iprep-appfw-policy<br/>                     priority : 20</p>                                                                                                                                                             |
| <p><b>Type : lbserver_appfwpolicy_binding</b><br/>                     bindpoint : REQUEST<br/>                     gotopriorityexpression : END<br/>                     invoke : true<br/>                     labelname : ns-lb-dep01-appfwpolicylabel<br/>                     labeltype : policylabel<br/>                     name : ns-lb-dep01-lb<br/>                     policyname : NOPOLICY-APPFW<br/>                     priority : 10</p> |

16. NetScaler ADM で作成された ConfigPack を表示するには、[アプリケーション] > [構成] に移動します。



## StyleBook を使用して WAF と BOT プロファイルを作成する

February 6, 2024

API **Gateway** で **API** リソースに対する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 トラフィックに対して 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 ゲートウェイの管理](#)」を参照してください。

WAF ポリシーと BOT ポリシーを API リソースに設定できます。ポリシーを構成する前に、NetScaler Application Delivery Management (ADM) で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、次のデフォルトの StyleBooks を使用します。

- API WAF 検出 StyleBook
- API ボット検出 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 ADM で、[アプリケーション] > [構成] > [**StyleBook**] に移動します。StyleBook を検索するには、`api-waf-profile` という名前を入力します。[構成を作成] 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ます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。
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。
  - アプリケーションタイプ -プロファイルへのアプリケーションの種類を追加します。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ます。
3. オプション、セキュリティ設定を有効にして、HTTP、JSON、または XML の保護チェックを指定します。Citrix Web App Firewall へのエラー URL を指定することもできます。詳細については、「[Web App Firewall プロファイルの作成](#)」を参照してください。
4. この構成を展開するターゲット NetScaler ADC インスタンスまたはインスタンスグループを選択します。
5. [作成] をクリックします。

WAF ポリシーを設定するには、[API デプロイメント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 ADM で、[アプリケーション] > [構成] > [StyleBook] に移動します。StyleBook を検索するには、`api-bot-profile`という名前を入力します。[構成を作成] 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ます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。

2. 「BOT プロファイル名」で、BOT プロファイルを識別する名前を指定します。
3. 必要に応じて、要件に応じ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、不要な要求を送信している IP アドレスを識別します。IP レピュテーションリストを使用すると、不正なレピュテーションを持つ IP からの要求をプリエンティブに拒否できます。
  - **BOT** 署名を有効にする -BOT 署名名を指定します。これは、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。このオプションを使用すると、BOT プロファイルは、指定した IPv4 アドレスまたはサブネットアドレスからの要求をバイパスできます。
  - 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。このオプションを使用すると、BOT プロファイルは、指定した IPv4 アドレスまたはサブネットアドレスからの要求をブロックできます。

4. この構成を展開するターゲット NetScaler ADC インスタンスまたはインスタンスグループを選択します。

5. [作成] をクリックします。

BOT ポリシーを設定するには、[API デプロイメントにポリシーを追加するを参照してください](#)。

## すべてのデフォルト StyleBook を非表示にする

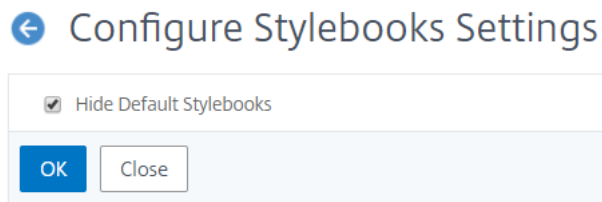
February 6, 2024

Citrix ADM は、Citrix ADM フォルダシステムに存在するすべての StyleBook を一覧表示します。StyleBook のリストには、プライベートとパブリックの両方に使用できるデフォルトの StyleBook とカスタム StyleBook が含まれています。管理者は、デフォルトの StyleBook をすべて非表示にしたい場合があります。ユーザーに、自分またはユーザーが作成したカスタム StyleBook のみの表示とアクセスを許可できます。

NetScaler ADM では、カスタム StyleBook を表示したり、NetScaler ADM に同梱されているデフォルトの StyleBook をすべて非表示にしたりできます。デフォルトの StyleBook をすべて非表示にできる新しい GUI オプションが提供されました。

すべてのデフォルトの **StyleBook** を非表示にするには:

1. NetScaler ADM で、[アプリケーション] > [構成] > [設定] に移動します。
2. 設定ページには、デフォルトの StyleBook がユーザーに表示されるかどうかに関する情報が表示されます。
3. デフォルトの StyleBook を非表示にするには、右上の編集アイコンをクリックします。
4. 「**StyleBook** 設定の構成」ページで、「デフォルトの **StyleBook** を非表示にする」オプションを選択します。
5. **[OK]** をクリックします。



RBAC 機能を使用してページを非表示にすることを選択していない場合でも、**StyleBook** 設定の構成ページはユーザーに表示されます。ユーザーには、デフォルトの StyleBook を再表示するためのオプションが残っている場合があります。

**StyleBook** の設定ページを非表示にするには、ポリシーを作成し、そのポリシーをデフォルトの StyleBook が表示されないはずのユーザーに割り当てる必要があります。

**RBAC** ポリシーを作成するには、次の手順を実行します。

1. NetScaler ADM で、[アカウント] > [ユーザー管理] > [アクセスポリシー] に移動します。
2. **[Add]** をクリックしてポリシーを作成します。
3. ポリシー名を入力します。
4. 「権限」セクションで、「すべて」>「アプリケーション」>「構成」>「設定」が選択されていないことを確認し、「**OK**」をクリックします。

ポリシーを作成したら、ロールを作成し、各ロールを 1 つ以上のポリシーにバインドし、ロールをユーザグループに割り当てる必要があります。ポリシーをユーザに関連付ける方法の詳細については、「[ロールベースのアクセス制御の設定](#)」を参照してください。

## StyleBooks 構成ビルダーを使用した NetScaler ADC アプリケーション構成の移行

February 6, 2024

注

この機能はテクニカルプレビュー中です。

StyleBooks 構成ビルダーは、既存の Citrix ADC 構成からアプリケーション構成 StyleBook を作成するために使用されます。この機能により、ある NetScaler ADC インスタンスから別のインスタンスへのアプリケーション構成の移行も自動化されます。

構成ビルダーを使用すると、カスタマイズされた StyleBook を作成する要件を簡素化できます。この機能により、StyleBooks の文法や構成に関する深い知識がなくても StyleBook を作成できます。それ以外の場合は、StyleBooks の作成には StyleBooks の文法と構文の知識が必要です。

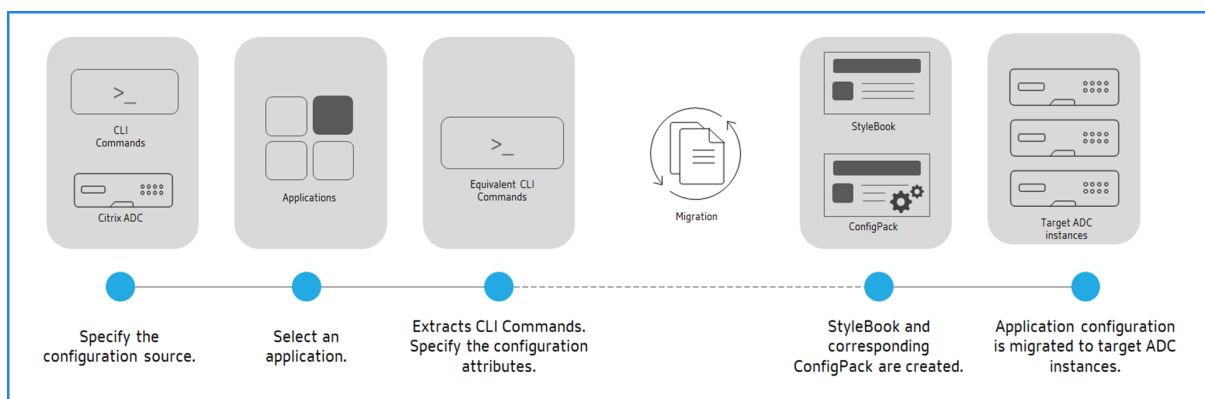
構成ビルダーは、同じ ADC 構成を新しい ADC インスタンスに反映する ConfigPack も作成します。この ConfigPack を使用すると、ある ADC インスタンスの初期 ADC 構成を別の ADC インスタンスに複製できます。初期設定ソースは、次のいずれかになります：

- **NetScaler ADC** インスタンス：複製するアプリケーション構成をホストするインスタンスを指定します。  
ターゲットインスタンスを指定しなくても、構成ビルダーは ADC 構成を StyleBook および ConfigPack に変換します。後でこの configpack を使用して、ADC 構成を他の ADC インスタンスに移行できます。
- **CLI** コマンドのセット： `ns.conf` または `Application config` から設定を貼り付けます。

構成ビルダーは、ソース構成に埋め込まれている個別のアプリケーションのリストを識別します。目的の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、ソース設定から抽出されます。また、入力が必要とする可能性のあるデプロイメントおよび構成属性も識別します。

- デプロイ属性 - 仮想サーバー、サービス、サービスグループメンバーの IP アドレスとポートを元の構成から表示および編集できます。
- 構成属性 - これらの属性には、ソース構成で指定されたパスワードまたは証明書を使用できます。

必要な情報を指定したら、ターゲット ADC インスタンスでアプリケーション構成の移行または複製を開始します。



アプリケーションの作成と移行が完了すると、ConfigPack が対応する StyleBook とともに Citrix ADM に作成されます。この ConfigPack は、ターゲット ADC インスタンスのアプリケーション構成を表します。作成した **ConfigPack** を表示するには、[ \*\* アプリケーション ] > [ **StyleBook** ] > [構成] に移動します。 \*\*

サポートされている **NetScaler ADC** 機能

StyleBook 構成ビルダーは、ソース構成内の以下の NetScaler ADC 機能を認識してサポートします。

- コンテンツスイッチ
- 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)

### StyleBook を作成して NetScaler ADC アプリケーション構成を移行する

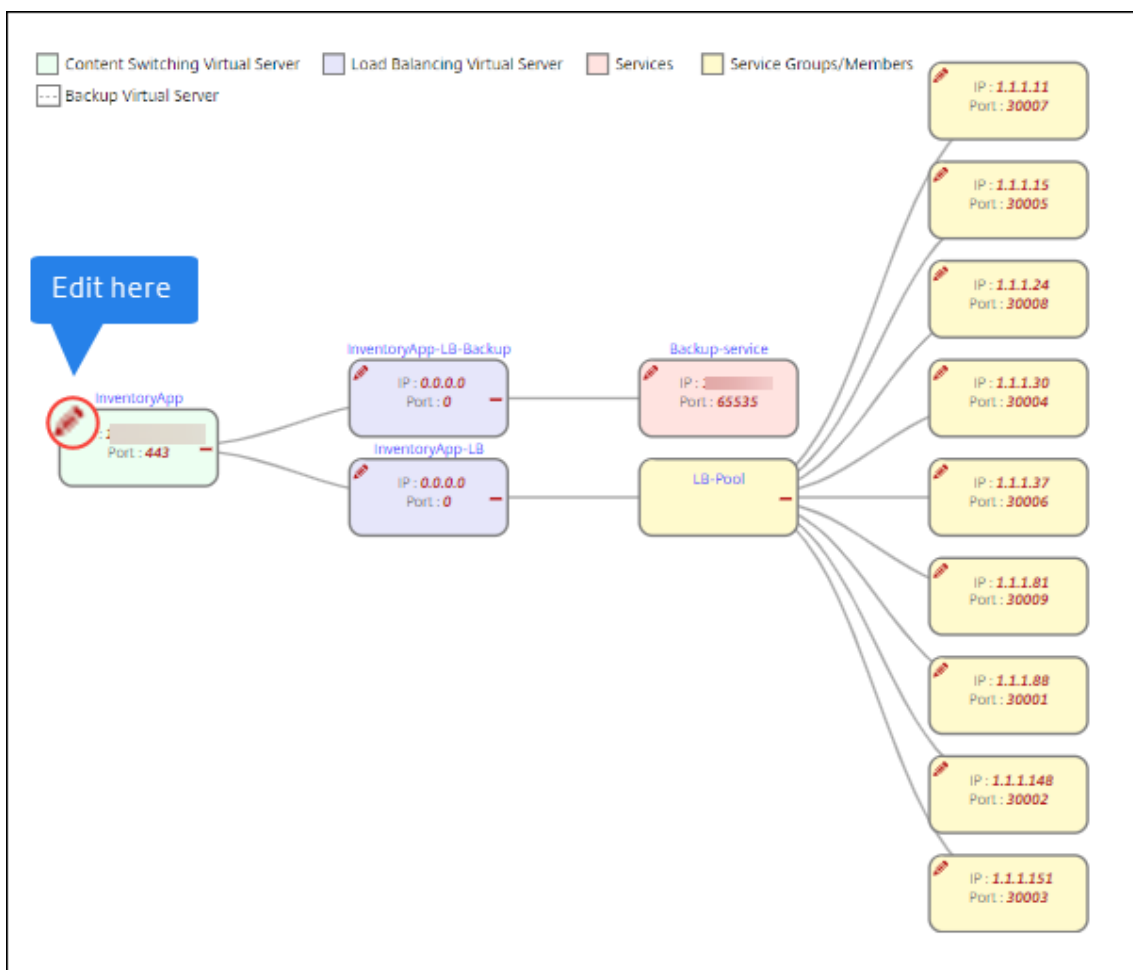
以下の手順は、NetScaler ADM で NetScaler ADC アプリケーションの移行を移行する StyleBook を作成することです。

1. 「アプリケーション」 > 「**StyleBook**」 > 「構成」 に移動します。
2. 「**ADC** 構成を移行」 をクリックします。
3. 「始める」 をクリックします。
4. 「構成を指定」 で、構成ソースを選択します。
  - **ADC** からインポート: このオプションは、選択した ADC インスタンス上のアクティブなアプリケーションを検出します。

- **CLI** コマンドを使用してインポート: 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の移行元または複製元の **ADC** インスタンスを指定します。
  6. アプリケーション構成の移行先または複製先となるターゲット **ADC** インスタンスを指定します。
  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。
    - 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. 「等価 **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です。
  9. 展開属性では、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、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。



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は異なります。
- CLI コマンドを使用して設定をインポートします。

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、パスワードや証明書を解読するためのキーなどの秘密が一覧表示されます。

注

: 移行を開始する前に、欠落している、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、欠落している構成またはサポートされていない構成をターゲットインスタンスに個別に適用する必要があります

。次に、[次へ]をクリックします。

11. 「移行」で、必要な StyleBook の詳細を指定します。[移行]をクリックします。



## 制限事項

- ソースインスタンスで指定された式や `responderhtmlpages` 言及は識別されません。移行する前に、必ずターゲットインスタンスで名前付き式と `responderhtmlpages` を設定してください。
- ソースに次のような `servicegroup` 設定とモニタバインディングがあるとします。

```
bind serviceGroup <Name> <Port> -monitorName <Monitor_Name>
```

次のエラーが表示されます。

```
1 CLI Command conversion failed: 100 - No such command [{
2   "errorcode": 1090, "message": "No such argument [XXX]", "
   severity": "ERROR"  }
3 ]
4 <!--NeedCopy-->
```

このエラーは、NetScaler ADC がサービスグループとモニターの間のバインディングを無効な形式で保存するために発生します。この問題は、NetScaler ADC 12.1.52.15 ビルドから修正されます。

## ビジネスアプリケーション **StyleBook**

February 6, 2024

NetScaler ADM には、特定のビジネスアプリケーション向けに ADC 構成を展開するのに役立つ StyleBook が用意されています。このような StyleBook について詳しくは、以下のトピックを参照してください。

- [SSO Google Apps StyleBook](#)
- [SSO Office 365 StyleBook](#)
- [Microsoft Skype for Business StyleBook](#)
- [Microsoft Exchange StyleBook](#)
- [Microsoft SharePoint StyleBook](#)
- [Microsoft ADFS proxy StyleBook](#)
- [Oracle e-ビジネス StyleBook](#)
- [Web アプリケーションファイアウォール StyleBook](#)
- [StyleBook を使用して WAF と BOT プロファイルを作成する](#)

## SSO Google Apps StyleBook

February 6, 2024

Google Apps は、Google が開発したクラウドコンピューティング、生産性向上およびコラボレーションツール、ソフトウェア、および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対して 1 回サインインすることで、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 ADM SSO Google Apps StyleBook を使用すると、NetScaler ADC インスタンスを介して Google Apps SSO を有効にすることができます。StyleBook は、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 NetScaler ADC インスタンスを構成します。

この StyleBook を使用して NetScaler ADC インスタンスで Google アプリの SSO を有効にすると、次の手順になります。

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設定
3. 認証仮想サーバーへのポリシーとプロファイルのバインド
4. インスタンスの LDAP 認証サーバーとポリシーの設定
5. LDAP 認証サーバーとポリシーを、インスタンスに構成されている認証仮想サーバーにバインドする

構成の詳細:

次の表に、この統合が正常に機能するために必要な最低限のソフトウェアバージョンを示します。統合プロセスは、同じの上位バージョンもサポートします。

| Product    | 最低限必要なバージョン                |
|------------|----------------------------|
| Citrix ADC | リリース 11.0、アドバンス/プレミアムライセンス |

次の手順では、認証要求を NetScaler ADC が監視する IP アドレスにルーティングするために、適切な外部または内部 DNS エントリをすでに作成していることを前提としています。

**SSO Google** アプリの **StyleBook** 設定をデプロイする:

次のタスクは、Microsoft SSO Google Apps StyleBook をビジネスネットワークにデプロイする際に役立ちます。

**SSO Google** アプリの **StyleBook** をデプロイするには

1. Citrix ADM で、「アプリケーション」>「構成」>「**StyleBook**」に移動します。[StyleBook] ページには、Citrix ADM で使用可能なすべての StyleBook が表示されます。下にスクロールして **SSO Google Apps StyleBook** を見つけてください。[構成を作成] をクリックします。

2. StyleBook がユーザーインターフェイスページとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。
  3. 次のパラメーターの値を入力します：
    - a) アプリケーション名。ネットワークにデプロイする SSO Google アプリ設定の名前。
    - b) 認証仮想 IP アドレス。Google アプリの SAML IdP ポリシーのバインド先となる認証、承認、および監査仮想サーバーで使用される仮想 IP アドレス。
    - c) **SAML** ルール式。デフォルトでは、HTTP.REQ.HEADER (「参照元」) .CONTAINS (「グーグル」) という NetScaler ADC ポリシー (PI) 式が使用されます。要件が異なる場合は、このフィールドを別の式で更新します。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に一致し、リファラーヘッダーが 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、手順 3 で作成した認証、承認、および監査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して、NetScaler ADC 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。このフィールドには、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 Auth VIP>/saml/login`
    - b) **SAML** サービスプロバイダー (**SP**) ID。(オプション) NetScaler ADC 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サービス **URL**。ユーザー認証が成功した後、NetScaler ADC 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サービス URL は、ID プロバイダサーサイトまたはサービスプロバイダサイトで開始できます。
    - d) このセクションには、他にも入力できるオプションフィールドがあります。たとえば、次のオプションを設定できます。
      - i. SAML バインディングプロファイル (デフォルトは「POST」プロファイル)。
      - ii. SAML リクエスト/レスポンスを検証/署名する署名アルゴリズム (デフォルトは「RSA-SHA1」)。
      - iii. SAML リクエスト/レスポンスのハッシュをダイジェストする方法 (デフォルトは「SHA-1」)。
      - iv. 暗号化アルゴリズム (デフォルトは AES256)、およびその他の設定
- 注

これらの設定は Google Apps との互換性がテストされているため、デフォルト設定のままにすることを勧めます。
- e) 「ユーザー属性」チェック・ボックスを有効にして、次のようなユーザー詳細を入力することもできます。
    - i. ユーザー属性の名前

- ii. 属性の値を抽出するために評価される NetScaler ADC PI 式
- iii. わかりやすい属性の名前
- 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ています。この StyleBook を使用して NetScaler ADC 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の次の詳細を入力します。ドメインユーザーが会社の電子メールアドレスを使用して NetScaler ADC インスタンスにログオンできるようにするには、以下を構成する必要があります。

- a) **LDAP (Active Directory)** ベース。認証を許可する Active Directory (AD) 内にユーザーアカウントが存在するドメインの基本ドメイン名を入力します。たとえば、`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 (構成を容易にするために電子メールアドレスを使用) を追加します。たとえば、`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) このセクションに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 ADC がユーザーを認証するために接続する 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 つのうち少なくとも 1 つ (LDAP サーバの IP アドレスまたは FQDN 名) を指定する必要があります。

- iii. NetScaler ADC がユーザーを認証するために接続する 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)、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。ログイン名の抽出に使用されるデフォルトの属性は「sAMAccountName」です。
- vi. その他のオプションの LDAP 設定

6. SAML IdP SSL 証明書セクションでは、SSL 証明書の詳細を指定できます。

- a) 証明書名。SSL 証明書の名前を入力します。
- b) 証明書ファイル。ローカルシステムまたは NetScaler ADM 上のディレクトリから、SSL 証明書ファイルを検索します。

- c) 証明書キー形式。ドロップダウンリストボックスから、証明書と秘密キー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 と .der 拡張子です。
  - d) 証明書キー名。証明書の秘密鍵の名前を入力します。
  - e) 証明書キーファイル。ローカルシステムまたは NetScaler ADM から、証明書の秘密鍵を含むファイルを選択します。
  - f) 秘密鍵のパスワード。秘密鍵ファイルがパスフレーズで保護されている場合は、このフィールドにそれを入力します。
  - g) 証明書の詳細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などの詳細を入力したり、証明書有効期限モニターを有効または無効にしたりすることもできます。
7. 上記で入力した SAML IdP 証明書で NetScaler ADC に CA パブリック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 IdP SSL CA 証明書を選択できます。詳細設定で「Is a CA Certificate」を必ず選択してください。
8. オプションで、[SAML SP SSL 証明書] を選択して、Google Apps (SAML SP) からの認証リクエストの検証に使用する Google SSL 証明書 (公開鍵) を指定できます。
9. [ターゲットインスタンス] をクリックし、この Google Apps SSO 構成を展開する NetScaler ADC 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 ADC インスタンスに構成を展開します。

注

更新アイコンをクリックして、NetScaler ADM で最近検出された NetScaler ADC 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。

また、

ヒント

実際の構成を実行する前に、[ドライ実行] を選択して、StyleBook によってターゲット NetScaler ADC インスタンスに作成された構成オブジェクトを視覚的に確認することをお勧めします。

## SSO Office 365 StyleBook

February 6, 2024

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向上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 iness など、Microsoft の一般的なサーバーベースのアプリケーションが含まれています。シングル・サインオン (SSO) により、ユーザーはすべてのエンタープライズ・クラウド・アプリケーションにアクセスできます。

- 管理者コンソールにサインインする管理者を含む
- エンタープライズ認証情報を使用して、すべての Microsoft Office 365 サービスにワンタイムサインオンします。

SSO Office 365 StyleBook を使用すると、NetScaler ADC インスタンスを介して Microsoft オフィス 365 の SSO を有効にすることができます。NetScaler ADC を SAML アイデンティティプロバイダー (IdP) として、Microsoft Office 365 を SAML サービスプロバイダーとして使用して、SAML 認証を構成できるようになりました。

この StyleBook を使用して NetScaler ADC 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設定
3. 認証仮想サーバーへのポリシーとプロファイルのバインド
4. インスタンスの LDAP 認証サーバーとポリシーの設定
5. LDAP 認証サーバーとポリシーを、インスタンスに構成されている認証仮想サーバーにバインドします。

この統合が正常に機能するために最低限必要なソフトウェアバージョンを示します。統合プロセスは、同じバージョンの上位バージョンでも機能するはずですが。

|Product| 最低限必要なバージョン |

|——|—————|

|Citrix ADC|11.0、アドバンスド/プレミアムライセンス |

次の手順は、適切な外部および内部 DNS エントリが既に作成されていることを前提としています。これらのエントリは、認証要求を NetScaler ADC 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、SSO Office 365 StyleBook をビジネスネットワークに実装するのに役立ちます。

### SSO Microsoft オフィス 365 StyleBook を展開するには

1. Citrix Application Delivery Management (ADM) で、「アプリケーション」>「**StyleBook**」に移動します。**StyleBook** ページには、Citrix ADM で使用できるすべての StyleBook が表示されます。下にスクロールして **SSO Office 365 StyleBook** を見つけてください。[構成を作成] をクリックします。
2. StyleBook がユーザーインターフェイスページとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。
3. 次のパラメーターの値を入力します：
  - a) アプリケーション名。ネットワークに展開する SSO Microsoft Office 365 構成の名前。
  - b) 認証仮想 IP アドレス。Microsoft Office 365 SAML IdP ポリシーがバインドされている AAA 仮想サーバーが使用する仮想 IP アドレス。

SSO Office 365 Application Name\*

Office365\_app\_server ?

Authentication Virtual IP address\*

192 . 10 . 10 . 10 ?

4. **SSL** 証明書の設定セクションで \*\*、SSL 証明書の名前と証明書キーを入力します。

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 ADC 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。また、秘密鍵パスワードを入力して、暗号化された秘密鍵を PEM 形式でロードすることもできます。

SSL Certificate for the Authentication Virtual IP

SSL Certification to be bound to authentication vserver on NetScaler (Not Office 365 Certificate)

Certificate Name\*

office365\_ssl\_test\_cert ?

Certificate File\*

Choose File ▾ test\_cert.pem ?

CertKey Format\*

PEM ▾

Certificate Key Name

office365\_ssl\_test\_cert\_key ?

Certificate Key File

Choose File ▾ test\_cert\_key.pem ?

Private Key Password

Advanced Certificate Settings

6. [証明書の詳細設定] チェックボックスをオン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入力したり、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ができます。

7. **SSL** 証明書で **NetScaler ADC** に **CA** パブリック証明書をインストールする必要がある場合は、オプションで認証仮想 **IP** チェックボックスに **SSL CA** 証明書を選択できます。上記の「証明書の詳細設定」セクションで「**Is a CA Certificate**」を選択してください。
8. [**SSO Office 365** の **LDAP** 設定] セクションで、次の詳細を入力して Office 365 ユーザーを認証します。ドメインユーザーが会社の電子メールアドレスを使用して NetScaler ADC インスタンスにログオンできるようにするには、次のように構成します。

- **LDAP (Active Directory)** ベース。認証を許可する Active Directory (AD) 内にユーザーアカウントが存在するドメインの基本ドメイン名を入力します。たとえば、dc=netScaler、dc=com
- **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 (構成を容易にするために電子メールアドレスを使用) を追加します。たとえば、CN= マネージャ、dc=netScaler、dc=com
- **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。
- このセクションに入力する必要があるその他のフィールドは次のとおりです。
  - NetScaler ADC がユーザーを認証するために接続する LDAP サーバーの IP アドレス。
  - LDAP サーバーの FQDN 名。

注:

上記の 2 つのうち少なくとも 1 つ (LDAP サーバの IP アドレスまたは FQDN 名) を指定する必要があります。

- NetScaler ADC がユーザーを認証するために接続する LDAP サーバーポート (デフォルトは 389 です)。LDAPS は 636 を使用している。
- LDAP ホスト名。検証がオン (デフォルトではオフ) の場合、ホスト名は LDAP 証明書の検証に使用されます。
- LDAP ログイン名属性。ログイン名の抽出に使用されるデフォルトの属性は「SAMAccountName」です。
- その他のオプションの LDAP 設定。



### Active Directory (LDAP) Settings for SSO Office 365

LDAP Settings for SSO Office 365

LDAP (Active Directory) Base\*  
 ?

LDAP (Active Directory) Bind DN\*  
 ?

LDAP (Active Directory) Bind DN Password\*  
 ?

LDAP Server (Active Directory) IP  
 ?

LDAP Server FQDN name  
 ?

LDAP Server (Active Directory) Port

LDAP Host name  
 ?

Active Directory LDAP  
 Validate LDAP Certificate

LDAP (Active Directory) Login username

9. **SAML IdP** 証明書 セクションでは、SAML アサーションに使用される SSL 証明書の詳細を指定できます。

- 証明書名。SSL 証明書の名前を入力します。
- 証明書ファイル。ローカルシステム上のディレクトリから SSL 証明書ファイルを選択します。
- 証明書キー形式。ドロップダウンリストボックスから、証明書と秘密キー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 と .der ファイル拡張子です。
- 証明書キー名。証明書の秘密鍵の名前を入力します。

- 証明書キーファイル。ローカルシステムから証明書の秘密キーを含むファイルを選択します。
- 秘密鍵のパスワード。プライベートキーファイルを保護するパスワードを入力します。

[ 証明書の詳細設定] チェックボックスをオン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入力したり、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ができます。

**SAML IdP Certificate**

SSL Certificate used by NetScaler to sign issued SAML assertions

Certificate Name\*  
 ?

Certificate File\*  
 test\_ssl\_saml\_cert.pem ?

CertKey Format\*

Certificate Key Name  
 ?

Certificate Key File  
 test\_ssl\_saml\_cert\_key.pem ?

Private Key Password

Advanced Certificate Settings

10. 上記の **SAML IdP** 証明書で **NetScaler ADC** に **CA** パブリック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「SAML IdP CA 証明書」を選択できます。上記の [ \*\* 証明書の詳細設定] セクションで [CA 証明書です \*\*] を選択してください。
11. [ **SAML SP** 証明書] セクションで、Office 365 SSL パブリック証明書について次の詳細を入力します。この証明書は、NetScaler ADC インスタンスが受信した SAML 認証要求を検証するために使用されます。
  - 証明書名。SSL 証明書の名前を入力します。

- 証明書ファイル。ローカルシステム上のディレクトリから SSL 証明書ファイルを選択します。
- 証明書キー形式。ドロップダウンリストボックスから、証明書と秘密キー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 と .der ファイル拡張子です。
- [ 証明書の詳細設定 ] チェックボックスをオン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入力したり、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ができます。

SAML SP Certificate

Office365 SSL Public Certificate used by NetScaler to verify incoming SAML authentication requests

Certificate Name\*  
office365\_ssl\_saml\_sp\_test\_cert

Certificate File\*  
Choose File test\_ssl\_saml\_sp\_cert.pem

CertKey Format\*  
PEM

12. **SAML Idp** 設定セクションでは、手順 3 で作成した 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で、Citrix ADC インスタンスを SAML ID プロバイダーとして構成できます。

- **SAML** 発行者名。このフィールドには、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 Auth VIP>/saml/login`
- 名前識別子の表現。評価される NetScaler ADC 式を入力して、SAML アサーションで送信された SAML `NameIdentifier` を抽出します。例：`"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`
- 署名アルゴリズム:SAML リクエスト/レスポンスを検証/署名するアルゴリズムを選択します (デフォルトは「RSA-SHA256」)。
- ダイジェスト方式。SAML リクエスト/レスポンスのハッシュをダイジェストする方法を選択します (デフォルトは「SHA256」)。
- オーディエンスの名前。サービスプロバイダー (Microsoft Office 365) を表すエンティティ名または URL を入力します。
- **SAML** サービスプロバイダー (**SP**) ID。(オプション) NetScaler ADC 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。
- アサーションコンシューマサービス **URL**。ユーザー認証が成功した後、NetScaler ADC 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サービス URL は、ID プロバイダサーバサイトまたはサービスプロバイダサイトで開始できます。
- このセクションには、他にも入力できるオプションフィールドがあります。たとえば、次のオプションを設定できます。
  - **SAML** 属性名。SAML アサーションで送信されるユーザー属性の名前。

- **SAML** 属性のわかりやすい名前。SAML アサーションで送信されるユーザー属性のわかりやすい名前。
- **SAML** 属性の **PI** 式。デフォルトでは、次の NetScaler ADC 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 (メール) から送信される最初のユーザー属性を SAML 認証属性として指定します。
- ユーザー属性の形式を選択します。

これらの値は、発行された SAML アサーションに含まれています。

ヒント

Citrix では、これらの設定は Microsoft Office 365 アプリで動作することがテストされているため、デフォルト設定のままにしておくことをお勧めします。

Saml issuer name

Name Identifier Expression  
 ?

Signature Algorithm  
 ?

Digest Method

Audience name or url

Option to Reject unsigned SAML Requests

SAML Attribute Name

SAML Attribute Friendly Name

PI Expression for SAML Attribute

SAML Attribute Format  
 ?

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 ADC 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 ADC インスタンスに構成を展開します。

**Target Instances**

10.102.58.78 > + ?

Create Close Dry Run

#### ヒント

実際の構成を実行する前に、[Dry Run] を選択して、StyleBook によってターゲットの NetScaler ADC インスタンスに作成された構成オブジェクトを表示することをお勧めします。

## StyleBook のための Microsoft Skype for Business

February 6, 2024

Skype for Business 2015 アプリケーションは、いくつかの外部構成要素に依存して機能します。Skype for Business ネットワークは、サーバーとそれらのオペレーティングシステム、データベース、認証システムと承認システム、ネットワーキングシステムとインフラストラクチャ、および電話の PBX (Private Branch Exchange: 構内交換機) 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 は、標準版とエンタープライズ版の 2 つのバージョンで利用可能です。主な違いは、Enterprise Edition のみに高可用性機能のサポートが含まれている点です。高可用性を実装するには、複数のフロントエンドサーバーをプールに展開し、SQL サーバーをミラーリングする必要があります。

Enterprise Edition の展開では、異なる役割がある複数のサーバーを作成できます。

### 主要コンポーネント

Skype for Business 2015 アプリケーションの主な構成要素を次に示します。

- フロントエンドサーバー
- エッジサーバー
- Director サーバー
- データベース (SQL) サーバー

### フロントエンドサーバー

Skype for Business アプリケーションでは、フロントエンドサーバーは、ネットワーク内の中核的なサーバーです。これは、ユーザー認証、登録、プレゼンス、アドレス帳、音声またはビデオ（Audio/Video: 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、および 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 を展開している場合、トポロジは、一般的には、1 つのフロントエンドプールに負荷分散される 2 台以上のフロントエンドサーバーと、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 1 つのデータベースサーバーで構成されています。

### エッジサーバー

組織の内部ネットワークにログインしていない外部ユーザーが内部ユーザーと対話できるようにする必要がある場合は、Skype for Business 用のエッジサーバーを導入する必要があります。これらの外部ユーザーとしては、認証されている匿名のリモートユーザー、連携パートナー、またはその他のモバイルクライアントが考えられます。

Skype For Business エッジサーバーにおける役割には、次の 4 種類があります。

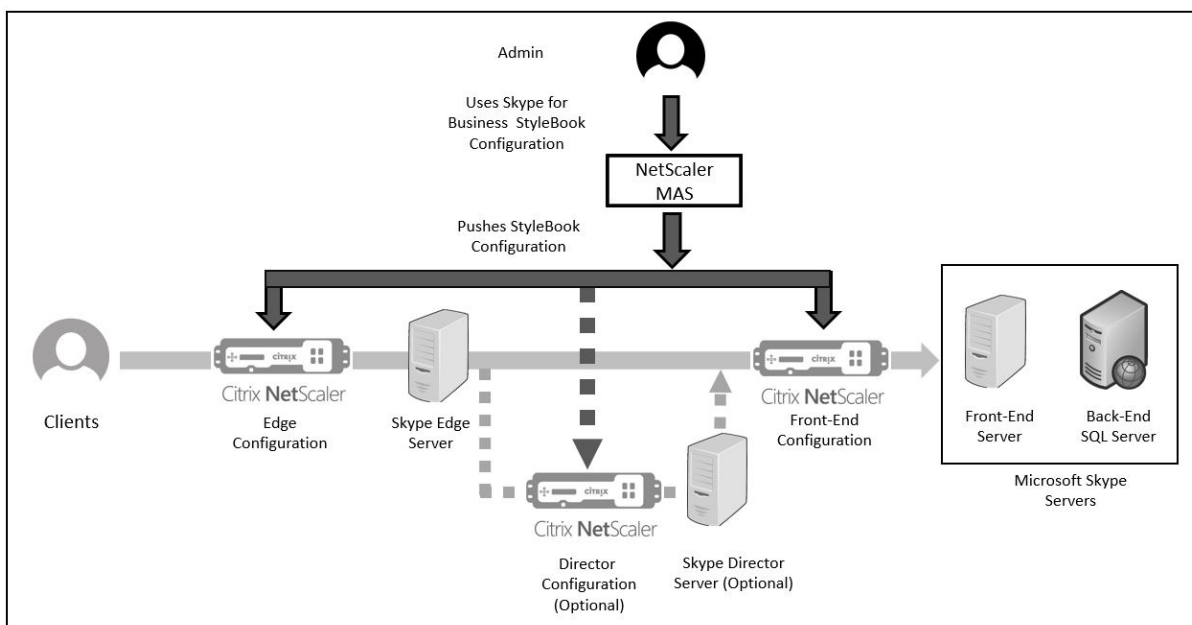
- Access Edge は、SIP トラフィックを処理し、外部接続を認証し、リモート接続を許可し、フェデレーション接続を許可します。
- Web Conferencing。これは、データ会議パケットを処理し、外部ユーザーに Skype for Business へのアクセスを許可します。
- A/V Conferencing。これは、A/V 会議パケットを処理し、音声とビデオ、アプリ共有、およびファイル転送の機能を外部ユーザーにも使用できるようにします。
- XMPP Proxy。これは、XMPP パケットを処理し、XMPP ベースのサーバーまたはクライアントに Skype for Business への接続を許可します。

### Director サーバー

Skype for Business 2015 における Director サーバーの主要機能は、エンドポイントを認証し、ユーザーを各自のアカウントが含まれているプールに「案内する」ことです。Skype for Business 2015 では、ディレクターはスタンダードアロンサーバー上で完全に専用の特定の役割ですが、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より簡単になることで、セキュリティが促進されます。

ディレクターは、複数のプールが存在する場合に最も役立ちます。これは、ディレクターがエンドポイントの認証を一元化できるためです。また、リモートユーザーについては、Director はエッジプールとフロントエンドプールとの間の追加のホップの役割を果たし、それによって攻撃に対する保護が強化されます。

次の図は、ネットワーク内の Skype サーバーの展開を示しています。



### エンタープライズでの NetScaler ADC 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 アドレスの一覧です。

| Skype for Business Servers | 仮想 IP アドレス            | サーバー IP アドレス                  | NetScaler ADC インスタンス |
|----------------------------|-----------------------|-------------------------------|----------------------|
| エッジサーバー                    | 外部 VIP - 192.20.20.20 | 192.20.20.21;<br>192.20.20.22 | 10.102.29.141        |
|                            | 内部 VIP - 10.10.10.20  | 10.10.10.21;<br>10.10.10.22   |                      |
| フロントエンドサーバー                | 10.10.10.10           | 10.10.10.11;<br>10.10.10.12   | 10.102.29.60         |
| Director サーバー              | 10.10.10.30           | 10.10.10.31;<br>10.10.10.32   | 10.102.29.93         |

フロントエンドサーバーを設定するには

1. NetScaler Application Delivery Management (ADM) で、[アプリケーション] > [構成] の順に選択し、[新規作成] をクリックします。「**StyleBook** の選択」ページには、NetScaler ADM で使用できるすべての StyleBook が表示されます。下にスクロールして、**Microsoft Skype for Business 2015 StyleBook** を選択します。StyleBook がユーザーインターフェイスページとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。



2. エッジサーバーセクションに、ネットワーク内のすべてのエッジサーバーの次の仮想 IP (VIP) アドレスと IP アドレスを入力します。
  - a) Access Edge、web conferencing Edge、および A/V Edge のために使用される、エッジサーバーの外部 VIP アドレスと IP アドレス。
  - b) 内部ネットワークに接続されるエッジサーバーの内部 VIP アドレスと IP アドレス。
  - c) ネットワーク内の 2 台の外部エッジサーバーと 2 台の内部エッジサーバー。
3. [フロントエンドサーバー] セクションで、Skype for Business フロントエンドサーバー用に作成する仮想フロントエンドサーバー (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 フロントエンドサーバーの IP アドレスも入力します。
4. [ディレクターサーバー] セクションで、Skype for Business アプリケーション用に作成される Director サーバーの仮想 IP アドレス (VIP) を入力します。また、ネットワーク内のすべての Skype for Business Director サーバーの IP アドレスを入力します。高可用性のためには、少なくとも 2 台の Director サーバーを作成します。
5. 詳細設定セクションには、3 つの Skype サーバーの NetScaler ADC 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表示されます。

次の表は、すべてのデフォルトポートとプロトコルのリストです。

| ラベル                        | ポート  | プロトコル | 説明                                                                                                    |
|----------------------------|------|-------|-------------------------------------------------------------------------------------------------------|
| HTTP Port                  | 80   | HTTP  | HTTPS が使用されないときに、フロントエンドサーバーから Web ファームの完全修飾ドメイン名 (Fully Qualified Domain Name: FQDN) への通信のために使用されます。 |
| HTTPS ポート                  | 443  | HTTPS | フロントエンドサーバーから Web ファームの FQDN への通信のために使用されます。                                                          |
| AutoDiscover Internal Port | 4443 | HTTPS | AutoDiscover サインインのための HTTPS 通信 (リバースプロキシから) と HTTPS フロントエンドプール内通信です。                                 |

| ラベル                        | ポート  | プロトコル                                              | 説明                                                                      |
|----------------------------|------|----------------------------------------------------|-------------------------------------------------------------------------|
| RPC Port                   | 135  | DCOM およびリモートプロシージャコール (Remote Procedure Call: 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、DCOM ベースの操作のために使用されます。                |
| SIP Port                   | 5061 | TCP (TLS)                                          | すべての内部 SIP 通信のためにフロントエンドサーバーによって使用されます。                                 |
| SIP Focus Port             | 444  | HTTPS、TCP                                          | Focus (Skype 会議状態を管理するコンポーネント) と個々のサーバーとの間の HTTPS 通信のために使用されます。         |
| SIP Group Port             | 5071 | TCP                                                | 応答グループアプリケーションの受信 SIP 要求のために使用されます。                                     |
| SIP AppSharing Port        | 5065 | TCP                                                | アプリケーション共有の受信 SIP リスニング要求のために使用されます。                                    |
| SIP Attendant Port         | 5072 | TCP                                                | 出席者の受信 SIP 要求のために使用されます (つまり、ダイヤルイン会議用)。                                |
| SIP Conf Announcement Port | 5073 | TCP                                                | Skype for Business サーバーの会議お知らせサービスの受信 SIP 要求のために使用されます (つまり、ダイヤルイン会議用)。 |
| SIP CallPark Port          | 5075 | TCP                                                | CallPark アプリケーションの受信 SIP 要求のために使用されます。                                  |
| SIP Call Admission Port    | 448  | TCP                                                | Skype for Business サーバーの帯域幅ポリシーサービスによる通話受付管理のために使用されます。                 |

| ラベル                                | ポート  | プロトコル | 説明                                                                                                                                      |
|------------------------------------|------|-------|-----------------------------------------------------------------------------------------------------------------------------------------|
| SIP Call Admission<br>TURN Port    | 5080 | TCP   | 音声/ビデオエッジ TURN<br>トラフィックの帯域幅ポリ<br>シーサービスによる通話受<br>付管理のために使用されま<br>す。                                                                    |
| SIP Audio Test Port                | 5076 | TCP   | 音声テストサービスの受信<br>SIP 要求のために使用され<br>ます。                                                                                                   |
| HTTPS External Port                | 443  | HTTPS | 内部 Web 会議へのリモー<br>トユーザーアクセスのため<br>の SIP/TLS 通信用、およ<br>び内部メディアおよび A/V<br>セッションにアクセスする<br>ための STUN/TCP 送受信<br>メディア通信用の外部ポー<br>トとして使用されます。 |
| HTTPS Internal Port                | 443  | HTTPS | 内部 Web 会議へのリモー<br>トユーザーアクセスのため<br>の SIP/TLS 通信用、およ<br>び内部メディアおよび A/V<br>セッションにアクセスする<br>ための STUN/TCP 送受信<br>メディア通信用の内部ポー<br>トとして使用されます。 |
| SIP External Remote<br>Access Port | 5061 | TCP   | リモートユーザーアクセス<br>またはフェデレーションの<br>ための SIP/MTLS 通信用<br>の外部ポートとして使用さ<br>れます。                                                                |
| SIP Internal Remote<br>Access Port | 5061 | TCP   | リモートユーザーアクセス<br>またはフェデレーションの<br>ための SIP/MTLS 通信用<br>の内部ポートとして使用さ<br>れます。                                                                |
| SIP External STUN UDP<br>Port      | 3478 | UDP   | STUN/UDP 送受信メディ<br>ア通信のための外部ポー<br>トとして使用されます。                                                                                           |

| ラベル                        | ポート  | プロトコル | 説明                                                                           |
|----------------------------|------|-------|------------------------------------------------------------------------------|
| SIP Internal STUN UDP Port | 3478 | UDP   | STUN/UDP 送受信メディア通信のための内部ポートとして使用されます。                                        |
| SIP Internal IM Port       | 5062 |       | 内部ファイアウォールを通過して送信方向に流れる IM 通信の SIP/MTLS 認証のための内部ポートとして使用されます。                |
| HTTP Port                  | 80   | TCP   | Director から Web ファームの FQDN への初期通信のために使用されます。                                 |
| HTTPS ポート                  | 443  | HTTPS | Director から Web ファームの FQDN への通信のために使用されます。                                   |
| AutoDiscover Internal Port | 4443 | HTTPS | AutoDiscover サインインのために HTTPS 通信 (リバースプロキシから) と HTTPS Director プール内通信に使用されます。 |
| SIP Internal Port          | 5061 | TCP   | サーバー間の通信とクライアント接続のために使用されます。                                                 |

6. 「ターゲットインスタンス」セクションで、3 つの Skype for Business サーバーをデプロイする 3 つの異なる Citrix ADC 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、Citrix ADM で最近検出された Citrix ADC 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。

7. 「作成」をクリックして、選択した Citrix ADC インスタンスで構成を作成します。

#### ヒント

インスタンスで実際の構成を実行する前に、**[Dry Run]** を選択して、ターゲットインスタンスに作成する必要がある構成オブジェクトを確認することをお勧めします。

構成が正常に作成されると、StyleBook により、25 台の負荷分散仮想サーバーが作成されます。つまり、ポートごとに、1 台の負荷分散仮想サーバーが 1 つのサービスグループとともに定義されます。そのサービスグループは、その負荷分散仮想サーバーにバインドされています。また、その構成では、フロントエンドサーバーが

サービスグループのメンバーとして追加され、それらがそのサービスグループにバインドされます。作成されたサービスグループメンバーの数は、作成されたフロントエンドサーバーの数と等しくなります。

次の図は、各サーバーで作成されるオブジェクトを示しています。

| Objects Added on Instance : 10.102.29.93   Roles : frontend   Count : 72                                                                                                                                                                                                                                                                                                                                                                    | Objects Added on Instance : 10.102.29.140   Roles : director   Count : 22                                                                                                                                                                                                                                                                                                                                                                    | Objects Added on Instance : 10.102.29.60   Roles : edge   Count : 35                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Type : lbserver</b><br/>                     appflowlog : ENABLED<br/>                     downstateflush : ENABLED<br/>                     ipv46 : 10.10.10.10<br/>                     lbmethod : LEASTCONNECTION<br/>                     name : microsoft-skype-application-sfb-fe-http-lb<br/>                     persistencetype : SOURCEIP<br/>                     port : 80<br/>                     servicetype : TCP</p> | <p><b>Type : lbserver</b><br/>                     appflowlog : ENABLED<br/>                     downstateflush : ENABLED<br/>                     ipv46 : 10.10.10.30<br/>                     lbmethod : LEASTCONNECTION<br/>                     name : microsoft-skype-application-sfb-dir-http-lb<br/>                     persistencetype : SOURCEIP<br/>                     port : 80<br/>                     servicetype : TCP</p> | <p><b>Type : lbserver</b><br/>                     ipv46 : 192.20.20.20<br/>                     name : microsoft-skype-application-sfb-edge-externalsip-lb<br/>                     port : 443<br/>                     servicetype : TCP</p> |
| <p><b>Type : servicegroup</b><br/>                     servicegroupname : microsoft-skype-application-sfb-fe-http-svcgrp<br/>                     servicetype : TCP</p>                                                                                                                                                                                                                                                                     | <p><b>Type : servicegroup</b><br/>                     servicegroupname : microsoft-skype-application-sfb-dir-http-svcgrp<br/>                     servicetype : TCP</p>                                                                                                                                                                                                                                                                     | <p><b>Type : servicegroup</b><br/>                     servicegroupname : microsoft-skype-application-sfb-edge-externalsip-svcgrp<br/>                     servicetype : TCP</p>                                                               |
| <p><b>Type : lbserver_servicegroup_binding</b><br/>                     name : microsoft-skype-application-sfb-fe-http-lb<br/>                     servicegroupname : microsoft-skype-application-sfb-fe-http-svcgrp</p>                                                                                                                                                                                                                    | <p><b>Type : lbserver_servicegroup_binding</b><br/>                     name : microsoft-skype-application-sfb-dir-http-lb<br/>                     servicegroupname : microsoft-skype-application-sfb-dir-http-svcgrp</p>                                                                                                                                                                                                                   | <p><b>Type : lbserver_servicegroup_binding</b><br/>                     name : microsoft-skype-application-sfb-edge-externalsip-lb<br/>                     servicegroupname : microsoft-skype-application-sfb-edge-externalsip-svcgrp</p>     |
| <p><b>Type : server</b><br/>                     ipaddress : 10.10.10.11<br/>                     name : 10.10.10.11</p>                                                                                                                                                                                                                                                                                                                    | <p><b>Type : server</b><br/>                     ipaddress : 10.10.10.31<br/>                     name : 10.10.10.31</p>                                                                                                                                                                                                                                                                                                                     | <p><b>Type : server</b><br/>                     ipaddress : 192.20.20.21<br/>                     name : 192.20.20.21</p>                                                                                                                     |
|                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                              | <p><b>Type : server</b><br/>                     ipaddress : 192.20.20.22</p>                                                                                                                                                                  |

## Microsoft Exchange StyleBook

February 6, 2024

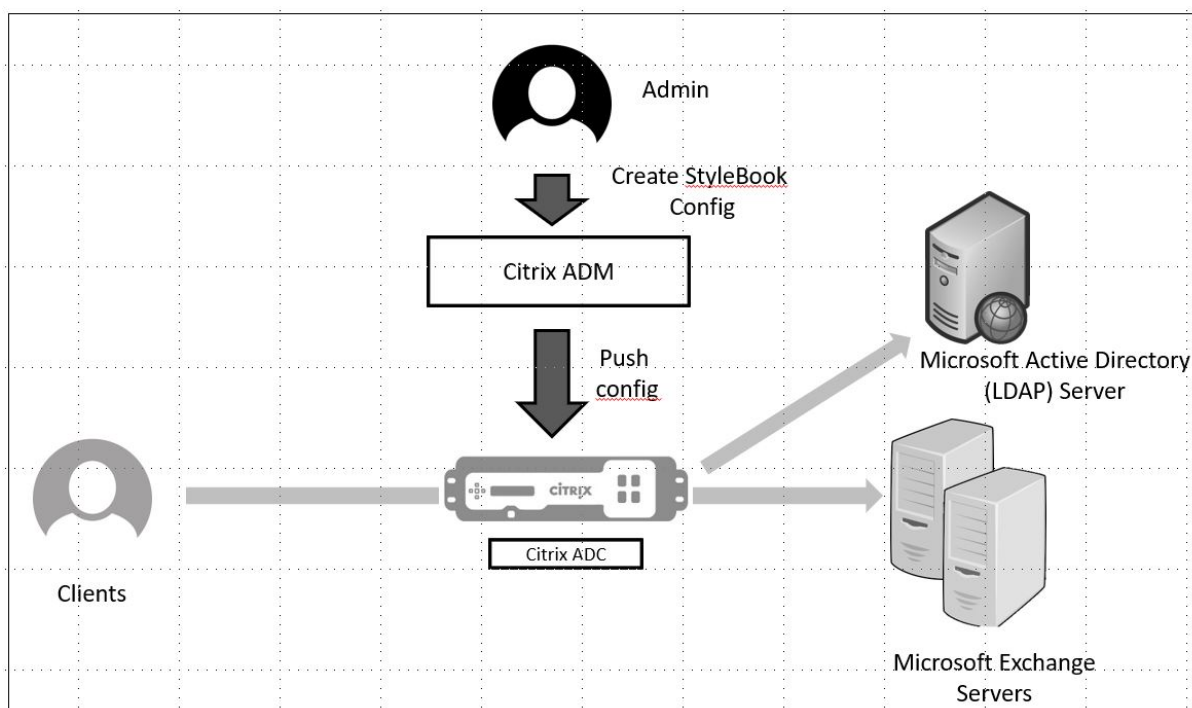
Microsoft Exchange 2016 StyleBook を使用して、ネットワーク内の Microsoft Exchange 2016 エンタープライズアプリケーションを最適化して保護する NetScaler ADC 構成を展開できます。Microsoft Exchange 2016 は、従業員やその他の利害関係者にメール、個人情報管理、およびメッセージングのサービスを提供するための主要なエンタープライズアプリケーションです。

### Microsoft ExchangeStyleBook を使用して構成された NetScaler ADC 機能

Microsoft Exchange 2016 StyleBook は、Microsoft Exchange 2016 サーバー向けに以下の Citrix ADC 機能を有効化および構成します。

- 負荷分散 - 複数の Exchange サーバーを負荷分散できる、基本的な負荷分散です。
- コンテンツスイッチ - シングル IP アクセス、および正しい負荷分散仮想サーバーへのクエリのリダイレクトができるようになるコンテンツスイッチです。
- 書き換え - ユーザーを安全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 ADC にオフロードするため、Exchange サーバーの負荷が軽減されます

次の図は、ネットワーク内の Exchange サーバーの展開を示しています。



### 前提条件

- 証明書ベースの認証の場合は、ネットワーク設定に含まれているアドレス可能なすべてのホストに、IP アドレスのみでなく解決できるドメイン名が必要となります。
- 必ず Microsoft Exchange 2016 サーバーの SIP ポートにアクセスできるようにしてください。

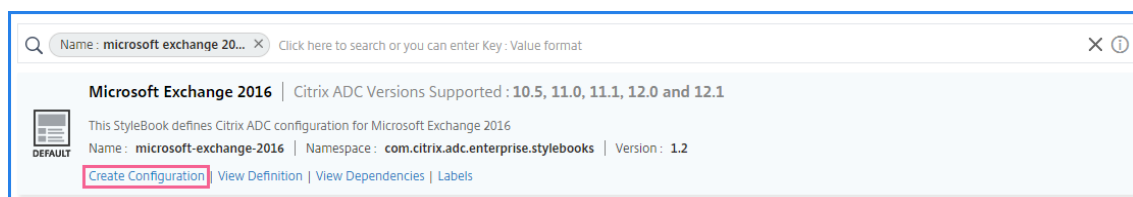
### Microsoft Exchange StyleBook の設定

企業内の Microsoft Exchange StyleBook を構成して、NetScaler ADC 構成を展開します。

#### Microsoft Exchange アプリケーションを設定するには

1. NetScaler ADM で、[アプリケーション] > [StyleBook] に移動します。
2. **Microsoft Exchange 2016 StyleBook** を検索し、「構成の作成」をクリックします。

StyleBook がユーザーインターフェイスフォームとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。



3. 以下のパラメーターに対して詳細を入力します。

- **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
- **Exchange VIP** - Microsoft Exchange アプリケーションに対するクライアントリクエストを受信する Citrix ADC 上の仮想 IP アドレス
- **Exchange Server IP**: ネットワーク内のすべての Exchange サーバの IP アドレス。

IP アドレスをさらに追加する場合は、プラス (+) アイコンをクリックします。通常は、ネットワーク内で 2 つの Exchange サーバが構成されます。

4. 「交換証明書」セクションで、交換証明書を NetScaler ADM にアップロードします。証明書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キーパスワードも指定できます。

注:

証明書ファイルが「.pem」または「.der」形式であることを確認してください。NetScaler ADM は、他の形式のファイルを拒否します。

証明書の有効期限の詳細や詳細設定を指定する場合は、「証明書の詳細設定」を選択します。

5. **Exchange Active Directory** 認証の構成 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** 認証 **VIP** -Citrix ADC アプライアンス上で AD (LDAP) 仮想サーバ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** サーバ **IP**-Active Directory ドメインコントローラーの IP アドレスです。
- **Active Directory** ベースストリング-Active Directory の LDAP ベースストリング。たとえば、CN=Users,DC=CTXNSSFB,DC=COM などです。
- **Active Directory** **LDAP** バインド識別名 (**DN**)-LDAP バインド識別名 (DN) を使用して、このオブジェクトを LDAP サーバ (AD) にバインドします。たとえば、「cn=Administrator,cn=Users,dc=acme,dc=com」などです。
- **Active Directory** **LDAP** バインド識別名 (**DN**) パスワード -LDAP バインド識別名 (DN) は AD 認証のパスワードです
- **Active Directory** ユーザー名属性 -ユーザー名の AD 属性。Citrix ADC は、LDAP 属性を使用して外部の Active Directory サーバにクエリを実行します。たとえば、「sAMAccountName」などです。
- **Active Directory** グループ属性名-LDAP サーバ上で設定されている LDAP グループ属性名。たとえば、LDAP のグループ属性には「memberOf」と入力します。
- **Active Directory** サブ属性名-LDAP サーバで構成された LDAP サブ属性名。たとえば、LDAP のサブ属性は「cn」です。
- **Active Directory** 認証ドメイン -認証に使用される AD/LDAP ドメイン名。たとえば、ctxnssf.com などです。

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 Citrix ADC インスタンスを選択します。

注

最近検出された NetScaler ADC インスタンスを表示する場合は、更新アイコンをクリックします。

7. 「作成」をクリックして構成ファイルを作成し、選択した Citrix ADC インスタンスで構成を実行します。

Citrix では、インスタンスで実際の構成を実行する前に、まず **Dry Run** を選択してターゲットインスタンスに作成された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 はコンテンツスイッチング仮想サーバー、5 つの負荷分散仮想サーバー、1 つの LDAP 認証仮想サーバーにバインドされた 1 つの LDAP ポリシーを作成します。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 StyleBook

February 6, 2024

Microsoft SharePoint 2016 は、主にドキュメント管理機能と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す。高度に構成可能であり、すべての主要 Web ブラウザーでサポートされています。

Microsoft SharePoint 2016 StyleBook を使用して、ネットワーク内の Microsoft SharePoint 2016 エンタープライズアプリケーションを最適化して保護する NetScaler ADC 構成を展開できます。

### 前提条件

- Microsoft SharePoint 2016
- NetScaler ADM、バージョン 12.0 以降
- NetScaler ADC、バージョン 10.5 以降

### Microsoft の SharePoint 2016 StyleBook によって構成された NetScaler ADC の機能

Microsoft SharePoint 2016 StyleBook を使用して、Microsoft SharePoint 2016 の次の NetScaler ADC 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
- レスポンダー
- 書き換え



- 圧縮
- 統合キャッシング

### 負荷分散

Citrix ADC 負荷分散は、要求をバックエンド SharePoint サーバーに均等に分散します。バックエンドサーバーをインテリジェントに監視することで、正常に動作していないサーバーに要求が送信されないようにします。

SharePoint 用 StyleBook では、12 台の負荷分散仮想サーバーが構成され、各仮想サーバーは、ドキュメント、画像、オーディオ、ビデオ、およびその他のファイルタイプなど、特定の種類のコンテンツの負荷分散要求専用となります。

SharePoint StyleBook は、SSL ベースの LB 仮想サーバーを構成することにより、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。SSL がフロントエンドプロトコルとして選択されていることを確認します。仮想ポートは、デフォルトで 443 に設定されています。SSL を選択して、サービスグループ (SharePoint アプリケーションサーバー) をターゲットの負荷分散仮想サーバーにバインドすることもできます。バックエンドプロトコルはデフォルトで HTTP に設定されていることに注意してください。

### コンテンツの切り替え

コンテンツスイッチ機能は、要求された特定種類の SharePoint コンテンツ (たとえば、ドキュメント、画像、およびオーディオまたはビデオファイル) に基づいて複数の負荷分散仮想サーバーにわたりクライアント要求を分散するために使用されます。コンテンツスイッチモジュールにより、受信トラフィックが、その種類のコンテンツを処理できる最適な負荷分散仮想サーバーに送られます。それにより、さまざまな最適化ポリシーをさまざまな種類のトラフィックに適用できます。たとえば、テキストドキュメントよりもさまざまな圧縮ポリシーやキャッシュポリシーをビデオに使用できます。

### レスポonder

NetScaler ADC インスタンスのレスポonder機能を使用して、ユーザーを HTTP から HTTPS にシームレスにリダイレクトできます。レスポonder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onderポリシーは、アクションを実行する必要がある要求 (トラフィック) を決定し、各ポリシーを負荷分散仮想サーバーにバインドします。SharePoint 用 StyleBook には、ユーザーを HTTP の URL から HTTPS の URL にリダイレクトする構成が含まれています。

### 書き換え

書き換えモジュールは、要求/応答のヘッダー、URL、またはコンテンツを即座に変更するために使用されます。このモジュールは、トラフィック処理でインラインで動作します。それにより、特定のユースケースに応じてトラフィック

クフローを変更できます。たとえば、書き換えにより、Web サイトのサーバーについて不要な情報が公開されることなく、要求されたコンテンツにアクセスできるようになります。

SharePoint 用 StyleBook では、書き換え機能は、ユーザーの要求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

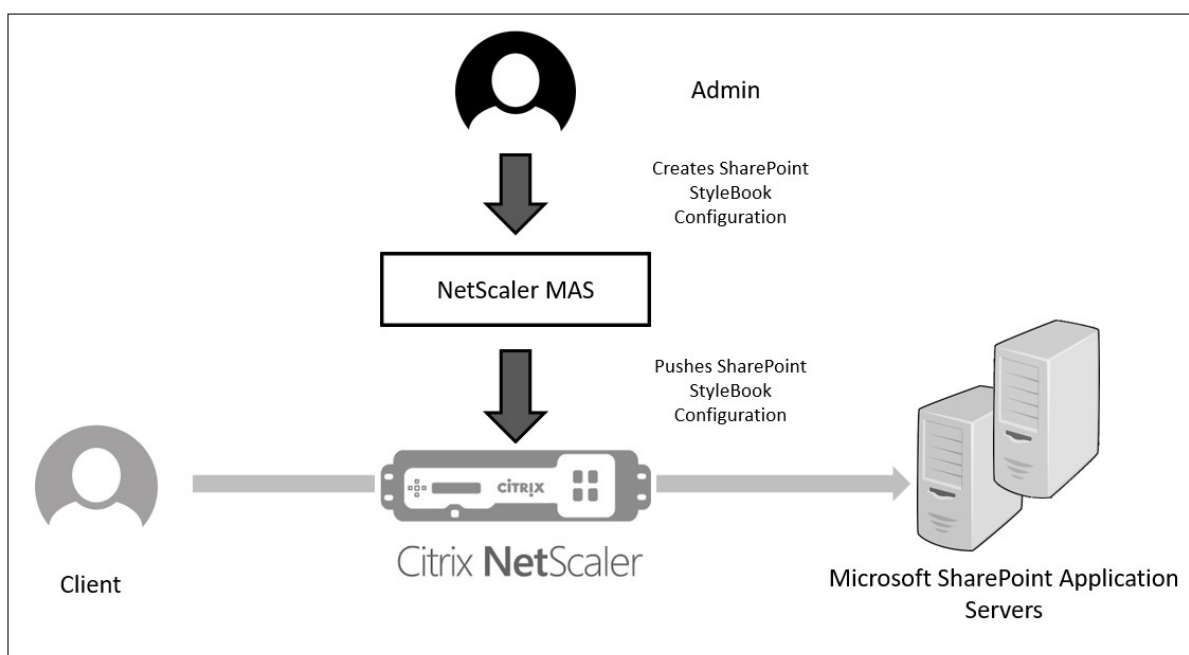
NetScaler ADC 圧縮エンジンは、圧縮可能なコンテンツを識別して圧縮します。このプロセスにより、データ転送時間が短縮され、クライアントに対するネットワーク帯域幅要件が減少するとともに、SharePoint コンテンツサーバー上の CPU サイクルが節約されます。NetScaler ADC インスタンスは、静的に生成されたデータと動的に生成されたデータの両方を圧縮できます。GZIP または DEFLATE 圧縮アルゴリズムが適用されることで、無関係で反復的な情報がサーバー応答から削除され、より簡潔で効率的な形式で元の情報が表されます。クライアントのブラウザのデータ展開機能は、サポートされているアルゴリズム (GZIP、DEFLATE、またはこれら両方) によって異なります。

NetScaler ADC 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。トラフィック圧縮の主な利点には、帯域幅コストの減少、WAN (Wide Area Network: ワイドエリアネットワーク) の遅延の減少、サーバーパフォーマンスの向上があります。

### 統合キャッシング

NetScaler ADC のインメモリキャッシュには、頻繁に要求されるコンテンツをユーザーに迅速に配信するために、SharePoint オブジェクトを保存できます。キャッシュされるコンテンツには、ダウンロードしたドキュメントや、オーディオ、ビデオ、および画像ファイルなどがあります。

次の図は、NetScaler ADM を使用して SharePointStyleBook 構成を展開する NetScaler ADC インスタンスによるネットワークフロントエンドでの SharePoint サーバーの展開を示しています。



## SharePoint StyleBook の構成を展開する

次の作業は、ビジネスネットワークで Microsoft SharePoint 2016 StyleBook を展開する場合に役立ちます。

**Microsoft SharePoint 2016 StyleBook** をデプロイするには:

1. NetScaler ADM で、[アプリケーション] > [管理] > [構成] の順に選択し、[新規作成] をクリックします。  
「**StyleBook** の選択」ページには、NetScaler ADM で使用できるすべての StyleBook が表示されます。
2. 下にスクロールして [ **Microsoft SharePoint 2016 StyleBook** ] を選択します。

注:

NetScaler ADM で、「アプリケーション」>「構成」>「**StyleBooks**」に移動します。下にスクロールして Microsoft SharePoint 2016 StyleBook を探し、「構成を作成」をクリックします。

StyleBook は、この StyleBook で定義されているすべてのパラメータの値を入力できるユーザーインターフェイスフォームとして開きます。

次のパラメーターの値を入力します:

- a) **SharePoint** アプリケーション名。ネットワーク内で展開する SharePoint 構成の名前です。
- b) **SharePoint** 仮想 IP。NetScaler ADC 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際に使用する 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。使用可能なオプションは、HTTP または SSL です。

注:

SSL を選択する場合は、この StyleBook の「SharePoint 詳細設定」セクションで「リライト構成」パラメータが有効になっていることを確認してください。

- e) **SharePoint** サーバー IP ネットワーク内のすべての SharePoint サーバーの IP アドレス。
- f) **SharePoint** サーバーポート。SharePoint サーバーで使用される TCP ポート番号です。デフォルト値は、80 です。必要な場合はこの値を編集できますが、必ず Microsoft SharePoint 2016 サーバー上でこのポートにアクセスできることを確認してください。

SharePoint Application Name\*

 ?

SharePoint Virtual VIP\*

 ?

Sharepoint Virtual Port

Sharepoint frontend Protocol

 ▾

Sharepoint Servers IPs\*

 ×
 × + ?

Sharepoint Servers Port

3. [ **SSL** 証明書の設定 ] セクションで、[+] をクリックして SSL 証明書の名前と証明書キーを入力し、ローカルストレージフォルダからそれぞれのファイルを選択します。

Certificate Name\*  
 ?

Certificate File\*  
 test\_cert.pem ?

CertKey Format\*  
 ▾

Certificate Key Name  
 ?

Certificate Key File  
 test\_cert\_key.pem ?

Private Key Password

**Advanced Certificate Settings**

4. 必要に応じて、[ 証明書の詳細設定 ] をクリックして、SSL 証明書の有効期限の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近づくこの数日後に NetScaler ADM がアラームを発行するように日数を設定します。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。

**Advanced Certificate Settings**

Advanced certificate settings

Certificate Expiry Monitor  
 ▾ ?

Certificate Expiry Notification Period  
 ?

Is a CA Certificate

Skip CA Name

OCSP Check  
 ▾ ?

SNI Certificate

5. [SharePoint の詳細設定] セクションでは、NetScaler ADC インスタンスで構成する NetScaler ADC 機能を有効にできます。負荷分散機能とコンテンツスイッチ機能はインスタンス上でデフォルトで構成されますが、その他の機能（つまり、インスタンス上で構成する必要がある、レスポンス構成、書き換え構成、圧縮構成、および統合キャッシュ構成）を選択できます。
6. 「ターゲットインスタンス」をクリックし、この SharePoint 構成を展開する NetScaler ADC 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 ADC 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、Citrix ADM で最近検出された Citrix ADC 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。

**Sharepoint Advanced Settings**

Options to selectively enable configurations of features for Sharepoint

- Enable Responder Configuration
- Enable Rewrite Configuration
- Enable Compression Configuration
- Enable Caching Configuration

**Target Instances**

Click to select

>

+

Create

Close

Dry Run

注:

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、ターゲットインスタンスに作成される構成オブジェクトを確認することをお勧めします。

構成が作成され、正常に展開されると、SharePoint 用 StyleBook により、1 台のコンテンツスイッチ仮想サーバーと 12 台の負荷分散仮想サーバーが作成されます。ポリシーとサービスグループも作成され、それらが負荷分散仮想サーバーにバインドされます。作成されるポリシーは、構成パックの作成中に StyleBook で選択した機能によって異なります。

## **NetScaler ADC** インスタンスに定義されているオブジェクトの表示

NetScaler ADM で構成パックを作成すると、SharePoint StyleBook の NetScaler ADC インスタンスで作成されたすべてのオブジェクトを表示できます。[アプリケーション] > [管理] > [構成] に移動し、[作成されたオブジェクトを表示] をクリックします。次の図は、作成されたオブジェクトの一部を示しています。この例では、「NetScaler ADM から SharePointStyleBook 構成を展開する」に示されている IP アドレスが指定されています。

|                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Type : lbvserver</b></p> <p>appflowlog : DISABLED<br/>backupperstencetimeout : 20<br/>downstateflush : DISABLED<br/>ipv46 : 0.0.0.0<br/>lbmethod : LEASTCONNECTION<br/>name : sharepoint application test frontpage services lb<br/>persistencebackup : SOURCEIP<br/>persistencetype : COOKIEINSERT<br/>port : 0<br/>servicetype : HTTP<br/>timeout : 20</p> |
| <p><b>Type : servicegroup</b></p> <p>cip : DISABLED<br/>cka : YES<br/>cmp : NO<br/>downstateflush : DISABLED<br/>healthmonitor : NO<br/>servicegroupname : sharepoint-application-test-frontpage-services-svcgrp<br/>servicetype : HTTP<br/>sp : ON<br/>state : ENABLED<br/>tcpb : NO<br/>useproxypport : NO<br/>usip : NO</p>                                     |
| <p><b>Type : lbvserver_servicegroup_binding</b></p> <p>name : sharepoint-application-test-frontpage-services-lb<br/>servicegroupname : sharepoint-application-test-frontpage-services-svcgrp</p>                                                                                                                                                                   |
| <p><b>Type : servicegroup_servicegroupmember_binding</b></p> <p>ip : 192.10.10.11<br/>port : 80<br/>servicegroupname : sharepoint-application-test-frontpage-services-svcgrp</p>                                                                                                                                                                                   |
| <p><b>Type : servicegroup_servicegroupmember_binding</b></p> <p>ip : 192.10.10.12<br/>port : 80<br/>servicegroupname : sharepoint-application-test-frontpage-services-svcgrp</p>                                                                                                                                                                                   |
| <p><b>Type : csaction</b></p> <p>name : sharepoint-application-test-cs-frontpage-services-csaction<br/>targetlbvserver : sharepoint-application-test-frontpage-services-lb</p>                                                                                                                                                                                     |
| <p><b>Type : cspolicy</b></p> <p>action : sharepoint-application-test-cs-frontpage-services-csaction<br/>policyname : sharepoint-application-test-cs-frontpage-services-cspol<br/>rule : HTTP.REQ.HEADER("X-Vermeer-Content-Type").EXISTS</p>                                                                                                                      |
| <p><b>Type : csvserver_cspolicy_binding</b></p> <p>name : sharepoint-application-test-cs<br/>policyname : sharepoint-application-test-cs-frontpage-services-cspol<br/>priority : 10</p>                                                                                                                                                                            |



## Microsoft ADFS proxy StyleBook

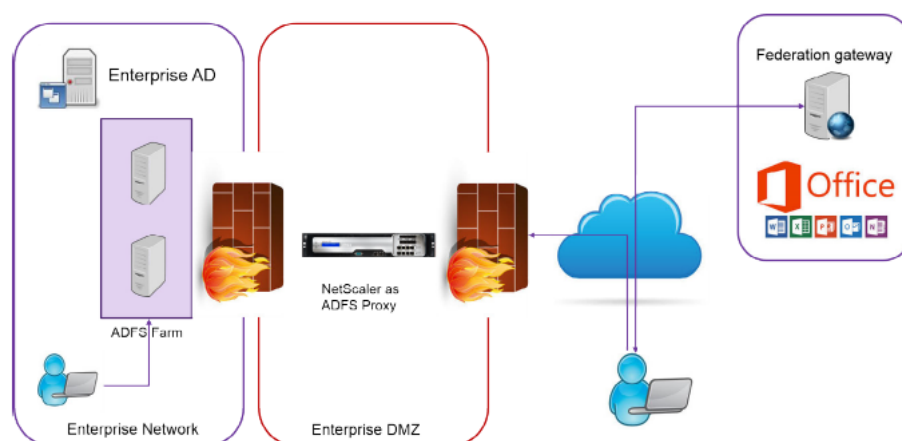
February 6, 2024

Microsoft™ ADFS プロキシは、内部のフェデレーション対応リソースとクラウドリソースの両方にシングルサインオンアクセスを提供することで重要な役割を果たします。クラウドリソースの一例が Office 365 です。ADFS プロキシサーバーの目的は、インターネットからアクセスできない ADFS サーバーに要求を受信および転送することです。ADFS プロキシはリバースプロキシで、通常は組織の境界ネットワーク (DMZ) にあります。ADFS プロキシは、リモートユーザーの接続とアプリケーションアクセスにおいて重要な役割を果たします。

NetScaler ADC には、フェデレーション ID の安全な接続、認証、および処理を可能にする正確なテクノロジーが搭載されています。NetScaler ADC を ADFS プロキシとして使用すると、DMZ に追加のコンポーネントを展開する必要がなくなります。

NetScaler Application Delivery Management (ADM) の Microsoft ADFS プロキシ StyleBook を使用すると、NetScaler ADC インスタンスで ADFS プロキシサーバーを構成できます。

次の図は、Citrix ADC インスタンスをエンタープライズ DMZ の ADFS プロキシサーバーとして展開しているところを示しています。



### ADFS プロキシとして NetScaler ADC を使用する利点

1. 負荷分散と ADFS プロキシの両方のニーズに対応
2. 内部ユーザーアクセスシナリオと外部ユーザーアクセスシナリオの両方をサポート
3. 事前認証のための豊富なメソッドをサポート
4. ユーザーにシングルサインオン環境を提供します
5. アクティブプロトコルとパッシブプロトコルの両方をサポート
  - a) アクティブなプロトコルアプリの例としては、Microsoft Outlook、Microsoft Skype for Business
  - b) パッシブプロトコルアプリの例としては、Microsoft Outlook Web アプリ、Web ブラウザー

6. DMZ ベースの展開のための強化されたデバイス
7. Citrix ADC ADC のコア機能を追加して付加価値を高める
  - a) コンテンツスイッチ
  - b) SSL オフロード
  - c) 書き換え
  - d) セキュリティ (NetScaler ADC AAA)

プロトコルベースのアクティブなシナリオでは、Office 365 に接続して認証情報を入力できます。Microsoft フェデレーションゲートウェイは、アクティブなプロトコルクライアントに代わって (ADFS プロキシを介して) ADFS サービスにアクセスします。次に、ゲートウェイは基本認証 (401) を使用して認証情報を送信します。NetScaler ADC は、ADFS サービスにアクセスする前にクライアント認証を処理します。認証後、ADFS サービスはフェデレーションゲートウェイに SAML トークンを渡します。次に、フェデレーションゲートウェイはトークンを Office 365 に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 制約付き委任 (KCD) ユーザーアカウントを作成します。KCD アカウントは、Kerberos SSO 認証で ADFS サーバーに接続するために必要です。StyleBook は LDAP ポリシーとセッションポリシーも生成します。これらのポリシーは、パッシブクライアントの認証を処理する NetScaler ADC AAA 仮想サーバーに後でバインドされます。

StyleBook は、NetScaler ADC 上の DNS サーバーが ADFS 用に構成されていることを確認することもできます。

以下の構成セクションでは、アクティブプロトコルベースと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 ADC を設定する方法について説明します。

#### 構成の詳細

以下の表は、この統合を正常にデプロイするために最低限必要なソフトウェアバージョンを示しています。

| Product    | 最低限必要なバージョン            |
|------------|------------------------|
| Citrix ADC | 11.0、アドバンスド/プレミアムライセンス |

次の手順は、適切な外部および内部 DNS エントリが既に作成されていることを前提としています。

#### NetScaler ADM からの Microsoft ADFS プロキシ StyleBook 構成の展開

以下の手順は、Microsoft ADFS プロキシ StyleBook をビジネスネットワークに実装する際に役立ちます。

**Microsoft ADFS** プロキシ **StyleBook** をデプロイするには

1. NetScaler ADM で、[アプリケーション] > [**StyleBook**] に移動します。**StyleBook** ページには、Citrix ADM で使用できるすべての StyleBook が表示されます。
2. 下にスクロールして **Microsoft ADFS** プロキシ **StyleBook** を見つけてください。[構成を作成] をクリックします。  
StyleBook がユーザーインターフェイスページとして開き、この StyleBook で定義されているすべてのパラメーターの値を入力できます。
3. 次のパラメータに値を入力します。
  - a) **ADFS** プロキシ展開名。ネットワークに導入されている 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 NetScaler ADC 上のパブリック仮想 IP アドレスを入力します。

ADFSProxy Deployment Name\*  
ns-adfs-dep01 ?

ADFS Servers FQDNs and/or IPs\*  
192.30.30.30 + ?

ADFSProxy Public VIP IP\*  
192 . 50 . 50 . 50 ?

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 ADC インスタンスで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からそれぞれのファイルを選択します。また、秘密キーのパスワードを入力して、暗号化された秘密キーを .pem 形式でロードすることもできます。

### ADFSProxy Certificates

ADFS certificates bound to the SSL VServers created by this StyleBook

#### Certificate File path

Certificate Name\*  
 ?

Certificate File\*  
 saml-idp.pem ?

CertKey Format\*  
 ▾

Certificate Key Name  
 ?

Certificate Key File  
 saml-idp.key ?

Private Key Password

Advanced Certificate Settings

CA Certificate File path

[ 証明書の詳細設定 ] チェックボックスをオン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入力したり、証明書有効期限モニターを有効または無効にしたりできます。

5. **SSL 証明書で NetScaler ADC に CA パブリック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 証明書] チェックボックスをオンにできます。[ 証明書の詳細設定 ] セクションで [ **CA 証明書** で ] 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およびパッシブクライアントの認証を有効にします。Active Directory でユーザー認証に使用されている 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のいずれか、あるいはその両方の認証を設定できます。

7. 次の詳細を入力して、アクティブなクライアントの認証を有効にします。

注:

アクティブクライアントのサポートの設定は任意です。

- a) **ADFS** プロキシアクティブ認証 **VIP** アクティブなクライアントが認証のためにリダイレクトされる NetScaler ADC インスタンス上の仮想認証サーバーの仮想 IP アドレスを入力します。
- b) サービスアカウントのユーザー名。NetScaler ADC が Active Directory へのユーザーを認証するために使用するサービスアカウントのユーザー名を入力します。
- c) サービスアカウントのパスワード。Active Directory に対するユーザーを認証するために NetScaler ADC が使用するパスワードを入力します。

Enable Authentication for ADFS Passive and/or Active clients

Turn on authentication for ADFSProxy for Active and Passive Clients

ADFSProxy Authentication Domain\*

 ?

Enable Active Clients Authentication

Parameters for configuring Active Client Authentication to ADFS (AD Negotiate + SSO to ADFS)

ADFSProxy Active Authentication VIP\*

 ?

Service Account Username\*

 ?

Service Account Password\*

 ?

Kerberos Delegate Username\*

 ?

Kerberos Delegate Password\*

 ?

8. 対応するオプションを有効にし、LDAP 設定を構成して、パッシブクライアントの認証を構成します。

注:

パッシブクライアントのサポートの設定は任意です。

パッシブクライアントの認証を有効にするには、次の詳細を入力します。

- a) **LDAP (Active Directory)** ベース。認証を許可する Active Directory (AD) 内にユーザーアカウントが存在するドメインの基本ドメイン名を入力します。たとえば、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 (構成を容易にするために電子メールアドレスを使用) を追加します。たとえば、CN= マネージャ、dc=netScaler、dc=com
- c) **LDAP (Active Directory)** バインド **DN** パスワード。認証用のドメインアカウントのパスワードを入力します。  
  
このセクションに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 (Active Directory) IP**。AD 認証が正しく機能するように、アクティブディレクトリサーバーの IP アドレスを入力します。
- e) **LDAP サーバの FQDN** 名。アクティブディレクトリサーバーの 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 名を指定します。
- f) **LDAP サーバの Active Directory** ポート。デフォルトでは、LDAP プロトコルの TCP ポートと 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)** ログインユーザ名。ユーザー名を「SAM アカウント名」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:

「\*」の付いたフィールドは必須です。

Enable Passive Clients Authentication

Parameters for configuring AD Auth for ADFSProxy

LDAP (Active Directory) Base\*  
 ?

LDAP (Active Directory) Bind DN\*  
 ?

LDAP (Active Directory) Bind DN Password\*  
 ?

LDAP Server (Active Directory) IP  
 ?

LDAP Server FQDN name  
 ?

LDAP Server (Active Directory) Port  
 ?

LDAP Host name  
 ?

Active Directory LDAP ?  
 Validate LDAP Certificate

LDAP (Active Directory) Login username

LDAP (Active Directory) Group Attribute Name  
 ?

LDAP (Active Directory) Group Sub-Attribute username

LDAP (Active Directory) default group

LDAP (Active Directory) SSO Attribute

Secure LDAP (Active Directory) Connection using SSL or TLS

9. 必要に応じて、DNS サーバーの 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 ADC 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 ADC インスタンスに構成を展開します。

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 ADC インスタンスに作成された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設定をデプロイできます。

オブジェクトが作成されました

ADFS プロキシ構成が NetScaler ADC インスタンスに展開されると、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。



# NetScaler Application Delivery Management 13.0

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Type : systemfile</b></p> <p><b>filecontent :</b><br/>LS0L5L1CRUjTBTDRVJUSZQDFURJ0L50ICK1JSURVENDQW9H20F3SJJ8Z0ICQX8Tma3Foa2HOKwQkFRi0ZBI<br/>VFRKXGVVRN11HQ12HZLNR6LN9J8LUNKQJZJWApjKxW7T7W0LkTmHR0ZGJYdF9yORJQZQVYQYjWEZEZV<br/>1URXIPVEEXTVrNd05Wd1HEVEISTVRF6UR9EQTFNNG3T7ZvZdZ3K9R0RBVQjNTEZCQUJNRRDnsdmrKxTmaatF6WVcx<br/>FR0JGaGw1YfNwWpXWXRjMkZ0YKvCafyMwMxV052Y5B0VYQXRNJK3CKYBWLURWUJFLREF3QEWU2DMVUS<br/>CQUJFQQR0R0RNSJUCQ20LQPRRURFSL1gpaVVC23TR69pQmPKSZZ6WmWmQJ1FKZ20d3Hf9pGT7T3ra5G4o4hNp5<br/>9KXQCCHNmeG5K2RbVjyaJHhakeEaZVPYKFSmd2N2NHaGhml3pVQVpDa3MyDkVocp6JJEKOWKQmBwc3NTI<br/>Hv3VpBakZvtnMTVh5kxMwWbuzndyTicQ3Vf7MyRtFDNp1WG1ZznwduLzInwDFZznov5DhQIMACjFV0VhAI<br/>0854NtZLkLkFQyWb0L1B0d0BMWWRHURRUSJ10KFCQmKwWThreus454B3CQJF8F8T0NBULV04L4CQz<br/>KOG3CjNlUjKbE15kUkVwXhN3V55XpR0ZaV1V8CmKLO9PCLUGR8R2NEFZWxz6UJhGLpWmZpWjZnJkM50<br/>zFRcNhdVYHdQkRW11M1NMcWwDGVVc0NSQX8uSjW1NnAqZV0D1TbU1RVVDH1ZQ9kUzJFHRTMzCZ1zhW0UjR<br/>N8VESLazE1V7C60UkWEKESPTAR0Z2mmdrczrv068Rf0kL0L3L3FTkQgQV0V65G5UNWELUS0LQp=</p> <p><b>fileencoding :</b> BASE64<br/><b>filelocation :</b> /nsconfig/ssl<br/><b>filename :</b> saml-idd.pem</p>                                                                                                                                                           |
| <p><b>Type : systemfile</b></p> <p><b>filecontent :</b><br/>LS0L5L1CRUjTBTBSU0EgUfJYKfURS8LrvktLS0LQpNSUJFEfJQkF850NBuUv859YMzFQnddEhkaEjW0dmelpM<br/>QzWwY71NzaJfT0EaJ9Cv0pR9SLQ59KXQJCOHnmeG4kaKkb26ymIRZpLrG1T2JBUjndYTR2hoZR0dFQZ1<br/>8T1U1159Qm00LUNSEKEEPUJN3V9BakQvRNRNTHC4HvZFHm53K5XNENJ1R6B0MLUQZV460ruZy4H<br/>h0bY1Y2Lb0jWaxdREFRQJBB0CQJvH51FG0EV2LV8BNDoveA03T0VhKIRTK3Rj2NEHrNFWjPc1VOLQZy2h2<br/>WUj0mTHBZDvR59DFQdmyNESS3hVxkQkpaZ0gleokRHzjT1oadtzc0XVY8LjmkovDnaah0sZ1aMEQ4J<br/>w50BBhYj0e0LjNMDaL0rN1M1G5AM7cc1N0Tha42pawWCKSDT78kzm3eJ53caRfemDNWFCR1A<br/>1Rz2hTzZPF6T9gWYUQWfWNC1QkoyeThubxpvMXNDW1dE9m8B8NAPGRhZNYXyKjQspWYpsRWY<br/>wWdAZWv5TzVYmVQ4WdQpYkTmIITFWR0zRVYQmNhmjmsXNDZ1PQkAQ2kKkFhdFT3htTQZ1zm<br/>1PZ7W1D0MwMwMwND0Sj1d0NNEWwQqPFWQWZNMW8w8yJfFwWwYd0T8kKzgdY5Cj0N0j0p<br/>IMzqNwStumpzTfFKZ1QNZLudFQkLpVUvXv0y0XpFanRbzRfThVUzJ3hVxVU11D0vLWg01Y1B50FfTE<br/>VCLWwQh5a0jUGV0dK53GLQmRQ0BME1BMNvaz0kVp5a08005TDPUYGNUGZCZKJURBLQKQRlvaAxl<br/>GELBBS3NEPFCWwJ4R75AKfFZ7NUL1c50m0Vr6E8kuz20NGHFCM0SLUW05V7PGWVGR3Zpc3w0k0wC<br/>EeloKumIWWJnr0eakU5TE5YU5STXapTWFYkhaF4R1L5D8yQnFYEUE0M1B4Zm9FjYdned5CAH2azRUempa<br/>0sLS0LUV0K85U0EgUfJYKfURS8LrvktLS0LQp=</p> <p><b>fileencoding :</b> BASE64<br/><b>filelocation :</b> /nsconfig/ssl<br/><b>filename :</b> saml-idd.key</p> |
| <p><b>Type : sslcertkey</b></p> <p><b>cert :</b> saml-idd.pem<br/><b>certkey :</b> adfs-certificate<br/><b>inform :</b> PEM<br/><b>key :</b> saml-idd.key</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**Objects Added on Instance : 192.168.153.160 | Count : 57**

**Type : nsfeature**

**Meta Properties**

action : enable

feature : cs lb ssl rewrite aaa

**Type : lbvserver**

ipv46 : 192.50.50.12

name : ns-ads-dep01-ads-dns

port : 53

servicetype : DNS

**Type : service**

ip : 10.30.30.5

name : ns-ads-dep01-dns-svc-1

port : 53

servicetype : DNS

**Type : lbvserver\_service\_binding**

name : ns-ads-dep01-ads-dns

servicename : ns-ads-dep01-dns-svc-1

**Type : authenticationnegotiateaction**

domain : ADFS.CITRIX.COM

domainuser : nsroot

domainuserpasswd : nsroot

name : ns-ads-dep01-negotiate-action

**Type : authenticationpolicy**

**action** : ns-ads-dep01-negotiate-action  
**name** : ns-ads-dep01-negotiate-policy  
**rule** : true

**Type : aaakcdaccount**

**delegateduser** : nsroot  
**kcdaccount** : ns-ads-dep01-ads-auth401-kcd-  
**kcdpassword** : nsroot  
**realmstr** : ADFS.CITRIX.COM

**Type : tmsessionaction**

**kcdaccount** : ns-ads-dep01-ads-auth401-kcd-  
**name** : ns-ads-dep01-ads-auth401-tmsession-action  
**persistentcookie** : ON  
**persistentcookievalidity** : 3  
**sso** : ON

**Type : tmsessionpolicy**

**action** : ns-ads-dep01-ads-auth401-tmsession-action  
**name** : ns-ads-dep01-ads-auth401-tmsession-policy  
**rule** : ns\_true

**Type : authenticationvserver**

**authenticationdomain** : ADFS.CITRIX.COM  
**failedlogintimeout** : 1  
**ipv46** : 192.50.50.40  
**maxloginattempts** : 255  
**name** : ns-ads-dep01-ads-auth401-auth-vserver  
**port** : 443  
**servicetype** : SSL

**Type : sslvserver\_sslcertkey\_binding**

**certkeyname** : adfs-certificate  
**vservername** : ns-adfs-dep01-adfs-auth401-auth-vserver

**Type : authenticationvserver\_authenticationpolicy\_binding**

**name** : ns-adfs-dep01-adfs-auth401-auth-vserver  
**policy** : ns-adfs-dep01-negotiate-policy  
**priority** : 10

**Type : authenticationvserver\_tmssessionpolicy\_binding**

**name** : ns-adfs-dep01-adfs-auth401-auth-vserver  
**policy** : ns-adfs-dep01-adfs-auth401-tmsession-policy  
**priority** : 10

**Type : authenticationldapaction**

**authentication** : ENABLED  
**authtimeout** : 30  
**followreferrals** : OFF  
**ldapbase** : dc=netScaler,dc=com  
**ldapbinddn** : cn=Manager,dc=netScaler,dc=com  
**ldapbinddnpassword** : nsroot  
**ldaploginname** : samAccountName  
**name** : ns-adfs-dep01-ldap-action  
**passwdchange** : DISABLED  
**sectype** : PLAINTEXT  
**serverip** : 10.30.30.3  
**serverport** : 389  
**ssonameattribute** : userPrincipalName  
**svrtype** : AD  
**validateservercert** : NO

**Type : authenticationpolicy**

**action** : ns-adfs-dep01-ldap-action  
**name** : ns-adfs-dep01-ldap-policy  
**rule** : true

**Type : aaakcdaccount**

**kcdaccount** : ns-ads-dep01-ads-ldap-kcd-acc  
**realmstr** : ADFS.CITRIX.COM

**Type : tmsessionaction**

**kcdaccount** : ns-ads-dep01-ads-ldap-kcd-acc  
**name** : ns-ads-dep01-ads-ldap-tmsession-action  
**persistentcookie** : OFF  
**sso** : ON

**Type : tmsessionpolicy**

**action** : ns-ads-dep01-ads-ldap-tmsession-action  
**name** : ns-ads-dep01-ads-ldap-tmsession-policy  
**rule** : ns\_true

**Type : authenticationvserver**

**authenticationdomain** : ADFS.CITRIX.COM  
**failedlogintimeout** : 1  
**ipv46** : 192.50.50.30  
**maxloginattempts** : 255  
**name** : ns-ads-dep01-ads-ldap-auth-vserver  
**port** : 443  
**servicetype** : SSL

**Type : sslvserver\_sslcertkey\_binding**

**certkeyname** : ads-certificate  
**vservername** : ns-ads-dep01-ads-ldap-auth-vserver

**Type : authenticationvserver\_authenticationpolicy\_binding**

**name** : ns-ads-dep01-ads-ldap-auth-vserver  
**policy** : ns-ads-dep01-ldap-policy  
**priority** : 10

**Type : authenticationvserver\_tmssessionpolicy\_binding**

**name** : ns-adfs-dep01-adfs-ldap-auth-vserver  
**policy** : ns-adfs-dep01-adfs-ldap-tmsession-policy  
**priority** : 10

**Type : csvserver**

**ipv46** : 192.50.50.50  
**name** : ns-adfs-dep01-cs  
**port** : 443  
**servicetype** : SSL

**Type : lbvserver**

**ipv46** : 192.50.50.50  
**name** : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb  
**port** : 445  
**servicetype** : SSL

**Type : servicegroup**

**servicegroupname** : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp  
**servicetype** : SSL

**Type : lbvserver\_servicegroup\_binding**

**name** : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb  
**servicegroupname** : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

**Type : server**

**ipaddress** : 192.30.30.30  
**name** : 192.30.30.30

**Type : servicegroup\_servicegroupmember\_binding**

**ip** : 192.30.30.30  
**port** : 443  
**servicegroupname** : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

**Type : sslserver\_sslcertkey\_binding**

**certkeyname** : adfs-certificate

**vservername** : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

**Type : csaction**

**name** : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction

**targetlbserver** : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

**Type : cspolicy**

**action** : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction

**policyname** : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol

**rule** : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") || HTTP.REQ.URL.CONTAINS("/federa

**Type : csvserver\_cspolicy\_binding**

**name** : ns-adfs-dep01-cs

**policyname** : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol

**priority** : 9800

**Type : lbvserver**

**appflowlog** : ENABLED

**authentication** : ON

**authenticationhost** : ADFS.CITRIX.COM

**authn401** : OFF

**authnvsname** : ns-adfs-dep01-adfs-ldap-auth-vserver

**downstateflush** : ENABLED

**ipv46** : 192.50.50.50

**lbmethod** : LEASTCONNECTION

**name** : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

**port** : 446

**servicetype** : SSL

**Type : servicegroup**

**servicegroupname** : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp  
**servicetype** : SSL

**Type : lbvserver\_servicegroup\_binding**

**name** : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb  
**servicegroupname** : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

**Type : servicegroup\_servicegroupmember\_binding**

**ip** : 192.30.30.30  
**port** : 443  
**servicegroupname** : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

**Type : sslvserver\_sslcertkey\_binding**

**certkeyname** : adfs-certificate  
**vservername** : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

**Type : csaction**

**name** : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction  
**targetlbvserver** : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

**Type : cspolicy**

**action** : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction  
**policyname** : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol  
**rule** : HTTP.REQ.URL.CONTAINS("/adfs/ls/auth/integrated") || HTTP.REQ.URL.CONTAINS("/adfs/ls/wia")

**Type : csvserver\_cspolicy\_binding**

**name** : ns-adfs-dep01-cs  
**policyname** : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol  
**priority** : 9900



**Type : lbvserver**

**appflowlog** : ENABLED  
**authentication** : OFF  
**authn401** : ON  
**authnvsname** : ns-ads-dep01-ads-auth401-auth-vserver  
**downstateflush** : ENABLED  
**ipv46** : 192.50.50.50  
**lbmethod** : LEASTCONNECTION  
**name** : ns-ads-dep01-ns-ads-dep01-ads-active-lb  
**port** : 444  
**servicetype** : SSL

**Type : servicegroup**

**servicegroupname** : ns-ads-dep01-ns-ads-dep01-ads-active-svcgrp  
**servicetype** : SSL

**Type : lbvserver\_servicegroup\_binding**

**name** : ns-ads-dep01-ns-ads-dep01-ads-active-lb  
**servicegroupname** : ns-ads-dep01-ns-ads-dep01-ads-active-svcgrp

**Type : servicegroup\_servicegroupmember\_binding**

**ip** : 192.30.30.30  
**port** : 443  
**servicegroupname** : ns-ads-dep01-ns-ads-dep01-ads-active-svcgrp

**Type : sslvserver\_sslcertkey\_binding**

**certkeyname** : ads-certificate  
**vservername** : ns-ads-dep01-ns-ads-dep01-ads-active-lb

**Type : csaction**

**name** : ns-ads-dep01-cs-ns-ads-dep01-ads-active-csaction  
**targetlbvserver** : ns-ads-dep01-ns-ads-dep01-ads-active-lb

**Type : cspolicy**

**action** : ns-ads-dep01-cs-ns-ads-dep01-ads-active-csaction  
**policyname** : ns-ads-dep01-cs-ns-ads-dep01-ads-active-cspol  
**rule** : true

**Type : csvserver\_cspolicy\_binding**

**name** : ns-ads-dep01-cs  
**policyname** : ns-ads-dep01-cs-ns-ads-dep01-ads-active-cspol  
**priority** : 10000

**Type : sslvserver\_sslcertkey\_binding**

**certkeyname** : ads-certificate  
**vservername** : ns-ads-dep01-cs

**Type : rewritepolicylabel**

**labelname** : ns-ads-dep01-request-rewritepolicylabel  
**transform** : HTTP\_REQ

**Type : rewritepolicylabel**

**labelname** : ns-ads-dep01-response-rewritepolicylabel  
**transform** : HTTP\_RES

**Type : rewriteaction**

**name** : ns-ads-dep01-HTTP.REQUEST-rewrite-action  
**stringbuilderexpr** : "/ads/services/trust/proxymex"  
**target** : HTTP.REQUEST  
**type** : REPLACE

**Type : rewritepolicy**

**action** : ns-ads-dep01-HTTP.REQUEST-rewrite-action  
**name** : ns-ads-dep01-HTTP.REQUEST-rewrite-policy  
**rule** : HTTP.REQUEST.CONTAINS("/ads/services/trust") && (!HTTP.REQUEST.CONTAINS("/trust/proxymex"))

**Type : rewritepolicylabel\_rewritepolicy\_binding**

gotopriorityexpression : END  
labelname : ns-adfs-dep01-request-rewritepolicylabel  
policyname : ns-adfs-dep01-HTTPREQ.URL-rewrite-policy  
priority : 10

**Type : lbvserver\_rewritepolicy\_binding**

bindpoint : REQUEST  
gotopriorityexpression : END  
invoke : true  
labelname : ns-adfs-dep01-request-rewritepolicylabel  
labeltype : policylabel  
name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb  
policyname : NOPOLICY-rewrite  
priority : 10

## Oracle e-ビジネス StyleBook

February 6, 2024

Oracle E-Business Suite は、統合されたグローバルなビジネス・アプリケーションの最も包括的なスイートです。このスイートは、組織が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を可能にします。以下のアプリケーションで構成されています。

- エンタープライズリソースプランニング (ERP)
- 顧客関係管理 (CRM)
- サプライチェーン管理 (SCM)

これらのコンピュータ・アプリケーションは、オラクルが開発または買収したものです。Oracle E-Business Suite 12.2 StyleBook を使用すると、選択した NetScaler ADC インスタンスに構成を展開できます。

この StyleBook は、負荷分散仮想サーバー、サービスグループ、およびサービスのリストで構成される負荷分散構成を作成します。また、サービスをサービスグループにバインドし、サービスグループを仮想サーバーにバインドできます。SSL を選択し、ローカルシステムから SSL ファイルとキーファイルを提供することで、暗号化された通信を選択できます。

## Oracle E-Business Suite 12.2 の構成を作成するには

1. Citrix Application Delivery Management (ADM) で、「アプリケーション」>「構成」>「StyleBooks」に移動します。[StyleBook] ページには、NetScaler ADM で使用可能なすべての StyleBook が表示されます。下にスクロールして、**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 パネルの「構成を作成」をクリックします。
3. ロードバランサー設定セクションにロードバランサーアプリケーションの名前と仮想 IP アドレスを入力します。
4. 必要なプロトコルを選択します。ここには、HTTP と HTTPS/SSL の 2 つのオプションがあります。ポート番号を入力することもできます。
5. 負荷分散の対象とな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、さらにサーバの IP アドレスを追加します。
6. **SSL** 証明書の設定セクションで、ローカルストレージからそれぞれのファイルを選択します。[証明書の詳細設定] チェックボックスをオン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。

構成を作成する対象の NetScaler ADC インスタンスを選択し、[作成] をクリックします。

This configuration will be created from the StyleBook 'oracle-ebusiness-suite12' (namespace: 'com.citrix.adc.enterprise.stylebooks', version: '1.0').

Application Name\*

Virtual IP (VIP)\*

Protocol

Virtual Port

Oracle E-Business Suite Server IPs\*  
 ×  
 × +

SSL Certificate settings

| Certificate Name | CertKey Format | Certificate Key Name | Private Key Password |
|------------------|----------------|----------------------|----------------------|
| oracle-cert-file | PEM            | oracle-cert-key-file | ×                    |

Advanced Settings

Target Instances  
 > +

Create Close Dry Run

### ヒント

更新アイコンをクリックして、Citrix ADM で最近検出された Citrix ADC 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。更新アイコンは現在、NetScaler

ADM でのみ使用できます。

## Citrix StoreFront StyleBooks

February 6, 2024

StoreFront は、Citrix Virtual Apps and Desktops サイトのアプリケーションとデスクトップをユーザー用の 1 つのストアに集約するエンタープライズアプリストアです。StoreFront は、リソースをホストするサイトへのユーザーを認証し、ユーザーがアクセスするアプリケーションストアとデスクトップを管理します。エンタープライズアプリケーションストアをホストし、ユーザーが利用できるアプリやデスクトップにセルフサービスでアクセスできるようにします。

この StyleBook では、StoreFront サーバーの NetScaler ADC 構成を定義します。この StyleBook では、StoreFront サーバーを目的の NetScaler ADC インスタンスに構成できます。SSL を選択し、ローカルシステムから SSL ファイルとキーファイルを提供することで、暗号化された通信を選択できます。

### Citrix StoreFront アプリケーションの構成の作成

1. Citrix ADM GUI で、[アプリケーション] > [StyleBook] に移動します。
2. 検索バーで、名前プロパティを使用して **Citrix StoreFront** を検索します。
3. Citrix StoreFront StyleBook で、「構成を作成」をクリックします。
4. 次の詳細を指定します：
  - **StoreFront** 名: StoreFront 名を指定します。StoreFront 構成パックは同じ StoreFront 名で作成されます。
  - 仮想 IP (VIP): Citrix ADC インスタンスがクライアント要求を受信する仮想 IP アドレスを指定します。
  - **StoreFront** サーバー: Citrix ADC インスタンスで構成する StoreFront StoreFront サーバーの IP アドレスを指定します。
  - **HTTPS** リダイレクト URL: **HTTPS** リクエストのリダイレクト先の HTTPS URL を指定します。

**Configuration > Deploy Configuration**

This configuration was created from the StyleBook 'storefront' (namespace: 'com.citrix.adc.stylebooks ,version: '1.0').

StoreFront Name\*

Virtual IP (VIP)\*

StoreFront Servers (IPs)\*

 +

HTTPS Redirect URL\*

+ **SSL Certificate settings**

| CERTIFICATE NAME | CERTKEY FORMAT | CERTIFICATE KEY NAME |
|------------------|----------------|----------------------|
| <i>No items</i>  |                |                      |

**Target Instances**

Click to select
>
+

OK

Close

Dry Run

5. [ **SSL 証明書の設定** ] セクションで、SSL 証明書の名前と証明書キーを入力します。
6. ローカルストレージフォルダからそれぞれのファイルを選択します。秘密鍵のパスワードを入力して、暗号化された秘密鍵を PEM 形式で指定することもできます。

Certificate Name\*

SF-certificate ⓘ

Certificate File\*

Choose File ▾ test-cert.pem ⓘ

CertKey Format\*

PEM ▾ ⓘ

Certificate Key Name

SF-key-name ⓘ

Certificate Key File

Choose File ▾ private-key.pem ⓘ

Private Key Password

Advanced Certificate Settings

Create Close

7. [ 証明書の詳細設定 ] チェックボックスをオン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入力したり、証明書有効期限モニターを有効または無効にしたりできます。
8. オプション: **SSL** 証明書で **Citrix ADC** に **CA** パブリック証明書をインストールする必要がある場合は、「認証仮想 IP 用の SSL CA 証明書」チェックボックスを選択します。「証明書の詳細設定」セクションで「CA 証明書です \*\*」を選択してください。
9. [作成] をクリックします。
10. 「ターゲットインスタンス」をクリックし、StoreFront サーバーを構成する Citrix ADC インスタンスを選択します。
11. [作成] をクリックして構成を作成し、選択した NetScaler ADC インスタンスに構成を展開します。

## カスタム **StyleBook** の作成と使用

February 6, 2024

デプロイメント用に独自の StyleBook を作成し、それを CitrixApplication Delivery Management (ADM) にインポートして、構成オブジェクトを作成できます。また、API を使用して、StyleBook から構成を作成することもできます。

このドキュメントでは、次の内容について説明します。

はじめに

StyleBook の作成を始める前に、次の知識があることを確認してください。

- NITRO API。詳しくは、[Nitro API のドキュメントを参照してください](#)。
- YAML

StyleBook ファイルでは 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 を作成するときは、次に示す YAML のガイドラインに注意する必要があります。

- YAML では、大文字と小文字が区別されます。
- YAML では、インデントを適切に使用する必要があります。
- `<spacebar>` キーを使用して適切なインデントを作成します。`<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 Service 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。文字列が句読点（ダッシュ、コロン、その他）を含む場合にのみ、文字列を引用符で囲ってください。数字を文字列として解釈する必要がある場合は、数字を引用符で囲むか、または StyleBook の組み込み関数 `str()` を使用します。
- YES/Yes/yes/Y/y/NO/no/No/n/N、ON/On/on/OFF/Off/off、TRUE/true/truthy/FALSE/False/false/falsely などのリテラルはブール値と見なされ、それぞれ真と偽と同等です。これらのリテラルを文字列として解釈するには、引用符で囲んでください。次に例を示します：
  - “YES”
  - “No”
  - “True”
  - “False” など。



注

StyleBook ファイルを NetScaler ADM にインポートする前に、ファイルが YAML 形式に準拠しているかどうかを確認することをお勧めします。StyleBooks に組み込みの YAML バリデータを使用して、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。

StyleBook の設定では、作成 および 削除操作 (**POST** および **DELETE** HTTP メソッド) をサポートする Nitro 構成リソースのみを使用できます。詳しくは、[Nitro API のドキュメントを参照してください](#)。

## StyleBook の構造

StyleBook を作成するには、StyleBook の文法、構文、および構造を理解する必要があります。通常、StyleBook には、次のセクションが含まれます。

- **ヘッダー:** このセクションでは、StyleBook のアイデンティティを定義し、その機能を説明できます。これは必須セクションです。
- **Import StyleBooks:** このセクションでは、現在の StyleBook から参照する他の StyleBook を宣言できます。StyleBook を作成するには、NetScaler ADC NITRO 構成の StyleBooks 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。
- **Parameters:** このセクションでは、構成を作成するために必要な StyleBook のパラメーターを定義します。StyleBook では、このセクションに記述された入力を使用されます。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、特定の構成用に StyleBook によって作成されるエンティティ (構成オブジェクト) を定義できます。このセクションは、StyleBook の中核です。Components では通常、Parameters セクションの入力値を使用して、StyleBook で生成される構成に適応させます。これはオプションのセクションです。

StyleBook には、Parameters セクションと Components セクションのいずれか、または両方を記述できます。他の StyleBook で使用可能なパラメーターの一覧を定義する場合、Parameters セクションのみを含む StyleBook を作成すると便利です。これにより、一連の StyleBook 全体で、パラメーターグループが再利用しやすくなります。ユーザー入力を取得するパラメーターを定義せずに、StyleBook の属性値を指定する場合は、Components セクションのみを含む StyleBook を使用します。

- **Outputs:** Parameters セクションでは、StyleBook の入力を定義しましたが、この省略可能な Outputs セクションでは StyleBook の出力を定義します。構成を作成するユーザーは、この省略可能な Outputs セクションで指定したコンポーネントを、この StyleBook から、この StyleBook をインポートする他の StyleBook に公開できます。これにより、ユーザーおよびインポートする側の StyleBook は、公開されたコンポーネントのプロパティを参照できます。
- **操作:** StyleBook には、StyleBook の一部である任意の仮想サーバー上の NetScaler ADM でアナリティクスを有効にするオプションセクションが含まれている場合があります。

次の図は、StyleBook の概略を簡単に示したものです。



次の例は、StyleBook の文法と構文について学び、より複雑な StyleBook の作成方法を理解するのに役立ちます。

- 負荷分散仮想サーバーを作成する [StyleBook](#)
- [StyleBook](#) による基本的な負荷分散構成の作成
- 複合 [StyleBook](#) の作成
- GUI 属性を使用して [StyleBook](#) をカスタマイズ

## 負荷分散仮想サーバーを作成する **StyleBook**

February 6, 2024

この例で設計する基本的な StyleBook では、プロトコルのタイプが HTTP で、ポート 80 でリッスンする負荷分散仮想サーバーを作成します。仮想サーバーの名前、IP アドレス、負荷分散方式の各パラメーターには、ユーザーが定義した値を指定できます（これらは StyleBook のパラメーターです）。

## Header

StyleBook の先頭の 6 行は、Header セクションです。この例の場合、Header セクションは、次のように記述されています。

```
1 name: lb-vserver
2 description: This StyleBook defines a load balancing virtual server
  configuration.
3 display-name: Load Balancing Virtual Server (HTTP)
4 namespace: com.example.stylebooks
5 schema-version: "1.0"
6 version: "0.1"
7 <!--NeedCopy-->
```

Header セクションには、次の情報が記述されています。

- **name:** この StyleBook の名前。
- **description:** この StyleBook の実行内容を示す説明。この説明は NetScaler ADM に表示されます。
- 表示名: NetScaler ADM に表示される StyleBook の説明的な名前。
- **namespace:** 名前空間は、StyleBook の一意の識別子の一部で、これにより名前の衝突を回避できます。
- **schema-version:** このリリースでは、値は常に「1.0」です。
- **version:** StyleBook のバージョン番号。バージョン番号は、StyleBook の更新時に変更できます。

**name**、**namespace**、および **version** 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 ADM では、名前、名前空間、およびバージョンの組み合わせが同じ 2 つの StyleBook を使用することはできません。ただし、**name** と **version** が同じであっても **namespace** が異なる場合、または **namespace** と **version** が同じであっても **name** が異なる場合は、それらの 2 つの StyleBook を使用できます。

### 注

StyleBook を更新して、**version** の番号が更新された場合を想定してください。別の StyleBook でこの StyleBook を参照している（つまりインポートしている）場合は、インポート元の StyleBook の正しいバージョン番号が使用されるように、別の StyleBook を確実に更新して、インポートされる StyleBook の正しいバージョンが使われるようにしてください。

## StyleBook のインポート

ヘッダーの次のセクションは「import-stylebooks」と呼ばれます。このセクションで、現在の StyleBook で参照する他の 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。このセクションを記述すると、他の StyleBook をインポートして再利用できるため、StyleBook で同じ構成を再作成する必要がなくなります。

この例の場合、import-stylebooks セクションは、次のように記述されています。

```
1 import-stylebooks:  
2 -  
3 namespace: netScaler.nitro.config  
4 prefix: ns  
5 version: "10.5"  
6 <!--NeedCopy-->
```

いずれかの NITRO 構成オブジェクトを直接使用する場合、StyleBook では、netScaler.nitro.config 名前空間を必ず参照する必要があります。この名前空間には、lbvServer など、すべての NetScaler ADC 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 以降を実行する任意の NetScaler ADC インスタンスで構成を作成して実行できます。

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示すための略語です。この場合、ns はバージョン 10.5 の netScaler.nitro.config を指します。StyleBook の以降のセクションでは、名前空間とバージョンを使用して、インポートされる StyleBook を示す代わりに、選択したプレフィックス文字列（上記の例では ns）を使用できます。

StyleBook で使用されるバージョンは、NetScaler ADC NITRO バージョンです。Nitro バージョン X をベースにした StyleBook を使用して、バージョン X 以降の任意の Citrix ADC を構成できます。

#### 注

StyleBook を使用してバージョン 10.5 以降の Citrix ADC インスタンスを構成できるようにするには、互換性を最大限に高めるために、Nitro 組み込み StyleBook（名前空間：netScaler.nitro.config、バージョン：10.5）を直接使用する StyleBook に Nitro 10.5 名前空間をインポートすることをお勧めします。

他の StyleBook をインポートする StyleBook は、インポートする StyleBook と同じかそれ以上のバージョンの Nitro バージョンをベースにしている必要があることが重要です。たとえば、Nitro バージョン 10.5 をベースにした StyleBook は、11.1 をベースにした StyleBook に依存したり、使用したり、インポートしたりすることはできません。しかし、バージョン 11.1 に基づく StyleBook は、11.1 未満のバージョンに基づく StyleBook をインポートすることができます。

StyleBook が Nitro 名前空間をまったくインポートしない可能性もあります。つまり、StyleBook は Nitro コンポーネントを直接定義する必要はありませんが、Nitro コンポーネントを定義する StyleBook をインポート（依存）できます。他の StyleBook をインポートする StyleBook は、依存関係の階層の中で常に最も高い Nitro バージョンを取得するため、そのバージョン以上の Citrix ADC を構成するために使用できます。

#### パラメーター

Parameters セクションでは、StyleBook で必要なすべてのパラメーターを宣言できます。StyleBook の作成者は、StyleBook のユーザーが指定する入力項目を決定する必要があります。この例の場合、ユーザーが、仮想サーバーの名前、IP アドレス、負荷分散方式を指定するように StyleBook を設計しました。

Parameters セクションは、次のようになっています。

```
1 parameters:
2   -
3     name: name
4     type: string
5     label: Application Name
6     description: Name of the application configuration.
7     required: true
8
9   -
10    name: ip
11    type: ipaddress
12    label: Application Virtual IP (VIP)
13    description: Application VIP that the clients access.
14    required: true
15
16  -
17    name: lb-alg
18    type: string
19    label: LoadBalancing Algorithm
20    description: Choose the load balancing algorithm (method) used for
21      load balancing client request between the application servers.
22    allowed-values:
23      - ROUNDROBIN
24      - LEASTCONNECTION
25    default: ROUNDROBIN
26  <!--NeedCopy-->
```

#### 注

パラメーターのラベルを指定しない場合、NetScaler ADM はこのパラメーターを表示するときに名前属性を使用します。NetScaler ADM での表示方法を制御できるように、必ずパラメーターにラベルを定義する必要があります。

ただし、API で使われる場合、パラメーターはその `name` で指定されます。

このセクションでは、**name** 属性の値で示される 3 つのパラメーターが宣言されています。**name** は仮想サーバー名、**ip** は仮想サーバーの IP アドレス、**lb-alg** は負荷分散方式を表します。

- **type**. これらのパラメータに指定できる値のタイプ。たとえば、`name` と `lb-alg` には、文字列値を使用できます。また、`ip` 値のタイプは、IP アドレスにする必要があります。StyleBook のパラメーターには、次のいずれかの組み込みタイプを指定できます。
- **string**. 文字の配列。長さが指定されていない場合、文字列値には、任意の数の文字を使用できます。ただし、`min-length` 属性と `max-length` 属性を使用すれば、文字列タイプの長さを制限できます。
- **number**. 整数値。 `min-value` 属性と `max-value` 属性により、このタイプで使用できる最小数と最大数を指定できます。
- **boolean**. 真でも偽でもかまいません。YAML では、すべてのリテラルがブール値（例：Yes または No）と見なされることに注意してください。
- **ipaddress**. 有効な IPv4 または IPv6 アドレスを表す文字列。

- **tcp-port**. TCP ポートまたは UDP ポートを表す 0 から 65535 までの数値です。
- **password**. 不透明/秘密の文字列値。NetScaler ADM でこのパラメータの値が表示される場合は、アスタリスク (\*\*\*\*\*) として表示されます。
- **certfile**. 証明書ファイル。
- **keyfile**. 証明書のプライベートキーファイル。
- **file**. このタイプのパラメータでは、ユーザーは証明書やキーファイルなどの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、これらの各要素はパラメータです。このタイプを使用すると、関連する複数のパラメータを 1 つの親パラメータの下にグループ化できます。
- **required**. パラメータが必須かオプションかを示します。true に設定すると、パラメータは必須になります。その場合、ユーザーは、StyleBook を使った構成の作成時にこのパラメータの値を指定する必要があります。デフォルトでは、すべてのパラメータが任意です。この例では、**name** と **ip** は必須パラメータですが、**lb-alg** はオプションパラメータで、デフォルト値は「ROUNDROBIN」です。

任意のパラメータにデフォルト値を割り当てるには、**default** 属性を使用します。構成の作成時、ユーザーが値を指定しない場合は、デフォルト値が使用されます。たとえば、**lb-alg** パラメータのデフォルト値は、ROUNDROBIN です。

構成の作成時にユーザーが選択できる値を定義するには、**allowed-values** 属性を使用します。この例の場合、**lb-alg** パラメータには、ROUNDROBIN および LEASTCONNECTION という 2 つの値が指定されています。

StyleBook をインポートして使用すると、NetScaler ADM はこれらの 3 つのパラメータを含むフォームが表示されます。name および ip に対して表示されるフィールドでは、文字列タイプと IP アドレスタイプの値を入力できます。lb-alg のフィールドは、ボックスの一覧として表示されます。デフォルトでは、ROUNDROBIN という値が選択されています。

#### 注

組み込みタイプに加えて、パラメータには他の StyleBook をタイプにすることができます。こうして他の StyleBook で定義されたパラメータを再利用できます。

## コンポーネント

この StyleBook の最後のセクションは、Components セクションです。Components セクションは、StyleBook で最も重要なセクションです。このセクションでは、StyleBook で作成する必要がある構成オブジェクトを定義します。

この例の場合、Components セクションは、次のように記述する必要があります。

```
1 components:
2   -
3     name: lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: $parameters.name
```

```
7   servicetype: HTTP
8   ipv46: $parameters.ip
9   port: 80
10  lbmethod: $parameters.lb-alg
11  <!--NeedCopy-->
```

この例では、コンポーネントが1つのみ含まれています。コンポーネントの主要な属性は、name、type、および properties です。このコンポーネントで指定するプロパティは、コンポーネントのタイプによって決まります。コンポーネントには、次の2つのタイプがあります。

- ビルトインタイプ。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「lbserver」や「servicegroup」などです。この例では、組み込みのコンポーネントのタイプが使われています。
- 複合タイプ。このタイプは、作成して NetScaler ADM にインポートした StyleBook、または NetScaler ADM に同梱されているデフォルトの StyleBook です。複合 StyleBook の詳細については、「[複合 StyleBook の作成](#)」を参照してください。

この例では、**lbserver-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のタイプは **ns:: lbserver**(組み込みの Nitro タイプ) で、「ns」は import-stylebooks セクションで指定した名前空間 netScaler.nitro.config とバージョン 10.5 を指すプレフィックスで、「lbserver」はこの名前空間の Nitro リソースです。

ここで定義されている **properties** は、「lbserver」リソースの属性です。使用可能なすべての NetScaler ADC Nitro リソースとその属性の詳細については、[NetScaler ADC NITRO REST API の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、「lbserver」リソースの必須属性が含まれています。そのため、これらの属性の値を指定できます。この例では、servicetype と port には静的な値が指定されていますが、name、ipv46、および lbmethod の各プロパティは、入力パラメーターから値を取得します。StyleBook の残りの部分では、を使用して、パラメータ・セクションで定義されたパラメータ名を参照できます。**\$parameters.<parameter-name>** 式 (例: **\$パラメータ.ip**) です。

#### 注

慣例により、「インポート StyleBook」セクションでは、常にプレフィックス「ns」を使用して Citrix ADC Nitro 名前空間を指定します。これは必須ではありませんが、一貫性を保つためにお使いの StyleBook で慣例に従うことをお勧めします。

## StyleBook を構築する

StyleBook の必須セクションをすべて定義しました。これらのセクションをまとめて、最初の StyleBook を作成します。StyleBook の内容をコピーして、テキストエディターに貼り付け、**lb-vserver.yaml** という名前でファイルを保存します。Citrix では、StyleBooks に組み込まれている YAML 検証ツールを使用して 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。

lb-vserver.yaml ファイルのすべての内容を次に示します。

```
1 name: lb-vserver
2 namespace: com.example.stylebook
3 version: "1.0"
4 display-name: Load Balancing Virtual Server (HTTP)
5 description: "This stylebook defines a very simple load balancing HTTP
6   virtual server configuration"
6 schema-version: "1.0"
7
8 import-stylebooks:
9   -
10    namespace: netscaler.nitro.config
11    version: "10.5"
12    prefix: ns
13   -
14    namespace: com.citrix.adc.stylebooks
15    version: "1.0"
16    prefix: stlb
17
18 parameters:
19   -
20    name: name
21    label: "Application Name"
22    description: "Give a name to the application configuration."
23    type: string
24    required: true
25   -
26    name: vip-ipaddress
27    label: "Load Balancer IP Address"
28    description: "The Application VIP that clients access"
29    type: ipaddress
30    required: true
31   -
32    name: lb-alg
33    label: LB Algorithm
34    description: Load Balancing Algorithm
35    type: string
36    default: ROUNDROBIN
37    allowed-values:
38     - ROUNDROBIN
39     - LEAST-CONNECTION
40
41 components:
42   -
43    name: lbvserver-comp
44    description: This StyleBook component (a Builtin Nitro StyleBook)
45      builds a Citrix ADC load balancing virtual server configuration
46      object.
47    type: ns::lbvserver
48    properties:
49     name: $parameters.name
50     ipv46: $parameters.vip-ipaddress
51     lbmethod: $parameters.lb-alg
```



```
50     servicetype: HTTP
51     port: 80
52 <!--NeedCopy-->
```

StyleBook を使用して構成を作成するには、NetScaler ADM にインポートしてから使用する必要があります。詳しくは、「[ユーザー定義の StyleBook を使用方法](#)」を参照してください。

またこの StyleBook を他の StyleBook に（import-stylebooks 構造を使って）インポートすることもできます。または、次のセクションで説明されるように、より多くのパラメーターとコンポーネントを含むようにこの StyleBook を修正することもできます。

## StyleBook による基本的な負荷分散構成の作成

February 6, 2024

前の例では、負荷分散仮想サーバーを作成するための基本的な StyleBook を作成しました。この StyleBook を別名で保存した後、基本的な負荷分散を構成するためのパラメーターとコンポーネントを追加して、StyleBook を更新します。この StyleBook ファイルを **basic-lb-config.yaml** という名前で保存します。

このセクションでは、負荷分散仮想サーバー、サービスグループ、およびサービス一覧からなる負荷分散の構成を作成する新しい StyleBook を設計します。また、サービスをサービスグループにバインドし、サービスグループを仮想サーバーにバインドできます。

### Header

この StyleBook を作成するには、最初に Header セクションを更新する必要があります。このセクションは、負荷分散仮想サーバーの StyleBook 用に作成したセクションと似ています。Header セクションで、**name** の値を basic-lb-config に変更します。また、この StyleBook の適切な説明を記述して、**description** と **display-name** を更新します。**namespace** と **version** の値は、変更する必要はありません。name を変更したため、name、namespace、および version の組み合わせにより、この StyleBook の一意の識別子がシステム内に作成されます。

```
1 name: basic-lb-config
2 description: This StyleBook defines a simple load balancing
  configuration.
3 display-name: Load Balancing Configuration
4 namespace: com.example.stylebooks
5 schema-version: "1.0"
6 version: "0.1"
7 <!--NeedCopy-->
```

## StyleBook のインポート

import-stylebooks セクションは、同じままです。このセクションでは、Nitro 構成オブジェクトを使用するために、netscaler.nitro.config 名前空間が指定されています。

```
1 import-stylebooks:  
2 -  
3 namespace: netscaler.nitro.config  
4 prefix: ns  
5 version: "10.5"  
6 <!--NeedCopy-->
```

## パラメーター

Parameters セクションを更新して、サービスまたはサーバーの一覧を定義するパラメーターと、サービスをリスンするポートを定義するパラメーターを追加する必要があります。先頭の 3 つのパラメーター (name、ip、lb-alg) は、同じままです。

```
1 parameters:  
2 -  
3 name: name  
4 type: string  
5 label: Application Name  
6 description: Name of the application configuration  
7 required: true  
8 -  
9 name: ip  
10 type: ipaddress  
11 label: Application Virtual IP (VIP)  
12 description: Application VIP that the clients access  
13 required: true  
14 -  
15 name: lb-alg  
16 type: string  
17 label: LoadBalancing Algorithm  
18 description: Choose the load balancing algorithm used for load  
19 balancing client requests between the application servers.  
20 allowed-values:  
21 - ROUNDROBIN  
22 - LEASTCONNECTION  
23 default: ROUNDROBIN  
24 -  
25 name: svc-servers  
26 type: ipaddress[]  
27 label: Application Server IPs  
28 description: The IP addresses of all the servers of this application  
29 required: true  
30 -  
31 name: svc-port  
32 type: tcp-port
```

```
32   label: Server Port
33   description: The TCP port open on the application servers to receive
           requests.
34   default: 80
35   <!--NeedCopy-->
```

この例では、アプリケーションのバックエンドサーバーを表すサービスの IP アドレスのリストを受け入れるように **svc-servers** パラメーターが追加されています。これは、**required: true** からわかるように、必須パラメーターです。2 番目のパラメーター、**svc-port** は、サーバーがリスンするポート番号を示しています。ユーザーの指定がなければ、**svc-port** パラメーターのデフォルトのポート番号は 80 です。

## コンポーネント

また、Components セクションを更新して、新しい 2 つのパラメーターを使用して完全な負荷分散構成を作成する追加コンポーネントを定義する必要があります。

この例の場合、Components セクションは、次のように記述する必要があります。

```
1  components:
2  -
3    name: lbvserver-comp
4    type: ns::lbvserver
5    properties:
6      name: $parameters.name + "-lb"
7      servicetype: HTTP
8      ipv46: $parameters.ip
9      port: 80
10     lbmethod: $parameters.lb-alg
11
12  components:
13  -
14     name: svcg-comp
15     type: ns::servicegroup
16     properties:
17       name: $parameters.name + "-svgrp"
18       servicetype: HTTP
19
20  components:
21  -
22     name: lbvserver-svg-binding-comp
23     type: ns::lbvserver_servicegroup_binding
24     properties:
25       name: $parent.parent.properties.name
26       servicegroupname: $parent.properties.name
27  -
28     name: members-svcg-comp
29     type: ns::servicegroup_servicegroupmember_binding
30     repeat: $parameters.svc-servers
31     repeat-item: srv
32     properties:
```

```

33     ip: $srv
34     port: str($parameters.svc-port)
35     servicegroupname: $parent.properties.name
36 <!--NeedCopy-->

```

この例では、元のコンポーネント **lbvserver-comp** (前の例の) に **svcg-comp** という子コンポーネントが追加されました。また、**svcg-comp** コンポーネントには 2 つの子コンポーネントがあります。コンポーネントを別のコンポーネント内にネストした場合、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オブジェクトが作成されるたびに、1 つまたは複数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 ADC インスタンス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 には静的な値が指定されていますが、name は、入力パラメーターから値を取得します。パラメーターセクションで定義されているパラメーター名は、**\$parameters.name+「-svcgrp」** という表記を使用して参照します。ここで、ユーザー定義名に **-svcgrp** を追加 (連結) します。

コンポーネント **svcg-comp** には、**lbvserver-svg-binding-comp** と **members-svcg-comp** という 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、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) との間で構成オブジェクトをバインドするために使用されます。**\$parent** 表記 (親参照とも呼ばれる) は、親コンポーネント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、サービスグループ名: **\$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指し、名前 **\*\*:\$parent.parent.properties.name** は親コンポーネント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指します。\*\*

**members-svcg** コンポーネントは、親コンポーネントによって作成されたサービスグループにサービスのリスト間の設定オブジェクトをバインドするために使用されます。複数のバインディング設定オブジェクトを作成するには、StyleBook の **repeat** 構造を使用して、パラメータ **svcg-servers** で指定されたサーバーのリストを反復処理します。繰り返し処理中、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 (繰り返し項目構造では **srv** と呼ばれます) に対して **servicegroup\_servicegroupmember\_binding** タイプの **Nitro** 構成オブジェクトを作成し、各 **Nitro** 構成オブジェクトの **ip** 属性を対応するサーバーの **IP** アドレスに設定します。

一般に、コンポーネントで **repeat** および **repeat-item** 構造を使用して、そのコンポーネントに同じタイプの複数の構成オブジェクトを構築させることができます。**repeat-item** コンストラクトに変数名 (srv など) を割り当てて、イテレーション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 **\$\** として参照されます (<varname\> 例: \$srv)。

上記の例では、お互いの内部でコンポーネントのネスティングを使って、簡単に構成を組み立てています。この場合、コンポーネントのネスティングが構成を組み立てる唯一の方法ではありません。次に示すように、ネストしなくても同じ結果が得られる可能性があります。

```

1 components:
2   -
3     name: members-svcg-comp

```

```

4   type: ns::servicegroup_servicegroupmember_binding
5   repeat: $parameters.svc-servers
6   repeat-item: srv
7   properties:
8     ip: $srv
9     port: str($parameters.svc-port)
10    servicegroupname: $components.svcg-comp.properties.name
11  -
12    name: lbvserver-svg-binding-comp
13    type: ns::lbvserver_servicegroup_binding
14    properties:
15      name: $components.lbvserver-comp.properties.name
16      servicegroupname: $components.svcg-comp.properties.name
17  -
18    name: lbvserver-comp
19    type: ns::lbvserver
20    properties:
21      name: $parameters.name + "-lb"
22      servicetype: HTTP
23      ipv46: $parameters.ip
24      port: 80
25      lbmethod: $parameters.lb-alg
26  -
27    name: svcg-comp
28    type: ns::servicegroup
29    properties:
30      name: $parameters.name + "-svcgrp"
31      servicetype: HTTP
32  <!--NeedCopy-->

```

ここでは、すべてのコンポーネントは同じレベルにあります（つまり、ネストされていません）が、達成される結果（生成された Citrix ADC 構成）は、以前に使用したネストされたコンポーネントと同じです。また、StyleBook のコンポーネントを宣言する順序が、構成オブジェクトの作成順序に影響を与えることはありません。この例では、**svcg-comp** と **lbvserver-comp** コンポーネントは、最後に宣言されたものであっても、**2** 番目のコンポーネント **lbvserver-svg-binding-comp** をビルドする前にビルドする必要があります。**2** 番目のコンポーネントにはこれらのコンポーネントへのフォワードリファレンスがあるためです。

#### 注

慣例によって、StyleBooks、パラメーター、置換、コンポーネント、出力の名前は小文字です。複数の単語を含む場合は「-」文字で区別されます。たとえば、「lb-bindings」、「app-name」、「rewrite-config」などがあります。別の慣例としては、コンポーネント名には文字列「-comp」を末尾に付け加えます。

## 結果

新しい StyleBook に最後に追加するセクションは Outputs セクションです。Outputs セクションでは、この StyleBook を使用して構成を作成した後にユーザーに（または他の StyleBook で）公開する情報を指定します。たとえば、Outputs セクションでは、この StyleBook で作成される lbvserver および servicegroup 構成オブジェ

クトを公開することを指定できます。

```
1 outputs:
2   -
3     name: lbvserver-comp
4     value: $components.lbvserver-comp
5     description: The component that builds the Nitro lbvserver
6                 configuration object
7   -
8     name: servicegroup-comp
9     value: $components.svcg-comp
10    description: The component that builds the Nitro servicegroup
11                configuration object
12 <!--NeedCopy-->
```

StyleBook の Outputs セクションは、必要に応じて記述します。StyleBook で必ずしも出力を返す必要はありません。ただし、内部コンポーネントを出力として返すと、この StyleBook をインポートするすべての StyleBook の柔軟性が向上します。このことは、複合 StyleBook の作成時にわかります。

#### 注

outputs セクションで、コンポーネントの単一のプロパティだけでなく、StyleBook のコンポーネントの全体を公開することが推奨されます（たとえば、`$components.lbvserver-comp.properties.name` という名前だけでなく、`$components.lbvserver-comp` 全体を公開します）。また出力には、特定の出力が何を表すかを説明する記述が追加されます。

## StyleBook を構築する

StyleBook の必須セクションをすべて定義したので、それらをまとめて 2 番目の StyleBook を作成します。この StyleBook ファイルは、**basic-lb-config.yaml** という名前で既に保存されています。Citrix では、StyleBooks ページの組み込み YAML 検証ツールを使用して 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。

**basic-lb-config.yaml** のすべての内容を次に示します。

```
1 name: basic-lb-config
2 namespace: com.example.stylebooks
3 version: "0.1"
4 display-name: Load Balancing Configuration
5 description: This StyleBook defines a simple load balancing
6             configuration.
7 schema-version: "1.0"
8
9 import-stylebooks:
10  -
11    namespace: netscaler.nitro.config
12    version: "10.5"
13    prefix: ns
14    parameters:
```

```
14 -
15   name: name
16   type: string
17   label: Application Name
18   description: Give a name to the application configuration.
19   required: true
20 -
21   name: ip
22   type: ipaddress
23   label: Application Virtual IP (VIP)
24   description: The Application VIP that clients access
25   required: true
26 -
27   name: lb-alg
28   type: string
29   label: LoadBalancing Algorithm
30   description: Choose the loadbalancing algorithm (method) used for
31     loadbalancing client requests between the application servers.
32   allowed-values:
33     - ROUNDROBIN
34     - LEASTCONNECTION
35   default: ROUNDROBIN
36 -
37   name: svc-servers
38   type: ipaddress[]
39   label: Application Server IPs
40   description: The IP addresses of all the servers of this application
41   required: true
42 components:
43 -
44   name: lbvserver-comp
45   type: ns::lbvserver
46   properties:
47     name: $parameters.name + "-lb"
48     servicetype: HTTP
49     ipv46: $parameters.ip
50     port: 80
51     lbmethod: $parameters.lb-alg
52 -
53   name: svcg-comp
54   type: ns::servicegroup
55   properties:
56     servicegroupname: $parameters.name + "-svcgrp"
57     servicetype: HTTP
58 -
59 -
60   name: lbvserver-svg-binding-comp
61   type: ns::lbvserver_servicegroup_binding
62   properties:
63     name: $components.lbvserver-comp.properties.name
64     servicegroupname: $components.svcg-comp.properties.servicegroupname
65 -
```

```
66   name: members-svcg-comp
67   type: ns::servicegroup_servicegroupmember_binding
68   repeat: $parameters.svc-servers
69   repeat-item: srv
70   properties:
71     ip: $srv
72     port: 80
73     servicegroupname: $components.svcg-comp.properties.servicegroupname
74   outputs:
75   -
76     name: lbvserver-comp
77     value: $components.lbvserver-comp
78     description: The component that builds the Nitro lbvserver
79                 configuration object
80   -
81     name: servicegroup-comp
82     value: $components.svcg-comp
83     description: The component that builds the Nitro servicegroup
84                 configuration object
85 <!--NeedCopy-->
```

StyleBook を使用して構成を作成するには、NetScaler ADM にインポートしてから使用する必要があります。詳しくは、「[ユーザー定義の StyleBook を使用する方法](#)」を参照してください。

この StyleBook を他の StyleBook にインポートして、そのプロパティを使用することもできます。詳しくは、次のセクションで説明します。

## 複合 **StyleBook** の作成

February 6, 2024

StyleBook の重要かつ便利な特徴の 1 つは、別の StyleBook の構築ブロックとして使用できる点です。StyleBook は別の StyleBook にインポートできます。その StyleBook は、Nitro に組み込まれている StyleBook と同様に、**2** つ目の **StyleBook** のコンポーネントで使用されるタイプと呼ぶことができます。

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、コンポジットサンプルという別の **StyleBook** を作成できます。「basic-lb-config」 StyleBook を使用するには、新しい StyleBook 内の `import-stylebooks` セクションで、この StyleBook をインポートする必要があります。

### StyleBook を構築する

新しい StyleBook は、次のようになります。

```
1 name: composite-example
2 namespace: com.example.stylebooks
3 version: "0.1"
```



```
4 display-name: Load Balancing Virtual Server (HTTP/RoundRobin)
5 description: This StyleBook defines a RoundRobin load balancing
  configuration with a monitor.
6 schema-version: "1.0"
7 import-stylebooks:
8   -
9     namespace: netscaler.nitro.config
10    version: "10.5"
11    prefix: ns
12   -
13     namespace: com.example.stylebooks
14    version: "0.1"
15    prefix: stlb
16 parameters:
17   -
18     name: name
19     type: string
20     label: Application Name
21     description: Give a name to the application configuration.
22     required: true
23   -
24     name: ip
25     type: ipaddress
26     label: Application Virtual IP (VIP)
27     description: The Application VIP that clients access
28     required: true
29   -
30     name: svc-servers
31     type: ipaddress[]
32     label: Application Server IPs
33     description: The IP addresses of all the servers of this
34     application
35     required: true
36   -
37     name: response-code
38     type: string[]
39     label: List of Response Codes
40     description: List of Response Codes - Provide a list of response
41     codes in integer.
42 components:
43   -
44     name: basic-lb-comp
45     type: stlb::basic-lb-config
46     description: This component's type is another StyleBook that builds
47     the NetScaler lbvserver, servicegroups and services
48     configuration objects.
49     properties:
50       name: $parameters.name
51       ip: $parameters.ip
52       svc-servers: $parameters.svc-servers
53   -
```

```

52     name: monit-comp
53     type: ns::lbmonitor
54     description: This component is a basic Nitro type (a Builtin
                    StyleBook) that builds the NetScaler monitor configuration
                    object.
55     properties:
56         monitorname: $parameters.name + "-mon"
57         type: HTTP
58         respcode: $parameters.response-code
59         httprequest: "'GET /'"
60         lrtm: ENABLED
61         secure: "YES"
62
63     components:
64         -
65         name: monit-svcgrp-bind-comp
66         type: ns::servicegroup_lbmonitor_binding
67         properties:
68             servicegroupname: $components.basic-lb-comp.outputs.
                                servicegroup-comp.properties.servicegroupname
69             monitor_name: $parent.properties.monitorname
70 <!--NeedCopy-->

```

import-stylebooks セクションで、名前空間とバージョンを指定して basic-lb-config StyleBook をインポートします。この StyleBook は、プレフィックス「stlb」で参照できます。

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設定を作成するために StyleBook で作成した StyleBook の名前です。このコンポーネントで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（必須とオプションの両方）を使用できます。lbserver、サービスグループ、サービスとサービスグループのバインディングを再構築する代わりに、これらすべてを行う StyleBook をコンポーネントとしてインポートし、それを使用して新しい StyleBook に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 monitor 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。このコンポーネントは、最初のコンポーネントで作成された servicegroup に monitor をバインドするバインド構成オブジェクトを作成する、サブコンポーネント「monit-svcgrp-bind-comp」も持っています。「**basic-lb-config**」StyleBook で作成されたサービスグループコンポーネントは出力として公開されるため、この StyleBook には **\$components.basic-lb-comp.outputs.servicegroup-comp** という表現を使用してアクセスできます。この例では、インポート先の StyleBook が、Outputs セクションを使用してインポート元の StyleBook のコンポーネントにアクセスする方法を示しています。この方法以外でアクセスすることはできません。

次に、StyleBook のコンテンツをコピーしてテキストエディターに貼り付け、そのファイルを **composite-example.yaml** として保存します。NetScaler ADM にファイルをインポートする前に、必ず YAML コンテンツを検証してください。次に、NetScaler ADM にインポートし、この StyleBook を使用して 1 つまたは複数の構成を作成します。

StyleBooks に組み込みの YAML バリデータを使用して、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** での **GUI** 属性の使用

February 6, 2024

StyleBook のパラメータセクションに GUI 属性を追加して、NetScaler Application Delivery Management (ADM) に表示されるフィールドを直感的に表示できます。

例。label 属性を使用してパラメーターにわかりやすい名前を追加し、description 属性を使用してこのパラメーターにツールチップを追加できます。

```
1 name: ip
2 label: Virtual Server IP Address
3 description: IP address of the virtual server that represents the load
  balanced application.
4 type: ipaddress
5 required: true
6 <!--NeedCopy-->
```

例。オブジェクト型のパラメータがある場合は、**gui** 属性を使用してレイアウトを定義できます。この例の場合、レイアウトは折りたたみ可能なオブジェクトで、フィールドが 2 列で表示されます。

```
1 name: svcg-advanced
2 label: Advanced Application Server Settings
3 type: object
4 required: false
5 gui:
6   collapse_pane: true
7   columns: 2
8 <!--NeedCopy-->
```

例。Citrix ADM の一部の StyleBook は、他の StyleBook の構成要素としてのみ使用されます。また、ユーザーがこれらの StyleBook から直接構成を作成しないようにすることもできます。これらの StyleBook は他の StyleBook の一部として使用されることになっているからです。StyleBook をプライベートとしてマークして、NetScaler ADM GUI で構成を作成するために StyleBook を直接使用しないようにします。

```
1 name: basic-lb-config
2 description: This stylebook defines a simple load balancing
  configuration.
3 display-name: Load Balancing Configuration
4 namespace: com.example.stylebooks
5 private: true
6 schema-version: "1.0"
7 version: "0.1"
8 <!--NeedCopy-->
```

## カスタム **StyleBook** をインポートする

February 6, 2024

StyleBook を構築したら、それを NetScaler Application Delivery Management (ADM) にインポートして使用する必要があります。NetScaler ADM では、単一の StyleBook を YAML 形式でインポートすることも、複数の StyleBookYAML ファイルを .zip、.tgz、または .gz 形式でバンドルとしてインポートすることもできます。NetScaler ADM システムは、インポート時に StyleBook を検証します。これで、StyleBook を使用して構成を作成する準備ができました。

NetScaler ADM には、StyleBook YAML コンテンツの作成に使用できる組み込みの YAML エディタもあります。YAML エディタを使用すると、NetScaler ADM GUI 自体から YAML 構造を検証できます。これらの検証チェックに個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 標準に照らして検証され、偏差が強調表示されます。その後、コンテンツを修正して、StyleBook を NetScaler ADM にインポートして試してみることができます。ビルトインの YAML エディターには、独自の StyleBook を作成する際に 2 つの利点があります。

- 色分けされています。エディタは、YAML ガイドラインに従って解析された StyleBook コンテンツを表示し、色分けを使用すると、YAML コンテンツで定義されているキーと値を簡単に区別するのに役立ちます。
- **YAML** 検証です。入力時にコンテンツが YAML エラーに対して検証され、偏差が即座に強調表示されます。この検証により、ADM に StyleBook をインポートする前でも、YAML ガイドラインに準拠したテキストを作成できます。

注:

現在、エディタは YAML ガイドラインに従ってコンテンツを検証します。コードの正確性と誤植は検証されません。

### StyleBook をインポートするには

1. NetScaler ADM で、[アプリケーション] > [構成] > [**StyleBook**] の順に選択し、[新しい **StyleBook** のインポート] をクリックします。
2. StyleBook をインポートするには、次のオプションのいずれかをクリックします。
  - ファイル - ローカルストレージから必要なファイルまたはファイルのバンドルを選択します。

注:

この例では、`lb-vserver.yml` StyleBook で作成した **StyleBook** をインポートして、**負荷分散仮想サーバー**を作成します。

**Import StyleBook**

File
  Bundle
  Raw
  Sync Repository

Choose a YAML StyleBook file.

Choose File ▾ lb-server.yml

Include an icon for the StyleBook

Create Close

- バンドル -NetScaler ADM では、複数の StyleBook を YAML 形式でインポートできます。zip (.zip) 形式または tarball (.tgz、.gz) 形式で圧縮された複数の YAML StyleBook ファイルをインポートできます。

**Import StyleBook**

File
  Bundle
  Raw
  Sync Repository

Choose zip (.zip) or tarball file (.tgz, .gz) bundle that includes multiple StyleBook YAML files.

Choose File ▾ StyleBooks-yaml.zip

Include an icon for the StyleBook

Create Close

バンドル内の各 StyleBook にアイコンを追加できるようになりました。PNG、GIF、または JPEG 形式のアイコンを含むリソースフォルダがあることを確認します。アイコンファイル名が StyleBook 名と一致する場合、アイコンは自動的に StyleBook にマッピングされます。それ以外の場合は、次の操作を行います。

- リソースフォルダに `icon_mapping.json` ファイルを追加します。
- `icon_mapping.json` ファイル内の StyleBooks とアイコンを次のようにマップします。

```

1 <StyleBook file name> : <icon file name>
2 <!--NeedCopy-->

```

StyleBook バンドルの例を次に示します。

| Name            | Type          | Compressed size | Password ... | Size | Ratio | Date modified    |
|-----------------|---------------|-----------------|--------------|------|-------|------------------|
| resources       | File folder   |                 |              |      |       | 29-07-2020 07:25 |
| .DS_Store       | DS_STORE File | 1 KB            | No           | 7 KB | 92%   | 18-08-2020 17:31 |
| exchange.yaml   | YAML File     | 2 KB            | No           | 6 KB | 78%   | 31-07-2020 11:37 |
| sharepoint.yaml | YAML File     | 1 KB            | No           | 1 KB | 56%   | 29-07-2020 10:13 |
| skype.yaml      | YAML File     | 1 KB            | No           | 1 KB | 55%   | 29-07-2020 10:13 |

resources フォルダには、必要なアイコンが含まれています。

| Name              | Type          | Compressed size | Password ... | Size | Ratio | Date modified    |
|-------------------|---------------|-----------------|--------------|------|-------|------------------|
| .DS_Store         | DS_STORE File | 1 KB            | No           | 7 KB | 96%   | 29-07-2020 11:55 |
| exch.png          | PNG File      | 3 KB            | No           | 3 KB | 0%    | 29-07-2020 07:20 |
| icon_mapping.json | JSON File     | 1 KB            | No           | 1 KB | 7%    | 29-07-2020 07:28 |
| sharepoint.jpeg   | JPEG File     | 4 KB            | No           | 4 KB | 9%    | 29-07-2020 07:19 |
| skype.png         | PNG File      | 7 KB            | No           | 7 KB | 1%    | 29-07-2020 07:20 |

この例では、sharepoint.yaml および skype.yaml ファイルはそれぞれ sharepoint.jpeg および skype.png に自動的にマップされます。

exchange.yaml を exch.png にマッピングするには、icon\_mapping.json ファイルに次のように指定します。

```

1  {
2
3  "exchange.yaml": "exch.png"
4  }
5
6  <!--NeedCopy-->
```

defaulticon エントリを指定すると、StyleBook は別のアイコンにマップされない限り、デフォルトのアイコンにマップされます。

```

1  defaulticon: <icon file name>
2  <!--NeedCopy-->
```

アプリケーション／**StyleBooks** では、インポートされた StyleBook がマップされたアイコンとともに表示されます。

- **Raw** -YAML エディタで StyleBook のコンテンツを作成します。

StyleBook のコンテンツを検証して、StyleBook の文法エラーをチェックできます。StyleBook のコンテンツを検証するには、「コンテンツを検証」をクリックします。

注:

StyleBook を作成する際には、次の概念を必ず理解してください。

- NITRO API
- YAML

独自の StyleBook を作成する方法については、「[独自の StyleBook を作成する方法](#)」を参照してください。

```
1 name: lb-vserver
2 namespace: com.example.stylebook
3 version: "1.0"
4 display-name: Load Balancing Virtual Server (HTTP)
5 description: "This stylebook defines a very simple load balancing HTTP virtual server configuration"
6 schema-version: "1.0"
7
8 import-stylebooks:
9 -
10   namespace: netscaler.nitro.config
11   version: "10.5"
12   prefix: ns
13 -
14   namespace: com.citrix.adc.stylebooks
15   version: "1.0"
16   prefix: stlb
17
18 #####
```

- リポジトリを同期 -このオプションは、ADM に追加されたリポジトリを一覧表示します。ADM と同期するリポジトリを選択します。

注:

StyleBook YAML ファイルから YAML エディタにコンテンツをコピーして貼り付けることもできます。

3. 必要に応じて、StyleBook のアイコンを選択します。

アプリケーション/**StyleBook** では、インポートされた StyleBook がこのアイコンとともに表示されます。

4. [作成] をクリックします。

NetScaler ADM は、StyleBook の文法に従って、すべての構文エラーと意味エラーについて StyleBook を検証するようになりました。エラーが発生した場合、StyleBook は NetScaler ADM にインポートされません。

エラーがなければ、StyleBook は正常にインポートされ、**StyleBooks** ページに表示されます。StyleBook のヘッダーセクションで定義した表示名で StyleBook を識別できます。

注:

ファイルのバンドルをインポートする場合、NetScaler ADM は圧縮されたフォルダーを解凍し、すべ

ての StyleBook を検証します。

1 つの StyleBook ファイルが検証テストに失敗しても、バンドルはインポートされません。

StyleBook の文法と、さまざまな構文と属性の構文について詳しくは、「[StyleBook 文法](#)」を参照してください。

5. この **StyleBook** から構成を作成するには、「構成の作成」リンクをクリックします。

StyleBook がユーザーインターフェイスページとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。

6. パラメーターに必要な値を指定します。

次の例では、

- a) アプリケーション名とロードバランサの **IP** アドレスの必須フィールドを指定します。
- b) リストから [ 負荷分散アルゴリズム ] を選択します。デフォルトでは **ROUNDROBIN** が選択されています。

7. [ターゲットインスタンス] で、構成を展開する NetScaler ADC インスタンスの IP アドレスを選択します。

ターゲットインスタンスを必要な数だけ指定して、複数の NetScaler ADC で構成を展開することもできます。

8. 構成を展開する前に、NetScaler ADC (NITRO) 構成オブジェクトをテストする場合は、[ドライ実行] をクリックします。

構成が有効な場合、設定オブジェクトは指定された値に基づいて作成されます。

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。この負荷分散サーバーは、この基本的な例 StyleBook で定義されている唯一のコンポーネントでした。

その後、[作成] をクリックして、選択した NetScaler ADC インスタンスに構成を展開します。

構成を正常に展開すると、[構成] ページに新しい構成パックが表示されます。

#### 注

更新アイコンをクリックして、NetScaler ADM で最近検出された NetScaler ADC 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。

## カスタム **StyleBook** の検索

Citrix ADM では、タイプに基づいて StyleBook を検索できるようになりました。つまり、デフォルトの StyleBook またはカスタム StyleBook のいずれかを検索できるようになりました。このオプションは、多数のデフォルト StyleBook の中からユーザー定義の StyleBook を検索する必要がある場合に特に便利です。



カスタム **StyleBook** を検索するには

1. NetScaler ADM で、[アプリケーション] > [構成] > [**StyleBook**] に移動します。
2. 右上にある検索アイコンをクリックします。
3. 検索バーで、[種類] を選択し、サブリストから [カスタム] を選択します。
4. NetScaler ADM では、ユーザー定義の StyleBook のみが表示されます。

## 構成パックを作成および編集する

February 6, 2024

NetScaler Application Delivery Management (ADM) では、StyleBook から構成パックを作成できます。また、構成パックは、作成元の StyleBook に関連付けられています。構成パックへの更新は、それが結び付けられている StyleBook を通じて行われます。

### 構成パックを作成する

StyleBook から構成パックを作成するには、次の手順に従います。

1. [アプリケーション] > [**StyleBooks**] > [構成] に移動します
2. [追加] をクリックします。
3. 「**StyleBooks**」で、構成パックを作成する必要な StyleBook を選択します。

このページでは、StyleBook をデフォルトとカスタム StyleBook に分類しています。それぞれのタブを選択して、必要な StyleBook を見つけます。

4. 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、ある StyleBook から別の StyleBook によって異なります。

5. [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 ADC に構成を展開できます。

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 ADC インスタンスから作成、変更、または削除されるオブジェクトが表示されます。

7. [作成] をクリックします

構成パックは、**StyleBook > [構成]** ページに表示されます。

既存の構成パックを編集する場合は、構成パックを選択して [編集] をクリックします。

### 構成パックの **StyleBook** を変更する

機能を追加したり、問題を解決したりするために、StyleBook を更新する必要がある場合があります。古い StyleBook を使用して構成パックをすでに作成している場合は、新しい更新された StyleBook を使用するように構成パックを更新することができます。新しい StyleBook を使用するには、構成パックの既存の StyleBook を変更します。

ADC インスタンスに基本的なロードバランサー設定をデプロイする 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設定でモニターを構成する場合は、新しい StyleBook が必要です。したがって、基本的なロードバランサー設定とともにモニターを構成する機能を含む、例 **lb-mon StyleBook** を作成します。

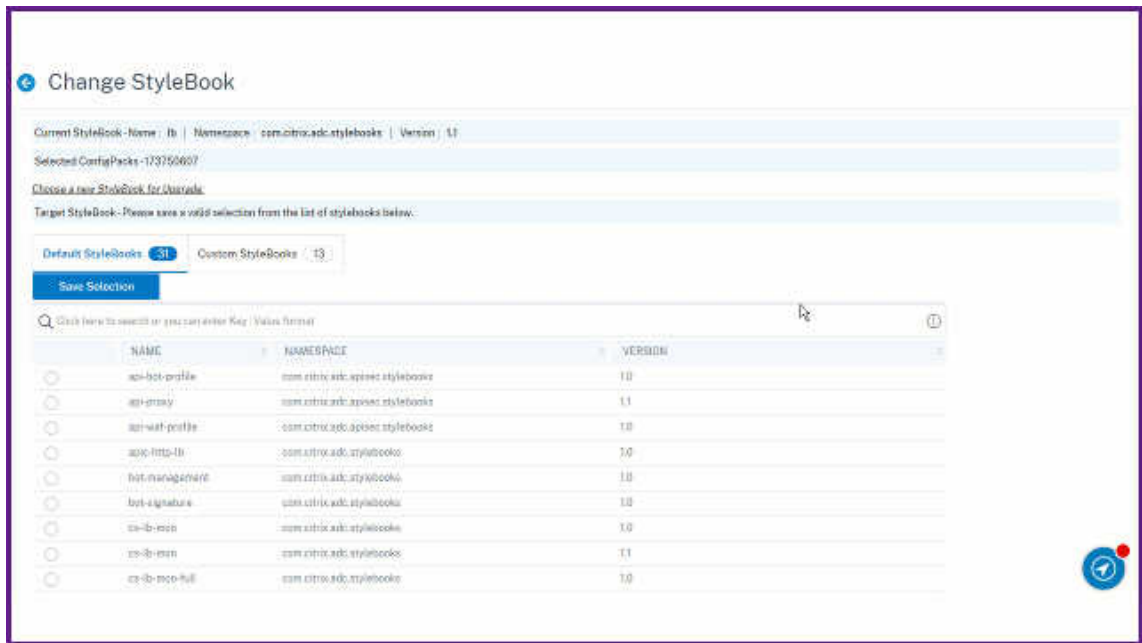
StyleBook を作成したら、既存の構成パック CP1 を更新してモニターを追加します。これを行うには、次の手順を実行します：

1. [アプリケーション] > [StyleBooks] > [構成] に移動します
2. 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. 「**StyleBook** の変更」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、[選択を保存] をクリックします。
5. [変更] 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。

構成パックの StyleBook を変更すると、新しい StyleBook のパラメータが既存の StyleBook とは異なる構造になることがあります。パラメータ構造が以前の StyleBook に似ている場合、パラメータの値はそれぞれのフィールドに自動的に保持されます。それ以外の場合は、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。たとえば、同じパラメータ名、タイプ、パラメータの親など。



新しい StyleBook に新しい必須パラメータを追加する場合は、StyleBook を変更した後、そのようなパラメータの値を手動で指定する必要があります。

この例では、**example-lb** StyleBook の設定ページに表示されるパラメータは次のとおりです：

This configuration was created from the StyleBook 'example-lb' (namespace: 'examples.stylebooks', version: '1.0').

Load Balanced Application Name  
example-lb-server-app

Load Balanced App Virtual IP address\*  
192 . 10 . 10 . 10

Load Balanced App Virtual Port  
80

Load Balanced App Protocol  
HTTP

Advanced Load Balancer Settings

Application Server Protocol\*  
HTTP

**Server IPs and Ports** +

| Application Server IP Address | Application Server Port |
|-------------------------------|-------------------------|
| No items                      |                         |

**Application Servers FQDN names** +

| Application Server Domain Name | Application Server Port |
|--------------------------------|-------------------------|
| No items                       |                         |

Advanced Application Server Settings

**SSL Certificate Settings** +

| Certificate Name | CertKey Format | Certificate Key Name | Private Key Password |
|------------------|----------------|----------------------|----------------------|
| No items         |                |                      |                      |

**Target Instances**

10.102.29.60 > +

新しい **example-lb-mon StyleBook** の設定ページに表示されるパラメーターは次のとおりです:

This configuration was created from the StyleBook 'example-lb-mon' (namespace: 'examples.stylebooks', version: '1.0').

Load Balanced Application Name

Load Balanced App Virtual IP address\*

Load Balanced App Virtual Port

Load Balanced App Protocol

Advanced Load Balancer Settings

Application Server Protocol\*

**Server IPs and Ports**

| Application Server IP Address | Application Server Port |
|-------------------------------|-------------------------|
| No items                      |                         |

**Application Servers FQDN names**

| Application Server Domain Name | Application Server Port |
|--------------------------------|-------------------------|
| No items                       |                         |

Advanced Application Server Settings

**SSL Certificate Settings**

| Certificate Name | CertKey Format | Certificate Key Name |
|------------------|----------------|----------------------|
| No items         |                |                      |

**List of Monitors**

| Monitor Name | Monitor Type | Destination IP | Destination P | HTTP Request | Send String | Custom HTTP |
|--------------|--------------|----------------|---------------|--------------|-------------|-------------|
| No items     |              |                |               |              |             |             |

**Target Instances**

 > +

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、StyleBooks は基本的なロードバ

ランサー設定の古い値を保持します。そして、それは新しいパラメータだけを追加します。モニタパラメータの場合は、必要な値を手動で指定します。

6. [ターゲットインスタンス] で、選択したインスタンスを確認し、必要に応じてリストを更新します。
7. [ドライラン] をクリックします。

[オブジェクト] ページには、NetScaler ADC インスタンスから作成、変更、または削除されるオブジェクトが表示されます。

8. [OK] をクリックします。

「**StyleBook**」 > 「構成」 ページの「**StyleBook 名**」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。

#### 複数の構成パックがある **StyleBook** を変更する

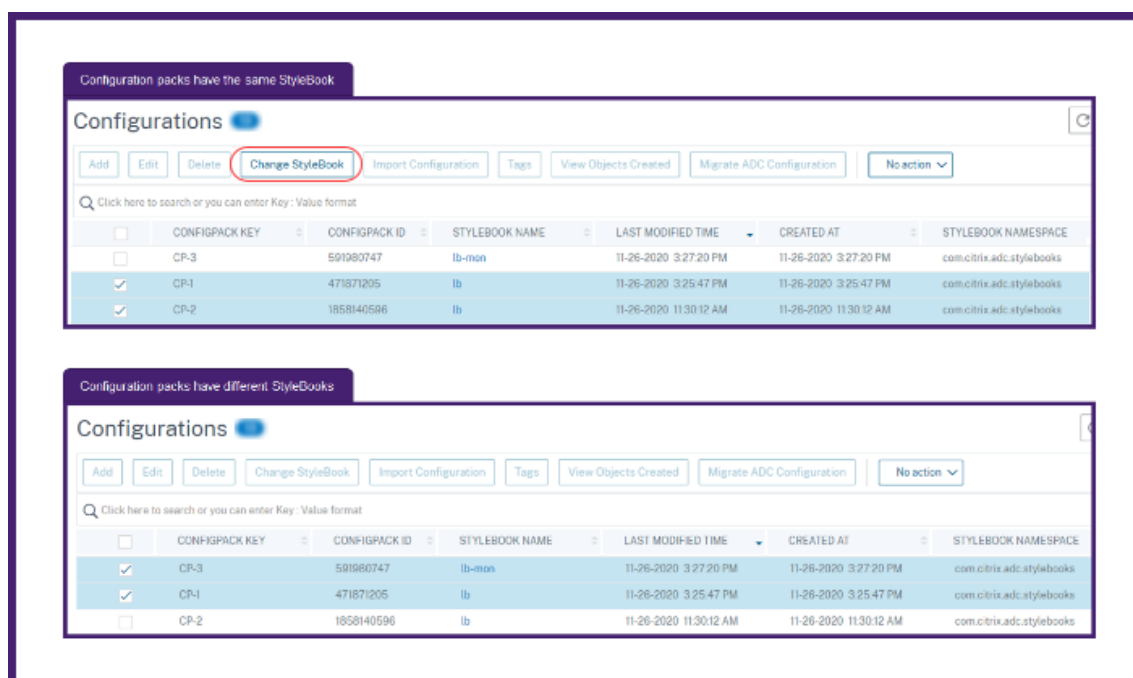
複数の構成パックを含む既存の StyleBook を変更する場合は、次の操作を行います。

1. 新しい StyleBook を ADM にインポートします。

通常、新しい StyleBook の名前と名前空間は、既存の StyleBook よりも高いバージョンを持ちます。ただし、名前、名前空間、またはバージョンが異なる場合は、この手順を省略できます。

2. 既存の StyleBook に関連付けられている構成パックの StyleBook を変更します。

選択した構成パックが同じ StyleBook に関連付けられている場合にのみ、**StyleBook** の変更を選択できません。



選択した構成パックについて、次の条件が満たされると、ADM は StyleBook を正常に変更します。

- 既存の StyleBook の設定パラメータはすべて、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、[構成] ページの【進行中/失敗】の [構成] を選択します。

|                          | CONFIGPACK KEY | CONFIGPACK ID | STATUS | STYLEBOOK NAME | TARGET INSTANCE(S) | LAST MODIFIED TIME    |
|--------------------------|----------------|---------------|--------|----------------|--------------------|-----------------------|
| <input type="checkbox"/> | ss             | 421101391     | failed | ss_stylebook   | 10.106.97.146      | 5-14-2020 11:47:56 PM |

3. すべての構成パックを新しい StyleBook に関連付けたら、古い StyleBook を ADM から削除します。

### 構成パックのエクスポートまたはインポート

StyleBooks のような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 設定を別の ADM サーバーに簡単に共有できます。構成パックをエクスポートすると、**tgz**または**zip**バンドルがローカルコンピュータ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たすべてのパラメーターを含む JSON ファイルが含まれます。

### 設定のエクスポート

構成パックをエクスポートするには、次の手順を実行します。

1. [アプリケーション] > [StyleBooks] > [構成] に移動します
2. エクスポートする構成パックを選択します。
3. 「アクションの選択」で、「構成のエクスポート」を選択します。

|                                     | CONFIGPACK KEY | CONFIGPACK ID | STYLEBOOK NAME | TARGET INSTANCE(S) | LAST MODIFIED TIME     | MODIFIED BY | CI |
|-------------------------------------|----------------|---------------|----------------|--------------------|------------------------|-------------|----|
| <input type="checkbox"/>            |                |               |                |                    | 10-1-2020 6:27:13 PM   | nsroot      | n  |
| <input type="checkbox"/>            |                |               |                |                    | 10-13-2020 7:58:46 PM  | nsroot      | n  |
| <input checked="" type="checkbox"/> |                |               |                |                    | 10-20-2020 11:08:32 AM | nsroot      | n  |

4. [構成のエクスポート] ペインで、次の項目を指定します。

- 設定がデプロイされるターゲットインスタンス情報: エクスポートバンドルにターゲットインスタンスの情報を含めるには、このオプションを選択します。

- 設定に関連付けられた **StyleBook**: StyleBook をエクスポートバンドルに含めるには、このオプションを選択します。
- 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、構成パックの機密データを保護します。
- 圧縮ファイルの種類: **ZIP** または **TGZ** ファイルタイプを選択します。

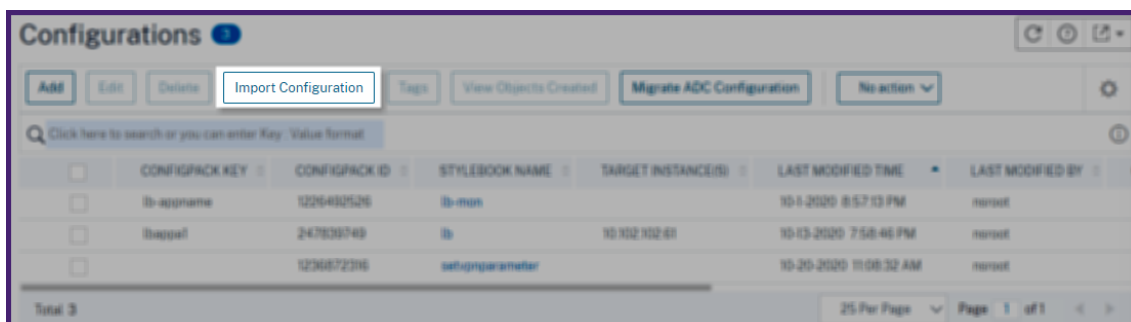
5. [エクスポート] をクリックします。

エクスポートバンドルをローカルコンピューターに保存します。

#### 構成をインポート

ローカルコンピューターから別の ADM サーバーに構成パックをインポートできます。構成パックをインポートするには、次の手順を実行します。

1. [アプリケーション] > [StyleBooks] > [構成] に移動します
2. [構成のインポート] を選択します。





3. コンピュータ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、[ **ADC** にすべての設定オブジェクトが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。

このオプションでは、ADC インスタンスにすでに作成されているオブジェクトは変更されません。

同じ ADC インスタンスを 2 つの ADM サーバに追加したとします。また、ある ADM サーバから別のサーバへ構成パックを移行する場合。このオプションは、ADC インスタンス上の設定オブジェクトを変更せずに構成パックをインポートする場合に使用します。

**重要:**

このオプションを使用するには、指定された設定バンドルにターゲットインスタンス情報が含まれていることを確認してください。「設定のエクスポート」を参照してください。

このオプションは、すべてのオブジェクトがターゲットインスタンスに存在する場合のみ、設定を移行します。

6. [インポート] をクリックします。

構成パックをインポートすると、ADM は次のことを検証します。

- 関連した **StyleBook**: 関連する StyleBook が ADM がない場合、StyleBook を構成パックとともにインポートします。
- ターゲットインスタンス: ターゲットインスタンスをチェックし、指定したターゲットインスタンスに設定をデプロイします。上記の ADC インスタンスが ADM 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

スなしでインポートされます。

- ソース **ADM**: 同じ ADM サーバー上に構成パックをインポートする場合、選択したバンドルによって既存の構成パックが更新されます。

## StyleBook を構築する

**example-lb** StyleBook の全コンテンツは、以下の参照用に提供されています。

```
1 name: example-lb
2 namespace: examples.stylebooks
3 version: "1.0"
4 display-name: Basic Load Balancer App
5 description: This is an example StyleBook that creates a load balancer
  application
6 schema-version: "1.0"
7 import-stylebooks:
8   -
9     namespace: com.citrix.adc.stylebooks
10    prefix: stlb
11    version: "1.0"
12 parameters-default-sources:
13   - stlb::lb
14 components:
15   -
16     name: lb-comp
17     type: stlb::lb
18     description: Uses the default lb StyleBook to build the typical lb
      configuration objects
19     properties-default-sources:
20      - $parameters
21 <!--NeedCopy-->
```

**example-lb-mon** StyleBook の全コンテンツは、参照用に次のように提供されます。

```
1 name: example-lb-mon
2 namespace: examples.stylebooks
3 version: "1.0"
4 description: This is an example StyleBook that creates a load balancer
  application with monitors
5 display-name: Basic Load Balancer App with Monitors
6 schema-version: "1.0"
7 import-stylebooks:
8   -
9     namespace: netscaler.nitro.config
10    prefix: ns
11    version: "10.5"
12   -
13     namespace: com.citrix.adc.stylebooks
14     prefix: stlb
15     version: "1.0"
16   -
```

```
17     namespace: com.citrix.adc.commontypes
18     prefix: cmtypes
19     version: "1.0"
20 parameters-default-sources:
21   - stlb::lb
22 parameters:
23   -
24     name: monitors
25     label: "List of Monitors"
26     description: "List of Monitors to monitor Application Servers"
27     type: cmtypes::monitor[]
28 substitutions:
29   mon-name(appname, monname): $appname + "-mon-" + $monname
30 components:
31   -
32     name: lb-comp
33     type: stlb::lb
34     description: Uses the default lb StyleBook to build the typical lb
35                 configuration objects
36     properties-default-sources:
37       - $parameters
38     name: monitors-comp
39     type: cmtypes::monitor
40     condition: $parameters.monitors
41     repeat: $parameters.monitors
42     repeat-item: mon
43     repeat-index: ndx
44     description: Builds a list of Citrix ADC monitor objects and binds
45                 them to the servicegroup of this LB config
46     properties-default-sources:
47       - $mon
48     properties:
49       monitorname: $substitutions.mon-name($parameters.lb-appname,
50         $mon.monitorname)
51     components:
52       -
53         name: monitor-svcg-binding-comp
54         condition: $parameters.svc-servers
55         type: ns::servicegroup_lbmonitor_binding
56         properties:
57           servicegroupname: $components.lb-comp.outputs.servicegroup.
58             properties.servicegroupname
59           monitor_name: $parent.properties.monitorname
60 <!--NeedCopy-->
```

## NetScaler ADM にファイルをアップロードする **StyleBook** を作成する

February 6, 2024

Citrix Application Delivery Management (Citrix ADM) StyleBooks を使用すると、Citrix ADM GUI または API を使用して、ローカルファイルシステムから Citrix ADC 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、とりわけ含めることができる Citrix ADC 構成を作成できます。これらのファイルは、証明書ファイルの例でも位置情報ファイルでもかまいません。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 の設定

以下は、NetScaler ADC インスタンスに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、地理的位置に基づいて静的近接を定義するために、GSLB 設定で通常使用されます。

## StyleBook の作成 -1

```
1 name: upload-geolocations
2 namespace: com.citrix.adc.stylebooks.samples
3 version: "1.0"
4 display-name: GeoLocation File Upload
5 description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
6 schema-version: "1.0"
7
8 import-stylebooks:
9 -
10 namespace: netscaler.nitro.config
11 version: "11.1"
12 prefix: ns
13
14 parameters:
15 -
16 name: locationfile
17 label: Location File
18 description: The system file path of the geolocation file on Citrix
   ADM
19 type: file
20 required: true
21
22 components:
23 -
24 name: upload-file-comp
25 type: ns::systemfile
26 properties:
27     filename: $parameters.locationfile.filename
28     filelocation: "/var/netscaler/inbuilt_db/"
29     filecontent: base64.encode($parameters.locationfile.contents)
30 <!--NeedCopy-->
```

**注:**

この例で使用されているパラメータはタイプファイルのものです。この StyleBook を NetScaler ADM にインポートして、ジオロケーションファイルをアップロードできます。

この StyleBook では、ファイルが Citrix ADM にすでに存在している必要があります（たとえば、scp などのユーティリティを使用して Citrix ADM に既にコピーしているはずです）。

NetScaler ADM ファイルシステムにファイルをコピーせずに、NetScaler ADM 経由で NetScaler ADC にファイルをアップロードする場合は、2つの「文字列」パラメータを持つ StyleBook を構築できます。1つは NetScaler ADC で使用するファイル名を指定し、もう1つは NetScaler ADC の内容を指定するものです。ファイルを作成し、upload-file-comp コンポーネントでこれら2つのパラメータを使用します。以下は、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 を構築する-2**

```
1 name: upload-geolocations-alt
2 namespace: com.citrix.adc.stylebooks.samples
3 version: "1.0"
4 display-name: GeoLocation File Upload
5 description: This StyleBook is used to upload a geolocation file to
6   Citrix ADC
7 schema-version: "1.0"
8
9 import-stylebooks:
10 -
11   namespace: netscaler.nitro.config
12   version: "11.1"
13   prefix: ns
14
15 parameters:
16 -
17   name: filename
18   label: Location Filename
19   description: The name of the location file on the Citrix ADC
20   type: string
21   required: true
22 -
23   name: filecontents
24   label: Location File Contents
25   description: The contents of the location file
26   type: string
27   required: true
28
29 components:
30 -
31   name: upload-file-comp
32   type: ns::systemfile
33   properties:
34     filename: $parameters.filename
```

```
34     filelocation: "/var/Citrix ADC/inbuilt_db/"
35     filecontent: base64.encode($parameters.filecontents)
36 <!--NeedCopy-->
```

### 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、選択した NetScaler ADC インスタンスに、上記の最初の StyleBook を使用して位置情報ファイルをアップロードする構成を作成します。

ファイルをアップロードするための設定を作成するには：

1. NetScaler ADM で、[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。「StyleBook の選択」ページには、NetScaler ADM で使用できるすべての StyleBook が表示されます。下方向にスクロールして、インポートした StyleBook を選択します。

StyleBook パラメーターは、この StyleBook で定義されているすべてのパラメーターの値を入力できるユーザーインターフェイスページとして表示されます。

2. ロードバランサーの基本設定セクションに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. [ロケーションファイル] 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

： Citrix ADM では、ファイルが現在のテナントのフォルダーのみにあることを確認してください。任意のファイル転送プロトコルを使用して、Citrix ADM ファイルシステムにファイルをコピーします。

4. ターゲットインスタンスにアクセスする前に、ユーザー認証情報を入力するように求められる場合があります。
5. 構成を作成する対象の NetScaler ADC インスタンスを選択し、[作成] をクリックします。

#### 注：

インスタンスで実際の構成を実行する前に、[Dry Run] を選択して、ターゲットインスタンス上に作成された構成オブジェクトをチェックすることをお勧めします。

構成パックが正常に作成されると、ファイルは NetScaler ADC インスタンスファイルシステムの `/var/netscaler/inbuilt_db/` という場所に保存されます。

#### 注

更新アイコンをクリックして、NetScaler ADM で最近検出された NetScaler ADC 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 ADM API を使用した構成パックの作成

NetScaler ADM API を使用して、選択した NetScaler ADC インスタンスにファイルをアップロードする構成パックを作成することもできます。API の使用方法の詳細については、「[API を使用して任意のファイルタイプをアップロ](#)

ードする構成を作成する方法」を参照してください。

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

February 6, 2024

SSL プロトコルを使用する StyleBook の構成を作成する場合、SSL 証明書ファイルと証明書キーファイルを StyleBook パラメーターの要求に応じてアップロードする必要があります。StyleBook では、NetScaler ADM GUI を使用して、SSL ファイルとキーファイルをローカルシステムから直接アップロードできます。NetScaler ADM API を使用して、NetScaler ADM によってすでに管理されている証明書ファイルとキーファイルをアップロードすることもできます。

### StyleBook の設定

このドキュメントは、**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た独自の **StyleBook-負荷分散仮想サーバー (SSL)** を作成するのに役立ちます。ここで例として提供している StyleBook は、選択した NetScaler ADC 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ーを選択し、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、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 NetScaler ADM に存在します。これらは下記のとおり、「parameters」セクションで指定されます。

```
1 parameters:
2 -
3   name: name
4   type: string
5   required: true
6 -
7   name: ip
8   type: ipaddress
9   required: true
10 -
11  name: lb-alg
12  type: string
13  allowed-values:
14    - ROUNDROBIN
15    - LEASTCONNECTION
16  default: ROUNDROBIN
17 -
18  name: certificate
19  label: "SSL Certificate File"
```

```

20   description: "The file name of the SSL certificate file"
21   type: certfile
22   -
23   name: key
24   label: "SSL Certificate Key File"
25   description: "The file name of the server certificate's private key
                file"
26   type: keyfile
27   <!--NeedCopy-->

```

下記のとおり、StyleBook のコンポーネントセクションに 2 つのコンポーネントが作成されます。「my-lbvserver-comp」コンポーネントのタイプは ns::lbvserver 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 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、同じ名前の Citrix ADC NITRO 負荷分散仮想サーバーリソースに対応します。

2 番目のコンポーネント「lbvserver-certificate-comp」は 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た、名前空間「com.citrix.adc.stylebooks」バージョン 1.0 を参照します。名前空間「com.citrix.adc.stylebooks」がフォルダーと考えることができるのであれば、「vserver-certs-binds」はフォルダー中の他の StyleBook（またはファイル）です。名前空間「com.citrix.adc.stylebooks」にある StyleBook は、NetScaler ADM の一部として出荷されます。

ユーザー定義の StyleBook で使用される「vserver-certs-binds」StyleBook を使用すると、証明書とキーファイルをターゲットの NetScaler ADC 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ことによって、証明書を簡単に構成できます。このコンポーネントのプロパティは、lb 仮想サーバーの名前と、構成パックの作成時に提供する SSL 証明書の名前です。

```

1  components:
2  -
3    name: my-lbvserver-comp
4    type: ns::lbvserver
5    properties:
6      name: $parameters.name
7      servicetype: SSL
8      ipv46: $parameters.ip
9      port: 443
10     lbmethod: $parameters.lb-alg
11  -
12     name: lbvserver-certificate-comp
13     type: stlb::vserver-certs-binds
14     description: Binds lbvserver with server certificate
15     properties:
16       vserver-name: $components.my-lbvserver-comp.properties.name
17       certificates:
18         -
19           cert-name: $parameters.name + "-lb-cert"
20           cert-file: $parameters.certificate
21           ssl-inform: PEM

```



```
22     key-name: $parameters.name + "--key"  
23     key-file: $parameters.key  
24 <!--NeedCopy-->
```

API を使ってこういった StyleBook から構成を作成する場合は、ファイル名だけを使うようにしてください（フルファイルパスではなく）。これらのファイルは、NetScaler ADM の証明書フォルダーとキーファイルフォルダーに既にあるはずで、アップロードされた SSL 証明書ファイルは、NetScaler ADM の /var/mps/tenants/… に保存されます。ns\_ssl\_certs ディレクトリで、SSL 証明書キーファイルは /var/mps/tenants/… に保存されています。NetScaler ADM の /ns\_ssl\_keys ディレクトリ。

### SSL ファイルをアップロードするための構成の作成

以下の手順では、上記で指定した StyleBook の SSL プロトコルを使用して、選択した NetScaler ADC インスタンス上に基本的な負荷分散仮想サーバー構成を作成します。この手順を使用して、NetScaler ADM で 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構成を作成するには

1. NetScaler ADM で、[アプリケーション] > [構成] > [StyleBook] に移動します。StyleBook ページには、Citrix ADM で利用できるすべての StyleBook が表示されます。
2. 下にスクロールして [負荷分散仮想サーバー (SSL)] を選択するか、検索フィールドに「負荷分散仮想サーバー (SSL)」と入力して **Enter** キーを押します。
3. StyleBook パネルで「設定を作成」リンクをクリックします。  
  
StyleBook パラメーターは、この StyleBook で定義されているすべてのパラメーターの値を入力できるユーザーインターフェイスページとして表示されます。
4. ロードバランサーの基本設定セクションに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 証明書の設定セクションで、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。または、NetScaler ADM 自体にあるファイルを選択することもできます。
6. 構成を作成する対象の NetScaler ADC インスタンスを選択し、[作成] をクリックします。

注:

更新アイコンをクリックして、NetScaler ADM で最近検出された NetScaler ADC 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。

Citrix ADM では、Citrix ADM の一部として付属している次のデフォルトの 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 負荷分散 StyleBook (lb)
- HTTP/SSL 負荷分散 (監視あり) StyleBook (lb-mon)

- HTTP/SSL コンテンツスイッチアプリケーション（監視あり）（cs-lb-mon）
- CS、LB、および SSL 機能を使ったサンプルアプリケーション StyleBook（sample-cs-app）

上記の StyleBook で説明されたものと同じ方法で SSL 証明書を使用する、ご自身の StyleBook を作成することも可能です。

## StyleBook を構築する

lb-vserver-ssl.yaml ファイルのすべての内容を次に示します。

```
1 name: lb-vserver-ssl
2 description: "This stylebook defines a load balancing virtual server
3   configuration."
4 display-name: "Load Balancing Virtual Server (SSL)"
5 namespace: com.example.ssl.stylebooks
6 schema-version: "1.0"
7 version: "0.1"
8
9 import-stylebooks:
10 -
11   namespace: netscaler.nitro.config
12   prefix: ns
13   version: "10.5"
14 -
15   namespace: com.citrix.adc.stylebooks
16   prefix: stlb
17   version: "1.0"
18
19 parameters:
20 -
21   name: name
22   type: string
23   required: true
24 -
25   name: ip
26   type: ipaddress
27   required: true
28 -
29   name: lb-alg
30   type: string
31   allowed-values:
32     - ROUNDROBIN
33     - LEASTCONNECTION
34   default: ROUNDROBIN
35 -
36   name: certificate
37   label: "SSL Certificate File"
38   description: "The file name of the SSL certificate file"
39   type: certfile
40 -
41   name: key
```

```
41  label: "SSL Certificate Key File"
42  description: "The file name of the server certificate's private key
43  file"
44  type: keyfile
45  components:
46  -
47    name: my-lbvserver-comp
48    type: ns::lbvserver
49    properties:
50      name: $parameters.name
51      servicetype: SSL
52      ipv46: $parameters.ip
53      port: 443
54      lbmethod: $parameters.lb-alg
55  -
56  name: lbvserver-certificate-comp
57  type: stlb::vserver-certs-binds
58  description: Binds lbvserver with server certificate
59  properties:
60    vserver-name: $ components.my-lbvserver-comp.properties.name
61    certificates:
62    -
63      cert-name: $parameters.name + "-lb-cert"
64      cert-file: $parameters.certificate
65      ssl-inform: PEM
66      key-name: $parameters.name + "-key"
67      key-file: $parameters.key
68  <!--NeedCopy-->
```

### NetScaler ADM API を使用した構成パックの作成

NetScaler ADM API を使用して、選択した NetScaler ADC インスタンスに証明書ファイルとキーファイルをアップロードする構成パックを作成することもできます。API の使用方法の詳細については、「[API を使用して 証明書とキーファイルをアップロードするための設定を作成する方法](#)」を参照してください。

### NetScaler ADC インスタンスに定義されているオブジェクトの表示

NetScaler ADM で StyleBook 構成パックを作成したら、[作成されたオブジェクトの表示] をクリックして、ターゲットの NetScaler ADC インスタンスで作成されたすべての NetScaler ADC オブジェクトを表示します。

Objects

Objects Added on Instance : 10.102.29.200

Type : lbvserver

ipv46 : 10.10.10.1  
 lbmethod : ROUNDROBIN  
 name : vsrver-1  
 port : 80  
 servicetype : SSL

Type : systemfile

filecontent :  
 LS0tLS1CRUdJTiBDRVJUSUZQOFURS0tLS0tck1JSUMzakNDQWtiZ0F3SUJBZ0lCQURBTkja3Foa2IHOXcwQkFrc0ZBREEVTVFzd0NRWURWUWFHRXdkVlV6RUwKUFrR0EXVUVDQk1D  
 WTJFeEV6QVJZC05WQkFjVENuTmhbljowWTJ4aGNTXhEakFNQmdOVk1RCV0Z3Y0d4bApNQjRFRFRMU1ERXhOekEYtURZMU5Gb1hEVEUyTURFeE56QTJNRFRkTKZvd1B6RUxN  
 WtHQTfVRUJotUNWVvK14CkN6QUpCZ05WQkFjVENuTmhbljowWTJ4aGNTXhEakFNQmdOVk1RCV0Z3Y0d4bApNQjRFRFRMU1ERXhOekEYtURZMU5Gb1hEVEUyTURFeE56QTJNRFRkTKZvd1B6RUxN  
 3MEJBUUVGUUQVFPQmpRQXdnWWTdZ1IFQXZFa2FoNjJFRnViTmVGVkNaQk9nN0pEZAo0dVQ1ZDBlM3UycUtaMTQrdzRjVkd5U053L1Rxt2Rk1F3T0xiaU9OdDBhLzhKRdVyc096Q3N  
 CWHRldUsyZzRPNhUwNi8wc28ZzFJKZTVkeFERNmNst2VsvjdPbUpFTWVXZDd5WjJGbfVqZHGzEROMjUxT25aa0pmeXN3NXdSVTKSnpuQnRza3hRcjBQbnj2S0tBa0NBd0VBQWFP  
 QjZUQ01akFkQmdOVkhRNEVGZ1FVam5XYVJsalF5N0pqnFozcwp0LzFIWmYVWUpRz3dad1JIEVllwakjHQxdYb0FVam5XYVJsalF5N0pqnFozc3QVmuHaZi9ZSmtpaFE2UkNjRDh4CkN6  
 QUpCZ05WQkFZVFE5VjRlNUN3Q1FzRFRUUIF0pQWVFRVE1CRUdBMVVFQnhNS2MyRnVkr0ZqYkdGeVIURU8KTUF3R0EXVUVDaE1GWWVhCd2JHV0NBUFF3REFRZSMFRQV3V3  
 QXdFQj96QUx0ZC05WSE4RUJBTUNBU3RVFZSgpZSvpjQVlINFFnRUJ0CQWdFR01DNEEdDV0NUH0FHRYtFSUJEUJFoRmgST1pYUURZMkZzWlhjZ1JyVnVaWepoCmRhmvtjRU5sY2  
 5ScFptbGpZWFJStUEwR0NtCudTSWizRFFQkN3VUBNEdCQU50RWY3aUFRIRUQlo0b2pJWm0KTHiTeFhGaTE0SGXjK0VpMUUnejv3R09Db3pibWNXemZOZXSSTdRQVlSSXQ3Wkh  
 hYWt0V0g0NxiVUhdPZXFkcgPsc2xNtZbnQ1hES3BtU2tXQ3VHdFhBbVhXU2xrTEt3tFHL0pkdTBhSEfkdVhtRvKwNW52M016RWHTWV8xehljCnFsYXjNcG9QUE14Qk50RmlBNWxs  
 QnAwTwt0LS0tLUVORCDBRVJUSUZQOFURS0tLS0tCg==  
 fileencoding : BASE64  
 filelocation : /nsconfig/ssl  
 filename : test\_cert.pem

Type : systemfile

filecontent :  
 LS0tLS1CRUdJTiB0EgUjFjVjRURSBURvktLS0tLQpNSUIDWEFjQkFB50jnUUM4U1jxSHjZUvc1cz0e0kVka0U2RHNRtjNpNVB5M1i3ZTdhb3BuWGo3RGdovWjKSTNECjlpBzUxcjVEQTR0  
 dUk0MjNSci93a1BtdXc3TU3RmUxNjRyYURnN0dmc9TeWpkMUv5N2tuRkQ3chVINTZWWHMKNlRUXg1WjN2SmxFV1pDTJNINB2M2juVTZkbVfSLoT6RG5CRIRbk5NRzj5VEZDdlEr  
 ZXU4b29DUUIEQVFBQgpBb0dBUUIENjZjaDBIRFJ0NS5VjMxc3FjbUz1NHJCM0Zub25ZN21ZT05sOHZ4WHRqU0wwdmcGRMZSTW9rMIMyCmU3Z0tjT040Rmo1YVWk1N1gn01aV1  
 dXY1o0aEhrMm5jMjMjOENLSWSoelhnyjFLQjRaMgp1TnUwNE1paVlyAHIKkNFROXluV0VMRIBDTjZWMHFQZwXGyXpVbnZjaH2pMfZGZCsyRNBUNy0drVhG0Z0VUdVEMkVODhGaU  
 kzVfJOYwpMcvjEMHh2ZVfWmkF6ZVBEYmFnTVFFRlNwZVZ3Yk11V3RjM2J0SkdwWXMkUkpleitOdGw0dVprRGVQbnNjZE5ZCjNjWjNsNUp4QWtFQXc5WDDkTDJanVpYaEVpM0Yzdj  
 YwU1U5RWm4Z01FdVhFZlHueDccZpuanjSckRIMUI0enyKR0hSU1ImUedYeHh5cjRKVmc4Q25kczZVOHEXN0N0SUXHUUpBS1Ft3UzYjVSMzByWURCS3BTQmFaaWpsM1NiMgo5Y3  
 VmdkVndVlQci9ZVXBtZTVNcEg5dXdlYXlHaINQblR6OTM3UUFNK2g0K2xWZGikS3Q0sKjNmtRskjBTHVScIRaUHBEV2UrcWVleGM1MmjzctjZz0Zc3Z2T3Ivam5Qtkx5STBjEh  
 FFVnlYk25KcDlmeEpXWEI5b3jJZxcKRzV1dmdEWG9ZdnRyI83eklyRUNRRDMzV1HeUw2MjJaRzZverHlxR1o1d1pCTFvtV1VyVE1zSngzOWZ5NUjoZgpkaJNwCe10Y3pIOFVKvmlPaGtyd  
 WNmb29tRlNPaUN4ZxhPQXM2MmVEZNNpQotLS0tLUVORCDBU50EgUjFjVjRURSBURvktLS0tLQo=  
 fileencoding : BASE64  
 filelocation : /nsconfig/ssl  
 filename : test\_cert\_key.pem

Type : sslcertkey

cert : test\_cert.pem  
 certkey : vsrver-1-lb-cert  
 inform : PEM  
 key : test\_cert\_key.pem

Type : sslvserver\_sslcertkey\_binding

certkeyname : vsrver-1-lb-cert  
 vsrvername : vsrver-1

## StyleBook で定義された仮想サーバーでの分析の有効化とアラームの設定

February 6, 2024

操作コンストラクトを使用して、StyleBook の一部である任意の仮想サーバーコンポーネントによって処理されるトラフィックトランザクションのすべてまたは一部に関する appflow レコードを収集するように Citrix ADM

Analytics を構成できます。また、このような操作構成を使用して、アラームを構成し、仮想サーバーが管理するトラフィックの詳細な情報を取得できます。

次の例は、StyleBook の Operations セクションを示しています。

```
1 operations:
2   analytics:
3     -
4     name: lbvserver-ops
5     properties:
6     target: $components.basic-lb-comp.outputs.lbvserver
7     filter: HTTP.REQ.URL.CONTAINS("catalog")
8     -
9     alarms:
10    -
11    name: lbvserver-alarm
12    properties:
13    target: $outputs.lbvserver
14    email-profile: $parameters.emailprofile
15    sms-profile: "NetScalerSMS"
16
17    rules:
18    -
19    metric: "total_requests"
20    operator: "greaterthan"
21    value: 25
22    period-unit: $parameters.period
23    -
24    metric: "total_bytes"
25    operator: "lessthan"
26    value: 60
27    period-unit: "day"
28 <!--NeedCopy-->
```

分析セクションの属性は、Citrix ADM 分析機能に、ターゲットプロパティで識別される仮想サーバーコンポーネント上のアプリケーションフローレコードを収集するように指示するために使用されます。また、NetScaler ADC ポリシー式を受け入れるフィルタプロパティを指定して、仮想サーバー上で収集される appflow レコードの要求をフィルタリングすることもできます。

この StyleBook から構成パックを作成すると、NetScaler ADM 分析機能は、構成パックの作成プロセスで仮想サーバーが作成されたときに指定された 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、アラーム生成のしきい値を設定し、ターゲットプロパティが指定する仮想サーバーの通知を送信するために使用されます。上の例では、email-profile と sms-profile のプロパティが通知を送信する場所を指定するために使用されています。rules セクションはしきい値を定義します。たとえば、ユーザーが定義した期間に、仮想サーバーが処理する要求の合計が 25 件を超えた場合、アラームが設定され、通知が送信されます。「period-unit」はアラームをトリガーする頻度を指定します。これは、日、時間、または毎週の値を取ることができます。

測定基準値としきい値の比較を用いる場合、次の演算子を使用できます。

- 「greaterthan」：「>」を示します
- 「Lessthan」：「<」を示します
- 「greaterthanequal」：「>=」を示します
- 「lessthanequal」：「<=」を示します

StyleBook では、メトリックスに API 名が使用され、NetScaler ADM 分析 GUI に表示される名前は使用されません。

構成パックの一部として作成された仮想サーバーで収集されたデータを表示および分析する方法については、NetScaler ADM Analytics のドキュメントを参照してください。

## インスタンスロール

February 6, 2024

Citrix Application Delivery Management (ADM) では、1 つのアプリケーションに対して複数の Citrix ADC インスタンスを構成する必要がある場合がありますが、各 ADC インスタンスをそれらに展開するには異なる構成が必要な場合もあります。このような場合の例は、Microsoft Skype for Business StyleBook のデフォルトです。

StyleBooks は現在、構成パックを作成し、複数の NetScaler ADC インスタンスに同じ構成を適用する機能をサポートしています。構成がすべての ADC インスタンスで同一であるようなシナリオを対称構成と呼ぶことができます。

StyleBooks の「インスタンスロール」機能を使用すると、非対称構成、つまり複数の ADC インスタンスに適用できる構成パックを作成できますが、異なる ADC インスタンスには異なる構成を使用できます。

インスタンスロール機能を備えた StyleBook を使用して構成パックを作成すると、構成パック内の各 ADC インスタンスに異なるロールを割り当てることができます。このロールは、ADC インスタンスが受け取る構成パックの設定オブジェクトを決定します。

注意事項:

- StyleBook のインスタンスロールのセットは、StyleBook の作成時に定義されます。
- ロールは、構成パックを作成または更新するときに、特定の ADC インスタンスに割り当てられます。

## 「ターゲットロール」セクション

StyleBook に「target-roles」と呼ばれる新しいセクションが導入されました。このセクションには、StyleBook でサポートされているすべてのロールが宣言されています。

このセクションは通常、StyleBook の「Import-StyleBooks」セクションの後、パラメーターセクションの前に配置されます。

次の StyleBook の例では、「ターゲットロール」セクション内に A と B の 2 つのロールが定義されています。

```

1 target-roles:
2
3   -
4     name: A
5     name: B
6     min-targets: 2
7     max-targets: 5
8 <!--NeedCopy-->

```

ルール B は、min-target と max-target という 2 つのオプションのサブプロパティも定義していることがわかります。

これら 2 つのサブプロパティはオプションですが、min-targets は、この StyleBook から構成パックを作成するときにこのルールを割り当てる ADC 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。

これらのサブプロパティが指定されていない場合、そのルールに設定できる ADC インスタンスの数の制限はありません。min-targets = 0 の場合、そのルールに関連付けられた設定はオプションであり、min-targets = 1 の場合、その設定は必須であり、そのルールに対して少なくとも 1 つの ADC インスタンスを設定する必要があります。

#### ルール「デフォルト」

明示的に定義されたルールに加えて、すべての StyleBook が持つ暗黙的なルールがあり、そのルールはデフォルトルールとして呼び出されます。このルールは、StyleBook の他のルールと同様に使用できます。構成パックを作成するときに、ADC インスタンスに特定のルールが割り当てられていない場合、インスタンスは「デフォルト」ルールに暗黙的に割り当てられます。これで、インスタンスは「default」ルールを持つコンポーネントによって生成された設定オブジェクトを受け取ります。

#### ルールを持つコンポーネント

StyleBook がサポートできるルール（「デフォルト」ルールを含む）を定義したら、そのルールを StyleBook のコンポーネントセクションで使用できます。コンポーネントを特定の役割を果たす ADC インスタンスにのみデプロイする場合は、次のコンポーネントの例に示すように、コンポーネントの一部として roles 属性を指定できます。

```

1   -
2     name: C1
3     type: ns::lbvserver
4     roles:
5       - A
6     properties:
7       name: lb1
8       servicetype: HTTP
9       ipv46: 1.1.1.1
10      port: 80
11 <!--NeedCopy-->

```

上記の例では、コンポーネントは「lbvserver」を生成し、このインスタンスはロール A を演じるインスタンスにデプロイされます。コンポーネントのロール属性はリストであり、コンポーネントには複数のロールを割り当てることができることに注意してください。これらのロールは、StyleBook の「ターゲットロール」セクションで宣言されていないはずで

注: StyleBook 内のコンポーネントがロール属性を指定しない場合、そのコンポーネントによって生成された構成オブジェクトは、ロールに関係なくすべての NetScaler ADC 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設定オブジェクトを作成できます。

A と B の 2 つのロールが定義されている StyleBook があり、4 つのコンポーネントが含まれていると仮定します。

- コンポーネント C1 にはロール A と B があります。
- コンポーネント C2 にはロール B があります。
- 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 には「デフォルト」の役割があります

この StyleBook のコンポーネントセクションを以下に示します。

```
1 components:
2   -
3     name: C1
4     type: ns::lbvserver
5     roles:
6       - A
7       - B
8     properties:
9       name: lb1
10      servicetype: HTTP
11      ipv46: 1.1.1.1
12      port: 80
13   -
14     name: C2
15     type: ns::lbvserver
16     roles:
17       - B
18     properties:
19       name: lb2
20       servicetype: HTTP
21       ipv46: 12.12.12.12
22       port: 80
23   -
24     name: C3
25     type: ns::lbvserver
26     properties:
27       name: lb3
28       servicetype: HTTP
29       ipv46: 13.13.13.13
30       port: 80
31   -
32     name: C4
33     type: ns::lbvserver
```



```

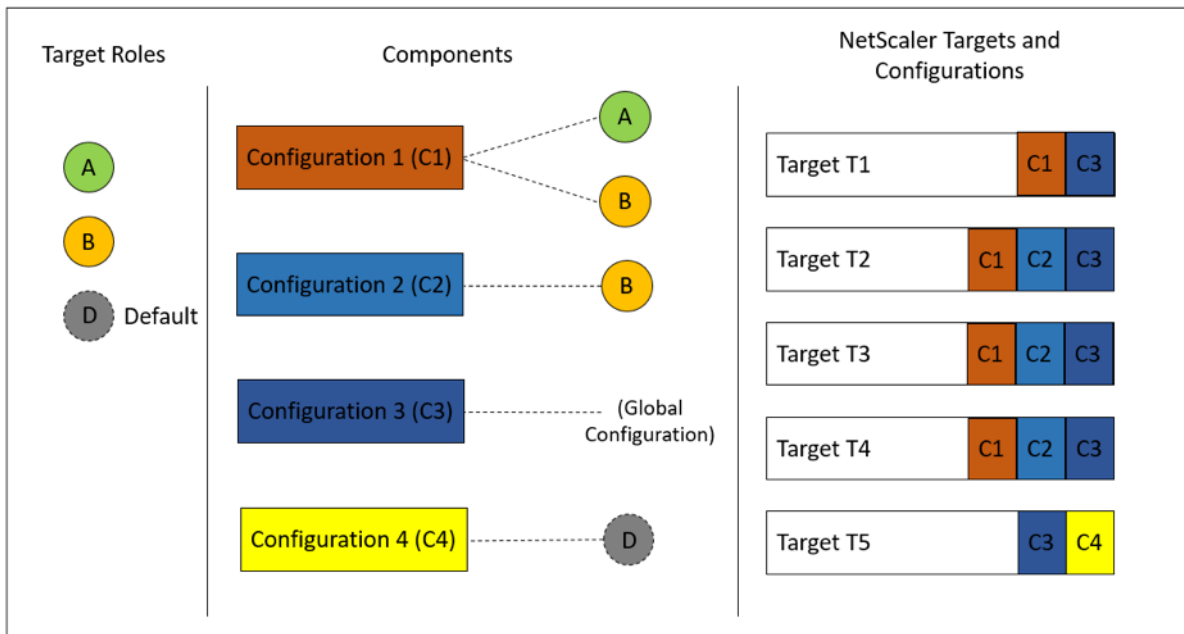
34     roles:
35       - default
36     properties:
37       name: lb4
38       servicetype: HTTP
39       ipv46: 14.14.14.14
40       port: 80
41 <!--NeedCopy-->
    
```

コンポーネント C3 にはロールが定義されていないことに注意してください。つまり、コンポーネントは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ます。一方、コンポーネント C4 には「default」というロールがあります。つまり、明示的なロールが割り当てられていないインスタンスに適用されます。

ここで、この StyleBook を使用して構成パックを作成し、5 つの ADC インスタンスにデプロイすることを検討します。この段階では、次の方法でインスタンスにロールを割り当てることができます：

- ロール A はインスタンス T1、T2、T3、T4 に割り当てられます
- ロール B はインスタンス T2、T3、T4 に割り当てられます
- インスタンス T5 にはロールが割り当てられていません

次の図は、役割の割り当てをまとめたもので、各 ADC インスタンスが受け取る構成を示しています。



コンポーネント C3 は、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ます。これは、このコンポーネントには roles 属性がないためです。

構成パックの作成時に「Dry Run」機能を使用して、各 ADC インスタンスに作成されるロールと設定オブジェクトの正しい割り当てを表示および検証することもできます。

## StyleBook を構築する

StyleBook 「デモターゲットロール」の全コンテンツを以下に示します：

```
1 ---
2 name: demo-target-roles
3 namespace: com.example.stylebooks
4 version: "1.2"
5 schema-version: "1.0"
6 import-stylebooks:
7   -
8     namespace: netScaler.nitro.config
9     prefix: ns
10    version: "10.5"
11 parameters:
12   -
13     name: appname
14     type: string
15     required: true
16     key: true
17 target-roles:
18   -
19     name: A
20   -
21     name: B
22     min-targets: 2
23     max-targets: 5
24 components:
25   -
26     name: C1
27     type: ns::lbserver
28     roles:
29       - A
30       - B
31     properties:
32       name: lb1
33       servicetype: HTTP
34       ipv46: 1.1.1.1
35       port: 80
36   -
37     name: C2
38     type: ns::lbserver
39     roles:
40       - B
41     properties:
42       name: lb2
43       servicetype: HTTP
44       ipv46: 12.12.12.12
45       port: 80
46   -
47     name: C3
48     type: ns::lbserver
49     properties:
```

```
50     name: lb3
51     servicetype: HTTP
52     ipv46: 13.13.13.13
53     port: 80
54 -
55     name: C4
56     type: ns::lbserver
57     roles:
58     - default
59     properties:
60     name: lb4
61     servicetype: HTTP
62     ipv46: 14.14.14.14
63     port: 80
64 <!--NeedCopy-->
```

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。

Objects created ( 9 ) x

|                                                                                                |
|------------------------------------------------------------------------------------------------|
| <b>Instance : 10.102.102.136   Roles : B   Count : 3</b>                                       |
| <b>Type : lbserver</b><br>ipv46 : 1.1.1.1<br>name : lb1<br>port : 80<br>servicetype : HTTP     |
| <b>Type : lbserver</b><br>ipv46 : 12.12.12.12<br>name : lb2<br>port : 80<br>servicetype : HTTP |
| <b>Type : lbserver</b><br>ipv46 : 13.13.13.13<br>name : lb3<br>port : 80<br>servicetype : HTTP |
| <b>Instance : 10.102.102.135   Roles : B   Count : 3</b>                                       |
| <b>Type : lbserver</b><br>ipv46 : 1.1.1.1<br>name : lb1<br>port : 80<br>servicetype : HTTP     |
| <b>Type : lbserver</b><br>ipv46 : 12.12.12.12<br>name : lb2<br>port : 80<br>servicetype : HTTP |
| <b>Type : lbserver</b><br>ipv46 : 13.13.13.13<br>name : lb3<br>port : 80<br>servicetype : HTTP |
| <b>Instance : 10.102.102.62   Roles : A, default   Count : 3</b>                               |
| <b>Type : lbserver</b><br>ipv46 : 1.1.1.1<br>name : lb1<br>port : 80<br>servicetype : HTTP     |
| <b>Type : lbserver</b><br>ipv46 : 13.13.13.13<br>name : lb3<br>port : 80<br>servicetype : HTTP |
| <b>Type : lbserver</b><br>ipv46 : 14.14.14.14<br>name : lb4<br>port : 80<br>servicetype : HTTP |

## API の使用

REST API を使用する場合、次のように構成パックを作成または更新するときに、各 ADC インスタンスに対してロールを指定できます。「targets」ブロックで、個々のコンポーネントを展開する特定の NetScaler ADC インスタンスの UUID を指定します。

```
1  "targets": [  
2      {  
3  
4      "id": "<ADC-UUID>",  
5      "roles": ["A"]  
6      }  
7  ,  
8  ]  
9  <!--NeedCopy-->
```

参考のために、完全なサンプル REST API が提供されています。

POST/<ADM-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpack

```
1  {  
2  
3  "configpack": {  
4  
5  "parameters": {  
6  
7  "appname": "app1"  
8  }  
9  ,  
10 "targets": [  
11     {  
12  
13     "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",  
14     "roles": ["A"]  
15     }  
16  ,  
17     {  
18  
19     "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",  
20     "roles": ["A", "B"]  
21     }  
22  ,  
23     {  
24  
25     "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",  
26     "roles": ["A", "B"]  
27     }  
28  ,  
29     {  
30  
31     "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
```

```
32     "roles": ["A", "B"]
33     }
34   ,
35     {
36     "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
37     "roles": ["default"]
38     }
39   ]
40 }
41 }
42 }
43 }
44 }
45 }
46 <!--NeedCopy-->
```

## StyleBook を作成して非 CRUD 操作を実行する

February 6, 2024

StyleBook は、NetScaler ADC インスタンス上で必要な構成オブジェクトを計算することによって、NetScaler ADC 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。つまり、「望ましい状態」を指定するときです。

ただし、一部の Citrix ADC 構成オブジェクトは、作成、更新、削除（CRUD 操作）以外のいくつかの操作をサポートしています。たとえば、ロードバランサーオブジェクト（lbvserver）または Citrix ADC 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、Citrix ADC 証明書キーは、証明書を別の証明書にリンクまたはリンク解除するための「リンク」および「リンク解除」操作をサポートしています。NetScaler ADC オブジェクトに対するこれらの操作は、非 CRUD 操作と呼ばれます。このセクションでは、StyleBook を使用して、それらをサポートする設定オブジェクトに対して非 CRUD 操作を実行する方法について説明します。

### 注:

設定オブジェクト間のバインディング（たとえば、証明書キーを lbvserver にバインドする）は、CRUD 以外の操作とは見なされません。これは、Nitro バインディングはそれ自体が設定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 ADC 構成オブジェクトと同様に作成および削除されます。

## CRUD 以外のオペレーションのサポート

「メタプロパティ」と呼ばれる新しい構成が、「プロパティ」構成と同じレベルでコンポーネントに追加されます。この構成でサポートされる唯一の属性は、現在「action」と呼ばれています。この属性は、その構成オブジェクトでサポートされている「enable」や「disable」のような値を取ることができます。

```
1 components:
2   -
3     name: my-lbvserver-comp
4     type: ns::lbvserver
5     meta-properties
6       action: enable
7     properties:
8       name: $parameters.name
9       servicetype: HTTP
10      ipv46: $parameters.ip
11      port: 80
12      lbmethod: $parameters.lb-alg
13 <!--NeedCopy-->
```

上記の例では、「my-lbvserver-comp」コンポーネントのタイプは「ns::lbvserver」です。「ns」は、インポート StyleBook のセクションで指定した名前空間 `netScaler.nitro.config` とバージョン 10.5 を指す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、LBV サーバーは最初に StyleBook によって作成され、次に「enable」操作が実行されます。

メタプロパティで指定されたアクションは、ConfigPack の作成時にのみ構成オブジェクトに対して実行されます。ConfigPack を更新しても、CRUD 以外のアクションは実行されません。

注:

action 属性の値は、動的に評価される StyleBook 式であってはなりません。

## StyleBook の構成パックを別の StyleBook に移行する

February 6, 2024

NetScaler Application Delivery Management (ADM) では、構成パックは常に作成元 StyleBook にバインドされます。構成パックへの更新は、構成パックがバインドされている StyleBook でのみ実行できます。NetScaler ADM では、既存の構成パックを新しい StyleBook に移行できるようになりました。新しい StyleBook は、構成パックにバインドされている現在の StyleBook のよりオリジナルバージョンにすることができます。または、構成パックをまったく異なる StyleBook に移行することもできます。

たとえば、**example-lb** という StyleBook を作成しました。この StyleBook は、NetScaler ADC インスタンスに基本的なロードバランサー構成を展開するために使用されます。NetScaler ADC インスタンスで、この StyleBook から構成パック CP1 を作成しました。その後、StyleBook に監視設定が含まれていないことに気がきました。これで **example-lb-mon** という **StyleBook** が作成されました。この StyleBook には、example-lb StyleBook と同じロードバランサー設定がありますが、モニターを設定する機能が追加されています。

次に、構成パック CP1 で作成された既存の構成を更新して、いくつかのモニターを追加します。以前は、構成パック CP1 を削除し、新しい StyleBook から構成パック CP2 を作成して、構成にモニターを追加する必要がありました。

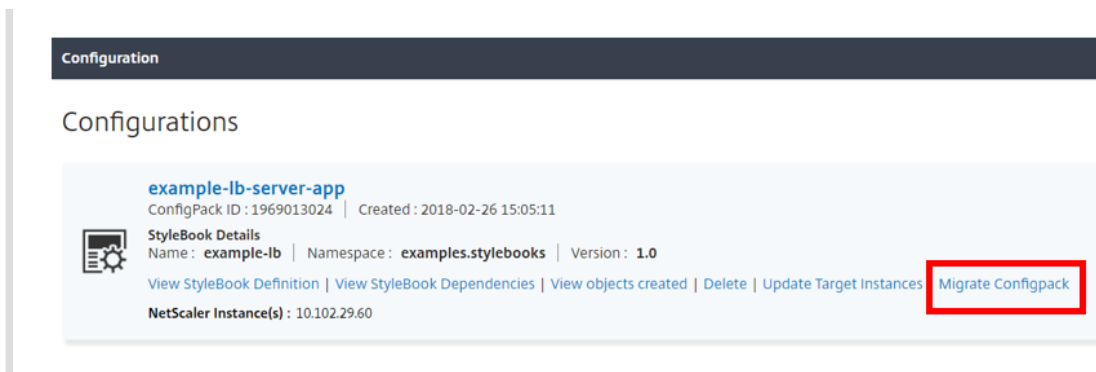
CP1 を削除すると、1 つ以上の NetScaler ADC インスタンス上の構成パック CP1 で作成されたすべての構成が削除されます。以前は、すべてのパラメータに値を入力して、新しい StyleBook で新しい構成パックを再作成する必要がありました。

代わりに、既存の構成パック CP1 を新しい example-lb-mon StyleBook に移行できるようになりました。新しい StyleBook では、モニターモニターの詳細を設定できます。これらのモニター関連の設定オブジェクトのみが、構成パックが展開された NetScaler ADC インスタンスに追加されます。あなたは今、モニタの詳細だけを提供する必要があります。変更されていない NetScaler ADC インスタンスにデプロイされた既存の構成は、影響を受けません。

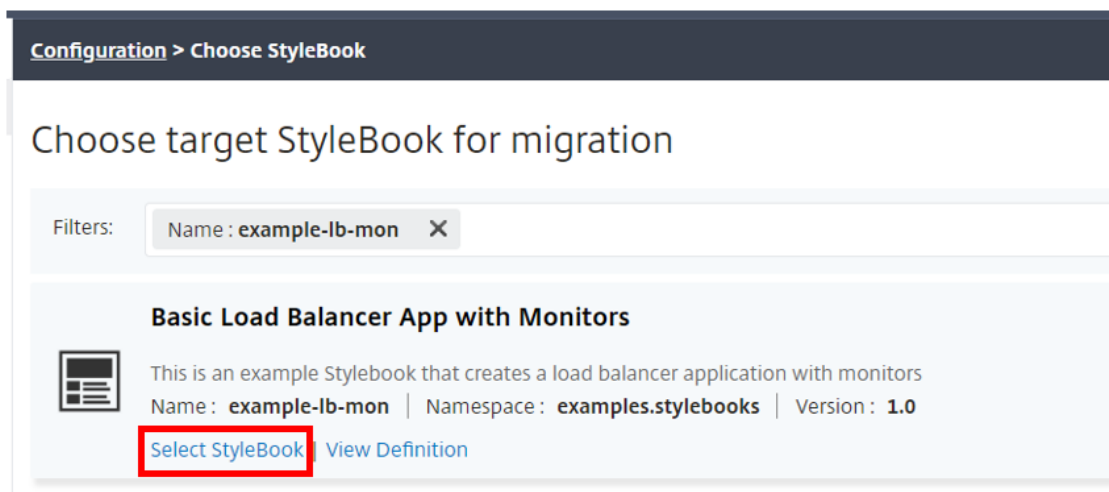
## 構成パックの移行

**example-lb StyleBook** を使用して作成した構成パックを **example-lb-mon StyleBook** に移行するには

1. NetScaler ADM で、[アプリケーション] > [構成] に移動します。[構成] ページには、システム内に存在するすべての構成パックが表示されます。
2. 下にスクロールして、以前に作成した例の **lb** 構成パックを探し、[ **Configpack** の移行 ] をクリックします。



3. [移行対象の **StyleBook** の選択] ページが開き、Citrix ADM で使用可能なすべての StyleBook が一覧表示されます。下にスクロールして example-lb-mon **StyleBook** を探し、「**StyleBook** を選択」をクリックします。example-lb-mon と入力して StyleBook を検索することもできます。





ある StyleBook から別の StyleBook に移行すると、2つの StyleBook のすべてのパラメーターが同じ構造にならない場合があります。パラメータ構造が類似している場合、以前の値はパラメータフィールドに自動的に保持されます。新しい StyleBook の一部のパラメーターは、新しいものであるか、構造が変更されている可能性があります。このような場合は、StyleBook パラメータの値を手動で入力する必要があります。たとえば、次の画像は example-lb StyleBook のパラメーターを示しています。

This configuration was created from the StyleBook 'example-lb' (namespace: 'examples.stylebooks', version: '1.0').

Load Balanced Application Name  
example-lb-server-app

Load Balanced App Virtual IP address\*  
192 . 10 . 10 . 10

Load Balanced App Virtual Port  
80

Load Balanced App Protocol  
HTTP

Advanced Load Balancer Settings

Application Server Protocol\*  
HTTP

**Server IPs and Ports** +

| Application Server IP Address | Application Server Port |
|-------------------------------|-------------------------|
| No items                      |                         |

**Application Servers FQDN names** +

| Application Server Domain Name | Application Server Port |
|--------------------------------|-------------------------|
| No items                       |                         |

Advanced Application Server Settings

**SSL Certificate Settings** +

| Certificate Name | CertKey Format | Certificate Key Name | Private Key Password |
|------------------|----------------|----------------------|----------------------|
| No items         |                |                      |                      |

**Target Instances**

10.102.29.60 > +

OK Close Dry Run

次の図は、構成パックを example-lb-mon StyleBook に移行した後のパラメータを示しています。

This configuration was created from the StyleBook 'example-lb-mon' (namespace: 'examples.stylebooks', version: '1.0').

Load Balanced Application Name

Load Balanced App Virtual IP address\*

Load Balanced App Virtual Port

Load Balanced App Protocol

Advanced Load Balancer Settings

Application Server Protocol\*

**Server IPs and Ports**

| Application Server IP Address | Application Server Port |
|-------------------------------|-------------------------|
| No items                      |                         |

**Application Servers FQDN names**

| Application Server Domain Name | Application Server Port |
|--------------------------------|-------------------------|
| No items                       |                         |

Advanced Application Server Settings

**SSL Certificate Settings**

| Certificate Name | CertKey Format | Certificate Key Name |
|------------------|----------------|----------------------|
| No items         |                |                      |

**List of Monitors**

| Monitor Name | Monitor Type | Destination IP | Destination P | HTTP Request | Send String | Custom HTTP |
|--------------|--------------|----------------|---------------|--------------|-------------|-------------|
| No items     |              |                |               |              |             |             |

**Target Instances**

> +

この場合、StyleBook は基本的なロードバランサー構成の古い値を保持していることがわかります。ただし、

モニターパラメーターの値は手動で入力する必要があります。

4. インスタンスでモニターを作成する際に使用する新しいパラメータの値を入力します。
5. [ターゲットインスタンス] で、構成を実行する Citrix ADC インスタンスの IP アドレスをクリックして選択します。必要な数のターゲットインスタンスを指定することで、構成を複数の Citrix ADC に展開できることに注意してください。
6. [ドライラン] をクリックします。オブジェクトページには、Citrix ADC インスタンスから新たに作成、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」 (Create) をクリックして、選択したインスタンスの設定を作成または更新します。ターゲットインスタンスが新しい場合は、構成パックが作成されます。それ以外の場合は、インスタンスにデプロイされた既存の設定が更新されます。

### 注

：更新アイコンをクリックして、最近検出された Citrix ADC インスタンスを追加することもできます。そのため、これらのインスタンスは、このウィンドウのインスタンス一覧ですぐに表示されます。更新アイコンは現在、NetScaler ADM でのみ使用できます。


StyleBook の 1 つのバージョンから次のバージョンに構成パックを移行することもできます。また、新しいバージョンに存在する新しい必須パラメータの値を入力する必要があります。構成パックを古いバージョンの StyleBook に移行することもできます。この場合、古い StyleBook に存在しない余分なパラメータは削除されます。オブジェクトページには、構成から削除されたすべてのオブジェクトが表示されます。

移行が成功すると、ConfigPack は新しい StyleBook にバインドされます。

### Configuration

## Configurations

**example-lb-server-app**  
ConfigPack ID : 1969013024 | Created : 2018-02-26 15:05:11

 **StyleBook Details**  
Name : example-lb-mon | Namespace : examples.stylebooks | Version : 1.0

[View StyleBook Definition](#) | [View StyleBook Dependencies](#) | [View objects created](#) | [Delete](#) | [Update Target Instances](#) | [Migrate Configpack](#)

NetScaler Instance(s) : 10.102.29.60

構成パックの名前と構成パック ID が以前と同じであることがわかります。しかし、NetScaler ADM は例-lb から例-lb-mon に StyleBook 名を更新します。

## StyleBook を構築する

参考までに、**example-lb** StyleBook の全コンテンツを以下に示します。

```
1 name: example-lb
```

```
2 namespace: examples.stylebooks
3 version: "1.0"
4 display-name: Basic Load Balancer App
5 description: This is an example StyleBook that creates a load balancer
  application
6 schema-version: "1.0"
7 import-stylebooks:
8   -
9     namespace: com.citrix.adc.stylebooks
10    prefix: stlb
11    version: "1.0"
12 parameters-default-sources:
13   - stlb::lb
14 components:
15   -
16     name: lb-comp
17     type: stlb::lb
18     description: Uses the default lb StyleBook to build the typical lb
  configuration objects
19     properties-default-sources:
20       - $parameters
21 <!--NeedCopy-->
```

あなたの参考のために、**example-lb-mon** StyleBook の全コンテンツを以下に示します。

```
1 name: example-lb-mon
2 namespace: examples.stylebooks
3 version: "1.0"
4 description: This is an example StyleBook that creates a load balancer
  application with monitors
5 display-name: Basic Load Balancer App with Monitors
6 schema-version: "1.0"
7 import-stylebooks:
8   -
9     namespace: netscaler.nitro.config
10    prefix: ns
11    version: "10.5"
12   -
13     namespace: com.citrix.adc.stylebooks
14     prefix: stlb
15     version: "1.0"
16   -
17     namespace: com.citrix.adc.commonotypes
18     prefix: cmtypes
19     version: "1.0"
20 parameters-default-sources:
21   - stlb::lb
22 parameters:
23   -
24     name: monitors
25     label: "List of Monitors"
26     description: "List of Monitors to monitor Application Servers"
27     type: cmtypes::monitor[]
```

```
28 substitutions:
29   mon-name(appname, monname): $appname + "-mon-" + $monname
30 components:
31   -
32     name: lb-comp
33     type: stlb::lb
34     description: Uses the default lb StyleBook to build the typical lb
35                 configuration objects
36     properties-default-sources:
37       - $parameters
38   -
39     name: monitors-comp
40     type: cmtypes::monitor
41     condition: $parameters.monitors
42     repeat: $parameters.monitors
43     repeat-item: mon
44     repeat-index: ndx
45     description: Builds a list of Citrix ADC monitor objects and binds
46                 them to the servicegroup of this LB config
47     properties-default-sources:
48       - $mon
49     properties:
50       monitorname: $substitutions.mon-name($parameters.lb-appname,
51         $mon.monitorname)
52     components:
53       -
54         name: monitor-svcg-binding-comp
55         condition: $parameters.svc-servers
56         type: ns::servicegroup_lbmonitor_binding
57         properties:
58           servicegroupname: $components.lb-comp.outputs.servicegroup.
59             properties.servicegroupname
60           monitor_name: $parent.properties.monitorname
61 <!--NeedCopy-->
```

## API を使用して **StyleBook** から設定を作成する

February 6, 2024

StyleBook を作成したら、それを Citrix Application Delivery Management (ADM) にインポートして、Citrix ADM または Citrix ADM API を使用して使用する必要があります。NetScaler ADM はインポート時に StyleBook を検証し、検証が成功すると、StyleBook の NetScaler ADM カタログに StyleBook が表示され、構成の作成に使用できます。

StyleBook API を使用して、この StyleBook に基づいて構成を作成できるようになりました。curl コマンドラインツールや Postman chrome ブラウザ拡張機能などの任意のツールを使用して、Citrix ADM に HTTP リクエストを送信できます。

**例 1**

負荷分散仮想サーバーを作成するために、StyleBook で作成した「lb-vserver」 StyleBook について考えてみます。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：

```
1 POST
2
3 https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/lb-vserver/configpacks
4
5 <!--NeedCopy-->
```

```
1 Content-Type: application/json
2 Accept: application/json
3 {
4
5   "configpack":
6   {
7
8     "parameters": {
9
10      "name": "lb1",
11      "ip": "10.102.117.31"
12    }
13  ,
14  "target_devices":
15  [
16    {
17
18      "id": "deec30-f478-4446-9741-a85041903410"
19    }
20  ]
21 }
22 }
23
24 }
25
26 <!--NeedCopy-->
```

この HTTP リクエストでは、ID (例: " deec30-f478-4446-9741-a85041903410") は、負荷分散仮想サーバー lb1 が IP アドレス 10.102.117.31 が作成される NetScaler ADC インスタンスのインスタンス ID です。NetScaler ADC インスタンスのインスタンス ID は NetScaler ADM から取得されます。

NetScaler ADM によって管理されるインスタンスの ID を取得するには、NetScaler ADM API を使用します。たとえば、IP アドレスが 192.168.153.160 の Citrix ADC 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。

```
1 GET https://<MAS-IP>/nitro/v1/config/ns?filter=ip_address
   :192.168.153.160
2 <!--NeedCopy-->
```

```
1 Accept: application/json
2 <!--NeedCopy-->
```

応答ではペイロード内に ID が含まれています。

```
1 200
2 OK
3 Content-Type: application/json
4 {
5
6   "errorCode": 0,
7   "message": "Done",
8   "operation": "get",
9   "resourceType": "ns",
10  "username": "nsroot",
11  "tenant_name": "Owner",
12  "resourceName": "",
13  "ns":
14  [
15    {
16
17      "is_grace": "false",
18      "hostname": "",
19      "std_bw_config": "0",
20      "gateway_deployment": "false",
21      ... "id": "deec30-f478-4446-9741-a85041903410",
22      ...
23    }
24  ]
25 }
26 }
27
28 <!--NeedCopy-->
```

構成パックが正常に作成されると、次の HTTP 応答が表示されます。

```
1 200 OK
2 Content-Type: application/json
3 {
4
5   "configpack":
6   {
7
8     "config_id": "1460806080"
9   }
10 }
11 }
12
13 <!--NeedCopy-->
```

ID 1460806080 を使用して一意に識別される最初の構成パックを作成しました。この ID を使用して、構成のクエリ、更新、削除を行えます。

## 例 2

同じ StyleBook を使用して別の構成パックを作成し、同じまたは異なる NetScaler ADC 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。また、負荷分散の方法として LEASTCONNECTION を指定します。この構成を 2 つの NetScaler ADC インスタンスにデプロイします。

HTTP 要求は次のとおりです。

```
1 POST
2
3 https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/lb-vserver/configpacks
4 <!--NeedCopy-->
```

```
1 Content-Type: application/json
2 Accept: application/json
3 {
4
5   "configpack":
6     {
7
8     "parameters":
9       {
10
11       "name": "lb2",
12       "ip": "10.102.117.32",
13       "lb-alg": "LEASTCONNECTION"
14     }
15   ,
16   "target_devices"
17     [
18     {
19     "id": "deecee30-f478-4446-9741-a85041903410" }
20   ,
21   {
22   "id": "debecc60-d589-4557-8632-a74032802412" }
23   ]
24   }
25 }
26
27 }
28
29 <!--NeedCopy-->
```

この HTTP リクエストでは、IP アドレス 10.102.117.32 の負荷分散仮想サーバー lb2 が、ids “deecee30-f478-4446-9741-a85041903410” と “debecc60-d589-4557-8632-a74032802412” で表される 2 つの NetScaler ADC インスタンスに作成されます。

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。



```
1 200 OK
2 Content-Type: application/json
3 {
4
5     "configpack":
6     {
7
8         "config_id": "1657696292"
9     }
10
11 }
12
13 <!--NeedCopy-->
```

この新しい構成パックには、異なる ID 165769629 があります。この ID を使用することで、この構成を更新または削除できます。

### 例 3

「[基本的な負荷分散の構成を作成するための StyleBook](#)」で作成した「basic-lb-config」StyleBook を参考にします。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：

```
1 POST
2
3 http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example
  .stylebooks/0.1/basic-lb-config/configpacks
4 <!--NeedCopy-->
```

```
1 Content-Type: application/json
2 Accept: application/json
3 {
4
5     "configpack":
6     {
7
8         "parameters":
9         {
10
11             "name": "myapp",
12             "ip": "10.70.122.25",
13             "svc-servers":
14             ["192.168.100.11", "192.168.100.12"],
15             "svc-port": 8080
16         }
17     ,
18     "target_devices":
19     [
20     {
21
22         "id": "deec30-f478-4446-9741-a85041903410"
23     }
24 ]
25 }
```

```
24   ,
25     {
26       "id": "debecc60-d589-4557-8632-a74032802412"
27     }
28   ]
29 }
30 }
31 }
32 }
33 }
34 }
35 <!--NeedCopy-->
```

この HTTP リクエストでは、2 つの NetScaler ADC インスタンスで負荷分散構成が実行されます。これらの NetScaler ADC 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 の **composite-example** を参考にします。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：

```
1 POST http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
  example.stylebooks/0.1/composite-example/configpacks
2 <!--NeedCopy-->
```

```
1 Content-Type: application/json
2 Accept: application/json
3 {
4   "configpack":
5   {
6     "parameters": {
7       "name": "myapp",
8       "ip": "2.2.2.2",
9       "svc-servers": ["10.102.29.52", "10.102.29.53"]
10    }
11  ,
12  "target_devices":
13  [
14    {
15      "id": "deec30-f478-4446-9741-a85041903410"
16    }
17  ,
18  {
19    "id": "debecc60-d589-4557-8632-a74032802412"
20  }
21  ]
22  }
23  }
24  "id": "debecc60-d589-4557-8632-a74032802412"
```

```

25     }
26
27     ]
28   }
29
30 }
31
32 <!--NeedCopy-->

```

この HTTP リクエストでは、構成は ID で表される 2 つの NetScaler ADC インスタンスに作成されます。NetScaler ADC インスタンスにログオンすると、「複合例」StyleBook にインポートされた「basic-lb-config」StyleBook で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 の一部だった「myapp-mon」という新しい HTTP モニターも表示されます。

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。

```

1 200 OK
2 Content-Type: application/json{
3
4   "configpack": {
5
6     "config_id": "4917276817"
7   }
8
9 }
10
11 <!--NeedCopy-->

```

### 構成の更新

たとえば、IP アドレス 10.102.29.54 の新しいバックエンドサーバーを負荷分散仮想サーバー myapp に追加して、この設定を更新するには、次のように設定パックを更新するための API を使用します。

```

1 PUT http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks/4917276817
2 <!--NeedCopy-->

```

```

1 Content-Type: application/json
2 Accept: application/json
3 {
4
5   "configpack": {
6
7     "parameters": {
8
9       "name": "myapp",
10      "ip": "2.2.2.2",
11      "svc-servers": ["10.102.29.52", "10.102.29.53", "10.102.29.54"]
12    }
13  ,

```

```
14  "target_devices":
15  [
16    {
17      "id": "deecce30-f478-4446-9741-a85041903410"
18    }
19  ],
20  {
21    "id": "debecc60-d589-4557-8632-a74032802412"
22  }
23  ]
24  }
25  }
26  }
27  }
28  }
29  }
30  }
31  <!--NeedCopy-->
```

構成パックが正常に更新されると、次の HTTP 応答が受信されます。

```
1  200 OK
2  Content-Type: application/json
3  {
4    "configpack": {
5      "config-id": "4917276817"
6    }
7  }
8  }
9  }
10 }
11 }
12 <!--NeedCopy-->
```

#### 構成の削除

この構成を（すべての NetScaler ADC インスタンスから）削除するには、次のように API を使用して構成パックを削除します。

```
1  DELETE http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks/4917276817
2  <!--NeedCopy-->
```

```
1  Accept: application/json
2  <!--NeedCopy-->
```

構成パックが正常に削除されると、次の HTTP 応答が受信されます。

```
1  200 OK
2  Content-Type: application/json
3  {
```

```
4
5   "configpack": {
6
7     "config_id": "4917276817"
8   }
9
10  }
11
12  <!--NeedCopy-->
```

NetScaler ADC インスタンスにログオンし、この構成パックに含まれるすべての構成オブジェクトが削除されたことを確認できます。

構成をすべてではなく特定の NetScaler ADC インスタンスから削除する場合は、上記の構成パックの更新操作を使用し、JSON ペイロードの「target\_devices」属性を変更して、特定の NetScaler ADC インスタンス ID を削除します。

## API を使用して証明書とキーファイルをアップロードする設定を作成する

February 6, 2024

StyleBook API を使用して、この StyleBook に基づいて構成を作成します。curl コマンドラインツールや Postman chrome ブラウザ拡張機能などの任意のツールを使用して、HTTP リクエストを NetScaler Application Delivery Management (ADM) に送信できます。

[SSL 証明書と証明書キーファイルを NetScaler ADM にアップロードする StyleBook を作成する方法で証明書とキーファイルをアップロードするために作成した StyleBook の例を考えてみましょう。](#) 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：

```
1 POST
2
3 https://<MAS_IP_Address>/stylebook/nitro/v1/config/stylebooks/com.
   citrix.adc.stylebooks/1.0/lb-mon/configpacks?mode=async
4 <!--NeedCopy-->
```

```
1 Content-Type: application/jsonAccept: application/json {
2
3   "configpack": {
4
5     "parameters": {
6
7       "lb-appname": "lbmon",
8       "lb-virtual-ip": "13.1.11.10",
9       "lb-virtual-port": "80",
10      "lb-service-type": "HTTP",
11      "svc-service-type": "HTTP",
12      "svc-servers": [
```

```
13         {
14
15             "ip": "14.1.1.15",
16             "port": "80"         }
17
18     ],
19     "certificates": [
20     {
21
22         "cert-name": "server_cert",
23         "cert-file": "server_cert.pem",
24         "ssl-inform": "PEM",
25         "key-name": "server_key",
26         "key-file": "server_key.pem",
27         "cert-password": "secret",
28         "cert-advanced": {
29
30             "is-ca-cert": false,
31             "skip-ca-name": false
32         }
33     }
34 ]
35
36 ],
37 "lb-advanced": {
38
39     "flush-on-state-down": "ENABLED",
40     "auth-params": {
41
42         "authentication": "OFF",
43         "authentication-http-401": "OFF"
44     }
45 },
46     "appflow-log": "ENABLED",
47     "algorithm": "LEASTCONNECTION"
48 }
49 ,
50     "svcg-advanced": {
51
52         "svc-client-ip": "DISABLED",
53         "svc-use-source-ip": "NO",
54         "svc-use-proxy-port": "NO",
55         "svc-surge-protection": "OFF",
56         "svc-client-keepalive": "NO",
57         "svc-tcp-buffering": "NO",
58         "svc-compression": "NO",
59         "svc-state": "ENABLED",
60         "svc-downstate-flush": "DISABLED",
61         "svc-enable-health-monitor": "NO"
62     }
63 }
64 }
65 ,
```

```

66     "targets": [
67         {
68             "id": "8c158e7a-0087-423f-91b0-0ccf16de552a"
69         }
70     ]
71 }
72 ]
73 }
74 }
75 }
76 }
77 <!--NeedCopy-->

```

この設定パックは、ID 8c158e7a-0087-423F-91b0-0ccf16de552a を使用して一意に識別されます。この ID を使用して、構成のクエリ、更新、削除を行えます。構成パックが正常に更新されると、証明書とキーファイルが NetScaler ADM ファイルシステムにアップロードされます。

## API を使用して任意のファイルタイプをアップロードする設定を作成する

February 6, 2024

NetScaler Application Delivery Management (ADM) API を使用して、選択した NetScaler ADC インスタンスにファイルをアップロードする構成パックを作成することもできます。

「[NetScaler ADC MA Service にファイルをアップロードする StyleBook を作成する方法](#)」で、あらゆる種類のファイルをアップロードするために作成した StyleBook の例を考えてみましょう。上記のトピックの例のように、構成パックを作成し、NetScaler ADM 上の場所ファイルのファイルパスとして「locationfile」パラメータの値を指定します。

次のように、REST API を使用して、この StyleBook から設定パックを作成します。

```

1 POST
2
3 https://<mas_ip>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.
   stylebooks.samples/1.0/upload-geolocations/configpacks
4 <!--NeedCopy-->

```

```

1 Content-Type: application/json
2 Accept: application/json
3 {
4     "configpack":
5     {
6         "parameters": {
7             "locationfile": "/var/mps/tenants/root/files/ /
8             custom_geolocations.csv"
9         }
10    }

```

```
11     }
12   ,
13     "targets": [
14       {
15
16         "id": "5e540839-cd6c-437e-ac53-7d49bc2602b5"
17       }
18     ]
19   }
20 }
21
22 }
23
24 <!--NeedCopy-->
```

## API を使用してカスタム **StyleBook** をインポートする

February 6, 2024

StyleBook API を使用して、カスタム StyleBook を NetScaler Application Delivery Management (ADM) にインポートできるようになりました。この StyleBook から設定パックを作成するには、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ツールで、次のようにします。たとえば、example-lb という名前の StyleBook をインポートして、NetScaler ADC インスタンスでロードバランサー構成を作成できます。

```
1 HTTP Method: POST
2 URL: http://<mas-ip>/stylebook/nitro/v1/config/stylebooks
3 Headers:
4 Content-Type: application/json
5 Accept: application/json
6 RequestBody:
7 {
8
9     "stylebook":
10    {
11
12      "file_name": "example-lb.yaml",
13      "source": "<base64-contents>",
14      "encoding": "base64"
15    }
16  }
17 }
18
19 <!--NeedCopy-->
```

ここで、「ソース」属性の値は、StyleBook ファイルのコンテンツの base64 エンコーディングです。たとえば、<https://www.browsersling.com/tools/file-to-base64> StyleBook ファイルの YAML コンテンツをオンライン



ツールに貼り付けて base64 文字列を取得し、それを上記の「source」属性の値として使用できます。

この API 呼び出しを使用すると、複数の StyleBook ファイルを含む圧縮された tarball ファイル (.tgz ファイル) を 1 つの API オペレーションでアップロードすることもできます。そのためには、file\_name 属性を.tgz ファイル名に、source 属性の値を.tgz ファイルの内容の base64 エンコーディングに変更するだけです。

ツールで API が正常に実行されると、StyleBook が NetScaler ADM にインポートされたことを示す次の応答が表示されます。

```
1 200 OK
2 <!--NeedCopy-->
```

レスポンス本文:

```
1 {
2
3
4   "stylebook":
5   {
6
7
8     "name": "example-lb",
9
10    "namespace": "com.example.stylebook",
11
12    "version": "1.0"
13  }
14 }
15
16
17 }
18
19 <!--NeedCopy-->
```

## API を使用してカスタム **StyleBook** をダウンロードする

February 6, 2024

以下の StyleBook REST API を提供することで、カスタム StyleBook をダウンロードできます。

```
1 GET
2
3 https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
4   VERSION>/<NAME>/actions/download
5 <!--NeedCopy-->
```

IP アドレス、名前、バージョン、名前空間のフィールドを変更した後は、curl コマンドラインツールや Postman chrome ブラウザ拡張機能など、どのツールでも API を実行できます。

```

1 GET
2
3 https://10.102.29.58/stylebook/nitro/v1/config/stylebooks/com.example.
  ssl.stylebooks/0.1/lb-vserver-ssl/actions/download`
4 <!--NeedCopy-->

```

.yaml 形式の StyleBook がダウンロードされます。

The screenshot shows a REST client interface with a GET request to `https://10.102.29.58/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-vserver-ssl/actions/download``. The response is a YAML file with the following content:

```

1 PK ..... 2 com.example.ssl.stylebooks$0.1$lb-vserver-ssl.yamlName: lb-vserver-ssl
2 namespace: com.example.ssl.stylebooks
3 version: "0.1"
4 display-name: Load Balancing Virtual Server (SSL)
5 description: This stylebook defines a very simple load balancing SSL virtual server configuration
6 schema-version: "1.0"
7 import-stylebooks:
8   -
9     namespace: netScaler.nitro.config
10    version: "10.5"
11    prefix: ns
12   -
13     namespace: com.citrix.adc.stylebooks
14     version: "1.0"
15     prefix: stlb
16 parameters:
17   -
18     prefix: ns
19   -
20     namespace: com.citrix.adc.stylebooks
21     version: "1.0"
22     prefix: stlb
23 parameters:
24   -

```

## API を使用してカスタム **StyleBook** を削除する

February 6, 2024

カスタム StyleBook を削除するには、次の StyleBook REST API を指定します。

```

1 DELETE
2
3 https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
  VERSION>/<NAME>?dependencies=true
4 <!--NeedCopy-->

```

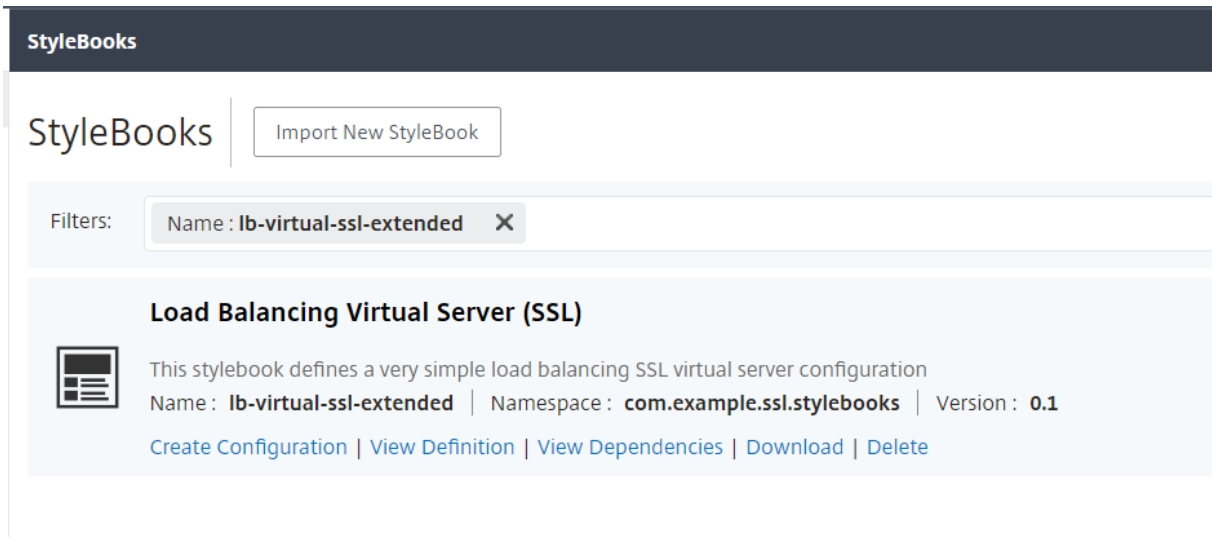
URL の依存関係クエリパラメータが指定されていないか、その値が `false` に設定されている場合、StyleBook の依存関係は削除されません（StyleBook 自体のみが削除されます）。

HTTP 応答ステータスコード 200 を受け取った場合は、カスタム StyleBook（およびその依存関係）が Citrix ADM から正常に削除されたことを意味します。

注:

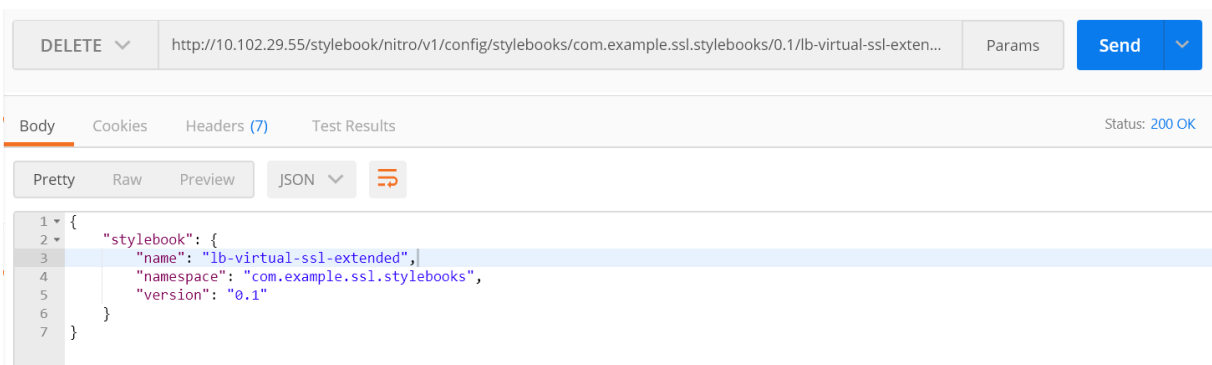
MA サービス内の他の StyleBook が依存しているカスタム StyleBook は削除できません。

たとえば、Citrix ADM で「lb-virtual-ssl-extended」という名前の StyleBook を作成したとします。後でその StyleBook を削除することにしました。

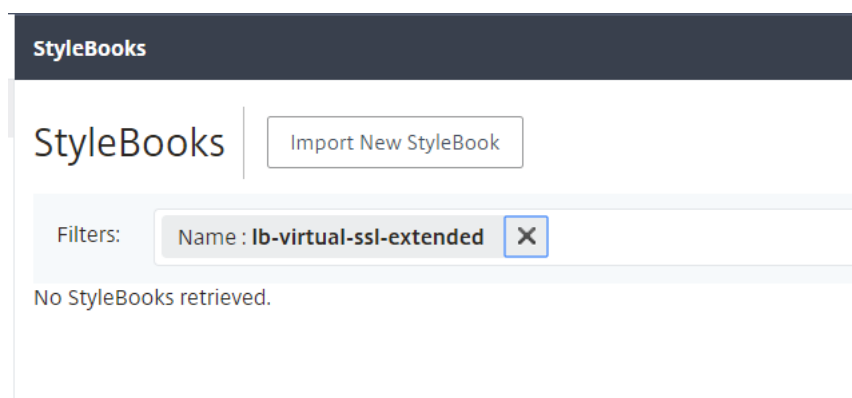


IP アドレス、名前、バージョン、名前空間のフィールドを変更した後は、curl コマンドラインツールや Postman chrome ブラウザ拡張機能など、どのツールでも API を実行できます。

<https://10.102.29.55/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-virtual-ssl-extended?dependencies=false> を削除する



StyleBook が NetScaler ADM から削除されます。



## StyleBook の文法

February 6, 2024

独自の StyleBook をデザインして CitrixApplication Delivery Management (ADM) にインポートし、Citrix ADM 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造および属性の文法と構文について理解しておく必要があります。

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造および参照について説明します。

次の表のセクション名、構造名、または参照名をクリックすると、詳細が表示されます。

|||

|—|

| [Header](/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/header-section.html) | [StyleBook のインポート](/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/import-stylebooks-section.html) |

| [Parameters](/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/parameters-section.html) | [パラメータデフォルトソース構成](/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/parameters-default-sources-construct.html) |

| [Substitutions](/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/substitutions.html) | [Components](/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/components.html) |

| [オプションのプロパティ](/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/optional-properties.html) | [ヘルパーコンポーネント](/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/helper-components.html) |

| [プロパティデフォルトソース](/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/properties-default-sources.html) | [ネストされたコンポーネント](/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/nested-components.html) |

| [\[条件構成\]](#)(/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/condition-construct.html) | [\[repeat 構造\]](#)(/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/repeat-construct.html) |  
| [\[繰り返し条件構成\]](#)(/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/repeat-condition-construct.html) | [\[Outputs\]](#)(/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/outputs.html) |  
| [\[ネストされた繰り返し\]](#)(/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/nested-repeats.html) | [\[親参照\]](#)(/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/parent-reference.html) |  
| [\[パラメータ参照\]](#)(/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/parameter-reference.html) | [\[置換参照\]](#)(/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/substitutions-reference.html) |  
| [\[コンポーネントのリファレンス\]](#)(/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/components-reference.html) | [\[Operations\]](#)(/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/operations.html) |  
| [\[変数参照\]](#)(/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/variable-reference.html) | [\[Alarms\]](#)(/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/alarms.html) |  
| [\[分析\]](#)(/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/analytics.html) | [\[組み込み関数\]](#)(/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/built-in-functions.html) |  
| [\[式\]](#)(/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/expressions.html) | [\[依存関係の検出\]](#)(/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/dependency-detection.html) |  
| [インブレース補間](#) |

#### 注

リポートアイテム、リポートインデックス、または置換関数の引数を定義する際には、次の予約語を使用してユーザー定義変数に \$ という名前を付けないでください。 <var-name>

- stylebook、parameters、substitutions、components、properties、outputs、parent、self、operations、analytics、alarms
- repeat-item、repeat-item-0、repeat-item-1、repeat-item-2
- repeat-index、repeat-index-0、repeat-index-1、repeat-index-2
- デフォルト
- roles、role、targets、target
- context、parent-context、parent\_context

独自の StyleBook を設計する方法とその例については、「[独自の StyleBook の作成方法](#)」を参照してください。

## Header

February 6, 2024

StyleBook の先頭の 6 行は、Header セクションです。このセクションでは、StyleBook の ID を定義し、StyleBook の実行内容を記述できます。これは必須セクションです。

次の表は、Header セクションの属性について説明しています。

| 属性                          | 説明                                                                                                                                                                                                                                    |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>name</code>           | StyleBook を識別する名前。この属性は必須です。                                                                                                                                                                                                          |
| <code>display-name</code>   | StyleBook を識別するための任意の名前。この名前は NetScaler ADM GUI に表示されます。これはオプションの属性です。                                                                                                                                                                |
| <code>説明</code>             | 説明テキストは、この StyleBook の機能を定義します。この説明は ADM GUI に表示されます。これはオプションの属性です。 <b>**注:**</b> これは HTML フラグメントで、HTML タグを使用して見出しをカスタマイズしたり、URL や埋め込み画像を含む <code>&lt;img&gt;</code> タグを使用して画像を挿入したりできます。                                             |
| <code>author</code>         | StyleBook を作成した作成者または組織。これはオプションの属性です。                                                                                                                                                                                                |
| <code>namespace</code>      | 名前空間は、StyleBook の一意の識別子の一部で、これにより名前の衝突を回避できます。namespace には任意の文字列を指定できますが、StyleBook のセットを作成したまたは所有している会社、部門または部署の名前を使用することをお勧めします。たとえば、次の形式を使用できます <code>&lt;company&gt;.&lt;department&gt;.&lt;unit&gt;.stylebooks</code> 。これは必須属性です。 |
| <code>version</code>        | StyleBook のバージョン番号。バージョン番号は、StyleBook の更新時に変更できます。異なるバージョンの StyleBook を共存させることができます。これは必須属性です。                                                                                                                                        |
| <code>schema-version</code> | StyleBook スキーマのバージョン。NetScaler ADM の現在のリリースでは「1.0」という値を使用します。これは必須属性です。                                                                                                                                                               |
| <code>private</code>        | この属性を <code>true</code> に設定すると、NetScaler ADM GUI に StyleBook は表示されません。これは、他の StyleBook の構築ブロックである StyleBook で有用な設定であり、ユーザーが直接使用するものではありません。これはオプションの属性です。デフォルト値は、 <code>false</code> です。                                              |

例:

```

1   name: lb
2   description: "This stylebook defines a sample load balancing
3   configuration."
4   display-name: "Load Balancing StyleBook (HTTP)"
5   author: Mike Smith (ACME Infra team)
6   namespace: com.example.stylebooks
7   schema-version: "1.0"
8   version: "0.1"
9   <!--NeedCopy-->
```

name、namespace、および version 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 ADM では、名前、名前空間、およびバージョンの組み合わせが同じ 2 つの StyleBook を使用することはできません。ただし、name と version が同じであっても namespace が異なる場合、または namespace と version が同じであっても name が異なる場合は、それらの 2 つの StyleBook を使用できます。

## StyleBook のインポート

February 6, 2024

これは StyleBook の第 2 セクションで、現在の StyleBook から参照するほかの StyleBook を宣言できます。このセクションを記述すると、他の StyleBook をインポートして再利用できるため、StyleBook で同じ構成を再作成する必要がなくなります。これは必須セクションです。

現在の StyleBook で参照する 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。いずれかの NITRO 構成オブジェクトを直接使用する場合、StyleBook では、netscaler.nitro.config 名前空間を必ず参照する必要があります。この名前空間には、lbserver サービスやモニターなど、すべての Citrix ADC NITRO タイプが含まれています。NetScaler ADC バージョン 10.5 以降の StyleBook がサポートされています。つまり、StyleBook を使用して、リリース 10.5 以降を実行するすべての NetScaler ADC インスタンス上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 **prefix** 属性は、名前空間とバージョンの組み合わせを示すための略語です。たとえば、「ns」プレフィックスを使用して、名前空間 netscaler.nitro.config とバージョン 10.5 を示すことができます。StyleBook の以降のセクションでは、StyleBook を名前空間とバージョンで示すたびにこの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 を一意に識別する名前を使用できます。

例:

```
1   import-stylebooks:
2   -
3     namespace: netscaler.nitro.config
4     version: "10.5"
5     prefix: ns
6   -
7     namespace: com.acme.stylebooks
8     version: "0.1"
9     prefix: stlb
10  <!--NeedCopy-->
```

上の例では、最初に定義されているプレフィックスは ns で、名前空間 netscaler.nitro.config とバージョン 10.5 を示します。2 番目に定義されているプレフィックスは stlb で、名前空間 com.acme.stylebooks とバージョン 0.1 を示します。

プレフィックスを定義した後は、特定の名前空間とバージョンに属するタイプまたは StyleBook を示すたびに、\*\*<名前空間の略語>::<タイプ名>\*\* という表記を使用できます。たとえば、\*\*ns::lbserver\*\* は、名前空間

netscaler.nitro.config、バージョン 10.5 で定義されているタイプ lbvserver を示します。タイプ名 > 名前空間の略語 >

同様に、com.acme.stylebooks 名前空間にあるバージョン「0.1」の StyleBook を示す場合は、\*\*stlb::\*\* という表記を使用できます。

注

慣例により、プレフィックス「ns」は、NetScaler ADC NITRO 名前空間を参照するために使用されます。

## パラメーター

February 6, 2024

このセクションでは、構成を作成するために必要な StyleBook のすべてのパラメーターを定義します。StyleBook では、このセクションに記述された入力を使用されます。このセクションはオプションですが、ほとんどの StyleBook には必要な場合があります。パラメータセクションを考慮して、StyleBook を使用して NetScaler ADC インスタンスで構成を作成するユーザーのフィールドを定義できます。

StyleBook を NetScaler ADM にインポートし、それを使用して構成を作成すると、GUI は StyleBook のこのセクションを使用してフォームを表示します。このフォームは、定義されたパラメータ値の入力を受け取ります。

次のセクションでは、このセクションの各パラメータに指定する必要がある属性について説明します。

### ‘名前’

定義するパラメーターの名前。英数字名を指定できます。

名前はアルファベットで始まる必要があり、さらに多くのアルファベット、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。

StyleBook を記述するときは、\$parameters.<name> という表記を使用して、この「名前」属性を使用して他のセクションのパラメータを参照できます。

必須? はい

### ‘ラベル’

ADM GUI でこのパラメータの名前として表示される文字列。

必須? いいえ



## ‘説明’

パラメーターの使用目的について説明するヘルプ文字列。ユーザーがこのパラメータのヘルプアイコンをクリックすると、ADM GUI にこのテキストが表示されます。

必須? いいえ

## ‘タイプ’

そのパラメーターで使用できる値のタイプ。パラメータには、次の組み込み型のいずれかを使用できます。

- **string**: 文字の配列。長さが指定されていない場合、文字列値には、任意の数の文字を使用できます。ただし、`min-length` 属性と `max-length` 属性を使用すれば、文字列タイプの長さを制限できます。
- **number**: 整数。 `min-value` 属性と `max-value` 属性により、このタイプで使用できる最小数と最大数を指定できます。
- **boolean**: 真または偽のどちらでもかまいません。YAML では、すべてのリテラルがブール値と見なされず (たとえば、`[はい]` または `[いいえ]`)。
- **ipaddress**: 有効な IPv4 または IPv6 アドレスを表す文字列。
- **tcp-port**: TCP または UDP ポートを表す 0 ~65535 の数値。
- **password**: 不透明/秘密の文字列値を表します。ADM GUI でこのパラメーターの値を表示すると、アスタリスク (\*\*\*\*\*) として表示されます。
- **certfile**: 証明書ファイルを表します。この値を使用すると、ADM GUI を使用して StyleBook 設定を作成するときに、ローカルシステムからファイルを直接アップロードできます。アップロードされた証明書ファイルは、ADM のディレクトリ `/var/mps/tenants/\<tenant_path>/ns_ssl_certs` に保存されます。

証明書ファイルは、ADM によって管理される証明書の一覧に追加されます。

- **keyfile**: 証明書キーファイルを表します。この値を使用すると、ADM GUI を使用して StyleBook 設定を作成するときに、ローカルシステムからファイルを直接アップロードできます。アップロードされた証明書ファイルは、ADM のディレクトリ `/var/mps/tenants/\<tenant_path>/ns_ssl_keys` に保存されます。

証明書キーファイルは、ADM によって管理される証明書キーの一覧に追加されます。

- **file**: ファイルを表します。
- **object**: この型は、親要素の下にいくつかの関連パラメータをグループ化する場合に使用されます。親パラメータのタイプを「object」として指定します。タイプが「object」のパラメーターにはネストされた「Parameters」セクションを含めることができ、そのセクションに含まれるパラメーターを記述できます。

- **another StyleBook:** このタイプのパラメータを使用する場合、このパラメータの値は、StyleBook で定義されたパラメータの形式で、その型を示します。

パラメータには、**type** 型のリストであるを持つこともできます。これを行うには、`[]` 型の末尾にを追加します。たとえば、**type** 属性が `string[]` の場合、このパラメータは文字列のリストを入力として受け取ります。この StyleBook から構成を作成するときは、このパラメータに対して 1 つまたは複数の文字列を指定できます。

必須? はい

### ‘network’

**type: ipaddress** では、ADM IPAM ネットワークから IP アドレスを自動割り当てる **network** 属性を指定できます。

ADM は、StyleBook 設定を作成するときに、**network** 属性から IP アドレスを自動的に割り当てます。

例:

```
1     name: virtual-ip
2     label: "Load Balancer IP Address"
3     type: ipaddress
4     network: "network-1"
5     required: true
6 <!--NeedCopy-->
```

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ます。IP アドレスは、構成が削除されると、ネットワークに解放されます。

### ‘dynamic-allocation’

**dynamic-allocation** 属性は、**type: ipaddress** のパラメータ定義に追加されます。ADM IPAM ネットワークを動的にリストするには、この属性を使用します。この属性は、**true** または **false** を入力として取ることができます。**type: ipaddress** では、ADM 内の ADM IPAM **dynamic-allocation: true** ネットワークを動的に一覧表示する属性を指定します。構成パック作成フォームでは、次の操作を実行できます。

1. リストから必要な IPAM ネットワークを選択します。
2. 選択した IPAM ネットワークから割り当てる IP アドレスを指定します。

IP アドレスが指定されていない場合、ADM は選択した IPAM ネットワークから IP アドレスを自動的に割り当てます。

例:

```
1     -
2     name: virtual-ip
3     label: "Load Balancer IP Address"
```

```
4     type: ipaddress
5     dynamic-allocation: true
6     required: true
7 <!--NeedCopy-->
```

この例では、`virtual-ip` フィールドには、ADM 内の ADM IPAM ネットワークが一覧表示されます。リストからネットワークを選択して、ネットワークから IP アドレスを自動割り当てます。設定が削除されると、IP アドレスはネットワークに解放されます。

### ‘key’

true または false を指定して、このパラメーターが StyleBook のキーパラメーターかどうかを示します。

StyleBook で「キー」パラメーターとして定義できるパラメーターは 1 つだけです。

同じ StyleBook から（同じまたは異なる ADC インスタンスで）異なる構成を作成する場合、各構成はこのパラメーターに対して異なる/一意の値を持ちます。

デフォルト値は false です。

必須? いいえ

### ‘required’

true または false を指定して、パラメーターが必須か、任意かを示します。true に設定した場合、パラメータは必須であり、ユーザーは構成の作成時にこのパラメータの値を指定する必要があります。

ADM GUI は、このパラメーターに有効な値を指定するようにユーザーを強制します。

デフォルト値は false です。

必須? いいえ

### ‘allowed-values’

型が「string」に設定されている場合、この属性を使用して、パラメータの有効な値のリストを定義します。

ADM GUI から構成を作成する場合、このリストからパラメータ値を選択するように求められます。

注:

リスト値をラジオオプションとして表示する場合は、`layout` 属性を設定します。

例 1:

```

1 -
2     name: ipaddress
3     type: string
4     allowed-values:
5         - SOURCEIP
6         - DEST IP
7         - NONE
8 <!--NeedCopy-->

```

**例 2:**

```

1 -
2     name: TCP Port
3     type: tcp-port
4     allowed-values:
5         - 80
6         - 81
7         - 8080
8 <!--NeedCopy-->

```

**サンプル 3:**

tcp-portsのリスト。リストの各要素は、で指定された値のみを持つことができます `allowed-values`。

```

1 -
2     name: tcpports
3     type: tcp-port[]
4     allowed-values:
5         - 80
6         - 81
7         - 8080
8         - 8081
9 <!--NeedCopy-->

```

必須? いいえ

**‘default’**

任意のパラメーターにデフォルト値を割り当てるには、この属性を使用します。ユーザーが値を指定せずに構成を作成すると、デフォルト値が使用されます。

次の条件が満たされた場合、パラメータは値を取れません。

- パラメータにはデフォルト値はありません。
- ユーザーは、パラメータの値を指定しません。

**例 1:**

```

1 -
2     name: timeout

```

```
3     type: number
4     default: 20
5 <!--NeedCopy-->
```

**例 2:**

パラメータのデフォルト値をリストするには、次の手順に従います。

```
1 -
2     name: protocols
3     type: string[]
4     default:
5         - TCP
6         - UDP
7         - IP
8 <!--NeedCopy-->
```

**サンプル 3:**

```
1 -
2     name: timeout
3     type: number
4     default: 20
5 <!--NeedCopy-->
```

**例 4:**

```
1 -
2     name: tcpport
3     type: tcp-port
4     default: 20
5 <!--NeedCopy-->
```

必須? いいえ

**‘pattern’**

この属性を使用して、パラメータの型が「string」の場合に、このパラメータの有効な値のパターン（正規表現）を定義します。

例:

```
1 -
2     name: appname
3     type: string
4     pattern: "[a-z]+"
5 <!--NeedCopy-->
```

必須? いいえ

### ‘min-value’

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:

```
1 -
2     name: audio-port
3     type: tcp-port
4     min-value: 5000
5 <!--NeedCopy-->
```

数字の`min-value`には負の値を指定できます。ただし、`tcp-port`の`min-value`は正でなければなりません。

必須? いいえ

### ‘max-value’

この属性を使用して、`number` 型または`tcp-port`のパラメータの最大値を定義します。

最大値が最小値より大きいことを確認します (定義されている場合)。

例:

```
1 -
2     name: audio-port
3     type: tcp-port
4     min-value: 5000
5     max-value: 15000
6 <!--NeedCopy-->
```

必須? いいえ

### ‘min-length’

この属性を使用して、「string」タイプ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は、ゼロ以上であることを確認します。

例:

```
1 -
2     name: appname
3     type: string
4     min-length: 3
5 <!--NeedCopy-->
```

必須? いいえ

### ‘max-length’

種類が「string」のパラメーターに入力できる値の最大文字数を定義するには、この属性を使用します。

値の最大長が、`min-length`で定義されている文字の長さ以上であることを確認します。

例:

```
1 -
2     name: appname
3     type: string
4     max-length: 64
5 <!--NeedCopy-->
```

必須? いいえ

### ‘min-items’

一覧となっているパラメーターの項目の最小数を定義するには、この属性を使用します。

アイテムの最小数がゼロ以上であることを確認します。

例:

```
1 -
2     name: server-ips
3     type: ipaddress[]
4     min-items: 2
5 <!--NeedCopy-->
```

必須? いいえ

### ‘max-items’

リストであるパラメータ内の項目の最大数を定義するには、この属性を使用します。

アイテムの最大数が、定義されている場合は、アイテムの最小数よりも大きいことを確認してください。

例:

```
1 -
2     name: server-ips
3     type: ipaddress[]
4     min-items: 2
```

```
5     max-items: 250
6 <!--NeedCopy-->
```

必須? いいえ

### ‘gui’

この属性を使用して、ADM 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? いいえ

### ‘columns’

この属性は、`gui` 属性のサブ属性です。この属性を使用して、ADM GUI で `type: object[]` パラメータを表示する列数を定義します。

必須? いいえ

### ‘updatable’

この属性は、`gui` 属性のサブ属性です。この属性を使用して、構成の作成後にパラメータを更新できるかどうかを指定します。この属性は、文字列、ブール、数値などの単純なパラメータタイプにのみ設定します。

値が `false` に設定されている場合、設定を更新すると、パラメータフィールドはグレー表示されます。

必須? 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が折りたたみ可能かどうかを指定します。

値を `true` に設定すると、ユーザーはこの親パラメーターの下にある子パラメーターを展開したり折りたたんだりできるようになります。

例:

```
1  gui:
2
3    collapse_pane: true
4
5    columns: 2
6 <!--NeedCopy-->
```

Parameters セクション全体の例:



```
1 parameters:
2
3   -
4
5     name: name
6
7     label: Name
8
9     description: Name of the application
10
11    type: string
12
13    required: true
14
15   -
16
17    name: ip
18
19    label: IP Address
20
21    description: The virtual IP address used for this application
22
23    type: ipaddress
24
25    required: true
26
27   -
28
29    name: svc-servers
30
31    label: Servers
32
33    type: object[]
34
35    required: true
36
37    parameters:
38
39      -
40
41        name: svc-ip
42
43        label: Server IP
44
45        description: The IP address of the server
46
47        type: ipaddress
48
49        required: true
50
51      -
52
53        name: svc-port
```

```
54
55     label: Server Port
56
57     description: The TCP port of the server
58
59     type: tcp-port
60
61     default: 80
62
63     -
64
65     name: lb-alg
66
67     label: LoadBalancing Algorithm
68
69     type: string
70
71     allowed-values:
72
73         - ROUNDROBIN
74
75         - LEASTCONNECTION
76
77     default: ROUNDROBIN
78
79     -
80
81     name: enable-healthcheck
82
83     label: Enable HealthCheck?
84
85     type: boolean
86
87     default: true
88 <!--NeedCopy-->
```

次の例では、一覧のすべての属性と、前のセクションで説明した値を定義しています。

```
1     -
2         name: features-list
3
4         type: string[]
5
6         min-length: 1
7
8         max-length: 3
9
10        min-items: 1
11
12        max-items: 3
13
14        pattern: "[A-Z]+"
15
```

```

16         allowed-values:
17
18             - SP
19
20             - LB
21
22             - CS
23
24         default:
25
26             - LB
27 <!--NeedCopy-->

```

### ‘layout’

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。`allowed-values` 属性を持つパラメータに適用されます。構成バックを作成すると、ADM GUI にラジオボタンとして `allowed-values` リストの値が表示されます。

例:

```

1 -
2     gui:
3         layout: radio
4         allowed-values:
5             - One
6             - Two
7             - Three
8 <!--NeedCopy-->

```

ADM GUI では、1、2、および 3 の値がラジオボタンとして表示されます。

### ‘dependent-parameters’

この属性は、`gui` 属性のサブ属性です。別のパラメータで指定された値に基づいて、StyleBook 設定フォームでのパラメータの外観または初期値を動的に制御します。

フォーム上でのパラメータの動作を制御するソースパラメータにこの属性を指定します。他のパラメータを制御する複数の条件を含めることができます。たとえば、`protocol` ソースパラメータには依存パラメータ `certificate` を指定できます。これは、`protocol` パラメータ値が `SSL` である場合にのみ表示されます。

各条件は、次の属性を持つことができます。

- **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で次のいずれかのアクションを指定します。
  - **read-only:** パラメーターは読み取り専用になります。
  - **show:** パラメーターが非表示の場合、フォームに表示されます。
  - **hide:** パラメーターがフォームから削除されます。
  - **set-value:** パラメーター値は、**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、ターゲットパラメーターの値。

ユーザー入力ソースパラメーターの指定された値と一致する場合、ターゲットパラメーターの外観または値は、指定されたアクションに従って変化します。

例:

```
1  -
2  name: lb-virtual-port
3  label: "Load Balanced App Virtual Port"
4  description: "TCP port representing the Load Balanced application"
5  type: tcp-port
6  gui:
7    updatable: false
8    dependent-parameters:
9      -
10     matching-values:
11       - 80
12     target-parameter: $parameters.lb-service-type
13     action: set-value
14     allowed-values:
15       - HTTP
16       - TCP
17       - UDP
18
19     default: 80
20
21 <!--NeedCopy-->
```

この例では、依存パラメータはパラメータ (**lb-virtual-port** ソースパラメータ) の下に指定されています。

ソースパラメーターの値が80に設定されている場合、**lb-service-type**パラメーターは**set-value**アクションをトリガーします。その結果、ユーザーは次のいずれかのオプションを選択できます。

- HTTP
- TCP
- UDP

## パラメータ-デフォルトソース構成

February 6, 2024

この構造を使用すると、ほかの StyleBook のパラメータ定義を再利用できます。

パラメータまたはパラメータグループを複数の StyleBook で繰り返し使用するシナリオについて考えてみます。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ことを避けるために、パラメータを一度定義してから、**parameters-default-sources** 構造を使用して、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、StyleBook の多くで仮想 IP を構成する必要がある場合は、新しく作成する各 StyleBook で仮想 IP に関連する同じパラメータの定義が必要になることがあります。代わりに、「vip-params」のような名前の StyleBook を別途作成し、この StyleBook で次の例に示すように、仮想 IP に関連するすべてのパラメータを定義できます。

```
1      -
2      name: vip-params
3      namespace: com.acme.commonypes
4      version: "1.0"
5      description: This StyleBook defines a typical virtual IP config.
6      private: true
7      schema-version: "1.0"
8      parameters:
9      -
10     name: lb-appname
11     label: Load Balanced Application Name
12     description: Name of the Load Balanced application
13     type: string
14     required: true
15     -
16     name: lb-virtual-ip
17     label: Load Balanced App Virtual IP address
18     description: Virtual IP address representing the Load
19     Balanced application
20     type: ipaddress
21     required: true
22     -
23     name: lb-virtual-port
24     label: Load Balanced App Virtual Port
25     description: TCP port representing the Load Balanced
26     application
27     type: tcp-port
28     default: 80
29     -
30     name: lb-service-type
31     label: Load Balanced App Protocol
32     description: Protocol used for the Load Balanced application
33     type: string
34     default: HTTP
```

```
33         required: true
34         allowed-values:
35             - HTTP
36             - SSL
37             - TCP
38 <!--NeedCopy-->
```

その後、これらのパラメーターを使用するその他の StyleBook を作成できます。以下に、このような StyleBook の例を示します。

```
1     -
2     name: acme-biz-app
3     namespace: com.acme.stylebooks
4     version: "1.0"
5     description: This stylebook defines the Citrix ADC configuration
6     for Biz App
7     schema-version: "1.0"
8     import-stylebooks:
9         -
10            namespace: com.acme.commontypes
11            prefix: cmtypes
12            version: "1.0"
13            parameters-default-sources:
14                - cmtypes::vip-params
15            parameters:
16                -
17                    name: monitorname
18                    label: Monitor Name
19                    description: Name of the monitor
20                    type: string
21                    required: true
22                -
23                    name: type
24                    label: Monitor Type
25                    description: Type of the monitor
26                    type: string
27                    required: true
28                    allowed-values:
29                        - PING
30                        - TCP
31                        - HTTP
32                        - HTTP-ECV
33                        - TCP-ECV
34                        - HTTP-INLINE
35 <!--NeedCopy-->
```

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をインポートします。次に、**parameters-default-sources** 構造を追加して、StyleBook 名、つまり vip-params を指定します。これにより、StyleBook vip-params のパラメーターをこの StyleBook で直接定義するのと同じ効果が得られます。

parameters-default-sources は一覧であり、一覧の各項目が StyleBook であると想定されるので、複数の

StyleBook のパラメーターを含めることができます。

ほかの StyleBook のパラメーターを含めることができるだけでなく、Parameters セクションを使用して独自のパラメーターを定義することもできます。StyleBook のパラメーターの一覧全体は、ほかの StyleBook のパラメーターとこの StyleBook で定義したパラメーターの組み合わせになります。したがって、式 **\$parameters** はこのパラメーターの組み合わせを参照します。

パラメーターがインポートした StyleBook と現在の StyleBook の両方で定義されている場合は、現在の StyleBook 内の定義によって別の StyleBook からインポートした定義が上書きされます。インポートしたパラメーターの一部を必要に応じてカスタマイズし、残りのパラメーターをそのまま使用することで、この動作を効果的に活用できます。

parameters-default-sources 構造は、次に示すようにネストされたパラメーターでも使用できます。

```

1 parameters:
2   -
3     name: vip-details
4     label: Virtual IP details
5     description: Details of the Virtual IP
6     type: object
7     required: true
8     parameters-default-sources:
9       - cmtypes::vip-params
10 <!--NeedCopy-->
```

これは、StyleBook vip-params のパラメーターをこの StyleBook の vip-details パラメーターの子パラメーターとして直接追加する場合と同様です。

## 自動置換

February 6, 2024

Substitutions セクションは、StyleBook のほかの部分で StyleBook を読み取りやすくするために使用できる、複雑な式の省略名を定義するために使用されます。また、このセクションは、StyleBook で同じ式または値を複数回使用する場合にも役立ちます（定数値など）。この値に置換名を使用すると、この値を変更する必要があるときに、StyleBook に出現するすべての箇所では値を更新するのではなく（この方法ではエラーが発生しやすくなります）、置換値のみを更新できます。

置換は、このドキュメントの後の例で示すように、値のマッピングの定義にも使用できます。

一覧の各置換はキーと値で構成されます。値には、単純な値、式、関数、またはマップを指定できます。

次の例では、2つの置換が定義されています。1つ目は、8181の省略名として使用できる「http-port」です。置換を使用することで、この値を StyleBook のほかの部分で、8181ではなく **\$substitutions.http-port** として参照できるようになります。

置換:

http-port: 8181

これにより、ポート番号のニーマニック名を指定できるほか、その使用回数に関係なく、このポート番号を StyleBook 内の 1 か所で定義できます。ポート番号を 8080 に変更する場合は、Substitutions セクションで変更すると、ニーマニック名 http-port を使用しているすべての箇所にその変更が適用されます。次の例は、コンポーネントで置換を使用する方法を示しています。

```

1 components:
2   -
3     name: my-lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: $parameters.name + "-lb"
7       servicetype: HTTP
8       ipv46: $parameters.ip
9       port: \*\*$substitutions.http-port\*\*
10      lbmethod: $parameters.lb-alg
11 <!--NeedCopy-->

```

置換は複雑な式にすることもできます。次の例は、2 つの置換で式を使用する方法を示しています。

```

1 substitutions:
2   app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS
3   app-name: str("acme-") + $parameters.name + str("-app")
4 <!--NeedCopy-->

```

また、置換式では、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。

```

1 substitutions:
2   http-port: 8181
3   app-name: str("acme-") + $parameters.name + str($substitutions.http-
4     port) + str("-app")
5 <!--NeedCopy-->

```

置換のもう 1 つの便利な機能がマップで、キーを値にマップできます。以下は、マップ置換の例です。

```

1 substitutions:
2   secure-port:
3     true: int("443")
4     false: int("80")
5   secure-protocol:
6     true: SSL
7     false: HTTP
8 <!--NeedCopy-->

```

次の例は、マップ secure-port および secure-protocol を使用する方法を示しています。

```

1 components:
2   -
3     name: my-lbvserver-comp
4     type: ns::lbvserver

```



```

5     properties:
6         name: $parameters.name + "-lb"
7         servicetype: $substitutions.secure-protocol[$parameters.is-
secure]
8         ipv46: $parameters.ip
9         port: $substitutions.secure-port[$parameters.is-secure]
10        lbmethod: $parameters.lb-alg
11 <!--NeedCopy-->

```

つまり、StyleBook のユーザーがパラメーター `is-secure` にブール値「true」を指定するか、Citrix ADM GUI でこのパラメーターに対応するチェックボックスを選択した場合、このコンポーネントの `servicetype` プロパティには **SSL** という値が割り当てられ、ポートプロパティには値 **443** が割り当てられます。ただし、ユーザーがこのパラメーターに「false」を指定するか、Citrix ADM GUI の対応するチェックボックスをオフにすると、`servicetype` プロパティには **HTTP** という値が割り当てられ、ポートには **80** という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 つまたは複数の引数を取ることができます。引数は、string、number、ipaddress、boolean などの単純な型にする必要があります。

置換:

```
form-lb-name(name): $name + "-lb"
```

この例では、「name」という文字列引数を取り、それを使用して名前引数の文字列に「-lb」\*\* という接尾辞を付けた新しい文字列を作成する置換関数「form-lb-name」を定義します。この置換関数を使用する式は、次のように記述することができます。

```
$substitutions.form-lb-name("my" )
```

これは、「my-lb」を返します。

別の例を考えてみましょう。

置換:

```
cspol-priority(priority): 10100 - 100 * $priority
```

置換 `cspol-priority` は、`priority` という引数を受け取って値の計算に使用する関数です。StyleBook のほかの部分で、この置換を次の例に示すように使用できます。

```

1  components:
2    -
3      name: cspolicy-binding-comp
4      type: ns::csvserver_cspolicy_binding
5      condition: not $parameters.is-default
6      properties:
7        name: $parameters.csvserver-name
8        policyname: $components.cspolicy-comp.properties.policyname
9        priority: $substitutions.cspol-priority($parameters.pool.
priority)
10 <!--NeedCopy-->

```

置換は、キーと値で構成することもできます。値には、単純な値、式、関数、マップ、一覧、またはディクショナリを指定できます。

以下は、値がリストである 'slist' という置換の例です。

```
1 substitutions:
2   slist:
3     - a
4     - b
5     - c
6 <!--NeedCopy-->
```

置換の値には、以下の「sdict」という置換の例に示すように、キーと値のペアのディクショナリも指定できます。

```
1 substitutions:
2   sdict:
3     a: 1
4     b: 2
5     c: 3
6 <!--NeedCopy-->
```

一覧とディクショナリを組み合わせると、もっと複雑な属性を作成できます。たとえば、「slistofdict」という名前の置換はキーと値のペアの一覧を返します。

```
1 slistofdict:
2   -
3     a: $parameters.cs1.lb1.port
4     b: $parameters.cs1.lb2.port
5   -
6     a: $parameters.cs2.lb1.port
7     b: $parameters.cs2.lb2.port
8 <!--NeedCopy-->
```

しかし、次の例では、置換「sdictoflist」はキーと値のペアを返します。ここでも値は別の一覧です。

```
1 sdictoflist:
2   a:
3     - 1
4     - 2
5   b:
6     - 3
7     - 4
8 <!--NeedCopy-->
```

コンポーネントでは、これらの置換は condition、properties、repeat、repeat-condition 構造で使用できます。

次のコンポーネントの例では、置換を使用して properties を指定する方法を示します。

```
1 properties:
2   a: $substitutions.slist
3   b: $substitutions.sdict
4   c: $substitutions.slistofdict
```

```

5     d: $substitutions.sdictionarylist
6 <!--NeedCopy-->

```

値が一覧またはディクショナリの置換を定義するユースケースは、コンテンツスイッチ仮想サーバーや複数の負荷分散仮想サーバーを構成する場合です。同一の cs 仮想サーバーに関連付けられたすべての lb 仮想サーバーはまったく同じ構成を持つことができるため、置換一覧およびディクショナリを使用してこの構成を作成し、各 lb 仮想サーバーでの構成の繰り返しを避けることができます。

次の例では、コンテンツスイッチ仮想サーバー構成を作成する cs-lb-mon StyleBook の置換とコンポーネントを示します。cs-lb-mon StyleBook のプロパティを構成しながら、複雑な置換「lb-properties」で 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、サービスの種類、仮想 IP アドレス、ポート、サーバーをパラメーターとして取り、値としてキーと値のペアを生成する関数です。「cs-pools」コンポーネントで、この置換の値を各プールの lb-pool パラメーターに割り当てます。

```

1 substitutions:
2   cs-port[]:
3     true: int("80")
4     false: int("443")
5   lb-properties(name, servicetype, vip, port, servers):
6     lb-appname: $name
7     lb-service-type: $servicetype
8     lb-virtual-ip: $vip
9     lb-virtual-port: $port
10    svc-servers: $servers
11    svc-service-type: $servicetype
12    monitors:
13      -
14        monitorname: $name
15        type: PING
16        interval: $parameters.monitor-interval
17        interval_units: SEC
18        retries: 3
19  components:
20    -
21      name: cs-pools
22      type: stlb::cs-lb-mon
23      description: | Updates the cs-lb-mon configuration with the
24                    different pools provided. Each pool with rule result in a dummy LB
25                    vserver, cs action, cs policy, and csvserver_cspolicy_binding
26                    configuration.
27      condition: $parameters.server-pools
28      repeat: $parameters.server-pools
29      repeat-item: pool
30      repeat-condition: $pool.rule
31      repeat-index: ndx
32      properties:
33        appname: $parameters.appname + "-cs"
34        cs-virtual-ip: $parameters.vip
35        cs-virtual-port: $substitutions.cs-port($parameters.protocol == "
36                    HTTP")
37        cs-service-type: $parameters.protocol

```

```

34     pools:
35     -
36         lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP"
37         , "0.0.0.0", 0, $pool.servers)
38         rule: $pool.rule
39         priority: $ndx + 1
40 <!--NeedCopy-->

```

#### 置換マップ:

キーを値にマップ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）を定義するシナリオを考えてみましょう。このタスクでは、次のように置換マップを記述します。

```

1 substitutions:
2   port:
3     HTTP: 80
4     DNS: 53
5     SSL: 443
6 <!--NeedCopy-->

```

この例では、HTTP は 80 に、DNS は 53 に、SSL は 443 にマップされます。パラメーターとして与えられた特定のプロトコルのポートを取得するには、次の式を使用します。

`$substitutions.port [$parameters.protocol]`

この式は、ユーザーが指定したプロトコルに基づいて値を返します。

- キーが HTTP の場合、この式は 80 を返します。
- キーが DNS の場合、この式は 53 を返します。
- キーが SSL の場合、この式は 443 を返します。
- キーがマップ内に存在しない場合、この式はいずれの値も返しません。

## コンポーネント

February 6, 2024

StyleBook の `components` 構造は、StyleBook で最も重要なセクションです。このセクションでは、作成する必要がある構成オブジェクトを定義します。この構造を使用すると、同じ種類の構成オブジェクトを 1 つまたは複数作成できます。

`components` 構造では、Parameters セクションの入力値を使用して、StyleBook で生成される構成に適合させることができます。このセクションはオプションですが、ほとんどの StyleBook で Components セクションが記述されています。

次の表は、コンポーネントの主要な属性を示しています。

| 属性 | 説明 |

|---|

| name | コンポーネントの名前。英数字名を指定できます。名前はアルファベットで始まる必要があり、追加でアルファベット、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。 |

| 説明 | StyleBook におけるこのコンポーネントの役割の説明。 |

| 種類 | このコンポーネントで指定するプロパティはタイプによって決まります。コンポーネントには 2 種類のタイプがあります。 \*\* 組み込みタイプ \*\*: このタイプはシステムによって提供され、定義する必要はありません。たとえば、NITRO エンティティタイプ「lbvserver」や「servicegroup」などです。コンポーネントに組み込みの type 属性がある場合、NetScaler ADC 上にそのタイプの構成オブジェクトが作成されます。たとえば、コンポーネントが組み込みタイプ「lbvserver」を参照している場合、このコンポーネントは、構成の対象である Citrix ADC インスタンス上に負荷分散仮想サーバーを作成します。 \*\* 複合タイプ \*\*: このタイプは、作成して NetScaler ADM にインポートした既存の StyleBook を指します。コンポーネントにコンポジットタイプ属性がある場合、参照先の StyleBook で指定されているすべての構成オブジェクトが、構成のターゲットである NetScaler ADC インスタンスに作成されます。これにより、それぞれが最終構成の一部を作成する複数の StyleBook を組み合わせ使用できるようになります。複合 StyleBook について詳しくは、「[複合 StyleBook の作成](/ja-jp/netscaler-application-delivery-management-software/13/stylebooks/how-to-create-custom-stylebooks)」を参照してください。 |

| properties | コンポーネントの type 属性で使用できるサブ属性。コンポーネントに対して有効なプロパティは、そのタイプによって決まります。組み込みタイプの場合、有効なプロパティは対応する NITRO オブジェクトのプロパティまたは属性です。コンポーネントのタイプが別の StyleBook である場合（つまり複合タイプの場合）、プロパティはその StyleBook で定義されているパラメーターに対応します。 |

例:

```

1 components:
2   -
3     name: my-lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: $parameters.name
7       servicetype: HTTP
8       ipv46: $parameters.ip
9       port: 80
10      lbmethod: $parameters.lb-alg
11 <!--NeedCopy-->

```

この例では、my-lbvserver-comp という名前のコンポーネントが定義されています。このコンポーネントのタイプは、ns::lbvserver（組み込みタイプ）です。ここで「ns」は、import-stylebooks セクションで指定された名前空間の netscaler.nitro.config とバージョン 10.5 を示すプレフィックス、「lbvserver」は、この名前空間の 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 4 つの必須属性と 1 つのオプション属性 (lbmethod) が含まれています。そのため、これらの属性の値を指定できます。この例では、servicetype と port には静的な値が指定されていますが、name、ipv46、および lbmethod の各プロパティは、入力パラメーターから値を取得しま

す。parameters セクションで定義されているパラメータ名は、\$parameters を使って参照します。\

#### 注

NITRO リソースの種類の属性名（コンポーネントのプロパティ）には、小文字を使用する必要があります。そうしないと、StyleBook のインポートに失敗します。

## ヘルパーコンポーネント

February 6, 2024

StyleBook のコンポーネントセクションの主な用途は、Nitro 組み込みタイプ、または実際の構成オブジェクトを作成する他の StyleBook を使って、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、それ自身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を入力として、それらを他の形式に変換します。これが後に他のコンポーネントで使用されて、実際の構成オブジェクトが生成されます。ヘルパーコンポーネントには 2 種類あり、オブジェクトタイプとコンポーネントセクションを含まない他の StyleBook です。

次の例は、Citrix ADC インスタンスでモニター（lb-mon-comp）を使用して負荷分散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。

```
1 parameters:
2   -
3     name: appname
4     type: string
5   -
6     name: ips
7     type: ipaddress[]
8   -
9     name: vip
10    type: ipaddress
11
12 components:
13   -
14     name: help-comp
15     type: cmtypes::server-ip-port-params
16     repeat:
17       repeat-list: $parameters.ips
18       repeat-item: server-ip
19     properties:
20       ip: $server-ip
21       port: 80
22   -
23     name: lb-mon-comp
24     type: stlb::lb-mon
25     properties:
```

```

26     lb-appname: $parameters.appname
27     lb-virtual-ip: $parameters.vip
28     lb-virtual-port: 80
29     lb-service-type: HTTP
30     svc-service-type: HTTP
31     svc-servers: $components.help-comp.properties
32 <!--NeedCopy-->

```

パラメーターセクションにはアプリケーションの名前と負荷分散サーバーの IP アドレスを入力することができます。lb-mon-comp コンポーネントセクションでは、lb-mon StyleBook の svc-servers パラメーターには、それぞれの項目が ip と port の 2 つのサブパラメーターを持つオブジェクトの一覧が预期されます。

ただし、この StyleBook のパラメーターセクションは、\$parameters.ips を使ってサーバー IP のみを受け取ります。この StyleBook では、すべてのサーバーがポート 80 で実行されると想定されています。lb-mon StyleBook を使って負荷分散構成を作成するには、\$parameters.ips をオブジェクトの一覧に変換する必要があります。これは上記の例ではヘルパーコンポーネント、help-comp を使って実現されます。help-comp コンポーネントのタイプは server-ip-port-params StyleBook です。この StyleBook はコンポーネントを持ちません。結果として、構成オブジェクトを作成しません。help-comp は \$parameters.ips 上にリピート一覧を作成し、\$parameters.ips の各項目に対して ip と port (80 に静的に設定) からなるオブジェクトを構築します。そうして help-comp は IP アドレスの一覧を、後で lb-mon-comp で svc-servers プロパティを割り当てるために使用できるオブジェクトの一覧に変換します。help-comp の結果は、lb-mon-comp の svc-servers プロパティに割り当てられます。

## オプションのプロパティ

February 6, 2024

コンポーネントのプロパティは、式からその値を取得する場合があります。式はパラメーター参照などの単純式の場合もあれば、より複雑な式の場合もあります。このプロパティ値の設定は、コンポーネントではオプションです。式から実際の値が返される場合にのみプロパティの値を設定し、値が返されない場合はこのプロパティを設定しなくてもかまいません。

たとえば、設定するプロパティの 1 つが、型を ns::lbserver とするコンポーネントの lbmethod (負荷分散アルゴリズム) であるとします。プロパティ lbmethod の値は、次に示すようにユーザーが指定したパラメーター値から取得されます。

```

1  components
2    -
3    name: lbserver_comp
4    type: ns::lbserver
5    properties:
6      name: $parameters.lb-appname + "-lb"
7      servicetype: $parameters.lb-service-type
8      ipv46: $parameters.lb-virtual-ip
9      port: 80
10     lbmethod: $parameters.lb-advanced.algorithm

```

```
11 <!--NeedCopy-->
```

ここで、パラメータ **lb-advanced.algorithm** がオプションのパラメータであることを考えてみましょう。また、オプションであるためにユーザーがこのパラメータの値を指定しない場合、式 **\$parameters.lb-advanced.algorithm** は空白の値に評価されます。そのため、lbmethod プロパティに無効な値が渡されます。このような状況を回避するには、次のようにプロパティ名に「?」のサフィックスを付けて、プロパティにオプションであることを示す注釈を付けることができます。

```
1 components
2   -
3     name: lbvserver_comp
4     type: ns::lbvserver
5     properties:
6       name: $parameters.lb-appname + "-lb"
7       servicetype: $parameters.lb-service-type
8       ipv46: $parameters.lb-virtual-ip
9       port: 80
10      lbmethod?: $parameters.lb-advanced.algorithm
11 <!--NeedCopy-->
```

「?」を使用すると、右側の式がなしに評価された場合、このプロパティは省略されます。この例では、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。

```
1 components
2   -
3     name: lbvserver_comp
4     type: ns::lbvserver
5     properties:
6       name: $parameters.lb-appname + "-lb"
7       servicetype: $parameters.lb-service-type
8       ipv46: $parameters.lb-virtual-ip
9       port: 80
10 <!--NeedCopy-->
```

**lbmethod** はオプションであるため、それを省略しても有効なコンポーネントになります。lbmethod は、「ns::lbvserver」型で定義されている場合、そのデフォルト値を取得する場合があります。

## プロパティ-デフォルトソース構成

February 6, 2024

properties-default-sources 構造は parameters-default-sources 構造に似ています。parameters-default-sources 構造では StyleBook で（他の StyleBook から）既存のパラメーターを再利用できますが、properties-default-sources 構造ではユーザーが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できます。

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される可能性があります。たとえば、オブジェクトのパラメーター、オブジェクトを返す置換、ほかのコンポーネントのプロパティ、またはほかのコ



コンポーネントの出力からプロパティが取得されることがあります。このような場合は、コンポーネントの定義で、StyleBook のほかのセクションで発生するプロパティを再定義する必要があります。明らかに、これは冗長でエラーにつながる可能性があります。この問題に対応するために、`properties-default-sources` 構造を使用できます。`properties-default-sources` 構造は、各項目がコンポーネントのプロパティのソースを識別する一覧です。

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、以下のように `lbvserver` のプロパティを定義する必要があります。

```

1 parameters:
2   -
3     name: lb
4     type: ns::lbvserver
5 components:
6   -
7     name: lb-comp
8     type: ns::lbvserver
9     properties:
10      name: $parameters.lb.name
11      ipv46: $parameters.lb.ipv46
12      port: $parameters.lb.port
13      servicetype: $parameters.lb.servicetype
14      lbmethod: $parameters.lb.lbmethod
15 <!--NeedCopy-->

```

上記の例では、`components` セクションで定義されているすべてのプロパティの値は `$parameters.lb` オブジェクトから取得されていることに注目してください。これらのプロパティは 1 つのソースから取得されますが、StyleBook で再定義されています。さらに、`lbvserver` の構成に関連する `$parameters.lb` オブジェクトに新しいサブパラメーターが追加された場合は、新しいサブパラメーターに対応する新しいプロパティを追加するために `lb-comp` コンポーネントを更新する必要があります。

プロパティの再定義を避け、コンポーネントのすべての関連プロパティを `properties` セクションで明示的にリストすることなく取得するために、`properties-default-sources` 構造を使用できます。上の例は、次のように記述することもできます。

```

1 parameters:
2   -
3     name: lb
4     type: ns::lbvserver
5 components:
6   -
7     name: lb-comp
8     type: ns::lbvserver
9     properties-default-sources:
10      - $parameters.lb
11 <!--NeedCopy-->

```

上の例では、`properties-default-sources` 構造を使用することでコンポーネント定義のサイズが小さくなり、そのためにコンポーネントを簡潔に定義できています。さらに、コンポーネントのプロパティのソースが変更されるたびに、変更内容が自動的に反映されます。たとえば、「`persistesetype`」という名前の新しいプロパティが

`$parameters.lb` オブジェクトに追加された場合、`persistencetype` は `lbserver` のプロパティであるため、デフォルトで `lb-comp` の構成に追加されます。このように、`properties-default-sources` 構造は、コンポーネントのプロパティのソースに対して行われる変更を気にすることなくコンポーネントを定義できる動的なインターフェイスを提供します。

### コンポーネントのプロパティの計算

このセクションでは、コンポーネントで `properties-default-sources` 構造を使用し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。はじめに、StyleBooks コンパイラがコンポーネントの種類（上の例では `lbserver`）に基づいてコンポーネントのプロパティの一覧を識別します。次に、コンパイラはこれらのプロパティを複数のソースから（コンポーネントの `properties-default-sources` セクションに）定義されている順に取得します。プロパティが複数のソースに存在する場合は、最後のソースに出現するプロパティがほかのプロパティより優先されます。最後に、`properties-default-sources` 構造を使用して取得されたプロパティは、コンポーネントの `properties` セクションで上書きすることができます。`component` セクションの定義は、少なくとも `properties-default-sources` セクションまたは `properties` セクションを持つ必要があることに気付くことが重要です。両方のセクションを持つこともできます。

### ネストされたコンポーネント

February 6, 2024

コンポーネントを別のコンポーネント内にネストした場合、ネストされたコンポーネントは、親コンポーネントによって作成される構成オブジェクトまたはコンテキストを参照してそ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オブジェクトが作成されるたびに、1 つまたは複数のオブジェクトを作成できます。コンポーネントを別のコンポーネント内にネストしても、作成される構成オブジェクト間に関係は生じません。ネストを使用すると、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作成するコンポーネントのタスクが容易になります。

例:

```
1 components:
2   -
3     name: my-lbserver-comp
4     type: ns::lbserver
5     properties:
6       name: $parameters.name + "-lb"
7       servicetype: HTTP
8       ipv46: $parameters.ip
9       port: 80
10      lbmethod: $parameters.lb-alg
11      components:
12        -
```

```

13     name: my-svcg-comp
14     type: ns::servicegroup
15     properties:
16         name: $parameters.name + "-svcgrp"
17         servicetype: HTTP
18     components:
19         -
20             name: lbvserver-svg-binding-comp
21             type: ns::lbvserver_servicegroup_binding
22             properties:
23                 name: $parent.parent.properties.name
24                 servicegroupname: $parent.properties.name
25             -
26                 name: members-svcg-comp
27                 type: ns::servicegroup_servicegroupmember_binding
28                 repeat:
29                     repeat-list: $parameters.svc-servers
30                     repeat-item: srv
31                 properties:
32                     ip: $srv
33                     port: str($parameters.svc-port)
34                     servicegroupname: $parent.properties.name
35 <!--NeedCopy-->

```

この例では、複数レベルのネストが使用されています。コンポーネント `my-lbvserver-comp` が、`my-svcg-comp` という名前の子コンポーネントを持っています。また、`my-svcg-comp` コンポーネントは、その内部に2つの子コンポーネントを持っています。`my-svcg-comp` コンポーネントは、組み込みの NITRO リソースタイプ「サービスグループ」の属性に値を指定することにより、Citrix ADC 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、親コンポーネントが作成したサービスグループと、さらにその親のコンポーネントが作成した負荷分散仮想サーバー (lbvserver) をバインドするために使用されます。`$parent` 表記 (親参照とも呼ばれる) は、親コンポーネント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、親コンポーネントが作成したサービスグループにサービス一覧をバインドするために使用されます。このバインドを実行するには、StyleBook の `repeat` 構造を使用して、`svc-servers` パラメーターに指定されたサービス一覧を反復処理します。`repeat` 構造については、「[repeat 構造](#)」を参照してください。

同じ構成オブジェクトを、コンポーネントのネストを使用せずに作成することもできます。追加の情報および例については、「[基本的な負荷分散の構成を作成するための StyleBook](#)」を参照してください。

## 条件構成

February 6, 2024

`condition` 構造を使用すると、コンポーネントを条件付きにすることができます。`condition` 構造の値は、`true` または `false` に評価されるブール式です。条件が `true` になる場合、このコンポーネントを使用して構成オブジェクトが

作成されます。条件が `false` になる場合、このコンポーネントはスキップされ、構成オブジェクトの作成には使用されません。多くの場合、ブール式はパラメーター値に基づきます。

例:

```
1 components:
2   -
3     name: servicegroup-comp
4     type: ns::servicegroup
5     condition: $parameters.svc-server-ips
6     properties:
7       name: $parameters.name + "-svcgrp"
8       servicetype: HTTP
9 <!--NeedCopy-->
```

この例では、ユーザーがオプションのパラメーター `svc-server-ips` に値を指定すると、StyleBook エンジンによってコンポーネント `servicegroup-comp` が処理されます。条件が `false` になる場合、つまり、ユーザーがこのパラメーターに値を指定しなかったためにこのパラメーターに `null` 値が割り当てられ、`false` に評価された場合は、StyleBook エンジンでこのコンポーネントの存在が無視され、サービスグループは作成されません。

ブール式は、StyleBook でサポートされる任意の有効な式に基づいて設定できます（たとえば、別のコンポーネントが存在するかどうかや、パラメーターに特定の値が指定されているかどうかなど）。

次の例では、条件が `true` に評価された場合に、NITRO タイプ `ns::systemfile` の構成オブジェクトを作成します。

例:

```
1     components
2       -
3         name: pem_key_files
4         type: ns::systemfile
5         condition: "$components.der-certificate-files-comp or
6 $components.pem-certificate-files-comp"
7         properties:
8           filecontent: $certificate.keyfile.contents
9           fileencoding: "BASE64"
10          filelocation: "/nsconfig/ssl"
11          filename: $certificate.keyfile.filename
12 <!--NeedCopy-->
```

この例では、条件は複雑な「OR」式です。StyleBook 内の他の 2 つのコンポーネントが処理されている（スキップされていない）場合にのみ、この構成オブジェクトを StyleBook で作成し、コンポーネント間の依存関係を作成します。

## repeat 構造

February 6, 2024

コンポーネントの **repeat** 構造を使用して、同じタイプの複数の構成オブジェクトを作成できます。

次の例では、**members-svcg-comp** コンポーネントは、親コンポーネントが作成したサービスグループにサービス一覧をバインドするために使用されます。各サーバーをサービスグループにバインドする構成オブジェクトを作成するには、**repeat** 構造を使用して、**svc-servers** パラメーターに指定されたサービス一覧を反復処理します。繰り返し処理中に、コンポーネントはサービスグループ内の各サービス (繰り返し項目構造では **\*\*srv** と呼ばれる) に **servicegroup\_servicegroupmember\_binding** タイプの NITRO オブジェクトを作成し、各 NITRO オブジェクトの IP 属性を対応するサービスの IP アドレスに設定します。 \*\*

例:

```

1 components:
2   -
3     name: my-lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: $parameters.name + "-lb"
7       servicetype: HTTP
8       ipv46: $parameters.ip
9       port: 80
10      lbmethod: $parameters.lb-alg
11      components:
12        -
13          name: my-svcg-comp
14          type: ns::servicegroup
15          properties:
16            name: $parameters.name + "-svcgrp"
17            servicetype: HTTP
18          components:
19            -
20              name: lbvserver-svg-binding-comp
21              type: ns::lbvserver\servicegroup\binding
22              properties:
23                name: $parent.parent.properties.name
24                servicegroupname: $parent.properties.
25              name
26            -
27              name: members-svcg-comp
28              type: ns::servicegroup\servicegroupmember\
29              binding
30              repeat:
31                repeat-list: $parameters.svc-servers
32                repeat-item: srv
33              properties:
34                ip: $srv
35                port: $parameters.svc-port
36                servicegroupname: $parent.properties.
37              name
38      <!--NeedCopy-->

```

リピートはそれ自体がオブジェクトであり、\*\* リピートリストとリピートアイテムはリピートオブジェクトの属性です \*\*。

- `repeat-list` は、コンポーネントが反復する一覧を識別する必須の属性です。
- `repeat-item` はオプションで、反復処理中の現在の項目にフレンドリ名を付けるために使用されます。

指定しない場合は、**`$repeat-item`** という式を使用して現在のアイテムにアクセスできます。上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：

```

1      -
2      name: members-svcg-comp
3      type: ns::servicegroup_servicegroupmember_binding
4      repeat:
5          repeat-list: $parameters.svc-servers
6      properties:
7          ip: $repeat-item
8          port: $parameters.svc-port
9          servicegroupname: $parent.properties.name
10     <!--NeedCopy-->
```

リスト上で現在の項目を白く反復して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できます。次の例では、**`repeat-index`** を使用して、現在のインデックスに基づいてポート番号を計算します。

```

1      name: services
2      type: ns::service
3      repeat:
4          repeat-list: $parameters.app-services
5          repeat-item: srv
6      properties:
7          ip: $parameters.app-ip
8          port: $parameters.base-port + repeat-index
9          servicegroupname: $parent.properties.name
10     <!--NeedCopy-->
```

**`repeat-item`** 構文と同様に、イテレーションの現在のインデックスを参照する別の変数名を割り当てることができます。前の例は次の例と同等です：

```

1      -
2      name: services
3      type: ns::service
4      repeat:
5          repeat-list: $parameters.app-services
6          repeat-item: srv
7          repeat-index: idx
8      properties:
9          ip: $parameters.app-ip
10         port: $parameters.base-port + $idx
11         servicegroupname: $parent.properties.name
12     <!--NeedCopy-->
```

## 繰り返し条件構成

February 6, 2024

repeat-condition 構造は repeat 構造の反復処理ごとに評価され、その結果によって、構成オブジェクトをその反復処理で作成するか次の反復処理に進むかが決定されます。次の例は、repeat-condition 構造の使用方法を示しています。

例:

```
1 components
2   -
3     name: der-key-files-comp
4     type: ns::systemfile
5     repeat:
6     repeat-list: $parameters.certificates
7     repeat-item: certificate
8     repeat-condition: $certificate.ssl-inform == DER
9     properties:
10    filecontent: base64($certificate.keyfile.contents)
11    fileencoding: BASE64
12    filelocation: /nsconfig/ssl
13    filename: $certificate.keyfile.file
14 <!--NeedCopy-->
```

この例では、der-key-files-comp コンポーネントはユーザーが指定したすべての証明書を反復処理しますが、DER エンコーディングの証明書に対応する構成オブジェクトのみを作成します。反復処理ごとに repeat-condition 式が評価され、証明書のエンコーディングのタイプが DER かどうかテストされます。タイプが DER でない場合、現在の反復処理では構成オブジェクトは作成されず、反復処理は一覧の次の証明書に進みます。

## ネストされた繰り返し

February 6, 2024

repeat 構造をネストにして使用することで、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 repeat 構造を含めることができます。2 レベルのネストになった repeat 構造を考えます。外側のリスト (最初の repeat-list) の要素ごとに、内側のリスト (2 番目の repeat-list) の要素すべてに対して repeat リストを作成できます。StyleBook コンパイラでは、ネストになった repeat は最大で 3 つまでサポートされます。各 repeat レベルには、repeat-item 属性および repeat-index 属性を関連付けます。repeat-item 属性と repeat-index 属性はともにオプションです。また、repeat ごとに repeat-condition を指定することもできます。

例:

```
1 parameters:
```

```

2  -
3      name: vips
4      type: ipaddress[]
5  -
6      name: vip-ports
7      type: tcp-port[]
8  components:
9  -
10     name: lbvservers-comp
11     type: ns::lbserver
12     repeat:
13         repeat-list: $parameters.vips
14         repeat-item: ip
15         repeat:
16             repeat-list: $parameters.vip-ports
17             repeat-item: port
18     properties:
19         name: str("lb-") + str($ip) + '-' + str($port)
20         servicetype: HTTP
21         ipv46: $ip
22         port: $port
23 <!--NeedCopy-->

```

上記の例では、`$parameters.vips` の項目ごとに、`$parameters.vip-ports` の項目すべてに対して反復処理を行います。つまり、`$parameters.vips` で指定した `ipaddress` ごとに、`$parameters.vip-ports` で指定したすべてのポートに対して `lbserver` 構成オブジェクトを作成します。properties セクションでは、IP アドレスとポートの組み合わせにプレフィックス「lb」を付けたオブジェクト名を定義しています。このため、反復処理のたびに、`$ip` と `$port` の結合により一意の IP アドレスとポート番号の組み合わせが定義されます。

`repeat-item` 属性を指定していない場合、コンパイラではこの属性のデフォルト値が生成されます。`repeat-item` のデフォルト値は、`repeat` レベルごとにそれぞれ `$repeat-item`、`$repeat-item-1`、`$repeat-item-2` となります。同様に、`repeat-index` 属性を指定していない場合、コンパイラではこの属性のデフォルト値が生成されます。`repeat-index` のデフォルト値は、`repeat` レベルごとにそれぞれ `$repeat-index`、`$repeat-index-1`、`$repeat-index-2` となります。

以下の例では、ネストになった `repeat` オブジェクトで `repeat-item` 属性および `repeat-index` 属性を指定していない場合の命名規則を示します。

例:

```

1  components:
2  -
3      name: lbvservers-comp
4      type: ns::lbserver
5      repeat:
6          repeat-list: $parameters.vips
7          repeat:
8              repeat-list: $parameters.vip-ports
9          properties:
10             name: str("lb-") + str($repeat-item) + '-' + str($repeat-item
-1)

```



```

11     servicetype: HTTP
12     ipv46: $repeat-item
13     port: $repeat-item-1
14 <!--NeedCopy-->

```

## 結果

February 6, 2024

Outputs セクションでは、StyleBook によってすべての構成オブジェクトが正常に作成された後にユーザーに公開する情報を指定します。StyleBook の Outputs セクションは、必要に応じて記述します。StyleBook で必ずしも出力を返す必要はありません。ただし、内部コンポーネントを出力として返すと、この StyleBook をインポートするすべての StyleBook の柔軟性が向上します。このことは、複合 StyleBook の作成時にわかります。

次の表は、Outputs セクションで使用する属性を示しています。

| 属性    | 説明                                     | 固定  |
|-------|----------------------------------------|-----|
| name  | 公開する構成オブジェクトに対応する出力の名前。                | はい  |
| 説明    | 出力について説明するテキスト文字列。                     | いいえ |
| value | この属性では、StyleBook によって返される値の抽出方法を指定します。 | はい  |

例:

```

1  outputs:
2  -
3    name: lbvserver
4    description: LBVServer component
5    value: $components.my-lbvserver-comp
6  -
7    name: svc-grp
8    description: ServiceGroup name
9    value: $components.my-svcg.properties.name
10 <!--NeedCopy-->

```

この例では、StyleBook で作成される **lbvserver** コンポーネントとサービスグループの名前 (**name**) を公開します。**lbvserver** という出力の値はコンポーネント **my-lbvserver-comp** です。同様に、**svc-grp** という出力の値は、コンポーネント **my-svcg** によって作成されたサービスグループの名前です。

## パラメータ参照

February 6, 2024

コンポーネント構成では、パラメーターセクションで定義されているパラメーターを`$parameters.<parametername>`表記法を使用して参照します。`<parametername>`それ自体にパラメーターが含まれている場合 (typeがobjectの場合)、表記法`$parameters.<parametername>.<sub-parametername>`などを使う必要があります。

例:

```
1 parameters:
2   -
3     name: name
4     label: Name
5     type: string
6     required: true
7     -
8     name: vip
9     label: Virtual IP and Port
10    type: object
11    required: true
12    parameters:
13      -
14        name: ip
15        label: Virtual IP
16        description: The Virtual IP Address
17        type: ipaddress
18        required: true
19        -
20        name: port
21        label: The Virtual Port
22        description: The TCP port for the Virtual IP
23        type: tcp-port
24        default: 80
25 components:
26   -
27     name: my-lbvserver-comp
28     type: ns::lbvserver
29     properties:
30       name: $parameters.name
31       servicetype: HTTP
32       ipv46: $parameters.vip.ip
33       port: $parameters.vip.port
34 <!--NeedCopy-->
```

## 親参照

February 6, 2024

ネストされたコンポーネントを使用している場合は、`$parent` 表記を使用して親コンポーネントを参照できます。親コンポーネントで `repeat` 構造を使用して複数の構成オブジェクトを作成し、反復処理ごとに子コンポーネントでほかの構成オブジェクトを作成する場合、`$parent` 表記は常に親コンポーネントの現在の反復処理を参照します。たとえば、`$parent.properties.name` は、親が現在の反復処理で作成する構成オブジェクトの `name` プロパティを参照します。

例:

```
1 components:
2   -
3     name: my-lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: $parameters.name + "-lb"
7       servicetype: HTTP
8       ipv46: $parameters.ip
9       port: 80
10      lbmethod: $parameters.lb-alg
11      components:
12        -
13          name: my-svcg-comp
14          type: ns::servicegroup
15          properties:
16            name: $parameters.name + "-svcgrp"
17            servicetype: HTTP
18            components:
19              -
20                name: lbvserver-svg-binding-comp
21                type: ns::lbvserver_servicegroup_binding
22                properties:
23                  name: $parent.parent.properties.name
24                  servicegroupname: $parent.properties.name
25                -
26                  name: members-svcg-comp
27                  type: ns::servicegroup_servicegroupmember_binding
28                  repeat: $parameters.svc-servers
29                  repeat-item: srv
30                  properties:
31                    ip: $srv
32                    port: str($parameters.svc-port)
33                    servicegroupname: $parent.properties.name
34 <!--NeedCopy-->
```

また、親の親のプロパティにアクセスしてコンポーネントの階層を上方向に移動し、最上位レベルのコンポーネントまで遡ることもできます。たとえば、コンポーネント **lbvserver-svg-binding-comp** のプロパティ名は、**\$parent.parent** 表記を使用して、その親の親である `my-lbvserver-comp` コンポーネントのプロパティ名から値

を取得します。

## コンポーネントのリファレンス

February 6, 2024

components コンストラクトでは、**\$components** を使って **StyleBook** の最上位コンポーネントを参照します。 \\$components という表記法が使用されます。 \

例:

```
1 components:
2   -
3     name: my-lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: $parameters.name + "-lb"
7       servicetype: HTTP
8       ipv46: $parameters.ip
9       port: 80
10      lbmethod: $parameters.lb-alg
11   -
12     name: my-svcg-comp
13     type: ns::servicegroup
14     properties:
15       name: $parameters.name + "-svcgrp"
16       servicetype: HTTP
17   -
18     name: members-svcg-comp
19     type: ns::servicegroup_servicegroupmember_binding
20     repeat: $parameters.svc-servers
21     repeat-item: srv
22     properties:
23       ip: $srv
24       port: str($parameters.svc-port)
25       servicegroupname: $components.my-svcg-comp.properties.name
26   -
27     name: lbvserver-svg-binding-comp
28     type: ns::lbvserver_servicegroup_binding
29     properties:
30       name: $components.my-lbvserver-comp.properties.name
31       servicegroupname: $components.my-svcg-comp.properties.name
32 <!--NeedCopy-->
```

この例では、**my-svcg-comp** コンポーネントと **my-lbvserver-comp** コンポーネントを作成してから、最後のコンポーネントである **lbvserver-svg-binding-comp** を作成する必要があります。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含まれるからです。これらの参照は、**\$components** で示されるコンポーネント参照を使用して提供されます。 \`<componentname\>`。

## 置換参照

February 6, 2024

コンポーネントセクションまたは操作セクションでは、代替セクションで定義されている代替を **\$substitutions.<substitution-name>** 表記法を使用して参照します。たとえば、**\$substitutions.http-port** のように指定します。

代替がマップの場合、マップ内のエレメントを **\$substitutions.<substitutions-name>[<map-key>]** と呼ぶことができます。たとえば、**\$substitutions.protocol-map[\$parameters.port]** のようになります。

## 変数参照

February 6, 2024

コンポーネントの `repeat` 構造と `repeat-item` 構造を使用して複数の構成オブジェクトを作成するときに、`repeat-item` 構造に変数名を割り当てることができます。その後、この変数は、そのコンポーネントのプロパティ内または子コンポーネント内の表記法 **\$\<varname\>** を使用して参照できます。コンポーネントで `repeat-item` 構造を省略して `repeat` 構造を使用する場合は、`$repeat-item` というデフォルトの変数を使用して反復処理項目にアクセスできます。

例:

```
1 components:
2   -
3     name: server-members-comp
4     type: ns::server
5     condition: $parameters.svc-server-domain-names
6     repeat: $parameters.svc-server-domain-names
7     repeat-item: server-name
8     properties:
9       name: $server-name + "-server"
10      domain: $server-name
11     components:
12       -
13         name: service-members-comp
14         type: ns::service
15         properties:
16           name: $server-name + "-service"
```

```
17     servername: $parent.properties.name
18     servicetype: $parameters.svc-service-type
19     port: $parameters.svc-server-port
20 <!--NeedCopy-->
```

上の例では、repeat-item 構造に変数名 server-name が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と子コンポーネント `$\langle varname \rangle` のプロパティで参照されます。

## オペレーション

February 6, 2024

操作は StyleBook のオプションセクションです。このセクションでは、すべてまたは一部のトラフィックトランザクションに関する AppFlow レコードを収集するように Citrix Application Delivery Management (ADM) 分析を構成できます。StyleBook を使用して NetScaler ADC インスタンス上に作成された仮想サーバーは、これらのトラフィックトランザクションを処理します。このセクションでは、仮想サーバーで特定のトラフィック条件が満たされたときにアラームをトリガーするように NetScaler ADM を構成することもできます。

StyleBooks を使用して NetScaler ADM を構成して、次のようにリストされているさまざまな NetScaler ADM Insights からトラフィック統計を収集できます。

- Web Insight
- Security Insight
- HDX Insight
- Citrix Gateway Insight

サポートされる仮想サーバーは、ロードバランシング、コンテンツスイッチング、および VPN 仮想サーバーです。

Web Insight と Security Insight の両方、またはどちらか一方を有効化して、負荷分散またはコンテンツスイッチング仮想サーバーの分析に使用します。ただし、VPN 仮想サーバーの場合は、HDX Insight と NetScaler Gateway Insight の両方を有効にする必要があります。

StyleBooks を介して NetScaler ADC インスタンス上で有効化された NetScaler ADM 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 ADC にデータを送信します。

また、Web Insight を有効にすると、負荷分散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の測定が有効になります。クライアント側の測定を有効にすると、ADM は HTML インジェクションを通じて HTML ページのロード時間とレンダリング時間メトリックをキャプチャします。管理者は、これらのメトリックスを使用して、L7 レイテンシーの問題を特定できます。

### 例 1:

次の例は、VPN 仮想サーバー上で HDX Insight と Citrix Gateway Insight の両方を有効にするための操作セクションを StyleBook に記述する方法を示しています。

```
1 name: simple-vpn-ops
2 namespace: com.example.stylebooks
3 schema-version: "1.0"
4 version: "0.1"
5 description: Test StyleBook to enable hdxinsight and gatewayinsight on
  a VPN vserver
6 import-stylebooks:
7   -
8     namespace: netScaler.nitro.config
9     version: "10.5"
10    prefix: ns
11  components:
12    -
13      name: vpnvserver-comp
14      type: ns::vpnvserver
15      properties:
16        name: str("vpn-") + str($current-target.ip)
17        servicetype: SSL
18        ipv46: 1.1.21.37
19        port: 443
20  operations:
21    analytics:
22      -
23        name: comp-ops
24        properties:
25          target: $components.vpnvserver-comp
26          filter: "true"
27          insights:
28            -
29              type: hdxinsight**
30            -
31              type: gatewayinsight
32  outputs:
33    -
34      name: myvpns
35      value: $components.vpnvserver-comp
36 <!--NeedCopy-->
```

**例 2:**

次の例は、StyleBook に操作セクションを記述して、負荷分散仮想サーバー上で Web Insight と SurityInsight の両方を有効にする方法を示しています。

```
1 name: simple-lb-ops
2 namespace: com.example.stylebooks
3 schema-version: "1.0"
4 version: "0.1"
5 description: Test StyleBook to enable webinsight and securityinsight on
  LB vserver
6 import-stylebooks:
7   -
8     namespace: netScaler.nitro.config
9     version: "10.5"
```

```

10     prefix: ns
11 components:
12     -
13         name: lbserver-comp
14         type: ns::lbserver
15         properties:
16             name: str("lb-") + str($current-target.ip)
17             servicetype: HTTP
18             ipv46: 1.1.21.37
19             port: 80
20 operations:
21     analytics:
22     -
23         name: comp-ops
24         properties:
25             target: $components.lbserver-comp
26             filter: "true"
27             insights:
28             -
29                 type: webinsight
30             -
31                 type: securityinsight
32 outputs:
33     -
34         name: mylbs
35         value: $components.lbserver-comp
36 <!--NeedCopy-->

```

## 分析

February 6, 2024

Operations セクションの analytics サブセクションには、Components セクションと似たような構造があります。分析セクションの各要素は、StyleBook によって作成された 1 つ以上の仮想サーバーの NetScaler ADM Analytics 機能を構成するために使用されます。

analytics セクションの要素には次の属性があります。

| 属性        | 説明                                         | 固定  |
|-----------|--------------------------------------------|-----|
| name      | 分析要素の名前。                                   | はい  |
| 説明        | この要素の内容を説明するテキスト文字列。                       | いいえ |
| condition | ブール式。この条件が false に評価された場合、分析要素全体がスキップされます。 | いいえ |



| 属性               | 説明                                                                                                                               | 固定  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------|-----|
| リピート             | リストを反復します。                                                                                                                       | いいえ |
| repeat-condition | ブール式。式が <code>false</code> に評価されると、現在の反復がスキップされます。                                                                               | いいえ |
| repeat-item      | 現在の反復の項目の名前。                                                                                                                     | いいえ |
| repeat-index     | 現在の反復の指数値の名前。                                                                                                                    | いいえ |
| properties       | 分析のプロパティの一覧。                                                                                                                     | はい  |
| target           | 一覧のいずれかのプロパティ。ターゲット表現は、分析が収集される NetScaler ADC で構成された仮想サーバーの名前です。                                                                 | はい  |
| filter           | 一覧のいずれかのプロパティ。この属性の値は、分析を収集する仮想サーバー上の要求をフィルタリングするために使用される NetScaler ADC の高度なポリシー表現です。デフォルトでは、分析データは仮想サーバーを通過するすべてのトラフィックで収集されます。 | いいえ |

例:

```

1 operations:
2   analytics:
3     -
4     name: lbvserver-ops-comp
5     properties:
6     target: $components-basic-lb-comp.outputs.lbvserver-name
7     filter: HTTP.REQ.URL.CONTAINS("catalog")
8   <!--NeedCopy-->

```

分析セクションの各属性を使用して、NetScaler ADM Analytics 機能に、ターゲットプロパティで識別される仮想サーバー上のアプリフローレコードを収集するように NetScaler ADC インスタンスを構成するように指示します。

## アラーム

February 6, 2024

Operations セクションの alarms サブセクションは、analytics サブセクションと同様の構造と同じ属性を持ちます。唯一異なるのは properties 属性です。(properties 属性以外の) すべての属性の一覧については、「[analytics](#)」を参照してください。

alarms サブセクションでは次のプロパティを使用できます。

| 属性            | 説明                                                                                 | 固定                                                    |
|---------------|------------------------------------------------------------------------------------|-------------------------------------------------------|
| target        | アラームが構成されている NetScaler ADC で構成された仮想サーバーの名前に評価される式。                                 | はい                                                    |
| email-profile | NetScaler ADM Analytics 機能で定義され、アラームがトリガーされたときに通知する電子メールアドレスのリストを含む電子メールプロファイルの名前。 | いいえ (email-profile または sms-profile のどちらかを定義する必要があります) |
| sms-profile   | NetScaler ADM Analytics 機能で定義され、アラームがトリガーされたときに通知する電話番号のリストを含む SMS プロファイルの名前。      | いいえ (email-profile または sms-profile のどちらかを定義する必要があります) |
| rules         | target プロパティで定義した仮想サーバーに対するアラームをトリガーする条件を定義する規則の一覧。                                | はい                                                    |
| metric        | rules の属性。NetScaler ADC 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      | rules の属性。測定基準と値の比較に使用する演算子。有効な演算子は「greaterthan」および「lessthan」です。                   | はい                                                    |
| value         | rules の属性。演算子を使用して測定基準と比較するしきい値。測定基準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                                                    |

| 属性          | 説明                                                                                                                                     | 固定 |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------|----|
| period-unit | rules の属性。アラームの規則条件が満たされている場合にユーザーに通知する頻度。day、hour、weekly の値を使用できます。つまり、規則条件が満たされている場合、アラームは period-unit に 1 回の頻度で送信されます (1 日に 1 回など)。 | はい |

次の表は、NetScaler ADC 仮想サーバーに関して追跡されるメトリックのリストを示しています。

カウンター | 説明 | 詳細な説明 | NetScaler ADM 計算

|---|---|

|VPN 仮想サーバーの場合: |

total\_requests|VPN セッションの合計起動数 | ユーザーが指定した期間内に、この VPN 仮想サーバーで起動されたアクティブなセッションの合計数。 | 新しいセッションの起動ごとに増分される、単調増加カウンター |

|app\_count|VPN アプリケーションの起動数 | ユーザーが指定した期間内に、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合計数。 | 新しいアプリケーションの起動ごとの単調増加カウンター |

|app\_launch\_duration|VPN アプリケーションの起動時間 | アプリケーションの起動にかかった平均時間 (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から算出された平均値 | |その他の仮想サーバー (CS、LB、Auth、GSLB) | |

Total\_requests| 要求数 | 要求数 | 前回のアプライアンスの再起動以降、または仮想サーバーの作成後のいずれか新しい方から、この仮想サーバーに対するクライアント要求の数。 | カウンタは単調に増加し、この仮想サーバーへの新しいリクエストごとに増加します。 ||

合計バイト | バイト | 指定された時間間隔に仮想サーバーから Citrix ADM に転送された合計バイト数。 | この仮想サーバーによって処理された合計バイト数を考慮して、カウンタが単調に増加している。 ||

アプリケーション\_ 応答時間 | 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後)、いずれか最後の方から、この仮想サーバーが受信したすべての要求の応答時間の平均値。 |

StyleBook の alarms セクションの例:

```

1 operations:
2   alarms:
3     -
4       name:lbvserver_alarm
5       properties:
6         target: $outputs.lbvserver
7         email-profile: $parameters.emailprofile
8         sms-profile: "NetScalerSMS"
9         rules:
10        -
11          metric: "total_requests"

```

```
12     operator: "greaterthan"
13     value: 25
14     period-unit: weekly
15     -
16     metric: "total_bytes"
17     operator: "lessthan"
18     value: 1024
19     period-unit: day
20
21 <!--NeedCopy-->
```

## 式

February 6, 2024

StyleBook の最も強力な機能の 1 つは、式の使用です。さまざまなシナリオで StyleBook の式を使用して動的な値を計算できます。次の例は、パラメータ値をリテラル文字列と連結する式です。

例:

```
1 $parameters.appname + "-mon"
2 <!--NeedCopy-->
```

この式は、`appname` という名前のパラメータを取得し、文字列 `-mon` と連結します。

次の種類の式がサポートされています。

### 算術式

- 加算 (+)
- 減算 (-)
- 乗算 (\*)
- 除算 (/)
- モジュロ (%)

例:

- 2 つの数字の加算: `$parameters.a + $parameters.b`
- 2 つの数字の乗算: `$parameters.a * 10`
- ある数を別の数で除算した後の余りを見つける:

5での結果15%10

## 文字列式

- 2つの文字列を連結する (+)

例:

2つの文字列を連結してください:`str(「app-」) + $parameters.appname`

## 式の一覧表示

2つのリスト (+) をマージします

例:

- 2つの一覧を連結: `$parameters.external-servers + $parameters.internal-servers`
- `$parameters.ports-1`が [80, 81] で、`$parameters.port-2`が [81, 82] の場合、`$parameters.ports-1 + $parameters.ports-2`はリスト [80、81、82] 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、それらが等しい場合は `true` を返し、それ以外の場合は `false` を返します。
- `!=`: 2つのオペランドが異なるかどうかをテストし、それらが異なっている場合は `true` を返し、それ以外の場合は `false` を返します。
- `>`: 最初のオペランドが2番目のオペランドより大きい場合は `true` を返し、それ以外の場合は `false` を返します。
- `>=`: 最初のオペランドが2番目のオペランド以上の場合は `true` を返し、それ以外の場合は `false` を返します。
- `<`: 最初のオペランドが2番目のオペランドより小さい場合は `true` を返し、それ以外の場合は `false` を返します。
- `<=`: 最初のオペランドが2番目のオペランド以下の場合は `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: `$parameters.name == "abcd"`
- 不等式演算子の使用: `$parameters.name != "default"`
- 他の関係演算子の例
  - `10 > 9`
  - `10 >= 10`
  - `0 < 9`

- $10 \leq 9$
- $10 == 10$
- $10 != 1$

### 論理式-ブール値

- **and**: 論理「and」演算子。両方のオペランドが true の場合、結果は true となり、それ以外の場合は false となります。
- **or**: 論理「or」演算子。いずれかのオペランドが true の場合、結果は true となり、それ以外の場合は false となります。
- **NOT**: 単項演算子。オペランドが真の場合、結果は偽になり、逆になります。
- **in**: 最初の引数が 2 番目の引数の部分文字列であるかどうかをテストします
- **in**: 項目がリストの一部であるかどうかをテストします

#### 注

文字列が数値に変換され、数字が文字列に変換されるタイプキャスト式を使用できます。同様に、`tcp-port` 数値にキャストすることも、IP アドレスを文字列にキャストすることもできます。

演算子の前と後に区切り文字を使用します。区切り記号は次のように使えます。

- 演算子の前: `space`、`tab`、`comma`、`(、)`、`[、]`
- 演算子のあと: `space`、`tab`、`(、`、`[`

例:

- `abc + def`
- `100 % 10`
- `10 > 9`

### 逐語的な文字列式

文字列内の特殊文字がリテラル形式を取る必要がある場合は、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、角かっこなどを含めることができます。逐語文字列では、特殊文字の通常の解釈はスキップされます。文字列内のすべての文字は、リテラル形式で保持されます。

StyleBooks では、逐語的な文字列を使用して、NetScaler ADC ポリシー式をリテラル形式で含めることができます。通常、ポリシー式には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間の文字列をカプセル化します。

```

1  ~{
2  string }
3  ~
4  <!--NeedCopy-->

```

StyleBook のどこにでも逐語的な文字列を使用できます。

注:

このシーケンスは逐語的な文字列の終わりを示すため、入力文字列には一連の文字 } ~ を使用しないでください。

例:

```

1  ~{
2  HTTP.REQ.COOKIE.VALUE("jsessionId") ALT HTTP.REQ.URL.BEFORE_STR("=").
   AFTER_STR(";jsessionid=") ALT HTTP.REQ.URL.AFTER_STR(";jsessionid="
   ) }
3  ~
4  <!--NeedCopy-->

```

## ターゲットエクスプレッション

StyleBook 定義では、`$current-target` 式を使用して、現在のターゲットの ADC インスタンスを参照できます。ターゲット ADC インスタンスの IP アドレスを具体的に参照するには、この式を次のように使用します。

```

1  $current-target.ip
2  <!--NeedCopy-->

```

例:

```

1  components:
2  -
3  name: lb-comp
4  type: ns::lbserver
5  properties:
6  name: $current-target.ip + "-lbserver"
7  <!--NeedCopy-->

```

この例では、`lbserver` という名前は、ターゲット ADC インスタンスの IP アドレスを使用して作成されます。

## 式の種類の検証

StyleBook エンジンでは、コンパイル時により強力な型チェックを行うことができます。つまり、StyleBook の作成時に使用される式は、設定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、置換、コンポーネント、コンポーネントのプロパティ、コンポーネントの出力、ユーザー定義変数 (`repeat-item`、`repeat-index`、置換関数への引数) などへの参照はすべて、その存在と型について検証されます。

タイプチェックの例:

次の例では、`lbvserver` StyleBook に期待されるポートプロパティのタイプは`tcp-port`です。NetScaler Application Delivery Management (ADM) では、タイプの検証はコンパイル時（インポート時）に行われます。コンパイラーはその文字列を検出し、`tcp-port`は互換性のない型であるため、StyleBook コンパイラーはエラーを表示し、StyleBook のインポートまたは移行に失敗します。

```

1 components:
2   -
3     name: lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: mylb
7       ipv46: 10.102.190.15
8       port: str("80")
9       servicetype: HTTP
10 <!--NeedCopy-->

```

この StyleBook を正常にコンパイルするには、コンパイラで以下を数値として宣言します。

`port: 80`

無効な式のフラグ付けの例:

以前のリリースでは、無効な式がプロパティ名に割り当てられている場合、コンパイラは無効な式を検出せず、StyleBook を NetScaler ADM にインポートすることができました。これで、この StyleBook が NetScaler ADM にインポートされると、コンパイラはこのような無効な式を識別し、フラグを付けます。その結果、StyleBook は NetScaler ADM へのインポートに失敗します。

この例では、`lb-sg-binding-comp`のコンポーネントの名前プロパティに割り当てられる式は`$components.lbvserver-comp.properties.lbvservername`です。ただし、コンポーネント`lbvserver-comp`には`lbvservername`と呼ばれるプロパティはありません。以前の NetScaler ADM リリースでは、コンパイラはこの式を許可し、正常にインポートされていました。実際の失敗はこの StyleBook を用いて構成パックを作成するときに起こります。ただし、インポート中にこの種のエラーが特定され、StyleBook は NetScaler ADM にインポートされません。このようなエラーを手動で修正し、StyleBooks をインポートします。

```

1 Components:
2   -
3     name: lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: mylb
7       ipv46: 10.102.190.15
8       port: 80
9       servicetype: HTTP
10  -
11  name: sg-comp
12  type: ns::servicegroup
13  properties:
14  servicegroupname: msg

```



```

15     servicetype: HTTP
16     -
17     name: lb-sg-binding-comp
18     type: ns::lbserver_servicegroup_binding
19     condition: $parameters.create-binding
20     properties:
21         name: $components.lbserver-comp.properties.lbservername
22         servicegroupname: $components.sg-comp.properties.servicegroupname
23 <!--NeedCopy-->

```

## インデックスの一覧

一覧のアイテムは直接インデックスすることでアクセスできます。

| 式                                                                                         | 説明                                                                                         |
|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| <code>\$components.test-lbs[0]</code>                                                     | test-lbs コンポーネントの最初のアイテムを参照します。                                                            |
| <code>\$components.test-lbs[0].properties.p1</code>                                       | test-lbs コンポーネントの最初のアイテムのプロパティ p1 を参照します。                                                  |
| <code>\$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname</code> | servicegroups コンポーネントの最初の項目からの出力である lbcomps コンポーネントの 2 番目の項目のプロパティ servicegroupname を参照します |

## インプレース補間

February 6, 2024

文字列の一部を、StyleBook 式で置き換えることができるようになりました。文字列式が StyleBook コンパイラで評価されるときに、StyleBook 式を使用した文字列の部分がその式の値で置き換えられます。文字列に StyleBook 式を含めるには、次のように記述します。

```
“...%{...}%...”
```

「%{」と「}%」で囲んだ文字が StyleBook 式となります。こうした式は、「インプレース補間」と呼ばれます。

例として、「lb-%{\$parameters.appname}%-svc」という StyleBook 式のインプレース補間を用いた文字列式を考えます。文字列式の値は、補間式の値によって決まります。**\$parameters.appname** に「app1」が割り当てられていることを考えてみましょう。次に、この文字列式は **lb-app1-svc** と評価されます。この機能を使用することで、値を文字列式に直接入力するのではなく、ユーザー定義値に応じて決めることができます。

インプレース補間の実用的な使用例としては、StyleBook のポリシー式のパラメーター化があります。HTTP URL に特定の語句（この例では「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記述するシナリオを考えます。

この場合、記述するポリシー式は「HTTP.REQ.URL.CONTAINS(\ "jpeg\" )」となります。

ここで、StyleBook に文字列パラメーター（この例では \$parameters.url-object）を追加して、HTTP URL のオブジェクトをパラメーター化できます。ポリシー式は、このパラメーターに基づいて記述する必要があります。この目的を達成するには、文字列連結を使用します。式は次のようになります。

```
str( "HTTP.REQ.URL.CONTAINS(\"" + $parameters.url-object + "\" )" )
```

\$parameter.url-object に「csv」が代入されている場合、上記の式の値は「HTTP.REQ.URL.CONTAINS(\ "csv\" )」となります。しかし、こうした式は読みにくいものです。インプレース補間を使用することで、こうしたパラメーター化を読みやすくわかりやすいものにすることができます。

インプレース補間を使用した式は次のようになります。

```
str( "HTTP.REQ.URL.CONTAINS(%{quotewrap($parameters.url-object)}%)" )
```

上記の式では、インプレース補間を使用して \$parameters.url-object の値の前後に内部引用を追加しています。この式の結果は先ほどのものと同じですが、より直感的で、実際の結果に近い形になっています。

#### 補間式内で使用できる型

補間式の内側では、boolean、number、tcp-port、ipaddress、および string の各型の値が生成される式を使用できます。生成された値は、補間式が結果に置き換えられるときに自動で文字列へ変換されます。

文字列式には補間を含めないことも、1 個以上の補間を含めることもできます。順次補間で、文字列式の各部分を異なる StyleBook 式に置き換えることができます。たとえば、文字列 lb-%{\$parameters.appname}%-%{\$parameters.vip}% では、\$parameters.appname が「app1」、\$parameters.vip が「1.1.1.1」の場合、lb-app1-1.1.1.1 が返されます。

文字列式では、入れ子補間もサポートされています。つまり、補間式を別の補間式の内側に入れ子にして、ある式の値を別の式の入力にすることができます。

たとえば、「% {lb-% {\$parameters.port + 1}%}%」という文字列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入れ子になっています。

以下の表に、さまざまな種類の補間を例と対応する結果とともに示します。例で使用しているパラメーターの値は次のとおりです。

- \$parameters.appname: “lb1”
- \$parameters.vip: “1.1.1.1”
- \$parameters.n1: 1
- \$parameters.n2: 3

単純な補間

| 式                                          | 結果         |
|--------------------------------------------|------------|
| lb- <code>{parameters.appname}</code> -def | lb-lb1-def |

自動型変換

| 式                                   | 結果         |
|-------------------------------------|------------|
| lb- <code>{1}</code> %              | lb-1       |
| lb- <code>{parameters.vip}</code> % | lb-1.1.1.1 |
| lb- <code>{true}</code> %           | lb-True    |

順次補間

| 式                                                                                               | 結果      |
|-------------------------------------------------------------------------------------------------|---------|
| <code>{parameters.appname}</code> %-% <code>{str</code><br><code>{parameters.appname}}</code> % | lb1-lb1 |
| lb- <code>{1}</code> %-% <code>{2}</code> %                                                     | lb-1-2  |

入れ子補間

| 式                                                                                  | 結果     |
|------------------------------------------------------------------------------------|--------|
| <code>{abc-% {parameters.n1 + 1}}</code> %                                         | abc-2  |
| <code>str( “%{abc-%{parameters.n1}}</code> %-%<br><code>{parameters.n2}</code> ” ) | bc-1-3 |

## quotewrap を使用した補間

| 式                                                                              | 結果                                                                                                      |
|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| <code>str( "%{quotewrap(abcd)}%" )</code>                                      | "abcd"                                                                                                  |
| <code>str( "%{quotewrap(https://)} % +HTTP.REQ.HOSTNAME+HTTP.REQ.URL" )</code> | "«code class=" language-plaintext highlighter-rouge" >https://" +HTTP.REQ.HOSTNAME+HTTP.REQ.URL</code>" |

### 補間式のエスケープ文字列

文字「% {」または「}%」が文字列の一部である場合、StyleBook コンパイラがこれらを補間タグとして評価しないように、エスケープ文字として「\」を指定する必要があります。

例:

`str( "%{\%{ + str($parameters.vip) + }\}%%" )` returns `"%{1.1.1.1}%"` if `$parameters.vip` is `1.1.1.1`

以下の表に、その他の式と結果を示します。

| カテゴリ     | 式                                                   | 結果                  |
|----------|-----------------------------------------------------|---------------------|
| 補間のエスケープ | <code>str( "%{str(\$parameters.n1) + }%}" )</code>  | <code>1}%</code>    |
|          | <code>lb-%{str(\$parameters.n1) + }%}"</code>       | <code>lb-1}%</code> |
|          | <code>" %{str(\$parameters.n1) + \" }%\" }%"</code> | <code>1}%</code>    |

## 組み込み関数

February 6, 2024

StyleBook の式では組み込み関数が使用できます。

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することもできます。

`int($parameters.priority)`

以下は、StyleBook の式でサポートされる組み込み関数とその使用例の一覧です。

## **str()**

`str()` 関数は、入力引数を文字列値に変換します。

許可される引数の種類は次のとおりです。

- `string`
- `number`
- `TCP-port`
- **`boolean`**
- `IP address`

例:

- `"set-" + str(10)` 関数は `"set-10"` を返します。
- `str(10)` 関数は `10` を返します。
- `str(1.1.1.1)` 関数は `1.1.1.1` を返します。
- `str(True)` 関数は `"True"` を返します。
- `str(ADM)` 関数は `"mas"` を返します。

## **int()**

この `int()` 関数は、文字列、数値、IP アドレス、または `tcpport` を引数として取り、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()**

`bool()` 関数は、引数として任意の型を取ります。引数の値が `false`、空の場合、または存在しない場合、この関数は `false` を返します。

それ以外の場合は、`true` を返します。

例:

- `bool(true)` 関数は `true` を返します。
- `bool(false)` 関数は `false` を返します。
- `bool($parameters.a)` 関数は、`$parameters.a` が `false`、空、または存在しない場合に `false` を返します。

## len()

`len()` 関数は、引数として文字列またはリストを受け取り、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:

次のように置換を定義した場合、

```
items: ["123", "abc", "xyz"]
```

`len($substitutions.items)` 関数は 3 を返します

### 例 2:

`len("Citrix ADM")` 関数は 10 を返します。

### サンプル 3:

`$parameters.vips` に 値 `['1.1.1.1', '1.1.1.2', '1.1.1.3']` が ある 場 合、`len($parameters.vips)` 関数は 3 を返します。

## min()

`min()` 関数は、リストまたは一連の数値または `tcp-ports` を引数として受け取り、最小の項目を返します。

一連の番号/`tcp` ポートを使用する例:

- `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。

番号/`tcp`-ポートのリストを持つ例:

- サポート `$parameters.ports` は、`tcp-ports` のリストであり、次の値を持ちます: `[80, 81, 8080]`。

`min($parameters.ports)` 関数は 80 を返します。

## max()

`max()` 関数は、引数として、リストまたは一連の数値または `tcp-ports` のいずれかを取って、最大の項目を返します。

一連の番号/`tcp` ポートを使用する例:

- `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。

番号/`tcp`-ポートのリストを持つ例:

- サポート `$parameters.ports` は `tcp-ports` のリストであり、次の値があります: [80, 81, 8080]。

`max($parameters.ports)` 関数は8080を返します。

## bin()

`bin()` 関数は、引数として数値を取り、バイナリ形式で数値を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()

`oct()` 関数は、引数として数値を取り、8進形式で数値を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()

`hex()` 関数は、引数として数値を取り、16進数形式で数値を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()

`lower()`関数は、引数として文字列を受け取り、小文字で同じ文字列を返します。

例:

`lower("ADM")`関数は`adm`を返します。

## upper()

`upper()`関数は、引数として文字列を受け取り、大文字で同じ文字列を返します。

例:

`upper("Citrix ADM")`関数は`CITRIX ADM`を返します。

## sum()

この`sum()`関数は、数値のリストまたは`tcpports`を引数として取り、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:

置換:

```
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()

`pow()`関数は、引数として2つの数字を取り、2番目の1の累乗に上げられた最初の引数を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、引数として整数、文字列、またはIPアドレスを受け取り、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` 関数に文字列を指定します。

`ip('2.1.1.1')` 関数は `2.1.1.1` を返します

- `ip` 関数に整数を指定します。

- `ip(12)` 関数は `0.0.0.12` を返します。

- `ip` 関数で文字列として整数を指定すると、入力と同等の IP アドレスを返します。

`ip('1025')` 関数は `0.0.4.1` を返します。

この関数は、整数の加算および減算操作もサポートし、結果の IP アドレスを返します。

- 追記: `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。

- 加算と減算を組み合わせる: `ip('1.1.1.1') + ip('1.1.1.1') - ip(2)` は `2.2.2.0` を返します。

## **base64.encode()**

`base64.encode()` この関数は、文字列引数を受け取り、base64 でエンコードされた文字列を返します。

例:

`base64.encode("abcd")` 関数は `YWJjZA==` を返します。

## **base64.decode()**

`base64.decode` 関数は、base64 でエンコードされた文字列を引数として取り、デコードされた文字列を返します。

例:

`base64.decode("YWJjZA==")` 関数は `abcd` を返します。

## **exists()**

`exists()` 関数は、任意の型の引数を受け取り、ブール値を返します。入力に値がある場合戻り値は `True` です。戻り値は、入力引数が値を持たない場合 (つまり、値がない場合) `False` です。

`$parameters.monitor` はオプションのパラメータであるとし、構成パックの作成時にこのパラメータに値を指定すると、(`$parameters.monitor`) 関数は `True` を返します。

それ以外の場合は、`False`を返します。

## **filter()**

`filter()`関数は2つの引数を取ります。

引数 1: 1つの引数を受け取ってブーリアン型の値を返す置換関数です。

引数 2: 一覧です。

この関数は、最初の引数の置換関数に渡されたときに各要素が`True`に評価される元のリストのサブセットを返します。

例:

置換関数を次のように定義したとします。

Substitutions:

`x(a): $a != 81`

この関数は、入力値が81と等しくない場合に `True` を返します。それ以外の場合は、`False`を返します。

`$parameters.ports`を `[81, 80, 81, 89]`と想定します。

`filter($substitutions.x, $parameters.ports)`は、リストからすべての81のオカレンスを削除して `[80, 89]`を返します。

## **if-then-else()**

`if-then-else()`関数は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`と評価された場合、関数は引数 2 として指定された式の値を返します。

それ以外の場合は、引数 3 が指定されている場合、この関数は引数 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:

`$parameters.servicetype`が値`HTTP`を持っている場合、`if-then-else($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:

`if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport)` 関数は、`$parameters.servicetype`がHTTP値を持っている場合、`$parameters.hport`の値を返します。

それ以外の場合、関数は`$parameters.sport`の値を返します。

サンプル 3:

`$parameters.servicetype`が値HTTPを持っている場合、`if-then-else($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()

`join()`関数は、次の2つの引数を取ります。

引数 1: 数値、`tcp-ports`、文字列、または IP アドレスのリスト

引数 2: 区切り文字列 (オプション)

この関数は、引数 1 として指定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 として提供される区切り文字列で区切られています。引数 2 を指定しない場合、リスト内の要素は 1 つの文字列として結合されます。

例:

- `$parameters.ports`は[81, 82, 83]です。
  - デリミタ引数付き:  
`join($parameters.ports, '-')`関数は81-82-83を返します。
  - デリミタ引数なし:  
`join($parameters.ports)`関数は818283を返します。

## split()

`split()`関数は、指定された区切り文字に応じて、複数のリストに入力文字列を分割します。セパレータを指定しなかったり、空白(' ')を指定した場合、この関数はスペースをセパレータとみなし、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、連続空間を 1 つのスペースとみなします。

## map()

`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: 要素の一覧

この関数は、リスト内の各要素は、引数 2 の対応する要素に `map()` 関数 (引数 1) を適用した結果であるリストを返します。

引数 1 で許可される関数は次のとおりです。

- 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`
- 1 つ以上の引数を受け取る置換関数。

例:

`$parameters.nums` が `[81, 82, 83]` だと仮定します。

- Map using a built-in function, `str`

`map(str, $parameters.nums)` 関数は `["81", "82", "83"]` を返します

`map` 関数の結果は文字列の一覧であり、文字列の各要素は、入力した一覧 (`$parameters.nums`) の対応する要素に `str` 関数を適用して処理されています。

- 置換関数を使用した `map`

- Substitutions:

```
add-10(port): $port + 10
```

- 表現:

```
map($substitutions.add-10, $parameters.nums) 関数は、数値のリストを返します。 [ 91, 92, 93 ]
```

このマップ関数の結果は、数字のリストであり、各要素は、入力リスト (`$parameters.nums`) 内の対応する要素に置換関数 `$substitutions.add-10` を適用することによって計算されます。

## quotewrap()

`quotewrap()`関数は、引数として文字列を受け取り、入力値の前後に二重引用符を追加した後に文字列を返します。

例:

`quotewrap("ADM")`関数は `"mas"`を返します

## replace()

`replace()`関数は、次の3つの引数を取ります。

引数 1: 文字列

引数 2: 文字列またはリスト

引数 3: 文字列 (オプション)

この関数は、引数 1 中にある引数 2 のすべてのアイテムを引数 3 で置き換えます。

引数 3 が指定されていない場合、引数 2 のすべての出現は引数 1 から削除されます (つまり、空の文字列に置き換えられます)。

文字列の一部を、別の文字列の一部で置き換えます。

- `replace('abcdef', 'def', 'xyz')`関数は`abcxyz`を返します。  
`def`のすべてのオカレンスは`xyz`に置き換えられます。
- `replace('abcdefabc', 'def')`は`abcabc`を返します。  
3番目の引数がないので、結果の文字列から`def`が削除されます。

置換する文字リストを文字列で指定します。

```
$parameters.sp1_chars = ['@', '#', '!', '%']
```

このリストには、入力文字列で置換する必要がある値が含まれています。

`replace('An#example@to%replace!characters', $parameters.sp1_chars, '_')`関数は`An_example_to_replace_characters`を返します。

出力文字列には、`$parameters.sp1_chars` リストで指定された文字の代わりにアンダースコア (`_`) が表示されます。

## trim()

`trim()`関数は、入力文字列から先頭と末尾の空白を取り除いた文字列を返します。

例:

`trim('abc ')`関数は`abc`を返します。

### **truncate()**

`truncate()`関数は、次の2つの引数を取ります。

引数 1: 文字列

引数 2: 数字

この関数は、引数 1 の入力文字列を、引数 2 で指定された長さに切り捨てた文字列を返します。

例:

`truncate('Citrix ADM', 6)`は`Citrix`を返します。

### **distinct()**

`distinct()`関数は、リスト入力から一意の項目を抽出します。

例:

`$parameters.input_list`が`['ADM', 'ADC', 'VPX', 'ADC', 'ADM', 'CPX']`の場合、`distinct($parameters.input_list)`関数は`['ADM', 'ADC', 'VPX', 'CPX']`を返します。

### **url.encode()**

`url.encode()`関数は、RFC 3986 に従って ASCII 文字セットを使用して文字が変換される文字列を返します。

例:

`url.encode("a/b/c")`関数は`a%2Fb%2Fc`を返します。

### **url.decode()**

`url.decode()`関数は、URL エンコードされた引数が RFC 3986 に従って通常の文字列にデコードされる文字列を返します。

例:

`url.decode("a%2Fb%2Fc")`関数は`a/b/c`を返します。

## is-ipv4 ()

`is-ipv4()`関数は、引数として IP アドレスを受け取り、IP アドレスが IPv4 形式の場合はブール値 `True` を返します。

`is-ipv4(10.10.10.10)`関数は `True` を返します

## is-ipv6 ()

`is-ipv6()`関数は、引数として IP アドレスを受け取り、IP アドレスが IPv6 形式の場合はブール値 `True` を返します。

`is-ipv6(2001:DB8::)`関数は `True` を返します

## startswith ()

`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決定します。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 ときに `True` を返します。

例:

- `startswith('Citrix', 'Ci')`関数は `True` を返します。
- `startswith('Citrix', 'iC')`関数は `False` を返します
- `startswith('Citrix', 'Ab')`関数は `False` を返します

## endswith ()

`endswith()`関数は、文字列が指定された接尾辞で終わるかどうかを決定します。この関数には、2 つの必須文字列引数が必要です。

`endswith(str, sub_str)`

この関数は、文字列 (`str`) が部分文字列 (`sub_str`) で終わる ときに `True` を返します。

例:

- `endswith('Citrix', 'ix')`関数は `True` を返します。
- `endswith('Citrix', 'Ix')`関数は `False` を返します。
- `endswith('Citrix', 'ab')`関数は `False` を返します。

## `()` を含む

`contains()` 関数は、文字列に指定された部分文字列が含まれているかどうかを判定します。この関数には、2 つの必須文字列引数が必要です。

`contains(str, sub_str)`

この関数は、`substring(sub_str)` が文字列 (`str`) 内のどこかに含まれている場合に、`True` を返します。

例:

- `contains('Citrix', 'tri')` 関数は `True` を返します。
- `contains('Citrix', 'Ci')` 関数は `True` を返します。
- `contains('Citrix', 'ti')` 関数は `False` を返します

## 部分文字列 (`()`)

`substring()` 関数を使用して、文字列から部分文字列を抽出します。

`substring(str, start_index, end_index)`

この関数には、2 つの必須引数と 1 つのオプションの整数引数が必要です。

- `str` (必須)
- `start_index` (必須)
- `end_index` (オプション)

この関数は、指定されたインデックス位置の間にある文字列 (`str`) から部分文字列を返します。終了インデックス位置を指定しない場合、関数は開始インデックスから文字列の末尾までの部分文字列を抽出します。

注:

`end_index` を指定すると、`end_index` 位置の文字は部分文字列から除外されます。

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、関数は空白の文字列を返します。
- `substring('Citrix', 2, 4)` 関数は `tr` を返します  
この例では、関数は 2 ~ 4 つのインデックス位置の間の文字を抽出します。
- `substring('Citrix', -3)` 関数は `rix` を返します  
文字列の末尾にある文字を抽出する場合は、`start_index` 引数に負の値を指定します。  
この例では、関数は、文字列の最後の 3 文字を含む部分文字列を抽出します。



## 依存関係の検出

February 6, 2024

StyleBook のコンポーネントでは、同じ StyleBook に含まれる別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が完成されたブロックであるため、実行する必要がある順序どおりに記載されていない場合があります。StyleBook コンパイラはコンポーネントの記載順をチェックして、論理順で実行します。

例:

```
1 components:
2   -
3     name: lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: mylb
7       ipv46: 10.102.190.15
8       port: 80
9       servicetype: HTTP
10  -
11    name: lb-sg-binding-comp
12    type: ns::lbvserver_servicegroup_binding
13    condition: $parameters.create-binding
14    properties:
15      name: $components.lbvserver-comp.properties.name
16      servicegroupname: $components.sg-comp.properties.servicegroupname
17  -
18    name: sg-comp
19    type: ns::servicegroup
20    properties:
21      servicegroupname: mysg
22      servicetype: HTTP
23 <!--NeedCopy-->
```

上記の例では、定義された 3 つのコンポーネントがあります- **lbvserver-comp**、**lb-sg-binding-comp**、および **sg-comp**。この StyleBook の実行時には、まず **lbvserver-comp** が作成されます。**lb-sg-binding-comp** は **lbvserver-comp** プロパティを参照しており、StyleBook で 2 番目に定義されているコンポーネントですが、この次に作成することはできません。これは、**lb-sg-binding-comp** にはまだ作成されていない **sg-comp** との依存関係もあるからです。このため、コンパイラはコンポーネントの作成時点でコンポーネントの依存関係が解決されるようにコンポーネントを並べ替え、並べ替えた順序でコンポーネントを実行します。上記の StyleBook の実行順は、**lbvserver-comp**、**sg-comp**、**lb-sg-binding-comp** のようになります。

したがって、StyleBook の作成者がコンポーネントの正確な順序を気にする必要はありません。コンポーネントはどのような順序で記載しても構いません。コンパイラにより、コンポーネント間の参照関係に基づいて適切なコンポーネントの実行順序が計算されます。この依存関係の検出と並べ替えは、**substitution** セクションおよび **outputs** 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

コンポーネントは別のコンポーネントを参照することがあるため、StyleBook の定義では依存関係の循環が生じ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 で定義されているプロパティを参照しており、さらにコンポーネント B がコンポーネント A で定義されているプロパティを参照している場合などです。こうした依存関係は、循環依存関係と呼ばれます。循環依存関係を自動で解決することはできません。StyleBook の作成者が手動で StyleBook の定義を修正し、こうした循環依存関係を解消する必要があります。コンパイラは循環依存関係を特定することができ、循環依存関係が存在する場合にはレポートします。

以下の例に、コンポーネントの循環依存関係を示します。

```
1 components:
2   -
3     name: lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: $components.lb-sg-binding-comp.properties.name
7       ipv46: 10.102.190.15
8       port: 80
9       servicetype: HTTP
10  -
11  name: lb-sg-binding-comp
12  type: ns::lbvserver_servicegroup_binding
13  condition: $parameters.create-binding
14  properties:
15    name: mylb
16    servicegroupname: $components.sg-comp.properties.servicegroupname
17  -
18  name: sg-comp
19  type: ns::servicegroup
20  properties:
21    servicegroupname: mysg
22    servicetype: $components.lbvserver-comp.properties.servicetype
23 <!--NeedCopy-->
```

上の例では、lbvserver-comp、lb-sg-binding-comp、sg-comp の 3 つのコンポーネントがあります。**lbvserver-comp** は **lb-sg-binding-comp** に依存し、**lb-sg-binding comp** は **sg-comp** に依存し、**sg-comp** は **lbvserver-comp** に依存します。このように、これらのコンポーネント間で依存関係の循環が生じており、この循環は自動で解決できません。このため、この StyleBook は実行できません。StyleBook コンパイラはこれを検出し、StyleBook が NetScaler ADM にインポートされないようにします。

## インスタンス管理

February 6, 2024

インスタンスは、NetScaler Application Delivery Management (ADM) を使用して管理、監視、トラブルシュー

ーティングを行うことができる Citrix Application Delivery Controller (ADC) アプライアンスです。インスタンスを監視するには、NetScaler ADM にインスタンスを追加する必要があります。インスタンスは、Citrix ADM のセットアップ時に追加することも、後で追加することもできます。NetScaler ADM にインスタンスを追加すると、継続的にポーリングされ、後で問題の解決やレポートデータとして使用できる情報を収集します。

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、設定ジョブなどの特定のタスクを実行する場合に便利です。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 ADM サーバーの初回セットアップ時に追加することも、後で追加することもできます。インスタンスを追加するには、各 NetScaler ADC インスタンスのホスト名または IP アドレス、または IP アドレスの範囲を指定する必要があります。

NetScaler ADM にインスタンスを追加する方法については、「[NetScaler ADM へのインスタンスの追加](#)」を参照してください。

NetScaler ADM サーバーにインスタンスを追加すると、サーバーは暗黙的にインスタンスのトラップ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。詳細については、「[NetScaler ADM がインスタンスを検出する方法](#)」を参照してください。

インスタンスを追加したら、[ネットワーク]>[ダッシュボード]に移動し、[すべてのインスタンス]をクリックすることでインスタンスを削除できます。[Instances] ページで、削除するインスタンスを選択し、[Remove] をクリックします。

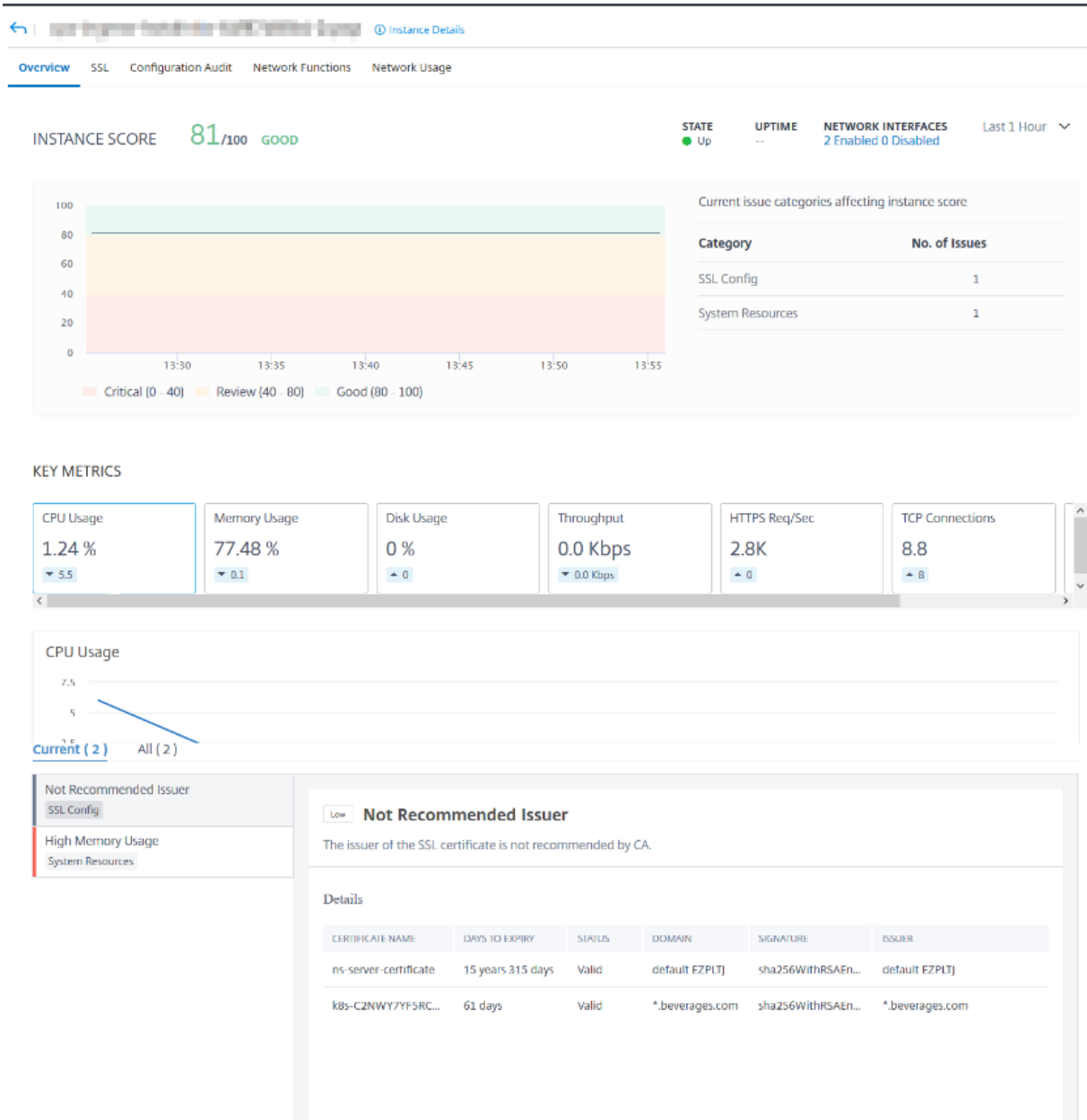
### インスタンスダッシュボードの使用方法

NetScaler ADM のインスタンスごとのダッシュボードには、選択したインスタンスのデータが表形式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は、ダッシュボードに表示されます。

デフォルトでは、1 分ごとに、マネージインスタンスが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、収集したデータをすべて 1 つのページに表示し、インスタンス内の問題を特定し、すぐに修正するための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、[ネットワーク]>[インスタンス]に移動します。概要からインスタンスタイプを選択し、表示するインスタンスを選択し、[Dashboard] をクリックします。

次の図は、インスタンス単位のダッシュボードに表示されるさまざまなデータの概要を示しています：



- 概要。概要タブには、選択したインスタンスの CPU とメモリの使用量が表示されます。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を表示することもできます。IP アドレス、ハードウェアと LOM のバージョン、プロファイルの詳細、シリアル番号、連絡先などのインスタンス固有の情報もここに表示されます。さらに下にスクロールすると、選択したインスタンスで使用できるライセンスされた機能と、そのインスタンスで設定された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、SSL プロトコルの詳細を表示または監視できます。グラフの「数字」をクリックすると、詳細が表示されます。

- 構成監査。[configuration audit] 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設定変更を表示できます。\*\* ダッシュボードの **NetScaler** 構成の保存状況と **NetScaler** 構成のドリフトチャートには \*\*、保存された構成と保存されていない構成の変更に関する詳細な情報が表示されます。
- ネットワーク機能。ネットワーク機能ダッシュボードを使用して、選択した NetScaler ADC 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。
- ネットワークの使用状況。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は、ネットワーク使用量タブで確認できます。1 時間、1 日、1 週間、または 1 か月のレポートを表示できます。タイムラインスライダ機能を使用して、生成されるネットワークレポートの持続時間をカスタマイズできます。デフォルトでは、8 つのレポートしか表示されませんが、画面の右下隅にある「プラス」アイコンをクリックすると、パフォーマンスレポートを追加できます。

### グローバルに分散したサイトの監視

February 6, 2024

ネットワーク管理者は、さまざまな地域に展開されたネットワークインスタンスを必要に応じて監視および管理する必要があります。ただし、地理的に分散し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評価することは容易ではありません。

NetScaler Application Delivery Management (ADM) のジオマップは、サイトをグラフィカルに表現し、ネットワーク監視エクスペリエンスを地理的に分類します。また、ネットワークインスタンスの分布を場所ごとに表示し、ネットワークの問題を監視することもできます。

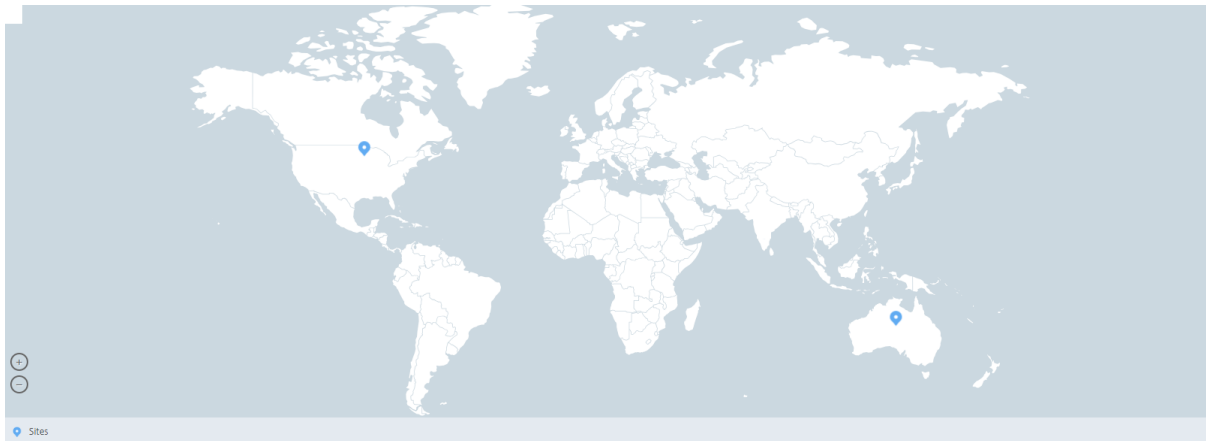
次のセクションでは、NetScaler ADM でデータセンターを監視する方法について説明します。

NetScaler ADM サイトは、特定の地理的な場所にある Citrix Application Delivery Controller (ADC) インスタンスを論理的にグループ化したものです。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。さらに別のサイトがテナントの敷地内にホストされています。NetScaler ADM は、すべてのサイトに接続されているすべての NetScaler ADC インスタンスを管理および監視します。NetScaler ADM を使用して、管理対象インスタンスから送信される syslog、AppFlow、SNMP、およびそのようなデータを監視および収集できます。

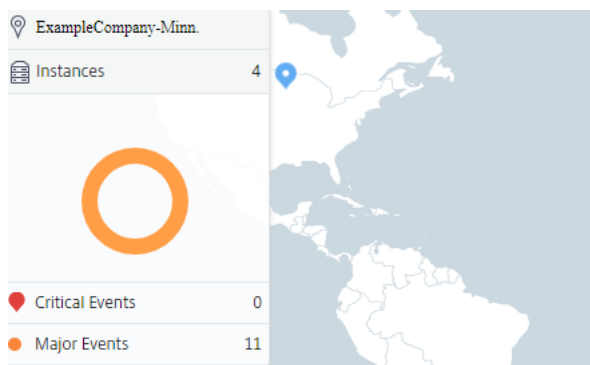
NetScaler ADM のジオマップでは、サイトをグラフィカルに表示できます。ジオマップでは、ネットワークモニタリング体験を地域ごとに分類することもできます。ジオマップを使用すると、場所ごとにネットワークインスタンスの分布を視覚化し、すべてのネットワーク問題を監視できます。ネットワーク > ダッシュボードページに移動すると、世界地図上に作成されたサイトを視覚的に表示できます。

## 使用例

ある大手携帯電話会社 ExampleCompany は、リソースとアプリケーションのホスティングを民間のサービスプロバイダーに頼っていました。同社はすでに 2 つの拠点を構えていました。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 2 つの既存のサイトを表していることがわかります。



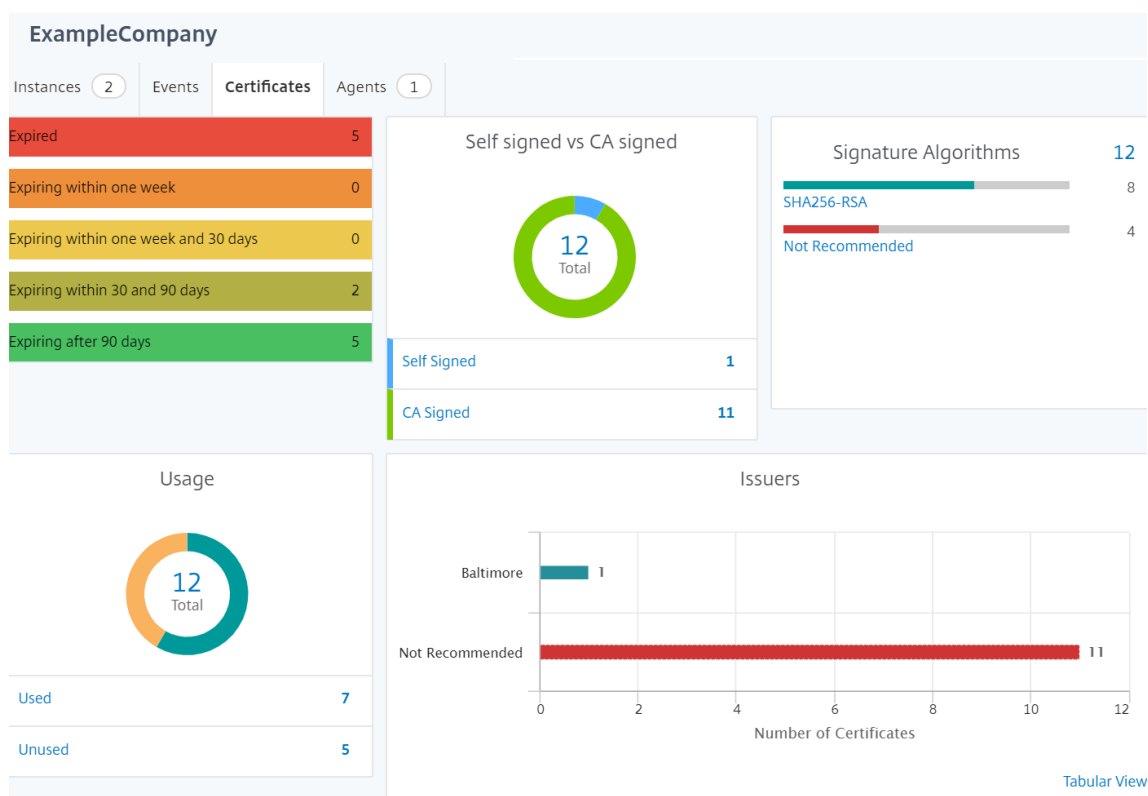
マーカーには、各サイトのアプリケーション数を示す数値も表示されます。これらのマーカーをクリックすると、各サイトの詳細情報が表示されます。



タブをクリックして、詳細情報を表示します。

- 「インスタンス」タブ: このタブには以下が表示されます。
  - 各ネットワークインスタンスの IP アドレス
  - インスタンスのタイプ
  - それらに関する重大なイベントの数
  - NetScaler ADC 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イベントのリストを表示します。
- 「証明書」タブ: このタブには以下が表示されます。

- 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、使用中の多くの証明書の上位 10 インスタンス。
- **[Agents]** 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。



## ジオマップの設定

ExampleCompany は、インドのバンガロールに 3 つ目のサイトを作成することにしました。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して、クラウドをテストしたいと考えていました。同社は AWS クラウドコンピューティングサービスを使用することにしました。

管理者は、最初にサイトを作成し、次に NetScaler ADM に NetScaler ADC インスタンスを追加する必要があります。また、インスタンスをサイトに追加し、エージェントを追加し、エージェントをサイトにバインドする必要があります。NetScaler ADM は、NetScaler ADC 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 ADC インスタンスの追加について詳しくは、「[インスタンスの追加](#)」を参照してください。

サイトを作成するには、次の手順に従います。

NetScaler ADM にインスタンスを追加する前にサイトを作成します。位置情報を提供することで、サイトを正確に見つけることができます。

[ネットワーク] > [サイト] に移動し、[追加] をクリックします。

1. [サイトの作成] ページで、次の情報を指定します。

- a) サイトタイプ: データセンターを選択します。

注

サイトは、プライマリデータセンターまたはブランチとして機能できます。適宜選択してください。

- b) タイプ: リストから AWS をクラウドプロバイダーとして選択します。

注:

[既存の VPC をサイトとして使用する] チェックボックスをオンにします。

- c) サイト名: サイトの名前を入力します。

- d) 市区町村: 市区町村を入力します。

- e) 郵便番号: 郵便番号を入力します。

- f) 地域: 地域を入力します。

- g) 国: 国を入力してください

- h) 緯度: 位置の緯度を入力します。

- i) 経度: 位置の経度を入力します。

2. [Create] をクリックします。

← Create Site

Site type  
 Data Center  Branch

Type\*  
AWS

Use existing VPC as a site

Site Name\*  
ExampleCompany

City\*  
Bangalore

ZIP Code\*  
560001

Region\*  
Karnataka

Country\*  
India

Latitude\*  
77.5946

Longitude\*  
12.9716

Create Close

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 ADM 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か、サイトを作成してインスタンスを関連付けることもできます。



サイトを作成したら、NetScaler ADM 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か、サイトを作成してインスタンスを関連付けることもできます。

1. NetScaler ADM で、[ ネットワーク ] > [ インスタンス ] に移動します。
2. 作成するインスタンスのタイプを選択し、[ **Add** ] をクリックします。
3. [ **NetScaler ADC VPX の追加** ] ページで、IP アドレスを入力し、リストからプロファイルを選択します。
4. リストからサイトを選択します。サイトフィールドの横にある + 記号をクリックしてサイトを作成するか、編集アイコンをクリックしてデフォルトサイトの詳細を変更できます。
5. 右矢印をクリックし、表示されるリストからエージェントを選択します。

### ← Add Citrix ADC VPX

Enter Device IP Address     Import from file  
 Enter one or more hostnames, IP addresses , and/or a range of IP addresses (for example, 10.102.40.30-10.102.40.45) using a comma separator.  
 IP Address\*  
 ?  
 Profile Name\*  
    
 Site\*  
    
 Agent  
 >  
 Tags  
 Location  + ?

6. エージェントを選択したら、エージェントをサイトに関連付ける必要があります。このステップにより、エージェントをサイトにバインドできます。エージェントを選択し、[ サイトの接続 ] をクリックします。

| Agents                                           |                                             |                                       |                                           |                                                       |                                                |
|--------------------------------------------------|---------------------------------------------|---------------------------------------|-------------------------------------------|-------------------------------------------------------|------------------------------------------------|
| <input checked="" type="button" value="Select"/> | <input type="button" value="View Details"/> | <input type="button" value="Delete"/> | <input type="button" value="Rediscover"/> | <input checked="" type="button" value="Attach Site"/> | <input type="button" value="Set Up Agent"/>    |
| No action ▾                                      |                                             |                                       |                                           |                                                       |                                                |
|                                                  | IP Address                                  | Host Name                             | Current Version                           | Recommended Version                                   | Upgrade Status                                 |
| <input checked="" type="radio"/>                 | 10.102.31.143                               | haproxyagent                          | 12.0-509.119                              | 12.0-509.119                                          | <input checked="" type="checkbox"/> Up-to-date |
| <input type="radio"/>                            | 192.168.4.63                                | ns                                    | 12.0-509.119                              | 12.0-509.119                                          | <input checked="" type="checkbox"/> Up-to-date |
| <input type="radio"/>                            | 10.102.107.126                              | sathiya-adtest                        | 12.0-509.119                              | 12.0-509.119                                          | <input checked="" type="checkbox"/> Up-to-date |

1. リストからサイトを選択し、[ 保存 ] をクリックします。

1. **[OK]** をクリックします。

[ネットワーク] > [エージェント] に移動して、エージェントをサイトに接続することもできます。

**NetScaler ADM** エージェントをサイトに関連付けるには:

1. Citrix ADM で、[ネットワーク] > [エージェント] に移動します。
2. エージェントを選択し、[サイトの接続] をクリックします。

## Agents

|                                     | View Details   | Delete         | Rediscover      | Attach Site         | Set Up Agent   | No action |
|-------------------------------------|----------------|----------------|-----------------|---------------------|----------------|-----------|
| <input type="checkbox"/>            | IP Address     | Host Name      | Current Version | Recommended Version | Upgrade Status |           |
| <input checked="" type="checkbox"/> | 10.102.31.143  | haproxyagent   | 12.0-509.119    | 12.0-509.119        | Up-to-date     |           |
| <input type="checkbox"/>            | 192.168.4.63   | ns             | 12.0-509.119    | 12.0-509.119        | Up-to-date     |           |
| <input type="checkbox"/>            | 10.102.107.126 | sathiya-adtest | 12.0-509.119    | 12.0-509.119        | Up-to-date     |           |
| <input type="checkbox"/>            | 10.221.42.57   | PROD-Agent2    | 12.0-509.119    | 12.0-509.119        | Up-to-date     |           |

1. サイトを関連付けて、[保存] をクリックします。

NetScaler ADM は、バンガロールサイトに追加された NetScaler ADC インスタンスと、他の 2 つのサイトのインスタンスの監視を開始します。

## タグを作成してインスタンスに割り当てる方法

February 6, 2024

Citrix Application Delivery Management (ADM) では、Citrix アプリケーション Delivery Controller (ADC) インスタンスをタグに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語の用語です。タグは、インスタンスに関するいくつかの追加情報を追加します。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および検索できます。1 つ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インスタンスをより適切に監視するため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:** タグを作成して、イギリスのすべてのインスタンスを識別できます。ここでは、キーを「国」、値を「UK」としてタグを作成することができます。このタグは、英国のすべてのインスタンスを検索および監視するのに役立ちます。
- **ユースケース 2:** ステージング環境にあるインスタンスを検索する場合。ここでは、キーを「目的」、値を「staging\_NS」としてタグを作成できます。このタグは、ステージング環境で使用されているすべてのインスタンスを、クライアント要求が実行されているインスタンスから分離するのに役立ちます。

- ユースケース 3: 英国の「Swindon」エリアにあり、David T (David T) が所有している NetScaler ADC インスタンスのリストを調べる状況を考えてみましょう。これらすべての要件に対応するタグを作成し、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 ADC VPX** インスタンスにタグを割り当てるには:

1. NetScaler ADM で、[ネットワーク] > [インスタンス] > [NetScaler ADC] に移動します。
2. [NetScaler ADC VPX] タブを選択します。
3. 必要な Citrix VPX を選択します。
4. [タグ] をクリックします。
5. タグを作成して「OK」をクリックします。

表示される [タグ] ウィンドウでは、作成したすべてのキーワードに値を割り当てることによって、独自の「キーと値」のペアを作成できます。

たとえば、次の画像は、作成されたいくつかのキーワードとその値を示しています。独自のキーワードを追加し、各キーワードに値を入力できます。

← Tags

IP Address

Apply tags to classify, identify, and search for the Citrix ADC instances.

Tag is a keyword or a term assigned to an instance. A tag consists of a key-value pair. For example, define a tag as follows:  
Key = country; Value = US

NOTE: You can type one or more values for each key using a comma separator.

Key and Value

Country UK + ?

OK Close

## ← Tags

IP Address

Apply tags to classify, identify, and search for the Citrix ADC instances.

Tag is a keyword or a term assigned to an instance. A tag consists of a key-value pair. For example, define a tag as follows:  
Key = country; Value = US

NOTE: You can type one or more values for each key using a comma separator.

Key and Value

|         |            |   |   |
|---------|------------|---|---|
| Purpose | Staging_NS | + | ? |
|---------|------------|---|---|

OK Close

「+」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と、インスタンスを効率的に検索できます。

← Tags

IP Address

Apply tags to classify, identify, and search for the Citrix ADC instances.

Tag is a keyword or a term assigned to an instance. A tag consists of a key-value pair. For example, define a tag as follows:  
Key = country; Value = US

NOTE: You can type one or more values for each key using a comma separator.

Key and Value

|         |         |   |   |
|---------|---------|---|---|
| Country | UK      | × |   |
| Area    | Swindon | × | ? |
| Owner   | David T | × | + |

OK Close

キーワードに複数の値を追加するには、カンマで区切ります。

たとえば、別の同僚の Greg T に管理者の役割を割り当てているとします。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を検索できます。NetScaler ADM は、カンマで区切られた値を 2 つの異なる値に認識します。

←

## Tags

IP Address

Apply tags to classify, identify, and search for the Citrix ADC instances.

Tag is a keyword or a term assigned to an instance. A tag consists of a key-value pair. For example, define a tag as follows:  
Key = country; Value = US

NOTE: You can type one or more values for each key using a comma separator.

Key and Value

|         |                 |   |   |
|---------|-----------------|---|---|
| Country | UK              | × |   |
| Area    | Swindon         | × | ? |
| Owner   | David T, Greg T | × | + |

OK
Close

タグに基づいてインスタンスを検索する方法の詳細については、「[タグとプロパティの値を使用してインスタンスを検索する方法](#)」を参照してください。

注:

後で新しいタグを追加したり、既存のタグを削除したりできます。作成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

February 6, 2024

NetScaler Application Delivery Management (ADM) が多くの NetScaler ADC インスタンスを管理している場合があります。管理者は、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できる柔軟性が必要な場合があります。NetScaler ADM では、検索フィールドで定義したパラメータに基づいて NetScaler ADC インスタンスのサブセットを検索する検索機能が強化されました。タグとプロパティの 2 つの基準に基づいてインスタンスを検索できます。

- タグ。タグは、NetScaler ADC インスタンスに割り当てて、NetScaler ADC インスタンスに関する追加の説明を追加できる用語またはキーワードです。これで、NetScaler ADC インスタンスをタグに関連付けることができます。これらのタグを使用すると、NetScaler ADC インスタンスをより適切に識別および検索できます。

- **[プロパティ]**。NetScaler ADM で追加された各 NetScaler ADC インスタンスには、そのインスタンスに関連付けられたデフォルトのパラメータまたはプロパティがいくつかあります。たとえば、各インスタンスには独自のホスト名、IP アドレス、バージョン、ホスト ID、ハードウェアモデル ID などがあります。これらのプロパティの値を指定して、インスタンスを検索できます。

たとえば、バージョン 12.0 にあり、稼働状態にある NetScaler ADC インスタンスのリストを調べたい場合を考えてみましょう。ここでは、インスタンスのバージョンと状態はデフォルトプロパティによって定義されます。

12.0 バージョンとインスタンスの稼働状態の他に、所有しているインスタンスを検索することもできます。「所有者」タグを作成し、そのタグに値「David T」を割り当てることができます。タグの作成方法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。

タグとプロパティの組み合わせを使用して、独自の検索条件を作成できます。

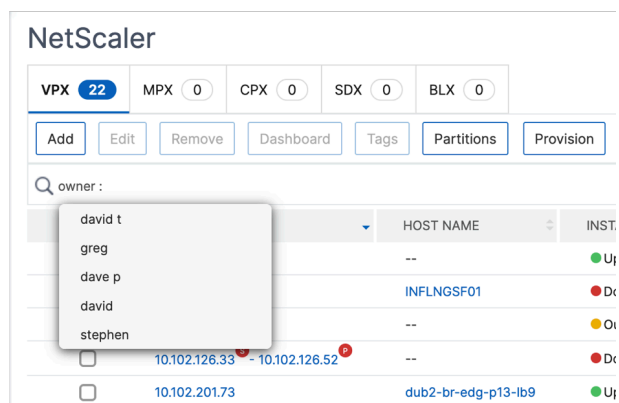
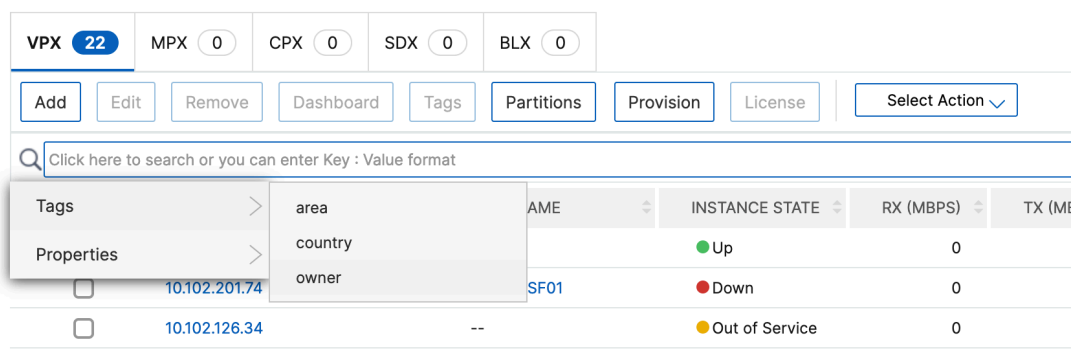
### NetScaler ADC VPX インスタンスを検索するには

1. Citrix ADM で、[ネットワーク]>[インスタンス]>[\*\*Citrix ADC\*\*]>[VPX] タブに移動します。
2. 検索フィールドをクリックします。検索式は、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。「デビッド T。」を選択します。

#### NetScaler



NetScaler ADM では、検索式で正規表現とワイルドカード文字がサポートされています。

- b) 正規表現を使用して検索条件をさらに広げることができます。たとえば、David または Stephen のどちらかが所有するインスタンスを検索したいとします。このような場合は、値を「|」式で区切って値を入力できます。

### NetScaler

The screenshot shows the NetScaler ADM interface with the search bar containing 'owner: david | greg'. Below the search bar, there is a table with columns: IP ADDRESS, HOST NAME, INSTANCE STATE, RX (MBPS), TX (MBPS), and HTTP REQ/S. One instance is listed with a state of 'Up'.

|                          | IP ADDRESS | HOST NAME | INSTANCE STATE | RX (MBPS) | TX (MBPS) | HTTP REQ/S |
|--------------------------|------------|-----------|----------------|-----------|-----------|------------|
| <input type="checkbox"/> |            | --        | ● Up           | 0         | 0         | 0          |

Total 1

- c) ワイルドカード文字を使用して、1つ以上の文字を置換または表すこともできます。たとえば、Dav\* と入力すると、David T と Dave P が所有するすべてのインスタンスを検索できます。

### NetScaler

The screenshot shows the NetScaler ADM interface with the search bar containing 'owner: dav\*'. Below the search bar, there is a table with columns: IP ADDRESS, HOST NAME, INSTANCE STATE, RX (MBPS), TX (MBPS), HTTP REQ/S, AGENT, and SITE. Two instances are listed, one with a state of 'Down' and one with a state of 'Up'.

|                          | IP ADDRESS    | HOST NAME  | INSTANCE STATE | RX (MBPS) | TX (MBPS) | HTTP REQ/S | AGENT | SITE    |
|--------------------------|---------------|------------|----------------|-----------|-----------|------------|-------|---------|
| <input type="checkbox"/> | 10.102.201.74 | INFLNGSF01 | ● Down         | 0         | 0         | 0          | --    | Default |
| <input type="checkbox"/> | 10.102.126.35 | --         | ● Up           | 0         | 0         | 3          | --    | Default |

#### 注:

正規表現とワイルドカード文字とその使用方法については、検索バーの「情報」アイコンをクリックします。

## NetScaler ADC インスタンスの管理パーティションの管理

February 6, 2024

Citrix アプリケーション Delivery Controller (ADC) インスタンスの管理パーティションを構成して、組織内のさまざまなグループに同じ Citrix ADC 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を割り当てて、複数の Citrix ADC インスタンス上の複数のパーティションを管理できます。

Citrix Application Delivery Management (ADM) を使用すると、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できます。これらのパーティションは、他のパーティション構成を中断することなく管理できます。

複数のユーザーが異なる管理パーティションを管理できるようにするには、グループを作成し、それらのグループにユーザーとパーティションを割り当てる必要があります。各ユーザーは、そのユーザーが属するグループ内のパーティションのみを表示および管理できます。各管理パーティションは、NetScaler ADM ではインスタンスと見なされます。NetScaler ADC インスタンスを検出すると、その NetScaler ADC インスタンスに構成されている管理パーティションが自動的にシステムに追加されます。

2 つの Citrix VPX インスタンスがあり、各インスタンスに 2 つのパーティションが設定されているとします。たとえば、NetScaler ADC インスタンス 10.102.216.49 にはパーティション \_1、パーティション \_2、パーティション \_3 があり、NetScaler ADC インスタンス 10.102.29.120 には p1 と p2 があります。

パーティションを表示するには、[ネットワーク] > [インスタンス] > [NetScaler ADC] > [VPX] の順に選択し、[パーティション] をクリックします。

ユーザ p1 には、10.102.29.120-p1 および 10.102.216.49-パーティション \_1 というパーティションを割り当てることができます。また、ユーザー p2 をパーティション 10.102.29.80-p2、10.102.216.49-Partition\_2、10.102.216.49-Partition\_3 の管理に割り当てることができます。

次に、user-p1 と user-p2 という 2 つのユーザーを作成し、それらのユーザーを、それぞれのために作成されているグループに割り当てる必要があります。

まず、適切な権限 (管理者権限など) を持つ 2 つのグループを作成し、各グループに必要な管理パーティションインスタンスを含める必要があります。たとえば、システムグループ partition1-admin を作成し、Citrix ADC 管理パーティション 10.102.29.120-p1 と 10.102.216.49-Partition\_1 をこのグループに追加します。また、システムグループ partition2-admin を作成し、Citrix ADC 管理パーティション 10.102.29.120-p2、10.102.216.49-Partition\_2、10.102.216.49-Partition\_3 をこのグループに追加します。

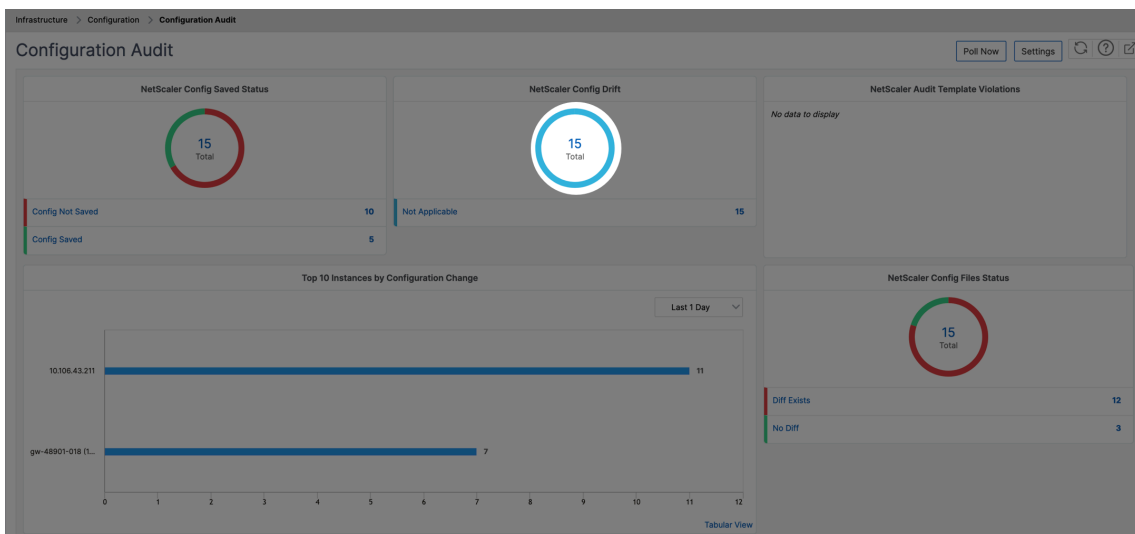
管理パーティションを作成したら、改訂履歴差分機能と管理パーティションの監査テンプレート機能を監査目的で使用することもできます。

管理パーティションのリビジョン履歴の違いにより、パーティション化された Citrix ADC インスタンスの最新の 5 つの構成ファイルの違いを表示できます。構成ファイルを相互に比較したり (たとえば、構成リビジョン-1 と構成リビジョン-2)、構成リビジョンを使用して現在実行/保存されている構成と比較したりできます。構成の違いとともに、修正構成も示されています。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、設定を修正できます。

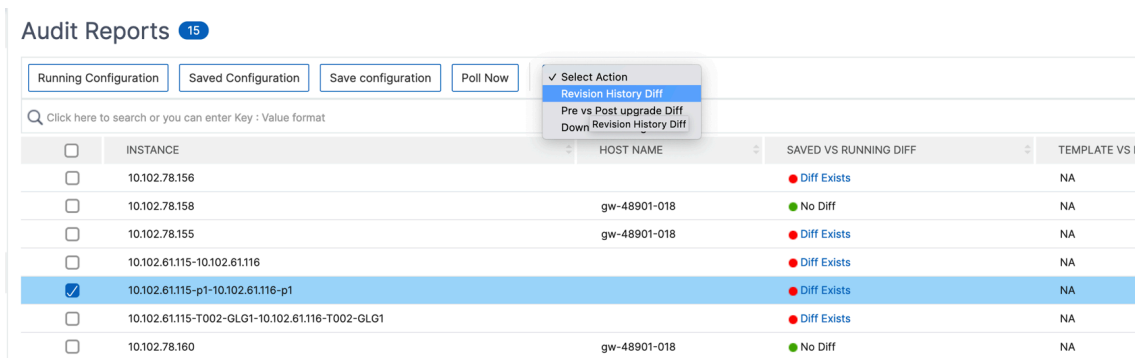
改訂履歴の差異を表示する手順は、次のとおりです。

1. [ネットワーク] > [構成監査] に移動します。インスタンスの構成ステータスを表すドーナツグラフ内をクリックします。表示される [監査レポート] ページで、パーティション分割された NetScaler ADC インスタンスをクリックします。

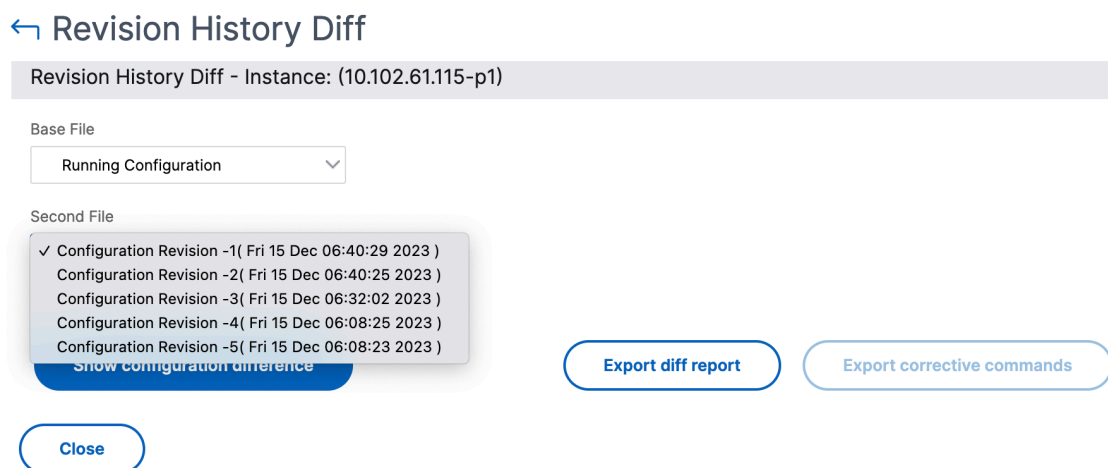




2. [操作]メニューから、[リビジョン履歴の差分]をクリックします。



3. [リビジョン履歴の差分] ページで、比較するファイルを選択します。たとえば、[保存された構成]と[構成リビジョン-1]を比較し、[構成の違いを表示]をクリックします。



4. 次に示すように、選択したパーティション分割された NetScaler ADC インスタンスの最新の 5 つの構成ファ

イルの違いを確認できます。修正構成コマンドを表示し、これらの修正コマンドをローカルフォルダにエクスポートすることもできます。これらの修正コマンドは、構成を目的の状態（比較に使用される構成ファイル）にするために、ベースファイルで実行する必要があるコマンドです。

← Revision History Diff

Revision History Diff - Instance: (10.102.61.115-p1)

Base File  
Running Configuration

Second File  
Configuration Revision -1( Fri 15 Dec

Ignore system user password diff in report

Show configuration difference Export diff report Export corrective commands

| Configuration Revision -1( Fri 15 Dec 06:40:29 2023 ) | Running Configuration                                 | Correction Configuration          |
|-------------------------------------------------------|-------------------------------------------------------|-----------------------------------|
| set cmp parameter -externalCache YES                  | set cmp parameter -cmpBypassPct 98 -externalCache YES | unset cmp parameter -cmpBypassPct |

Close

パーティションの監査テンプレートを使用すると、カスタム設定テンプレートを作成して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。監査テンプレートを使用したインスタンスの実行構成にばらつきがある場合は、監査レポートページの「テンプレートと実行中の違い」列に表示されます。構成の違いとともに、修正構成も示されています。また、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、設定を修正することもできます。

テンプレートと実行差分を表示するには：

1. [監査レポート] ページで、パーティション化された NetScaler ADC インスタンスをクリックします。

Audit Reports 15

Running Configuration Saved Configuration Save configuration Poll Now Select Action

Click here to search or you can enter Key : Value format

| INSTANCE | HOST NAME    | SAVED VS RUNNING DIFF | TEMPLATE VS RUNNING DIFF | CONFIG SAVED |
|----------|--------------|-----------------------|--------------------------|--------------|
|          | gw-48901-018 | No Diff               | NA                       | Yes          |
|          | gw-48901-018 | No Diff               | Diff Exists              | Yes          |
|          | gw-48901-018 | No Diff               | NA                       | Yes          |
|          |              | No Diff               | NA                       | Yes          |
|          |              | No Diff               | NA                       | Yes          |

Total 15 250 Per Page Page 1 of 1

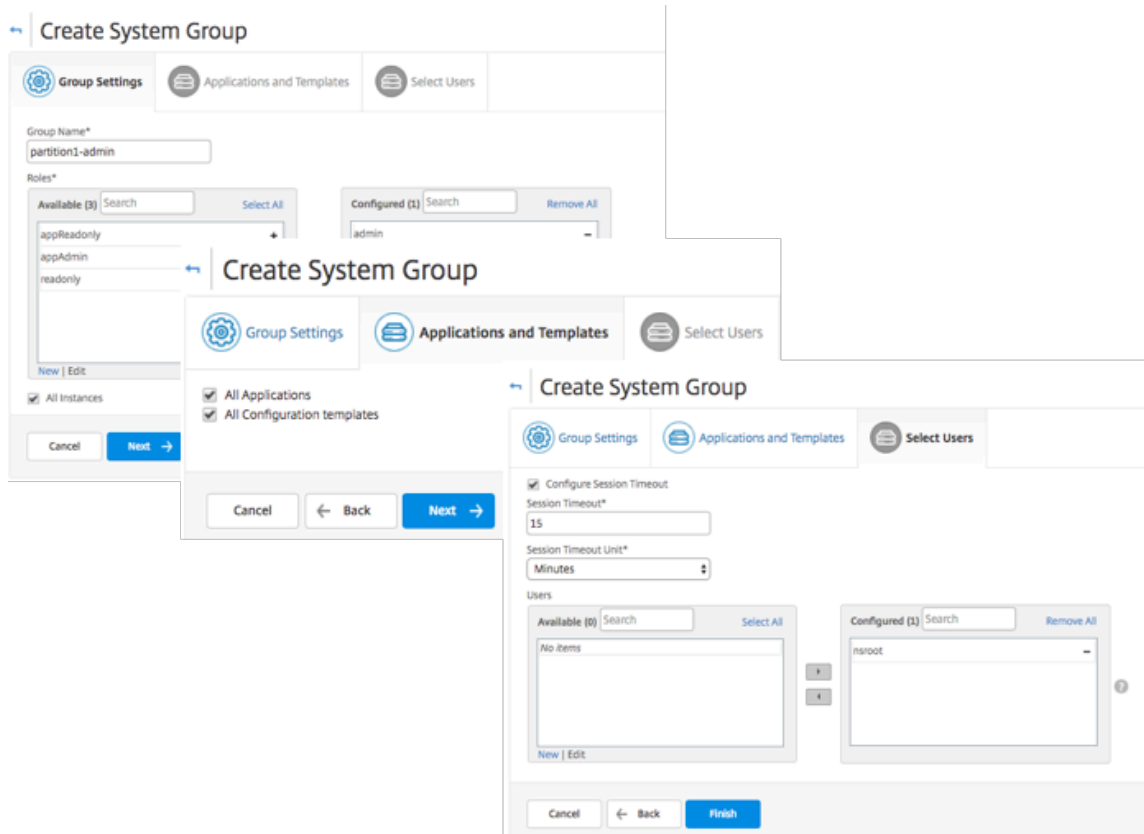
2. 監査テンプレートと実行中の違いに違いがある場合、その差はハイパーリンクとして表示されます。ハイパーリンクをクリックすると、相違点が表示されます（存在する場合）。構成の違いとともに、修正構成も示されています。また、すべての修正コマンドをローカルフォルダにエクスポートして、設定を修正することもできます。

グループを作成するには、次の手順に従います。

1. [システム] > [ユーザー管理] > [グループ] に移動し、[追加] をクリックします。
2. [システムユーザーの作成] ページで、次の項目を指定します。
  - グループ設定タブ: グループ名とロール権限を入力します。特定のインスタンスへのアクセスを許可するには、「All Instances」チェックボックスをオフにし、「Select Instances」ページでインスタンスを選択します。

- 「アプリケーションとテンプレート」 タブ: このグループをすべてのアプリケーションと構成テンプレートで使用できます。
- [ユーザーの選択] タブ: このグループに追加するユーザーを選択します。「使用可能」 (Available) テーブルの「新規」 (New) リンクをクリックすると、新しいユーザーを作成できます。必要に応じて、セッションタイムアウトを構成します。ここでは、ユーザーがアクティブな状態でいられる期間を構成できます。

3. [完了] をクリックします。



ユーザーを作成するには、次の手順に従います。

1. [システム] > [ユーザー管理] > [ユーザー] に移動し、[追加] をクリックします。
2. [システムユーザーの作成] ページで、ユーザー名とパスワードを指定します。必要に応じて、外部認証を有効にすることや、セッションタイムアウトを構成することができます。
3. 「使用可能」 リストのグループ名を「構成済み」 リストに追加して、ユーザーをグループに割り当てます。
4. [Create] をクリックします。

ログアウトして、user-p1 の資格情報でログオンします。管理および監視が割り当てられた管理パーティションのみを表示、管理することができます。

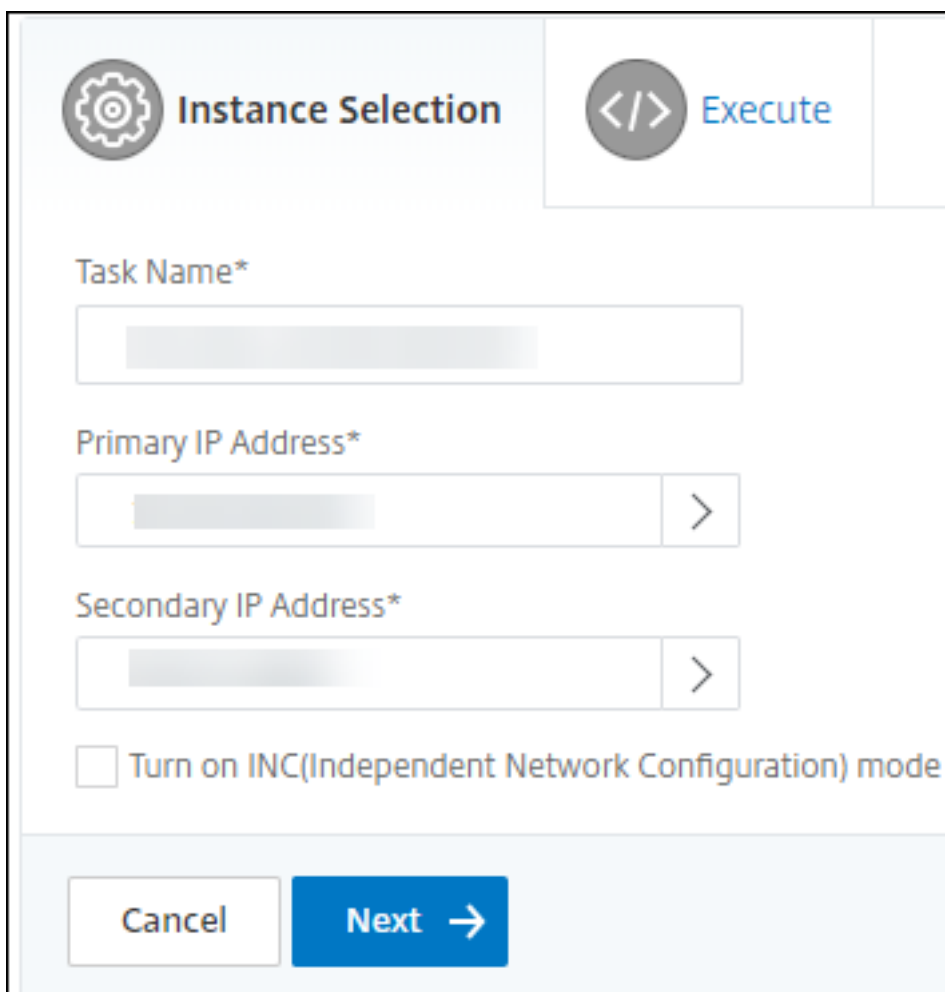
## NetScaler ADC の高可用性ペアの作成

January 29, 2024

Citrix ADC 高可用性 (HA) ペアを使用すると、ダウンタイムやネットワーク障害が発生しても中断することなく操作できます。NetScaler ADM を使用して、ADC インスタンスの高可用性ペアを作成できます。詳しくは、「[NetScaler ADC の高可用性](#)」を参照してください。

NetScaler ADM で ADC インスタンスの高可用性ペアを作成するには、次の手順に従います。

1. [ネットワーク] > [インスタンス] > [Citrix ADC] に移動します。
2. HA ペアの作成に使用するリストから ADC インスタンスを選択します。  
選択したインスタンスが HA ペアのプライマリインスタンスになります。
3. アクションの選択 > **HA** ペアの作成をクリックします。
4. 「インスタンスの選択」で、次の手順を実行します。
  - a) 「セカンダリ **IP** アドレス」で、セカンダリインスタンスをクリックして選択します。
  - b) HA ペアのセカンダリとして設定する ADC インスタンスを選択します。
  - c) オプションとして、2 つのサブネットに **HA** ペアインスタンスがある場合は、「**INC** (独立ネットワーク構成) モードを有効にする」を選択します。
  - d) [次へ] をクリックします。



The screenshot shows a dialog box titled "Instance Selection" with a gear icon. In the top right corner, there is an "Execute" button with a code icon. The main area contains three input fields: "Task Name\*", "Primary IP Address\*", and "Secondary IP Address\*", each with a right-pointing arrow. Below these is a checkbox labeled "Turn on INC(Independent Network Configuration) mode". At the bottom, there are "Cancel" and "Next >" buttons.

5. **Execute** では、HA ペアを今すぐ作成するか、後で作成するかを決定できます。


a) 「実行モード」で、次の実行モードのいずれかを選択します。


- 今すぐ - このオプションを選択して HA ペアを今すぐ作成してください。
- **[Later ]**: 特定の日に HA ペアを作成するには、このオプションを選択します。

b) 「実行モード」リストで「後で」を選択した場合は、このタスクを実行するときに「実行日」と「開始時刻」を選択します。

注:

実行時間は、NetScaler ADM で設定されたタイムゾーンで表示されます。


Instance Selection


Execute

You can either execute the task now or schedule to execute the task at a later time.

Execution Mode\*

Later
▼

NOTE: Select the execution time in your selected timezone

Execution Date

📅 6 Feb 2020
▼

Start Time\*

01 ▼

00 ▼

AM

PM

Receive Execution Report through email

Email\*

test
▼

Add

Edit

Test

Receive Execution Report through slack

Cancel

← Back

Finish

このタスクの実行レポートは、次の方法で受け取ることができます。

- 電子メール - リストから電子メールの配布を選択します。

配布リストを追加するには、[追加] をクリックします。配布リストを追加するために必要なパラメータを指定し、[作成] をクリックします。

### Create Email Distribution List

Name\*

Email Servers\*

From

To\*

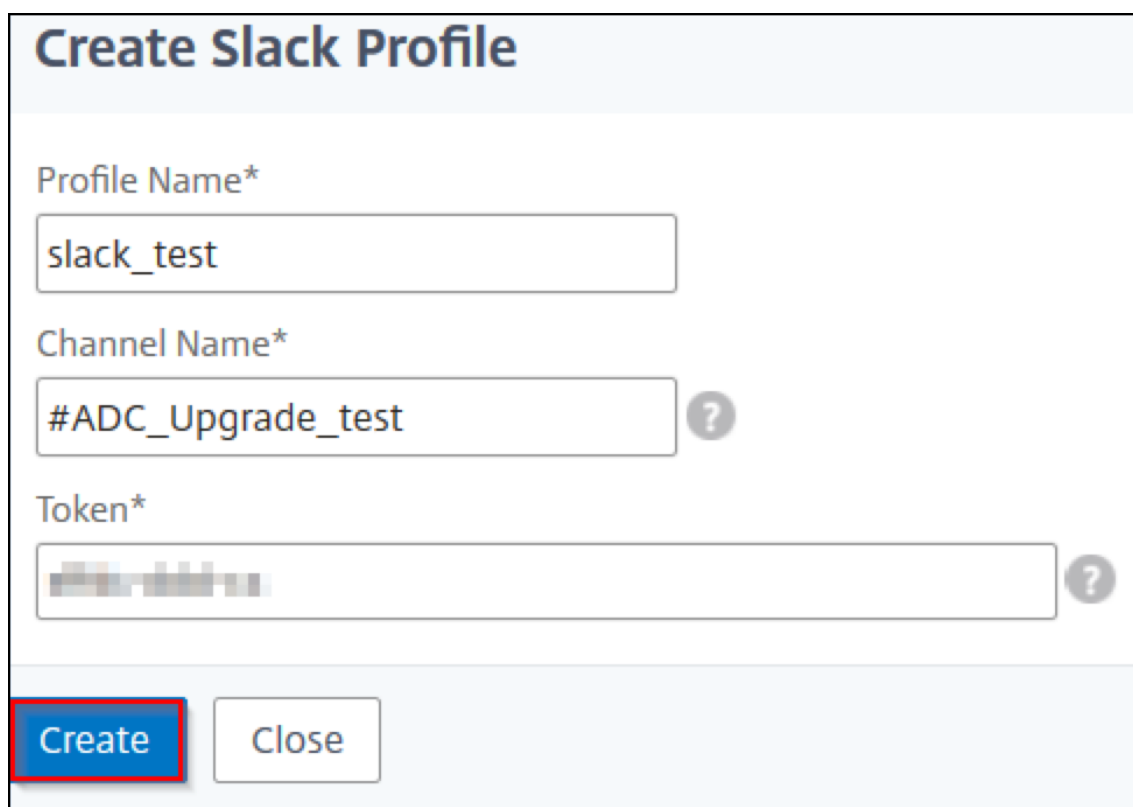
Cc

Bcc

- **Slack** -リストから Slack プロファイルを選択します。

Slack プロフィールを追加するには、「追加」をクリックします。プロフィール名、チャンネル名 **\*\***、**\*\*** トークンを指定し、「作成」をクリックします。



**Create Slack Profile**

Profile Name\*  
slack\_test

Channel Name\*  
#ADC\_Upgrade\_test ?

Token\*  
[blurred] ?

Create Close

## NetScaler ADC インスタンスのバックアップと復元

February 6, 2024

NetScaler ADC インスタンスの現在の状態をバックアップし、後でバックアップしたファイルを使用して同じ状態に復元できます。アップグレードする前または予防上の理由から、必ずインスタンスをバックアップしてください。安定したシステムのバックアップを使用すると、不安定になった場合に、安定した状態に復元できます。

NetScaler ADC インスタンスでバックアップおよびリストアを実行する方法は複数あります。GUI と CLI を使用して、Citrix ADC 構成を手動でバックアップおよび復元できます。Citrix ADM を使用して自動バックアップと手動復元を実行することもできます。

NetScaler ADM は、NITRO コールとセキュアシェル (SSH) プロトコルとセキュアコピー (SCP) プロトコルを使用して、管理対象 NetScaler ADC インスタンスの現在の状態をバックアップします。

NetScaler ADM は完全なバックアップを作成し、次の NetScaler ADC インスタンスタイプを復元します。

- Citrix SDX
- Citrix VPX
- Citrix MPX



- Citrix BLX

詳細については、「[ADC インスタンスのバックアップと復元](#)」を参照してください。

#### 注

- Citrix ADM プロファイルに、ADC インスタンスをバックアップおよび復元するための管理者アクセス権があることを確認します。
- NetScaler ADM では、NetScaler ADC クラスタでバックアップと復元操作を実行できません。
- あるインスタンスから取られたバックアップファイルを、異なるインスタンスを復元するために使用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。

```
1 /var/mps/tenants/root/device_backup/  
2 <!--NeedCopy-->
```

ディスク容量がないことによる問題を回避するため、このディレクトリには ADC インスタンスごとに最大 50 個のバックアップファイルを保存できます。

NetScaler ADC インスタンスをバックアップおよび復元するには、まず NetScaler ADM でバックアップ設定を構成する必要があります。設定を構成したら、1 つの Citrix ADC インスタンスまたは複数のインスタンスを選択して、これらのインスタンス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 Citrix ADC インスタンスを復元することもできます。

#### インスタンスのバックアップ設定の構成

[インスタンスのバックアップ設定] ページでは、選択した NetScaler ADC インスタンスまたは複数のインスタンスをバックアップするための NetScaler ADM の設定を構成できます。

1. Citrix ADM で、[システム] > \*\*[ \*\* 管理] に移動します。
2. 「バックアップ」で、「システムとインスタンスのバックアップを設定」を選択します。
3. [インスタンス] を選択し、以下を指定します。
  - インスタンスバックアップを有効にする: デフォルトでは、NetScaler ADM は NetScaler ADC インスタンスのバックアップを作成するために有効になっています。インスタンスのバックアップファイルを作成しない場合は、このオプションをクリアしてください。
  - パスワード保護ファイル:(オプション) パスワード保護オプションを選択して、バックアップファイルを暗号化します。バックアップファイルを暗号化すると、バックアップファイル内のすべての機密情報が安全に保たれます。

注

暗号化されたバックアップファイルはローカルマシンにダウンロードできますが、NetScaler ADM GUI またはテキストエディタで開くことはできません。暗号化されたバックアップファイルを復元する場合は、パスワードを入力するように要求されます。暗号化されていないバックアップファイルは、システム上で開くことができます。

- 保持するバックアップファイルの数: NetScaler ADM で保持するバックアップファイルの数を指定します。ADC インスタンスごとに最大 50 個のバックアップファイルを保持できます。デフォルトでは、バックアップファイルは 3 つです。

注

各バックアップファイルには、ある程度のストレージ要件があります。要件に応じて、NetScaler ADC バックアップファイルを最適な数の NetScaler ADM に保存することをお勧めします。

- バックアップのスケジュール設定: (オプション) バックアップファイルの作成には 2 つのオプションがありますが、一度に使用できるオプションは 1 つだけです。
  - a) デフォルトのバックアップスケジュールオプションは「間隔ベース」です。指定した間隔が経過すると、Citrix ADM にバックアップファイルが作成されます。デフォルトのバックアップ間隔は 12 時間です。
  - b) スケジュール・バックアップのタイプを「時間ベース」に変更することもできます。このオプションでは、`hours:minutes` 指定した時間にインスタンスをバックアップする形式で時刻を指定します。NetScaler ADM では、インスタンスで毎日バックアップを 4 回まで実行できます。

**▼ Backup Scheduling Settings**

Scheduling Option

Interval Based  Time Based

Specify time for daily Backup (Maximum-limit: 4)

Add Time

|       |   |   |
|-------|---|---|
| 00:00 | × |   |
| 06:00 | × |   |
| 12:00 | × |   |
| 18:00 | × | + |

- **NetScaler ADC 設定:** (オプション) デフォルトでは、NetScaler ADM は「NetScalerConfigSave」トラップを受信したときにバックアップファイルを作成しません。ただし、Citrix ADC インスタンスが Citrix ADM に「NetScalerConfigSave」トラップを送信するたびに、バックアップファイルを作成するオプションを有効にできます。Citrix ADC 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。
- **ジオデータベースファイル:**(オプション) デフォルトでは、Citrix ADM はジオデータベースファイルをバックアップしません。このオプションを有効化して、これらのファイルもバックアップファイルを作成することができます。

**▼ Citrix ADC Settings**

Do instance backup when NetScalerConfigSave trap is received

Include GeoDB Files

- **外部転送:** (オプション) NetScaler ADM では、NetScaler ADC 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) ロケーションの IP アドレスを指定します。
  - b) バックアップファイルの転送先となる外部サーバーのユーザー名とパスワードを指定します。

- c) 転送プロトコルとポート番号を指定します。
- d) ファイルを保存するディレクトリパスを指定できます。
- e) オプションで、バックアップファイルを外部サーバーに転送した後、Citrix ADM から削除することもできます。

**External Transfer**

Enable External Transfer

Server\*

192 . 10 . 10 . 1

User Name\*

davidT

Password\*

\*\*\*\*\*

Port\*

-1

Transfer Protocol

SCP     SFTP     FTP

Directory Path\*

/test/backups

Delete file from Application Delivery Management after transfer

注

Citrix ADM は、選択した Citrix ADC インスタンスのいずれかでバックアップが失敗すると、SNMP トラップまたは Syslog 通知をそれ自体に送信します。

**Citrix ADNetScaler ADM** を使用して、選択した **NetScaler ADC** インスタンスのバックアップを作成する

選択した NetScaler ADC 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、次のタスクを実行します。

1. Citrix ADM で、[ネットワーク] > [インスタンス] に移動します。[インスタンス] で、画面に表示するインスタンスのタイプ (Citrix VPX など) 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、BLX インスタンスの場合は、アクションの選択リストから [ \*\* バックアップ/復元 ] を選択します \*\*。
  - SDX インスタンスの場合は、[ バックアップ/復元 ] をクリックします。
3. [ファイルのバックアップ] ページで、[バックアップ] をクリックします。
4. セキュリティを強化するために、バックアップファイルを暗号化するかどうかを指定できます。パスワードを入力するか、[インスタンスバックアップ設定] ページで以前に指定したグローバルパスワードを使用できます。
5. [続行] をクリックします。

### NetScaler ADM を使用して NetScaler ADC インスタンスを復元する

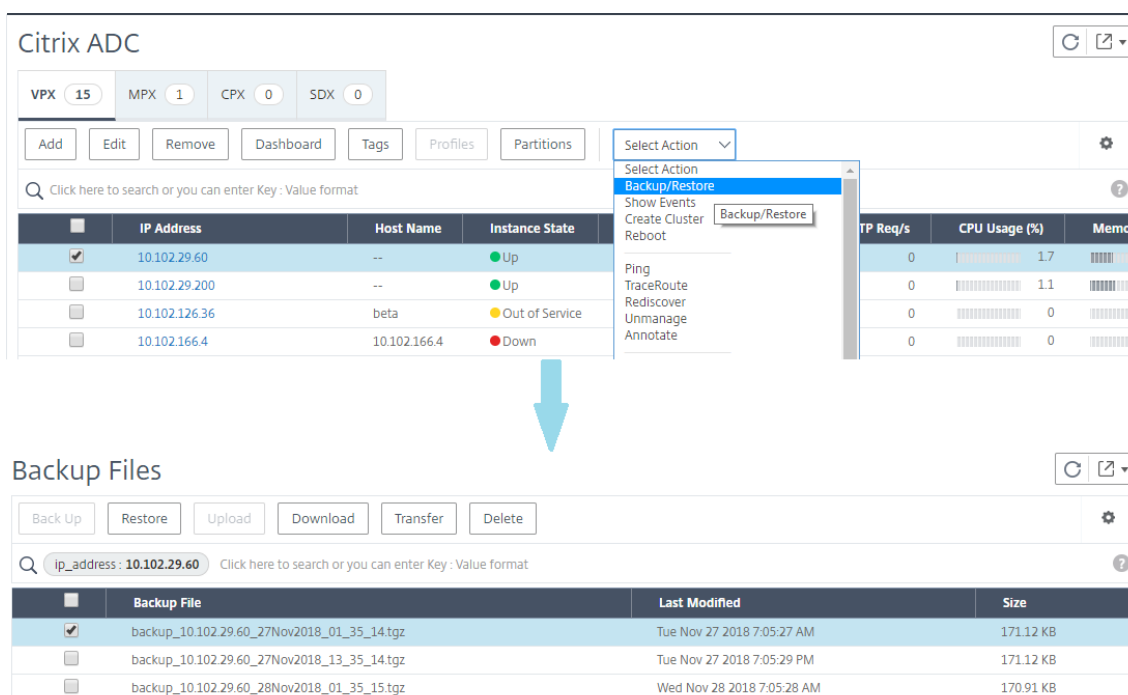
注:NetScaler ADC インスタンスが HA

ペアになっている場合は、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の作成元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作成されたシナリオを考えてみましょう。復元プロセス中は、プライマリインスタンスではなくなった場合でも、必ず同じインスタンスを復元してください。
- プライマリ ADC インスタンスで復元プロセスを開始すると、プライマリインスタンスにアクセスできなくなり、セカンダリインスタンスが **STAYSECONDARY** に変更されます。プライマリインスタンスで復元プロセスが完了すると、セカンダリ ADC インスタンスは **STAYSECONDARY** モードから **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 ADC インスタンスを復元するには、次のタスクを実行します。

1. [ネットワーク]>[インスタンス] に移動し、復元するインスタンスを選択して、[バックアップを表示] をクリックします。
2. [バックアップファイル] ページで、復元する設定を含むバックアップファイルを選択し、[復元] をクリックします。



## NetScaler ADM を使用して NetScaler ADC SDX アプライアンスを復元する

Citrix ADM では、Citrix ADC SDX アプライアンスのバックアップには次のものが含まれます。

- アプライアンスでホストされている NetScaler ADC インスタンス
- SVM SSL 証明書とキー
- Instance の削除設定 (XML 形式)
- Instance のバックアップ設定 (XML 形式)
- SSL 証明書ポーリング設定 (XML 形式)
- SVM データベースファイル
- SDX 上に存在するデバイスの NetScaler ADC 構成ファイル
- NetScaler ADC ビルドイメージ
- NetScaler ADC 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 単一バンドルイメージ (SVM+XS)
- サードパーティの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)

Citrix ADC SDX アプライアンスをバックアップファイルにある構成に復元します。アプライアンスの復元中に、現在の構成全体は削除されます。

別の Citrix ADC SDX アプライアンスのバックアップを使用して Citrix ADC SDX アプライアンスを復元する場合は、復元プロセスを開始する前に、必ずライセンスを追加し、バックアップファイルの設定と一致するようにアプライアンスの管理サービスネットワーク設定を構成してください。

SDX アプライアンスを復元する前に、バックアップした SDX アプライアンスプラットフォームバリエーションがアプライアンスと同じであることを確認してください。異なるプラットフォームのバリエーションでは復元できません。

注

:SDX RMA アプライアンスを復元する前に、バックアップしたバージョンが RMA バージョンと同じかそれ以上であることを確認してください。

バックアップしたファイルから SDX アプライアンスを復元するには:

1. Citrix ADM GUI で、[ ネットワーク ] > [ インスタンス ] > [ Citrix ADC ] に移動します。
2. [ バックアップ/復元 ] をクリックします。
3. 復元したい同じインスタンスのバックアップファイルを選択します。
4. 「バックアップを再パッケージ化」をクリックします。

SDX アプライアンスをバックアップすると、ネットワーク帯域幅とディスク容量を節約するために、XVA ファイルとイメージは別々に保存されます。そのため、SDX アプライアンスを復元する前に、バックアップしたファイルを再パッケージ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すると、SDX アプライアンスを復元するためにバックアップされたすべてのファイルが一緒に含まれます。再パッケージされたバックアップファイルにより、SDX アプライアンスが正常に復元されます。

5. 再パッケージするバックアップファイルを選択し、[ Restore ] をクリックします。

## セカンダリ NetScaler ADC インスタンスへのフェイルオーバーを強制する

February 6, 2024

たとえば、プライマリの Citrix Application Delivery Controller (ADC) 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は、強制的にフェイルオーバーを実行する必要があります。プライマリインスタンス、セカンダリインスタンスのいずれからでもフェイ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イルオーバーを強制した場合、プライマリがセカンダリとなり、セカンダリがプライマリとなります。強制フェイルオーバーを実行できるのは、セカンダリインスタンスが UP の状態であることをプライマリインスタンスが判別できる時のみです。

強制フェイルオーバーは継承されたり、同期されたりしません。強制フェイルオーバー後の同期の状態を確認するには、インスタンスの状態を表示してください。

次の状況では、強制フェイルオーバーを実行できません。

- スタンドアロンシステムにフェイルオーバーを強制する。

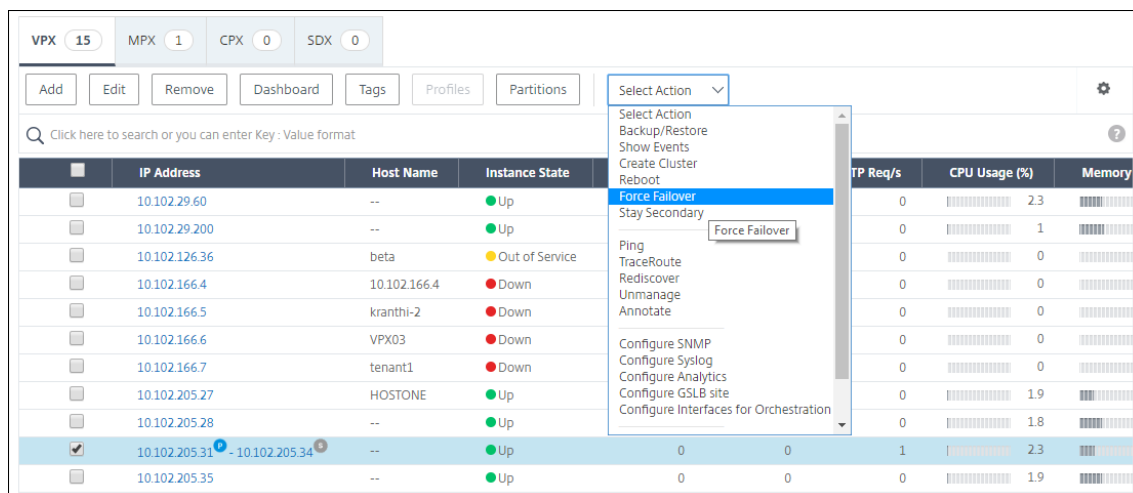
- セカンダリインスタンスが無効または非アクティブである。セカンダリインスタンスが非アクティブの場合、状態が UP になるまで待ってからフェールオーバーを強制してください。
- セカンダリを維持するようにセカンダリインスタンスが構成されている。

NetScaler ADC インスタンスは、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を検出すると、警告メッセージを表示します。メッセージには警告の要因に関する情報が含まれており、手順を進める前に確認が求められます。

プライマリインスタンスまたはセカンダリインスタンスでフェールオーバーを強制できます。

**Citrix ADNetScaler ADM** を使用してセカンダリ **NetScaler ADC** インスタンスにフェールオーバーを強制するには:

1. NetScaler Application Delivery Management (ADM) で、[ネットワーク]>[インスタンス]>[NetScaler ADC] > [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の種類にリストされているインスタンスから、HA セットアップを構成するインスタンスを選択します。
3. 「アクション」メニューから、「強制フェールオーバー」を選択します。
4. [Yes] をクリックして強制フェールオーバーアクションを確定します。



## セカンダリ NetScaler ADC インスタンスを強制的にセカンダリとして保持する

February 6, 2024

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強制的に維持できます。



たとえば、プライマリノードをアップグレードする必要があり、アップグレード処理に数秒かかるものとします。アップグレード中、プライマリノードが数秒間停止することがありますが、セカンダリノードを引き継ぎたくないようにします。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にします。

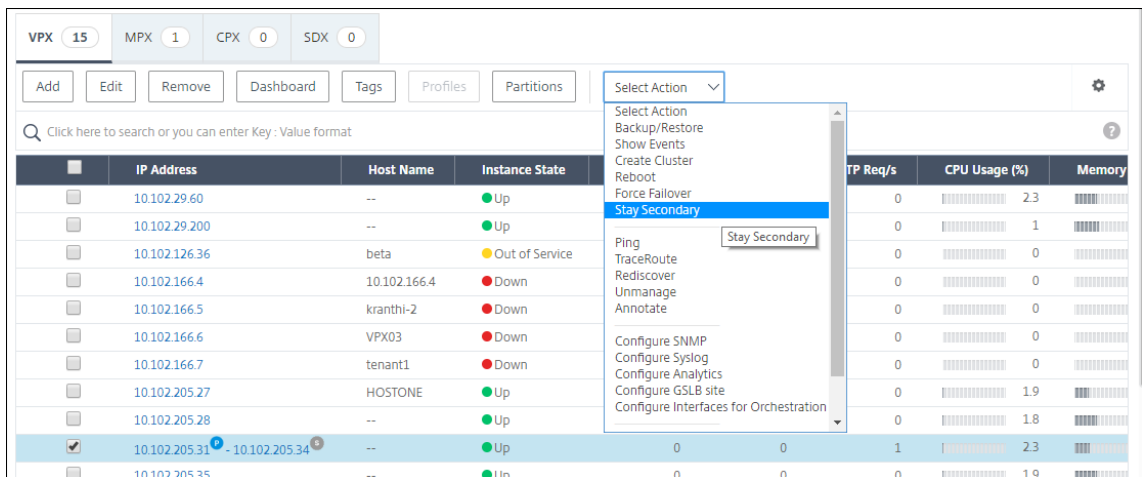
セカンダリノードを強制的にセカンダリのままにすると、プライマリノードがダウンしてもセカンダリのままになります。HA ペアの一方のノードのステータスをセカンダリのまま強制的に維持すると、そのノードは、HA 状態マシン遷移には参加しません。ノードのステータスは、STAYSECONDARY として表示されます。

注

システムをセカンダリのまま強制的に維持する場合、その強制を実施するプロセスは、伝播も同期もされません。コマンドを実行するノードのみが対象となります。

**NetScaler ADM** を使用してセカンダリ **NetScaler ADC** インスタンスをセカンダリとして保持するように構成するには:

1. Citrix Application Delivery Management (ADM) で、[ ネットワーク ] > [ インスタンス ] > [ \*\*Citrix ADC\*\* ] > [ 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の種類にリストされているインスタンスから、HA セットアップを構成するインスタンスを選択します。
3. 「アクション」メニューから「セカンダリーを維持」を選択します。
4. [Yes] をクリックして、「Stay Secondary」アクションの実行を確定します。



## インスタンスグループの作成

February 6, 2024

インスタンスグループを作成するには、まずすべての NetScaler ADC インスタンスを NetScaler ADM に追加する必要があります。インスタンスを正常に追加したら、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を一度にアップグレード、バックアップ、または復元するのに役立ちます。

**NetScaler ADM** を使用してインスタンスグループを作成するには

1. NetScaler ADM で、[ネットワーク] > [インスタンスグループ] の順に選択し、[追加] をクリックします。
2. インスタンスグループの名前を指定し、[インスタンスファミリー] リストから [**NetScaler ADC**] を選択します。
3. [インスタンスを選択] 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、選択したインスタンスとその詳細が表示されます。グループからインスタンスを削除する場合は、テーブルからインスタンスを選択して [削除] をクリックします。
4. [作成] をクリックします。

**Create Instance Group**

Name\*

Instance Family\*

Instances

| <input type="checkbox"/>            | IP ADDRESS | HOST NAME | STATE |
|-------------------------------------|------------|-----------|-------|
| <input checked="" type="checkbox"/> |            | --        | ● Up  |
| <input checked="" type="checkbox"/> |            | --        | ● Up  |

## ADM を使用して SDX 上の ADC VPX インスタンスのプロビジョニング

February 6, 2024

NetScaler ADM を使用して、SDX アプライアンス上に 1 つ以上の ADC 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。追加するインスタンスの数がライセンスで指定されている数と同じである場合、ADM はより多くの NetScaler ADC インスタンスをプロビジョニングすることを制限します。

開始する前に、VPX インスタンスをプロビジョニングする ADM に SDX インスタンスを追加してください。

VPX インスタンスをプロビジョニングするには、次の手順を実行します。

1. [ネットワーク] > [インスタンス] > [Citrix ADC] 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. 「アクションの選択」で、「VPX のプロビジョニング」を選択します。

### ステップ 1-VPX インスタンスを追加する

ADM は、次の情報を使用して、SDX アプライアンスの VPX インスタンスを構成します。

- 名前 - ADC インスタンスに名前を指定します。
- SDX と VPX 間の通信ネットワークを確立します。これを行うには、リストから必要なオプションを選択します。
  - 内部ネットワークを介して管理 - このオプションは、ADM と VPX インスタンス間の通信のための内部ネットワークを確立します。
  - IP アドレス - Citrix VPX インスタンスを管理するために、IPv4 または IPv6 アドレス、またはその両方を選択できます。VPX インスタンスは、1 つの管理 IP (NetScaler ADC IP と呼ばれます) のみを持つことができます。NetScaler ADC 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で、IP アドレスのネットマスク、デフォルトゲートウェイ、およびネクストホップを ADM サーバに割り当てます。
- XVA ファイル - VPX インスタンスをプロビジョニングする XVA ファイルを選択します。XVA ファイルを選択するには、次のいずれかのオプションを使用します。
  - ローカル-ローカルマシンから XVA ファイルを選択します。
  - アプライアンス - ADM ファイルブラウザから XVA ファイルを選択します。
- 管理者プロファイル - このプロファイルは、VPX インスタンスをプロビジョニングするためのアクセスを提供します。このプロファイルを使用すると、ADM はインスタンスから設定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。

- **Agent** : 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。

Name\*

 ⓘ

Manage through internal network ⓘ

IPv4

IPv4 Address\*

Netmask\*

Gateway

 ⓘ

Nexthop to Management Service

 ⓘ

IPv6

XVA File\*

  ⓘ

Admin Profile\*

  ⓘ

Agent\*

Site\*

## ステップ 2-ライセンスの割り当て

[ライセンスの割り当て] セクションで、VPX ライセンスを指定します。スタンダード、アドバンスト、プレミアムライセンスを使用できます。

- 割り当てモード：帯域幅プールに対して [ 固定 ] または [ パースト可能 ] モードを選択できます。  
パ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追加の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) を割り当てます。

### 注:

SDX アプライアンス上の Citrix Secure Web Gateway (SWG) インスタンス用のライセンス (Secure Web Gateway 用の SDX 2 インスタンスアドオンパック) を別途購入してください。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。

詳しくは、「[SDX アプライアンスへの Citrix Secure Web Gateway インスタンスの展開](#)」を参照してください。

**License Allocation**

Feature License\* For more information about Citrix ADC editions, see [Citrix ADC Editions](#)

| Pool     | Total | Available | Allocate |
|----------|-------|-----------|----------|
| Instance | 2     | 1         | 1        |

Bandwidth Allocation Mode\*

|  |        |        |                                                      |
|--|--------|--------|------------------------------------------------------|
|  | 4 Gbps | 3 Gbps | Throughput (Mbps)* <input type="text" value="1000"/> |
|--|--------|--------|------------------------------------------------------|

**Crypto Allocation**

|           | Asymmetric Crypto Units | Symmetric Crypto Units | Crypto Virtual Interfaces |
|-----------|-------------------------|------------------------|---------------------------|
| Available | 11248                   | 10000                  | 4                         |
| Total     | 11248                   | 10000                  | 4                         |

Asymmetric Crypto Units

Symmetric Crypto Units

SDX 12.0 57.19 バージョンから、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。詳しくは、「[暗号容量の管理](#)」を参照してください。

## ステップ 3-リソースを割り当てる

「リソース割り当て」セクションで、リソースを VPX インスタンスに割り当てて、トラフィックを維持します。

- 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。

- [パケット/秒]-1 秒あたりに送信するパケット数を指定します。
- **CPU** -インスタンスに対する CPU コアの数を選択します。共有 CPU コアまたは専用の CPU コアを使用できます。

インスタンスに対して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は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ます。

SDX 2500xx プラットフォームを使用している場合は、インスタンスには最大 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は、インスタンスには最大 11 個のコアを割り当てることができます。

注:

インスタンスの場合、構成する最大スループットは 180 Gbps です。

**Resource Allocation**

Total Memory (MB)\*

2048

Packets per second\*

1000000

CPU\*

Shared (1 core) ▼

次の表に、サポートされている VPX、シングルバングルイメージのバージョン、およびインスタンスに割り当て可能なコア数を示します。

| プラットフォーム名                                                   | 総コア数 | VPX プロビジョニングで使用可能なコアの合計 | 1つのインスタンスに割り当て可能な最大コア数 |
|-------------------------------------------------------------|------|-------------------------|------------------------|
| SDX 8015、SDX 8400、SDX 8600                                  | 4    | 3                       | 3                      |
| SDX 8900                                                    | 8    | 7                       | 7                      |
| SDX 11500、SDX 13500、SDX 14500、SDX 16500、SDX 18500、SDX 20500 | 12   | 10                      | 5                      |

| プラットフォーム名                                                                                                         | 総コア数 | VPX プロビジョニングで<br>使用可能なコアの合計 | 1つのインスタンスに割り<br>当て可能な最大コア数                                                                       |
|-------------------------------------------------------------------------------------------------------------------|------|-----------------------------|--------------------------------------------------------------------------------------------------|
| SDX 11515、SDX 11520、<br>SDX 11530、SDX 11540、<br>SDX 11540、SDX 11542                                               | 12   | 10                          | 5                                                                                                |
| SDX 17500、SDX<br>19500、SDX 21500                                                                                  | 12   | 10                          | 5                                                                                                |
| SDX 17550、SDX 19550、<br>SDX 20550、SDX 21550                                                                       | 12   | 10                          | 5                                                                                                |
| SDX 14020、SDX 14030、<br>SDX 14040、SDX 14060、<br>SDX 14080、SDX 14100                                               | 12   | 10                          | 5                                                                                                |
| SDX 22040、SDX<br>22060、SDX 22080、<br>SDX 22100、SDX 22120                                                          | 16   | 14                          | 7                                                                                                |
| SDX 24100 と SDX<br>24150                                                                                          | 16   | 14                          | 7                                                                                                |
| SDX 14020 40G、SDX<br>14030 40G、SDX 14040<br>40G、SDX 14060 40G、<br>SDX 14060 40G、SDX<br>14080 40G、SDX 14100<br>40G | 12   | 10                          | 10                                                                                               |
| SDX 14020 FIPS、SDX<br>14030 FIPS、SDX 14040<br>FIPS、SDX 14060 FIPS、<br>SDX 14080 FIPS、SDX<br>14100。FIPS            | 12   | 10                          | 5                                                                                                |
| SDX 14040 40S、SDX<br>14060 40S、SDX 14080<br>40S、SDX 14100 40S                                                     | 12   | 10                          | 5                                                                                                |
| SDX 25100A、25160A、<br>25200A                                                                                      | 20   | 18                          | 9                                                                                                |
| SDX 25100-40G、<br>25160-40G、25200-40G                                                                             | 20   | 18                          | 16 (バージョンが<br>11.1-51.x 以上の場合); 9<br>(バージョンが 11.1-50.x<br>以下の場合、11.0 および<br>10.5 のすべてのバージョ<br>ン) |



| プラットフォーム名                      | 総コア数 | VPX プロビジョニングで使用可能なコアの合計 | 1つのインスタンスに割り当て可能な最大コア数 |
|--------------------------------|------|-------------------------|------------------------|
| SDX 26100, 26160, 26200, 26250 | 28   | 26                      | 13                     |
| 15000-50G                      | 16   | 14                      | 7                      |

## 注:

SDX 26xxx プラットフォームでは、VPX インスタンスに最大 26 個の CPU コアを割り当てることができます。暗号化ユニットがインスタンスに割り当てられている場合、コアの最大数は、暗号ユニットとデータインターフェイスの数によって異なります。

たとえば、24000 暗号ユニットをインスタンスに割り当てると、24 の CPU コアと最大 2 つのデータインターフェイスをインスタンスに割り当てることができます。SDX アプライアンスは、データインターフェイスと暗号ユニットを PCI デバイスと見なします。26000 暗号ユニットでは、データインターフェイスを追加するスペースがないため、VPX インスタンスのプロビジョニングが失敗します。

## ステップ 4-インスタンス管理を追加する

VPX インスタンスの管理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]\*\* セクションの [\*\* インスタンス管理を追加] を選択します。

次の詳細を指定します:

- ユーザー名: Citrix ADC インスタンス管理者のユーザー名。このユーザはスーパーユーザアクセスできますが、VLAN およびインターフェイ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がありません。
- パスワード: ユーザー名のパスワードを指定します。
- シェル/**Sftp/Scp** アクセス: Citrix ADC インスタンス管理者に許可されているアクセス。このオプションはデフォルトで選択されています。

### Instance Administration

Add Instance Administration

User Name\*

 ⓘ

Password\*

Confirm Password\*

 ⓘ

Shell/SFTP/SCP Access

#### 手順 5-ネットワーク設定を指定する

インスタンスに必要なネットワーク設定を選択します。

- ネットワーク設定で **L2** モードを許可する -NetScaler ADC 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、L2 モードを有効にする前に。詳しくは、「[NetScaler ADC 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、インスタンスにログオンし、そのインスタンスから L2 モードを無効にする必要があります。そうしないと、インスタンスの再起動後に他のすべての NetScaler ADC モードが無効になる可能性があります。

- **0/1 - VLAN** タグで、管理インターフェイスの VLAN ID を指定します。
- **0/2 - VLAN** タグで、管理インターフェイスの VLAN ID を指定します。

デフォルトでは、インターフェイス **0/1** および **0/2** が選択されます。

**Network Settings**

Allow L2 Mode ⓘ

0/1      VLAN Tag:  ⓘ

**Data Interfaces**

| INTERFACE | ALLOW UNTAGGED TRAFFIC | ALLOWED VLANS |
|-----------|------------------------|---------------|
| No items  |                        |               |

「データ・インタフェース」で、「追加」をクリックしてデータ・インタフェースを追加し、次を指定します。

- [インタフェース]-リストからインターフェイスを選択します。

注:

インスタンスに追加するインターフェイスのインターフェイス ID は、SDX アプライアンスでの物理インターフェイスの番号付けに対応しているとは限りません。

たとえば、インスタンス 1 に関連付ける最初のインターフェイスは SDX インターフェイス 1/4 で、そのインスタンスのインターフェイス設定を表示すると、インターフェイス 1/1 として表示されます。このインターフェイスは、instance-1 に関連付けた最初のインターフェイスであることを示します。

- 許可された **VLAN** : NetScaler ADC 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を選択します:
  - デフォルト - Citrix Workspace によって MAC アドレスが割り当てられます。
  - [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。
  - **Generated** - 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、[インターフェイスへの 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** を設定するための **IPv4** および **IPv6 VRID**)
  - **VRID IPV4** - VMAC を識別する IPv4 VRID。可能な値: 1 ~ 255 詳細については、「[インターフェイスでの VMC の設定](#)」を参照してください。
  - **VRID IPV6** - VMAC を識別する IPv6 VRID。可能な値: 1 ~ 255 詳細については、「[インターフェイスでの VMC の設定](#)」を参照してください。

## Add Data Interface

Interfaces\*

1/2

Allow Untagged Traffic

Allowed VLANs

100-110,142,151-155

MAC Address Mode\*

Default

▼ VMAC Settings (IPv4 and IPv6 VRIDs to configure Virtual MAC)

VRID IPv4

100-110,142,151-155

VRID IPv6

100-110,142,151-155

**Add** Close

[追加] をクリックします。

### ステップ 6-管理 VLAN 設定を指定する

VPX インスタンスの管理サービスと管理アドレス (NSIP) は同じサブネットワークにあり、通信は管理インターフェースを介して実行されます。

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 インスタンスのプロビジョニング中に VLAN ID を指定します。したがって、インスタンスは、アクティブなときにネットワーク経由で到達可能です。

VPX インスタンスのプロビジョニング中に、選択したインターフェイスからのみ NSIP にアクセスできるようにする必要がある場合は、[NSVLAN] を選択します。また、NSIP は他のインターフェイスを介してアクセスできなくなります。

- HA ハートビートは、NSVLAN の一部であるインターフェイスだけで送信されます。
- NSVLAN は、VPX XVA ビルド 9.3-53.4 以降からのみ構成できます。

### 重要

- VPX インスタンスをプロビジョニングした後は、この設定を変更できません。
- **NSVLAN** が選択されていない場合、VPX インスタンス上で **clear config full** コマンドを実行すると、**VLAN** 構成が削除されます。

Management VLAN Settings

VLAN for Management Traffic

10.103.23.56 ⓘ

**L2VLAN**

When this option is selected, the configured VLAN is created as a data VLAN on Citrix ADC Instance, and is used by the Management Service to access the NSIP for all communication with the instance. This option is suitable for performing in-band management of the instance over the data VLAN, without creating a separate management network.

**NSVLAN**

When this option is selected, the configured VLAN is created as the NSVLAN on Citrix ADC Instance, and is used by the Management Service to access the NSIP for all communication with the instance. This option is suitable for performing out-of-band management of the instance over a separate management network. i.e., the NSVLAN.

Tagall ⓘ

Interfaces

Configured (0) Remove All

No items

+ Add

Done Close

「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 インスタンスの表示

新しくプロビジョニングされたインスタンスを表示するには、次の手順を実行します。

1. [ネットワーク] > [インスタンス] > [Citrix ADC] 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、そのインスタンスに SDX インスタンスの IP を指定します。

| <input type="checkbox"/> | IP ADDRESS | HOST NAME | INSTANCE STATE | RX (MBPS) | TX (MBPS) | HTTP REQ/S | AGENT  | SITE             |
|--------------------------|------------|-----------|----------------|-----------|-----------|------------|--------|------------------|
| <input type="checkbox"/> |            | NS1       | Up             | 0         | 0         | 0          | ns ( ) | 9k0p84w86lxn_def |

Total 1

25 Per Page Page 1 of 1

## 複数の Citrix VPX インスタンスの再検出

February 6, 2024

NetScaler Application Delivery Management (ADM) のセットアップで複数の Citrix VPX インスタンスを再検出できます。また、それらのインスタンスの最新の状態と構成を表示する場合は、複数の Citrix VPX インスタンスを再検出できます。NetScaler ADM サーバーはすべての Citrix VPX インスタンスを再検出し、Citrix Application Delivery Controller (ADC) インスタンスに到達可能かどうかを確認します。

複数の **Citrix VPX** インスタンスを再検出するには：

1. Web ブラウザで、Citrix ADM サーバーの IP アドレス（たとえば、<http://192.168.100.1>）を入力します。
  2. **[User Name]** と **[Password]** の各フィールドに管理者の資格情報を入力します。デフォルトの管理者クレデンシャルは **nsroot** と **nsroot** です。
  3. **[ネットワーク]** > **[インスタンス]** > **[NetScaler ADC]** > **[VPX]** タブに移動し、再検出するインスタンスを選択します。
  4. **[アクションの選択]** メニューで、**[再検出]** をクリックします。
  5. 再検出ユーティリティを実行するための確認メッセージが表示されたら、**[はい]** をクリックします。
- 各 Citrix VPX インスタンスの再検出の進行状況が画面に表示されます。

## インスタンスの管理解除

February 6, 2024

Citrix Application Delivery Management (ADM) とネットワーク内のインスタンス間の情報交換を停止したい場合は、インスタンスを管理解除できます。

インスタンスの管理を解除するには、次の手順に従います。

[ ネットワーク ] > [ インスタンス ] > [ \*\*Citrix ADC\*\* ] > [ VPX ] タブに移動します。インスタンスのリストで、インスタンスを右クリックして [ **UnManage** ] を選択するか、インスタンスを選択し、[ **Select Action** ] リストから [ **UnManage** ] を選択します。

次の図に示すように、選択したインスタンスのステータスが [ **Out of Service** ] に変わります。

|  | IP Address    | Host Name    | Instance State   | Rx (Mbps) | Tx (Mbps) | HTTP Req/s | CPU Usage (%) | Memor |
|--|---------------|--------------|------------------|-----------|-----------|------------|---------------|-------|
|  | 10.102.29.60  | --           | ● Up             | 0         | 0         | 0          | 2.4           |       |
|  | 10.102.29.200 | --           | ● Up             | 0         | 0         | 0          | 1.1           |       |
|  | 10.102.126.36 | beta         | ● Out of Service | 0         | 0         | 0          | 0             |       |
|  | 10.102.166.4  | 10.102.166.4 | ● Down           | 0         | 0         | 0          | 0             |       |
|  | 10.102.166.5  | kranthi-2    | ● Down           | 0         | 0         | 0          | 0             |       |

インスタンスは NetScaler ADM によって管理されなくなり、NetScaler ADM とデータを交換できなくなります。

## インスタンスへのルートをトレースする

February 6, 2024

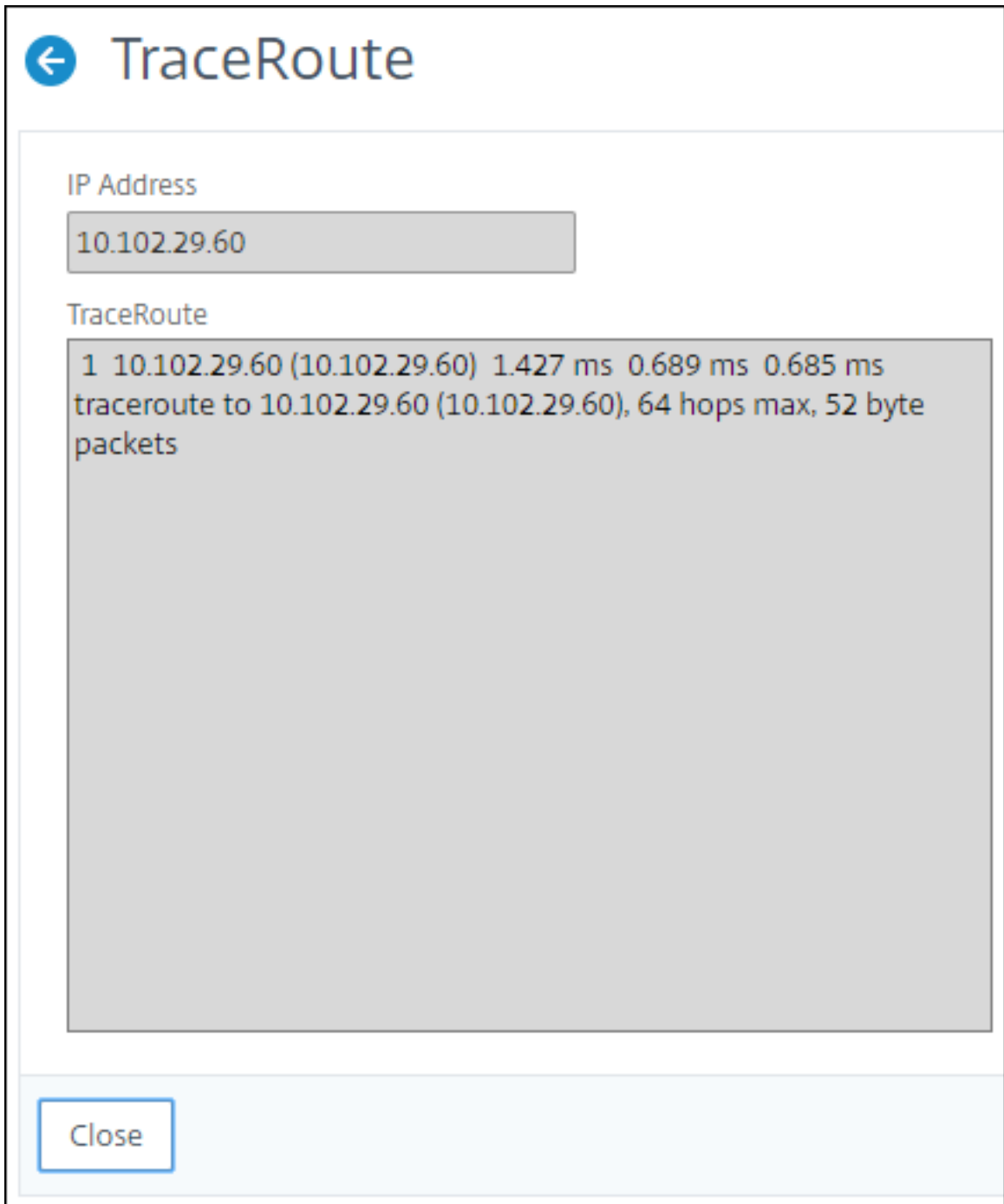
NetScaler Application Delivery Management (ADM) からインスタンスへのパケットのルートを追跡することで、インスタンスに到達するために必要なホップ数などの情報を確認できます。Traceroute では、ソースから宛先までのパケットのパスがトレースされます。これには、ルート内の各エンティティのホスト名と IP アドレスと共に、ネットワークホップの一覧が表示されます。

また、Traceroute では、あるホップから別のホップへパケットが移動するのにかかる時間が記録されます。パケットの転送に中断があった場合は、traceroute によって、問題が存在する場所が示されます。

インスタンスのルートをトレースするには:

1. Citrix ADM で、[ ネットワーク ] > [ インスタンス ] > [ \*\*Citrix ADC\*\* ] > [ VPX ] タブに移動します。
2. インスタンスのリストで、インスタンスを右クリックして [ **TraceRoute** ] を選択するか、インスタンスを選択し、[ アクションの選択 ] メニューから [ **TraceRoute** ] をクリックします。

**TraceRoute** メッセージボックスには、インスタンスへのルートと、各ホップで消費された時間 (ミリ秒単位) が表示されます。



## アップグレードアドバイザリ

February 6, 2024

ネットワーク管理者は、NetScaler ADM 異なる ADC リリースで実行されている多数の ADC インスタンスを管理で



きます。各 ADC インスタンスのライフサイクルの監視は、面倒な作業になります。[Citrix 製品マトリックスにアクセスして](#)、サポート終了（EOL）またはメンテナンス終了（EOM）に近づいている、または近づいている ADC 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。

アップグレードアドバイザーは、ADC 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/EOM に達しているインスタンスを識別し、EOL または EOM 日より前に ADC のアップグレードを計画できます。

アップグレードアドバイザーは、ADC のバージョンスキャンを実行し、ADC インスタンス全体の EOM/EOL ビルドを表示します。

ADC インスタンスの 1 つを選択して ADM サービスにオンボーディングできます。「**ADM Service**」をクリックし、ADC インスタンスをオンボーディングすると、詳細な分析情報が表示されます。ADM Service Upgrade アドバイザリ機能の詳細については、アップグレードアドバイザーページの gif アニメーションをプレビューしてください。

### アップグレードアドバイザーを表示

「ネットワーク」>「インスタンス・アドバイザー」>「アップグレード・アドバイザー」の順にナビゲートし、次の情報を表示します。

- ADC インスタンスの総数。
- インスタンスは、寿命の終わりに達しました。
- インスタンスがメンテナンスの終了に達しました。

**Upgrade Advisory** Preview

We found the below ADCs running EOM/EOL builds in your deployment.

For detailed insights, Try ADM Service with just one of your ADC instance  
Save your time and effort to plan your upgrades with an admin-friendly view & a simple workflow!

1 ADC instances nearing EOM/EOL

MPX & VPX SDX

2 TOTAL MPX & VPX 0 INSTANCES REACHING END OF LIFE 1 INSTANCES REACHING END OF MAINTENANCE

ADC instances grouped by releases / builds

| Release 13.1         | End of Maintenance: 15 Sep, 2025 | Release 13.0         | End of Maintenance: 15 May, 2023 |     |     |
|----------------------|----------------------------------|----------------------|----------------------------------|-----|-----|
| 1 Total ADC Instance |                                  | 1 Total ADC Instance |                                  |     |     |
| Build                | MPX                              | VPX                  | Build                            | MPX | VPX |
| 24.25                | 0                                | 1                    | 88.14                            | 0   | 1   |

**Admins love ADM service, see why** [Try ADM Service](#)

ADM Service Upgrade advisory is Simple, Efficient & Admin Friendly.  
Start by trying Upgrade advisory for 1 instance in ADM Service now.

Identification of all the ADC instances that are:  
1. Reaching EOL/EOM  
2. On older build  
3. Not on preferred build

- Proactively view & plan upgrades for detailed view & selection of EOM/EOL builds across your ADC instances
- Simple 1 Click workflow Custom create scheduled upgrades or trigger an on-demand upgrade
- View Most downloaded builds by other ADC customers and plan your upgrade build choice
- Pre and post validation checks for controlled and effective upgrades

For more details, please refer the product documentation [here](#)

「アップグレードアドバイザー」ページには、リリースごとに ADC インスタンスがグループ化されます。

## セキュリティアドバイザー

February 6, 2024

安全で耐障害性に優れたインフラストラクチャは、あらゆる組織のライフラインです。組織は、新たな共通脆弱性と危険性 (CVE) を追跡し、CVE が自社のインフラストラクチャに与える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緩和策と修復方法を理解し、計画する必要があります。

NetScaler ADM のセキュリティアドバイザーでは、ADC インスタンスを危険にさらす Citrix CVE に焦点を当てています。

### セキュリティ勧告を見る

セキュリティアドバイザーにアクセスするには、[ネットワーク]>[インスタンスアドバイザー]>[セキュリティアドバイザー]に移動します。NetScaler ADM で管理しているすべての ADC インスタンスの脆弱性ステータスを確認できます。

### Security Advisory Preview

We found the below ADCs are vulnerable to some CVEs in your deployment.

Try ADM Service with just one of your ADC instance and see how quickly we help save your time and effort in helping you maintain your security posture with remediation/mitigation workflows!

**Note:** The below advisory details are based on ADC build version scan only. More conclusive and exhaustive security advisory insights can be seen after onboarding your ADCs to ADM Service.

**4**  
ADC instances are vulnerable

**Details**

| CVE ID         | VULNERABILITY TYPE                  | AFFECTED ADC INSTANCES |
|----------------|-------------------------------------|------------------------|
| CVE-2020-8197  | Elevation of privileges             | 3 ADC                  |
| CVE-2020-8187  | Denial of service                   | 3 ADC                  |
| CVE-2022-27509 | Unauthenticated redirection to ...  | 4 ADC                  |
| CVE-2020-8196  | Information disclosure              | 3 ADC                  |
| CVE-2020-8247  | Escalation of privileges on the ... | 3 ADC                  |

Showing 1-5 of 19 items Page 1 of 4 5 rows

### ADM Service helps secure your ADCs better, check how

Assess your Security posture quickly and remediate efficiently. Start by trying Security advisory for 1 instance in ADM Service now.

- ! Review CVEs and the impacted ADCs in your fleet
- i Product led CVE impact analysis to aid admins on quick and effective remediation/mitigation.
- ✓ On Demand or Weekly ADM driven System scans to assess current or post remediation security posture

For more details, please refer the product documentation [here](#)

セキュリティアドバイザーは、ADC バージョンスキャンのみを実行して CVE をチェックし、ADC インスタンスに影響する CVE の数を示す表が表示されます。

- **CVE ID:** インスタンスに影響する CVE の ID。
- **脆弱性タイプ:** この CVE の脆弱性のタイプ。
- **影響を受ける ADC インスタンス:** CVE ID が影響しているインスタンス数。

特定の CVE の脆弱性の種類と、その脆弱性を解決するための緩和策と修復に関する情報を確認するには、ADC インスタンスを 1 つ選択して [ **Try ADM Service** ] をクリックし、**ADC** インスタンスを ADM Service にオンボーディングします。**ADM Service** セキュリティアドバイザリ機能の詳細については、セキュリティアドバイザリページの **gif** アニメーションをプレビューしてください。

### イベント

February 6, 2024

Citrix Application Delivery Controller (ADC) インスタンスの IP アドレスが NetScaler Application Delivery Management (ADM) に追加されると、NetScaler ADM は NITRO 呼び出しを送信し、そのインスタンスがトラップまたはイベントを受信するためのトラップ宛先として暗黙的に追加します。

イベントは、管理対象 NetScaler ADC インスタンスでのイベントまたはエラーの発生を表します。たとえば、システム障害や構成の変更があった場合、イベントが生成され、NetScaler ADM サーバーに記録されます。NetScaler ADM で受信したイベントは、[ イベントの概要 ] ページ ([ ネットワーク ] > [ 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 ([ ネットワーク ] > [ イベント ] > [ イベントメッセージ ]) に表示されます。

また、NetScaler ADM は、インスタンスで生成されたイベントをチェックして、異なる重大度レベルのアラームを生成します。これらのアラームはメッセージとして表示され、そのうちのいくつかは即時対応が必要な場合があります。たとえば、システム障害は「Critical」イベントの重大度に分類でき、直ちに解決する必要があります。

特定のイベントを監視するように規則を構成できます。ルールを使用すると、NetScaler ADC インフラストラクチャ全体で生成されるイベント（多数のイベント）を簡単に監視できます。

特定の条件で規則を構成し、規則にアクションを割り当てることで、一連のイベントにフィルターを適用できます。生成されたイベントがルール内のフィルタ条件を満たすと、そのルールに関連付けられたアクションが実行されます。フィルタを作成できる条件は、重大度、NetScaler ADC インスタンス、カテゴリ、障害オブジェクト、構成コマンド、メッセージです。

また、イベントがクリアされるまで、特定の時間間隔で 1 つのイベントに対して複数の通知がトリガーされるようにすることもできます。追加の対策として、特定の件名とユーザーメッセージを使用して電子メールをカスタマイズし、添付ファイルをアップロードすることができます。

### イベントダッシュボードの使用

February 6, 2024

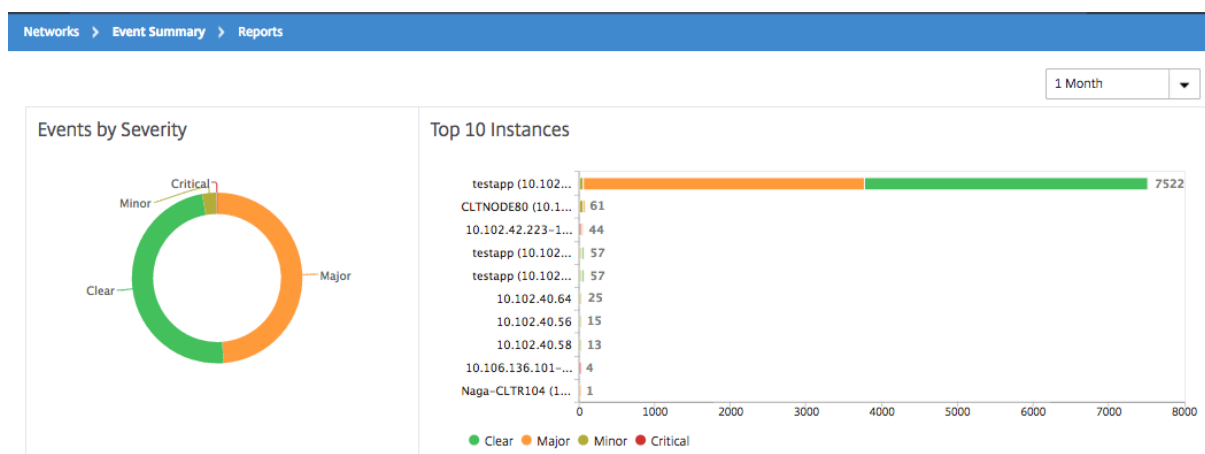
ネットワーク管理者は、Citrix Application Delivery Controller (ADC) インスタンスの構成変更、ログイン条件、ハードウェア障害、しきい値違反、エンティティ状態の変化などの詳細を、特定のインスタンスでのイベントとその

重大度とともに表示できます。NetScaler Application Delivery Management (ADM) のイベントダッシュボードを使用すると、すべての NetScaler ADC インスタンスの重要なイベントの重大度について生成された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、次の手順に従います。

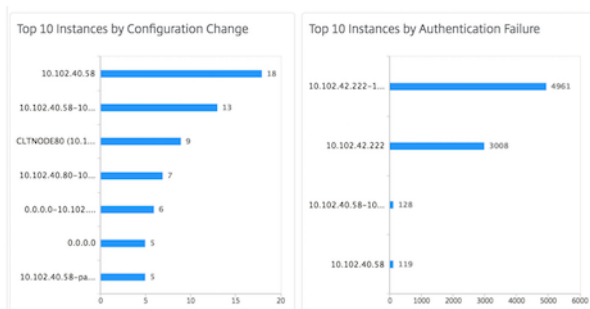
[ ネットワーク ] > [ イベント ] > [ レポート ] に移動します。

ダッシュボードの [ Top 10 Devices ] グラフには、各インスタンスで生成されたイベントの数に基づき、上位 10 個のインスタンスが表示されます。グラフ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。

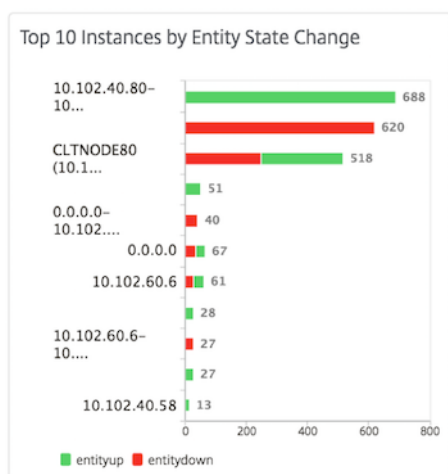


詳細を表示するには、NetScaler ADC インスタンスタイプ ([ ネットワーク ] > [ イベント ] > [ レポート ] > [ **NetScaler ADC/NetScaler ADC SDX/NetScaler ADC SD-WAN WO** ] ) に移動して、次の項目を表示します。

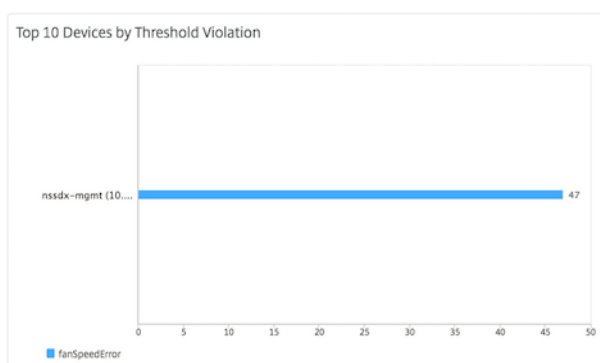
- ハードウェアエラー件数上位 10 デバイス
- 構成変更件数上位 10 デバイス
- 認証エラー件数上位 10 デバイス



- エンティティの状態変更件数上位 10 デバイス



- しきい値の超過件数上位 10 デバイス



## イベントのイベント期間を設定する

February 6, 2024

イベントの経過時間オプションを設定して、時間間隔 (秒単位) を指定できます。NetScaler ADM は、設定された期間までアプライアンスを監視し、イベントの経過時間が設定された期間を超えた場合にのみイベントを生成します。

注:

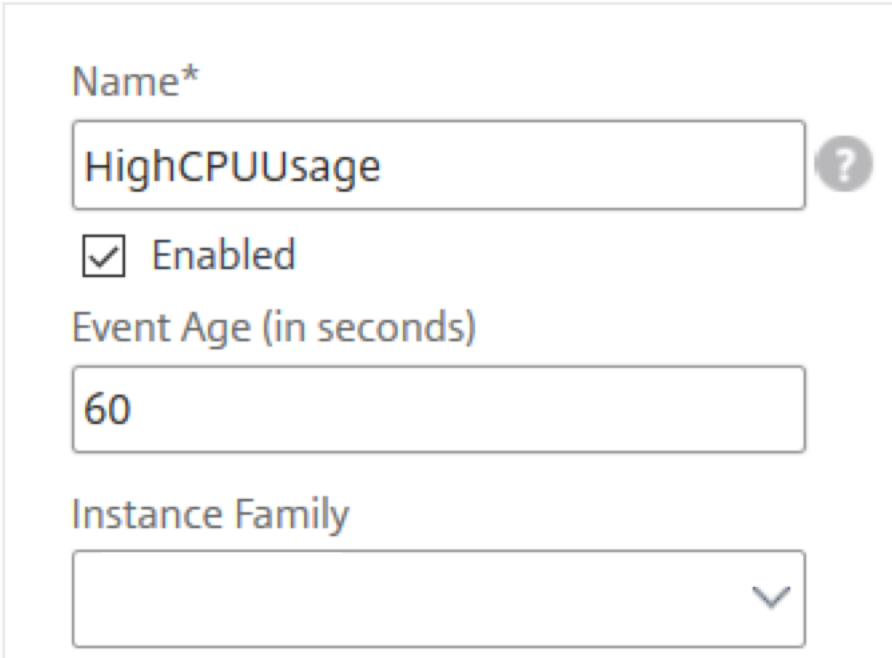
イベント期間の最小値は 60 秒です。[ **Event Age** ] フィールドを空白のままにすると、イベントが発生した直後にイベントルールが適用されます。

たとえば、さまざまな ADC アプライアンスを管理し、仮想サーバーのいずれかが 60 秒以上ダウンしたときに電子メールで通知を受け取りたいとします。必要なフィルタを使用してイベントルールを作成し、ルールのイベント経過時間を 60 秒に設定できます。その後、仮想サーバーが 60 秒以上ダウンしたままになるたびに、エンティティ名、ステータスの変更、時刻などの詳細が記載された電子メール通知を受信します。

**NetScaler ADM** でイベントの経過期間を設定するには:

1. Citrix ADM で、[ネットワーク] > [イベント] > [ルール] に移動し、[追加] をクリックします。
2. [Create Rule] ページで規則パラメーターを設定します。
3. イベント期間を秒数で指定します。

## Create Rule



Name\*

HighCPUUsage ?

Enabled

Event Age (in seconds)

60

Instance Family

イベントの経過期間を設定するときは、[ **Category** ] セクションですべての関連トラップを設定し、[ **Severity** ] セクションでそれぞれの重大度を設定してください。前の例では、`entityup`、`entitydown`、および `entityofs` トラップを選択します。

### イベントフィルタをスケジュールする

February 6, 2024

ルールのフィルターを作成した後、生成されたイベントがフィルター条件を満たすたびに Citrix Application Delivery Management (ADM) サーバーに通知を送信させたくない場合は、毎日、毎週、または毎月などの特定の時間間隔でのみフィルターがトリガーされるようにスケジュールできます。

たとえば、インスタンスの複数のアプリケーションを対象に、異なるタイミングでシステムメンテナンスのスケジュールを指定している場合、それらのインスタンスによって複数のアラームが生成される可能性があります。

これらのアラームのフィルターを構成し、これらのフィルターの電子メール通知を有効にした場合、Citrix ADM が

これらのトラップを受信すると、サーバーは大量の電子メール通知を送信します。このようなサーバーによるメール通知の送信を特定期間に限定するには、フィルターにスケジュールを指定します。

**NetScaler ADM** を使用してフィルタをスケジュールするには：

1. Citrix ADM で、[ネットワーク] > [イベント] > [ルール] に移動します。
2. スケジュールを指定するフィルターの対象となっている規則を選択し、[View Schedule] をクリックします。
3. [Scheduled Rule] ページの [Schedule] をクリックして、次のパラメーターを指定します。
  - [ルールを有効にする] –スケジュールされたイベントルールを有効にするには、このチェックボックスをオンにします。
  - **Recurrence** - 規則に適用するスケジュールの間隔です。特定の曜日または月の特定の日付を選択します。
  - 日数: ルールを実行する曜日を選択します。複数の日を選択できます。
  - 日付: 日付を入力します。複数の日付をカンマ区切りの値として入力できます。
  - [スケジュールされた時間間隔 (時間)] : 規則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。

## ← Schedule Rule

You can enable or disable the event rule and schedule them.

Enable Rule ?

Recurrence\*

Specific day(s) of the week ▼

**NOTE:** Enter the schedule time interval in your local timezone

Days

|     |     |     |     |     |     |     |
|-----|-----|-----|-----|-----|-----|-----|
| Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|-----|-----|-----|-----|-----|-----|-----|

Scheduled Time Interval (Hours)

16-17

イベントに対して繰り返し電子メール通知を設定する

February 6, 2024

すべての重大なイベントに対応し、重要なメール通知を見落とさないために、指定した条件を満たすイベント規則に関して、連続してメール通知を送信するように指定できます。たとえば、ディスクエラーを伴うインスタンスに対するイベント規則を作成し、問題が解決するまで通知するようにする場合、それらのイベントに関して連続メール送信を指定できます。

これらのメール通知は、受信者が通知を見たことを確認するか、イベント規則が解除されるまで、定義された間隔で繰り返し送信されます。

### 注

イベントを自動的にクリアできるのは、同等の「クリア」トラップが設定され、Citrix Application Delivery Controller (ADC) インスタンスから送信された場合のみです。

イベントを手動でクリアするには、次の操作を行います。

- [ネットワーク] > [イベント] > [イベント概要] に移動し、カテゴリを選択し、カテゴリ内のイベントを選択して [クリア] をクリックします。
- または、[ネットワーク] > [イベント] > [イベントメッセージ] に移動します。インスタンスタイプを選択し、下のグリッドからイベントを選択し、[ **Clear** ] をクリックします。

**NetScaler ADM** から繰り返し電子メール通知を設定するには:

1. Citrix Application Delivery Management (ADM) で、[ネットワーク] > [イベント] > [ルール] に移動し、[追加] をクリックしてルールを作成します。
2. [ **Create Rule** ] ページで規則パラメーターを設定します。
3. 「イベントルールアクション」で、「アクションを追加」をクリックします。次に、\*\* アクションタイプドロップダウンリストから「電子メールを送信アクション \*\*」を選択し、電子メール配布リストを選択します。
4. 構成した規則と受信イベントが適合したときに、カスタマイズした件名とユーザーメッセージを追加し、添付ファイルをメールにアップロードすることもできます。
5. [ **Repeat Email Notification until the event is cleared** ] チェックボックスをオンにします。



### Add Event Action

Action Type\*  
Send e-mail Action

Email Distribution List\*  
abc-mails Add Edit Test

Email Subject  
Critical event ?  
 Prefix severity, category, and failure object information to the custom email subject ?

Attachment  
Choose File Upload

Message  
Disk failures to be resolved

Repeat Email Notification until the event is cleared ?

Time Interval (minutes)\*  
5

OK Close

イベントを抑制する

February 6, 2024

**Suppress Action** イベントアクションを選択すると、イベントを抑制またはドロップする期間を分単位で設定できます。最短で1分間イベントを非表示にできます。

注:

抑制時間を 0 分に設定することもできます。これは無限時間を意味します。期間を指定しない場合、NetScaler ADM は抑制時間をゼロとみなし、期限切れになることはありません。

**NetScaler ADM** を使用してイベントを抑制するには:

1. Citrix Application Delivery Management (ADM) で、[ネットワーク] > [イベント] > [ルール] に移動します。[追加] をクリックします。
2. 規則を作成するために必要なすべてのパラメーターを指定します。
3. **[Event Rule Actions]** の **[Add Action]** をクリックして、イベントの通知アクションを割り当てます。
4. [ イベントアクションの追加 ] ページで、[ アクションタイプ ] ドロップダウンリストから **[アクションの抑制]** を選択し、イベントを抑制する必要がある期間を分単位で指定します。
5. **[OK]** をクリックします。

**Add Event Action**

Action Type\*

Suppress Action

Suppress time (in minutes)

10

OK Close

## イベントルールの作成

February 6, 2024

特定のイベントを監視するように規則を構成できます。規則を使用すると、インフラストラクチャ全体で生成された多数のイベントを容易に監視できます。

特定の条件で規則を構成し、規則にアクションを割り当てることで、一連のイベントにフィルターを適用できます。生成されたイベントがルール内のフィルタ条件を満たすと、そのルールに関連付けられたアクションが実行されます。フィルターを作成できる条件は、重大度、Citrix Application Delivery Controller (NetScaler ADC) インスタンス、カテゴリ、障害オブジェクト、構成コマンド、メッセージです。

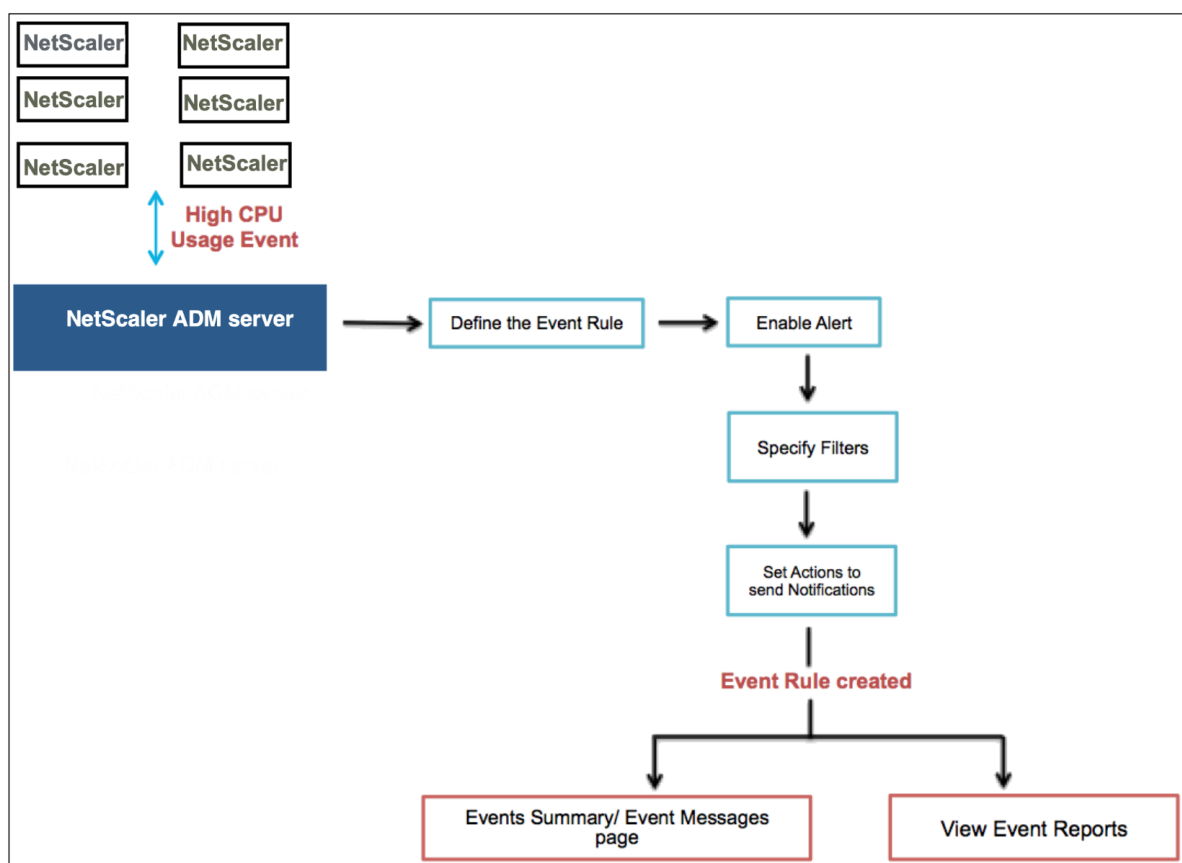
次のアクションをイベントに割り当てられます。

- メール送信アクション: フィルター条件に一致するイベントについてメールを送信します。

- トラップ送信アクション: 外部トラップ宛先に SNMP トラップを送信または転送します。
- **Run Command Action:** 受信イベントが設定されたルールを満たしたときにコマンドを実行します。
- [ジョブアクションの実行]: 指定したフィルタ条件に一致するイベントに対してジョブを実行します。
- 抑制処理: 特定の期間のイベントのドロップを抑制します。
- **Slack** 通知を送信: フィルター条件に一致するイベントについて、設定した Slack チャンネルに通知を送信します。
- **PagerDuty** 通知を送信: フィルター条件に一致するイベントの PagerDuty 設定に基づいてイベント通知を送信します。
- **ServiceNow** 通知の送信: フィルター条件に一致するイベントの ServiceNow インシデントを自動生成します。

詳細については、「イベントルールのアクションを追加する」を参照してください。

イベントが解決されるまで指定した間隔で通知が再送信されるように設定することもできます。また、特定の件名、ユーザーメッセージ、および添付ファイルを使用して電子メールをカスタマイズすることもできます。



たとえば、管理者が特定の NetScaler ADC インスタンスの「高い CPU 使用率」イベントを監視すると、NetScaler ADC インスタンスが停止する可能性があります。次の操作を実行できます：

- インスタンスを監視するルールを作成し、「高 CPU 使用率」カテゴリのイベントが発生したときに電子メール通知を送信するアクションを指定します。
- イベントが発生するたびに通知されないように、ルールを午前 11 時から午後 11 時などの特定の時刻に実行するようにスケジュールします。

イベント規則の構成では以下の作業を行います。

1. 規則を定義する
2. 規則の検出対象イベントの重要度を選択する
3. イベントのカテゴリを指定する
4. ルールを適用する NetScaler ADC インスタンスの指定
5. 障害オブジェクトの選択
6. 詳細フィルターの指定
7. 規則でイベントが検出された場合に実行するアクションを指定する

### ステップ 1-イベントルールを定義する

[ネットワーク]>[イベント]>[ルール]に移動し、[追加]をクリックします。ルールを有効にする場合は、[ルールを有効にする]チェックボックスをオンにします。

イベント経過時間オプションを設定して、NetScaler ADM がイベントルールを更新するまでの時間間隔（秒単位）を指定できます。

注:

イベント期間の最小値は 60 秒です。[ **Event Age** ] フィールドを空白のままにすると、イベントが発生した直後にイベントルールが適用されます。

上記の例に基づくと、NetScaler ADC インスタンスで「CPU 使用率が高い」イベントが 60 秒以上発生するたびに電子メールで通知を受ける必要がある場合があります。イベントの経過時間を 60 秒に設定すると、NetScaler ADC インスタンスで「CPU 使用率が高い」イベントが 60 秒以上発生するたびに、イベントの詳細が記載されたメール通知が届きます。

## ← Create Rule

Name\*

 ⓘ

Enabled

Event Age (in seconds)

Instance Family

 ▼

Enable Advanced Filter with Regex Matching ⓘ

また、イベントルールをインスタンスファミリーでフィルタリングして、NetScaler ADM がイベントを受信する NetScaler ADC インスタンスを追跡することもできます。

アスタリスク (\*) パターンマッチング以外の正規表現を含める場合は、「正規表現マッチングによる高度なフィルタを有効にする」を選択します。

### ステップ 2-イベントの重要度を選択する

デフォルトの重要度設定を使用したイベント規則を作成できます。重要度により、イベント規則に追加するイベントの現在の重要度を指定します。

重要度レベルは、Critical、Major、Minor、Warning、Clear、Information で定義できます。

▼ Severity

If none selected, all severity values will be considered

|                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |   |         |   |       |   |             |   |                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                              |       |   |          |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---|---------|---|-------|---|-------------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---|----------|---|
| <div style="border: 1px solid #ccc; padding: 5px;"> <p>Available (4) <span style="float: right;">Select All</span></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Minor</td><td style="text-align: right;">+</td></tr> <tr><td>Warning</td><td style="text-align: right;">+</td></tr> <tr><td>Clear</td><td style="text-align: right;">+</td></tr> <tr><td>Information</td><td style="text-align: right;">+</td></tr> </table> </div> | Minor | + | Warning | + | Clear | + | Information | + | <div style="border: 1px solid #ccc; padding: 2px; width: 20px; margin: 0 auto;">▶</div> <div style="border: 1px solid #ccc; padding: 2px; width: 20px; margin: 0 auto;">◀</div> | <div style="border: 1px solid #ccc; padding: 5px;"> <p>Configured (2) <span style="float: right;">Remove All</span></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Major</td><td style="text-align: right;">-</td></tr> <tr><td>Critical</td><td style="text-align: right;">-</td></tr> </table> </div> | Major | - | Critical | - |
| Minor                                                                                                                                                                                                                                                                                                                                                                                                                                                      | +     |   |         |   |       |   |             |   |                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                              |       |   |          |   |
| Warning                                                                                                                                                                                                                                                                                                                                                                                                                                                    | +     |   |         |   |       |   |             |   |                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                              |       |   |          |   |
| Clear                                                                                                                                                                                                                                                                                                                                                                                                                                                      | +     |   |         |   |       |   |             |   |                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                              |       |   |          |   |
| Information                                                                                                                                                                                                                                                                                                                                                                                                                                                | +     |   |         |   |       |   |             |   |                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                              |       |   |          |   |
| Major                                                                                                                                                                                                                                                                                                                                                                                                                                                      | -     |   |         |   |       |   |             |   |                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                              |       |   |          |   |
| Critical                                                                                                                                                                                                                                                                                                                                                                                                                                                   | -     |   |         |   |       |   |             |   |                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                              |       |   |          |   |

注

汎用イベントとアドバンス固有のイベントの両方について、重大度を設定できます。NetScaler ADM で管理されている NetScaler ADC インスタンスのイベントの重要度を変更するには、[ネットワーク] > [イベント] > [イベント設定] に移動します。イベントの重大度を設定する **カテゴリ** 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。

ステップ 3-イベントカテゴリの指定

NetScaler ADC 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 ADC インスタンスに作成されます。これらのカテゴリは、イベントルールの定義に使用できる NetScaler ADM にマッピングされます。考慮するカテゴリを選択し、「使用可能」(Available) テーブルから「構成済み」(構成済み) テーブルに移動します。

先ほどの例では、表示されるテーブルで [cpuUsageHigh] をイベントカテゴリとして選択します。

▼ Category

If none selected, all categories will be considered

Available (261)  Select All

|                         |   |
|-------------------------|---|
| devicePowerStateChanged | + |
| entityup                | + |
| appfwBufferOverflow     | + |
| appfwStartUrl           | + |
| memoryUtilizationNormal | + |

▶

◀

Configured (1)  Remove All

|              |   |
|--------------|---|
| cpuUsageHigh | - |
|--------------|---|

ステップ 4-NetScaler ADC インスタンスの指定

イベントルールを定義する NetScaler ADC インスタンスの IP アドレスを選択します。「インスタンス」セクションで、「インスタンスを選択」をクリックします。[ **Select Instances** ] ページで、インスタンスを選択し、[ **Select** ] をクリックします。

▼ Instances

If none selected, all instances be considered

Select Instances
Delete

|                                     | IP Address     | Name        | State |
|-------------------------------------|----------------|-------------|-------|
| <input checked="" type="checkbox"/> | 10.102.100.101 | SDX-2-VPX-1 | ● Up  |

## ステップ 5-障害オブジェクトの選択

表示されたリストから障害オブジェクトを選択するか、イベントが生成された障害オブジェクトを追加できます。正規表現を指定して失敗オブジェクトを追加することもできます。指定された正規表現に応じて、失敗オブジェクトは自動的にリストに追加されます。エラーオブジェクトは、イベント生成の対象となるエンティティのインスタンスまたはカウンターです。

### 重要

: 正規表現を使用して失敗オブジェクトを一覧表示するには、手順 1 で [ 正規表現による高度なフィルタを有効にする ] を選択します。

障害オブジェクトは、イベントの処理方法に影響し、通知されたとおりに正確な問題を反映します。このフィルターを使用すると、障害オブジェクトの問題をすばやく追跡し、問題の原因を特定できます。たとえば、ユーザーにログインの問題がある場合、ここでの失敗オブジェクトはユーザー名またはパスワード (`nsroot` など) です。

このリストには、すべてのしきい値関連のイベントではカウンター名、すべてのエンティティ関連のイベントではエンティティ名、証明書関連のイベントでは証明書名などが含まれます。

▼ Failure Objects

If none selected, all failure objects will be considered

Add Failure Objects

 +

| <input type="checkbox"/> | Name       |
|--------------------------|------------|
| <input type="checkbox"/> | [REDACTED] |
| <input type="checkbox"/> | [REDACTED] |

## ステップ 6-高度なフィルタを指定する

イベント規則は以下の基準によりフィルタリングできます。

- 設定コマンド - 完全な設定コマンドを指定することも、イベントをフィルタリングする正規表現を指定することもできます。

コマンドの認証ステータスや実行ステータスによってイベントルールをさらに絞り込むことができます。たとえば、`NetscalerConfigChange event` の場合は、`[.]*bind system global policy_name[.]*` と入力します。

▼ Advance Filters

Filter By  
 Configuration Command

If the Advanced Filter checkbox is enabled, enter a valid regular expression.  
 For example, for a NetscalerConfigChange event, type `[.]*bind system global policy_name[.]`  
 If the checkbox is not enabled, specify the complete configuration command, or specify the description pattern within asterisk(\*) to filter the events.  
 For example, for a NetscalerConfigChange event, type `*bind system global policy_name*`

Configuration Command  
`[.]*bind system global policy_name`

Command Authentication Status  
 Failed

Command Execution Status  
 Failed

- メッセージ-メッセージの詳細な説明を指定することも、正規表現を指定してイベントをフィルタリングすることもできます。

たとえば、`NetscalerConfigChange` イベントの場合は、`[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :^(.[.]*10.122.132.142[.]*)` と入力します。

▼ Advance Filters

Filter By  
 Message

If the Advanced Filter checkbox is enabled, enter a valid regular expression.  
 For example, for a NetscalerConfigChange event, type `[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :^(.[.]*10.122.132.142[.]*)`  
 If the checkbox is not enabled, specify the complete message description, or specify the description pattern within asterisk(\*) to filter the events.  
 For example, for a NetscalerConfigChange event, type `*ns_client_ipaddress :10.122.132.142* or !*ns_client_ipaddress :10.122.132.142*`

Message  
`[.]*ns_client_ipaddress :10.122.132.`

## ステップ 7-イベントルールアクションを追加する

イベント規則アクションを追加して、イベントに対する通知アクションを割り当てることができます。指定した通知は、上の手順で設定したフィルター条件イベントをイベントが満たした場合に送信または実行されます。追加できるイベントアクションは以下のとおりです。

- メール送信アクション
- Send Trap Action
- Run Command Action
- ジョブアクションの実行
- Suppress Action
- Slack 通知を送信



- PagerDuty 通知を送信
- サービス通知の送信

電子メールイベントルールのアクションを設定するには

**Send email Action** イベントアクションタイプを選択すると、イベントが定義されたフィルター条件を満たすと Eメールがトリガーされます。メールサーバーまたはメールプロファイルの詳細を入力してメール配布リストを作成するか、以前に作成したメール配布リストを選択する必要があります。

NetScaler ADM では多数の仮想サーバーを構成しているため、毎日多数の電子メールを受信することがあります。電子メールには、イベントの重大度、イベントのカテゴリ、および障害オブジェクトに関する情報を提供するデフォルトの件名があります。ただし、件名には、これらのイベントが発生した仮想サーバーの名前に関する情報は含まれていません。これで、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の追加情報を含めることができるようになりました。

また、カスタマイズされた件名とユーザーメッセージを追加したり、受信イベントが設定されたルールと一致した場合にメールに添付ファイルをアップロードしたりすることもできます。

イベント通知の電子メールを送信するときに、テスト電子メールを送信して、構成済みの設定をテストすることができます。「テスト」ボタンでは、メールサーバー、関連する配布リスト、その他の設定を構成した後に、テストメールを送信できるようになりました。この機能により、設定が正常に動作することが保証されます。

また、「イベントがクリアされるまで電子メール通知を繰り返す」チェックボックスをオンにして、選択した条件を満たすイベントルールについて電子メール通知を繰り返し送信することで、すべての重要なイベントに対処し、重要な電子メール通知を見逃さないようにすることもできます。たとえば、ディスクエラーを伴うインスタンスに対するイベント規則を作成し、問題が解決するまで通知するようにする場合、それらのイベントに関して連続メール送信を指定できます。

### Add Event Action

Action Type\*

Email Distribution List\*

Subject

Prefix severity, category, and failureobject information to the custom email subject ?

Attachment

Message

Repeat Email Notification until the event is cleared ?

Time Interval (minutes)\*

トラップイベントルールアクションを設定するには

[ **Send Trap Action** ] イベントアクションタイプを選択すると、SNMP トラップは外部トラップ宛先に送信または転送されます。トラップ配信リスト（またはトラップ送信先とトラッププロファイルの詳細）を定義すると、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、トラップメッセージが特定のトラップリスナーに送信されます。

[コマンドを実行] アクションを設定するには

**Run Command Action** イベントアクションを選択すると、特定のフィルター条件に一致するイベントに対して NetScaler ADM で実行できるコマンドまたはスクリプトを作成できます。

**Run Command Action** スクリプトには、次のパラメータを設定することもできます：

| パラメーター   | 説明                                    |
|----------|---------------------------------------|
| \$source | このパラメーターは、受信したイベントのソース IP アドレスに相当します。 |

|              |                                                                                                                                     |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------|
| \$category   | このパラメーターは、フィルターのカテゴリで定義したトラップのタイプに相当します。                                                                                            |
| \$entity     | このパラメーターは、イベント生成の対象となるエンティティのインスタンスまたはカウンターに相当します。このパラメーターには、しきい値関連のイベントではカウンター名、エンティティ関連のイベントではエンティティ名、すべての証明書関連のイベントでは証明書名が含まれます。 |
| \$severity   | このパラメーターは、イベントの重要度に相当します。                                                                                                           |
| \$failureobj | エラー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問題がエラーオブジェクトに反映されるようにします。このオブジェクトを使用すると、単にイベントをありのままレポートするのではなく、問題を素早く突き止めてエラーの原因を特定することができます。   |

## 注

コマンドの実行中、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、負荷分散仮想サーバーのステータスがダウンしているときに `run command` アクションを設定するとします。管理者は、別の仮想サーバーを追加して簡単な回避策を提供することを検討することをお勧めします。NetScaler ADM では、次のことができます。

- スクリプト (.sh) ファイルを記述します。

次に、サンプルスクリプト (.sh) ファイルを示します。

```

1  #!/bin/sh
2  source=$1
3  failureobj=$2
4  payload='{
5  "params":{
6  "warning":"YES" }
7  ,"lbvserver":{
8  "name":"$failureobj","servicetype":"HTTP","ipv46":"x.x.x.x","
      port":"80","td":"","m":"IP","state":"ENABLED","rhistate":"
      PASSIVE","appflowlog":"ENABLED","
9  bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":"" }
10 }
11 '
12 url="http://$source/nitro/v1/config/lbvserver"
13 curl --insecure -basic -u nsroot:nsroot -H "Content-type:
      application/json" -X POST -d $payload $url

```

```
14
15 <!--NeedCopy-->
```

- .sh ファイルを NetScaler ADM エージェントの任意の永続的な場所に保存します。例: `/var`。
- ルールの条件が満たされたときに実行する NetScaler ADM 内の .sh ファイルの場所を指定します。

新しい仮想サーバーを作成するための「コマンドの実行」アクションを設定するには、次の手順で行います。

1. 規則を定義する
2. イベントの重要度を選択してください
3. イベントカテゴリを選択してください **entitydown**
4. 仮想サーバーが設定されているインスタンスを選択します。
5. 仮想サーバーの障害オブジェクトを選択または作成します
6. 「イベントルールアクション」で、「アクションを追加」をクリックし、「\*\* アクションタイプ」リストから「コマンドアクションを実行 \*\*」を選択します。
7. 「コマンド実行リスト」で、「追加」をクリックします。

「コマンド配布リストの作成」ページが表示されます。

- a) 「プロファイル名」で、任意の名前を指定します。
- b) [コマンドの実行] で、スクリプトを実行する NetScaler ADM エージェントの場所を指定します。例:  
`/sh/var/demo.sh $source $failureobj`。
- c) [出力を追加] と [エラーを追加] を選択します

注

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（存在する場合）を **NetScaler ADM** サーバーのログファイルに保存する場合は、[Append Output] オプションと [Append Errors] 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と、NetScaler ADM はコマンドスクリプトの実行中に生成されたすべての出力とエラーを破棄します。

- d) [作成] をクリックします。
8. [イベントアクションの追加] ページで、[OK] をクリックします。

Add Event Action > Create Command Distribution List

### Create Command Distribution List

Profile Name

Run Command\*

 ⓘ  
 Append Output  
 Append Errors

OK Close

#### 注

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（存在する場合）を **NetScaler ADM** サーバのログファイルに保存する場合は、**[Append Output]** オプションと **[Append Errors]** 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と、NetScaler ADM はコマンドスクリプトの実行中に生成されたすべての出力とエラーを破棄します。

### Execute ジョブアクションを設定するには

構成ジョブを使用して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とアラームについて、NetScaler ADC、NetScaler ADC SDX、および Citrix SD-WAN WO インスタンスの組み込みジョブまたはカスタムジョブとしてジョブが実行されます。

1. [ イベントルールアクション ] で、[ アクションの追加 ] をクリックし、[ アクションタイプ ] ドロップダウンリストから [ ジョブアクションの実行 ] を選択します。
2. イベントが定義済みのフィルタ基準を満たす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。
3. ジョブの作成では、プロファイル名、インスタンスタイプ、構成テンプレート、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。
4. 選択したインスタンスタイプと選択した設定テンプレートに基づいて、変数の値を指定し、[ **Finish** ] をクリックしてジョブを作成します。

**Create Job**

Select Job Specify Variable Values

Profile Name\*  
Test ?

Instance Type\*  
Citrix ADC

Configuration Template Name\*  
DeployMasterConfiguration

On Command Failure\*  
Ignore error and continue

Cancel Next →

抑制アクションを設定するには

**Suppress Action** イベントアクションを選択すると、イベントが抑制またはドロップされる期間を分単位で設定できます。最短で 1 分間イベントを非表示にできます。

**Add Event Action**

Action Type\*  
Suppress Action

Suppress time (in minutes)  
10

OK Close

NetScaler ADM から **Slack** 通知を設定するには

NetScaler ADM GUI でプロファイル名と Webhook URL を指定して、必要な Slack チャンネルを構成します。イベント通知はこのチャンネルに送信されます。複数の Slack チャンネルを設定して、これらの通知を受け取ることができます。

1. Citrix ADM で、[ネットワーク] > [イベント] > [ルール] に移動し、[追加] をクリックしてルールを作成します。
2. 「ルールの作成」ページで、重要度やカテゴリなどのルールパラメータを設定します。監視が必要なインスタンスと障害オブジェクトを選択します。
3. 「イベントルールアクション」で、「アクションを追加」をクリックします。次に、「アクションタイプ」リストから「**Slack** 通知を送信」を選択し、「**Slack** プロフィールリスト」を選択します。

4. Slack プロファイルリスト欄の横にある「追加」をクリックして、**Slack** プロファイルリストを追加することもできます。
5. 次のパラメータを入力してプロファイルリストを作成します。
  - a) プロファイル名。NetScaler ADM で構成するプロファイルリストの名前を入力します。
  - b) チャンネル名。イベント通知の送信先となる Slack チャンネルの名前を入力します。
  - c) ウェブフック **URL**。先に入力したチャンネルのウェブフック URL を入力します。受信ウェブフックは、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 は内部的にチャンネル名にリンクされ、イベント通知はすべてこの URL に送信され、指定された Slack チャンネルに投稿されます。ウェブフックの例は次のとおりです。[https://hooks.slack.com/services/T0\\*\\*\\*\\*\\*E/B9X55DU MQ/c4tewWAIgVTT51Fl6oEOVirK](https://hooks.slack.com/services/T0*****E/B9X55DU MQ/c4tewWAIgVTT51Fl6oEOVirK)
6. [**Create**] をクリックし、[ **Add Event Action** ] ウィンドウで [**OK**] をクリックします。

注:

「システム」>「通知」>「Slack プロフィール」に移動して **Slack** プロフィールを追加することもできます。[追加] をクリックし、前のセクションの説明に従ってプロファイルを作成します。

作成した Slack プロフィールのステータスを表示できます。

これで、適切なフィルターが設定され、適切なイベント規則アクションが定義されたイベント規則が作成されました。

### NetScaler ADM から PagerDuty 通知を設定するには

NetScaler ADM オプションとして PagerDuty プロファイルを追加して、PagerDuty 構成に基づいてインシデント通知を監視できます。PagerDuty では、電子メール、SMS、プッシュ通知、登録番号への電話による通知を設定できます。

NetScaler ADM で PagerDuty プロファイルを追加する前に、PagerDuty で必要な構成が完了していることを確認します。詳細については、[PagerDuty のドキュメントを参照してください](#)。

PagerDuty プロファイルをオプションの 1 つとして選択して、次の機能に関する通知を受け取ることができます。

- イベント—NetScaler ADC インスタンスに対して生成されるイベントのリスト。
- [**Licenses**]: 現在アクティブで、間もなく期限切れになるなどのライセンスのリスト。
- **SSL** 証明書—NetScaler ADC インスタンスに追加される SSL 証明書のリスト。

### ADM に PagerDuty プロファイルを追加するには:

1. 管理者の資格情報を使用して NetScaler ADM にログインします。
2. [システム]>[通知]>[ **PagerDuty** プロファイル] に移動します。

3. [追加] をクリックして、新しいプロファイルを作成します。
4. 「ページデューティプロファイルの作成」 ページで、次の操作を行います。
  - a) 任意のプロファイル名を入力します。
  - b) 統合キーを入力します。  
インテグレーションキーは PagerDuty ポータルから取得できます。
  - c) [作成] をクリックします。

ユースケース:

次のようなシナリオを考えてみましょう。

- PagerDuty プロフィールに通知を送信したい。
- PagerDuty で通知を受信するオプションとして電話を設定しました。
- NetScaler ADC イベントの電話アラートを受け取りたい。

構成するには、以下を実行します:

- a) [ イベント ] > [ ルール ] に移動します
- b) 「規則の作成」 ページで、規則を作成するための他のすべてのパラメータを設定します。
- c) 「ルールアクションの作成」 で、「アクションを追加」 をクリックします。  
「イベントアクションの追加」 ページが表示されます。
  - i. [ アクションタイプ ] で、[ **PagerDuty** 通知を送信 ] を選択します。
  - ii. PagerDuty プロファイルを選択し、[ **OK** ] をクリックします。

構成が完了すると、NetScaler ADC インスタンスに対して新しいイベントが生成されるたびに、電話が送信されます。電話から、次のことを決定できます。

- イベントを確認する
- 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ション

### NetScaler ADM から ServiceNow インシデントを自動生成するには

NetScaler ADM GUI で ServiceNow プロファイルを選択すると、NetScaler ADM イベントの ServiceNow インシデントを自動生成できます。イベントルールを構成するには、Citrix ADM で ServiceNow プロファイルを選択する必要があります。



ServiceNow インシデントを自動生成するようにイベントルールを構成する前に、NetScaler ADM と ServiceNow インスタンスを統合します。詳細については、「[ServiceNow 用に ITSM アダプタを構成する](#)」を参照してください。

イベントルールを設定するには、[イベント] > [\*\* ルール] に移動します。 \*\*

1. 「規則の作成」 ページで、規則を作成するための他のすべてのパラメータを設定します。

2. 「ルールアクションの作成」 で、「アクションを追加」 をクリックします。

「イベントアクションの追加」 ページが表示されます。

a) アクションタイプで、「**ServiceNow** 通知を送信」 を選択します。

b) **ServiceNow** プロファイルで、リストから **Citrix\_Workspace\_SN** プロファイルを選択します。

c) [OK] をクリックします。

## NetScaler ADC 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

February 6, 2024

すべてのデバイスで生成されたイベントのレポート機能を管理できます。これにより、特定のインスタンスの特定のイベントに関するイベント詳細を確認したり、イベントの重要度に基づいてレポートを表示したりできます。デフォルトの重要度設定を使用したイベント規則を作成できます。また、重要度設定を変更できます。汎用イベントとエンタープライズ固有のイベント双方に対して、重要度を構成できます。

重要度レベルは、Critical、Major、Minor、Warning、Clear で定義できます。

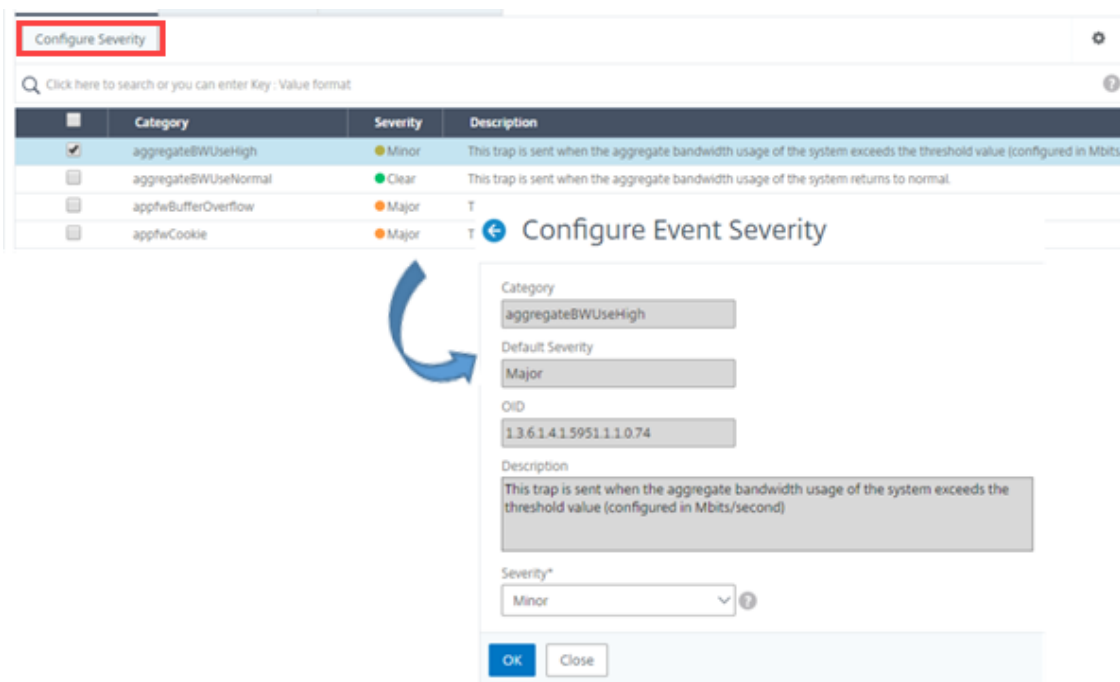
イベントの重大度を変更するには、次の手順に従います。

1. [ネットワーク] > [イベント] > [イベント設定] に移動します。

2. 変更する Citrix Application Delivery Controller (ADC) インスタンスタイプのタブをクリックします。次に、リストからカテゴリを選択し、[重要度の設定] をクリックします。

3. [Configure Event Severity] でボックスの一覧から重要度レベルを選択します。

4. [OK] をクリックします。



## イベントの概要の表示

February 6, 2024

[イベントの概要] ページを表示して、NetScaler Application Delivery Management (ADM) サーバーで受信したイベントとトラップを監視できるようになりました。[ネットワーク] > [イベント] に移動します。[Events Summary] ページには、以下の情報が表形式で表示されます。

- **NetScaler ADM** が受信したすべてのイベントの概要。イベントはカテゴリ別にリスト表示され、各列にそれぞれの重要度 (Critical、Major、Minor、Warning、Clear、Information) が表示されます。たとえば、Citrix Application Delivery Controller (ADC) インスタンスがダウンし、NetScaler ADM サーバーへの情報の送信を停止すると、クリティカルなイベントが発生します。イベント中は、インスタンスがダウンした理由、インスタンスがダウンしていた時間などを説明する通知が管理者に送信されます。イベントは [Events Summary] ページに記録され、このページでイベントの概要を確認し詳細にアクセスできます。

Event Summary 🔄 📄

| Critical              | Major    | Minor | Warning | Clear   | Information |             |
|-----------------------|----------|-------|---------|---------|-------------|-------------|
| 1                     | 20       | 6     | 0       | 3       | 0           |             |
| Category              | Critical | Major | Minor   | Warning | Clear       | Information |
| coldstart             | 0        | 2     | 0       | 0       | 0           | 0           |
| entitydown            | 0        | 6     | 0       | 0       | 0           | 0           |
| entityup              | 0        | 0     | 0       | 0       | 3           | 0           |
| HABadSecState         | 1        | 0     | 0       | 0       | 0           | 0           |
| netScalerLoginFailure | 0        | 2     | 0       | 0       | 0           | 0           |
| warmRestartEvent      | 0        | 1     | 0       | 0       | 0           | 0           |
| netScalerConfigChange | 0        | 0     | 3       | 0       | 0           | 0           |
| ipConflict            | 0        | 6     | 0       | 0       | 0           | 0           |
| snmpAuthentication    | 0        | 2     | 0       | 0       | 0           | 0           |
| changeToPrimary       | 0        | 1     | 0       | 0       | 0           | 0           |
| netScalerConfigSave   | 0        | 0     | 3       | 0       | 0           | 0           |

- 各カテゴリに対して受信されたトラップの数。重要度で分類された受信済みのトラップの数。デフォルトでは、NetScaler ADC インスタンスから NetScaler ADM に送信される各トラップには重大度が割り当てられていますが、ネットワーク管理者は NetScaler ADM GUI で重要度を指定できます。

カテゴリタイプまたはトラップをクリックすると、[

**Events**] ページが表示され、[Category] や [Severity] などのフィルタが事前を選択されます。このページには、NetScaler ADC インスタンスの IP アドレスとホスト名、トラップを受信した日付、カテゴリ、障害オブジェクト、構成コマンドの実行、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。

Events 🔄 📄

Details History Delete Clear ⚙️

🔍 Category: coldstart Click here to search or you can enter Key: Value format ?

| Severity | Source        | Host Name     | Date                 | Category  | Failure Objects | Configuration Command | Message      |
|----------|---------------|---------------|----------------------|-----------|-----------------|-----------------------|--------------|
| Major    | 10.102.71.220 | abcd          | Nov 25 2018 21:03:12 | coldstart | 10.102.71.220   |                       | enterprise_c |
| Major    | 10.102.186.95 | DataCenter-CB | Oct 27 2018 05:14:13 | coldstart | 10.102.186.95   |                       | enterprise_c |

## イベントの重大度と SNMP トラップの詳細を表示します

February 6, 2024

Citrix Application Delivery Management (ADM) でイベントとその設定を作成すると、そのイベントは [イベントの概要] ページにすぐに表示されます。同様に、Citrix ADM サーバーに追加されたすべての Citrix Application Delivery Controller (ADC) インスタンスの状態、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。

Infrastructure ダッシュボードでは、無関係な値をマスクして、重要度、正常性、稼働時間、モデル、NetScaler ADC インスタンスのバージョンなどの情報をより簡単に表示および監視できるようになりました。

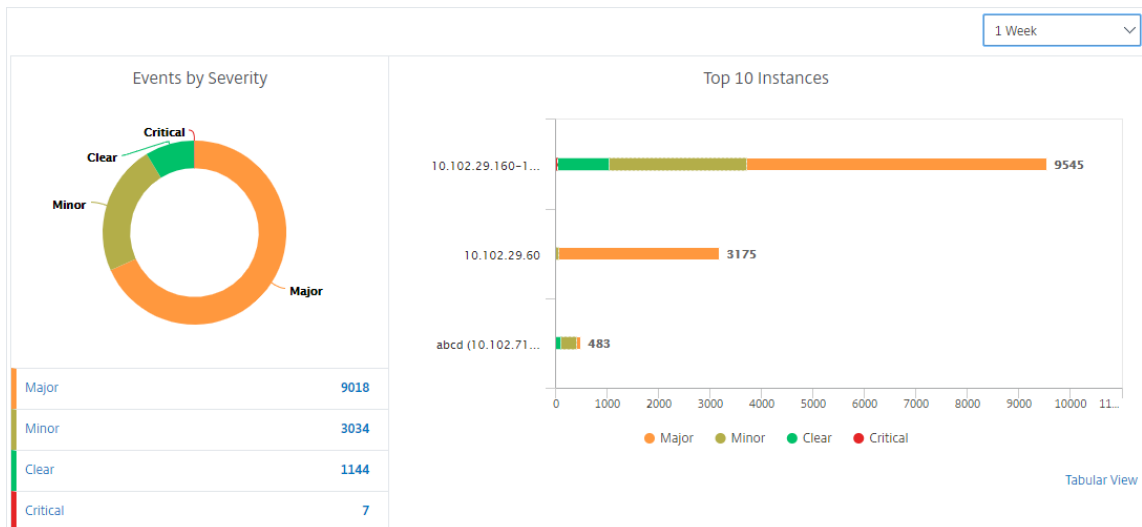
たとえば、重要度レベルが「緊急」のイベントはまれにしか発生しない場合があります。しかしながら、ネットワー

上でこれらの重大イベントが実際に発生した場合は、そのイベントが発生した場所と時間をさらに調査、トラブルシューティング、監視できます。Critical 以外のすべての重要度レベルを選択すると、グラフに重大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 bared events** ] ページが表示されます。このページには、選択した期間におけるクリティカルイベントの発生時期に関するすべての詳細（インスタンスのソース、日付、カテゴリ、およびクリティカル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、Citrix VPX インスタンスの正常性をダッシュボードに表示できます。インスタンスが稼働していた時間をマスクし、インスタンスが稼働停止してい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が表示され、サービス外 フィルタが既に適用され、ホスト名、1 秒あたりに受信した HTTP リクエストの数、CPU 使用率などの詳細が表示されます。インスタンスを選択し、特定の Citrix インスタンスのダッシュボードで詳細を確認することもできます。

**NetScaler ADM** で特定のイベントを重要度別に選択するには：

1. 管理者の資格情報を使用して NetScaler ADM にログオンします。
2. [ ネットワーク ] > [ ダッシュボード ] に移動します。  
 または  
 [ ネットワーク ] > [ イベント ] > [ レポート ] に移動します。
3. ページの右上隅のメニューから、重大度別にイベントを表示する期間を選択します。

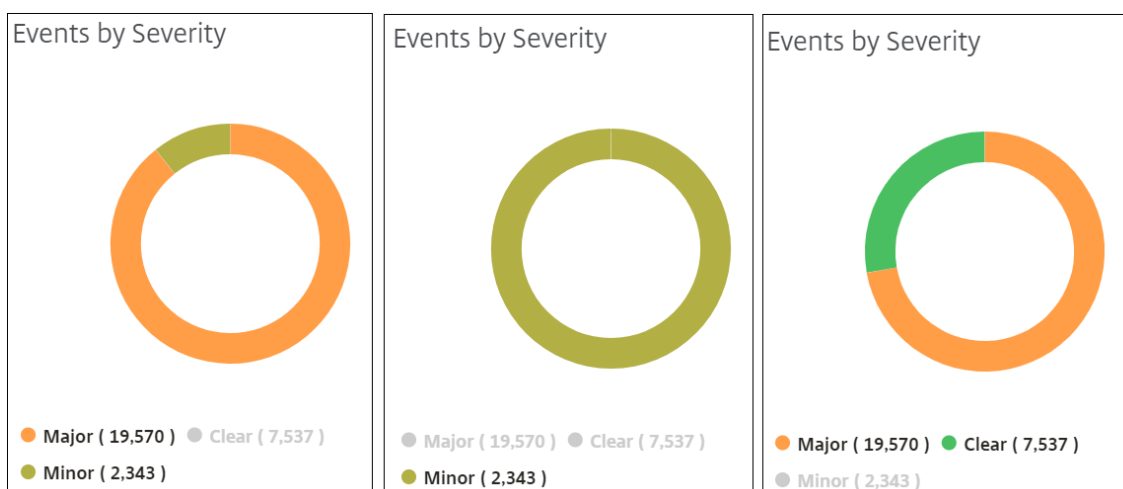


4. [ **Events by Severity** ] ドーナツグラフには、すべてのイベントが重要度別に視覚的に表示されます。異なる種類のイベントは異なる色が付いたセクションとして表され、各セクションの長さは、その種類の重要度の合計イベント数に対応しています。
5. ドーナツグラフの各セクションをクリックすると、対応する「重大度ベースのイベント」ページが表示されます。このページには、選択した期間における選択した重要度に関する次の詳細が表示されます。
  - インスタンスのソース
  - イベントの日付

- NetScaler ADC インスタンスによって生成されるイベントのカテゴリ
- 送信されたメッセージ通知

注

ドーナツグラフの下には、チャートに表示されている重大度のリストが表示されます。デフォルトでは、ドーナツグラフには、すべての重要度タイプのすべてのイベントが表示されます。そのため、一覧内のすべての重要度タイプが強調表示されます。選択した重要度をより簡単に表示して監視するには、重要度タイプを切り替えます。



**NetScaler ADM** で **NetScaler ADC SNMP** トラップの詳細を表示するには：

管理対象の NetScaler ADC インスタンスから受信した各 SNMP トラップの詳細を、[イベント設定] ページで NetScaler ADM サーバーに表示できるようになりました。[ネットワーク]>[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は、タブ形式で次の詳細を表示できます。

- **Category** : 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。
- **重大度** : イベントの重大度は、色とその重大度タイプで示されます。
- **説明** : イベントに関連付けられたメッセージを指定します。

たとえば、トラップカテゴリが **MonRespTimeoutBelowThresh** のイベントの場合、トラップの説明は「モニタープローブの応答タイムアウトが、設定されたしきい値を下回って正常に戻ったときに送信されます」と表示されます。

## NetScaler ADC Syslog メッセージの表示とエクスポート

February 6, 2024

ADM ソフトウェアから、Citrix アプリケーション Delivery Controller (ADC) インスタンスで生成された syslog イベントを監視できます。そのためには、NetScaler ADC インスタンスの syslog サーバーとして ADM を構成する必要があります。ADM を設定すると、すべての syslog メッセージが ADC インスタンスから ADM にリダイレクトされます。

## ADM を Syslog サーバとして設定する

ADM を syslog サーバとして設定するには、次の手順を実行します。

1. ADM GUI から、[ネットワーク] > [インスタンス] に移動します。
2. Syslog メッセージを収集して NetScaler ADM に表示する NetScaler ADC インスタンスを選択します。
3. 「アクションの選択」リストで、「**Syslog** の設定」を選択します。
4. [有効にする] をクリックします。
5. ファシリティ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。

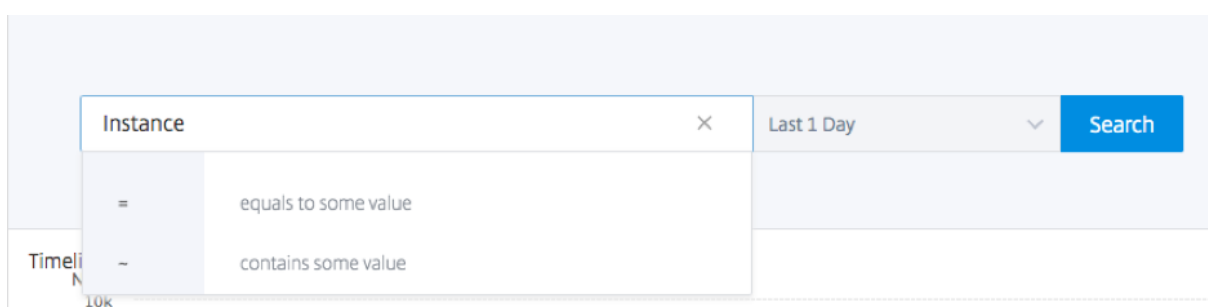
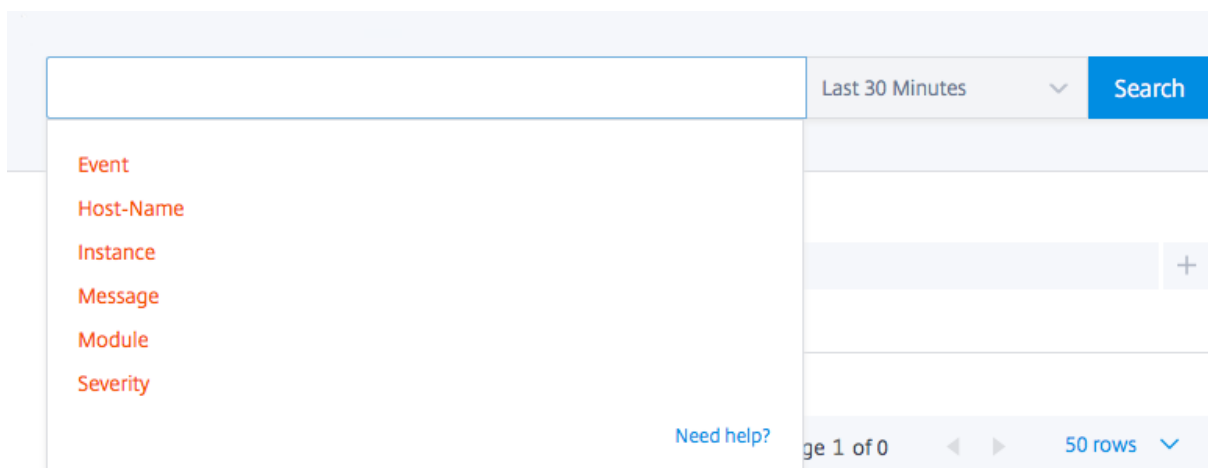
The screenshot shows a configuration dialog box for Syslog. It includes a 'Source Instance' dropdown menu, an 'Enable' checkbox, a 'Facility\*' dropdown menu set to 'LOCAL0', and a 'Choose Log Level' section with radio buttons for 'All', 'None' (selected), and 'Custom'. Below this are checkboxes for various log levels: Alert, Critical, Debug, Emergency, Error, Informational, Notice, and Warning. A note at the bottom states: 'Selecting Debug, Informational, Notice or Warning log-levels will effect storage and performance of ADM'. At the bottom of the dialog are 'OK' and 'Close' buttons.

以下の手順では、NetScaler ADC インスタンス内のすべての syslog コマンドを構成し、NetScaler ADM が syslog メッセージの受信を開始します。

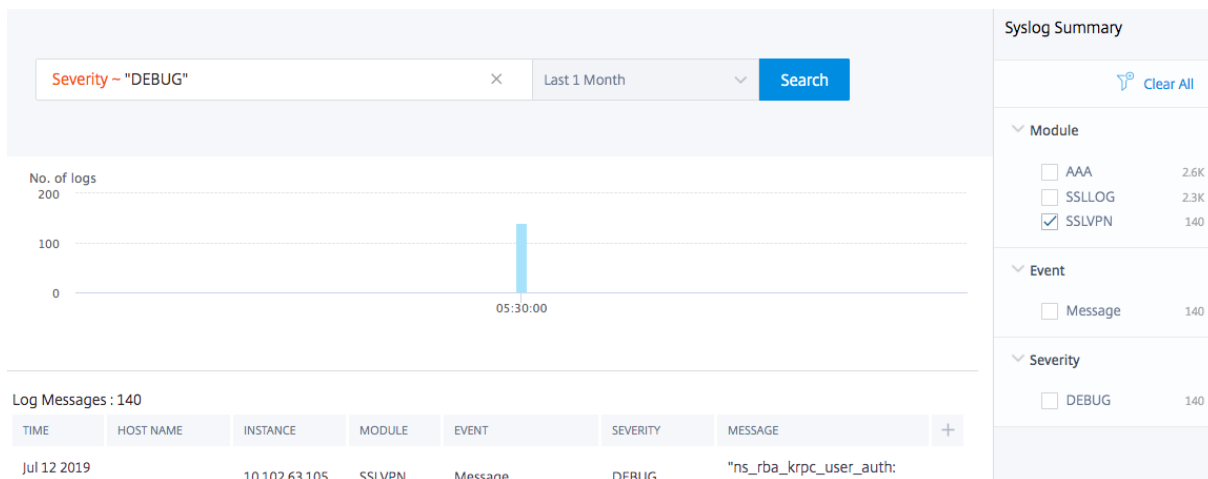
## syslog メッセージの表示と検索

管理対象 NetScaler ADC インスタンスで生成されたすべての syslog メッセージを表示できます。Syslog メッセージは、データベースの中央に格納され、監査目的で [ネットワーク] > [イベント] > [Syslog メッセージ] の下に表示されます。このログ情報を組み合わせて、収集されたデータから分析用のレポートを生成できます。

さらに、フィルタを使用して syslog メッセージの検索結果を絞り込み、探しているものをリアルタイムで正確に見つけることができます。[ヘルプが必要ですか?] をクリックします。をクリックして、組み込みの検索ヘルプを開きます。



次に、検索語を追加します。一部のカテゴリでは、事前に入力された検索語のリストが表示されます。デフォルトでは、検索時間は 1 日です。下向き矢印をクリックすると、時刻と日付の範囲を変更できます。[ **Syslog Summary** ] ペインからオプションを選択して、検索をさらに絞り込むことができます。

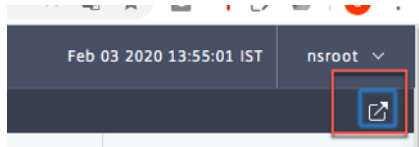


### syslog メッセージのエクスポートとスケジュール設定

サーバ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リングすることで、ADM にログインせずに syslog メッセージを表示できます。ADC インスタンスで生成された syslog メッセージを PDF、CSV、PNG、お

よび JPEG 形式でエクスポートできます。指定したメールアドレスまたは Slack アカウントへのレポートのエクスポートをさまざまな間隔でスケジュールできます。

ログメッセージをエクスポートしてスケジュールするには、右上隅にある矢印アイコンをクリックします。



- ログメッセージをエクスポートするには、[レポートのエクスポート] > [今すぐエクスポート] をクリックし、必要な形式を選択して [エクスポート] をクリックします。
- syslog メッセージのエクスポートをスケジュールするには、[レポートのエクスポート] > [レポートのスケジュール] をクリックし、必要なパラメータを設定します。レポートはメールまたは Slack で受信できます。

### Schedule Export

appflow.export\_now\_message

Subject\*

Select export option

Tabular

Select the export file format

PDF  CSV

Recurrence\*

Description

NOTE: Enter the schedule time in your selected timezone

Export Time\*

How many data records do you want to export?\*

Email

Slack

**Schedule**



## syslog メッセージの抑制

February 6, 2024

Syslog サーバーとして構成すると、CitrixApplication Delivery Management (ADM) は、構成済みの Citrix アプリケーション Delivery Controller (ADC) インスタンスから送信されたすべての syslog メッセージを受信します。表示する必要のないメッセージの数が大量になる場合もあります。たとえば、情報レベルのすべてのメッセージを表示する必要がない場合があります。必要のない一部の syslog メッセージ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 ADM に届く Syslog メッセージの一部を抑制できます。Citrix ADM は、条件に一致するすべてのメッセージをドロップします。これらのドロップされたメッセージは NetScaler ADM GUI には表示されません。また、これらのメッセージはお客様の NetScaler ADM 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 ADM に届くログに記録された Syslog メッセージの一部を抑制できます。syslog メッセージを非表示にするために使用できる 2 つのフィルターは、重要度とファシリティです。特定の NetScaler ADC インスタンスまたは複数のインスタンスからのメッセージを抑制することもできます。また、NetScaler ADM でメッセージを検索および非表示にするテキストパターンを指定することもできます。Citrix ADM は、条件に一致するすべてのメッセージをドロップします。これらのドロップされたメッセージは NetScaler ADM GUI には表示されません。また、これらのメッセージは顧客データベースにも保存されません。それにより、ストレージサーバー上のかなりの領域が節約されます。

syslog メッセージを非表示にするためのいくつかのユースケースを次に示します。

- 情報レベルのすべてのメッセージを無視する場合は、レベル 6 (情報) を非表示にします。
- ファイアウォールのエラー条件のみを記録する場合は、レベル 3 (エラー) 以外のすべてのレベルを非表示にします。

### フィルタの作成による **syslog** メッセージの抑制

1. Citrix ADM で、[ネットワーク] > [イベント] > [**Syslog** メッセージ] > [フィルターの抑制] に移動します。
2. 「抑制フィルタの作成」 ページで、次の情報を更新します。

- a) 名前-フィルタの名前を入力します。

注:

ユーザーごとに複数の NetScaler ADC インスタンスに異なるアクセス権がある場合、ユーザーにはすべてのインスタンスにアクセスできるフィルターのみが表示されるため、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) 重要度-メッセージを非表示に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、受信した情報メッセージを表示する必要がない場合は、[Informational] を選択してそれらのメッセージを非表示にします。

- c) インスタンス -syslog メッセージが構成されている NetScaler ADC インスタンスを選択します。

## ← Create Suppress Filter

Application Delivery Management filters and discards the logs that match the filter criteria that you specify.

Name\*  
 ?

Enable Filter

▼ Severity

**Available (8)** Select All

|           |   |
|-----------|---|
| Alert     | + |
| Critical  | + |
| Debug     | + |
| Emergency | + |
| Error     | + |

▶

◀

**Configured (0)** Remove All

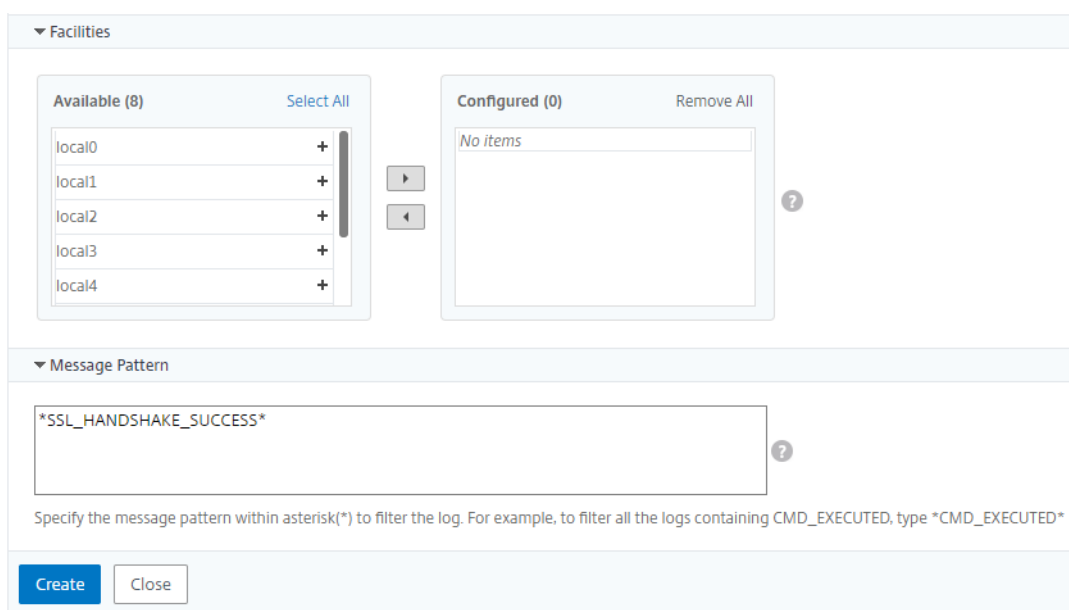
No items

▼ Instances

If none selected, all instances be considered

|                                     | IP Address   | Host Name |
|-------------------------------------|--------------|-----------|
| <input checked="" type="checkbox"/> | 10.102.29.60 | --        |

- 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、メッセージを非表示にすることもできます。メッセージに対してテキストパターン文字列が検索され、このパターンが含まれているメッセージが非表示になります。



## フィルターの無効化

NetScaler ADM でメッセージを表示できるようにするには、フィルタを無効にする必要があります。

1. [ ネットワーク ] > [ イベント ] > [ **Syslog** メッセージ ] > [ フィルタの抑制 ] に移動し、[ フィルタの抑制 ] ページでフィルタを選択して [ 編集 ] をクリックします。
2. [ 抑制フィルタの構成 ] ページで、[ フィルタの有効化 ] チェックボックスをオフにしてフィルタを無効にします。

## インスタンスイベントのプルーニング設定の構成

February 6, 2024

Citrix Application Delivery Management (ADM) サーバーによって管理される Citrix アプリケーション Delivery Controller (ADC) インスタンスは、イベントメッセージデータを継続的に送信して Citrix ADM に保存します。NetScaler ADM でネットワークレポートデータ、イベント、監査ログ、タスクログを保持する間隔を指定できます。デフォルトでは、これらのデータは 24 時間ごとに (00:00 の時刻に) 削除されます。

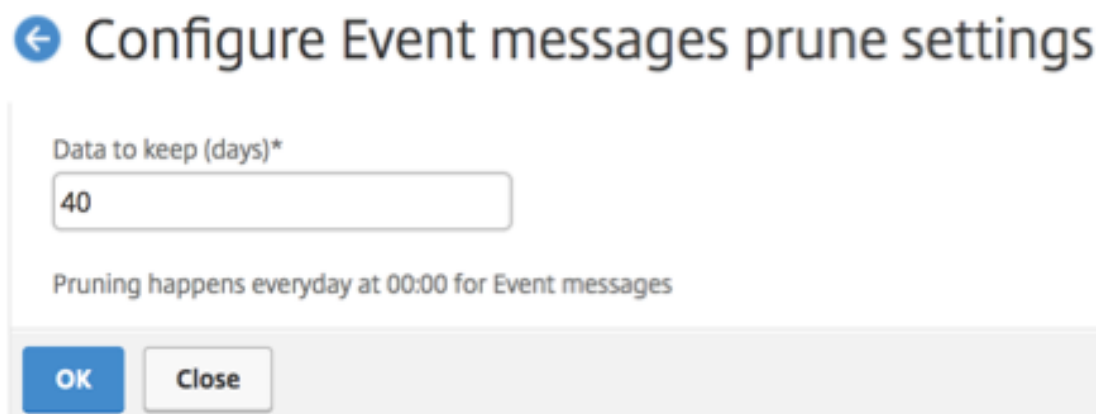
### 注

指定できる値は 40 日を超えることも、1 日未満にすることもできません。

インスタンスイベントのプルーニング設定を構成するには:

1. [ システム ] > [ システム管理 ] に移動します。

2. 「ブルーニング設定」で、「インスタンスイベント」>「ブルーニング設定」をクリックします。
  3. NetScaler ADM サーバーでデータを保持する間隔を日単位で入力し、[OK] をクリックします。
- 



## SSL 証明書の管理

February 6, 2024

機密情報または機密情報の処理を必要とする組織または個々の Web サイトには、SSL 証明書が必要です。Web サーバー上の SSL 証明書は、接続しているクライアントに対する Web サーバーの信頼性を保証するのに役立ちます。これは、ウェブサイトのアイデンティティを認証するだけでなく、セッション全体の暗号化のために後で使用されるセッションキーを生成するのに役立ちます。

SSL トランザクションの一部であるセキュアソケットレイヤー (SSL) 証明書は、企業 (ドメイン) または個人を識別するデジタルデータフォーム (X509) です。この証明書には、サーバーとの安全なトランザクションを開始しようとするすべてのクライアントが確認できる公開キーコンポーネントが含まれます。対応する秘密キーは、Citrix Application Delivery Controller (ADC) アプライアンスに安全に配置され、非対称キー (または公開キー) の暗号化と復号化を完了するために使用されます。

NetScaler Application Delivery Management (ADM) は、SSL 証明書のインストール、更新、削除、リンク、ダウンロードを自動化するための統合コンソールを提供します。これは、ウェブサイトや顧客の信頼の評判を維持するのに役立ちます。NetScaler ADM では、証明書管理のあらゆる側面が合理化されるようになりました。統合コンソールを使用して、組織の IT ポリシーに従って、推奨される発行者、キー強度、プロトコル、およびアルゴリズムを確実にするための自動化されたポリシーを構成できます。そうすることで、未使用の証明書や有効期限が近い証明書について監視し続けることができます。

SSL 証明書およびキーは、次のいずれかの方法で入手できます。

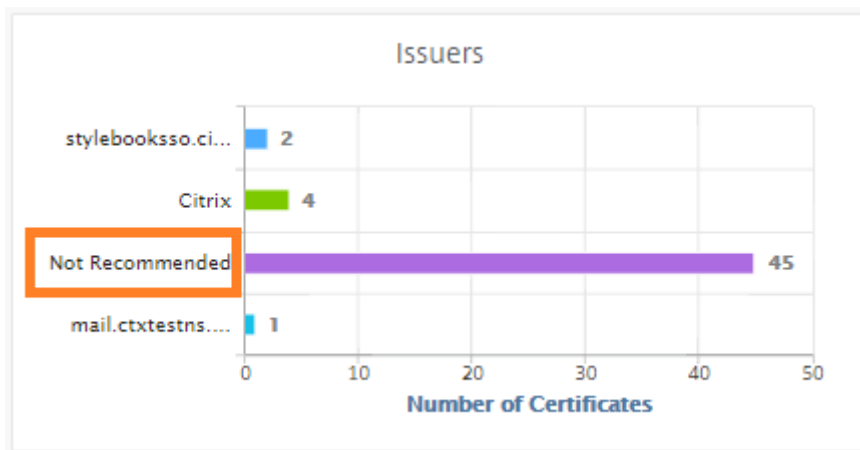
- Verisign などの承認された認証局 (CA) から
- NetScaler ADC アプライアンスで新しい SSL 証明書とキーを生成する

## エンタープライズ **SSL** ポリシー設定

すべての企業には独自の SSL ポリシーがあり、すべての SSL 証明書が遵守する必要がある要件を定義します。セキュリティは、すべての企業ユーザーにとって常に最優先事項の 1 つであり、したがって、SSL 設定は重要な役割を果たしています。

たとえば、ABC Company では、すべての証明書の最小キー強度が 2,048 ビット以上であることが義務付けられています。証明書は、信頼された CA または発行者によって承認されている必要があります。管理者は、証明書が会社のポリシーに準拠していることを確認するために、このようなすべての SSL パラメータをチェックする必要があります。各証明書を手動で検証するのは面倒な作業です。このシナリオを克服するために、NetScaler ADM はエンタープライズ SSL ポリシー設定を構成し、「推奨しない」タグが付いた非準拠証明書を表示します。

SSL ダッシュボードで、非対応 (非推奨) 証明書の概要を表示できます。



### 注

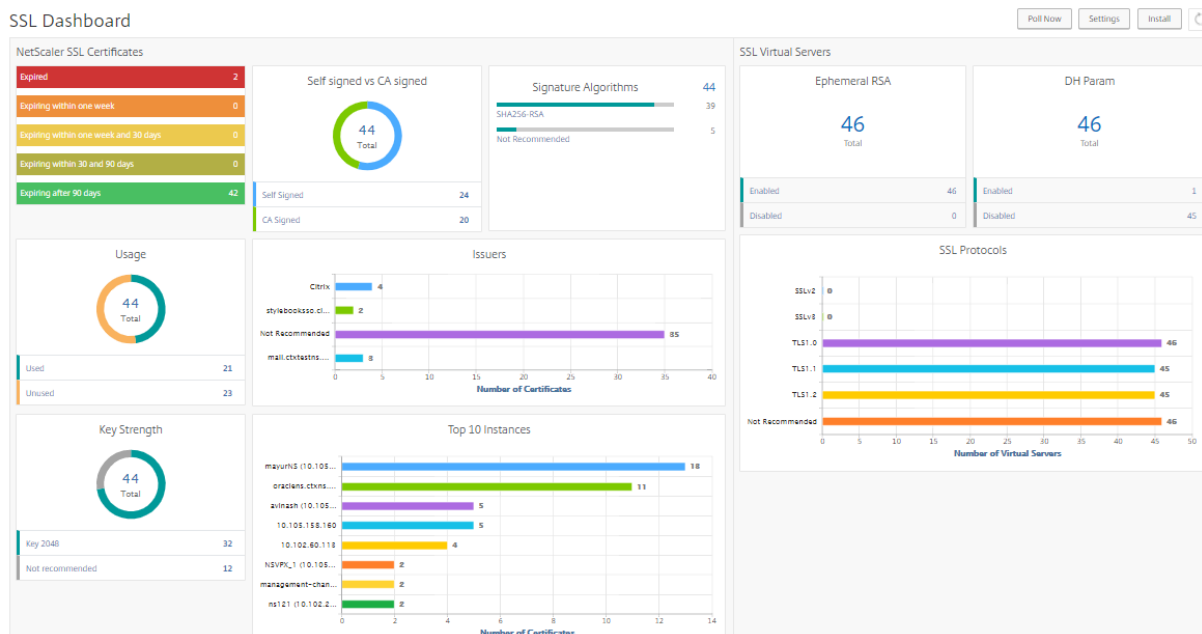
「推奨しない」証明書は、さまざまなパラメータに基づいて分類され、関連するコンポーネントで表示できます。

## NetScaler ADM 証明書の仕組み

SSL ダッシュボードでは、異なる NetScaler ADC インスタンスにインストールされているすべての SSL 証明書が視覚的に表示されます。SSL ダッシュボードには、NetScaler ADC インスタンスにインストールされている各証明書について、次の情報が表示されます。これは、以下に基づいて分類されます。

- 自己署名対 **CA** 署名付き。自己署名と CA 署名付きのセクションでは、証明書を自己署名証明書と CA 署名証明書に分離できます。
- 署名アルゴリズム。このセクションでは、暗号化に使用される署名アルゴリズムに基づいて SSL 証明書を分離します。
- 使用法。このセクションでは、使用済み証明書と未使用の証明書に基づいて SSL 証明書を分離します。未使用の証明書は、仮想サーバーにバインドされない可能性があるため、特別な注意が必要です。
- 発行者。このセクションでは、証明書の発行者に基づいて SSL 証明書を分離します。

- **[キーの強度]**。このセクションでは、秘密キーのキー強度に基づいて SSL 証明書を分離します。
- **上位 10 インスタンス**。このセクションでは、インストールされている SSL 証明書の数に基づいて、上位 10 個の NetScaler ADC インスタンスの詳細について説明します。



## SSL 証明書管理のユースケース

次のユースケースでは、SSL 証明書を使用して複数の NetScaler ADC インスタンス間で証明書を管理および監視する方法について説明します。

### SSL 証明書をインストールする

たとえば、複数の NetScaler ADC インスタンスがあり、その上に必要な SSL 証明書を展開する必要があります。NetScaler ADM は、複数の NetScaler ADC インスタンスに SSL 証明書を 1 回の試行で展開するための統合コンソールを提供します。

たとえば、1 つ以上の NetScaler ADC インスタンスに SSL 証明書をインストールするとします。この方法では、各 NetScaler ADC インスタンスへの SSL 証明書のインストールの手動介入を最小限に抑えることができます。1 つ以上の NetScaler ADC インスタンス間で SSL 証明書の一括インストールを実行できます。

SSL 証明書の概要を取得するには、**NetScaler ADM** にログオンし、[ネットワーク] > [SSL ダッシュボード] に移動します。

### 証明書の有効期限の通知設定

このユースケースでは、複数の NetScaler ADC インスタンスに複数の証明書が存在する可能性があり、各証明書の有効期限を追跡するオーバーヘッドになります。各証明書を手動で追跡し、有効期限が切れる前に更新するのは面倒な作業です。このようなシナリオを回避するには、構成済みの電子メール、ポケットベル、Slack、または ServiceNow プロファイルに通知またはアラートを送信するように NetScaler ADM を構成できます。この方法では、証明書の有効期限を遅らし、有効期限の前に証明書を更新することができます。

たとえば、有効期限が近づいている証明書を追跡するのを忘れることがあります。また、証明書の有効期限が切れると、サービスの停止が発生するため、多くのアプリケーションがユーザーに影響を及ぼす可能性があります。ADM 証明書の有効期限通知設定を使用すると、このような予期しないシナリオを回避できます。

**SSL** ダッシュボードで概要を表示し、有効期限が近づいている証明書を追跡できます。

任意の期間で期限切れになる証明書のレポートを表示するには、タイトルをクリックすると、そのウィンドウで期限切れになる証明書の詳細を確認できます。

| <input type="checkbox"/> | Certificate Name | Instance | Host Name          | Days To Expiry | Status | Domain       |
|--------------------------|------------------|----------|--------------------|----------------|--------|--------------|
| <input type="checkbox"/> | authcertvsrver   | ns100    | oradlens.ctxns.net | 59 days        | Valid  | 10.10.10.100 |

### 証明書の更新

これで、NetScaler ADM から証明書を更新できます。既存の証明書を更新するか、次の内容に基づいて証明書を作成できます。

**既存の証明書を更新する** このユースケースでは、認証局 (CA) から更新された証明書を受け取ったら、既存の証明書を更新する必要があります。NetScaler ADC インスタンスにログインすることなく、NetScaler ADM から既存の証明書を更新できるようになりました。

たとえば、既存の証明書にいくつかの変更や変更がある可能性があります。CA は、更新された証明書を発行します。NetScaler ADC アプライアンスに移動する代わりに、NetScaler ADM から SSL 証明書を更新できるようになりました。

証明書を更新するには、NetScaler ADM にログオンし、[ネットワーク] > [SSL ダッシュボード] に移動します。

更新する証明書を選択し、[更新] をクリックします。

NetScaler ADM から選択した証明書の関連フィールドを更新するオプションがあります。

## ← Update SSL Certificate

|                                             |                                                                       |
|---------------------------------------------|-----------------------------------------------------------------------|
| IP Address                                  | <input type="text"/>                                                  |
| Certificate Name                            | <input type="text" value="http2Cert"/>                                |
| Certificate File*                           | <input type="text" value="Choose File"/> /nsconfig/ssl/http2Cert.cert |
| Key File                                    | <input type="text" value="Choose File"/> /nsconfig/ssl/http2Cert.key  |
| Certificate Format*                         | <input type="text" value="PEM"/>                                      |
| Password                                    | <input type="text"/>                                                  |
| <input type="checkbox"/> Save Configuration |                                                                       |
| <input type="checkbox"/> No Domain Check    |                                                                       |
| <input type="button" value="OK"/>           | <input type="button" value="Close"/>                                  |

証明書署名要求の作成 SSL 証明書の 1 つが組織のポリシーに準拠していないユースケースを想像してください。証明機関から新しい証明書を取得したい。NetScaler ADM から証明書署名要求 (CSR) を生成できるようになりました。CSR と公開鍵を CA に送信して SSL 証明書を取得できます。

CSR を決定して作成するには、目的の証明書を選択し、[ **Create CSR** ] をクリックします。

公開キーまたは秘密キーの値ペアが必要です。キーをアップロードするには、[ **Choose File** ] をクリックし、リストから選択します。キーを作成するには、[ キーがありません ] オプションを選択し、関連するパラメータを指定します。



## ← Create Certificate Signing Request (CSR)

Name\*

When creating a certificate signing request, the first step is to create/upload a key for the certificate

I have a Key  I do not have a Key

Upload Key File\*

Choose File

Passphrase

CSRを作成するには、共通名、組織名、都市、国、州、組織単位、電子メール ID など、選択したキーの詳細を指定します。

← Create Certificate Signing Request (CSR)

**Key File Details**

|                                            |                                                               |                      |                   |
|--------------------------------------------|---------------------------------------------------------------|----------------------|-------------------|
| Certificate Signing Request Name<br>SBKey2 | Certificate type<br>Public Certificate Issued by a Trusted CA | Key file<br>aug1-key | Key Format<br>PEM |
|--------------------------------------------|---------------------------------------------------------------|----------------------|-------------------|

**Distinguished Name Fields**

Common Name\*

Organization Name\*

City\*

Country\*

State or Province\*

Organization Unit

Email ID

**SSL 証明書のリンクとリンク解除**

複数の SSL 証明書を相互にバインドして、証明書バンドルを作成できます。証明書を別の証明書に関連付けるとき、1 番目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なければなりません。

SSL Certificates - Issuer: Not Recommended 9

Details
Update
Delete
Poll Now
Select Action ▾

🔍 Issuer: **Not Recommended** Click here to search or you can enter Key : Value format

|                                     | CERTIFICATE NAME     | INSTANCE | HOST NAME   | DAYS TO EXPIRY    | STATUS |
|-------------------------------------|----------------------|----------|-------------|-------------------|--------|
| <input checked="" type="checkbox"/> | docs.dev.marquee.net | ...      | hostadc.dev | 343 days          | Valid  |
| <input type="checkbox"/>            | ...                  | ...      | hostadc.dev | 354 days          | Valid  |
| <input type="checkbox"/>            | A256-G2              | ...      | hostadc.dev | 354 days          | Valid  |
| <input type="checkbox"/>            | ...                  | ...      | --          | 359 days          | Valid  |
| <input type="checkbox"/>            | ...                  | ...      | --          | 15 years 17 days  | Valid  |
| <input type="checkbox"/>            | ...                  | ...      | --          | 15 years 198 days | Valid  |
| <input type="checkbox"/>            | ...                  | ...      | hostadc.dev | 15 years 204 days | Valid  |
| <input type="checkbox"/>            | ...                  | ...      | --          | 15 years 209 days | Valid  |
| <input type="checkbox"/>            | ...                  | ...      | --          | 15 years 209 days | Valid  |

- Details
- Update
- Delete
- Poll Now
- Download
- Link
- Unlink
- Create CSR

## 監査ログ

監査ログは、NetScaler ADM によって生成されるテキストログファイルのコレクションです。NetScaler ADM を使用して特定の NetScaler ADC アプライアンスに追加、変更、および変更された SSL 証明書の履歴が表示されます。監査ログには、NetScaler ADC アプライアンスの IP アドレス、ステータス、開始時刻、および特定の操作の終了時刻も表示されます。

この例では、特定の証明書に対して一定の間に行われた変更を確認することができます。また、デバイスログとコマンドログに証明書の変更履歴を表示するオプションがあります。

SSL 証明書の情報を調べるには、**SSL** ダッシュボードで、「監査ログ」をクリックします。アプリケーションの概要には、[開始時刻] と [終了時刻] の SSL 証明書ステータスが含まれます。

### SSL Audit Trails

| Device Log               |               |           |                               |                               |
|--------------------------|---------------|-----------|-------------------------------|-------------------------------|
| <input type="checkbox"/> | Name          | Status    | Start Time                    | End Time                      |
| <input type="checkbox"/> | ModifySSLCert | Completed | Fri, 19 Jan 2018 14:14:26 GMT | Fri, 19 Jan 2018 14:14:31 GMT |

特定の SSL 証明書の NetScaler ADC アプライアンスの情報を特定するには、該当する証明書のチェックボックスをオンにします。[デバイスログ] をクリックします。

### Device Log

| Command Log              |           |            |                               |                               |
|--------------------------|-----------|------------|-------------------------------|-------------------------------|
| <input type="checkbox"/> | Status    | IP Address | Start Time                    | End Time                      |
| <input type="checkbox"/> | Completed |            | Fri, 19 Jan 2018 14:14:26 GMT | Fri, 19 Jan 2018 14:14:31 GMT |

コマンドの種類とメッセージを表示するには、[ **Command Log** ] をクリックします。

### Command Log

| Status    | Message | Command                                                                            | Start Time                    | End Time                      |
|-----------|---------|------------------------------------------------------------------------------------|-------------------------------|-------------------------------|
| Completed | Done    | save config                                                                        | Fri, 19 Jan 2018 14:14:26 GMT | Fri, 19 Jan 2018 14:14:31 GMT |
| Completed | Done    | modify ssl certkey authcertserver -cert authcert.pem -key authcert.pem -inform DER | Fri, 19 Jan 2018 14:14:26 GMT | Fri, 19 Jan 2018 14:14:26 GMT |
| Completed | Done    | put /var/mps/tenants/root/ns_ssl_keys/authcert.pem /nsconfig/ssl/authcert.pem      | Fri, 19 Jan 2018 14:14:26 GMT | Fri, 19 Jan 2018 14:14:26 GMT |
| Completed | Done    | put /var/mps/tenants/root/ns_ssl_certs/authcert.pem /nsconfig/ssl/authcert.pem     | Fri, 19 Jan 2018 14:14:26 GMT | Fri, 19 Jan 2018 14:14:26 GMT |

## SSL ダッシュボードの使用

February 6, 2024

CitrixApplication Delivery Management (ADM) の SSL 証明書ダッシュボードを使用すると、証明書の発行者、主な強み、および署名アルゴリズムを追跡するのに役立つグラフを表示できます。SSL 証明書ダッシュボードには、次の項目を示すグラフも表示されます。

- 証明書が有効期限切れになるまでの日数

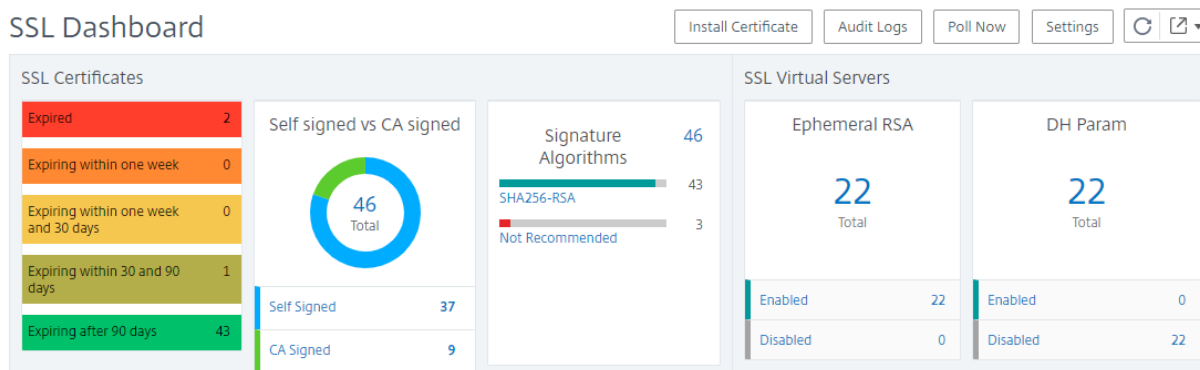
- 使用されている証明書および未使用の証明書の数
- 自己署名および CA 署名の証明書の数
- 発行者数
- 署名アルゴリズム
- SSL プロトコル
- 使用中の証明書件数上位 10 インスタンス

### SSL 証明書を監視するには

会社に SSL ポリシーがあり、すべての証明書の最小キー強度が 2048 ビットで、信頼できる CA 機関による承認が必要など、特定の SSL 証明書要件を定義している場合は、Citrix ADM SSL ダッシュボードを使用して証明書を監視できます。

別の例として、新しい証明書をアップロードしたが、それを仮想サーバーにバインドするのを忘れている場合があります。SSL ダッシュボードでは、使用中または未使用の SSL 証明書が強調表示されます。[ 使用法 ] セクションには、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が表示されます。さらにグラフをクリックすると、証明書名、証明書が使用されているインスタンス、有効性、署名アルゴリズムなどが表示されます。

NetScaler ADM で SSL 証明書を監視するには、[ ネットワーク ] > [ **SSL** ダッシュボード ] に移動します。



NetScaler ADM では、SSL 証明書をポーリングし、インスタンスのすべての SSL 証明書を直ちに NetScaler ADM に追加できます。そのためには、

1. [ ネットワーク ] > [ **SSL** ダッシュボード ] に移動します。
2. [ 今すぐ投票 ] をクリックします。

「**Poll Now**」 ページでは、すべての管理対象 ADC インスタンスをポーリングすることも、特定のインスタンスを選択することもできます。

3. [ ポーリングの開始 ] をクリックします。

**SSL** ダッシュボードでは、ADC SSL 証明書、SSL 仮想サーバー、および SSL プロトコルを監視できます。

ダッシュボードのメトリックをクリックすると、SSL 証明書、SSL 仮想サーバー、または SSL プロトコルに関連する詳細を表示できます。

たとえば、ダッシュボードの [自己署名と **CA** 署名済み] の下の番号をクリックすると、ADM GUI に NetScaler ADC インスタンスのすべての SSL 証明書が表示されます。

|                          | CERTIFICATE NAME | INSTANCE | HOST NAME | DAYS TO EXPIRY    | STATUS  | DOMAIN        |
|--------------------------|------------------|----------|-----------|-------------------|---------|---------------|
| <input type="checkbox"/> |                  |          | --        | Expired           | Expired | CTX4          |
| <input type="checkbox"/> |                  |          | --        | 360 days          | Valid   | hh            |
| <input type="checkbox"/> |                  |          | --        | 2 years 97 days   | Valid   | --            |
| <input type="checkbox"/> |                  |          | --        | 14 years 191 days | Valid   | default LUJFB |
| <input type="checkbox"/> |                  |          | --        | 14 years 331 days | Valid   | default MBNL  |
| <input type="checkbox"/> |                  |          | NS105     | 15 years 295 days | Valid   | default UZEK  |
| <input type="checkbox"/> |                  |          | --        | 15 years 361 days | Valid   | Citrix        |
| <input type="checkbox"/> |                  |          | --        | 28 years 203 days | Valid   | *.hotdrink.be |

NetScaler ADM SSL ダッシュボードには、仮想サーバーで実行されている SSL プロトコルの分布も表示されます。管理者は、SSL ポリシーを通じて監視するプロトコルを指定できます。詳細については、「[SSL ポリシーの設定](#)」を参照してください。サポートされるプロトコルは、SSLv2、SSLv3、TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3 です。仮想サーバー上で使用されている 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) キーまたはエフェメラル RSA キーを有効または無効にすると、ドーナツチャートが表示されます。これらのキーにより、1024 ビットの証明書の場合のように、サーバー証明書でエクスポートクライアントがサポートされていない場合でも、エクスポートクライアントとの安全な通信が実現されます。適切なグラフをクリックすると、DH または Ephemeral RSA キーが有効になっている仮想サーバーのリストが表示されます。

### SSL 証明書の監査記録を表示するには

NetScaler ADM で SSL 証明書のログの詳細を表示できるようになりました。ログの詳細には、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 ADM で SSL 証明書を使用して実行された操作が表示されます。監査記録情報は、複数の所有者によるアプリケーション上での SSL 証明書変更を監視するときに役立ちます。

SSL 証明書を使用して NetScaler ADM で実行された特定の操作の監査ログを表示するには、[ネットワーク] > [SSL ダッシュボード] の順に選択し、[監査ログ] をクリックします。

## SSL Audit Trails

| <input type="checkbox"/> | Name           | Status    | Start Time                    | End Time                      |
|--------------------------|----------------|-----------|-------------------------------|-------------------------------|
| <input type="checkbox"/> | InstallSSLCert | Completed | Mon, 17 Apr 2017 12:19:48 GMT | Mon, 17 Apr 2017 12:19:50 GMT |
| <input type="checkbox"/> | InstallSSLCert | Completed | Mon, 17 Apr 2017 12:14:13 GMT | Mon, 17 Apr 2017 12:14:15 GMT |
| <input type="checkbox"/> | InstallSSLCert | Completed | Mon, 17 Apr 2017 12:08:37 GMT | Mon, 17 Apr 2017 12:08:39 GMT |
| <input type="checkbox"/> | InstallSSLCert | Completed | Mon, 17 Apr 2017 12:06:18 GMT | Mon, 17 Apr 2017 12:06:22 GMT |
| <input type="checkbox"/> | InstallSSLCert | Completed | Mon, 17 Apr 2017 11:40:42 GMT | Mon, 17 Apr 2017 11:40:47 GMT |
| <input type="checkbox"/> | InstallSSLCert | Completed | Mon, 17 Apr 2017 11:37:22 GMT | Mon, 17 Apr 2017 11:37:24 GMT |

SSL 証明書を使用して実行された特定の操作については、その状態、開始時間、および終了時間を表示できます。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 Audit Trails

The screenshot shows the SSL Audit Trails interface. It includes a 'Device Log' section with a table of audit events. One event is selected, and its details are shown in a 'Device Log' section below. This section includes a 'Command Log' table with columns for Status, Message, Command, and Start Time.

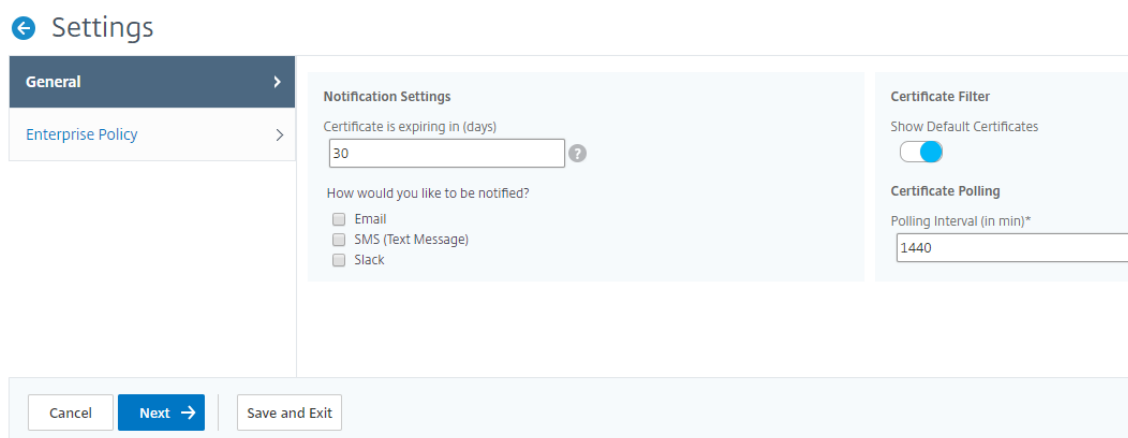
| Status | Message | Command                                                                           | Start Time                    |
|--------|---------|-----------------------------------------------------------------------------------|-------------------------------|
| Done   |         | add ssl certkey 88d2ee -cert multicon.pem -key multicon.key                       | Mon, 17 Apr 2017 12:19:48 GMT |
| Done   |         | put /var/impd/temants/rood/hs_ssl_keys/multicon/ky /nsconf/fig/ssl/multicon/ky    | Mon, 17 Apr 2017 12:19:48 GMT |
| Done   |         | put /var/impd/temants/rood/hs_ssl_certs/multicon.pem /nsconf/fig/ssl/multicon.pem | Mon, 17 Apr 2017 12:19:48 GMT |

SSL ダッシュボードでデフォルトの **NetScaler ADC** 証明書を除外するには

NetScaler ADM では、SSL ダッシュボードのグラフに表示されるデフォルトの NetScaler ADC 証明書の表示と非表示を切り替えることができます。デフォルトでは、デフォルトの証明書を含むすべての証明書が 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 ADM GUI で [ネットワーク] > [SSL ダッシュボード] に移動します。
2. [SSL ダッシュボード] ページで、[設定] をクリックします。
3. [設定] ページで、[一般] を選択します。
4. 証明書の有効期限が切れるまでの日数を入力して、証明書の有効期限切れに関する通知を受け取ります。
5. 通知方法を選択し、それぞれのプロファイルを作成します。
6. [証明書フィルタ] セクションで、[既定の証明書を表示する] チェックボックスをオフにし、[保存して終了] をクリックします。



## SSL ファイルの表示、アップロード、およびダウンロード

Citrix ADM で SSL ファイルを表示するには、Citrix ADM の [ネットワーク] > [SSL ダッシュボード] > [SSL ファイル] に移動します。

このページでは、NetScaler ADM で次のファイルを表示、アップロード、およびダウンロードできます。

- SSL 証明書
- SSL キー
- SSL CSR

Citrix ADC インスタンスで SSL ファイルを表示およびダウンロードするには、Citrix ADC の [ネットワーク] > [SSL ダッシュボード] > [SSL ファイル] に移動します。

### 重要

ADC インスタンスからの SSL ファイルのダウンロードを有効にするには、インスタンス **SSL 証明書** 機能を有効にします。詳しくは、「[ADM 機能の有効化または無効化](#)」を参照してください。

## SSL 証明書の有効期限の通知を設定する

February 6, 2024

セキュリティ管理者は、証明書の有効期限が近づいたときに通知し、どの Citrix Application Delivery Controller (ADC) インスタンスがそれらの証明書を使用しているかについての情報を含む通知を設定できます。通知を有効にすることで、SSL 証明書を遅れずに更新できます。

たとえば、証明書が満期になる 30 日前にメール配布リストを送信するようにメール通知を設定できます。

**NetScaler ADM** からの通知を設定するには：

1. Citrix Application Delivery Management (ADM) で、[ ネットワーク ] > [ **SSL** ダッシュボード ] に移動します。
2. [ **SSL** ダッシュボード ] ページで、[ 設定 ] をクリックします。
3. [ **SSL** 設定 ] ページで、[ 編集 ] アイコンをクリックします。
4. [ **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。ボックスの一覧メニューから通知の種類と配布リストを選択します。通知の種類を次に示します。
  - **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。
  - **SMS** - ショートメッセージサービス (SMS) サーバーとプロファイルの詳細を指定します。証明書の有効期限が近づくと、SMS メッセージがトリガーされます。
  - **Slack** - Slack プロファイルの詳細を指定します。
  - **PagerDuty** アラート - PagerDuty プロファイルを指定します PagerDuty ポータルで構成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、既定の ServiceNow プロファイルに通知が送信されます。

**重要:**

Citrix Cloud ITSM アダプタが ServiceNow 用に構成され、NetScaler ADM と統合されていることを確認します。詳しくは、「[NetScaler ADM と ServiceNow インスタンスの統合](#)」を参照してください。



**Notification Settings**

Certificate is expiring in (days)

30 ⓘ

How would you like to be notified?

Email

Mail Profile\*

default\_email\_profile ▼ Add Edit Test

Slack

Slack Profile

net\_scaler\_profile ▼ Add Edit

PagerDuty

PagerDuty Profile

myprofile ▼ Add Edit

ServiceNow

ServiceNow Profile\*

Citrix\_Workspace\_SN ▼

6. [保存して終了]をクリックします。

SSL 証明書の有効期限が切れると、NetScaler ADM が SSL 証明書の有効期限トラップを外部トラップ送信先サーバーに送信するようになりました。Citrix ADM は、次の 2 つの条件が満たされるとトラップを送信します。

- SSL ダッシュボード設定ページで証明書の有効期限が切れる日数を設定しました。
- トラップの宛先が追加されました。

トラップ宛先を設定するには、[システム] > [SNMP] > [トラップ送信先] に移動します。トラップが送信される宛先 SNMP サーバの IP アドレスを入力します。ポート番号を入力し、コミュニティストリングとして「public」（引用符なし）を入力します。

インストールされた証明書を更新する

February 6, 2024

認証局（CA）から更新された証明書を受け取ったら、個々の Citrix Application Delivery Controller（ADC）インスタンスにログオンしなくても、Application Delivery Management（ADM）から既存の証明書を更新できます。

**NetScaler ADM** から **SSL** 証明書、キー、またはその両方を更新するには：

1. NetScaler ADM で、[ネットワーク] > [**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 証明書の一覧を表示します。
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 証明書**] ページの右上隅にある [更新] をクリックします。
4. [**Update SSL Certificate**] ページで、証明書およびキーに必要な変更を加えて、[**OK**] をクリックします。

## NetScaler ADC インスタンスへの **SSL** 証明書のインストール

February 6, 2024

Citrix アプリケーション Delivery Controller（ADC）インスタンスに SSL 証明書をインストールする前に、証明書が信頼できる CA によって発行されていることを確認してください。また、証明書キーのキー強度が 2048 ビット以上であり、キーが安全な署名アルゴリズムで署名されていることを確認します。

別の **NetScaler ADC** インスタンスから **SSL** 証明書をインストールするには：

また、選択した NetScaler ADC インスタンスから証明書をインポートして、NetScaler Application Delivery Management（ADM）GUI から他のターゲット NetScaler ADC インスタンスに適用することもできます。

1. [ネットワーク] > [**SSL** ダッシュボード] に移動します。
2. SSL ダッシュボードの右上隅にある [インストール] をクリックします。
3. 「**Citrix ADC** 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) [証明書のソース]  
][[インスタンスからインポート] オプションを選択します。
    - 証明書のインポート元のインスタンスを選択します。
    - インスタンスのすべての SSL 証明書 ファイルのリストから [Certificate] を選択します。
  - b) 証明書詳細
    - 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、暗号化された秘密キーをアップロードできます。

4. 「インスタンスを選択」をクリックして、証明書をインストールする NetScaler ADC インスタンスを選択します。

5. **[OK]** をクリックします。

Install SSL Certificate on Citrix ADC Instances

▼ Certificate Source

Import from Instance  Upload Certificate File

Instance\*  
 > ?

Certificate\*

▼ Certificate Details

Certificate Name\*

Password  
 ?

Save Configuration

|                                     | IP Address    | Host Name | Instance State |
|-------------------------------------|---------------|-----------|----------------|
| <input checked="" type="checkbox"/> | 10.102.29.200 | --        | ● Up           |
| <input checked="" type="checkbox"/> | 10.102.29.160 | NS        | ● Up           |

**NetScaler ADM** から **SSL** 証明書をインストールするには:

1. NetScaler ADM で、[ネットワーク] > **[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 **[Install]** をクリックします。
3. **NetScaler ADC** インスタンスに **SSL 証明書をインストールする** ページで、[証明書ファイルのアップロード] を選択し、次のパラメーターを指定します。
  - 証明書ファイル: [ローカル] (ローカルマシン) または [アプライアンス] (証明書ファイルは NetScaler ADM 仮想インスタンス上に存在する必要があります) を選択して、SSL 証明書ファイルをアップロードします。
  - **Key File** - キーファイルをアップロードします。
  - **Certificate Name** - 証明書のキーの名前を指定します。
  - **Password** - 秘密キーを暗号化するためのパスワード。このオプションを使用して、暗号化された秘密キーをアップロードできます。
  - インスタンスの選択-証明書をインストールする Citrix ADM インスタンスを選択します。
4. 今後使用するために構成を保存するには、[構成を保存] 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。

## ← Install SSL Certificate on Citrix ADC Instances

▼ Certificate Source

Import from Instance     Upload Certificate File

Certificate File\*

Choose File ▾ pickCA\_rootcert.pem ?

Key File\*

Choose File ▾ pickCA\_rootcert.pem ?

▼ Certificate Details

Certificate Name\*

nsroot

Password

..... ?

Save Configuration

Select Instances    Delete

| <input type="checkbox"/>            | IP Address    | Host Name |
|-------------------------------------|---------------|-----------|
| <input checked="" type="checkbox"/> | 10.102.29.200 | --        |
| <input checked="" type="checkbox"/> | 10.102.29.160 | NS        |

### 証明書署名要求（CSR）の作成

February 6, 2024

CSR（Certificate Signing Request: 証明書署名要求）は、証明書が使用されるサーバー上で生成される暗号化済みテキストのブロックです。CSRには、組織名、共通名（ドメイン名）、地域、国など、証明書に格納される情報が含まれています。

**NetScaler ADM** を使用して **CSR** を作成するには:

1. NetScaler Application Delivery Management (ADM) で、[ネットワーク] > [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インストールされている SSL 証明書のリストを表示し、CSR を作成する証明書を選択し、[Select Action] リストから [ **\*\*Create CSR** ] を選択します **\*\***。
3. [ **Create Certificate Signing Request (CSR)** ] ページで、CSR の名前を指定します。
4. 次のいずれかを行います：
  - **Upload a key - [ I have a Key ]** オプションを選択します。キーファイルをアップロードするには、[ローカル] (ローカル マシン) または [アプライアンス] (キーファイルは NetScaler ADM 仮想インスタンスに存在している必要があります) を選択します。
  - キーの作成 - 「キーがありません」オプションを選択し、次のパラメータを指定します。

|                           |                                                                                                                      |
|---------------------------|----------------------------------------------------------------------------------------------------------------------|
| 暗号化アルゴリズム                 | キーの種類。たとえば、RSA などがあります。                                                                                              |
| キーファイル名                   | RSA キーが保存されたファイル名。                                                                                                   |
| キーサイズ                     | キーサイズ (ビット)。                                                                                                         |
| 公開指数値                     | 表示されるドロップダウンリストから [ <b>3</b> ] または [ <b>F4</b> ] を選択します。この値は、RSA キーを作成するのに必要な暗号アルゴリズムの一部です。                          |
| キーの形式                     | デフォルトでは PEM が選択されています。SSL 証明書には、PEM が推奨されるキーの形式です。                                                                   |
| <b>PEM</b> エンコーディングアルゴリズム | 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 ( <b>DES</b> または <b>DES3</b> ) を選択します。このアルゴリズムを選択すれば、PEM パスフレーズを入力する必要があります。 |
| <b>PEM</b> パスフレーズ         | PEM エンコーディングアルゴリズムを選択したのであれば、パスフレーズを入力します。                                                                           |
| <b>PEM</b> パスフレーズの確認      | PEM パスフレーズを確認します。                                                                                                    |

5. [ **続行** ] をクリックします。

6. 次のページで、詳細を入力します。

大半のフィールドには、選択した証明書のサブジェクトから抽出したデフォルト値が設定されます。サブジェクトには、共通名、組織名、州、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、単一の証明書を使用して、ドメイン名や IP アドレスなどの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。

```
1 DNS:<Domain name>, IP:<IP address>
2 <!--NeedCopy-->
```

### ← Create Certificate Signing Request (CSR)

| Key File Details                 |                                           |             |            |
|----------------------------------|-------------------------------------------|-------------|------------|
| Certificate Signing Request Name | Certificate type                          | Key file    | Key Format |
| 10.217.206.64_svr                | Public Certificate Issued by a Trusted CA | example-key | PEM        |

#### Distinguished Name Fields

Common Name\*

Organization Name\*

City\*

Country\*

State or Province\*

Organization Unit

Email ID

Subject Alternative Name

この例では、10.0.0.1とwww.example.comがセキュリティで保護されています。

フィールドを確認し、[ **Continue** ] をクリックします。

注

ほとんどの CA が電子メールによる証明書の送信を受け付けています。CA は、CSR の送信元の電子メールアドレスに有効な証明書を返します。

## SSL 証明書のリンクとリンク解除

February 6, 2024

複数の証明書をまとめて関連付けて、証明書パッケージを作成します。証明書を別の証明書に関連付けるとき、1 番目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なければなりません。たとえば、証明書 A を証明書 B に関連付ける場合、証明書 A の「発行者」は証明書 B の「ドメイン」と一致する必要があります。

**NetScaler ADM** を使用して **SSL** 証明書を別の証明書にリンクするには:

1. NetScaler Application Delivery Management (ADM) で、[ネットワーク] > [**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 証明書の一覧を表示します。
3. 関連付ける証明書を選択して、[Action] ボックスの一覧から [**Link**] を選択します。
4. 一致する証明書の一覧から関連付ける対象の証明書を選択して、[**OK**] をクリックします。

### 注

一致する証明書がない場合は「No certificate found to link.」というメッセージが表示されます。

**NetScaler ADM** を使用して **SSL** 証明書のリンクを解除するには:

1. NetScaler ADM で、[ネットワーク] > [**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 証明書の一覧を表示します。
3. 関連付けられているいずれかの証明書を選択し、[Action] ボックスの一覧から [**Unlink**] をクリックします。
4. [**OK**] をクリックします。

### 注

選択した証明書が別の証明書に関連付けられていない場合、「Certificate does not have any CA link.」というメッセージが表示されます。

## エンタープライズポリシーの構成

February 6, 2024

エンタープライズポリシーを構成し、すべての信頼できる CA、安全な署名アルゴリズムを追加し、NetScaler Application Delivery Management (ADM) で証明書キーの推奨キー強度を選択できます。Citrix Application Delivery Controller (ADC) インスタンスにインストールされている証明書のいずれかがエンタープライズポリシ

ーに追加されていない場合、SSL 証明書ダッシュボードには、これらの証明書の発行元が [推奨されていません] と表示されます。

また、証明書キーの強度がエンタープライズポリシーの推奨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「推奨なし」と表示されます。

**NetScaler ADM** でエンタープライズポリシーを構成するには:

1. Citrix ADM で、[インフラストラクチャ] > [**SSL** ダッシュボード] に移動し、[設定] をクリックします。
2. SSL 設定のページで、編集アイコンをクリックし、信頼できるすべての認証機関と安全な署名アルゴリズムを追加して、証明書のキーの推奨キー強度を選択します。
3. [**Save**] をクリックして、企業のポリシーを保存します。

## NetScaler ADC インスタンスからの SSL 証明書のポーリング

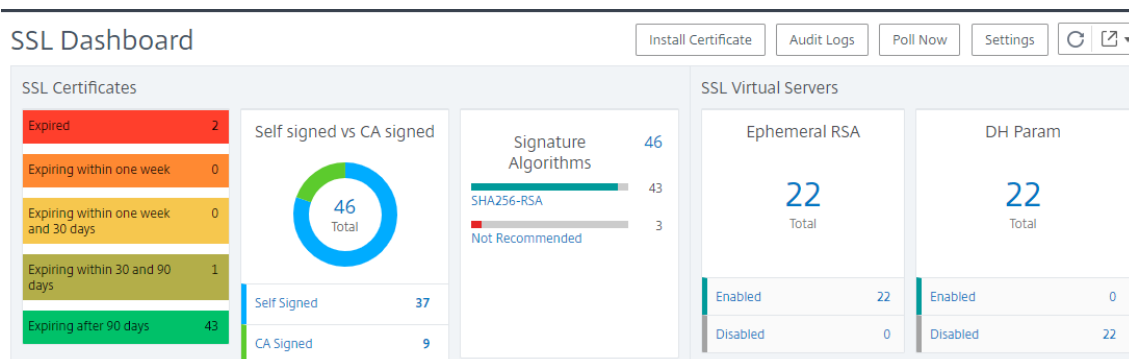
February 6, 2024

Citrix の Application Delivery Management (ADM) は、NITRO コールとセキュアコピー (SCP) プロトコルを使用して、24 時間に 1 回、SSL 証明書を自動的にポーリングします。SSL 証明書を手動でポーリングして、Citrix Application Delivery Controller (ADC) インスタンスに新しく追加された SSL 証明書を見つけることもできます。すべての NetScaler ADC 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 ADC 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 ADC** インスタンスで **SSL** 証明書をポーリングするには:

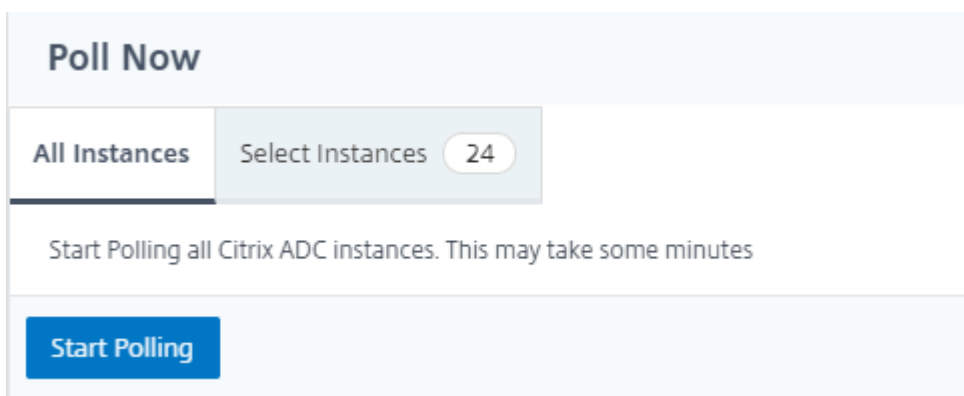
1. NetScaler ADM で、[ネットワーク] > [**SSL** ダッシュボード] に移動します。
2. [**SSL** ダッシュボード] ページの右上隅にある [今すぐポーリングする] をクリックします。



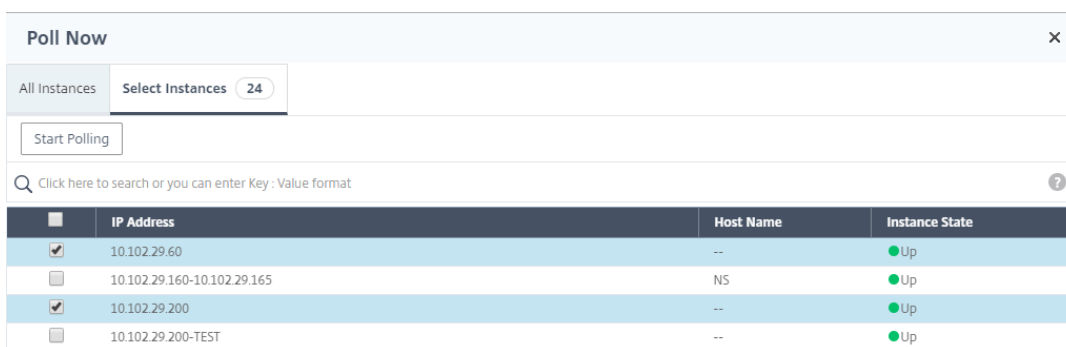
3. **Poll Now** ページが表示され、ネットワーク内のすべての Citrix ADC インスタンスをポーリングするか、選択したインスタンスをポーリングするかを選択できます。



- a) すべての Citrix ADC インスタンスの SSL 証明書をポーリングするには、[すべてのインスタンス] タブを選択し、[ポーリング開始] をクリックします。



- b) 特定のインスタンスをポーリングするには、[SelectInstances] タブを選択し、リストからインスタンスを選択し、[\*\*Poll Now] をクリックします。 \*\*



## IP アドレス管理 (IPAM) の構成

February 6, 2024

ADM IPAM では、ADM 管理構成で IP アドレスを自動的に割り当てたり解放したりすることができます。次の IP プロバイダーを使用して定義されたネットワークまたは IP 範囲から IP を割り当てることができます。

- ADM ビルトイン IP アドレス管理プロバイダー。
- Infoblox IPAM ソリューション。詳細については、「[Infoblox DDI](#)」を参照してください。

現在、ADM IPAM は次の用途で使用できます。

- **StyleBooks**: 構成を作成するときに仮想サーバーに IP を自動割り当てします。
- **Kubernetes** 入力: 仮想 IP アドレスを Kubernetes クラスタ内の入力設定に自動的に割り当てます。

また、ADM によって管理される各ネットワークまたは IP 範囲で、割り当てられた IP アドレスと使用可能な IP アドレスを追跡することもできます。

## 外部 IP アドレスプロバイダーの追加

ADM には、IP および IP 範囲を管理するための IP アドレス管理プロバイダーが組み込まれています。ADM で外部 IP プロバイダーソリューションを追加する場合は、次の手順を実行します。

1. [ネットワーク] > [IPAM] に移動します。
2. 「プロバイダ」で、「追加」をクリックします。
3. IP プロバイダーを追加するには、次の詳細を指定します。
  - 名前 -ADM で使用する IP プロバイダー名を指定します。
  - ベンダー -リストから IP アドレスベンダーを選択します。
  - URL -ADM 環境で IP アドレスを割り当てる IP アドレス管理ソリューションの URL を指定します。
  - ユーザー名 -IPAM ソリューションにログインする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。

## ネットワークの追加

ADM 管理設定で IP アドレス管理を使用するネットワークを追加します。

1. [ネットワーク] > [IPAM] に移動します。
2. [ネットワーク] で、[追加] をクリックします。
3. 次の詳細を指定します：
  - ネットワーク名 -ADM でネットワークを識別する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、ADM 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 -要件に応じて、リストから IP アドレス範囲または 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:

ADM IPAM は IPv4 アドレスのみをサポートします。

IP 範囲には、次の形式でネットワーク値を指定します。

- ```
1 <first-IP-address>-<last-IP-address>
2 <!--NeedCopy-->
```

例:

```
1 10.0.0.20-10.0.0.100
2 <!--NeedCopy-->
```

**CIDR** では、次の形式でネットワーク値を指定します。

```
1 <IP-address>/<subnet-mask>
2 <!--NeedCopy-->
```

例:

```
1 10.70.124.0/24
2 <!--NeedCopy-->
```

4. [作成] をクリックします。

### 割り当てられた **IP** アドレスの表示

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. [ネットワーク] > [**IPAM**] に移動します。
2. [ネットワーク] タブで、[割り当てられた **IP** をすべて表示] をクリックします。

このペインには、IP アドレス、プロバイダー名、プロバイダーのベンダー、および説明が表示されます。また、この IP アドレスを予約したリソースの詳細も表示されます。

- **モジュール:** IP アドレスを予約する ADM モジュールを表示します。たとえば、IP アドレスが StyleBooks によって予約されている場合、この列には StyleBooks がモジュールとして表示されません。
- **リソースタイプ:** そのモジュールのリソースタイプを表示します。StyleBooks モジュールでは、設定リソースタイプだけが IPAM ネットワークを使用します。
- 

注:

IP アドレスを解放する場合は、解放する IP アドレスを選択し、[割り当てられた **IP** を解放] をクリックします。

### 構成ジョブ

February 6, 2024

NetScaler Application Delivery Management (NetScaler ADM) 構成管理プロセスにより、ネットワーク内の複数の Citrix Application Delivery Controller (ADC) インスタンス間で、構成の変更、システムのアップグレード、およびその他のメンテナンスアクティビティを適切に複製できます。

NetScaler ADM では、これらのすべてのアクティビティを 1 つのタスクとして複数のデバイスで簡単に実行できる構成ジョブを作成できます。構成ジョブとテンプレートは、NetScaler ADM 上で最も反復的な管理タスクを単一のタスクに簡素化します。構成ジョブには、1 つまたは複数の管理対象デバイスで実行できる一連の構成コマンドが含まれています。

構成ジョブでは、ローカルストレージから他のアプライアンスに対して、SSH コマンドを使用して構成コマンドを実行したり、SCP を使用してファイルのコピーを実行したりできます。たとえば、HA フェールオーバーや HA アップグレードのスケジュールを設定できます。

NetScaler ADM で以下の 4 つのオプションのいずれかを使用して、構成ジョブを作成できます。これらのいずれかを使用して、構成ジョブを実行するためのシステムへのコマンドおよび指示の再利用可能なソースを作成します。

1. 設定テンプレート
2. インスタンス
3. ファイル
4. Record and Play

### 設定テンプレート

ジョブを作成し、一連の構成コマンドをテンプレートとして保存するときに、構成テンプレートを作成できます。これらのテンプレートは、[Create Jobs] ページで保存すると、[Create Template] ページに自動的に表示されます。

#### 注:

デフォルトの設定テンプレートでは、「名前を変更」オプションは無効になっています。ただし、カスタム設定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、それを使用してジョブを構成できます。

**組み込みテンプレート:** 構成テンプレートのリストから選択できます。これらのテンプレートには CLI コマンドの構文が用意されており、変数の値を指定できます。組み込みテンプレートは、説明とともに下の表に一覧表示されます。組み込みテンプレートオプションを使用して、ジョブにスケジュールを指定できます。ジョブとは、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のことです。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にスケジュールを指定できます。また、ジョブをすぐに実行するか、後段階で実行するようにジョブをスケジュールすることもできます。

### インスタンス

Citrix ADC リリース 11.0 以降を実行している Citrix 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。シングルバンドルのアップグレードを実行するには、NetScaler ADM 組み込みタスクを使用します。実行構成または保存された構成を抽出し、同じタイプの別の NetScaler ADC インスタンスでコマンドを実行することによって、NetScaler ADC インスタンスをアップグレードすることもできます。これにより、一方のインスタンスの構成をもう一方のインスタンス上にレプリケートできます。

### ファイル

ローカルマシンから構成ファイルをアップロードして、ジョブを作成できます。

#### ファイル使用の利点

- 任意のテキストファイルを使用して、構成コマンドの再利用可能なソースを作成できます。
- 書式設定は一切必要ありません。
- 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および保存するか、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。

## Record and Play

Create job を使用して独自の 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 ADC セッションからコマンドを取得できます。ジョブを実行すると、選択したインスタンスの ns.conf の変更が記録され、NetScaler ADM にコピーされます。

### 関連トピック

- [構成ジョブで SCP \(put\) コマンドを使う方法](#)
- [設定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](#)
- [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](#)
- [記録と再生を使用して構成ジョブを作成する方法](#)
- [NetScaler ADM でマスター構成テンプレートを使用する方法](#)

### 構成ジョブの作成

February 6, 2024

ジョブとは、1つまたは複数の管理対象インスタンスに対して作成および実行できる構成コマンドのセットです。Citrix Application Delivery Management (ADM) GUI を使用して、[インスタンス間で構成を変更したり、ネットワーク上の複数のインスタンスで構成を複製したり](<https://docs.citrix.com/ja-jp/netscaler-mas/11-1/configuration-jobs-rotate-configuration.html>)、構成タスクを記録して再生したりするジョブを作成し、CLI コマンドに変換できます。

NetScaler ADM 構成ジョブ機能を使用して、構成ジョブの作成、電子メール通知の送信、および作成されたジョブの実行ログの確認を行うことができます。

**NetScaler ADM** で構成ジョブを作成するには：

1. [ネットワーク] > [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] ページの [設定の選択] タブで、ジョブ名を指定し、一覧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ことも、保存されている設定テンプレートから既存のコマンドをインポートすることもできます。
  - 構成ジョブでジョブを作成するときに、構成エディタで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、さまざまなテンプレートを選択し、構成エディターにテンプレートをドラッグします。テンプレートタイプには、設定テンプレート、組み込みテンプレート、マスター設定、録音と再生、インスタンス、ファイルがあります。

注

Deploy Master Configuration Job テンプレートを初めて追加する場合、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 Master Configuration タイプになります。

設定エディタでコマンドを再配置したり、並べ替えたりすることもできます。コマンドラインをドラッグアンドドロップすることで、コマンドをある行から別の行に移動できます。テキストボックスでコマンドライン番号を変更するだけで、コマンドラインを 1 行から任意のターゲットラインに移動または再配置することもできます。構成ジョブの編集時に、コマンドラインを並べ替えたり、並べ替え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間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時に定義したすべての変数を、1 つの統合ビューで確認できます。「変数のプレビュー」タブをクリックすると、構成ジョブの作成または編集時に定義した 1 つの統合ビューで変数をプレビューできます。

設定エディタのコマンドごとに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てください。そして、「実行」タブの「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. [ **Select Instance** s] 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 ADC 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対してローカルに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。

- [セカンダリノードで実行]: セカンダリノードでのみジョブを実行するには、このオプションを選択します。

プライマリノードとセカンダリノードの両方を選択して、同じ構成ジョブを実行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を選択しない場合、構成ジョブはプライマリノード上で自動的に実行されます。

6. [変数値の指定] 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、NetScaler ADM サーバーにファイルをアップロードします。
- b) すべてのインスタンスに定義した変数に共通の値を入力します。
- c) [次へ] をクリックします。

ジョブにメールと **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、関連する詳細とともに、ジョブの成功または失敗などの詳細が含まれます。

1. [ネットワーク] > [設定ジョブ] に移動します。
2. メールと 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」タブの「実行レポートの受信」ペインに移動します。
  - 「電子メール」チェックボックスを選択し、実行レポートを送信する電子メール配布リストを選択します。メール配布リストを追加する場合は、「追加」をクリックして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て、実行レポートを送信したい Slack チャンネルを選択します。Slack プロファイルを追加する場合は、[追加] をクリックし、必要な Slack チャンネルのプロファイル名 **\*\***、チャンネル名、**\*\*** トークン を指定します。

4. [完了] をクリックします。

ジョブにメールと **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、関連する詳細とともに、ジョブの成功または失敗などの詳細が含まれます。

1. [ネットワーク] > [設定ジョブ] に移動します。
2. メールと 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」タブの「実行レポートの受信」ペインに移動します。
  - 「電子メール」チェックボックスを選択し、実行レポートを送信する電子メール配布リストを選択します。  
メール配布リストを追加する場合は、「追加」をクリックして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て、実行レポートを送信したい Slack チャンネルを選択します。  
Slack プロファイルを追加する場合は、[追加] をクリックし、必要な Slack チャンネルのプロファイル名 **\*\***、チャンネル名、**\*\*** トークン を指定します。

4. [完了] をクリックします。

実行要約の詳細を表示する手順は、次のとおりです。

1. [ネットワーク] > [構成ジョブ] に移動します。
2. 実行サマリーを表示するジョブを選択し、「詳細」をクリックします。



3. 「実行サマリー」をクリックすると、次の項目が表示されます。

- ジョブを実行したインスタンスのステータス
- コマンドはジョブで実行される
- 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

Execution Summary					
Instances 1		Last Execution Sep 16 1:04 PM			
Status of Instances					
IP Address	Status	Commands	Start Time	End Time	Instance User
10.102.29.191	Completed	3/3	Sep 16 1:04 PM	Sep 16 1:04 PM	nsroot >

レコードアンドプレイを使用して構成ジョブを作成する

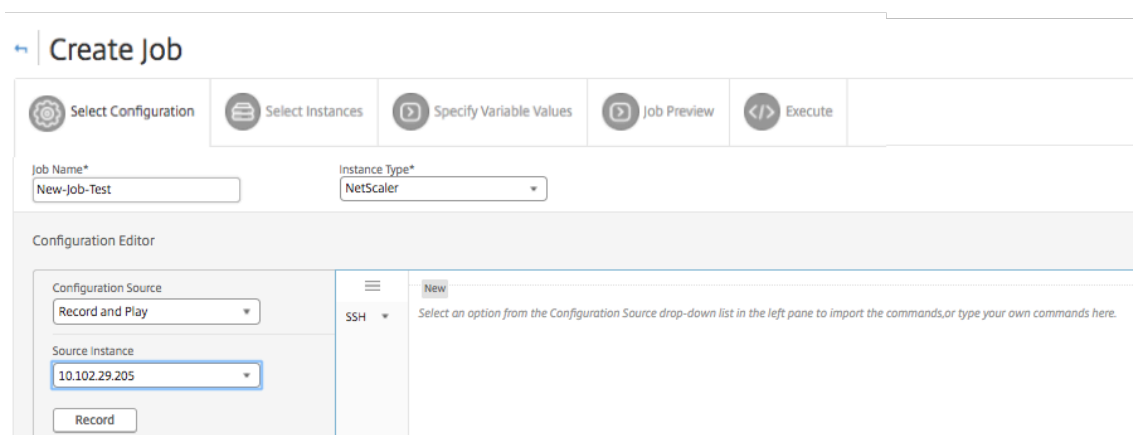
February 6, 2024

NetScaler ADC GUI を使用して NetScaler ADC 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て複数の NetScaler ADC インスタンスで実行するための正確な CLI コマンドを呼び出すことが困難な場合があります。

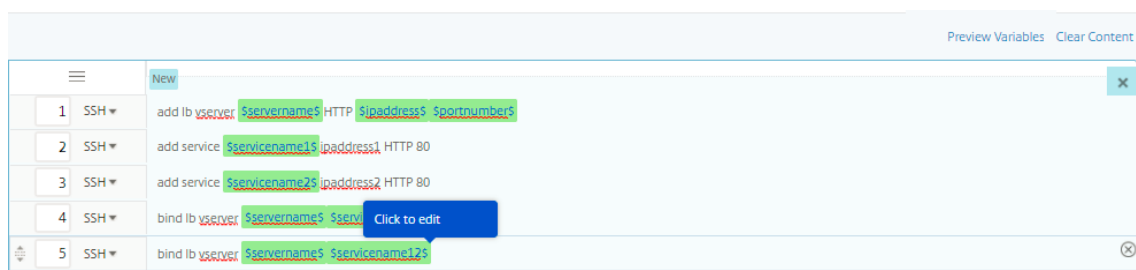
NetScaler ADM を使用すると、NetScaler ADC インスタンスの GUI を使用して実行された構成タスクを記録し、CLI コマンドに変換できます。変換された CLI コマンドから構成タスクを作成し、複数のインスタンスでそのタスクを実行できます。

**GUI** による構成を記録して構成タスクに変換するには

1. **[Networks]** > **[Configuration Jobs]** の順に選択してから、**[Create Job]** をクリックします。
2. ジョブ名とインスタンスのタイプを指定します。
3. 「設定ソース」リストから「記録して再生」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。

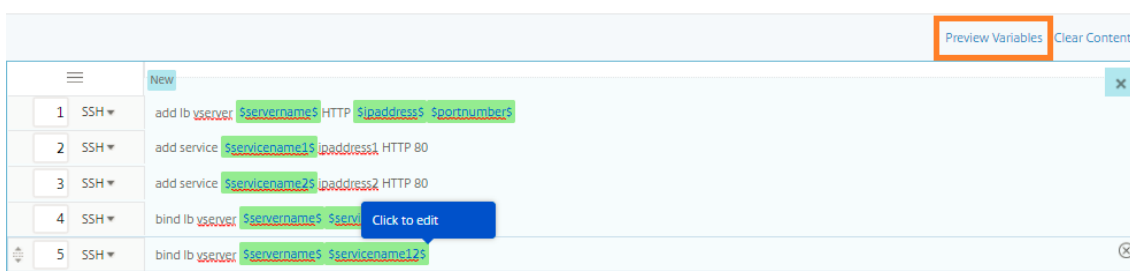


4. **NetScaler ADC の GUI** が開きます。構成タスクに含める機能と設定を構成します。次に、NetScaler ADC GUI ウィンドウを閉じて、構成エディタの [停止] をクリックします。左ペインにコマンドがリンクとして表示されます。コマンドを右側のウィンドウ枠にドラッグし、[次へ] をクリックします。

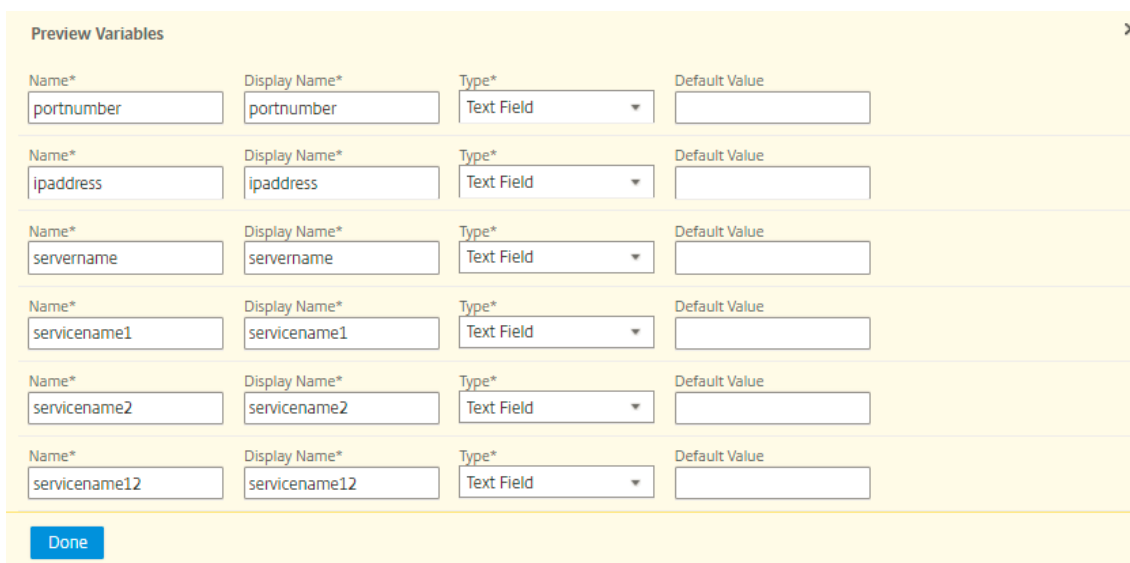


その後、構成レーションエディタでコマンドを並べ替えたり、並べ替えたりすることができます。コマンドラインをドラッグアンドドロップすることで、コマンドをある行から別の行に移動できます。テキストボックスでコマンドライン番号を変更するだけで、コマンドラインを 1 行から任意のターゲットラインに移動または再配置することもできます。

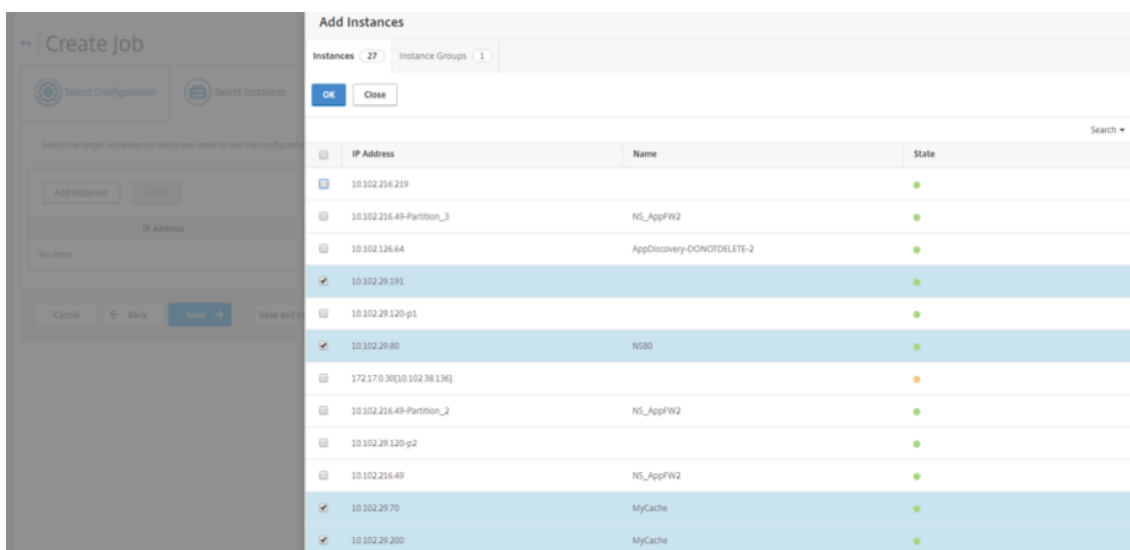
5. 構成ジョブの作成または編集集中に定義したすべての変数を、1 つの統合ビューで確認できます。
6. 次のいずれかの操作を行って、すべての変数を 1 つの統合ビューに表示します。
  - 構成ジョブを作成するときに、[ ネットワーク ] > [ 構成ジョブ ] に移動し、[ ジョブの作成 ] を選択します。[ **Create Job** ] ページでは、構成ジョブの作成時に追加したすべての変数を確認できます。
  - 構成ジョブの編集集中に、[ ネットワーク ] > [ 構成ジョブ ] に移動し、ジョブ名を選択して [ 編集 ] をクリックします。[ ジョブの構成 ] ページでは、構成ジョブの作成時に追加されたすべての変数を確認できます。
7. 次に、「変数のプレビュー」(Preview Variables) タブをクリックして、設定ジョブの作成または編集集中に定義した 1 つの統合ビューで変数を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修正することもできます。パラメータを編集または変更したら、[完了] ボタンをクリックします。



9. [Add Instances] をクリックし、構成ジョブを実行するインスタンスを選択します。[OK] をクリックし、[次へ] をクリックします。



10. コマンドで変数を指定した場合は、[Specified Variable Values] タブで、次のいずれかのオプションを選

択して、インスタンスの変数を指定します：

- 変数値の入力ファイルをアップロード：「入力キー ファイルをダウンロード」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、コマンドで定義した変数の値を入力し、NetScaler ADM サーバーにファイルを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。選択したテンプレートによって、変数は変わります。

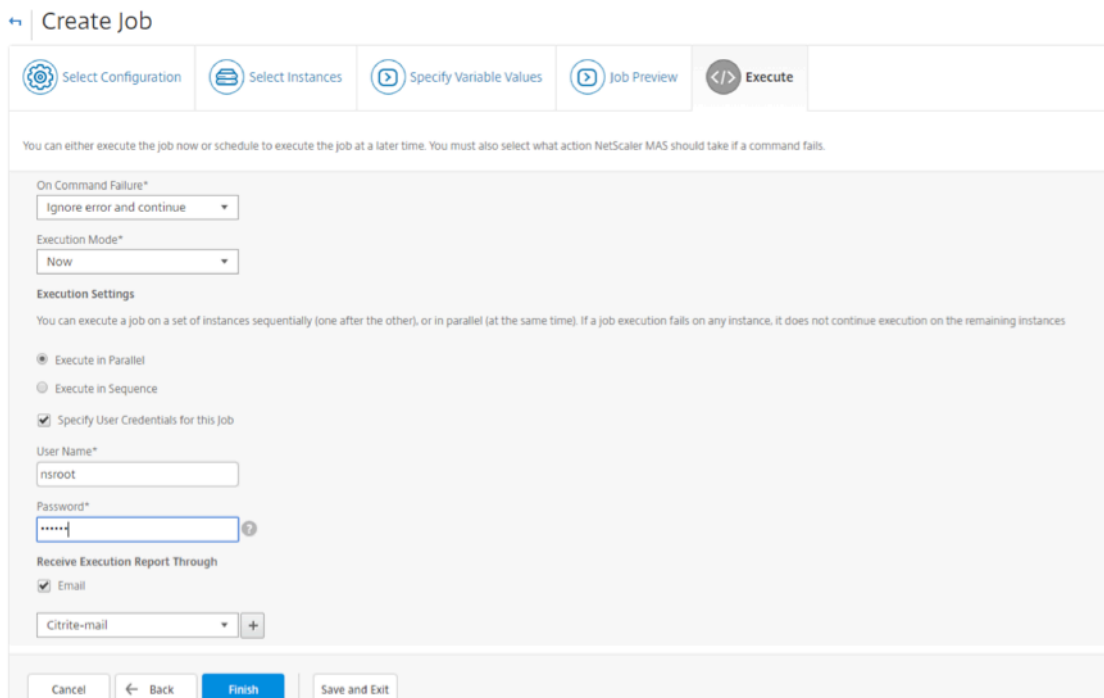
変数値を含む入力ファイルは、設定ジョブで (同じファイル名で) 保持されます。設定ジョブの作成または編集中に、以前に使用およびアップロードした入力ファイルを表示および編集できます。

構成ジョブの作成中に実行中の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。[ 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 ] オプションを選択し、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、ファイルを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)。

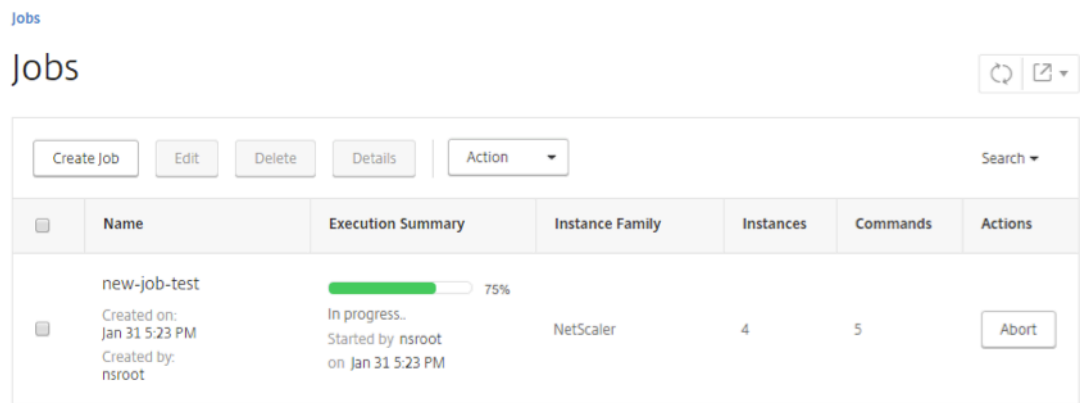
構成ジョブの編集中に実行済みの構成ジョブを表示するには、[ ネットワーク ] > [ 構成ジョブ ] に移動し、[ ジョブ名 ] を選択して [ 編集 ] をクリックします。[ ジョブの設定 ] ページの [ 変数値の指定 ] タブで、[ すべてのインスタンスに共通変数値 ] オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします (同じファイル名を使用)。10. [ **Job Preview** ] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。

11. [ **Job Preview** ] タブでは、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および確認できます。
12. [ **Execute** ] タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。コマンドが失敗した場合に NetScaler ADM が実行する必要があるアクションを選択することもできます。

また、承認されたユーザーが管理対象インスタンスでジョブを実行できるようにすることもできます。また、ジョブの成功または失敗に関する電子メール通知を他の詳細とともに送信するかどうかを選択できます。



13. [ **Jobs** ] ページでは、すべてのインスタンスでの設定タスク実行の進行状況を表示できます。



構成ジョブを使用して、**1**つのインスタンスから複数のインスタンスに構成を複製する

February 6, 2024

Citrix ADM の構成ジョブ機能を使用して、Citrix ADC インスタンスから特定の構成を抽出し、それを複数のインスタンスに複製できます。

たとえば、導入環境の Citrix ADC インスタンスで負荷分散とフロントエンド最適化 (FEO) の両方を構成している場合があります。ただし、今度は FEO 構成だけを他の Citrix ADC インスタンスに複製する必要があります。

あるインスタンスから他の **NetScaler ADC** インスタンスに構成を取得して複製するには:

1. **[Networks]** > **[Configuration Jobs]** の順に選択してから、**[Create Job]** をクリックします。

The screenshot displays the NetScaler Configuration Jobs interface. On the left, a navigation sidebar lists various system components, with 'Configuration Jobs' highlighted. The main area, titled 'Jobs', contains a toolbar with 'Create Job', 'Edit', 'Delete', 'Details', and 'Action' buttons. Below the toolbar is a table listing configuration jobs:

<input type="checkbox"/>	Name	Execution Summary
<input type="checkbox"/>	<b>Draft</b> LB Variables Created on: Dec 13 6:22 PM Created by: nsroot	
<input type="checkbox"/>	variables Created on: Nov 09 4:37 PM Created by: nsroot	<div style="text-align: right;">0%</div> In progress.. Started by nsroot on Nov 09 4:48 PM

2. ジョブ名とインスタンスのタイプを指定します。
3. 構成ソースとして [インスタンス] を選択し、構成を複製するソースインスタンスを選択します。抽出する設定のタイプを選択します。[期間による構成] を選択した場合は、この構成を実行した期間を設定し、[抽出] をクリックします。

選択した期間内にそのインスタンスで実行されたコマンドの数が、次の図で強調表示されているように画面に表示されます。

Job Name\*

replicate-job

### Configuration Editor

Configuration Source

Instance

Source Instance

10.102.29.120

Running Configuration

Saved Configuration

Configuration by time duration

Duration

Today

**Extract**

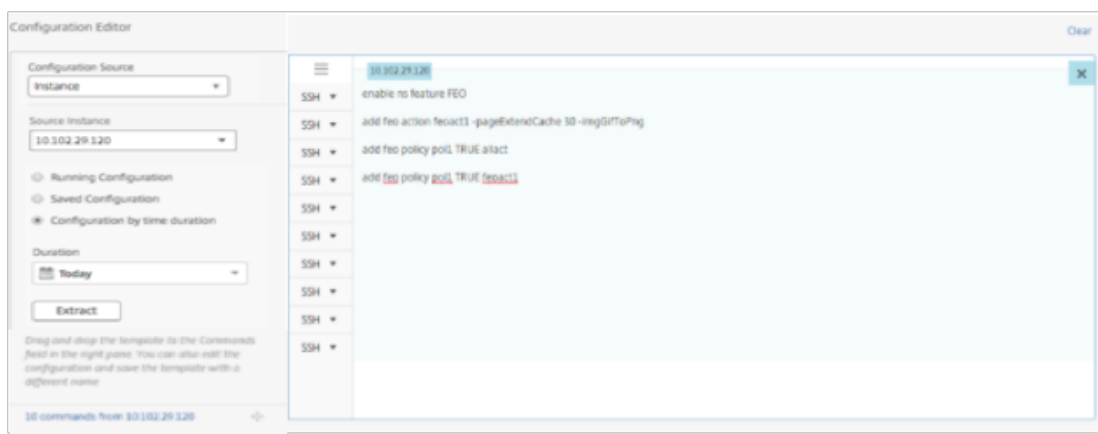
*Drag and drop the template to the Commands field in the right pane. You can also edit the configuration and save the template with a different name*

10 commands from 10.102.29.120

4. 右ペインの [Commands] フィールドにコマンドをドラッグします。



FEO に関するコマンドのみを保持します。負荷分散に関するコマンド、または他のすべての構成に関するコマンドは手動で削除し、[Next] をクリックします。



- [Add Instances] をクリックし、FEO 設定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。
- コマンドに変数を指定した場合は、[Specify Variable Values] タブで [Download Input Key File] をクリックします。ダウンロードしたファイルで、変数の値を指定し、NetScaler ADM にファイルをアップロードします。
- [Job Preview] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。
- [実行] タブで [完了] をクリックして、選択した NetScaler ADC インスタンスでジョブを実行します。



## 構成ジョブでの変数の使用

February 6, 2024

設定ジョブは、1つまたは複数の管理対象インスタンスで実行できる設定コマンドのセットです。複数のインスタンスで同じ設定を実行する場合、設定で使用されるパラメーターに異なる値を使用することが必要な場合があります。変数を定義して、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間でジョブを実行したりできます。

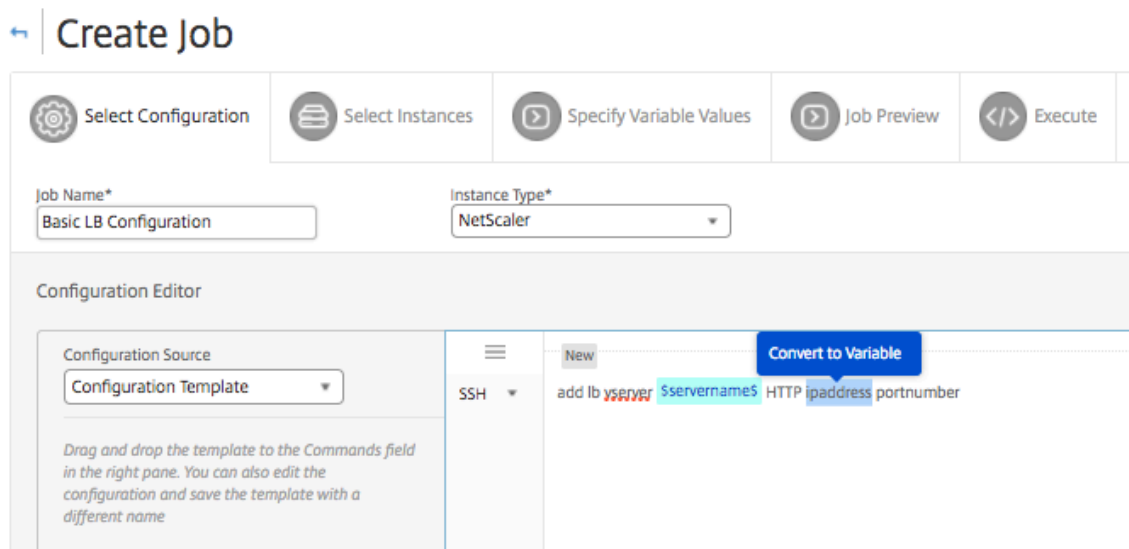
たとえば、負荷分散仮想サーバーを追加し、2つのサービスを追加し、それらのサービスをその仮想サーバーにバインドするという、基本的な負荷分散構成を考えてみましょう。ここでは、2つのインスタンスで同じ構成を使用するが、仮想サーバーとサービスの名前および IP アドレスに異なる値を使用する必要があります。これを実現するには、変数を使用して仮想サーバーとサービスの名前および IP アドレスを定義することで、構成ジョブ機能を使用します。

この例では、次のコマンドと変数を使用します。

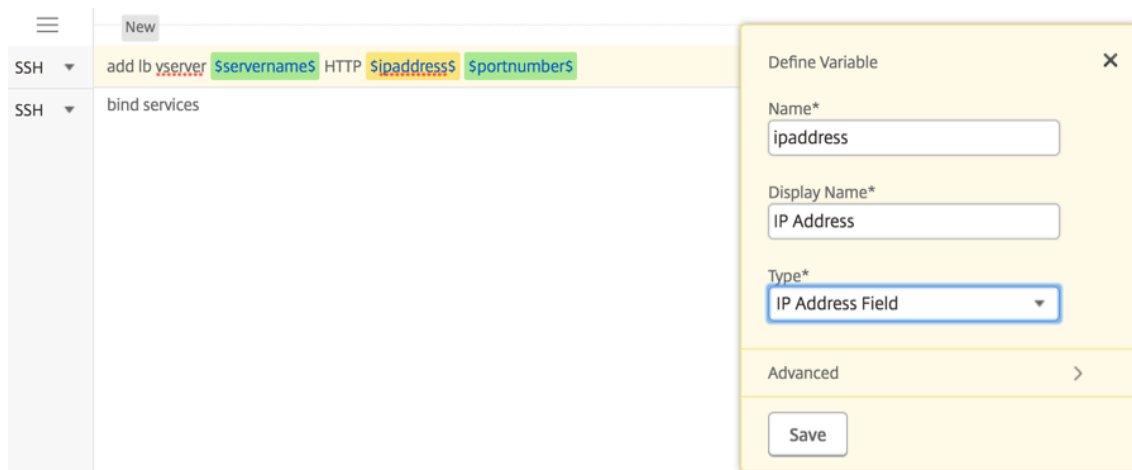
```
add lb vserver <servername> HTTP <ipaddress> <portnumber>
add service <servicename1> <ipaddress1> HTTP 80
add service <servicename2> <ipaddress2> HTTP 80
bind lb vserver <servername> <servicename1>
bind lb vserver <servername> <servicename2>
```

**NetScaler ADM** で変数を定義して構成ジョブを作成するには:

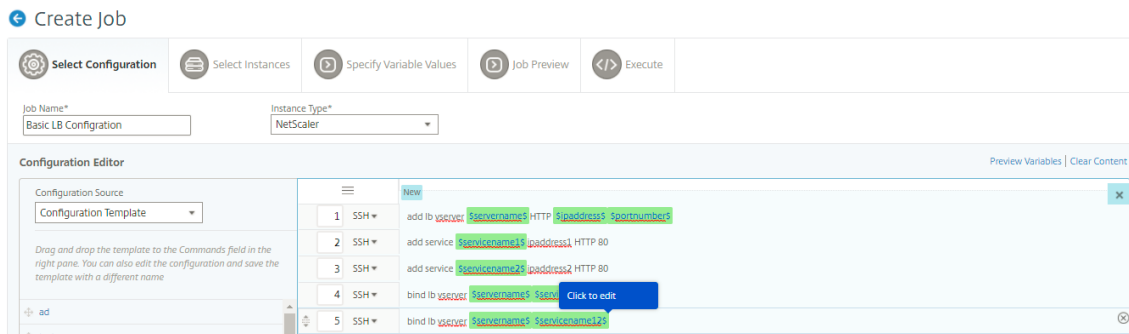
1. [ネットワーク]>[構成ジョブ]に移動します。
2. [ジョブの作成]をクリックします。
3. **Create Job** ページで、ジョブの名前、インスタンスタイプ、設定タイプなどのカスタムジョブパラメータを選択します。
4. [Configuration Editor] でコマンドを入力して、負荷分散仮想サーバー、2つのサービスを追加し、それらのサービスをその仮想サーバーにバインドします。変数に変換する値をダブルクリックして選択し、[変数に変換]をクリックします。たとえば、次の図に示すように、負荷分散サーバーの IP アドレス\***ipaddress**\*を選択し、[変数に変換]をクリックします。



- 変数の値を囲むドル記号が表示されたら、変数をクリックして、名前、表示名、タイプなどの変数の詳細をさらに指定します。変数のデフォルト値をさらに指定する場合は、「詳細」 (**Advanced**) オプションをクリックすることもできます。[保存] をクリックし、[次へ] をクリックします。



残りのコマンドを入力し、すべての変数を定義します。

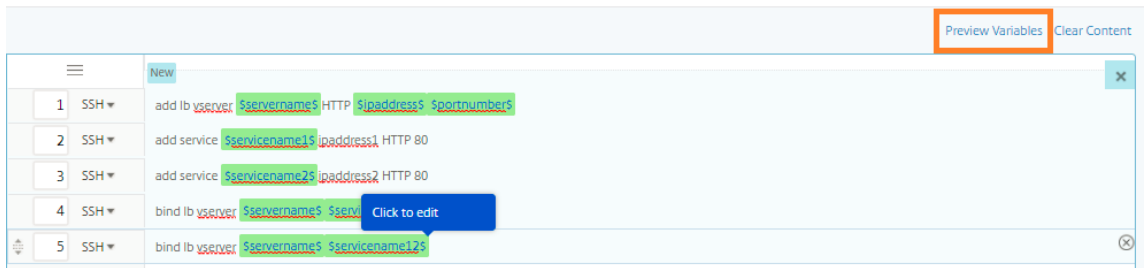


- 構成ジョブの作成または編集集中に定義したすべての変数を、1つの統合ビューで確認できます。

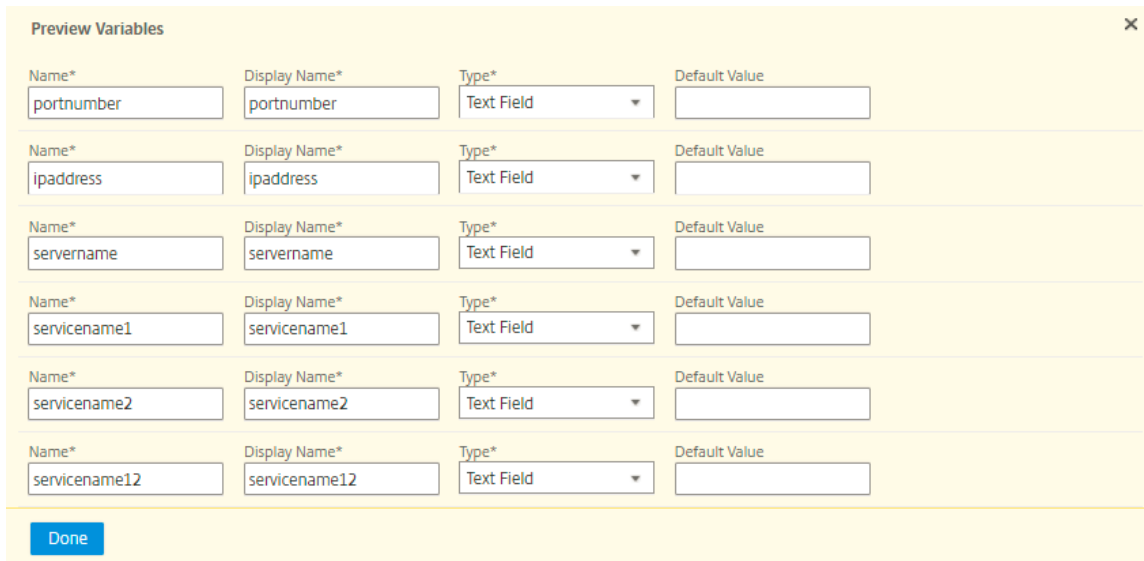
7. 次のいずれかの操作を行って、すべての変数を 1 つの統合ビューに表示します。

- 構成ジョブを作成するときに、[ ネットワーク ] > [ 構成ジョブ ] に移動し、[ ジョブの作成 ] を選択します。[ **Create Job** ] ページでは、構成ジョブの作成時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、[ 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 ] ページでは、構成ジョブの作成時に追加されたすべての変数を確認できます。

8. 次に、「変数のプレビュー」(Preview Variables) タブをクリックして、設定ジョブの作成または編集集中に定義した 1 つの統合ビューで変数を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示されます。これらのパラメータを編集および修正することもできます。パラメータを編集または変更したら、[ 完了 ] ボタンをクリックします。



10. その後、構成レーションエディタでコマンドを並べ替えたり、並べ替えたりすることができます。コマンドラインをドラッグアンドドロップすることで、コマンドをある行から別の行に移動できます。テキストボックスでコマンドライン番号を変更するだけで、コマンドラインを 1 行から任意のターゲットラインに移動または再配置することもできます。

11. 構成ジョブを実行するインスタンスを選択します。

12. 「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、「入力キーファイルのダウンロード」をクリックします。例では、各インスタンス上のサーバー名、サーバーとサービスの IP アドレ

ス、ポート番号、およびサービス名を指定する必要があります。ファイルを保存し、アップロードします。値が正確に定義されていない場合は、システムによってエラーがスローされる場合があります。

13. 入力キーファイルが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 Citrix ADC インスタンスの変数値を指定して編集し、「アップロード」をクリックして入力キーファイルを Citrix ADM にアップロードできます。[次へ] をクリックします。入力キーファイルが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 ADC インスタンスの変数値を指定することで編集できます。

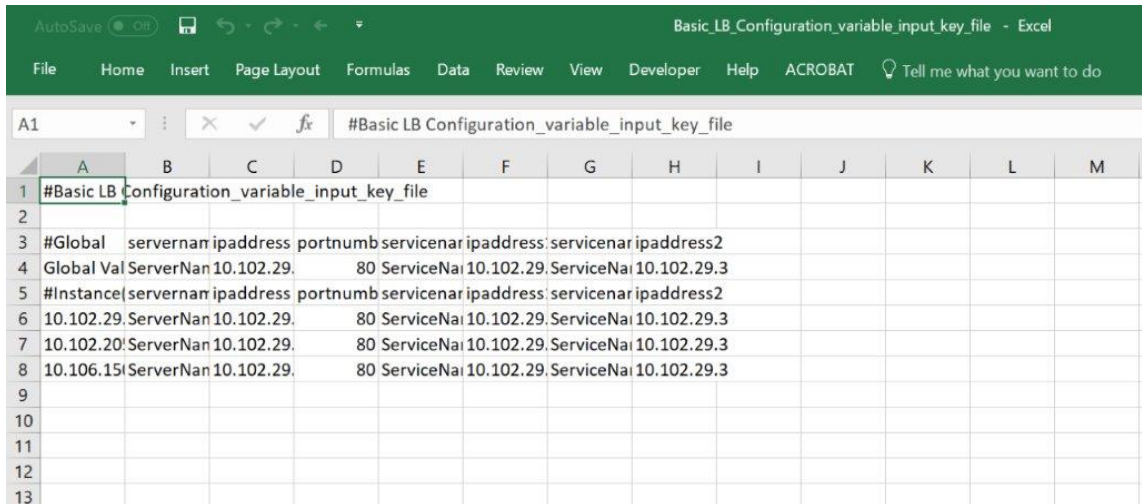
注：入力キーファイルでは、変数は3つのレベルで定義されています。

- グローバルレベル
- インスタンスグループレベル
- インスタンスレベル

グローバル変数は、すべてのインスタンスに適用される変数値です。インスタンスグループレベルの変数値は、グループで定義されているすべてのインスタンスに適用されます。インスタンスレベルの変数値は、特定のインスタンスにのみ適用されます。

NetScaler ADM では、インスタンスレベルの値が最優先されます。個々のインスタンスの変数に値が提供されていない場合、NetScaler ADM 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指定されていない場合、NetScaler ADM 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つのレベルすべてにわたって変数の入力を指定すると、NetScaler ADM はインスタンスレベル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 Citrix ADM にアップロードします。[次へ] をクリックします。



**重要**

Mac から CSV ファイルをアップロードすると、CSV ファイルはコンマではなくセミコロンで保存されます。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と、設定が失敗します。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行い、ファイルをアップロードします。

15. すべてのインスタンスに共通の変数値を指定し、「アップロード」をクリックして入力キーファイルを Citrix ADM にアップロードすることもできます。


変数値を含むキー入力ファイルは、設定ジョブで (同じファイル名で) 保持されます。設定ジョブの作成または編集に、以前に使用およびアップロードした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中の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。[ 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 ] オプションを選択し、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、ファイルを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実行済みの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。[ ジョブの設定 ] ページの [ 変数値の指定 ] タブで、[ すべてのインスタンスに共通変数値 ] オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを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** ] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。
17. [ **Execute** ] タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。また、コマンドが失敗した場合に NetScaler ADM が実行する必要があるアクションや、ジョブの成功または失敗に関する電子メール通知を他の詳細とともに送信するかどうかを選択することもできます。


← | **Configure Job**

 Select Configuration

 Select Instances

 Specify Variable Values

 Job Preview

 **Execute**

You can either execute the job now or schedule to execute the job at a later time. You must also select what action NetScaler MAS should take if a command fails.

On Command Failure\*

Ignore error and continue ▼

Execution Mode\*

Now ▼

**Execution Settings**

You can execute a job on a set of instances sequentially (one after the other), or in parallel (at the same time). If a job execution fails on any instance, it does not conti

Execute in Parallel

Execute in Sequence

Specify User Credentials for this Job

**Receive Execution Report Through**

Email

Cancel

← Back

Finish

Save and Exit

ジョブを構成して実行した後、[ ネットワーク ] > [ 構成ジョブ ] に移動して、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、[ 変数の詳細 ] をクリックして、ジョブに追加された変数の

リストを表示します。

Jobs / Job Details

### Job Details

Configuration Parameters	Name Basic LB Configuration	Instance Type NetScaler	Commands 5
--------------------------	--------------------------------	----------------------------	---------------

Execution Summary	Instances 2	Last Execution Nov 23 5:06 PM	100% C
-------------------	----------------	----------------------------------	--------

Variable Details	Variables 7
------------------	----------------

Variable	Display Name	Type
ipaddress	ipaddress	IP Address Field
ipaddress1	ipaddress1	IP Address Field
ipaddress2	ipaddress2	IP Address Field
servicename2	servicename2	Text Field
servename	servename	Text Field
servicename1	servicename1	Text Field

Execution Parameters	Execution Frequency Once	Next Execution N/A	Execute In Para
----------------------	-----------------------------	-----------------------	--------------------

注

**STEP 5** で変数に指定した値は、ジョブを保存して終了するとき、または後でジョブを実行するようにスケジュールするときに、NetScaler ADM によって保持されます。

## 修正コマンドからの構成ジョブの作成

February 6, 2024

NetScaler Application Delivery Management (ADM) の監査テンプレート機能を使用して、管理対象の NetScaler ADC インスタンスの構成変更を監視し、構成エラーのトラブルシューティングを行うことができます。

監査テンプレートを用いた構成変更の監査の通常のワークフローは、以下の手順で構成されます。

1. インスタンス構成を監査するための有効/期待される Citrix ADC 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. 監査テンプレートを実行する NetScaler ADC インスタンスを選択して、実行構成と予想される構成の違いがないか確認します。
3. 差分と修正コマンドを理解し、[Create Job] 機能を利用して、インスタンスの構成を必要な状態にします。

複数の管理者が 5 つの NetScaler ADC 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。これらの管理者すべてが、既存のインスタンスの構成に、変更が必要になれば更新するとします。スーパー管理者は他の管理者からの変更にかかわらず、特定の重要な構成の設定は触れられずに保持されることを確保したいと考えます。このユースケースでは、スーパー管理者が Citrix ADC インスタンスに存在すると予想される構成のテンプレートを作成し、そ

れをインスタンスに対して実行します。NetScaler ADM は監査テンプレート構成と実行構成を比較し、[構成監査] ダッシュボードで不一致を報告します。

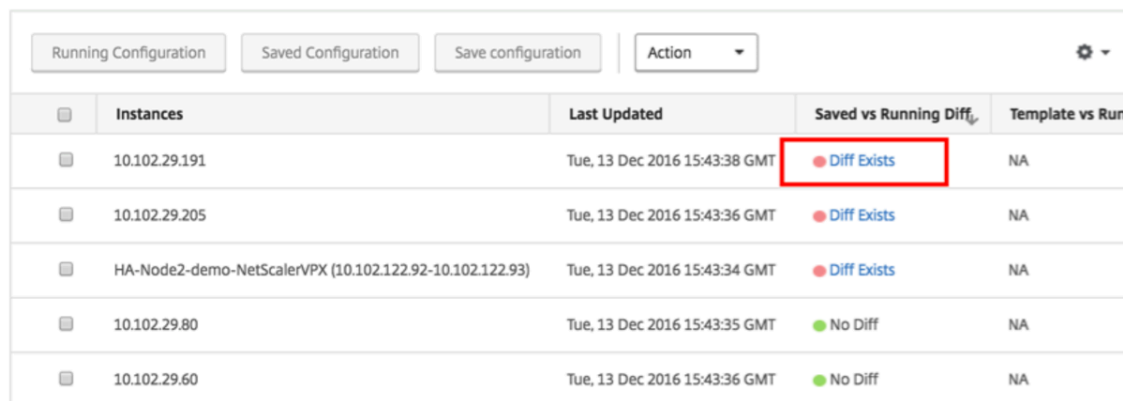
一部のインスタンスの構成に変更があることに気付いた場合は、NetScaler ADM 修正コマンド機能を使用して、特定の NetScaler ADC インスタンス用の変更および修正された構成コマンドを含む構成ジョブを作成できます。

監査テンプレート設定と構成実行の間に相違がある場合は、「監査レポート」(Audit Report) ページに「差分」( **Diff Exist s**) ステータスメッセージが表示されます。「相違の出口」リンクをクリックすると、「構成の差分」ページが表示され、修正コマンドを表示できます。また、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 ADC インスタンスで実行して、必要な構成に戻すこともできます。

### NetScaler ADM 修正コマンドで構成ジョブを作成するには

1. [ネットワーク]>[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の中をクリックして、[監査レポート] ページにアクセスします。
3. 設定コマンドを修正するインスタンスの「**Diff Exists**」リンク (表の「保存済みと実行中の相違点」列の下) をクリックします。[ **Configuration Diff** ] ページが表示され、そのインスタンスの [保存された設定]、[実行設定]、[修正設定] の相違点が一覧表示されます。

## Audit Reports



<input type="checkbox"/>	Instances	Last Updated	Saved vs Running Diff	Template vs Run
<input type="checkbox"/>	10.102.29.191	Tue, 13 Dec 2016 15:43:38 GMT	<b>Diff Exists</b>	NA
<input type="checkbox"/>	10.102.29.205	Tue, 13 Dec 2016 15:43:36 GMT	Diff Exists	NA
<input type="checkbox"/>	HA-Node2-demo-NetScalerVPX (10.102.122.92-10.102.122.93)	Tue, 13 Dec 2016 15:43:34 GMT	Diff Exists	NA
<input type="checkbox"/>	10.102.29.80	Tue, 13 Dec 2016 15:43:35 GMT	No Diff	NA
<input type="checkbox"/>	10.102.29.60	Tue, 13 Dec 2016 15:43:36 GMT	No Diff	NA

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、修正コマンドがあらかじめ入力されています。構成ジョブの作成方法については、「[NetScaler ADM で構成ジョブを作成する方法](#)」を参照してください。

← Configuration Diff

Saved vs Running Diff of Device: (10.102.29.191) Create Job Export all the corrective commands

Saved Configuration	Running Configuration	Correction Configuration
	bind serviceGroup servicegroup-nmas1 10.10.10.1 80	unbind serviceGroup servicegroup-nmas1 10.10.10.1 80
	bind lb vserver nmas-ha-lb service_nmas3	unbind lb vserver nmas-ha-lb service_nmas3
	add service service_nmas3 10.102.29.54 HTTP 80 -psb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO	rm service service_nmas3
	add server 10.102.29.54 10.102.29.54	rm server 10.102.29.54
	add server 10.10.10.1 10.10.10.1	rm server 10.10.10.1
set appflow param -templateRefresh 3600 -httpUrl ENABLED -httpCookie ENABLED -httpReferer ENABLED -httpMethod ENABLED -httpHost ENABLED -httpUserAgent ENABLED -httpContentType ENABLED	set appflow param -templateRefresh 60 -httpUrl ENABLED -httpCookie ENABLED -httpReferer ENABLED -httpMethod ENABLED -httpHost ENABLED -httpUserAgent ENABLED -httpContentType ENABLED	set appflow param -templateRefresh 3600 -httpUrl ENABLED -httpCookie ENABLED -httpReferer ENABLED -httpMethod ENABLED -httpHost ENABLED -httpUserAgent ENABLED -httpContentType ENABLED

Close

ある **NetScaler ADC** インスタンスから別のインスタンスに実行および保存された構成を複製する

February 6, 2024

2018年5月24日

Citrix ADC インスタンスの構成を他のインスタンスに複製できるようになりました。NetScaler ADM でジョブを構成する場合は、構成ソースとしてインスタンスを選択し、選択したインスタンスの実行中または保存された構成を選択します。

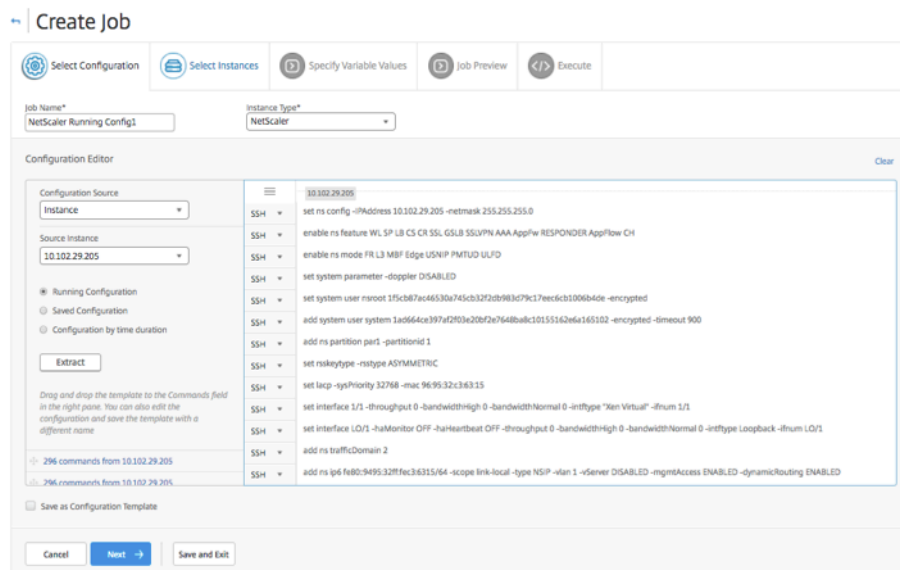
たとえば、NetScaler ADM [実行構成] を選択して [抽出] をクリックすると、選択した NetScaler ADC インスタンスに実行構成を検索する要求が送信され、テンプレートとして表示されます。テンプレートは、右側のペインの [Commands] フィールドにドラッグできます。コマンド、パラメータ、およびインスタンスを修正できます。

あるインスタンスの実行および保存された構成コマンドを **NetScaler ADM** 上の別のインスタンスにレプリケートするには:

1. [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。
2. ジョブ名とインスタンスのタイプを指定します。たとえば、ジョブの名前として *Citrix ADC Running Config1* を指定し、インスタンスタイプを *CitrixADC* として指定します。
3. [構成ソース] として [インスタンス] を選択し、他のインスタンスに構成をレプリケートするソース・インスタンスを選択します。
4. 次の3つのオプションが表示されます。
  - [Running Configuration]
  - [Saved Configuration]
  - [Configuration by time duration]



- 「実行構成」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ている実行構成の数が表示されます。



- 右ペインの [Commands] フィールドでコマンドをドラッグします。
- [Commands] 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 ADC インスタンスをセットアップする場合などです。これには、パーティションの追加、負荷分散の設定、負荷分散サーバーのサービスへのバインドなどが含まれます。コマンドを編集して、パーティションなしで新しい NetScaler ADC インスタンスをセットアップすることもできます。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。
- [ **Add Instances** ] をクリックし、実行中の設定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、「次へ」をクリックします。
- コマンドで変数を指定した場合は、[ 変数値の指定 ] タブで [ 入力キーファイルのダウンロード ] をクリックします。ダウンロードしたファイルで、変数の値を指定し、NetScaler ADM にファイルをアップロードします。
- [ **Job Preview** ] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。
- [ **Execute** ] タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。また、NetScaler ADM がコマンドが失敗するアクションや、ジョブの成功または失敗に関する電子メール通知を他の詳細とともに送信するかどうかを選択することもできます。

## 実行構成ジョブを再利用する

February 6, 2024

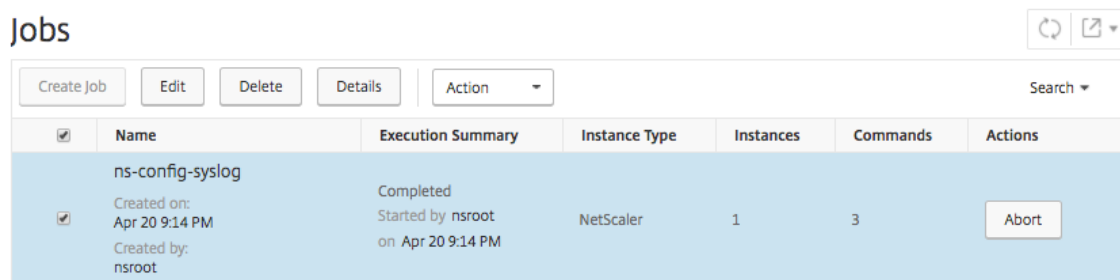
設定ジョブを使用すると、1つ以上の管理対象インスタンスで実行できる設定コマンドのセットを作成できます。また、保存した構成ジョブのコマンド、パラメーター、構成ソース、インスタンスを変更してから、そのジョブの同様のセットを実行することもできます。これは、同じ一連のコマンドを別のインスタンスで実行する必要がある場合や、ジョブでエラーが発生してそれ以降の実行を停止する場合に便利です。

NetScaler Application Delivery Management (ADM) には、完了したジョブを再度実行する機能があります。この機能を使用すると、完全に実行されたジョブは、ジョブ名を変更せずに再度実行できます。

注: 実行モードが「今」のときに実行されるジョブのみを再実行できます。

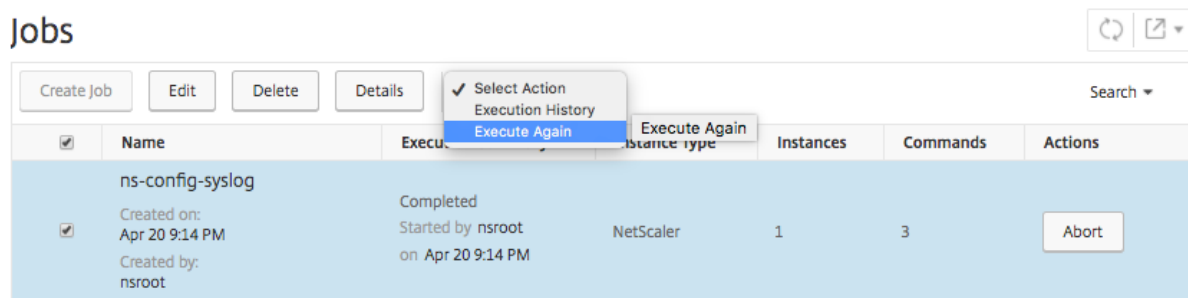
完了したジョブを編集するには、次の手順に従います。

1. NetScaler ADM ホームページから、[ネットワーク] > [構成ジョブ] に移動します。
2. 「ジョブ」ページで、「実行サマリー」が「完了」と表示されるジョブを選択し、「編集」をクリックします。スケジューリング指定された構成ジョブも編集できます。
3. [Configure Job] ページで、[Job Name] と [Instance Type] が編集できないことを確認できます。構成ソースをはじめとするその他のフィールドの変更、インスタンスの追加、変数値の編集、実行設定の指定を行うことができます。
4. [完了] をクリックして、構成ジョブを再度実行します。



注

ジョブを選択し、もう一度 [Execute] 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。場合によっては、ジョブがサーバー側から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。



## 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

February 6, 2024

組み込みテンプレートオプションを使用して、ジョブにスケジュールを指定できます。ジョブとは、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のことです。たとえば、組み込みのテンプレートオプションを使用して、syslog サーバを設定するジョブをスケジュールします。ジョブをすぐに実行するか、後段階で実行するようにジョブをスケジュールすることもできます。

**Citrix Application Delivery Management (ADM)** で組み込みテンプレートを使用してジョブをスケジュールするには

1. NetScaler ADM で、[ネットワーク] > [構成ジョブ] の順に選択し、[ジョブの作成] をクリックします。
2. [ **Create Job** ] ページの [ **Select Configuration** ] タブで、[ **Job Name** ] を指定し、ドロップダウンリストから [ **Instance Type** ] を選択します。
3. 「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** コマンドを右側のウィンドウ枠にドラッグし、[ 次へ ] をクリックします。

## ← Create Job

Configuration Editor

Configuration Source: Inbuilt Template

Drag and drop the template to the Commands field in the right pane. You can not edit the configuration or save the template with a different name

NSConfigureSyslogServer

SSH	Commands
SSH	add audit syslogaction action_name_ \$serverIP \$serverIP -serverPort \$serverPort -logLevel all
SSH	add audit syslogpolicy policy_name_ \$serverIP ns_true action_name_ \$serverIP
SSH	bind system global policy_name_ \$serverIP

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、[ **OK** ] をクリックします。
5. [ 次へ ] をクリックします。[ **Specify Variable Values** ] タブで次のいずれかのオプションを選択してインスタンスの変数を指定します。
  - 入力ファイルからの変数値 -入力ファイルをダウンロードして、コマンドで定義した変数の値を入力します。次に、ファイルを Citrix ADM サーバーにアップロードします。

- **Common variable values for all instances** - Syslog サーバーの IP アドレスとポートを指定します。
6. [ **Job Preview** ] タブでは、各インスタンスまたはインスタンスグループで実行す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：
    - コマンド失敗の場合 -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、ジョブのさらなる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ことも、後でジョブを実行するようにスケジュールすることもできます。後でジョブを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。ジョブに定めるスケジュールをボックスの一覧から選択します。
  9. 「実行設定」 ( **Execution Settings**) で必要なメソッドを選択して、一連のインスタンスに対してジョブを順次または並列で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にエラーが発生した場合、残っているインスタンスに続行することはありません。
 

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することを許可するように選択できます。ジョブの成功または失敗に関する電子メール通知は、他の詳細とともに送信することもできます。
  10. [完了] をクリックします。

↩ Create Job

⚙ Select Configuration
📄 Select Instances
⏪ Specify Variable Values
👁 Job Preview
Execute

You can either execute the job now or schedule to execute the job at a later time. You must also select what action NetScaler MAS should take if a command fails.

On Command Failure\*

Ignore error and continue

Execution Mode\*

Now

**Execution Settings**

You can execute a job on a set of instances sequentially (one after the other), or in parallel (at the same time). If a job execution fails on any instance, it does not continue execution on the remaining instances

Execute in Parallel  
 Execute in Sequence

Specify User Credentials for this Job

User Name\*

nsroot

Password\*

.....

Receive Execution Report Through

Email

Citrite-mail

Cancel
← Back
Finish
Save and Exit

## メンテナンス・ジョブを使用した **NetScaler ADC SDX** インスタンスのアップグレード

February 6, 2024

NetScaler ADC リリース 11.0 以降を実行している NetScaler ADC 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。シングルバンドルのアップグレードを実行するには、NetScaler ADM 組み込みタスクを使用します。この組み込みタスクを使用すると、Citrix ADC SDX 管理サービス、Citrix Hypervisor、および Citrix Hypervisor のサプリメントパックとホットフィックスをアップグレードできます。

**NetScaler ADM** を使用して **NetScaler ADC SDX** インスタンスをアップグレードするには：

1. [ネットワーク] > [構成ジョブ] > [メンテナンスジョブ] に移動します
2. [ジョブの作成] をクリックします。[ジョブの作成] ページで、[**NetScaler ADC SDX** のアップグレード] ビルトインタスクを選択して、NetScaler ADC SDX インスタンスをアップグレードします。[続行] をクリックします。
3. [**NetScaler ADC** アプライアンスのアップグレード] ページの [インスタンスの選択] タブで、ジョブ名を指定し、[インスタンスの追加] をクリックします。
4. アップグレードするターゲット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. NetScaler ADC インスタンスまたはインスタンスグループを追加したら、[次へ] をクリックして、選択したインスタンスでアップグレード前の検証を開始します。画面には、各 NetScaler ADC インスタンスの事前検証の進行状況が報告されます。
6. [アップグレード **NetScaler ADC** アプライアンスの変更] ページで、[アップグレード] タブを選択します。[ソフトウェアイメージ] ドロップダウンメニューから、[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 ADM に存在している必要があります) を選択します。
7. また、検証前のアップグレードエラーが発生しているインスタンスがあるかどうかを確認することもできます。これらのエラーは、メッセージ形式で表示されます。メッセージでは、ディスクスペース、ハードディスクドライブ、およびユーザーのカスタマイズに関するエラーが示されます。事前検証アップグレードチェックに失敗したインスタンスの使用を続行しない場合は、そのインスタンスを削除できます。インスタンスを削除するには、インスタンスを選択して [削除] をクリックします。
8. [**Schedule Task**] タブでは、アップグレード・プロセスを今すぐ実行したり、後日スケジュールを設定したりできる実行の詳細を設定することもできます。また、NetScaler ADC SDX インスタンスのバックアップ、電子メールによる実行レポートの受信、高可用性ノードの 2 段階アップグレードの実行を選択することもできます。

HA のノードの 2 段階アップグレードでは、アップグレードをすぐに実行するか、ノードを次々に更新する時間をスケジュールするかを選択できます。ノードの同期と伝播は、両方のノードが正常にアップグレードされるまで無効になります。

## Citrix SD-WAN WANOP インスタンスの構成ジョブの作成

February 6, 2024

ジョブとは、管理対象インスタンスに対して作成およびスケジュール設定できる構成コマンドのセットです。Citrix SD-WAN WANOP インスタンスの場合、次のオプションを使用してジョブを作成できます。

- **構成テンプレート:** 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、それを使用してジョブを設定できます。
- **組み込みテンプレート:** 構成テンプレートのリストから選択できます。これらのテンプレートには CLI コマンドの構文が用意されており、変数の値を指定できます。組み込みテンプレートは、説明とともに下の表に一覧表示されます。
- **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、ジョブを作成できます。

ジョブを作成したら、ジョブをすぐに実行するか、後で実行するようにジョブをスケジュールするかを選択できます。また実行頻度も設定できます。

組み込みテンプレート	説明
EnableCloudBridgeWANOpt	Citrix SD-WAN WANOP アプライアンスを介したトラフィックを有効にします。
DisableCloudBridgeWANOpt	Citrix SD-WAN WANOP アプライアンスを経由するトラフィックを無効にします。
RestartCloudBridgeWANOpt	Citrix SD-WAN WANOP アプライアンスを再起動します。
RestoreConfig	Citrix SD-WAN WANOP アプライアンスの構成を復元します。
AddLink	リンクを作成または定義することで、SD-WAN WANOP アプライアンスはリンクの混雑や損失を防ぎ、トラフィックシェーピングを実行できます。リンク上で送信または受信された最大帯域幅を定義でき、LAN 側または WAN 側のトラフィックを指定することもできます。帯域幅の制限と他の帯域幅管理の設定を設定します。
ConfigureBandwidth	
AddUser	特権を割り当てる新しいユーザーを追加します。
AddUserAdvancedPlatform	新しいユーザーを追加すると、 <a href="#">AddUser</a> テンプレートで使用できない権限を割り当てることができます。
AddService-class	1 つ以上のサービスクラスのフィルターを使用して、Citrix SD-WAN WANOP アプライアンスのサービスクラスを作成し、有効にします。

組み込みテンプレート	説明
SetApplication	アプリケーション分類子の定義を設定します。
AddorRemoveVideoCachingPorts	ビデオソースがデータを送受信するポート番号を追加または削除します。デフォルトポートは 80 です。
RemoveVideoCachingSource	1 つまたは複数のビデオキャッシュソースを削除します。ビデオソースの IP アドレスまたはドメイン名を指定します。
RemoveAllVideoCaching	すべての利用可能なビデオキャッシュソースを削除します。
VideoCachingState	Citrix SD-WAN WANOP アプライアンスのビデオキャッシュ機能を有効または無効にします。
ClearVideoCaching	ビデオキャッシュまたはビデオキャッシュ統計情報のいずれかをクリアします。
SetVideoCaching	キャッシュされるオブジェクトの最大サイズを設定します。この制限より大きなオブジェクトはキャッシュされません。デフォルトでは、キャッシュされるオブジェクトサイズは最大 100MB です。
AddVideoCachingSource	ビデオソースの IP アドレスまたはドメイン名を追加します。そのソースのビデオキャッシュを有効または無効にするオプションが含まれています。
ConfigureRemoteLicenseServer	集中ライセンスサーバーを構成します。ライセンスサーバーのモデル、IP アドレス、およびポート番号を指定します。
ConfigureLocalLicenseServer	ライセンスサーバーの場所をローカルに設定します。
InstallCACert	Citrix SD-WAN WANOP アプライアンスに CA 証明書をインストールします。証明書名、ファイル名、およびキーストアのパスワードを指定します。
InstallCombinedCerKey	統合された SSL 証明書とキーのペアファイルをインストールします。
InstallSeperateCertKey	SSL 証明書とキーを別のファイルとしてインストールします。
EnableWCCP	WCCP 展開モードを有効にします。
AddWCCPServiceGroup	Citrix SD-WAN WANOP アプライアンスの新しい WCCP サービスグループ定義を追加します。
DisableWCCP	WCCP 展開モードを無効にします。
AddTrafficShapingPolicy	Citrix SD-WAN アプライアンスのトラフィックシェーピングポリシーを作成します。このポリシーはネットワーク帯域幅を制御します。

組み込みテンプレート	説明
SetTrafficShapingPolicy	Citrix SD-WAN WANOP アプライアンスのトラフィックシェーピングポリシーを変更します。このポリシーはネットワーク帯域幅を制御します。
AddVideoPrePopulation	事前のビデオのダウンロードとキャッシュを有効にする、ビデオの事前設定エントリを作成します。いつビデオをキャッシュするかも指定できます。
UpdateVideoPrePopulation	いつビデオをキャッシュするかを指定する、ビデオの事前設定エントリを変更します。
AddVideoPrePopulationNow	ビデオを即座にダウンロードしてキャッシュを有効にする、ビデオ事前設定を構成します。URL から動画をダウンロードしてキャッシュする方法を制御できます。
VideoPrePopulationState	ビデオの事前設定を変更、開始、更新、および削除します。
ConfigureSyslogServer	syslog サーバーの IP アドレスとポート番号を設定します。
ConfigureAlert	アラートレベルを構成します。

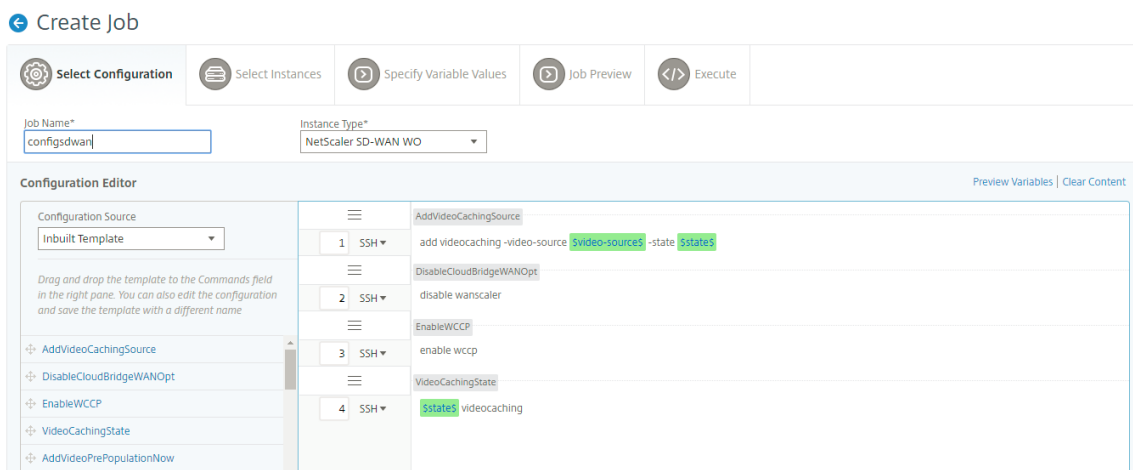
**Citrix SD-WAN WANOP** インスタンスの構成ジョブを作成するには:

1. Citrix ADM で、[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。
2. [ジョブの作成] ページの [構成の選択] タブで、[ジョブ名] を指定します。
3. 「インスタンスタイプ」フィールドで、「**Citrix SD-WAN WO**」を選択します。
4. 「構成ソース」ドロップダウンリストで、ジョブを作成するオプションを選択します。

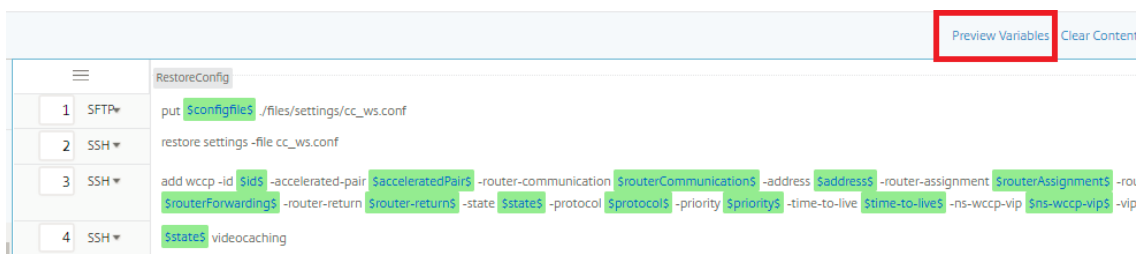
注

[構成テンプレートとして保存] を選択し、名前を指定して構成をテンプレートとして保存し、再利用します。

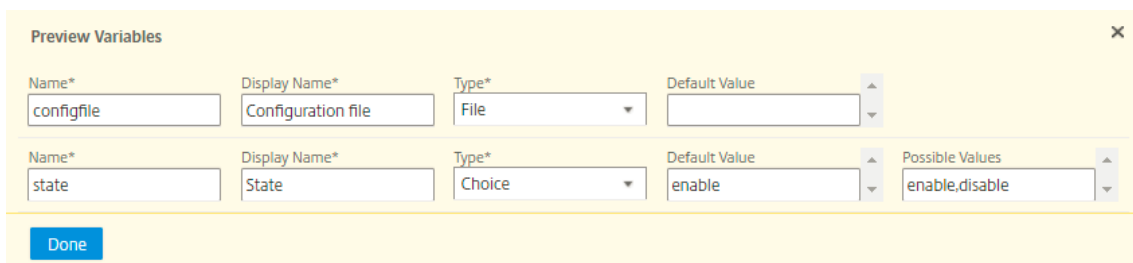




5. 構成ジョブの作成または編集集中に定義したすべての変数を、1つの統合ビューで確認できます。
6. 次のいずれかの操作を行って、すべての変数を1つの統合ビューに表示します。
  - 構成ジョブを作成するときに、[ネットワーク] > [構成ジョブ] に移動し、[ジョブの作成] を選択します。[ **Create Job** ] ページでは、構成ジョブの作成時に追加したすべての変数を確認できます。
  - 構成ジョブの編集集中に、[ネットワーク] > [構成ジョブ] に移動し、ジョブ名を選択して [編集] をクリックします。[ジョブの構成] ページでは、構成ジョブの作成時に追加されたすべての変数を確認できます。
7. 次に、「変数のプレビュー」(Preview Variables) タブをクリックして、設定ジョブの作成または編集集中に定義した1つの統合ビューで変数を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修正することもできます。パラメータを編集または変更したら、[完了] ボタンをクリックします。



9. [次へ] をクリックし、[インスタンスの選択] タブで [インスタンスの追加] をクリックします。ジョブを実行するインスタンスを選択し、「OK」をクリックします。

10. [次へ] をクリックし、[変数値を指定] タブで次のオプションのいずれかを選択して、インスタンスの変数を指定します。

- 変数値の入力ファイルをアップロード: 「入力キー ファイルをダウンロード」 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、コマンドで定義した変数の値を入力し、NetScaler ADM サーバーにファイルを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。選択したテンプレートによって、変数は変わります。

変数値を含む入力ファイルは、設定ジョブで (同じファイル名で) 保持されます。設定ジョブの作成または編集中に、以前に使用およびアップロードした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、「変数値の指定」タブで、「すべてのインスタンスの共通変数値」オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを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すでに実行されている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。[ジョブの設定] ページの [変数値の指定] タブで、[すべてのインスタンスの共通変数値] オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします (同じファイル名を使用)。

11. [次へ] をクリックし、[ジョブプレビュー] タブで、ジョブとして実行するコマンドを評価および確認できます。

12. [次へ] をクリックし、[実行] タブで、次の条件を設定します。

- コマンドが失敗した場合: コマンドが失敗した場合の対処方法: エラーを無視してジョブを続行するか、ジョブの実行を停止します。ボックスの一覧からアクションを選択します。
- 実行モード: ジョブをすぐに実行するか、後で実行をスケジュールします。後で実行するようにスケジュールを指定する場合、ジョブの実行頻度の設定を指定する必要があります。「実行頻度」ドロップダウン

ン・リストから、ジョブが従うスケジュールを選択します。

← Create Job

Select Configuration | Select Instances | Specify Variable Values | Job Preview | Execute

You can either execute the job now or schedule to execute the job at a later time. You must also select what action NetScaler MAS should take if a command fails.

On Command Failure\*  
 ▼

Execution Mode\*  
 ▼

Execution Settings  
 You can execute a job on a set of instances sequentially (one after the other), or in parallel (at the same time). If a job execution fails on any instance, it does not continue execution on the remaining instances.

Execute in Parallel  
 Execute in Sequence

Receive Execution Report Through  
 Email

Cancel | ← Back | Finish | Save and Exit

13. 「実行設定」で、ジョブを順番に実行するか（次々に）実行するか、並行して（同時に）実行するかを選択します。
14. ジョブ実行レポートを受信者のリストに電子メールで送信するには、[実行レポートの受信方法] セクションの [電子メール送信] チェックボックスをオンにします。表示されるボックスの一覧から電子メール配布リストを選択します。メール配信リストを作成するには、+ アイコンをクリックし、受信者のメールアドレスとメールサーバーの詳細を入力します。
15. [完了] をクリックします。

## マスター構成テンプレートの使用

February 6, 2024

メイン構成テンプレートの使用は、複数の NetScaler ADC インスタンスにマスター構成を作成して展開するための柔軟なオプションです。

管理者は、構成を変更し、ライセンス、証明書、およびその他のファイルを ADC インスタンスに保存することができます。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。

ADC インスタンスからマスター設定テンプレートを保存するには、次のいずれかの操作を行います。

- コマンドプロンプトに対して、**save ns config** と入力します。構成は、インスタンスのフラッシュメモリ内の /nsconfig/ns.conf ファイルに保存されます。
- インスタンスの GUI から、[診断] > [設定の表示] 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、インスタンスの保存済み設定を保存する場合は、[ **Saved configuration n** ] を選択します。「ファイルにテキストを保存」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デプロイする場合、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 ADC インスタンスごとにカスタマイズできます。

たとえば、管理者として、さらに ns.conf ファイルに ADC インスタンスに証明書キーをアップロードし、マスター設定もデプロイできます。

**重要**

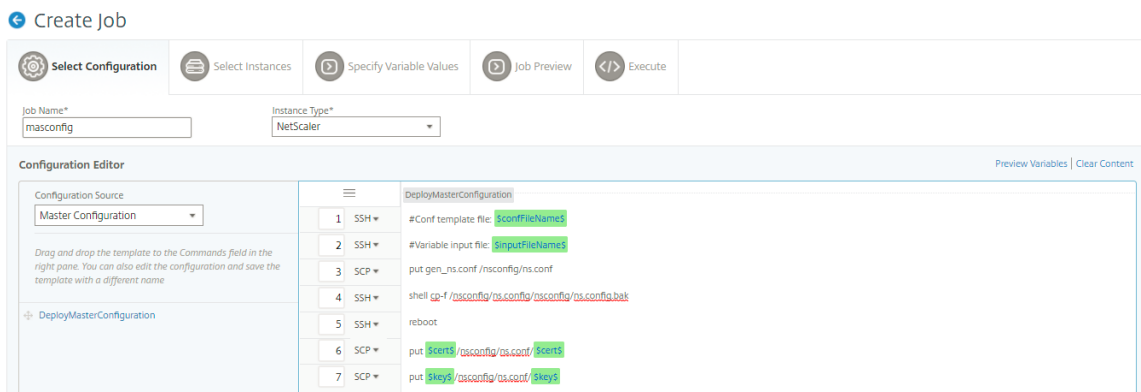
NetScaler ADC CPX インスタンス、クラスターで構成されたインスタンス、またはパーティション化された ADC インスタンスでは、DeployMasterConfiguration テンプレートを使用して構成ジョブを実行することはできません。

**NetScaler ADM** でマスター構成構成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. Citrix ADM で、[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。
2. [ **Create Job** ] ページの [ **Select Configuration** ] タブで、[ **Job Name** ] を指定し、ドロップダウンリストから [ **Instance Type** ] を選択します。
3. 「構成ソース」ドロップダウンリストから「マスター構成」を選択します。DeployMasterConfiguration テンプレートのコマンドを右側のペインにドラッグします。右側のペインでは、コマンドを追加、変更、削除することもできます。[次へ] をクリックします。

**注**

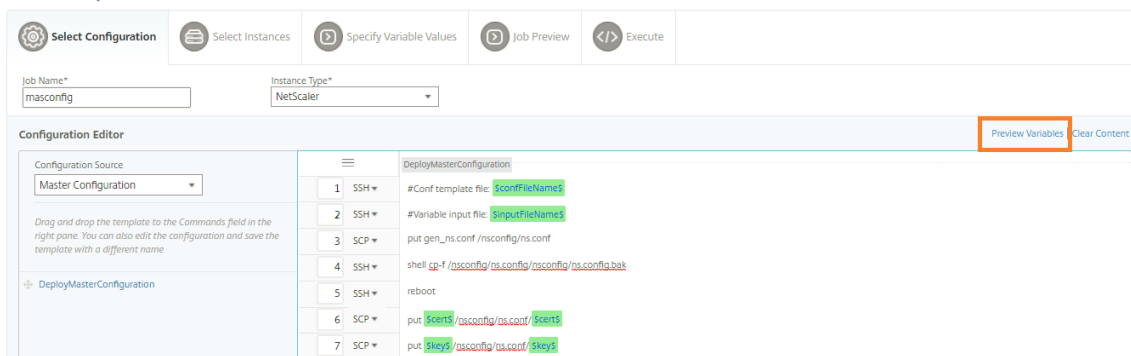
`put` コマンドを追加して、入力ファイルをテンプレートに追加できます。この例では、設定テンプレートファイルと変数入力ファイルに加えて、証明書とキーファイルをアップロードする必要があります。



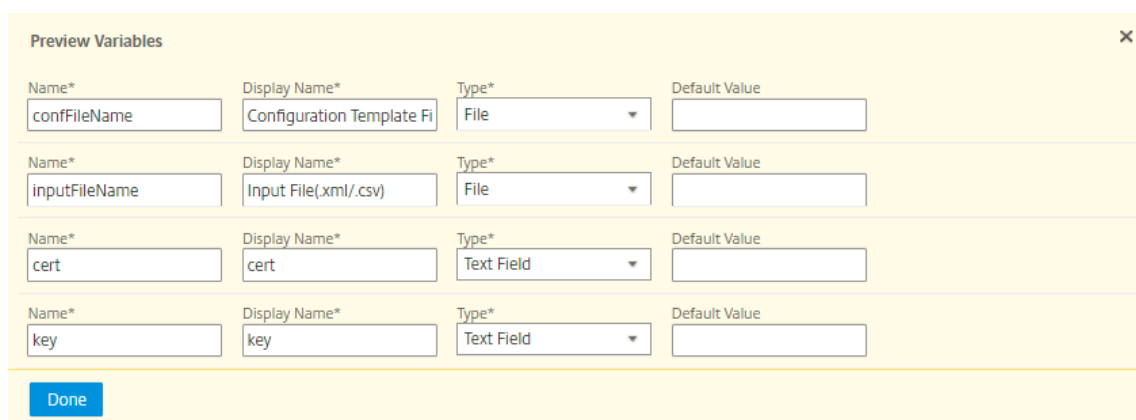
4. 構成ジョブの作成または編集集中に定義したすべての変数を、1つの統合ビューで確認できます。
5. 次のいずれかの操作を行って、すべての変数を1つの統合ビューに表示します。
  - 構成ジョブを作成するときに、[ネットワーク] > [構成ジョブ] に移動し、[ジョブの作成] を選択します。[ **Create Job** ] ページでは、構成ジョブの作成時に追加したすべての変数を確認できます。
  - 構成ジョブの編集集中に、[ネットワーク] > [構成ジョブ] に移動し、ジョブ名を選択して [編集] をクリックします。[ジョブの構成] ページでは、構成ジョブの作成時に追加されたすべての変数を確認できます。

6. 次に、「変数のプレビュー」(Preview Variables) タブをクリックして、設定ジョブの作成または編集集中に定義した 1 つの統合ビューで変数をプレビューできます。

← Create Job



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が表示されます。これらのパラメータを編集および修正することもできます。パラメータを編集または変更したら、[完了] 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. [ 変数値の指定 ] タブで、次のファイルをアップロードします。

- 設定テンプレートファイル (**.conf**) -ADC インスタンスから抽出した.conf ファイルをアップロードします。
- 入力ファイルのアップロード (**.xml/csv**) -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。

ここでは、使用例としてサンプルの xml ファイルを用意しています。xml ファイルに、使用している ADC インスタンスに対応する詳細が含まれていることを確認します。

```

1 <?xml version="1.0" encoding="UTF-8" ?>
2
3 <properties>
4
5 <!--

```

```
6
7 Provide inputs for all the parameters defined in the master config
  file.
8
9 - global. This tag contains all the common parameters and value.
10
11 - devicegroup. This tag contains all the instance group specific
  parameters and values.
12
13 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.
14
15 - name. This attribute represents the name of the instance group.
16
17 - device. This tag contains all the instance specific parameters
  and value.
18
19 If the same parameters are defined in global and instance tags,
  the instance specific parameters value will take precedence in
  the execution.
20
21 - name. This attribute represents the IP Address of the instance.
  Host name is not supported for the attribute.
22
23 HA pair should be represented as <primaryip>-<secondaryip>.
  Example 10.102.2.1-10.102.2.2
24
25 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.
26 -->
27
28 <global>
29
30 </global>
31 <devicegroup name="BLR_DEVS">
32 </devicegroup>
33 <device name="10.106.101.209">
34 <param name="IP" value="10.106.101.209"/>
35 </device>
36
37 <!-- HA PAIR-->
38 <!--<device name="10.102.43.154-10.102.43.155">
39 <param name="NSIP" value="10.102.43.154"/>
40 <param name="HostName" value="NS43HA"/>
41 <param name="LBSERVER" value="haserver43http"/>
42 <param name="SNMPTrapDest" value="10.102.43.130"/>
43 </device-->
44 </properties>
45
```

```
46 <!--NeedCopy-->
```

10. [次へ] をクリックします。

## ← Create Job

The screenshot shows the 'Create Job' wizard with the 'Specify Variable Values' step selected. The interface includes a progress bar at the top with icons for 'Select Configuration', 'Select Instances', 'Specify Variable Values', 'Job Preview', and 'Execute'. Below the progress bar, there are two file selection fields: 'Configuration Template File(.conf)\*' and 'Input File(.xml/.csv)\*', each with a 'Choose File' button. At the bottom, there are four buttons: 'Cancel', 'Back', 'Next', and 'Save and Exit'.

変数値を含む入力ファイルは、設定ジョブで (同じファイル名で) 保持されます。設定ジョブの作成または編集中に、以前に使用およびアップロードした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中の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。[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] オプションを選択し、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、ファイルを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実行済みの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。[ジョブの設定] ページの [変数値の指定] タブで、[すべてのインスタンスに共通変数値] オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを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)。

1. [ **Job Preview** ] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価して確認し、[ **Next** ] をクリックします。

← Create Job

Select Configuration    Select Instances    Specify Variable Values    **Job Preview**    Execute

Select an instance or instance group to preview

10.106.43.177

Preview of Job on the Instance 10.106.43.177

```
[Task ns.conf for 10.106.43.177]
set ns config -IPAddress 10.106.43.177 -netmask 255.255.255.0
enable ns mode FR L3 Edge USNIP PMTUD
set system parameter -doppler DISABLED
set system user nsroot 1d88eecb931c4166b9891fbbaf242260116f9e59ec171716 -encrypted
set rsskeytype -rsstype ASYMMETRIC
set lacp -sysPriority 32768 -mac 3a:52:5f:a6:af:70
set interface 1/1 -throughput 0 -bandwidthHigh 0 -bandwidthNormal 0 -intftype "Xen Virtual" -ifnum 1/1
set interface LO/1 -haMonitor OFF -throughput 0 -bandwidthHigh 0 -bandwidthNormal 0 -intftype Loopback -ifnum LO/1
add ns ip6 fe80::3852:5fff:fea6:af70/64 -scope link-local -type NSIP -vian 1 -vServer DISABLED -mgmtAccess ENABLED -dynamicRouting ENABLED
set ipsec parameter -lifetime 28800
set nd6RAvariables -vian 1
add snmp community public123 ALL
add snmp community kii all
add vian 233
set snmp alarm APPFW-BUFFER-OVERFLOW -timeout 1
```

2. **[Execute]** タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。コマンドが失敗した場合に NetScaler ADM が実行する必要があるアクションを選択することもできます。
- また、承認されたユーザーが管理対象インスタンスでジョブを実行できるようにすることもできます。また、ジョブの成功または失敗に関する電子メール通知を他の詳細とともに送信するかどうかを選択できます。



ジョブの実行後、[ネットワーク]>[構成ジョブ]に移動して、設定したジョブを選択すると、ジョブの詳細を確認できます。[詳細]をクリックし、[実行の概要]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 **Command Logs** を表示して、ジョブで実行されたコマンドを確認します。

Command Log		
Status	Command	Message
✓	put /var/mps/tenants/root/config_mgmt/MySSLCert.crt /nsconfig/ssl/MySSLCert.crt	Done
✓	put /var/mps/tenants/root/config_mgmt/MySSLCertKey.key /nsconfig/ssl/MySSLCertKey.key	Done
✓	shell cp -f /nsconfig/ns.conf /nsconfig/ns.conf.bak	Done
✓	#Conf template file: NS12_0_41_Template.conf	Done
✓	#Variable input file: NS12_0_41_AnswerKey.xml	Done
✓	put /var/mps/tenants/root/config_mgmt/ns_#7A818EB30E94FAA36144CC5F0782E06A13C3122F6BC67B32190444FC6F06.conf /nsconfig/ns.conf	Done
✓	shell	Done
✓	reboot	Done

## ジョブを使用して **NetScaler ADC** インスタンスをアップグレードする

February 6, 2024

NetScaler Application Delivery Management (ADM) を使用して、1つ以上の NetScaler ADC 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タイプを知っておく必要があります。

メンテナンスジョブを作成して NetScaler ADC インスタンスをアップグレードする場合は、アップグレードするインスタンスに対して事前検証チェックを実行します。

1. カスタマイズをチェックする -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。
2. ディスク使用量の確認 - /var フォルダの容量が 6 GB 未満で、/flash フォルダの容量が 200 MB 未満の場合は、ディスク容量をクリーンアップします。次のフォルダパスを確認して、ディスク容量を空けてください。

- /var/nstrace
- /var/log
- /var/nslog
- /var/tmp/support
- /var/core
- /var/crash
- /var/nsinstall
- /var/netscaler/nsbackup

3. ディスクハードウェアの問題の確認 -ハードウェアの問題があれば解決します。

ADC HA 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. 後で残りのノードで実行するようにアップグレードジョブをスケジュールします。最初のノードのアップグレード後に、必ずこのジョブをスケジュールしてください。

ADC HA ペアをアップグレードするときは、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。
- ノードの同期と伝播は、両方のノードが正常にアップグレードされるまで無効になります。
- HA ペアのアップグレードが成功すると、実行履歴にエラーメッセージが表示されます。このメッセージは、HA ペアのノードのビルドまたはバージョンが異なる場合に表示されます。このメッセージは、1 次ノードと 2 次ノード間の同期が無効になっていることを示します。

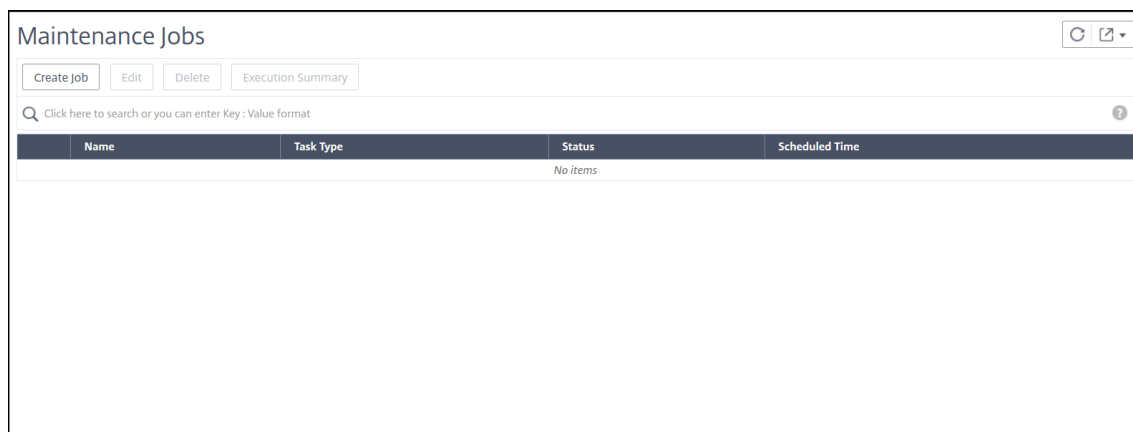
ADC クラスターをアップグレードすると、ADM は指定されたインスタンスでのみアップグレード前の検証を行います。アップグレードする前に、クラスターノードのカスタマイズ、ディスク使用量、およびハードウェアの問題を確認して解決してください。

### **ADC** インスタンスをアップグレードするためのアップグレードメンテナンスジョブの作成

注

上位バージョンから下位バージョンへの ADC のアップグレードはサポートされていません。たとえば、NetScaler ADC インスタンスが 13.0 82.x の場合、ADC インスタンスを 13.0 79.x または他の以前のバージョンにダウングレードすることはできません。

1. Citrix ADM で、[ネットワーク] > [構成ジョブ] > [メンテナンスジョブ] に移動します。[ジョブの作成] ボタンをクリックします。



2. [メンテナンスジョブの作成] で、[NetScaler ADC (スタンドアロン/高可用性/クラスタ) のアップグレード] を選択し、[続行] をクリックします。

## ← Create Maintenance Job

Select a task to create Maintenance Job\*

Upgrade NetScaler (Standalone/High-Availability/Cluster)

Upgrade NetScaler SDX

Upgrade NetScaler BLX

Upgrade AutoScale Group

Configure HA Pair of NetScaler Instances

Convert HA Pair of Instances to 2 Node Cluster

Proceed
Close

3. [インスタンスの選択] で、[ジョブ名] に任意の名前を入力します。
4. [Add Instances] をクリックして、アップグレードする ADC インスタンスを追加します。
  - HA ペアをアップグレードするには、プライマリノードまたはセカンダリノードの IP アドレスを指定します。

- クラスターをアップグレードするには、クラスターの IP アドレスを指定します。

5. [ **Next** ] をクリックして、選択したインスタンスでアップグレード前の検証を開始します。

[アップグレード前の検証] 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て、[次へ] をクリックします。

インスタンスのディスク領域が不足している場合は、ディスク領域を確認してクリーンアップできます。「ADC のディスク領域をクリーンアップする」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、ADM は、他のクラスターノードではなく、指定されたインスタンスでのみアップグレード前の検証を行います。

6. 必要に応じて、[カスタムスクリプト] で、インスタンスのアップグレードの前後に実行するスクリプトを指定します。次のコマンドを実行するには、次のいずれかの方法を使用します。

カスタムスクリプトは、ADC インスタンスのアップグレードの前後に変更をチェックするために使用されます。次に例を示します:

- アップグレード前とアップグレード後のインスタンスのバージョン。
- アップグレード前後のインターフェイス、高可用性ノード、仮想サーバ、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。
- ダイナミックルート。

インスタンスのアップグレードには、複数のステージがあります。これで、これらのスクリプトを次の段階で実行するように指定できます。

- アップグレード前: インスタンスをアップグレードする前に、指定されたスクリプトが実行されます。
- アップグレード前のフェールオーバー後 (**HA** に適用可能): このステージは、高可用性配置にのみ適用されます。指定されたスクリプトは、ノードのアップグレード後、フェールオーバーの前に実行されません。
- アップグレード後 (スタンドアロンに適用) / フェールオーバー後のアップグレード後 (**HA** に適用可能): 指定されたスクリプトは、スタンドアロンデプロイでインスタンスをアップグレードした後に実行されます。高可用性展開では、スクリプトはノードとフェールオーバーをアップグレードした後に実行されます。

**注:**

必要な段階でスクリプトの実行を有効にしてください。そうしないと、指定されたスクリプトは実行されません。

ADM GUI では、スクリプトファイルをインポートしたり、コマンドを直接入力したりできます。

- ファイルからコマンドをインポートする: ローカルコンピュータからコマンド入力ファイルを選択します。

- コマンドの入力: **GUI** 上でコマンドを直接入力します。

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スクリプトを使用できます。

← Upgrade NetScaler

Select Instances Select Image Pre-upgrade Validation **Custom Scripts** Schedule Task Create Job

Specify the scripts/commands to do pre and post instance upgrade validations at various stages. The scripts/commands output is sent to the configured email distribution list/slack channel. The diff reports are generated only if you specify the same script in the pre and post upgrade stages.

▼ Pre upgrade

Enable Script/Command Execution

Import commands from file  Type commands

Command Input File

Choose File

▼ Post upgrade pre failover (applicable for HA)

Enable Script/Command Execution

Use same script as Pre upgrade  Import commands from file  Type commands

```

1 show arp
2 show neighbors
3 show ha nodes
4 show ha node-summary
5 show servicegroup
    
```

▼ Post upgrade (applicable for Standalone/Cluster) / Post upgrade post failover (applicable for HA)

Enable Script/Command Execution

Use same script as Pre upgrade  Import commands from file  Type commands

Cancel Back **Next** Skip

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実行されます。
- ADC HA ペアを 2 段階でアップグレードする場合は、[ 高可用性のノードに対して 2 段階アップグレードを実行する] を選択します。

HA ペアの別のインスタンスをアップグレードする場合は、[ **Execution Date** ] と [ **Start Time** ] を指定します。

8. 「ジョブの作成」で、次の詳細を指定します。

a) [ ソフトウェアイメージ ] リストから次のオプションのいずれかを選択します。

- 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 -ADM ファイルブラウザからインスタンスのアップグレードファイルを選択します。ADM GUI には、`/var/mps/ns_images` に存在するインスタンスファイルが表示されます。

- b) イメージをインスタンスにアップロードするタイミングを指定します。
- 今すぐアップロード -画像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。
  - アップグレードの成功時に **NetScaler ADC** 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に ADC インスタンスでアップロードされたイメージをクリアするには、このオプションを選択します。
  - アップグレードを開始する前に、**ADC** インスタンスをバックアップしてください。: 選択した ADC インスタンスのバックアップを作成します。
  - アップグレード後に **HA** ノードのプライマリおよびセカンダリステータスを維持する: 各ノードのアップグレード後にアップグレードジョブでフェールオーバーを開始する場合は、このオプションを選択します。このようにして、アップグレードジョブはノードのプライマリとセカンダリのステータスを維持します。
  - アップグレード開始前に **ADC** 設定を保存-**ADC** インスタンスをアップグレードする前に、実行中の ADC 設定を保存します。
  - **ISSU** を有効にして、**ADC HA** ペアでのネットワーク停止を回避する -ISSU は、ADC 高可用性ペアでのダウンタイムなしの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使用する移行機能を提供します。したがって、ダウンタイムなしで ADC HA ペアをアップグレードできます。ISSU 移行タイムアウトを分単位で指定します。
  - 実行レポートを電子メールで受信する-実行レポートを電子メールで送信します。電子メール配布リストを追加するには、「[電子メール配布リストを作成する](#)」を参照してください。
  - **slack** による実行レポートの受信-実行レポートを slack で送信します。Slack プロフィールを追加するには、[Slack プロフィールを作成する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、[ネットワーク] > [構成ジョブ] > [メンテナンスジョブ] に表示されます。既存のジョブを編集するときに、必須フィールドにすでに入力されている場合は、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] タブが表示されている場合は、[ジョブプレビュー] タブに切り替えることができます。

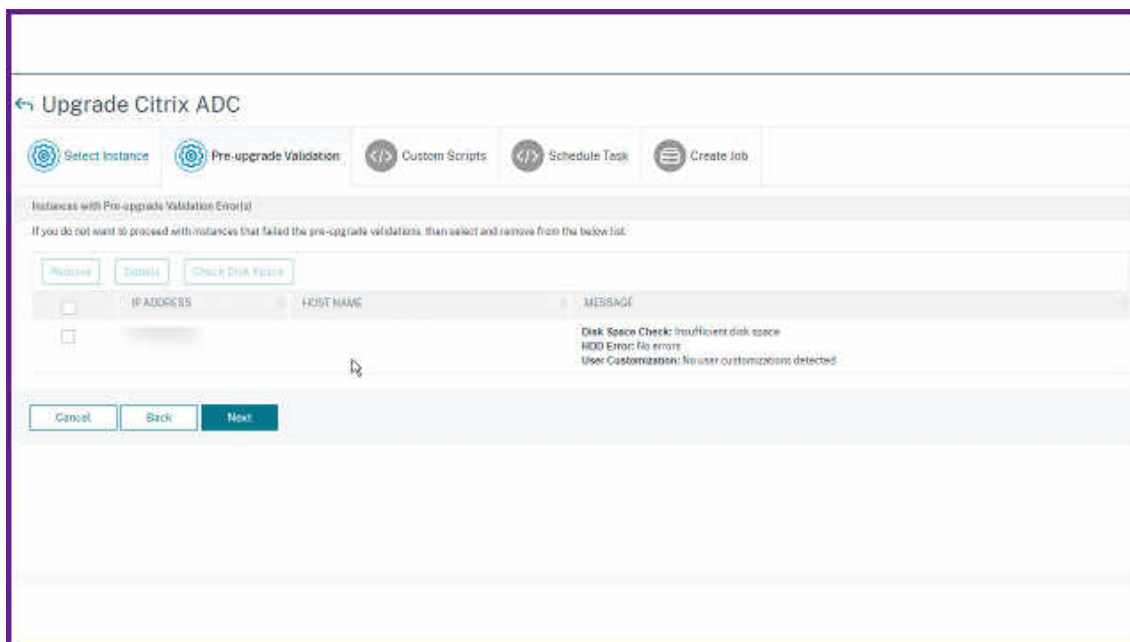
### ADC ディスク領域をクリーンアップする

ADC 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、ADMGUI 自体からディスク領域をクリーンアップしてください。

1. [アップグレード前の検証] タブで、ディスク領域の問題があるインスタンスを選択します。
2. [ディスク領域の確認] を選択します。

このペインには、容量の少ないインスタンスのディスクが表示されます。また、ディスク上で使用され、使用可能なメモリの量も表示されます。

3. [ **Check Disk Space** ] 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ます。
4. [ ディスククリーンアップ ] をクリックします。



5. 消去するファイルを選択します。

6. [削除] をクリックします

### ADC アップグレード・ジョブの統合差分レポートのダウンロード

カスタムスクリプトが指定されている場合は、ADC アップグレードジョブの相違レポートをダウンロードできます。差分レポートには、アップグレード前スクリプトとアップグレード後のスクリプトの出力の違いが含まれます。このレポートを使用すると、アップグレード後に ADC インスタンスで発生した変更を確認できます。

注:

相違レポートが生成されるのは、アップグレード前および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のみです。

アップグレードジョブの相違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. [ネットワーク] > [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. 「相違レポート」をクリックします。
4. 相違レポートで、選択したアップグレードジョブの統合差分レポートをダウンロードします。

このページでは、次の相違レポートの種類をダウンロードできます。

- アップグレード前とポストアップグレード前のフェイルオーバー差分レポート
- アップグレード前とアップグレード後の差分レポート



Diff Reports <span style="float: right;">🔄 📄</span>		
Download a consolidated diff report of the upgrade job.		
<input type="button" value="Pre vs Post upgrade pre failover diff report"/> <input type="button" value="Pre vs Post upgrade diff report"/>		
<input type="text" value="Click here to search or you can enter Key : Value format"/> <span style="float: right;">🔍</span>		
IP ADDRESS	PRE VS POST UPGRADE PRE FAILOVER	PRE VS POST UPGRADE
10.10.10.10	↓ Diff Report	↓ Diff Report
10.10.10.10	↓ Diff Report	↓ Diff Report
Total 2		25 Per Page Page 1 of 1

## 構成テンプレートを使用した監査テンプレートの作成

February 6, 2024

以前に構成テンプレートとして保存した構成コマンドを使用して、特定の NetScaler ADC 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、以前に保存した設定テンプレートを [Commands] 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 ADC インスタンスに適用できます。NetScaler ADM は、これらのインスタンスを監査テンプレートと比較し、不一致を報告します。このプロセスは、エラーを識別し、直ちに修正するために役立ちます。

ジョブを作成し、一連の構成コマンドをテンプレートとして保存するときに、構成テンプレートを作成できます。これらのテンプレートを [ジョブの作成] ページで保存すると、[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、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その仮想サーバーにバインドするという、基本的な負荷分散構成を考えてみましょう。

この例では、次のコマンドを使用します。

```
add lb vserver <servername> HTTP <ipaddress portnumber>
add service <servicename1 ipaddress1> HTTP 80
add service <servicename2 ipaddress2> HTTP 80
bind lb vserver <servername servicename1>
bind lb vserver <servername servicename2>
```

**NetScaler ADM** で構成テンプレートを保存するには：

1. [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。
2. [Create Job] ページで、ジョブ名とインスタンスタイプを指定します。
3. 構成ソースとして [Configuration Template] を選択し、[Commands] フィールドに上記の例のようなコマンドを入力します。

4. [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。同じ名前が付いた他のテンプレートが存在する場合はそれを上書きすることを選択できます。

5. [保存] をクリックします。

The screenshot shows the Configuration Editor interface. At the top, there are fields for 'Job Name\*' (containing 'LB Variables') and 'Instance Type\*' (containing 'NetScaler'). Below this is the 'Configuration Editor' section, which is divided into a left pane for 'Configuration Source' (set to 'Configuration Template') and a right pane for 'Commands'. The right pane contains several SSH commands for adding and binding services. At the bottom, a dialog box is open, highlighted with a red border. The dialog has a checked checkbox 'Save as Configuration Template', a text input field containing 'LBVariablesTemplate', an unchecked checkbox 'Overwrite if exists', and 'Save' and 'Cancel' buttons.

構成テンプレートを使用して **NetScaler ADM** で監査テンプレートを作成するには:

1. [ネットワーク]>[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、テンプレート名の名前を指定し、説明を入力します。
3. [構成ソース] ボックスの一覧から [構成テンプレート] を選択し、右側のペインの [コマンド] フィールドにテンプレートをドラッグします。構成を編集し、テンプレートを別の名前でも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 [インスタンスを追加] をクリックし、設定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。

← Create Template

Audit Commands Select Instances

Template Name\* LBVariableTemplate Description Create LB server with variables

Configuration Editor

Configuration Source Configuration Template

Drag and drop the template to the Commands field in the right pane. You can also edit the configuration and save the template with a different name

LBVariablesTemplate

```
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
```

Cancel Next →

監査テンプレートは、[Audit Templates] ボックスの一覧に表示され、指定し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。

## 設定ジョブで **SCP (put)** コマンドを使用する

February 6, 2024

Citrix ADM の構成ジョブ機能を使用して、構成ジョブの作成、電子メール通知の送信、作成されたジョブの実行ログの確認を行うことができます。ジョブとは、管理対象インスタンスに対して作成および実行できる構成コマンドのセットです。たとえば、デバイスのアップグレードのために構成ジョブを使用できます。

NetScaler ADM の構成ジョブでは、Secure Shell (SSH) コマンドを使用してインスタンスを構成し、Secure Copy (SCP) を使用してファイルを安全に転送するように構成ジョブを構成できます。SCP は、SSH プロトコルに基づいています。設定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、システムのローカルディレクトリに保存されている 1 つ以上のファイルを NetScaler ADM にアップロードまたは転送し、次に NetScaler ADC インスタンスまたは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 Citrix ADM にアップロードされ、後で選択した Citrix ADC インスタンスにコピー（配置）されます。アップロードされたファイルは NetScaler ADM に保存され、ジョブが削除されたときにのみ削除されます。これは、後で実行するようにスケジュールされているジョブに必要です。

このコマンドの構文を次に示します：

```
put <local_filename> <remote_path/remote_filename>
```

各項目の意味は次のとおりです。

<local\_filename> は、アップロードするローカルファイルの名前です。

<remote\_path/remote\_filename> はリモートディレクトリへのパスと、そのディレクトリにコピーされるときにファイルに割り当てる名前です。

構成ジョブの作成中に、ローカルファイル名と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 ADC 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、1 つのファイルをジョブ内の複数の位置で使用しており、そのファイルの名前を変更する必要がある場合は、すべての位置でファイル名を変更するのではなく、変数を再定義できます。

**put** コマンドを使用して、設定ジョブで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。

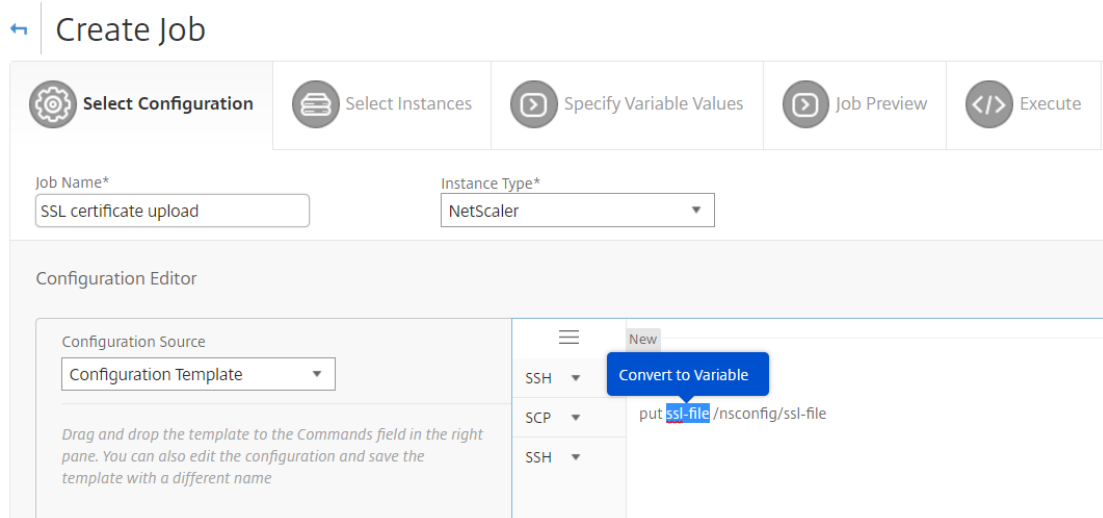
1. [ネットワーク]>[構成ジョブ]に移動します。
2. [ジョブ] ページで、[ジョブの作成] をクリックします。
3. [ジョブの作成] ページで、[ジョブ名] フィールドにジョブの名前を入力し、[構成エディタ] ペインで [put] コマンドを入力します。

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 ADC インスタンスにコピーする構成ジョブを作成する場合は、特定のファイルの名前の代わりに変数を使用する「put」コマンドを追加し、変数の種類を「file」として定義できます。

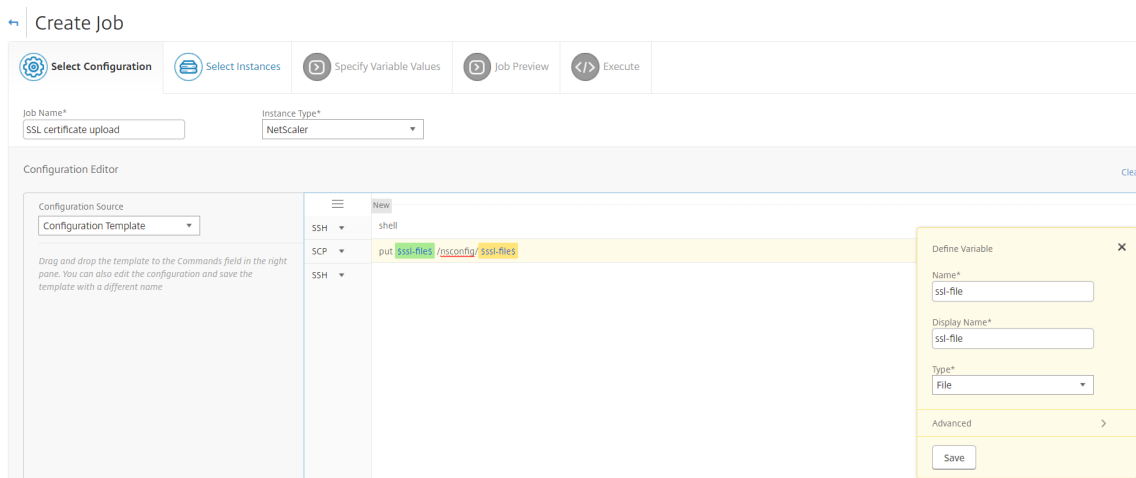
```
put ssl-file /nsconfig/ssl-file
```

この例の説明を次に示します。

- `ssl-file` -NetScaler ADC 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です。
4. 次の図に示すように、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。



5. ファイル名がドル記号 (現在の変数であることを示す) で囲まれていることを確認し、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. [タイプ] ドロップダウンリストから [ファイル] を選択します。[保存] 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、ファイルを NetScaler ADM にアップロードできます。



8. [次へ] をクリックし、ファイルのコピー先となる NetScaler ADC インスタンスを選択します。
9. [変数値の指定] タブで、[すべてのインスタンスの共通変数値] 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、[アップロード] をクリックして NetScaler ADM にファイルをアップロードし、[次へ] をクリックします。

10. **[Job Preview]** タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。
11. **[Execute]** タブでは、ジョブを今すぐ実行することも、後で実行するようにスケジュールすることもできます。コマンドが失敗した場合に NetScaler ADM が実行する必要があるアクションを選択することもできます。また、ジョブの成功または失敗、およびその他の詳細について通知を受け取るように、メール通知を作成できます。[完了] をクリックします。
12. ジョブの詳細を表示するには、[ネットワーク] > [構成ジョブ] に移動し、設定したジョブを選択します。[詳細] をクリックし、[変数の詳細] をクリックして、ジョブに追加された変数を一覧表示します。

Job Details

Configuration Parameters	Name SSL certificate upload	Instance Type NetScaler	Commands z
Execution Summary	Instances 1	Last Execution May 04 4:49 PM	100% Complete (1 out of 1 Instances)
Variable Details	Variables 1		
Execution Parameters	Execution Frequency Once	Next Execution N/A	Execute Commands In Parallel

**Variable Details**

Variables  
1

Variable	Display Name
ssl-file	ssl-file

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

February 6, 2024

Citrix Application Delivery Management (ADM) の組み込みテンプレートを使用して、スケジュールしたジョ

ブを再スケジュールできます。たとえば、コマンドが失敗した場合に NetScaler ADM が実行する必要があるアクションを変更できます。エラーを無視して続行するように設定していた場合、その設定を、1つのコマンドが失敗したらすべての成功したコマンドをロールバックするように変更できます。

**NetScaler ADM** で組み込みテンプレートを使用して構成されたジョブを再スケジュールするには

1. NetScaler ADM で、[ネットワーク] > [構成ジョブ] に移動します。
2. インスタンスを編集、追加、または削除するジョブを選択し、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. **[Finish]** 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 **[Execute Again]** をクリックすると、ソース、インスタンス、コマンドを変更せずにジョブを実行することもできます。この機能は、同じインスタンスで同じコマンドセットを実行する必要がある場合に便利です。場合によっては、ジョブがサーバー側から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。

## 構成ジョブでの構成監査テンプレートの再利用

February 6, 2024

管理者は、ジョブを作成して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。構成ジョブで作成および保存された構成テンプレートは、構成監査で使用して、特定の Citrix ADC 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ます。同様に、構成監査モジュールで作成された監査テンプレートは、構成ジョブとして実行できるように、構成ジョブで使用できます。テンプレート内で行われた変更は、構成ジョブモジュール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、構成ジョブテンプレートと構成監査テンプレートを同じ構成のために別々に作成し、別のファイルとして保存する必要がありました。このため、テンプレートの作成時と保守時に同じ作業を繰り返す必要がありました。

Citrix Application Delivery Management (ADM) では、このテンプレートをシステムに保存して、構成ジョブでも監査テンプレートを使用できるようにします。ここでは、監査テンプレートを構成ジョブの作成に使用できます。上記のように、テンプレートは、構成ジョブと構成監査との間で区別なく使用できます。

たとえば、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その仮想サーバーにバインドするという、基本的な負荷分散構成を考えてみましょう。

この例では、次のコマンドを使用します。

```
1 add lb vserver servername HTTP ipaddress portnumber
2
3 add service servicename1 ipaddress1 HTTP 80
4
5 add service servicename2 ipaddress2 HTTP 80
6
7 bind lb vserver servername servicename1
8
9 bind lb vserver servername servicename2
10 <!--NeedCopy-->
```

### 構成監査でのテンプレートの作成と構成ジョブでのその使用

次のタスクを実行して、構成監査モジュールでテンプレートを作成し、それを構成ジョブモジュールで再利用します。

監査テンプレートを作成するには、次の手順に従います。


1. NetScaler ADM で、[ネットワーク] > [構成監査] > [監査テンプレート] の順に選択し、[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、テンプレートの詳細情報を追加することもできます。
3. [ **Commands** ] ペインで、例のコマンドを入力します。
4. [構成テンプレートとして保存] チェックボックスをオンにし、テンプレートの名前を指定します。たとえば、このテンプレートに「LBVariablesTemplate」という名前を付けることができます。同じ名前が付いた他のテンプレートが存在する場合はそれを上書きすることを選択できます。


注: 監査テンプレート名は、設定テンプレート名と同じでもかまいません。

5. [保存] をクリックし、[次へ] をクリックします。



## ← Create Template

 **Audit Commands**

 Select Instances

Template Name\*

Description

**Configuration Editor**

Configuration Source

Configuration Template ▾

*Drag and drop the template to the Commands field in the right pane. You can also edit the configuration and save the template with a different name*

✦ config-template2

✦ config-template1

New

```

shell
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
                    
```

Save as Configuration Template

LBVariablesTemplate

Overwrite if exists

Save

Cancel

Cancel

Next →

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 **Citrix ADC** 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一覧に表示されるようになります。

## Audit Templates

<input type="checkbox"/>	Template Name	Description
<input type="checkbox"/>	LBVariablesTemplate	Basic load balancing configuration to add a load balancing virtual server
<input type="checkbox"/>	config-template2	abc
<input type="checkbox"/>	abc	

8. これらの構成コマンドを実行する場合は、[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。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一覧に表示されます。

構成ジョブで監査テンプレートを再利用するには、次の手順に従います。

1. ジョブの名前を入力し、インスタンスタイプを選択し、テンプレートをコマンドペインにドラッグします。  
構成ジョブの作成中に、ローカルファイル名と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 ADC 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。
2. 入力したコマンドで、変数に変換するファイル名を選択し、[変数に変換] をクリックします。
3. [ **Select Instances** ] 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. コマンドで 変数を指定した場合は、[ **Specify Variable Values** ] タブで、次のいずれかのオプションを選択して、インスタンスの変数を指定します。
  - 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 Citrix ADM サーバーにアップロードします。
  - [Common variable values for all instances] - 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して、「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。この時点で、別のサービスをこの負荷分散サーバーに追加して、そのサービスをそのサーバーにバインドする必要がある場合は、コマンドページでコマンドを編集し、保存することができます。
7. 「監査テンプレート」にナビゲートし、「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。そのテンプレートが新しいコマンドで更新されたことがわかります。

監査テンプレートは、[Audit Templates] ボックスの一覧に表示され、指定し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、構成ジョブモジュールと構成監査モジュールとの間で再使用できるようになりました。

## 構成テンプレートのインポートとエクスポート

February 6, 2024

構成テンプレートは、どの Citrix Application Delivery Management (ADM) からでもエクスポートできます。また、将来いつでも同じまたは別の Citrix ADM にファイルをインポートできます。設定テンプレートデータ (設定コマンド、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** ファイル形式にエクスポートし、ローカルフォルダに保存できます。構成テンプレートをインポートできます。**JSON** ファイルを Citrix ADM に保存します。このファイルは新しい場合もあれば、同じまたは別の Citrix ADM からエクスポートしたファイルである場合もあります。

構成テンプレートをエクスポートするには、次の手順に従います。

1. [ネットワーク] > [構成ジョブ] > [構成テンプレート] に移動します。
2. [Add] ボタンをクリックして、設定テンプレートを作成します。
3. [Create Configuration Template] ページで、設定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。[構成エディタ] で、ドロップダウンメニューから [構成テンプレート] として構成ソースを選択します。既存の構成テンプレートを構成エディターにドラッグできます。[作成] をクリックします。

Configuration Editor

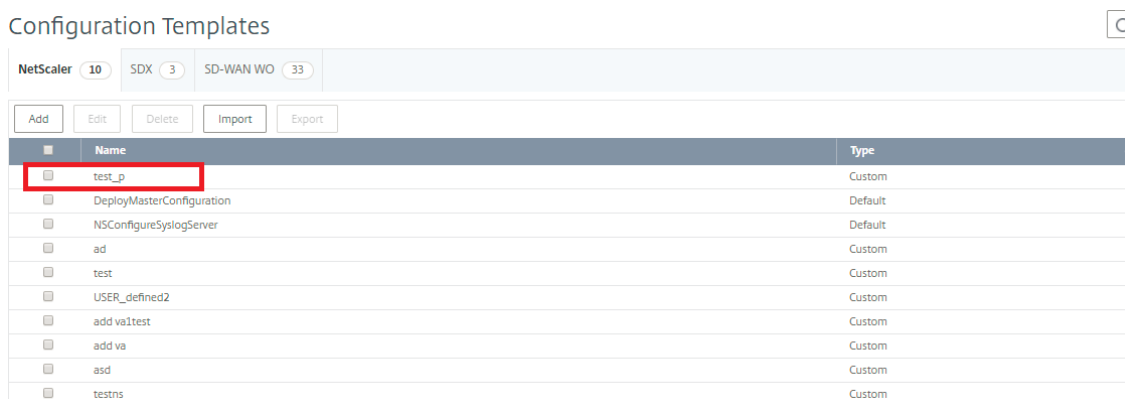
Configuration Source: Configuration Template

Drag and drop the template to the Commands field in the right pane. You can also edit the configuration and save the template with a different name

		USER_defined2
1	SSH	add vlan 50
2	SSH	add vlan 89

Buttons: Create, Close

4. [ネットワーク] > [構成ジョブ] > [構成テンプレート] に移動して、構成テンプレートのリストに作成されたテンプレートを表示します。

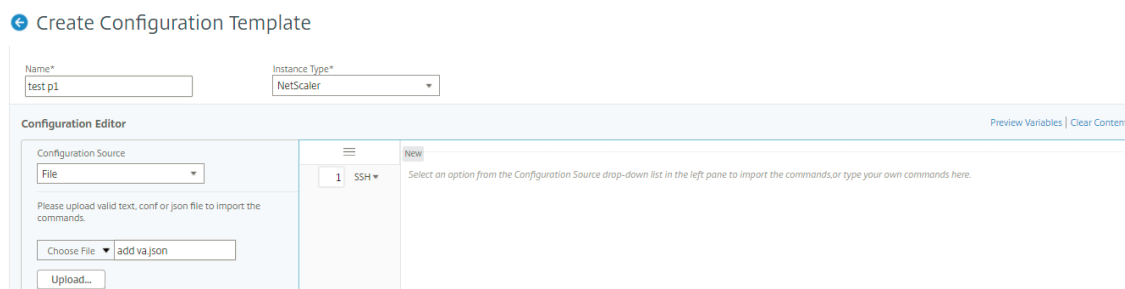


5. 新しく作成した構成テンプレートを選択し、[ **Export** ] ボタンをクリックします。

対応する構成テンプレートが **.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、次の手順に従います。

1. [ ネットワーク ] > [ 構成ジョブ ] > [ 構成テンプレート ] に移動し、[ インポート ] ボタンをクリックします。構成テンプレートの **.json** ファイルがあるパスを選択し **.json** ファイルをアップロードします。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お勧めします。
2. 構成エディターの [ ファイル ] オプションを使用して構成テンプレートをインポートすることもできます。
3. 構成エディターのドロップダウンメニューから [ ファイル ] を選択します。
4. [ ファイルを選択 ] (**.json files**) をローカルシステムからアップロードし、設定テンプレートをアップロードします。 **JSON** ファイル。



注

- 新しくインポートされたテンプレートはすべて、新しい ID 文字列で保存されます。
- 構成テンプレートをインポートできるのは、ファイルが **json** 形式で保存されている場合だけです。**.json** ファイル以外の構成テンプレートをローカルシステムからインポートすると、エラーが表示され、ファイルのインポートに失敗します。

## メンテナンス・ジョブ

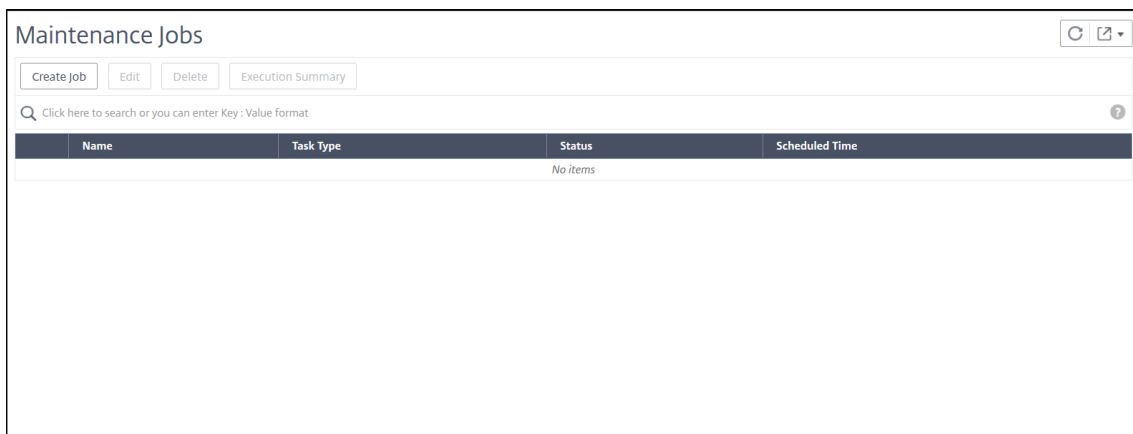
February 6, 2024

Citrix ADM を使用して次のメンテナンスジョブを作成できます。その後、特定の日にメンテナンスジョブをスケジュールできます。

- NetScaler ADC インスタンスのアップグレード
- Citrix ADC SD WAN-WO インスタンスのアップグレード
- NetScaler ADC SDX インスタンスのアップグレード
- AAutoscale グループの NetScaler ADC インスタンスをアップグレードする
- NetScaler ADC インスタンスの HA ペアを構成する
- インスタンスの HA ペアを 2 ノードクラスタに変換

### NetScaler ADC インスタンスのアップグレードをスケジュールする

1. Citrix ADM で、[ネットワーク] > [構成ジョブ] > [メンテナンスジョブ] に移動します。[ジョブの作成] ボタンをクリックします。



2. [メンテナンスジョブの作成] で、[NetScaler ADC (スタンドアロン/高可用性/クラスタ) のアップグレード] を選択し、[続行] をクリックします。

## ← Create Maintenance Job

Select a task to create Maintenance Job\*

- Upgrade NetScaler (Standalone/High-Availability/Cluster)
- Upgrade NetScaler SDX
- Upgrade NetScaler BLX
- Upgrade AutoScale Group
- Configure HA Pair of NetScaler Instances
- Convert HA Pair of Instances to 2 Node Cluster

**Proceed** **Close**

3. [インスタンスの選択] で、[ジョブ名] に任意の名前を入力します。
4. [ **Add Instances** ] をクリックして、アップグレードする ADC インスタンスを追加します。
  - HA ペアをアップグレードするには、プライマリノードまたはセカンダリノードの IP アドレスを指定します。ただし、プライマリインスタンスを使用して HA ペアをアップグレード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、クラスターの IP アドレスを指定します。
5. [ **Next** ] をクリックして、選択したインスタンスでアップグレード前の検証を開始します。

アップグレード前の検証] タブには、失敗したインスタンスが表示されます。障害が発生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、ADM は、他のクラスターノードではなく、指定されたインスタンスでのみアップグレード前の検証を行います。
6. 必要に応じて、[カスタムスクリプト] で、インスタンスのアップグレードの前後に実行するスクリプトを指定します。次の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 で直接コマンドを入力します。

← Upgrade NetScaler

Select Instances Select Image Pre-upgrade Validation **Custom Scripts** Schedule Task Create Job

Specify the scripts/commands to do pre and post instance upgrade validations at various stages. The scripts/commands output is sent to the configured email distribution list/slack channel. The diff reports are generated only if you specify the same script in the pre and post upgrade stages.

▼ Pre upgrade

Enable Script/Command Execution

Import commands from file  Type commands

Command Input File

Choose File

▼ Post upgrade pre failover (applicable for HA)

Enable Script/Command Execution

Use same script as Pre upgrade  Import commands from file  Type commands

```

1 show arp
2 show neighbors
3 show ha node
4 show ha node-summary
5 show servicegroup
    
```

▼ Post upgrade (applicable for Standalone/Cluster) / Post upgrade post failover (applicable for HA)

Enable Script/Command Execution

Use same script as Pre upgrade  Import commands from file  Type commands

Cancel Back Next Skip

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の前後に変更を確認できます。次に例を示します：

- アップグレード前とアップグレード後のインスタンスバージョン。
- アップグレード前後のインターフェイス、高可用性ノード、仮想サーバ、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。
- ダイナミックルート。

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。
- ADC HA ペアを 2 段階でアップグレードする場合は、[ 高可用性のノードに対して 2 段階アップグレードを実行する ] を選択します。

HA ペアの別のインスタンスをアップグレードする場合は、[ **Execution Date** ] と [ **Start Time** ] を指定します。

8. 「ジョブの作成」で、次の詳細を指定します。

a) [ ソフトウェアイメージ ] リストから次のオプションのいずれかを選択します。

- 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 -ADM ファイルブラウザからインスタンスのアップグレードファイルを選択します。ADM GUI には、`/var/mps/mps_images`に存在するインスタンスファイルが表示されます。

b) イメージをインスタンスにアップロードするタイミングを指定します。

- 今すぐアップロード -画像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。

- アップグレードの成功時に **NetScaler ADC** 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に ADC インスタンスでアップロードされたイメージをクリアするには、このオプションを選択します。
- アップグレードを開始する前に、**ADC** インスタンスをバックアップしてください。: 選択した ADC インスタンスのバックアップを作成します。
- 実行レポートを電子メールで受信する-実行レポートを電子メールで送信します。電子メール配布リストを追加するには、「[電子メール配布リストを作成する](#)」を参照してください。
- **slack** による実行レポートの受信-実行レポートを slack で送信します。Slack プロフィールを追加するには、[Slack プロフィールを作成するを参照してください](#)。

Select Instance | Select Image | Pre-upgrade Validation | Custom Scripts | Schedule Task | **Create Job**

When do you want to upload the software image to ADC?

Upload now  Upload at the time of execution

Backup the ADC instances before starting the upgrade.

Save ADC configuration before starting the upgrade

Enable ISSU to avoid network outage on an ADC HA pair.

Note: ISSU applies only to the ADC version 13.0.58.x and later.

ISSU migration timeout (minutes)

150

Citrix ADM Service Connect

Upgrade Reports

Receive upgrade report through email

Email\*

with-ui-repo-bundle

Receive upgrade report through slack ⓘ

Note: Upgrade summary, custom script outputs and the diff reports are sent to the configured email distribution list/slack channel.

9. [ジョブの作成] をクリックします。



## NetScaler ADC SD-WAN WO インスタンスのアップグレードをスケジュールする

1. [ネットワーク] > [構成ジョブ] > [メンテナンスジョブ] に移動します。[ジョブの作成] ボタンをクリックします。
2. [メンテナンスジョブの作成] ページで、[NetScaler ADC SD-WAN WO のアップグレード] を選択し、[続行] をクリックします。

### ← Create Maintenance Job

Select a task to create Maintenance Job\*

Upgrade NetScaler/Upgrade NetScaler HA

Upgrade NetScaler SD-WAN WO

Upgrade NetScaler SDX

Configure HA Pair of NetScaler Instances

Convert HA Pair of Instances to 2 Node Cluster

3. [NetScaler ADC SD-WAN WO のアップグレード] ページの [インスタンスの選択] タブで、[タスク名] を追加します。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 ADM 仮想アプライアンスにある必要があります）を選択します。アップグレードプロセスを実行する Citrix ADC SD-WAN WO インスタンスを追加します。[次へ] をクリックします。

← Upgrade NetScaler SD-WAN WO

Instance Selection  Schedule Task

Once the upgrade is initiated, select the template and click on execution summary button to view the execution summary of the upgrade.

Task Name\*

Software Image\*

Select the target instances to run this task.

	IP Address	Host Name	State
<input checked="" type="checkbox"/>	10.102.186.95	DetAcCenter-CB	Up

4. NetScaler ADC SD-WAN WO インスタンスを今すぐアップグレードするには、[実行モード] リストから [今すぐ実行] を選択します。[完了] をクリックします。
5. Citrix ADC SD-WAN WO インスタンスを後でアップグレードするには、実行モードリストから「後で」を選択します。次に、Citrix ADC SD-WAN WO インスタンスのアップグレードの実行日と開始時間を選択できます。
6. 電子メール通知を有効にして、Citrix ADC SD-WAN WO インスタンスのアップグレードの実行レポートを受け取ることができます。「実行レポートを電子メールで受信」チェックボックスをクリックして、電子メール通知を有効にします。

7. + アイコンを選択して、メール配布リストを作成します。

← Upgrade NetScaler SD-WAN WO

Instance Selection Schedule Task

Perform NetScaler backup  
 Receive Execution Report through email

▼ Execution Details

You can either execute the task now or schedule to execute the task at a later time.

Execution Mode\*  
 Later

**NOTE:** Select the execution time in your local timezone

Execution Date  
 20 Jul 2018

Start Time\*  
 01 00 AM PM

Perform two stage upgrade for nodes in HA

Cancel Back Finish

8. [電子メール配布リストの作成] ページで、電子メール配布リストの名前を指定します。メール通知をメールサーバーに送信するために使用する SMTP メールサーバーを追加します。[差出人] ボックスに、メッセージの送信元の電子メールアドレスを追加します。「宛先」ボックスに、メッセージを送信する1つまたは複数のアドレスを追加します。また、メッセージのコピーやコピーを送信する電子メールアドレスを1つまたは複数追加できます。これらのアドレスは、メッセージやコピーに表示されません。[作成] をクリックします。電子メール同報リストを作成したら、[Finish] をクリックして設定プロセスを完了します。

### NetScaler ADC 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. Citrix ADM で、[ネットワーク] > [構成ジョブ] > [メンテナンスジョブ] に移動します。[ジョブの作成] ボタンをクリックします。
2. [メンテナンスジョブの作成] ページで、[NetScaler ADC SDX のアップグレード] を選択し、[続行] をクリックします。

## ← Create Maintenance Job

Select a task to create Maintenance Job\*

- Upgrade NetScaler/Upgrade NetScaler HA
- Upgrade NetScaler SD-WAN WO
- Upgrade NetScaler SDX
- Configure HA Pair of NetScaler Instances
- Convert HA Pair of Instances to 2 Node Cluster

3. **[NetScaler ADC SDX アプライアンスのアップグレード]** ページの [インスタンスの選択] タブで、[タスク名] を追加します。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 ADM 仮想アプライアンスにある必要があります）を選択します。アップグレードプロセスを実行する NetScaler ADC SDX インスタンスを追加します。[次へ] をクリックします。
4. 電子メール通知を有効にして、NetScaler ADC SDX インスタンスのアップグレードの実行レポートを受け取ることができます。「実行レポートを電子メールで受信」チェックボックスをクリックして、電子メール通知を有効にします。
5. + アイコンを選択して、メール配布リストを作成します。
6. Citrix ADC SDX インスタンスを今すぐアップグレードするには、実行モードリストから「Now」を選択します。[完了] をクリックします。
7. Citrix ADC SDX インスタンスを後でアップグレードするには、実行モードリストから「後で」を選択します。その後、NetScaler ADC SDX 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できます。
8. **[電子メール配布リストの作成]** ページで、電子メール配布リストの名前を指定します。メール通知をメールサーバーに送信するために使用する SMTP メールサーバーを追加します。[差出人] ボックスに、メッセージの送信元の電子メールアドレスを追加します。「宛先」ボックスに、メッセージを送信する 1 つまたは複数のアドレスを追加します。また、メッセージのコピーやコピーを送信する電子メールアドレスを 1 つまたは複数追加できます。これらのアドレスは、メッセージやコピーに表示されません。[作成] をクリックします。電子メール同報リストを作成したら、**[Finish]** をクリックして設定プロセスを完了します。

### Autoscale グループのアップグレードのスケジュール

Autoscale グループの一部であるクラウドサービス内のすべてのインスタンスをアップグレードするには、以下の手順を実行します。

1. NetScaler ADM で、[ネットワーク] > [構成ジョブ] > [メンテナンスジョブ] に移動します。[ジョブの作成] ボタンをクリックします。

2. 「メンテナンスジョブの作成」 ページで、「**Autoscale** グループのアップグレード」を選択し、「続行」をクリックします。
3. [アップグレード設定] タブで、次の操作を行います。
  - a) アップグレードする **Autoscale** グループを選択します。
  - b) [イメージ] で、NetScaler ADC のバージョンを選択します。このイメージは、Autoscale グループの NetScaler ADC インスタンスの既存のバージョンです。
  - c) **NetScaler ADC** イメージで、アップグレードする NetScaler ADC バージョンファイルを参照します。  
グレースフルアップグレード (**Gracful 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) [次へ] をクリックします。
4. [タスクのスケジュール] タブで、次の操作を行います
  - a) 「実行モード」 リストから、次のいずれかを選択します。
    - **Now**: NetScaler ADC インスタンスのアップグレードをすぐに開始します。
    - **後で**: NetScaler ADC インスタンスのアップグレードを後で開始します。
  - b) 「後で」 オプションを選択した場合は、アップグレード・タスクを開始するときに「実行日」と「開始時刻」を選択します。

メール通知と Slack 通知を有効にして、Autoscale グループのアップグレードの実行レポートを受信することもできます。通知を有効にするには、[電子メールによる実行レポートの受信] チェックボックスおよび **[Slack による実行レポートの受信]** チェックボックスをオンにします。
5. [完了] をクリックします。

### NetScaler ADC インスタンスの HA ペアの構成をスケジュールする

1. Citrix ADM で、[ネットワーク] > [構成ジョブ] > [メンテナンスジョブ] に移動します。[ジョブの作成] ボタンをクリックします。
2. [メンテナンスジョブの作成] ページで、**NetScaler ADC** インスタンスの高可用性ペアの構成] を選択し、[続行] をクリックします。

## ← Create Maintenance Job

Select a task to create Maintenance Job\*

Upgrade NetScaler/Upgrade NetScaler HA

Upgrade NetScaler SD-WAN WO



Upgrade NetScaler SDX

Configure HA Pair of NetScaler Instances

Convert HA Pair of Instances to 2 Node Cluster

3. [NetScaler ADC 高可用性ペア] ページの [インスタンスの選択] タブで、[タスク名] を追加します。プライマリ IP アドレスとセカンダリアドレスを入力し、[Next] をクリックします。

## ← NetScaler HA Pair

 Instance Selection  Schedule Task

Task Name\*

Primary IP Address\*

>

Secondary IP Address\*

>

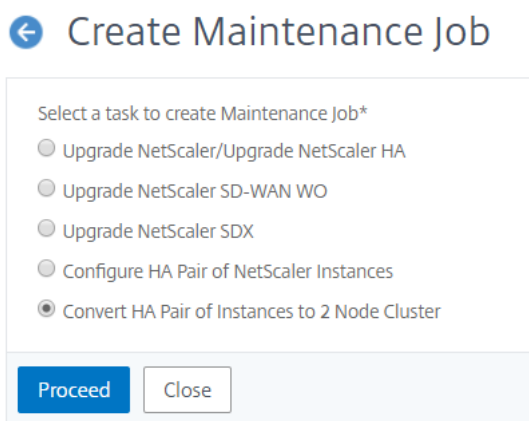
Turn on INC(Independent Network Configuration) mode

4. [タスクのスケジュール] タブで、NetScaler ADC HA ペアを今すぐ構成するか、後で構成するかを選択できます。
5. Citrix ADC HA ペアを今すぐ構成するには、実行モードリストから「Now」を選択します。電子メール通知を有効にして、NetScaler ADC HA ペアの実行レポートを受信できます。「実行レポートを電子メールで受信」チェックボックスをクリックして、電子メール通知を有効にします。
6. Citrix ADC HA ペアを後で構成するには、実行モードリストから「後で」を選択します。その後、eExecution 日と開始時刻を選択できます。電子メール通知を有効にして、NetScaler ADC HA ペアの実行レポートを受信できます。「実行レポートを電子メールで受信」チェックボックスをクリックして、電子メール通知を有効にします。
7. + アイコンを選択して、メール配布リストを作成します。

- 「メール配布リストの作成」ページで、メール配布リストの名前を指定します。メール通知をメールサーバーに送信するために使用する SMTP メールサーバーを追加します。「差出人」ボックスに、メッセージの送信元の電子メールアドレスを追加します。「宛先」ボックスに、メッセージを送信する 1 つまたは複数のアドレスを追加します。また、メッセージのコピーやコピーを送信する電子メールアドレスを 1 つまたは複数追加できます。これらのアドレスは、メッセージやコピーに表示されません。[作成] をクリックします。電子メール同報リストを作成したら、[ **Finish** ] をクリックして設定プロセスを完了します。

インスタンスの **HA** ペアをクラスタに変換するスケジュールを設定する

- Citrix ADM で、[ネットワーク] > [構成ジョブ] > [メンテナンスジョブ] に移動します。[ジョブの作成] ボタンをクリックします。
- [メンテナンスジョブの作成] ページで、[ **HA** ペアの **2** ノードクラスタに変換] を選択し、[続行] をクリックします。



- [**NetScaler ADC HA** をクラスターに移行する] ページの [インスタンスの選択] タブで、[タスク名] を追加します。プライマリ IP アドレス、セカンダリアドレス、プライマリノード ID、セカンダリノード ID、クラスタ IP アドレス、クラスタ ID、およびバックプレーンを指定します。[次へ] をクリックします。

## ← Migrate NetScaler HA to Cluster

⚙️ Instance Selection </> Schedule Task

Task Name\*

Primary IP Address\*

Secondary IP Address\*

Primary Node ID\*

Secondary Node ID\*

Cluster IP Address\*

Cluster ID\*

Backplane\*

4. [タスクのスケジュール] タブでは、NetScaler ADC HA をクラスターに移行するか、後で移行するかを選択できます。
5. Citrix ADC HA ペアを後で構成するには、実行モードリストから「後で」を選択します。その後、実行日と開始時間を選択できます。電子メール通知を有効にして、NetScaler ADC HA ペアの実行レポートを受信できます。「実行レポートを電子メールで受信」チェックボックスをクリックして、電子メール通知を有効にします。
6. + アイコンを選択して、メール配布リストを作成します。
7. [電子メール配布リストの作成] ページで、電子メール配布リストの名前を指定します。メール通知をメールサーバーに送信するために使用する SMTP メールサーバーを追加します。「差出人」ボックスに、メッセージの送信元の電子メールアドレスを追加します。「宛先」ボックスに、メッセージを送信する 1 つまたは複数のアドレスを追加します。また、メッセージのコピーやコピーを送信する電子メールアドレスを 1 つまたは複数追加できます。これらのアドレスは、メッセージやコピーに表示されません。[作成] をクリックします。電子メール同報リストを作成したら、[ **Finish** ] をクリックして設定プロセスを完了します。

## 構成監査

February 6, 2024

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](#)
- [複数インスタンスにまたがる監査構成の変更](#)
- [ネットワーク構成に関するアドバイスの表示](#)
- [NetScaler ADC インスタンスの構成監査をポーリングする方法](#)

## 監査テンプレートの作成

February 6, 2024

ネットワークのパフォーマンスを最適化するため、特定の構成を特定のインスタンス上で実行する場合があります。また、管理対象の Citrix Application Delivery Controller (ADC) インスタンス間の構成変更の監視、構成エラーのトラブルシューティング、および突然のシステムシャットダウン後に未保存の構成の回復も行う必要があります。特定のインスタンスで監査する特定の構成を持つ監査テンプレートを作成できます。Citrix Application Delivery Management (Citrix ADM) は、これらのインスタンスを監査テンプレートと比較し、構成に不一致がある場合は報告します。構成の不一致があると、Citrix ADM は構成差分レポートを生成します。これにより、不要な構成変更のトラブルシューティングと修正が可能になります。

監査テンプレートの実行を自動化するには、

- テンプレートを実行する必要がある時刻をスケジュールする
- NetScaler ADM がテンプレートを実行する必要がある頻度の設定。テンプレートは、毎日、週の特定の日、または月の特定の日に実行できます。

また、NetScaler ADM によって生成された差分レポートを、構成可能な特定の電子メールアドレスに送信するオプションもあります。このオプションを使用すると、ユーザーはレポートをメール添付ファイルとして受信できます。ユーザーが NetScaler ADM にログオンしてレポートを手動でエクスポートする必要はありません。

### 注:

デフォルトの設定テンプレートでは、「名前を変更」オプションは無効になっています。ただし、カスタム設定テンプレートの名前は変更できます。

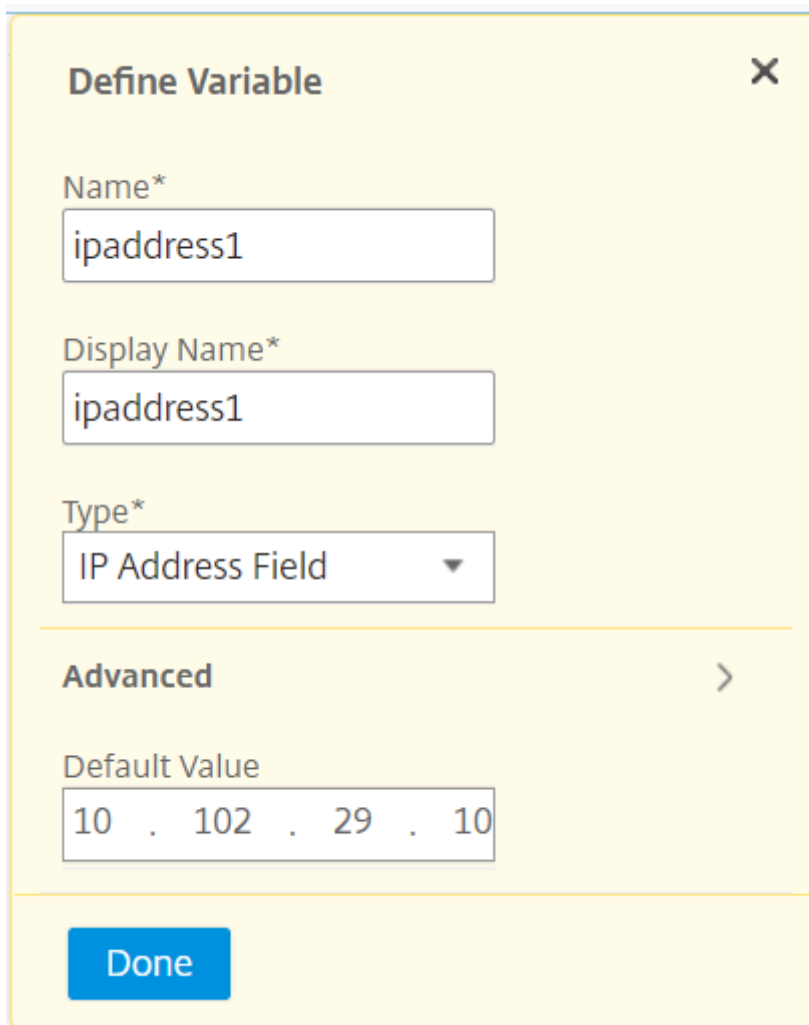
監査テンプレートを作成するには、次の手順に従います。



1. [ネットワーク] > [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] ページおよび [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] 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。既存のテンプレートを左ペインからエディタにドラッグすることもできます。
4. 変数に変換する値を選択し、[変数に変換] をクリックします。たとえば、負荷分散サーバーの IP アドレス「ipaddress1」を選択し、「変数に変換」をクリックします。この変数は、下の図のように「\$」で囲まれています。

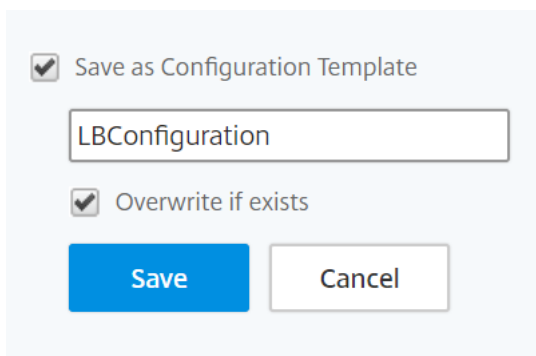
The screenshot shows the 'Audit Commands' tab in the NetScaler Configuration Editor. At the top, there are five buttons: 'Audit Commands', 'Select Instances', 'Specify Variable Values', 'Template Preview', and 'Schedule Template'. Below these buttons are two input fields: 'Template Name\*' with the value 'LBConfiguration' and 'Description' with the value 'Define names and IP addresses of the virtual server and services'. The main area is the 'Configuration Editor', which is split into two panes. The left pane shows 'Configuration Source' set to 'Configuration Template' and a list of templates including 'LBVariablesTemplate'. The right pane shows the configuration code for 'LBVariablesTemplate', which includes several lines of commands: 'add service db1 HTTP \$ipaddress15', 'add service db1 HTTP \$ipaddress25', 'add lbserver cpx-vip1 HTTP \$ipaddress35', 'add lbserver cpx-vip2 HTTP \$ipaddress45', 'bind lbserver cpx-vip1 db1', and 'bind lbserver cpx-vip2 db2'. The variable names are highlighted in green.

「変数の定義」(Define Variable) ウィンドウで、この変数のプロパティ (名前、表示名、変数のタイプ) を設定します。変数のデフォルト値をさらに指定する場合は、「詳細」(**Advanced**) オプションをクリックします。



The image shows a 'Define Variable' dialog box with a close button (X) in the top right corner. It contains three input fields: 'Name\*' with the value 'ipaddress1', 'Display Name\*' with the value 'ipaddress1', and 'Type\*' with a dropdown menu set to 'IP Address Field'. Below these fields is an 'Advanced' section with a right-pointing chevron (>). Under 'Advanced', there is a 'Default Value' field containing the IP address '10 . 102 . 29 . 10'. At the bottom of the dialog is a blue 'Done' button.

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。



The image shows a 'Save as Configuration Template' dialog box. It has a checked checkbox for 'Save as Configuration Template' and a text input field containing 'LBConfiguration'. Below this is another checked checkbox for 'Overwrite if exists'. At the bottom are two buttons: a blue 'Save' button and a white 'Cancel' button.

5. [保存] をクリックし、[次へ] をクリックします。
6. [ **Select Instances** ] タブで、設定監査を実行するインスタンスを選択し、[ **Next** ] をクリックします。

7. [変数値の指定] 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、NetScaler ADM サーバーにファイルをアップロードします。
- b) すべてのインスタンスに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。

### ← Create Template

9. [ **Template Preview** ] タブでは、各インスタンスまたはインスタンスグループで実行す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。

Select an instance or instance group to preview

10.102.29.60

Preview of the template on the Instance 10.102.29.60

Commands
add service db1 HTTP 10.102.29.10
add service db1 HTTP 10.102.29.11
add lbserver cpx-vip1 HTTP 10.102.29.4
add lbserver cpx-vip2 HTTP 10.102.29.5
bind lbserver cpx-vip1 db1
bind lbserver cpx-vip2 db2

Cancel   ← Back   Next →

10. [ **Schedule Template** ] タブには、テンプレートの実行をスケジュールし、差分レポートを送信するようにメールアドレスを設定する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します。NetScaler ADM でグローバルに構成されたインスタンスでテンプレートを一度に実行するには、このオプションを選択します。

注:

NetScaler ADM でグローバルポーリング間隔を構成するには、[ネットワーク] > [構成監査] > [監査テンプレート] の順に選択し、[グローバルポーリング間隔] をクリックします。[ポーリング間隔] フィールドに、NetScaler ADM がインスタンスをグローバルにポーリングする必要がある分を入力します。

- テンプレート集計表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。
- レポートを電子メールで送信する。このオプションを使用して、差分レポートの送信先となるメールプロファイルをメール添付ファイルとして構成します。

11. [完了] をクリックします。

### ← Create Template

Audit Commands  Select Instances  Specify Variable Values  Template Preview  Schedule Template

You can either use polling interval or customized schedule

Use global polling interval

Customize template schedule

Recurrence\*

Daily

Schedule time (format HH:MM)\*

06:00

Send report through email

Mail Profile

abcd

監査テンプレートは [ **Audit Templates** ] リストに表示され、指定されたインスタンスの設定に対してスケジュールされた時刻に実行されます。

## 監査レポートを表示する

February 6, 2024

Citrix Application Delivery Management (Citrix ADM) 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。設定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に概要レポートをエクスポートできます。また、インスタンスとテンプレートのペアごとに詳細な差分レポートをエクスポートすることもできます。

[Audit Templates] リストに表示される監査テンプレートは、指定したインスタンスの設定に対してスケジュールされた時刻に実行されます。[構成監査] ダッシュボードの [ **NetScaler Config Drift** ] グラフには、保存されていない構成に対して保存された構成の変更に関する詳細な情報が表示されます。 **NetScaler Config Drift** チャートをクリックすると、次の監査レポートページに「Diff Exists (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。Citrix ADM 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 ADM では、差分のレポートの自動エクスポートをメール添付ファイルとしてスケジュール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。

構成監査レポートをエクスポートするには、次の手順に従います。

1. NetScaler ADM で、[ネットワーク] > [構成監査] に移動します。

2. [構成監査] ページで、**NetScaler ADC** の構成ドリフトグラフ内をクリックします。
3. 「監査レポート」 ページには、相違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、構成実行に違いがないインスタンスのリストも表示されます。

Audit Reports

Instance	Host Name	Saved vs Running Diff	Template vs Running Diff	Config Saved
10.106.43.13		No Diff	NA	Yes
10.102.29.191		NA	No Diff	No
10.106.43.12		Diff Exists	NA	No
10.106.43.7		No Diff	NA	Yes
10.102.205.27	HA-Node2-admin-NetScalerVPX	No Diff	No Diff	Yes
10.102.29.140	MyCache	Diff Exists	No Diff	No
10.102.29.191-P1		NA	No Diff	No
10.102.29.60		Diff Exists	Diff Exists	No

画像では、一部のインスタンスでは差分が保存済みと実行差分にのみ存在し、一部のインスタンスでは差分がテンプレートと実行差分にのみ存在することがわかります。場合によっては、保存された差分と実行中の差分とテンプレートと実行中の差分の両方に違いがあります。

### 保存された差分と実行中の差分比較

インスタンスに保存された設定と、そのインスタンスで現在実行中の設定との相違のレポートを表示できます。たとえば、[保存済みと実行中の \*\*相違の比較\*\*] で、インスタンスの [相違が存在する] をクリックします。 \*\*

Instance	Host Name	Saved vs Running Diff	Template vs Running Diff	Config Saved
10.106.43.13		No Diff	NA	Yes
10.102.29.191		NA	No Diff	No
10.106.43.12		Diff Exists	NA	No
10.106.43.7		No Diff	NA	Yes
10.102.205.27	HA-Node2-admin-NetScalerVPX	No Diff	No Diff	Yes
10.102.29.140	MyCache	Diff Exists	No Diff	No
10.102.29.191-P1		NA	No Diff	No
10.102.29.60		Diff Exists	Diff Exists	No

ここでは、そのインスタンスの構成実行差分に対する、保存された構成のレポートを確認できます。

Configuration Diff

Saved vs Running Diff - Instance: (10.102.29.60)

Create job **Export diff report** Export corrective commands

Saved Configuration	Running Configuration	Correction Configuration
set unfiltering parameter -TimeOfDayToUpdateDB 03:00 -ProxyPa ssword b63a0b9e68619fe528b62402791659d8719aee26ec0c10661aedd9e78e80509 7 -encrypted -encryptmethod ENCMTHD_3	set unfiltering parameter -TimeOfDayToUpdateDB 03:00 -ProxyPa ssword a3962b89cfc8a32e2e34d690e9d2142c1a744386f8adb1822b405d31fa494f -encrypted -encryptmethod ENCMTHD_3	

Close

[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。[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、構成ジョブから関連する Citrix ADM インスタンスでコマンドを実行して、そのインスタンスの構成を修正できます。

## テンプレートと実行中の差分

テンプレートと実行差分には、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構成の違いを確認できます。たとえば、「テンプレート」と「実行中差分」のインスタンスの **1** つに対して「差分」をクリックします。

Instance	Host Name	Saved vs Running Diff	Template vs Running Diff	Config Saved
10.106.43.13		No Diff	NA	Yes
10.102.29.191		NA	No Diff	No
10.106.43.12		Diff Exists	NA	No
10.106.43.7		No Diff	NA	Yes
10.102.205.27	HA-Node2-admin-NetScalerVPX	No Diff	No Diff	Yes
10.102.29.140	MyCache	Diff Exists	No Diff	No
10.102.29.191-P1		NA	No Diff	No
10.102.29.60		Diff Exists	Diff Exists	No

これで、2つのテンプレートに diff が表示され、NetScaler ADM インスタンスはテンプレートが探しているものとは異なる構成になっていることがわかります。

Templates of Instance: 10.102.29.60

Templates	Diff Exists	Last Updated
LBVariablesTemplate	Diff Exists	Oct 10 2017 05:30:02
LBConfigurationAudit	Diff Exists	Oct 27 2017 12:14:30

もう一度「相違が存在する」をクリックします。次の図は、テンプレートが探している設定と、そのようなコマンドが設定されていないか、削除されていないために空白になっている実行構成を示しています。また、修正設定や、設定を修正するために実行するコマンドも表示されます。

Configuration Diff

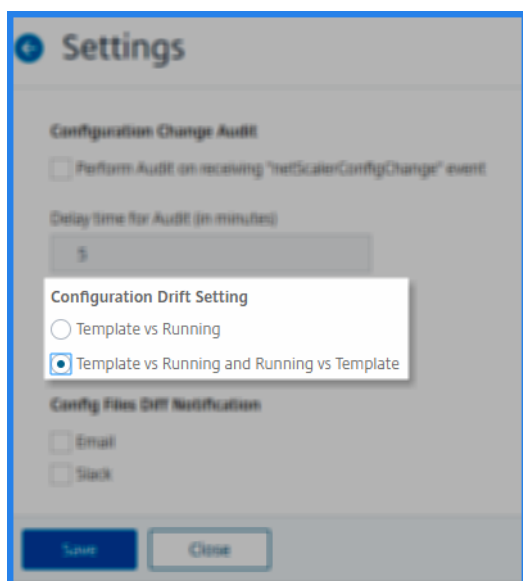
Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate

Template Configuration	Running Configuration	Correction Configuration
add service lbservice2 10.102.29.11 HTTP 80		add service lbservice2 10.102.29.11 HTTP 80
add service lbservice1 10.102.29.10 HTTP 80		add service lbservice1 10.102.29.10 HTTP 80
add lb vserver lserver1 HTTP 10.102.29.1 80		add lb vserver lserver1 HTTP 10.102.29.1 80
bind lb vserver servername lbservice2		bind lb vserver servername lbservice2

また、テンプレートと実行と実行とテンプレートのドリフト設定を使用して、両方の方法で設定を比較することもできます。

- 監査テンプレート設定と、インスタンスの実行設定を比較します。
- インスタンスの実行構成を監査テンプレートと比較します。

デフォルトでは、「テンプレート対ランニングドリフト」設定が選択されています。ドリフト設定を変更するには、ADM GUI から、[構成監査] ページで [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。[修正コマンドのエクスポート] をクリックして、コマンドを.txt ファイルにエクスポートすることもできます。その後、CLI でコマンドを実行して、そのインスタンスの設定を修正できます。

次の図は、システムにダウンロードされる.csv diff ファイルの例を示しています。

#Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate		
Template Configuration	Running Configuration	Correction Configuration
add service lbservice2 10.102.29.11 HTTP 80		add service lbservice2 10.102.29.11 HTTP 80
add service lbservice1 10.102.29.10 HTTP 80		add service lbservice1 10.102.29.10 HTTP 80
add lb vserver lserver1 HTTP 10.102.29.1 80		add lb vserver lserver1 HTTP 10.102.29.1 80
bind lb vserver servername lbservice2		bind lb vserver servername lbservice2

#### ファイルステータス監査レポートの表示

**NetScaler ADC** ファイルの状態グラフを使用して、`nsconfig` フォルダ内のファイルが追加、変更、または削除されているかどうかを監視できます。たとえば、ADC インスタンスでライセンス・ファイルが更新された場合、このファイルが最後に更新された日時を確認し、適切なアクションを実行できます。

NetScaler ADC インスタンスのファイルステータス監査レポートをエクスポートするには:

1. NetScaler ADM で、[ネットワーク] > [構成監査] に移動します。
2. [構成監査] ページで、[NetScaler ADC ファイルステータス] グラフ内をクリックします。

監査レポートページには、Diff ステータスのインスタンスが一覧表示されます。



INSTANCE	HOST NAME	DIFF STATUS	PREVIOUS POLLED TIME	LATEST POLLED TIME
		No Diff	Sun Oct 06 2019 1:52 PM	Sun Oct 06 2019 11:52 PM
		No Diff	Fri Oct 11 2019 3:30 PM	Mon Oct 14 2019 11:37 AM
		NA	NA	NA
	InfraNS	Diff Exists	Mon Oct 14 2019 9:47 PM	Tue Oct 15 2019 07:47 AM
	InfraNS	Diff Exists	Tue Aug 27 2019 02:33 AM	Wed Sep 25 2019 9:22 PM
	InfraNS	NA	NA	NA
	InfraNS	NA	NA	NA
	InfraNS	NA	NA	NA
	InfraNS	NA	NA	NA

**Diff Status** は、\*\* 前回のポーリング時刻から最新のポーリング時刻までの間隔で計算されます。\*\* 差分ステータスは次のいずれかになります。

- **Diff exists** -このステータスは、前回のポーリング時間以降、インスタンスの `nsconfig` フォルダ内のファイルが変更されたことを示します。ファイルの変更内容を表示するには、「相違が存在する」をクリックします。

FILE NAME	DIFF STATUS	LAST MODIFIED TIME
ssl/certmew	File Added	Tue Oct 15 2019 05:51 AM
ssl/certeest	File Added	Tue Oct 15 2019 05:45 AM
ssl/csrmew	File Added	Tue Oct 15 2019 05:50 AM
ssl/csrtest	File Added	Tue Oct 15 2019 05:44 AM
ssl/keyew	File Added	Tue Oct 15 2019 05:50 AM
ssl/keytest	File Added	Tue Oct 15 2019 05:44 AM
ns.conf	File Content Modified	Mon Oct 14 2019 9:19 PM
ns.conf0	File Content Modified	Mon Oct 14 2019 9:19 PM
ns.conf1	File Content Modified	Mon Oct 14 2019 9:18 PM
ns.conf2	File Content Modified	Mon Oct 14 2019 9:18 PM
ns.conf3	File Content Modified	Mon Oct 14 2019 1:00 PM
ns.conf4	File Content Modified	Mon Oct 14 2019 1:00 PM
ssl/ns-root.srl	File Content Modified	Tue Oct 15 2019 05:51 AM

- **相違なし** -このステータスは、前回のポーリング時刻以降、`nsconfig` フォルダ内のファイルが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は適用できないことを示します。このステータスは、NetScaler ADM がインスタンスをポーリングしない場合に表示されます。たとえば、インスタンスが新しく追加された場合、またはインスタンスの状態が非アクティブの場合、インスタンスのポーリングは行われません。

## インスタンス間の設定変更の監査

February 6, 2024

ネットワークのパフォーマンスを最適化するため、特定の構成を特定のインスタンス上で実行する場合があります。また、管理対象の Citrix Application Delivery Controller (ADC) インスタンス間の構成変更の監視、構成エラーのトラブルシューティング、および突然のシステムシャットダウン後に未保存の構成の回復も行う必要があります。特定のインスタンスで実行する特定の設定を使用して、監査テンプレートを作成できます。NetScaler Application Delivery Management (NetScaler ADM) は、これらのインスタンスを監査テンプレートと比較し、構成に不一致があるかどうかを報告します。これにより、エラーのトラブルシューティングと修正が可能になります。

監査テンプレートの実行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。NetScaler ADM がテンプレートを実行する必要がある頻度を設定することもできます。テンプレートは、毎日、週の特定の日、または月の特定の日に実行できます。Citrix ADM によって生成された差分レポートを、構成可能な指定された電子メールアドレスに送信することもできます。このオプションを選択すると、ユーザーはレポートをメール添付ファイルとして受信します。ユーザーが NetScaler ADM にログオンしてレポートを手動で確認する必要はありません。

監査テンプレートを作成するには、次の手順に従います。

1. [ネットワーク] > [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] ページおよび [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. 構成エディタでコマンドを入力し、構成テンプレートとしてコマンドを保存します。エディタ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. 変数に変換する値を選択し、[変数に変換] をクリックします。たとえば、負荷分散サーバーの `ipaddress` を選択し、次の図に示すように [変数に変換] をクリックします。

### ← Create Template

変数のデフォルト値をさらに指定する場合は、「詳細」 (**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。

Save as Configuration Template

Overwrite if exists

5. [保存] をクリックし、[次へ] をクリックします。
6. [ **Select Instances** ] タブで、設定監査を実行するインスタンスを選択します。
7. [変数値の指定] 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、NetScaler ADM サーバーにファイルをアップロードします。
  - b) すべてのインスタンスに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。

← Create Template

Specify the values to all the command variables.

Upload input file for variables values  
 Common Variable Values for all Instances

servername

ipaddress

portnumber

servicename1

ipaddress1

servicename2

ipaddress2

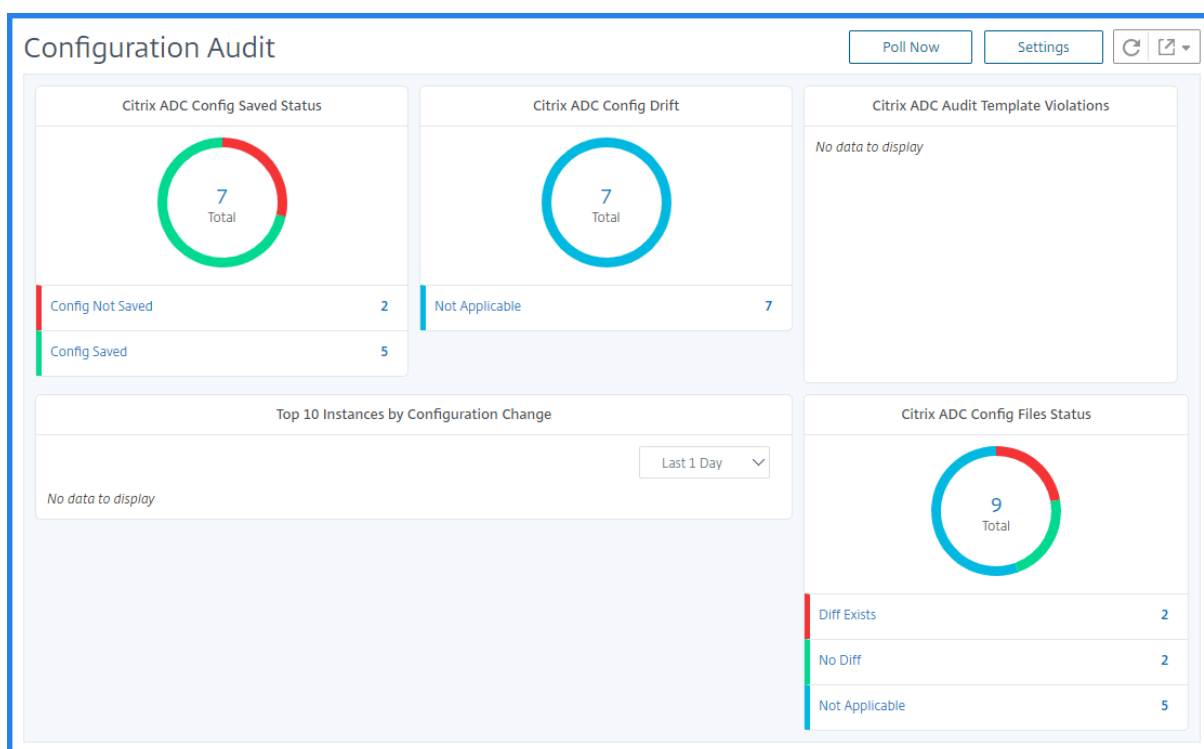
9. [ **Template Preview** ] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。[次へ] をクリックします。
10. スケジュールテンプレートタブには、テンプレートの実行を自動化する 3 つのオプションと、差分レポートを送信するメールアドレスがあります。
  - グローバルポーリング間隔を使用します。このオプションを選択すると、NetScaler ADM でグローバルに設定されたインスタンス上でテンプレートを一度に実行します。
  - テンプレート集計表をカスタマイズします。このオプションを使用して、テンプレートを実行する必要がある時間と頻度を設定します。
  - レポートを電子メールで送信する。このオプションを使用して、差分レポートの送信先となるメールプロファイルをメール添付ファイルとして構成します。
11. [完了] をクリックします。

監査テンプレートは [ Audit Templates ] リストに表示され、指定されたインスタンスの設定に対してスケジュールされた時刻に実行されます。

#### 設定変更の詳細の表示

「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度な詳細を表示することもできます。

- 構成変更による上位 10 のインスタンス
- 保存済みおよび未保存の構成の数
- nsconfig フォルダ内で追加、削除、または変更されたファイル



また、NetScaler ADM では、構成監査を手動でポーリングし、インスタンスのすべての構成監査を直ちに NetScaler ADM に追加します。そのためには、[ ネットワーク ] > [ 構成監査 ] に移動し、[ 今すぐ投票 ] をクリックします。ポップアップページの [ 今すぐ投票 ] に、ネットワーク内のすべての Citrix ADC 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を選択できます。

特定のインスタンスに対して監査を強制することもできます。これを行うには、次のグラフのいずれかをクリックします。

- **NetScaler ADC** 構成保存ステータス
- **NetScaler ADC** 構成ドリフト

[ **Audit Reports** ] ページで、インスタンスを選択し、[ **Action** ] リストで [ **Poll Now** ] を選択します。

**Audit Reports**

Buttons: Refresh, Share

Buttons: Running Configuration, Saved Configuration, Save configuration, **Poll Now**, Action

Instance	Host Name	Last Updated	Saved vs Running Diff	Template vs Running Diff	Config Saved
<input checked="" type="checkbox"/> 10.102.29.140	MyCache	Thu, 13 Jul 2017 15:21:31 GMT	Diff Exists	NA	No
<input type="checkbox"/> 10.102.29.60		Thu, 13 Jul 2017 15:21:35 GMT	No Diff	Diff Exists	Yes

**NetScaler ADC** 構成ファイルのステータス グラフには、`nsconfig` フォルダー内に存在する NetScaler ADC ファイルのステータスが表示されます。NetScaler ADM は、`nsconfig` フォルダー内のファイルの変更を記録して比較し、相違点を表示します。ファイルステータス監査レポートの表示を参照してください。

### 構成監査通知の設定

1. [ ネットワーク ] > [ 構成監査 ] に移動します。

2. [構成の監査] ページで、[設定] をクリックします。
3. [Notification Settings] ページで、[Edit] アイコンをクリックして、通知設定を有効にします。
4. [Enabled] チェックボックスをオンにして、ボックスの一覧からメール配布リストを選択します。[+] アイコンをクリックしてメールサーバーの詳細を指定することによって、メール配布リストを作成することもできます。

## ネットワーク構成に関する設定アドバイスを取得

February 6, 2024

アプリケーションのパフォーマンスを最適化できるように、Citrix Application Delivery Controller (ADC) インスタンスを最適な構成でセットアップします。ただし、一部の構成は標準構成ではない場合があり、アプリケーションのパフォーマンスに影響を与える可能性があります。

アプリケーションのパフォーマンスを最適化するために、NetScaler Application Delivery Management (NetScaler ADM) は NetScaler ADC インスタンス構成を分析し、推奨事項を提供します。NetScaler ADM から推奨される構成を適用できます。

**NetScaler ADC** インスタンスを分析するには：

1. [ネットワーク] > [構成監査] > [構成アドバイス] に移動します。
2. 次のいずれかを行います：
  - [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。
  - [デバイスの選択] をクリックし、分析する NetScaler ADC インスタンスを選択します。

NetScaler ADM は、インスタンスの構成を分析し、次の図に示すように、推奨される構成のリストを提供します。構成のアドバイスの隣にあるチェックボックスをオンにすると、修正コマンドが表示されます。

## 10.102.29.60

Recommendations | 52

Search in Advice

Filter By: Category All

Commands Selected 1

Category	Advice	
System Settings	DNS server is currently not configured. Please make sure this is configured.	<input type="checkbox"/>
User Administration	Please ensure there are accounts other than nsroot. Command: add system user <userName> <Password> -timeout 600 add system user <userName> <Password> -timeout 600	<input checked="" type="checkbox"/>
User Administration	Please ensure system users other than nsroot are bound to an RBA policy.	<input type="checkbox"/>
System Settings	The following features must be enabled : IPV6PT, AAA, SUBSCRIBER, AAA, APPFW.	<input type="checkbox"/>

構成を更新する場合は、修正コマンドで変数の値を指定し、次の図に示すように [ **Apply Now** ] をクリックします。

注:

ここに記載されているコマンドは、推奨事項に過ぎません。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。コマンドを編集してはならないと考えられるユーザーには、限定された特権アクセスを許可してください。

## 10.102.29.60

Recommendations | 52

Search in Advice

Filter By: Category All

Commands Selected 1

Category	Advice	
System Settings	DNS server is currently not configured. Please make sure this is configured.	<input type="checkbox"/>
User Administration	Please ensure there are accounts other than nsroot. Command: add system user <userName> <Password> -timeout 600 add system user new-user new-user -timeout 600	<input checked="" type="checkbox"/>

Download File  
Apply Now

ネットワークインスタンスでコマンドが正常に実行されると、アドバイスの隣にあるチェックボックスが消えます。

User Administration	Please ensure there are accounts other than nsroot.	<input type="checkbox"/>
---------------------	---	--------------------------

ネットワークインスタンスで実行されるコマンドの詳細を表示するには、[ ネットワーク ] > [ インスタンス ] > [ ] に移動し、インスタンスの <Instance\\_Type> IP アドレスを選択し、[ **Actions** ] ドロップダウンリストから [

**Events** ] をクリックします。

Networks > Instances > NetScaler VPX

### NetScaler VPX

	IP Address	Host Name	State	Rx (Mbps)	Tx (Mbps)	HTTP requests/sec
<input checked="" type="checkbox"/>	10.102.29.60	10.102.29.60	● Up	0	0	0
<input type="checkbox"/>	10.102.29.140	MyCache	● Up	0	0	0
<input type="checkbox"/>	10.102.29.93	10.102.29.93	● Up	0	0	0
<input type="checkbox"/>	10.102.29.200	MyCache	● Up	0	0	0

- ✓ Select Action
- Create Cluster
- Reboot
- Events**
- Ping
- TraceRoute
- Rediscover
- Enable/Disable Insight
- Unmanage
- Annotate

[ **Events** ] ページでは、構成変更の詳細を表示できます。

Networks > Instances > NetScaler VPX > Events

### Events

Details History Delete Clear Search ⌵ ⚙ ⌵

Filters: Source : 10.102.29.60 ✕ Remove all

	Severity	Source	Host Name	Date	Category	Failure Objects	Configuration Command
<input checked="" type="checkbox"/>	● Minor	10.102.29.60	10.102.29.60	Fri, 21 Apr 2017 16:32:48 GMT	netScalerConfigChange	nsroot	add system user new-user "*****"
<input type="checkbox"/>	● Minor	10.102.29.60	10.102.29.60	Wed, 19 Apr 2017 01:57:54 GMT	netScalerConfigSave	nsroot	
<input type="checkbox"/>	● Major	10.102.29.60	10.102.29.60	Wed, 19 Apr 2017 01:57:41 GMT	ipConflict	10.10.10.10	

## NetScaler ADC インスタンスの構成監査をポーリングする

February 6, 2024

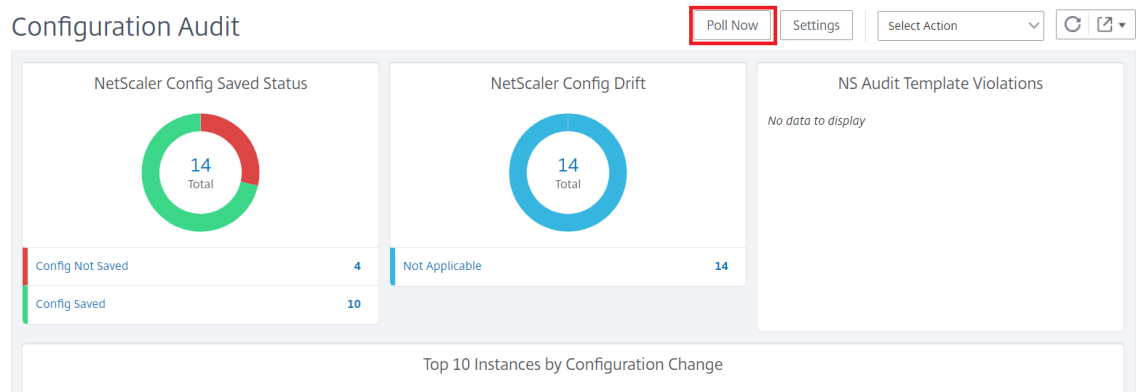
Citrix Application Delivery Management (Citrix ADM) は、Citrix アプリケーション Delivery Controller (ADC) インスタンスで発生した構成変更を確認するために、10 時間ごとに構成監査を自動的にポーリングします。構成監査を手動でポーリングして最近の変更を検出することもできますが、すべての NetScaler ADC インスタンスの構成をポーリングすると、ネットワークに大きな負荷がかかります。

NetScaler ADC 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 ADC** インスタンスの構成監査をポーリングするには：

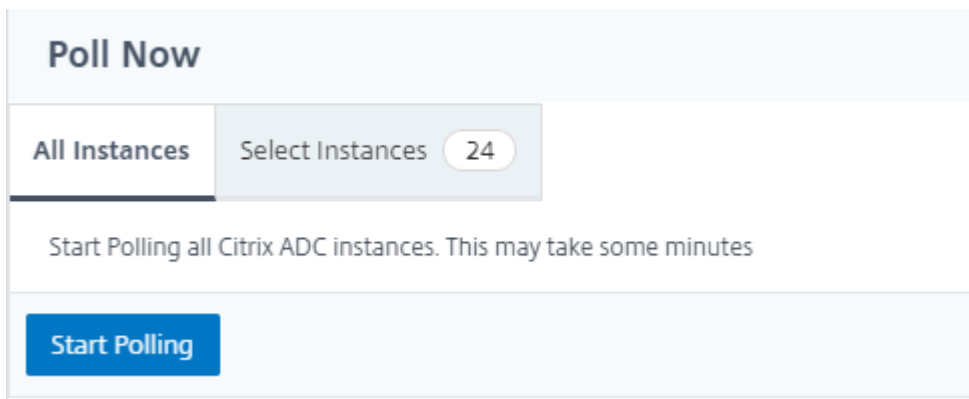
1. NetScaler ADM で、[ネットワーク] > [構成監査] に移動します。
2. [構成の監査] ページの右上隅にある [今すぐポーリングする] をクリックします。





3. **[Poll Now]** ページが表示され、ネットワーク内のすべての NetScaler ADC 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を選択できます。

- a) すべての NetScaler ADC インスタンスをポーリングするには、[すべてのインスタンス] タブを選択し、[ポーリング開始] をクリックします。



- b) 特定のインスタンスをポーリングするには、**[SelectInstances]** タブを選択し、リストからインスタンスを選択し、**[Poll Now]** をクリックします。

The "Poll Now" page shows the "Select Instances" tab active, with 24 instances selected. A "Start Polling" button is visible. Below is a table of instances:

	IP Address	Host Name	Instance State
<input checked="" type="checkbox"/>	10.102.29.60	--	● Up
<input type="checkbox"/>	10.102.29.160-10.102.29.165	NS	● Up
<input checked="" type="checkbox"/>	10.102.29.200	--	● Up
<input type="checkbox"/>	10.102.29.200-TEST	--	● Up

## 構成変更 **SNMP** トラップの構成監査差分を生成

February 6, 2024

ネットワーク内の Citrix Application Delivery Controller (ADC) インスタンスの構成が変更されるたびに、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 Application Delivery Management (Citrix ADM) に送信します。インスタンスが ConfigChange SNMP トラップを送信するときに、そのインスタンスに対して NetScaler ADM で構成監査を実行するように設定できます。

監査テンプレート設定と構成実行の間に相違がある場合は、「監査レポート」 (Audit Report) ページに「差分」 (Diff Exist s) ステータスメッセージが表示されます。「相違の出口」リンクをクリックすると、「構成の差分」ページが表示され、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 ADC インスタンスで実行できます。設定ジョブを実行すると、インスタンスは目的の設定に戻ります。修正コマンドから構成ジョブを作成する方法の詳細については、「[NetScaler ADM で修正コマンドから構成ジョブを作成する方法](#)」を参照してください。

**ConfigChange SNMP** トラップの受信時に構成監査テンプレートを実行するには、次の手順に従います。

NetScaler ADM では、NetScaler ADM で構成監査テンプレートを実行するオプションを有効にできます。

1. NetScaler ADM で、[ネットワーク] > [構成監査] に移動します。
2. 「構成監査」ページの「設定」をクリックします。
3. 「構成変更の監査設定」セクションの編集アイコンをクリックします。
4. 「**NetScalerConfigChange** イベントの受信時に構成監査を行う」チェックボックスを選択します。

### 注:

これはすべてのインスタンスのグローバル設定です。NetScaler ADM は、将来 NetScalerConfigChange SNMP トラップを受信するすべてのインスタンスに対して構成監査を実行します。

1. 「監査テンプレートを実行するための遅延時間 (分単位)」フィールドに、分数を入力します。NetScaler ADM は、そのインスタンスによって ConfigChange SNMP トラップを受信すると、この時間が経過すると、NetScaler ADC インスタンス上で構成監査テンプレートを実行します。

## ネットワーク機能

February 6, 2024

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 (ADC) インスタンスで構成されたエンティティの状態を監視できます。負荷分散仮想サーバーのトランザクション詳細、接続詳細、スルー

プットなどの統計を表示できます。また、メンテナンスの計画時には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。

- クライアント接続が多い上位 5 つの仮想サーバー
- サーバー接続が多い上位 5 つの仮想サーバー
- スループット (MB/秒) が高い上位 5 つの仮想サーバー
- スループット (MB/秒) が低い下位 5 つの仮想サーバー
- 仮想サーバーが多い上位 5 つのインスタンス
- 仮想サーバーの状態
- 負荷分散仮想サーバーの正常性
- プロトコル

### 負荷分散エンティティのレポートを生成する

February 6, 2024

Citrix Application Delivery Management (ADM) では、Citrix アプリケーション Delivery Controller (ADC) インスタンスエンティティのレポートをすべてのレベルで表示できます。NetScaler ADM / ネットワーク機能でダウンロードできるレポートには、統合レポートと個別レポートの 2 種類があります。

統合レポート: NetScaler ADC インスタンスで管理されているすべてのエンティティの統合レポートまたは要約レポートをダウンロードして表示できます。

このレポートでは、NetScaler ADC インスタンス、パーティション、およびネットワークに存在する対応する負荷分散エンティティ (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確認できます。

次の画像は、概要レポートの例を示しています。

Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
	beta		Load Balancing				
			Load Balancing				
			Load Balancing				
			Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:80
			Load Balancing	ADM-Test-LB3#10.1.1.3:80			
			Load Balancing	334-lb#1.33.2.2:80			
			Load Balancing				
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbc74-07fb-45b6-b		33f97d16-0413-4e6e-9f3d-844	
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8		33f97d16-0413-4e6e-9f3d-844	
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-9		33f97d16-0413-4e6e-9f3d-844	
			Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
			Load Balancing				

統合レポートは、CSV 形式です。各列のエントリの説明は次のとおりです。

- **NetScaler IP** アドレス: Citrix ADC 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, server\_Member3\_IP\_Address: Port、…、server\_membern\_IP\_Address: Port

#### 注

- 利用可能なホスト名がない場合は、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 ADC インスタンスに対して構成されていないことを示します。

個別レポート: 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、負荷分散仮想サーバー、負荷分散サービス、負荷分散サービスグループのいずれかのみをダウンロードできます。

NetScaler ADM では、レポートをすぐにダウンロードできます。1日1回、1週間に1回、または1か月に1回の頻度で、特定の時間にレポートが生成されるようにスケジュールを設定することもできます。

#### 結合された負荷分散レポートの生成

1. NetScaler ADM で、[ネットワーク] > [ネットワーク機能] > [負荷分散] に移動します。
2. [負荷分散] ページで、[!\[矢印をクリック\] をクリック](#)します。
3. 表示される [エクスポート] ページには、次の2つのオプションが表示され、レポートを表示できます:
  - a) 「今すぐエクスポート」タブを選択し、「**OK**」をクリックします。

システムに統合レポートがダウンロードされます。
  - b) レポートの生成とエクスポートを定期的にスケジュールするには、「レポートのスケジュール」タブを選択します。レポート生成の繰り返し設定を指定し、レポートのエクスポート先のメールプロファイルを作成します。
    - i. 繰り返し - ドロップダウンリストボックスから [毎日]、[\*\* 毎週 \*\*]、または [毎月] を選択します。
    - ii. 繰り返し時間-時間を 24 時間形式で「時:分」で入力します。
    - iii. メールプロファイル-ドロップダウンリストボックスからプロファイルを選択するか、+ をクリックしてメールプロファイルを作成します。

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平日を選択してください。

### Export

Subject\*

Format\*

Recurrence\*

Description

**NOTE:** Enter the schedule time in your selected timezone

Days of Week

Sun	Mon	Tue	Wed	Thu	Fri	Sat
-----	-----	-----	-----	-----	-----	-----

Export Time\*

Email

Email Distribution List\*  
 Add Edit Test

Slack

**Schedule**

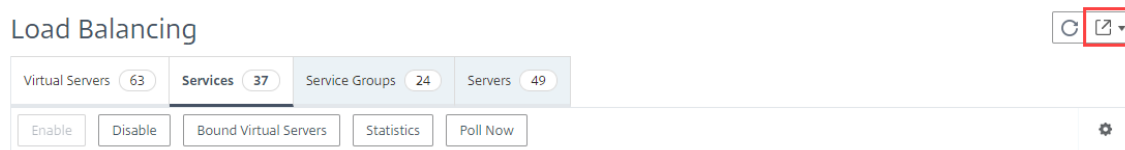
注

[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カンマで区切って入力します。

### 個々の負荷分散エンティティレポートを生成する

インスタンスに関連付けられた特定の種類のエンティティを対象に、個別レポートを生成してエクスポートできます。たとえば、ネットワークのすべての負荷分散サービスの一覧を表示するとします。

1. Citrix ADM で、[ネットワーク] > [ネットワーク機能] > [負荷分散] > [サービス] に移動します。
2. [サービス] ページで、右上隅にある [エクスポート] ボタンをクリックします。



- a) この瞬間にレポートを生成して表示する場合は、[ **Export Now** ] タブを選択します。
- b) レポートの生成とエクスポートを定期的なスケジュールするには、「エクスポートのスケジュール」を選択します。

注

レポートは、メールの添付ファイルとしてのみ、ダウンロードまたはエクスポートできます。NetScaler ADM 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スケジュール設定

February 6, 2024

Citrix Application Delivery Management (ADM) では、負荷分散、コンテンツスイッチング、キャッシュリダイレクト、グローバルサーバー負荷分散 (GSLB)、認証、NetScaler Gateway などの特定のネットワーク機能に関する包括的なレポートを生成できます。このレポートでは、ネットワークに存在する NetScaler ADC 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、サービス) 間のマッピングの高レベルなビューを表示できます。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。

このレポートには、次の仮想サーバ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
- 仮想サーバ名
- 仮想サーバのタイプ
- 仮想サーバ
- ターゲット LB 仮想サーバ

注:

コンテンツスイッチおよびキャッシュリダイレクト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の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

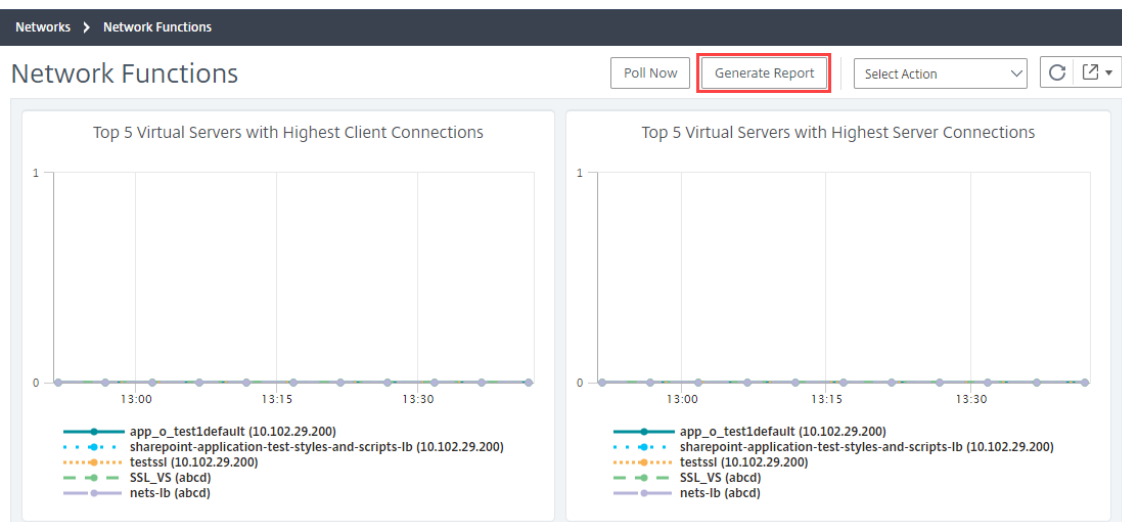
これらのレポートを指定のメールアドレスに異なる間隔でエクスポートするようにスケジュールできます。

注

- GSLB 仮想サーバーの場合、ネットワーク機能レポートには GSLB 仮想サーバーと関連サービスのみが表示されます。
- コンテンツスイッチングとキャッシュリダイレクトの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。
- NetScaler ADM では 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、SSL 仮想サーバーは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、古いレポートは自動的にアカウントから削除されます。
- HAProxy のネットワーク機能レポートは生成できません。

ネットワーク機能レポートをエクスポートおよびスケジュールする手順は、次のとおりです。

1. [ネットワーク] > [ネットワーク機能] に移動します。
2. [ネットワーク機能] ページの右ペインで、ページの右上隅にある [レポートの生成] をクリックします。



3. [レポートの生成] ページには、次の 2 つのオプションがあります:

- a) 「今すぐエクスポート」タブを選択し、「OK」をクリックします。レポートがシステムにダウンロードされます。

## ← Generate Report

Export Now
 Schedule Export

You can generate the report and download now for the following selected Network Functions

- Load Balancing
- Content Switching
- Cache Redirection
- Authentication
- Citrix Gateway
- GSLB

OK
Close

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。

NetScaler ADC IP Address	NetScaler ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
10.102.61.110	10.102.61.110		Load Balancing	lb_test_1#10.10.10.10:80		adm_metric_collector_svc_10.106.171.41#10.102.61.110:80	
10.102.61.110	10.102.61.110		Load Balancing	lbvs_511#51.1.1.1:80		test_1#10.102.61.110:80	
10.102.61.110	10.102.61.110		Load Balancing	lbvs_521#52.1.1.1:80		test_1#10.102.61.110:80	
10.102.61.110	10.102.61.110		Load Balancing	SG_HS_DNS_MON#1.2.22.2:80			sc1
10.102.61.110	10.102.61.110		Load Balancing	SG_HS_DNS_MON#1.3.4.5:80			
10.102.61.110	10.102.61.110		Load Balancing	atest94#1.1.1.11:80			
10.102.61.110	10.102.61.110		Load Balancing	lbvs1_101#1.10.1.1:80			
10.102.61.110	10.102.61.110		Load Balancing	lbvs1_1010#1.10.1.10:80			
10.102.61.110	10.102.61.110		Load Balancing	lbvs1_10100#1.10.1.100:80			
10.102.61.110	10.102.61.110		Load Balancing	lbvs1_10101#1.10.1.101:80			
10.102.61.110	10.102.61.110		Load Balancing	lbvs1_10102#1.10.1.102:80			
10.102.61.110	10.102.61.110		Load Balancing	lbvs1_10103#1.10.1.103:80			

b) レポートの生成とエクスポートを定期的にスケジュールするには、[レポートのスケジュール] タブを選択します。レポート生成の繰り返し設定を指定し、レポートのエクスポート先のメールプロファイルを作成します。

- i. 繰り返し-ドロップダウンリストボックスから [毎日]、[毎週]、または [毎月] を選択します。
- ii. 繰り返し時間-時間を 24 時間形式で時間: 分として入力します。
- iii. メールプロファイル-ドロップダウンリストボックスからプロファイルを選択するか、+ をクリックしてメールプロファイルを作成します。

[スケジュールを有効にする] をクリックしてレポートをスケジュールし、[ **OK** ] をクリックします。[ **Enable Schedule** ] チェックボックスをオンにすると、選択したレポートを生成できます。



## ← Generate Report

Export Now  Schedule Export

You can schedule the export of the reports to specified email addresses at various intervals for the following selected Network Functions

- Load Balancing
- Content Switching
- Cache Redirection
- Authentication
- Citrix Gateway
- GSLB

**Schedule Details**

Recurrence\*

**NOTE:** Enter the schedule time in your selected timezone

Export time\*

Email

Email Profile\*

Slack

Enable Schedule

### ネットワークレポート作成

February 6, 2024

NetScaler Application Delivery Management (NetScaler ADM) でネットワークレポートを監視することで、リソースの使用状況を最適化できます。多数のアプリケーションを複数の場所に展開する、分散展開環境を使用する場合があります。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、複数の Citrix Application Delivery Controller (NetScaler ADC) インスタンスをデプロイして、負荷分散、コンテンツの切り替え、またはトラフィックの圧縮を行っています。ネットワークのパフォーマンスは、アプリケーションのパフォーマンスに影響を与える可能性があります。アプリケーションのパフォーマンスを維持し続けるには、ネットワークパフォーマンスを定期的に監視し、すべてのリソースが最適に使用されていることを確認する必要があります。

NetScaler ADM では、グローバルレベルのインスタンスだけでなく、仮想サーバーやネットワークインターフェイスなどのエンティティのレポートを生成できるようになりました。インスタンスファミリーは、NetScaler ADC インスタンスと SD-WAN インスタンスの両方で構成されます。レポートを生成できる仮想サーバーは次のとおりです。

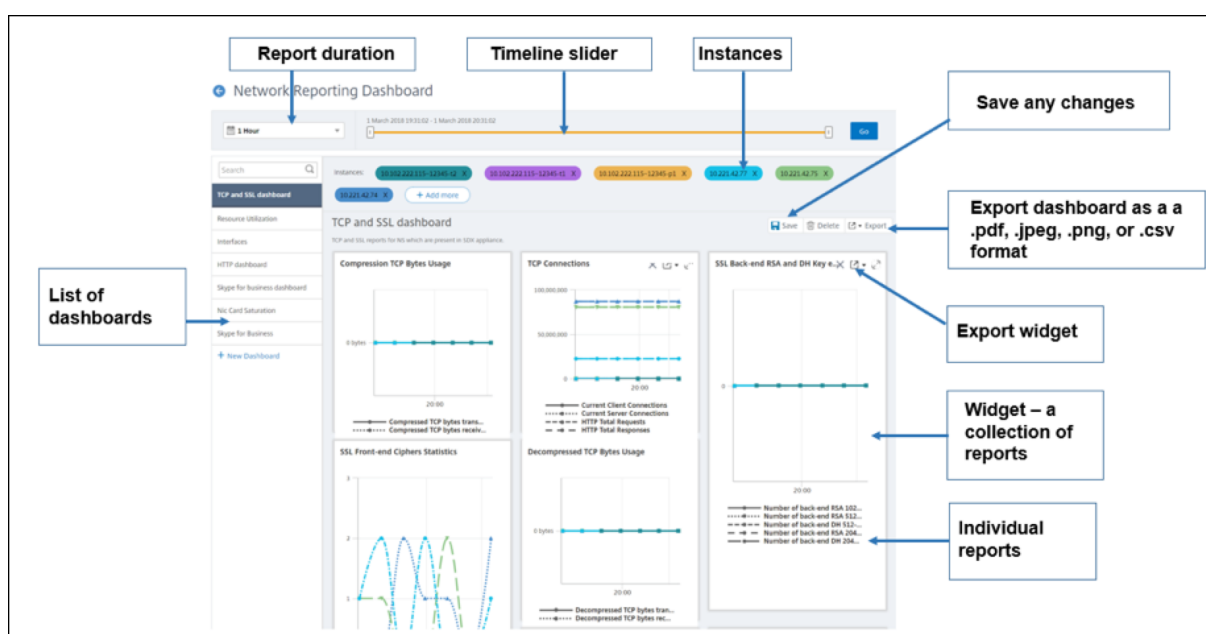
- サーバ、サービス、およびサービスグループの負荷分散

- コンテンツ・スイッチ・サーバ
- キャッシュリダイレクションサーバ
- グローバルサービス負荷分散 (GSLB)
- 認証
- NetScaler Gateway

NetScaler ADM のネットワークレポートダッシュボードは高度にカスタマイズ可能です。さまざまなインスタンス、仮想サーバ、その他のエンティティ用に複数のダッシュボードを作成できるようになりました。

### ネットワークレポートダッシュボード

次の図は、ダッシュボードのさまざまな機能を示しています。



左側のパネルには、NetScaler ADM で作成されたすべてのカスタムダッシュボードが表示されます。これらのいずれかをクリックすると、ダッシュボードを構成するさまざまなレポートを表示できます。たとえば、TCP および SSL ダッシュボードには、TCP および SSL プロトコルに関連するさまざまなレポートが含まれています。

複数のウィジェットを使用して各ダッシュボードをカスタマイズして、さまざまなレポートを表示できます。ウィジェットは、より関連性のあるレポートのコレクションであるダッシュボード上のレポートを表します。たとえば、圧縮 TCP バイト使用状況レポートには、1 秒あたりに送受信された圧縮された TCP バイト数のレポートが含まれます。

1 時間、1 日、1 週間、または 1 か月のレポートを表示できます。さらに、タイムラインスライダーオプションを使用して、NetScaler ADM で生成されるレポートの期間をカスタマイズできるようになりました。

「X」をクリックすると、レポートを削除できます。レポートを .pdf、.jpeg、.png、.csv 形式でシステムにエクスポートすることもできます。また、レポートを生成する必要がある時刻と繰り返しをスケジュールすることもできます。また、レポートの送信先となる電子メール配布リストを構成することもできます。

ダッシュボードの上部にある [Instances] 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。

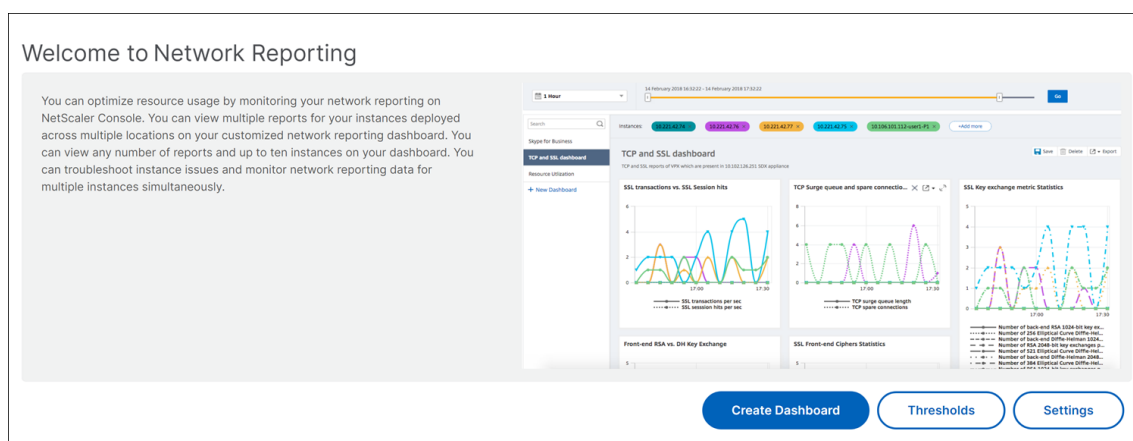
をクリックしてインスタンスを削除するか、レポートにインスタンスを追加できます。しかし、現在、NetScaler ADM では、10 インスタンスのレポートを表示できます。

ダッシュボード全体を .pdf、.jpeg、.png、.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られた変更はすべて保存する必要があります。[保存] をクリックして変更を保存します。

次のセクションでは、ダッシュボードの作成、レポートの生成、およびレポートのエクスポートの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手順は、次のとおりです。

1. NetScaler ADM で、[ネットワーク] > [ネットワークレポート] に移動します。



2. 既存のダッシュボードを表示するには、[ダッシュボードの表示] をクリックします。[ネットワークレポートダッシュボード] ページが開き、すべてのダッシュボードとレポートウィジェットを表示できます。
3. ダッシュボードを作成するには、[新規ダッシュボード] をクリックします。「ダッシュボードの作成」ページが開きます。

← Create Dashboard

Basic Settings Select Reports Select Entities

Name\*

Example Dashboard ⓘ

Instance Family

Citrix ADC  Citrix SD-WAN  Citrix ADC SDX

Type\*

Global ⓘ

Global

Interface

Authentication Virtual Servers

Cache Redirection Virtual Servers

Citrix Gateway Virtual Servers

Content Switching Virtual Servers

GSLB Virtual Servers

Load Balancing Services

Load Balancing Virtual Servers

Cancel Next →

4. [基本設定] タブで、次の詳細を入力します:
  - a) 名前。ダッシュボードの名前を入力します。
  - b) インスタンスファミリー。インスタンスのタイプ (Citrix ADC、Citrix SD-WAN、または Citrix ADC SDX) を選択します。
  - c) タイプ。レポートを生成するエンティティタイプを選択します。この例では、負荷分散仮想サーバーを選択します。
  - d) 【説明】。ダッシュボードの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。インスタンスと特定のエンティティでサポートされているすべてのレポートが表示されます。

6. [レポートの選択] タブで、必要なレポートを選択します。この例では、トランザクション、接続、スループットを選択できます。[次へ] をクリックします。

Select target reports that you want to add to your custom dashboard.

<input type="checkbox"/>	Name	Description
<input checked="" type="checkbox"/>	Transactions	Hits rate of Load Balancing virtual servers
<input checked="" type="checkbox"/>	Connections	Connection reports contains Client Connections, Server Connections,
<input checked="" type="checkbox"/>	Throughput	Throughput reports contains Packets Received/s, Packets Sent/s, Requ
<input type="checkbox"/>	SSL Traffic	SSL counters Session Hits/s, Packets Sent/s, Request Bytes/s and Repc

Buttons: Cancel, Back, Next

1. [エンティティの選択] タブで、[追加] をクリックします。

[基本設定] タブで選択したエンティティタイプに応じて、エンティティリストを含むウィンドウが表示されます。この例では、「LB 仮想サーバーの選択」ウィンドウが表示されます。

2. 監視するエンティティを選択します。

Choose LB Virtual Servers

Buttons: Select, Close

<input type="checkbox"/>	Instance	Host Name	Name	Throughput (Mbps)	Virtual IP Address
<input checked="" type="checkbox"/>	10.106.118.120	-NA-	v_120_1_148	0	2.120.1.148
<input checked="" type="checkbox"/>	10.106.118.120	-NA-	v_120_3_28	0	2.120.3.28
<input checked="" type="checkbox"/>	10.102.238.89-p1	-NA-	tcpvip4	0	100.1.1.60
<input checked="" type="checkbox"/>	10.106.118.120	-NA-	v_120_4_68	0	2.120.4.68
<input checked="" type="checkbox"/>	10.106.118.120	-NA-	v_120_6_130	0	2.120.6.130
<input checked="" type="checkbox"/>	10.106.118.120	-NA-	v_120_5_21	0	2.120.5.21
<input checked="" type="checkbox"/>	10.106.118.120	-NA-	v_120_2_21	0	2.120.2.21
<input checked="" type="checkbox"/>	10.106.118.120	-NA-	v_120_5_147	0	2.120.5.147

3. [作成] をクリックします。

ダッシュボードが作成され、選択したすべてのレポートが表示されます。

**注:**

現在のところ、凡例またはフィルタに加えた変更は保存できません。

### ネットワークレポートのエクスポート

ウィジェットレポートは.pdf、.png、.jpeg、または.csv形式でエクスポートできますが、ダッシュボード全体は.pdf、.jpeg、または.png形式でのみエクスポートできます。

**注**

読み取り専用権限を持っている場合、NetScaler ADM でレポートをエクスポートすることはできません。NetScaler ADM でファイルを作成したり、ファイルをエクスポートしたりするには、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、次の手順に従います。

1. [ネットワーク]>[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、「ダッシュボード 1」をクリックします。
4. 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。
5. [今すぐエクスポート] タブで、必要な形式を選択し、[エクスポート] をクリックします。

[エクスポート] ページでは、次のいずれかの操作を実行できます：

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 形式で表示して保存します。
7. [スケジュールエクスポート] 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、電子メールまたは余裕期間メッセージでレポートを送信するには。

[ **Network Reporting** ] ダッシュボードページのエクスポートを繰り返し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。その後、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。ユーザーが設定した場合、レポートは時刻と日付のスタンプを上書きします。

**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平日を必ず選択してください。
- [ 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カ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ときに、件名フィールドにテキスト文字列を入力して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刻に作成されたレポートには、この文字列が名前になります。

たとえば、特定の仮想サーバからのネットワークレポートの場合、サブジェクトに「認証レポート-10.106.118.120」と入力します。ここで、10.106.118.120 は監視対象の仮想サーバの IP アドレスです。

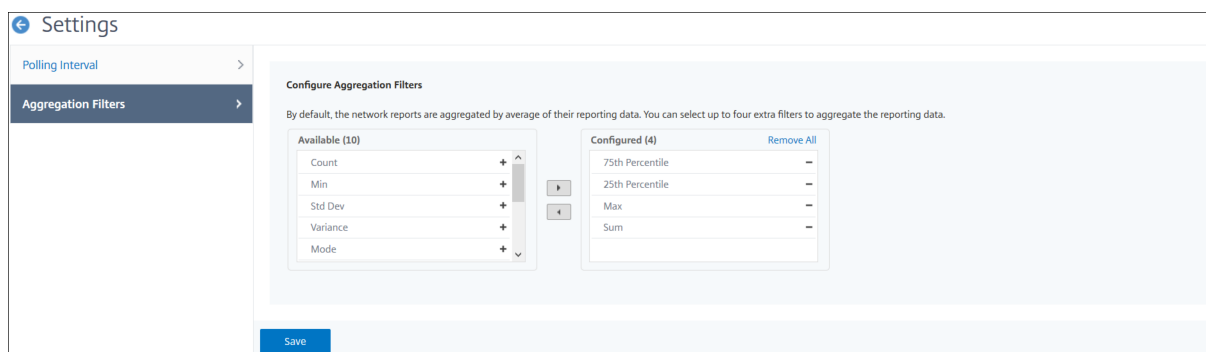
注:

現在、このオプションはレポートのエクスポートをスケジュールしている場合にのみ使用できます。即座にエクスポートするときに、レポートに見出しを追加することはできません。

### 集約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約を適用し、ダッシュボードでアプリケーションの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。これらの集計をデータに適用すると、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し、確認することができます。[ネットワーク] > [ネットワークレポート] に移動し、1 日以降の期間を選択すると [表示別] オプションが表示されます。

既存の平均データでは、「表示別」( **View By**) リストからオプションを選択して集計を適用できます。集計を適用すると、ダッシュボードの各指標のデータが更新されます。[設定] をクリックし、[集約フィルタ] を選択します。



追加できる集計を次に示します。

- Count
- 最大
- 最小
- SUM
- 標準開発
- 差異
- Mode
- 中央値
- 第 25 パーセンタイル
- 第 75 パーセンタイル

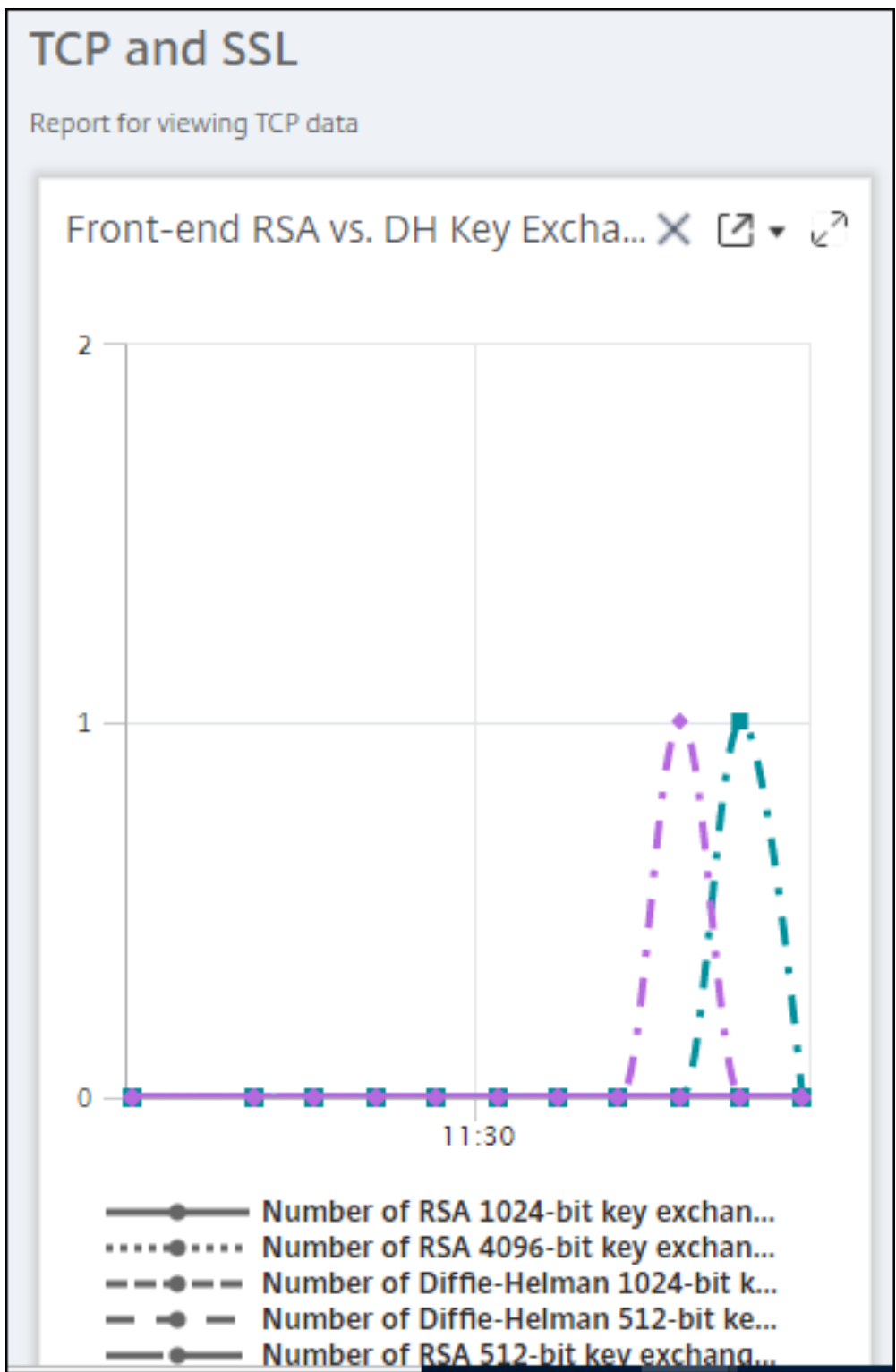
- 第 95 パーセンタイル
- 第 99 パーセンタイル
- 第 1
- 最終

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。集約オプションを追加した後、選択した集約オプションのレポートが生成されるまでに約 1 時間かかります。

ウィジェット・レポートをエクスポートするには、次の手順に従います。

1. [ネットワーク]>[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、「**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. [今すぐエクスポート] タブで、必要な形式を選択し、[エクスポート] をクリックします。





## NetScaler ADM でネットワークレポートのしきい値を管理する方法

NetScaler ADC インスタンスの状態を監視するには、カウンタにしきい値を設定し、しきい値を超えたときに通知を受け取ることができます。NetScaler ADM では、しきい値を設定したり、表示、編集、削除したりできます。

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のしきい値を定義できます。選択したインスタンスから特定のカウンタメトリックス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 (ルールで指定された) しきい値を超えるか下回ると、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、[ネットワーク]>[イベント]>[\*\* レポート] に移動すると表示できます。「レポート」ページで、「重要度別のイベント \*\*」ドーナツをクリックすると、イベントを重要度別に表示できます。

また、しきい値を超えたときに電子メールや SMS メッセージを送信するなど、アクションをしきい値に関連付けることもできます。

しきい値を作成するには、次の手順に従います。

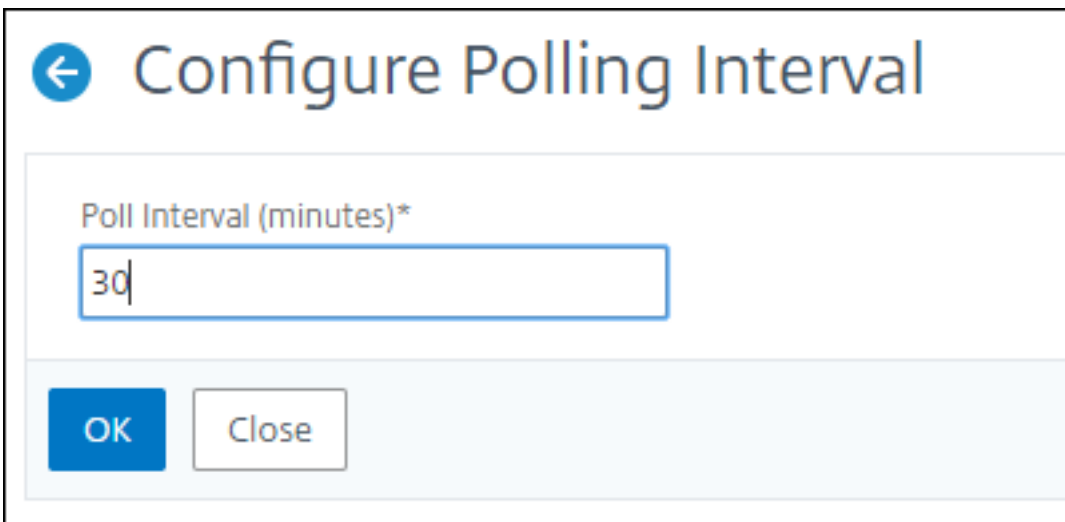
1. Citrix ADM で、[ネットワーク] > [ネットワークレポート] > [しきい値] に移動します。[Thresholds] の [Add] をクリックします。
2. [しきい値の作成] ページで、次の詳細を指定します。
  - 名前。しきい値の名前。
  - インスタンスタイプ。Citrix ADC または Citrix SD-WAN WO を選択してください。
  - レポート名。このしきい値に関する情報を提供するパフォーマンスレポートの名前。
3. また、イベントを生成またはクリアするタイミングを指定するルールを設定することもできます。「ルールの設定」セクションでは、次の詳細を指定できます。
  - メトリック。しきい値を設定する指標を選択します。
  - コンパレータ。比較器を選択して、監視対象値が閾値以上か、それ以下かをチェックします。
  - しきい値。イベントの重要度を計算する基準となる値を入力します。たとえば、現在のクライアント接続の監視対象の値が 80% に達すると、重大なイベント重大度を持つイベントを生成することができます。この場合、しきい値として 80 を入力します。「重大度」イベントは、[ネットワーク]>[イベント]>[\*\* レポート \*\*] に移動すると表示できます。「レポート」ページで、「重要度別のイベント」ドーナツをクリックすると、イベントを重要度別に表示できます。
  - 明確な価値。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% に達すると、現在のクライアント接続のしきい値をクリアすることができます。この場合、クリア値として 50 を入力します。
  - イベントの重要度。閾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の IP アドレスを選択します。
5. イベントメッセージを追加することもできます。しきい値に達したときに表示するメッセージを入力します。NetScaler ADM により、監視対象の値としきい値がこのメッセージに追加されます。

6. アラームを生成するためのしきい値を有効にするには、**[Enable]** を選択します。
7. オプションで、メールや Slack 通知、またはメールと Slack 通知の両方などのアクションを設定できます。
8. [作成] をクリックします。

#### ネットワークレポートのパフォーマンスポーリング間隔の設定

デフォルトでは、NITRO 呼び出しは 5 分ごとにネットワークレポート用のパフォーマンスデータを収集します。ADM は、カウンタ情報などのインスタンス統計を取得し、1 分単位、時間単位、日単位、週単位で集計します。この集計データを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、[ネットワーク]>[ネットワークレポート]に移動し、[ポーリング間隔の設定]をクリックします。ポーリング間隔は 5 分未満または 60 分を超えることはできません。



← Configure Polling Interval

Poll Interval (minutes)\*

30

OK Close

#### ネットワークレポートプルーニング設定の構成

NetScaler ADM でネットワークレポートデータの消去間隔を構成できます。この設定では、NetScaler ADM サーバーのデータベースに保存されるネットワークレポートデータの量を制限します。デフォルトでは、ネットワークが履歴データをレポートする場合、プルーニングは 24 時間ごと（01.00 時間ごと）実行されます。

#### 注

指定できる値は、90 日を超えるか、1 日未満にすることはできません。

#### ADM 監査ログを使用してインフラストラクチャの管理と監視

February 6, 2024

Citrix ADM サービスを使用して、ADM のすべてのイベントと、ADM が管理する ADC インスタンスで生成された syslog イベントを追跡できます。これらのメッセージは、インフラストラクチャの管理と監視に役立ちます。ただし、ログメッセージは確認して初めて優れた情報源となり、ADM ではログメッセージの確認方法が簡略化されます。

フィルターを使用して ADM Syslog メッセージと監査ログメッセージを検索できます。フィルターは結果を絞り込み、探しているものを正確かつリアルタイムに見つけるのに役立ちます。組み込みの検索ヘルプでは、ログを絞り込むことができます。ログメッセージを表示するもう 1 つの方法は、ログメッセージを PDF、CSV、PNG、および JPEG 形式でエクスポートすることです。また、指定した電子メールアドレスにさまざまな間隔でこれらのレポートをエクスポートするようにスケジュールすることもできます。

ADM GUI では、次の種類のログメッセージを確認できます。

- ADC インスタンス関連の監査ログ
- ADM 関連の監査ログ
- アプリケーション監査ログ

### **ADC** インスタンス関連の監査ログ

ADM からの ADC インスタンス関連の syslog メッセージを表示する前に、Citrix ADM サービスを Citrix ADC インスタンスの syslog サーバーとして構成します。設定が完了すると、すべての syslog メッセージがインスタンスから ADM にリダイレクトされます。

### **ADM** サービスを **Syslog** サーバーとして設定する

ADM を syslog サーバとして設定するには、次の手順を実行します。

1. ADM GUI から、[ネットワーク] > [インスタンス] に移動します。
2. Syslog メッセージを収集して NetScaler ADM に表示する NetScaler ADC インスタンスを選択します。
3. 「アクションの選択」リストで、「**Syslog** の設定」を選択します。
4. [有効にする] をクリックします。
5. ファシリティ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。

以下の手順では、NetScaler ADC インスタンス内のすべての syslog コマンドを構成し、NetScaler ADM が 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、[ネットワーク] > [イベント] > **[Syslog メッセージ]** に移動します。[ヘルプが必要ですか?] をクリックします。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。

OPERATOR	DESCRIPTION	EXAMPLE
=	Equals to some value	Abc = '100'
-	Contains some value	Abc - '100'

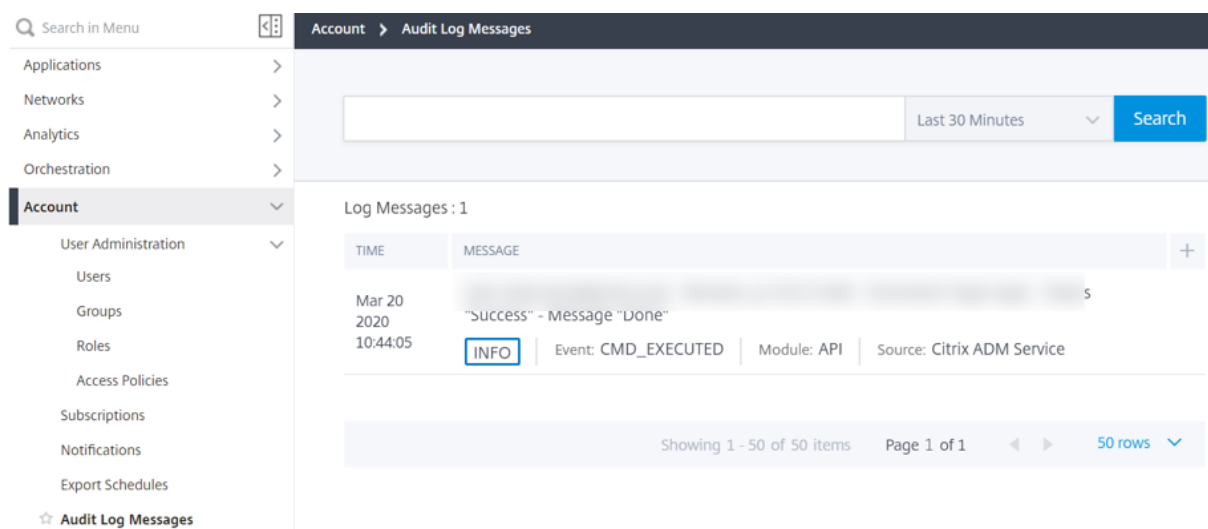
OPERATOR	DESCRIPTION	EXAMPLE
AND	Requires both to be true	A = '1' AND B = '2'
OR	Requires one to be true	A = '1' OR B = '2'

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、[今すぐエクスポート] または [エクスポートのスケジュール] をクリックします。詳細については、「[Syslog メッセージの表示とエクスポート](#)」を参照してください。

## ADM 関連の監査ログ

ADM は、事前設定されたルールに基づいて、上の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できるようにします。ADM にあるすべての監査ログメッセージを表示するには、[システム] > **[監査ログメッセージ]** に移動します。



ログメッセージをエクスポートするには、右上隅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 ADM アプリケーションまたは特定のアプリケーションの監査ログメッセージを表示できます。

- ADM に存在するすべてのアプリケーションのすべての監査ログメッセージを表示するには、[ネットワーク] -> [ネットワーク機能] > [監査] に移動します。
- ADM 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、[アプリケーション] > [ダッシュボード] > [仮想サーバーをダブルクリックする] > [監査ログ] に移動します。

### 分析

February 6, 2024

Citrix ADM Analytics 機能を使用すると、Citrix ADC のさまざまな洞察を簡単かつスケーラブルに調べて、アプリケーションのパフォーマンスを分析および改善できます。NetScaler ADM では、1 つ以上の分析機能を同時に使用できます。

次の表では、Citrix ADM でサポートされているさまざまな分析機能について説明します。

分析機能	説明
Web Insight	Web Insight を使用すると、エンタープライズ Web アプリケーションを可視化し、Citrix ADC のすべての Web アプリケーションを監視できます。管理者は、アプリケーションを統合的かつリアルタイムで監視できます。
HDX insight	HDX Insight は、NetScaler ADC 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、クライアントとネットワークの遅延メトリクス、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リアルタイムで表示し、パフォーマンス問題のトラブルシューティングを行うことができます。
Gateway Insight	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。
Security Insight	Security Insight は、アプリケーションのセキュリティ状況を判断し、是正処置を実施してアプリケーションを保護するための統一管理コンソールソリューションです。
SSL Insight	SSL Insight は、安全な Web トランザクション (HTTPS) を可視化し、Citrix ADC のすべての安全な Web アプリケーションを監視できるようにします。管理者は、安全なウェブトランザクションを統合的かつリアルタイムかつ履歴的に監視できます。
TCP Insight	TCP Insight は、データ転送におけるネットワークの輻輳を回避するために Citrix ADC インスタンスで使用される最適化手法と輻輳制御戦略（またはアルゴリズム）のメトリックを監視するための簡単でスケーラブルなソリューションを提供します。
Video Insight	Video Insight 機能は、Citrix ADC アプライアンスで使用されるビデオ最適化手法のメトリックを監視して、カスタマーエクスペリエンスと運用効率を向上させ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。

## WAN Insight

WAN Insight の分析機能を使用すると、管理者はデータセンターと Branch WAN 最適化アプライアンス間を流れる高速および非高速の WAN トラフィックを容易に監視できます。また、WAN Insight は、ネットワーク上のクライアント、アプリケーション、ブランチを可視化して、ネットワークの問題を効果的にトラブルシューティングできるようにします。

## ライセンス要件

February 6, 2024

次の表は、NetScaler ADM のさまざまな分析レポートを表示するための NetScaler ADC インスタンスのライセンス要件を示しています。

NetScaler ADM アナリティクスの機能	Citrix ADC ライセンス要件
Web Insight	NetScaler ADM に関する Web Insight レポートは、すべての NetScaler ADC ライセンスエディション（スタンダード/アドバンスド/プレミアム）でサポートされています。
HDX Insight	NetScaler ADM に関する HDX Insight レポートは、アドバンスエディション（1 時間未満のレポート用）またはプレミアムエディション（レポートが無制限の場合）の NetScaler ADC ライセンスのいずれかでサポートされます。注: Standard ライセンスエディションはサポートされていません。
Security Insight	NetScaler ADM のセキュリティインサイトレポートは、App Firewall ライセンスのプレミアムエディションまたはアドバンスエディションでサポートされています。注: 標準ライセンスエディションおよびスタンドアロン App Firewall ライセンスはサポートされていません。
SSL Insight	NetScaler ADM の SSL Insight レポートは、すべての NetScaler ADC ライセンスエディション（スタンダード/アドバンスド/プレミアム）でサポートされています。



NetScaler ADM アナリティクスの機能	Citrix ADC ライセンス要件
Gateway Insight	NetScaler ADM の Gateway Insight レポートは、アドバンスエディション（1 時間未満のレポート用）またはプレミアムエディション（無制限のレポート用）の NetScaler ADC ライセンスのいずれかでサポートされています。注: Standard ライセンスエディションはサポートされていません。
TCP Insight	TCP Insight レポートは、すべての NetScaler ADC ライセンスエディション（スタンダード/アドバンスト/プレミアム）でサポートされています。
Video Insight	NetScaler ADM に関するビデオインサイトレポートは、Citrix ADC プレミアム（VPX-T 1000 シリーズ、VPX-T）エディションでサポートされています。
WAN Insight	Citrix ADM に関する WAN インサイトレポートは、Citrix SD-WAN WO エディション (WAN 最適化エディション) でサポートされています。

## ログストリームの概要

February 6, 2024

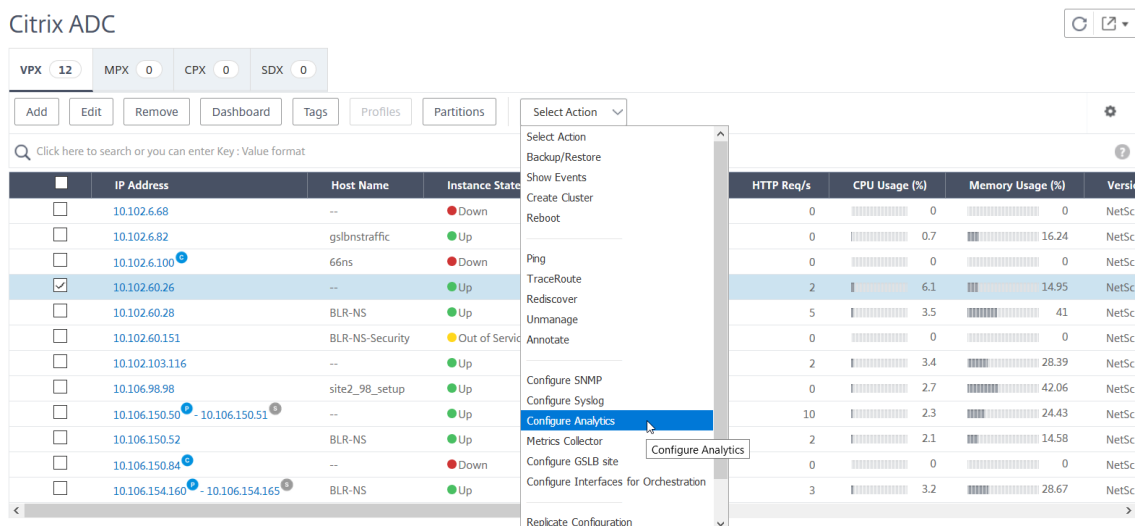
NetScaler ADC インスタンスは AppFlow レコードを生成し、データセンター内のすべてのアプリケーショントラフィックの中央制御ポイントとなります。IPFIX とログストリームは、Citrix ADC インスタンスから Citrix ADM にこれらの AppFlow レコードを転送するプロトコルです。詳細については、[AppFlow](#) を参照してください。

- IPFIX (IPFIX) は、RFC 5101 で定義されているオープンなインターネット技術タスクフォース (IETF) 規格である。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ています。IPFIX は UDP プロトコルを使用するため、IPFIX 標準に準拠すると、NetScaler ADM でより多くのリソースを処理することになります。
- Logstream は、Citrix が所有するプロトコルで、分析ログデータを Citrix ADC インスタンスから Citrix ADM に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ており、データ処理に必要なリソースも少なく済みます。

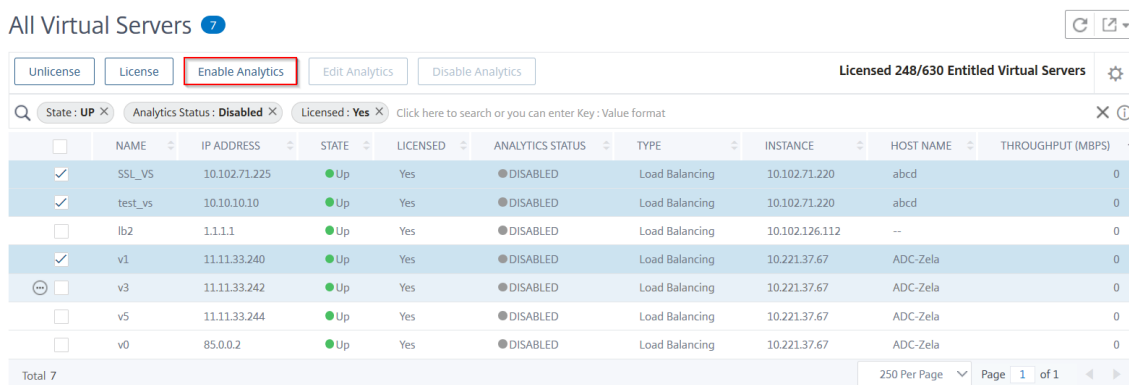
**11.1** ビルド **47.14** から **11.1** ビルド **62.8** までの **CitrixADC** では、ログストリームが Web Insight (HTTP) を有効にするデフォルトのトランスポートモードであり、IPFIX は他のインサイトを有効にする唯一のトランスポートモードです。**12.0** から最新バージョンの Citrix ADC では、転送モードとしてログストリームまたは **IPFIX** のいずれかを選択できます。

ログストリームを転送モードとして有効にする

1. [ネットワーク]>[インスタンス]に移動し、分析を有効にする ADC インスタンスを選択します。
2. [アクションの選択] リストから、[ **Analytics** の設定] を選択します。



3. 仮想サーバーを選択し、[ **Analytics** を有効にする] をクリックします。



4. [ **Analytics** の有効化] ウィンドウで、次の操作を行います。
  - a) インサイトタイプ (Web Insight または Security Insight) を選択します。
  - b) **Logstream** をトランスポートモードとして選択

注

**11.1** ビルド **47.14** から **11.1** ビルド **62.8** までの CitrixADC では、ログストリームが Web Insight (HTTP) を有効にするデフォルトのトランスポートモードであり、IPFIX は他のインサイトを有効にする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の Citrix ADC では、転送モードとしてログストリームまたは **IPFIX** のいずれかを選択できます。

- c) 式はデフォルトで true です

d) **[OK]** をクリックします

Enable Analytics
✕

**Selected Virtual Server - Load Balancing: 3**

Web Insight

Security Insight

▼ Advanced Options

Transport Mode

Logstream     IPFIX

Instance level options

Enable HTTP X-Forwarded-For

Citrix Gateway

▼ Expression Configuration

Select expression for Load Balancing/Content Switching

Select Expression

Edit Expression

true

OK

Close

注

- ライセンスされていない仮想サーバーを選択すると、NetScaler ADM はまずそれらの仮想サーバーのライセンスを取得し、次に分析を有効にします。
- 管理パーティションでは、**Web Insight** のみがサポートされます
- キャッシュリダイレクト、認証、GSLB などの仮想サーバーでは、分析を有効にすることはできません。エラー・メッセージが表示される

次の表では、転送モードとして Logstream をサポートする Citrix ADM の機能について説明します：

機能	IPFIX	Logstream
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	未サポート	•
CR Insight	•	•
IP レピュテーション	•	•
AppFirewall	•	•
クライアント側の測定	•	•
Syslog/Auditlog	•	•

## URL データ収集を無効にする

February 6, 2024

Citrix Application Delivery Management (ADM) のダッシュボードの Web Insight ノードに URL レポートを表示したくない場合は、URL データ収集を無効にできます。

### NetScaler ADM からの URL データ収集を無効にするには

1. Citrix ADM で、[分析] > [設定] に移動し、[分析データレコードログの設定] をクリックします。
2. **[Web Insight URL Data Collection Settings]** セクションで **[Enable URL Data Collection]** オプションがオンになっている場合は、このチェックボックスをオフにします。
3. **[OK]** をクリックします。

← Configure Analytics Data Record Logs

**Data Record Log Settings**

Data record logs provide detailed information about appflow records that Application Delivery Management collects from the Citrix ADCs.

- Enable HDX Insight Logs ?
- Enable Web Insight Logs
- Enable CB WAN Insight Logs
- Enable Security Insight Logs
- Enable Video Insight Logs
- Enable TCP Insight Logs

**Web Insight Report Settings**

Select the Web Insight entities for which you want to view reports on the dashboard.

- Show HTTP Request Method Report
- Show HTTP Response Status Report
- Show User Agent Report
- Show Operating System Report
- Show Domain Report

**Web Insight URL Data Collection Settings**

If you do not want the URL reports to be displayed on the Web Insight node of the dashboard, disable the URL data collection settings.

- Enable URL Data Collection ?

## しきい値およびアラートの作成

February 6, 2024

しきい値とアラートを設定して、Citrix ADC インスタンスの状態を監視できます。カウンターにしきい値を設定して、インスタンスや管理対象インスタンスのエンティティを監視できます。

カウンターの値がしきい値を超えると、Citrix Application Delivery Management (ADM) はパフォーマンス関連の問題を通知するイベントを生成します。カウンターの値がしきい値で指定されているクリア値に一致するとイベントは消去されます。これは、そのしきい値が通常の状態に戻ったことを意味します。

しきい値にアクションを割り当てることもできます。アクションには、アラート、メール、SMS 通知の送信があります。しきい値を超えると、Citrix ADM は、アラートの有効化や電子メールまたは SMS 通知の送信など、ユーザーが定義したアクションを自動的に実行します。

**NetScaler ADM** を使用してしきい値およびアラートを作成するには:

1. NetScaler ADM で、**[Analytics]** > **[設定]** > **[しきい値]** に移動します。**[Thresholds]** の **[Add]** をクリックします。
2. 「しきい値の作成」ページで、次の詳細を指定します。
  - **Name** - しきい値の構成の名前
  - **Traffic Type** - しきい値を設定するトラフィックのタイプ。
  - **Entity** - しきい値構成時のカテゴリまたはリソースの種類

- **Reference Key** - トラフィックの種類とエンティティの選択に基づいて自動的に生成される値
- **Duration** - しきい値構成時の間隔
- **[ Configure Rule ]**: しきい値を構成するメトリックのルール。
- 通知設定 -しきい値を有効にし、しきい値を超えたときに電子メール、余裕期間、または SMS などのさまざまなチャネルを介して通知を受信します。

3. [作成] をクリックします。

HDX insight では、構成されたしきい値にすべてのエンティティが違反した場合にのみアラートが生成される、複数のしきい値を設定することもできます。

## 適応しきい値の設定

February 6, 2024

アダプティブしきい値機能によって、各 URL の最大ヒット数のしきい値が設定されます。URL の最大ヒット数が、その URL に設定されたしきい値を超えると、外部 Syslog サーバーに Syslog メッセージが送信されます。しきい値の間隔は、日単位または週単位で指定できます。

しきい値は、次のように計算されます。

しきい値 = 最大ヒット数 × しきい値乗数

各項目の意味は次のとおりです：

- 最大ヒット数：URL のヒットの最大数。
- しきい値乗数：ユーザーが定義する整数値（デフォルト：2）。

**Citrix ADM** を使用してアダプティブしきい値を作成するには

1. Citrix ADM で、[分析] > [設定] > [適応しきい値] に移動し、[追加] をクリックします。
2. 「適応しきい値」 ページで、次のパラメータを指定します。

- **Name** - しきい値名
- エンティティ -URL
- **Duration** - しきい値の期間（日または週）
- しきい値乗数 -URL の適応しきい値を取得するために、指定した URL の最大ヒット数を乗算するユーザー定義の整数。

## データベースの永続性の構成

February 6, 2024

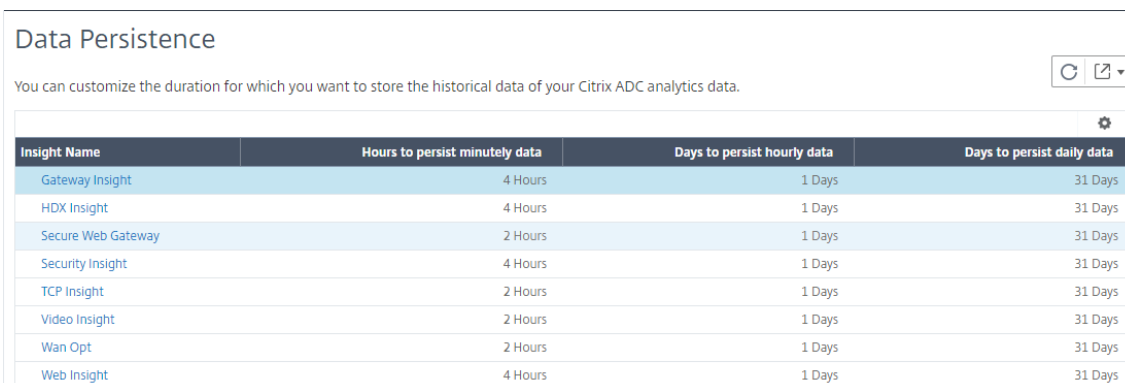
Citrix Application Delivery Management (ADM) でデータベース永続性を構成すると、Citrix ADC 分析データの履歴データを保存する期間をカスタマイズできます。分析の履歴データには、次のデータベース永続性タイプを選択できます。

- 分単位のデータを保持するのにかかる時間
- 時間単位のデータを保存する日数
- 毎日データを保持する日数

データベースの永続性を構成するには、次の手順に従います

1. [ **Analytics** ] > [ 設定 ] > [ データベースの永続性 ] に移動します。

2. データベースの永続性を構成するインサイトタイプをクリックします。



Insight Name	Hours to persist minutely data	Days to persist hourly data	Days to persist daily data
Gateway Insight	4 Hours	1 Days	31 Days
HDX Insight	4 Hours	1 Days	31 Days
Secure Web Gateway	2 Hours	1 Days	31 Days
Security Insight	4 Hours	1 Days	31 Days
TCP Insight	2 Hours	1 Days	31 Days
Video Insight	2 Hours	1 Days	31 Days
Wan Opt	2 Hours	1 Days	31 Days
Web Insight	4 Hours	1 Days	31 Days

3. Citrix ADM で Insight データを保持する期間を指定します。たとえば、Gateway Insight に関して、分析の分単位の履歴データを 2 時間保存したり、時間単位のデータを 1 日保存したりできます。

## ← Gateway Insight

Configure the duration you want to persist the Gateway Insight data for on per summarization level

Hours to persist minutely data

 ?

Days to persist hourly data

Days to persist daily data

## Analytics のセルフサービス診断

February 6, 2024

Citrix Application Delivery Management (ADM) は、セルフサービス診断を実行して、以下の分析機能について、管理対象インスタンスのライセンスと構成の問題を特定します。

- Web Insight
- HDX Insight
- Gateway Insight
- Security Insight
- SSL Forward Proxy Analytics

セルフサービス診断は 12 時間ごとに実行され、指定した分析機能ごとに問題が見つかった場合に診断レポートを生成します。診断レポートには、問題の原因、問題の種類、および問題を解決するための是正措置が記載されています。セルフサービス診断により、問題をより迅速に特定してトラブルシューティングできます。

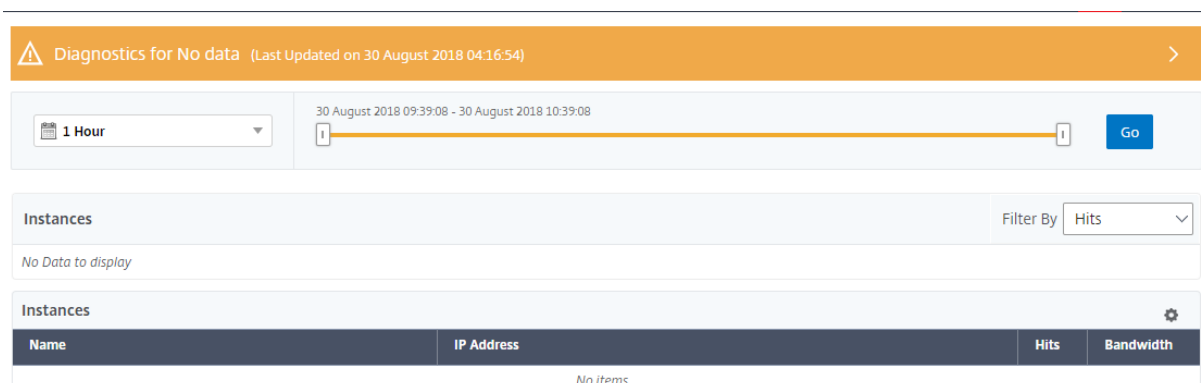
たとえば、AppFlow ポリシーが仮想サーバーにバインドされていない場合、または仮想サーバーにライセンスがない場合、NetScaler ADM は Web Insight 監視に必要なデータを取得しません。セルフサービス診断は問題を特定し、診断レポートを生成します。診断レポートを表示して問題を確認し、修正アクションを実行できます。



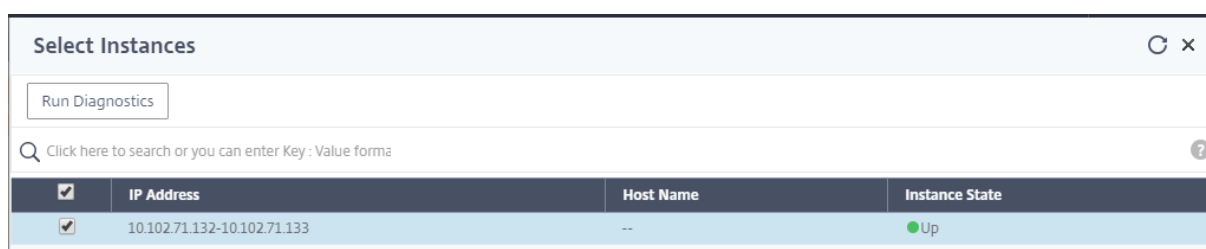
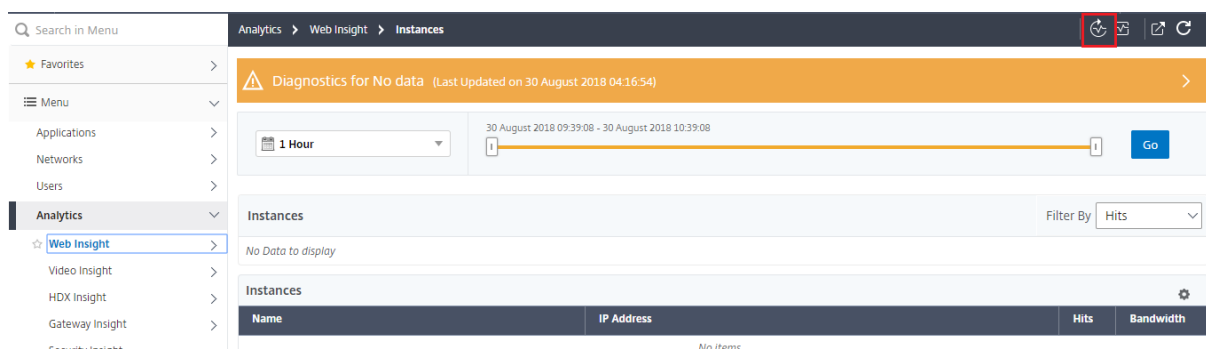
## 診断レポートを表示する

指定した分析機能の診断レポートを表示するには、NetScaler ADM ダッシュボードでそれぞれの分析ノードに移動する必要があります。

たとえば、Web Insight の診断レポートを表示するには、[分析] > [Web インサイト] に移動します。[Web Insight] ページで、[診断の表示] アイコンを選択します。



問題をチェックする場合は、インスタント診断を実行することもできます。[診断を実行] をクリックします。インスタンスを選択し、[Run Diagnostics] を選択します。



## 診断レポートの分析

セルフサービス診断では、問題の重要度に応じて、診断レポートがオレンジ色または青色の背景で表示されます。

オレンジ色の背景の診断レポートは、青色の背景よりも重要度が高いことを示しています。

たとえば、NetScaler ADC インスタンスには 5 つの仮想サーバーが設定されています。どの仮想サーバーでも AppFlow パラメーターを有効にしていない場合、NetScaler ADM は分析用の Web Insight および Security

Insight トラフィックを受信しません。セルフサービス診断では、構成の問題が重大であることが特定されます。診断レポートは、Web Insight と Security Insight 機能でオレンジ色の背景で表示されます。



いずれかの仮想サーバーで AppFlow を有効にしている場合、NetScaler ADM は分析用のデータを受信します。少なくとも 1 つの仮想サーバーが分析のためにトラフィックを送信しているため、青色の背景で診断レポートが表示されます。

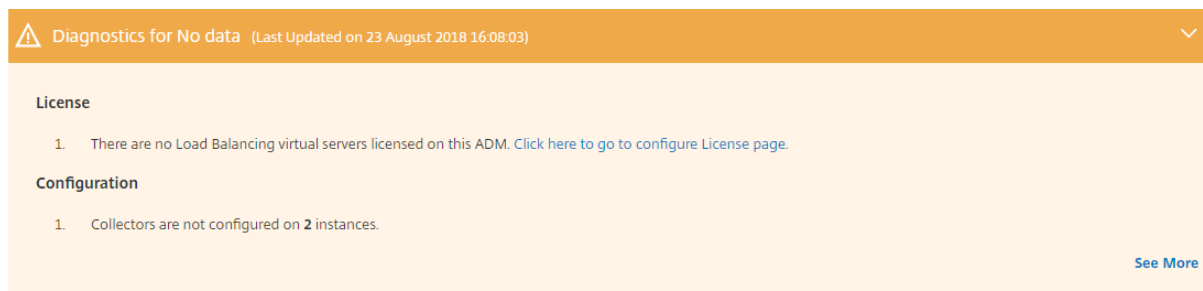


**重要:** セルフサービス診断では、トラフィックフローはチェックされません。管理対象インスタンスの指定した分析機能に関連するライセンスまたは設定の問題のみをチェックします。仮想サーバーを経由するアクティブなトラフィックがないため、分析データが表示されないことがあります。

診断レポートには、概要ページと詳細情報ページがあります。

概要ページには、問題の種類 (ライセンスまたは構成) の概要が表示されます。このページには、関連する設定ページに移動するハイパーリンクが含まれている場合があります。

たとえば、NetScaler ADM でライセンスされた負荷分散仮想サーバーがない場合、概要ページには [システムライセンス] ページへのハイパーリンクが表示されます。



問題に関する詳細情報を表示するには、サマリページの [詳細を表示] をクリックします。

詳細情報ページには、問題に関する完全な情報と、実行する必要があるアクションが推奨されます。各問題に対するハイパーリンクをクリックして、管理対象インスタンスまたは仮想サーバーを構成できます。

IP Address	Host Name	Virtual Server Name	Issue Type	Message	Action
10.102.71.150	NS150	-NA-	Configuration	This Citrix ADM or Agent is not bound to any action on the instance	Please add this Citrix ADM or Agent as collector in an action to receive data
10.102.71.150	NS150	test pooja	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.102.71.150	NS150	test pooja check with	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest5	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest77	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppTest132	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppTest194	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest95	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest30	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest29	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest35	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppTest131	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest71	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy

アクション、ホスト名、IP アドレス、問題の種類などに基づいて問題を検索することもできます。

The screenshot shows the 'Diagnostics Details' window with a search bar at the top. A red box highlights the search bar, and a dropdown menu is open below it, listing search criteria: Properties, Action, Host Name, IP Address, Issue Type, Message, and Virtual Server Name. The table below the search bar contains the same data as the previous screenshot.

問題を解決したら、インスタント診断を実行して最新の診断レポートを生成する必要があります。

## Web Insight

February 6, 2024

Web Insight を使用すると、管理者は Citrix ADC インスタンスによって提供されるすべての Web アプリケーションを監視できます。管理者は、Citrix ADC インスタンスからアプリケーションを統合的かつリアルタイムで監視できます。Web Insight は、クライアントネットワークの遅延やサーバーの応答時間などの重要な情報を提供し、アプリケーションのパフォーマンスを確実に監視および改善します。分析に使用されるデータは、Citrix ADC インスタンスによって処理される各 HTTP、HTTPS トランザクションからキャプチャされます。分析データにより、環境内の Citrix ADC インスタンス、アプリケーション、URL、クライアント、およびサーバーのパフォーマンスを分析できま

す。

Web Insight を使用してデータを表示できるユースケースには、次のようなものがあります。

- SharePoint などのアプリケーションへのアクセス中に遅延が発生しているクライアントのリスト
- 1 時間以内に最もヒット数が多かったアプリケーション
- クライアントからアクセスされたアプリケーションと URL のリスト
- 特定のクライアントが使用するオペレーティングシステムとブラウザ
- エラー関連の応答を最も多く送信するアプリケーションまたはサーバー
- 特定のクライアントでのアクセシビリティの問題
- 特定のクライアントからの少数のアプリケーションまたはすべてのアプリケーションにおけるアクセシビリティの問題
- 特定のクライアントとバックエンドサーバーからのアプリケーションのいくつかのページが遅い
- 特定のクライアントとバックエンドサーバーからアクセスすると、アプリケーションが遅くなる

選択したインスタンス上の特定の仮想サーバーに対して Web Insight を有効にして、Web アプリケーション上のトラフィックを監視できます。Web Insight 機能は、NetScaler ADM の仮想サーバーの統計情報を提供します。

Web Insight を有効にする手順は、次のとおりです。

Citrix ADM が **13.0** ビルド **41.x** 以降の場合：

1. [ネットワーク]>[インスタンス]>[**NetScaler ADC**] に移動し、インスタンスタイプを選択します。たとえば、VPX です。
2. インスタンスを選択し、[アクションの選択] リストから [**Analytics** の設定] をクリックします。
3. [仮想サーバーでの **Analytics** の設定] ページで、仮想サーバーを選択し、[**Analytics** を有効にする] をクリックします。
4. 「アナリティクスを有効にする」ウィンドウで：
  - a) **Web** インサイトを選択
  - b) **Logstream** をトランスポートモードとして選択

注

NetScaler ADC 12.0 以前の場合、**IPFIX** はトランスポートモードのデフォルトのオプションです。NetScaler ADC 12.0 以降では、トランスポートモードとして [ログストリーム] または [**IPFIX**] を選択できます。

IPFIX とログストリームの詳細については、「ログストリームの概要」を参照してください。

- c) 式はデフォルトで true です

d) **[OK]** をクリックします

Enable Analytics
✕

**Selected Virtual Server - Load Balancing: 3**

Web Insight

Security Insight

▼ Advanced Options

Transport Mode

Logstream     IPFIX

Instance level options

Enable HTTP X-Forwarded-For

Citrix Gateway

▼ Expression Configuration

Select expression for Load Balancing/Content Switching

Select Expression

▼

Edit Expression

true

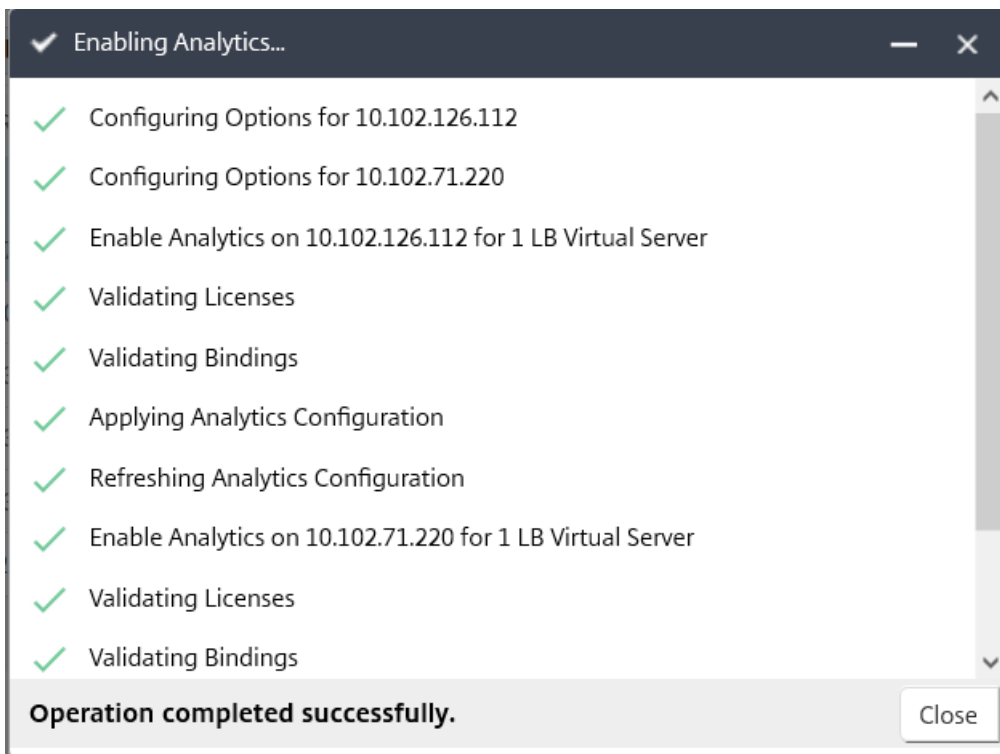
OK

Close

注

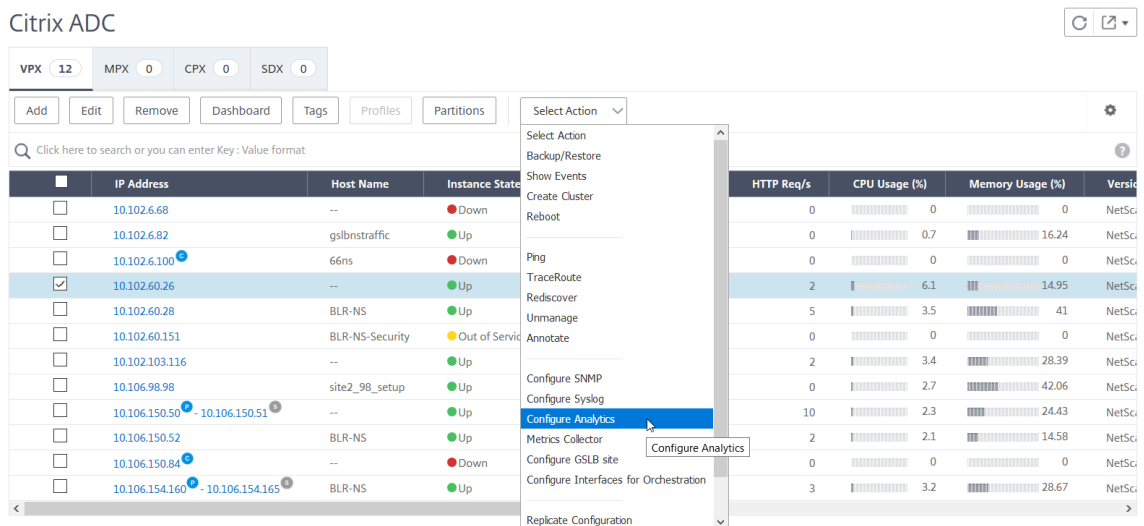
- ライセンスされていない仮想サーバーを選択すると、NetScaler ADM はまずそれらの仮想サーバーのライセンスを取得し、次に分析を有効にします。
- 管理パーティションでは、**Web Insight** のみがサポートされます
- キャッシュリダイレクト、認証、GSLB などの仮想サーバーでは、分析を有効にすることはできません。エラーメッセージが表示されます。

**[OK]** をクリックすると、NetScaler ADM は選択した仮想サーバー上で分析を有効にするために処理します。



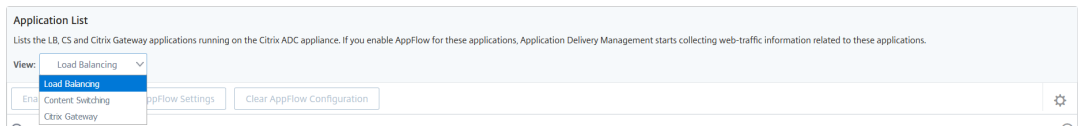
Citrix **ADM** が **13.0** ビルド **36.27** 以前の場合:

1. [ネットワーク] > [インスタンス] > [Citrix ADC] に移動し、分析を有効にする NetScaler ADC インスタンスを選択します。
2. [アクションの選択] リストから、[Analytics の設定] を選択します。

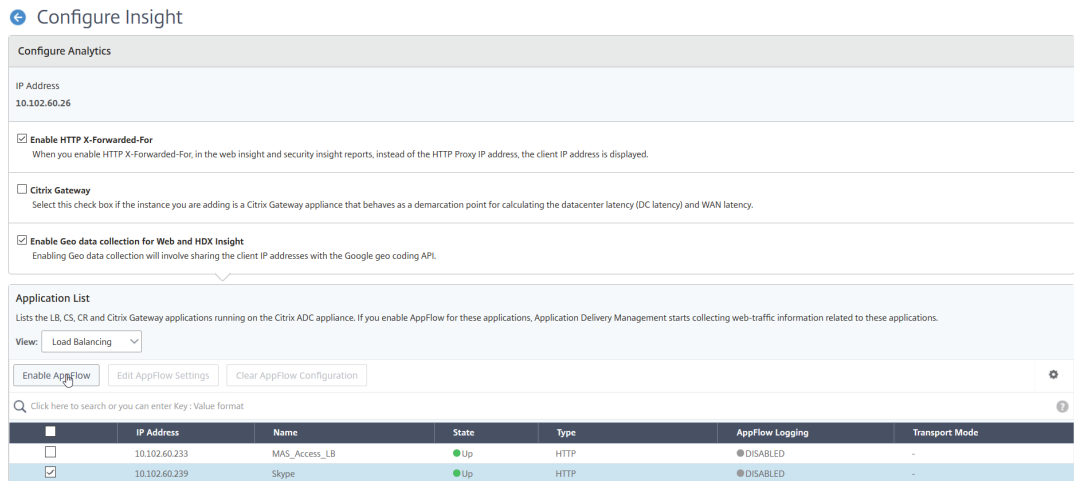


3. [\*\* Insight の設定 \*\*] ページで、次の操作を行います。

a) ロードバランシングまたはコンテンツスイッチングの アプリケーションリスト を選択します。



b) 仮想サーバーを選択し、[ **AppFlow** を有効にする ] をクリックします。



4. [AppFlow を有効にする] ダイアログボックスで、次の操作を行います。

- テキストボックスに **true** と入力します。
- 転送モードとして [ ログストリーム ] を選択します。

注: Citrix では、転送モードとして Logstream を選択することを推奨しています。

- [ **Web Insight** ] を選択し、[ **OK** ] をクリックします。

### Enable AppFlow

**Select Expression**

Load Balancing

▼

true

**Transport Mode**    IPFIX    Logstream

Web Insight  
 Client Side Measurement  
 Security Insight

If there is a firewall between Citrix ADM and the Citrix ADC instance, please make sure the TCP port 5557 is open. This is to allow ADM to collect AppFlow traffic.

OK

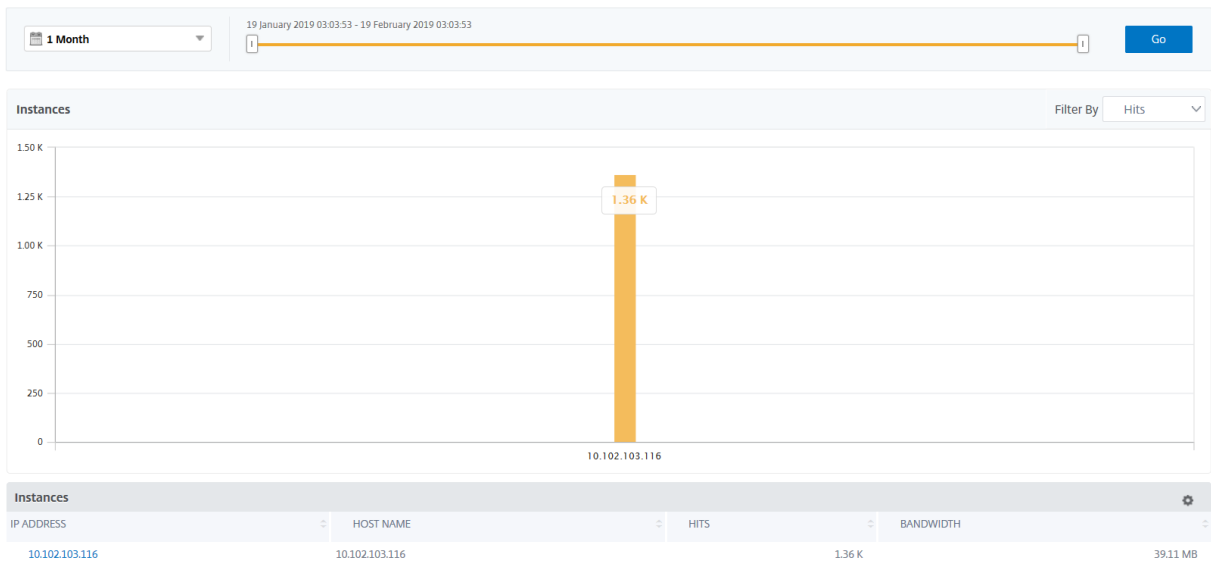
Cancel

### Web アプリケーションの問題を分析する

管理者が特定する必要がある一般的な問題の 1 つは、遅延の問題です。管理者は、遅延の問題がサーバーネットワーク、クライアントネットワーク、またはサーバーの応答時間にあるかどうかを確認する必要があります。Citrix ADM を使用すると、[分析]> [Web インサイト] に移動してこの情報を特定できます。

[Analytics]> [Web Insight] に移動すると、Web Insight が有効になっている NetScaler ADC インスタンスが表示されます。IP アドレス、ホスト名、総ヒット数、帯域幅など、インスタンスの詳細情報を表示できます。

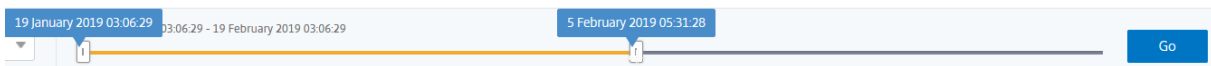




リストを使用して、インスタンスのインサイトを表示する期間を選択できます。

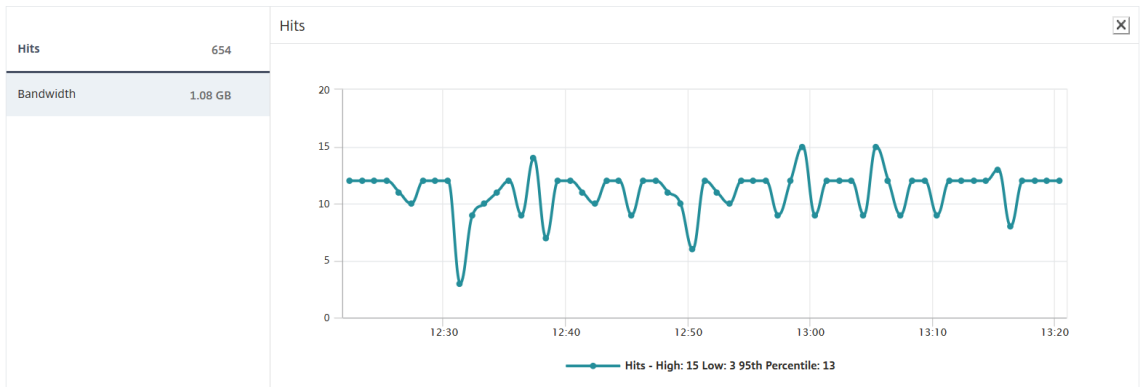


スライダーを使用して時間をカスタマイズし、[ **Go** ] をクリックして結果を表示することもできます。

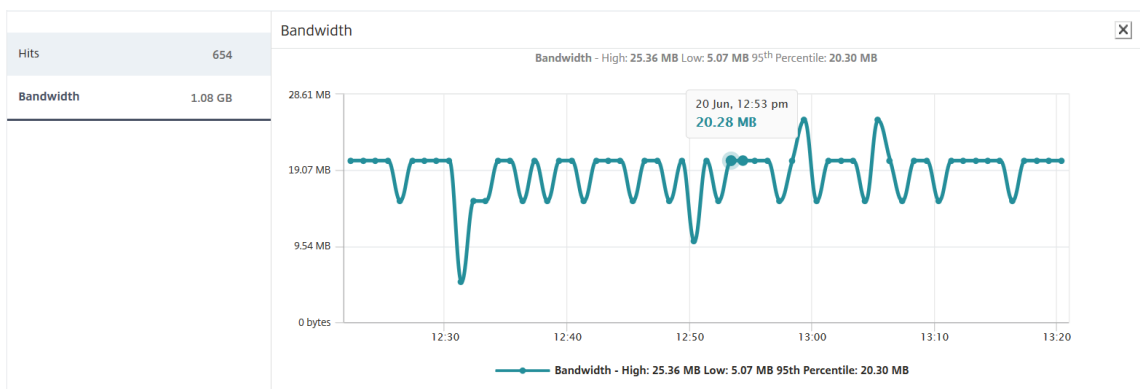


インスタンスのグラフまたは IP アドレスをクリックすると、インスタンスに関する詳細情報が表示されます。次のインサイトを表示できます。

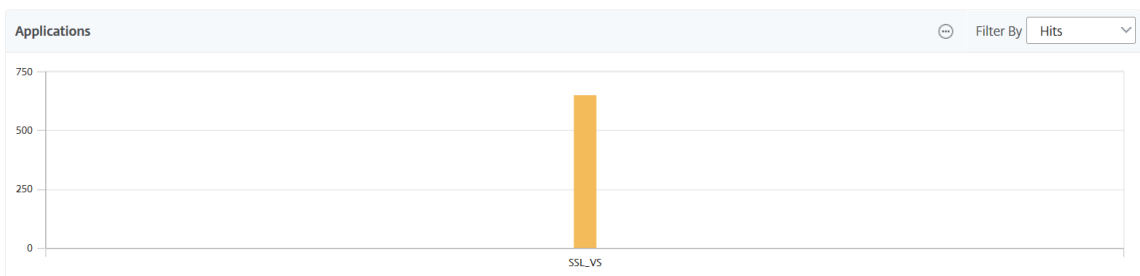
- 総ヒット数



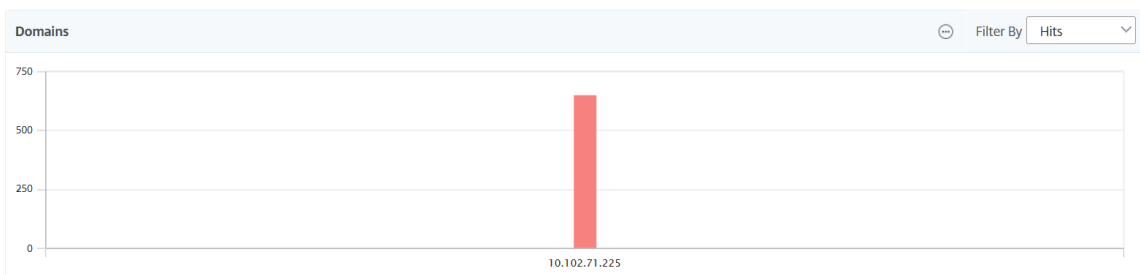
• 帯域幅



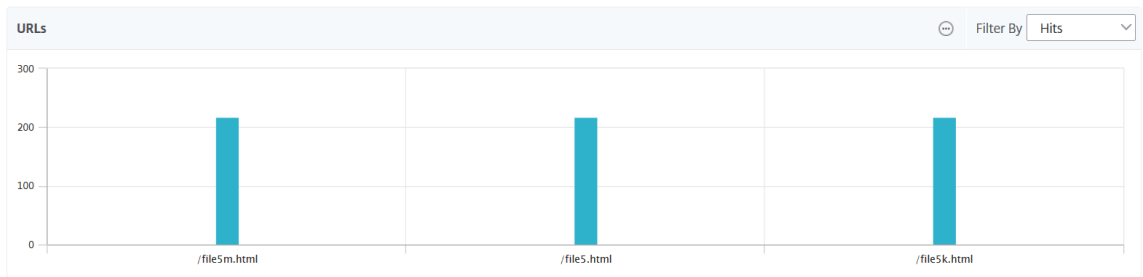
• アプリケーション



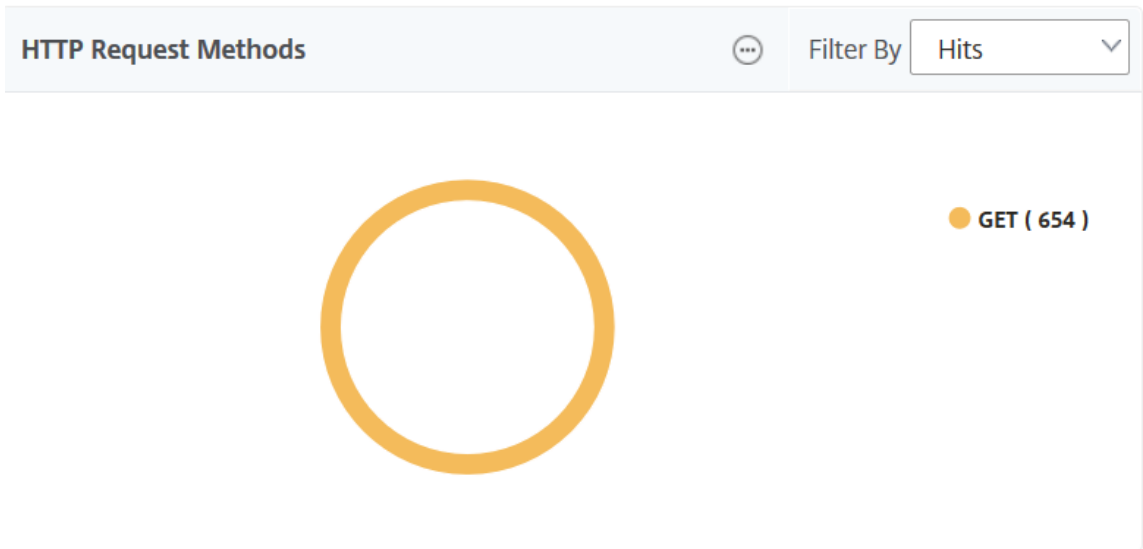
• ドメイン



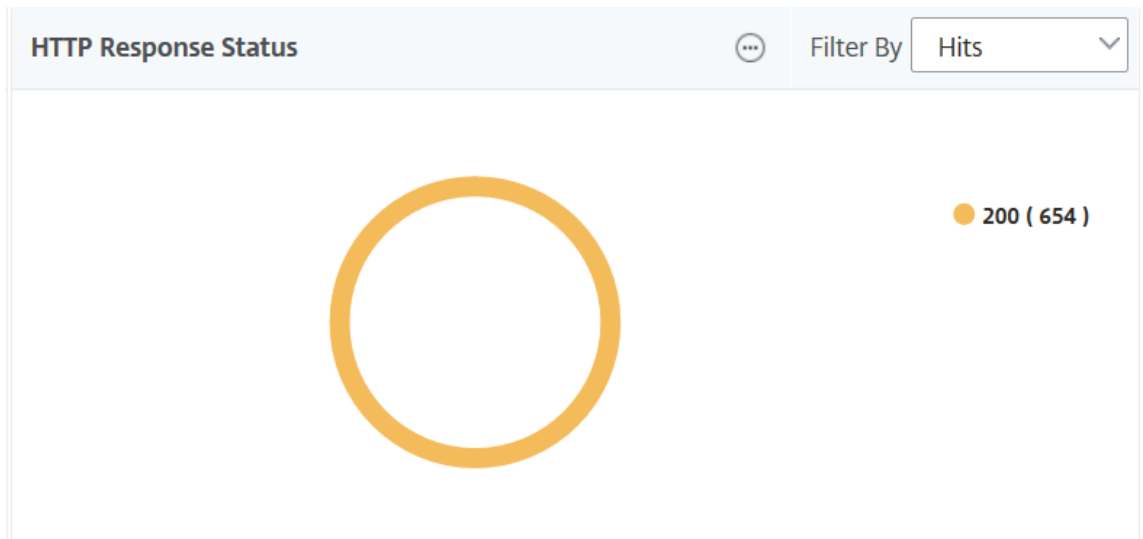
• URL



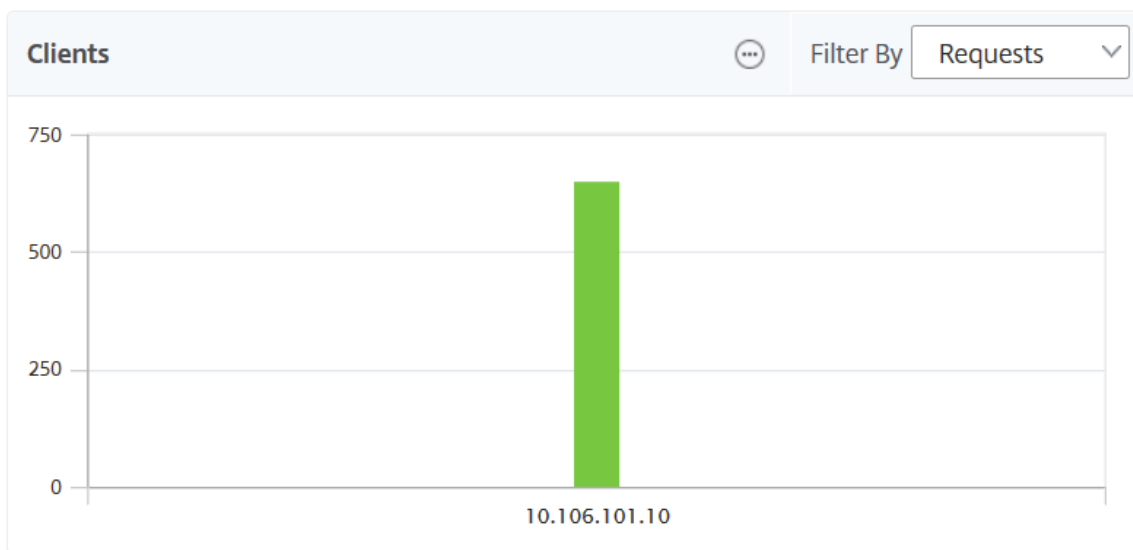
- **HTTP** 要求メソッド



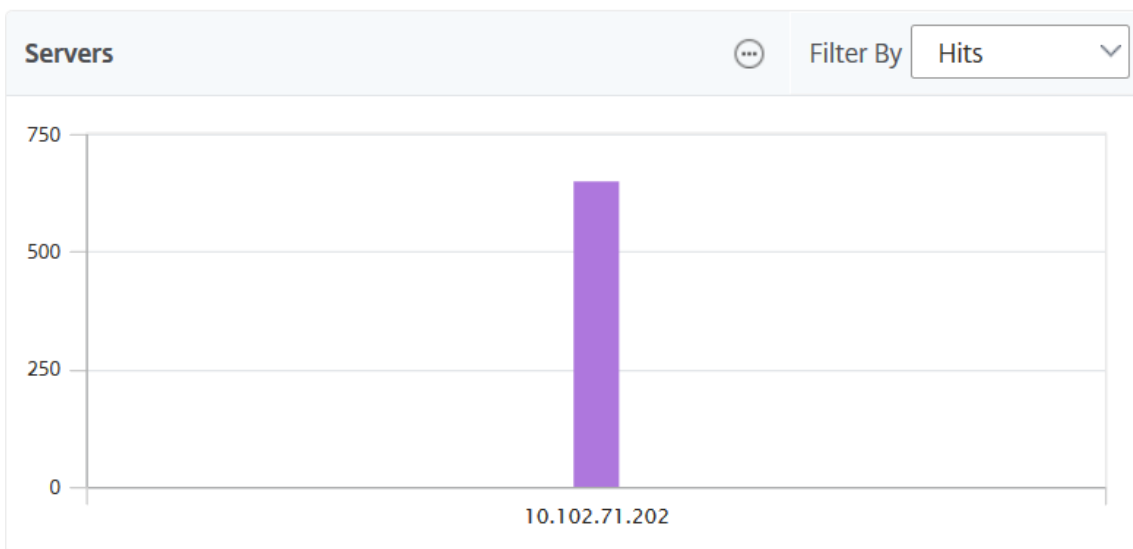
- **HTTP** 応答の状態



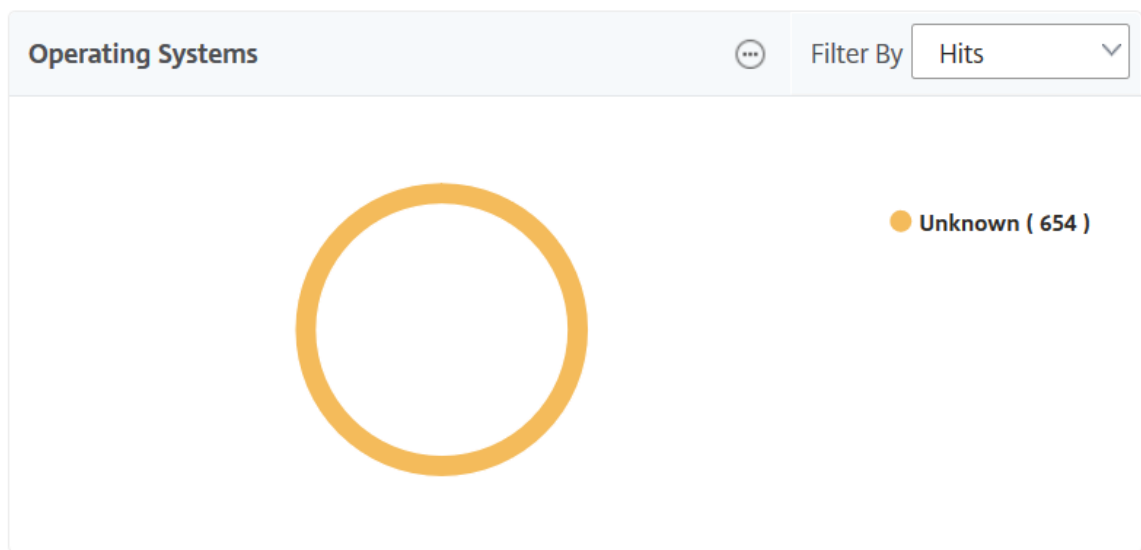
- クライアント



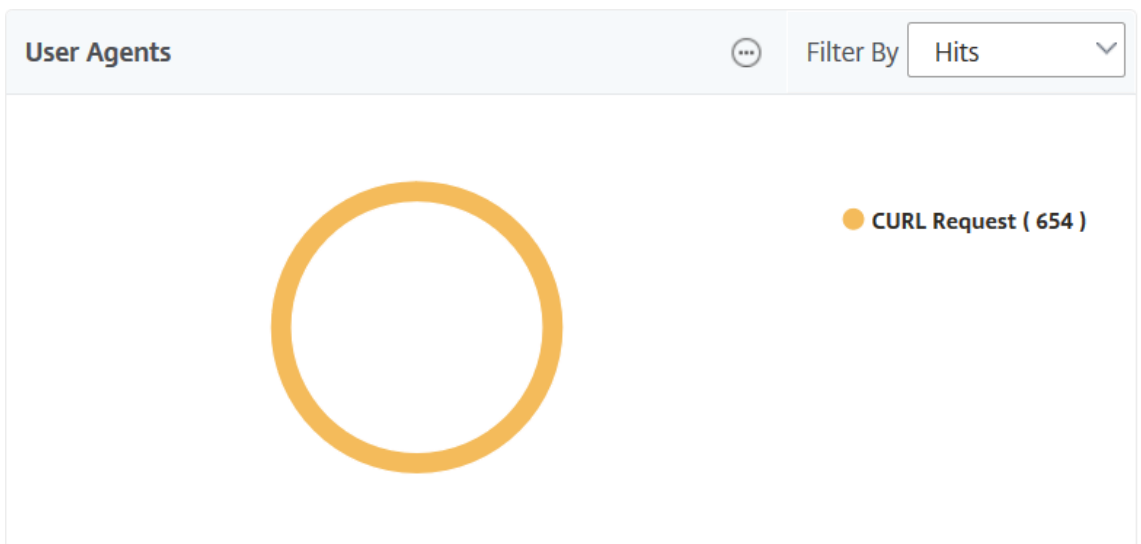
- サーバー



- オペレーティング システム

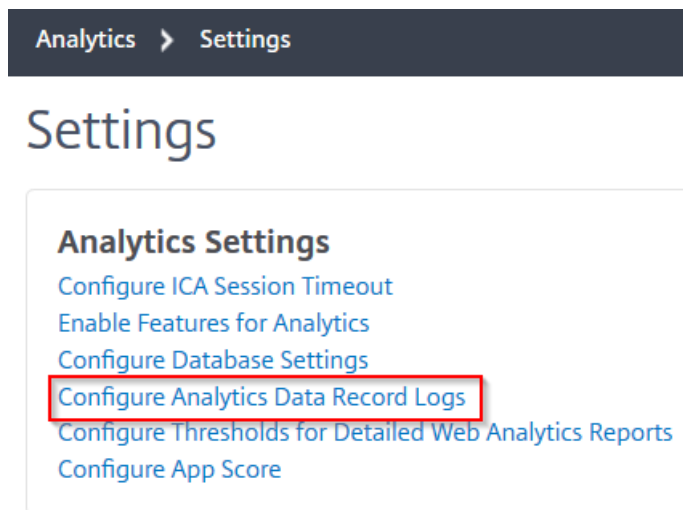


- ユーザー エージェント

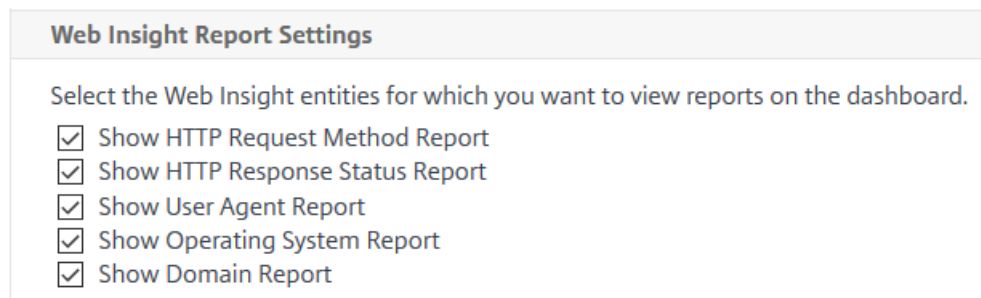


GUI でレポートを表示する **Web Insight** エンティティ を選択することもできます。

1. [アナリティクス] > [ **Web** インサイト ] > [設定] に移動します。
2. [ **Analytics** データレコードログの構成 ] をクリックします。



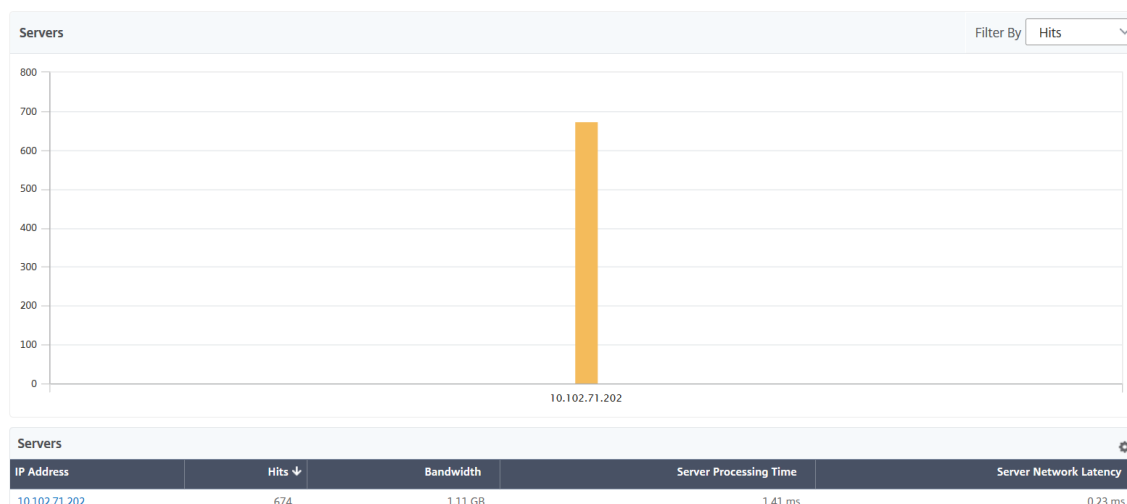
3. [ **Web Insight** レポートの設定] で、GUI でレポートを表示するエンティティを選択します。



4. [ **OK** ] をクリックします。

詳細な分析のためにドリルダウンするには、GUI の [Web Insight] の下の各インサイトカテゴリをクリックします。たとえば、構成済みサーバーの問題をチェックする場合は、次のようにします。

1. [分析] > [ **Web** インサイト] > [サーバー] に移動します。
2. 「サーバー」 ページには、設定されているすべてのサーバーが表示されます。
3. グラフの IP アドレスをクリックします。テーブルから IP アドレスをクリックすることもできます。



選択したサーバーの詳細なインサイトビューが表示されます。このビューから、次のような複数のインサイトを確認できます。

- サーバーが受信したヒットの総数
- 帯域幅
- サーバー処理時間
- サーバーネットワークの待ち時間
- サーバー用に構成された仮想サーバー
- サーバーにアクセスしているクライアントの総数
- サーバーから提供された応答コードの総数

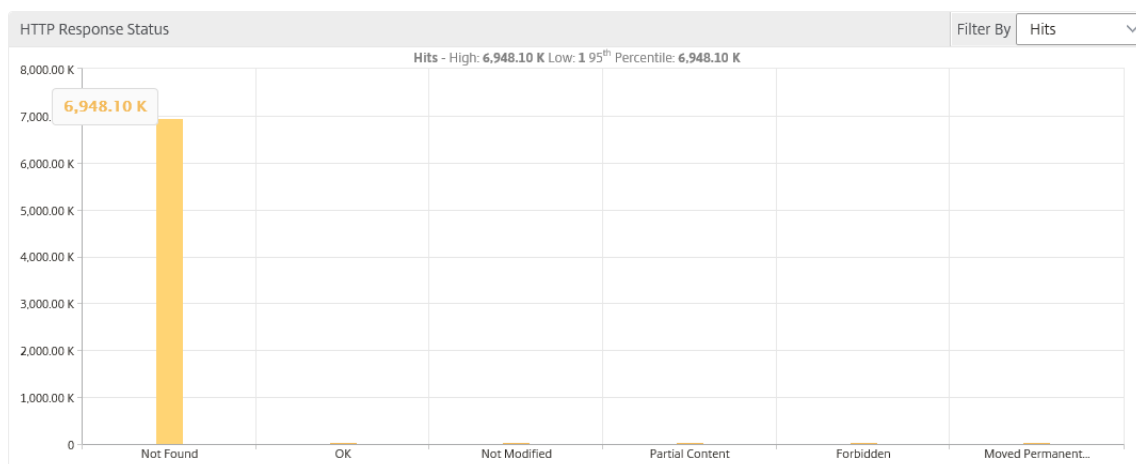
#### ユースケース 1-内部サーバーエラー

Web アプリケーションのアクセス不能エラー 500 がユーザーに発生しているシナリオを考えてみましょう。エラー 500（見つかりません）は、Web サーバー上の問題を示す HTTP 応答ステータスエラーですが、サーバーは問題を明示的に示しません。実際の問題を特定してドリルダウンするには、次の手順に従います。

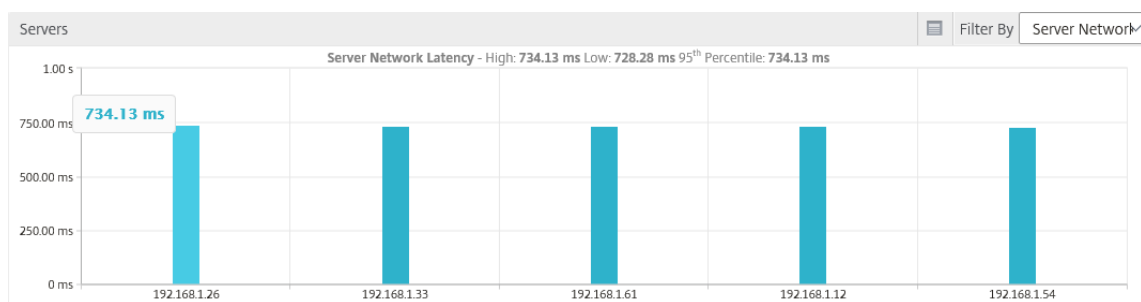
1. [ **Analytics** ] > [ **Web Insight** ] > [ 応答ステータス ] に移動します。

ダッシュボードページが表示されます。ダッシュボードには、処理された HTTP トランザクションの成功と失敗を分析するために使用できるメトリックが表示されます。

2. グラフで [ 見つかりません ] をクリックします。



- 下にスクロールして [サーバー] グラフを表示し、[フィルタ] リストから [サーバーネットワーク遅延] を選択します。



グラフは、すべてのアプリケーションサーバーが Web アプリケーションの取得に問題を抱えていたため、Web サーバーの応答時間が長くなっていることを示しています。この問題は、Web サーバーがどのサーバーからの要求にも応答しないことが原因である可能性があります。

## ユースケース 2-Web アプリケーションへのアクセスが遅いユーザーの場合

Web アプリケーションが 10 台の異なる Web サーバーでホストされているシナリオを考えてみましょう。複数のユーザーが同時にアプリケーションにアクセスすると、1 人以上のユーザーがアプリケーションの動作が遅くなる場合があります。管理者は、次のシナリオを分析して問題の根本原因を理解する必要があります。

### シナリオ 1-サーバーの処理時間:

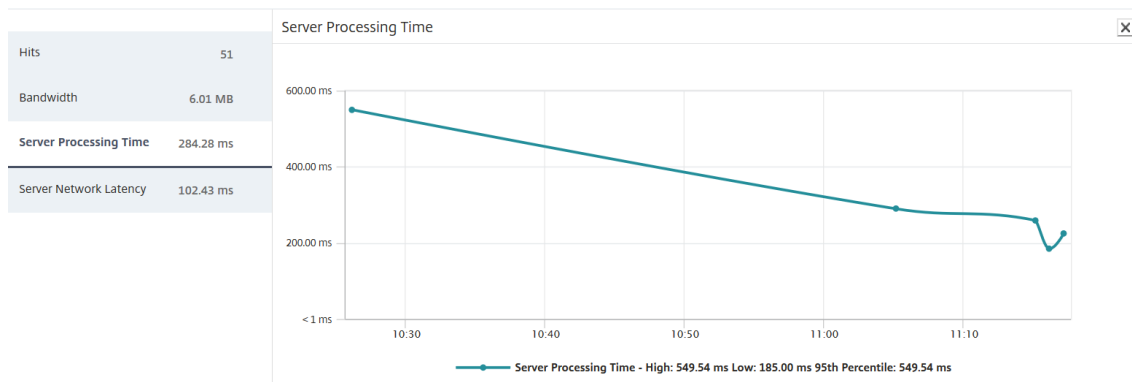
複数のリクエストが 10 台のウェブサーバーに同時に届いた場合、リクエストの読み込みにかかる時間は以下によって異なります。

- キュー内のリクエスト数。
- HTTP トランザクションを処理するために各リクエストによって消費される帯域幅。

サーバーグラフは、サーバーによって処理されたリクエストに対する各サーバーの処理時間を理解するのに役立ちます。同様に、アプリケーショングラフには、ヒット数、応答時間、および各 HTTP トランザクションで消費された帯域幅が表示されます。



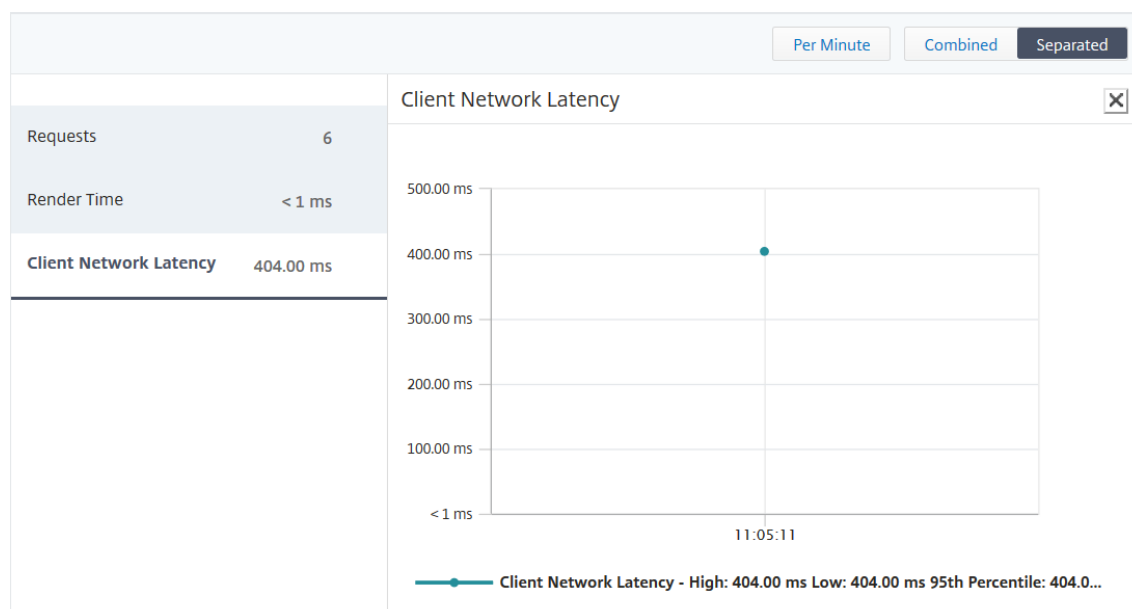
1. [分析] > [Web インサイト] > [サーバー] に移動します。
2. グラフからサーバーを選択します。
3. サーバーの処理時間を分析するには、[サーバーの処理時間] をクリックします。



シナリオ **2**-クライアントの待ち時間:

アプリケーションの応答時間と合計ヒット数が、アプリケーションアクセスが遅くなる原因である可能性があります。クライアントネットワーク遅延を確認し、クライアントネットワーク遅延のメトリックを分析できます。根本原因を分析するには:

1. [アナリティクス] > [Web インサイト] > [クライアント] に移動します。
2. グラフからクライアントを選択します。
3. [クライアントネットワーク遅延] をクリックして、高遅延を分析します。



この例では、管理者として、クライアントネットワークのレイテンシーが高いことを示すため、クライアントネットワークからの問題の根本原因を確認できます。

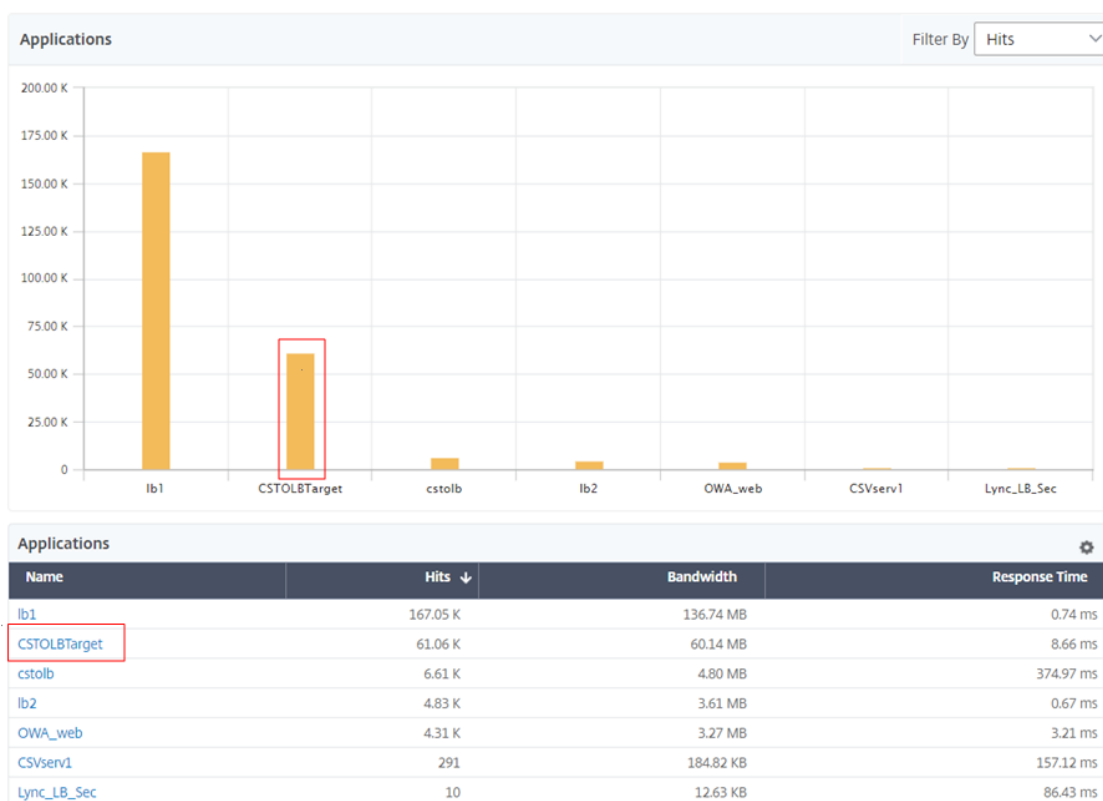
ユースケース **3-Web** アプリケーションへのアクセスが遅い

Windows ユーザー用の Web サーバーと Mac ユーザー用の Web サーバーがあり、ユーザーが Web アプリケーションへのアクセスが遅いと報告しているシナリオを考えてみましょう。管理者は、次のようなことを認識しては  
ずです。

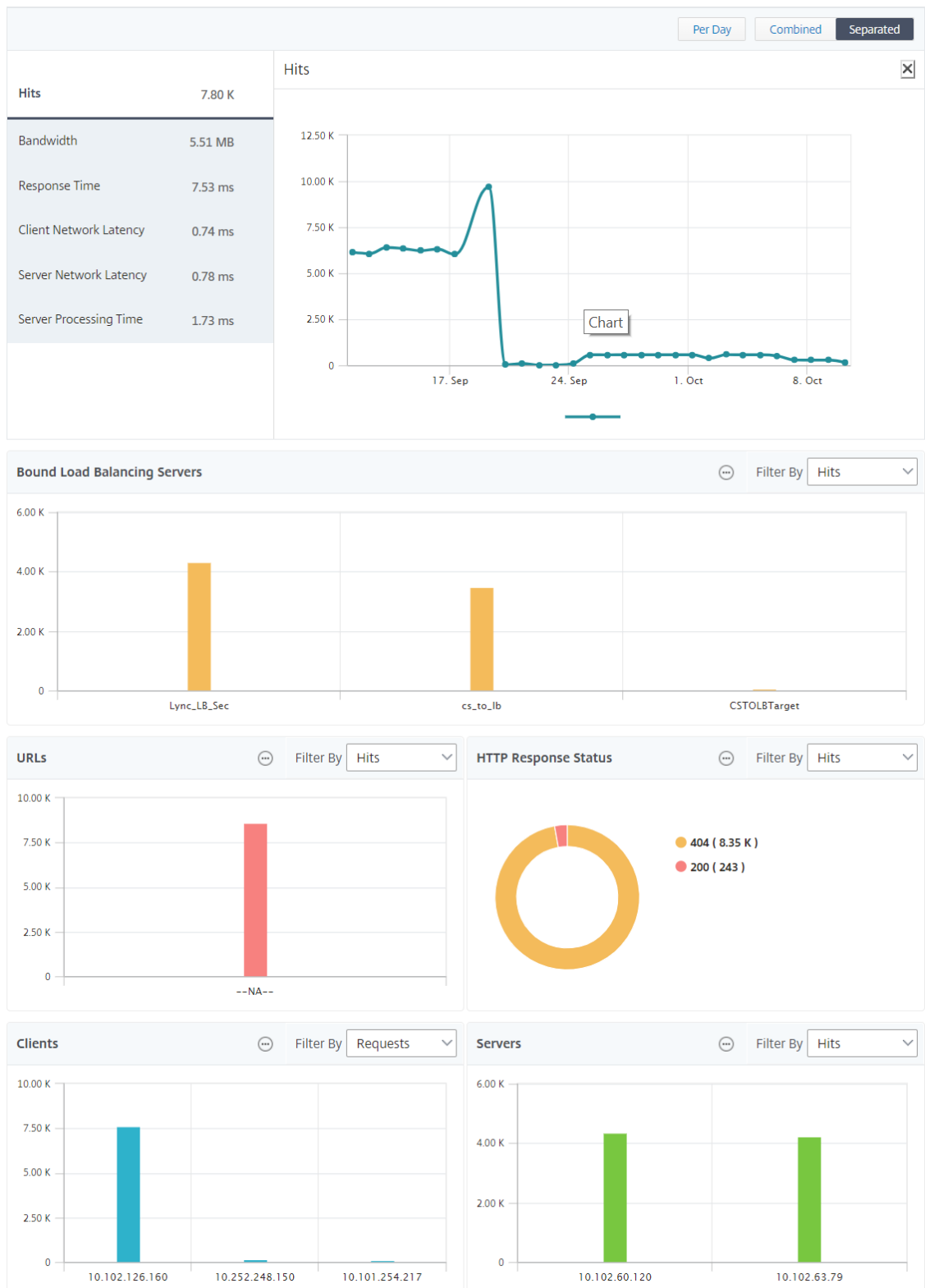
- Windows ユーザー用のコンテンツスイッチ仮想サーバーを構成しました。
- Mac ユーザー用のコンテンツスイッチング仮想サーバーを設定しました。
- Windows および Mac ユーザーに基づいてリクエストをリダイレクトするように、仮想サーバーにバインドされた関連サービスを構成しました。

Web アプリケーションの速度低下問題の根本原因を分析するには:

1. [分析] > [ **Web** インサイト ] > [ アプリケーション ] に移動します。
2. コンテンツスイッチング仮想サーバーを選択します。  
たとえば、イメージ内の「CSolbTarget」アプリケーションは、他の負荷分散仮想サーバーにバインドされたコンテンツスイッチング仮想サーバーです。



3. コンテンツスイッチング仮想サーバーをクリックして、他の負荷分散仮想サーバーを表示します。テーブル内のアプリケーション名をクリックすることもできます。



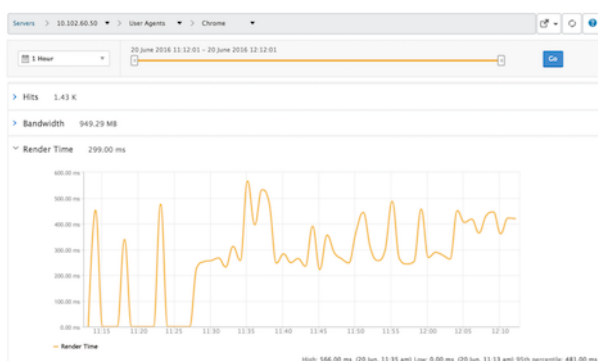
バインドされた負荷分散サーバーをクリックして、それらのアプリケーションの Web Insight の詳細を表示できます。

### ブラウザとオペレーティングシステムのインサイトを分析

Web Insight を使用すると、L7 遅延の問題を分離して、モバイルデバイスの使用状況を理解できます。管理者にとって、この洞察は、ユーザーベース全体でさまざまなオペレーティングシステムが採用されていることを理解するのに役立ちます。

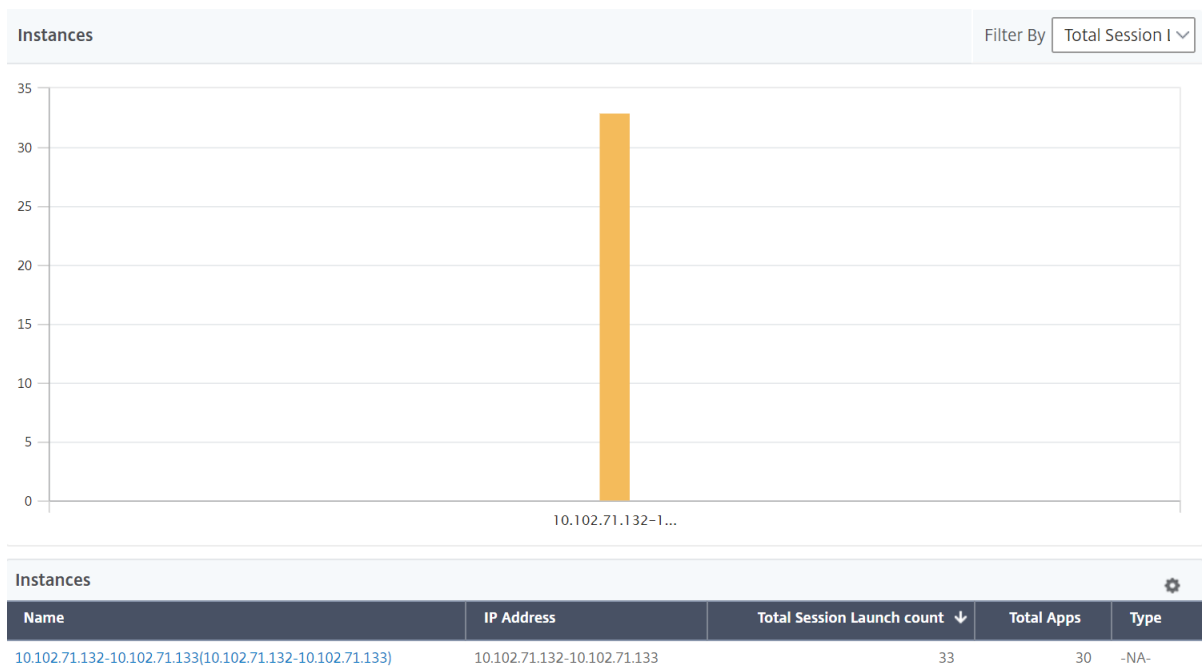
[ **Analytics** ] > [ **Web Insight** ] > [ オペレーティングシステム ] に移動して、ユーザーアクセスが遅くなる理由と、特定のブラウザ間の非互換性が原因であるかどうかを確認してください。また、特定のクライアントで使用されているオペレーティングシステムや、アクセスされているブラウザを確認することもできます。異なるブラウザ間でレンダリング時間を比較し、さらに特定のブラウザにドリルダウンして、そのブラウザで最も長いレンダリング時間に関連付けられているアプリケーションページを特定できます。

たとえば、**Google Chrome** を選択すると、特定のアプリケーションのさまざまな URL ページの対応するレンダリング時間を確認できます。



### 高可用性モードでデプロイされた **NetScaler ADC** インスタンス

Citrix ADM は、高可用性モードでデプロイされた ADC インスタンスのレポートを提供します。高可用性モードのインスタンスの集約レポートは、すべての分析でサポートされます。



高可用性にあるインスタンスの名前をクリックすると、詳細を表示できます。

1 Week

1

19 September 2018 08:29:00 - 26 September 2018 08:29:00

1

Go

IP Address  
10.102.71.132-10.102.71.133

Per Day

Combined

Separated

**Total Session Launch count** 33

---

Total Apps 30

**Total Session Launch count** ✕

**Applications** Filter By Launch Durati

**Users** Filter By Bandwidth

**Desktop Users** Filter By Desktop Laun

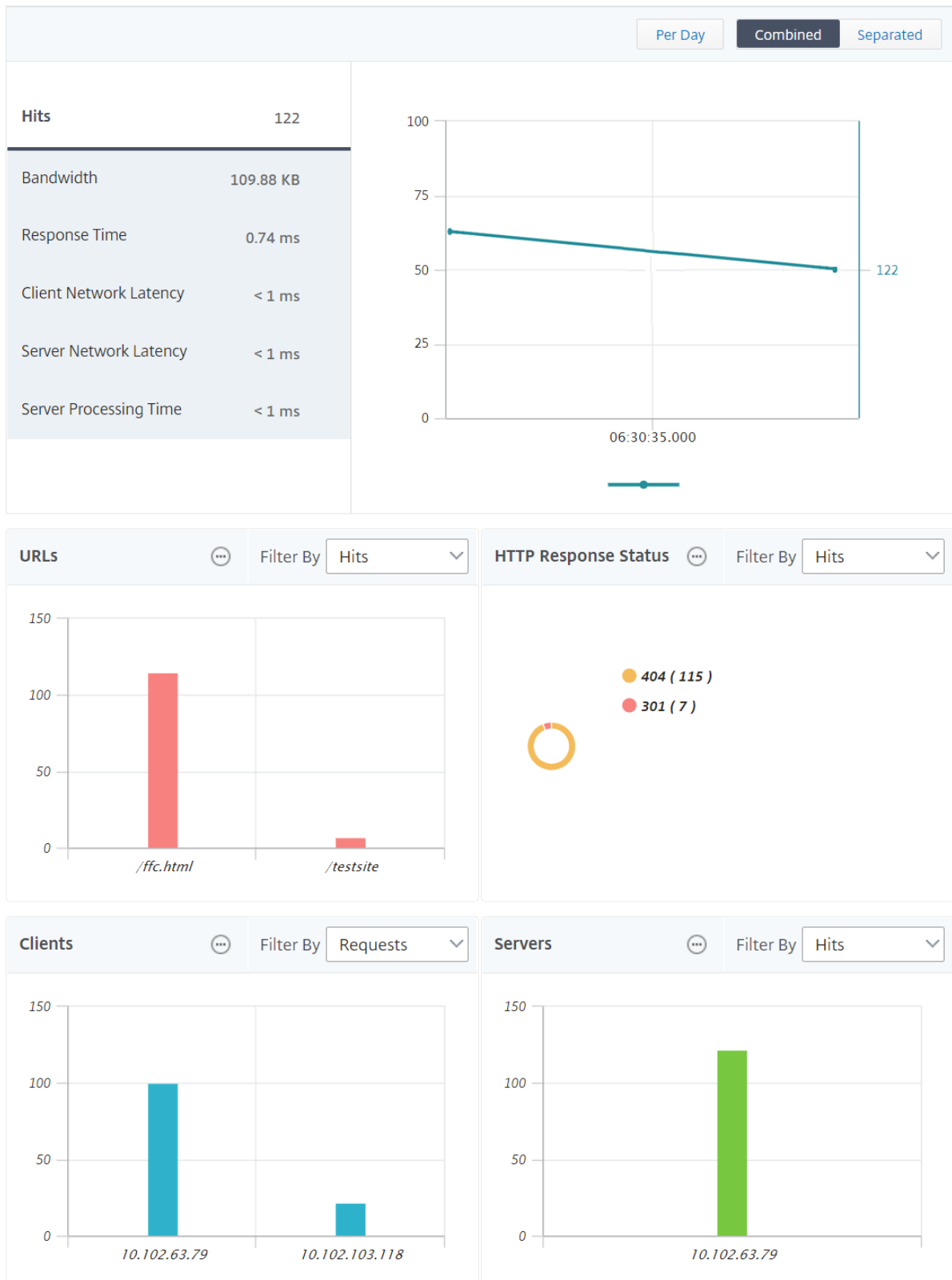
Name	Desktop Launch Count ↓	Session Duration	Bandwidth	DC latency	WAN latency	ICA RTT
XENAPP	2	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms
XA65	1	0 h: 7 m: 33s	18.35 Kbps	0 ms	5.00 ms	23.67 ms
XENAPP	1	0 h: 49 m: 0s	0.63 bps	16.00 ms	14.00 ms	20.00 ms
XENAPP	1	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms

クラスターモードでデプロイされた **NetScaler ADC** インスタンス

Citrix ADM は、クラスターモードでデプロイされた ADC インスタンスのレポートを提供します。クラスターモードのインスタンスの集約レポートは、すべての分析でサポートされます。



**CLIP** ホスト名をクリックして、クラスターモードでデプロイされた ADC インスタンスに関するすべての詳細を表示することもできます。





注

- NetScaler ADM 12.1 build 503.x にアップグレードする前に収集されたすべてのデータは、データが保持されるまで、独立したレポートとして表示されます。
- クラスタモードでデプロイされた ADC インスタンスの場合、オブザベーションドメイン ID/オブザベーションドメイン名は CLIP ホスト名と CLIP に置き換えられます。以前に収集されたすべてのデータは、引き続き観測ドメイン ID/観測ドメイン名を報告します。

## Web Insight 地理マップの設定

NetScaler ADM ジオマップ機能は、マップ上の異なる地理的場所にわたる Web アプリケーションの使用状況を表示します。管理者は、この情報を使用して、アプリケーション使用率の傾向を把握し、容量計画を立てることができます。

地域マップは、国、州、および都市に固有の次の指標に関する情報を提供します。

- 合計ヒット数: 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の送信に要した平均時間。

ジオマップは、次のようないくつか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数が最大であるリージョン
- 応答時間が最も長い地域
- 最も帯域幅を消費するリージョン

Citrix ADM には、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構成するオプションが用意されています。

### プライベート IP アドレスのジオマップの構成

注

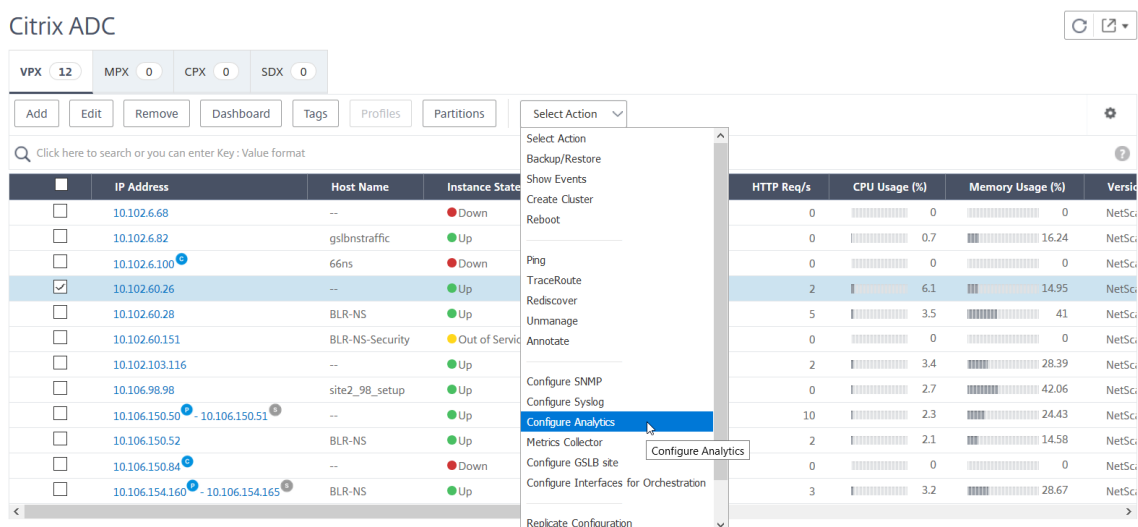
次の手順は、Citrix ADM が **13.0** ビルド **36.27** 以前の場合にのみ適用されます。NetScaler ADM **13.0 Build 41.x** 以降では、Web Insight を有効にすると、地理的データ収集が自動的に有効になります。

プライベート IP アドレスから発信された Web アプリケーショントラフィックを地理マップに表示するには、最初にプライベート IP アドレスブロックを作成し、次に geo データ収集を有効にする必要があります。

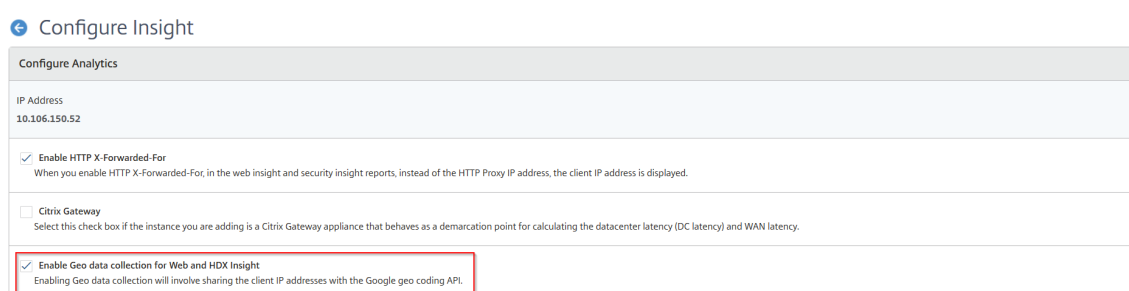
地理データ収集を有効にするには:

1. [ネットワーク] > [\*\* インスタンス] > [\*\*Citrix ADC] に移動し、Citrix ADC インスタンスを選択します。

2. [アクションの選択] リストから、[Analytics の設定] を選択します。



3. [Insight の構成] ページで、[Web および HDX Insight の地域データ収集を有効にする] を選択します。



プライベート IP ブロックを作成する NetScaler ADM は、クライアントのプライベート IP アドレスが NetScaler ADM サーバーに追加されると、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 A 市に関連付けられたプライベート IP アドレスブロックの範囲内にある場合、NetScaler ADM はこのクライアントの A 市町からトラフィックが発信していることを認識します。

IP ブロックを作成するには、次の手順を実行します。

1. Citrix ADM で、[分析] > [設定] > [IP ブロック] に移動し、[追加] をクリックします。
2. [IP ブロックの作成] ページで、次のパラメータを指定します。
  - 名前。プライベート IP ブロックの名前を指定してください
  - IP アドレスを開始します。IP ブロックの最下位 IP アドレス範囲を指定します。
  - 終了 IP アドレス。IP ブロックの最大の IP アドレス範囲を指定します。
  - カントリー。リストから国を選択します。
  - 地域。国に基づいて地域は自動入力されますが、地域を選択できます。
  - 市。地域に基づいて都市は自動入力されますが、都市を選択できます。

- \*\* 都市の緯度と都市の経度 \*\*。選択した都市に基づいて、緯度と経度が自動的に入力されます。

3. [Create] をクリックすると、作業が終了します。

## ← Create IP Blocks

Name\*

 ?

Start IP Address\*

End IP Address\*

 ?

Country\*

 ?

Region\*

 ?

City\*

 ?

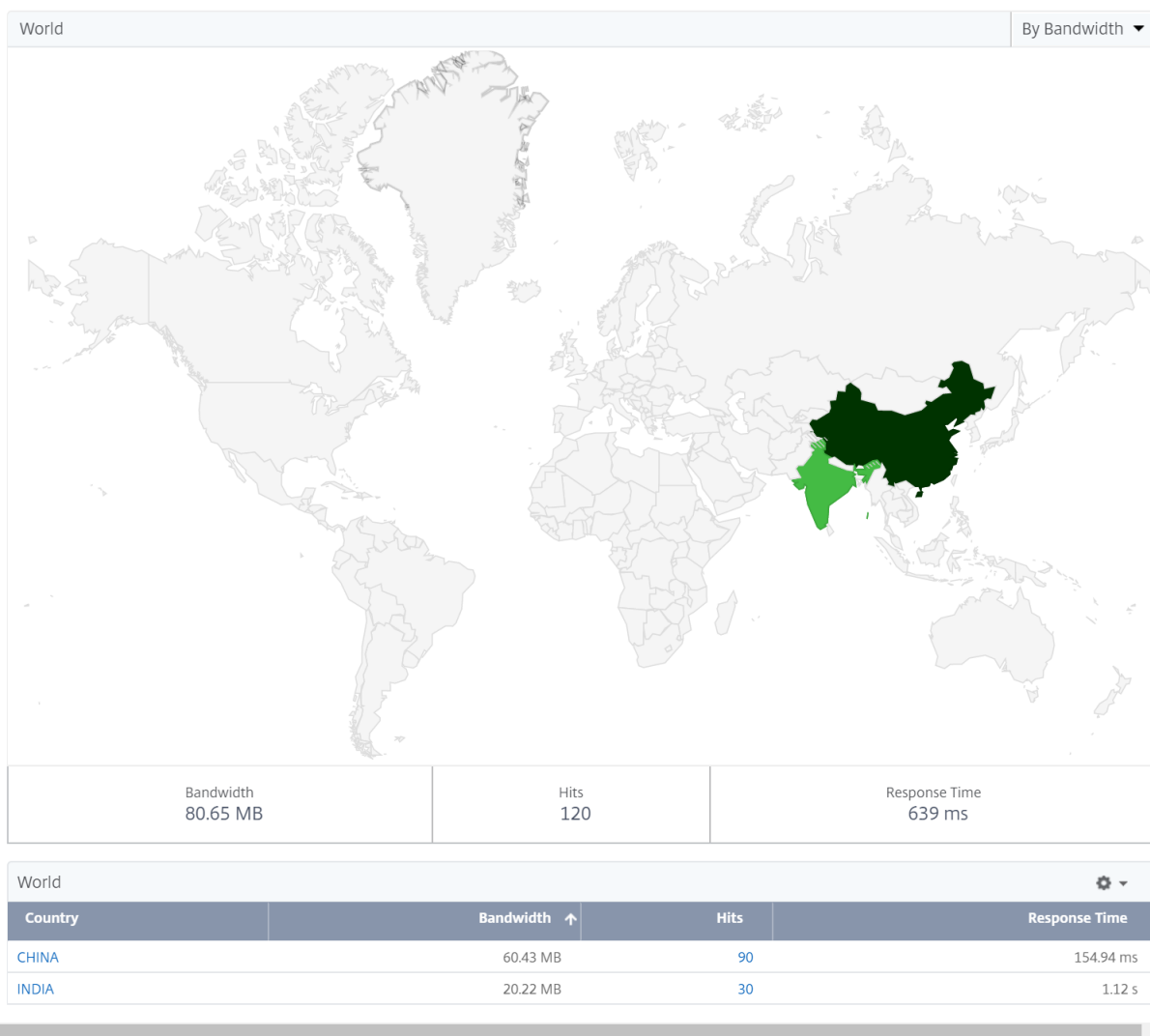
City Latitude\*

City Longitude\*

パブリック IP ブロック Citrix ADM は、クライアントがパブリック IP アドレスを使用している場合、クライアントの場所を認識することもできます。NetScaler ADM には組み込みの場所 CSV ファイルがあり、これはクライアントの IP アドレス範囲に基づいて場所と一致します。パブリック IP ブロックを使用する場合の唯一の要件は、**Configure Insight** ページから [地理データ収集を有効にする] を有効にする必要があることです。

#### 注

NetScaler ADM では、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が必要です。GeoMap を.pdf、.png、または.jpg 形式でエクスポートするには、インターネット接続も必要です。



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、次の手順に従います。

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、次のいずれかの操作を実行できます：

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 形式で表示して保存します。
2. [スケジュールエクスポート] 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て、メールまたはスラック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平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カンマで区切って入力します。

## しきい値の構成

しきい値を作成して、しきい値を超えるたびに通知を受け取ることができます。一般的な導入環境では、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ックをトラッキング
- 計画を促進
- アプリケーションの指標値が設定されたしきい値を超えると通知を受け取る

しきい値を設定するには:

1. [アナリティクス] > [設定] > [しきい値] に移動します。
2. 「しきい値」 ページで、「追加」 をクリックします。  
「しきい値の作成」 ページが表示されます。
3. 次の詳細を指定します:
  - a) 名前-イベントを作成する名前を指定します。
  - b) トラフィックタイプ-リストから [WEB] 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。デフォルトでは、「アプリケーション」 がエンティティとして選択されます。
  - d) 参照キー -参照キーは、選択したトラフィックタイプとエンティティに基づいて自動的に生成されます。
  - e) 期間-一覧から、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 週間の期間を監視できます。

### ← Create Threshold

Name*	<input type="text" value="Test"/>
Traffic Type*	<input type="text" value="WEB"/>
Entity*	<input type="text" value="Servers"/>
Reference Key	<input type="text" value="Server IP"/>
Duration*	<input type="text" value="Hour"/>

- f) [ **Configure Rule** ] セクションで、メトリック、必要なコンパレータを選択してルールを作成し、しきい値を指定します。

**Configure Rule**

Metric*	Comparator*	Value*
<input style="width: 90%;" type="text" value="Server Network Latency"/>	<input style="width: 90%;" type="text" value="&gt;"/>	<input style="width: 90%;" type="text" value="200"/>

- g) [通知の設定] セクションで、[しきい値の有効化] を選択し、アラートを取得するアラート・モードを選択します。

**Notification Settings**

Enable Threshold ?

Notify through Email ?

Email Distribution List\*

▼

Add

Edit

Test

Notify through SMS ?

SMS Distribution List\*

▼

Add

Notify through Slack ?

▼

Add

Edit

4. [作成] をクリックします。

## Web Insight に関する問題のトラブルシューティング

詳細については、「[Web Insight の問題のトラブルシューティング](#)」のトラブルシューティングを参照してください。

## Web Insight に関する問題のトラブルシューティング

February 6, 2024

NetScaler ADM Web Insight ダッシュボードを使用すると、アプリケーションの使用状況を視覚化し、NetScaler ADC インスタンス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 を使用して、ADC インスタンスは HTTP および SSL トランザクションデータを AppFlow コレクターとして構成された ADM に送信します。AppFlow は、ネットワークインフラストラクチャ内のアプリケーションおよびトランザクションデータを識別して収集するために使用されるフローエクスポート標準です。

このドキュメントは、Web Insight の展開に関する一般的な問題のトラブルシューティングに役立ちます。

## NetScaler ADM Web Insight ダッシュボードレポートに関連する問題

ADM Web Insight ダッシュボード (ADM **GUI > Analytics > Web Insight**) にレポートが表示されない場合、問題は次のいずれかが考えられます。

- Web Insight 設定の問題
- NetScaler ADC と NetScaler ADM 間の接続性の問題
- カウンターの問題
- ライセンスの問題
- 観測ポイント ID の問題
- AppFlow パラメーターが欠落している問題

構成の問題: **NetScaler ADM Web Insight** にレポートが表示されない

この問題をトラブルシューティングするには、次の手順を実行します。

1. NetScaler ADC インスタンスで AppFlow 機能が有効になっていることを確認します。詳細については、「[AppFlow の有効化](#)」を参照してください。
2. ADC インスタンスで Web Insight の設定を確認します。
  - a) `show running | grep -i <appflow_policy>` コマンドを実行して、ポリシーの Web Insight 設定を確認します。バインドタイプが REQUEST であることを確認します。たとえば、次のようになります: `bind lb vserver afsanity -policy afp -priority 100 -type REQUEST`
  - b) `show appflow action` コマンドを実行して、アクションの Web Insight 構成を確認します。 `-webinsight` オプションが有効になっていることを確認します。
  - c) LB/CS/CR 仮想サーバーの `appflowlog` パラメーターを適宜チェックします。このパラメーターが有効になっていることを確認します。

**NetScaler ADC と NetScaler ADM 間の接続性の問題: NetScaler ADM Web Insight** にレポートが表示されない

この問題をトラブルシューティングするには、次の手順を実行します。

1. NetScaler ADC で AppFlow コレクタのステータスを確認します。詳しくは、「[NetScaler ADC と AppFlow Collector 間の接続状態を確認する方法](#)」を参照してください。
2. ADC の GUI で、AppFlow ポリシーがヒットしているかどうかを確認します。コマンド `show appflow policy <policy_name>` を実行して、AppFlow ポリシーのヒットをチェックします。GUI で [システム] > [AppFlow] > [ポリシー] に移動して、AppFlow ポリシーのヒットを確認することもできます。
3. 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を検証します。

カウンター問題: **NetScaler ADM Web Insight** にレポートが表示されない

この問題をトラブルシューティングするには、次の手順を実行します。

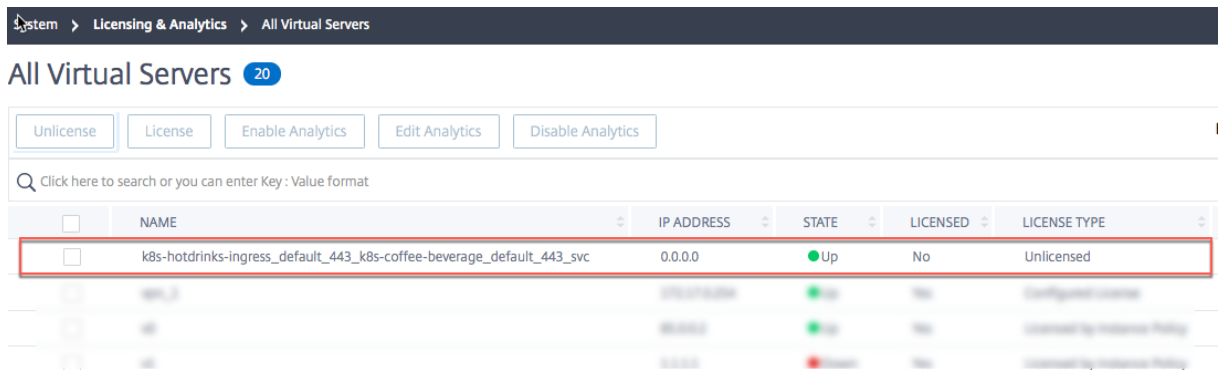
1. AppFlow の構成と接続の問題がないことを確認します。詳しくは、このトピックの NetScaler ADC と NetScaler ADM 間の構成の問題および接続の問題に関する解決策のセクションを参照してください。
2. ADC インスタンスのシェルプロンプトで、`nsconmsg -g appflow_tmpl -d current` コマンドを実行し、次のカウンターを確認します。

- `appflow_tmpl_v4_l7_clt2ns_complete`
- `appflow_tmpl_v4_l7_srvr2ns_complete`
- `appflow_tmpl_v46_ulfd_client_eot`
- `appflow_tmpl_v46_ulfd_server_eot`

カウンターのいずれかが欠落している場合は、ADC インスタンスのトレースを実行します。次に、トランザクションが完了し、応答が元のサーバーから提供されていることを確認します。トランザクションが適切で、一部のカウンターが欠落している場合は、バグを報告してください。

ライセンスの問題: **NetScaler ADM Web Insight** にレポートが表示されない

この問題では、Web Insight レポートを表示したい特定の仮想サーバーのライセンスが、[システム] > [ライセンスと分析] > [ライセンスの設定] に「いいえ」と表示されます。



この問題をトラブルシューティングするには、次の手順を実行します。

1. ADC インスタンスで、AppFlow ポリシーヒットが増加し、インスタンスが AppFlow レコードを ADM に送信していることを確認します
2. 対応する仮想サーバーのライセンスがあるかどうかを確認します。仮想サーバーのライセンスがない場合、ADM は AppFlow レコードを削除します。その結果、Web Insight レポートは表示されません。

観測ポイント ID の問題: **NetScaler ADM Web Insight** にレポートが表示されない

この問題は、観測ポイント ID が一意ではないために発生します。



注:

観測ポイント ID は、AppFlow レコードのエクスポート元である NetScaler ADC の識別子です。デフォルトでは、NetScaler ADC IP が観測ポイント ID です。

この問題をトラブルシューティングするには、次の手順を実行します。

1. ADC インスタンスで、AppFlow ポリシーヒットが増加していることと、インスタンスが AppFlow レコードの ADM への送信を終了していることを確認します。
2. 対応する仮想サーバーのライセンスがあるかどうかを確認します。
3. ADC インスタンスから別の ADC インスタンスに構成がコピーされないようにします。構成がコピーされると、エクスポート ID の問題が発生し、ADM が AppFlow レコードをドロップする可能性があります。
4. ADC インスタンスにログインし、`unset appflow param -observationpointId` コマンドを実行します。

#### AppFlow パラメータがない問題: **NetScaler ADM Web Insight** にレポートが表示されない

この問題は、データが欠落しているために ADM が AppFlow レコードを削除するために発生します。

この問題をトラブルシューティングするには、次の手順を実行します。

1. ADC インスタンスで、AppFlow ポリシーヒットが増加していることと、インスタンスが AppFlow レコードの ADM への送信を終了していることを確認します。
2. 対応する仮想サーバーのライセンスがあるかどうかを確認します。
3. ADC インスタンスから別の ADC インスタンスに構成がコピーされないようにします。構成がコピーされると、エクスポート ID の問題が発生し、ADM が AppFlow レコードをドロップする可能性があります。
4. ADC インスタンスで次の AppFlow パラメータが有効になっていることを確認します。
  - a) `HTTP method logging`
  - b) `HTTP domain name logging`
  - c) `HTTP URL logging`
  - d) `HTTP host logging`
  - e) `HTTP Content-Type header logging`

#### Citrix ADM Web Insight のその他の問題

- 問題: HTTP クライアントで、AppFlow を有効にしてもページが読み込まれません。
- 解決策: この問題のトラブルシューティングを行うには、次の手順を実行してください。

1. AppFlow アクションコマンドで、「ページトラッキング」機能 `set appflow action <name> -pageTracing disable` を無効にします。このアクションは、機能には影響しません。

問題が解決しない場合は、次の手順を実行します。

1. 同じアクションで、機能 `set appflow action <name> -clientsidemeasurements disable` の `clientsidemeasurement` 設定を解除します。このステップで問題が解決した場合は、ADC インスタンス のトレースをキャプチャしてバグを報告してください。

- 問題: AppFlow を有効にすると、ADC アプライアンスがクラッシュします。
- 解決策: この問題のトラブルシューティングを行うには、次の手順を実行してください。

バックトレース (BT) に AppFlow 機能がある場合、問題は AppFlow 機能にある可能性があります。BT が機能固有のコードに含まれている場合、問題は AppFlow を使用してコレクターにデータを送信する機能にある可能性があります。

後者の場合は、機能固有の AppFlow 構成を無効にして確認してください。AppFlow 機能をグローバルに無効にしないでください。この手順では問題をあまり把握できません。

### カウンターに関するトラブルシューティング

AppFlow または Web Insight に関連する問題については、次の AppFlow カウンターを確認してください。

カウンター	説明
<code>appflow_tot_record_drop</code>	コレクターが無効なため、AppFlow レコードが削除されました。通常、コレクター構成が変更され、既存の接続が古いコレクター構成を使用する場合に発生します。
<code>lstream_tot_trans_written</code>	このカウンターは、ログに記録されるトランザクションごとに増分する必要があります。
<code>lstream_sent</code>	このカウンターは、送信されるトランザクションログごとに増分します。

## HDX Insight

February 6, 2024

HDX Insight は、Citrix ADC を通過する Citrix Virtual Apps and Desktops への HDX トラフィックをエンドツーエンドで可視化します。管理者は、HDX Insight を通じて、リアルタイムのクライアントとネットワークの遅延測定基準、履歴レポート、エンドツーエンドのパフォーマンスデータを確認し、パフォーマンスの問題をトラブルシューティングできます。リアルタイムの可視性と履歴データの両方を利用できるため、NetScaler Application Delivery Management (ADM) はさまざまなユースケースをサポートできます。

データを表示するには、Citrix 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することができます。

注

ICA ラウンドトリップ時間の計算を記録できるようにするには、次のポリシー設定を有効にします。

- ICA 往復計算
- ICA ラウンドトリップ計算間隔
- アイドル接続の ICA 往復計算

個々のユーザーをクリックすると、選択した時間枠内でユーザーが行った各 HDX セッション（アクティブまたは終了済み）を確認できます。その他の情報には、セッション中に消費されるレイテンシー統計および帯域幅が含まれません。オーディオ、プリンタマッピング、クライアントドライブマッピングなど、個々の仮想チャネルから帯域幅情報を取得することもできます。

注:

グループを作成するときに、グループに役割を割り当てたり、グループへのアプリケーションレベルのアクセスを提供したり、ユーザーをグループに割り当てたりすることができます。NetScaler ADM 分析では、仮想 IP アドレスベースの認証がサポートされるようになりました。ユーザーは、権限のあるアプリケーション（仮想サーバー）のみのすべての Insight のレポートを表示できるようになりました。グループ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、「[グループを設定する](#)」を参照してください。

「**HDX Insight**」 > 「アプリケーション」の順に選択し、「起動期間」をクリックして、アプリケーションの起動に要した時間を表示することもできます。**HDX Insight-Users** に移動して、接続し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 ADC 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が 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

## パフォーマンス遅延問題の根本原因の特定

### シナリオ 1

ユーザーが Citrix Virtual Apps and Desktops にアクセスする際に遅延が発生しています。

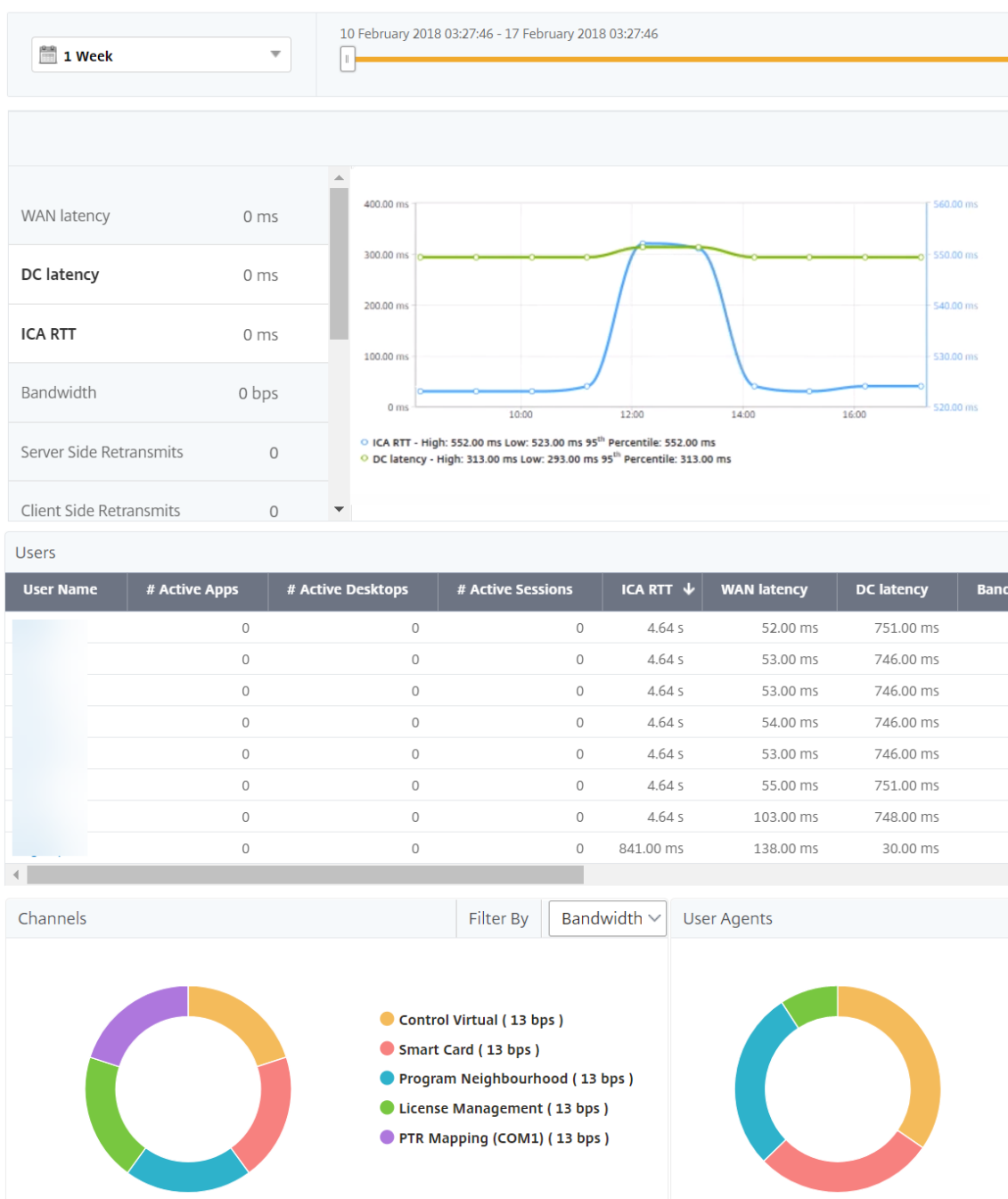
遅延の原因として考えられるのは、サーバーネットワークの遅延、サーバーネットワークに起因する ICA トラフィックの遅延、またはクライアントネットワークの遅延です。

問題の根本原因を特定するために、次の測定基準を分析します。

- WAN 遅延
- DC の遅延
- ホストの遅延

クライアント・メトリックを表示する手順は、次のとおりです。

1. **[Analytics]** タブで、**[HDX Insight]** > [ユーザー] 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、リストからピリオドを選択します。期間は、1 日、1 週間、1 か月にすることができます。また、データを表示する期間をカスタマイズすることもできます。
3. グラフには、指定した期間におけるユーザーの ICA RTT および DC レイテンシー値がグラフとして表示されます。



- [現在のセッション] テーブルで、**RTT** 値の上にマウスを置き、ホスト遅延、DC 遅延、および WAN 遅延の値をメモします。
- 「現在のセッション」 (Current Sessions) テーブルで、ホップ図のシンボルをクリックして、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。

Session ID: 00000000-0000-0465-0000-000100000001



23.18.6.11

```

User Name      jayden
Session ID     00000000-0000-0465-0000-000100000001
Client IP Address 23.18.6.11
ICA RTT        1.08 s
Client Type     Citrix Blackberry phone client
Client Version  11.8
                PUERTO RICO
                *
                Guaynabo
    
```

まとめ この例では、**DC** 遅延は 751 ミリ秒、**WAN** 遅延は 52 ミリ秒、ホスト遅延は 6 秒です。これは、サーバネットワークによる平均遅延が原因で、ユーザが遅延していることを示します。

## シナリオ 2

ユーザーが Citrix Virtual App または Desktop でアプリケーションを起動する際に遅延が発生する

遅延の原因として考えられるのは、サーバーネットワークの遅延、サーバーネットワークに起因する ICA トラフィックの遅延、クライアントネットワークの遅延、またはアプリケーションの起動にかかる時間です。

問題の根本原因を特定するために、次の測定基準を分析します。

- 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手順は、次のとおりです。

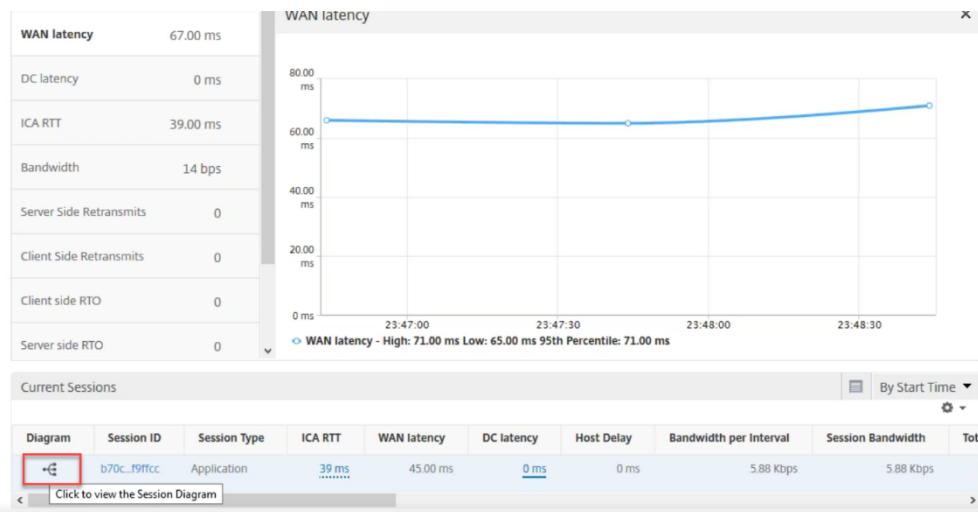
1. [分析] タブで、[HDX Insight] > [ユーザー] に移動します。
2. 下にスクロールし、ユーザー名をクリックします。
3. グラフィカル表示で、特定のセッションの WAN レイテンシー、DC レイテンシー、および RTT の値をメモします。

4. 「現在のセッション」 (Current Sessions) テーブルで、ホストの遅延が大きいことに注意してください。

Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
☛	0000_000001 (NON EUEM)	Application	784 ms .....	517.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	758 ms .....	287.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	768 ms .....	191.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	815 ms .....	608.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	845 ms .....	107.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	775 ms .....	535.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	809 ms .....	86.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	796 ms .....	591.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	777 ms .....	83.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	825 ms .....	622.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	770 ms .....	67.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	805 ms .....	602.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	870 ms .....	628.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	767 ms .....	55.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	788 ms .....	634.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	850 ms .....	52.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	864 ms .....	569.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
☛	0000_000001 (NON EUEM)	Application	759 ms .....	48.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10

まとめ この例では、**DC** 遅延は 1 ミリ秒、**WAN** 遅延は 12 ミリ秒、ホスト遅延は 517 ミリ秒です。DC および WAN のレイテンシーが低い RTT が高いのは、ホストサーバ上のアプリケーションエラーを示します。

注: ソフトウェア 11.1 ビルド 51.21 以降を実行している NetScaler ADM を使用している場合、HDX Insight は、WAN ジッタやサーバー側の再送信など、より多くのユーザーメトリックも表示されます。これらの指標を表示するには、[ **\*\*Analytics** ] > [ **HDX Insight** ] > [ユーザー]\*\* の順に選択し、ユーザー名を選択します。ユーザーの測定基準がグラフの隣の表に表示されます。



## HDX Insight 用ジオマップ

Citrix ADM Geomaps 機能は、地理的に異なる場所でのアプリケーションの使用状況を地図上に表示します。この情報を使用して、管理者は、さまざまな地理的な場所でのアプリケーション使用状況の傾向を把握できます。

特定の地理的場所または LAN のジオマップを表示するように Citrix ADM を構成するには、その場所のプライベート IP 範囲（開始 IP アドレスと終了 IP アドレス）を指定します。

HDX Insight でジオロケーションマップから履歴とアクティブなユーザーの詳細も表示できます。[ **Analytics** ] > [ **HDX Insight** ] に移動し、マップの [ ワールド ] セクションで、詳細を表示する国または地域をクリックします。更に情報を表示するために、市と州でドリルダウンすることができます。

データセンターの **geomap** を設定するには、次の手順に従います。

[ **Analytics** ] タブで、[ 設定 ] > [ IP ブロック ] に移動し、特定の場所のジオマップを設定します。

### 使用例

このシナリオでは 2 つのブランチオフィスを持つ ABC という名前の企業を扱います。ABC はサンタクララとインドにブランチオフィスがあります。

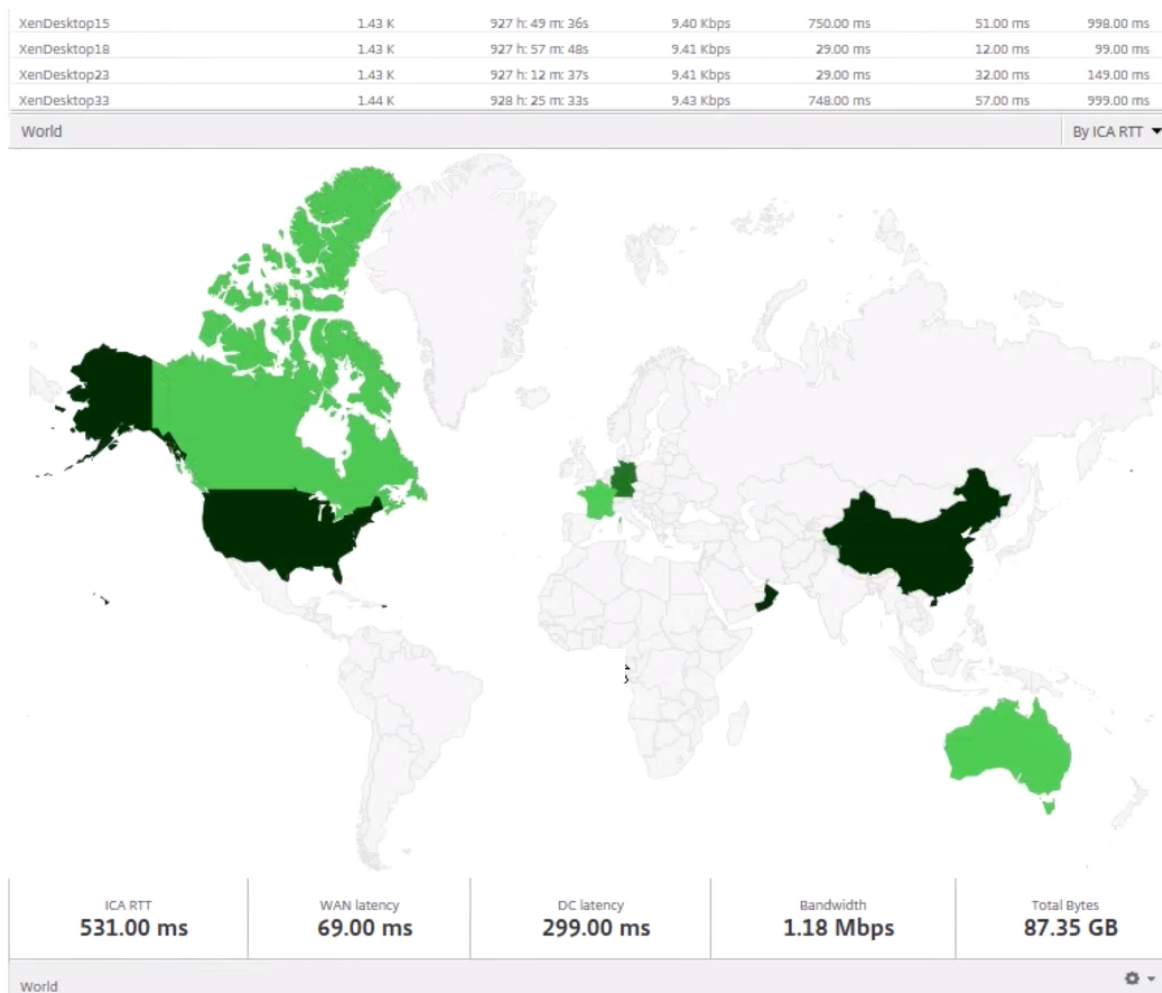
サンタクララのユーザーは、Sclara.x.com の Citrix Gateway アプライアンスを使用して VPN トラフィックにアクセスします。インドのユーザーは、India.x.com の Citrix Gateway アプライアンスを使用して VPN トラフィックにアクセスします。

サンタクララでは、午前 10 時から午後 5 時などの特定の時間帯に SClara.x.com に接続し、VPN トラフィックにアクセスします。ほとんどのユーザーは同じ NetScaler Gateway にアクセスするため、VPN への接続に遅延が生じます。そのため、一部のユーザーは Sclara.x.com ではなく India.x.com に接続します。

トラフィックを分析する NetScaler ADC 管理者は、地理マップ機能を使用して、サンタクララオフィスのトラフィックを表示できます。このマップは、サンタクララオフィスの応答時間が長くなることを示しています。これは、サ



ンタクララオフィスには、ユーザーがVPNトラフィックにアクセスできる NetScaler Gateway アプライアンスが1つしかないためです。したがって、管理者は別の NetScaler Gateway をインストールして、ユーザーがVPNにアクセスするための2つのローカル NetScaler Gateway アプライアンスを持つようにすることもできます。



### 制限事項

NetScaler ADC インスタンスに Advanced ライセンスがある場合、分析データは1時間しか収集されないため、NetScaler ADM for HDX Insight に設定されたしきい値はトリガーされません。

## HDX Insight データ収集の有効化

February 6, 2024

HDX Insight は、NetScaler ADC インスタンスまたは Citrix SD-WAN アプライアンスを通過する ICA トラフィックをこれまでにないエンドツーエンドで可視化することで、NetScaler Application Delivery Management

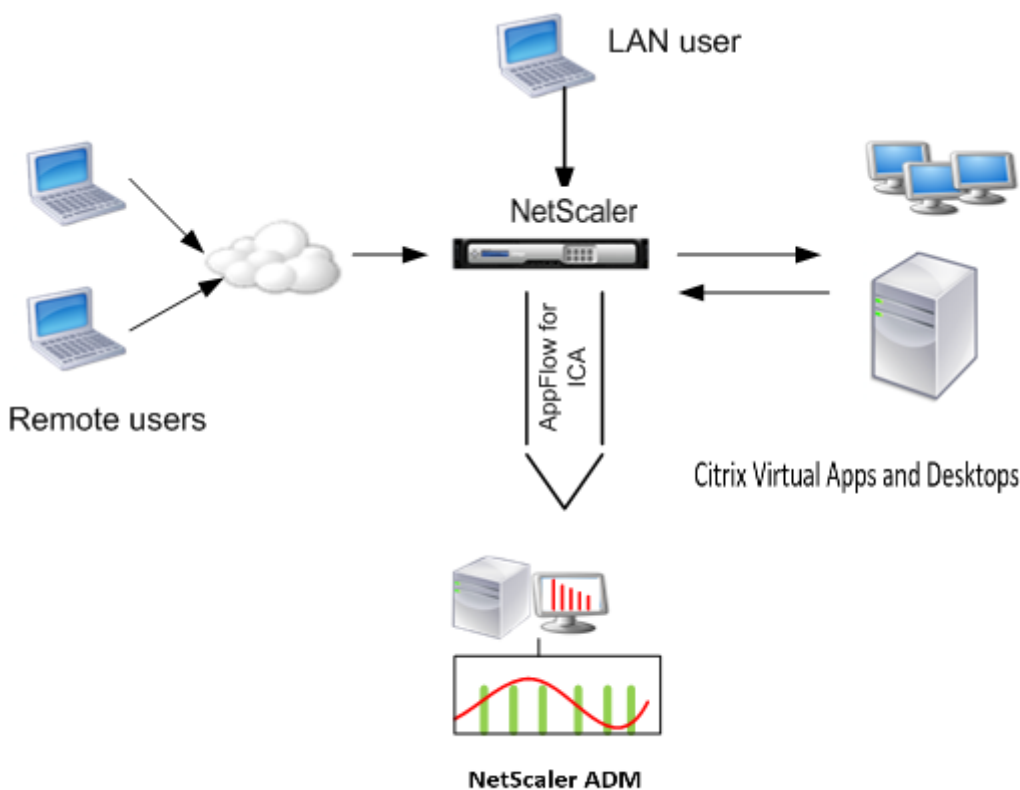
(ADM) Analytics が卓越したユーザーエクスペリエンスを提供できるようにします。HDX Insight は、ネットワーク、仮想デスクトップ、アプリケーション、アプリケーションファブリックに対して、魅力的で強力なビジネスインテリジェンスと障害分析機能を提供します。HDX Insight はユーザーの問題を優先度によってすぐに選別すると同時に、仮想デスクトップ接続に関するデータを収集し、AppFlow レコードを生成して、それらをビジュアルレポートとして提示します。

NetScaler ADC でデータ収集を有効にする構成は、導入トポロジーにおけるアプライアンスの位置によって異なります。

### LAN ユーザーモードで展開された Citrix ADC を監視するためのデータ収集の有効化

Citrix 仮想アプリおよびデスクトップアプリケーションにアクセスする外部ユーザーは、NetScaler Gateway で自分自身を認証する必要があります。ただし、内部ユーザーは NetScaler Gateway にリダイレクトする必要がない場合があります。また、透過モードの展開では、管理者が手動でルーティングポリシーを適用して、要求が NetScaler ADC アプライアンスにリダイレクトされるようにする必要があります。

これらの課題を克服し、LAN ユーザーが Citrix Virtual App および Desktop アプリケーションに直接接続できるようにするには、NetScaler Gateway アプライアンスで SOCKS プロキシとして機能するキャッシュリダイレクト仮想サーバーを構成することで、NetScaler ADC アプライアンスを LAN ユーザーモードで展開します。



注： NetScaler ADM と NetScaler Gateway アプライアンスは同じサブネットにあります。

このモードで展開された NetScaler ADC アプライアンスを監視するには、まず NetScaler ADC 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 ADC アプライアンスを NetScaler ADM インベントリに追加した後、データ収集のために AppFlow を有効にする必要があります。

注

- ADC インスタンスで、[システム] > [AppFlow] > [コレクタ] の順に選択し、コレクタ (NetScaler ADM) が起動しているかどうかを確認できます。NetScaler ADC インスタンスは、NSIP を使用して AppFlow レコードを NetScaler ADM に送信します。ただし、インスタンスは SNIP を使用して NetScaler ADM との接続を確認します。そのため、SNIP がインスタンスに設定されていることを確認してください。
- NetScaler ADM 構成ユーティリティを使用して、LAN ユーザーモードで展開された NetScaler ADC でデータ収集を有効にすることはできません。
- コマンドとその用法について詳しくは、「[コマンドリファレンス](#)」を参照してください。
- ポリシー式については、「[ポリシーと式](#)」を参照してください。

コマンドラインインターフェイスを使用して **NetScaler ADC** アプライアンスでデータ収集を構成するには:

コマンドプロンプトで、次の操作を行います:

1. アプライアンスにログオンします。
2. プロキシ IP およびポートを指定してフォワードプロキシキャッシュリダイレクト仮想サーバーを追加します。また、サービスタイプとして HDX を指定します。

```
1 add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
  cacheType <cachetype>] [ - cltTimeout <secs>]
2 <!--NeedCopy-->
```

例

```
1 add cr vserver cr1 HDX 10.12.2.2 443 - cacheType FORWARD -
  cltTimeout 180
2 <!--NeedCopy-->
```

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する場合は、VPN トラフィックと一致するポリシーによって適用されるアクションを追加してください。

```
1 add vpn trafficAction <name> <qual> [-HDX ( ON or OFF )]
2
3 add vpn trafficPolicy <name> <rule> <action>
4 <!--NeedCopy-->
```

例

```
1 add vpn trafficAction act1 tcp -HDX ON
2
3 add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
4 <!--NeedCopy-->
```

3. NetScaler ADM を AppFlow コレクタとして NetScaler ADC アプライアンスに追加します。

```
1 add appflow collector <name> -IPAddress <ip_addr>
2 <!--NeedCopy-->
```

Example:

```
“
add appflow collector MyInsight -IPAddress 192.168.1.101
“
```

4. AppFlow アクションを作成し、コレクタをアクションに関連付けます。

```
1 add appflow action <name> -collectors <string>
```

例:

```
1 add appflow action act -collectors MyInsight
```

5. AppFlow ポリシーを作成して、トラフィックを生成するためのルールを指定します。

```
1 add appflow policy <polycyname> <rule> <action>
```

例:

```
1 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。

```
1 bind appflow global <polycyname> <priority> -type <type>
```

例:

```
1 bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

注

タイプの値は、ICA トラフィックに適用するには、ICA\_REQ\_OVERRIDE または ICA\_REQ\_DEFAULT である必要があります。

7. AppFlow の flowRecordInterval パラメーターの値を 60 秒に設定します。

```
1 set appflow param -flowRecordInterval 60
```

例:

```
1 set appflow param -flowRecordInterval 60
```

8. 構成を保存します。種類: `save ns config`

シングルホップモードで展開された **NetScaler Gateway** アプライアンスのデータ収集を有効にする

NetScaler Gateway をシングルホップモードで展開すると、ネットワークのエッジになります。Gateway インスタンスは、デスクトップ配信インフラストラクチャへのプロキシ ICA 接続を提供します。シングルホップは、最も単純で最も一般的な導入方法です。シングルホップモードは、外部ユーザーが組織内の内部ネットワークにアクセスしようとした場合にセキュリティを確保します。

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 ADC 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 Citrix Application Delivery Management (ADM) インベントリに追加し、ADM で AppFlow を有効にする必要があります。

**NetScaler ADM** から **AppFlow** 機能を有効にするには:

1. Web ブラウザで、Citrix ADM IP アドレス (例: <http://192.168.100.1>) を入力します。
2. **[User Name]** と **[Password]** に管理者の資格情報を入力します。
3. **[ネットワーク]** > **[インスタンス]** に移動し、分析を有効にする NetScaler ADC インスタンスを選択します。
4. **[アクションの選択]** リストから、**[Analytics の設定]** を選択します。
5. VPN 仮想サーバーを選択し、「アナリティクスを有効にする」をクリックします。
6. **[HDX Insight]** を選択し、次に **[ICA]** を選択します。
7. **[OK]** をクリックします。

#### 注

シングルホップモードで AppFlow を有効にすると、次のコマンドがバックグラウンドで実行されます。トラブルシューティングのため、こちらにそのコマンドを明記します。

```
1 - add appflow collector <name> -IPAddress <ip_addr>
2
3 - add appflow action <name> -collectors <string>
4
5 - set appflow param -flowRecordInterval <secs>
6
7 - disable ns feature AppFlow
8
9 - enable ns feature AppFlow
10
11 - add appflow policy <name> <rule> <expression>
12
```

```

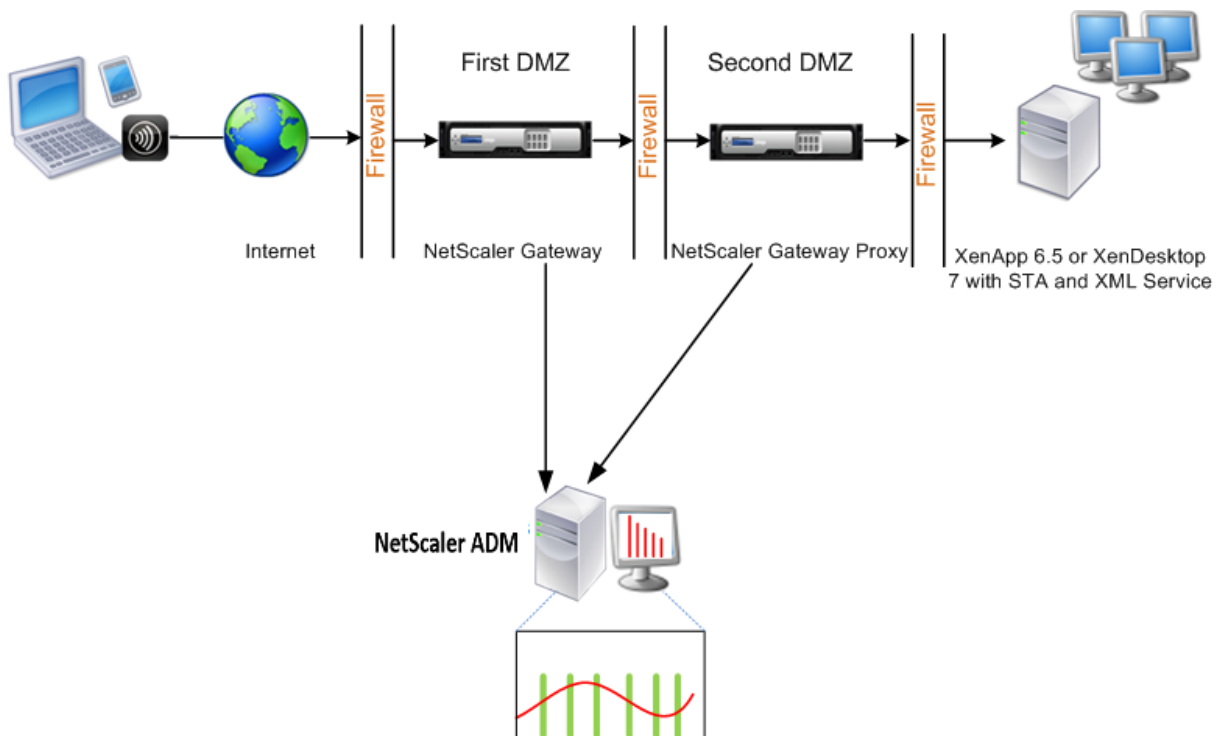
13 - set appflow policy <name> -rule <expression>
14
15 - bind vpn vserver <vsname> -policy <string> -type <type> -priority <
    positive_integer>
16
17 - set vpn vserver <name> -appflowLog ENABLED
18
19 - save ns config

```

EUEM 仮想チャネルデータは、NetScaler ADM がゲートウェイインスタンスから受信する HDX Insight データの一部です。EUEM 仮想チャネルは、ICA RTT に関するデータを提供します。EUEM 仮想チャネルが有効になっていない場合でも、残りの HDX Insight データは NetScaler ADM に表示されます。

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では、攻撃者が複数のセキュリティゾーンまたは非武装地帯 (DMZ) に侵入してセキュアネットワークのサーバーに到達する必要があるため、組織の内部ネットワークをさらに保護できます。ICA 接続が通過するホップ (NetScaler Gateway アプライアンス) の数と、各 TCP 接続のレイテンシーの詳細と、クライアントが認識する ICA レイテンシーの合計とどのようにフェアするかを分析する場合は、NetScaler ADM をインストールして、NetScaler Gateway アプライアンスこれらの重要な統計を報告する。



最初の DMZ の 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、ユーザーの認証方法を決定し、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 つ目の DMZ の NetScaler Gateway は、NetScaler Gateway プロキシデバイスとして機能します。この NetScaler Gateway により、ICA トラフィックが 2 番目の DMZ を通過して、サーバーファームへのユーザー接続を完了できます。

NetScaler ADM は、最初の DMZ の NetScaler Gateway アプライアンスに属するサブネットか、2 番目の DMZ の NetScaler Gateway アプライアンスに属するサブネットのいずれかに展開できます。上の画像では、最初の DMZ の NetScaler ADM と NetScaler Gateway が同じサブネットにデプロイされています。

ダブルホップモードでは、NetScaler ADM は 1 つのアプライアンスから TCP レコードを、もう 1 つのアプライアンスから ICA レコードを収集します。NetScaler Gateway アプライアンスを NetScaler ADM インベントリに追加してデータ収集を有効にすると、各アプライアンスはホップカウントと接続チェーン ID を追跡してレポートをエクスポートします。

NetScaler ADM がレコードをエクスポートするアプライアンスを識別するために、各アプライアンスはホップ数で指定され、各接続は接続チェーン ID で指定されます。ホップカウントは、トラフィックがクライアントからサーバーに流れる NetScaler Gateway アプライアンスの数を表します。接続チェーン ID は、クライアントとサーバー間のエンドツーエンド接続を表します。

NetScaler ADM は、ホップカウントと接続チェーン ID を使用して、両方の NetScaler Gateway アプライアンスからのデータを相互に関連付け、レポートを生成します。

このモードで展開されている NetScaler Gateway アプライアンスを監視するには、まず NetScaler Gateway を NetScaler ADM インベントリに追加し、NetScaler ADM で AppFlow を有効にして、NetScaler ADM ダッシュボードでレポートを表示する必要があります。

### オプティマルゲートウェイに使用される仮想サーバーでの **HDX Insight** の設定

最適なゲートウェイで使用する仮想サーバーで HDX Insight を設定する手順:

1. [ネットワーク]>[インスタンス]に移動し、分析を有効にする NetScaler ADC インスタンスを選択します。
2. [アクションの選択] リストから、[ **Analytics** の設定] を選択します。
3. 認証用に設定された VPN 仮想サーバーを選択し、「**Analytics** を有効にする」をクリックします。
4. [ **HDX Insight** ] を選択し、次に [ **ICA** ] を選択します。
5. 必要に応じて他の詳細オプションを選択します。
6. [ **OK** ] をクリックします。
7. 他の VPN 仮想サーバーで手順 3~6 を繰り返します。

### NetScaler ADM でのデータ収集の有効化

両方のアプライアンスから ICA 詳細の収集を開始するように NetScaler ADM を有効にすると、収集された詳細情報は冗長になります。これは、両方のアプライアンスが同じ測定基準を報告するためです。この状況を解決するには、

最初の NetScaler Gateway アプライアンスの 1 つで AppFlow for ICA を有効にしてから、2 番目のアプライアンスで AppFlow for TCP を有効にする必要があります。これにより、一方のアプライアンスが 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が TCP AppFlow レコードをエクスポートします。これにより、ICA トラフィックを解析するときの処理時間も短縮されます。

**NetScaler ADM** から **AppFlow** 機能を有効にするには:

1. Web ブラウザで、Citrix ADM IP アドレス (例: <http://192.168.100.1>) を入力します。
2. [**User Name**] と [**Password**] に管理者の資格情報を入力します。
3. [ネットワーク]>[インスタンス]に移動し、分析を有効にする NetScaler ADC インスタンスを選択します。
4. [アクションの選択] リストから、[**Analytics** の設定] を選択します。
5. VPN 仮想サーバーを選択し、「アナリティクスを有効にする」をクリックします。
6. **HDX Insight** を選択し、\*\* ICA トラフィックまたは TCP トラフィックにはそれぞれ **ICA** または **TCP** を選択します \*\*。

注

NetScaler ADC アプライアンスのそれぞれのサービスまたはサービスグループで AppFlow ロギングが有効になっていない場合、Insight 列に「有効」と表示されていても、NetScaler ADM ダッシュボードにはレコードが表示されません。

7. [**OK**] をクリックします。

データをエクスポートするための **NetScaler Gateway** アプライアンスの設定

NetScaler Gateway アプライアンスをインストールした後、NetScaler Gateway アプライアンスで次の設定を構成して、レポートを NetScaler ADM にエクスポートする必要があります。

- 第 1 および第 2 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 の NetScaler Gateway 仮想サーバーを、最初の DMZ の NetScaler Gateway 仮想サーバーにバインドします。
- 2 つ目の DMZ で NetScaler Gateway でダブルホップを有効にします。
- 2 番目の DMZ の NetScaler Gateway 仮想サーバーでの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できるようにします
- 他の NetScaler Gateway アプライアンスが TCP レコードをエクスポートできるようにします。
- 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。

コマンドラインインターフェイスを使用して **NetScaler Gateway** を構成します。



1. 最初の DMZ の NetScaler Gateway 仮想サーバーが、2 番目の DMZ の NetScaler Gateway 仮想サーバーと通信するように構成します。

```
1 add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (
    ON or OFF)] [-imgGifToPng]
2
3 add vpn nextHopServer nh1 10.102.2.33 8443 - secure ON
```

2. 2 番目の DMZ の NetScaler Gateway 仮想サーバーを、最初の DMZ の NetScaler Gateway 仮想サーバーにバインドします。最初の DMZ の NetScaler Gateway で次のコマンドを実行します。

```
1 bind vpn vsriver <name> -nextHopServer <name>
2
3 bind vpn vsriver vs1 -nextHopServer nh1
```

3. 2 つ目の DMZ の NetScaler Gateway でダブルホップと AppFlow を有効にします。

```
1 set vpn vsriver <name> [- doubleHop ( ENABLED or DISABLED )] [-
    appflowLog ( ENABLED or DISABLED )]
2
3 set vpn vsriver vpnhop2 - doubleHop ENABLED - appFlowLog ENABLED
```

4. 2 番目の DMZ の NetScaler Gateway 仮想サーバーでの認証を無効にします。

```
1 set vpn vsriver <name> [-authentication (ON or OFF)]
2
3 set vpn vsriver vs -authentication OFF
```

5. いずれかの NetScaler Gateway アプライアンスで TCP レコードをエクスポートできるようにします。

```
1 bind vpn vsriver <name> [-policy <string> -priority <
    positive_integer>] [-type <type>]
2
3 bind vpn vsriver vpn1 -policy appflowpol1 -priority 101 - type
    OTHERTCP_REQUEST
```

6. 他の NetScaler Gateway アプライアンスで ICA レコードをエクスポートできるようにします:

```
1 bind vpn vsriver <name> [-policy <string> -priority <
    positive_integer>] [-type <type>]
2
3 bind vpn vsriver vpn2 -policy appflowpol1 -priority 101 -type
    ICA_REQUEST
```

7. 両方の NetScaler Gateway アプライアンスで接続チェーンを有効にします:

```
1 set appFlow param [-connectionChaining (ENABLED or DISABLED)]
2
3 set appflow param -connectionChaining ENABLED
```

構成ユーティリティを使用して **NetScaler Gateway** を構成します。

1. 最初の DMZ の NetScaler Gateway を構成して、2 番目の DMZ の NetScaler Gateway と通信し、2 番目の DMZ の NetScaler Gateway を最初の DMZ の NetScaler Gateway にバインドします。
  - a) [構成] タブで **[Citrix Gateway]** を展開し、[仮想サーバー] をクリックします。
  - b) 右側のウィンドウで、仮想サーバーをダブルクリックし、[詳細設定] グループで [公開アプリケーション] を展開します。
  - c) [ネクストホップサーバー] をクリックし、ネクストホップサーバーを 2 つ目の NetScaler Gateway アプライアンスにバインドします。
2. 2 つ目の DMZ で NetScaler Gateway でダブルホップを有効にします。
  - a) [構成] タブで **[Citrix Gateway]** を展開し、[仮想サーバー] をクリックします。
  - b) 右側のペインで仮想サーバーをダブルクリックし、[基本設定] グループで編集アイコンをクリックします。
  - c) さらに展開して「ダブルホップ」を選択し、「**OK**」をクリックします。
3. 2 番目の DMZ の NetScaler Gateway 上の仮想サーバーでの認証を無効にします。
  - a) 「構成」タブで「**Citrix Gateway**」を展開し、「仮想サーバー」をクリックします。
  - b) 右側のペインで仮想サーバーをダブルクリックし、[基本設定] グループで編集アイコンをクリックします。
  - c) [その他] を展開し、[認証を有効にする] をオフにします。
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) 「構成」タブで「**Citrix Gateway**」を展開し、「仮想サーバー」をクリックします。
  - b) 右側のウィンドウで、仮想サーバーをダブルクリックし、[詳細設定] グループで [ポリシー] を展開します。
  - c) 「+」アイコンをクリックし、「ポリシーの選択」リストから「**AppFlow**」を選択し、「タイプの選択」リストから「その他の **TCP** 要求」を選択します。
  - d) [続行] をクリックします。
  - e) ポリシーのバインドを追加して、[**Close**] をクリックします。
5. 他の NetScaler Gateway アプライアンスで ICA レコードをエクスポートできるようにします:
  - a) 「構成」タブで「**Citrix Gateway**」を展開し、「仮想サーバー」をクリックします。
  - b) 右側のペインで仮想サーバーをダブルクリックし、[詳細設定] グループで [ポリシー] を展開します。
  - c) 「+」アイコンをクリックし、「ポリシーの選択」リストから「AppFlow」を選択し、「タイプの選択」リストから「その他の **TCP** リクエスト」を選択します。

- d) [続行] をクリックします。
  - e) ポリシーのバインドを追加して、[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] の順に選択します。
  - b) 右側のペインの [設定] グループで、[Appflow 設定の変更] をダブルクリックします。
  - c) [Connection Chaining] を選択し、[OK] をクリックします。
7. 最初の DMZ の NetScaler Gateway を構成して、2 番目の DMZ の NetScaler Gateway と通信し、2 番目の DMZ の NetScaler Gateway を最初の DMZ の NetScaler Gateway にバインドします。
- a) [構成] タブで [NetScaler Gateway] を展開し、[仮想サーバー] をクリックします。
  - b) 右側のペインで仮想サーバーをダブルクリックし、「詳細設定」グループで「公開 アプリケーション」を展開します。
  - c) [ネクストホップサーバー] をクリックし、ネクストホップサーバーを 2 番目の NetScaler Gateway アプライアンスにバインドします。
8. 2 つ目の DMZ で NetScaler Gateway でダブルホップを有効にします。
- a) [構成] タブで [NetScaler Gateway] を展開し、[仮想サーバー] をクリックします。
  - b) 右側のペインで仮想サーバーをダブルクリックし、[基本設定] グループで編集アイコンをクリックします。
  - c) 「その他」を展開して「ダブルホップ」を選択し、「OK」をクリックします。
9. 2 番目の DMZ の NetScaler Gateway 上の仮想サーバーでの認証を無効にします。
- a) 「構成」タブで「Citrix Gateway」を展開し、「仮想サーバー」をクリックします。
  - b) 右側のペインで仮想サーバーをダブルクリックし、[基本設定] グループで編集アイコンをクリックします。
  - c) [その他] を展開し、[認証を有効にする] をオフにします。
10. 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) [構成] タブで [Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
  - b) 右側のウィンドウで、仮想サーバーをダブルクリックし、[詳細設定] グループで [ポリシー] を展開します。
  - c) 「+」アイコンをクリックし、「ポリシーの選択」リストから「AppFlow」を選択し、「タイプの選択」リストから「その他の TCP 要求」を選択します。
  - d) [続行] をクリックします。

- e) ポリシーのバインドを追加して、**[Close]** をクリックします。
11. 他の NetScaler Gateway アプライアンスが ICA レコードをエクスポートできるようにします。
    - a) [構成] タブで **[NetScaler Gateway]** を展開し、[仮想サーバー] をクリックします。
    - b) 右側のペインで仮想サーバーをダブルクリックし、[詳細設定] グループで [ポリシー] を展開します。
    - c) 「+」アイコンをクリックし、「ポリシーの選択」リストから「AppFlow」を選択し、「タイプの選択」リストから「その他の TCP 要求」を選択します。
    - d) [続行] をクリックします。
    - e) ポリシーのバインドを追加して、**[Close]** をクリックします。
  12. 両方の NetScaler Gateway アプライアンスで接続チェーンを有効にします。

透過モードで展開された **NetScaler ADC** を監視するためのデータ収集を有効にする

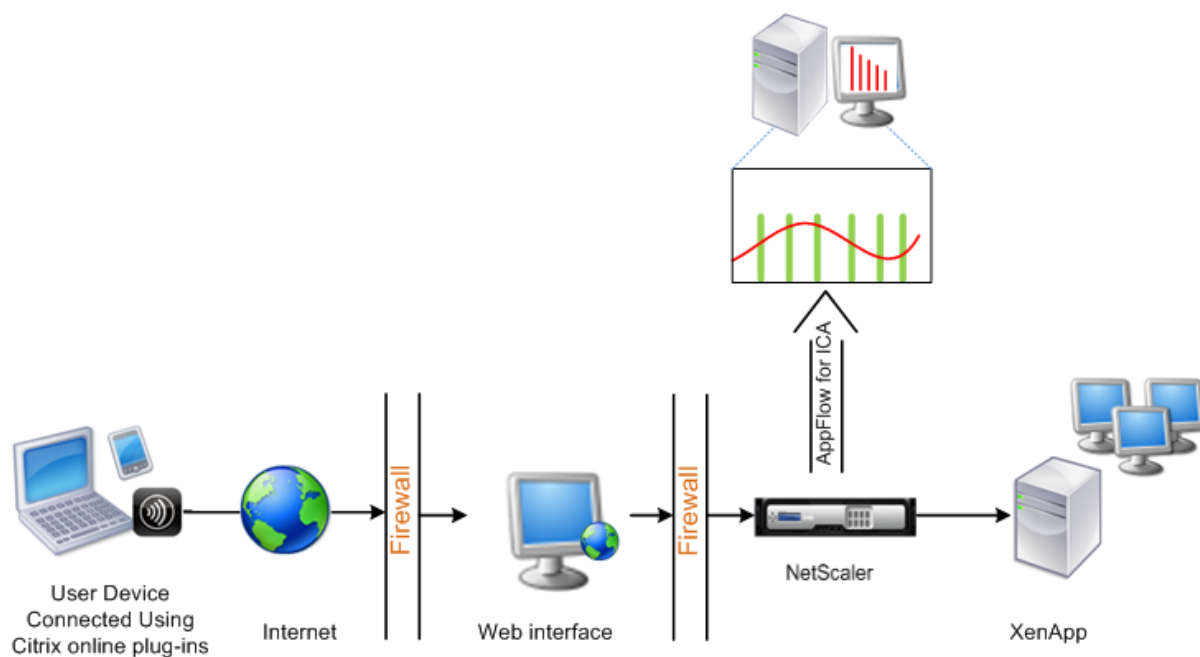
NetScaler ADC を透過モードで展開すると、クライアントは仮想サーバーを介さず、直接サーバーにアクセスできます。NetScaler ADC アプライアンスが Citrix Virtual Apps and Desktop 環境にトランスペアレントモードで展開されている場合、ICA トラフィックは VPN 経由で送信されません。

NetScaler ADC を NetScaler ADM インベントリに追加した後、データ収集のために AppFlow を有効にする必要があります。データ収集を有効にできるかどうかは、デバイスとモードによって決まります。その場合は、NetScaler ADM を AppFlow コレクタとして各 NetScaler ADC アプライアンスに追加する必要があります。また、AppFlow ポリシーを構成して、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必要があります。

注

- NetScaler ADM 構成ユーティリティを使用して、透過モードで展開された NetScaler ADC 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について詳しくは、「[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 ADC が透過モードで展開された場合の NetScaler ADM のネットワーク展開を示しています。



コマンドラインインターフェイスを使用して **NetScaler ADC** アプライアンスでデータ収集を構成するには:

コマンドプロンプトで、次の操作を行います:

1. アプライアンスにログオンします。
2. NetScaler ADC アプライアンスがトラフィックをリスンする ICA ポートを指定します。

```
1 set ns param --icaPorts <port>...
```

例:

```
1 set ns param -icaPorts 2598 1494
```

注

- このコマンドでは、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。ポート番号は、必要に応じて変更できます。

3. NetScaler ADC アプライアンスで、NetScaler Insight Center を AppFlow コレクタとして追加します。

```
1 add appflow collector <name> -IPAddress <ip_addr>
```

例:

```
1 add appflow collector MyInsight -IPAddress 192.168.1.101
```

注: NetScaler ADC アプライアンスで構成された AppFlow コレクタを表示するには、**show appflow** コレクタコマンドを使用します。

4. AppFlow アクションを作成し、コレクタをアクションに関連付けます。

```
1 add appflow action <name> -collectors <string> ...
```

例:

AppFlow アクションアクションコレクターを追加する MyInsight

5. AppFlow ポリシーを作成して、トラフィックを生成するためのルールを指定します。

```
1 add appflow policy <polname> <rule> <action>
```

例:

```
1 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。

```
1 bind appflow global <polname> <priority> -type <type>
```

例:

```
1 bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

注

ICA トラフィックに適用するには、**TYPE** の値は ICA\_REQ\_OVERRIDE または ICA\_REQ\_DEFAULT である必要があります。

7. AppFlow の flowRecordInterval パラメーターの値を 60 秒に設定します。

```
1 set appflow param -flowRecordInterval 60
```

例:

```
1 set appflow param -flowRecordInterval 60
```

8. 構成を保存します。種類: `save ns config`

““

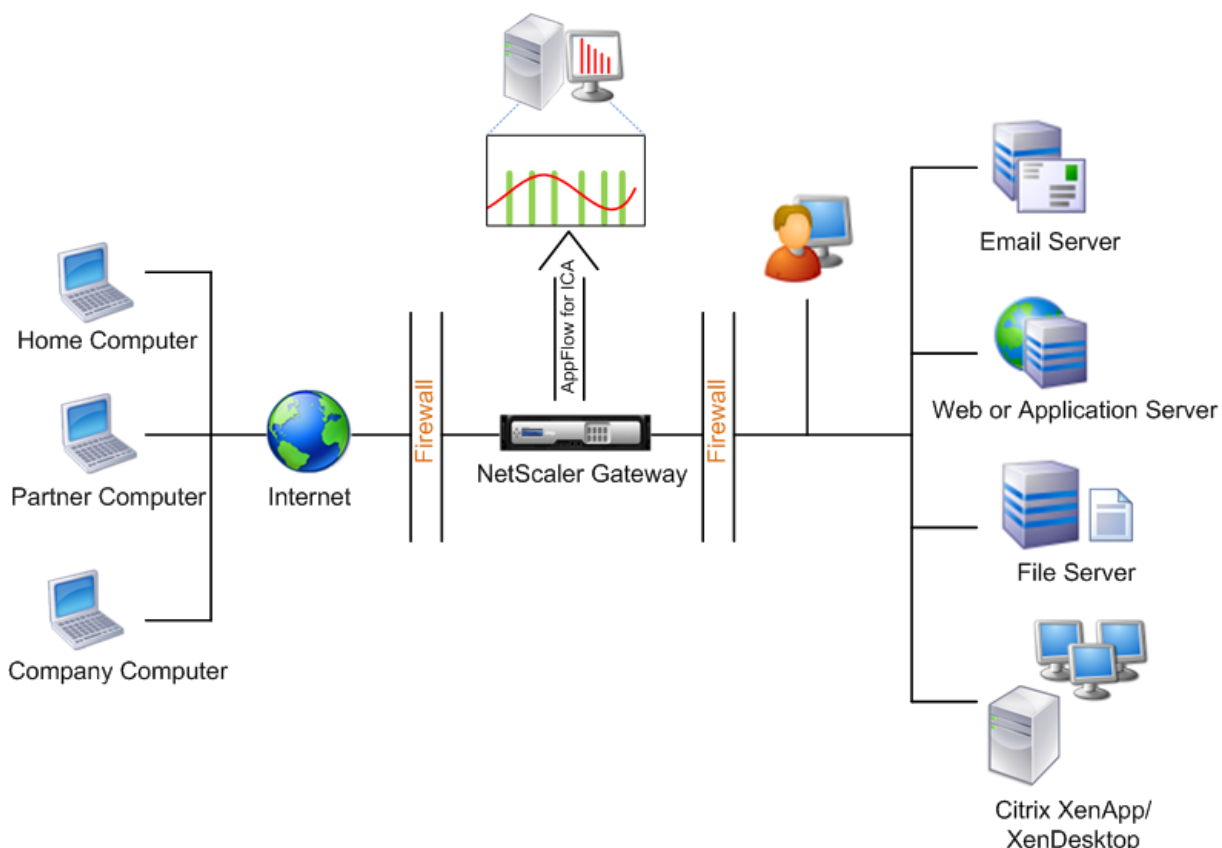
シングルホップモードで展開された **NetScaler Gateway** アプライアンスのデータ収集を有効にする

February 6, 2024

NetScaler Gateway をシングルホップモードで展開すると、ネットワークのエッジになります。Gateway インスタンスは、デスクトップ配信インフラストラクチャへのプロキシ ICA 接続を提供します。シングルホップは、最も単純で最も一般的な導入方法です。シングルホップモードは、外部ユーザーが組織内の内部ネットワークにアクセスしようとした場合にセキュリティを確保します。

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 ADC アプリ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 アプリアンスを Citrix Application Delivery Management (ADM) インベントリに追加し、ADM で AppFlow を有効にする必要があります。



**ADM** から **AppFlow** 機能を有効にするには:

1. [インフラストラクチャ] > [インスタンス] に移動し、分析を有効にする NetScaler ADC インスタンスを選択します。
2. 「アクション」リストから「**Insight**の有効化/無効化」を選択します。
3. **VPN** 仮想サーバーを選択し、「**AppFlow**を有効にする」をクリックします。
4. 「**AppFlow**を有効にする」フィールドに「**true**」と入力し、「**ICA**」を選択します。
5. [**OK**] をクリックします。

## 注

シングルホップモードで AppFlow を有効にすると、次のコマンドがバックグラウンドで実行されます。トラブルシューティングのため、こちらにそのコマンドを明記します。

- `add appflow collector \<name\> -IPAddress \<ip\_\_addr\>`
- `add appflow action \<name\> -collectors \<string\>`
- `set appflow param -flowRecordInterval \<secs\>`
- `disable ns feature AppFlow`
- `enable ns feature AppFlow`
- `add appflow policy \<name\> \<rule\> \<expression\>`
- `set appflow policy \<name\> -rule \<expression\>`
- `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\>  
>-priority \<positive\_\_integer\>`
- `set vpn vserver \<name\> -appflowLog ENABLED`
- `save ns config`

EUEM 仮想チャネルデータは、NetScaler ADM がゲートウェイインスタンスから受信する HDX Insight データの一部です。EUEM 仮想チャネルは、ICA RTT に関するデータを提供します。EUEM 仮想チャネルが有効になっていない場合でも、残りの HDX Insight データは NetScaler ADM に表示されます。

透過モードで展開された **NetScaler ADC** を監視するためのデータ収集を有効にする

February 6, 2024

NetScaler ADC を透過モードで展開すると、クライアントは仮想サーバーを介さず、直接サーバーにアクセスできます。Citrix ADC が Citrix Virtual Apps and Desktops 環境で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 ADC を NetScaler ADM インベントリに追加した後、データ収集のために AppFlow を有効にする必要があります。データ収集を有効にできるかどうかは、デバイスとモードによって決まります。その場合は、Citrix ADM を AppFlow コレクターとして各 Citrix ADC インスタンスに追加する必要があります。また、アプライアンスを通過するすべてまたは特定の ICA トラフィックを収集するように AppFlow ポリシーを構成する必要があります。

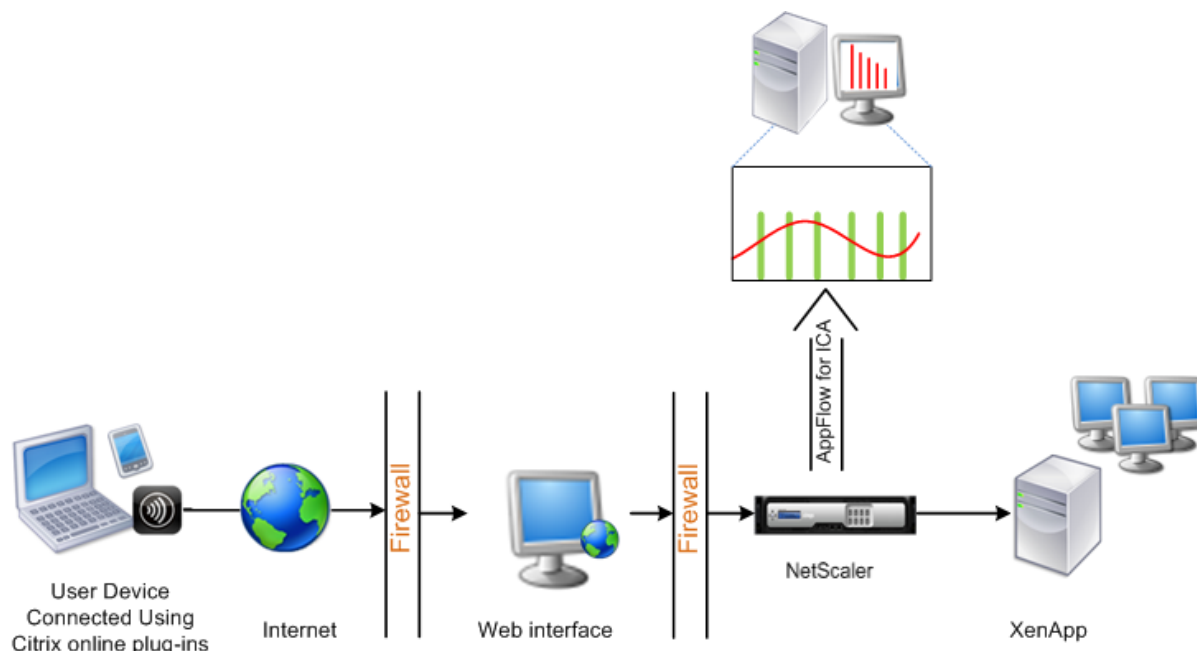
## 注

- NetScaler ADM 構成ユーティリティを使用して、透過モードで展開された NetScaler ADC 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 ADC が透過モードで展開された場合の NetScaler ADM のネットワーク展開を示しています。



コマンドラインインターフェイスを使用して **NetScaler ADC** アプライアンスでデータ収集を構成するには：

コマンドプロンプトで、次の操作を行います：

1. アプライアンスにログオンします。
2. NetScaler ADC 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。

```
1 set ns param --icaPorts \<port\>...
2 <!--NeedCopy-->
```

例：

```
1 set ns param -icaPorts 2598 1494
2 <!--NeedCopy-->
```

注

- このコマンドでは、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。ポート番号は、必要に応じて変更できます。

3. NetScaler ADC インスタンスで、NetScaler Insight Center を AppFlow コレクターとして追加します。

```
1 add appflow collector <name> -IPAddress <ip_addr>
2 <!--NeedCopy-->
```

例:

```
1 add appflow collector MyInsight -IPAddress 192.168.1.101
2 <!--NeedCopy-->
```

注: NetScaler ADC インスタンスで構成された AppFlow コレクタを表示するには、**show appflow** コレクタコマンドを使用します。

#### 4. AppFlow アクションを作成し、コレクタをアクションに関連付けます。

```
1 add appflow action <name> -collectors <string> ...
2 <!--NeedCopy-->
```

例:

```
1 add appflow action act -collectors MyInsight
2 <!--NeedCopy-->
```

#### 5. AppFlow ポリシーを作成して、トラフィックを生成するためのルールを指定します。

```
1 add appflow policy <policyname> <rule> <action>
2 <!--NeedCopy-->
```

例:

```
1 add appflow policy pol true act
2 <!--NeedCopy-->
```

#### 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。

```
1 bind appflow global <policyname> <priority> -type <type>
2 <!--NeedCopy-->
```

例:

```
1 bind appflow global pol 1 -type ICA_REQ_DEFAULT
2 <!--NeedCopy-->
```

注

ICA トラフィックに適用するには、**TYPE** の値は ICA\_REQ\_OVERRIDE または ICA\_REQ\_DEFAULT である必要があります。

#### 7. AppFlow の flowRecordInterval パラメーターの値を 60 秒に設定します。

```
1 set appflow param -flowRecordInterval 60
2 <!--NeedCopy-->
```

## 8. 構成を保存します。

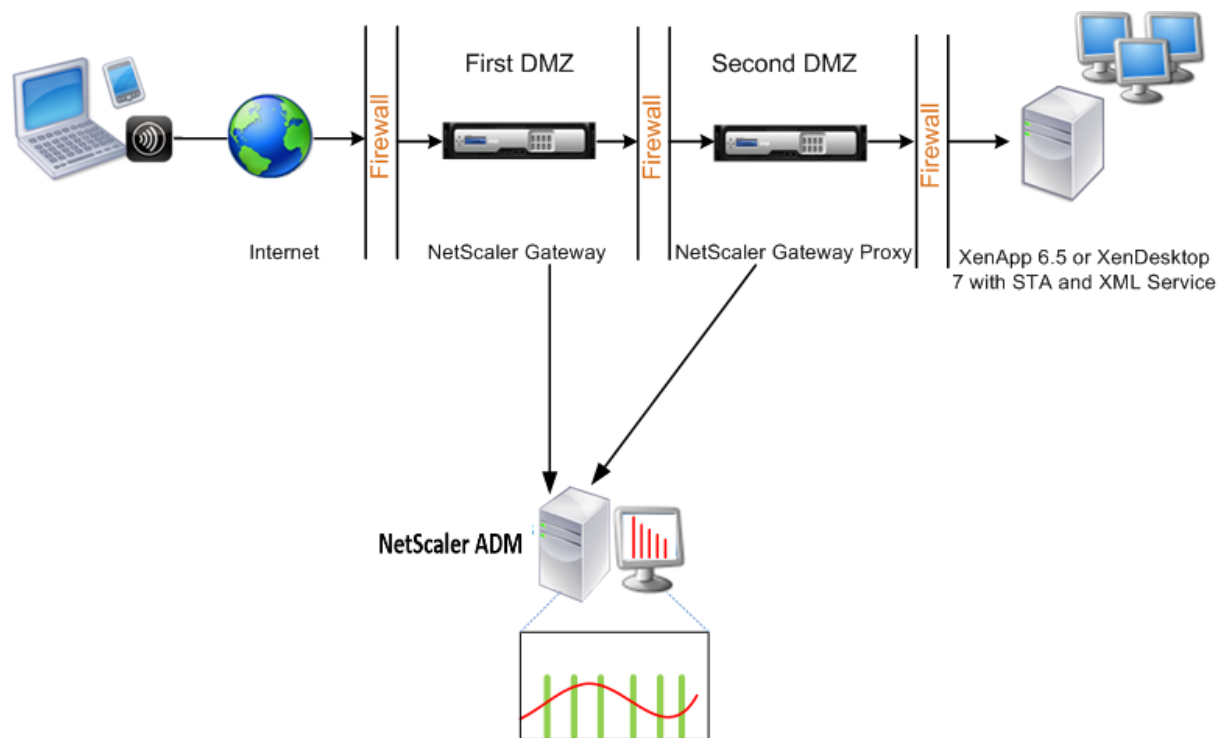
```
1 save ns config
2 <!--NeedCopy-->
```

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

February 6, 2024

NetScaler Gateway のダブルホップモードでは、攻撃者が複数のセキュリティゾーンまたは非武装ゾーン (DMZ) を侵入して安全なネットワーク内のサーバーに到達する必要があるため、組織の内部ネットワークをさらに保護します。ICA 接続が通過するホップ (NetScaler Gateway アプライアンス) の数と、各 TCP 接続のレイテンシーの詳細と、クライアントが認識する ICA レイテンシーの合計とどのようにフェアするかを分析する場合は、NetScaler ADM をインストールする必要があります。これにより、NetScaler Gateway アプライアンスこれらの重要な統計を報告する。

図 3: ダブルホップモードで展開される NetScaler ADM



最初の DMZ の 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、ユーザーの認証方法を決定し、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 つ目の DMZ の NetScaler Gateway は、NetScaler Gateway プロキシデバイスとして機能します。この NetScaler Gateway により、ICA トラフィックが 2 番目の DMZ を通過して、サーバーファームへのユーザー接続を完了できます。

NetScaler ADM は、最初の DMZ の NetScaler Gateway アプライアンスに属するサブネットか、2 番目の DMZ の NetScaler Gateway アプライアンスに属するサブネットのいずれかに展開できます。上の画像では、最初の DMZ の NetScaler ADM と NetScaler Gateway が同じサブネットにデプロイされています。

ダブルホップモードでは、NetScaler ADM は 1 つのアプライアンスから TCP レコードを、もう 1 つのアプライアンスから ICA レコードを収集します。NetScaler Gateway アプライアンスを NetScaler ADM インベントリに追加してデータ収集を有効にすると、各アプライアンスはホップカウントと接続チェーン ID を追跡してレポートをエクスポートします。

NetScaler ADM がレコードをエクスポートするアプライアンスを識別するために、各アプライアンスはホップ数で指定され、各接続は接続チェーン ID で指定されます。ホップカウントは、トラフィックがクライアントからサーバーに流れる NetScaler Gateway アプライアンスの数を表します。接続チェーン ID は、クライアントとサーバー間のエンドツーエンド接続を表します。

NetScaler ADM は、ホップカウントと接続チェーン ID を使用して、両方の NetScaler Gateway アプライアンスからのデータを相互に関連付け、レポートを生成します。

このモードで展開されている NetScaler Gateway アプライアンスを監視するには、まず NetScaler Gateway を NetScaler ADM インベントリに追加し、NetScaler ADM で AppFlow を有効にして、NetScaler ADM ダッシュボードでレポートを表示する必要があります。

## NetScaler ADM でのデータ収集の有効化

両方のアプライアンスから ICA 詳細の収集を開始するように NetScaler ADM を有効にすると、収集された詳細情報は冗長になります。これは、両方のアプライアンスが同じ測定基準を報告するためです。この状況に対処するには、最初の NetScaler Gateway アプライアンスのいずれかで AppFlow for TCP を有効にし、2 番目のアプライアンスで AppFlow for ICA を有効にする必要があります。これにより、一方のアプライアンスが 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が TCP AppFlow レコードをエクスポートします。これにより、ICA トラフィックを解析するときの処理時間も短縮されます。

NetScaler ADM から **AppFlow** 機能を有効にするには：

1. [インフラストラクチャ] > [インスタンス] に移動し、分析を有効にする NetScaler ADC インスタンスを選択します。
2. 「アクション」リストから「**Insight** の有効化/無効化」を選択します。
3. VPN 仮想サーバーを選択し、[ **AppFlow** を有効にする ] をクリックします。
4. [ **AppFlow** を有効にする ] フィールドに「**true**」と入力し、ICA トラフィックの場合は「**ICA/TCP**」を TCP トラフィックにそれぞれ選択します。

## 注

NetScaler ADC アプライアンス上のサービスまたはサービスグループで AppFlow ログが有効になっていない場合、インサイト列に [有効] と表示されていても、NetScaler ADM ダッシュボードにレコードは表示されません。

5. [OK] をクリックします。

### データをエクスポートするための **NetScaler Gateway** アプライアンスの構成

NetScaler Gateway アプライアンスをインストールした後、NetScaler Gateway アプライアンスで次の設定を構成して、レポートを NetScaler ADM にエクスポートする必要があります。

- 第 1 および第 2 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 の NetScaler Gateway 仮想サーバーを、最初の DMZ の NetScaler Gateway 仮想サーバーにバインドします。
- 2 つ目の DMZ で NetScaler Gateway でダブルホップを有効にします。
- 2 番目の DMZ の NetScaler Gateway 仮想サーバーでの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できるようにします
- 他の NetScaler Gateway アプライアンスが TCP レコードをエクスポートできるようにします。
- 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。

コマンドラインインターフェイスを使用して **NetScaler Gateway** を構成します。

1. 最初の DMZ の NetScaler Gateway 仮想サーバーが、2 番目の DMZ の NetScaler Gateway 仮想サーバーと通信するように構成します。

---

**add vpn nextHopServer** [**\*\*-secure\*\***(ON OFF)] [**-imgGifToPng**] ...

---

```
1 add vpn nextHopServer nh1 10.102.2.33 8443 -secure ON
2 <!--NeedCopy-->
```

2. 2 番目の DMZ の NetScaler Gateway 仮想サーバーを、最初の DMZ の NetScaler Gateway 仮想サーバーにバインドします。最初の DMZ の NetScaler Gateway で次のコマンドを実行します。

**bind vpn vsriver** <name> **-nextHopServer** <name>

```
1 bind vpn vsriver vs1 -nextHopServer nh1
2 <!--NeedCopy-->
```

3. 2 つ目の DMZ の NetScaler Gateway でダブルホップと AppFlow を有効にします。

```
set vpn vserver vpnhop2 (DISABLED) [- appflowLog (DISABLED)]
vserver [**- doubleHop** (ENABLED)
ENABLED
```

---

```
1 set vpn vserver vpnhop2 - doubleHop ENABLED - appFlowLog ENABLED
2 <!--NeedCopy-->
```

4. 2 番目の DMZ の NetScaler Gateway 仮想サーバーでの認証を無効にします。

```
set vpn vserver [**-authentication** (ON OFF)]
```

---

```
1 set vpn vserver vs -authentication OFF
2 <!--NeedCopy-->
```

5. いずれかの NetScaler Gateway アプライアンスで TCP レコードをエクスポートできるようにします。

```
bind vpn vserver<name> [-policy<string> -priority<positive_integer>] [-type<type>]
```

```
1 bind vpn vserver vpn1 -policy appflowpol1 -priority 101 - type
OTHERTCP_REQUEST
2 <!--NeedCopy-->
```

6. 他の NetScaler Gateway アプライアンスで ICA レコードをエクスポートできるようにします:

```
bind vpn vserver<name> [-policy<string> -priority<positive_integer>] [-type<type>]
```

```
1 bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
ICA_REQUEST
2 <!--NeedCopy-->
```

7. 両方の NetScaler Gateway アプライアンスで接続チェーンを有効にします:

```
set appFlow param [-connectionChaining (ENABLED)
DISABLED)]
```

---

```
1 set appflow param -connectionChaining ENABLED
2 <!--NeedCopy-->
```

構成ユーティリティを使用して **Citrix Gateway** を構成する方法:

- 最初の DMZ の NetScaler Gateway を構成して、2 番目の DMZ の NetScaler Gateway と通信し、2 番目の DMZ の NetScaler Gateway を最初の DMZ の NetScaler Gateway にバインドします。

- a) [構成] タブで **[Citrix Gateway]** を展開し、[仮想サーバー] をクリックします。
  - b) 右側のウィンドウで、仮想サーバーをダブルクリックし、[詳細設定] グループで [公開アプリケーション] を展開します。
  - c) [ネクストホップサーバー] をクリックし、ネクストホップサーバーを 2 つ目の NetScaler Gateway アプライアンスにバインドします。
2. 2 つ目の DMZ で NetScaler Gateway でダブルホップを有効にします。
- a) [構成] タブで **[Citrix Gateway]** を展開し、[仮想サーバー] をクリックします。
  - b) 右側のペインで仮想サーバーをダブルクリックし、[基本設定] グループで編集アイコンをクリックします。
  - c) **[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 の NetScaler Gateway 上の仮想サーバーでの認証を無効にします。
- a) 「構成」タブで 「**Citrix Gateway**」 を展開し、「仮想サーバー」 をクリックします。
  - b) 右側のペインで仮想サーバーをダブルクリックし、[基本設定] グループで編集アイコンをクリックします。
  - c) [その他] を展開し、[認証を有効にする] をオフにします。
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) 「構成」タブで 「**Citrix Gateway**」 を展開し、「仮想サーバー」 をクリックします。
  - b) 右側のウィンドウで、仮想サーバーをダブルクリックし、[詳細設定] グループで [ポリシー] を展開します。
  - c) [+] アイコンをクリックし、[ポリシーの選択] リストから **[AppFlow]** を選択し、[タイプの選択] ドロップダウンリストから [その他の **TCP** 要求] を選択します。
  - d) [続行] をクリックします。
  - e) ポリシーのバインドを追加して、**[Close]** をクリックします。
5. 他の NetScaler Gateway アプライアンスで ICA レコードをエクスポートできるようにします:
- a) 「構成」タブで 「**Citrix Gateway**」 を展開し、「仮想サーバー」 をクリックします。
  - b) 右側のウィンドウで、仮想サーバーをダブルクリックし、[詳細設定] グループで [ポリシー] を展開します。
  - c) [+] アイコンをクリックし、[ポリシーの選択] ドロップダウンリストから **[AppFlow]** を選択し、[TheChoose Type] ドロップダウンリストから [その他の **TCP** 要求] を選択します。
  - d) [続行] をクリックします。

- e) ポリシーのバインドを追加して、**[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) [構成] タブで、[システム] > **[Appflow]** に移動します。
  - b) 右側のウィンドウの [設定] で、**[Appflow 設定の変更]** をクリックします。
  - c) **[Connection Chaining]** を選択し、**[OK]** をクリックします。

## LAN ユーザーモードで展開された **NetScaler ADC** を監視するためのデータ収集を有効にする

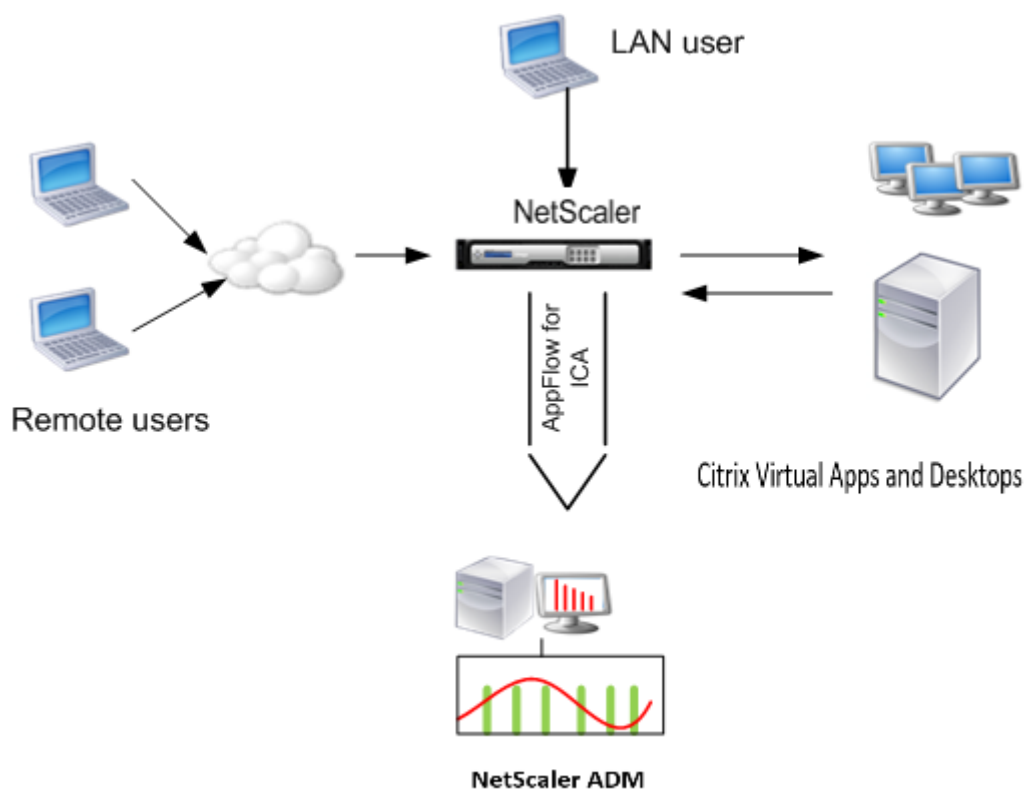
February 6, 2024

Citrix Virtual App またはデスクトップアプリケーションにアクセスする外部ユーザーは、Citrix Gateway で自身自身を認証する必要があります。ただし、内部ユーザーは NetScaler Gateway にリダイレクトする必要がない場合があります。また、透過モードの展開では、管理者が手動でルーティングポリシーを適用して、要求が NetScaler ADC 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、NetScaler Gateway アプライアンス上で SOCKS プロキシとして機能するキャッシュリダイレクト仮想サーバーを構成して、LAN ユーザーモードで NetScaler ADC アプライアンスを展開します。

図 4: LAN ユーザーモードで展開される NetScaler ADM





注: NetScaler ADM と NetScaler Gateway アプライアンスは同じサブネットにあります。

このモードで展開された NetScaler ADC アプライアンスを監視するには、まず NetScaler ADC 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 ADC アプライアンスを NetScaler ADM インベントリに追加した後、データ収集のために AppFlow を有効にする必要があります。

注

- NetScaler ADM 構成ユーティリティを使用して、LAN ユーザーモードで展開された NetScaler ADC 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について詳しくは、「コマンドリファレンス」を参照してください。
- ポリシー式については、「ポリシーと式」を参照してください。

コマンドラインインターフェイスを使用して **NetScaler ADC** アプライアンスでデータ収集を構成するには:

コマンドプロンプトで、次の操作を行います:

1. アプライアンスにログオンします。
2. プロキシ IP およびポートを指定してフォワードプロキシキャッシュリダイレクト仮想サーバーを追加します。また、サービスタイプとして HDX を指定します。

```

1 add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
  cacheType <cachetype>] [ - cltTimeout <secs>]
2 <!--NeedCopy-->

```

例:

```

1 add cr vserver cr1 HDX 10.12.2.2 443 - cacheType FORWARD -
  cltTimeout 180
2 <!--NeedCopy-->

```

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する場合は、VPN トラフィックに一致するポリシーによって適用されるアクションを追加します。

```

1 add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]
2
3 add vpn trafficPolicy** \<name\> \<rule\> \<action\>
4 <!--NeedCopy-->

```

例:

```

1 add vpn trafficAction act1 tcp -HDX ON
2
3 add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
4 <!--NeedCopy-->

```

### 3. NetScaler ADM を AppFlow コレクタとして NetScaler ADC アプライアンスに追加します。

```

1 add appflow collector** \<name\> \*\*-IPAddress\*\* \\<ip\_\_addr
  \>
2 <!--NeedCopy-->

```

例:

```

1 add appflow collector MyInsight -IPAddress 192.168.1.101
2 <!--NeedCopy-->

```

### 4. AppFlow アクションを作成し、コレクタをアクションに関連付けます。

```

1 add appflow action** \<name\> \*\*-collectors\*\* \<string\> ...
2 <!--NeedCopy-->

```

例:

```

1 add appflow action act -collectors MyInsight
2 <!--NeedCopy-->

```

### 5. AppFlow ポリシーを作成して、トラフィックを生成するためのルールを指定します。

```

1 add appflow policy** \<policyname\> \<rule\> \<action\>
2 <!--NeedCopy-->

```

例:

```
1 add appflow policy pol true act
2 <!--NeedCopy-->
```

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。

```
1 bind appflow global** \<pollicyname\> \<priority\> \*\*-type\*\* \<
  type\>
2 <!--NeedCopy-->
```

例:

```
1 bind appflow global pol 1 -type ICA_REQ_DEFAULT
2 <!--NeedCopy-->
```

注

タイプの値は、ICA トラフィックに適用するには、ICA\_REQ\_OVERRIDE または ICA\_REQ\_DEFAULT である必要があります。

7. AppFlow の flowRecordInterval パラメーターの値を 60 秒に設定します。

```
1 set appflow param -flowRecordInterval 60
2 <!--NeedCopy-->
```

例:

```
1 set appflow param -flowRecordInterval 60
2 <!--NeedCopy-->
```

8. 構成を保存します。

```
1 save ns config
2 <!--NeedCopy-->
```

## HDX Insight のしきい値を作成してアラートを構成する

February 6, 2024

Citrix Application Delivery Management (ADM) に関する HDX Insight を使用すると、Citrix ADC インスタンスを通過する HDX トラフィックを監視できます。NetScaler ADM では、Insight トラフィックの監視に使用するさまざまなカウンターのしきい値を設定できます。また、NetScaler ADM でルールを構成し、アラートを作成することもできます。

HDX トラフィックの種類は、アプリケーション、デスクトップ、ゲートウェイ、ライセンス、ユーザーなどのさまざまなエンティティに関連付けられます。すべてのエンティティには、それらに関連付けられた異なるメトリックを含

めることができます。たとえば、アプリケーションエンティティは、さまざまなヒット、アプリケーションによって消費される帯域幅、およびサーバーの応答時間に関連付けられます。ユーザーエンティティは、WAN 遅延、DC 遅延、ICA RTT、およびユーザーが消費する帯域幅に関連付けることができます。

NetScaler ADM の HDX Insight のしきい値管理により、事前にルールを作成し、設定されたしきい値に違反するたびにアラートを構成できます。今回のリリースでは、このしきい値管理を拡張して、複数のしきい値ルールを設定できるようになりました。個別のルールの代わりに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用の 1 つ以上のユーザー定義のしきい値ルールで構成されます。各ルールは、ルールの作成時に入力した期待値に対して監視されます。ユーザーエンティティの場合、閾値グループをジオロケーションに関連付けることもできます。

NetScaler ADM でアラートが生成されるのは、構成されたしきい値グループ内のすべてのルールに違反した場合のみです。たとえば、アプリケーションの合計セッション起動数とアプリケーション起動数を 1 つのしきい値グループとして監視できます。アラートは、両方のルールに違反した場合にのみ生成されます。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。

以下に、いくつかの例を挙げる。

- 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 ミリ秒以下である必要があります
- しきい値ルール 2: ユーザー (エンティティ) の WAN 遅延 (メトリック) は 100 ミリ秒以下である必要があります

しきい値グループの例は次のようになります。{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、最初に監視するエンティティを選択する必要があります。次に、ルールの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回数] または [アプリケーションの起動回数] を選択できます。エンティティと指標の組み合わせごとに 1 つのルールを作成できます。付属のコンパレータ (>、<、>=、<=) を使用して、各指標の閾値を入力します。

### 注

単一グループ内の複数のエンティティを監視したくない場合は、エンティティごとに個別のしきい値ルールグループを作成する必要があります。

カウンターの値がしきい値を超えると、NetScaler ADM はしきい値違反を示すイベントを生成し、イベントごとにアラートを作成します。

アラートの受信方法を構成する必要があります。アラートを Citrix ADM に表示したり、モバイルデバイスでアラートを電子メールまたは SMS として受信したりできるようにすることができます。最後の 2 つの操作では、NetScaler ADM で電子メールサーバーまたは SMS サーバーを構成する必要があります。

閾値グループは、ユーザーエンティティの地理固有の監視のためにジオロケーションにバインドすることもできます。

### 使用事例の例

ABC Inc. はグローバル企業で、50 カ国以上にオフィスを構えています。同社は、シンガポールとカリフォルニア州に Citrix Virtual Apps and Desktops をホストする 2 つのデータセンターを持っています。同社の従業員は、NetScaler Gateway および Citrix GSLB ベースのリダイレクトを使用して、世界中の Citrix Virtual Apps and Desktops にアクセスします。ABC Inc. の Citrix Virtual Apps and Desktops 管理者であるエリックは、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、いつでもどこでもアクセスできるようにアプリとデスクトップ配信を最適化したいと考えています。また、ICA の RTT やレイテンシーなどのユーザーエクスペリエンス指標をチェックし、偏差を積極的に引き上げたいと考えています。

ABC Inc. のユーザーは、分散した存在感を持っています。データセンターの近くにいるユーザーもあれば、データセンターから離れた場所にいるユーザーもいます。ユーザーベースが広く分散されているため、メトリックと対応するしきい値もこれらの場所によって異なります。たとえば、データセンターに近い場所の ICA RTT は 5~10 ミリ秒ですが、遠隔地の場合は約 100 ミリ秒になることがあります。

HDX Insight の閾値ルールグループ管理により、Eric は場所ごとに地域固有の閾値ルールグループを設定し、エリアごとの違反があった場合はメールまたは SMS でアラートを受け取ることができます。また、Eric は、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、根本原因をキャパシティの問題に絞り込むこともできます。Eric は、Citrix Virtual Apps and Desktops ポートフォリオのすべてのメトリックを手動で調べるという複雑さを心配することなく、あらゆる偏差をプロアクティブに追跡できるようになりました。

**NetScaler ADM** を使用してしきい値ルールグループを作成し、**HDX Insight** のアラートを構成するには：

1. Citrix ADM で、**[Analytics]** > **[設定]** > **[しきい値]** に移動します。[しきい値] ページが表示されたら、**[追加]** をクリックします。
2. **[Create Thresholds and Alerts]** ページで次の詳細を指定します。
  - a) 名前。NetScaler ADM 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) トラフィックタイプ。リストボックスから HDX を選択します。
  - c) エンティティ。リスト・ボックスから、カテゴリまたはリソース・タイプを選択します。エンティティは、以前に選択したトラフィックタイプごとに異なります。
  - d) 参照キー。参照キーは、選択したトラフィックタイプとエンティティに基づいて自動的に生成されます。
  - e) 期間。リストボックスから、エンティティを監視する時間間隔を選択します。エンティティは、1 時間、1 日、または 1 週間の期間を監視できます。

## ← Create Threshold

Name\*  
ABC-users ?

Traffic Type\*  
HDX ?

Entity\*  
Users ?

Reference Key  
UserName

Duration\*  
Day ?

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しています。

HDX トラフィックの場合は、「ルールを追加」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 [ルールを追加 \*\*] ポップアップ \*\* ウィンドウに値を入力します。

### Add Rules

Metric\*  
ICA RTT (seconds) ?

Comparator\*  
> ?

Value\*  
500 ?

OK

Close

複数のルールを作成して、各エンティティを監視できます。1つのグループに複数のルールを作成すると、個々のルールではなく、しきい値ルールグループとしてエンティティを監視できます。[ **OK** ] をクリックしてウィンドウを閉じます。

Configure Rule	
<input type="button" value="Add Rule"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	Metric
<input type="checkbox"/>	ICA RTT (seconds) > 500
<input type="checkbox"/>	WAN latency (ms) > 100

#### 4. Users エンティティの位置情報タグの構成

必要に応じて、[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 レイテンシーのパフォーマンスを監視するジオロケーションベースのタグ付けを作成する例を示しています。

Configure Geo Details
Country <input type="text" value="UNITED STATES"/>
Region <input type="text" value="CALIFORNIA"/>
City <input type="text" value="CALIFORNIA CITY"/>

- [しきい値を有効にする] をクリックして、NetScaler ADM でエンティティの監視を開始できるようにします。
- オプションで、電子メール通知や SMS 通知などのアクションを構成します。
- [ **Create** ] をクリックして、しきい値ルールグループを作成します。

## HDX Insight レポートと指標の表示

February 6, 2024

HDX Insight は、NetScaler ADC インスタンスの HDX トラフィックに関するレポートとメトリックを完全に可視化します。

選択した任意のエンティティについて、HDX メトリックを確認できます。各ビューには、次のカテゴリのエンティティが含まれます。

- ユーザー: 選択した時間間隔内に Citrix Virtual App または Desktop にアクセス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のレポートと、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、関連するすべての関連情報を表示します。

- インスタンス: 着信トラフィックのゲートウェイとして機能する NetScaler ADC インスタンスに関するレポートを表示します。
- デスクトップ: 選択した期間内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: 指定したタイムスロット内に使用された SSL VPN ライセンスの合計に関するレポートを表示します。

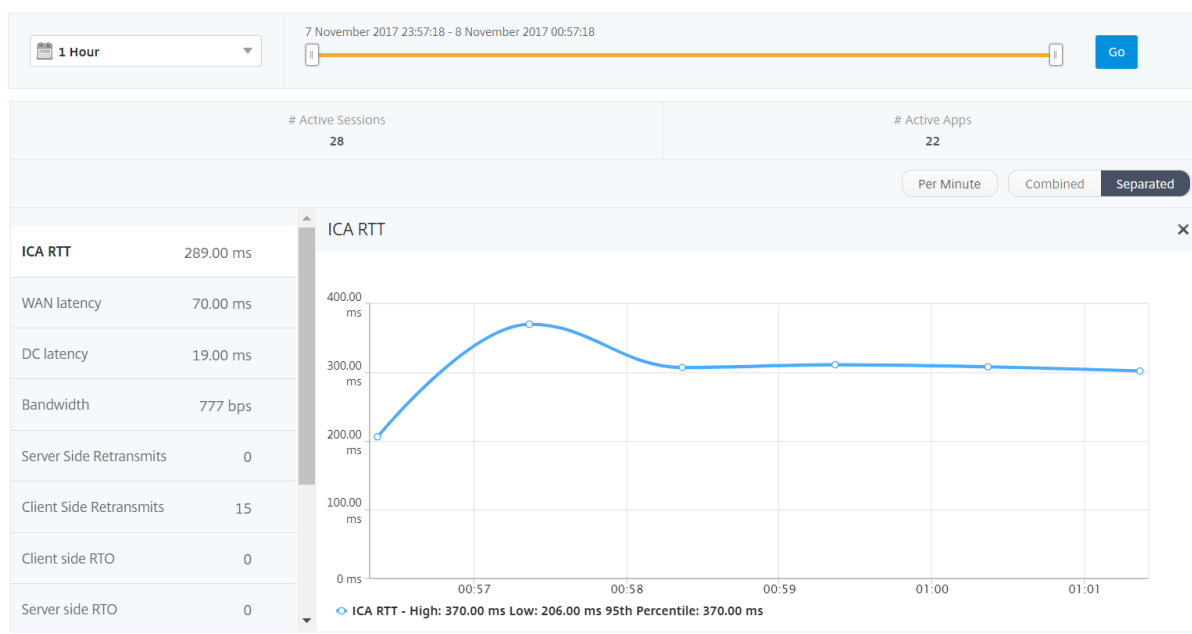
注

[ライセンス] の値は、Citrix SD-WAN アプライアンスには適用されません。

### ユーザービューのレポートとメトリック

このビューのレポートとメトリックは、Citrix Virtual Apps and Desktops ユーザーごとに表示されます。

[Analytics] > [HDX Insight] > [ユーザー] に移動します。



ユーザー・ビュー・レポートおよびメトリックは、次のセクションで構成されます。

- [Summary] ビュー
- [Per User] ビュー
- Per User Session ビュー

### [Summary] ビュー

[Summary] ビューには、選択した期間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指標/レポートには、特に指定がない限り、選択した期間の対応する値が表示されます。

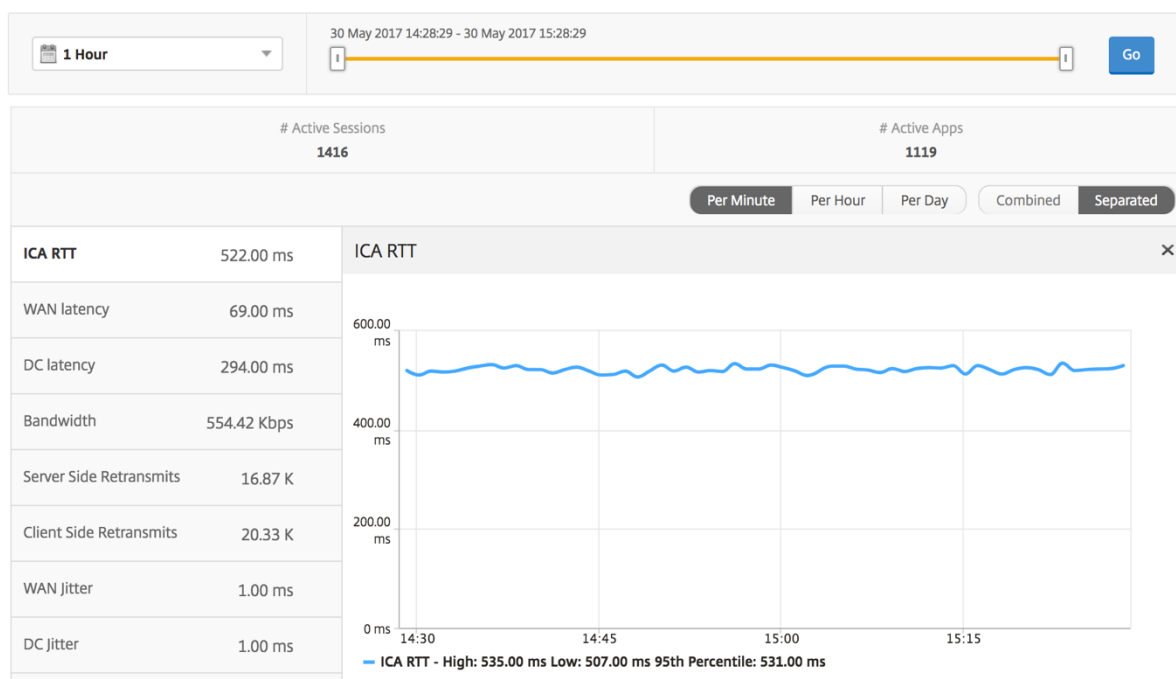


選択した期間を変更するには、次の手順に従います。

1. 期間リストまたはタイムスライダを使用して、目的の時間間隔を設定します。
2. **[Go]** をクリックします。

#### 折れ線グラフ

メトリック	説明
アクティブセッション	この数字は、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ケーション数	この数字は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	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、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	NetScaler ADC 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。
Server side fast RTO	NetScaler ADC 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、TCP ウィンドウのサイズがゼロであることをクライアントがアダバタイズした回数を表します。
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、TCP ウィンドウサイズがゼロであることをサーバーがアダバタイズした回数を表します。



ユーザー概要レポート このレポートに固有のメトリックは以下のとおりです。

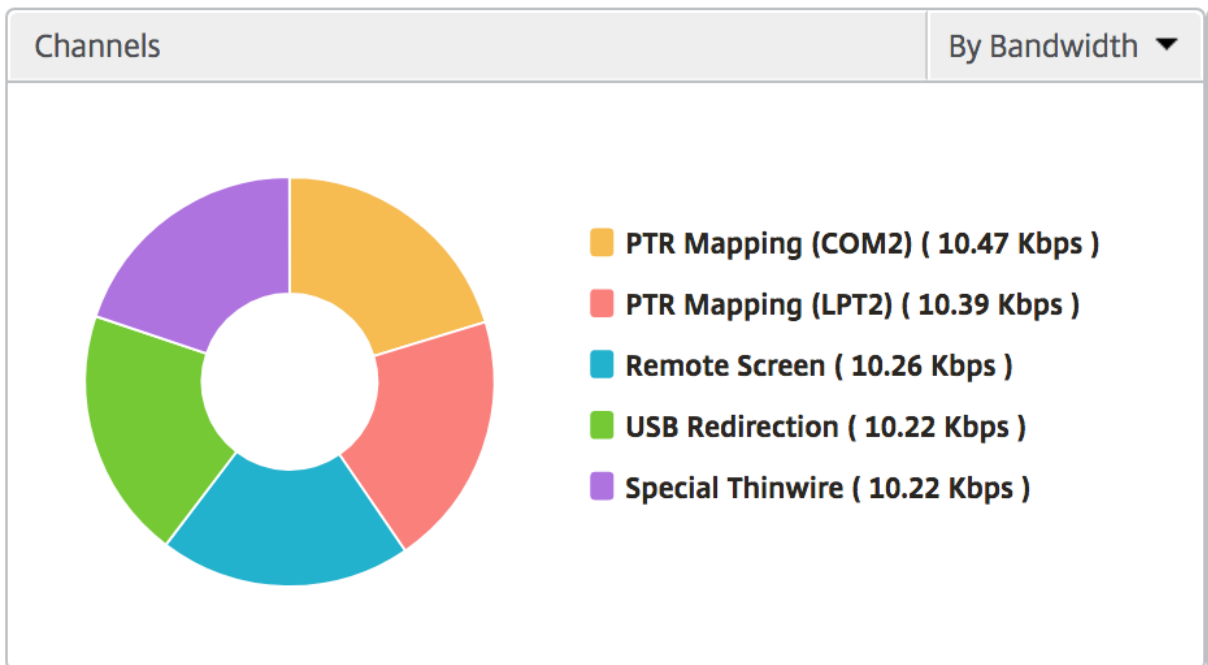
メトリックス	説明
アクティブセッション	この数字は、アクティブな Citrix Virtual App and Desktop セッションの数を示します。
アクティブなアプリケーション数	この数字は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
サーバー側の再転送	NetScaler ADC 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。

メトリックス	説明
クライアント側の再転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	NetScaler ADC 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。
Server side fast RTO	NetScaler ADC 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、TCP ウィンドウのサイズがゼロであることをクライアントがアダプタイズした回数を表します。
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、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。
アプリケーションの起動数合計	指定した期間にユーザーによって起動された合計アプリ数です。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。
Active Desktops	特定の時間間隔におけるアクティブな Citrix Virtual Desktops 合計数。

---

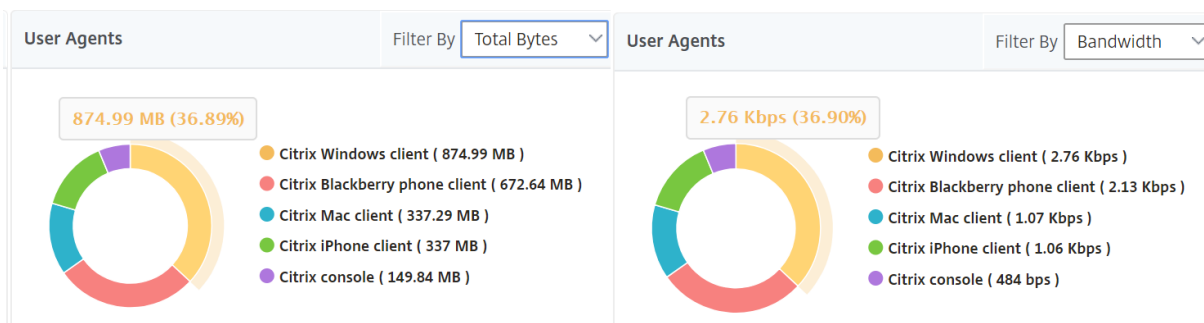
User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Client Side Retransmits
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	0
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	0
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	0
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	0
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	0
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	0
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	0
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	0
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	0
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	0
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	0
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	0
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	0
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	0
randyby	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	0
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	0

チャンネル Channels では、各 ICA 仮想チャンネルで消費された全帯域幅または総バイト数をドーナツグラフ形式で表します。これらのメトリックは、[Bandwidth] または [Total bytes] で並べ替えることができます。



ユーザーエージェント ユーザーエージェントは、各レシーバクライアントが消費する全体の帯域幅/合計バイトをドーナツチャートの形式で表します。グラフ内の色付きの各セグメントは、1つの受信側クライアントを表します。

セグメントの長さは、その受信側クライアントでアプリケーションを起動するユーザーの数によって異なります。また、帯域幅または合計バイト数でメトリックをソートすることもできます。



各セグメントをクリックすると、そのレシーバクライアントを使用しているユーザーの詳細が表示されます。

### User Details

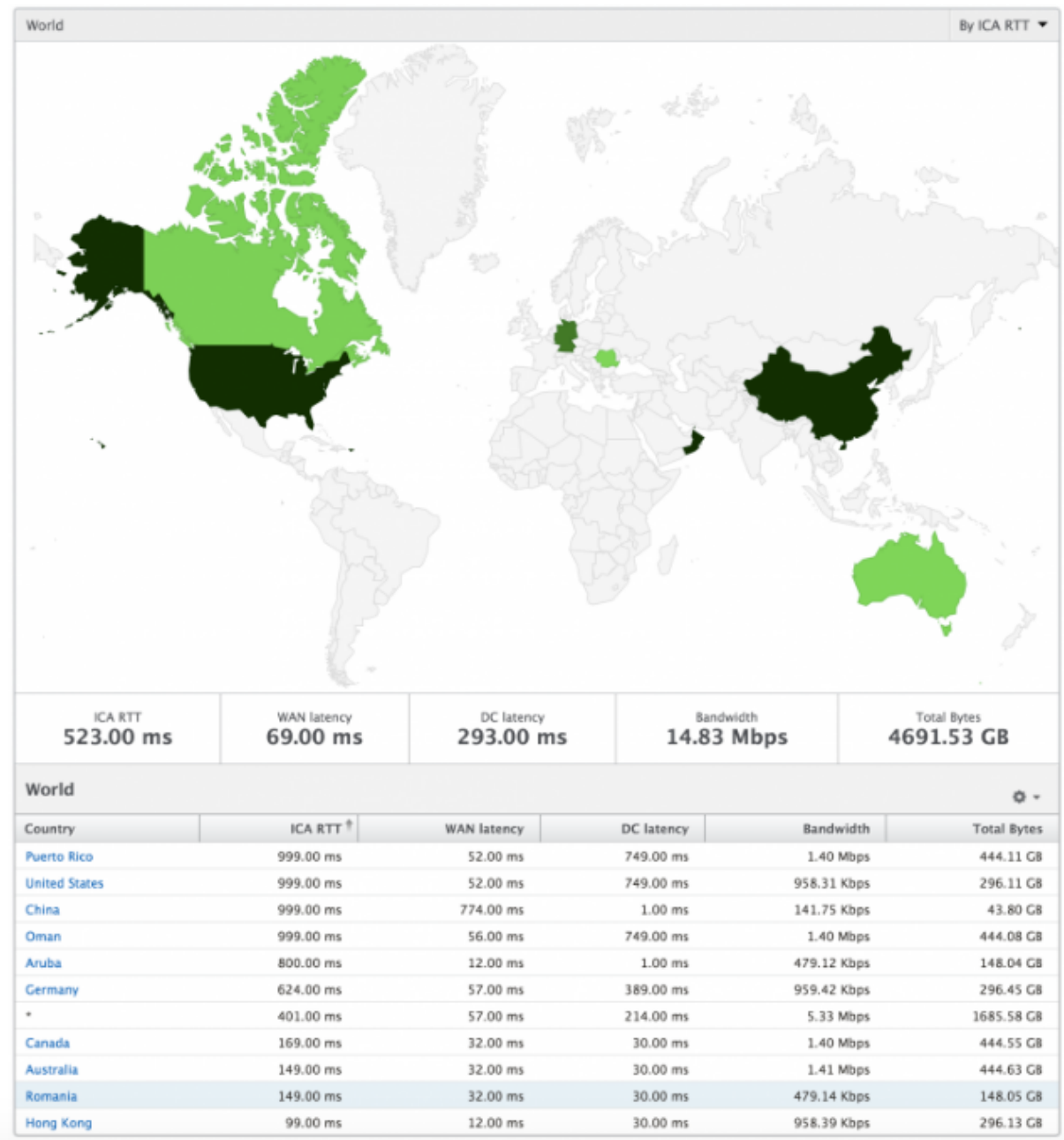
Name	Server Side Retransmits	ICA RTT	Client SRTT	Session Reconnect	Latency	Clientside zero window size event	Server SRTT
c1\daniel	0	149.44	1		149.44	0	
ryan	5071	4640	1		4640	0	
ramas	0	994.71	1		994.71	0	

しきい値違反数 [Thresholds Breach Count] メトリックは、指定した期間において違反があったしきい値の数を表します。

世界地図 HDX Insight の [World Map] ビューでは、管理者が地理的な観点からユーザー履歴およびアクティブユーザーの詳細を確認できます。管理者は、単に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持つことができ、特定の国にドリルダウンし、さらに都市にドリルダウンすることができます。管理者はさらにドリルダウンして、都市および州別に情報を表示できます。NetScaler ADM バージョン 12.0 以降では、地理的な場所から接続しているユーザーにドリルダウンできます。

HDX Insight のワールドマップでは、以下の詳細を表示できます。また、各指標の密度はヒートマップの形式で表示されます。

- ICA 往復時間
- WAN 遅延
- DC の遅延
- 帯域幅
- バイト数合計



ユーザーごとのビュー

[Per User] ビューには、選択した特定のユーザーについて詳細なエンドユーザーエクスペリエンスに関するレポートが示されます。

特定のユーザーのメトリックに移動する手順は、次のとおりです。

1. サポートされている Web ブラウザを使用して、NetScaler ADM にログインします。
2. [ **Analytics** ] > [ **HDX Insight** ] > [ ユーザー ] に移動します。

### 3. [User Summary] レポートで目的のユーザーを選択します。

折れ線グラフ 折れ線グラフには、指定した期間における選択したユーザーのメトリックすべての概要が表示されます。

現在/終了したセッションレポート このレポートは、選択したユーザーの現在/終了済みのユーザーセッションすべてに関係します。これらのメトリックは、Start Time、Session Reconnects、ACR Counts を基準にして並べ替えることができます。

メトリックス	説明
セッション ID	ICA セッションの一意の ID。
セッションの種類	アプリケーション/デスクトップ。
状態	緑はアクティブなセッション、赤は非アクティブなセッション。
ホストの遅延	サーバーネットワークが原因で NetScaler ADC 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	特定の期間にセッションで使用された帯域幅です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
インターバルあたりのバイト数	特定の期間にセッションで使用されたバイト数。
開始時刻	セッションの開始時間。
アップタイム	セッションの実行時間
クライアント IP アドレス	エンドユーザーの IP。
サーバー IP アドレス	バックエンド/Citrix Virtual Apps サーバー IP。
NetScaler IP Address	NetScaler の管理 IP (NSIP)。
クライアントの種類	受信者の種類-Citrix Windows クライアントなど
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値 ([Yes] または [No])。セッションがマルチストリーム ICA かどうかを表します。
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。たとえば、NetScaler Gateway のユーザー/透過モードなどです。

メトリックス	説明
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。
ICA 往復時間	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、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
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、TCP ウィンドウのサイズがゼロであることをクライアントがアドバタイズした回数を表します。
Client side fast RTO	NetScaler ADC 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。

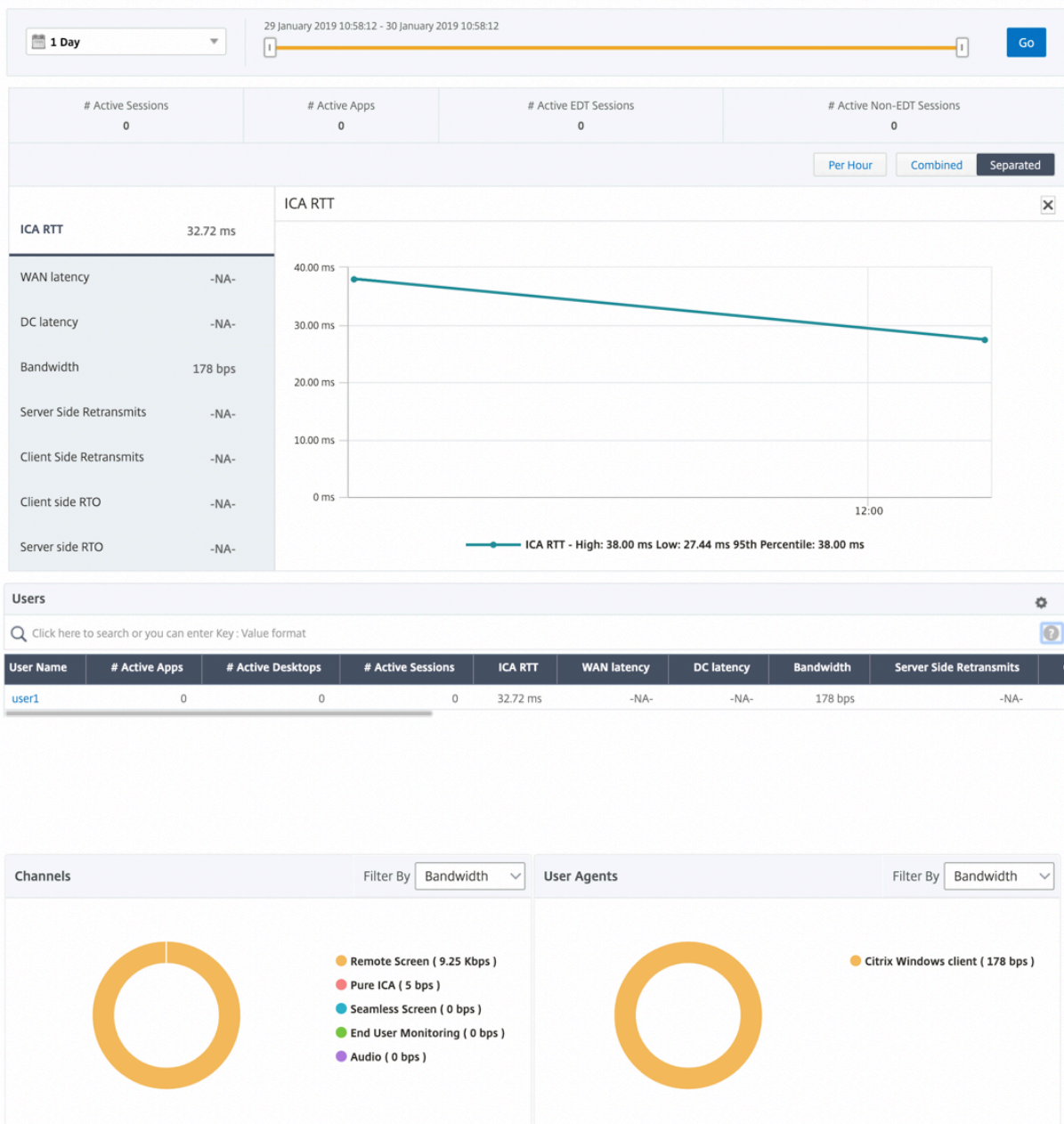


メトリックス	説明
サーバー側のゼロ ウィンドウ サイズ イベント	このカウンターは、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。
Server side fast RTO	NetScaler ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。

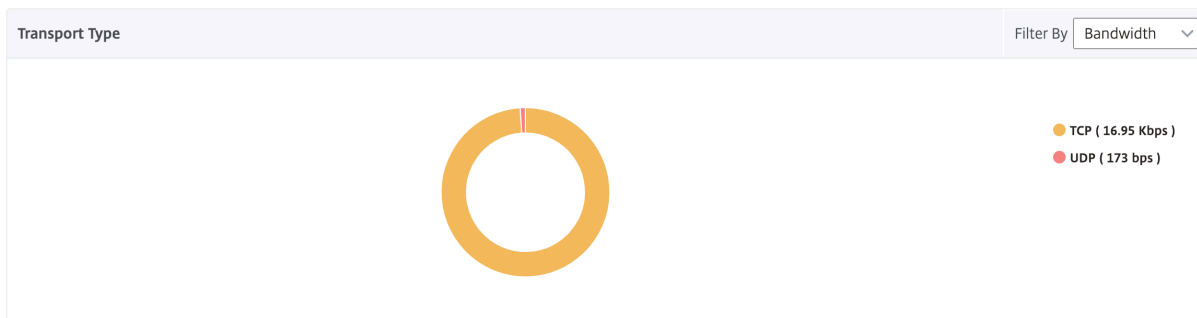
### HDX Insight における EDT のサポート

NetScaler Application Delivery Management (ADM) では、HDX Insight ight の分析を表示するための啓発データトランスポート (EDT) がサポートされるようになりました。つまり、ADM は UDP と TCP の両方のプロトコルをサポートするようになりました。NetScaler Gateway の EDT サポートにより、Citrix Receiver を実行しているユーザーの仮想デスクトップの高品位セッション内ユーザーエクスペリエンスが保証されます。

HDX Insight は、アクティブセッションレポートの一部として、EDT セッションと非 EDT セッションの数を表示するようになりました。「ユーザー」 (Users) テーブルには、システム内のすべてのユーザーの詳細なレポートが表示されます。この表には、WAN レイテンシー、DC レイテンシー、再送信、RTO などのメトリックが示されています。これらのメトリックのいくつかは、現在 TCP スタックから計算されるため、EDT セッションを持つユーザーには使用できません。したがって、彼らは「NA」として登場する。



新しいドーナツグラフが導入され、ユーザーが使用したプロトコルの種類に基づいて、ユーザーが消費した帯域幅と合計バイト数を確認できるようになりました。



注

HDX Insight の EDT は、リリース 12.1 ビルド 50.28 の NetScaler ADM でサポートされ、リリース 12.1 ビルド 49.23 の ADC インスタンスで使用できます。

**NetScaler ADM 12.0** 以降から入手可能な **HDX Insight** メトリック:

L7 Client-side Latency	ICA クライアントと NetScaler ADC インスタンスの間で観測された平均 L7 遅延時間。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。
L7 Server-side Latency	NetScaler ADC デバイスと Citrix Virtual Apps の間で観測された平均 L7 遅延。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。
違反の最大遅延	定義済みしきい値の違反が一定期間に発生した場合の、L7 遅延の最大値。
平均侵害待ち時間	システムが「L7 遅延時間を超過」した状態のときの、L7 遅延の平均値。
L7 しきい値違反数	L7 のしきい値違反が発生した回数。

Current Sessions By Start Time

Diagram	Session ID	Total Bytes	Bandwidth per Interval	Session Type	ICA RTT	Bytes per Interval	WAN latency	DC latency	Host Delay
	0000...000001	209.84 KB	11.58 Kbps	Application	854 ms	209.84 KB	83.00 ms	771 ms	4.00 ms
	0000...000001	127.18 KB	40.70 Kbps	Application	848 ms	127.18 KB	65.00 ms	710 ms	4.00 ms

Terminated Sessions By Start Time

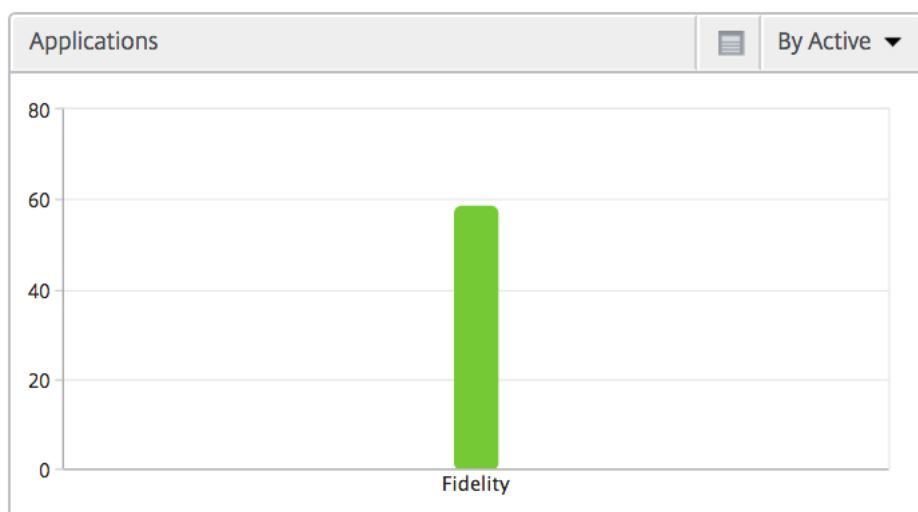
Session ID	Session Type	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Session Bandwidth	Total Bytes	Bytes per Interval
0000...000001	Application	1.01 s	59.00 ms	763.00 ms	9.40 Kbps	9.40 Kbps	1.38 MB	1.38 MB
0000...000001	Desktop	971.00 ms	59.00 ms	733.00 ms	8.82 Kbps	8.82 Kbps	1.29 MB	1.29 MB
0000...000001	Application	998.00	51.00 ms	732.00 ms	9.91 Kbps	9.91 Kbps	1.45 MB	1.45 MB

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示しています。以下のメトリクスは [Desktop Launch Count] および [Bandwidth] を基準にしてソートできます。

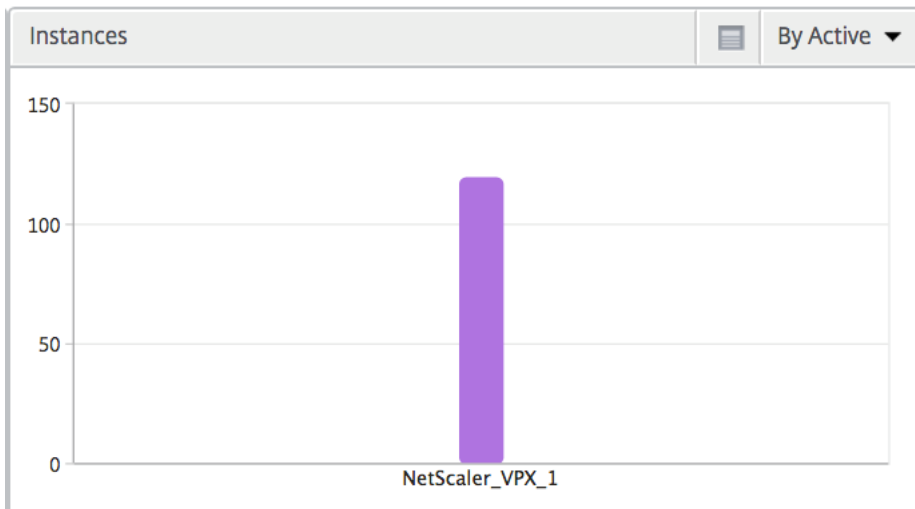
メトリクス	説明
名前	Citrix Virtual Desktops の名前。
デスクトップ起動回数	デスクトップが起動された回数です。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
ICA 往復時間	ICA RTT は、Citrix Virtual App または 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、ユーザーに表示される画面の遅れです。

Desktop Users						By Desktop Launch Count ▾
Name	Desktop Launch Count ↑	Bandwidth	DC latency	WAN latency	ICA RTT	
XenDesktop33	177	9.38 Kbps	749.00 ms	57.00 ms	1.00 s	

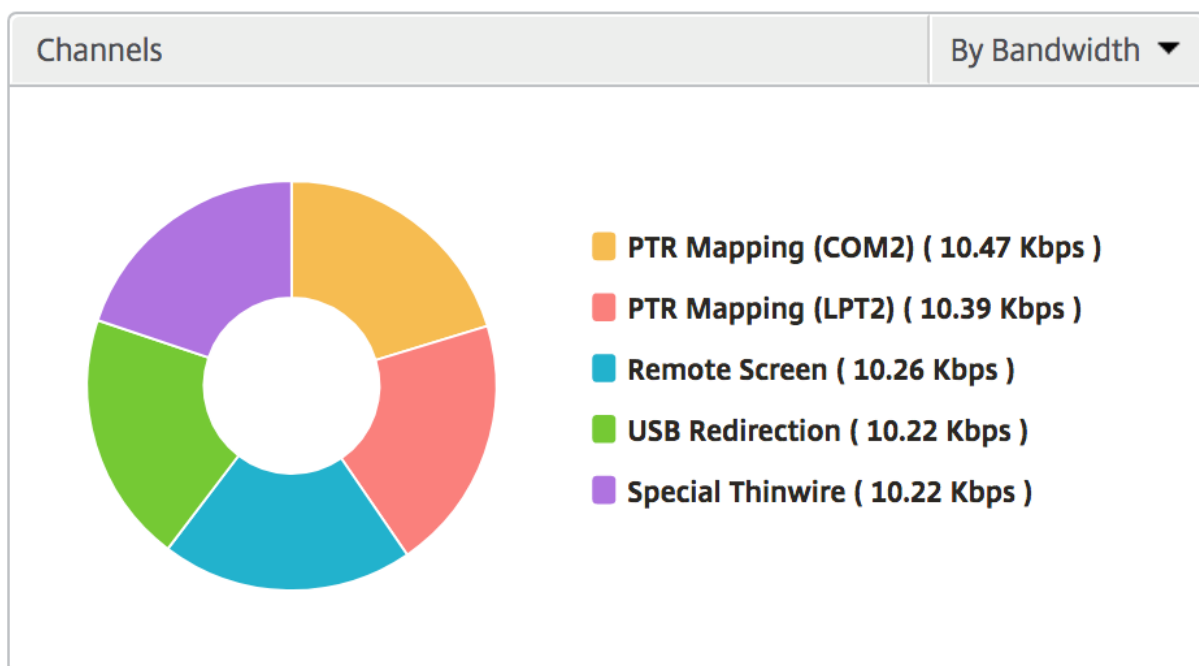
アプリケーション アクティブでソートされたアプリ、合計セッション起動数、合計アプリ起動数、および起動期間を表す棒グラフ。



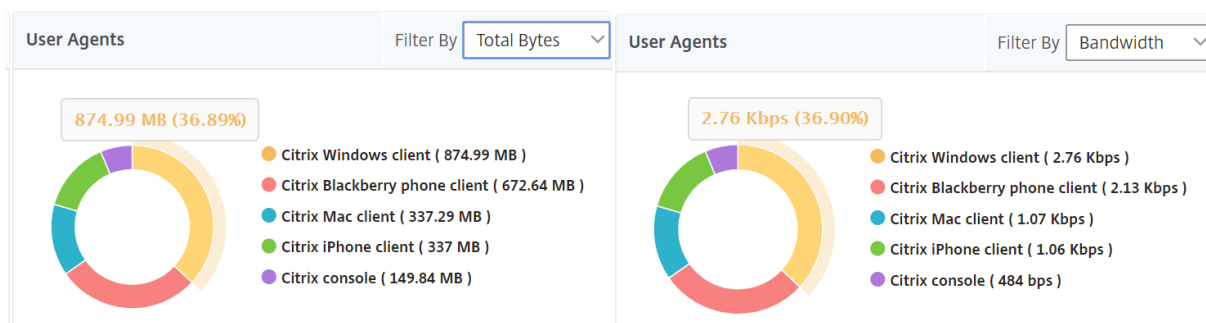
インスタンス NetScaler ADC インスタンスをアクティブおよび合計アプリでソートした棒グラフ



チャンネル Channels では、各 ICA 仮想チャンネルで消費された全帯域幅または総バイト数をドーナツグラフ形式で表します。これらのメトリックは、[Bandwidth] または [Total bytes] で並べ替えることができます。



ユーザーエージェント User Agents では、各エンドポイントで消費された全帯域幅または総バイト数をドーナツグラフ形式で表します。これらのメトリックは、[Bandwidth] または [Total bytes] で並べ替えることができます。



ユーザー単位のセッション・ビュー [Per User Session] ビューには、選択したユーザーのセッションに関するレポートが表示されます。

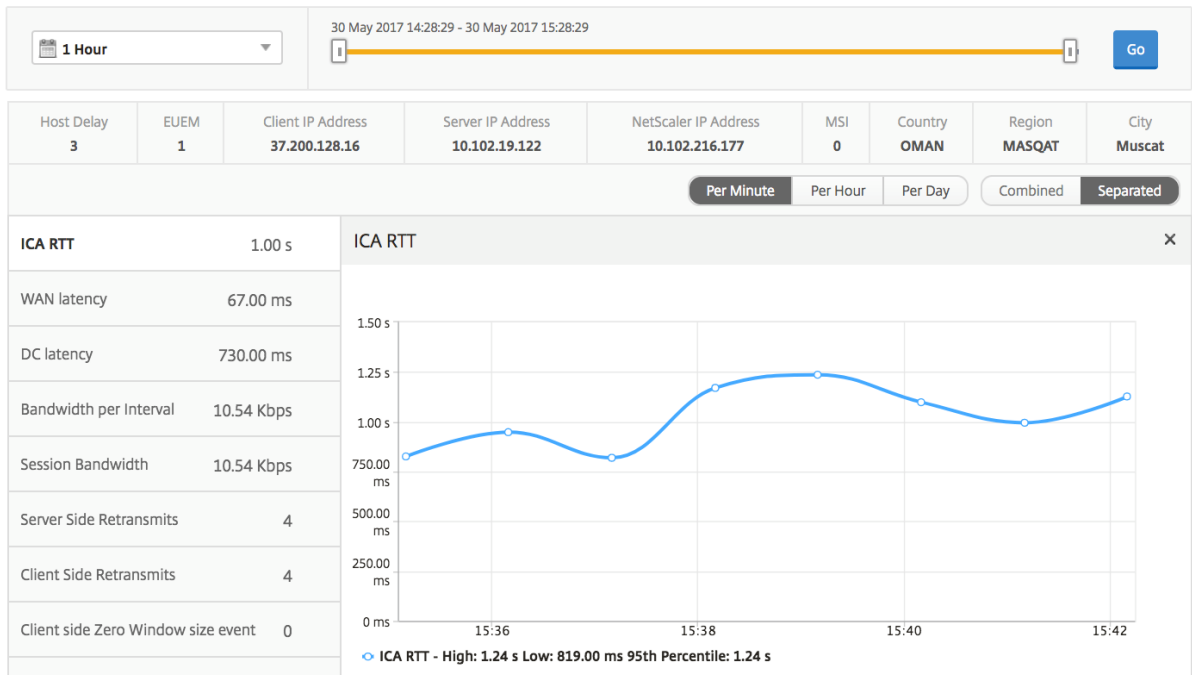
選択したユーザーのセッションのメトリックを表示する手順は、次のとおりです。

1. [ **Analytics** ] > [ **HDX Insight** ] > [ ユーザー ] に移動します。
2. 「ユーザー 概要レポート」セクションから特定のユーザー を選択します。
3. 「現在のセッション」または「終了したセッション」列からセッションを選択します。

#### 時系列グラフ

メトリックス	説明
セッション再接続	この数字は、アクティブな Citrix Virtual Apps and Desktops セッションの数を示します。
ACR 数	この数字は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	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それぞれ操作しているときにユーザーが経験する画面遅延です。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
サーバー側の再転送	NetScaler ADC 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。

メトリックス	説明
クライアント側の再転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	NetScaler ADC 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。
Server side fast RTO	NetScaler ADC 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	特定の期間にセッションで使用された帯域幅です。
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、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。
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、TCP ウィンドウのサイズがゼロであることをクライアントがアダプタイズした回数を表します。



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および起動時間で並べ替えることができます。

Active Applications				By # Active Sessions
Name	# Active Sessions	Launch Duration	# Active Apps	
Fidelity	1	557.00 ms	1	

関連セッション [Related Sessions] セクションには、選択したユーザーのセッションに関連するセッションが表示されます。このリレーションシップは、共通サーバーまたは共通 NetScaler ADC として選択できます。

Related Sessions											By Common Server
Session ID	Session Type	User Name	State	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Total Bytes	Total Bytes	Bytes	
0000...000001	Application	grahmm	●	1.021 s	51.00 ms	737 ms	9.26 Kbps	9.26 Kbps	977.73 KB		
0000...000001	Application	liam	●	955 ms	50.00 ms	733 ms	10.91 Kbps	10.91 Kbps	1.26 MB		
0000...000001	Application	grahmm	●	1.058 s	38.00 ms	817 ms	10.27 Kbps	10.27 Kbps	367.24 KB		

### Application ビューのレポートとメトリック

このビューのレポートとメトリックは、Citrix Virtual Apps に焦点を当てています。

アプリケーション・ビューに移動する手順は、次のとおりです。

1. 「Analytics」 > 「HDX Insight」 > 「アプリケーション」の順に選択します。

#### [Summary] ビュー

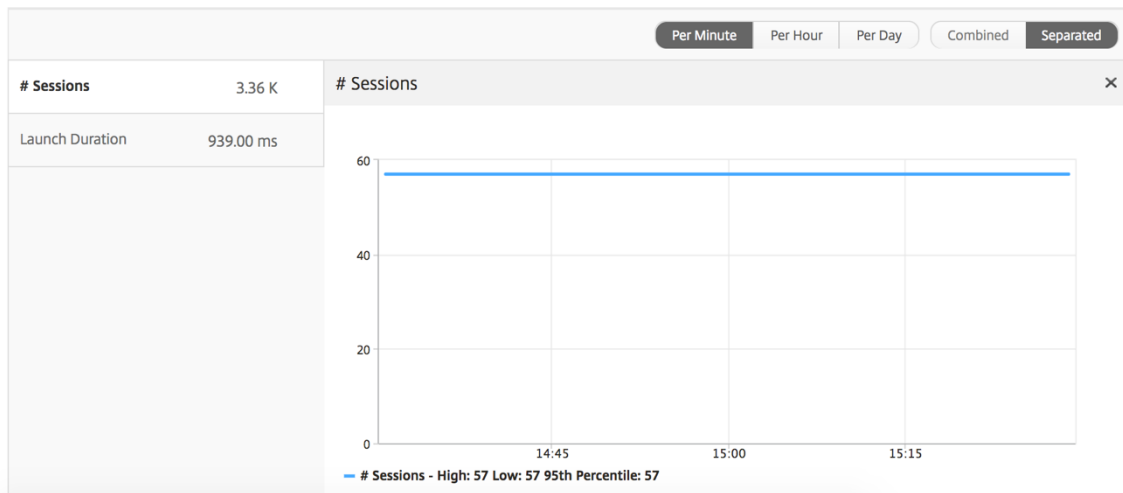
Summary ビューには、選択した期間中にログインしたすべてのアプリケーションのレポートが表示されます。

明示的に言及しない限り、すべての指標/レポートには、選択した期間に対応する値が含まれます。

#### 折れ線グラフ

メトリック	説明
セッション	特定の期間の合計セッション数。
起動時間	アプリケーションの起動にかかった平均時間。





アプリケーション・サマリー・レポート

メトリックス	説明
名前	Citrix Virtual Apps の名前。
セッションの起動数合計	特定の時間間隔におけるアクティブな Citrix Virtual App セッションの総数。
アプリケーションの起動数合計	特定の期間中に起動された Citrix Virtual App アプリケーションの総数。
起動期間	Citrix Virtual App の起動に要した平均時間。

Applications			
Name	Total App Launch Count	Launch Duration	Total Session Launch count
Microsoft Outlook	531	514.00 ms	531
Microsoft Visio	354	555.00 ms	354
Microsoft Word	354	557.00 ms	354
Microsoft Excel	354	555.00 ms	354

アクティブなアプリケーションレポート

メトリックス	説明
名前	Citrix Virtual Apps 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	特定の期間にこのアプリケーションを使用したアクティブなユーザーセッション数。

メトリックス

説明

アクティブなアプリケーション数

このアプリケーションのアクティブなセッション数。

### Active Applications

Name	State	# Active Sessions	# Active Apps
Communicator	●	60	60
Fidelity	●	60	60
GoToMeeting	●	60	60
...		--	--

しきい値レポート しきい値レポートは、選択した期間内に エンティティが「アプリケーション」として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、「しきい値の作成方法」を参照してください。

折れ線グラフ

メトリック

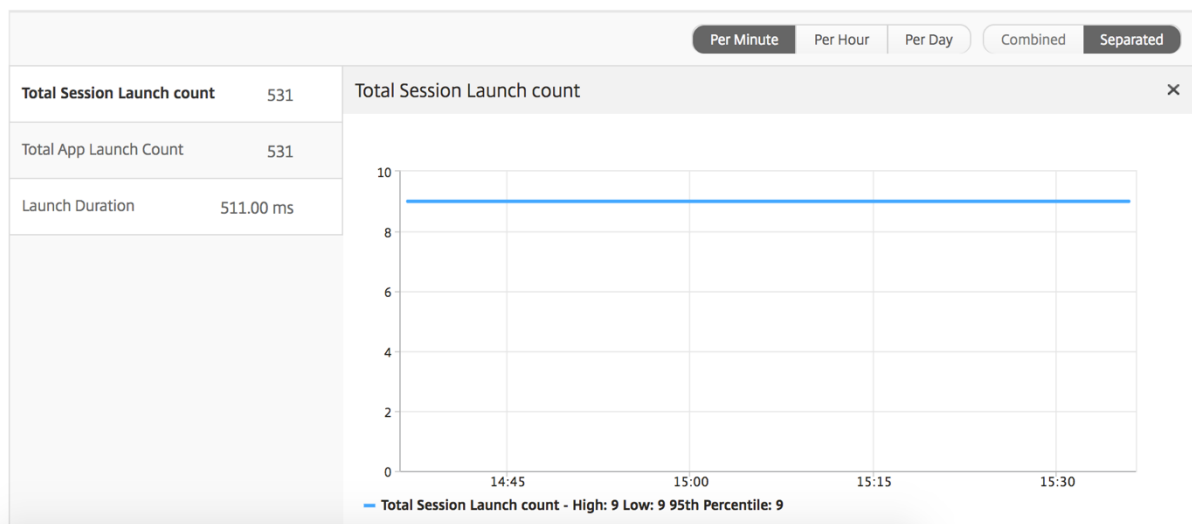
説明

アクティブセッション

この数字は、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った平均時間。



現在のセッションレポート

メトリックス	説明
セッション ID	ICA セッションの一意の ID。
セッションの種類	アプリケーション/デスクトップ。
状態	緑はアクティブなセッション、赤は非アクティブなセッション。
ホストの遅延	サーバーネットワークが原因で NetScaler ADC 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	特定の期間にセッションで使用された帯域幅です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
インターバルあたりのバイト数	特定の期間にセッションで使用されたバイト数。
開始時刻	セッションの開始時間。
アップタイム	セッションの実行時間
クライアント IP アドレス	エンドユーザーの IP。
サーバー IP アドレス	バックエンド/Citrix Virtual Apps サーバー IP。
NetScaler IP Address	NetScaler の管理 IP (NSIP)。
クライアントの種類	受信者の種類-Citrix Windows クライアントなど
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値 ([Yes] または [No])。セッションがマルチストリーム ICA かどうかを表します。
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。たとえば、NetScaler Gateway のユーザー/透過モードなどです。
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。

メトリックス	説明
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。
ICA 往復時間	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それぞれ操作しているときにユーザーが経験する画面遅延です。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
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、TCP ウィンドウのサイズがゼロであることをクライアントがアドバタイズした回数を表します。
Client side fast RTO	NetScaler ADC 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、TCP ウィンドウサイズがゼロであることをサーバーがアドバタイズした回数を表します。
Server side fast RTO	NetScaler ADC 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 にアクセスするユーザーのユーザー名。
セッション ID	Citrix Virtual Apps セッションの一意の識別子。
セッションの種類	「Application」になります。
状態	セッション状態: 緑はアクティブ、赤は非アクティブ。

メトリックス	説明
違反の最大遅延	定義済みしきい値の違反が一定期間に発生した場合の、L7 遅延の最大値。
平均侵害待ち時間	システムが「L7 遅延時間を超過」した状態のときの、L7 遅延の平均値。
L7 しきい値違反数	L7 のしきい値違反が発生した回数。
L7 Client-side Latency	ICA クライアントと NetScaler ADC インスタンスの間で観測された平均 L7 遅延時間。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。
L7 Server-side Latency	NetScaler ADC デバイスと Citrix Virtual Apps の間で観察された平均 L7 遅延。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。

Current Sessions									
Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
	0000...000001	Application	1.012 s	2.00 ms	2017-6-12 15:39:58	0 h: 0 m: 59s	23.18.6.21	10.102.19.122	10.102.216.177
	0000...000001	Application	880 ms	1.00 ms	2017-6-12 15:39:58	0 h: 0 m: 59s	1.2.16.12	10.102.60.50	10.102.216.219

### アプリケーションごとのセッション・ビュー

Per Application Session ビューには、選択した特定の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。

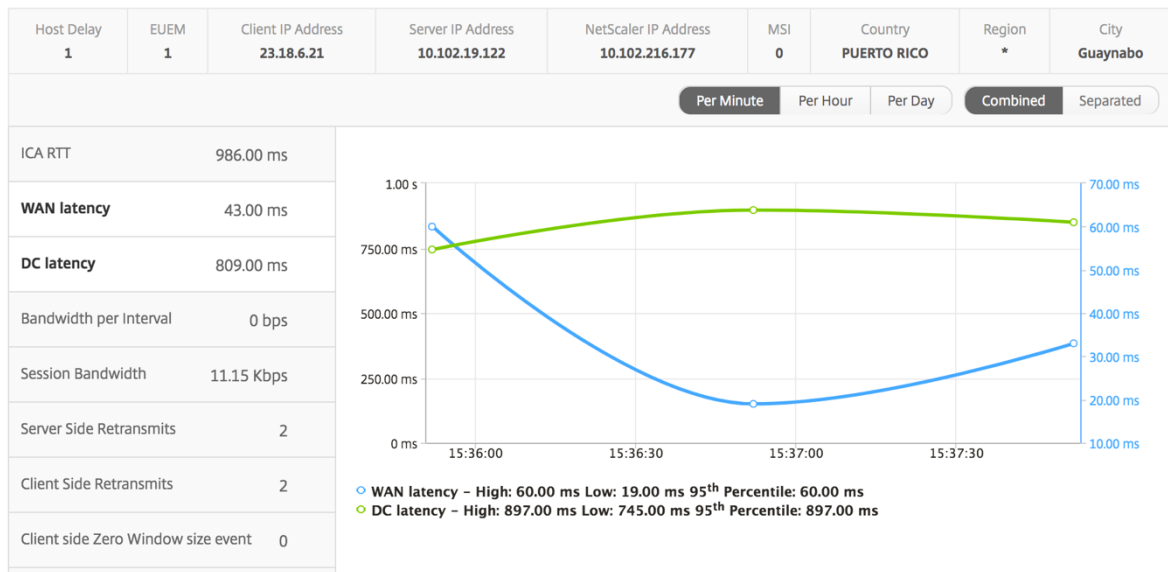
セッション・レポートを表示するには、次の手順に従います。

1. サポートされている Web ブラウザを使用して、NetScaler ADM にログインします。
2. 「Analytics」 > 「HDX Insight」 > 「アプリケーション」の順に選択します。
3. Application Summary レポートから特定のユーザーを選択します。
4. Current Sessions レポートからセッションを選択します。

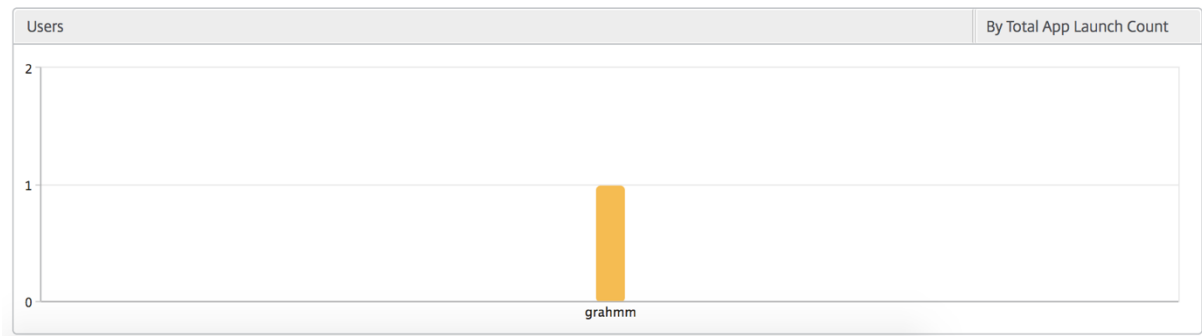
### 折れ線グラフ

メトリック	説明
セッション再接続	セッションが再接続された回数。

メトリック	説明
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
サーバー側のゼロ ウィンドウ サイズ イベント	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。
間隔あたりの帯域幅	特定の期間にセッションで使用された帯域幅です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
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、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。
Client side fast RTO	NetScaler ADC 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。
Server side fast RTO	NetScaler ADC 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、TCP ウィンドウのサイズがゼロであることをクライアントがアダプタイズした回数を表します。



ユーザー棒グラフ ユーザーの棒グラフは、この特定のアプリにログインしたユーザー数を表します。



### デスクトップビューのレポートおよびメトリクス

このビューのレポートとメトリックは、Citrix Virtual Desktops に焦点を当てています。

デスクトップ・ビューに移動するには:

1. サポートされている Web ブラウザを使用して、NetScaler ADM にログインします。
2. [アナリティクス]>[ **HDX Insight** ]>[ デスクトップ ]に移動します。

### [Summary] ビュー

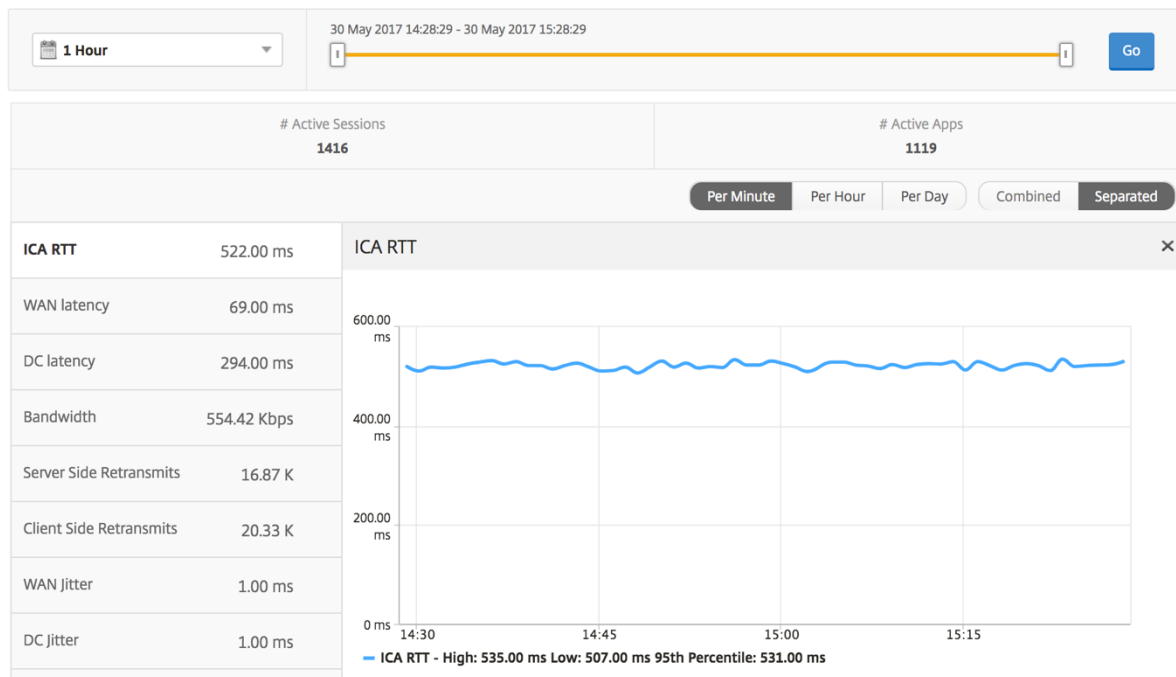
概要ビューには、選択したタイムライン中にログインしたすべての Citrix Virtual Desktops のレポートが表示されます。

明示的に言及しない限り、すべての指標/レポートには、選択した期間に対応する値が含まれます。

折れ線グラフ

メトリック	説明
アクティブセッション	この数字は、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ケーション数	この数字は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	NetScaler ADC 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。
Server side fast RTO	NetScaler ADC 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、TCP ウィンドウのサイズがゼロであることをクライアントがアダプタイズした回数を表します。
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、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。





デスクトップの概要レポート

メトリックス	説明
アクティブなセッション	特定の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。
Active Desktops	特定の時間間隔におけるアクティブな Citrix Virtual Desktops 合計数。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。

Desktop Users							Search ▾	🔍
User Name	# Active Desktops	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes		
liam	60	1.00 s	56.00 ms	746.00 ms	9.27 Kbps	251.24 MB		
jayden	60	1.00 s	52.00 ms	746.00 ms	9.27 Kbps	251.34 MB		
juan	60	169.00 ms	32.00 ms	30.00 ms	9.26 Kbps	250.99 MB		
daniel	60	149.00 ms	31.00 ms	30.00 ms	9.26 Kbps	251.02 MB		
randyb	60	99.00 ms	11.00 ms	30.00 ms	9.26 Kbps	250.97 MB		

しきい値レポート しきい値レポートは、選択した期間内に エンティティ が Desktop として選択された場合に、違反したしきい値の数を表します。詳細については、「しきい値の作成方法」を参照してください。

### デスクトップごとのビュー

デスクトップごとの表示では、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が表示されます。

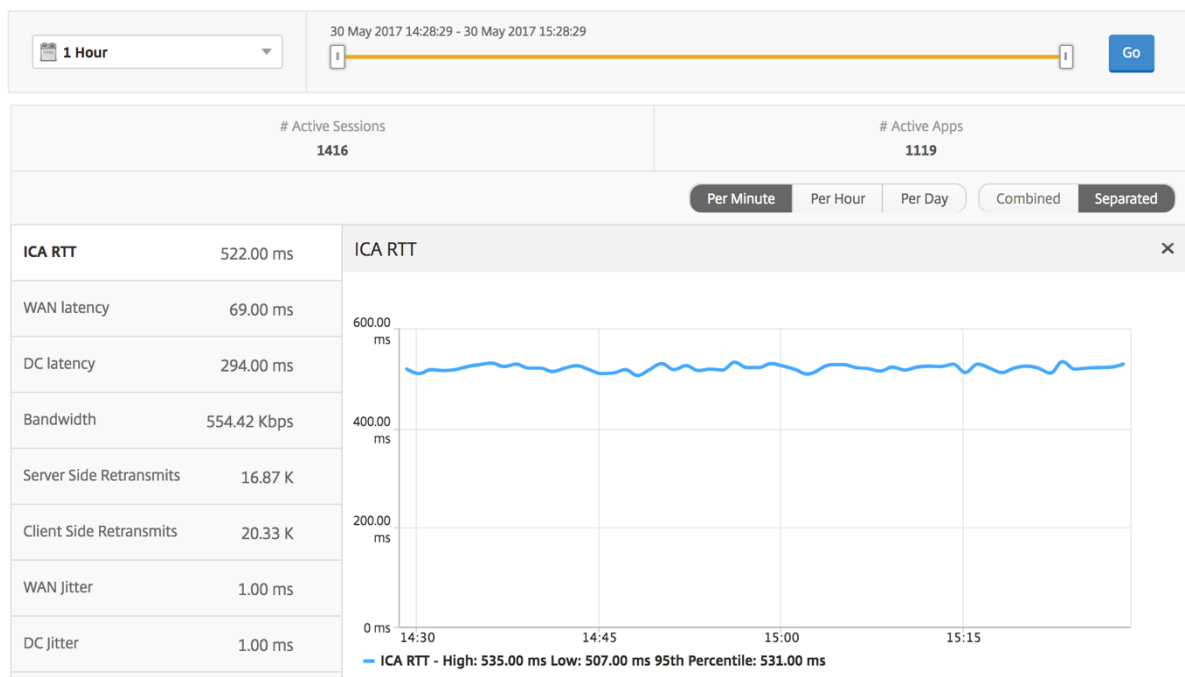
特定のデスクトップビューに移動するには:

1. サポートされている Web ブラウザを使用して、Citrix ADM にログオンします。
2. [分析] > [HDX Insight] > [デスクトップ] に移動します。
3. デスクトップの概要レポートから特定のデスクトップを選択します。

### 折れ線グラフ

メトリック	説明
アクティブセッション	この数字は、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ケーション数	この数字は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。

メトリック	説明
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	NetScaler ADC 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。
Server side fast RTO	NetScaler ADC 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、TCP ウィンドウのサイズがゼロであることをクライアントがアダプタイズした回数を表します。
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、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。



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示しています。以下のメトリクスは [Desktop Launch Count] および [Bandwidth] を基準にしてソートできます。

メトリックス	説明
名前	Citrix Virtual Desktops 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です。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。

Desktop Users						By Desktop Launch Count ▾
Name	Desktop Launch Count ↑	Bandwidth	DC latency	WAN latency	ICA RTT	
XenDesktop33	177	9.38 Kbps	749.00 ms	57.00 ms	1.00 s	

ユーザーデスクトップアクティブ/非アクティブレポート 以下のメトリックスは、[Bandwidth per Interval]、[Session Reconnects]、および [ACR Counts] を基準にしてソートできます。

メトリックス	説明
セッション ID	ICA セッションの一意の ID。
セッションの種類	アプリケーション/デスクトップ。
状態	緑はアクティブなセッション、赤は非アクティブなセッション。
ホストの遅延	サーバーネットワークが原因で NetScaler ADC 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	特定の期間にセッションで使用された帯域幅です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
インターバルあたりのバイト数	特定の期間にセッションで使用されたバイト数。
開始時刻	セッションの開始時間。
アップタイム	セッションの実行時間

メトリックス	説明
クライアント IP アドレス	エンドユーザーの IP。
サーバー IP アドレス	バックエンド/Citrix Virtual Apps サーバー IP。
NetScaler IP Address	NetScaler の管理 IP (NSIP)。
クライアントの種類	受信者の種類-Citrix Windows クライアントなど
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値 ([Yes] または [No])。セッションがマルチストリーム ICA かどうかを表します。
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。たとえば、NetScaler Gateway のユーザー/透過モードなどです。
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。

メトリックス	説明
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
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、TCP ウィンドウのサイズがゼロであることをクライアントがアダプタイズした回数を表します。
Client side fast RTO	NetScaler ADC 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、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。
Server side fast RTO	NetScaler ADC 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 ダイアグラム	ユーザーが接続している Citrix Virtual Desktop の名前

User Desktops Active								By Bandwidth per Interval	
Diagram	Session ID	VDI Image Name	ICA RTT	WAN latency	DC latency	Host Delay	Bandwidth per Interval	Session Bandwidth	Total B
	0000..000001	XenDesktop33	1.094 s	48.00 ms	767 ms	5.00 ms	12.87 Kbps	12.87 Kbps	1.65
	0000..000001	XenDesktop33	1.007 s	37.00 ms	691 ms	4.00 ms	9.27 Kbps	9.27 Kbps	1.35
	0000..000001	XenDesktop33	0.914 s	53.00 ms	747 ms	5.00 ms	9.28 Kbps	9.28 Kbps	1.35

### デスクトップごとのセッションビュー

デスクトップごとのセッションビューでは、選択した特定の Citrix Virtual Desktop セッションのレポートが表示されます。

デスクトップ・セッション・ビューに移動するには:

1. サポートされている Web ブラウザを使用して、Citrix ADM にログオンします。

2. [分析] > [HDX Insight] > [デスクトップ] に移動します。
3. デスクトップ 概要レポートから特定のデスクトップを選択します。
4. 現在のセッションレポートからセッションを選択します。

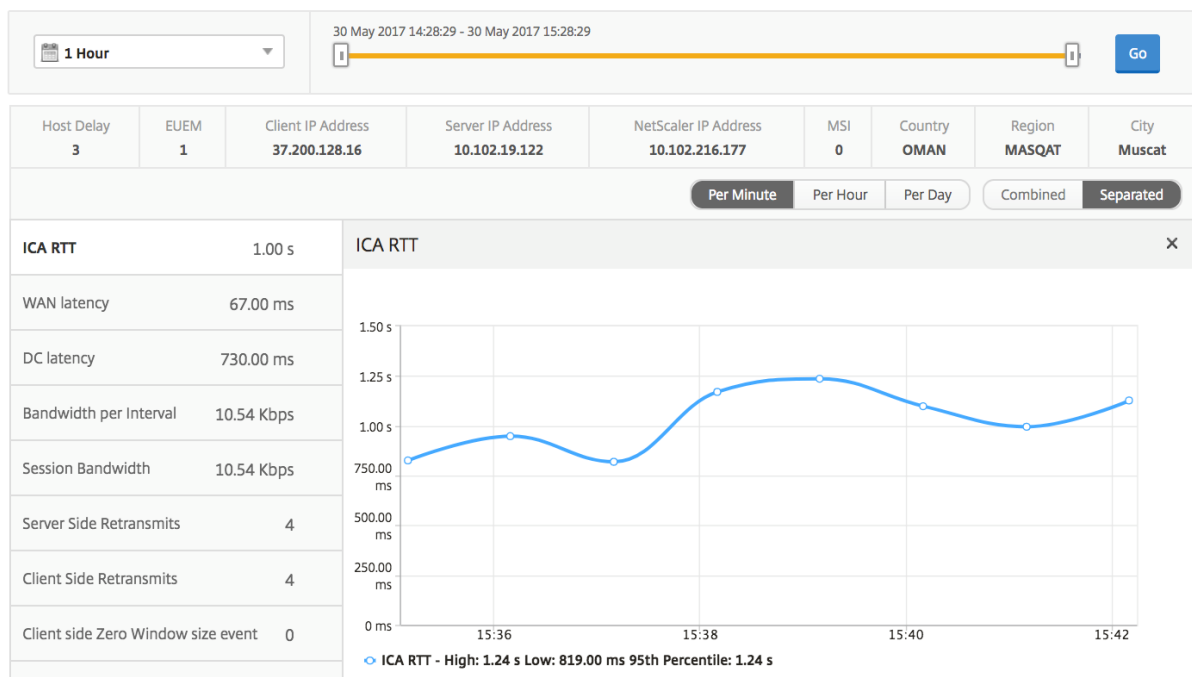
時系列グラフ [Per User Session] ビューには、選択したユーザーのセッションに関するレポートが表示されません。

選択したユーザーのセッションのメトリックを表示する手順は、次のとおりです。

1. サポートされている Web ブラウザを使用して、NetScaler ADM にログインします。
2. [Analytics] > [HDX Insight] > [ユーザー] に移動します。
3. 「ユーザー 概要レポート」セクションから特定のユーザーを選択します。
4. 「現在のセッション」または「終了したセッション」列からセッションを選択します。

メトリック	説明
セッション再接続	この数字は、アクティブな Citrix Virtual Apps and Desktops セッションの数を示します。
ACR 数	この数字は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	NetScaler ADC 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。

メトリック	説明
Server side fast RTO	NetScaler ADC 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	特定の期間にセッションで使用された帯域幅です。
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、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。
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、TCP ウィンドウのサイズがゼロであることをクライアントがアダプタイズした回数を表します。



関連するデスクトップセッションレポート 以下のメトリクスは、[Bandwidth per Interval]、[Session Reconnects]、および [ACR Counts] を基準にしてソートできます。

メトリックス	説明
セッション ID	ICA セッションの一意の ID。
セッションの種類	アプリケーション/デスクトップ。
状態	緑はアクティブなセッション、赤は非アクティブなセッション。
ホストの遅延	サーバーネットワークが原因で NetScaler ADC を通過する ICA トラフィックの平均遅延。



メトリックス	説明
間隔あたりの帯域幅	特定の期間にセッションで使用された帯域幅です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
インターバルあたりのバイト数	特定の期間にセッションで使用されたバイト数。
開始時刻	セッションの開始時間。
アップタイム	セッションの実行時間
クライアント IP アドレス	エンドユーザーの IP。
サーバー IP アドレス	バックエンド/Citrix Virtual Apps サーバー IP。
NetScaler IP Address	NetScaler の管理 IP (NSIP)。
クライアントの種類	受信者の種類-Citrix Windows クライアントなど
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値 ([Yes] または [No])。セッションがマルチストリーム ICA かどうかを表します。
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。たとえば、NetScaler Gateway のユーザー/透過モードなどです。
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。

メトリックス	説明
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
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、TCP ウィンドウのサイズがゼロであることをクライアントがアダプタイズした回数を表します。
Client side fast RTO	NetScaler ADC 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、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。
Server side fast RTO	NetScaler ADC 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。

User Desktops Active								By Bandwidth per Interval	
Diagram	Session ID	VDI Image Name	ICA RTT	WAN latency	DC latency	Host Delay	Bandwidth per Interval	Session Bandwidth	Total B
	0000...000001	XenDesktop33	1.094 s	48.00 ms	767 ms	5.00 ms	12.87 Kbps	12.87 Kbps	1.65
	0000...000001	XenDesktop33	1.007 s	37.00 ms	691 ms	4.00 ms	9.27 Kbps	9.27 Kbps	1.35
	0000...000001	XenDesktop33	0.94 s	53.00 ms	747 ms	5.00 ms	9.27 Kbps	9.27 Kbps	1.35

### インスタンスビューのレポートとメトリックス

インスタンスビューのレポートとメトリックは、NetScaler ADC インスタンスに焦点を当てています。

[インスタンス] ビューにナビゲートするには、次の手順を実行します。

1. サポートされている Web ブラウザを使用して、NetScaler ADM にログインします。
2. [分析] > [HDX Insight] > [インスタンス] に移動します。

インスタンスビューのレポートとメトリクスは、次のセクションで構成されています。

- インスタンス概要ビュー
- インスタンス別ビュー

### インスタンスの概要ビュー

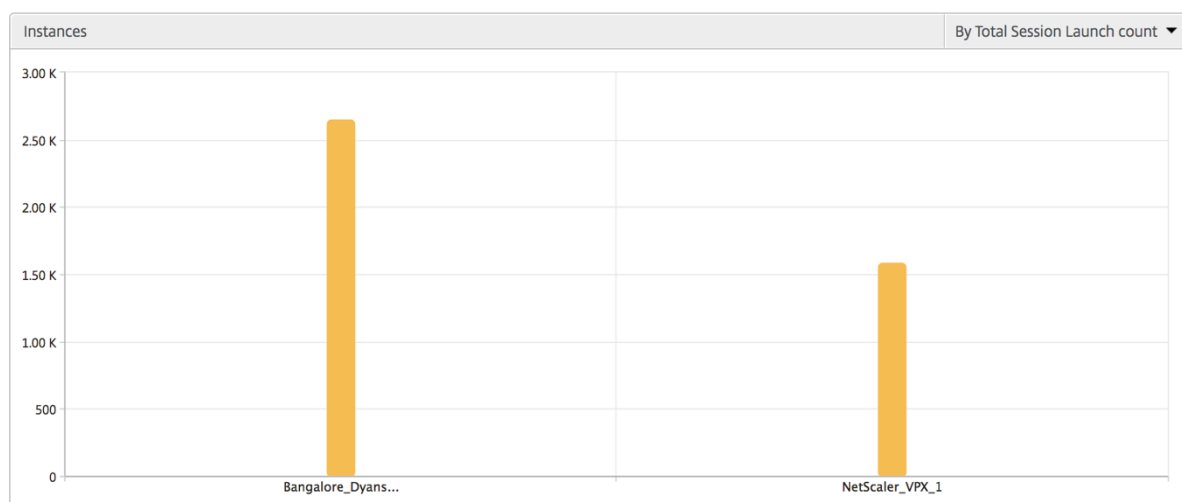
このビューは、Citrix ADNetScaler ADM に追加されたすべての NetScaler ADC インスタンスのレポートを表示するため、概要ビューと呼ばれます。

以下のメトリクスとレポートでは、明確な記載がない限り選択した期間の対応する値が表示されます。

### インスタンス棒グラフ

このグラフには、インスタンスと合計セッション起動回数が表示されます。

グラフキャンバスの右上のリストから選択できるアプリの総数。



### インスタンス/アクティブインスタンスの概要レポート

メトリックス	説明
名前	NetScaler ADC インスタンスのホスト名。
IP アドレス	NetScaler の IP アドレスです。
セッションの起動数合計	特定の期間に作成された一意のユーザーセッションの合計数です。
アプリケーション合計数	特定の期間に起動された一意のアプリケーションの合計数です。
種類	-

Instances				
Name	IP Address	Total Session Launch count ↑	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances					
Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

**しきい値レポート** しきい値レポートは、選択した期間内に エンティティ がインスタンスとして選択された場合に、違反したしきい値の数を表します。詳細については、「[しきい値の作成方法](#)」を参照してください。

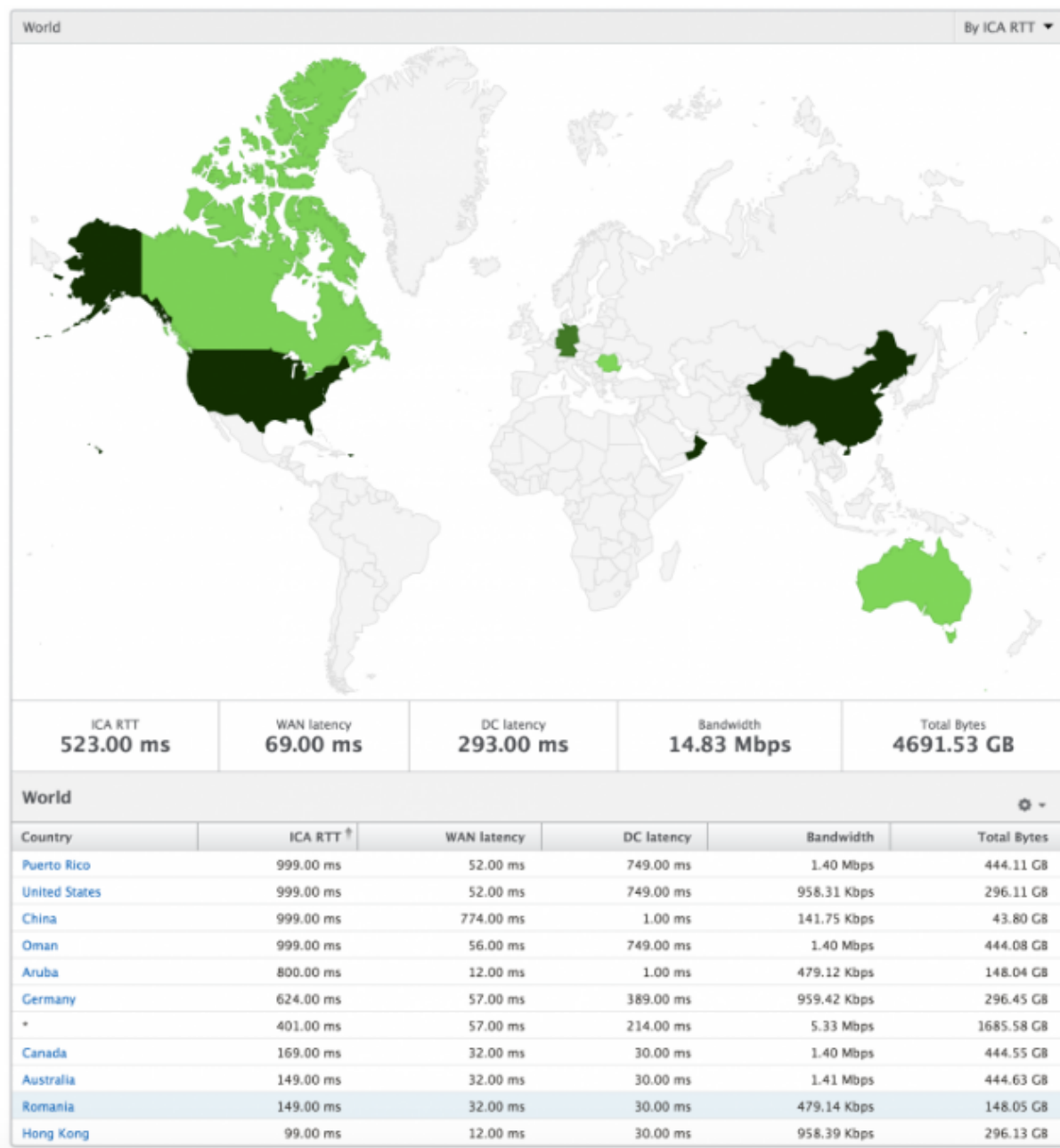
**スキップされたフロー** スキップフローは、ICA 接続の解析が省略されたレコードのことです。これは、サポートされていない Citrix Virtual Apps および Desktop バージョンの使用、サポートされていないバージョンのレシーバーまたはレシーバータイプなど、複数の理由で発生する可能性があります。この表は、IP アドレスとスキップされたフロー数を示しています。これらの受信機は、ホワイトリストに登録された受信機の一部ではない場合があります。したがって、これらのセッションはモニタリングからスキップされます。

Skipped Flows	
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

**世界観** HDX Insight の世界地図ビューでは、管理者が地理的な観点からユーザー履歴およびアクティブユーザーの詳細を確認できます。管理者は、単に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たり、特定の国や都市にドリルダウンすることができます。管理者はさらにドリルダウンして、都市および州別に情報を表示できます。NetScaler ADM バージョン 12.0 以降では、地理的な場所から接続しているユーザーにドリルダウンできます。

HDX Insight のワールドマップでは、以下の詳細を表示できます。また、各指標の密度はヒートマップの形式で表示されます。

- ICA 往復時間
- WAN 遅延
- DC の遅延
- 帯域幅
- バイト数合計



### インスタンスごとのビュー

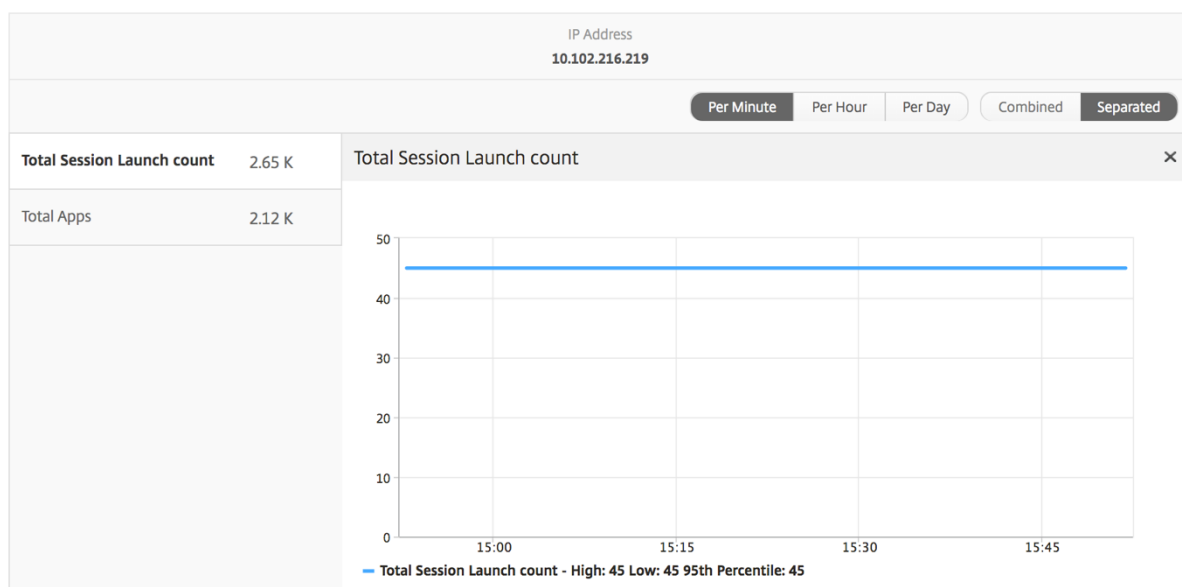
インスタンスごとのビューでは、選択した特定の NetScaler ADC インスタンスに関する詳細なエンドユーザーエクスペリエンスレポートが提供されます。

インスタンス・ビューに移動するには、次の手順に従います。

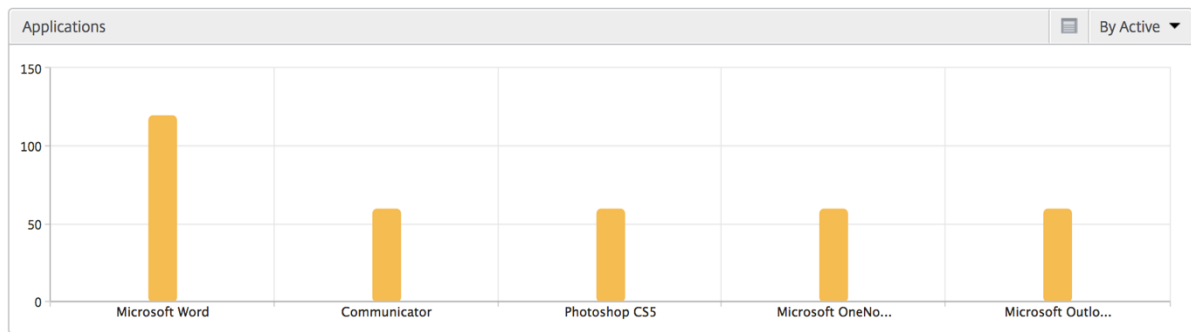
1. サポートされている Web ブラウザを使用して、NetScaler ADM にログインします。
2. [分析] > [HDX Insight] > [インスタンス] に移動します。
3. インスタンス 概要レポートから特定のインスタンスを選択します。

### 折れ線グラフ

メトリック	説明
IP アドレス	選択したインスタンスの NetScaler IP アドレスを表します。
Total session launch count	特定の時間間隔におけるアクティブな Citrix Virtual App セッションの総数。
アプリケーション合計数	特定の期間に起動された一意のアプリケーションの合計数です。

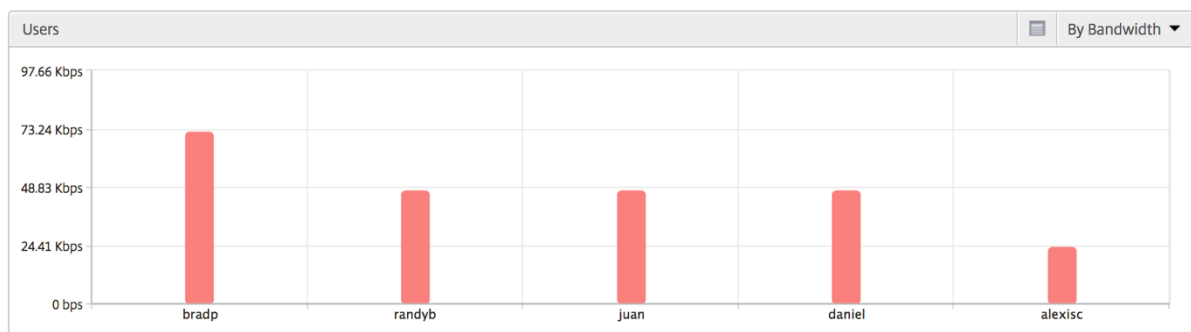


アプリケーション棒グラフ アクティブなアプリ、セッションの合計起動数、アプリの合計起動数、起動時間などの条件に基づいて、上位 5 個のアプリケーションを表示します。



ユーザー棒グラフ ユーザー棒グラフには、以下の基準別に上位 5 人のユーザーが表示されます。

- 帯域幅
- WAN 遅延
- DC の遅延
- ICA 往復時間



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示しています。以下のメトリクスは [Desktop Launch Count] および [Bandwidth] を基準にしてソートできます。

メトリクス	説明
名前	Citrix Virtual Desktops 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です。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。

メトリックス	説明
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。

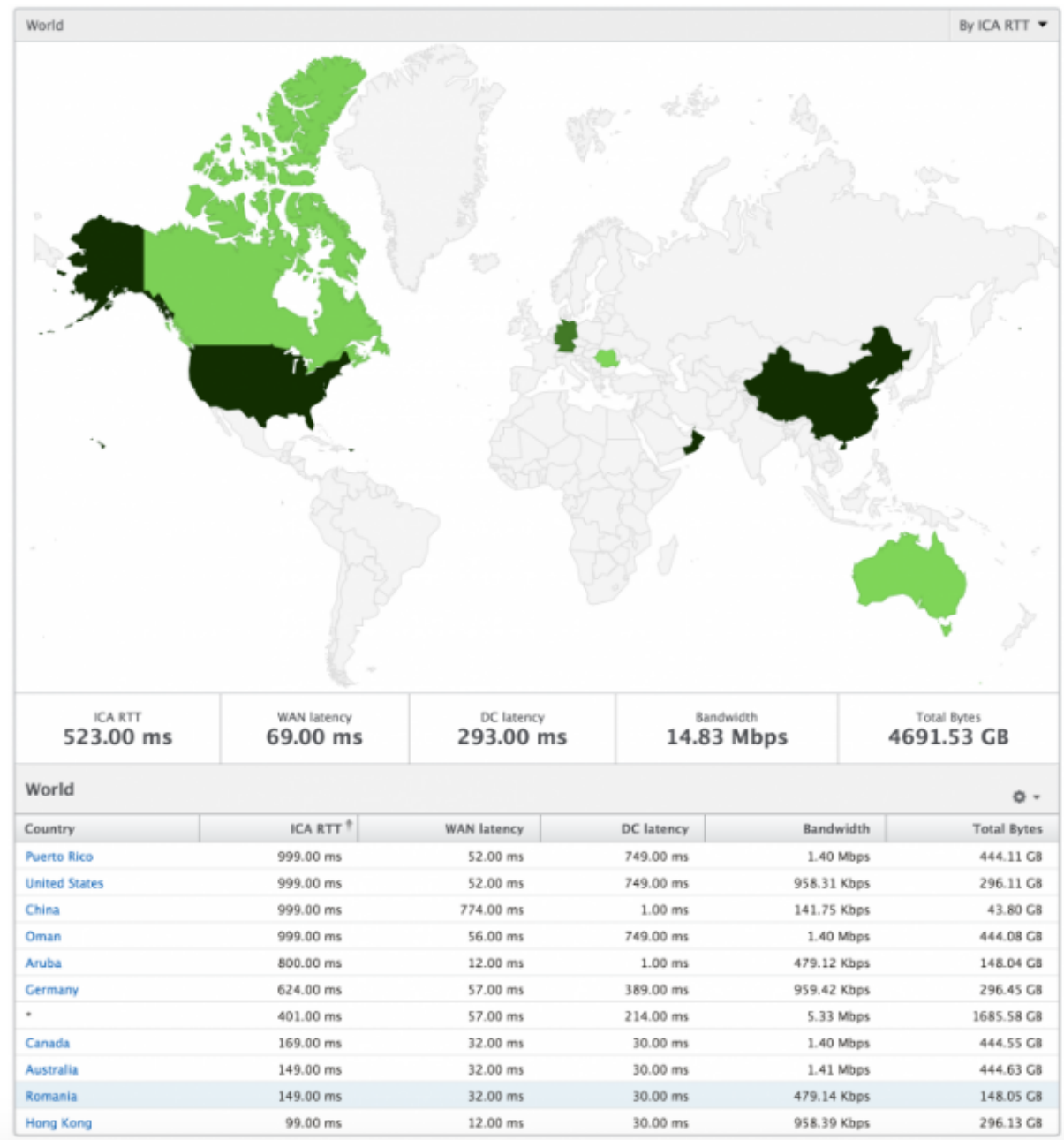
Desktop Users						By Desktop Launch Count ▾
Name	Desktop Launch Count ↕	Bandwidth	DC latency	WAN latency	ICA RTT	
XenDesktop33	177	9.38 Kbps	749.00 ms	57.00 ms	1.00 s	

世界観 HDX Insight の世界地図ビューでは、管理者が地理的な観点からユーザー履歴およびアクティブユーザーの詳細を確認できます。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ビューを表示したり、特定の国や都市にドリルダウンしたりできます。また、さらにドリルダウンして市区町村および都道府県別の情報を確認することもできます。NetScaler ADM バージョン 12.0 以降では、地理的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ます。また、各指標の密度はヒートマップの形式で表示されます。

- ICA 往復時間
- WAN 遅延
- DC の遅延
- 帯域幅
- バイト数合計





### ライセンスビューのレポートとメトリック

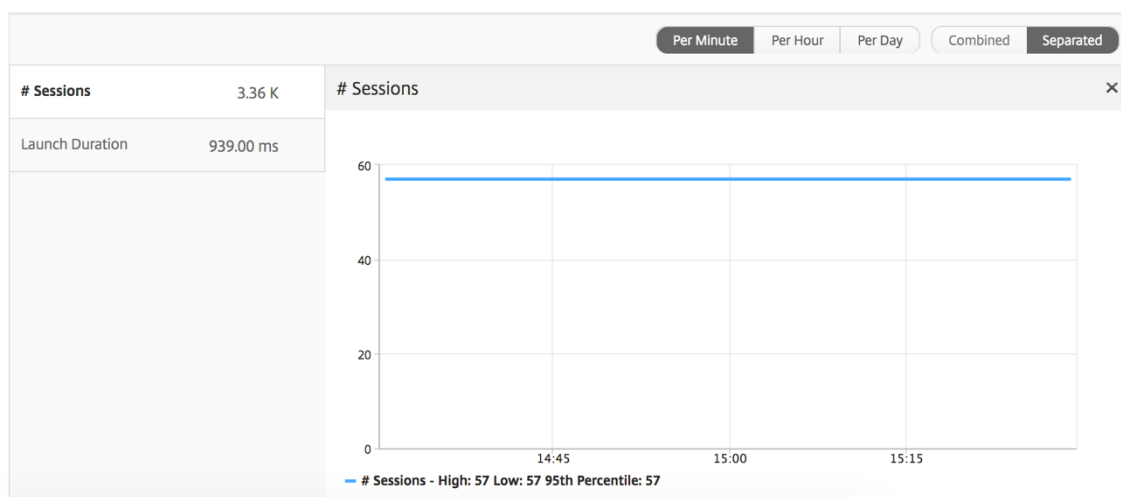
ライセンスビューには、NetScaler Gateway のライセンス情報が表示されます。

[ライセンス] ビューに移動するには、次の手順に従います。

1. サポートされている Web ブラウザを使用して、NetScaler ADM にログオンします。
2. [アナリティクス] > [HDX Insight] > [ライセンス] に移動します。

折れ線グラフ

メトリック	説明
使用中のライセンス	選択した期間中に使用されている NetScaler Gateway CCU ライセンス。各カウントは、ユーザーセッションの数を表します。このカウントには、各ユーザーが起動したアプリケーションセッションおよびデスクトップセッションは含まれません。
総ライセンス数	お客様が利用できる NetScaler Gateway CCU ライセンスの合計数。



しきい値レポート しきい値レポートは、選択した期間内に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、違反したしきい値の数を表します。詳細については、「しきい値の作成方法」を参照してください。

## Application ビューのレポートとメトリック

February 6, 2024

このビューのレポートとメトリックは、Citrix Virtual Apps に焦点を当てています。

アプリケーション・ビューに移動する手順は、次のとおりです。

1. 「Analytics」 > 「HDX Insight」 > 「アプリケーション」の順に選択します。

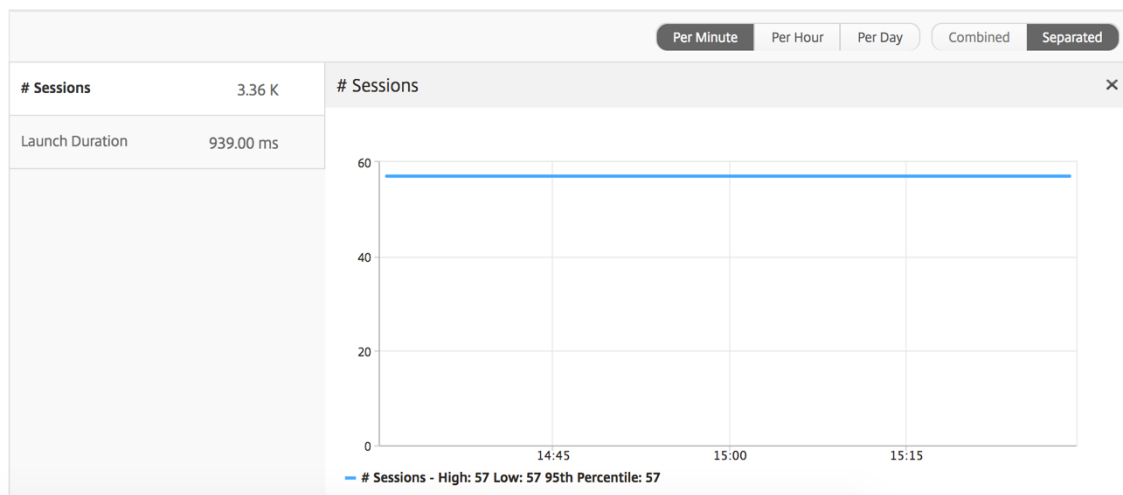
[Summary] ビュー

Summary ビューには、選択した期間中にログインしたすべてのアプリケーションのレポートが表示されます。

以下のメトリクスとレポートでは、明確な記載がない限り選択した期間の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	特定の期間の合計セッション数。
起動時間	アプリケーションの起動にかかった平均時間。



アプリケーション・サマリー・レポート

メトリックス	説明
名前	Citrix Virtual Apps の名前。
セッションの起動数合計	特定の時間間隔におけるアクティブな Citrix Virtual App セッションの総数。
アプリケーションの起動数合計	特定の期間中に起動された Citrix Virtual App アプリケーションの総数。
起動期間	Citrix Virtual App の起動に要した平均時間。

Applications <span style="float: right;">⚙️ ▾</span>			
Name	Total App Launch Count	Launch Duration	Total Session Launch count
Microsoft Outlook	531	514.00 ms	531
Microsoft Visio	354	555.00 ms	354
Microsoft Word	354	557.00 ms	354
Microsoft Excel	354	555.00 ms	354

### アクティブなアプリケーションレポート

メトリックス	説明
名前	Citrix Virtual Apps 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	特定の期間にこのアプリケーションを使用したアクティブなユーザーセッション数。
アクティブなアプリケーション数	このアプリケーションのアクティブなセッション数。

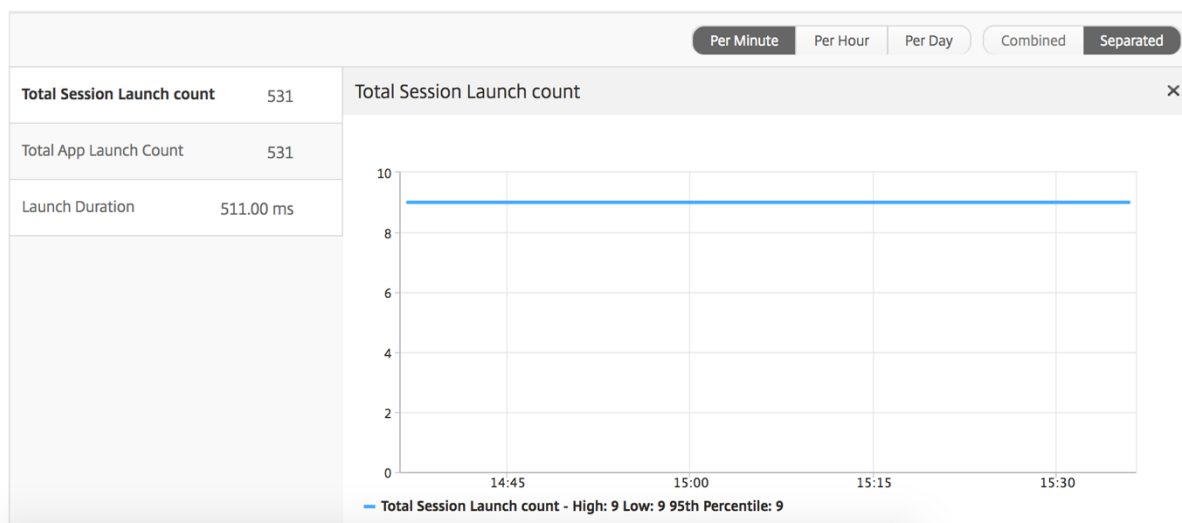
Active Applications			
Name	State	# Active Sessions	# Active Apps
Communicator	●	60	60
Fidelity	●	60	60
GoToMeeting	●	60	60
...	..	--	--

### しきい値レポート

しきい値レポートは、選択した期間内に エンティティ が「アプリケーション」として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。

### 折れ線グラフ

メトリック	説明
アクティブセッション	この数字は、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った平均時間。



現在のセッションレポート

メトリックス	説明
セッション ID	ICA セッションの一意の ID。
セッションの種類	アプリケーション/デスクトップ。
状態	緑はアクティブなセッション、赤は非アクティブなセッション。
ホストの遅延	サーバーネットワークが原因で NetScaler ADC 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	特定の期間にセッションで使用された帯域幅です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
インターバルあたりのバイト数	特定の期間にセッションで使用されたバイト数。
開始時刻	セッションの開始時間。
アップタイム	セッションの実行時間
クライアント IP アドレス	エンドユーザーの IP。
サーバー IP アドレス	バックエンド/Citrix Virtual Apps サーバー IP。
NetScaler IP Address	NetScaler の管理 IP (NSIP)。
クライアントの種類	受信者の種類-Citrix Windows クライアントなど
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値 ([Yes] または [No])。セッションがマルチストリーム ICA かどうかを表します。

メトリックス	説明
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。たとえば、NetScaler Gateway のユーザー/透過モードなどです。
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。

メトリックス	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、TCP ウィンドウのサイズがゼロであることをクライアントがアダプタイズした回数を表します。
Client side fast RTO	NetScaler ADC 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、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。
Server side fast RTO	NetScaler ADC 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 にアクセスするユーザーのユーザー名。
セッション ID	Citrix Virtual Apps セッションの一意の識別子。
セッションの種類	「Application」になります。
状態	セッション状態: 緑はアクティブ、赤は非アクティブ。
違反の最大遅延	定義済みしきい値の違反が一定期間に発生した場合の、L7 遅延の最大値。
平均侵害待ち時間	システムが「L7 遅延時間を超過」した状態のときの、L7 遅延の平均値。
L7 しきい値違反数	L7 のしきい値違反が発生した回数。
L7 Client-side Latency	ICA クライアントと NetScaler ADC インスタンスの間で観測された平均 L7 遅延時間。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。
L7 Server-side Latency	NetScaler ADC デバイスと Citrix Virtual Apps の間で観察された平均 L7 遅延。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。

Current Sessions									
Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
	0000...000001	Application	1.012 s	2.00 ms	2017-6-12 15:39:58	0 h: 0 m: 59s	23.18.6.21	10.102.19.122	10.102.216.177
	0000...000001	Application	880 ms	1.00 ms	2017-6-12 15:39:58	0 h: 0 m: 59s	1.2.16.12	10.102.60.50	10.102.216.219

### アプリケーションごとのセッション・ビュー

Per Application Session ビューには、選択した特定の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、次の手順に従います。

1. 「**Analytics**」 > 「**HDX Insight**」 > 「アプリケーション」の順に選択します。
2. Application Summary レポートから特定のユーザーを選択します。
3. Current Sessions レポートからセッションを選択します。

#### 折れ線グラフ

メトリック	説明
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
サーバー側のゼロ ウィンドウ サイズ イベント	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。
間隔あたりの帯域幅	特定の期間にセッションで使用された帯域幅です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
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、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。
Client side fast RTO	NetScaler ADC 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。
Server side fast RTO	NetScaler ADC 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。

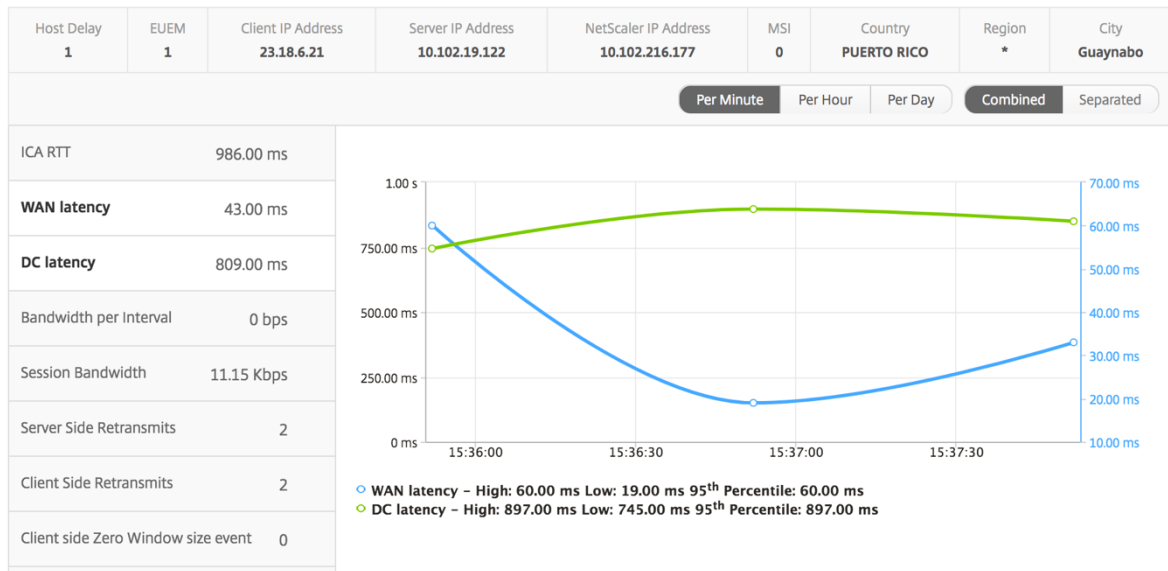


メトリック

説明

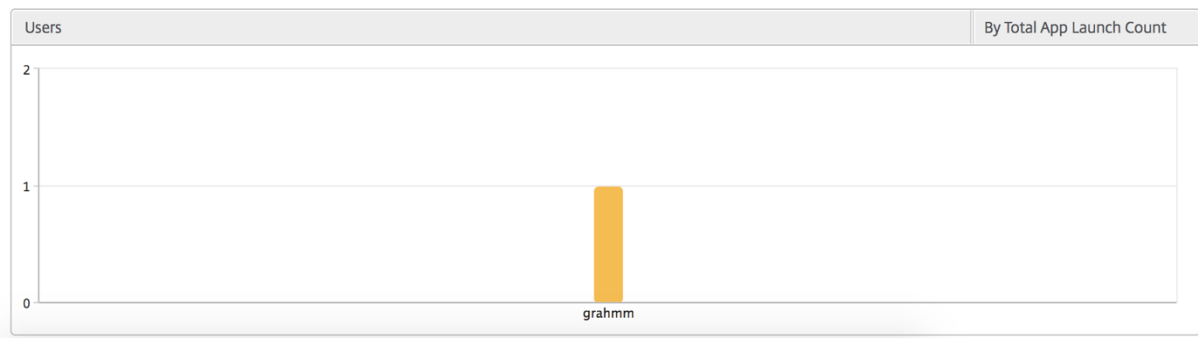
クライアント側のゼロウィンドウサイズ イベント

このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがアダバタイズした回数を表します。



ユーザー棒グラフ

ユーザーの棒グラフは、この特定のアプリにログインしたユーザー数を表します。



デスクトップビューのレポートおよびメトリクス

February 6, 2024

このビューのレポートとメトリックは、Citrix Virtual Desktops に焦点を当てています。

デスクトップ・ビューに移動するには:

1. [アナリティクス] > [ **HDX Insight** ] > [デスクトップ] に移動します。

## [Summary] ビュー

概要ビューには、選択したタイムライン中にログインしたすべての Citrix Virtual Desktops のレポートが表示されます。

明示的に言及しない限り、すべての指標/レポートには、選択した期間に対応する値が含まれます。

### 折れ線グラフ

メトリック	説明
アクティブセッション	この数字は、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ケーション数	この数字は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	NetScaler ADC 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。
Server side fast RTO	NetScaler ADC 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。

メトリック	説明
クライアント側のゼロ ウィンドウ サイズ イベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがアダプタイズした回数を表します。
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、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。



デスクトップの概要レポート

メトリックス	説明
アクティブなセッション	特定の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。
Active Desktops	特定の時間間隔におけるアクティブな Citrix Virtual Desktops 合計数。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。

メトリックス	説明
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。

User Name	# Active Desktops	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
liam	60	1.00 s	56.00 ms	746.00 ms	9.27 Kbps	251.24 MB
jayden	60	1.00 s	52.00 ms	746.00 ms	9.27 Kbps	251.34 MB
juan	60	169.00 ms	32.00 ms	30.00 ms	9.26 Kbps	250.99 MB
daniel	60	149.00 ms	31.00 ms	30.00 ms	9.26 Kbps	251.02 MB
randyb	60	99.00 ms	11.00 ms	30.00 ms	9.26 Kbps	250.97 MB

### しきい値レポート

しきい値レポートは、選択した期間内に エンティティ が Desktop として選択された場合に、違反したしきい値の数を表します。詳細については、「[しきい値とアラートの作成方法](#)」を参照してください。

### デスクトップごとのビュー

デスクトップごとの表示では、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が表示されます。

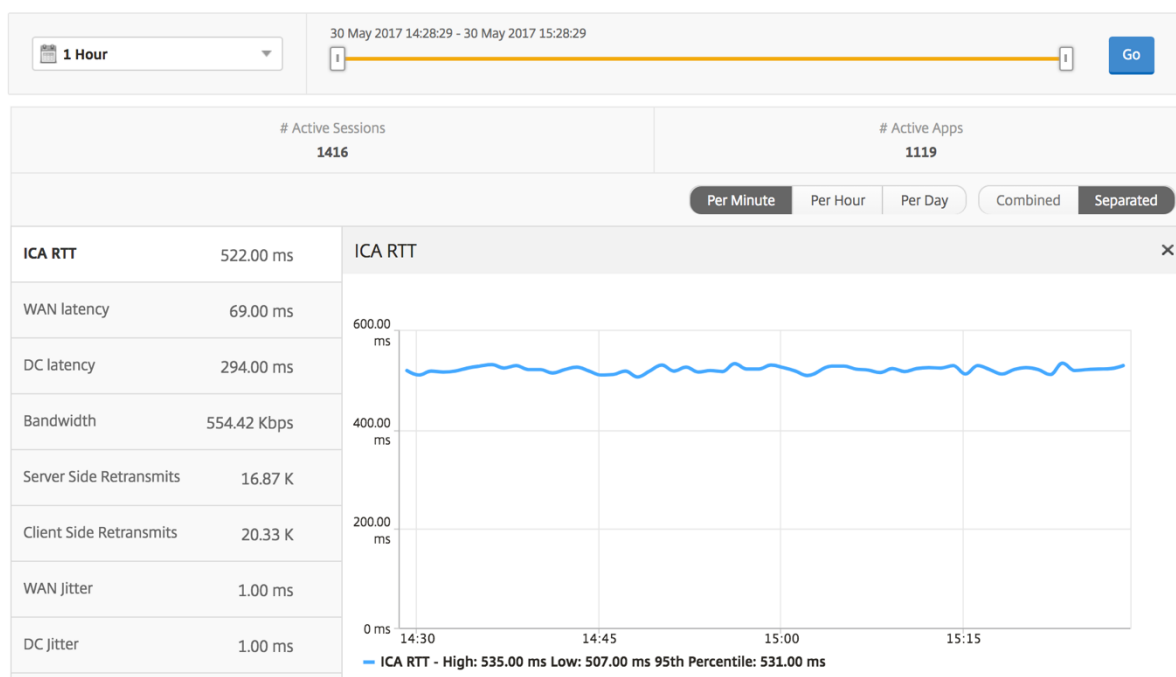
特定のデスクトップビューに移動するには:

1. [分析] > [HDX Insight] > [デスクトップ] に移動します。
2. デスクトップの概要レポートから特定のデスクトップを選択します。

### 折れ線グラフ

メトリック	説明
アクティブセッション	この数字は、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ケーション数	この数字は、アクティブな Citrix Virtual App セッションの数を示します。

メトリック	説明
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	NetScaler ADC 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。
Server side fast RTO	NetScaler ADC 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、TCP ウィンドウのサイズがゼロであることをクライアントがアダバタイズした回数を表します。
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、TCP ウィンドウサイズがゼロであることをサーバーがアダバタイズした回数を表します。



### 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示しています。以下のメトリクスは [Desktop Launch Count] および [Bandwidth] を基準にしてソートできます。

メトリクス	説明
名前	Citrix Virtual Desktops 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です。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。

Desktop Users					By Desktop Launch Count ▾
Name	Desktop Launch Count ↑	Bandwidth	DC latency	WAN latency	ICA RTT
XenDesktop33	177	9.38 Kbps	749.00 ms	57.00 ms	1.00 s

ユーザーデスクトップのアクティブ/非アクティブレポート

以下のメトリクスは、[Bandwidth per Interval]、[Session Reconnects]、および [ACR Counts] を基準にしてソートできます。

メトリクス	説明
セッション ID	ICA セッションの一意の ID。
セッションの種類	アプリケーション/デスクトップ。
状態	緑はアクティブなセッション、赤は非アクティブなセッション。
ホストの遅延	サーバーネットワークによる NetScaler ADC 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	特定の期間にセッションで使用された帯域幅です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
インターバルあたりのバイト数	特定の期間にセッションで使用されたバイト数。
開始時刻	セッションの開始時間。
アップタイム	セッションの実行時間
クライアント IP アドレス	エンドユーザーの IP。
サーバー IP アドレス	バックエンド/Citrix Virtual Apps サーバー IP。
NetScaler IP Address	NetScaler の管理 IP (NSIP)。
クライアントの種類	受信者の種類-Citrix Windows クライアントなど
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値 ([Yes] または [No])。セッションがマルチストリーム ICA かどうかを表します。
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。たとえば、NetScaler Gateway のユーザー/透過モードなどです。

メトリックス	説明
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。
ICA 往復時間	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それぞれ操作しているときにユーザーが経験する画面遅延です。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
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、TCP ウィンドウのサイズがゼロであることをクライアントがアドバタイズした回数を表します。
Client side fast RTO	NetScaler ADC 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。



メトリックス	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、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。
Server side fast RTO	NetScaler ADC 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
ダイアグラム	

User Desktops Active								By Bandwidth per Interval	
Diagram	Session ID	VDI Image Name	ICA RTT	WAN latency	DC latency	Host Delay	Bandwidth per Interval	Session Bandwidth	Total B
	0000..000001	XenDesktop33	1.094 s	48.00 ms	767 ms	5.00 ms	12.87 Kbps	12.87 Kbps	1.65
	0000..000001	XenDesktop33	1.007 s	37.00 ms	691 ms	4.00 ms	9.27 Kbps	9.27 Kbps	1.35
	0000..000001	XenDesktop33	0.94 ms	53.00 ms	747 ms	5.00 ms	0.70 Kbps	0.70 Kbps	1.25

### デスクトップごとのセッションビュー

デスクトップごとのセッションビューでは、選択した特定の Citrix Virtual Desktop セッションのレポートが表示されます。

デスクトップ・セッション・ビューに移動するには:

1. [アナリティクス] > [HDX Insight] > [デスクトップ] に移動します。
2. デスクトップ 概要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。

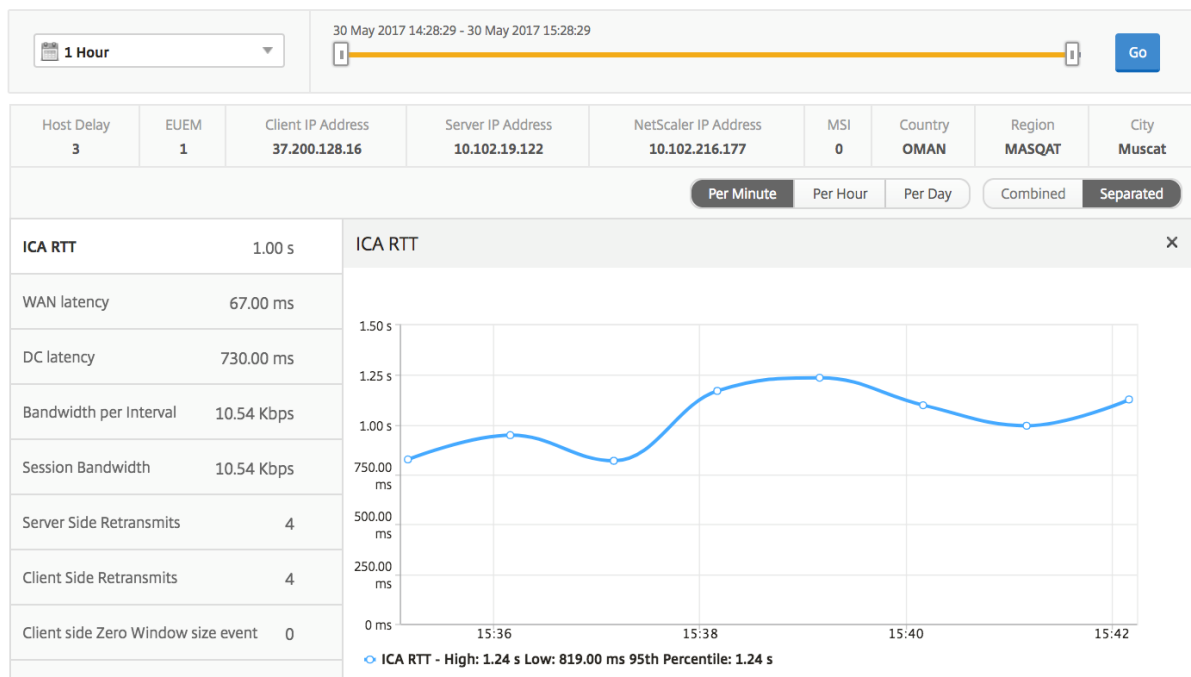
### 時系列グラフ

[Per User Session] ビューには、選択したユーザーのセッションに関するレポートが表示されます。

選択したユーザーのセッションのメトリックを表示する手順は、次のとおりです。

1. [Analytics] > [HDX Insight] > [ユーザー] に移動します。
2. 「ユーザー 概要レポート」セクションから特定のユーザーを選択します。
3. 「現在のセッション」または「終了したセッション」列からセッションを選択します。

メトリック	説明
セッション再接続	この数字は、アクティブな Citrix Virtual App and Desktop セッションの数を示します。
ACR 数	この数字は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual App と Desktop でそれぞれホストされているアプリケーションまたはデスクトップを操作しているときにユーザーが経験するスクリーンラグです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	NetScaler ADC 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。
Server side fast RTO	NetScaler ADC 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	特定の期間にセッションで使用された帯域幅です。
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、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。
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、TCP ウィンドウのサイズがゼロであることをクライアントがアダプタイズした回数を表します。



関連するデスクトップセッションレポート

以下のメトリクスは、[Bandwidth per Interval]、[Session Reconnects]、および [ACR Counts] を基準にしてソートできます。

メトリクス	説明
セッション ID	ICA セッションの一意の ID。
セッションの種類	アプリケーション/デスクトップ。
状態	緑はアクティブなセッション、赤は非アクティブなセッション。
ホストの遅延	サーバーネットワークが原因で NetScaler ADC 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	特定の期間にセッションで使用された帯域幅です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
インターバルあたりのバイト数	特定の期間にセッションで使用されたバイト数。
開始時刻	セッションの開始時間。
アップタイム	セッションの実行時間
クライアント IP アドレス	エンドユーザーの IP。
サーバー IP アドレス	バックエンド/Citrix Virtual Apps サーバー IP。

メトリックス	説明
NetScaler IP Address	NetScaler の管理 IP (NSIP)。
クライアントの種類	受信者の種類-Citrix Windows クライアントなど
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値 ([Yes] または [No])。セッションがマルチストリーム ICA かどうかを表します。
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。たとえば、NetScaler ADC Gateway ユーザー/トランスペアレントモードなどです。
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。
ICA 往復時間	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、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。

メトリックス	説明
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
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、TCP ウィンドウのサイズがゼロであることをクライアントがアダプタイズした回数を表します。
Client side fast RTO	NetScaler ADC 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、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。
Server side fast RTO	NetScaler ADC 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

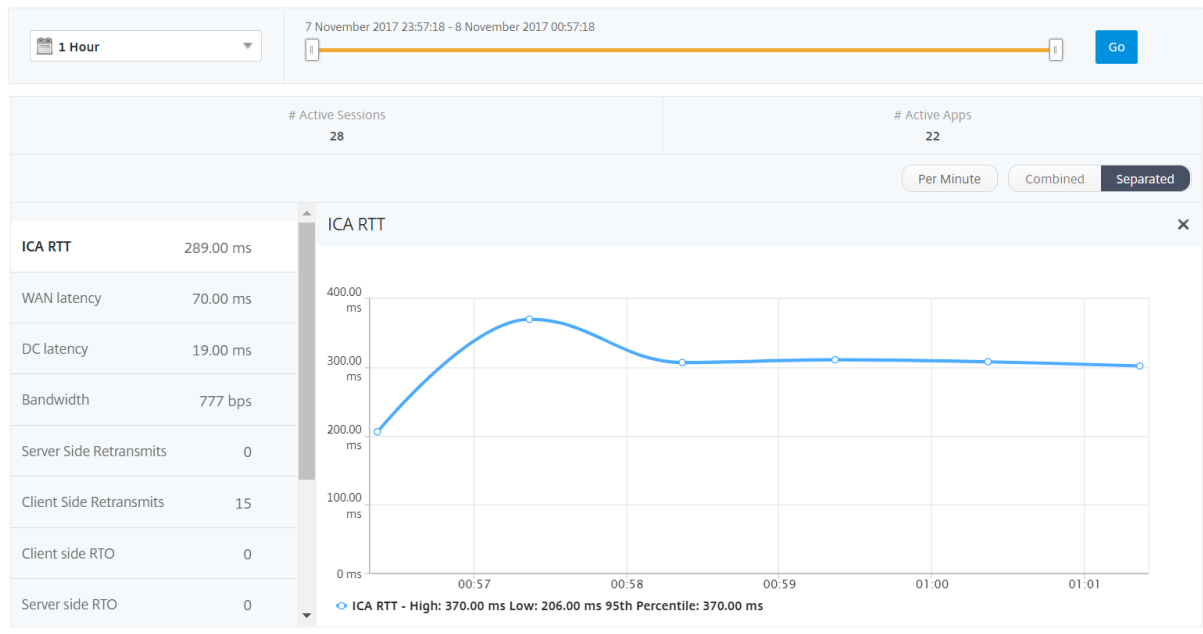
User Desktops Active								By Bandwidth per Interval	
Diagram	Session ID	VDI Image Name	ICA RTT	WAN latency	DC latency	Host Delay	Bandwidth per Interval	Session Bandwidth	Total B
	0000..0000001	XenDesktop33	<a href="#">1.094 s</a>	48.00 ms	767 ms	5.00 ms	12.87 Kbps	12.87 Kbps	1.63
	0000..0000001	XenDesktop33	<a href="#">1.007 s</a>	37.00 ms	691 ms	4.00 ms	9.27 Kbps	9.27 Kbps	1.35
	0000..0000001	XenDesktop33	<a href="#">0.94 s</a>	53.00 ms	747 ms	5.00 ms	8.38 Kbps	8.38 Kbps	1.25

## ユーザービューのレポートとメトリック

February 6, 2024

このビューのレポートとメトリックは、Citrix Virtual Apps and Desktops ユーザーごとに表示されます。

[ **Analytics** ] > [ **HDX Insight** ] > [ ユーザー ] に移動します。



**[Summary] ビュー**

[Summary] ビューには、選択した期間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指標/レポートには、特に指定がない限り、選択した期間の対応する値が表示されます。

選択した期間を変更するには、次の手順に従います。

1. 期間リストまたはタイムスライダを使用して、目的の時間間隔を設定します。
2. **[Go]** をクリックします。

折れ線グラフ

メトリック	説明
アクティブセッション	この数字は、アクティブな Citrix Virtual App and Desktop セッションの数を示します。
アクティブなアプリケーション数	この数字は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	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、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。

メトリック	説明
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	NetScaler ADC 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。
Server side fast RTO	NetScaler ADC 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、TCP ウィンドウのサイズがゼロであることをクライアントがアダバタイズした回数を表します。
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、TCP ウィンドウサイズがゼロであることをサーバーがアダバタイズした回数を表します。



## ユーザー概要レポート

このレポートに固有のメトリックは以下のとおりです。

メトリックス	説明
アクティブセッション	この数字は、アクティブな Citrix Virtual App and Desktop セッションの数を示します。
アクティブなアプリケーション数	この数字は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	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、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	NetScaler ADC 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。
Server side fast RTO	NetScaler ADC 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、TCP ウィンドウのサイズがゼロであることをクライアントがアダバタイズした回数を表します。
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、TCP ウィンドウサイズがゼロであることをサーバーがアダバタイズした回数を表します。
アプリケーションの起動数合計	指定した期間にユーザーによって起動された合計アプリ数です。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。



メトリックス

説明

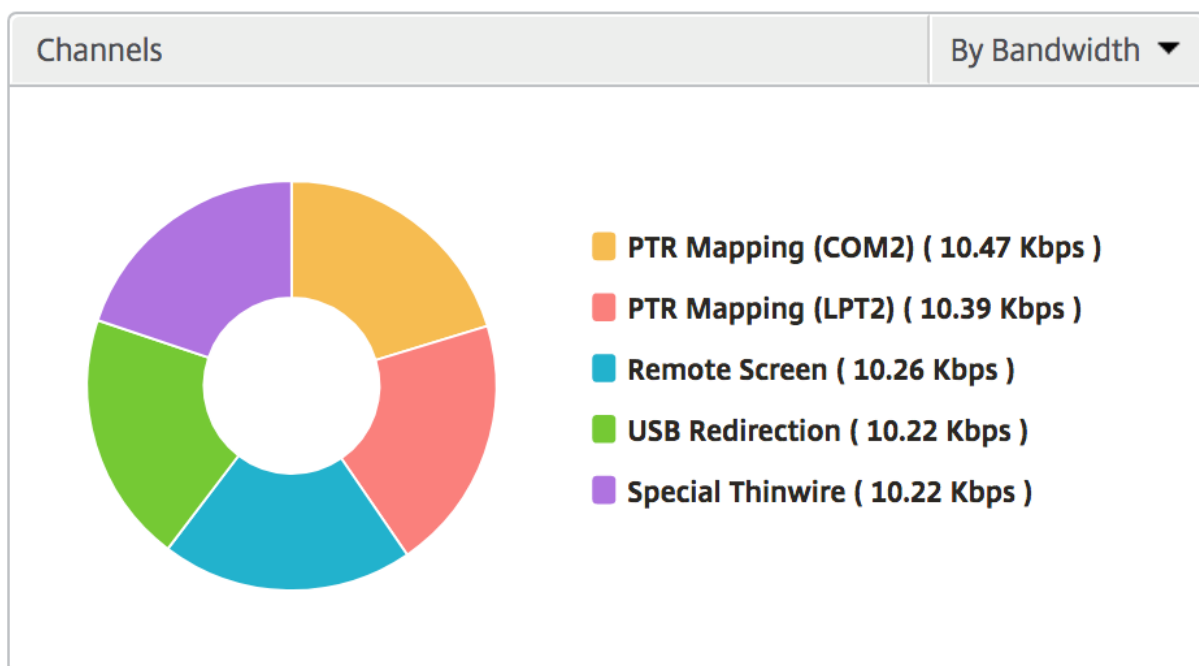
Active Desktops

特定の時間間隔におけるアクティブな Citrix Virtual Desktops 合計数。

Users										Search	
User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT ↑	WAN latency	DC latency	Bandwidth	Server Side Retransmits	CI		
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K			
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K			
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K			
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0			
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K			
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K			
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K			
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0			
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K			
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0			
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0			
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0			
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0			
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0			
randyby	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0			
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0			

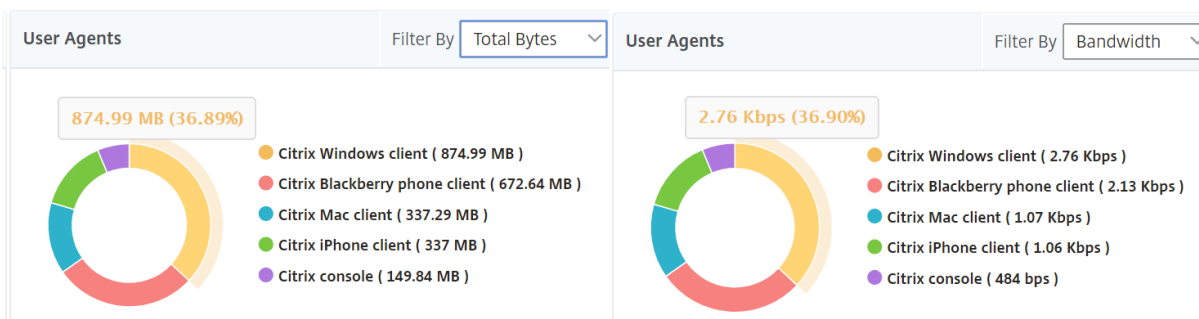
チャンネル

Channels では、各 ICA 仮想チャンネルで消費された全帯域幅または総バイト数をドーナツグラフ形式で表します。これらのメトリックは、[Bandwidth] または [Total bytes] で並べ替えることができます。



### ユーザーエージェント

User Agents では、各エンドポイントで消費された全帯域幅または総バイト数をドーナツグラフ形式で表します。これらのメトリックは、[Bandwidth] または [Total bytes] で並べ替えることができます。



### しきい値違反数

[Thresholds Breach Count] メトリックは、指定した期間において違反があったしきい値の数を表します。詳細については、「しきい値とアラートの作成方法」を参照してください。

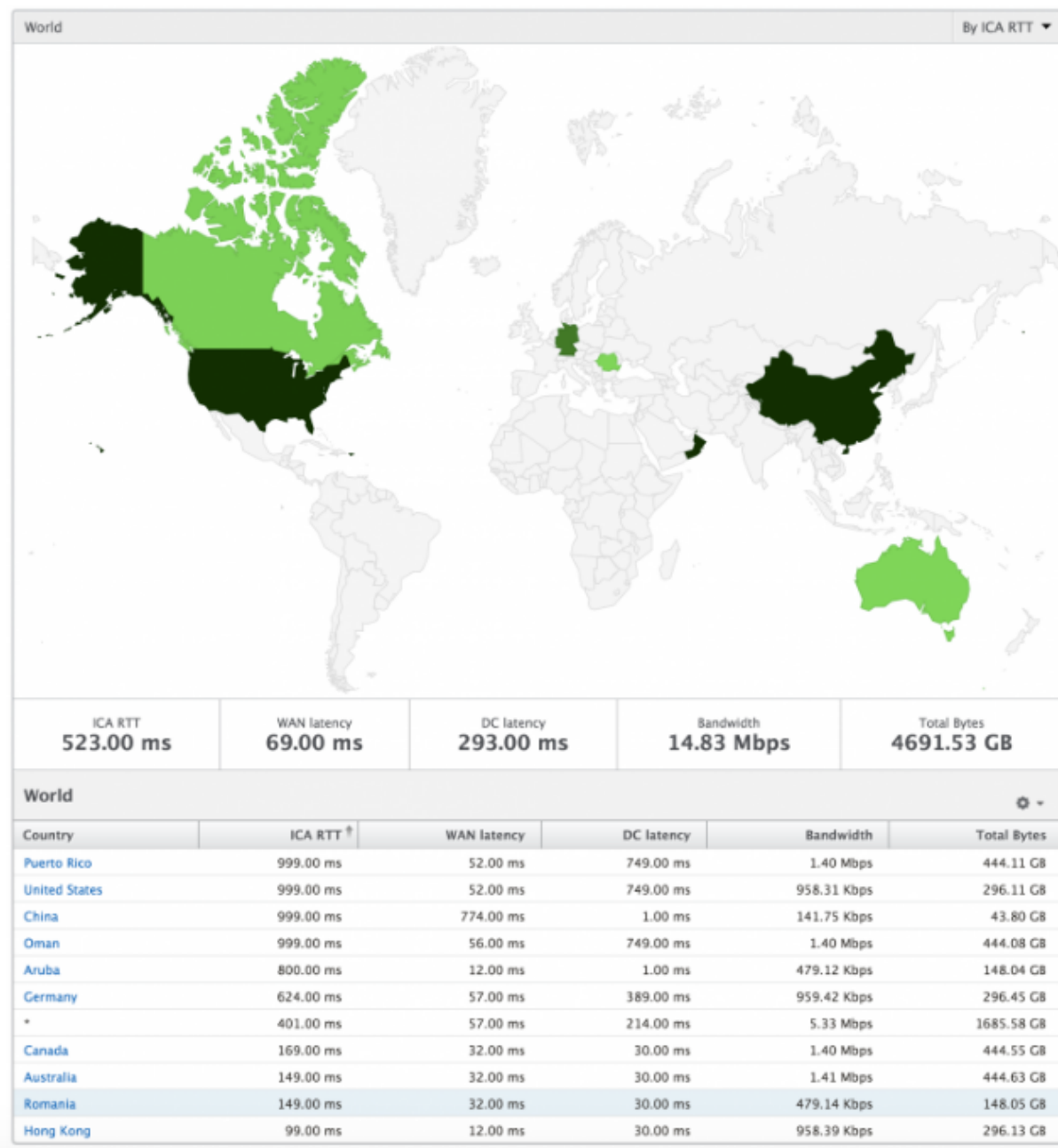
### 世界地図

HDX Insight の [World Map] ビューでは、管理者が地理的な観点からユーザー履歴およびアクティブユーザーの詳細を確認できます。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ビューを表示したり、特定の国や

都市にドリルダウンしたりできます。また、さらにドリルダウンして市区町村および都道府県別の情報を確認することもできます。NetScaler ADM バージョン 12.0 以降では、地理的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ます。また、各指標の密度はヒートマップの形式で表示されます。

- ICA 往復時間
- WAN 遅延
- DC の遅延
- 帯域幅
- バイト数合計



ユーザーごとのビュー

[Per User] ビューには、選択した特定のユーザーについて詳細なエンドユーザーエクスペリエンスに関するレポートが示されます。

特定のユーザーのメトリックに移動する手順は、次のとおりです。

1. [ **Analytics** ] > [ **HDX Insight** ] > [ ユーザー ] に移動します。
2. [User Summary] レポートで目的のユーザーを選択します。

## 折れ線グラフ

折れ線グラフには、指定した期間における選択したユーザーのメトリックすべての概要が表示されます。

## 現在/終了したセッションレポート

このレポートは、選択したユーザーの現在/終了済みのユーザーセッションすべてに関係します。これらのメトリックは、Start Time、Session Reconnects、ACR Counts を基準にして並べ替えることができます。

メトリックス	説明
セッション ID	ICA セッションの一意の ID。
セッションの種類	アプリケーション/デスクトップ。
状態	緑はアクティブなセッション、赤は非アクティブなセッション。
ホストの遅延	サーバーネットワークによる NetScaler ADC 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	特定の期間にセッションで使用された帯域幅です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
インターバルあたりのバイト数	特定の期間にセッションで使用されたバイト数。
開始時刻	セッションの開始時間。
アップタイム	セッションの実行時間
クライアント IP アドレス	エンドユーザーの IP。
サーバー IP アドレス	バックエンド/Citrix Virtual Apps サーバー IP。
NetScaler IP Address	NetScaler の管理 IP (NSIP)。
クライアントの種類	受信者の種類-Citrix Windows クライアントなど
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値 ([Yes] または [No])。セッションがマルチストリーム ICA かどうかを表します。
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。たとえば、NetScaler Gateway のユーザー/透過モードなどです。
国	セッションが確立された国。

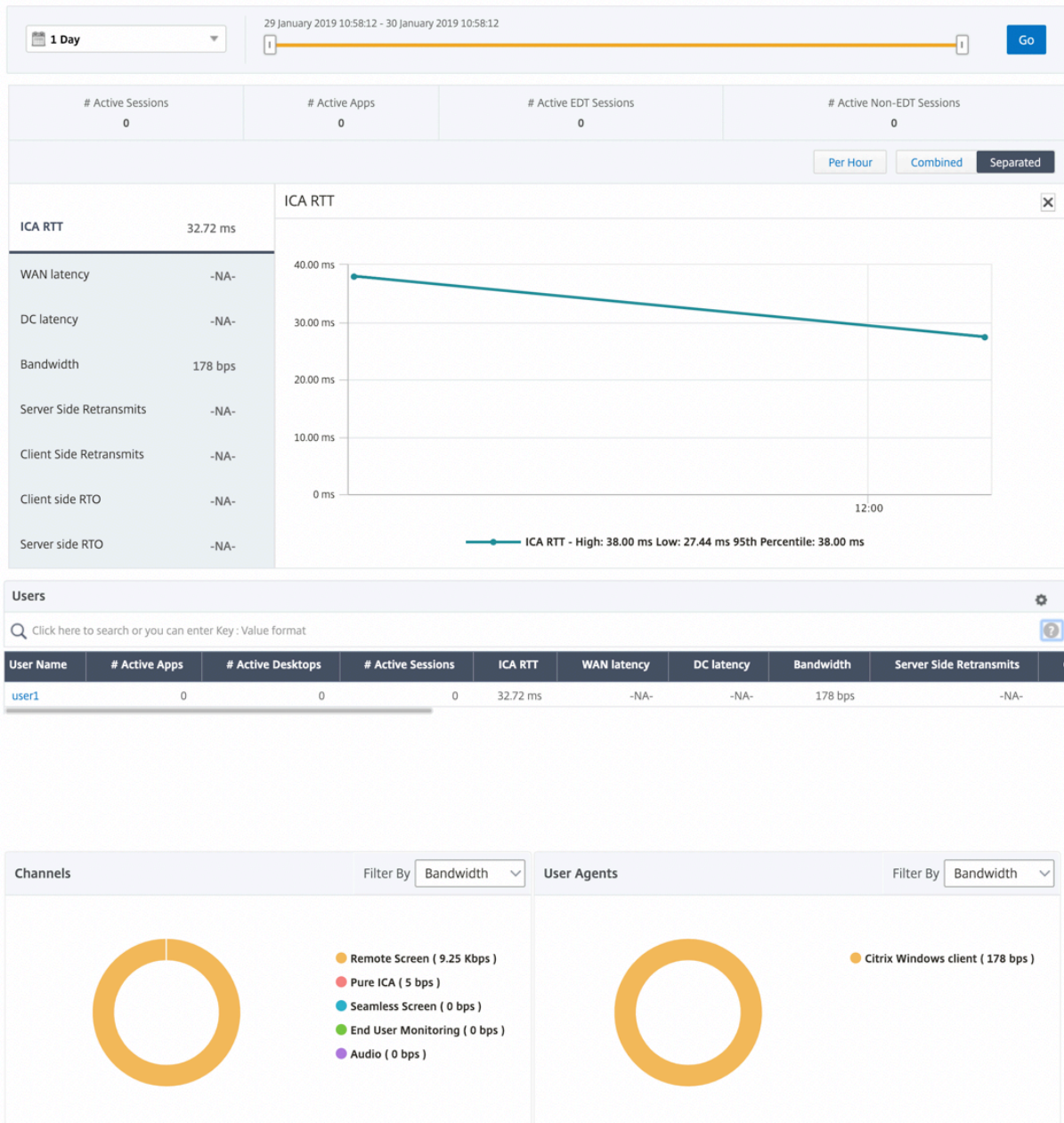
メトリックス	説明
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。
ICA 往復時間	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、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
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、TCP ウィンドウのサイズがゼロであることをクライアントがアダプタイズした回数を表します。
Client side fast RTO	NetScaler ADC 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、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。

メトリックス	説明
Server side fast RTO	NetScaler ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。

### **HDX Insight** における **EDT** のサポート

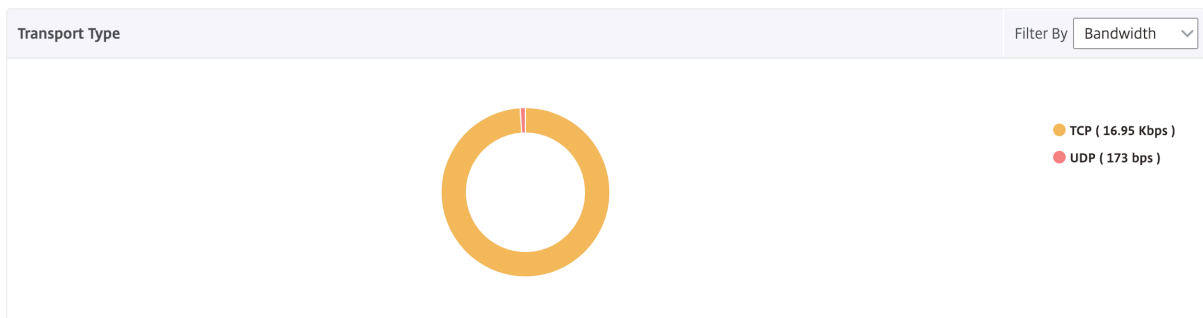
NetScaler Application Delivery Management (ADM) では、HDX Insight ight の分析を表示するための啓発データトランスポート (EDT) がサポートされるようになりました。つまり、ADM は UDP と TCP の両方のプロトコルをサポートするようになりました。NetScaler Gateway の EDT サポートにより、Citrix Receiver を実行しているユーザーの仮想デスクトップの高品位セッション内ユーザーエクスペリエンスが保証されます。

HDX Insight は、アクティブセッションレポートの一部として、EDT セッションと非 EDT セッションの数を表示するようになりました。「ユーザー」 (Users) テーブルには、システム内のすべてのユーザーの詳細なレポートが表示されます。この表には、WAN 遅延、DC 遅延、再送信、RTO などの指標が表示されます。これらのメトリックの一部は、現在 TCP スタックから計算されているため、EDT セッションを使用しているユーザーには使用できません。したがって、彼らは「NA」として登場する。



新しいドーナツグラフが導入され、ユーザーが使用したプロトコルの種類に基づいて、ユーザーが消費した帯域幅と合計バイト数を確認できるようになりました。





**NetScaler ADM 12.0** 以降から入手可能な **HDX Insight** メトリック:

L7 Client-side Latency

ICA クライアントと NetScaler ADC インスタンスの間で観測された平均 L7 遅延時間。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。

L7 Server-side Latency

NetScaler ADC デバイスと Citrix Virtual Apps の間で観察された平均 L7 遅延。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。定義済みしきい値の違反が一定期間に発生した場合の、L7 遅延の最大値。

違反の最大遅延

平均侵害待ち時間

システムが「L7 遅延時間を超過」した状態のときの、L7 遅延の平均値。

L7 しきい値違反数

L7 のしきい値違反が発生した回数。

Current Sessions									
Diagram	Session ID	Total Bytes	Bandwidth per Interval	Session Type	ICA RTT	Bytes per Interval	WAN latency	DC latency	Host Delay
	0000...000001	209.84 KB	11.58 Kbps	Application	854 ms	209.84 KB	83.00 ms	771 ms	4.00 ms
	0000...000001	127.18 KB	40.70 Kbps	Application	848 ms	127.18 KB	65.00 ms	710 ms	4.00 ms

Terminated Sessions								
Session ID	Session Type	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Session Bandwidth	Total Bytes	Bytes per Interval
0000...000001	Application	1.01 s	59.00 ms	763.00 ms	9.40 Kbps	9.40 Kbps	1.38 MB	1.38 MB
0000...000001	Desktop	971.00 ms	59.00 ms	733.00 ms	8.82 Kbps	8.82 Kbps	1.29 MB	1.29 MB
0000...000001	Application	998.00	51.00 ms	732.00 ms	9.91 Kbps	9.91 Kbps	1.45 MB	1.45 MB

デスクトップ ユーザー

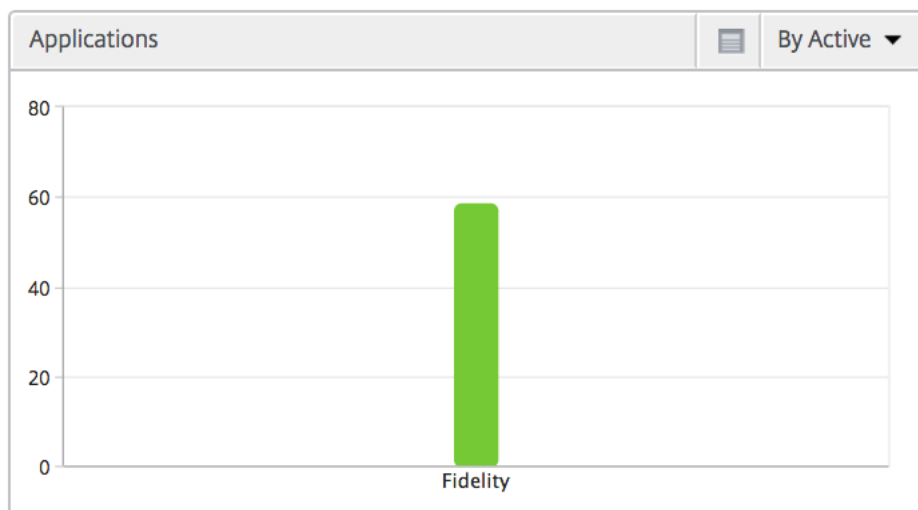
この表は、特定のユーザーの Citrix Virtual Desktop セッションに関する洞察を示しています。以下のメトリクスは [Desktop Launch Count] および [Bandwidth] を基準にしてソートできます。

メトリックス	説明
名前	Citrix Virtual Desktops 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です。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
ICA 往復時間	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、ユーザーに表示される画面の遅れです。

Desktop Users						By Desktop Launch Count ▾
Name	Desktop Launch Count ↑	Bandwidth	DC latency	WAN latency	ICA RTT	
XenDesktop33	177	9.38 Kbps	749.00 ms	57.00 ms	1.00 s	

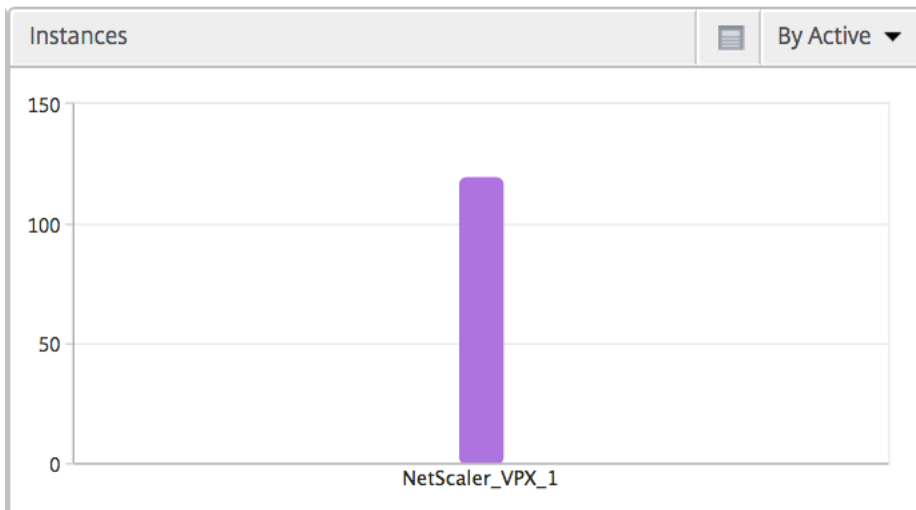
### アプリケーション

アクティブでソートされたアプリ、合計セッション起動数、合計アプリ起動数、および起動期間を表す棒グラフ。



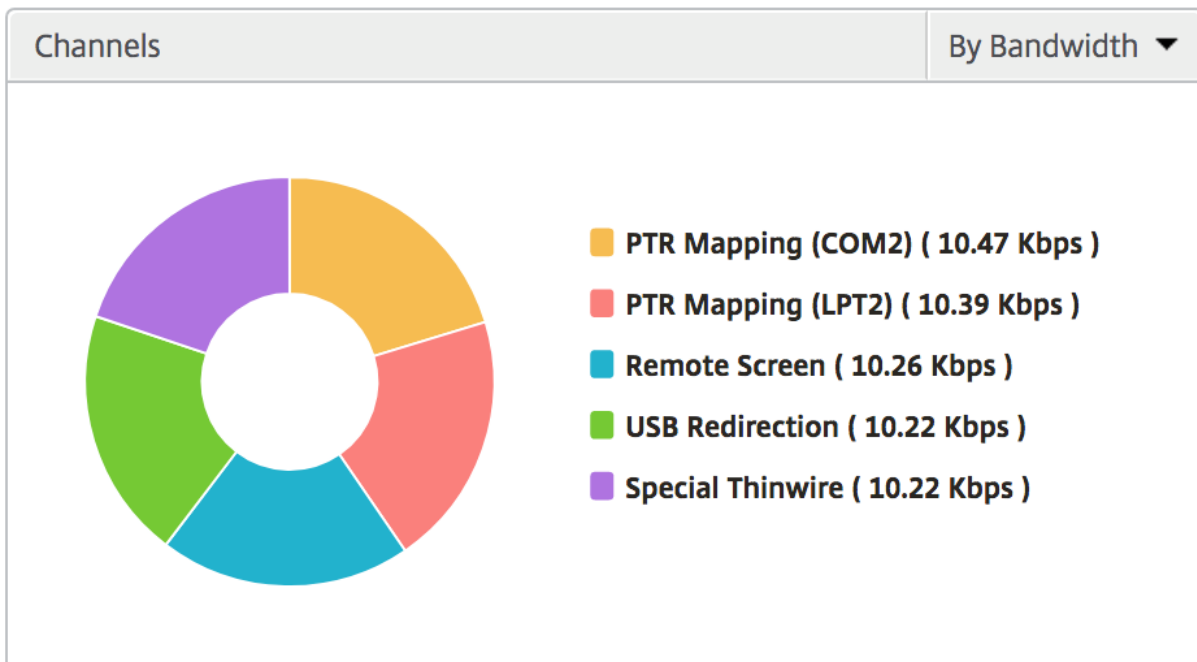
### インスタンス

NetScaler ADC インスタンスをアクティブおよび合計アプリ別にソートした棒グラフ



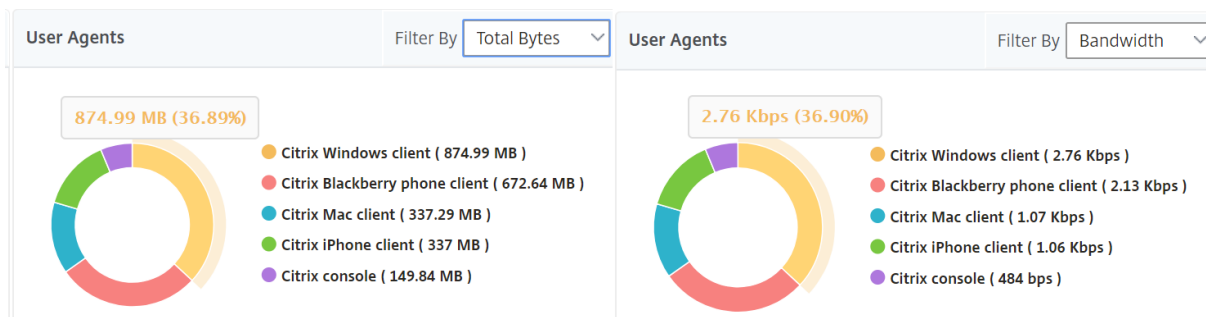
### チャンネル

Channels では、各 ICA 仮想チャンネルで消費された全帯域幅または総バイト数をドーナツグラフ形式で表します。これらのメトリックは、[Bandwidth] または [Total bytes] で並べ替えることができます。



## ユーザーエージェント

User Agents では、各エンドポイントで消費された全帯域幅または総バイト数をドーナツグラフ形式で表します。これらのメトリックは、[Bandwidth] または [Total bytes] で並べ替えることができます。



## ユーザー単位のセッション・ビュー

[Per User Session] ビューには、選択したユーザーのセッションに関するレポートが表示されます。

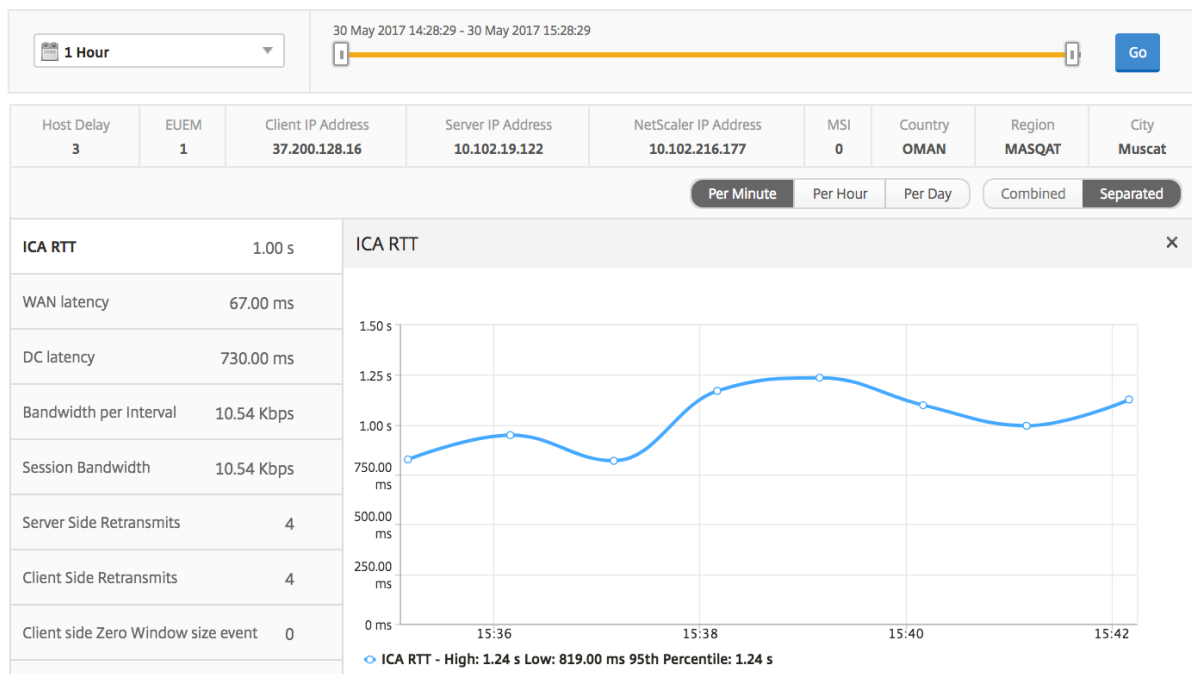
選択したユーザーのセッションのメトリックを表示する手順は、次のとおりです。

1. [ **Analytics** ] > [ **HDX Insight** ] > [ ユーザー ] に移動します。
2. 「ユーザー 概要レポート」セクションから特定のユーザー を選択します。
3. 「現在のセッション」または「終了したセッション」列からセッションを選択します。

## 時系列グラフ

メトリックス	説明
セッション再接続	この数字は、アクティブな Citrix Virtual App and Desktop セッションの数を示します。
ACR 数	この数字は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	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、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。

メトリックス	説明
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
サーバー側の再転送	NetScaler ADC 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転送	NetScaler ADC 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大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	NetScaler ADC 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。
Server side fast RTO	NetScaler ADC 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	特定の期間にセッションで使用された帯域幅です。
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、TCP ウィンドウサイズがゼロであることをサーバーがアダプタイズした回数を表します。
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、TCP ウィンドウのサイズがゼロであることをクライアントがアダプタイズした回数を表します。



### 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および起動時間で並べ替えることができます。

Active Applications				By # Active Sessions
Name	# Active Sessions	Launch Duration	# Active Apps	
Fidelity	1	557.00 ms	1	

### 関連セッション

[Related Sessions] セクションには、選択したユーザーのセッションに関連するセッションが表示されます。このリレーションシップは、共通サーバーまたは共通 NetScaler ADC として選択できます。

Related Sessions											By Common Server
Session ID	Session Type	User Name	State	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Total Bytes	Total Bytes	Byte	
0000...000001	Application	grahmm	●	1.021 s	51.00 ms	737 ms	9.26 Kbps	9.26 Kbps	977.73 KB		
0000...000001	Application	liam	●	955 ms	50.00 ms	733 ms	10.91 Kbps	10.91 Kbps	1.26 MB		
0000...000001	Application	qrahmm	●	1.058 s	38.00 ms	817 ms	10.27 Kbps	10.27 Kbps	367.24 KB		

## インスタンスビューのレポートとメトリックス

February 6, 2024

インスタンスビューのレポートとメトリックは、NetScaler ADC 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、次の手順に従います。

1. [分析] > [HDX Insight] > [インスタンス] に移動します。

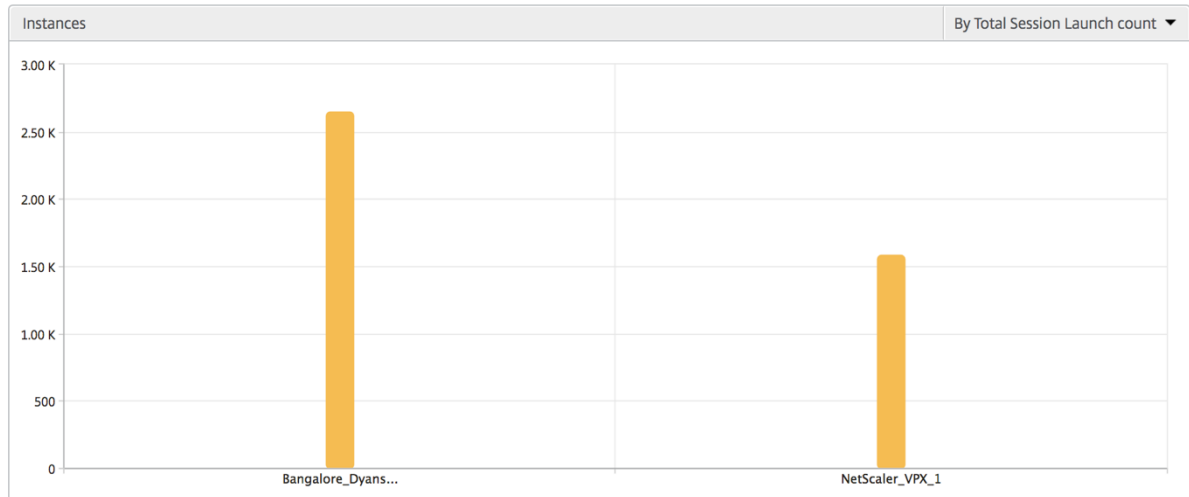
### インスタンスの概要ビュー

このビューは、Citrix ADNetScaler ADM に追加されたすべての NetScaler ADC インスタンスのレポートを表示するため、概要ビューと呼ばれます。

特に明記されていない限り、すべての指標/レポートには、選択した期間のそれらに対応する値が含まれます。

インスタンス棒グラフ

このグラフには、インスタンスの合計セッション起動回数と、グラフキャンバスの右上のリストから選択できるアプリケーションの合計が表示されます。



インスタンス/アクティブインスタンスの概要レポート

メトリックス	説明
名前	NetScaler ADC インスタンスのホスト名。
IP アドレス	NetScaler の IP アドレスです。
セッションの起動数合計	特定の期間に作成された一意のユーザーセッションの合計数です。
アプリケーション合計数	特定の期間に起動された一意のアプリケーションの合計数です。
種類	-

Instances				
Name	IP Address	Total Session Launch count ↑	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances					
Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

## しきい値レポート

しきい値レポートは、選択した期間内に エンティティ がインスタンスとして選択された場合に、違反したしきい値の数を表します。詳細については、「[しきい値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

スキップフローは、ICA 接続の解析が省略されたレコードのことです。これは、サポートされていない Citrix Virtual Apps and Desktops のバージョン、サポートされていないバージョンのレシーバーまたはレシーバータイプを使用するなど、複数の理由で発生する可能性があります。このテーブルでは、IP アドレスとスキップフロー数が示されます。これらの受信機は、ホワイトリストに登録された受信機の一部ではない場合があります。したがって、これらのセッションはモニタリングからスキップされます。

エラーを参照してください。ICA 解析に関連する問題の詳細については、[ハイパーリンク参照](#)が有効ではありません。

Skipped Flows	
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

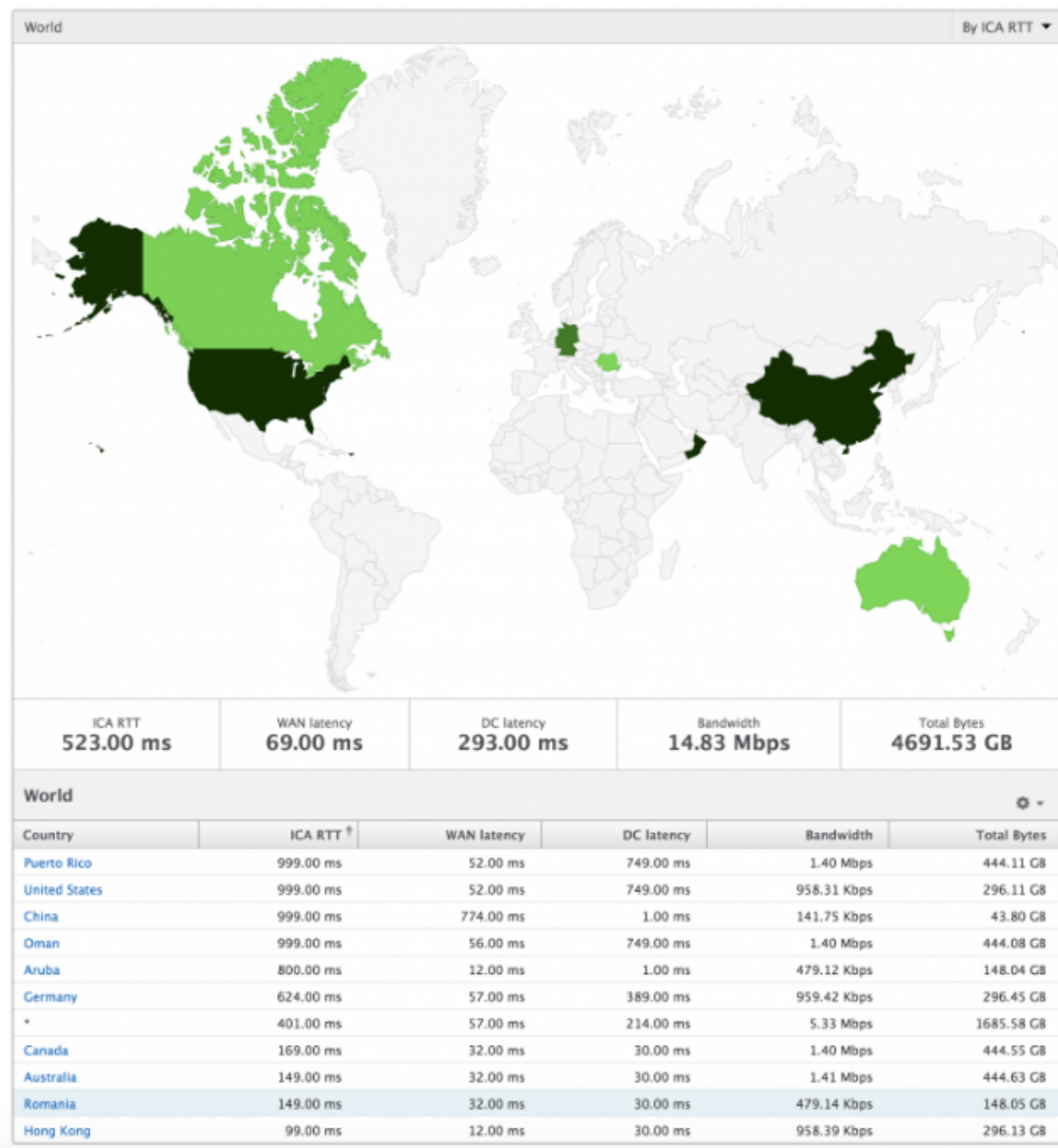
## 世界観

HDX Insight の世界地図ビューでは、管理者が地理的な観点からユーザー履歴およびアクティブユーザーの詳細を確認できます。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ビューを表示したり、特定の国や都市にドリルダウンしたりできます。管理者はさらにドリルダウンして、都市および州別に情報を表示できます。NetScaler ADC 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ます。また、各指標の密度はヒートマップの形式で表示されます。

- ICA 往復時間
- WAN 遅延
- DC の遅延
- 帯域幅
- バイト数合計





インスタンスごとのビュー

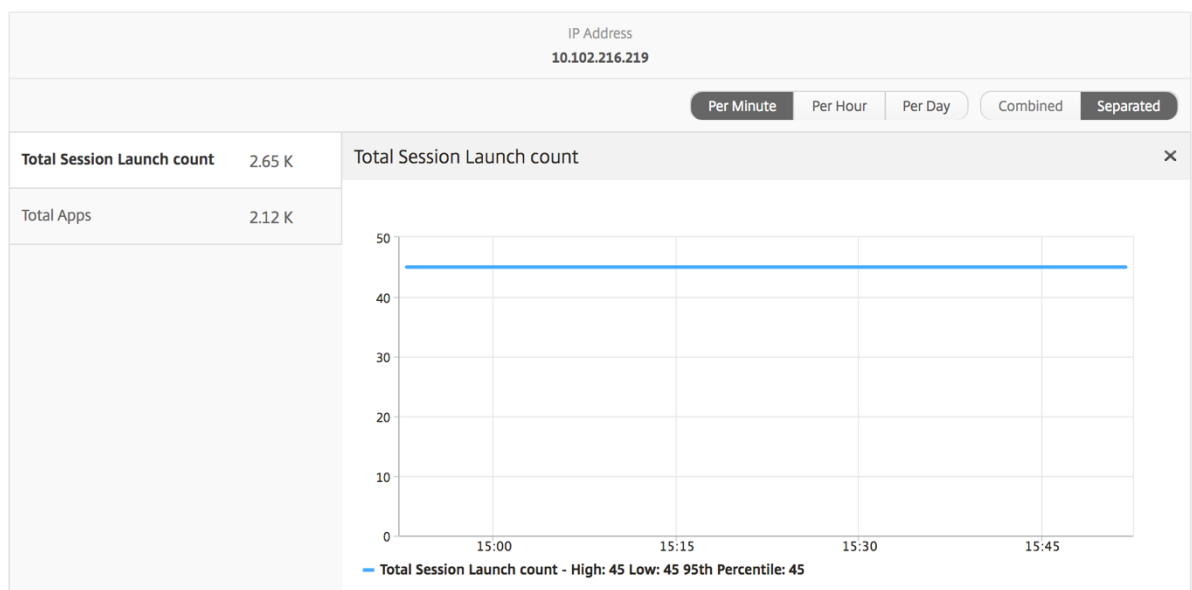
インスタンスごとのビューでは、選択した特定の NetScaler ADC インスタンスに関する詳細なエンドユーザーエクスペリエンスレポートが提供されます。

インスタンス・ビューに移動するには、次の手順に従います。

1. [分析] > [HDX Insight] > [インスタンス] に移動します。
2. インスタンス 概要レポートから特定のインスタンスを選択します。

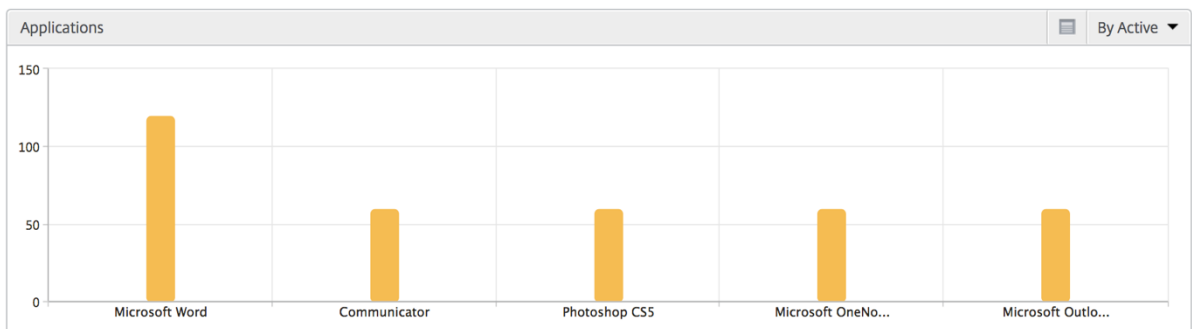
折れ線グラフ

メトリック	説明
IP アドレス	選択したインスタンスの NetScaler IP アドレスを表します。
Total session launch count	特定の時間間隔におけるアクティブな Citrix Virtual App セッションの総数。
アプリケーション合計数	特定の期間に起動された一意のアプリケーションの合計数です。



アプリケーション棒グラフ

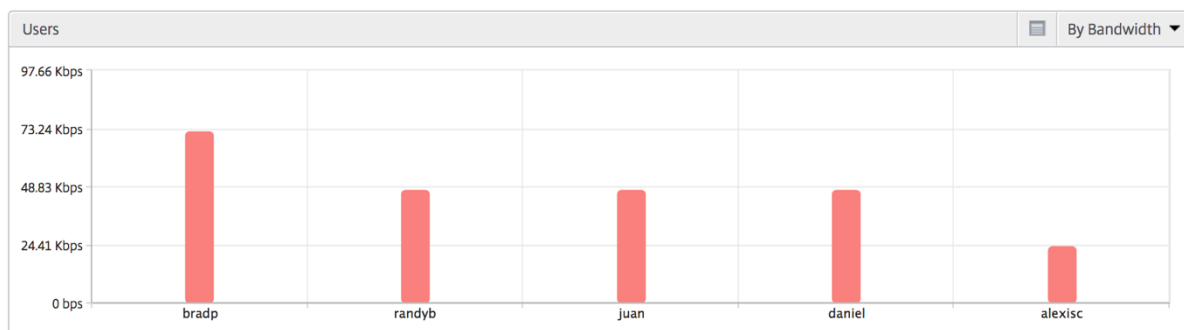
アクティブなアプリ、セッションの合計起動数、アプリの合計起動数、起動時間などの条件に基づいて、上位 5 個のアプリケーションを表示します。



### ユーザー棒グラフ

ユーザー棒グラフには、以下の基準別に上位 5 人のユーザーが表示されます。

- 帯域幅
- WAN 遅延
- DC の遅延
- ICA 往復時間



### 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示しています。以下のメトリクスは [Desktop Launch Count] および [Bandwidth] を基準にしてソートできます。

メトリックス	説明
名前	Citrix Virtual Desktops 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です。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
ICA 往復時間	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、ユーザーに表示される画面の遅れです。

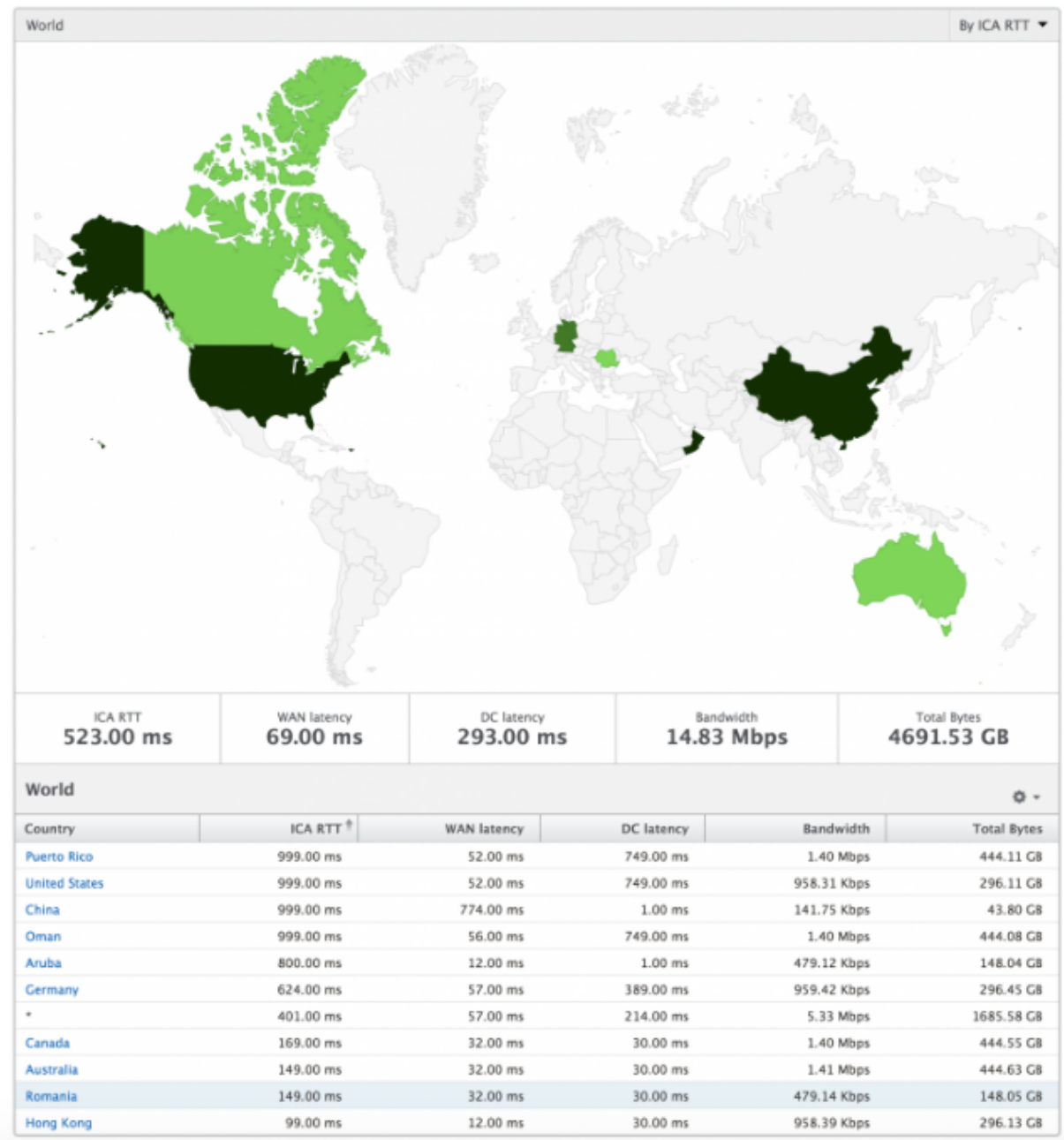
Desktop Users					By Desktop Launch Count ▾
Name	Desktop Launch Count ↕	Bandwidth	DC latency	WAN latency	ICA RTT
XenDesktop33	177	9.38 Kbps	749.00 ms	57.00 ms	1.00 s

### 世界観

HDX Insight の世界地図ビューでは、管理者が地理的な観点からユーザー履歴およびアクティブユーザーの詳細を確認できます。管理者は、システムのワールドビューを表示したり、特定の国にドリルダウンしたり、さらに都市にドリルダウンしたり、地域をクリックしたりできます。管理者はさらにドリルダウンして、都市および州別に情報を表示できます。NetScaler ADM バージョン 12.0 以降では、地理的な場所から接続しているユーザーにドリルダウンできます。

HDX Insight のワールドマップでは、以下の詳細を表示できます。また、各指標の密度はヒートマップの形式で表示されます。

- ICA 往復時間
- WAN 遅延
- DC の遅延
- 帯域幅
- バイト数合計



## ライセンスビューのレポートとメトリック

February 6, 2024

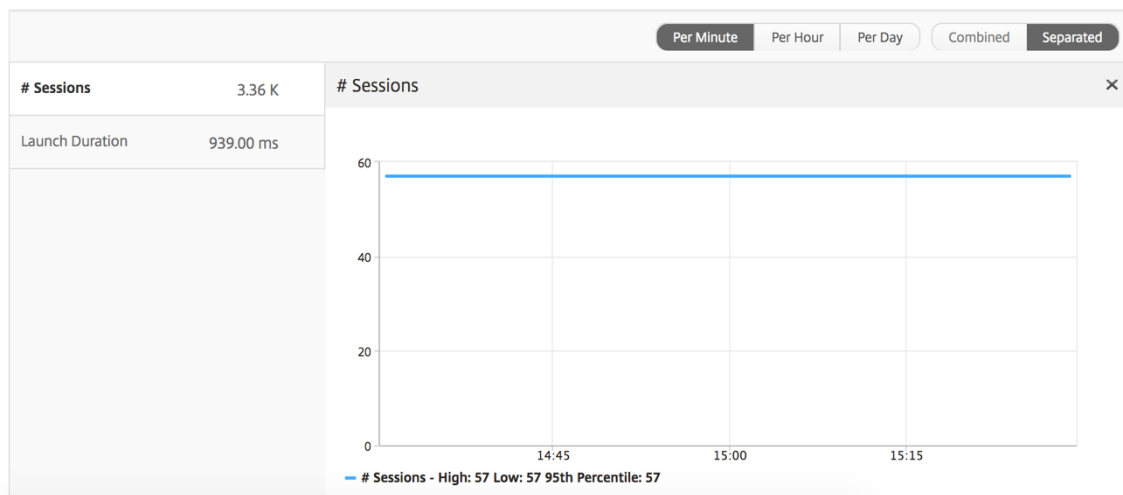
ライセンスビューには、NetScaler Gateway のライセンス情報が表示されます。

ライセンスビューに移動するには、次の操作を行います。

1. [アナリティクス] > [HDX Insight] > [ライセンス] に移動します。

### 折れ線グラフ

メトリック	説明
使用中のライセンス	選択した期間中に使用されている NetScaler Gateway CCU ライセンス。各カウントは、ユーザーセッションの数を表します。このカウントには、各ユーザーが起動したアプリケーションセッションおよびデスクトップセッションは含まれません。
総ライセンス数	お客様が利用できる NetScaler Gateway CCU ライセンスの合計数。



### しきい値レポート

しきい値レポートは、選択した期間内に 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、違反したしきい値の数を表します。詳細については、「しきい値とアラートの作成方法」を参照してください。

## HDX Insight の問題のトラブルシューティング

February 6, 2024

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、各セクションのチェックリストを参照してください。

- HDX Insight の構成。
- NetScaler ADC と NetScaler ADM 間の接続性。
- NetScaler ADC での HDX/ICA トラフィックのレコード生成。
- NetScaler ADM 内のレコードの設定。

### HDX Insight 構成チェックリスト

- NetScaler ADC 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 ADC の実行構成で HDX Insight 構成を確認します。

`show running | grep -i <appflow_policy>` コマンドを実行して、HDX Insight の設定を確認します。バインドタイプが ICA REQUEST であることを確認します。たとえば、

```
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 でなければなりません。たとえば、

```
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は、HDX/ICA トラフィックが流れている VPN 仮想サーバーに HDX Insight AppFlow ポリシーがバインドされていることを確認してください。
- 透過モードまたは LAN ユーザーモードの場合は、ICA ポート 1494 と 2598 が設定されていることを確認します。
- Citrix `appflowlog` Gateway または VPN 仮想サーバーのチェックパラメータは、Access Gateway またはダブルホップ展開で有効になっています。詳しくは、「[仮想サーバーに対する AppFlow の有効化](#)」を参照してください。
- ダブルホップ NetScaler ADC で「接続チェーン」が有効になっていることを確認します。詳しくは、「[データをエクスポートするための NetScaler Gateway アプライアンスの構成](#)」を参照してください。
- 高可用性フェイルオーバー後、HDX Insight の詳細が解析されスキップされている場合は、ICA パラメータ「`EnablesronHaFailover`」が有効になっていることを確認します。詳しくは、「[NetScaler ADC 高可用性ペアのセッション画面の保持](#)」を参照してください。

### NetScaler ADC と NetScaler ADM の間の接続チェックリスト

- NetScaler ADC で AppFlow コレクタのステータスを確認します。詳しくは、「[NetScaler ADC と AppFlow Collector 間の接続状態を確認する方法](#)」を参照してください。
- HDX Insight の AppFlow ポリシー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チェックします。

GUI で [システム] > [AppFlow] > [ポリシー] に移動して、AppFlow ポリシーのヒットを確認することもできます。

- 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を検証します。

## NetScaler ADC チェックリストでの HDX/ICA トラフィックのレコード生成

`tail -f /var/log/ns.log | grep -i "default ICA Message"` ログ検証のためにコマンドを実行します。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使用できます。

- ログ: **ICA** 接続の解析をスキップしました - **HDX Insight** がこのホスト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が **0x53** を受信しました。サポートされていません。  
原因: サポートされていないバージョンの Citrix Workspace  
解決策: Citrix Workspace をサポートされているバージョンにアップグレードします。詳しくは、「[Citrix Workspace アプリ](#)」を参照してください。
- ログ: 展開パケットからのエラー-このフローのすべての **hdx** 処理をスキップします  
原因: ICA トラフィックの圧縮解除に関する問題  
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: 移行が無効です: **NS\_ICA\_ST\_FLOW\_INIT/NS\_ICA\_EVT\_INVALID-> NS\_ICA\_ST\_UNINIT**  
原因: ICA ハンドシェイクの解析に関する問題  
解決策: 新しいセッションが確立されるまで、この特定の ICA セッションのレポートは利用できません。
- ログ: **EUEM ICA RTT** が見つかりません  
原因: エンドユーザー状況監視チャンネルのデータを解析できません  
解決策: エンドユーザー状況監視サービスが Citrix Virtual Apps and Desktops サーバーで開始されていることを確認します。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: 無効なチャンネルヘッダー  
原因: チャンネルヘッダーを識別できません  
解決策: 新しいセッションが確立されるまで、この特定の ICA セッションのレポートは利用できません。



- ログ: スキップコード

スキップコードに次の値のいずれかが表示された場合、その Insight 詳細の解析がスキップされます。

スキップコード 0 は、レコードが NetScaler ADC 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中にエラーが発生しました。おそらくメモリ状態が原因です
101	NS_ICA_ERR_INVALID_HS_CMD	無効なハンドシェイクコマンドを受け取りました
102	NS_ICA_ERR_REduc_PARAM_CNTV3	エクスパンダーの初期化に無効なパラメーターが指定されました
103	NS_ICA_ERR_REduc_INIT	V3 エクスパンダーを正しく初期化できません
104	NS_ICA_ERR_REduc_PARAM_BYTES	エクスパンダーをチャンネルに割り当てるにはバイト数が足りません
105	NS_ICA_ERR_INVALID_CHANNEL	ICA チャンネル番号が無効です
106	NS_ICA_ERR_INVALID_DECODER	チャンネルに無効なデコーダーが指定されました
107	NS_ICA_ERR_INVALID_TW_PARAM	Thinwire チャンネルに無効なパラメーター数が指定されました
108	NS_ICA_ERR_INVALID_TW_DECODER	Thinwire チャンネルのデコーダーが無効です
109	NS_ICA_ERR_REduc_NO_DECODER	チャンネルにデコーダーが定義されていません
110	NS_ICA_ERR_REduc_V3_EXPANDER	チャンネルデータを拡張できませんでした
111	NS_ICA_ERR_REduc_BYTES_V3_OOR	エクスパンダーエラー: 使用可能なバイト数を超えるバイトが消費されました
112	NS_ICA_ERR_REduc_BYTES_OOR	エラー: 非圧縮データオーバーラン
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

スキップコード	エラーメッセージ	エラーの原因
116	NS_ICA_ERR_MEM_REDUCE_CTX_ALLOC	100 バ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	Packet Init 要求はフラグメント化されており、処理できません
119	NS_ICA_ERR_INIT_ICA_CAPS	ICA 機能初期化エラー
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 のバージョンが 6.5 以前か、XenDesktop のバージョンが 5.0 以前かを示します
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_INSUFFICIENT_CHANNEL_SIZE	チャンネル全体で不十分なバイト数
123	NS_ICA_ERR_CHANNEL_DATA	EUEM、CONTROL、または SEAMLESS チャンネルのデータが正しくない
124	NS_ICA_ERR_INVALID_PURE_CMD	PURE ICA チャンネルデータの処理中に無効なコマンドを受け取りました
125	NS_ICA_ERR_INVALID_PURE_LEN	PURE ICA チャンネルデータの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 チャンネルデータの処理中に無効な長さが検出されました
127	NS_ICA_ERR_INVALID_CLNT_DATA	クライアントから受信したデータ長が無効です
128	NS_ICA_ERR_MSI_GUID_SZ	MSI GUID サイズエラー
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	チャンネルヘッダーが検出されました
130	NS_ICA_ERR_CGP_PARSE_RECONNECT	再接続したセッションの取得に失敗しました
131	NS_ICA_ERR_DISABLE_SR_NON_RECONNECT	NSI RECONNECT トリの無効化中にエラーが発生しました
132	NS_ICA_ERR_REDUCE_NOT_V3	サポートされていない ICA リデュースerverバージョン
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	DISABLED で、ホストには適用されません

スキップコード	エラーメッセージ	エラーの原因
134	NS_ICA_ERR_IDENT_PROTO	ICA または CGP プロトコルを識別できない、不正なレシーバーを使用している
135	NS_ICA_ERR_INVALID_SIGNATURE	ICA 署名またはマジックストリングが正しくありません
136	NS_ICA_ERR_PARSE_RAW	ICA ハンドシェイクパケットの解析中にエラーが発生しました
137	NS_ICA_ERR_INCOMPLETE_PKT	ハンドシェイクで不完全なパケットを受信しました
138	NS_ICA_ERR_ICAFRAME_TOO_LARGE	ICA フレームが大きすぎます、1460 バイトを超えています
139	NS_ICA_ERR_FORWARD	ICA データの転送中にエラーが発生しました
140	NS_ICA_ERR_MAX_HOLES	CGP コマンドはサポートされている制限を超えて分割されているため、処理できません
141	NS_ICA_ERR_ASSEMBLE_FRAME	ICA フレームを正しく再構成できません
142	NS_ICA_ERR_UNSUPPORTED_RECONNECT_VERSION	クライアントバージョンのため、このレシーバ (クライアント) に対する ICA 解析をスキップしました
143	NS_ICA_ERR_LOOKUP_RECONNECT_COOKIE	クライアント再接続 Cookie の解析状態を検出できません
144	NS_ICA_ERR_SYNCUP_RECONNECT_COOKIE	クライアントの再接続後に無効な再接続 Cookie 長が検出されました
145	NS_ICA_ERR_INVALID_RECONNECT_COOKIE	クライアントの再接続クッキーが必要な制約を逃しました
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	クライアントから受信した受信者バージョン文字列が無効です
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	クライアントから受け取った製品 ID が無効です
148	NS_ICA_ERR_V3_HDR_CORRUPT	再接続後のチャンネル長が無効です
149	NS_ICA_ERR_SPECIAL_THINWIRE	解凍エラー
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTES	SEAMLESS コマンドのバイト数が不足しています
151	NS_ICA_ERR_EUEM_INSUFFBYTE	EUEM コマンドのバイト数が不足しています

スキップコード	エラーメッセージ	エラーの原因
152	NS_ICA_ERR_SEAMLESS_INVALID_EVENT	SEAMLESS チャンネル解析のイベントが無効です
153	NS_ICA_ERR_CTRL_INVALID_EVENT	CTRL チャンネル解析のイベントが無効です
154	NS_ICA_ERR_EUEM_INVALID_EVENT	EUEM チャンネル解析のイベントが無効です
155	NS_ICA_ERR_USB_INVALID_EVENT	USB チャンネル解析のイベントが無効です
156	NS_ICA_ERR_PURE_INVALID_EVENT	PURE チャンネル解析のイベントが無効です
157	NS_ICA_ERR_VCP_INVALID_EVENT	仮想チャンネル解析のイベントが無効です
158	NS_ICA_ERR_ICAP_INVALID_EVENT	ICA データ解析のイベントが無効です
159	NS_ICA_ERR_CGPP_INVALID_EVENT	CGP データ解析のイベントが無効です
160	NS_ICA_ERR_BASICCRYPT_INVALID_STATE	基本レベルの暗号化の crypt コマンドの状態が無効です
161	NS_ICA_ERR_BASICCRYPT_INVALID_COMMAND	基本レベルの暗号化の crypt コマンドが無効です
162	NS_ICA_ERR_ADVCRYPT_INVALID_STATE	RC5 暗号化の crypt コマンドの状態が無効です
163	NS_ICA_ERR_ADVCRYPT_INVALID_COMMAND	RC5 暗号化の crypt コマンドが無効です
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_REDUCED_VERSION	サーバーはリデューサーバージョン 3 をサポートしていません
167	NS_ICA_ERR_CLIENT_NOT_REDUCED_VERSION	クライアントはリデューサーバージョン 3 をサポートしていません
168	NS_ICA_ERR_ICAP_INSUFFBYTE	ICA ハンドシェイクで予期しないバイト数
169	NS_ICA_ERR_HIGHER_RECONSEQ	ピア再接続後の 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 の解析状態を復元できない
171	NS_ICA_ERR_NSAP_PARSING	Insight チャンネルデータの解析中にエラーが発生しました

スキップコード	エラーメッセージ	エラーの原因
172	NS_ICA_ERR_NSAP_APP	Insight チャン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 チャンネルデータから 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 チャン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 チャンネルサポートがないため、サービスノードの ICA 解析をスキップしました
176	NS_ICA_ERR_NON_NSAP_CLIENT	NSAP はクライアントではサポートされていません
177	NS_ICA_ERR_NON_NSAP_SERVER	NSAP は VDA では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にエラーが発生しました
179	NS_ICA_ERR_SN_RECONNECT_TKT_FAILURE	クライアントでサービスの再接続チケットを取得中にエラーが発生しました
180	NS_ICA_ERR_SN_HIGHER_RECONNECT_SEQ	サービスノードでより高い再接続シケンス番号を受信するとエラーが発生しました
181	NS_ICA_ERR_DISABLE_HDXINSIGHTS_FROM_NSAP	NSAP から再接続で HDX Insight を無効にしているときにエラーが発生しました

サンプルログ:

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT
ns-223 0-PPE-2 : default ICA Message 1234 0 : "Session setup data
send: Session GUID [57af35043e624abab409f5e6af7fd22c], Client IP/
Port [10.105.232.40/52314], Server IP/Port [10.106.40.215/2598], MSI
Client Cookie [Non-MSI], Session setup time [01/09/2020:22:56:49
GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [
user1], Client [10.105.232.40], Server [WIN2K12-215], Ctx Flags [0
x8820220228], 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 [0
x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```

### エラーカウンター

さまざまなカウンターが ICA 解析でキャプチャされます。次の表に、ICA 解析用の各種カウンタを示します。コマンド `nsconmsg -g hdx -d statswt0` を実行して、カウンタの詳細を表示します。

HDX カウンタ名	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ピュア ICA 接続の総数を示します。クライアント PCB 上の ICA 署名に基づく ICA 接続が検出されるたびに増加します。	Stats
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 (セッション信頼性オン)。クライアント PCB の CGP 署名に基づく CGP 接続が検出されるたびに増分されます。	Stats
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	Stats
hdx_dbg_tot_nsap_conn	NS が検出した NSAP がサポートする接続の総数を示します	Stats
skip_conn	ICA または CGP 署名が無効であるために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。	統計情報
hdx_dbg_active_conn	その時点でのアクティブな EDT/CGP/ICA 接続の合計数。	統計情報
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。	統計情報
hdx_dbg_skip_appflow_disabled	AppFlow を無効にしたために AppFlow がセッションから接続解除されたインスタンスの総数	ステータス/診断
hdx_dbg_transparent_user	透過的なユーザーアクセスの総数	ステータス/診断

HDX カウンタ名	目的	カテゴリ (統計/エラー/診断)
hdx_dbg_ag_user	Access Gateway のユーザーアクセスの総数	ステータス/診断
hdx_dbg_lan_user	LAN ユーザーモードアクセスの総数	ステータス/診断
hdx_basic_enc	基本暗号化を使用する ICA 接続の数を示します	ステータス/診断
advanced_enc	高度な RC5 ベースの暗号化を使用する ICA 接続の数を示します	ステータス/診断
dx_dbg_wanscaler_on_clientside	クライアント側に Citrix SD-WAN がある CGP/ICA 接続の総数	ステータス/診断
hdx_dbg_wanscaler_on_serverside	Citrix SD-WAN サーバー側の CGP/ICA 接続の総数	ステータス/診断
reconnected_session	NetScaler ADC エラーのないクライアントからの再接続要求の総数	ステータス/診断
hdx_dbg_host_rejected_ns_reconnect	クライアント別の再接続要求を拒否したホストの総数	ステータス/診断
hdx_euem_available	エンドユーザーエクスペリエンスモニタリングチャンネルが使用できる接続の数を示します。ICA RTT などの統計を収集するには、エンドユーザーエクスペリエンス監視チャンネルが必要です。	ステータス/診断
hdx_err_disabled_sr	nsapimgr ノブを使用してセッション画面の保持が無効になります。セッションはこのセッションでは機能しません。	エラー
hdx_err_skip_no_msi	XA/XD サーバーに MSI 機能がありません。これは古いサーバーバージョンを示しており、HDX Insight はこの接続をスキップします。	エラー
hdx_err_skip_old_server	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	クライアント受信機が許可リストにない、HDX Insight はこの接続をスキップします	エラー
hdx_sm_ica_cam_channel_disabled	SmartAccess ポリシーによって無効化された NS_ICA_CAM_CHANNEL の総数	診断

HDX カウンタ名	目的	カテゴリ (統計/エラー/診断)
hdx_sm_ica_usb_channel_disabled	SmartAccess ポリシーによって無効にされた NS_ICA_USB_CHANNEL の総数	診断
hdx_sm_ica_clip_channel_disabled	SmartAccess ポリシーによって無効化された NS_ICA_CLIP_CHANNEL の総数	診断
hdx_sm_ica_ccm_channel_disabled	SmartAccess ポリシーによって無効にされた NS_ICA_CCM_CHANNEL の総数	診断
hdx_sm_ica_cdm_channel_disabled	SmartAccess ポリシーによって無効にされた 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にされた 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にされた 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にされた NS_ICA_CPM_CHANNEL の総数	診断
hdx_sm_ica_lpt1_channel_disabled	SmartAccess ポリシーによって無効にされた 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にされた 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 が無効になっているケースの総数	診断
hdx_sm_ica_file_channel_disabled	SmartAccess ポリシーによって無効になっている NS_ICA_FILE_CHANNEL の総数	診断
hdx_dbg_usb_accept_device	受け入れられた 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 カウンタ名	目的	カテゴリ (統計/エラー/診断)
hdx_dbg_usb_reset_endpoint	リセットされた USB エンドポイントの総数	診断
hdx_dbg_usb_reset_device	リセットされた USB デバイスの総数	診断
hdx_dbg_usb_stop_device	停止した 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の総数	診断
hdx_dbg_usb_device_gone	なくなった USB デバイスの総数	診断
hdx_dbg_usb_device_stopped	停止した USB デバイスの総数	診断

### nstrace 検証

CFLOW プロトコルをチェックして、NetScaler ADC から送信されるすべての AppFlow レコードを確認します。

### NetScaler ADM チェックリスト内のレコードの移入数

- `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"` コマンドを実行し、ログをチェックして、NetScaler ADM が AppFlow レコードを受信していることを確認します。
- NetScaler ADC インスタンスが NetScaler ADM に追加されていることを確認します。
- NetScaler Gateway/VPN 仮想サーバーが NetScaler ADM でライセンスされていることを検証します。
- ダブルホップのマルチホップパラメータ設定が有効になっていることを確認してください。
- ダブルホップ展開では、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連絡する前に

迅速に解決するには、Citrix テクニカルサポートに連絡する前に、次の情報があることを確認してください。

- 展開とネットワークポロジの詳細。
- NetScaler ADC と NetScaler ADM のバージョン。
- Citrix Virtual Apps and Desktops サーバーのバージョン。
- クライアント側レシーバーのバージョン。

- 問題が発生したときのアクティブな ICA セッションの数。
- NetScaler ADC コマンドプロンプトで `show techsupport` コマンドを実行して取得されたテクニカルサポートバンドル。
- NetScaler ADM 用にキャプチャされた技術サポートバンドル。
- すべての NetScaler ADC でキャプチャ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'`  
、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 テーブル内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 ADC リリースノートを参照してください。

## Gateway Insight

February 6, 2024

NetScaler Gateway 展開では、ユーザーのアクセス詳細を可視化することは、アクセス障害の問題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は、ユーザーがいつ Citrix Gateway にログオンできないか、ユーザーのアクティビティとログオンが失敗した理由を知りたいと考えています。この情報は通常、ユーザーが解決のリクエストを送信しない限り入手できません。

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。あらゆる期間を対象にして、すべての有効なユーザーの一覧、アクティブユーザーの数、アクティブセッションの数、ユーザー全体によって使用されたバイト数とライセンス数を表示できます。ユーザーごとの EPA (End Point Analysis: エンドポイント分析)、認証、SSO (Single Sign On: シングルサインオン)、アプリケーション起動のエラーを表示できます。また、ユーザーごとのアクティブセッションと終了したセッションの詳細を表示できます。

さらに、Gateway Insight は、仮想アプライアンスのアプリケーション起動エラーの理由に関する情報を提供します。これは、あらゆる種類のログオンまたはアプリケーション起動におけるエラーの問題のトラブルシューティングに役立ちます。起動されたアプリケーションの数、アクティブなセッションの合計数、合計バイト数、アプリケーションが消費した帯域幅を表示できます。アプリケーションごとのユーザー、セッション、帯域幅、起動のエラーの詳細を表示できます。

Citrix Gateway アプライアンスに関連付けられているすべての Gateway が使用している Gateway の数、アクティブなセッションの数、合計バイト数、および帯域幅をいつでも表示できます。ゲートウェイごとの EPA、認証、SSO、アプリケーション起動のエラーについて表示できます。また、ゲートウェイに割り当てられたすべてのユーザーの詳細と、ユーザーのログオンアクティビティを表示できます。

すべてのログメッセージは NetScaler ADM データベースに保存されるため、いつでもエラーの詳細を表示できます。また、ログオンエラーの概要を表示して、エラーが発生したログオンプロセスの段階を特定できます。

### 注意事項

- Gateway Insight は次の展開においてサポートされています。
  - Access Gateway
  - Unified Gateway
- NetScaler ADM のリリースおよびビルドは、NetScaler Gateway アプライアンスのリリースおよびビルドと同じかそれ以降である必要があります。
- アドバンスライセンスを持つ NetScaler ADC インスタンスについては、1 時間の Gateway Insight レポートを表示できます。プレミアムライセンスは、1 時間を超えると Gateway Insight レポートを閲覧することが必須です。

### 制限事項

- 認証方法が証明書ベースの認証として構成されている場合、NetScaler Gateway Gateway は Gateway Insight をサポートしません。
- Gateway Insight レポートの場合、NetScaler ADC アプライアンスから地理的位置情報は提供されません。
- 仮想 ICA アプリケーションおよびデスクトップに関する成功したユーザーログオン、遅延、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確認できます。
- ダブルホップモードでは、2 つ目の DMZ にある Citrix Gateway アプライアンスの障害を確認できません。
- RDP (Remote Desktop Protocol: リモートデスクトッププロトコル) のデスクトップアクセスの問題は報告されません。
- Gateway Insight は次の認証タイプでサポートされています。これら以外の認証タイプが使用されている場合、Gateway Insight に不一致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

## Gateway Insight の有効化

Citrix Gateway アプライアンスで Gateway インサイトを有効にするには、まず Citrix Gateway アプライアンスを Citrix ADM に追加する必要があります。次に、VPN アプリケーションを代表する仮想サーバー向けに AppFlow を有効にしてください。Citrix ADM へのデバイスの追加について詳しくは、「デバイスの追加」を参照してください。

### 注

NetScaler ADM でエンドポイント分析 (EPA) の障害を表示するには、NetScaler Gateway アプライアンスで AppFlow の認証、承認、および監査ユーザー名のログ記録を有効にする必要があります。

Gateway Insight を有効にする手順は、NetScaler ADM が **13.0 Build 36.27** の場合に適用されます。

1. [ **\*\* ネットワーク** ] > [ インスタンス ] に移動し、AppFlow を有効にするインスタンスを選択します。 **\*\***
2. [ アクションの選択 ] リストから、[ **Analytics** の設定 ] を選択します。
3. [ **Insight** の構成 ] ページの [ **Analytics** 構成 ] で、[ **NetScaler Gateway** ] を選択します。
4. 仮想サーバーを選択し、「**AppFlow** を有効にする」をクリックします。
5. [ **AppFlow** を有効にする ] 画面の [ 式の選択 ] ボックスの一覧で、[ true ] をクリックします。
6. [ トランスポートモード ] の横にある [ ログストリーム ] チェックボックスをオンにします。

### 注

転送モードとして **IPFIX** または **Logstream** のいずれかを選択できます。

**IPFIX** とログストリームの詳細については、「ログストリームの [概要](#)」を参照してください。

7. [ **OK** ] をクリックします。

## NetScaler ADM バージョン **13.0** ビルド **41.x** 以降の場合

1. [ ネットワーク ] > [ インスタンス ] に移動し、インスタンスを選択します。
2. [ アクションの選択 ] リストから、[ **Analytics** の設定 ] を選択します。
3. 仮想サーバーを選択し、「分析を有効にする」をクリックします。
4. 「詳細オプション」の下:
  - a) ログストリームを選択
  - b) **Citrix Gateway** を選択してください
5. [ **OK** ] をクリックします。

**GUI** を使用して **NetScaler Gateway** アプライアンスで **AppFlow** 認証、承認、および監査ユーザー名ログを有効にする

1. [構成] > [システム] > [AppFlow] > [設定] に移動し、[AppFlow 設定の変更] をクリックします。
2. [AppFlow 設定の構成] 画面で、[AAA ユーザ名] を選択し、[OK] をクリックします。

## Gateway Insight レポートの表示

Citrix ADM では、Citrix Gateway アプライアンスに関連するすべてのユーザー、アプリケーション、および Gateway 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 Gateway の詳細を表示できます。「概要」セクションでは、EPA、SSO、認証、およびアプリケーション起動の失敗を表示できます。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の概要、クライアントの種類、時間ごとのログオンしたユーザーの数を表示することもできます。

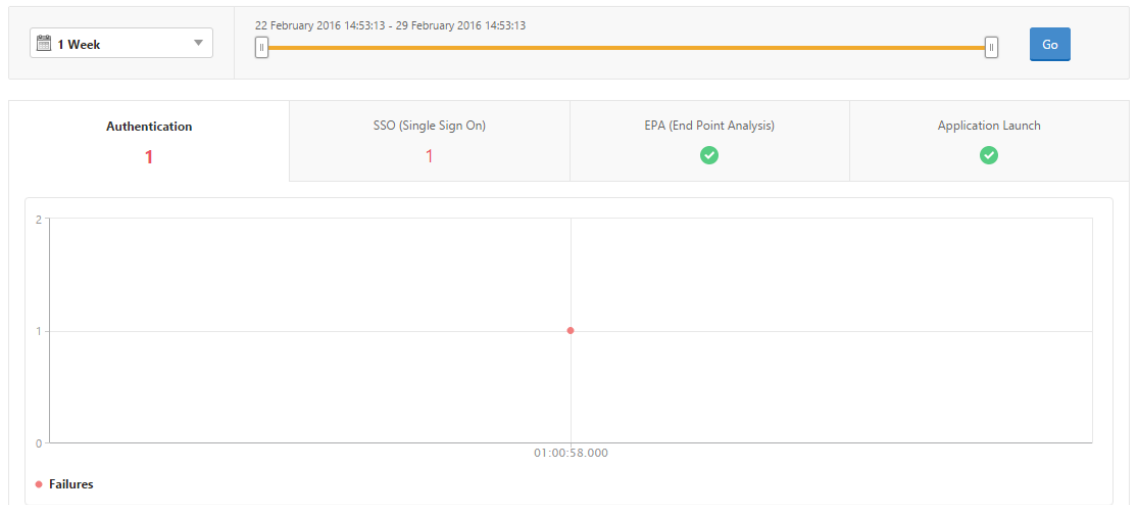
### 注

グループを作成するときに、グループにロールを割り当てたり、グループへのアプリケーションレベルのアクセスを提供したり、ユーザーをグループに割り当てることができます。NetScaler ADM 分析では、仮想 IP アドレススペースの認証がサポートされるようになりました。ユーザーは、権限のあるアプリケーション（仮想サーバー）のみのすべての Insight のレポートを表示できるようになりました。グループ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、「[グループを設定する](#)」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の起動の失敗を表示するには**

1. NetScaler ADM で、[Analytics] > [Gateway Insight] に移動します。
2. ユーザーの詳細を表示する期間を選択します。時間スライダーを使用して選択する期間をカスタマイズできます。[Go] をクリックします。
3. [EPA (End Point Analysis)], [Authentication], [Authorization], [SSO (Single Sign On)], [Application Launch] タブのいずれかをクリックして、エラーの詳細を表示します。

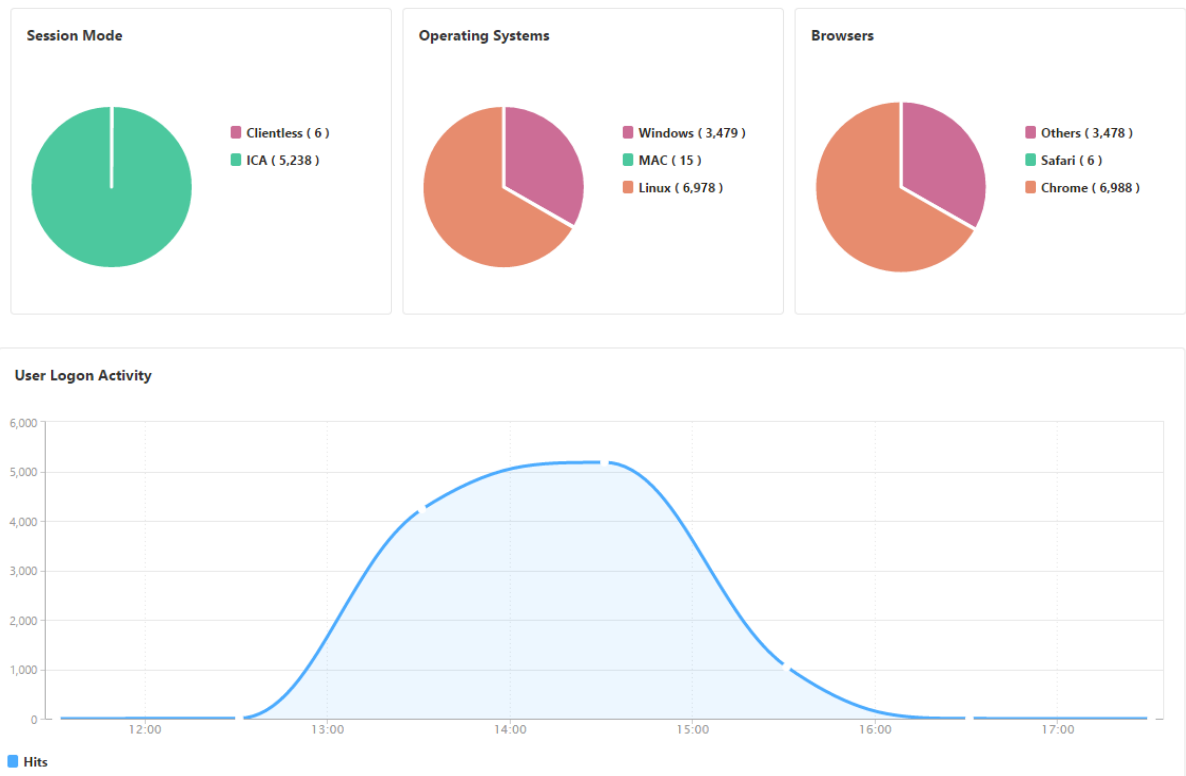
### Overview



セッションモード、クライアント、ユーザーの数の概要を表示するには

NetScaler ADM で、[ **Analytics** ] > [ **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。

### General Summary



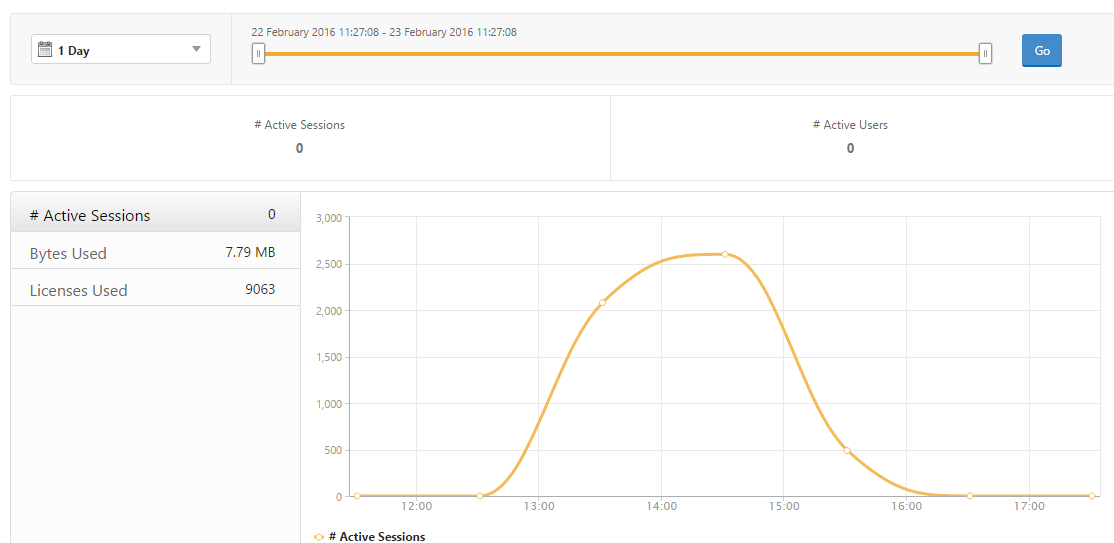
## ユーザーの **Gateway Insight** レポートの表示

次のレポートを表示できます。

- NetScaler Gateway アプライアンスに関連付けられているすべてのユーザー。
- ユーザーの EPA、認証、SSO、およびアプリケーションの起動の失敗。
- 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。
- フルトンネル、クライアントレス VPN、ICA プロキシなどのセッションモードのタイプ。

ユーザーの詳細を表示するには

1. Citrix ADM で、[分析] > [**Gateway** インサイト] > [ユーザー] に移動します。
2. ユーザーの詳細を表示する期間を選択します。時間スライダーを使用して選択する期間をカスタマイズできます。[Go] をクリックします。
3. 期間中にすべてのユーザーが使用したアクティブユーザー数、アクティブなセッション数、バイト数、ライセンスを表示できます。

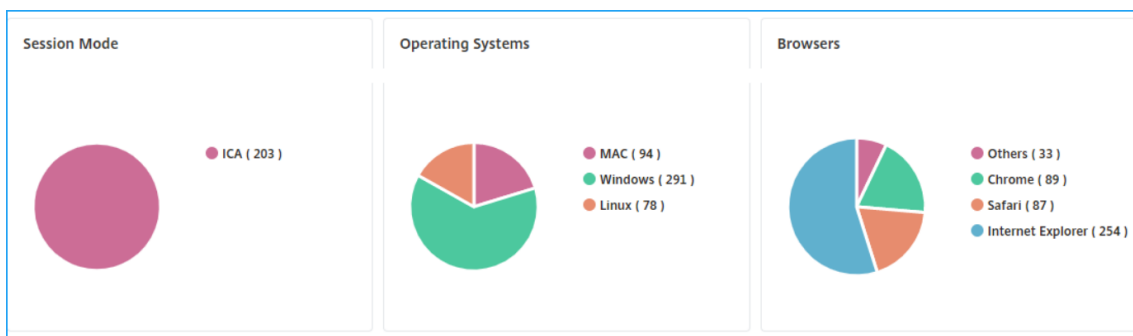


下にスクロールすると、有効なユーザーとアクティブユーザーの一覧が表示されます。

Users		Active Users	
User Name	Total Bytes	# Sessions Used	
user1	191.94 KB	11	
user10	0	4	
user100	2.81 KB	4	
user1000	42.66 KB	5	
user1001	2.11 KB	4	
user1002	4.22 KB	4	
user1003	4.22 KB	4	

[ユーザー] または [アクティブなユーザー] タブで、ユーザーをクリックして、次のユーザーの詳細を表示します。

- ユーザーの詳細 -ADC Gateway アプライアンスに関連付けられた各ユーザーのインサイトを表示できます。[分析]>[Gateway Insight]>[ユーザー]に移動し、ユーザーをクリックして、セッションモード、オペレーティングシステム、ブラウザーなど、選択したユーザーのインサイトを表示します。

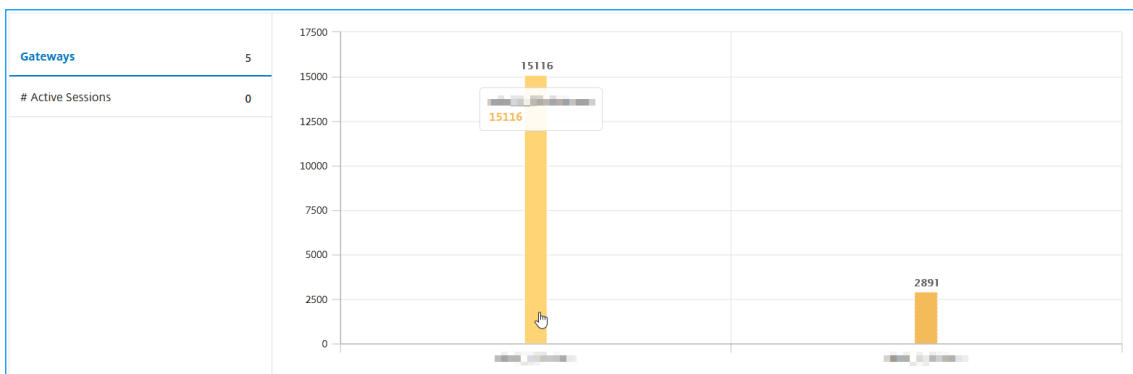


- 選択した Gateway のユーザーとアプリケーション-[Analytics]>[Gateway Insight]>[Gateway]に移動し、Gateway ドメイン名をクリックして、選択した Gateway に関連付けられている上位 10 のアプリケーションと上位 10 人のユーザーを表示します。



- アプリケーションとユーザーの表示オプション-10 を超えるアプリケーションおよびユーザーの場合、[アプリケーションとユーザー]の[詳細]アイコンをクリックすると、選択したゲートウェイに関連付けられているすべてのユーザーとアプリケーションの詳細を表示できます。
- 棒グラフをクリックして詳細を表示-棒グラフをクリックすると、関連する詳細を表示できます。たとえば、[アナリティクス]>[Gateway Insight]>[Gateway \*\*]の順に選択し、Gateway の棒グラフをクリックして Gateway の詳細を表示します。





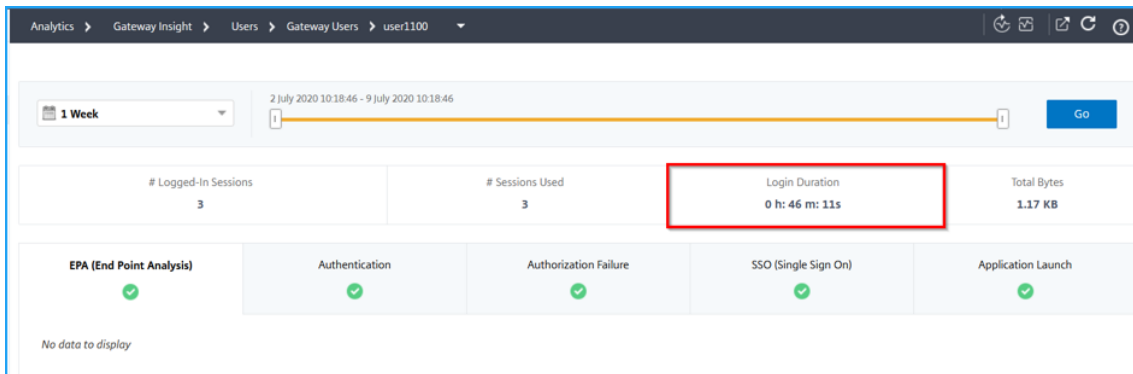
- ユーザーのアクティブセッションと終了したセッション。

Active Sessions								
GATEWAY SESSION ID	SESSION TYPE	GATEWAY DOMAIN NAME	GATEWAY IP ADDRESS	BANDWIDTH	TOTAL BYTES	OS	CLIENT IP ADDRESS	STATUS
31353934-3231-3533-3938-2e3730383935	Full Tunnel		10.102.1.23	4 bps	200 bytes	--		7

Total 1

Terminated Sessions								
GATEWAY SESSION ID	SESSION TYPE	GATEWAY DOMAIN NAME	GATEWAY IP ADDRESS	BANDWIDTH	TOTAL BYTES	OS	CLIENT IP ADDRESS	LOGOUT REASON
No items								

- アクティブセッションのゲートウェイドメイン名とゲートウェイの IP アドレス。
- ユーザーのログイン時間。



- 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。
  - セッションのタイムアウト
  - 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がタイムアウトした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

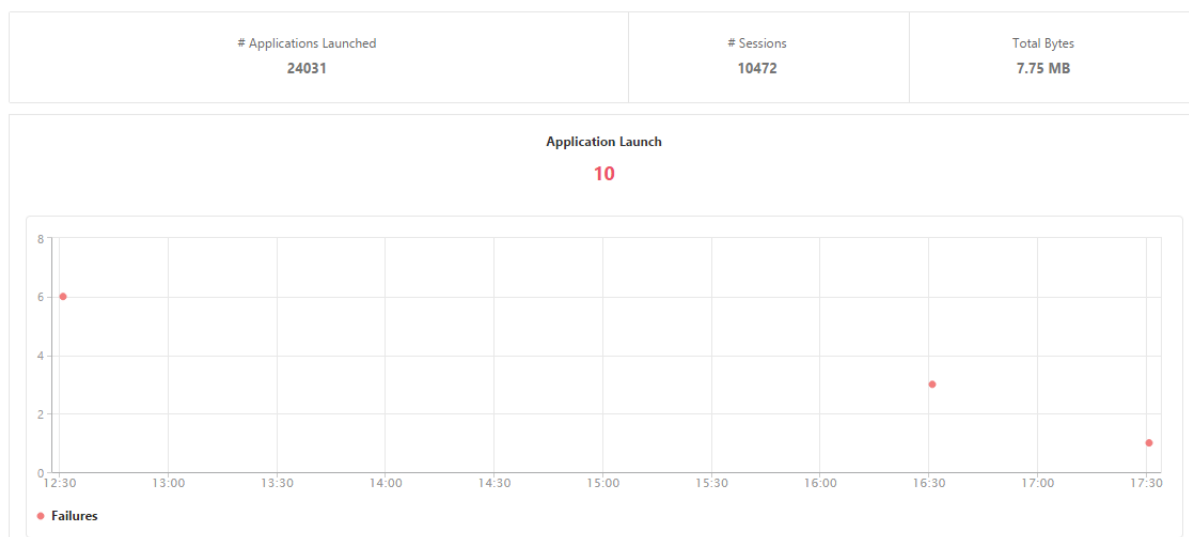
## アプリケーションの Gateway Insight レポートの表示

起動されたアプリケーション数、アクティブなセッションの合計数、合計バイト数、アプリケーションが消費した帯域幅を表示できます。アプリケーションごとのユーザー、セッション、帯域幅、起動のエラーの詳細を表示できます。

アプリケーションの詳細を表示するには

1. NetScaler ADM で、[分析] > [Gateway Insight] > [アプリケーション] に移動します。
2. アプリケーションの詳細を表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。[Go] をクリックします。

起動されたアプリケーション数、アクティブなセッションの合計数、合計バイト数、アプリケーションが消費した帯域幅を表示できるようになりました。



下にスクロールすると、ICA とその他のアプリケーションによって使用されたセッション数、帯域幅、合計バイト数が表示されます。

ICA Applications		Other Applications		
Name	# Sessions	Bandwidth	Total Bytes	
10.102.61.249	3972	52 bps	3.79 MB	
c-go-mpulse.net	2	0 bps	1.53 KB	
cdn.kendostatic.com	1	0 bps	805	
code.jquery.com	1	0 bps	1.51 KB	
engtools.citrite.net	2	0 bps	160	
onebug.citrite.net	2	1 bps	86.21 KB	

[その他のアプリケーション] タブで、[名前] 列で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を表示できます。

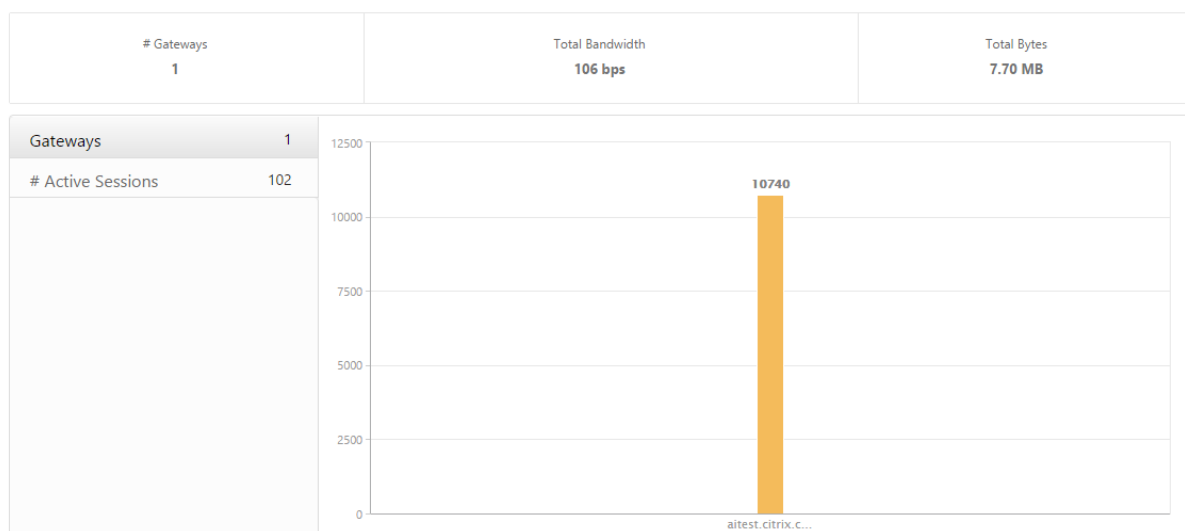
## Gateway の Gateway Insight レポートの表示

Citrix Gateway アプライアンスに関連付けられているすべての Gateway が使用している Gateway の数、アクティブなセッションの数、合計バイト数、および帯域幅をいつでも表示できます。ゲートウェイごとの EPA、認証、SSO、アプリケーション起動のエラーについて表示できます。また、ゲートウェイに割り当てられたすべてのユーザーの詳細と、ユーザーのログオンアクティビティを表示できます。

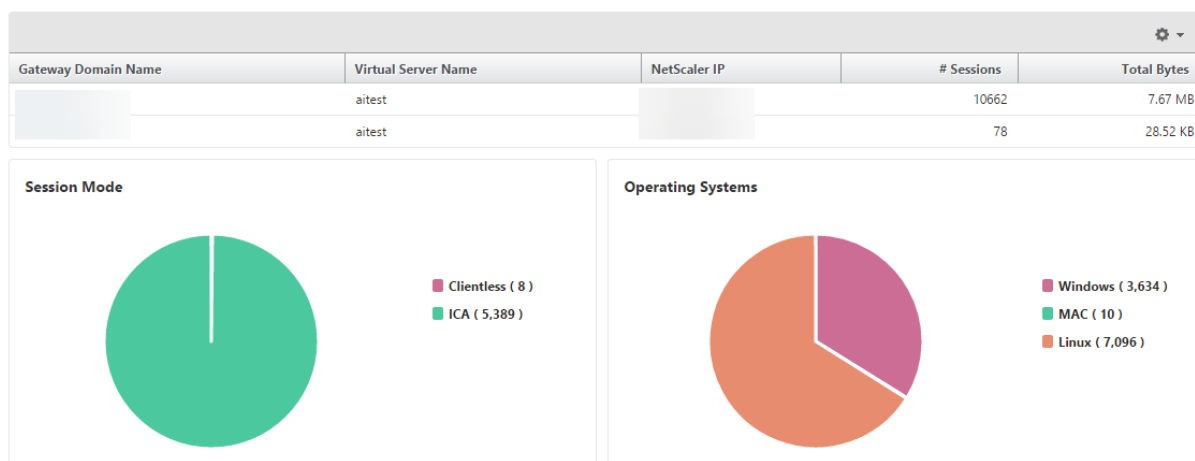
ゲートウェイの詳細を表示するには

1. **Citrix ADM** で、[分析] > [**Gateway** インサイト] > [**Gateway**] 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。時間スライダーを使用すると、選択した期間をさらに調整できます。[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たすべての Gateway で使用された Gateway 数、アクティブセッション数、合計バイト数、帯域幅をいつでも表示できるようになりました。



下にスクロールすると、Gateway 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 Gateway の詳細が表示されます。



「Gateway **Domain Name**」列で **G** ateway をクリックすると、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 Gateway に関するその他の詳細を表示できます。

### 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 レポートは、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、指定された電子メールアドレスへのレポートのエクスポートを、さまざまな間隔でスケジュール設定することができます。

#### 注

- 読み取り専用アクセス権のユーザーは、レポートをエクスポートすることができません。
- 地理地図レポートは、NetScaler ADM がインターネットに接続されている場合にのみエクスポートされます。

レポートをエクスポートするには、次の手順に従います

- [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。
- [今すぐエクスポート] で、必要な形式を選択し、[エクスポート] をクリックします。

エクスポートをスケジュールするには:

- [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。
- [エクスポートのスケジュール] で詳細を指定し、[スケジュール] をクリックします。

電子メールサーバーまたは電子メール配布リストを追加するには、次の手順を実行します。

- [構成] タブで、[システム] > [通知] > [電子メール] に移動します。
- 右側のペインで、[電子メールサーバー] を選択して電子メールサーバーを追加するか、[電子メール配布リスト] を選択して電子メール配布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] で [PDF 形式] を選択し、[エクスポート] をクリックします。

## Gateway Insight のユースケース

次のユースケースは、Gateway Insight を使用して、NetScaler Gateway アプライアンス上のユーザーのアクセスの詳細、アプリケーション、および Gateway を可視化する方法を示しています。

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

あなたは Citrix ADM を介して Citrix Gateway アプライアンスを監視している Citrix Gateway 管理者であり、ユーザーがログインできない理由や、ログインプロセスのどの段階で障害が発生したかを確認したいと考えています。

NetScaler ADM では、ログインプロセスの次の段階でユーザーログインエラーの詳細を表示できます。

- 認証
- エンドポイント分析 (EPA)
- シングルサインオン

NetScaler ADM では、特定のユーザーを検索して、そのユーザーの詳細をすべて表示できます。

ユーザーを検索するには、次の手順に従います。

Citrix ADM で、[分析] > [Gateway インサイト] に移動し、[ユーザーの検索] テキストボックスで検索するユーザーを指定します。

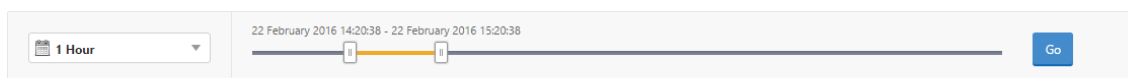
### 認証の失敗

資格情報が正しくない、または認証サーバーから応答がないなどの認証エラーについて確認できます。認証が失敗した要因も確認できます。

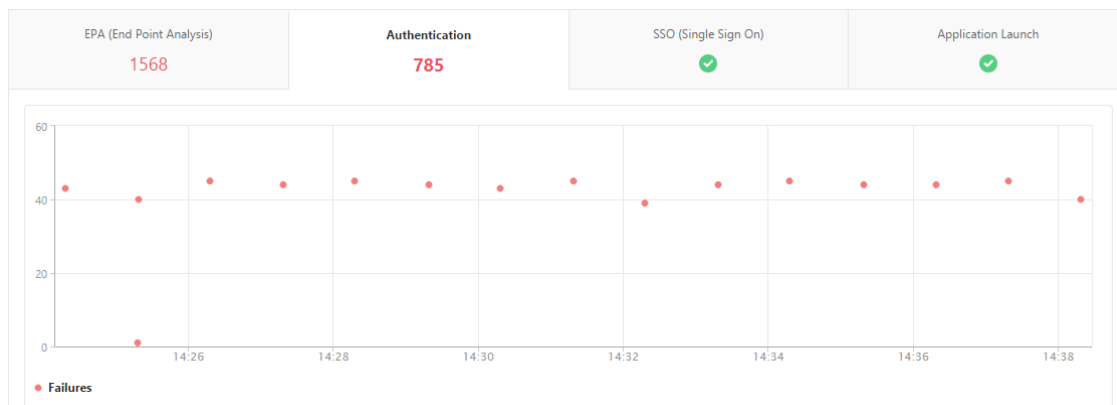
認証失敗の詳細を表示する手順は、次のとおりです。

1. NetScaler ADM で、[Analytics] > [Gateway Insight] に移動します。
2. [概要] セクションで、認証エラーを表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。[Go] をクリックします。

#### Overview



3. [ 認証 ] タブをクリックします。特定の時点での認証エラーの数は、「失敗」グラフでいつでも確認できます。



そのタブのまま下にスクロールすると、**Username**、**Client IP Address**、**Error Time**、**Authentication Type**、**Authentication Server IP Address** などの各認証エラーの詳細を表で確認できます。表の [ エラーの説明 ] 列にはログインに失敗した理由が表示され、[ 状態 ] 列には失敗が発生した n 番目の要因が表示されます。

IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR TIME	ERROR DESCRIPTION	ERROR COUNT	STATE	AUTHEN
183	vpnserver		15/03/2019, 06:30:04	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	3	2nd Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	1	2nd Factor	RADIUS
111	vpnvip		19/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	3	1st Factor	LDAP
183	vpnserver		13/04/2019, 06:30:28	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Account is disabled	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	Local
183	vpnserver		12/04/2019, 06:30:13	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Bad(format) password passed to nsaaad	5	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	4	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	22	1st Factor	RADIUS
i:88	_XD_10.217.205.88_443		15/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP

[ **Username** ] 列で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を表示できます。設定アイコンを使用して、テーブルをカスタマイズして列を追加または削除できます。

### EPA エラー

EPA の失敗は、認証前または認証後の段階で表示できます。

**重要:**

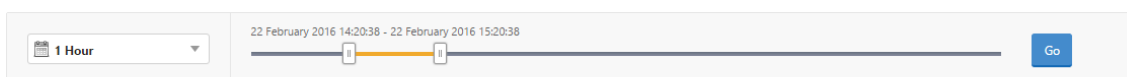
- EPA の失敗は、クラシック式が設定されている場合にのみ報告されます。

- 事前認証ポリシーまたは認証後ポリシーで高度な式が設定されている場合、EPA の失敗は報告されません。
- EPA が nFactor 認証フローの要素の 1 つとして構成されている場合、EPA の失敗は報告されません。

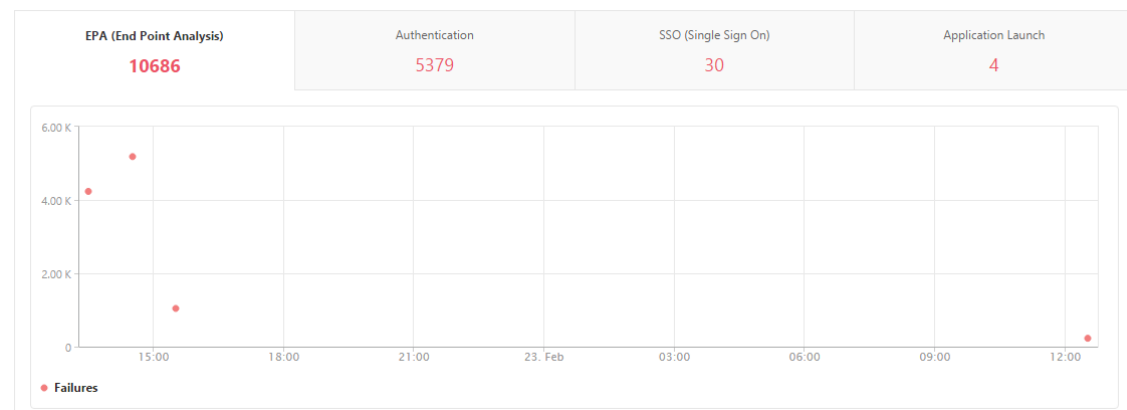
EPA 障害の詳細を表示するには、次の手順に従います。

1. NetScaler ADM で、[ **Analytics** ] > [ **Gateway Insight** ] に移動します。
2. [ **Overview** ] セクションで EPA エラーを表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。[ **Go** ] をクリックします。

**Overview**



3. [ **EPA (終点解析)** ] タブをクリックします。特定の時点における EPA エラーの数は、障害 グラフで表示できます。



そのタブのまま下にスクロールすると、**Username**、**NetScaler IP Address**、**Gateway IP Address**、**VPN**、**Error Time**、**Policy Name**、**Gateway Domain Name** などの各 EPA エラーの詳細を表で確認できます。表の [ **Error Description** ] 列には EPA エラーの理由が記載されており、[ **Policy Name** ] 列にはエラーの原因となったポリシーが示されています。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

[ **Username** ] 列で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を表示できます。下向き矢印を使用して、テーブルをカスタマイズして列を追加または削除できます。

注

「ClientSecurity」式がVPNセッションポリシールールとして構成されている場合、NetScaler GatewayはEPAの失敗を報告しません。

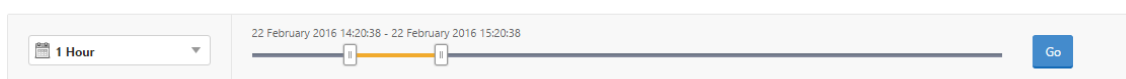
**SSO** の障害

Citrix 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すべての SSO 障害を任意の段階で表示できます。

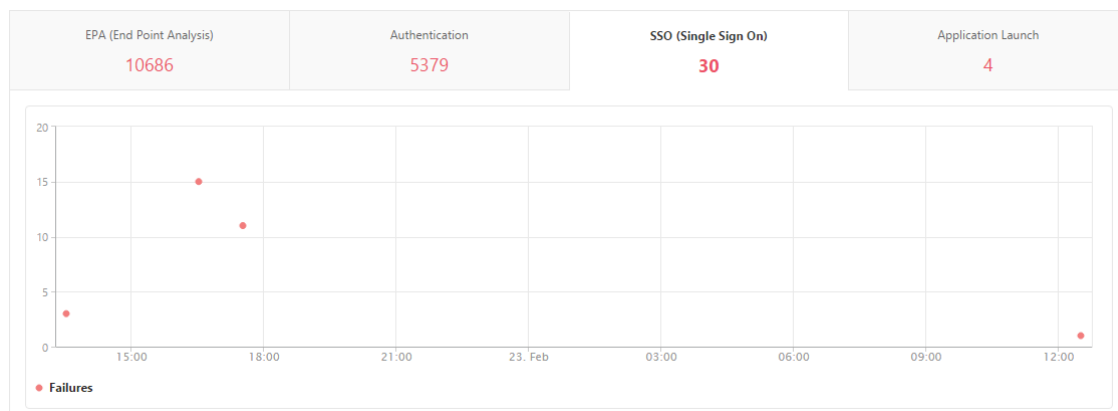
**SSO** 障害の詳細を表示するには、次の手順に従います。

1. NetScaler ADM で、[ **Analytics** ] > [ **Gateway Insight** ] に移動します。
2. [ **Overview** ] セクションで SSO エラーを表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。[ **Go** ] をクリックします。

**Overview**



3. [ **SSO (シングルサインオン)** ] タブをクリックします。特定の期間における SSO エラーの数が、[ **Failures** ] のグラフに表示されます。



そのタブのまま下にスクロールすると、**Username**、**NetScaler IP Address**、**Error Time**、**Error Description**、**Resource Name** などの各 SSO エラーの詳細を表で確認できます。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com



[Username] カラムでユーザをクリックすると、そのユーザの SSO エラーやその他の詳細を表示できます。下向きの矢印を使用して、テーブルをカスタマイズして列を追加または削除できます。

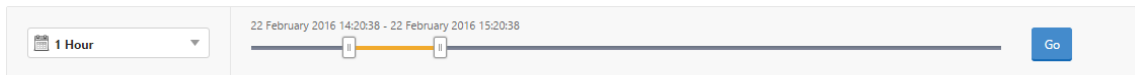
**NetScaler Gateway** に正常にログオンした後、ユーザーは仮想アプリケーションを起動できない

アプリケーションの起動に失敗した場合、Secure Ticket Authority (STA) または Citrix Virtual App Server にアクセスできない、または STA チケットが無効であるなどの原因を可視化できます。エラーの時間や詳細、STA 検証ができなかったリソースについて確認できます。

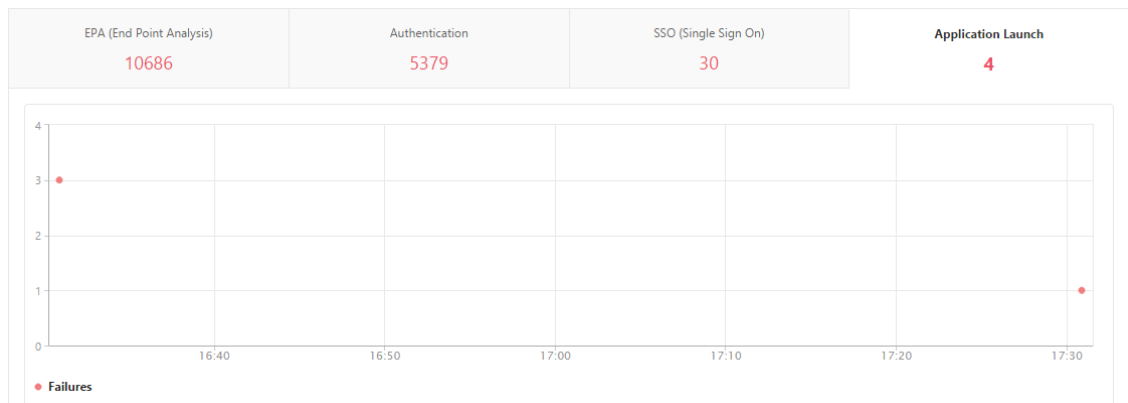
アプリケーションの起動失敗の詳細を表示するには、次の手順に従います。

1. NetScaler ADM で、[ **Analytics** ] > [ **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。時間スライダーを使用すると、選択した期間をさらに調整できます。[ **Go** ] をクリックします。

**Overview**



3. [ **アプリケーションの起動** ] タブをクリックします。[ **失敗** ] グラフでは、任意の時点でのアプリケーション起動の失敗数を表示できます。



そのタブのまま下にスクロールすると、**NetScaler IP Address**、**Error Time**、**Error Description**、**Resource Name**、**Gateway Domain Name** などの各アプリケーション起動エラーの詳細を表で確認できます。表の [ **Error Description** ] 列には STA サーバーの IP アドレスが、[ **Resource Name** ] 列には STA 検証ができなかったリソースの詳細が表示されています。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

[Us ername] 列でユーザーをクリックすると、アプリケーションの起動エラーとそのユーザーのその他の詳細を表示できます。下向きの矢印を使用して、テーブルをカスタマイズして列を追加または削除できます。

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

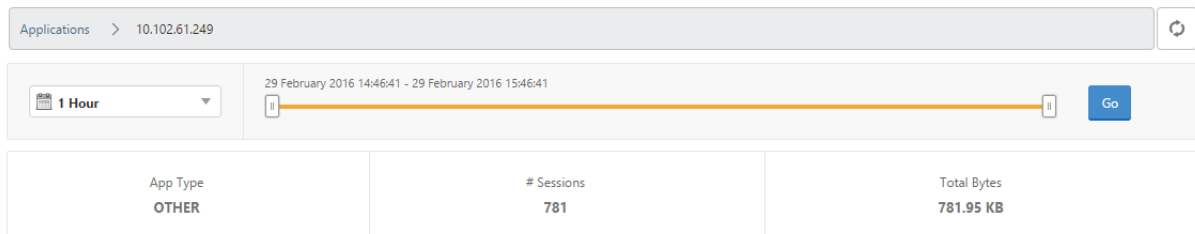
新しいアプリケーションを正常に起動したら、NetScaler ADM で、そのアプリケーションによって消費された合計バイト数と帯域幅を表示できます。

アプリケーションによって消費された合計バイト数と帯域幅を表示するには、次の手順を実行します。

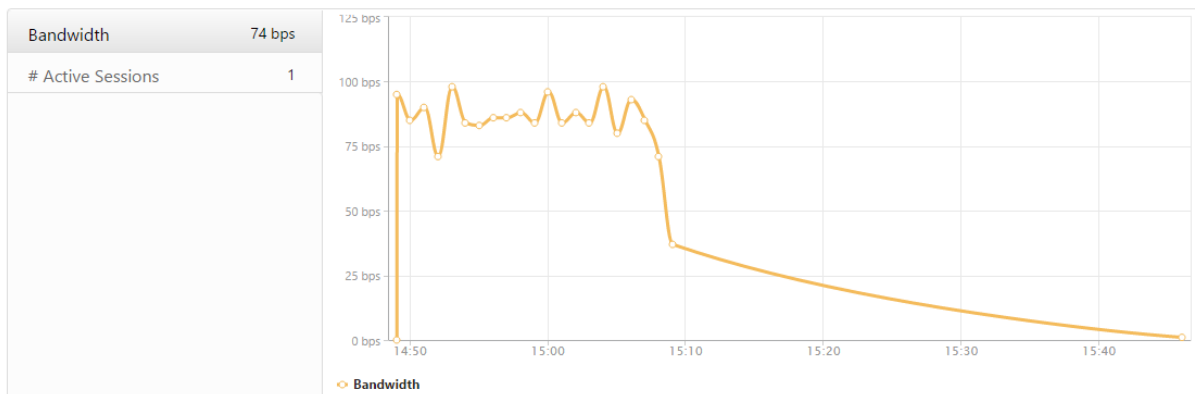
NetScaler ADM で、[ **Analytics** ] > [ **Gateway Insight** ] > [ アプリケーション ] に移動し、下にスクロールして、[ その他のアプリケーション ] タブで詳細を表示するアプリケーションをクリックします。

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.134	1	0 bps	12.19 KB
10.102.61.249	4	0 bps	82.32 KB
alt1-safebrowsing.google.com	1	0 bps	1.04 KB
bcwhwkevnw	1	0 bps	1.98 KB
bcwhwkevnw.citrite.net	1	0 bps	1.01 KB

そのアプリケーションが使用したセッション数と合計バイト数が表示されます。



そのアプリケーションが使用した帯域幅も表示されます。



ユーザーが **NetScaler Gateway** に正常にログオンしたが、内部ネットワークの特定のネットワークリソースにアクセスできない

Gateway Insight では、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特定できます。また、エラーの原因となったポリシーの名前を確認できます。

リソースのユーザー・アクセスを表示するには、次の手順に従います。

1. Citrix ADM で、[分析] > [**Gateway** 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、[その他のアプリケーション] 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。

ICA Applications		Other Applications	
Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	2499	32 bps	2.36 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB
rock.citrite.net	1	0 bps	120

3. 下にスクロールすると、「ユーザー」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。

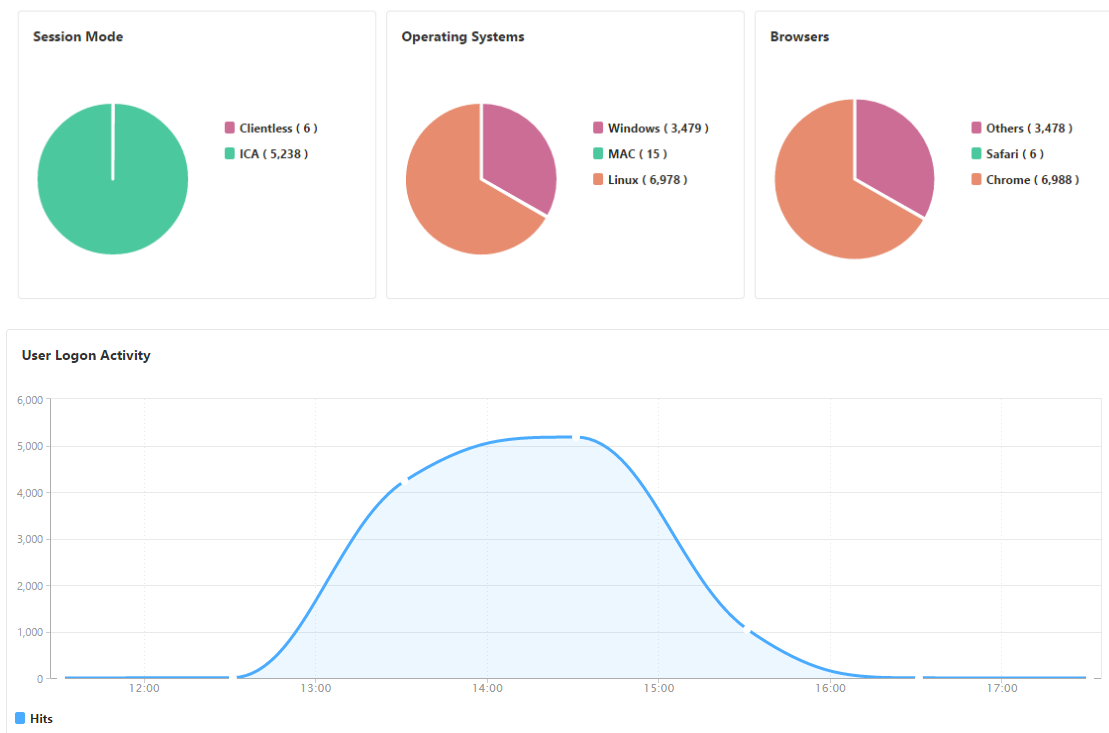
ユーザーが異なる **NetScaler Gateway** 展開環境を使用している場合や、異なるアクセスモードで **NetScaler Gateway** にログオンしている場合があります。管理者は、展開の種類とアクセスモードの詳細を表示する必要があります

Gateway Insight では、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の概要、クライアントの種類、時間ごとのログオンしたユーザー数を確認できます。また、ユーザーの展開が統合 Gateway 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。Unified Gateway の展開では、コンテンツスイッチ仮想サーバーの名前と IP アドレス、VPN 仮想サーバー名を確認できます。

セッション・モード、クライアントのタイプ、ログオンしたユーザー数の概要を表示するには、次の手順に従います。

1. NetScaler ADM で、[Analytics] > [Gateway Insight] に移動します。
2. [概要] セクションで、下にスクロールして、[セッションモード]、[オペレーティングシステム]、[ブラウザ]、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するために使用するさまざまなセッションモード、クライアントの種類、および 1 時間ごとにログオンしたユーザー数が表示されます。

## General Summary



## Gateway Insight の問題のトラブルシューティング

February 6, 2024

Gateway Insight ソリューションが期待どおりに機能しない場合は、次のいずれかに問題がある可能性があります。トラブルシューティングについては、各セクションのチェックリストを参照してください。

- Gateway Insight 設定。
- Citrix ADC と NetScaler ADM 間の接続に問題があります。
- NetScaler ADC でのレコード生成。
- NetScaler ADM での検証。

### Gateway Insight 設定チェックリスト

- NetScaler ADC アプライアンスで AppFlow 機能が有効になっていることを確認します。詳細については、「[AppFlow の有効化](#)」を参照してください。
- NetScaler ADC の実行構成で Gateway Insight 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 の設定を確認します。バインドタイプが REQUEST であることを確認します。たとえば、

```
1 bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
2 <!--NeedCopy-->
```

Gateway Insight には、バインドタイプ OTHERTCP\_REQUEST も必要です。

```
1 bind vpn vserver afsanity -policy afp -priority 100 -type
  OTHERTCP_REQUEST
2 <!--NeedCopy-->
```

- シングルホップ、アクセスゲートウェイ、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ます。詳しくは、[HDX Insight データ収集の有効化を参照してください](#)。
- ダブルホップの場合、Gateway Insight は両方のホップで構成する必要があります。
- NetScaler Gateway/VPN 仮想サーバーの `appflowlog` パラメータをチェックします。詳しくは、「[仮想サーバーに対する AppFlow の有効化](#)」を参照してください。

### NetScaler ADC と NetScaler ADM の間の接続チェックリスト

- NetScaler ADC で AppFlow コレクタのステータスを確認します。詳しくは、「[NetScaler ADC と AppFlow Collector 間の接続状態を確認する方法](#)」を参照してください。
- Gateway Insight AppFlow ポリシーヒットをチェックします。

コマンド `show appflow policy <policy_name>` を実行して、AppFlow ポリシーのヒットをチェックします。

GUI で [システム] > [AppFlow] > [ポリシー] に移動して、AppFlow ポリシーのヒットを確認することもできます。

- 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を検証します。

### NetScaler ADC チェックリストでのレコード生成

- `nsconmsg -d stats -g ai_tot` コマンドを実行し、NetScaler ADC で統計値の増分を確認します。
- `nstrace logs` をキャプチャして CFLOW パケットをチェックし、NetScaler ADC が AppFlow レコードをエクスポートすることを確認します。

注:

`nstrace logs` は IPFIX にのみ必要です。Logstream の場合、`nstrace logs` ログは ADC アプライアンスが AppFlow レコードをエクスポートしたかどうかを確認しません。

## NetScaler ADM でのレコードの検証

- `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` コマンドを実行して、ログをチェックして、NetScaler ADM が AppFlow レコードを受信していることを確認します。
- NetScaler ADC インスタンスが NetScaler ADM に追加されていることを確認します。
- NetScaler Gateway/VPN 仮想サーバーが NetScaler ADM でライセンスされていることを確認します。

## NetScaler ADM でのログストリームログの検証

NetScaler ADM が受信したログストリームデータの検証は、次の方法を使用して実行できます。

- **NetScaler ADM** でのデータレコードログの有効化  
有効にすると、ログは `/var/mps/log/mps_afdecoder.log` で確認できます
- **ULFD** ライブラリロギングの有効化  
コマンド `/mps/decoder_enable_debug` を実行する  
ログは `/var/ulfdlog/libulfd.log` にキャプチャされます  
ログを無効にするには、`/mps/decoder_disable_debug` コマンドを使用します。

## Gateway Insight カウンタ

次の Gateway Insight カウンタを使用できます。

- `ai_tot_preauth_epa_export`
- `ai_tot_auth_export`
- `ai_tot_auth_session_id_update_export`
- `ai_tot_postauth_epa_export`
- `ai_tot_vpn_update_export`
- `ai_tot_ica_fileinfo_export`
- `ai_tot_app_launch_failure`
- `ai_tot_logout_export`
- `ai_tot_skip_appflow_export`
- `ai_tot_sso_appflow_export`
- `ai_tot_authz_appflow_export`
- `ai_tot_appflow_pol_eval_failure`
- `ai_tot_vpn_export_state_mismatch`
- `ai_tot_appflow_disabled`
- `ai_tot_appflow_pol_eval_in_gwinsight`
- `ai_tot_app_launch_success`

**NetScaler ADC** ログ内の **AppFlow** レコード

リリース 13.0 ビルド 71.x から、NetScaler ADC ログをチェックして、AppFlow レコードがエクスポートされているかどうかを確認できます。syslogparamsのデフォルトのログレベルでは、すべてのエラーログと情報ログがキャプチャされます。エラーに関する手がかりが見つからない場合は、syslogparamsのDEBUGを含むすべてのログレベルを有効にして、DEBUG ログもキャプチャします。

## サンプルログ

```

1 <local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 147 0 : "
  GwInsight: Sent auth record Func=ns_sslvpn_export_auth_data Username
=<name> Clientip=<ip>:<port> Destip=0:80 SessSeq=0 Sessid=<sessid>
Gwip=<ip>:443 StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<
vpnfqdn> Authtype=3 EPAid=(null) AuthStage=1 AuthDuration=309
AuthAgent=<auth_server_ip> Groupname= Policyname=<name>
CurfactorPolname=<name> NextfactorPolname= CSecExpr= Devicetype
=16777219 Deviceid=0 email="
2 <local0.err> ... GMT 0-PPE-0 : default SSLVPN Message 143 0 : "GwInsight
: Func=ns_aaa_copy_email_id_to_vpn_record input hash_attrs_len is
zero"
3 <local0.err> ... GMT 0-PPE-0 : default SSLVPN Message 148 0 : "GwInsight
: Func=update_session_appflow_collector pcb or session is NULL"
4 <local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 165 0 : "
  GwInsight: Sent session update record Func=
ns_sslvpn_send_update_record Username=<> Clientip=<ip>:<port> Destip
=<ip>:80 SessSeq=1 Sessid=<sessid> Gwip=<ip>:443 StatusCode=0
CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=0 SessState
=2 SessMode=2 IIP=0 AppByteCount=0 ReqURL=/Citrix/Store
5 Web BackendServername= SSUrl= email="
6 SSO logs:
7 <!--NeedCopy-->

```

```

1 <local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 463 0 : "
  GwInsight: Sent session update record Func=
ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
=150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=1
SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
BackendServername=<> SSUrl= email="
2 <!--NeedCopy-->

```

```

1 <local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 582 0 : "
  GwInsight: Sent session update record Func=
ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
=150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=3
SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
BackendServername=<> SSUrl= email="
2 <!--NeedCopy-->

```

```

1 <local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 513 0 : "
  GwInsight: Sent session update record Func=
  ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
  Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
  =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=2
  SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
  BackendServername=<> SSUrl= email="
2 <!--NeedCopy-->

```

```

1 <local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 29796 0 : "
  GwInsight: Sent session update record Func=
  ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
  Destip=<ip>:443 SessSeq=c Sessid=<sessid> Gwip=<ip>:443 StatusCode
  =155 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=6
  SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
  BackendServername=<> SSUrl= email="
2 <!--NeedCopy-->

```

## Citrix テクニカルサポートに問い合わせてください

迅速に解決するには、Citrix テクニカルサポートに連絡する前に、次の情報があることを確認してください。

- 展開とネットワークポロジの詳細。
- NetScaler ADC と NetScaler ADM のバージョン。
- NetScaler ADC および NetScaler ADM のテクニカルサポートバンドル。
- `nstrace` は問題発生中にキャプチャします。

## 既知の問題

ゲートウェイインサイトに関する既知の問題については、NetScaler ADC リリースノートを参照してください。

## Security Insight

February 6, 2024

### 注

NetScaler ADM ビルドが **13.0-79.x** より前の場合は、[分析] > [セキュリティ] > [Security Insight] の順に選択して、セキュリティインサイトを表示できます。ビルド **13.0-79.x** 以降では、[分析] > [セキュリティ] > [セキュリティ違反] > [アプリケーションの概要] に移動し、[アプリケーションの内訳] の [WAF] をクリックすると、WAF 違反の詳細を表示できます。



インターネットに接続している Web アプリケーションや Web サービスアプリケーションの攻撃に対する脆弱性が高まってきています。アプリケーションを攻撃から保護するには、過去、現在の脅威、近い将来起こり得る脅威の性質と程度、攻撃発生時にすぐ利用できるリアルタイムデータ、対策に関する推奨事項を把握する必要があります。Security Insight は、アプリケーションのセキュリティ状況を判断し、是正処置を実施してアプリケーションを保護するための統一管理コンソールソリューションです。

### 注

セキュリティインサイトは、バージョン 11.0 ビルド 65.31 以降で動作する Citrix ADC アプライアンスを搭載した Citrix Application Delivery Management (ADM) でサポートされています。

## セキュリティインサイトの仕組み

Security Insight は、アプリケーションに関連するさまざまな脅威を把握できる直感的なダッシュボード型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 Citrix ADM に含まれており、アプリケーションファイアウォールと Citrix ADC システムの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。このレポートには、アプリケーション別に次の情報が含まれています。

- **脅威指数:** アプリケーションが Citrix ADC アプライアンスによって保護されているかどうかに関係なく、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の重大度が高いほど、そのアプリケーションの脅威指数は大きくなります。この指数の範囲は 1~7 です。

脅威指数は攻撃情報に基づいています。違反の種類、攻撃のカテゴリ、場所、クライアントの詳細などの、攻撃に関連する情報により、アプリケーションに対する攻撃について正確かつ詳細に把握できます。違反情報は、違反または攻撃が発生した場合にのみ NetScaler ADM に送信されます。多くの侵害や脆弱性は、高い脅威指数の値につながります。

- **安全性指数:** 外部から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 ADC インスタンスをどのように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小さいほど、安全性指数は高くなります。この指数の範囲は 1~7 です。

安全指標では、アプリケーションファイアウォール構成と NetScaler ADC システムセキュリティ構成の両方が考慮されます。高い安全性指数値を得るためには、両方の構成を堅牢にする必要があります。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行われていて、`nsroot` ユーザーの強力なパスワードなど、NetScaler ADC システムの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指数の値が割り当てられます。

- **アクションナブルインフォメーション:** 脅威指数を下げ安全指数を増やすために必要な情報。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、違反に関する情報、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に関する既存の、または欠落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割合を確認できます。

## セキュリティインサイトの設定

Citrix ADM は、アプリケーションファイアウォールが構成されているすべての Citrix ADC インスタンスからのセキュリティインサイトをサポートします。

ADC インスタンスでセキュリティインサイトを設定するには、まずアプリケーションファイアウォールプロファイルとアプリケーションファイアウォールポリシーを設定します。その後、アプリケーションファイアウォールポリシーをグローバルにバインドできますが、Citrix ではポリシーを仮想サーバーにバインドすることをお勧めします。

Citrix ADM で分析を表示するには、インスタンスで AppFlow 機能を有効にし、AppFlow コレクター、アクション、およびポリシーを構成し、ポリシーをグローバルにバインドします。この場合も、アプリケーションファイアウォールポリシーをグローバルにバインドできますが、Citrix ではポリシーを仮想サーバーにバインドすることをお勧めします。また、Citrix ADM を使用して AppFlow 構成を ADC インスタンスにデプロイすることも推奨しています。コレクタを構成するときは、レポートを監視する NetScaler ADM サーバーの IP アドレスを指定する必要があります。

**Citrix ADC** インスタンスでセキュリティインサイトを設定するには:

1. 次のコマンドを実行して、アプリケーションファイアウォールのプロファイルとポリシーを構成し、アプリケーションファイアウォールポリシーをグローバルに、または負荷分散仮想サーバーにバインドします。

---

```
add appfw profile <名前> \[*-defaults* ( basic advanced )]
```

名前 >

---

```
set appfw profile \<名前> \[-startURLAction \<開始 URL アクション> …\]
```

```
add appfw policy \<名前> \<規則> \<プロファイル名>
```

```
bind appfw global \<ポリシー名> \<優先度>
```

または、

```
bind lb vserver \<lb 仮想サーバー> -policyName \<ポリシー> -priority \<優先度>
```

```
1 add appfw profile pr_appfw -defaults advanced
2 set appfw profile pr_appfw -startURLAction log stats learn
3 add appfw policy pr_appfw_pol "HTTP.REQ.HEADER("Host").EXISTS"
  pr_appfw
4 bind appfw global pr_appfw_pol 1
5 or,
6 bind lb vserver outlook -policyName pr_appfw_pol -priority "20"
7 <!--NeedCopy-->
```

2. 次のコマンドを実行して AppFlow 機能を有効化し、AppFlow コレクター、アクション、ポリシーを構成し、そのポリシーをグローバルに、または負荷分散仮想サーバーにバインドします。

```
add appflow collector \<名前> -IPAddress \<IP アドレス>
```

```
set appflow param DISABLED ]]
```

```
[-SecurityInsightRecordInterval <秒>]
```

```
\[**-SecurityInsightTraffic** ( ENABLED 秒 >
```

アプリフローアクションを追加 \<name\> -コレクター \<string\>

```
add appflow policy \<名前\> \<規則\> \<アクション\>
```

```
bind appflow global \<ポリシー名\> \<優先度\> \[ \<goto 優先度式\> ] \[-type \<タイプ\>]
```

または

```
bind lb vserver \<仮想サーバー\> -policyName \<ポリシー\> -priority \<優先度\>
```

```
1 add appflow collector col -IPAddress 10.102.63.85
2 set appflow param -SecurityInsightRecordInterval 600 -
  SecurityInsightTraffic ENABLED
3 add appflow action act1 -collectors col
4 add appflow action af_action_Sap_10.102.63.85 -collectors col
5 add appflow policy pol1 true act1
6 add appflow policy af_policy_Sap_10.102.63.85 true
  af_action_Sap_10.102.63.85
7 bind appflow global pol1 1 END -type REQ_DEFAULT
8 or,
9 bind lb vserver Sap -policyName af_action_Sap_10.102.63.85 -
  priority "20"
10 <!--NeedCopy-->
```

NetScaler ADM から **Security Insight** を有効にするには:

NetScaler ADM が **13.0** ビルド **41.x** の場合:

1. [ネットワーク]>[インスタンス]>[ **NetScaler ADC** ]に移動し、インスタンスタイプを選択します。たとえば、VPX です。
2. インスタンスを選択し、[アクションの選択] リストから [ **Analytics** の設定 ] をクリックします。
3. 「仮想サーバーの分析の設定」 ページで、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. 「アナリティクスを有効にする」 ウィンドウで:
  - a) セキュリティインサイトを選択
  - b) **Logstream** をトランスポートモードとして選択

注

NetScaler ADC 12.0 以前の場合、**IPFIX** はトランスポートモードのデフォルトのオプションです。NetScaler ADC 12.0 以降では、トランスポートモードとして [ログストリーム] または [**IPFIX**] を選択できます。

IPFIX とログストリームの詳細については、「ログストリームの概要」を参照してください。

c) 式はデフォルトで true です

d) [OK] をクリックします

### Enable Analytics ✕

**Selected Virtual Server - Load Balancing: 3**

Web Insight

Security Insight

▼ Advanced Options

Transport Mode

Logstream     IPFIX

Instance level options

Enable HTTP X-Forwarded-For

Citrix Gateway

▼ Expression Configuration

Select expression for Load Balancing/Content Switching

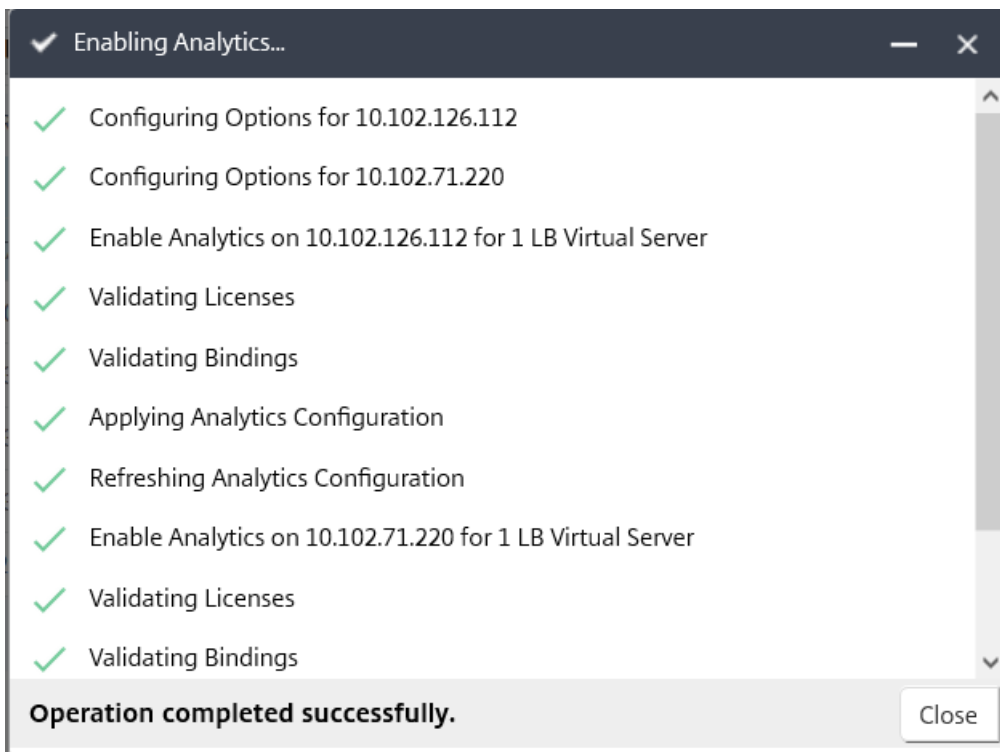
Select Expression

Edit Expression

注

- ライセンスされていない仮想サーバーを選択すると、NetScaler ADM はまずそれらの仮想サーバーのライセンスを取得し、次に分析を有効にします。
- 管理パーティションでは、**Web Insight** のみがサポートされます
- キャッシュリダイレクト、認証、GSLB などの仮想サーバーでは、分析を有効にすることはできません。エラーメッセージが表示されます。

[OK] をクリックすると、NetScaler ADM は選択した仮想サーバー上で分析を有効にするために処理します。



Citrix ADM が **13.0** ビルド **36.27** の場合:

1. [ネットワーク]>[インスタンス]に移動し、AppFlow を有効にする NetScaler ADC インスタンスを選択します。
2. [アクションの選択] リストから、[ **Analytics** の設定] を選択します。
3. 仮想サーバーを選択し、「**AppFlow** を有効にする」をクリックします。
4. 「**AppFlow** を有効にする」フィールドに「**true**」と入力し、「セキュリティインサイト」を選択します。
5. [**OK**] をクリックします。

### Enable AppFlow

**Select Expression**

Load Balancing

▼

true

**Transport Mode**    IPFIX    Logstream

Web Insight

Client Side Measurement

Security Insight

If there is a firewall between Citrix ADM and the Citrix ADC instance, please make sure the TCP port 5557 is open. This is to allow ADM to collect AppFlow traffic.

OK

Cancel

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、グループへのアプリケーションレベルのアクセスを提供したり、ユーザーをグループに割り当てたりすることができます。NetScaler ADM 分析では、仮想 IP アドレスベースの認証がサポートされるようになりました。ユーザーは、権限のあるアプリケーション（仮想サーバー）のみのすべての Insight のレポートを表示できるようになりました。グループおよびグループへのユーザの割り当ての詳細については、「[グループを設定する](#)」を参照してください。

### Security Insight レポートの地理的な場所を表示する

Security Insight レポートには、クライアントのリクエストが発生した正確な地理的場所が含まれます。Citrix ADM で地理的な場所を表示できます。Citrix ADC に組み込まれている地理データベースファイルには、ほとんどのパブリック IP アドレスが含まれています。このファイルは、Citrix ADC の `/var/netscaler/inbuilt_db` という場所にあります。

位置情報を有効にするには:

次のコマンドを実行して位置情報ログおよび CEF 形式でのログを有効にします。

- ロケーションファイルを追加 <Complete path with the DB filename>
- **set appfw settings -geoLocationLogging ON**

• **set appfw settings -CEFLogging ON**

地理データベースファイルで使用できない IP アドレスがある場合は、地理的位置の IP アドレスを追加できます。IP アドレスに加えて、都市/州/国の名前と各場所の緯度と経度の座標を追加することもできます。

vi エディタなどのテキストエディタで geo データベースファイルを開き、すべての場所のエントリを追加します。

エントリは、次の形式で指定する必要があります。

```
\<start IP\>,\<end IP\>,,\<country\>,\<state\>,,\<city\>,,longitude,latitude
```

例:

```
1 4.17.142.224,4.17.142.239,,US,New York,,Harrison,,73.7304,41.0568
2 <!--NeedCopy-->
```

**IP レピュテーション**

NetScaler Insight Center を使用して着信トラフィックの IP レピュテーションを監視および管理できます。悪意のある IP を追加するよう各種ポリシーを構成して、カスタマイズされたブロックリストを作成できます。

IP レピュテーションの設定と使用については、[IP レピュテーションを参照してください](#)。

**IP レピュテーションの監視**

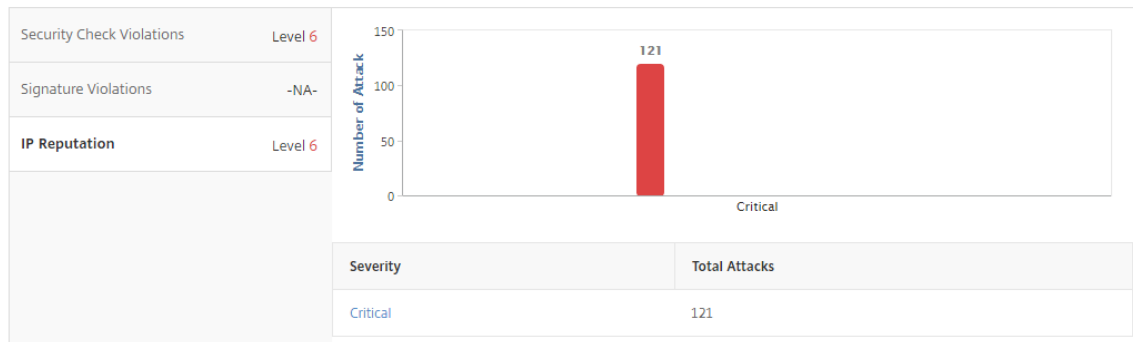
IP レピュテーション機能は、悪意のある IP アドレスに関する攻撃関連情報を提供します。たとえば、IP レピュテーションスコア、IP レピュテーションカテゴリ、IP レピュテーション攻撃時間、デバイス IP、およびクライアント IP アドレスに関する詳細がレポートされます。

IP レピュテーションスコアは、IP アドレスに関連付けられたリスクを示します。このスコアの範囲は次のとおりです。

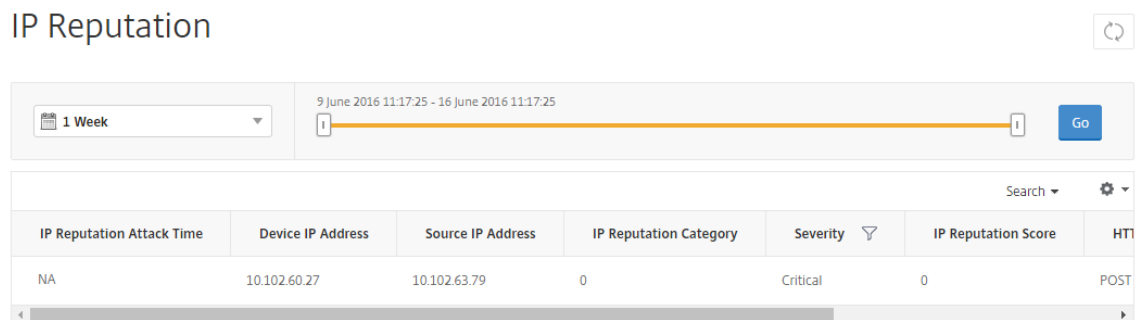
IP レピュテーションスコア	リスクの程度
1-20	高リスク
21-40	疑わしい
41-60	中程度のリスク
61-80	低リスク
81-100	信頼できる

IP レピュテーションを監視するには、次の手順に従います。

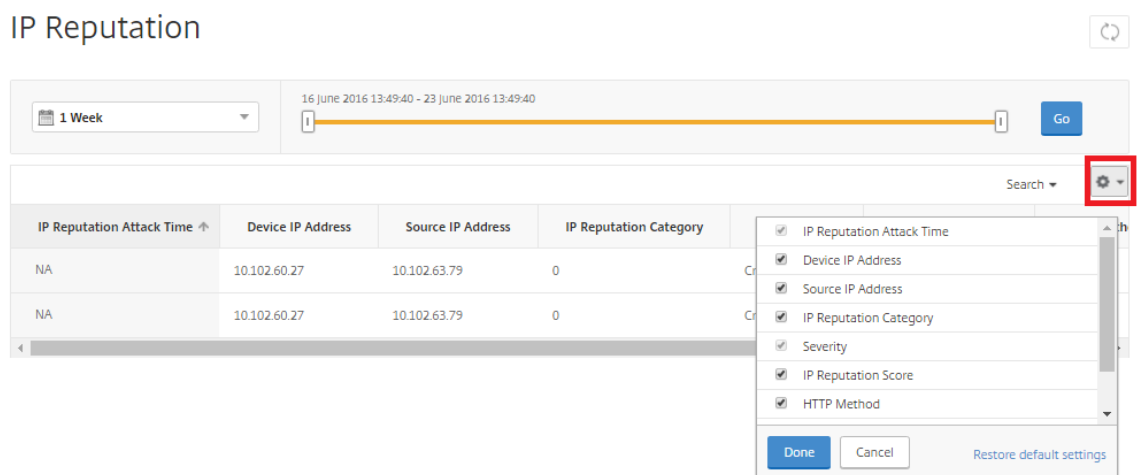
1. [分析] > [セキュリティインサイト] に移動し、監視するアプリケーションを選択します。
2. [脅威インデックス] タブで、[IP レピュテーション] を選択します。



3. 重大度を選択して、そのレベルの攻撃の詳細を表示します。棒グラフをクリックするか、グラフの下の表をクリックします。
4. 詳細を表示する期間を選択します。時間スライダーを使用して選択する期間をカスタマイズできます。次に [Go] をクリックします。



5. 表示をカスタマイズするには、[Settings] をクリックします。





## しきい値

Security Insight でアプリケーションの安全性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. [アナリティクス] > [設定] > [しきい値] に移動し、[追加] を選択します。
2. 「トラフィックタイプ」フィールドで「セキュリティ」としてトラフィックタイプを選択し、名前、期間、エンティティなどの他の適切なフィールドに必要な情報を入力します。
3. 「ルールを設定」セクションで、「メトリック」、「コンパレーター」、「値」の各フィールドを使用してしきい値を設定します。  
  
入力例: "Threat Index" ">" "5"
4. 通知設定で、通知タイプを選択します。
5. [作成] をクリックします。

しきい値違反を確認するには:

1. [分析] > [セキュリティインサイト \*\*] > [\*\* デバイス] に移動し、Citrix ADC インスタンスを選択します。
2. [アプリケーション] セクションの [Threshold **Breach**] 列には、各仮想サーバで発生したしきい値違反の数が表示されます。

## セキュリティインサイトのユースケース

次のユースケースでは、Security Insight を使用して、アプリケーションの脅威環境を査定し、セキュリティ対策を向上する方法を説明します。

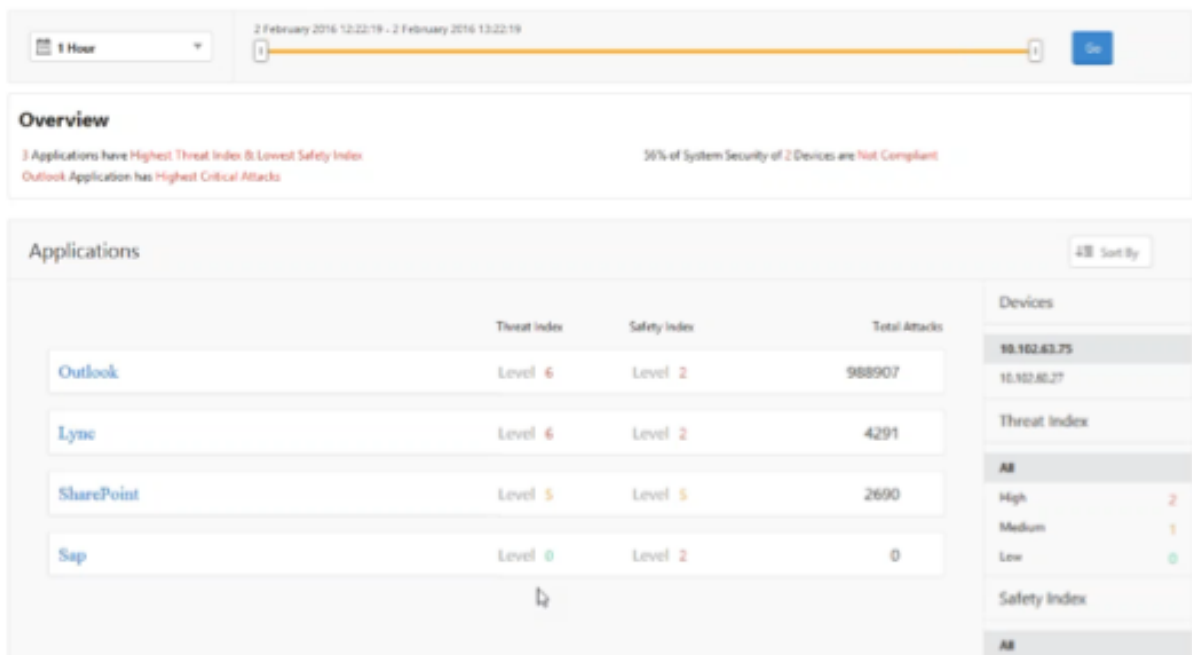
### 脅威環境の概要を把握する

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 ADM を構成しています。脅威指数、安全性指数、およびアプリケーションで発生した可能性のある攻撃の種類と重大度を頻繁に確認して、最も注意が必要なアプリケーションに特に注意を払うようにします。Security Insight ダッシュボードには、選択した期間および選択した NetScaler ADC 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要が表示されます。アプリケーションの一覧、脅威指数と安全性指数、選択した期間の攻撃回数の合計が表示されます。

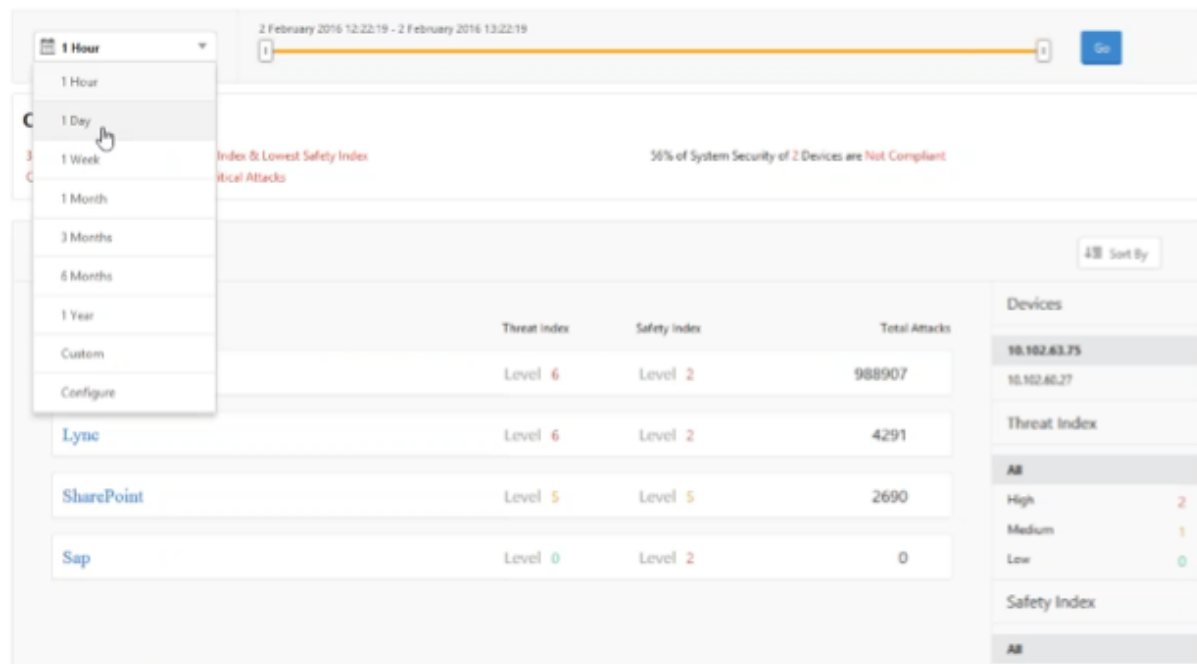
たとえば、Microsoft Outlook、Microsoft Lync、SharePoint、および SAP アプリケーションを監視していて、これらのアプリケーションの脅威環境の概要を確認する必要がある場合があります。

脅威環境の概要を取得するには、**NetScaler ADM** にログオンし、[Analytics] > [Security Insight] に移動します。

各アプリケーションの主要情報が表示されます。デフォルトの期間は 1 時間です。



異なる期間の情報を表示するには、左上のリストから期間を選択します。



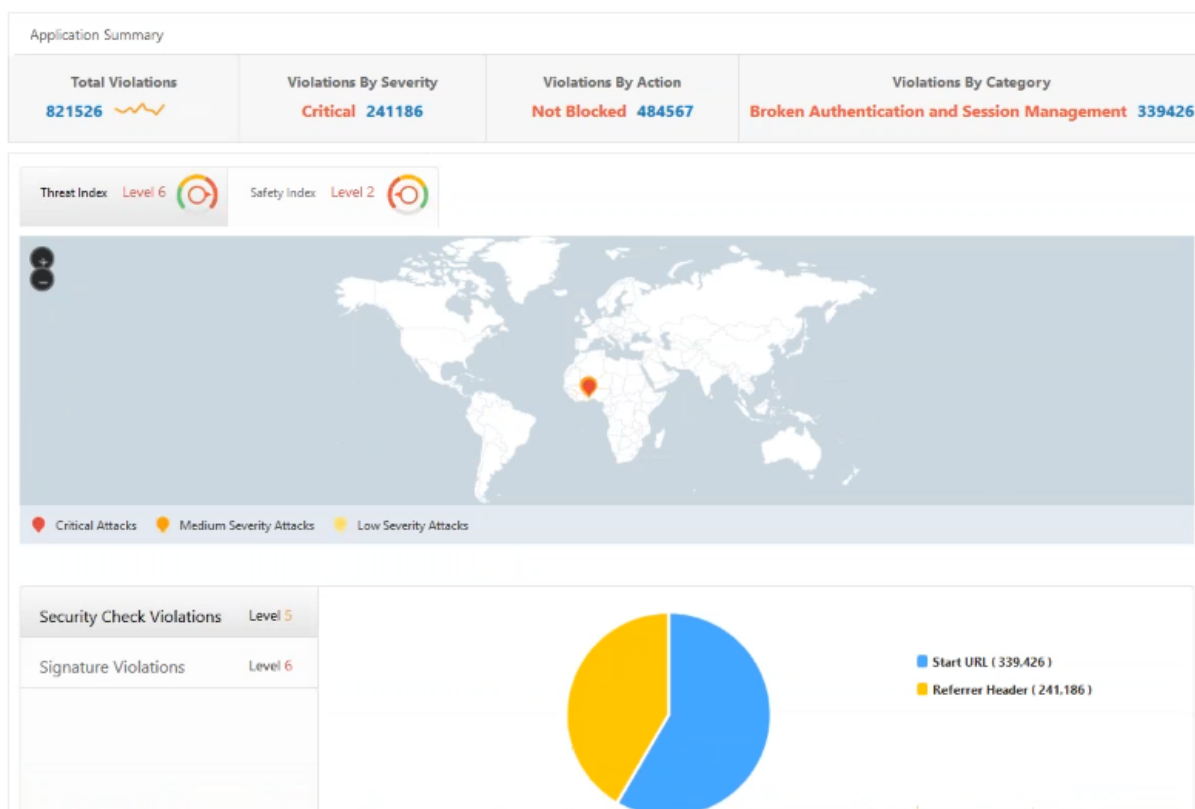
別の NetScaler ADC インスタンスの概要を表示するには、[デバイス] で、NetScaler ADC インスタンスの IP アドレスをクリックします。特定の列でアプリケーションの一覧を並べ替えるには、その列の見出しをクリックします。

アプリケーションが脅威にさらされる危険性を判断する

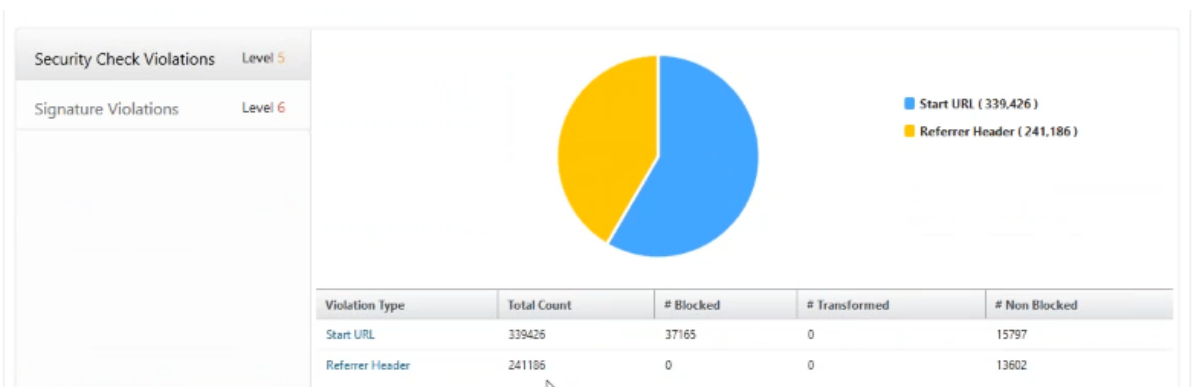
Security Insight ダッシュボードで脅威指数が高く安全性指数が低いアプリケーションを特定するには、保護を決定する前に脅威にさらされる危険性を判断する必要があります。つまり、指数値を下げている攻撃の種類と重大度を確認します。アプリケーションの脅威への露出度を判断するには、アプリケーションの概要を表示します。

この例では、Microsoft Outlook の脅威指数値が 6 になっており、この高い脅威指数の原因となっている要因を調べる必要があります。

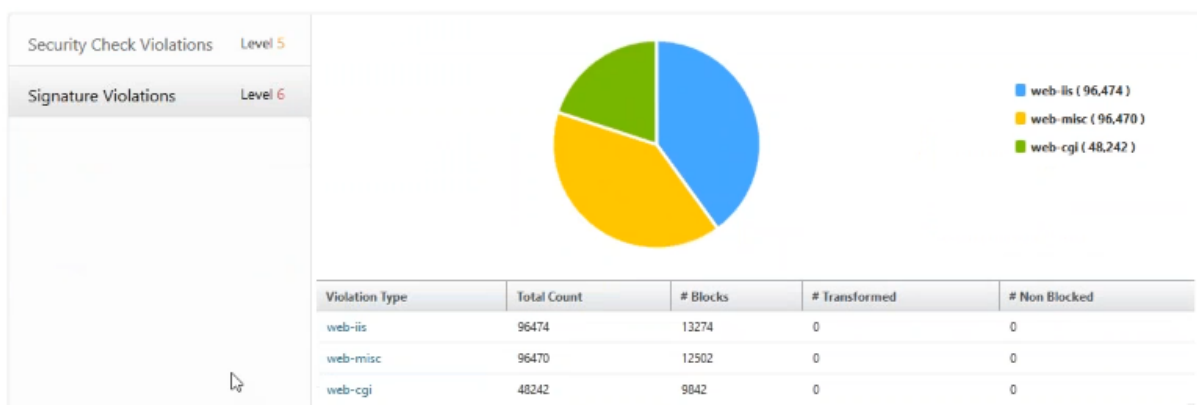
Microsoft Outlook の脅威への露出度を調べるには、[Security Insight] ダッシュボードで、[Outlook] をクリックします。アプリケーション概要に、サーバーの位置情報を特定する地図が含まれています。



[Threat Index] > [Security Check Violations] をクリックして、表示される違反情報を確認します。



[署名] [違反] をクリックし、表示される違反情報を確認します。

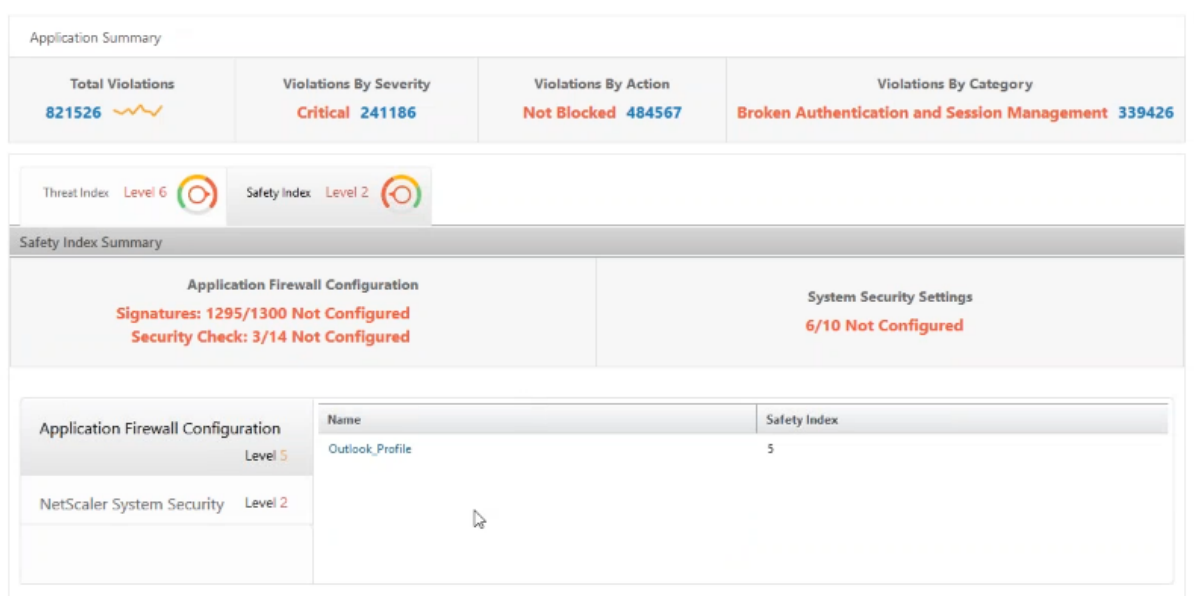


アプリケーションの既存のセキュリティ構成と欠落しているセキュリティ構成を判別する

アプリケーションの脅威への露出度を確認したら、そのアプリケーションに設定されているセキュリティ構成と欠落しているセキュリティ構成を確認します。この情報は、アプリケーションの安全性指数概要にドリルダウンすると表示されます。

安全性指数概要には、次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。構成されていないシグネチャおよびセキュリティエンティティの数を表示します。
- **NetScaler** システムセキュリティ。構成されていないシステムセキュリティ設定の数を表示します。



前出のユースケースでは、Microsoft Outlook の脅威への露出度（脅威指数値は6）について調査しました。次に、Outlook に設定されているセキュリティ構成と、どのような構成を追加すれば脅威指数を改善できるのかを調べる必要があります。

[**Security Insight**] ダッシュボードで、[**Outlook**] をクリックし、[**Safety Index**] タブをクリックします。[**Safety Index Summary**] 領域に表示された情報を確認します。



[アプリケーションファイアウォールの構成] ノードで、[**Outlook\_Profile**] をクリックし、セキュリティチェックと署名違反の情報を円グラフで確認します。

Application Firewall Configuration	Name	Safety Index
Level 5	Outlook_Profile	5
NetScaler System Security		Level 2

Security Check Level 5

- Blocked (10)
- Not Blocked (4)
- Disabled (0)

Signatures Violation Level 7

- Blocked (1,340)
- Not Blocked (4)
- Disabled (0)

アプリケーションファイアウォール概要表で各保護タイプの構成ステータスを確認します。特定の列で表を並べ替えるには、列見出しをクリックします。

Application Firewall Summary

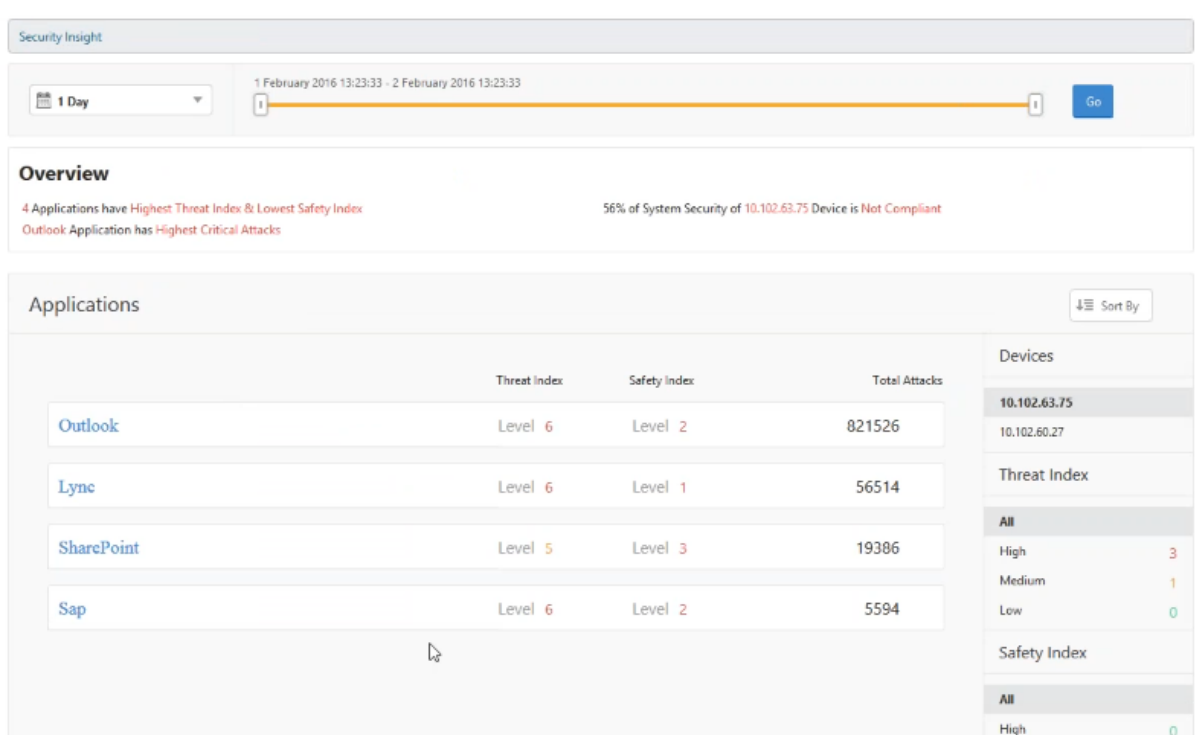
Protections	Configuration Status
XML Attachment	Not Configured
XML DoS	Not Configured
XML Format	Not Configured
XML SOAP Fault	Not Configured
XML SQL	Not Configured
XML Validation	Not Configured
XML WSI	Not Configured
XML XSS	Not Configured
Buffer Overflow	Log Stat Block
Buffer Overflow	Log Block
Content Type	Log

[**NetScaler System Security**] ノードをクリックして、システムセキュリティ設定と Citrix の推奨事項を確認し、アプリケーションの安全性指数を改善します。

即時の対応が必要なアプリケーションを特定

直ちに対処する必要があるアプリケーションとは、脅威指数が高く安全性指数が低いアプリケーションです。

この例では、Microsoft Outlook と Microsoft Lync が高い脅威指数値（6）を示していますが、安全性指数は Lync のほうが低くなっています。したがって、最初に Lync に注意を払い、その後で Outlook の脅威環境を改善します。



特定の時間内の攻撃数を決定する

特定のアプリケーションで特定の時間帯に発生した攻撃の数や、指定した期間の攻撃発生率を調べてみます。

**Security Insight** ページで任意のアプリケーションをクリックし、[アプリケーションの概要] で違反の数をクリックします。違反合計ページには、1 時間、1 日、1 週間および 1 ヶ月の攻撃がグラフィカルに表示されます。



[アプリケーションの概要] テーブルには、攻撃の詳細が表示されます。それらのいくつかは以下のとおりです。

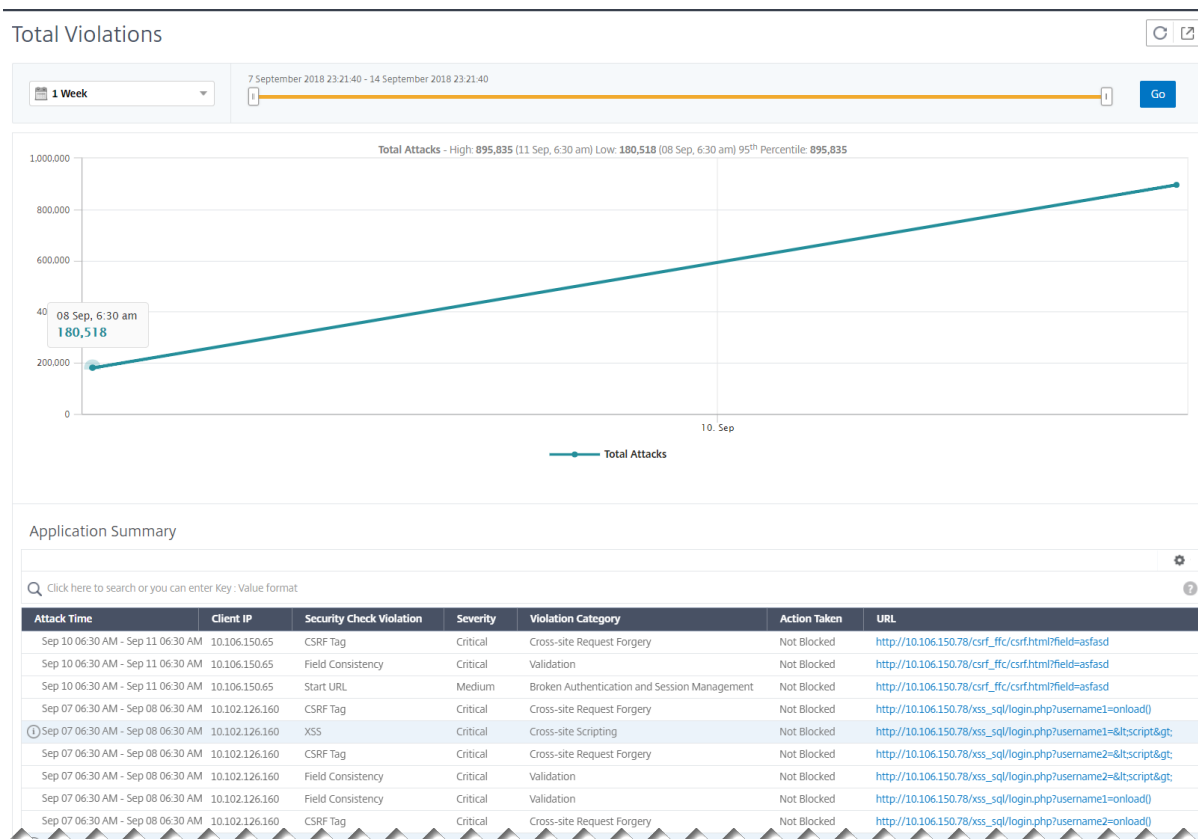
- アタックタイム
- 攻撃が発生したクライアントの IP アドレス
- 重要度
- 違反のカテゴリ
- 攻撃の発信元の URL、およびその他の詳細。

Application Summary

Click here to search or you can enter Key - Value format

Attack Time	Client IP	Security Check Violation	Severity	Violation Category	Action Taken	URL	Transaction ID
Sep 11 11:05 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 10:22 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 11:02 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 10:46 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 10:57 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 11:11 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 10:50 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 10:54 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 11:02 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 10:46 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 11:10 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 10:50 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 10:54 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 11:05 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 11:05 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0

攻撃時間は、画像のように時間ごとのレポートでいつでも表示できますが、日次レポートや週次レポートでも、集計レポートの攻撃時間範囲を表示できるようになりました。期間リストから「1日」を選択すると、セキュリティインサイトレポートには、集計されたすべての攻撃が表示され、攻撃時間が1時間の範囲で表示されます。「1週間」または「1ヶ月」を選択すると、すべての攻撃が集計され、攻撃時間が1日の範囲で表示されます。



### セキュリティ侵害に関する詳細情報の取得

アプリケーションに対する攻撃のリストを表示して、攻撃の種類と重大度、Citrix ADC インスタンスが実行したアクション、要求されたリソース、および攻撃の原因に関する洞察を得たい場合があります。

たとえば、Microsoft Lync に対する攻撃がブロックされた数、要求されたリソース、発信元の IP アドレスを調べます。

[ **Security Insight** ] ダッシュボードで、[ **Lync** ] > [違反総数] をクリックします。表の [ **Action Taken** ] 列の見出しにあるフィルターアイコンをクリックし、[ **Blocked** ] を選択します。



Application Summary									
Security Check Violation	Severity	Violation Category	Action Taken	Location	Signature Violation	Violation Name	Violation Value	Found In	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	uri/test1.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	uri/test2.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test3.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test4.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test5.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test6.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test7.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test8.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test10.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test9.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test11.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test12.html			Form Field	

要求されたリソースについて詳しくは、[ URL ] 列を参照してください。攻撃の発信元に関する情報を知りたい場合は、[ Client IP ] 列を確認します。

#### ログ式の詳細を表示する

Citrix ADC インスタンスは、アプリケーションファイアウォールプロファイルで構成されたログ式を使用して、企業内のアプリケーションに対する攻撃に対してアクションを実行します。セキュリティインサイトでは、Citrix ADC インスタンスで使用されるログ式に対して返された値を表示できます。これらの値には、リクエストヘッダー、リクエストボディなどが含まれます。ログ式の値とは別に、Citrix ADC インスタンスが攻撃に対するアクションを実行するために使用したアプリケーションファイアウォールプロファイルに定義されているログ式の名前とコメントを表示することもできます。

前提条件 次のことを確実にします。

- アプリケーションファイアウォールプロファイルでログ式を設定します。詳しくは、「[アプリケーションファイアウォール](#)」を参照してください。
- Citrix ADM でログ式ベースのセキュリティインサイト設定を有効にします。以下を実行します：
  1. [ アナリティクス ] > [ 設定 ] に移動し、[ アナリティクスの機能を有効にする ] をクリックします。
  2. [ Analytics の機能を有効にする ] ページで、[ ログ式ベースの **Security Insight** 設定 ] セクションの [ **Security Insight** を有効にする ] を選択し、[ **OK** ] をクリックします。

←

## Enable Features for Analytics

---

**Multihop Settings**

Enable the Multihop feature if the network deployment has more than one NetScaler appliance or NetScaler Gateway appliance between a single client and a server connection. NetScaler MAS analyses the number of hops for NetScaler Gateway appliances through which the ICA connections pass. NetScaler MAS also collects and correlates the AppFlow records from all the appliances.

Enable Multihop ?

**Adaptive Threshold Settings**

Enable the adaptive threshold functionality feature to send a syslog message to the syslog server if the maximum number of hits on a URL is greater than the threshold value set. The feature dynamically sets the threshold value in NetScaler MAS for the maximum number of hits on each URL.

Enable Adaptive Threshold

**TCP Insight Settings**

Enable the TCP Insight feature of NetScaler MAS to provide an easy and scalable solution for monitoring the metrics of the optimization techniques and congestion control strategies (or algorithms) used in NetScaler appliances to avoid network congestion in data transmission.

Enable TCP Insight

**Web Insight Settings**

Enable the Web Insight feature to allow NetScaler MAS to retrieve the performance reports of web applications (load balancing and content switching virtual servers) that are bound to the NetScaler ADC. Web Insight enables visibility into enterprise web applications and allows IT administrators to monitor all web applications being served by the NetScaler ADC by providing integrated and real-time monitoring of applications.

Enable Web Insight

**Log Expression Based Security Insights Settings**

Enable Log Expression based Security Insights to report log expression data configured with Application Firewall profile.

Enable Security Insight ?

OK
Close

たとえば、企業内の Microsoft Lync に対する攻撃に対して実行したアクションについて、NetScaler ADC インスタンスによって返されるログ式の値を表示できます。

セキュリティインサイトダッシュボードで、[ **Lync** ] > [違反総数] に移動します。[アプリケーションの概要] 表で URL をクリックすると、[違反 情報] ページで違反の完全な詳細が表示されます。ログ式名、コメント、および NetScaler ADC インスタンスがアクションに対して返す値が含まれます。

The screenshot shows the 'Violation Information' window in NetScaler ADM. It displays details for a security violation, including the attack time (NA), signature violation name, violation value (Start URL), security check violation (Broken Authentication and Session Management), threat index (5), severity (Medium), and action taken (Blocked). The URL is http://10.102.60.245/csrf\_ffc/ffc.html?field1=asfasd. The client IP is 10.102.63.79 and the location is Bangalore. There was 1 total attack.

Log Expression Name	Log Expression Comment	Log Expression Value
LGEXPR7	http request contains keyword	false
LGEXPR8	http request contains header	false
LGEXPR6	http method expression	GET /csrf_ffc/ffc.html?field1=asfasd HTTP/1.1 User-Agent: curl/7.19.7 (x86_64-pc-linux-gnu) libcurl/7.19.7 OpenSSL/0.9.8k zlib/1.2.3.3 libidn/1.15 Host: 10.102.60.245 Accept: */*
LGEXPR3	http method expression	true
LGEXPR4	http request contains header	
LGEXPR1	http request header contains user agent	curl/7.19.7 (x86_64-pc-linux-gnu) libcurl/7.19.7 OpenSSL/0.9.8k zlib/1.2.3.3 libidn/1.15
LGEXPR2	http method expression	false
LGEXPR5	http method expression	

**Web** アプリケーションファイアウォール (WAF) の違反パターンを強調表示

HTTP ヘッダーや HTTP ペイロードなどの攻撃の詳細を取得して、攻撃をトラブルシューティングまたは分析できるようになりました。攻撃の詳細を取得するには、次のコマンドを使用して、アプリケーションファイアウォールプロファイルの「VerboseLogLevel」を更新する必要があります。

```
Set appfw profile <profile_name> -VerboseLogLevel (pattern|patternPayload |patternPayloadHdr)
```

- **pattern** -違反パターンのみが記録されます
- **patternPayload** -違反パターン + 攻撃パターンの前のフィールド要素値の 150 バイトが記録される
- **patternPayloadHdr** -違反パターン + 攻撃パターン前のフィールド要素値 150 バイト + HTTP リクエストヘッダーが記録される

「VerboseLogLevel」構成に基づいて、NetScaler ADM は詳細なログ式レコードを表示します。

以下の画像は、GET リクエストの攻撃パターンを強調した例です。

**Violation Information** ✕

Violation Information

---

Attack Time **Aug 22 11:34 PM - Aug 23 00:34 AM**

Signature Category

Violation Name **password18**

Violation Value **Bad tag: javascript**

Security Check Violation **XSS**

Violation Category **Cross-site Scripting**

Threat Index **6**

Severity **Critical**

Action Taken **Blocked**

URL **http://10.106.150.109/xss\_sql/login.php?password18=<javascript>**

Found In **Form Field**

Client IP **10.102.63.79**

Location **Bangalore**

Total Attacks **1**

LOG EXPRESSION NAME	LOG EXPRESSION COMMENT	LOG EXPRESSION VALUE
TX_ATTACK_PAYLOAD		PAYLOAD_OFFSET 34 FIELDNAME: password18 ATTACK_PATTERN:<javascript
TX_HEADERS		GET /xss_sql/login.php?password18=<javascript> HTTP/1.1 User-Agent: curl/7.19.7 (x86_64-pc-linux-gnu) libcurl/7.19.7 OpenSSL/0.9.8k zlib/1.2.3.3 libidn/1.15 Host: 10.106.150.109 Accept: */*

次の画像は、POST リクエストの攻撃パターンを強調した例です。

**Violation Information**

Violation Information

---

Attack Time **Oct 22 06:30 AM - Oct 23 06:30 AM**

Signature Category

Violation Name **password**

Violation Value

Security Check Violation **XSS**

Violation Category **Cross-site Scripting**

Threat Index **6**

Severity **Critical**

Action Taken **Blocked**

URL **http://demo.citrite.net/action\_page.php**

Found In **Form Field**

Client IP **10.252.241.69**

Location

Total Attacks **2**

LOG EXPRESSION NAME	LOG EXPRESSION COMMENT	LOG EXPRESSION VALUE
TX_HEADERS		POST /action_page.php HTTP/1.1 Referer: http://demo.citrite.net/ext_demo/index.html Cache-Control: max-age=0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US Content-Type: application/x-www-form-urlencoded Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18362 Accept-Encoding: gzip, deflate Host: demo.citrite.net Content-Length: 214 Connection: Keep-Alive
TX_ATTACK_PAYLOAD		PAYLOAD_OFFSET 32 FIELDNAME: password ATTACK_PATTERN:ped her after other known defer his. For county now sister engage had season better had waited. Occasional mrs acceptance <script

次の 2 つの例では、

- **FIELDNAME** は、攻撃パターンに対応するフィールド名を指します。
- **PAYLOAD\_OFFSET** は、実際のペイロードのアタックオフセットを指します。
- **ATTACK\_PATTERN** は攻撃パターンを強調表示し、値に 150 バイトのプレフィクスペイロードを含めます。

NetScaler ADC で詳細ログレベルを構成する方法について詳しくは、「[Web アプリケーションファイアウォールログによるトラブルシューティングのしやすさ](#)」を参照してください。

構成を展開する前に安全指数を決定する

セキュリティ侵害は、NetScaler ADC インスタンスにセキュリティ構成を展開した後に発生しますが、展開する前にセキュリティ構成の有効性を評価することをお勧めします。

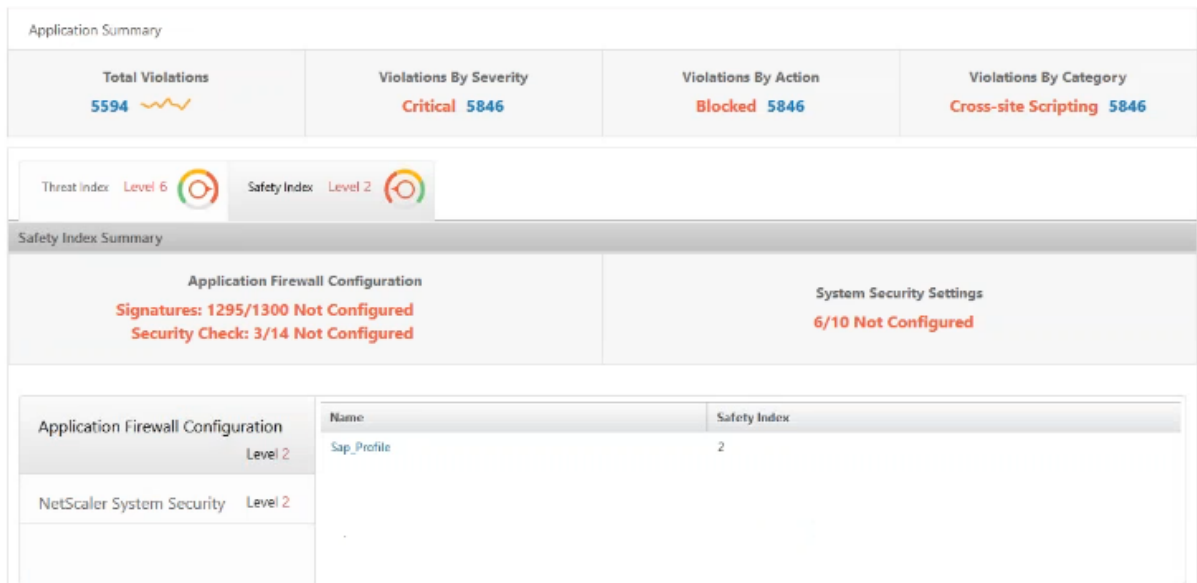
たとえば、IP アドレスが 10.102.60.27 の Citrix ADC インスタンス上の SAP アプリケーションの構成の安全性指数を評価したい場合があります。

セキュリティインサイトダッシュボードの「デバイス \*\*」で、構成した Citrix ADC インスタンスの IP アドレスをクリックします。脅威指数と攻撃総数はどちらも 0 になっています。脅威指数には、アプリケーションに対する攻撃の数と種類が直接反映されます。攻撃回数がゼロということは、アプリケーションがまったく脅威にさらされていないことを示しています。

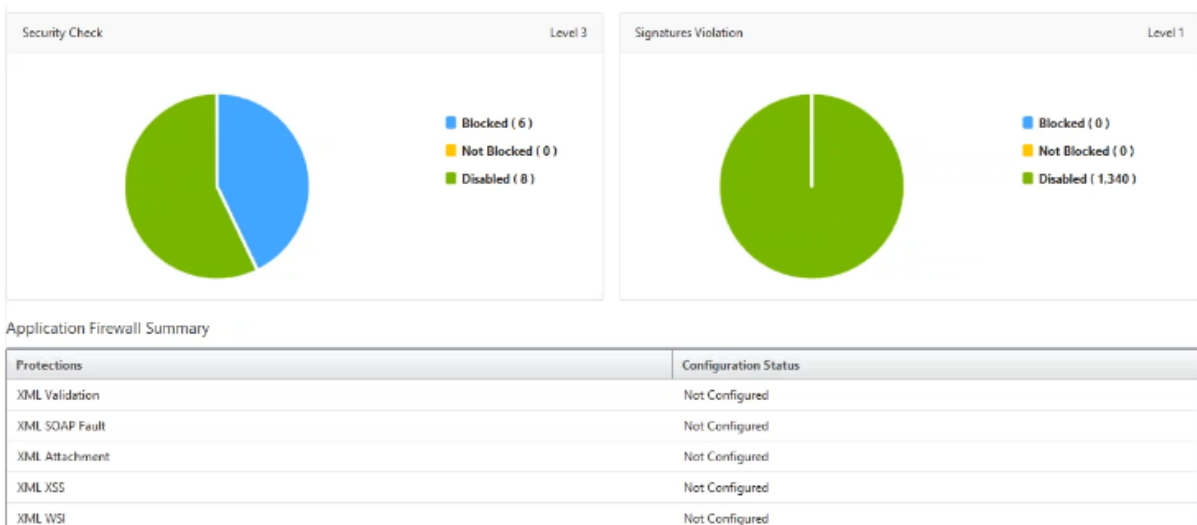
The screenshot displays the Security Insights dashboard for a Citrix ADC instance. At the top, there is a time range selector set to '1 Day' and a date range from '1 February 2016 13:33:35' to '2 February 2016 13:33:35'. Below this is an 'Overview' section with summary statistics: '4 Applications have Highest Threat Index & Lowest Safety Index' and 'Outlook Application has Highest Critical Attacks'. A compliance status indicates '56% of System Security of 10.102.63.75 Device is Not Compliant'. The main section is titled 'Applications' and contains a table with columns for Application, Threat Index, Safety Index, and Total Attacks. The table lists Lync, Sap, Outlook, and SharePoint. A 'Sort By' dropdown is visible on the right. To the right of the table is a 'Devices' sidebar with a list of IP addresses, including 10.102.63.75 and 10.102.60.27. Below the devices is a 'Threat Index' section showing counts for All, High, Medium, and Low threats, all currently at 0. At the bottom of the sidebar is a 'Safety Index' section.

Application	Threat Index	Safety Index	Total Attacks
Lync	Level 6	Level 2	4922
Sap	Level 0	Level 3	0
Outlook	Level 0	Level 6	0
SharePoint	Level 0	Level 6	0

[Sap] > [Safety Index] > [SAP\_Profile] の順に選択して、表示される安全性指数情報を評価します。



アプリケーションファイアウォールの概要では、さまざまな保護設定の構成ステータスを確認できます。ログを記録する設定になっている場合や、構成されていない設定がある場合は、アプリケーションに割り当てられる安全性指数は低くなります。



## ポット

February 6, 2024

注

NetScaler ADM ビルドが **13.0-79.x** より前の場合は、[分析] > [セキュリティ] > [ポットインサイト] に移動してポットインサイトを表示できます。**13.0-79.x** 以降のビルドでは、[分析] > [セキュリティ] > [セキュリテ

【違反】>【アプリケーションの概要】に移動し、【アプリケーションの分類】の【ボット】をクリックすると、ボットの詳細を表示できます。

ボットは、特定のアクションを人間よりもはるかに速い速度で何度も自動的に実行するソフトウェアプログラムです。ウェブトラフィックの 35% 以上がボットで、80% の組織がボット攻撃に苦しんでいます。Web ページを操作したり、フォームを送信したり、リンクをクリックしたり、テキストをスキャンしたり、コンテンツをダウンロードしたりできます。ボットは、ソーシャルメディアプラットフォームで動画にアクセスしたり、コメントを投稿したり、ツイートしたりできます。一部のボットは、人間のユーザーとの基本的な会話さえできます。これらはチャットボットとして知られています。

このような顧客サービス、チャットボット、検索エンジンのクローラなどの必要または有用なサービスを実行するボットは、良いボットとして知られています。悪意のあるボットの中には、Web サイトからコンテンツをスクレイピングまたはダウンロードしたり、ユーザーの資格情報を盗んだり、スパムコンテンツを拡散させたり、さまざまな種類のサイバー攻撃を実行したりすることがあります。これらの悪意のあるボットは、悪いボットとして知られています。悪質なボットを特定し、高度なセキュリティ攻撃からアプライアンスを保護することは不可欠です。これは、ボット管理システムを使用して実現できます。

ボットの詳細については、「[ボット管理](#)」を参照してください。

### NetScaler ADC でのボット検出技術の構成

NetScaler ADC では、受信するボットトラフィックを検出するようにボット検出技術を構成できます。NetScaler ADC インスタンスで構成するボットテクニックを次に示します。

- **許可リスト。**このルールには、Web リソースにアクセスできる適切なボットの特定のセットかどうかを評価するための URL とポリシー式のリストがあります。
- **ブロックリスト。**このルールには、特定の不正なボットがウェブサイトアクセスできるかどうかを評価する URL とポリシー式のリストがあります。
- **IP レピュテーション。**このルールは、受信ボットトラフィックが悪意のある IP アドレスかどうかを検出します。
- **デバイスフィンガープリント。**このルールは、受信ボットトラフィックの受信リクエストヘッダーと受信クライアントボットトラフィックのブラウザ属性にデバイスフィンガープリント ID が含まれているかどうかを検出します。
- **レート制限。**このルールは、同じクライアントから送信される複数の要求をレート制限します。
- **署名。**このルールは、シグネチャ検出に基づいてボットを検出してブロックします。また、ウェブサイトのスクレイプ、ログインの強制、脆弱性を調査するボットの不正な URL も防止します。
- **ボットトラップ。**このルールは、Web ページで有効になっているスクリプトにアクセスするボットを検出します。
- **TPS。**このルールは、最大リクエスト数とリクエストの増加率が設定された時間間隔を超えると、着信トラフィックをボットとして検出します。

Bot 管理の設定について詳しくは、[Bot 管理の構成を参照してください](#)。

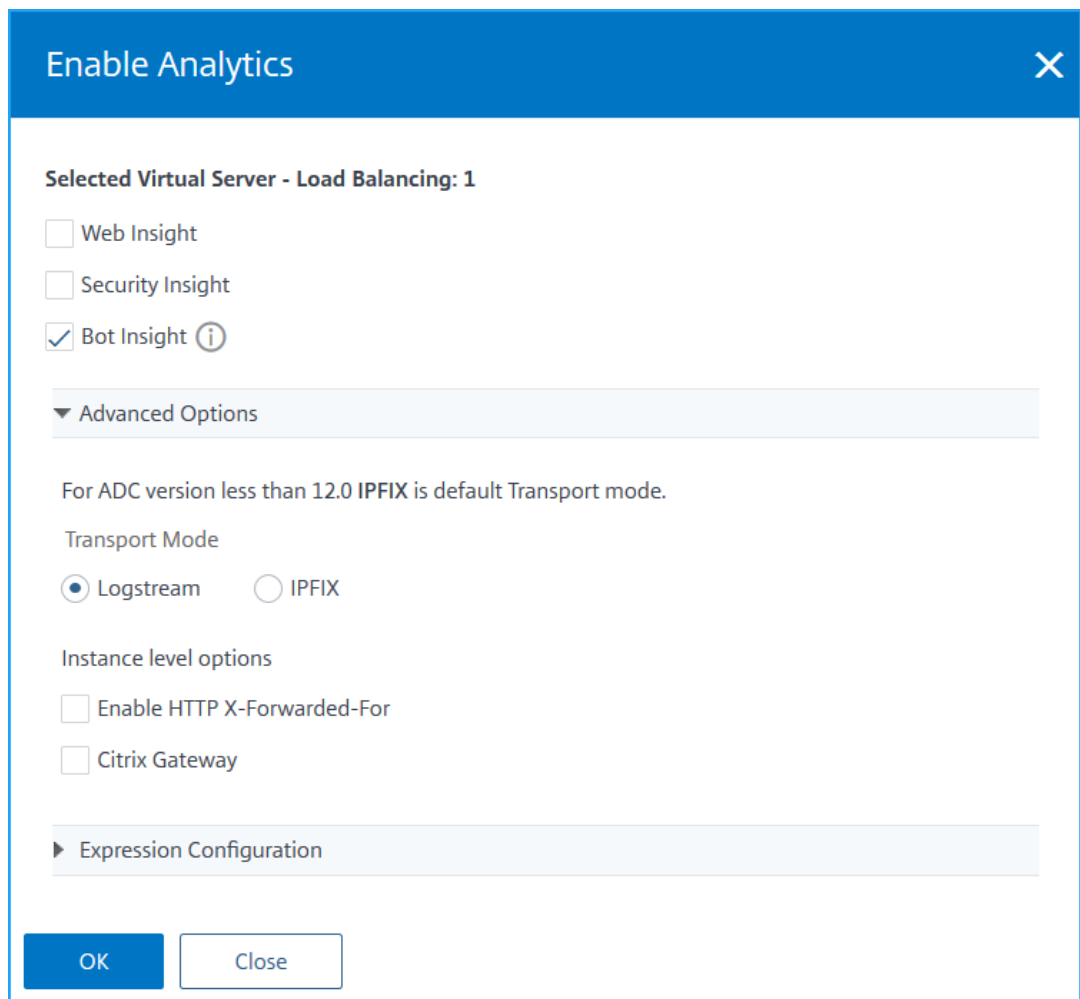
## NetScaler ADM での Bot Insight の使用

NetScaler ADC でボット管理を構成したら、仮想サーバーで **Bot Insight** を有効にして、NetScaler ADM でインサイトを表示する必要があります。

ボットインサイトを有効にするには:

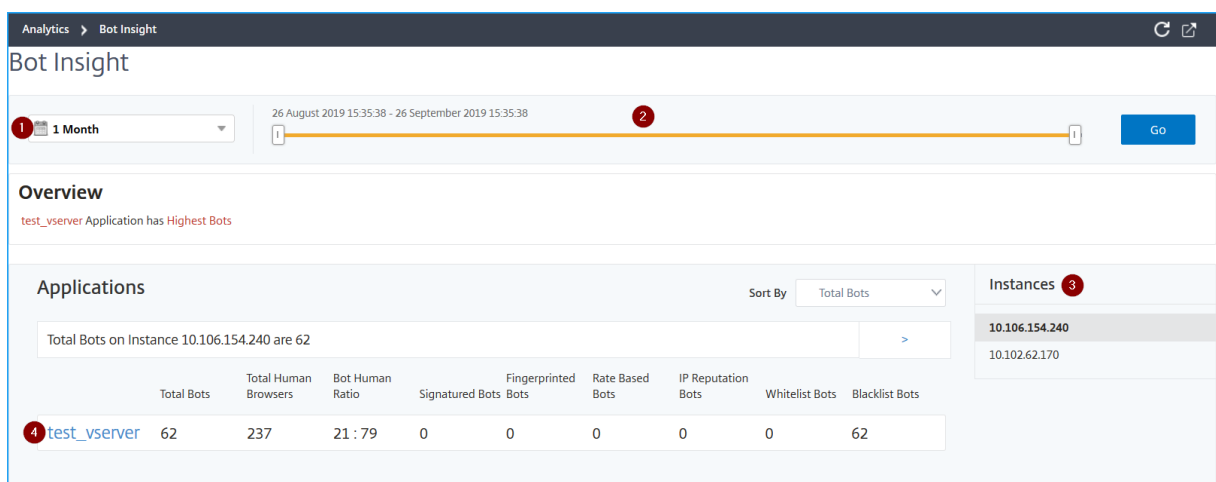
1. [ ネットワーク ] > [ インスタンス ] > [ **NetScaler ADC** ] に移動し、インスタンスタイプを選択します。たとえば、VPX です。
2. インスタンスを選択し、[ アクションの選択 ] リストから [ **Analytics を設定** ] を選択します。
3. 仮想サーバーを選択し、「分析を有効にする」をクリックします。
4. [ **Analytics の有効化** ] ウィンドウで、次の操作を行います。
  - a) ボットインサイトを選択
  - b) [ 詳細オプション ] で [ ログストリーム ] を選択します。





c) [OK] をクリックします。

ボットインサイトを有効にしたら、[分析]>[ボットインサイト]に移動します。



1 -ボットの詳細を表示するタイムリスト

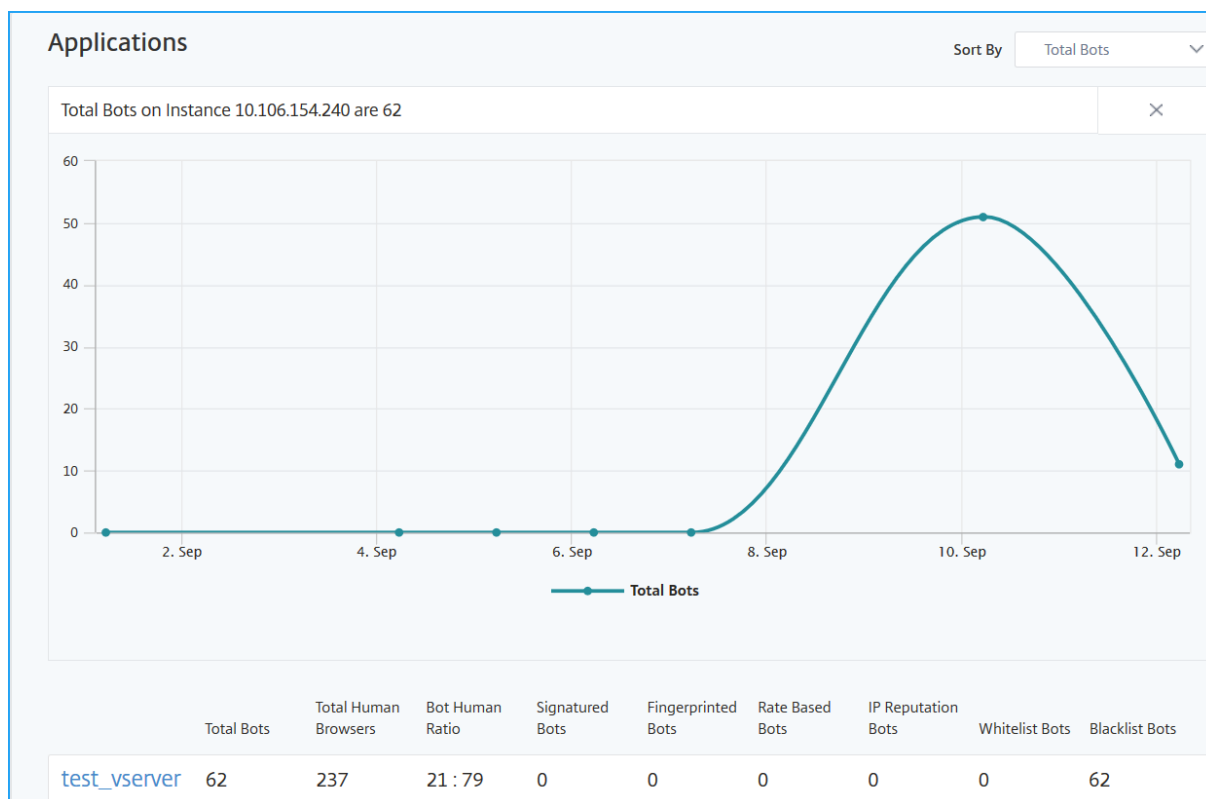
2 スライダーをドラッグして特定の時間範囲を選択し、「Go」をクリックしてカスタマイズされた結果を表示します。

3 ボットの影響を受けたインスタンスの総数

4 選択したインスタンスの合計ボット攻撃を受けた仮想サーバー

- ボット総数—仮想サーバーで見つかったボット攻撃の合計数 (すべてのボットカテゴリを含む) を示します。
- ヒューマンブラウザ総数—仮想サーバーにアクセスしているヒューマンユーザーの総数を示します。
- **Bot Human Ratio**—仮想サーバーにアクセスする人間のユーザーとボットの比率を示します。
- 署名ボット、指紋ボット、レートベースのボット、IP レピュテーションボット、許可リストボット、ブロックリストボット—設定されたボットカテゴリに基づいて発生したボット攻撃の総数を示します。ボットカテゴリについては、「NetScaler ADC でのボット検出手法の構成」を参照してください。

5 -[>] をクリックして、ボットの詳細をグラフ形式で表示します。



### イベント履歴の表示

ボットシグネチャの更新は、次の場合にイベント履歴で確認できます。

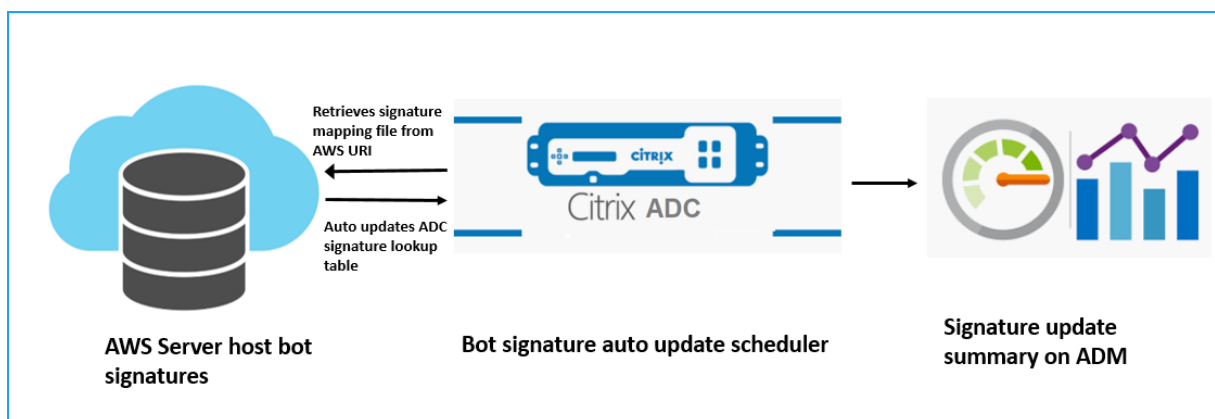
- 新しいボットシグネチャが NetScaler ADC インスタンスに追加されます。
- 既存のボットシグネチャは、NetScaler ADC インスタンスで更新されます。

ボットインサイトページで時間を選択してイベント履歴を表示できます。

DATE	MESSAGE
Apr 01 2020 10:17:02	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Apr 01 2020 09:25:41	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Apr 01 2020 09:25:30	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 31 2020 13:33:20	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 31 2020 11:38:26	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 31 2020 11:31:07	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 26 2020 15:17:47	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 26 2020 13:53:47	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 26 2020 13:47:51	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 26 2020 13:45:54	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 26 2020 13:43:24	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 26 2020 13:41:09	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 26 2020 13:37:56	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 26 2020 13:37:06	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 26 2020 13:36:22	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 26 2020 13:33:38	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 26 2020 13:12:07	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 24 2020 15:49:18	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 24 2020 13:17:23	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 24 2020 13:11:37	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537
Mar 24 2020 12:26:35	botLogMsg : 0.0.0.0 0-PPE0 - Bot New Signature Available. Newly added Rules:0 Deleted:3537

Total 21      25 Per Page      Page 1 of 1

次の図は、AWS クラウドからボット署名を取得し、NetScaler ADC で更新し、NetScaler ADM で署名更新の概要を表示する方法を示しています。

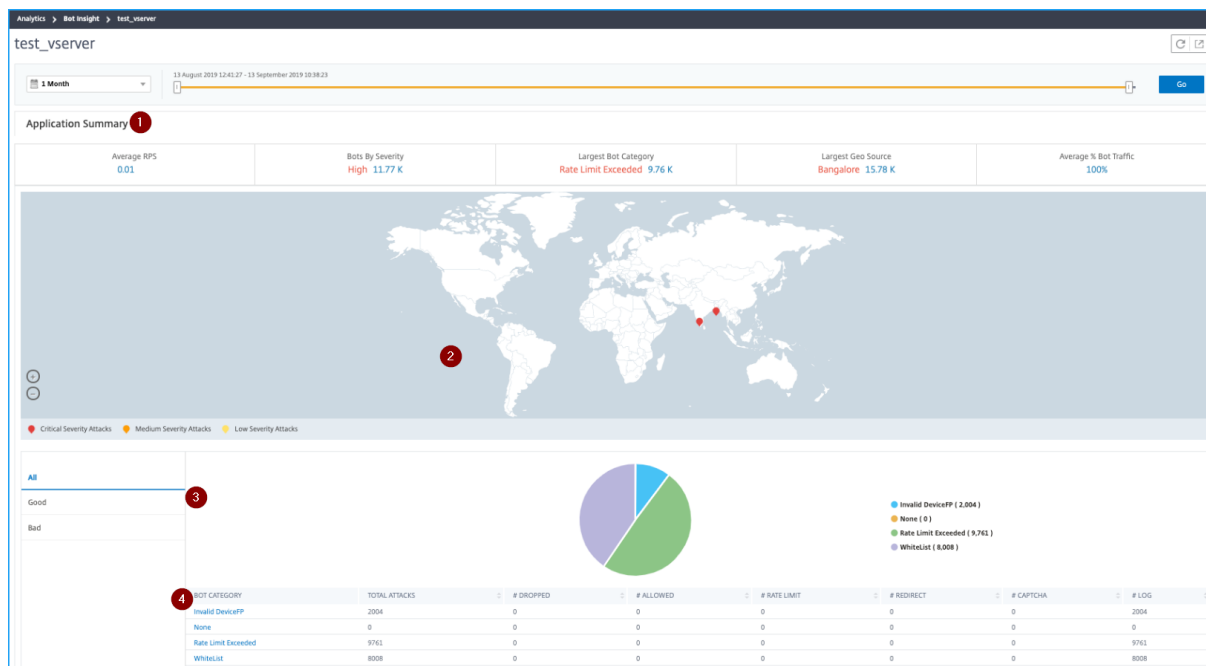


1. ボット署名の自動更新スケジューラは、AWS URI からマッピングファイルを取得します。
2. マッピングファイル内の最新のシグネチャを、ADC アプライアンス内の既存のシグネチャと照合します。
3. AWS から新しい署名をダウンロードし、署名の整合性を検証します。
4. 既存のボット署名を、ボット署名ファイル内の新しい署名で更新します。

5. SNMP アラートを生成し、署名の更新の概要を NetScaler ADM に送信します。

ボットを表示

仮想サーバーをクリックすると、アプリケーションの概要が表示されます。



1: 次のようなアプリケーション・サマリーの詳細を提供します。

- 平均 **RPS** –仮想サーバーで受信した 1 秒あたりの平均ボットトランザクションリクエスト数 (RPS) を示します。
- 重大度ごとのボット–重大度 に基づいて発生したボットのトランザクションの最大数を示します。重要度は、「緊急」、「高」、「中」、「低」に基づいて分類されます。

たとえば、仮想サーバーに重大度の高いボットが **11770** 個、重大度が **1550** 個のボットがある場合、**Citrix ADM** では [重要度別のボット] に [ \*\* クリティカル **1.55 K**] が表示されます。 \*\*

- 最大ボットカテゴリー–ボットカテゴリー に基づいて発生したボット攻撃の最大数を示します。
- たとえば、仮想サーバーに 8000 ブロッカー一覧ボット、リストされたボットを 5000 許可する、および 10000 レート制限超過ボットがある場合、NetScaler ADM では、 [最大ボットカテゴリー] に [レート制限が **10 K** を超えました] と表示されます。
- 最大地域ソース–リージョン に基づいて発生したボット攻撃の最大数を示します。

たとえば、仮想サーバーでサンタクララで **5000** 件のボット攻撃、ロンドンで **7000** 件のボット攻撃、バンガロールで **9000** 件のボット攻撃が発生した場合、**Citrix ADM** では「最大ジオソース」に「バンガロール **9K**」と表示されます。

- 平均ボットトラフィック率—ヒューマンボットの割合を示します。
- 2—マップビュー内の場所に基づいてボット攻撃の重大度を表示します
  - 3—ボット攻撃の種類（「良好」、「悪い」、「すべて」）を表示します。
  - 4—ボット攻撃の総数と、対応する設定済みアクションを表示します。たとえば、次の設定があるとします。
    - IP アドレスの範囲 (192.140.14.9 ~192.140.14.254) をブロックリストボットとして選択し、これらの IP アドレス範囲のアクションとして [ドロップ] を選択します。
    - IP 範囲 (192.140.15.4 ~192.140.15.254) をブロックリストボットとして設定し、これらの IP 範囲のアクションとしてログメッセージを作成するように選択されました

このシナリオでは、NetScaler ADM には次の情報が表示されます。

- ブロックリストされたボットの総数
- ドロップされた下のボットの合計
- ログに記録されているボットの総数

## CAPTCHA ボットを表示する

ウェブページでは、CaptCha は、着信トラフィックが人間か自動化されたボットからのものかを識別するように設計されています。NetScaler ADM で CAPTCHA アクティビティを表示するには、NetScaler ADC インスタンスで IP レピュテーションとデバイスフィンガープリント検出技術のボットアクションとして CAPTCHA を構成する必要があります。詳しくは、「[ボット管理](#)」を参照してください。

NetScaler ADM が Bot Insight に表示する CAPTCHA アクティビティを次に示します。

- キャプチャ試行回数超過—ログイン失敗後に行われた **CAPTCHA** 試行の最大回数を示します
- **Captcha client muted**—CAPTCHA チャレンジで以前にこれらのリクエストが不正なボットとして検出されたためにドロップまたはリダイレクトされたクライアントリクエストの数を示します
- **Human**—人間のユーザーから実行されたキャプチャエントリを示します
- 無効なキャプチャ応答—NetScaler ADC が CAPTCHA チャレンジを送信したときに、ボットまたは人間から受信した不正な CAPTCHA 応答の数を示します

BOT CATEGORY	TOTAL ATTACKS	# DROPPED	# CAPTCHA	# ALLOWED	# RATE LIMIT	# REDIRECT	# LOG
Captcha Attempts Exceeded	11	11	0	0	0	0	0
Captcha Client Muted	2	0	0	0	0	2	0
Crawler	36	36	0	0	0	0	0
Feed Fetcher	8	8	0	0	0	0	0
Human	0	0	0	0	0	0	0
Invalid Captcha Response	48	33	8	0	0	0	7
Marketing	262	262	0	0	0	0	0
NULL	1	0	0	0	0	0	1
Scraper	33	33	0	0	0	0	0
Search Engine	155	155	0	0	0	0	0
Site Monitor	57	57	0	0	0	0	0
Tool	82	82	0	0	0	0	0
Uncategorized	0	0	0	0	0	0	0

ボットトラップボットの表示

NetScaler ADM でボットトラップを表示するには、NetScaler ADC インスタンスでボットトラップを構成する必要があります。詳しくは、「[ボット管理](#)」を参照してください。

Applications											Instances	
Total Bots	Total Human Browsers	Bot Human Ratio	Signatured Bots	Fingerprinted Bots	Rate Based Bots	IP Reputation Bots	Whitelist Bots	Blacklist Bots	Honeytrap Bots			
Total Bots on Instance 10.106.154.240 are 33.7 K											BLR_240 (10.106.154.240)	
test_vserve	33.7 K	6	100:0	4	33.45 K	0	0	0	244	10.217.219.38	10.217.32.56	

ボットトラップを識別するために、ウェブページでスクリプトが有効になり、このスクリプトは人間からは見えますが、ボットには表示されません。このスクリプトがボットによってアクセスされると、NetScaler ADM はボットトラップを識別してレポートします。

仮想サーバーをクリックし、「ゼロピクセルリクエスト」を選択します。

BOT CATEGORY	TOTAL	# DROPPED	# CAPTCHA	# ALLOWED	# RATE LIMIT	# REDIRECT	# LOG
Invalid DeviceFP	33450	33450	0	0	0	0	0
Zero Pixel Request	246	0	0	0	0	0	246
Human	100	0	0	100	0	0	0

TPS ボットの表示

NetScaler ADM で表示できる TPS ボットのカテゴリを次に示します。

- 接続元 IP

- 地理的位置
- ホスト
- URL

仮想サーバーをクリックして TPS ボットを表示します。

Applications											Sort By	Total Bots	Instances
Total Bots on Instance 10.106.154.240 are 9.77 K												>	BLR_240 (10.106.154.240)
	Total Bots	Total Human Browsers	Bot Human Ratio	Signed Bots	Fingerprinted Bots	Rate Based Bots	IP Reputation Bots	Whitelist Bots	Blacklist Bots	Bot Traps	TPS Bots		10.217.219.38
test_lb1	440	0	100 : 0	0	0	0	0	0	0	0	440		
test_vserver	9.33 K	0	100 : 0	0	0	0	0	0	0	5	9.32 K		

[ TPS ボット ] カテゴリをクリックして、ボットの詳細を表示します。

All	Good	Bad	Source IP ( 5 )									
			BOT CATEGORY	TOTAL	# DROPPED	# REDIRECT	# RESET	# ALLOWED	# LOG	# CAPTCHA	# MITIGATION	# RATE LIMIT
			Source IP	5	0	0	0	0	5	0	0	0

詳細ページが表示されます。

Analytics > Security > Bot Insight > test\_vserver > Bot Attack Category

Bot-Category = "Source IP" [X] Last 1 Hour [v] Search

Timeline Details 19 Aug 2020, 10:41 to 19 Aug 2020, 11:41

ATTACK TIME	CLIENT IP	BOT TYPE	SEVERITY	ACTION TAKEN	BOT CATEGORY	BOT DETECTION	LOCATION	REQUEST URL
Aug 19 04:52 PM - A...	10.102.103.25	Bad	High	Log	Source IP	TPS	Unknown	http://10.106.154.24...
Instance IP: 10.106.154.240				HTTP Request URL: http://10.106.154.242/test_site/data2				
Country Code: Unknown				Region: Unknown				
Profile Name: bot_profile				Domain Name: 10.106.154.242				
> Aug 19 04:52 PM - A...	10.102.103.25	Bad	High	Log	Source IP	TPS	Unknown	http://10.106.154.24...
> Aug 19 04:52 PM - A...	10.102.103.25	Bad	High	Log	Source IP	TPS	Unknown	http://10.106.154.24...

モバイル (Android) アプリケーションのボットカテゴリを表示する

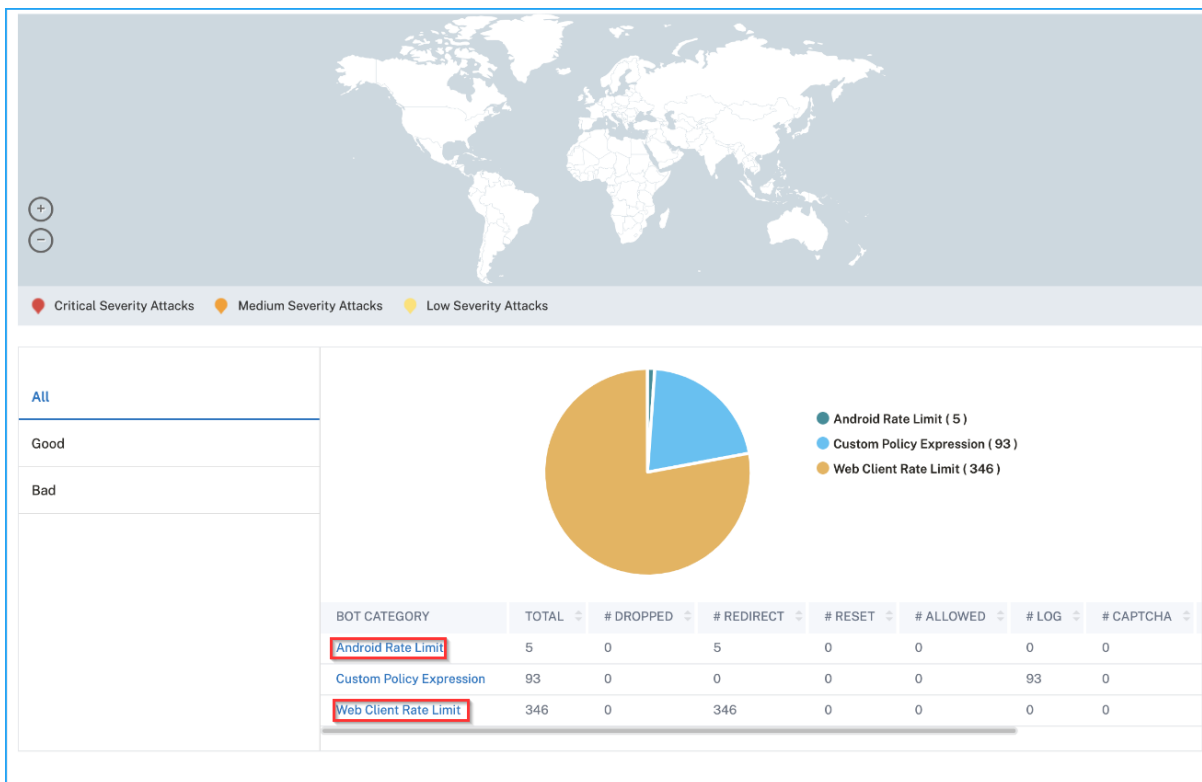
モバイル (Android) アプリケーションのボットを表示するには、NetScaler ADC で指紋検出技術を構成する必要があります。詳しくは、「モバイルアプリケーション用のデバイスフィンガープリント手法の構成」を参照してください

い。

NetScaler ADC で設定を構成すると、NetScaler ADM で次のボットカテゴリを表示できます。

- Web クライアントレート制限
- Android レート制限
- Web クライアントデバイス
- Android 端末

仮想サーバーをクリックして、モバイルアプリケーションに適用可能なボットカテゴリを表示します。

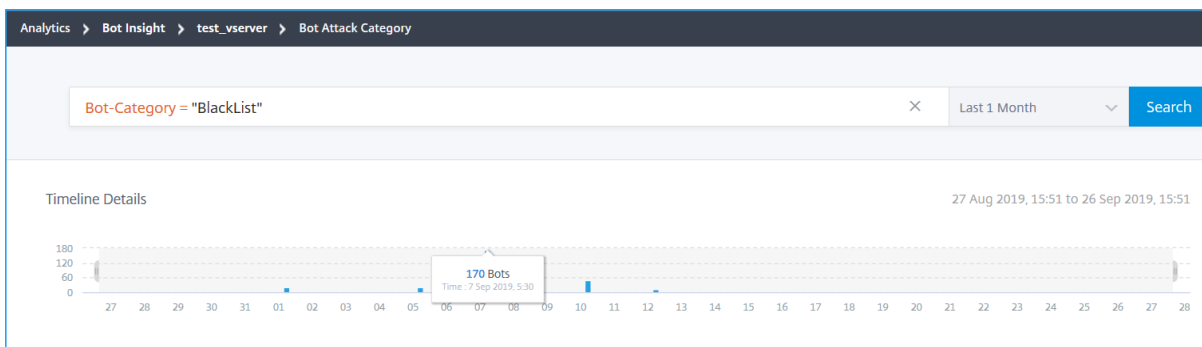


### ボットの詳細の表示

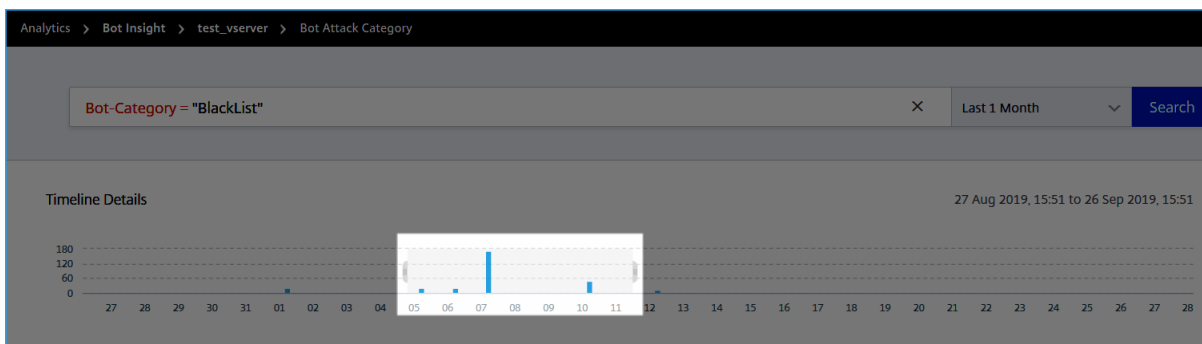
詳細をドリルダウンするには、[ボット カテゴリ] の下のボット攻撃タイプをクリックします。たとえば、ブロックリストされたボット攻撃の詳細を表示する場合は、[ボットカテゴリ] の [ブロックリスト] をクリックします。

攻撃時間、ボット攻撃の総数などの詳細が表示されます。





棒グラフをドラッグして、ボット攻撃で表示する特定の時間範囲を選択することもできます。



ボット攻撃の追加情報を取得するには、をクリックして展開します。

Instance Name	Instance IP	Bot Type	Severity	Action	Bot-Category	Bot-Profile	Location	Request URL
▼ Sep 09 02:48 P...	10.102.1.98	Bad	Critical	Drop	BlackList	BlackList	Bangalore	/black_list_test...
Instance IP: 10.106.154.240		Total Bots: 1						
HTTP Request URL: /black_list_test.html		Country Code: IN						
Region: Karnataka		Profile Name: bot_profile						

- **インスタンス IP**—Citrix ADC インスタンスの IP アドレスを示します
- **Total Bots**—特定の時間に発生したボット攻撃の総数を示します。
- **「HTTP 要求 URL」**—ブロッカー一覧に構成された URL を示します。
- **国コード**—ボット攻撃が発生した国を示します。
- **地域**—ボット攻撃が発生した地域を示します
- **プロファイル名**—設定時に指定したプロファイル名を示します

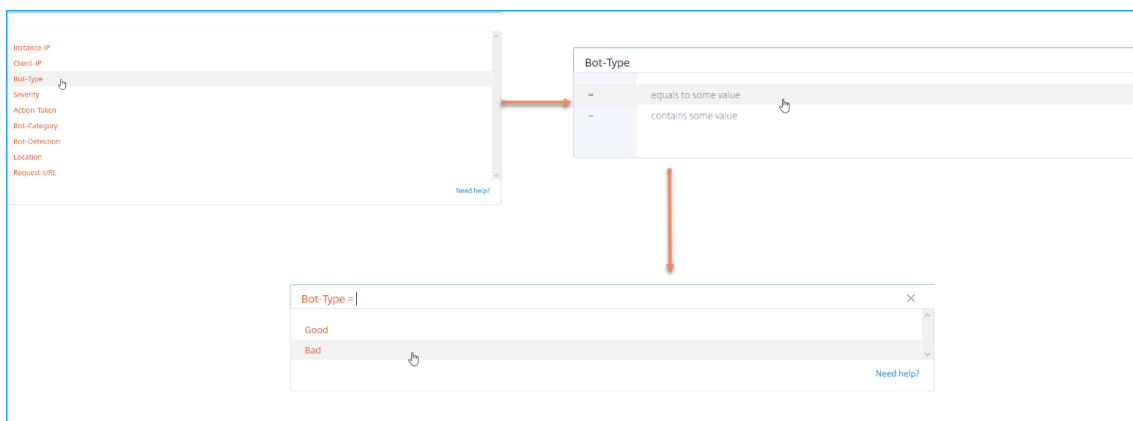
### 高度な検索

検索テキストボックスと期間リストを使用して、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、検索ボックスに次の検索候補のリストが表示されます。

- インスタンス **IP** –NetScaler ADC インスタンスの IP アドレス
- クライアント **IP** –クライアント IP アドレス
- ボットタイプ–良し悪しなどのボットタイプ
- 重要度–ボット攻撃の重大度
- アクション撮影–ボット攻撃後に実行されるアクション（ドロップ、アクションなし、リダイレクトなど）
- **Bot-Category**：ブロックリスト、許可リスト、指紋などのボット攻撃のカテゴリ。カテゴリに基づいて、ボットアクションをそのカテゴリに関連付けることができます
- ボット検出–NetScaler ADC インスタンスで構成したボット検出タイプ（ブロックリスト、許可リストなど）
- 場所–ボット攻撃が発生した地域/国
- **Request-URL** –ボット攻撃を受ける可能性のある URL

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。たとえば、すべての不良ボットを表示したい場合:

1. 検索ボックスをクリックし、ボットタイプを選択します
2. 検索ボックスをもう一度クリックし、演算子 **=** を選択します。
3. 検索ボックスをもう一度クリックし、「**Bad**」を選択します
4. [ 検索 ] をクリックして結果を表示します



## アプリケーションのセキュリティ違反の詳細を表示する

February 6, 2024

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、攻撃に対して非常に脆弱になっています。NetScaler ADM を使用すると、アクション可能な違反の詳細を視覚化し、アプリケーションを攻撃から保護できます。単一ページソリューションの [ 分析 ] > [ セキュリティ ] > [ セキュリティ違反 ] に移動して、次の操作を行います。

- 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て、アプリケーションを可視化
- 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する
- アプリケーションを保護するための是正措置を講じる

「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。

- **[Application Overview]**: 違反合計、WAF および Bot 違反の合計、国別の違反など、アプリケーションの概要を表示します。詳しくは、「[アプリケーションの概要](#)」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。

#### 前提条件

メトリクスコレクタが有効になっていることを確認します。デフォルトでは、メトリクスコレクターは NetScaler ADC インスタンスで有効になっています。詳細については、「[インテリジェントアプリケーション分析の構成](#)」を参照してください。

## SSL Insight

February 6, 2024

SSL Insight は、セキュアな Web トランザクション (HTTPS) を可視化し、IT 管理者は、セキュアな Web トランザクションのリアルタイムおよび履歴の統合監視を提供することで、NetScaler ADC 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ます。状態を把握することで管理者は以下の評価を行うことができます。

- 構成変更が顧客の使用に与える影響の特定: 管理者は、SSLv3 の無効化や RC4-MD5 などの暗号の削除などの構成変更によるクライアントへの影響を把握できます。そのためには、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します。
- クライアントのパフォーマンスを定量化: 管理者は、使用された SSL 暗号化/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、アプリケーションの応答時間への影響を把握できます。
- アプリケーションセキュリティ: セキュリティーの低いプロトコル、暗号、または弱い鍵強度でトランザクションが実行されているアプリケーションがないかを評価します。

NetScaler ADC インスタンスで SSLAnalytics を有効にすると、SSL 統計情報が記録され、SSL トランザクションごとに記録されます。この統計により SSL フローの詳細が分かります。また、成功した接続はすべて CitrixApplication

## Delivery Management (ADM)

Analytics によってログに記録され、表示されます。

SSL Insight は、NetScaler ADM Analytics によって表示される次の重要な情報を提供します。

- SSL プロトコルのバージョンがネゴシエ
- 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 フロントエンドエラーとバックエンドエラー

### 注

SSL 接続が成功すると、SSL AppFlow のロギングは各トランザクションの最後に行われます。

## 前提条件

- SSL Insight を構成する NetScaler ADC インスタンスは、NetScaler ADC ソフトウェアリリース 11.1 51.21 以降を実行している必要があります。11.1 51.21 を実行する ADC インスタンスで次のコマンドを実行して、SSL Insight トランスポートタイプとして Logstream を有効にします。

1. `enable ns mode ulfd`

2. `add ulfd server <IP Address of the ADM>`

バージョン 12.0 以降を実行する ADC インスタンスの場合は、ADM から AppFlow を有効にしなが、トランスポートタイプとして Logstream を選択します。

- NetScaler ADM バージョンとビルドは、NetScaler ADC のバージョンとビルドと同等かそれ以上でなければなりません。たとえば、NetScaler ADM 11.1 ビルド 61.7 をインストールしている場合は、NetScaler ADC 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ます。

## SSL Insight 構成

次の要素を有効にした場合、SSL Insight メトリックは Web Insight レポートに組み込まれます。

- 各 Citrix ADC インスタンスで AppFlow for Web Insight を有効にします。
- 各 Citrix ADC インスタンスで ULFD モードを有効にします。
- 各 NetScaler ADC インスタンスで必要な AppFlow パラメータを有効にします。

## AppFlow 機能を有効にする

### 注

AppFlow 機能は、Citrix ADM または各 Citrix ADC インスタンスから有効にできます。

NetScaler ADM から AppFlow 機能を有効にするには:

Citrix ADM が **13.0** ビルド **41.x** 以降の場合:

1. [ネットワーク]>[インスタンス]>[**NetScaler ADC**] に移動し、インスタンスタイプを選択します。たとえば、VPX です。
  2. インスタンスを選択し、[アクションの選択] リストから [**Analytics の設定**] をクリックします。
  3. [仮想サーバーでの **Analytics の設定**] ページで、仮想サーバーを選択し、[**Analytics を有効にする**] をクリックします。
  4. 「アナリティクスを有効にする」ウィンドウで:
    - a) **Web** インサイトを選択
    - b) **Logstream** をトランスポートモードとして選択
- ### 注
- NetScaler ADC 12.0 以前の場合、**IPFIX** はトランスポートモードのデフォルトのオプションです。NetScaler ADC 12.0 以降では、トランスポートモードとして [ログストリーム] または [**IPFIX**] を選択できます。
- IPFIX とログストリームの詳細については、「ログストリームの[概要](#)」を参照してください。
- c) 式はデフォルトで true です
  - d) [**OK**] をクリックします

Enable Analytics
✕

**Selected Virtual Server - Load Balancing: 3**

Web Insight

Security Insight

▼ Advanced Options

Transport Mode

Logstream     IPFIX

Instance level options

Enable HTTP X-Forwarded-For

Citrix Gateway

▼ Expression Configuration

Select expression for Load Balancing/Content Switching

Select Expression

▼

Edit Expression

true

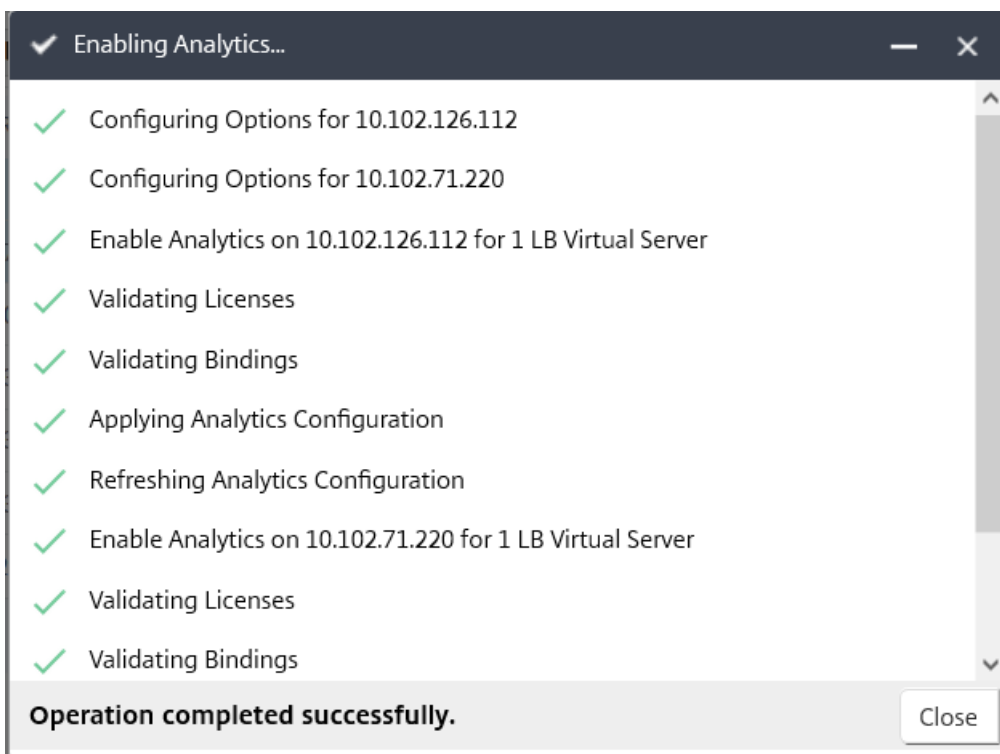
OK

Close

注

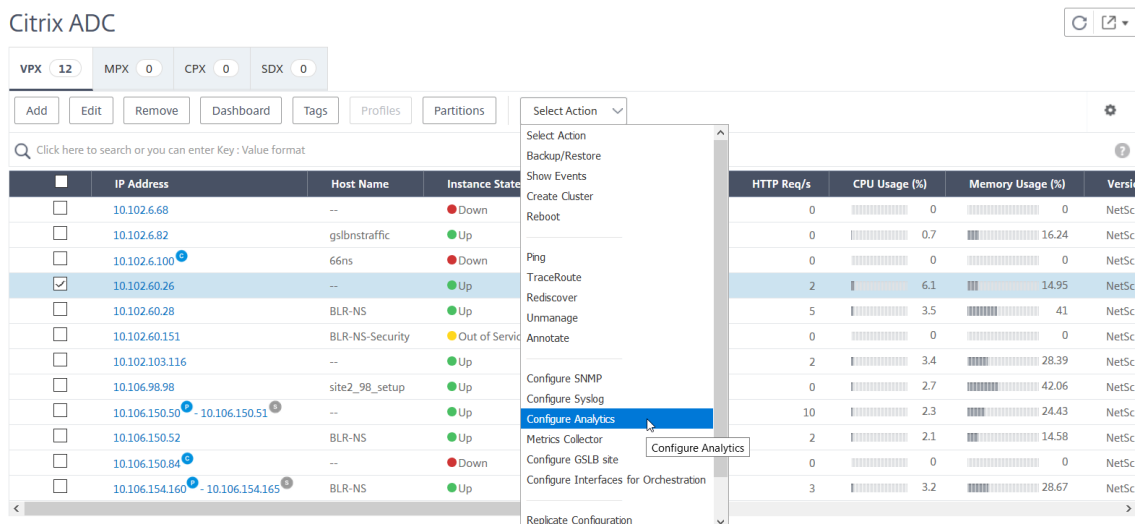
- ライセンスされていない仮想サーバーを選択すると、NetScaler ADM はまずそれらの仮想サーバーのライセンスを取得し、次に分析を有効にします。
- 管理パーティションでは、**Web Insight** のみがサポートされます
- キャッシュリダイレクト、認証、GSLB などの仮想サーバーでは、分析を有効にすることはできません。エラーメッセージが表示されます。

[OK] をクリックすると、NetScaler ADM は選択した仮想サーバー上で分析を有効にするために処理します。



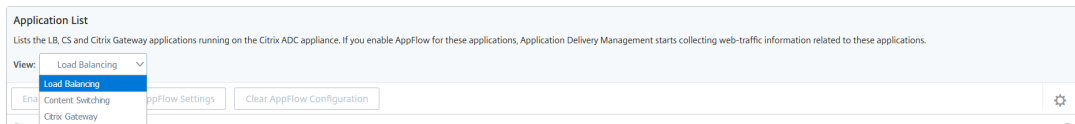
Citrix **ADM** が **13.0** ビルド **36.27** 以前の場合:

1. [ネットワーク] > [インスタンス] > [Citrix ADC] に移動し、分析を有効にする NetScaler ADC インスタンスを選択します。
2. [アクションの選択] リストから、[Analytics の設定] を選択します。

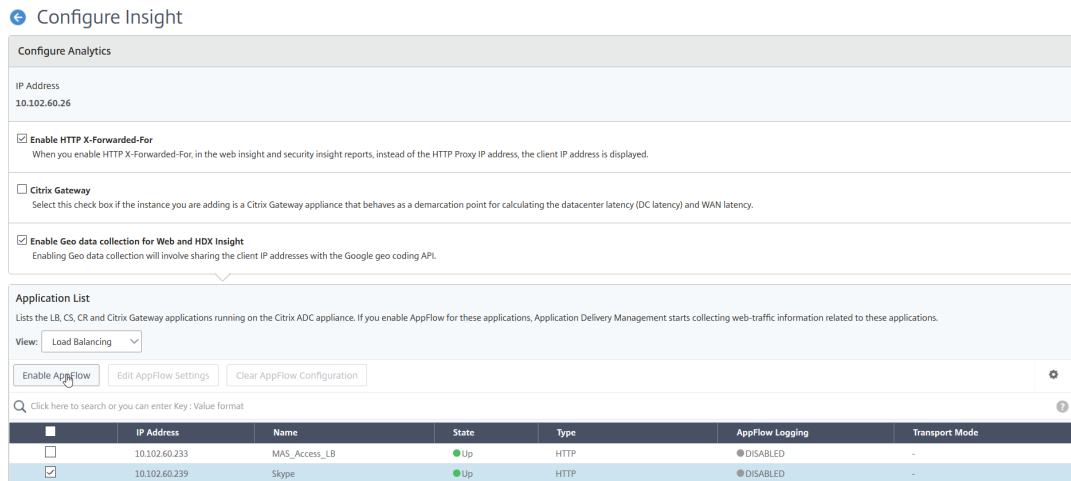


3. [\*\* Insight の設定 \*\*] ページで、次の操作を行います。

a) ロードバランシングまたはコンテンツスイッチングの アプリケーションリスト を選択します。



b) 仮想サーバーを選択し、[ **AppFlow** を有効にする ] をクリックします。



4. [AppFlow を有効にする] ダイアログボックスで、次の操作を行います。

- テキストボックスに **true** と入力します。
- 転送モードとして [ ログストリーム ] を選択します。

注: Citrix では、転送モードとして Logstream を選択することを推奨しています。

- [ **Web Insight** ] を選択し、[ **OK** ] をクリックします。



### Enable AppFlow

Select Expression

Load Balancing

▼

true

Transport Mode  IPFIX  Logstream

Web Insight

Client Side Measurement

Security Insight

If there is a firewall between Citrix ADM and the Citrix ADC instance, please make sure the TCP port 5557 is open. This is to allow ADM to collect AppFlow traffic.

OK

Cancel

**NetScaler ADC GUI** を使用して **AppFlow** 機能を有効にするには:

NetScaler ADC インスタンスの GUI で、[構成] > [システム] > [設定] の順に選択し、[高度な機能の構成] をクリックし、[AppFlow] を選択します。

### SSL Insight パラメータの有効化

NetScaler ADC インスタンスごとに、一部の HTTP パラメーターを有効にして、NetScaler ADM で SSL Insight レコードを表示する必要があります。

**Citrix ADC** 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には:

1. 「構成」 > 「システム」 > 「AppFlow」 に移動し、「AppFlow 設定の変更」をクリックします。
2. 「HTTP ドメイン」、「HTTP ホスト」、「HTTP メソッド」、「HTTPURL」、「HTTP ユーザーエージェント」、「HTTP コンテンツタイプ」のチェックボックスを選択します。
3. [OK] をクリックします。

## ← Configure AppFlow Settings

- |   |  |
|---|--|
| <input checked="" type="checkbox"/> HTTP URL            | <input type="checkbox"/> AAA Username                            |
| <input type="checkbox"/> HTTP Cookie                    | <input type="checkbox"/> HTTP Referrer                           |
| <input checked="" type="checkbox"/> HTTP Method         | <input checked="" type="checkbox"/> HTTP host                    |
| <input checked="" type="checkbox"/> HTTP User-Agent     | <input checked="" type="checkbox"/> HTTP Content-Type            |
| <input type="checkbox"/> HTTP Authorization             | <input type="checkbox"/> HTTP X-Forwarded-For                    |
| <input type="checkbox"/> HTTP Via                       | <input type="checkbox"/> HTTP Location                           |
| <input type="checkbox"/> HTTP Setcookie                 | <input type="checkbox"/> HTTP Setcookie2                         |
| <input type="checkbox"/> Client Traffic Only            | <input type="checkbox"/> Connection Chaining                     |
| <input checked="" type="checkbox"/> HTTP Domain         | <input type="checkbox"/> Skip Cache Redirection HTTP Transaction |
| <input type="checkbox"/> Stream Identifier Name logging | <input type="checkbox"/> Stream Identifier Session Name logging  |
| <input type="checkbox"/> Security Insight Traffic       | <input type="checkbox"/> Cache Insight                           |
| <input type="checkbox"/> Subscriber Awareness           |  |

### SSL Insight メトリックスの表示

NetScaler ADM SSL Insight メトリックは、NetScaler ADC インスタンスが処理する SSL トランザクションのパフォーマンスを詳細に表示します。クライアント、サーバー、またはアプリケーションレベルの SSL Insight メトリック、および成功した SSL トランザクションおよび失敗した SSL トランザクションのメトリックを表示できます。これらのメトリックを使用すると、**NetScaler ADC HTTPS** 設定と **SSL** 証明書設定を分析および最適化し、パフォーマンスの問題を追跡できます。

注:

グループを作成するときに、グループに役割を割り当てたり、グループへのアプリケーションレベルのアクセスを提供したり、ユーザーをグループに割り当てたりすることができます。NetScaler ADM 分析では、仮想 IP アドレスベースの認証がサポートされるようになりました。ユーザーは、権限のあるアプリケーション（仮想サーバー）のみのすべての Insight のレポートを表示できるようになりました。グループおよびグループへのユーザの割り当ての詳細については、「[グループを設定する](#)」を参照してください。

**NetScaler ADM** で **SSL Insight** メトリックスを監視するには:

以下の SSL メトリックスを表示できます。

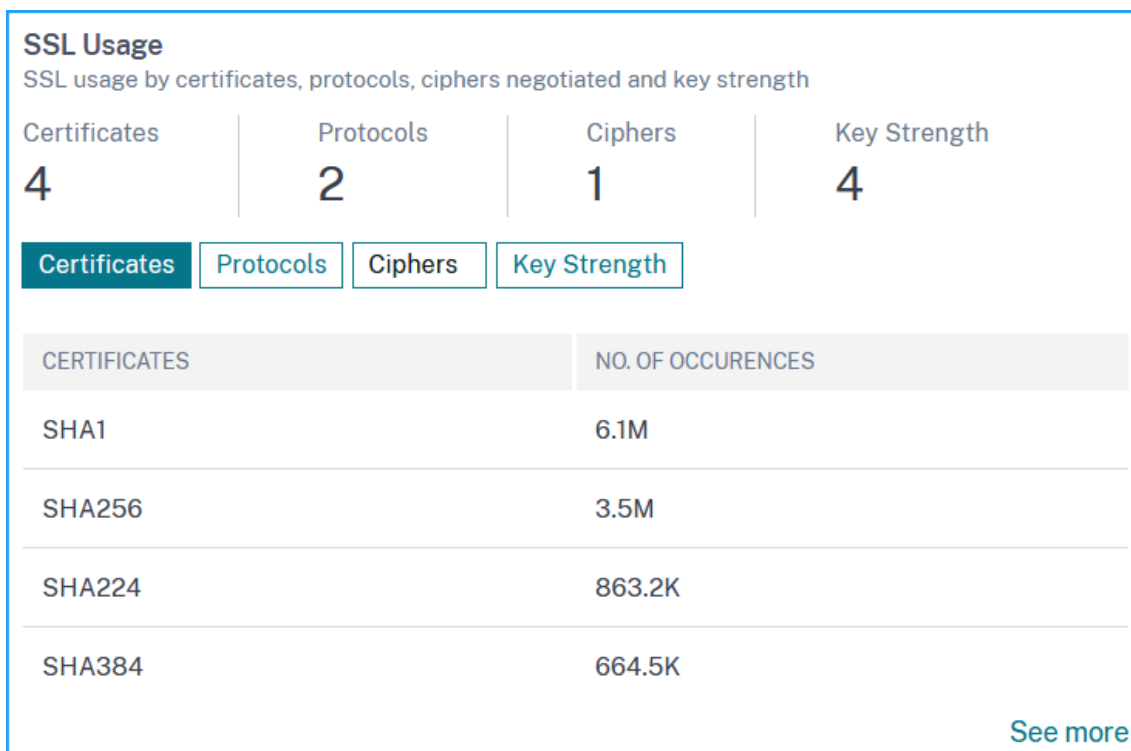
- アプリケーション。[アプリケーション] > [ダッシュボード] に移動し、アプリケーションをクリックし、[**Web Insight**] タブを選択して詳細なメトリックスを表示します。詳細については、「[アプリケーション使用状況分析](#)」を参照してください。
- すべてのアプリケーション。[アプリケーション] > [**Web Insight**] に移動し、[アプリケーション] タブと [クライアント] タブをクリックして SSL メトリックを表示します。

ユースケース:**SSL** トランザクションの概要を取得する

次のユースケースは、SSL Insight を使用してさまざまな SSL パラメータの使用状況进行评估し、セキュリティ対策を改善する方法について説明しています。

通信に SSL トランザクション (HTTPS) を使用している一連のアプリケーションがあり、SSL コンポーネントを監視するように NetScaler ADM を構成しているとします。最も注意が必要なアプリケーションに特に注意を払えるように、アプリケーションを頻繁に確認する必要があります。1 つのアプリケーションまたはすべてのアプリケーションの **Web Insight** ダッシュボードには、[SSL エラー] と **[SSL \*\* 使用状況]** の下に次の SSL\*\* パラメーターの概要が表示されます。

- SSL 証明書
- SSL プロトコル
- SSL 暗号
- SSL キーの強度
- SSL 障害—フロントエンド
- SSL 障害—バックエンド



各タブをクリックすると、詳細を表示できます。

## ユースケース: クライアントの **SSL** メトリクス

クライアントのリスト (IP アドレスで識別) と、クライアントごとの合計発生数を確認できます。[アプリケーション] > [Web Insight] に移動し、[クライアント] タブを選択して [SSL 使用状況] の下に詳細を表示します。

メトリックをクリックして詳細を表示し、[クライアント] で任意のクライアント IP アドレスをクリックすると、選択したクライアントの SSL メトリックが表示されます。

The screenshot shows the NetScaler Web Insight interface for 'Certificate-SHA1'. It features a breadcrumb trail 'Applications > Web Insight > Applications > Certificate-SHA1' and a 'Last 1 Month' filter. The main content is divided into two sections: 'Applications' and 'Clients'.

**Applications Section:** 'Top apps with high bandwidth and response time'. It has tabs for 'Requests', 'Bandwidth', and 'Response Time'. The table below shows the following data:

APPLICATION	BANDWIDTH (AVG)	RESPONSE TIME (AVG)	REQUESTS
Internet_Banking	2.37 GB	1.65 s	3.2M
Mobile_Banking	1.89 GB	584 ms	2.7M
Employee-Portal	803.69 MB	3 ms	278.3K

A 'See more' link is present at the bottom right of this section.

**Clients Section:** 'Top clients accessing the application'. It has tabs for 'Requests', 'Client Network Latency', and 'Render Time'. The table below shows the following data:

CLIENT	CLIENT NETWORK LATENCY (AVG)	RENDER TIME (AVG)	REQUESTS
[Redacted]	<1 ms	<1 ms	5.9M
[Redacted]	<1 ms	<1 ms	70.8K

## TCP Insight

February 6, 2024

Citrix Application Delivery Management (ADM) の TCP Insight 機能は、データ転送におけるネットワークの輻輳を回避するために Citrix ADC アプライアンスで使用される最適化手法と輻輳制御戦略 (またはアルゴリズム) のメトリックを監視するための簡単でスケーラブルなソリューションを提供します。この機能では、TCP を最適化して、またはしないで TCP ファイルのダウンロードやアップロードのパフォーマンスを測定する「TCP スピードレポート」機能を使用します。

データ量、スループット、速度などの主要なトランスポート層メトリックを表示し、その情報を使用して NetScaler ADC インスタンスが処理するトラフィック量を測定し、TCP 最適化の利点を検証できます。上記のメトリックでは、ストリーム方向 (クライアントから NetScaler ADC、NetScaler ADC からオリジンサーバー)、TCP ポート、および仮想 LAN による内訳が提供されています。

## 前提条件

TCP Insight 機能の構成を開始する前に、以下の前提条件が満たされていることを確認してください。

- NetScaler ADC インスタンスは、ソフトウェアバージョン 11.1 ビルド 51.21 以降で実行されています。
- ソフトウェアバージョン 11.1 ビルド 51.21 以降で動作する NetScaler ADM がインストールされています。
- アプリケーション用に構成されているすべての仮想サーバーには、NetScaler ADM の管理と監視のライセンスが付与されます。  
NetScaler ADM ライセンスについて詳しくは、「[ライセンス](#)」を参照してください。

## TCP Insight の有効化

TCP Insight メトリックを表示する前に、NetScaler ADM でこの機能を有効にする必要があります。

**TCP Insight** を有効にするには:

1. Web ブラウザで、Citrix ADM 仮想アプライアンスの IP アドレス（たとえば、<http://192.168.100.1>）を入力します。
2. [User Name] と [Password] に管理者の資格情報を入力します。
3. [Analytics] > [設定] に移動し、[Analytics の機能を有効にする] をクリックします。
4. [Analytics の機能を有効にする] ページで、[TCP Insight を有効にする] を選択します。
5. 確認ウィンドウで、[OK] をクリックします。

## NetScaler ADM で TCP インサイトメトリクスを表示する

NetScaler ADM で TCP Insight を有効にすると、トラフィックモード（インターネットまたはモバイルデータ）、データボリューム、スループット、インターフェイス、ポート、平均アップロード速度、平均ダウンロード速度などの主要なトランスポート層情報を表示できます。

**NetScaler ADM** で **TCP Insight** メトリックを表示するには:

[アナリティクス] > [TCP インサイト] に移動します。

棒グラフにマウスポインターを合わせると、対応するトランスポートテクニックのデータ量が表示されます。また、グラフの下にデータボリュームとその他のメトリックを表示できます。

注: 表の設定アイコンを使用して、グラフに表示されるメトリクスをカスタマイズできます。メトリックに関連する期間を選択したり、タイムスライダーを使用して期間を調整することもできます。

**TCP Insight** リストから選択して、インターフェイス、ポート、ビットレートなどのメトリックを表示することもできます。

## 使用例

以下のユースケースは、NetScaler ADC アプライアンスで TCP Insight を使用方法のいくつかを示しています。

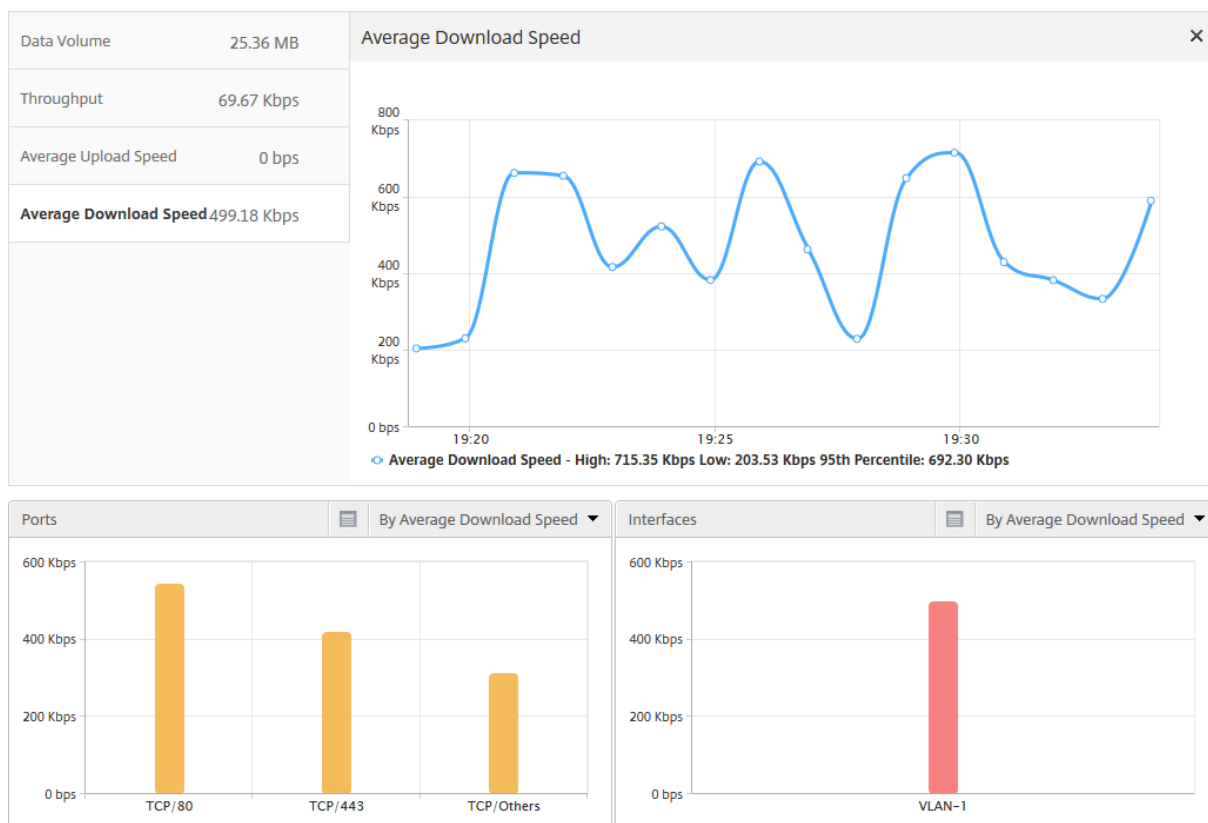
- TCP 最適化のメリットを評価
- TCP パラメータの調整
- トラフィック量に対する TCP 最適化の影響を測定

### TCP 最適化のメリットを評価

NetScaler ADC TCP 最適化は、モバイル（無線）または企業ネットワーク（インターネット）に実際にどの程度のメリットがありますか。TCP 経路で発生するデータ転送の速度を表示して、最適化されていないパフォーマンスと最適化されたパフォーマンスを比較できます。これらの測定は、ダウンロード方向とアップロード方向（常に無線/クライアント側から）や異なる宛先ポート（HTTP (80) と HTTPS (443)）で個別に表示されます。

TCP Insight メトリクスを調べることで、TCP フローを最適化することで得られる速度の向上を定量化できます。

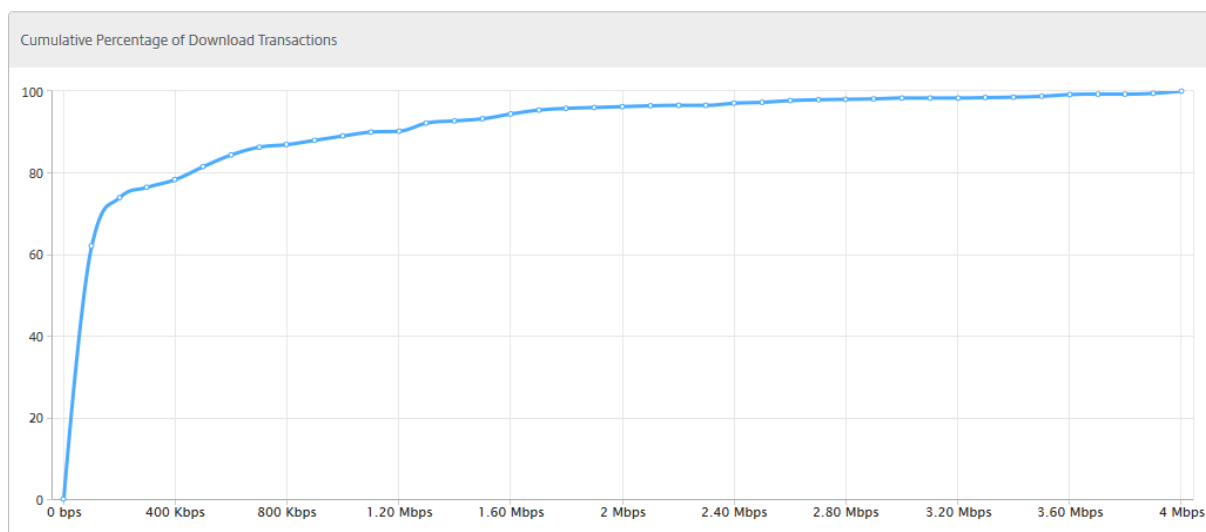
これらのパラメーターの概要を表示するには、NetScaler ADM にログオンし、[TCP Insight] タブをクリックします。次に、[側面] をクリックし、棒グラフまたはグラフの下から [インターネット] または [ラジオ] を選択します。



## TCP パラメータの調整

異なる TCP プロファイルを使用すると、同じトラフィックから異なる出力が生成されます。このような状況では、NetScaler ADC がさまざまな TCP 最適化プロファイルを実行している期間の速度測定値を表示して比較したい場合があります。それらの結果を利用して、転送速度が上がるように TCP パラメータを調整したり、特定のお客様のネットワークでのユーザー体験を最大限に高める TCP プロファイルを作成したりできます。

レポートを表示するには、NetScaler ADM にログオンします。次に、[ **TCP Insight** ] タブで [ ビットレート ] をクリックし、棒グラフまたはグラフの下にある表から目的のビットレートを選択します。

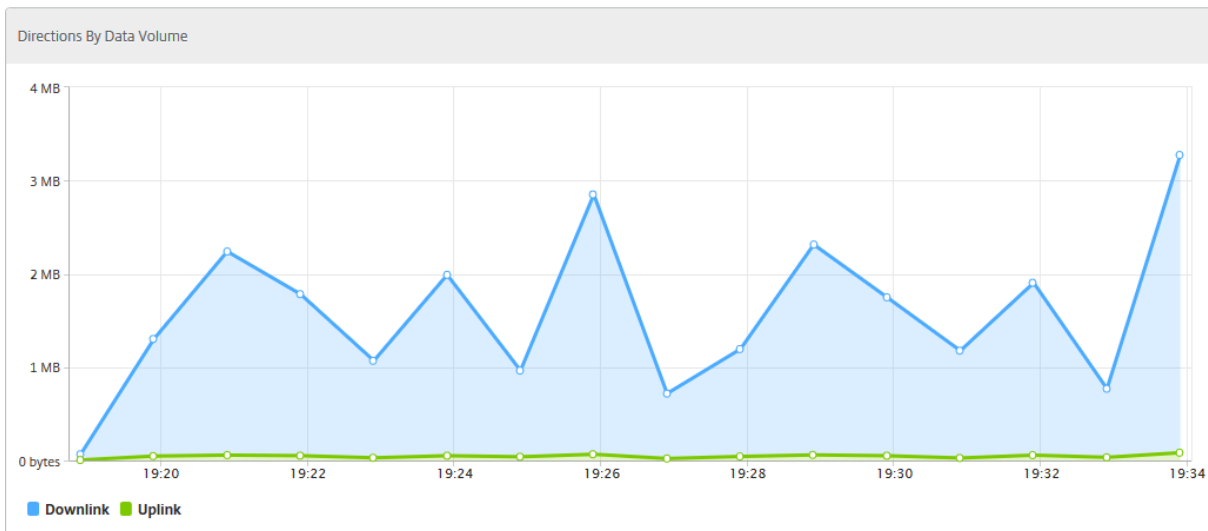


## トラフィック量に対する TCP 最適化の影響を測定

NetScaler ADC インスタンスが処理する IP 層のデータ量/スループットの測定値をさまざまな期間で比較して、TCP 最適化が加入者のデータ消費に及ぼす影響を評価できます。測定は、ネットワークの各サイド（無線サイドとインターネットサイド）、さまざまなトラフィックセグメント（さまざまなインターフェイスや VLAN によって線引き）、各方向（ダウンリンクとアップリンク）、さまざまな宛先ポート（HTTP と HTTPS）に個別に適用できます。この比較を利用して、TCP 最適化によりサブスクリバラーのデータ消費が促進されていることを確認できます。

測定値の概要を確認するには、NetScaler ADM にログオンし、「**TCP Insight**」タブの「サイド」をクリックし、棒グラフまたはグラフの下の表から「インターネット」または「ラジオ」を選択します。

タイムリストから別の時間枠を選択することもできます。期間は、スライダーを使用してカスタマイズできます。



## WAN Insight

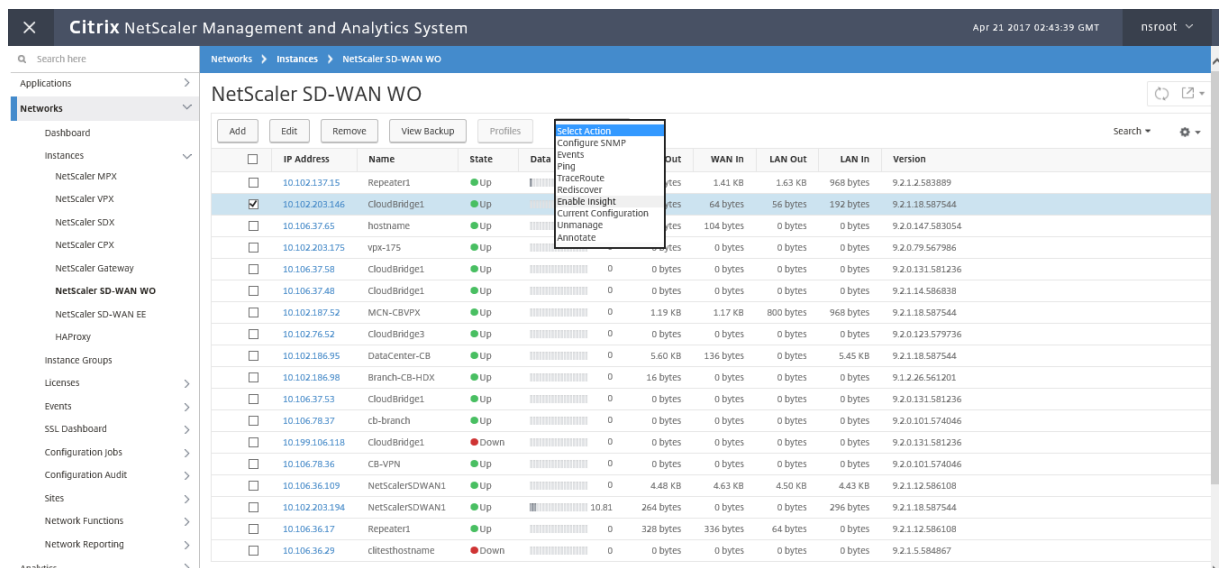
February 6, 2024

Citrix SD-WAN WAN 最適化 (WO) アプライアンスは、データセンターとブランチサイト間のネットワークを介したデータフローの効率を向上させることにより、WAN を介した多くのアプリケーションの配信を最適化します。

WAN Insight 分析により、管理者はデータセンターとブランチの WAN 最適化アプライアンスの間を流れる高速化および高速化されていない WAN トラフィックを簡単に監視できます。WAN Insight は、ネットワーク上のクライアント、アプリケーション、ブランチを可視化し、ネットワークの問題を効果的にトラブルシューティングできるようにします。ライブレポートと履歴レポートを使用すると、問題があればプロアクティブに解決できます。

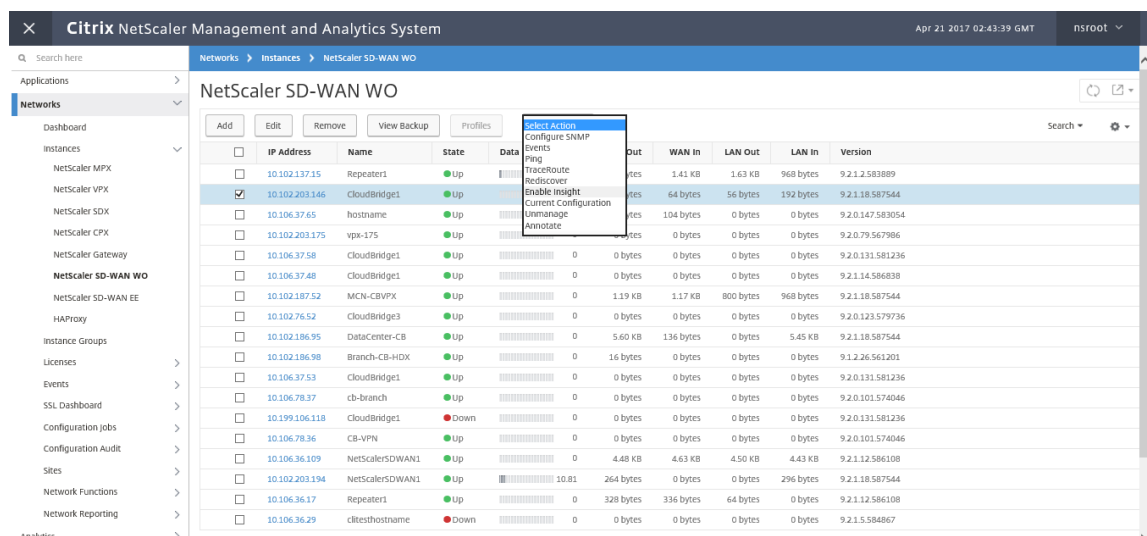
データセンター WAN 最適化アプライアンスで分析を有効にすると、NetScaler ADM はデータを収集し、データセンターとブランチ WAN 最適化アプライアンスのレポートと統計を提供できます。





**WAN** 最適化アプライアンス上で分析を有効にするには:

1. [ ネットワーク ] > [ インスタンス ] > [ **Citrix SD-WAN** ] に移動し、SD-WAN 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、[ **Analytics** の設定 ] を選択します。

3. 必要に応じて以下のパラメーターを選択します。

- **HDX Insight** の地理データ収集: クライアントの IP アドレスを Google Geo API と共有します。

- **AppFlow**: WAN 最適化インスタンスからのデータ収集を開始します。

- **TCP** と **WANOpt**: **TCP** と **WanOpt** のインサイトレポートを提供します。
- **HDX**: HDX Insight レポートを提供します。
- **HDX** 用の **TCP** のみ: HDX Insight レポートにのみ **TCP** を提供します。

Configure Insight

Enable data collection on the NetScaler SD-WAN WO instance, so that the performance of applications can be monitored.

Geo data collection for HDX insight

AppFlow

Data Set:

TCP and WANOpt  HDX  TCP only for HDX

4. **[OK]** をクリックします。

**WAN** インサイトレポートを表示するには、次の手順を実行します。

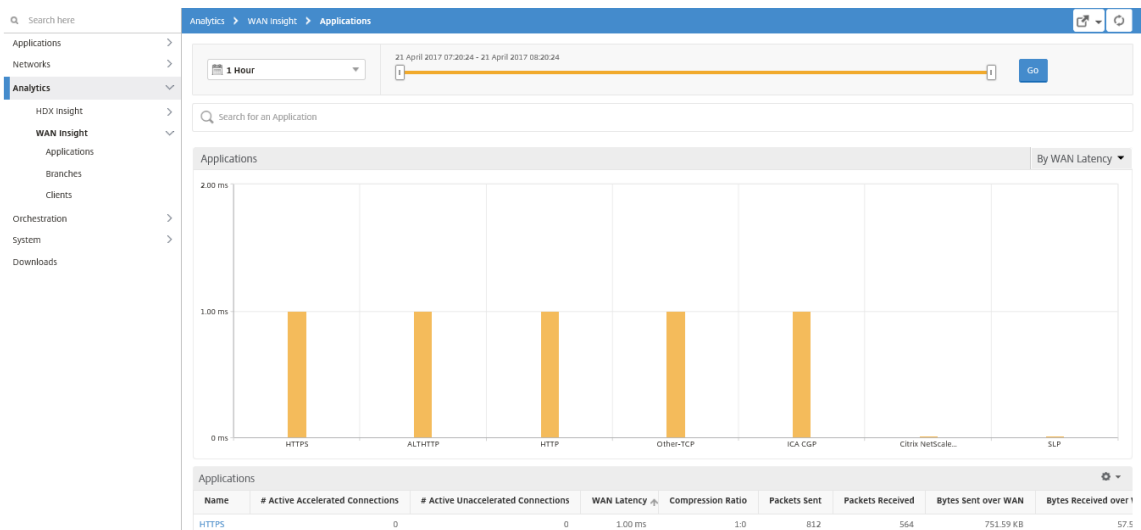
1. **[Analytics]** > **[WAN Insight]** に移動します。

注

WAN インサイトオプションは、SD-WAN WO インスタンスを NetScaler ADM に追加した後にのみ表示されます。

次のレポートを表示できます。

- アプリケーション - 選択した期間のすべてのアプリケーションの使用状況とパフォーマンスの統計を表示します。
- ブランチ - すべての WAN 最適化ブランチアプライアンスの使用状況とパフォーマンスの統計を表示します。
- **Clients** - 各ブランチで、WAN 最適化アプライアンスにアクセスするすべてのクライアントの使用状況とパフォーマンスの統計情報を表示します。



次のメトリックが表示されます。

測定基準	説明
Active Accelerated Connections	アクセラレーションが有効なアクティブ WAN 接続の数です。
Active Unaccelerated Connections	アクセラレーションが無効なアクティブ WAN 接続の数です。
WAN 遅延	アプリケーションとの対話中にユーザーに生じる遅延（ミリ秒単位）です。
圧縮率	選択した期間における、ブランチオフィスとデータセンターアプライアンス間のデータ圧縮率。
送信済みパケット	選択した期間に WAN 最適化アプライアンスからネットワーク経由で送信されたパケットの数です。
受信済みパケット	選択した期間に WAN 最適化アプライアンスがネットワークから受信したパケットの数です。
WAN で送信されたバイト数	選択した期間に Citrix WAN 最適化アプライアンスが WAN 経由で送信したバイト数。
WAN で受信したバイト数	選択した期間に WAN 最適化アプライアンスが WAN から受信したバイトの数です。
LAN RTO	選択した期間に WAN 最適化アプライアンスから LAN への再送信がタイムアウトになった回数です。
WAN RTO	選択した期間に WAN 最適化アプライアンスから WAN への再送信がタイムアウトになった回数です。
再送信パケット (LAN)	選択した期間に WAN 最適化アプライアンスから LAN ネットワークに再送信されたパケットの数です。
再送信パケット (WAN)	選択した期間に WAN 最適化アプライアンスから WAN ネットワークに再送信されたパケットの数です。

## Video Insight

February 6, 2024

ビデオインサイト機能は、NetScaler ADC アプライア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、カスタマーエクスペリエンスと運用効率を向上させます。次のようなメリットがあります。

- ピーク時間における混雑時にネットワークを管理する。
- 動画再生の一貫性を向上させ動画の再生速度低下を抑える。
- 新しい動画サービスオフファリング（Binge-on 動画サービスなど）を有効にする。

- 顧客が持続可能で最適な動画品質を選択できるようにする。
- サブスクリイパーに一貫性のあるユーザーエクスペリエンスを提供する。

NetScaler ADC アプライアンスは、ビデオトラフィックを最適化する際に、ビデオビットレートを動的にペースさせる特別なメカニズムと、ランダムサンプリング手法を使用して、最適化手法による節約額を推定します。NetScaler ADC ビデオ最適化機能について詳しくは、「[ビデオの最適化](#)」を参照してください。NetScaler ADC アプライアンスを NetScaler Application Delivery Management (ADM) と統合すると、NetScaler ADC アプライアンスを流れるビデオデータから重要な情報が収集されます。この情報を使用することで、最適化している場合としていない場合の ABR 動画トラフィックのパフォーマンスを比較したり、最適化による削減率を求めたりすることができます。

### 注

NetScaler ADM で提供される最適化されていないセッションの統計情報は、NetScaler ADC アプライアンスでランダムサンプリングで選択したセッションに対応します。ランダムサンプリングの詳細については、「[ビデオの最適化](#)」を参照してください。

NetScaler ADM Video Insight は、次の種類のビデオトラフィックに関するメトリックを提供します。

- HTTP 経由でのプログレッシブダウンロード (PD) 動画
- HTTP 経由の ABR 動画
- HTTPS 経由の ABR 動画
- QUIC 経由の YouTube ABR 動画

## Video Insight の構成

### 注

ビデオインサイトは、NetScaler ADC プレミアムライセンスを持つ NetScaler ADC インスタンスでサポートされます。NetScaler ADC Premium ライセンスは、NetScaler ADC Telco プラットフォーム (VPX T1000 および VPX-T) でサポートされています。

Citrix ADC インスタンスでビデオインサイトを構成するには、まず AppFlow 機能を有効にし、AppFlow コレクター、アクション、およびポリシーを構成して、ポリシーをグローバルにバインドします。コレクターを構成するときは、レポートを監視する Citrix ADM サーバーの IP アドレスを指定する必要があります。

NetScaler ADC インスタンスでビデオインサイトを構成するには、次のコマンドを実行して AppFlow プロファイルとポリシーを構成し、AppFlow ポリシーをグローバルにバインドします。

```
add appflow collector \<< 名前 \> -IPAddress \<< IP アドレス \> -port < ポート番号 > **Transport**  
logstream ポート番号 >
```

```
set appflow param -videoInsight ENABLED
```

```
add appflow action \<< 名前 \> -collectors \<< 文字列 \> -videoAnalytics ENABLED
```

**add appflow policy** \<名前\> \<規則\> \<アクション\>

**bind appflow global** \<ポリシー名\> \<優先度\> \[ \<goto 優先度式\> \] \[-type \<タイプ\> \]

**ns** モードを有効にする **ulfd**

機能を有効にする AppFlow

サンプル

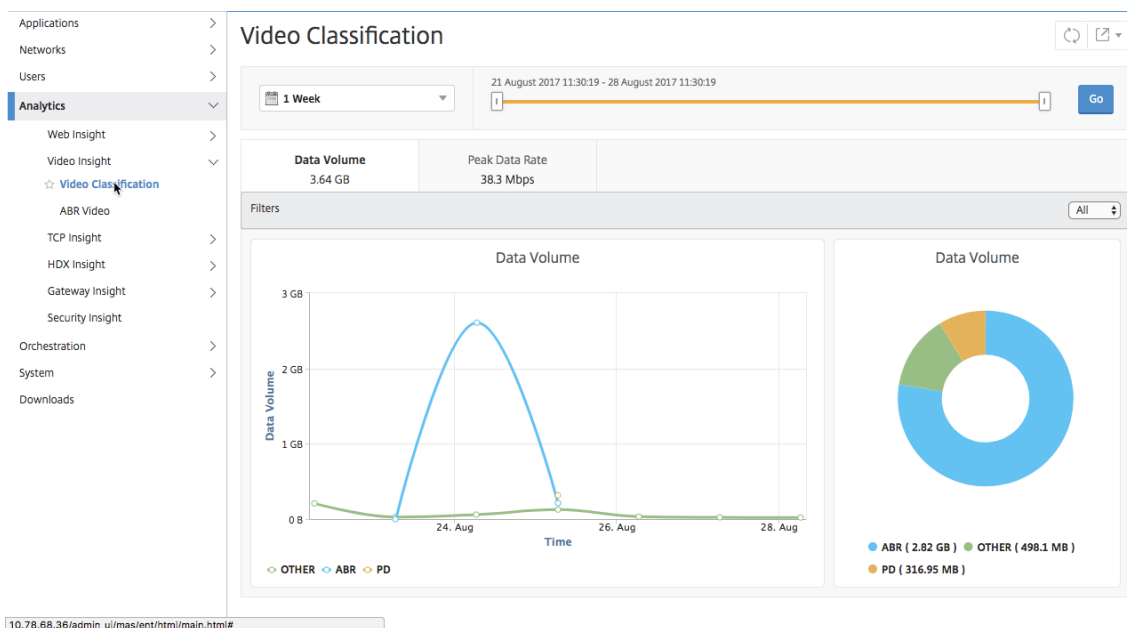
```
1 add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -  
  Transport logstream  
2 set appflow param -videoInsight ENABLED  
3 add appflow action act1 -collectors col1 -videoAnalytics ENABLED  
4 add appflow policy appol true act1  
5 bind appflow global appol 1  
6 enable ns mode ulfd  
7 enable feature appflow  
8 <!--NeedCopy-->
```

## NetScaler ADM でのビデオインサイトメトリックの表示

NetScaler ADM で Video Insight を有効にすると、ビデオの分類、データボリューム、ピークデータレート、ABR ビデオの再生などのビデオの最適化指標を表示できます。これらのメトリックにより、ネットワークを分析して動画を最適化し、サブスクライバーのエクスペリエンス、操作の効率、その他のパフォーマンス基準を改善することができます。

**Citrix ADM** でビデオインサイトメトリックを表示するには:

1. Web ブラウザで、Citrix ADM 仮想アプライアンスの IP アドレス（たとえば、<http://192.168.100.1>）を入力します。
2. **[User Name]** と **[Password]** に管理者の資格情報を入力します。
3. **[Analytics] > [Video Insight]** に移動します。



注

グラフの **OTHER** という凡例で示されている値は、選択したフィルタに応じて、ビデオトラフィックの非 ABR データと PD 以外のデータを表します。

- **All**：ビデオトラフィック内の非 ABR (HTTP、HTTPS、および QUIC) および非 PD (HTTP) データの合計。
- **HTTP** –ビデオトラフィックの非 ABR データと非 PD データの合計。
- **HTTPS** –ビデオトラフィックの非 ABR ビデオデータの合計。
- **QUIC** –ビデオトラフィックの非 ABR ビデオデータの合計。

ネットワーク効率の表示

February 6, 2024

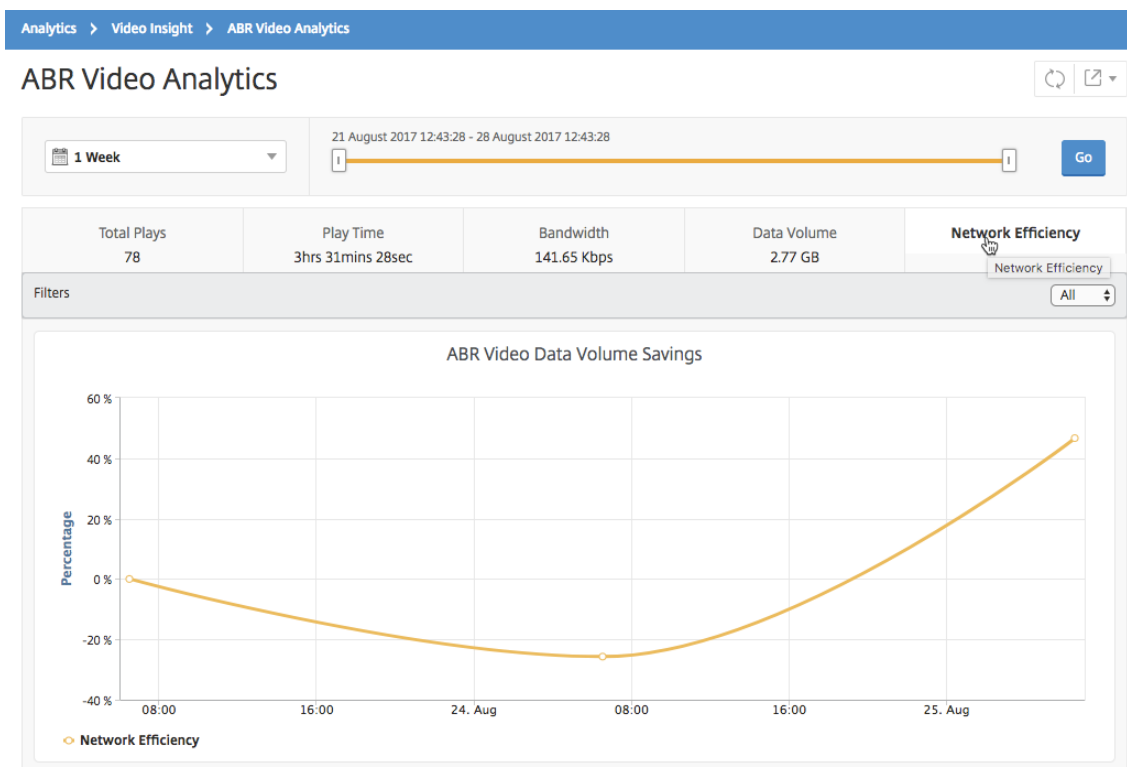
特定の時間枠について、Citrix Application Delivery Management (ADM) は、その時間枠における最適化されたビデオセッションと最適化されていないビデオセッションの比率を示すグラフを提供します。グラフには、最適化により削減された帯域幅の割合も表示されます。削減された帯域幅の割合は、次の式により計算されます。

保存帯域幅の割合 = 最適化された **ABR** ビデオデータボリュームの平均/最適化されていない **ABR** ビデオデータボリュームの平均。

最適化によって節約された帯域幅の割合を確認するには:

1. [分析] > [ビデオインサイト] に移動し、[ **ABR** ビデオ] をクリックします。

2. 右側のペインで、リストから時間枠を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。
3. [Go] をクリックし、[ネットワーク効率] タブを選択します。



最適化された **ABR** ビデオと最適化されていない **ABR** ビデオで使用されるデータ量を比較する

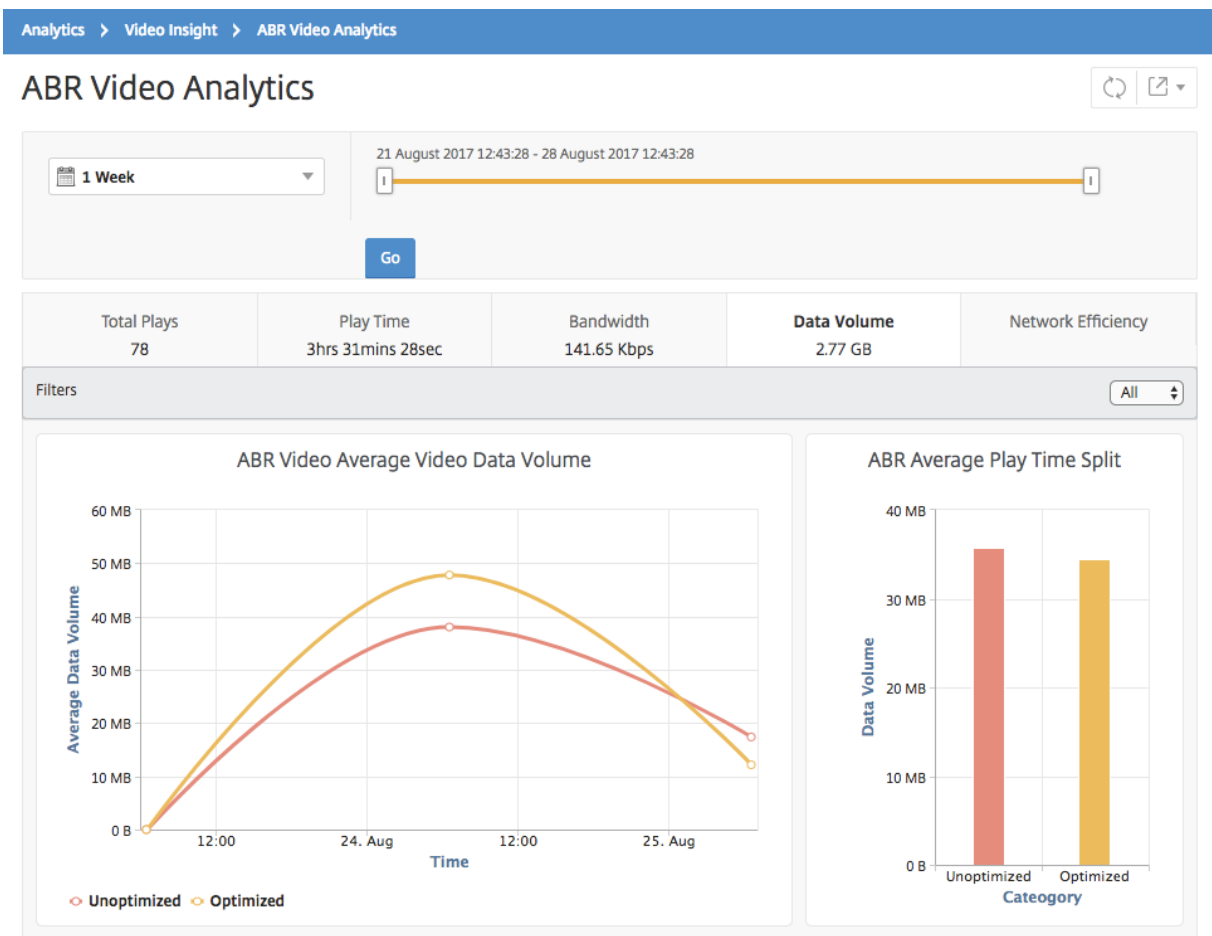
February 6, 2024

Citrix Application Delivery Management (ADM) では、特定の期間に、最適化された ABR ビデオと最適化されていない ABR ビデオが使用したデータ量が表示されるため、2 つのボリュームを比較できます。

ABR ビデオで使用されているデータ量を確認するには:

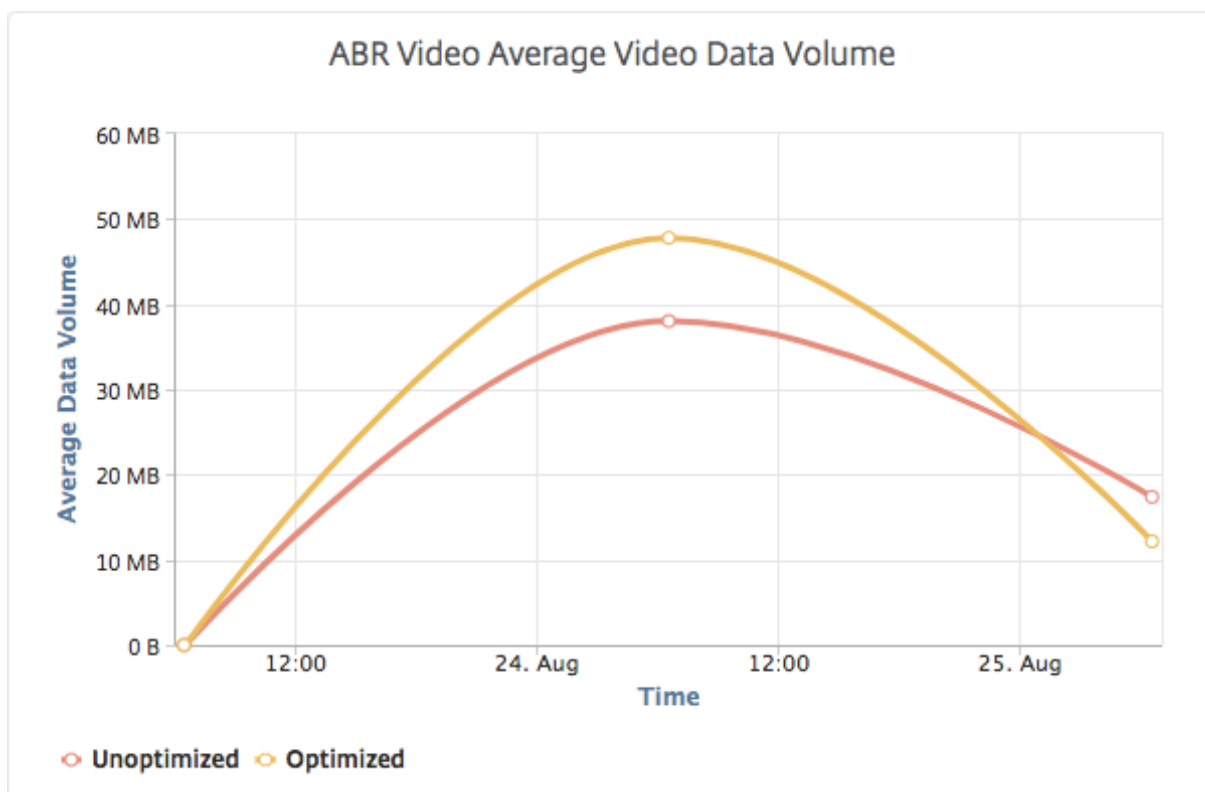
1. [分析] > [ビデオインサイト] に移動し、[ **ABR** ビデオ] をクリックします。
2. 右側のペインで、リストから時間枠を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。
3. 「実行」 をクリックし、「データボリューム」 タブを選択します。

[フィルタ] リストを使用して、HTTP、HTTPS、または QUIC ABR ビデオを選択できます。



[ **Data Volume** ] タブには、ABR ビデオで使用される平均データ量、および選択した時間枠におけるネットワークからの最適化および最適化されていない ABR ビデオによって消費されるデータ量を示す折れ線グラフと円グラフが表示されます。マウスポインターを折れ線グラフに重ねると、特定の期間に使用された平均データボリュームを確認できます。





ストリーミングされる動画の種類とネットワークから消費されるデータ量の表示

February 6, 2024

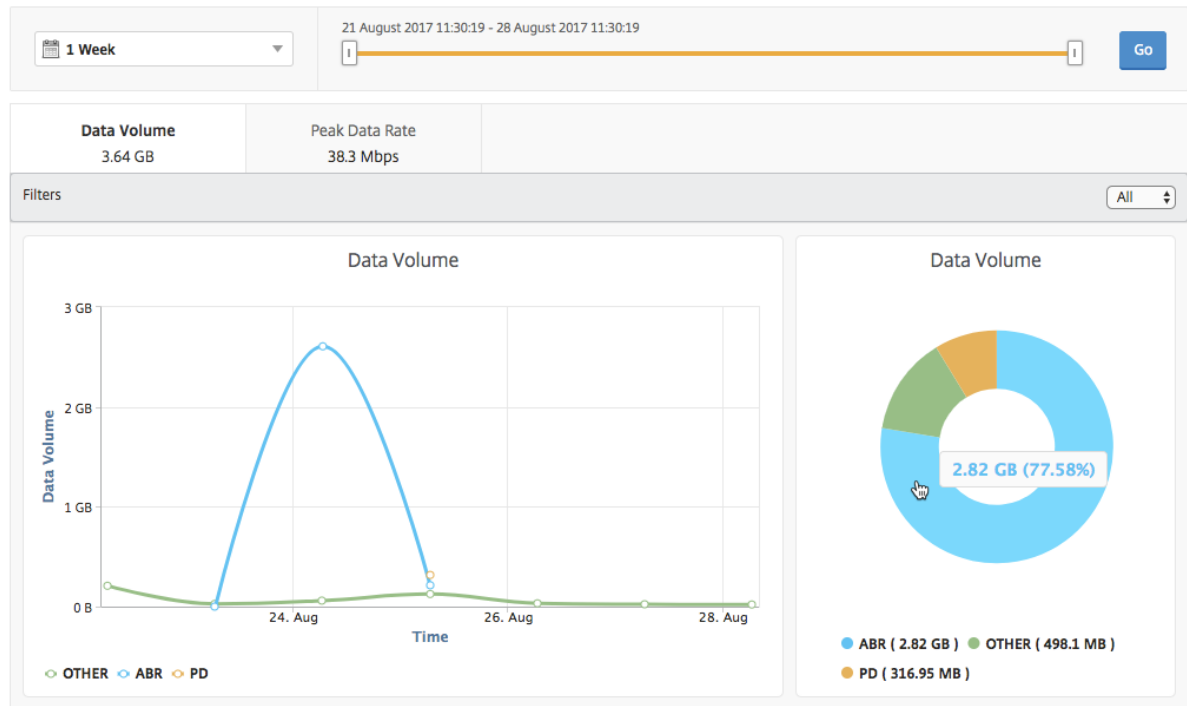
NetScaler ADC アプライアンスは、ネットワーク内の暗号化または暗号化されていないビデオトラフィック、およびビデオストリーミングの種類（PD または ABR）を検出します。NetScaler Application Delivery Management (ADM) では、これらのメトリックと、定義された期間内にビデオトラフィックによって消費されるデータ量が表示されます。

動画の種類と消費データ量を確認するには:

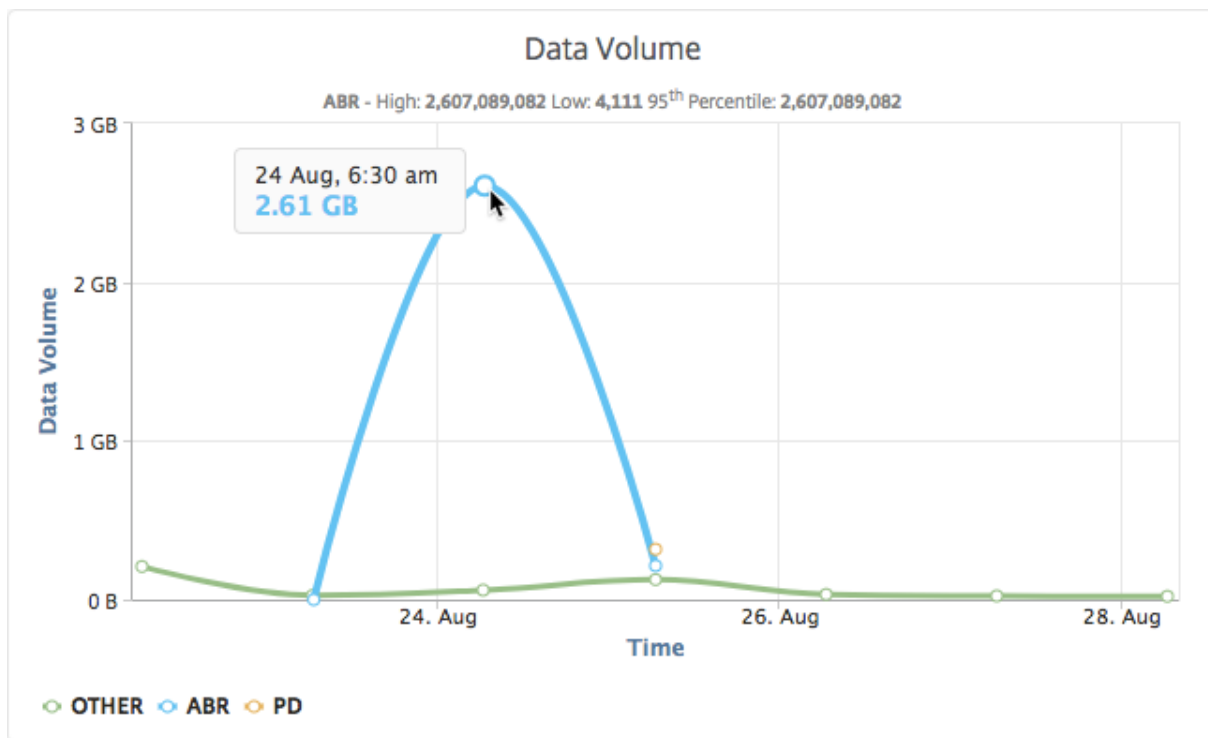
1. [分析] > [ビデオインサイト] に移動し、[ビデオ分類] をクリックします。
2. 右側のペインで、リストから時間枠を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。
3. [Go] をクリックします。

[フィルタ] リストを使用して、HTTP、HTTPS、または QUIC トラフィックを選択できます。

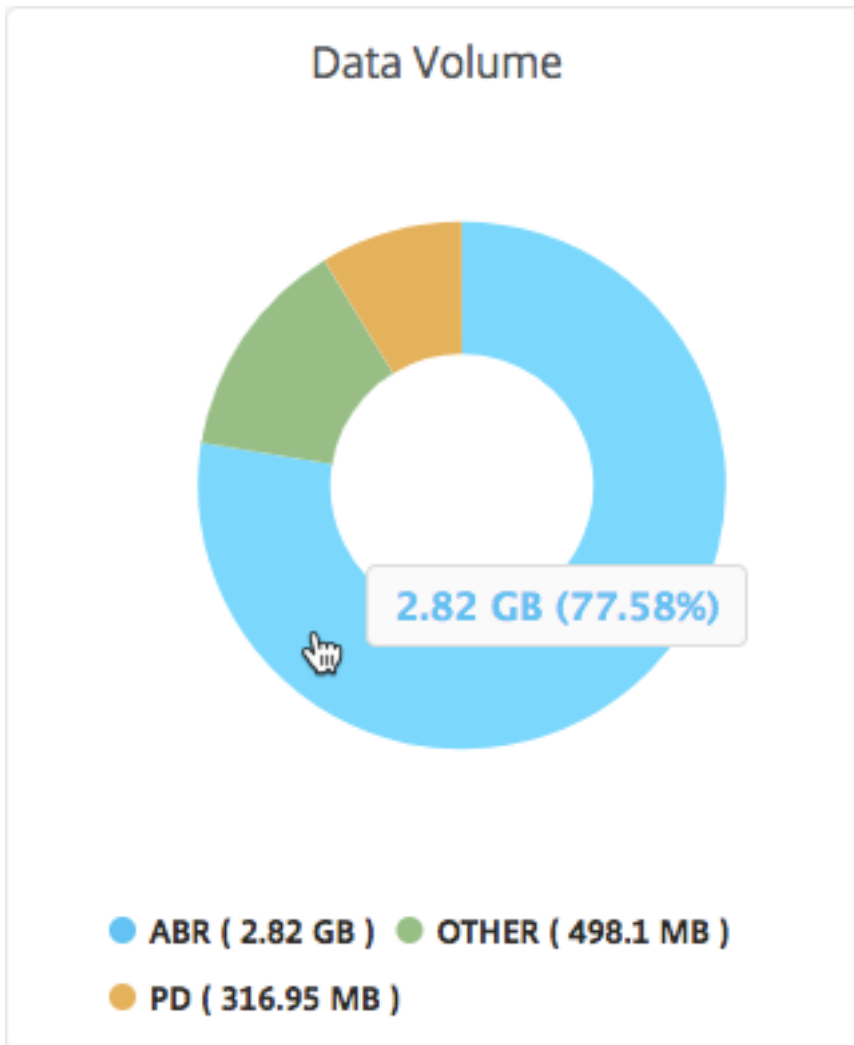
## Video Classification



[ **Data Volume** ] タブには、ネットワークからストリーミングされるビデオトラフィックの種類と、ネットワークによって消費されるデータ量を示す折れ線グラフと円グラフが表示されます。マウスポインターを折れ線グラフに重ねると、特定の期間に使用されたデータを確認できます。



また、円グラフにマウスポインタを置くと、特定の種類のビデオトラフィックで消費されたデータボリュームの割合を確認できます。



## ABR ビデオの最適化と非最適化の再生時間を比較する

February 6, 2024

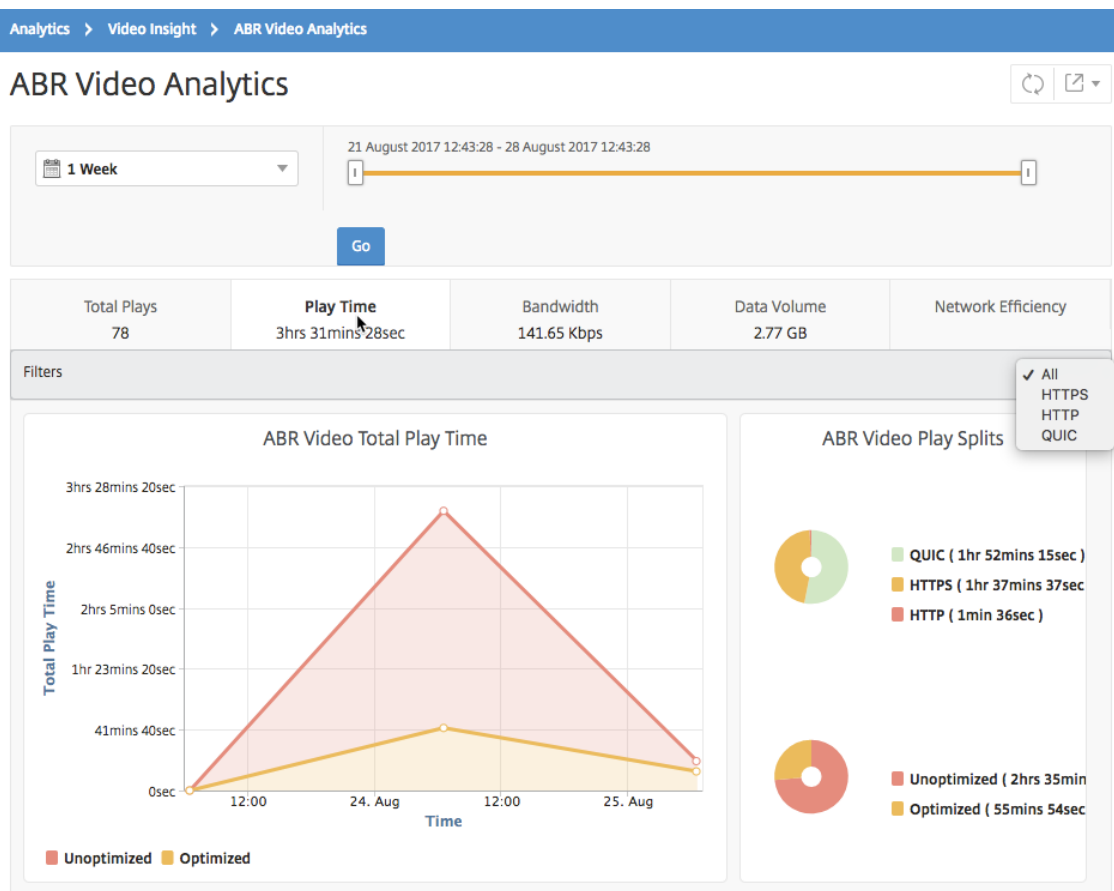
Citrix Application Delivery Management (ADM) は、特定の時間枠における ABR ビデオの再生時間を表示し、ネットワーク内の最適化された ABR ビデオと最適化されていない ABR ビデオの再生時間を比較することもできます。

プレイ時間を確認するには:

1. [分析] > [ビデオインサイト] に移動し、[ABR ビデオ] をクリックします。
2. 右側のペインで、リストから時間枠を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。

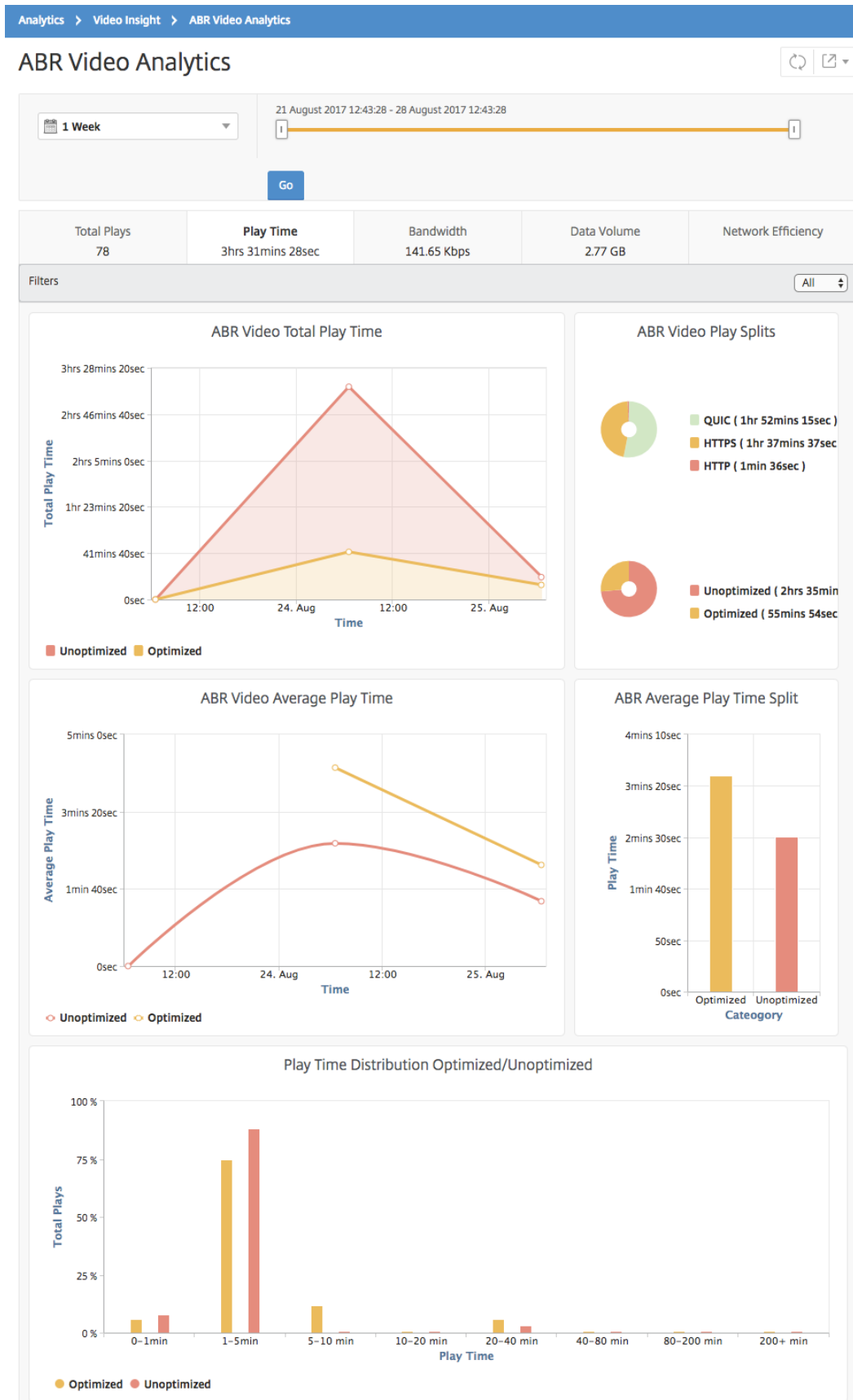
3. [移動] をクリックし、[再生時間] タブを選択します。

[フィルタ] リストを使用して、HTTP、HTTPS、または QUIC ABR ビデオを選択できます。



選択した時間枠の [ Play Time ] タブには、次の内容を示す折れ線グラフと円グラフが表示されます。

- ネットワークからの ABR ビデオの再生時間の合計
- 選択した期間における、ネットワーク上の ABR 動画の最適再生と非最適化再生の合計再生時間
- 暗号化された ABR 動画と暗号化されていない ABR 動画の合計再生時間
- ABR ビデオの平均再生時間
- ABR ビデオの最適化および非最適化された再生の、平均再生時間
- 暗号化および暗号化解除された ABR ビデオの平均再生時間
- 最適化および非最適化された ABR ビデオ間の再生時間の分布



最適化された **ABR** ビデオと最適化されていない **ABR** ビデオの帯域幅消費の比較

February 6, 2024

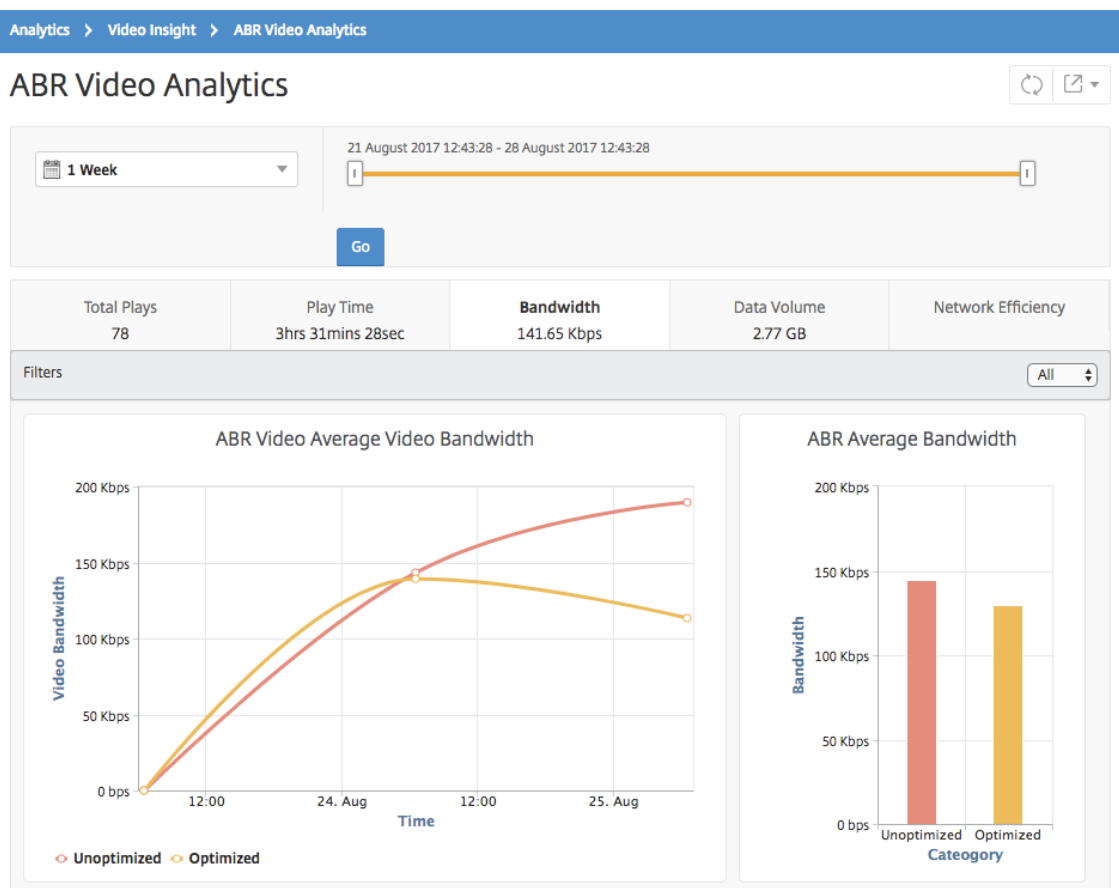
NetScaler Application Delivery Management (ADM) は、特定の時間枠において、ABR ビデオの最適化および非最適化によって消費される帯域幅を提供します。また、ネットワーク内で最適化された ABR ビデオと最適化されていない ABR ビデオによって消費される帯域幅を、以下に基づいて比較することもできます。

- 再生時間
- データ量

帯域幅の消費量を確認するには:

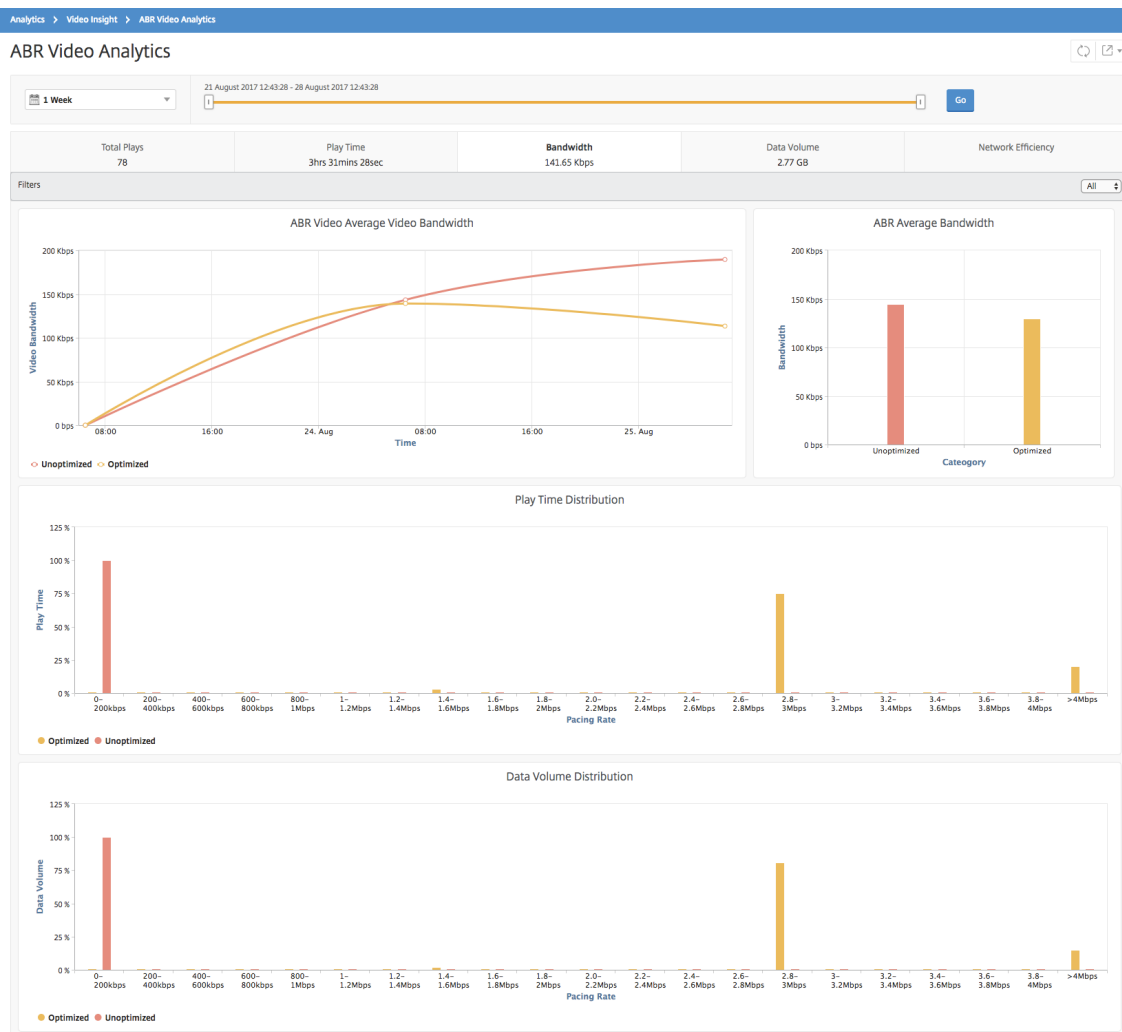
1. [分析] > [ビデオインサイト] に移動し、[ **ABR** ビデオ分析 ] をクリックします。
2. 右側のペインで、リストから時間枠を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。
3. [移動] をクリックし、[帯域幅] タブを選択します。

[フィルタ] リストを使用して、HTTP、HTTPS、または QUIC ABR ビデオを選択できます。



選択した時間枠の [ 帯域幅 ] タブには、次の内容を示す折れ線グラフと円グラフが表示されます：

- 最適化および非最適化された ABR ビデオによって消費された平均帯域幅。
- 最適化および非最適化された ABR ビデオ間の再生時間の分布に基づく、帯域幅消費。
- 最適化および非最適化された ABR ビデオ間のデータボリュームの分布に基づく、帯域幅消費。



## ABR ビデオの再生の最適化数と非最適化数を比較する

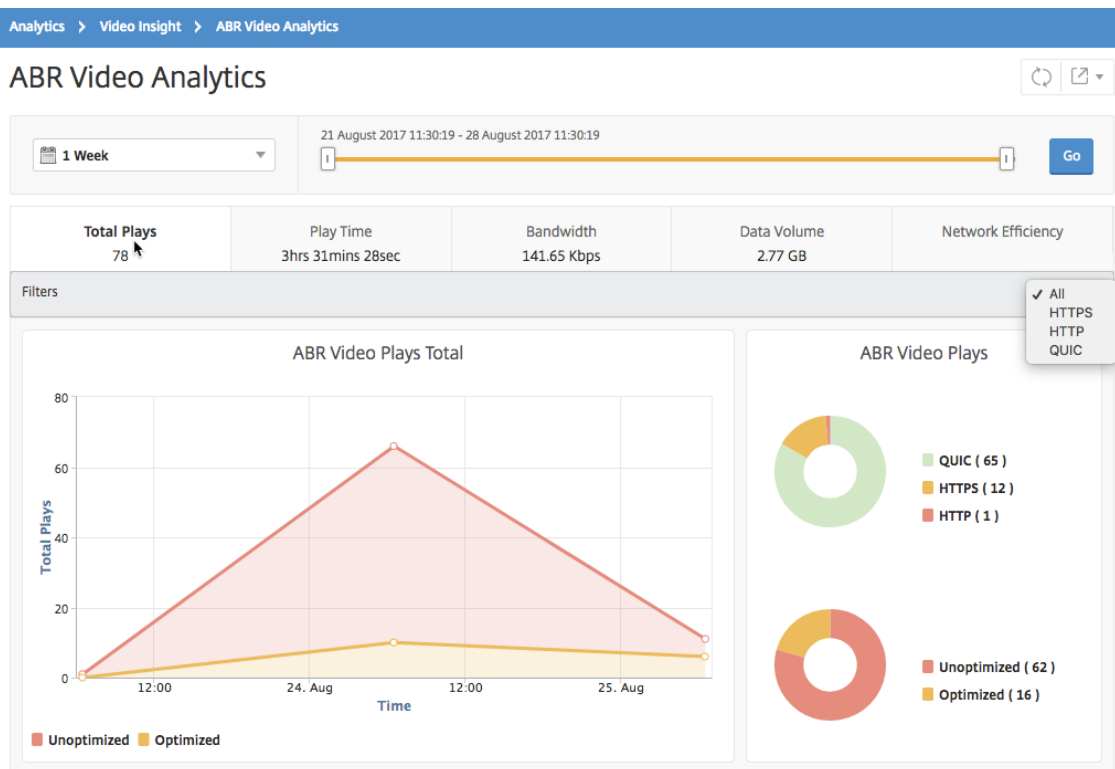
February 6, 2024

特定の期間において、NetScaler Application Delivery Management (ADM) は ABR ビデオの再生数を表示し、ネットワーク内の最適化された再生数と最適化されていない再生数を比較できます。

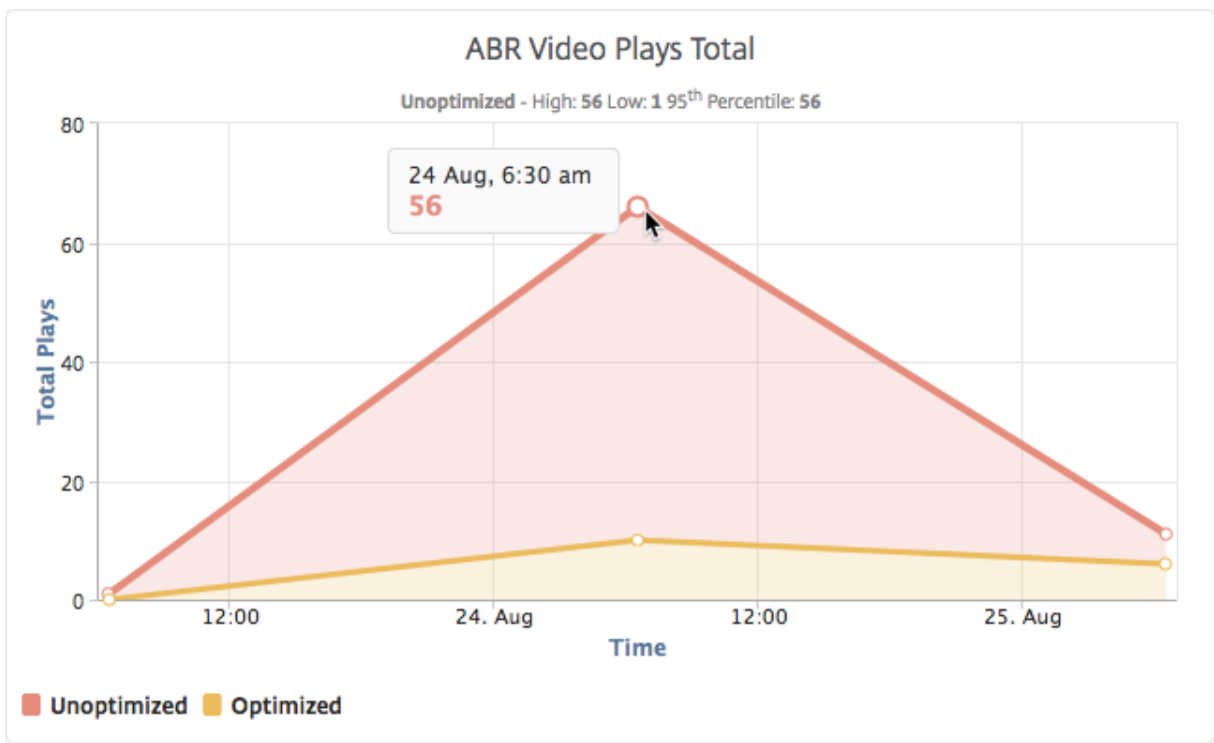
プレイ回数を確認するには：



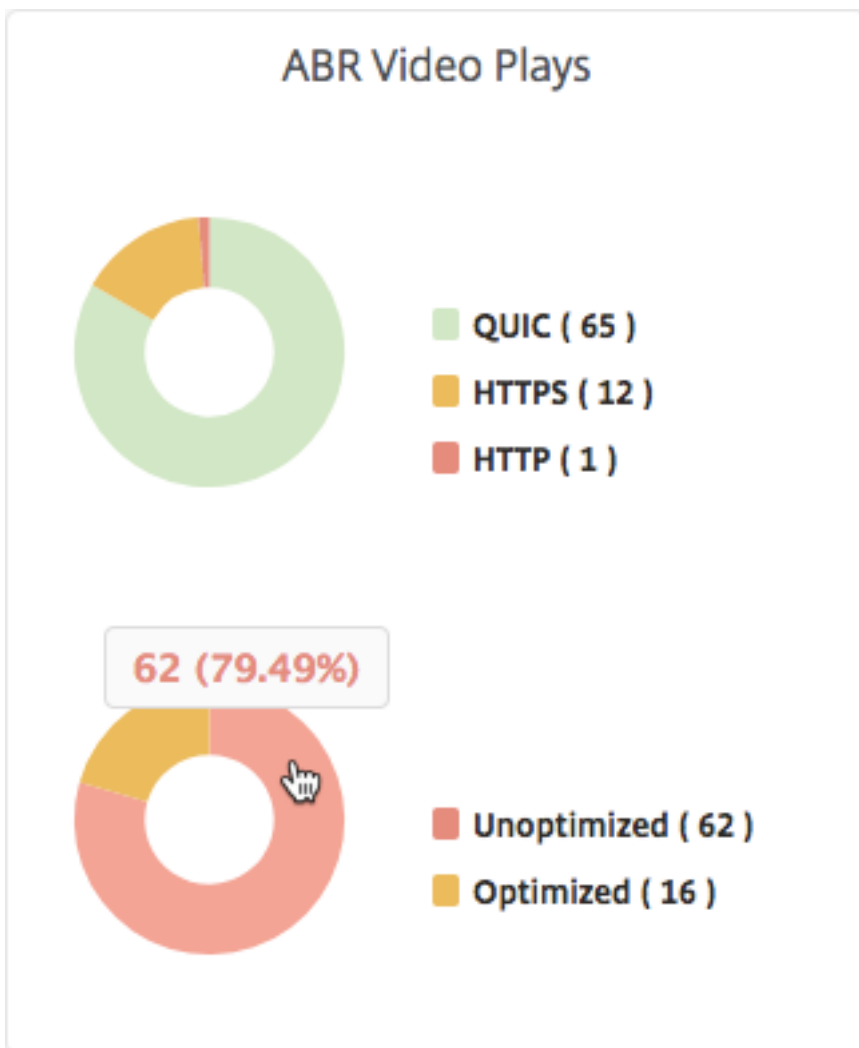
1. [分析] > [ビデオインサイト] に移動し、[ **ABR** ビデオ分析 ] をクリックします。
  2. 右側のペインで、リストから時間枠を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。
  3. [移動] をクリックし、[再生数] タブを選択します。
- [フィルタ] リストを使用して、HTTP、HTTPS、または QUIC ABR ビデオを選択できます。



[再生数] タブには、ネットワークからの ABR ビデオの再生数、および選択した時間枠における ABR ビデオの最適化および非最適化再生数を示す折れ線グラフと円グラフが表示されます。マウスポインターを折れ線グラフに重ねると、特定の期間の再生回数を確認できます。



また、マウスポインターを円グラフに重ねると、選択した期間に最適化および非最適化された再生の割合と、暗号化および暗号解除された ABR ビデオの割合を確認できます。



特定の時間枠のピークデータレートを表示する

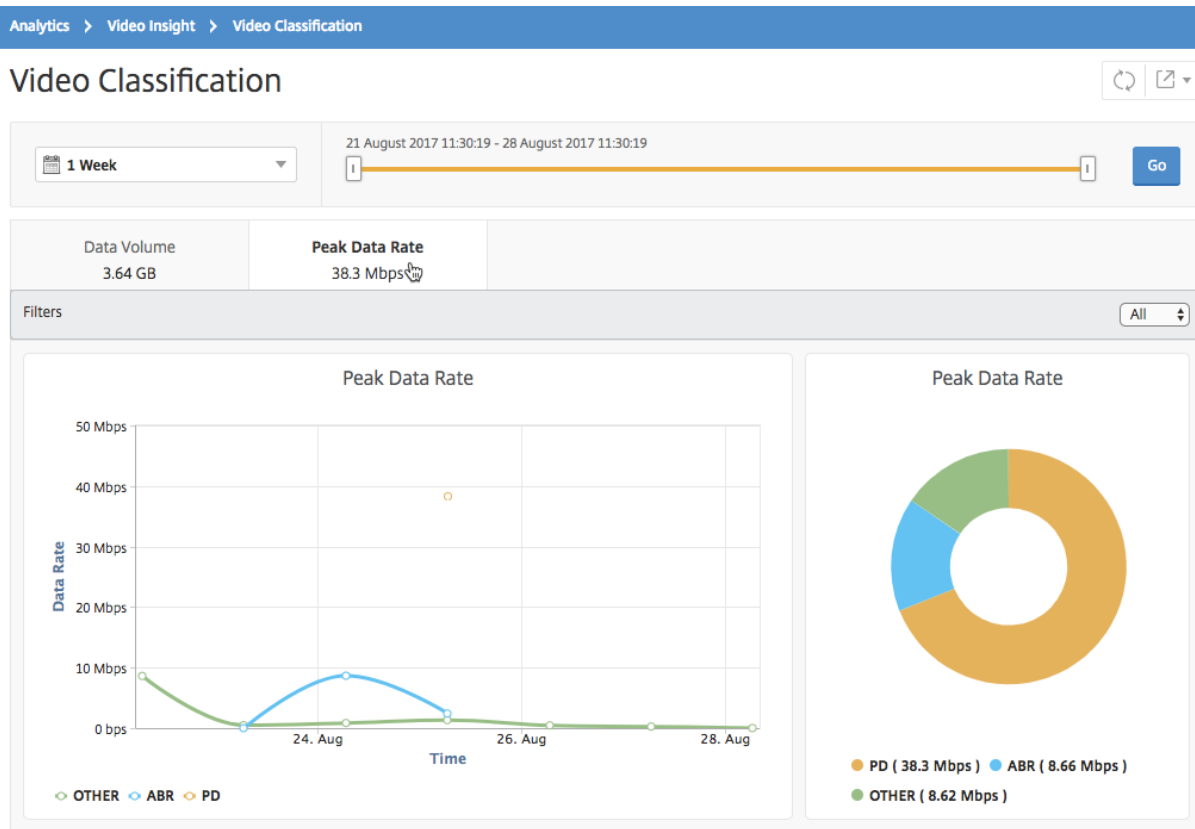
February 6, 2024

NetScaler Application Delivery Management (ADM) では、ネットワーク内のビデオトラフィックのピークスルーットまたはデータレートが表示されます。

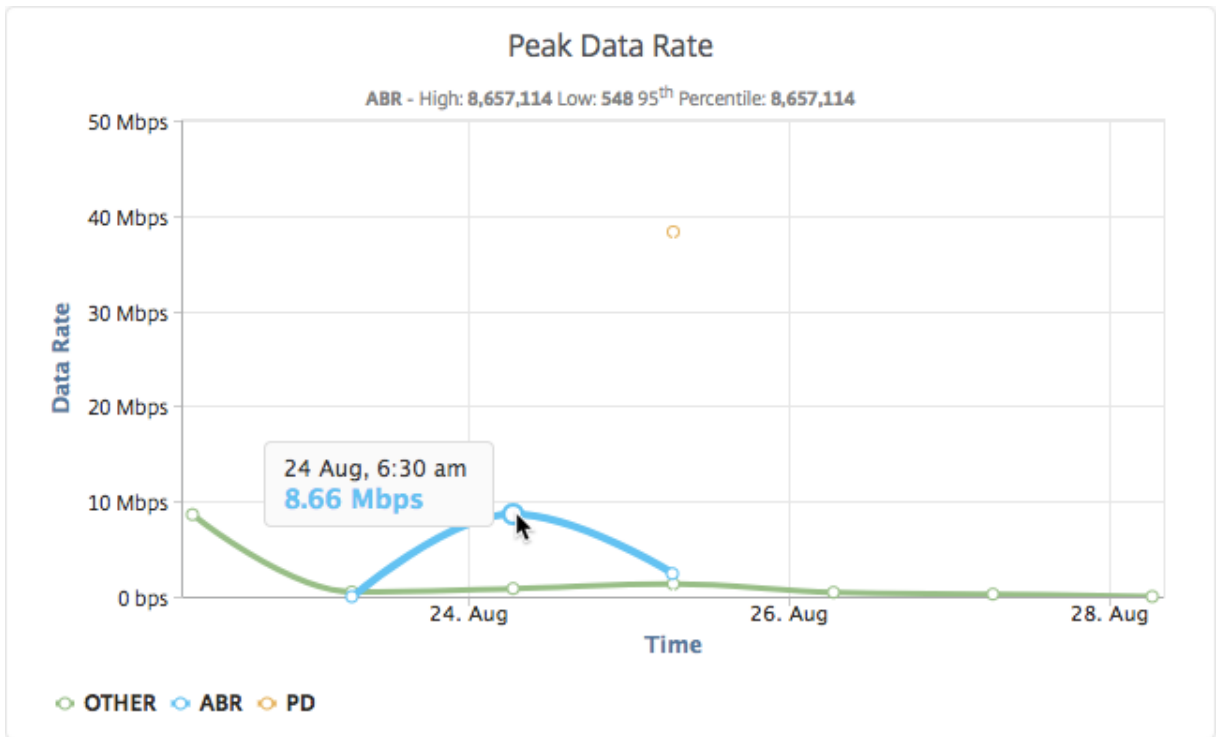
ビデオトラフィックのピークデータレートを確認するには:

1. [分析] > [ビデオインサイト] に移動し、[ビデオ分類] をクリックします。
2. 右側のペインで、リストから時間枠を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。
3. 「進む」をクリックし、「ピークデータレート」タブを選択します。

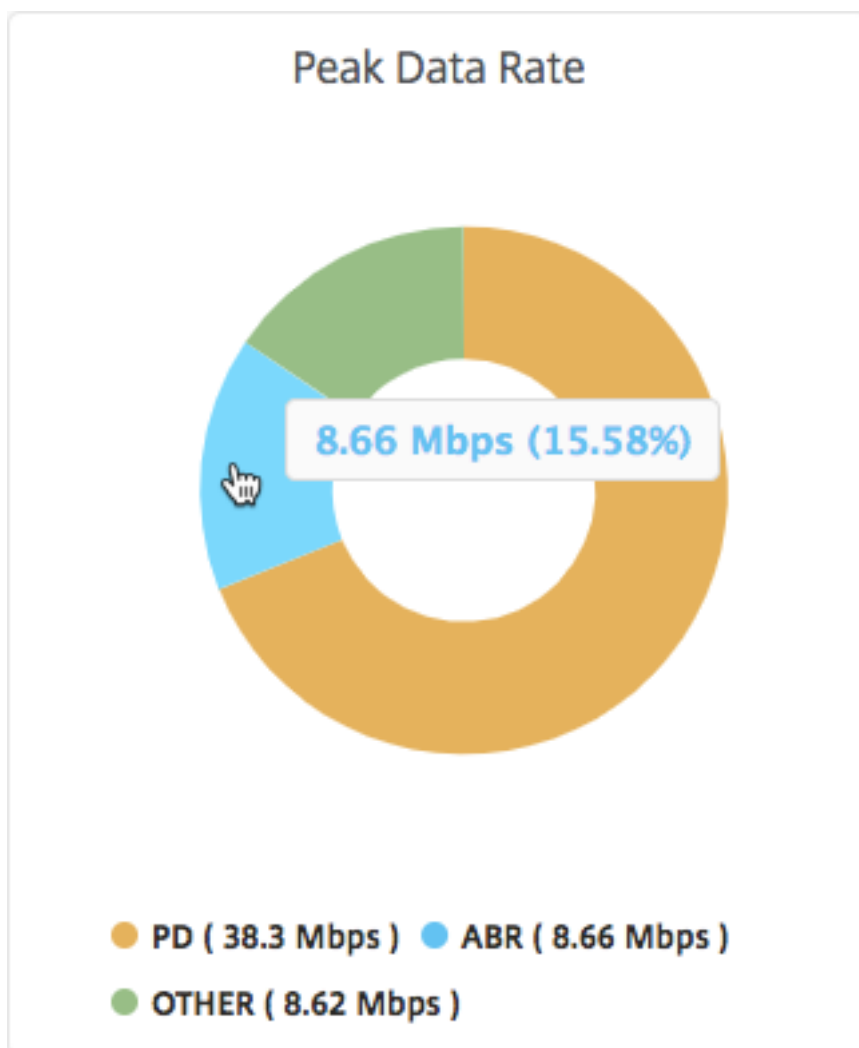
[フィルタ] リストを使用して、HTTP、HTTPS、または QUIC トラフィックを選択できます。



[ **Peak Data Rate** ] タブには、ネットワークからストリーミングされるビデオトラフィックのタイプのピークデータレートと、選択した時間枠におけるネットワーク上のビデオトラフィックのピークデータレートを示す折れ線グラフと円グラフが表示されます。マウスポインターを折れ線グラフに重ねると、特定の期間における最大データレートを確認できます。



また、円グラフにマウスポインターを重ねると、選択した期間に特定の種類の動画トラフィックで消費された最大データレートの割合を確認できます。



## SSL フォワードプロキシ分析

February 6, 2024

企業ネットワークのエッジにある NetScaler ADC アプライアンスは、インターネットプロキシとして機能します。このアプライアンスは透過プロキシモードまたは明示的プロキシモードで動作し、HTTPS を含むインターネットトラフィックの傍受を制御できるようにします。任意の要求を傍受するか、バイパスするか、禁止するかの決定は、アプライアンスに設定されたポリシーに基づいて行われます。ユーザーは社内ネットワークにログオンする前に認証されます。すべての要求と応答はユーザーにタグ付けされ、ユーザーのアクティビティはアプライアンスで記録されます。詳しくは、「[Citrix SSL フォワードプロキシ](#)」を参照してください。

NetScaler Application Delivery Management (ADM) を NetScaler ADC アプライアンスと統合すると、ログストリームを使用してアプライアンス上のログユーザーアクティビティとその後のレコードが NetScaler ADM にエクスポートされます。NetScaler ADM は、訪問した Web サイトや消費された帯域幅など、ユーザーのアクティビ

ティに関する情報を照合して表示します。また、帯域幅の使用量と検出された脅威（マルウェアやフィッシングサイトなど）をレポートします。これらの主要なメトリックを使用して、ネットワークを監視し、NetScaler ADC アプライアンスで是正措置を講じることができます。

**NetScaler ADC** アプライアンスを **NetScaler ADM** と統合するには：

1. NetScaler ADC アプライアンスで、SSL フォワードプロキシを構成する際に、分析を有効にして、分析に使用したい NetScaler ADM インスタンスの詳細を指定します。
2. NetScaler ADM で、NetScaler ADC アプライアンスをインスタンスとして NetScaler ADM に追加します。詳しくは、「[NetScaler ADM へのインスタンスの追加](#)」を参照してください。

## ダッシュボード

February 6, 2024

NetScaler Application Delivery Management (ADM) には、送信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があります。これらのダッシュボードには、組織内ネットワークからアクセスされた Web サイトとアプリケーション、およびネットワーク内のユーザーが実行したアクティビティの概要を示す複数のグラフが表示されます。

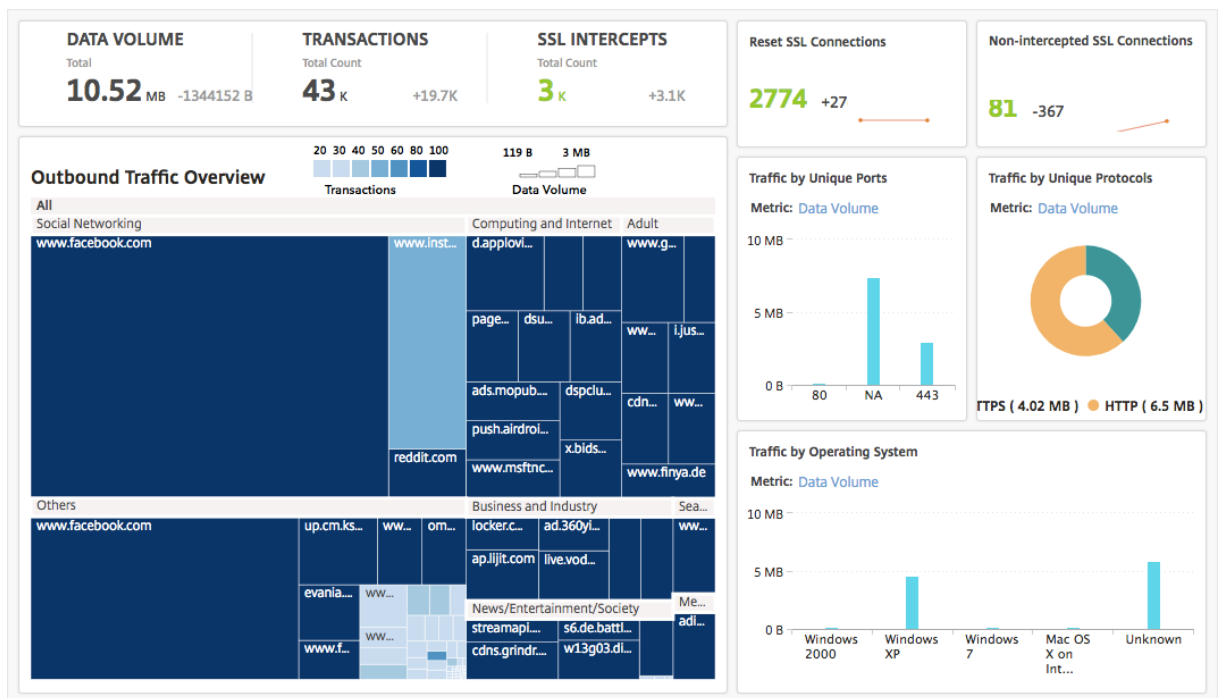
### アウトバウンドトラフィックダッシュボード

アウトバウンドトラフィックダッシュボード には、ネットワークからアクセスされた URL またはドメインの概要が表示されます。このダッシュボードでは、URL またはドメインで使用されたトランザクション数別またはデータボリューム別に URL とドメインの全体像を確認できます。

また、次のような詳細も表示されます。

1. ネットワークからアクセスされた URL またはドメインで使用された帯域幅の量
2. ネットワークから URL およびドメインへのアクセス中に発生したトランザクション数
3. トランザクション中に NetScaler ADC 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 ADC 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 ADC アプライアンスによってリセットされた SSL 接続の数。
6. トラフィックの送信に使用されたポート、Web トラフィックにより使用されたプロトコル、およびトラフィックの送信に使用されたクライアントオペレーティングシステムごとの Web トラフィックの送信量

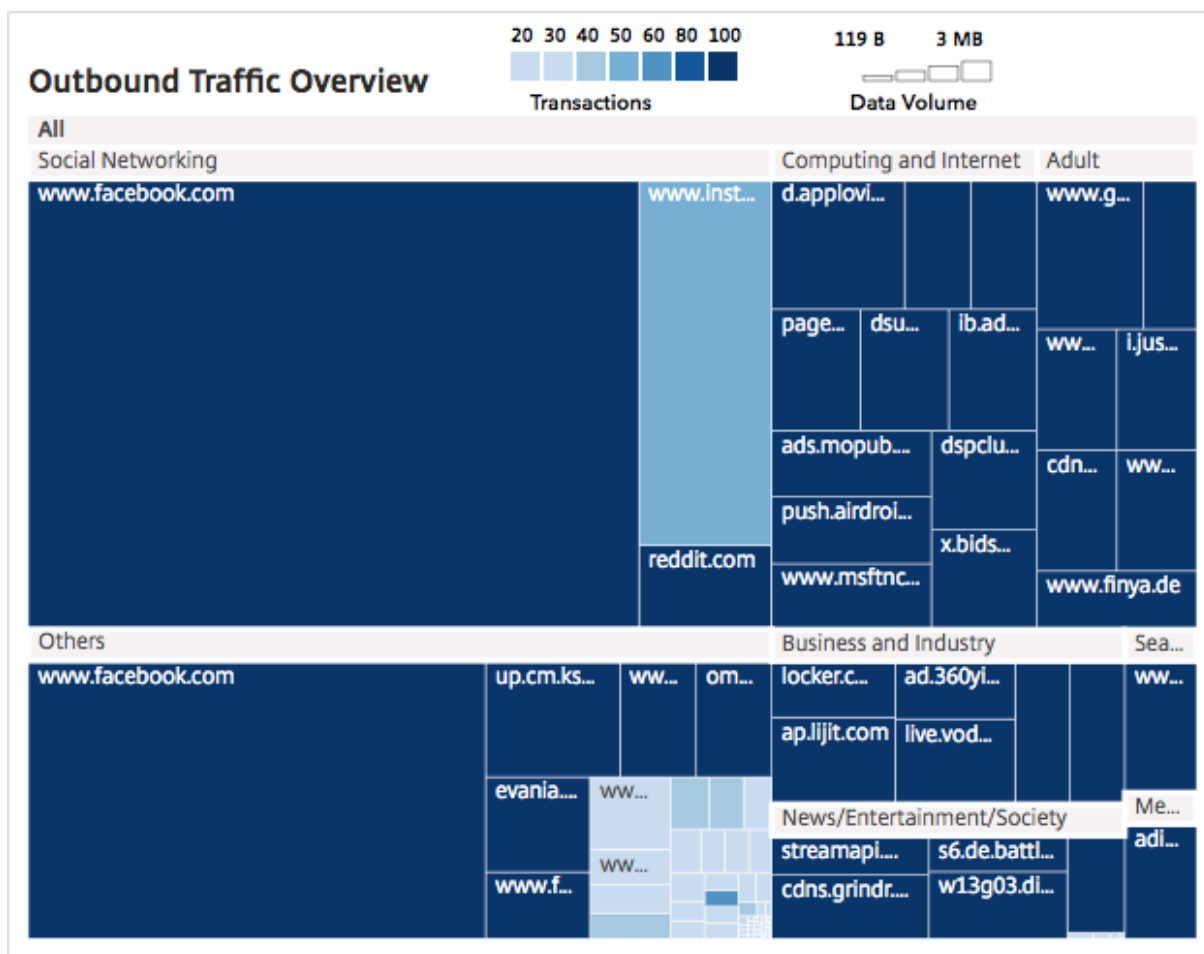
アウトバウンドトラフィックダッシュボードにアクセスするには、「アプリケーション」>「アウトバウンドトラフィックダッシュボード」に移動します。



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の概要ペインがあります。アウトバウンドトラフィックの概要ペインでは、NetScaler ADM はアクセスされた URL またはドメインを「ショッピング」、「ニュース」、「ソーシャルネットワーキング」などのカテゴリに分類します。アウトバウンドトラフィックの概要ペインには、ネットワークからアクセスされた URL またはドメインが URL カテゴリ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で使用されたデータボリュームに応じて決まります。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回数を示しています。





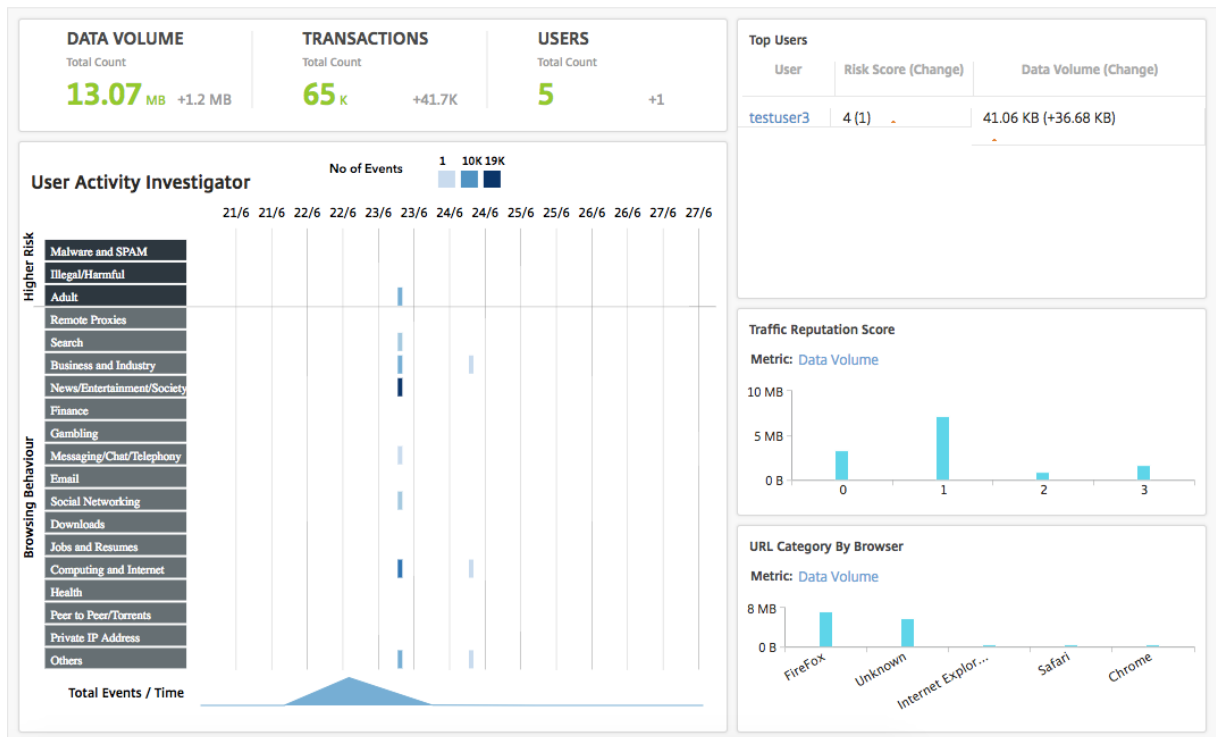
カテゴリをクリックすると、チャートをフィルタリングして、指定した時間枠のカテゴリに関連する詳細を表示できます。

### 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。このダッシュボードにはキーマトリックが用意されており、これらを使用して以下を確認することができます。

1. 社内ユーザーのブラウジング行動
2. 社内ユーザーがアクセスした URL カテゴリ。
3. リスクスコアおよび使用帯域幅量に基づく上位 5 名のユーザー。リスクスコアについて詳しくは、「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 Web ブラウザー。
5. トラフィックレピュテーションスコアに基づく、ユーザーにより生成された Web トラフィックの量

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。

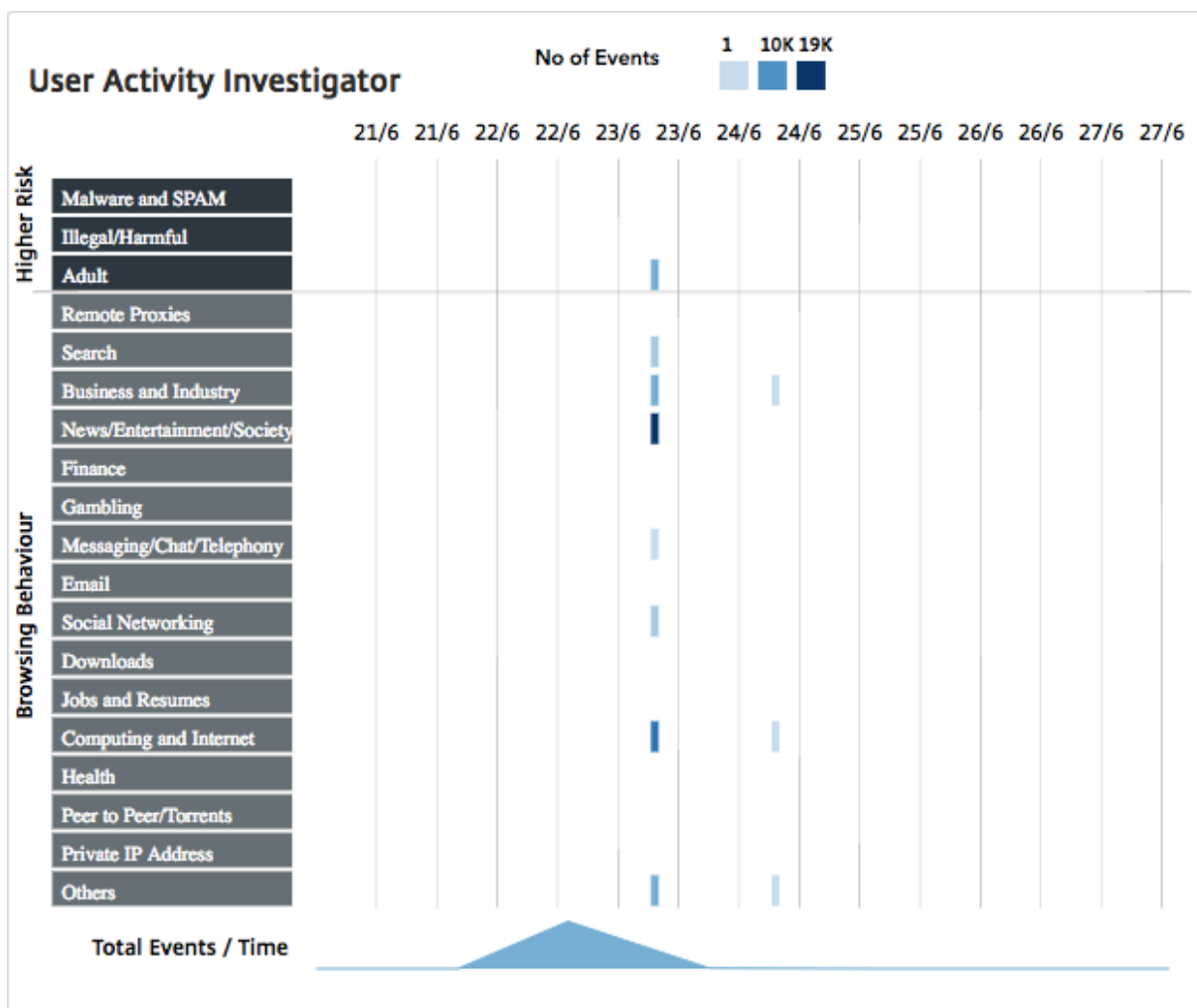


[ **Top Users** ] ペインでユーザー をクリックすると、グラフをフィルタリングして、指定した時間枠内でユーザーが実行した Web アクティビティの詳細を表示できます。

## User activity investigator

ユーザーダッシュボード には、ユーザーによって実行されたさまざまな **Web** アクティビティを表示する「**User Activity Investigator**」ペインがあります。このペインには、選択した時間内にユーザーがアクセスした URL カテゴリと、URL カテゴリごとの実行された各種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が表示されます。

**User Activity Investigator** は、URL カテゴリごとに、ユーザーの閲覧行動、ユーザーによるリスクの高いアクティビティ、トリガーされたイベントなどの重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。凡例はそれぞれ、選択した期間が 1 時間の場合は 1 分間隔、選択した期間が 1 日の場合は 1 時間間隔で集計されます。



集計された凡例は、イベントの発生回数に応じて色分けされます。凡例にマウスポインターを重ねると、時間や選択した凡例について集計されたイベント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して、グラフの期間をカスタマイズできます。

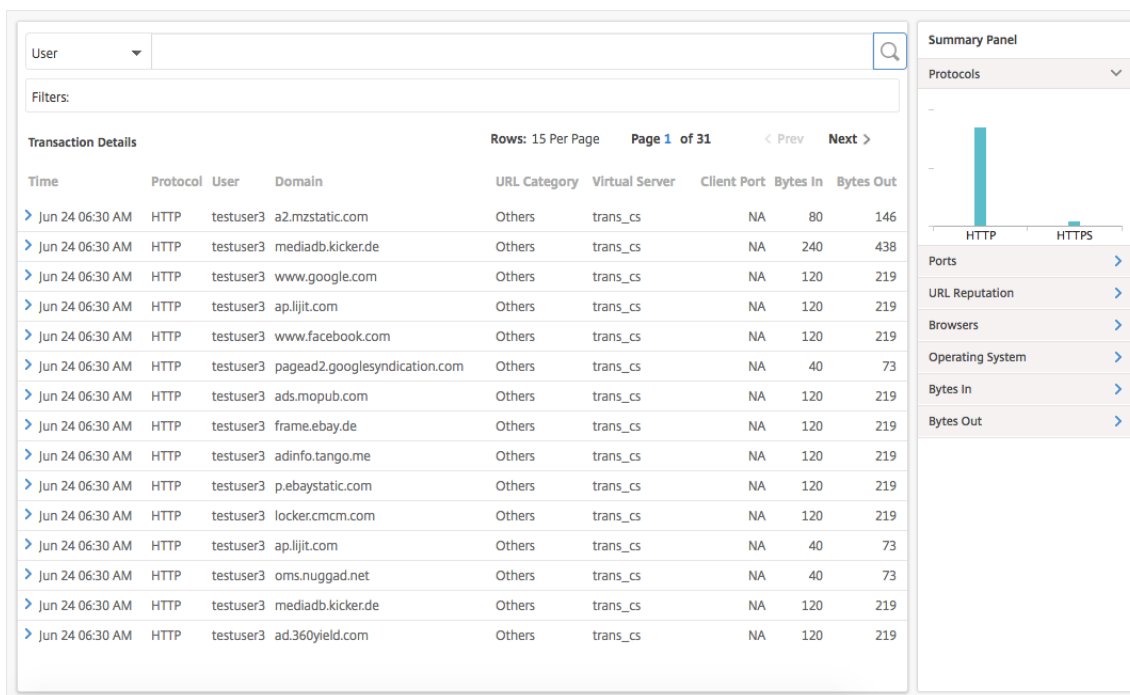
イベントをクリックすると、さらに掘り下げて取引の詳細を確認できます。

#### ユーザー取引

[User Transactions] ペインには、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。このペインでは、以下のようなトランザクションレベルの詳細が示されます。

1. トランザクションの発生日時
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. トランザクションの傍受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



**Summary panel** 概要パネルには、トランザクションの詳細ペインに表示されるトランザクションのすべてのメトリックが表示されます。このパネルでは、メトリックを選択または選択解除することで、トランザクションの詳細ペインでトランザクションをソートして表示できます。概要パネルには次の指標が表示されます。

メトリックス	説明
プロトコル	トランザクションで使用されたプロトコル
ポート	トランザクションで使用されたポート
URL レピュテーション	URL レピュテーションスコア
Web ブラウザー	トランザクションで使用された Web ブラウザー
オペレーティングシステム	トランザクションで使用されたオペレーティングシステム
受信バイト数	Citrix ADC アプライアンスを介して受信したデータ量。

メトリックス	説明
送信バイト数	Citrix ADC アプライアンスを介して送信されたデータの量。

## リスクスコア

リスクスコアは、NetScaler ADM 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するスコアリングシステムです。NetScaler ADM は、ネットワーク上のユーザーがアクセスする URL に対して、NetScaler ADC 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](#)。次の表では、NetScaler ADM によって割り当てられるリスクスコアについて説明します。

リスクスコア	説明
1	ユーザーの Web アクティビティについて脅威は認められず異常ではありません。
2	ユーザーの Web アクティビティについて脅威は認められず異常でもありませんが、ユーザーは URL レピュテーションスコアが設定されていない「不明サイト」にアクセスしています。
3	ユーザーの Web アクティビティに脅威は検出されていませんが、ユーザーは潜在的な危険性があるサイトにアクセスしようとしたか、こうしたサイトと関係しています。
4	ユーザーが侵害を受けた可能性があります。
5	ユーザーの Web アクティビティは異常であり、ユーザーは既知の悪意のあるサイトにアクセスしました。

## 使用例

February 6, 2024

### SSL インターセプトの監視

NetScaler ADC アプライアンスを使用すると、暗号化されたアウトバウンドトラフィックを検査できます。アプライアンスで設定されたポリシーに基づいて、任意の HTTPS 要求を傍受したり、バイパスしたり、ブロックしたりで

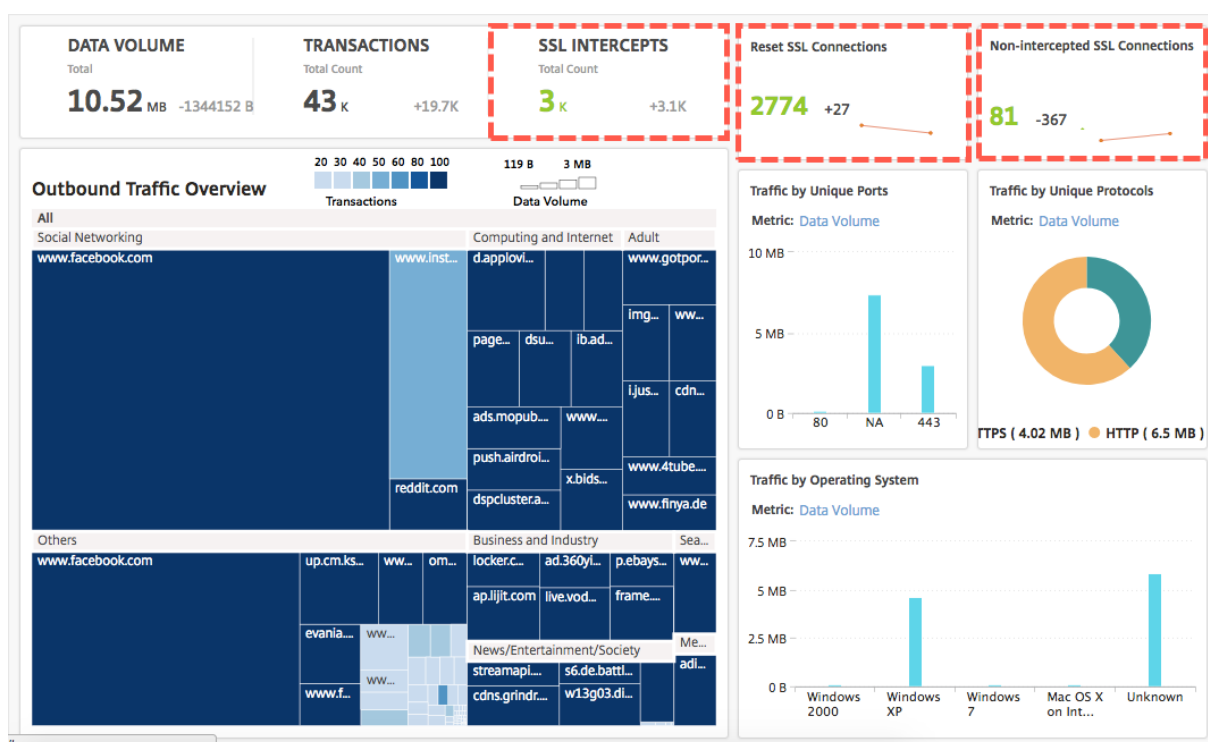
きます。NetScaler Application Delivery Management (ADM) では、選択した期間における送信トラフィックダッシュボードのSSL接続に関する次の詳細が提供されます。

- NetScaler ADC アプライアンスによって傍受された、傍受されていない、リセットされた SSL 接続の数
- SSL 接続のトランザクションの詳細

これらの詳細を使用して、NetScaler ADC アプライアンスのポリシーをさらに微調整して、暗号化された送信トラフィックを効率的に検査できます。詳しくは、「Citrix SSL フォワードプロキシ」を参照してください。

傍受された、傍受されていない、およびリセットされた **SSL** 接続の数を表示するには、以下を行います。

「アプリケーション」 > 「アウトバウンドトラフィックダッシュボード」に移動します。送信トラフィックダッシュボードに、傍受された、傍受されていない、およびリセットされた SSL 接続の数が表示されます。



傍受された **SSL** 接続のトランザクションの詳細を表示するには、以下を行います。

1. 「アプリケーション」 > 「アウトバウンドトラフィックダッシュボード」に移動します。
2. 送信トラフィックダッシュボードで、「**SSL INTERCEPTS**」セクションの合計数をクリックします。



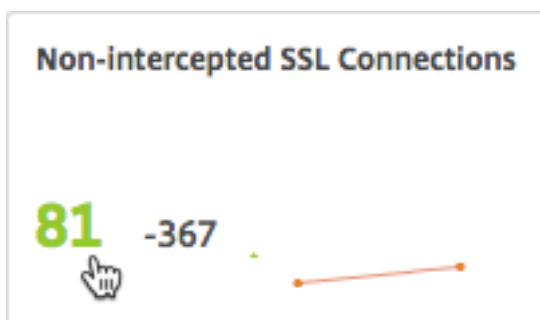
選択した期間中に傍受された SSL 接続のトランザクション詳細が、[トランザクション詳細] ページに表示されます。

Time	Protocol	User	Domain	URL Category	Virtual Server	Client Port	Bytes In	Bytes Out
Jun 24 06:30 AM	HTTPS	testuser3	www.facebook.com	Others	starcs	NA	338	0
Jun 23 06:31 AM	HTTPS	testuser3	a2.mzstatic.com	Social Networking	starcs	NA	337	0
Jun 23 06:31 AM	HTTPS	testuser3	www.facebook.com	Others	starcs	NA	338	0
Jun 23 06:31 AM	HTTPS	testuser3	m.momondo.pt	News/Entertainment/Society	starcs	NA	668	0
Jun 23 06:31 AM	HTTPS	testuser3	adinfo.tango.me	Messaging/Chat/Telephony	starcs	NA	674	0
Jun 23 06:31 AM	HTTPS	testuser3	locker.cmc.com	Business and Industry	starcs	NA	674	0
Jun 23 06:31 AM	HTTPS	testuser3	www.instagram.com	Others	starcs	443	2448	30032
Jun 23 06:31 AM	HTTPS	testuser3	s6.de.battleknight.gameforge.com	News/Entertainment/Society	starcs	NA	708	0
Jun 23 06:31 AM	HTTPS	testuser3	www.facebook.com	Social Networking	starcs	80	1671	0
Jun 23 06:31 AM	HTTPS	testuser3	www.facebook.com	Others	starcs	443	2228	0
Jun 23 06:31 AM	HTTPS	testuser3	www.facebook.com	Social Networking	starcs	443	34400	1775373
Jun 23 06:31 AM	HTTPS	testuser3	www.instagram.com	Social Networking	starcs	NA	12280	150313
Jun 23 06:31 AM	HTTPS	testuser3	www.facebook.com	Social Networking	starcs	NA	6127	0
Jun 23 06:31 AM	HTTPS	testuser3	www.instagram.com	Social Networking	starcs	443	33497	405990
Jun 23 06:31 AM	HTTPS	testuser3	www.instagram.com:443	Others	starcs	443	1560	3081

トランザクションの詳細をユーザーや URL カテゴリでさらにフィルターできます。

トラフィックが傍受されなかった **SSL** 接続のトランザクション詳細を表示するには:

1. 「アプリケーション」 > 「アウトバウンドトラフィックダッシュボード」に移動します。
2. 送信トラフィックダッシュボードで、代行受信されていない **SSL** 接続セクションの合計数をクリックします。



選択した期間中にトラフィックが傍受されなかった SSL 接続のトランザクションの詳細は、[ **Transaction Details** ] ページに表示されます。

The screenshot displays the 'Transaction Details' page in NetScaler. At the top, there is a search bar and a filter set to 'Not Intercept'. The main table lists transactions with columns for Time, User, Domain, SSL Executed Action, SSL Policy Action, Reset, and Not-intercepted. The right-hand side features a 'Summary Panel' with two bar charts: 'SSL Executed Action' and 'SSL Policy Action', both showing a count of 2.

Time	User	Domain	SSL Executed Action	SSL Policy Action	Reset	Not-intercepted
Jun 24 06:30 AM	testuser3	p.ebaystatic.com	2	2	0	1
Jun 24 06:30 AM	testuser3	frame.ebay.de	2	2	0	1
Jun 24 06:30 AM	testuser3	www.google.com	2	2	0	1
Jun 24 06:30 AM	testuser3	ap.lijit.com	2	2	0	1
Jun 23 06:31 AM	testuser3	adyoulike.omnitagjs.com	2	2	0	1
Jun 23 06:31 AM	administrator	www.facebook.com	2	2	0	8
Jun 23 06:31 AM	testuser3	www.immobilienscout24.de	2	2	0	1
Jun 23 06:31 AM	testuser3	p.ebaystatic.com	2	2	0	2
Jun 23 06:31 AM	testuser3	pcache-pv-eu1.badoocdn.com	2	2	0	1
Jun 23 06:31 AM	testuser3	pagead2.googlesyndication.com	2	2	0	1
Jun 23 06:31 AM	testuser3	streamapi.majorleaguegaming.com	2	2	0	2
Jun 23 06:31 AM	testuser3	live.vodafone.de	2	2	0	2
Jun 23 06:31 AM	testuser3	www.finya.de	2	2	0	2
Jun 23 06:31 AM	testuser3	www.google.co.in	2	2	0	1
Jun 23 06:31 AM	testuser3	reiseauskunft.bahn.de	2	2	0	2

トランザクションの詳細をユーザーや URL カテゴリでさらにフィルターできます。

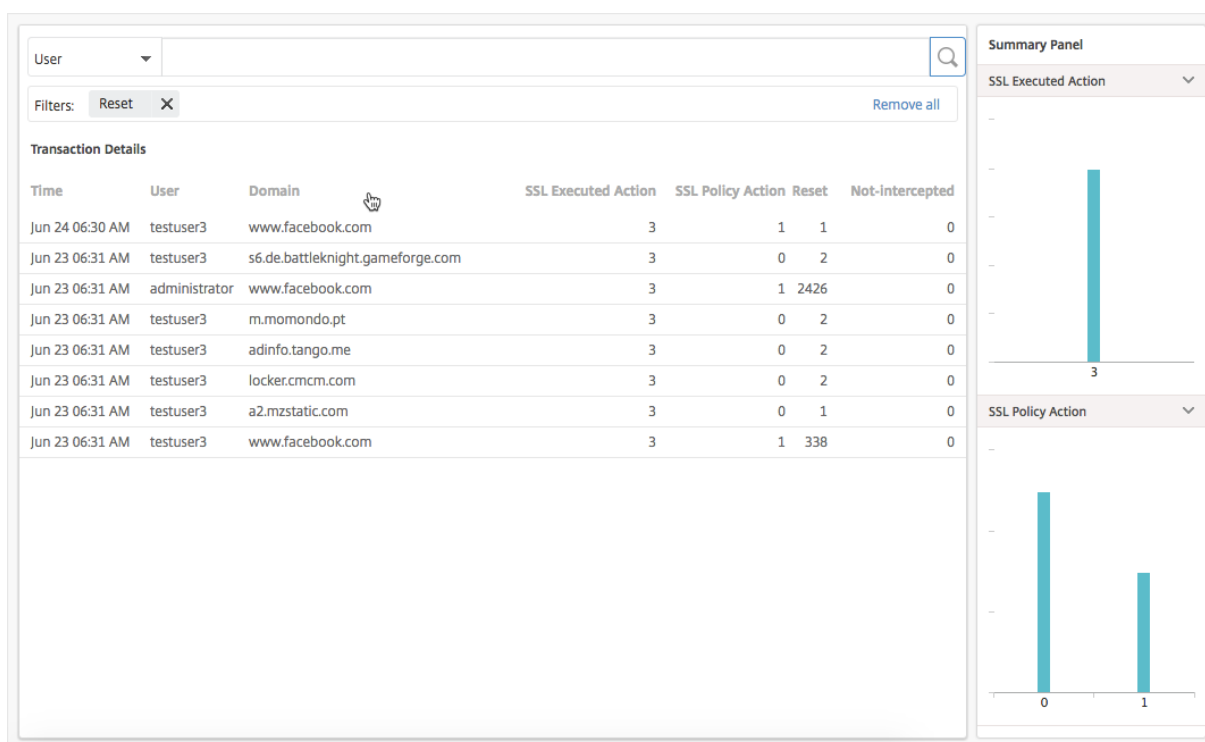
リセットされた **SSL** 接続のトランザクション詳細を表示するには:

1. 「アプリケーション」 > 「アウトバウンドトラフィックダッシュボード」に移動します。
2. 送信トラフィックダッシュボードで、[ **SSL** 接続のリセット ] セクションで合計数をクリックします。



選択した期間中にトラフィックが傍受されなかった SSL 接続のトランザクションの詳細は、[ **Transaction Details** ] ページに表示されます。





トランザクションの詳細をユーザーや URL カテゴリでさらにフィルターできます。

## エンドポイントの検査

NetScaler ADC アプライアンスで構成したポリシーは、アプライアンスが企業内で実行されたすべてのユーザーアクティビティをどのように記録するかを指定します。NetScaler ADM は、次の項目を決定するために使用できる主要なメトリックを提供します。

1. 社内ユーザーのブラウジング行動
2. 社内ユーザーがアクセスした URL カテゴリ。
3. リスクスコアおよび使用帯域幅量に基づく上位 5 名のユーザー。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 Web ブラウザー。
5. トラフィックレピュテーションスコアに基づく、ユーザーにより生成された Web トラフィックの量

たとえば、ユーザー ID testuser3 のユーザーが企業内のマルウェア関連サイトに常にアクセスする場合、NetScaler ADM はそのユーザーを危険度の高いアクティビティユーザーとして識別し、より高いリスクスコアを割り当てます。testuser3 情報は、ユーザーダッシュボードの「上位ユーザー」セクションに表示されます。

Top Users		
User	Risk Score (Change)	Data Volume (Change)
<a href="#">testuser3</a>	5 (4)	2.19 KB (0B)

testuser3 をクリックすると、ユーザーダッシュボードをフィルタリングして、testuser3 に関連するすべての主要なメトリックを表示できます。

<b>BANDWIDTH</b> <small>Total Count</small> <span style="font-size: 24pt; color: green;">969</span> KB 0 B →	<b>TRANSACTIONS</b> <small>Total Count</small> <span style="font-size: 24pt; color: green;">168</span> 0 →	<b>USERS</b> <small>Total Count</small> <span style="font-size: 24pt; color: green;">1</span> 0 →
--	--	---

Top Users		
User	Risk Score (Change)	Data Volume (Change)
<a href="#">testuser3</a>	5 (4)	2.19 KB (0B)

**User Activity Investigator** No of Events: 1 84 168

13/6 13/6 14/6 14/6 15/6 15/6 16/6 16/6 17/6 17/6 18/6 18/6 19/6 19/6

Higher Risk	Malware and SPAM	Illegal/Harmful	Adult	Remote Proxies	Search	Business and Industry	News/Entertainment/S	Finance	Gambling	Messaging/Chat/Telep	Email	Social Networking	Downloads	Jobs and Resumes	Computing and Intern	Health	Peer to Peer/Torrents	Private IP Address	Others
Browsing Behaviour	Malware and SPAM	Illegal/Harmful	Adult	Remote Proxies	Search	Business and Industry	News/Entertainment/S	Finance	Gambling	Messaging/Chat/Telep	Email	Social Networking	Downloads	Jobs and Resumes	Computing and Intern	Health	Peer to Peer/Torrents	Private IP Address	Others

Total Events / Time

**Traffic Reputation Score**  
Metric: Data Volume

**URL Category By Browser**  
Metric: Data Volume

[ユーザーアクティビティの調査] ペインでは、testuser3 の高リスクアクティビティが、それぞれの URL カテゴリにイベントとして表示されます。



イベントにカーソルを合わせると、イベントの数が表示されます。イベントをクリックすると、イベント中に発生したトランザクションを調査できます。

Users > Dashboard > Transactions

User: [dropdown] [search icon]

Filters: URL Category: Others X User: testuser3 X [Remove all]

Transaction Details Rows: 20 Per Page Page 1 of 4 < Prev Next >

Time	Protocol	User	Domain	URL Category	Virtual Server	Client Port	Bytes In	Bytes Out
> Jun 14 06:30 AM	HTTPS	testuser3	dev.visualwebsiteoptimizer.com	Others	testswg	80	40	1043
> Jun 14 06:30 AM	HTTPS	testuser3	edellroot.badssl.com:443	Others	testswg	443	237	79
> Jun 14 06:30 AM	HTTPS	testuser3	dev.visualwebsiteoptimizer.com:443	Others	testswg	443	247	79
> Jun 14 06:30 AM	HTTPS	testuser3	no-common-name.badssl.com:443	Others	testswg	443	242	79
> Jun 14 06:30 AM	HTTPS	testuser3	connect.facebook.net:443	Others	testswg	443	237	79
> Jun 14 06:30 AM	HTTPS	testuser3	www.malwaredomainlist.com:443	Others	testswg	443	242	79
> Jun 14 06:30 AM	HTTPS	testuser3	www.vizury.com	Others	testswg	80	80	2453
> Jun 14 06:30 AM	HTTPS	testuser3	www.google.co.in:443	Others	testswg	443	233	79
> Jun 14 06:30 AM	HTTPS	testuser3	ecc256.badssl.com:443	Others	testswg	443	234	79
> Jun 14 06:30 AM	HTTPS	testuser3	hbchat.senseforth.com	Others	testswg	80	1040	74789
	OS	Windows 7		URL Category			0	
	HTTP Req Method	GET		User Agent			FireFox	
	HTTP Res Status	???		Client IP Address			10.144.8.12	
> Jun 14 06:30 AM	HTTPS	testuser3	sha512.badssl.com:443	Others	testswg	443	234	79
> Jun 14 06:30 AM	HTTPS	testuser3	revoked.badssl.com:443	Others	testswg	443	235	79
> Jun 14 06:30 AM	HTTPS	testuser3	hbsearch.senseforth.com:443	Others	testswg	443	240	79
> Jun 14 06:30 AM	HTTPS	testuser3	gp.symcd.com	Others	testswg	80	80	2197
> Jun 14 06:30 AM	HTTPS	testuser3	cbc.badssl.com:443	Others	testswg	443	231	79
> Jun 14 06:30 AM	HTTPS	testuser3	null.badssl.com:443	Others	testswg	443	232	79
> Jun 14 06:30 AM	HTTPS	testuser3	self-signed.badssl.com:443	Others	testswg	443	239	79
> Jun 14 06:30 AM	HTTPS	testuser3	invalid-expected-sct.badssl.com:443	Others	testswg	443	248	79
> Jun 14 06:30 AM	HTTPS	testuser3	www.google-analytics.com:443	Others	testswg	443	241	79
> Jun 14 06:30 AM	HTTPS	testuser3	search.services.mozilla.com:443	Others	testswg	443	619	79

Summary Panel

Protocols

Ports

URL Reputation

Browsers

Operating System

Bytes In

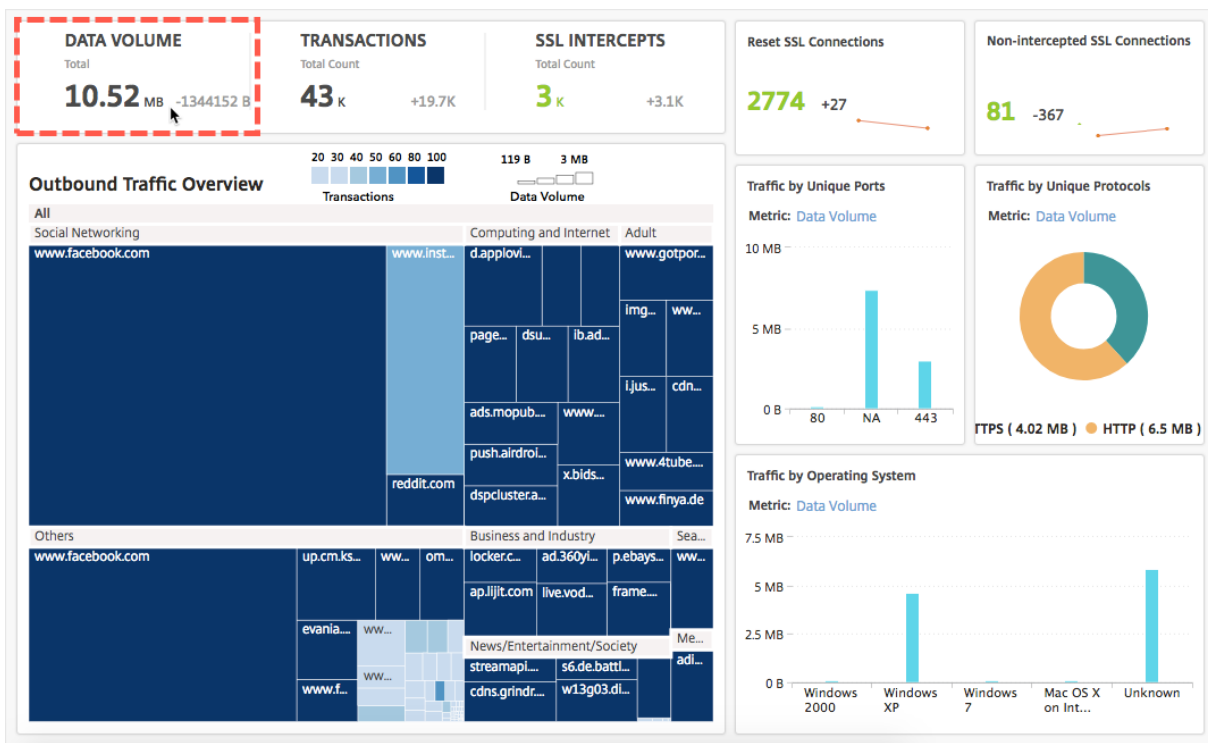
Bytes Out

この情報を使用して、システムがマルウェアに感染しているかどうかを判断したり、ユーザーの帯域幅消費パターンを把握したり、NetScaler ADC ポリシーを微調整したりできます。詳しくは、[Citrix SSL フォワードプロキシのドキュメントを参照してください](#)。

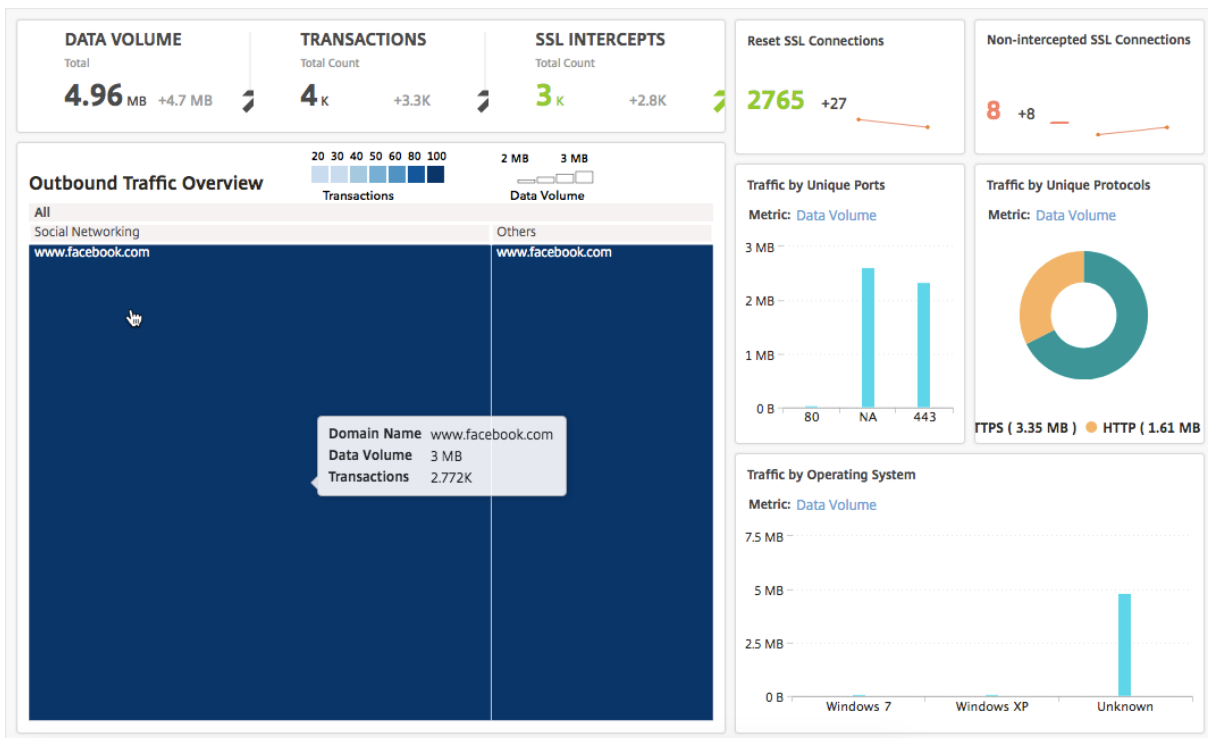
### 帯域幅消費のレポート

**Outbound Traffic Dashboard** と **User Dashboard** には、企業ネットワークからアクセスした 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が実行したアクティビティをまとめた複数のグラフが用意されています。

アウトバウンドトラフィックダッシュボードには、ネットワークからアクセスされた URL またはドメインによるデータ量の消費の詳細が表示されます。「アプリケーション」>「アウトバウンドトラフィックダッシュボード」に移動します。「データボリューム」セクションにデータボリュームの詳細が表示されます。

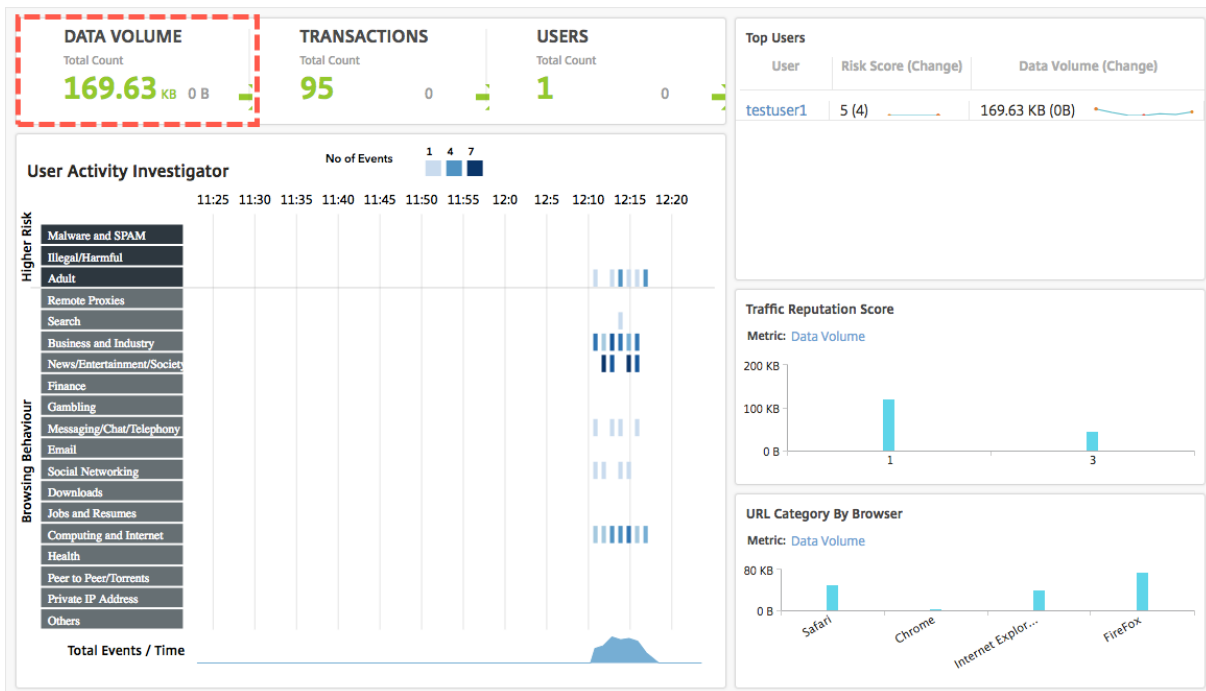


[ **Outbound Traffic Overview** ] ペインで、ドメインまたは URL をクリックすると、ドメインまたは URL によって消費されるデータボリュームの詳細を表示できます。

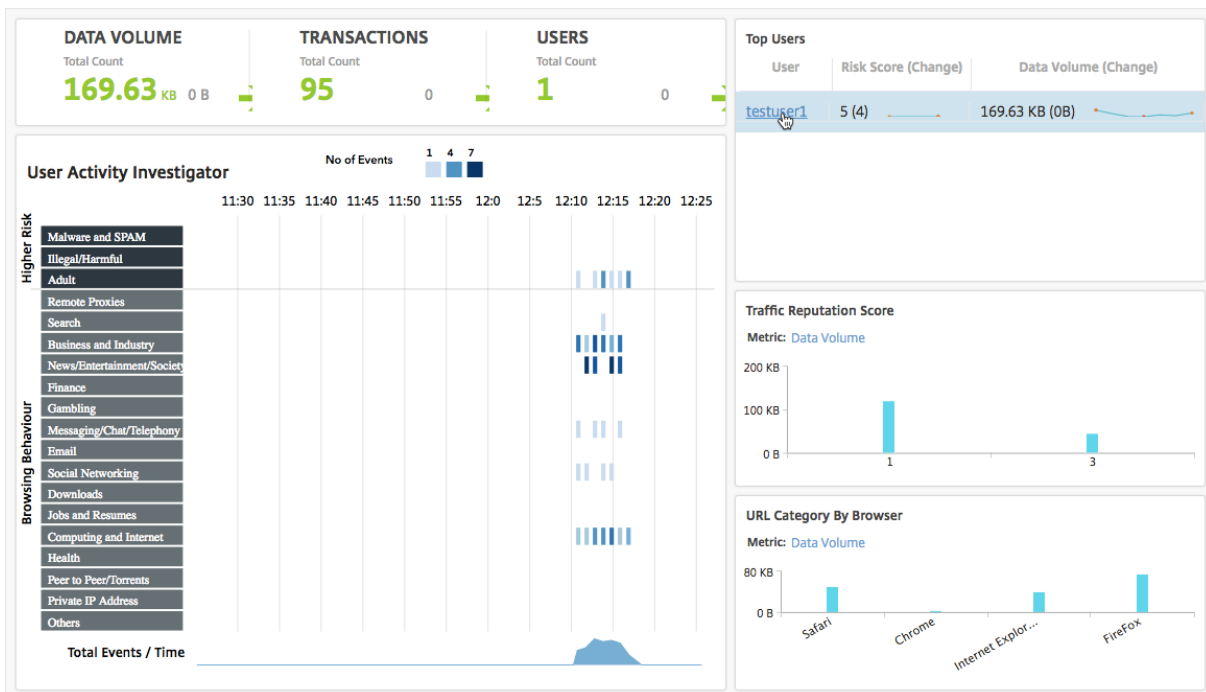


**User Dashboard** には、ネットワーク内のユーザが消費する帯域幅の詳細が表示されます。「ユーザー」>「ダッシュボード」に移動し、「ユーザー ダッシュボード」の「**DATA VOLUME**」セクションにユーザが消費した帯域幅の

詳細を表示します。



[ **Top Users** ] セクションからユーザーを選択すると、ユーザーが消費した帯域幅の詳細を表示できます。グラフ内の **DATA VOLUME** セクションおよびその他の主要なメトリックは、選択したユーザーに対してフィルタリングされます。



これらの詳細を使用して、消費帯域幅とその消費理由を把握できます。たとえば、ユーザーがソーシャルネットワーキング Web サイトにアクセスしていて、これにより帯域幅の消費量が多くなっている場合、管理者は NetScaler

ADC アプライアンスにアクセスし、URL リスト機能を構成して Web サイトへのアクセスを制御できます。詳細については、「ユースケース: カスタム URL セットを使用した URL フィルタリング」トピックを参照してください。

### アウトバウンドトラフィック分散の表示

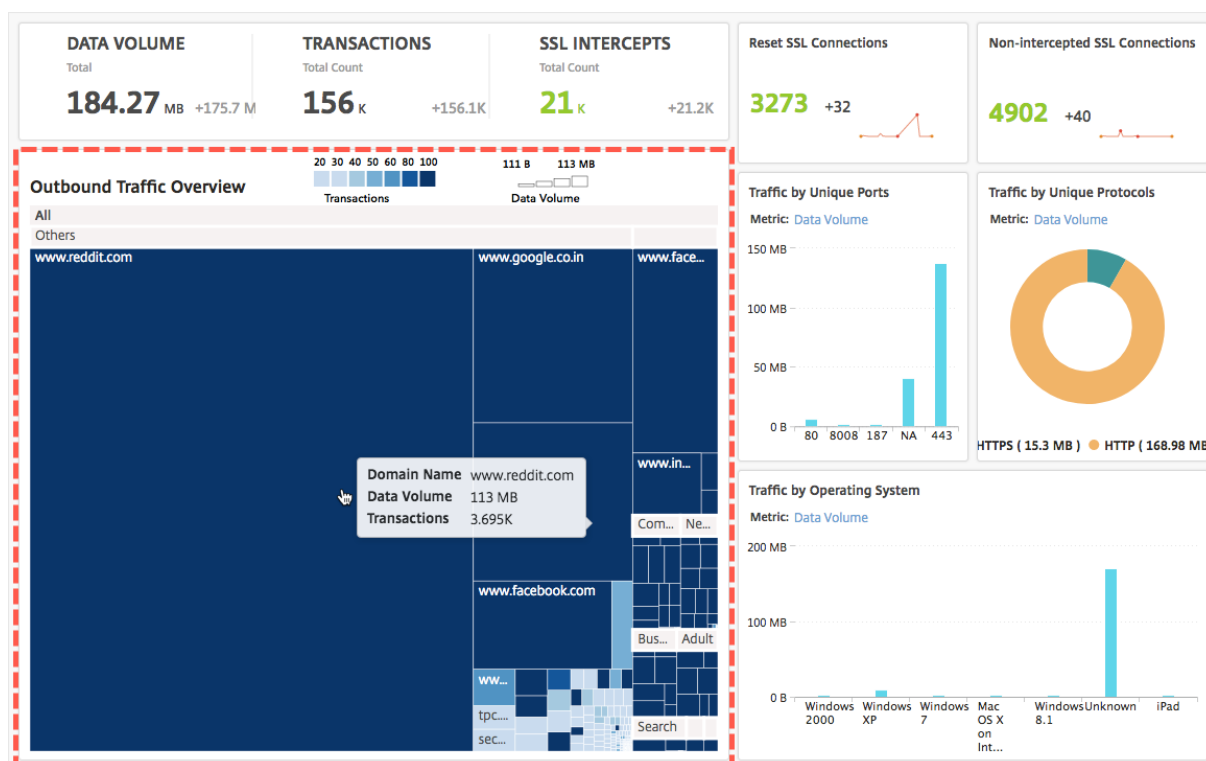
NetScaler ADC アプライアンスには、ネットワークからアクセスされる URL を分類するために使用できる URL の分類とフィルタリング機能が用意されています。NetScaler ADM では、送信トラフィックダッシュボードに [送信トラフィックの概要] ペインが表示されます。NetScaler ADM では、[アウトバウンドトラフィックの概要] ペインで、アクセスした URL またはドメインがショッピング、ニュース、モバイルなどのカテゴリにグループ化され、ネットワーク内のアウトバウンドトラフィックの分布が表示されます。選択した期間について、URL をクリックすると、次のことがわかります。

1. URL へのアクセスによって消費された帯域幅
2. URL にアクセス中に発生したトランザクション
3. URL にアクセス中に傍受された、傍受されていない、およびリセットされた SSL 接続の数

この情報により、送信トラフィックパターンを把握できるほか、特定の URL をブロックすべきかどうかなどの適切な意思決定を行うことができます。

アウトバウンドトラフィックの分布を表示するには：

「アプリケーション」>「アウトバウンドトラフィックダッシュボード」に移動します。[アウトバウンドトラフィックダッシュボード] の [アウトバウンドトラフィックの概要] ペインに URL が表示されます。



特定の URL の詳細を表示する場合には、その URL を選択します。

この情報を使用して、送信トラフィックパターンを理解し、NetScaler ADC アプライアンスで構成された URL フィルターを使用してネットワークトラフィックを制御できます。詳細については、「[URL フィルタリング](#)」を参照してください。

## オーケストレーション

February 6, 2024

SDN (Software Defined Networking: ソフトウェア制御ネットワーク) では、ネットワークをサポートするハードウェアに代わり、ソフトウェアアプリケーションコントローラーがネットワークとそのアクティビティを管理します。つまり SDN の場合、ネットワーク管理者は物理ネットワーク接続を論理ネットワーク接続に仮想化し、ソフトウェアベースの集中管理ツールを使用してネットワークサービスを管理できます。ネットワークエンジニアや管理者は、SDN を使用することで、頻繁に変わるビジネスの要件に対応できます。

よく知られている SDN のメリットには、トラフィックのプログラミング機能、優れたアジリティ、ポリシーに基づくネットワーク監視の設定、ネットワーク自動処理の実装がありますが、さらに SDN の特徴的なメリットとして次が挙げられます。

- 集中型ネットワークプロビジョニング
- 詳細なレベルによる優れたネットワークセキュリティ
- 運用コストの削減
- クラウド抽象化の促進
- コンテンツデリバリーの保証
- ネットワークダウンタイムの削減

Citrix アプリケーションデリバリー管理 (ADM) は、さまざまなベンダーの SDN コントローラーと統合することにより、企業ネットワーク内の SDN をサポートします。Citrix ADM は、VMware NSX Manager とシスコアプリケーションポリシーインフラストラクチャコントローラ (APIC) の両方をサポートしています。

## VMware NSX Manager

Citrix ADM は VMware ネットワーク仮想化プラットフォームと統合され、Citrix ADC サービスのデプロイ、構成、および管理を自動化します。この統合により、物理ネットワークトポロジに関連する従来の複雑さが解消され、vSphere/vCenter 管理者は Citrix ADC サービスをプログラムにより迅速に展開できるようになります。

VMware NSX Manager は、論理ファイアウォール、スイッチ、ルーター、ポートなどのネットワーク要素を明らかにして、さまざまなハイパーバイザー、クラウド管理システム、関連するネットワークハードウェアにおける仮想ネットワークを可能にします。また、外部ネットワークやセキュリティサービスをサポートします。



Citrix ADM のクラウドオーケストレーション機能により、Citrix ADC 製品と VMware NSX の統合が可能になり、次の機能が提供されます。

- 事前にプロビジョニングされたオンデマンドの VPX を、サービス挿入の一環として特定の Edge ゲートウェイに割り当てる。
- SSL や CS などの NetScaler ADC の高度な機能と、NSX 環境内で実行されているインスタンス上のアプリケーションテンプレートによる基本的な負荷分散を構成できます。
- サービス削除の一環として特定の Edge ゲートウェイから VPX の割り当てを解除し、同じ VPX を別の Edge ゲートウェイに再割り当てする機能。
- アプリケーションに必要なすべてのインフラストラクチャの展開ワークフローの一部として、vCenter コンソールから NetScaler ADC 機能を迅速に展開する機能。

長所:

- アプリケーション展開ワークフローの一環として、新しい ADC サービスをオンデマンドで自動的に割り当てる。
- アプリケーションテンプレートを通じて、アプリケーション固有の高度な ADC の機能をシンプルに構成できる。
- マルチテナントによる職務分掌とセルフサービス利用モデルを実現しつつ、クラウド管理者に一元的な管理を提供
- NetScaler ADM API との統合が簡単で、将来の予期せぬ使用をサポートできます。

NetScaler ADM で VMware NSX Manager を構成する方法の詳細については、「[NetScaler ADC アプライアンスと VMware NSX Manager の統合](#)」を参照してください。

### Cisco ACI のハイブリッドモード

Cisco ACI では、バージョン 1.3 (2f) でハイブリッドモードのサポートが導入されています。ハイブリッドモードでは、アプリケーションポリシーインフラストラクチャコントローラー (APIC) を介してネットワーク自動化を実行しながら、L4-L7 構成を APIC のデバイスマネージャーとして機能する Citrix ADM に委任できます。

Citrix ADC ハイブリッドモードソリューションは、ハイブリッドモードのデバイスパッケージと Citrix ADM でサポートされています。APIC のハイブリッドモードデバイスパッケージをアップロードする必要があります。詳細については、「[Cisco ACI のハイブリッドモードで NetScaler ADM を使用した NetScaler ADC オートメーション](#)」を参照してください。

### OpenStack: NetScaler ADC インスタンスの統合

February 6, 2024

NetScaler Application Delivery Management (ADM) のクラウドオーケストレーション機能により、NetScaler ADC 製品と OpenStack プラットフォームを統合できます。OpenStack プラットフォームでこの機能を使用することで、OpenStack ユーザーは NetScaler ADC 負荷分散機能 (LBaaS) を利用することができます。この後、OpenStack ユーザーは Citrix ADC インスタンスの OpenStack からロードバランサー構成をデプロイできます。

以下のセクションでは、Citrix ADM と OpenStack の統合ワークフローの機能について簡単に説明します。

### オープンスタック中性子 LBaaS 用 NetScaler ADC ドライバ

OpenStack ニュートロン LBaaS プラグインには、OpenStack が NetScaler ADM と通信できるようにする NetScaler ADC ドライバーが含まれています。OpenStack はこのドライバーを使用して、LBaaS API を介して行われた負荷分散設定を NetScaler ADM に転送します。これにより、目的の NetScaler ADC インスタンスにロードバランサー設定が作成されます。また、OpenStack はドライバーを使用して Citrix ADM を定期的に呼び出し、すべての負荷分散構成のさまざまなエンティティ (VIP やプールなど) のステータスを Citrix ADC から取得します。OpenStack プラットフォーム用の Citrix ADC ドライバーソフトウェアは、Citrix ADM にバンドルされています。ドライバーをダウンロードしてインストールするには、まず NetScaler ADM をインストールしてアプリケーションを起動する必要があります。

### Citrix ADM と OpenStack を相互に登録する

まず、NetScaler ADM に OpenStack 情報を登録する必要があります。OpenStack コントローラー IP アドレスとクラウド管理ユーザーの認証情報、および OpenStack Citrix ADC ドライバーのユーザー認証情報を指定します。後で Neutron 設定ファイル (neutron.conf) の Citrix ADC\_Driver セクションに同じログイン認証情報を指定して、OpenStack の Citrix ADC ドライバーが LB 構成中に Citrix ADM に接続できるようにすることができます。

OpenStack と Citrix ADM を相互に登録すると、両方が相互に通信できるようになります。また、OpenStack ユーザーは、OpenStack の既存の認証情報を使用して Citrix ADM ユーザーインターフェイスにログオンし、自分の LB 構成が Citrix ADC でどのように機能しているかを確認できます。

### OpenStack におけるテナント

OpenStack では、テナントはプロジェクトとも呼ばれます。テナントはユーザーのグループであり、テナント (プロジェクト) は、分離されたユーザーグループに割り当てられるリソースのセット (コンピューティング、ネットワーク、ストレージなど) として定義されることもあります。

### 配置ポリシー

配置ポリシーにより、ユーザーが作成した各ロードバランサー構成で使用される Citrix ADC インスタンスを柔軟に決定できます。または、Citrix ADM には、OpenStack テナントに基づいて Citrix ADC インスタンスを割り当てるオプションも用意されています。

### サービスパッケージ

サービスパッケージは、ポリシーおよび SLA と、デバイスまたは自動プロビジョニングの構成仕様、テナントおよび配置ポリシーがまとめられたものです。サービスパッケージは、通常、テナントに提供される分離ポリシーの条件で定義されています。

サービスパッケージに関するいくつかの重要点は次のとおりです。

- テナントを複数のサービスパッケージに含めることはできません。
- 複数のテナントを同一のサービスパッケージに割り当てることはできます。
- 自動プロビジョニング用に設定されたサービスパッケージでは、仮想 NetScaler ADC インスタンスは、1 つのプラットフォームタイプ (SDX プラットフォームまたは OpenStack Compute プラットフォーム) からのみ作成できます。

### LBaaS V1 と LBaaS V2 でサポートされている機能

OpenStack の LBaaS V1 ドライバーは OpenStack Horizon ユーザーインターフェイスからの操作をサポートしていますが、LBaaS V2 ドライバーがサポートしているのはコマンドライン操作のみです。

次の一覧は、OpenStack の LBaaS V1 と LBaaS V2 でサポートされている機能を示しています。

- LBaaS V1
  - 負荷分散
- LBaaS V2
  - 負荷分散
  - OpenStack のキーマネージャーである **Barbican** が管理する証明書で SSL オフロード
  - 証明書パッケージ (中間証明機関を含む)
  - SNI サポート

このドキュメントでは、以下の内容について説明します。

- [ユースケースのシナリオ](#)
- [Citrix ADM と OpenStack ワークフローの統合](#)
- [Prerequisites](#)
- [Citrix ADM と OpenStack の事前構成タスク](#)
- [Horizon を使用した LBaaS V1 の構成手順](#)
- [コマンドラインを使用した LBaaS V2 の構成手順](#)

- [OpenStack での Citrix ADC VPX インスタンスの手動 Provisioning](#)
- [Citrix ADM と OpenStack Heat サービスの統合](#)
- [NetScaler ADM での OpenStack アプリケーションの監視](#)

## ユースケースのシナリオ

以下のユースケースシナリオでは、NetScaler ADM と OpenStack プラットフォームを統合するワークフローについて説明します。

Example-Cloud-Provider という名前のある企業では、OpenStack コンポーネントを使用してクラウドをセットアップし、テナントにインフラストラクチャを提供しています。スティーブはこのクラウドプロバイダーの管理者であり、トムは Example-Cloud-Provider のクラウドインフラストラクチャのテナントです。トムの組織である Example-Sportsonline.com は、S1 と S1 の 2 台のサーバを必要とする。また、Tom は OpenStack プラットフォーム上のサーバ S1 と S2 間のトラフィックを負荷分散するために、専用の NetScaler ADC デバイスも必要とする。

この要件を満たすには、Steve は OpenStack と NetScaler ADM の両方をインストールして構成し、相互に互換性を持たせるように準備する必要があります。スティーブは、OpenStack に Example-SportsOnline という名前のテナントアカウントを作成し、そのテナントアカウントにリソースを割り当てる必要があります。また、リソースと構成を管理するために、Example-SportsOnline 用の複数のログオン資格情報（ユーザー）も作成する必要があります。これらの手順を経ると、トムが OpenStack に 2 台のサーバー、S1 と S2 を作成し、Example-SportsOnline.com のトラフィックを管理できるようになります。

スティーブは OpenStack の詳細を Citrix ADM に登録し、OpenStack のネットワークコンポーネントである Neutron で Citrix ADC LBaaS ドライバーを設定する必要があります。登録が完了すると、Citrix ADM は OpenStack のすべてのテナントの詳細を表示します。スティーブは、Citrix ADC LBaaS 機能を希望するユーザーのリストから Example-SportsOnline を選択し、Citrix ADM のロードバランサー構成に専用の Citrix ADC が割り当てられるようにトムを構成できます。

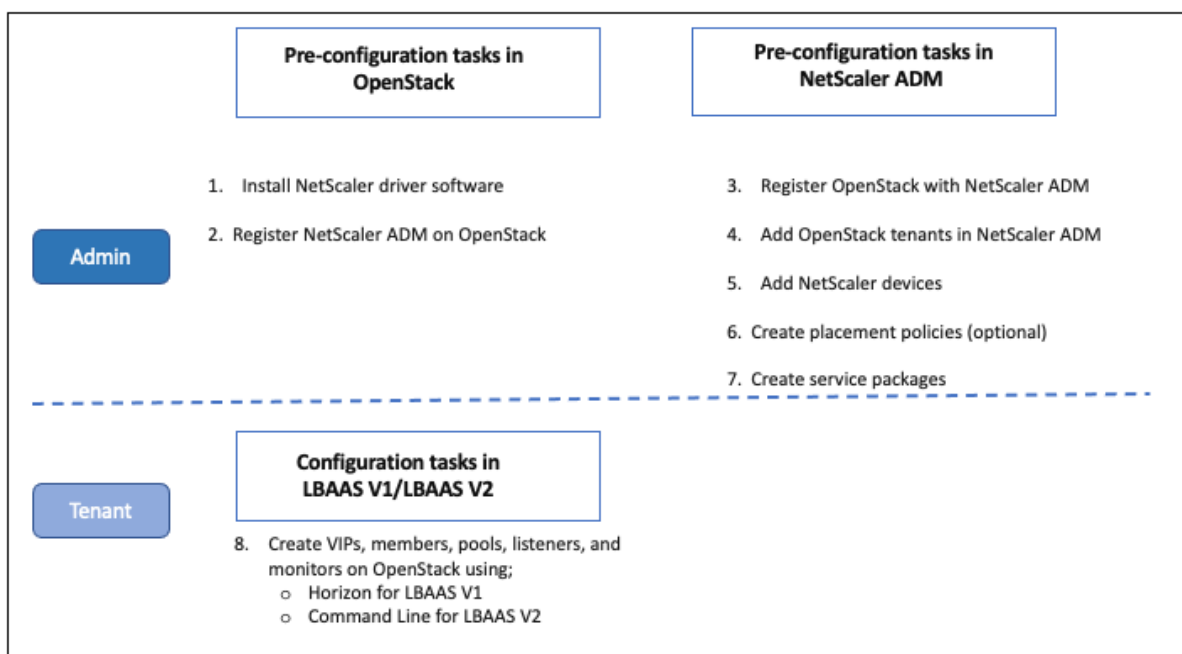
このため、スティーブは Citrix ADM ユーザーインターフェイスを使用して OpenStack のコンピューティングレイヤー（Nova）に Citrix ADC VPX インスタンスをプロビジョニングするか、トムが OpenStack で LB 構成を行うときに MAS が Citrix ADC VPX インスタンスをオンデマンドで自動プロビジョニングできるようにすることができます。いずれの場合も、Citrix ADM が VPX インスタンスを管理します。これを実現するために、スティーブは Citrix ADM でサービスパッケージを作成し、SLA でトムと合意したサービスパッケージの条件を定義します。たとえば、ロードバランサー構成を実現する専用インスタンスをトムに提供する場合、スティーブは「Dedicated」分離ポリシーを選択します。つまり、サービスパッケージでトムに対して非共有インスタンスを選択します。次に、多数の Citrix ADC VPX インスタンスをサービスパッケージに割り当て、Example-SportsOnline を、専用の Citrix ADC を必要とする他のテナントと一緒にサービスパッケージに関連付けます。その結果、トムが初めてロードバランサー構成を実行すると、Citrix ADM はサービスパッケージ内の Citrix ADC VPX インスタンスの 1 つを Example-SportsOnline に割り当てて、その構成をその Citrix ADC にも展開します。

これでTomは、OpenStackのLBaaSおよびUIによるプール、VIP (Virtual IP: 仮想IPアドレス)、ヘルスマニターの作成を通じて、負荷分散構成を作成できるようになります。OpenStackのプールとVIPは、Citrix ADC インスタンスにサービスグループおよび仮想サーバーとしてデプロイされます。Tomは、ヘルスマニターを作成してサーバーを監視し、いつでも稼働してCitrix ADCからアクセスできるサーバーのみにアプリケーショントラフィックを送信することもできます。

OpenStackで作成された負荷分散設定がCitrix ADCインスタンスに実装されるようになりました。完全に構成されると、NetScaler ADC VPXインスタンスが負荷分散機能を引き継ぎ、アプリケーショントラフィックの受け入れを開始し、Tomによって作成されたサーバーS1とS2間のトラフィックの負荷分散を行います。

### Citrix ADM と OpenStack ワークフローの統合

次のフローチャートは、LBaaS V1 および LBaaS V2 構成時に従う必要のあるワークフローです。



### 前提条件

February 6, 2024

Citrix ADC 仮想インスタンスを OpenStack プラットフォームと統合する前に、次の要件が満たされていることを確認してください。

## NetScaler ADM および OpenStack ソフトウェア要件

- Citrix ADM 13.0 は、最小ハードウェア要件システムを満たす、サポートされているハイパーバイザーワークステーションにインストールされます。
- OpenStack コンポーネントがインストールされ、実行されています。
- NetScaler ADM 13.0 では、ニュートン、オカタ、パイク、クイーンズの **OpenStack** バージョンがサポートされています。

## NetScaler ADM ハードウェア要件

NetScaler ADC 仮想インスタンスをインストールするには、OpenStack サーバーに次の仮想コンピューティングリソースがあることを確認してください。

コンポーネント	条件
RAM	8 GB
仮想 CPU	8
記憶域	500 GB
仮想ネットワーク インターフェイス	1
スループット	1Gbps または 100Mbps

### 注

指定されたメモリとハードディスクの要件は、ホスト上で他の仮想マシンが実行されていないことを考慮して、Citrix ADM を OpenStack プラットフォームにデプロイするためのものです。OpenStack のハードウェア要件は、OpenStack で実行される仮想マシンの数によって異なります。

## NetScaler ADM および OpenStack での事前構成タスク

February 6, 2024

このセクションでは、Citrix Application Delivery Management (ADM) と OpenStack を設定する前に、事前設定タスクを実行するのに役立ちます。

## Citrix ADM のインストール

サポートされている Hypervisor に NetScaler ADM をインストールします。NetScaler ADM をダウンロードしてインストールする方法については、「NetScaler ADM の展開」を参照してください。


## NetScaler ADC ドライバーソフトウェアのインストールと OpenStack への NetScaler ADM 登録

Citrix ADM ダウンロードページから OpenStack 用の Citrix ADC バンドルをダウンロードします。

**Citrix ADM GUI** を使用して **OpenStack** プラットフォームに **Citrix ADC** ドライバーをインストールするには:

1. Citrix ADM で、「ダウンロード」をクリックします。Citrix ADM のダウンロードページには、ニュートン、オカタ、およびパイクの OpenStack バージョンに必要な **OpenStack** ソフトウェア用の **Citrix ADC** バンドルをダウンロードするためのリンクがあります。
2. 最新の Citrix ADC バンドル tar ファイルを OpenStack Controller の一時ディレクトリ (たとえば、/tmp) にダウンロードします。このバンドルには、すべての OpenStack リリース用の LBaaS V2 ドライバーと Heat プラグインが含まれています。

Downloads for OpenStack

 Citrix ADC bundle for OpenStack. Contains Citrix ADC LBaaS drivers and Heat plugin.  
Citrix ADC bundle for OpenStack has Heat plugin and drivers for both OpenStack LBaaS V1 and V2. The Citrix ADC bundle files provided here includes the following drivers and plugins: LBaaS V1 and LBaaS V2 drivers for OpenStack Liberty and Mitaka releases, LBaaS V2 driver for OpenStack Newton release and Heat plug-in for Heat across OpenStack releases

3. 次のコマンドを実行して、NetScaler ADC ドライバの tar ファイルからファイルを抽出します。

```
tar -xvzf <name_of_tar_file>
```

4. OpenStack <Release Name> setup がある場合は、プロンプトで次のコマンドを入力します。

```
cd <Release Name>
```

例:

```
cd Newton
```

5. 次のコマンドを実行してドライバをインストールし、Citrix ADM IP アドレス、OpenStack を Citrix ADM に登録したときに設定した Citrix ADC ドライバパスワード、およびプロトコルを指定します。

```
./install.sh --ip=<NetScaler_MAS_IP> --password=<password> --  
protocol=<protocol> --neutron-lbaas-path <neutron-lbaas-directory  
-path>
```

単一ノード **OpenStack** のセットアップ例:

```
./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --  
neutron-lbaas-path=/opt/stack/neutron-lbaas
```

マルチノード **OpenStack** セットアップ例:

```
./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --  
neutron-lbaas-path=/usr/lib/python2.7/site-packages
```

注

システムのneutron-lbaasディレクトリのパスの指定は任意です。このパスを指定すると、スクリプトによるドライバーの検索が容易になります。

Citrix ADM が OpenStack に正常に登録されたら、OpenStack のユーザー認証情報を使用して Citrix ADM にログオンすることもできます。

Citrix ADM が OpenStack に正常に登録されたら、OpenStack Neutron サービスを再起動します。

## OpenStack を Citrix ADM に登録する

**Citrix ADM GUI** を使用して **OpenStack** を **Citrix ADM** に登録するには:

1. Citrix ADM で、[オーケストレーション] > [クラウドオーケストレーション] > [OpenStack\*\*] に移動します。
2. 「**OpenStack** の設定を設定」をクリックします。
3. 「**OpenStack** 設定の構成」ページでは、Citrix ADM で OpenStack を設定するためのパラメータを設定できます。[Default] と [Customized] の 2 つのオプションがあります。

**OpenStack** の **Newton** および **Ocata** リリースでは、デフォルトまたはカスタマイズされたデプロイメントタイプを使用できます。ただし、Pike リリースでは、カスタマイズされたデプロイタイプを使用して OpenStack を Citrix ADM に登録する必要があります。

- 既定のデプロイタイプ

OpenStack サービスがデフォルトポートで実行されている場合は、「デフォルト」を選択します。たとえば、Neutron サービスのデフォルトポートは 9696 で、Keystone サービスのデフォルトポートは 5000 です。

1. OpenStack コントローラー IP アドレス-OpenStack コントローラーの IP アドレス ( **KeyStone** サービスと **Neutron** サービスの両方がこの IP アドレスで到達可能である必要があります)。たとえば、IP アドレスを「10.102.205.23」と入力します。
2. OpenStack Admin ユーザー名-OpenStack コントローラーの管理ユーザー名。たとえば、「admin1」と入力します。
3. Password - OpenStack コントローラーの管理者ユーザーのパスワード。
4. OpenStack 管理テナント-OpenStack 上の管理テナントの名前。たとえば、「admin」と入力します。



OpenStack Details

Configure access details of OpenStack controller which can be used by NetScaler Console. NetScaler Console will use these credentials to create NetScaler virtual appliances, to reserve IPs, to fetch tenants/flavours/images etc

Openstack Deployment Type\*

Default  Customized

OpenStack Controller IP Address/FQDN\*

HTTPS  HTTP

Neutron Service URL/FQDN\*

Keystone Service URL/FQDN\*

Keystone Admin Service URL/FQDN\*

Nova Service URL/FQDN\*

Glance Service URL/FQDN\*

OpenStack Admin Username\*

Password\*

OpenStack Admin Tenant\*

 ⓘ

• カスタマイズされた展開の種類

OpenStack サービスがデフォルトポートと異なるポートで実行されている場合は、デプロイタイプを **Customized** として選択します。サービスが異なるポートで実行されている場合は、ここでそのポートを指定します。NetScaler ADM への **OpenStack** ニュートンおよび **Ocata** リリースの登録は、OpenStack Pike リリースの登録とは異なります。

**OpenStack** のニュートンとオカタのリリース:

1. OpenStack の Newton リリースを登録する場合は、さまざまな OpenStack サービスのポート番号を指定します。
2. OpenStack Admin のユーザ名、パスワード、および OpenStack Admin テナントのユーザ名を [デフォルト] 設定で先に指定したとおりに指定します。

### OpenStack Details

Configure access details of OpenStack controller which can be used by NetScaler Console. NetScaler Console will use these credentials to create NetScaler virtual appliances, to reserve IPs, to fetch tenants/flavours/images etc

Openstack Deployment Type\*

Default  Customized

OpenStack Controller IP Address/FQDN\*

HTTPS  HTTP

Neutron Service URL/FQDN\*

Keystone Service URL/FQDN\*

Keystone Admin Service URL/FQDN\*

Nova Service URL/FQDN\*

Glance Service URL/FQDN\*

OpenStack Admin Username\*

Password\*

OpenStack Admin Tenant\*

ⓘ

**OpenStack の Pike リリース:**

OpenStack の Pike リリースを登録する場合は、次の図に示すように、OpenStack サービスの詳細を入力します。また、OpenStack Admin ユーザー名、パスワード、および OpenStack Admin テナントユーザー名をデフォルト設定で指定する必要があります。

OpenStack Details

Configure access details of OpenStack controller which can be used by NetScaler Console. NetScaler Console will use these credentials to create NetScaler virtual appliances, to reserve IPs, to fetch tenants/flavours/images etc

Openstack Deployment Type\*

Default  Customized

OpenStack Controller IP Address/FQDN\*

HTTPS  HTTP

Neutron Service URL/FQDN\*

Keystone Service URL/FQDN\*

Keystone Admin Service URL/FQDN\*

Nova Service URL/FQDN\*

Glance Service URL/FQDN\*

OpenStack Admin Username\*

Password\*

OpenStack Admin Tenant\*

 ?

1. 「**OpenStack Neutron LBaaS-NetScaler ADC** ドライバーが使用する資格情報」セクションで、OpenStack NetScaler ADC ドライバーのユーザーアカウントの NetScaler ADC ドライバーのパスワードを設定します。NetScaler ADM は、これらの資格情報を使用して、OpenStack NetScaler ADC ドライバーからの呼び出しを認証します。OpenStack コントローラーで NetScaler ADC ドライバーのインストールスクリプトを実行するときは、同じパスワードを指定する必要があります。

OpenStack - Credentials Used by NetScaler Driver and Heat

Configure an account in NetScaler Console that can be used by NetScaler driver and Heat, present in OpenStack Controller, to contact NetScaler Console. Once configured here, provide these credentials in the [citrix\_adc\_driver] section of neutron configuration file /etc/neutron/neutron.conf .

NetScaler Username

NetScaler Password\*

 ?

Confirm NetScaler Password\*

 ?

2. **[OK]** をクリックします。

## OpenStack でのテナントの作成

OpenStack にプロジェクトまたはテナントを作成し、そのプロジェクトまたはテナントにユーザーを追加し、すべてのユーザーに役割を割り当てます。OpenStack の Identity サービスである **KeyStone** は、各 OpenStack サービスに認証サービスを提供します。KeyStone 認証サービスでは、ドメイン、プロジェクト（テナント）、ユーザー、および役割の組み合わせを使用します。

OpenStack でプロジェクトを作成する方法や、他のタスクを実行する方法の詳細については、にある OpenStack のドキュメントを参照してください。 <http://docs.openstack.org/>

## OpenStack テナントの追加

1. Citrix ADM で、「オーケストレーション」>「クラウドオーケストレーション」>「**OpenStack**」>「**OpenStack テナント**」に移動し、「追加」をクリックします。
2. **[Add OpenStack Tenants]** ページで **[+Add]** をクリックして、OpenStack テナントを選択します。
3. **[OK]** をクリックします。

OpenStack を統合するときに、事前プロビジョニングされたインスタンスと自動プロビジョニングされたインスタンスのどちらを使用するのかに応じて、次のどちらかのタスクを実行します。

- NetScaler ADC デバイスの事前プロビジョニング
- OpenStack で NetScaler ADC VPX デバイスを自動プロビジョニングする

## NetScaler ADC デバイスのプロビジョニング

OpenStack を統合するときに、事前プロビジョニングされたインスタンスと自動プロビジョニングされたインスタンスのどちらを使用するのかに応じて、次のどちらかのタスクを実行します。

- NetScaler ADC デバイスの事前プロビジョニング
- OpenStack で NetScaler ADC VPX デバイスを自動プロビジョニングする

## NetScaler ADC デバイスの事前プロビジョニング

Citrix ADC デバイスを Citrix Hypervisor、KVM、ESX などの任意のハイパーバイザープラットフォームにインストールし、そのインスタンスを Citrix ADM に追加します。次に、NetScaler ADM がこのデバイスを管理し、サーバーのトラフィックを負荷分散します。

既存の **Citrix ADC VPX** インスタンスを **Citrix ADM** に追加するには:

1. Citrix ADM で、[インフラストラクチャ] > [インスタンス] > **[Citrix ADC VPX]** に移動し、[追加] をクリックします。

2. **[Citrix ADC VPX の追加]** ページで、Citrix ADC VPX インスタンスの IP アドレスを指定し、[プロファイル名] リストからインスタンス プロファイルを選択します。インスタンスプロファイルには、Citrix ADC VPX へのログオンに使用される認証情報が含まれています。[+] アイコンをクリックして新規のインスタンスプロファイルを作成することもできます。[OK] をクリックします。

### Citrix ADC デバイスの自動プロビジョニング

Citrix ダウンロードページから必要な Citrix ADC インスタンスイメージをダウンロードし、OpenStack イメージングサービスの Glance にアップロードします。Glance でイメージを利用できるようにすると、テナントにインスタンスを割り当てるときに、Citrix ADC インスタンスをオンデマンドで構成できます。

**Citrix ADC VPX** デバイスを **OpenStack** に自動プロビジョニングするには:

1. Citrix ADM で、[オーケストレーション] > [クラウドオーケストレーション] > [OpenStack\*\*] に移動します。
2. 「デプロイ設定」をクリックします。
3. 次のパラメーターを設定します。
  - a) 管理ネットワーク-自動プロビジョニングされた Citrix ADC VPX が接続されている OpenStack 上の管理ネットワークを選択します。
  - b) Profile Name - ボックスの一覧からプロファイルを選択します。NetScaler ADM は、このプロファイルに含まれているパスワードを使用して、新しい自動プロビジョニングされた NetScaler ADC VPX インスタンスを構成します。
  - c) ライセンス-新しい自動プロビジョニングされた NetScaler ADC インスタンスのライセンス認証に使用される NetScaler ADM ライセンスアクセスコードを提供します。NetScaler ADM は、管理ネットワーク内の OpenStack コンピューティング上の NetScaler ADC インスタンスをプロビジョニングし、指定されたライセンスコードを使用してライセンスのインストールをトリガーします。NetScaler ADC インスタンスは、ここで指定したライセンスアクセスコードを使用して、Citrix Web サイトからライセンスファイルをダウンロードします。
  - d) NetScaler ADC VPX イメージの概要-NetScaler ADC VPX インスタンスの作成に使用される OpenStack Glance で使用できる NetScaler ADC VPX イメージを選択します。
  - e) プロキシ設定-ライセンスをインストールするための Citrix ADC プロキシサーバーの詳細を指定します。これは、Citrix ADC が管理ネットワーク経由でインターネットに直接アクセスできない場合に必要になることがあります。
4. [OK] をクリックします。

## NetScaler ADM でのサービスパッケージの作成

**Citrix ADM** でテナント用のサービスパッケージを作成するには:

1. Citrix ADM で、[オーケストレーション] > [クラウドオーケストレーション] > [OpenStack\*\*] > [\*\* サービスパッケージ] に移動し、[追加] をクリックします。
2. 「サービスパッケージ」 ページで、次のパラメータを指定します。
  - a) Name - サービスパッケージの名前。たとえば、「SVC-PKG-GOLD」と入力します。
  - b) Citrix ADC インスタンス割り当て-サービスパッケージで定義されているインスタンス割り当てのタイプで、これに基づいて Citrix ADC インスタンスリソースがテナントに割り当てられます。[専用] を選択します。ポリシーの詳細については、「[サービスパッケージ分離ポリシー](#)」を参照してください。
  - c) NetScaler ADC インスタンスのプロビジョニング: [既存のインスタンス] を選択して、既存の NetScaler ADC インスタンスをテナントに割り当てます。構成中に Citrix ADC インスタンスを作成する場合は、「オンデマンドでインスタンスを作成」を選択します。
  - d) Citrix ADC インスタンスタイプ- **Citrix ADC VPX** を選択します。

注

:SDX プラットフォームでホストされている事前にプロビジョニングされた Citrix ADC インスタンスを割り当てるには、Citrix ADC VPX を選択します。

3. [ 続行 ] をクリックして、テナントをサービスパッケージに関連付けます。

注

: **Citrix ADC** インスタンス を高可用性モードでデプロイする場合は、高可用性のために Citrix ADC インスタンス のプロビジョニングペアを有効にします。

4. 「インスタンスの割り当て」セクションで、「追加」をクリックし、テナントに割り当てる Citrix ADC インスタンスを選択して、「続行」をクリックします。
5. 「**OpenStack** テナント/プレイスメントポリシーの割り当て」セクションの「**OpenStack** テナント」で、「追加」をクリックしてテナントを選択します。
6. [**Continue**]、[**Done**] の順にクリックします。

注:

ポリシーが見つからない場合、フォールバックメカニズムが復活し、NetScaler ADM はテナントに基づいて NetScaler ADC インスタンスを割り当てます。テナントがどのサービスパッケージにも含まれていない場合、NetScaler ADM は次のエラーメッセージを表示します。「テナント\

## 配置ポリシーの作成（オプション）

分離ポリシーはテナントベースではありません。柔軟な配置ポリシーを作成することもできます。このポリシーは、テナント名またはテナント ID だけでなくその他のカスタム属性にも基づきます。

**Citrix ADM** でテナントの配置ポリシーを作成するには:

1. Citrix ADM で、[オーケストレーション] > [クラウドオーケストレーション] > [OpenStack\*\*] > [**\*\* 配置ポリシー**] に移動し、[追加] をクリックします。
2. [**Add Placement Policy**] ページで、次のパラメーターを設定します。
  - a) Name - 配置ポリシーの名前を入力します。
  - b) Sample Expressions - 一覧から式のサンプルを選択します。これらのサンプルは、配置ポリシーを作成するのに役立ちます。
  - c) Expression - このボックスには、前のボックスで選択したサンプル式に基づいて、ブール式を入力します。必要に応じてボックス名を編集します。
3. [**OK**] をクリックします。

## NetScaler ADC インスタンスからクライアントネットワーク経由でバックエンドサーバーへのトラフィックを有効にする

デフォルトでは、OpenStack オーケストレーションワークフローでは、NetScaler ADC インスタンスはロードバランサーまたはクライアントネットワーク、メンバーまたはサーバーネットワークに動的にバインドされます。

一部のデプロイメントでは、クライアントネットワーク経由でサーバーにアクセスでき、クライアントゲートウェイ経由でルーティングすることもできます。このような場合、Citrix ADC インスタンスをサーバーネットワークにバインドする必要はなく、クライアントネットワークにのみバインドする必要があります。

クライアントゲートウェイ経由のトラフィックを設定するには、次の設定を行います。

[オーケストレーション] > [クラウドオーケストレーション] > [OpenStack] > [デプロイ設定] に移動し、[VIP ネットワークのみをプロビジョニングし、VIP ネットワーク経由でプールトラフィックをルーティングする] オプションを選択します。

次に、Citrix ADM は、クライアントネットワークに SNIP を追加して Citrix ADC インスタンスをクライアントネットワークに構成し、さらにクライアントネットワークゲートウェイにデフォルトルートを追加します。これにより、インスタンスはクライアントゲートウェイを介してサーバーに到達できます。

## Citrix ADC SDX プラットフォームにデプロイされた Citrix ADC VPX デバイスの自動プロビジョニング

Citrix ADM に Citrix ADC SDX プラットフォームを追加して、Citrix ADM がこのプラットフォーム上のインスタンスをオンデマンドでプロビジョニングできるようにします。

NetScaler ADC SDX プラットフォームにデプロイされた NetScaler ADC インスタンスを自動プロビジョニングするには：

1. Citrix ADM GUI で、[ネットワーク] > [インスタンス] > [Citrix ADC SDX] に移動し、[追加] をクリックして Citrix ADC SDX プラットフォームを追加します。
2. [オーケストレーション] > [クラウドオーケストレーション] > [OpenStack] > [デプロイ設定] に移動します。
3. 管理ネットワーク セクションで、自動プロビジョニングされた Citrix ADC SDX が接続されている OpenStack 上の管理ネットワークを選択します。
  - a) 「プロファイル名」で、ドロップダウンリストからプロファイルを選択します。NetScaler ADM は、このプロファイルに含まれているパスワードを使用して、新しい自動プロビジョニングされた NetScaler ADC VPX インスタンスを構成します。
  - b) [OK] をクリックします。
4. Citrix ADC SDX プラットフォームを OpenStack でプロビジョニングするには、[オーケストレーション] > [クラウドオーケストレーション] > [OpenStack\*\*] > [サービスパッケージ \*\*] に移動します。
  - a) [追加] をクリックして新しいサービスパッケージを作成します。



- b) サービスパッケージの名前を入力します。
  - c) **Citrix ADC** インスタンス割り当て フィールドで、「専用」を選択します。
  - d) 「**Citrix ADC** インスタンス **Provisioning**」フィールドで「インスタンスをオンデマンドで作成」を選択し、「自動プロビジョニングプラットフォーム」フィールドで「**Citrix ADC SDX**」を選択します。
  - e) デフォルトでは、Citrix ADC VPX インスタンスのみが Citrix ADC SDX プラットフォームにプロビジョニングされます。
  - f) [続行] をクリックします。
  - g) 自動プロビジョニング設定セクションで、リソースプロパティを設定します。
    - i. スループットフィールド。「1000 Mbps」と入力します。
    - ii. **NetScaler ADC** バージョン] フィールド。リストから、Citrix ADC **SDX プラットフォーム** に存在する Citrix ADC VPX イメージの適切なバージョンを選択します。
  - h) [**NetScaler ADC SDX** プラットフォーム] セクションで、[追加] をクリックして SDX プラットフォームをサービスパッケージに追加します。
  - i) [続行] をクリックします。
  - j) 「**OpenStack** テナントの設定」セクションで、「追加」をクリックしてテナントを追加します。[新規] をクリックして新しいテナントを追加することもできます。
  - k) 「完了」をクリックします。
5. LBaaS V2 API を実装するには、Neutron LBaaS コマンドを使用します。任意の Neutron クライアントに接続し、設定タスクを実行します。設定コマンドの実行方法の詳細については、「[コマンドラインを使用した LBaaS V2 の設定](#)」を参照してください。

## Horizon を使用した LBaaS V1 の設定

February 6, 2024

これでトムは、OpenStack Horizon ポータルにログオンして LBaaS プールを作成し、このプールのすべてのメンバーが存在するサブネットを選択できるようになりました。トムは仮想 IP (VIP) アドレスを追加して、自分で作成したプールに割り当てる必要があります。この操作は、コマンドラインまたは API 経由でも実行できます。トムのサーバーの外部クライアントは、割り当てられた Citrix ADC でホストされているこの VIP アドレスに接続でき、Citrix ADC はすべての要求を構成されたポート上のプールメンバーに配信します。

LBaaS プールメンバーは、選択したプールに追加される負荷分散サーバー群です。トムは、これらの各メンバーに重要度とポートを割り当てることができます。

ヘルスマニターを使用して、プールのすべてのメンバーのヘルス状況と機能状態を監視します。トムは、OpenStack 内にサーバーヘルスマニター用テンプレートを作成できます。テンプレートには、遅延、タイムアウト、リトライ回数、メソッド、URL パス、成功時に返される HTTP コードを指定します。モニタを作成したら、トムはそのモニターを、作成済みのプールと関連付ける必要があります。

OpenStack でプールやその他の LBaaS 設定タスクを作成する方法の詳細については、[OpenStack ドキュメント](#) を参照してください。

重要

OpenStack の Liberty リリースでは、LBaaS V1 はサポートされません。詳細については、「[OpenStack リリースノート](#)」を参照してください。

## コマンドラインを使用した **LBaaS V2** の設定

February 6, 2024

LBaaS V2 は、**Barbican** が管理する証明書による SSL オフロード、証明書バンドル (中間認証局を含む)、SNI サポート、および通常の負荷分散機能をサポートしています。LBaaS V2 では、設定タスクを実行するためのコマンドラインインターフェイスのみをサポートしています。LBaaS V2 API を実装するには、Neutron LBaaS コマンドを使用します。

注

SSL オフロード機能が必要な場合は、証明書とキーを **Barbican** サービスにアップロードしてください。手順 1、2、3 は、SSL オフロードがサポートされている場合に実行してください。それ以外の場合は、[手順 4](#)から作業を続行して、ロードバランサー、リスナー、プール、メンバーを作成してください。

1. 次のコマンドを使用して、証明書を **Barbican** サービスにアップロードします:

```
1 barbican secret store --payload-content-type <content_type> --name
   <certificate_name> --payload<certificate_location>
2 <!--NeedCopy-->
```

例:

```
1 barbican secret store --payload-content-type='text/plain' --name='
   hp_server_certificate' --payload=" hp_server/tmp/
   server_certificate"
2 <!--NeedCopy-->
```

```
stack@ubuntu:/opt/stack/devstack$ barbican secret store --payload-content-type='text/plain' --name='server-cert5' --payload="$(cat /tmp/server_cert5)"
Starting new HTTP connection (1): 10.106.43.15
Starting new HTTP connection (1): 10.106.43.15
-----
| Field      | Value
|-----|-----
| Secret href | http://localhost:9311/v1/secrets/c36a4a82-87e4-4873-9efe-55108875ef58
| Name        | server-cert5
| Created     | None
| Status      | None
| Content types | (u'default': u'text/plain')
| Algorithm    | aes
| Bit length   | 256
| Secret type  | opaque
| Mode         | cbc
| Expiration   | None
-----
stack@ubuntu:/opt/stack/devstack$
```

2. 以下のコマンドを使用して **Barbican** サービスにキーをアップロードします:

```
1 barbican secret store --payload-content-type <content_type> --name
  <key_name> --payload<key_location>
2 <!--NeedCopy-->
```

例:

```
1 barbican secret store -- payload-content-type='text/plain' --name=
  'shp_server_key' --payload="hp-server/tmp/server_key"
2 <!--NeedCopy-->
```

```
stack@ubuntu:/opt/stack/devstack$ barbican secret store --payload-content-type='text/plain' --name='server-key5' --payload="$(cat /tmp/server_key5)"
Starting new HTTP connection (1): 10.106.43.15
Starting new HTTP connection (1): 10.106.43.15
-----
| Field      | Value
|-----|-----
| Secret href | http://localhost:9311/v1/secrets/1b9e1a93-2aeb-4101-8002-e52acab987b0
| Name        | server-key5
| Created     | None
| Status      | None
| Content types | (u'default': u'text/plain')
| Algorithm    | aes
| Bit length   | 256
| Secret type  | opaque
| Mode         | cbc
| Expiration   | None
-----
stack@ubuntu:/opt/stack/devstack$
```

注

これらの2つの **Barbican** コマンドを実行して証明書とキーを読み込む場合、Secret href フィールドには場所または URL が表示されます。証明書とキーは、OpenStack がインストールされているシステムのこの場所に保存されます。ステップ3で **Barbican** サービスでコンテナを作成するときに、これらのリンクをコピーしてパラメーターとして指定します。

3. 次のコマンドを使用して、証明書とキーを保存するコンテナを **Barbican** サービスで作成します:

コマンドで、以下のように置き換えます。証明書をアップロードしたときに [Secret href] フィールドから取得した URL を指定します。同様に、キーをアップロードしたときに Secret href フィールドから取得した URL を使用します。

```
1 barbican secret container create --name<container_name> --type<
  container_type> --secret<certificate_url> --secret<key_url>
2 <!--NeedCopy-->
```

例:

```

1 barbican secret container create --name='hp_container' --type='
  certificate' --secret="`certificate=http://localhost:9311/v1/
  secrets/e36a4a82-87e4-4873-9efe-55108875ef58 --secret="
  private_key=http://localhost:9311/v1/secrets/1b9e1a93-2aeb
  -4101-8002-e52acab987b0`"
2 <!--NeedCopy-->

```

```

stack@ubuntu:/opt/stack/devstack$ barbican secret container create --name='hp_container' --type='certificate' --secret="`certificate=http://localhost:9311/v1/secrets/e36a4a82-87e4-4873-9efe-55108875ef58 --secret="private_key=http://localhost:9311/v1/secrets/1b9e1a93-2aeb-4101-8002-e52acab987b0`"
Starting new HTTP connection (1): 10.106.43.15
Starting new HTTP connection (1): 10.106.43.15
Starting new HTTP connection (1): localhost
-----
| Field | Value |
-----
| Container href | http://localhost:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa |
| Name | hp_container |
| Created | None |
| Status | ACTIVE |
| Type | certificate |
| Certificate | http://localhost:9311/v1/secrets/e36a4a82-87e4-4873-9efe-55108875ef58 |
| Intermediates | None |
| Private Key | http://localhost:9311/v1/secrets/1b9e1a93-2aeb-4101-8002-e52acab987b0 |
| PK Passphrase | None |
| Consumers | None |
-----
stack@ubuntu:/opt/stack/devstack$

```

Container href の値をコピーします。手順 6 でリスナーを作成するときに、このリンクをコンテナに指定する必要があります。

4. OpenStack で環境変数を設定します。これらの変数を設定すると、OpenStack クライアントコマンドが OpenStack サービスと通信できるようになります。

例:

```

export OS_PASSWORD=hp
export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/
export OS_USERNAME=hp_user
export OS_TENANT_NAME=hp
export OS_IDENTITY_API_VERSION=2.0
export BARBICAN_ENDPOINT=" http://10.106.43.15:9311/"

```

```

stack@ubuntu:/opt/stack/devstack$ export OS_PASSWORD=hp
stack@ubuntu:/opt/stack/devstack$ export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/
stack@ubuntu:/opt/stack/devstack$ export OS_USERNAME=hp_user
stack@ubuntu:/opt/stack/devstack$ export OS_TENANT_NAME=hp
stack@ubuntu:/opt/stack/devstack$ export OS_IDENTITY_API_VERSION=2.0
stack@ubuntu:/opt/stack/devstack$ export BARBICAN_ENDPOINT="http://10.106.43.15:9311/"
stack@ubuntu:/opt/stack/devstack$

```

注  
ほかのコマンドを実行する前に、これらの変数を SSH セッションごとに設定します。OpenStack の環境変数について詳しくは、[OpenStack の環境変数に関するドキュメント](#)を参照してください。

5. 次のコマンドを使用してロードバランサーを作成します。

```
1 neutron lbaas-loadbalancer-create --name <loadbalancer-name> <
  subnet-name> --provider <netscaler>
2 <!--NeedCopy-->
```

例:

```
1 neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --
  provider netscaler
2 <!--NeedCopy-->
```

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --provider netscaler
Created a new loadbalancer:
+-----+-----+
| Field          | Value                                     |
+-----+-----+
| admin_state_up | True                                     |
| description    |                                           |
| id             | 746d730b-3b63-418f-a816-d8dd5472963c   |
| listeners      |                                           |
| name           | hp-lb-test                               |
| operating_status | OFFLINE                                 |
| provider       | netscaler                                |
| provisioning_status | PENDING CREATE                         |
| tenant_id      | 0f30b93cd0cd4482b92d033e1628aa8f       |
| vip_address    | 15.0.0.27                               |
| vip_port_id    | 36636748-15c1-4ec3-9328-496ee74e64fc   |
| vip_subnet_id  | 0bb433c4-4b90-4de0-803f-9df92aa46ac4   |
+-----+-----+
stack@ubuntu:/opt/stack/devstack$
```

ロードバランサーが正常に作成されると、状態が PENDING\_CREATE から ACTIVE に変わります。

id	name	vip_address	provisioning_status	provider
0d5e8e17-41c2-41bb-aab5-2b3f8f5af4c5	hp-lb8	15.0.0.25	ACTIVE	netscaler
1092f752-aa25-4262-aacc-014725fe2921	hp_lb3	15.0.0.19	ACTIVE	netscaler
41dbe490-6d9c-4ce5-8d88-bb55953f5961	hp-lb7	15.0.0.24	ACTIVE	netscaler
746d730b-3b63-418f-a816-d8dd5472963c	hp-lb-test	15.0.0.27	ACTIVE	netscaler
9d65f6a4-5be5-44fd-a4bd-0808084557b0	hp-lb1	15.0.0.18	ACTIVE	netscaler
cf8ee4b7-a9f5-41c5-a76a-cd2520e0a7a3	hp-lb6	15.0.0.23	ACTIVE	netscaler
f7f7dd6e-28eb-40f2-b26c-e541138c6a06	hp-lb4	15.0.0.20	ERROR	netscaler

6. 次のコマンドを使用して、リスナーを作成します。

```
1 neutron lbaas-listener-create --loadbalancer <loadbalancer-name>
  --name <listener-name> --protocol <protocol_type> --protocol-
  port <port_number> --default-tls-container-id<container_url>
2 <!--NeedCopy-->
```

例:

```
1 neutron lbaas-listener-create --name hp-lb-test-list --
  loadbalancer hp-lb-test --protocol TERMINATED_HTTPS --protocol-
  port 443 --default-tls-container-id `http://10.106.43.15:9311/
  v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa`
2 <!--NeedCopy-->
```

注

SSL オフロードサポートなしでリスナーを作成する場合は、コンテナに場所を指定せずに次のコマンドを実行します。

```
neutron lbaas-listener-create --loadbalancer <loadbalancer-
name> --name <listener-name> --protocol <protocol_type> --
protocol-port <port_number>
```

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-listener-create --name hp-lb-test-list --loadbalancer hp-lb-test --protocol TERMINATED_HTTPS --prot
ocol-port 443 --default-tls-container-id http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa
Created a new listener:
-----
| Field | Value |
-----+-----
| admin_state_up | True |
| connection_limit | -1 |
| default_pool_id | |
| default_tls_container_id | http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa |
| description | |
| id | 734a0361-153d-4983-bc2c-55a3ec2ff6fb |
| loadbalancers | [{"id": "746d730b-3b63-418f-a816-d8dd5472963c"}] |
| name | hp-lb-test-list |
| protocol | TERMINATED_HTTPS |
| protocol_port | 443 |
| sni_container_ids | |
| tenant_id | 0f30b93cd0cd4482b92d033e1628aa8f |
-----
stack@ubuntu:/opt/stack/devstack$
```

7. 次のコマンドを使用してプールを作成します。

- 1 neutron lbaas-pool-create --lb-algorithm <algorithm\_type> --
listener <listener-name> --protocol <protocol\_type> --name <
pool-name>
- 2 <!--NeedCopy-->

例:

- 1 neutron lbaas-pool-create --lb-algorithm LEAST\_CONNECTIONS --
listener demolistener --protocol http --name demopool
- 2 <!--NeedCopy-->

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-pool-create --lb-algorithm ROUND_ROBIN --listener hp-lb-test-list --protocol HTTP --name hp-lb-test
-pool
Created a new pool:
-----
| Field | Value |
-----+-----
| admin_state_up | True |
| description | |
| healthmonitor_id | |
| id | 714c44d0-5cf7-4ef8-b84d-f6d3a258c770 |
| lb_algorithm | ROUND_ROBIN |
| listeners | [{"id": "734a0361-153d-4983-bc2c-55a3ec2ff6fb"}] |
| members | |
| name | hp-lb-test-pool |
| protocol | HTTP |
| session_persistence | |
| tenant_id | 0f30b93cd0cd4482b92d033e1628aa8f |
-----
stack@ubuntu:/opt/stack/devstack$
```

8. 次のコマンドを使用してメンバーを作成します。

- 1 neutron lbaas-member-create --subnet <subnet-name> --address <ip-
address of the web server> --protocol-port <port\_number> <pool
-name>
- 2 <!--NeedCopy-->

例:

- 1 neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15
--protocol-port 80 hp-lb-test-pool
- 2 <!--NeedCopy-->

```

stack@ubuntu:/opt/stack/devstack$ neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15 --protocol-port 80 hp-lb-test-pool
Created a new member:
-----+-----+
| Field          | Value                                     |
+-----+-----+
| address        | 15.0.0.15                               |
| admin_state_up | True                                     |
| id             | ced7a563-5ecc-474f-8d2a-cb69923215b0    |
| protocol_port  | 80                                       |
| subnet_id      | 0bb433c4-4b90-4de0-803f-9df92aa46ac4    |
| tenant_id      | 0f30b93cd0cd4482b92d033e1628aa8f      |
| weight         | 1                                       |
+-----+-----+
stack@ubuntu:/opt/stack/devstack$

```

## NetScaler ADM での OpenStack アプリケーションの監視

テナントは、OpenStack の認証情報を使用して NetScaler Application Delivery Management (ADM) にログインし、OpenStack から作成された VIP とプールを任意のブラウザから監視できます。URL は次の形式である必要があります。

[http://<mas\\_ip>/<admin\\_ui>/mas/ent/html/cc\\_tenant\\_main.html](http://<mas_ip>/<admin_ui>/mas/ent/html/cc_tenant_main.html)

ここで `mas-ip-address` は OpenStack に登録されている NetScaler ADM IP アドレスです。

### 注

- OpenStack VIP は Citrix ADM の仮想サーバーに対応しています。
- オープンスタックプールは、Citrix ADM のサービスグループに対応しています。
- OpenStack プールのメンバーは、NetScaler ADM のサービスグループメンバーに対応しています。

## レイヤ 7 コンテンツスイッチングの構成

February 6, 2024

Citrix Application Delivery Management (ADM) は OpenStack と連携して、Citrix ADC インスタンスのレイヤー 7 (L7) スwitching またはコンテンツベースの Switching 機能を設定します。コンテンツスイッチは、指定した種類の要求を指定のサーバーに送信できるという点で単純な負荷分散とは異なります。Citrix ADC インスタンスをプロバイダーとして使用して OpenStack で L7 構成を作成すると、Citrix ADM は Citrix ADC インスタンスを割り当て、L7 構成に対応するコンテンツスイッチング構成とレスポンス構成を展開します。その後、Citrix ADC インスタンスは、要求のアプリケーション層の特性に基づいてユーザー要求を分散し、負荷分散することができます。

OpenStack のレイヤー 7 (L7) 負荷分散機能では、負荷分散とコンテンツスイッチを組み合わせることで特定の種類のコンテンツを最適に配信できます。これにより、コンテンツに適用可能なポリシーのみを実行することにより、ロードバランサーのパフォーマンスが向上します。レイヤー 7 負荷分散では、アプリケーションインフラストラクチャの効率も向上できます。タイプ、URI、データに応じてコンテンツを分離できるため、アプリケーションインフラストラクチャへの物理リソースの割り当てを改善できます。たとえば、<http://example-sports.com/about-us>

を参照するエンドユーザーは、<http://example-sports.com/shopping-cart-football> 会社およびサービスに関するコンテンツをホストするサーバーのプールによって提供され、を参照しているユーザーは、オンライン購入を可能にする別のサーバープールによって提供されます。

L7 スイッチでは、ロードバランサーは、ユーザーからの HTTP 要求を受け付けてアプリケーションサーバーに配信するコンテンツスイッチ仮想サーバーとして実装されます。L7 スイッチまたはコンテンツスイッチでは、Web アプリケーションや Web サービスポータル、Web メールだけでなく、モバイル管理や異なる言語のコンテンツなども含むさまざまなバックエンドサービスにアクセス可能な単一のエン트리ポイントを設定できます。つまり、1つのパブリック IP アドレスで、ユーザーに提供するサービスすべてに対応できるということです。

低レベルの負荷分散とは異なり、レイヤー 7 スイッチではプール内の全サーバーのコンテンツを同じにする必要はありません。L7 スイッチを使用するロードバランサーの構成では、アプリケーションサーバーまたはバックエンドサーバーとプールのコンテンツを違うものにする必要があります。L7 スイッチでは、URI やホスト、HTTP ヘッダーなど、アプリケーションメッセージに含まれるあらゆる要素を基に要求を送信できます。アプリケーションサーバーは、基本的に特定の種類のコンテンツを提供します。たとえば、あるサーバーは画像のみを提供でき、別のサーバーは PHP や ASP などのサーバーサイドスクリプト言語を実行し、別のサーバーは HTML、CSS、JavaScript などの静的コンテンツを提供できます。

## L7 の規則

トラフィックの評価規則では以下の属性が定義されており、規則で定義されている値と比較されます。

- **ホスト名:**HTTP 要求内のホスト名は、ルールの value パラメータと比較されます。（「[www.example-sports.com](http://www.example-sports.com)」など）。
- **path:** HTTP URI のパス部分が、規則のこの値パラメーターと比較されますたとえば、「[www.example-sports.com/shopping-cart/football\\_pump.html](http://www.example-sports.com/shopping-cart/football_pump.html)」
- **file\_type:** HTTP URI の最後の部分が、規則のこの値パラメーターと比較されますたとえば、txt、html、JPG、PNG、xls、その他。
- **header:** キーパラメーターで定義されているヘッダーが、規則のこの値パラメーターと比較されます。
- **cookie:** キーパラメーターで指定されている Cookie が、規則のこの値パラメーターと比較されます。要求ヘッダーフィールドの Cookie 値には、該当する URL に格納されている情報の名前と値のペアが含まれています。一般的な構文は「Cookie: 名前 = 値」です。たとえば、値が「football-」で始まる「stores」という名前のクッキーを検索するルールは、「type = Cookie、compare\_type=startsWith」、「key = storesvalue = football-」のようになります。

## 比較型

トラフィックの評価時には、L7 ポリシーにより以下の式と規則で定義されている値が比較されます。

- **regex:** Perl 型の正規表現マッチング



- starts\_with: 次で始まる文字列
- ends\_with: 次で終わる文字列
- contains: 次を含む文字列
- equal\_to: 次に等しい文字列

注:

ホスト名、パス、ヘッダー、および Cookie 属性はすべての比較タイプをサポートしますが、file\_type 属性は regex と equal\_to のみをサポートします。

## L7 ポリシー

L7 ポリシーは受信 HTTP トラフィックを処理し、このポリシーで定義されているすべての規則が満たされている場合「true」を返します。

すべての L7 ポリシーで、規則はすべて AND 演算子により論理的に結合されます。要求はすべての規則を満たす必要があります、すべての規則が満たされた場合ポリシーは「true」値を返します。ロードバランサーが実行するアクションは、ポリシーから返される値に基づきます。アクションが同じ 2 つ目のポリシーを作成し、規則どうして論理 OR 演算を行うことができます。

たとえば、単語「EXAMPLE-SPORTS」、「SPORTS-FOOTBALL」、または「EXAMPLE-FOOTBALL」を含む受信 HTTP 要求を許可するポリシーを作成し、ロードバランサーには、適切なアクションとして、要求されたコンテンツを提供する E コマース企業である Example-sports のサーバープールにこれらの要求を転送させるとします。同じアクションを実行するものの「example-sports」、「example-sports-football」、「example-football」とのマッチングを行う別のポリシーを作成します。ユーザーがこれら 6 個のキーワードのいずれかを含む HTTP 要求を送信すると、ロードバランサーはその要求を Example-Sports サーバーに転送します。

ポリシーの定義規則に応じて、L7 ポリシーでは以下のアクションのいずれかを行うことができます。

- プールへのリダイレクト - L7 ポリシーに関連付けられた規則で指定されているアプリケーションサーバープールに要求を転送します。これにより、ドメイン名に応じて要求を特定のロードバランサープールに送信するアプリケーション規則を作成できます。たとえば、example-football.com に対する要求を pool\_1 に、example-sports-online\_purchase.com に対する要求を pool\_2 に送信するルールを作成できます。
- URL へのリダイレクト - クライアントを、Location 応答ヘッダーに新しい場所が設定されたリダイレクト HTTP 応答に送信します。Web ブラウザーのアドレスバーはこの新しい場所で更新され、新しい要求が発行されます。このアクションの使用例は多岐にわたります。たとえば、Web サイトのアドレスが変更された場合、ドロップを行うことなく要求を新しいアドレスにリダイレクトすることができます。また、Web サイトのメンテナンス中にユーザーを読み取り専用のサイトにリダイレクトすることも可能です。
- 拒否 - 要求を拒否し、それ以上のアクションを行いません。たとえば、401 無許可応答を返して、制限された Web ページのユーザーへのアクセスを拒否できます。

コンテンツスイッチの構成には、コンテンツスイッチ仮想サーバー、負荷分散仮想サーバーとサービスから成る負荷分散セットアップ、およびコンテンツスイッチポリシーが含まれます。コンテンツスイッチ仮想サーバーとコンテンツスイッチポリシーの作成後、各ポリシーをコンテンツスイッチ仮想サーバーにバインドします。ポリシーをコンテンツスイッチ仮想サーバーにバインドするときには、ターゲットとなる負荷分散仮想サーバーを指定します。要求がコンテンツスイッチ仮想サーバーに到達すると、仮想サーバーはその要求に対して関連するコンテンツスイッチポリシーを適用します。ポリシーの優先順位により、コンテンツスイッチ仮想サーバーにバインドされたポリシーを評価する順序を定義します。

リスナー ID が設定されているプールはすべて、トラフィックの迂回先となるデフォルト仮想サーバープールに割り当てることができます。プールとリスナーのバインドはゆるく、プールは L7 ポリシーの実装でのみリスナーと関連付けられます。プールは、リスナーに関連付けることなくロードバランサーの下に直接作成することもできます。この場合、作成されたプールは「pending\_create」状態となります。L7 ポリシーとリスナーのバインドは密接であるため、プールを「active」状態にしてトラフィック要求の受信を開始するには、プール ID を含む L7 ポリシーを作成して実装する必要があります。

1 つのプールを複数の L7 ポリシーで提供できますが、1 つ以上のポリシーが関連付けられている場合プールは「active」のままとなります。最後のポリシーが削除されるとプールは「pending\_create」状態に戻り、別のポリシーを作成して関連付けるまでその状態のままとなります。プール自体が削除されると、このプールが受信するはずであった HTTP 要求はすべてデフォルトプールにリダイレクトされます。

### OpenStack L7 ポリシーと Citrix ADC エンティティ間のマッピング

OpenStack	Citrix ADC エンティティ	説明
REDIRECT_TO_POOL アクションが設定された L7 ポリシー	コンテンツスイッチポリシー > コンテンツスイッチアクション	Citrix ADM は、コンテンツスイッチ仮想サーバーにバインドされ、コンテンツの取得とユーザーへの表示のためのアプリケーションサーバーのターゲットプールを指定するコンテンツ切り替えアクションに関連付けられたコンテンツスイッチングポリシーを作成します。
REDIRECT_TO_URL アクションが設定された L7 ポリシー	レスポンスポリシー > レスポンスアクション	Citrix ADM は、コンテンツスイッチ仮想サーバーにバインドされ、ユーザーに表示するターゲット URL を指定するレスポンスアクションに関連付けられたレスポンスポリシーを作成します。

REJECT アクションが設定された L7 ポリシー	レスポンスポリシー > 要求のドロップ	Citrix ADM は、コンテンツスイッチ仮想サーバーにバインドされ、要求をドロップするレスポンスアクションに関連付けられたレスポンスポリシーを作成します。
----------------------------	---------------------	---

「true」と評価された L7 ポリシーのアクションが「create\_pending」状態のプールにトラフィックをリダイレクトする場合、Citrix ADM は指定されたプールを負荷分散仮想サーバーとともに実装します。Citrix ADM は、L7 ポリシーからコンテンツスイッチングポリシーを作成し、対応するコンテンツスイッチアクションを使用して、そのプールに関連付けられた負荷分散仮想サーバーに要求をリダイレクトします。2 つ目の L7 ポリシーが同じプールにリダイレクトされると、Citrix ADM はコンテンツスイッチングポリシーとコンテンツスイッチアクションを作成して、プールに関連付けられている既存の負荷分散仮想サーバーにトラフィックをリダイレクトします。

#### ポリシーの順位付け

OpenStack での L7 ポリシーの評価は、ポリシーの優先度に従って行われます。デフォルトでは、OpenStack のポリシーは作成された順番に優先度が付けられます。最初に作成されたポリシーが「1」番となり、以降に作成されたポリシーには連続した番号が付けられます。ただし、ポリシーの優先順位を変更し、異なる優先度を割り当てることができます。ポリシーは常に優先度の順番に評価されます。特定の要求に一致する最初のポリシーは、常に最初に実行される。

ポリシーを作成する場合、以下の点に注意してください。

- 新しいポリシーに既存のポリシーと同じ優先度を割り当てた場合、その優先度は新しいポリシーに設定されます。既存のポリシーの優先度は下がります。必要に応じて、ポリシーの評価順序を維持するために別のポリシーの優先度が下げられることもあります。
- 優先順位を指定せずに新しいポリシーを作成した場合、新しいポリシーはポリシーリストの末尾に追加されます。
- 新しいポリシーを作成し、リストに既に存在するポリシーの数よりも大きい順位を付けた場合、新しいポリシーはリストの末尾に追加されます。つまり、新しいポリシーには、次に利用可能な優先度が常に設定されます。たとえば、優先順位が 1、2、3 のポリシー A、B、C がある場合にポリシーを作成し優先順位として 8 を割り当てると、新しいポリシーの優先順位は 4 になります。
- リストにポリシーを追加するかリストからポリシーを削除すると、ポリシーの優先順位の値は 1 から順に連続して付け直されます。たとえば、優先順位の値が 1、2、3、4 のポリシー A、B、C、D がある場合にリストからポリシー B を削除すると、ポリシー C の優先順位が 2 となり、ポリシー D の優先順位は 3 となります。

NetScaler ADM では、常に優先度 1 のデフォルトポリシーが `csvserver` に関連付けられています。このデフォルトポリシーは、特定の時点で `lbvserver` で処理する TCP 接続の数を指定します。したがって、対応するレスポ

リダイレクトポリシーとコンテンツスイッチングポリシーが NetScaler ADC で作成されると、対応する L7 ポリシーの優先度よりも高い優先度が常に割り当てられます。たとえば、優先順位が 1 の L7 ポリシーを評価する場合、優先順位が 2 のコンテンツスイッチポリシーが作成されます。同様に、優先順位が 2 の L7 ポリシーを評価する場合、優先順位が 3 のレスポンスポリシーが作成されます。

OpenStack では、最初に「拒否」または「redirect\_to\_url」ポリシーが評価され、次に「redirect\_to\_pool ポリシー」が評価されます。NetScaler ADC インスタンスでは、レスポンスポリシーは常に最初に評価され、リクエストを削除するか、リダイレクトされた Web アドレスをユーザーに提示します。コンテンツスイッチングポリシーは最後に評価されます。通常、コンテンツスイッチポリシーとレスポンスポリシーが相互に排他的であれば、この評価順により競合が発生することはありません。つまり、2 つの L7 ポリシーが同じ式を持つことはできません。派生式は、このような競合を回避するために、応答側およびコンテンツスイッチングポリシーに追加されます。たとえば、「sports-football.com」に対する要求をすべて拒否する式と、「example-sports-football.com」に対する要求を許可する別の式を作成してください。要求を拒否するすべてのレスポンスポリシーを評価リストの先頭に配置し、その後に Web リダイレクト用のレスポンスポリシー、コンテンツスイッチポリシーの順となるように L7 ポリシーを作成してください。

NetScaler ADM では、常に優先度 1 のデフォルトポリシーが `csvserver` に関連付けられています。このデフォルトポリシーは、特定の時点で `lbvserver` で処理する TCP 接続の数を指定します。したがって、対応するレスポンスポリシーとコンテンツスイッチングポリシーが NetScaler ADC で作成されると、対応する L7 ポリシーの優先度よりも高い優先度が常に割り当てられます。たとえば、優先順位が 1 の L7 ポリシーを評価する場合、優先順位が 2 のコンテンツスイッチポリシーが作成されます。同様に、優先順位が 2 の L7 ポリシーを評価する場合、優先順位が 3 のレスポンスポリシーが作成されます。

OpenStack では、最初に「拒否」または「redirect\_to\_url」ポリシーが評価され、次に「redirect\_to\_pool ポリシー」が評価されます。NetScaler ADC では、レスポンスポリシーは常に最初に評価され、リクエストを削除するか、リダイレクトされた Web アドレスをユーザーに提示します。コンテンツスイッチングポリシーは最後に評価されます。通常、コンテンツスイッチポリシーとレスポンスポリシーが相互に排他的であれば、この評価順により競合が発生することはありません。つまり、類似する表現を持つ L7 ポリシーが 2 つありません。このような競合を回避するために、応答側とコンテンツスイッチングポリシーに、同様の派生式が追加されます。たとえば、「sports-football.com」に対する要求をすべて拒否する式と、「example-sports-football.com」に対する要求を許可する別の式を作成してください。要求を拒否するすべてのレスポンスポリシーを評価リストの先頭に配置し、その後に Web リダイレクト用のレスポンスポリシー、コンテンツスイッチポリシーの順となるように L7 ポリシーを作成してください。

### 構成タスク

Neutron LBaaS コマンドを使用して、L7 ポリシーとアクションを実装します。

OpenStack で環境変数を設定し、ロードバランサーを作成します (例: LB1)。ロードバランサーを正常に作成できたら、リスナーとプール (例: L1、P1、P2) を作成しプールにメンバーとモニターを追加します。たとえば、P1 を L1 のデフォルトプールに設定し、P2 は LB1 に関連付け、アプリケーションサーバーを管理するプールにします。

コマンドラインを使用して LBaaS V2 を設定する方法の詳細については、「[コマンドラインを使用した LBaaS V2 の設定](#)」を参照してください。

以下のコマンドにより、ポリシーを定義して特定のアクションを定義します。

要求をドロップする **L7** ポリシーの作成

```
1 neutron lbaas-l7policy-create --name <L7 policy name> --listener <
  listener name> --action<action-name>
```

例:

```
neutron lbaas-l7policy-create -name policy11 -action REJECT -listener L1
```

上記のコマンドでは、要求を拒否するレスポンスポリシー `policy11` を作成して、コンテンツスイッチサーバーにバインドします。このポリシーには規則が作成されていないため、ポリシーは「false」と評価され要求が拒否されます。

特定の **URL** に要求をリダイレクトする **L7** ポリシーの作成

```
1 neutron lbaas-l7policy-create --name <L7 policy name> --listener <
  listener name> --action <action-name> --redirect-url <redirect-url>
```

例:

```
neutron lbaas-l7policy-create -name policy12 -action REDIRECT_TO_URL -listener admin-list1 -
redirect-url http://example-sports/about-us.html
```

上記のコマンドでは、URL へ要求をリダイレクトするレスポンスアクションを作成し、このアクションが設定されたレスポンスポリシーを作成してコンテンツスイッチ仮想サーバーにバインドします。

```
1 neutron lbaas-l7rule-create --type HOST_NAME --compare-type CONTAINS --
  value <value-string> <L7 policy name>
2
3 neutron lbaas-l7rule-create --type PATH --compare-type CONTAINS --value
  <value-string> <L7 policy name>
```

上記 2 つの規則は AND 演算子により結合され、レスポンスポリシーの式が導出されます。

プールに要求をリダイレクトする **L7** ポリシーの作成

```
1 neutron lbaas-l7policy-create --name <L7 policy name> --listener <
  listener name> --action <action-name> --redirect-pool <redirect-pool
  >
```

例:

```
neutron lbaas-l7policy-create -name policy13 -action REDIRECT_TO_POOL -listener admin-list1 -
redirect-pool admin-pool2
```

この L7 ポリシーが最初のポリシーである場合、上記のコマンドでは LB1 とともに P2 が実装され、コンテンツスイッチリダイレクトアクションが作成されて要求が LB1 へリダイレクトされます。P2 が既に存在する場合、このコマンドではコンテンツスイッチリダイレクトアクションが作成され、要求が LB1 にリダイレクトされます。

## OpenStack での NetScaler ADC VPX インスタンスの手動 Provisioning

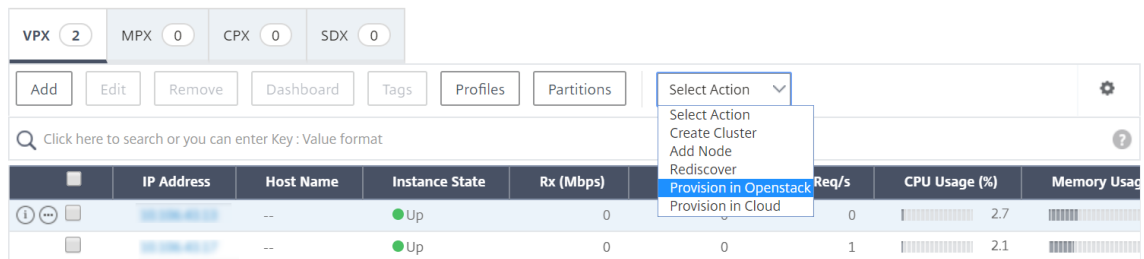
February 6, 2024

一部のエンタープライズネットワークでは、セキュリティ上の理由から、NetScaler ADC VPX インスタンスが Citrix License Server に接続してライセンスを自動的にダウンロードできません。このようなシナリオでは、NetScaler ADC VPX インスタンスを OpenStack プラットフォームに手動でデプロイする必要があります。Citrix から受け取ったライセンスアクセスコードを使用して、適切な NetScaler ADC VPX ライセンスをダウンロードしてローカルシステムに保存します。

**OpenStack で NetScaler ADC VPX インスタンスを手動でプロビジョニングするには：**

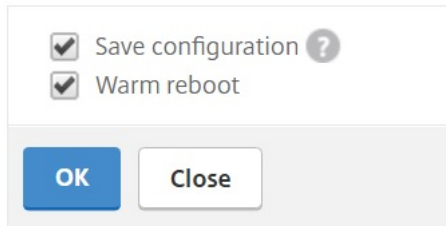
1. Citrix ADC ドライバソフトウェアをインストールし、OpenStack に Application Delivery Management (ADM) を登録する
  - a) Citrix ADM で、[オーケストレーション] > [クラウドオーケストレーション] > [OpenStack\*\*] に移動します。
  - b) 「**OpenStack** の設定を設定」をクリックします。「**OpenStack** 設定の構成」ページでは、Citrix ADM で OpenStack を設定するためのパラメータを設定できます。ここには、[デフォルト]と[カスタマイズ]の2つのオプションがあります。
  - c) OpenStack サービスがデフォルトポートで実行されている場合は、[Default] をクリックします。
2. [オーケストレーション] > [\*\*クラウドオーケストレーション\*\*] > [**\*\*OpenStack**] に移動し、[デプロイ設定] をクリックします。\*\*
  - a) 管理ネットワーク-自動プロビジョニングされた Citrix ADC VPX が接続されている OpenStack 上の管理ネットワークを選択します。
  - b) プロファイル名-ドロップダウンリストからプロファイルを選択します。NetScaler ADM は、このプロファイルに含まれているパスワードを使用して、新しい自動プロビジョニングされた NetScaler ADC VPX インスタンスを構成します。
  - c) Citrix ADC VPX イメージ・イン・グランズ-Citrix ADC VPX インスタンスの作成に使用される OpenStack Glance で利用可能な Citrix ADC VPX イメージを選択します。ボックスの一覧には、OpenStack Glance に存在するイメージのみが表示されます。
3. Citrix ADM で、[オーケストレーション] > [クラウドオーケストレーション] > [OpenStack\*\*] > [**\*\*サービスパッケージ**] に移動し、[追加] をクリックします。
4. 「サービスパッケージ」ページで、次のパラメータを指定します。
  - a) 名前: サービスパッケージの名前。たとえば、「SVC-PKG-GOLD」と入力します。
  - b) **Citrix ADC** インスタンス割り当て-サービスパッケージで定義されているインスタンス割り当てのタイプとして、[専用]または[パーティション]を選択します。

- c) **Citrix ADC** インスタンス **Provisioning**-構成中に Citrix ADC インスタンスを作成するには、「オンデマンドでインスタンスを作成」を選択します。
  - d) 自動プロビジョニングプラットフォーム - **OpenStack Compute** を選択します。デフォルトでは、Citrix ADC VPX がインスタンスタイプとして選択されます。
  - e) **OpenStack** テナント/ブレースメントポリシーの割り当て-セクションの OpenStack テナントで [追加] をクリックし、テナントを選択します。
  - f) [**Continue**]、[**Done**] の順にクリックします。
5. [システム]>[システム管理]>[システム設定の変更]に移動し、ドロップダウンリストから [**http**] を選択します。
  6. [ネットワーク]>[インスタンス]>[\*\*Citrix ADC VPX\*\*]に移動します。
  7. **NetScaler ADC VPX** ページで、[管理] ドロップダウンリストをクリックし、[デバイスのプロビジョニング] を選択します。



- a) [**Device Provisioning**] ページで、デバイスの名前を入力し、前の手順で作成したサービスパッケージを選択します。
  - b) [**OK**] をクリックします。
8. [オーケストレーション]>[\*\*クラウドオーケストレーション\*\*]>[OpenStack\*\*]>[リクエスト] タブに移動します。\*\* リクエストを選択し、「タスク」をクリックしてタスクを表示します。タスクのステータスが [完了] に変わると、NetScaler ADC VPX が NetScaler ADM でプロビジョニングされます。
  9. [ネットワーク]>[インスタンス]>[**Citrix ADC VPX**] に移動して、Citrix ADC VPX インスタンスが Citrix ADC VPX ページに表示されていることを確認します。
  10. NetScaler ADC VPX インスタンスをクリックします。NetScaler ADC VPX インスタンスがブラウザウィンドウで開いたら、インスタンスにログオンします。[構成]>[システム]>[ライセンス] に移動し、新しいライセンスを手動で追加します。新しいライセンスを追加する方法については、「[NetScaler ADC ライセンスの概要](#)」を参照してください。
  11. NetScaler ADC VPX インスタンスを再起動します。

## Reboot

A dialog box titled "Reboot" with two checked checkboxes: "Save configuration ?" and "Warm reboot". Below the checkboxes are two buttons: "OK" (blue) and "Close" (white with grey border).

12. 数分後、OpenStack にログオンし、[システム] > [インスタンス] で、NetScaler ADC VPX インスタンスが OpenStack にデプロイされていることがわかります。
13. LBaaS V2 API を実装するには、Neutron LBaaS コマンドを使用します。任意の Neutron クライアントに接続し、設定タスクを実行します。設定コマンドの実行方法の詳細については、「[コマンドラインを使用した LBaaS V2 の設定](#)」を参照してください。

## StyleBook を使用した OpenStack での NetScaler ADC VPX インスタンスのプロビジョニング

February 6, 2024

OpenStack オーケストレーションワークフローでは、NetScaler Application Delivery Management (ADM) が `os-cs-lb-mon` StyleBook を使用して、OpenStack テナントに割り当てられた NetScaler ADC インスタンスに LBaaS 構成を展開するようになりました。OpenStack ユーザーによって作成されたロードバランサーごとに、設定パックが作成されます。

OpenStack ワークフローで StyleBooks を設定することには、次のような利点があります。

- すべての設定オブジェクトを表示することで、視覚化が改善されました。
- ロールバックによる信頼性。
- さまざまな NetScaler ADC インスタンスタイプ (NetScaler ADC HA、パーティション、VPX、CPX、MPX など) のサポート。
- 独自の StyleBooks を使用して OpenStack テナントの設定をデプロイすることによるカスタマイズ。

NetScaler ADM 管理者として、[アプリケーション] > [構成] に移動して、NetScaler ADC インスタンスに展開されている構成パックを表示します。

次のタスクを実行できます。

- スクロールして、ロードバランサーにデプロイされた `os-cs-lb-mon` 構成パックを表示します。



- `os-cs-lb-mon` StyleBook パネルで [ **View Definition** ] をクリックして、インスタンスにデプロイされている設定を確認します。
- [ オブジェクトの表示 ] をクリックして、インスタンスにデプロイされた NetScaler ADC オブジェクトまたはエンティティの一覧を表示します。

### StyleBook を使用してインスタンスを **Provisioning** する前の注意点

NetScaler ADM 12.1 ビルド 49.23 以降、OpenStack オーケストレーションワークフローのアーキテクチャが更新されました。ワークフローでは、NetScaler ADM StyleBook を使用して NetScaler ADC インスタンスを構成するようになりました。バージョン 12.0 またはバージョン 12.1 ビルド 48.18 のいずれかから NetScaler ADM 12.1 ビルド 49.23 にアップグレードする場合は、次の移行スクリプトを実行する必要があります。

```
1 /mps/scripts/migration_scripts/migrate_configurations.py
2 <!--NeedCopy-->
```

- 移行スクリプトを実行すると、既存の OpenStack 設定に対応する `os-cs-lb-mon` StyleBook の設定パックが作成されます。
- 以前のビルドから OpenStack 設定をデプロイした場合は、この移行スクリプトの実行が必須です。
- バージョン 12.1 ビルド 49.23 から移行スクリプトを実行した後にはのみ、`os-cs-lb-mon` StyleBook を使用してインスタンスに新しい設定をデプロイできます。
- OpenStack から試行されたすべての設定は、移行スクリプトが実行されるまで失敗します。

#### 注

- 移行スクリプトを実行すると、Citrix ADM の以前のビルドにダウングレードすることはできません。
- OpenStack LBaaS V2 用の NetScaler ADC ドライバを最新バージョンにアップグレードしていることを確認します。最新の Citrix ADM 13.0 ビルドに付属している Citrix ADC バンドルファイルを使用してください。

LBaaS V2 API を実装するには、Neutron LBaaS コマンドを使用します。任意の Neutron クライアントに接続し、設定タスクを実行します。設定コマンドの実行方法の詳細については、「[コマンドラインを使用した LBaaS V2 の設定](#)」を参照してください。

### VPX チェックインとチェックアウトのライセンスおよび **OpenStack** 環境のプールライセンスのサポート

February 6, 2024

OpenStack オーケストレーションワークフローでは、**OpenStack** コンピュートでサービスパッケージを選択すると、NetScaler Application Delivery Management (ADM) がオンデマンドで NetScaler ADC VPX インスタンスを作成します。これで、Citrix ADM のオーケストレーション機能のサービスパッケージページが拡張され、オンデマンドで作成される Citrix ADC VPX インスタンスにインストールする必要があるライセンスが提供されるようになりました。提供されるライセンスは、VPX チェックインおよびチェックアウトライセンスまたはプールライセンスのいずれかです。

この機能を使用するには、まず Citrix ADM にライセンスをアップロードしてから、OpenStack Compute を使用するサービスパッケージを作成する必要があります。

- チェックイン、チェックアウトライセンスの場合は、利用可能なさまざまなライセンスからインストールするライセンスを選択できます。

← Service Package

**Service Level Agreement**

Name **sp-nova**

**Auto Provision Settings**

**Resources**

Maximum Number of Instances to Auto Provision\*

10

Flavor\*

m1.medium, 2 vcpus, 4096 RAM

Install License

VPX Licenses  Pooled License

License Type\*

Enterprise  Platinum  Standard

Model\*

VPX8000\_Platinum, 1 available

- プールライセンスの場合は、帯域幅とインストールするライセンスエディションのタイプの両方を選択できます。

## ← Service Package

**Service Level Agreement**

Name **sp-nova**

---

**Auto Provision Settings**

**Resources**

Maximum Number of Instances to Auto Provision\*

Flavor\*

Install License

VPX Licenses     Pooled License

License Type\*

Enterprise     Platinum     Standard

Available Bandwidth

Bandwidth\*                      Bandwidth Unit\*

NetScaler ADM をプロバイダーとして最初のロードバランサーを展開すると、NetScaler ADM によって NetScaler ADC VPX インスタンスが作成され、サービスパッケージで指定されたライセンスが新しく作成されたインスタンスにインストールされます。

また、既存の負荷分散インスタンスを削除すると、そのインスタンスは不要になります。インスタンスは廃止され、ライセンスは Citrix ADM に返却されます。これにより、Citrix ADM で利用可能なライセンスを最適に使用できます。

### 注

: Citrix ADM を高可用性モードで展開する場合は、ライセンスを現在のアクティブまたはプライマリの Citrix ADM、MAS-HA-1 にアップロードすることを検討してください。最初のリクエストを展開し、Citrix ADM が

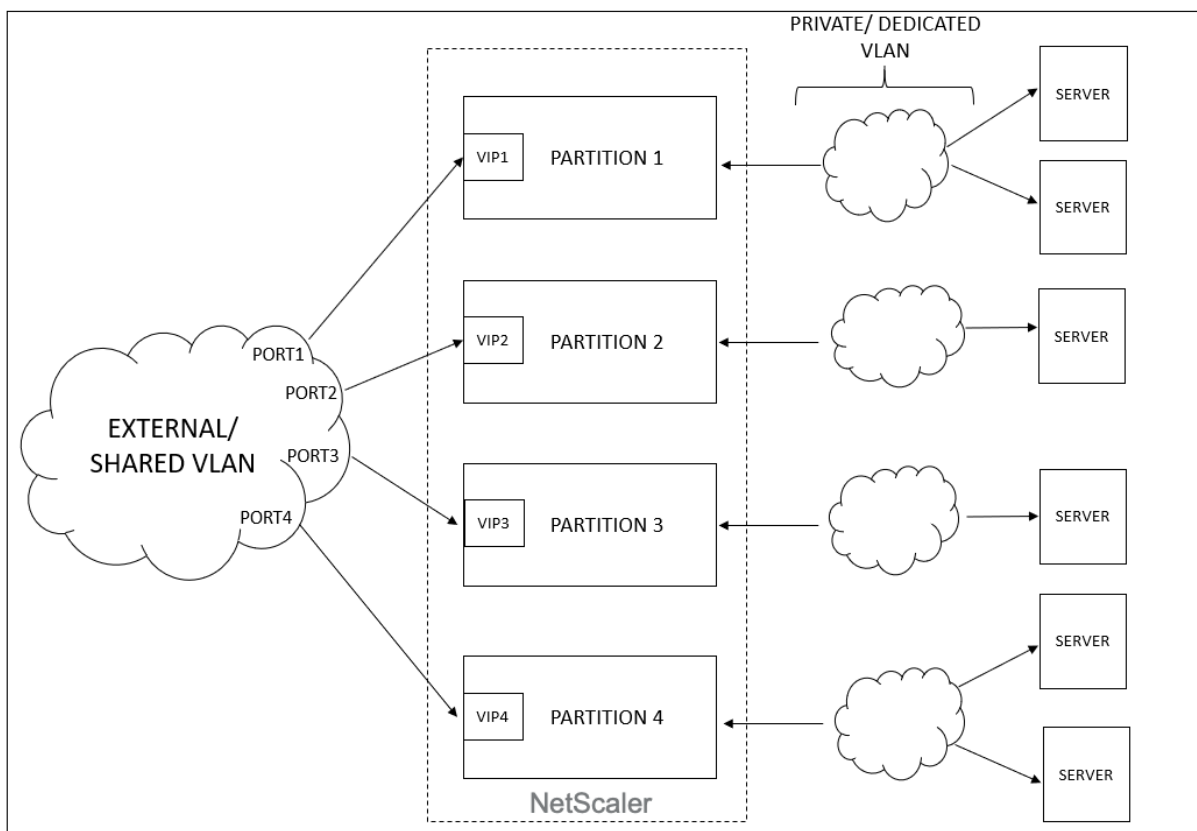
Citrix ADC VPX インスタンスを作成すると、インスタンスは MAS-HA-1 から必要なライセンスをチェックアウトします。後で、ライセンスを持たないセカンダリ Citrix ADM MAS-HA-2 が現在アクティブになっていると仮定します。現在、ADC VPX インスタンスは MAS-HA-2 からライセンスをチェックアウトできないため、新しいユーザー用にインスタンスを作成できません。

このような場合は、MAS-HA-1 が稼働していて、現在のプライマリノードになっていることを確認してください。つまり、Citrix ADM を MAS-HA-2 から MAS-HA-1 に手でフェールオーバーします。その後、OpenStack から設定を再試行する必要があり、インスタンスは適切なライセンスで再作成されます。NetScaler ADM 高可用性展開でのライセンスサポートについて詳しくは、「[高可用性](#)」を参照してください。

## 管理パーティションの共有 VLAN サポート

February 6, 2024

プライベートネットワークから接続するテナントの場合、Citrix Application Delivery Management (ADM) は分離ポリシーをサポートしているため、各テナントには独自の専用パーティション、専用 VLAN、および専用サーバーがあります。パブリックネットワークから接続するテナントの場合は、専用の VLAN を使用すると、大量の IP アドレスが必要になります。共有 VLAN では、各パーティション上に 1 つの仮想 IP アドレスを作成することで、1 つの IP サブネットを作成して、この問題を回避します。

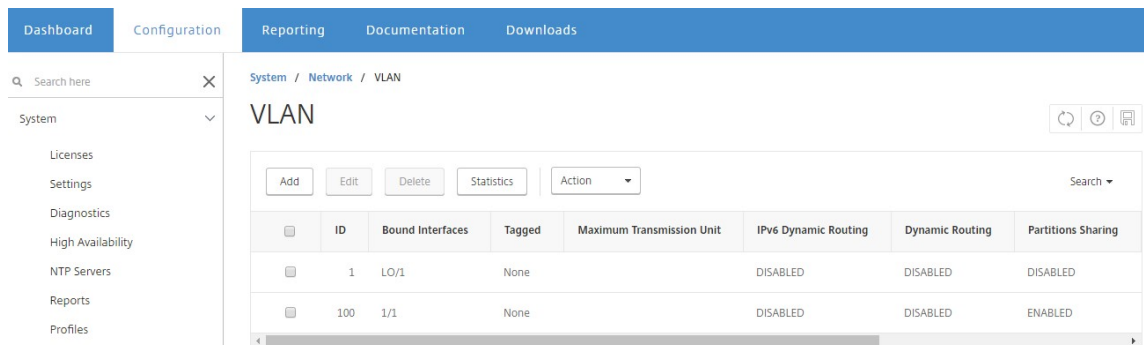


テナントがVIP またはリスナーを構成すると、そのテナントの NetScaler ADC デバイスに管理パーティションが作成されます。すべてのロードバランサー構成は、作成された admin パーティションにプッシュされます。テナントが共有ネットワークまたは外部ネットワークを使用してロードバランサーを作成している場合は、そのネットワークの VLAN が追加され、共有機能が有効化されます。別のテナントが同じ共有ネットワークを使用してロードバランサーを作成する場合、VLAN は Citrix ADC に再度追加されませんが、VLAN は 2 番目のパーティションにもバインドされます。したがって、同じ共有ネットワークを使用しているテナントには、同じ VLAN に結合されているパーティションが与えられます。

Citrix ADM は仮想デスティネーション MAC アドレスをサポートしています。テナントが VLAN を共有する場合、Citrix ADM は Citrix ADC デバイスのパーティションに異なる MAC アドレスを割り当てます。これにより、1 つの VLAN を、パーティション間、またはすべてのテナントおよびすべてのトラフィックドメイン間で共有できます。

### Citrix ADC インスタンスからの共有 VLAN の設定

1. Citrix ADC インスタンスで、[ 構成 ] \*\*> [ \*\* システム ] > [ ネットワーク ] > \*\*[VLAN] に移動し、**VLAN** プロファイルを選択し、[ \*\* 編集 ] をクリックしてパーティション共有パラメータを設定します。
2. 「**VLAN** の設定」 ページで、「パーティション共有」 チェックボックスを選択します。
3. [OK] をクリックします。

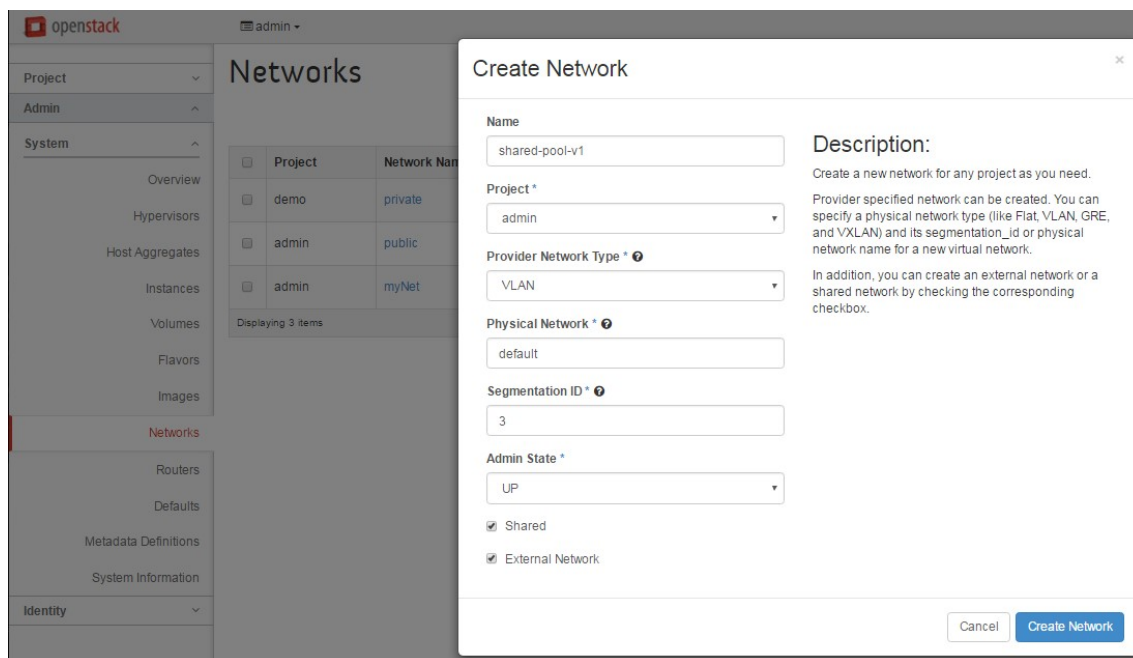


### OpenStack Orchestration から共有 VLAN を構成する

1. OpenStack で、[ 管理 ] > [ システム ] > [ ネットワーク ] に移動し、[ ネットワークの作成 ] をクリックします。
2. [Create Network] で、次のパラメーターを設定します。
  - a) Name - ネットワークの名前を入力します。
  - b) Project - ボックスの一覧からプロジェクトを選択します。
  - c) プロバイダーネットワークタイプ-ドロップダウンリストから **VLAN** を選択します。これにより、仮想ネットワークが VLAN として確立されます。
  - d) Physical Network - ここでデフォルトの物理ネットワークを選択します。このボックスは編集可能です。

- e) Admin State - デフォルトでは、ネットワークの管理状態は UP です。
- f) VLAN が共有されており、外部ネットワークを使用していることを定義するには、**[Shared]** と **[External]** を選択します。

3. **[Create Network]** をクリックします。



## 試用版ライセンスのワークフロー

February 6, 2024

OpenStack オーケストレーションを使用した NetScaler ADC VPX インスタンスの自動プロビジョニングでは、NetScaler Application Delivery Management (ADM) は OpenStack コンピュートを使用して NetScaler ADC VPX インスタンスを起動します。新しくプロビジョニングされた NetScaler ADC VPX インスタンスは、セットアップ中に Citrix ライセンスポータルに接続し、ライセンスアクセスコードを使用してライセンスファイルを自動的にダウンロードおよびインストールします。

### 試用版ライセンス

テクニカルサポートスタッフは、Citrix ADM および Citrix ADC VPX デバイスを現場にインストールするときに試用版ライセンスを使用します。Citrix ADC VPX の試用版または評価版ライセンスは 90 日間有効です。複数の Citrix ADC を評価する必要がある場合、または 90 日後にテストを延長する必要がある場合は、新しい評価ライセンスをリクエストする必要があります。Citrix ADM は、試用版ライセンスファイルを自動的にインストールする代わりに、代

替ソリューションを提供します。ライセンスファイルを手動でダウンロードして Citrix ADC VPX にインストールすると、インスタンスのインストールを完了できます。

Citrix ADC VPX がインターネットに接続できない場合は、Citrix ADM を Citrix ライセンスポータルのプロキシサーバーとして動作するように構成し、ライセンスファイルをインストールします。

トライアルライセンスを持つ Citrix ADC VPX インスタンスは、HTTP でのみ Citrix ADM と通信できます。Citrix ADM で HTTP 通信を構成するには、[システム] > [システム管理] に移動し、[システム設定の変更] をクリックします。ドロップダウンリストから「**http**」を選択して通信方法を設定し、「**OK**」をクリックします。

## ← Modify System Settings

Communication with instance(s)\*

http ▼

- Secure Access Only
- Enable Session Timeout
- Allow Basic Authentication
- Enable nsrecover Login
- Enable Certificate Download
- Enable Shell access for non-nsroot User

**OK** Close

## OpenStack Heat サービスとの統合

February 6, 2024

OpenStack Neutron LBaaS を利用すると、負荷分散、SSL オフロード、コンテンツスイッチなどの主要な負荷分散サービスをアプリケーションで使用できます。LBaaS は REST API を通じて管理され、API により、テナントは、LBaaS オブジェクトを作成、更新、削除するための REST 呼び出しを行うことができます。LBaaS では負荷分散サービスが提供されるため、オーケストレーションプロセス中により高度な NetScaler ADC 機能を使用することはできません。Citrix ADC Heat プラグインはこの制限を克服します。

## Heat オーケストレーションサービス

OpenStack Heat オーケストレーションサービスでは、テンプレートに基づいて複雑なクラウドアプリケーションを展開することができます。クラウドアプリケーションのインフラストラクチャは、バージョン管理ツールで管理可能な Heat オーケストレーションテンプレート (HOT: Heat orchestration template) により、人間が読み取り/書き込み可能なテキストファイルで指定します。このテンプレートは、YAML という構造化言語を使用して記述します。HOT を使用することでほとんどの種類の OpenStack リソースを作成でき、このテンプレート内で定義したリソース間の関係を指定できます。Citrix ADC Heat プラグインを使用すると、任意の Citrix ADC インスタンスで高度なアプリケーションデリバリーコントローラー (ADC) 機能を設定できます。

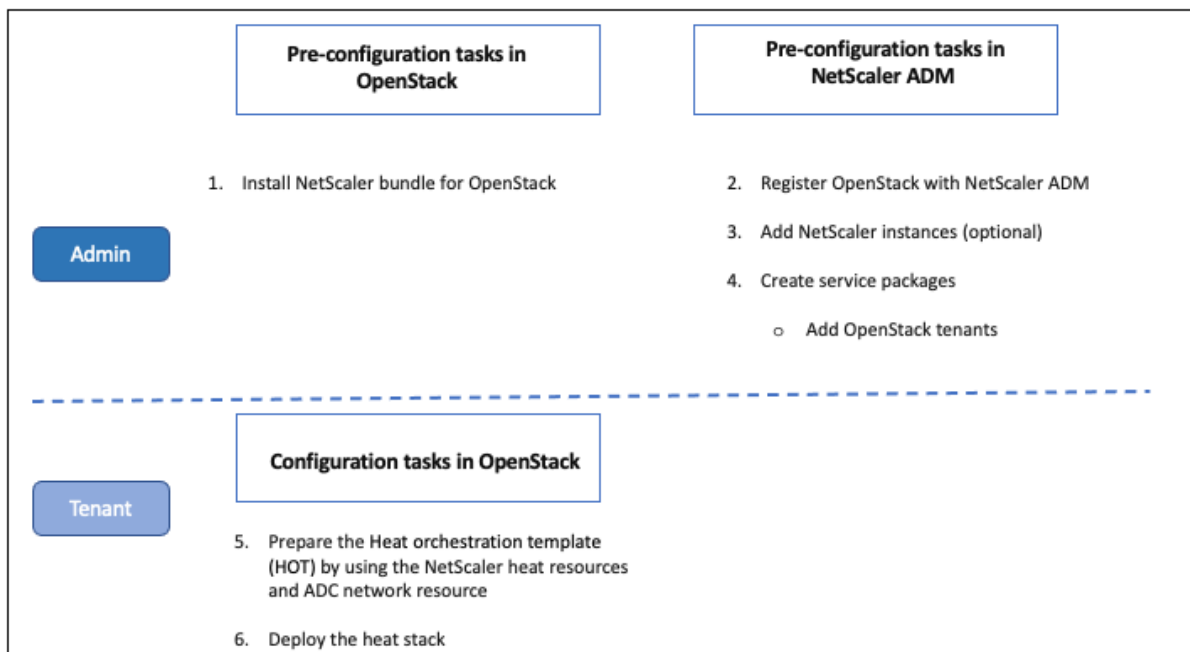
## Citrix ADC StyleBook

Citrix Application Delivery Management (ADM) StyleBook を使用して、Citrix ADC 機能を作成および構成できます。Heat テンプレートと同様に、StyleBook も YAML で記述します。機能ごとに個別の StyleBook を作成でき、1 つの StyleBook を使用して複数の Citrix ADC インスタンスに構成を展開できます。

Citrix ADC と OpenStack の統合中、Citrix ADM はすべての Citrix ADM StyleBook を Heat サービスのリソースとして公開します。これには、Citrix ADM に同梱されている StyleBook と、ユーザーが後で作成した StyleBook の両方が含まれます。Heat テンプレートを使用すると、これらの StyleBooks リソースを使用して Citrix ADC の高度な機能を構成できます。

## Heat を使用して Citrix ADC インスタンスを設定するためのワークフロー

以下のフローチャートに、Heat スタックを展開するワークフローを示します。





クラウド管理者として次のタスクを実行します。

**OpenStack** で **Heat** サービスを設定するには:

1. OpenStack 用 Citrix ADC バンドルのダウンロード

Citrix ADC バンドルを OpenStack にインストールします。Citrix ADM で、「ダウンロード」に移動して Citrix ADC ドライバーバンドルをダウンロードし、バンドルを解凍して、バンドル内の Heat フォルダーの内容を OpenStack の Heat エンジンリソースディレクトリにコピーします。ディレクトリパスは次のとおりです。

```
/opt/stack/heat/heat/engine/resources/netscaler_resources
```

2. heat.conf ファイルに「netscaler\_plugin」セクションを作成し、そのセクションの以下のパラメーターを更新します。

```
[netscaler_plugin]
```

- a) 通信が HTTP の場合、パラメータは次のように更新されます。

```
NMAS_BASE_URI=<http://10.146.103.45:80>
```

```
NMAS_USERNAME=
```

```
NMAS_PASSWORD=
```

- b) 通信が https の場合、パラメータは次のように更新されます。

```
NMAS_BASE_URIhttps://common_name_used_in_certificate
```

```
NMAS_USERNAME=<openstack_driver_username
```

```
NMAS_PASSWORD=<openstack_driver_password>
```

```
SSL_CERT_VERIFY=<True_or_False>
```

```
CERT_FILE_PATH=<path_of_the_certificate_file>
```

ユーザーが `ssl_cert_verify` を「False」に設定すると、Citrix ADM はリクエスト呼び出しで `verify=False` を送信し、SSL 証明書の検証を無効にします。`ssl_cert_verify` が「True」に設定されていて、`cert_file_path` エントリが存在する場合、NetScaler ADM はリクエストの `verify` パラメータにこのパスを送信します。そうでない場合、NetScaler ADM は `verify=true` を送信します。

注:

NetScaler ADM を「高可用性」モードで展開する場合は、heat.conf ファイルの次のパラメータを更新します:

```
NMAS_BASE_URI= <IP address of the front-end virtual server>
```

3. OpenStack で Heat サービスを再起動します。

OpenStack で Citrix ADC Heat サービスを再起動すると、定義されているすべての Citrix ADM StyleBook がリソースとして Heat にインポートされます。また、Citrix ADC ネットワークリソースと証明書リソースは、Citrix ADC Heat リソースとして OpenStack にインポートされます。

4. Citrix ADM を OpenStack に登録します。

- a) Citrix ADM で、「オーケストレーション」 > 「クラウドオーケストレーション」 > 「**OpenStack**」に移動し、「**OpenStack** 設定の構成」をクリックします。
- b) **OpenStack** の設定ページでは、OpenStack を設定するためのパラメーターを設定できます。[Default] と [Customized] の 2 つのオプションがあります。
- c) OpenStack サービスがデフォルトポートで実行されている場合は、「デフォルト」を選択します。以下のパラメーターを入力します。
  - i. OpenStack コントローラーの IP アドレス
  - ii. 管理者ユーザー名
  - iii. パスワード
  - iv. OpenStack 管理者テナント
  - v. Citrix ADC ドライバーと Heat のパスワード

注:

これは heat.conf ファイルに入力したパスワード (NMASS\_PASSWORD) と同じです。

5. サービスパッケージを作成し、テナントで SLA を定義します。

OpenStack の登録時に、Citrix ADM でユーザーごとにテナントが作成され、テナント情報は LBaaS ドライバーと Heat プラグインの両方で使用されます。Heat プラグインはこの情報を使用して NetScaler ADM に連絡し、OpenStack に Heat リソースとして StyleBook をインポートします。

注:

NetScaler ADM および OpenStack でのサービスパッケージの作成およびその他の事前構成タスクの詳細については、「[NetScaler ADM と OpenStack Platform の統合](#)」を参照してください。

6. NetScaler ADM 内の関連するすべての StyleBook がリソースとして OpenStack Heat にインポートされます。また、NetScaler ADC ネットワークリソースと NetScaler ADC 証明書リソースがリソースとして OpenStack Heat にインポートされることも確認します。

注

現在、使用できるのは Citrix ADM に付属している StyleBook のみです。

テナントは OpenStack で Heat テンプレートを作成して必要な Heat パラメーターの値を入力し、Heat スタックを展開できるようになりました。Heat スタックがデプロイされると、構成が Citrix ADM にプッシュされ、必要な Citrix ADC インスタンスが設定されます。

**Heat** テンプレートを準備して **Heat** スタックを起動するには:

1. OpenStack では、テナントで Heat リソースを使用して HOT を作成できます。
2. OpenStack Horizon では、テナント管理者はプロジェクト > \*\* オークストレーション \*\* > スタックに移動して Heat テンプレートを作成し、Heat スタックを起動できます。HOT を作成するには 2 つの方法があります。
  - ファイル - ローカルディレクトリから更新されたテンプレートを選択します
  - 直接入力 - YAML コンテンツをテンプレートからコピーしてウィンドウに貼り付けます

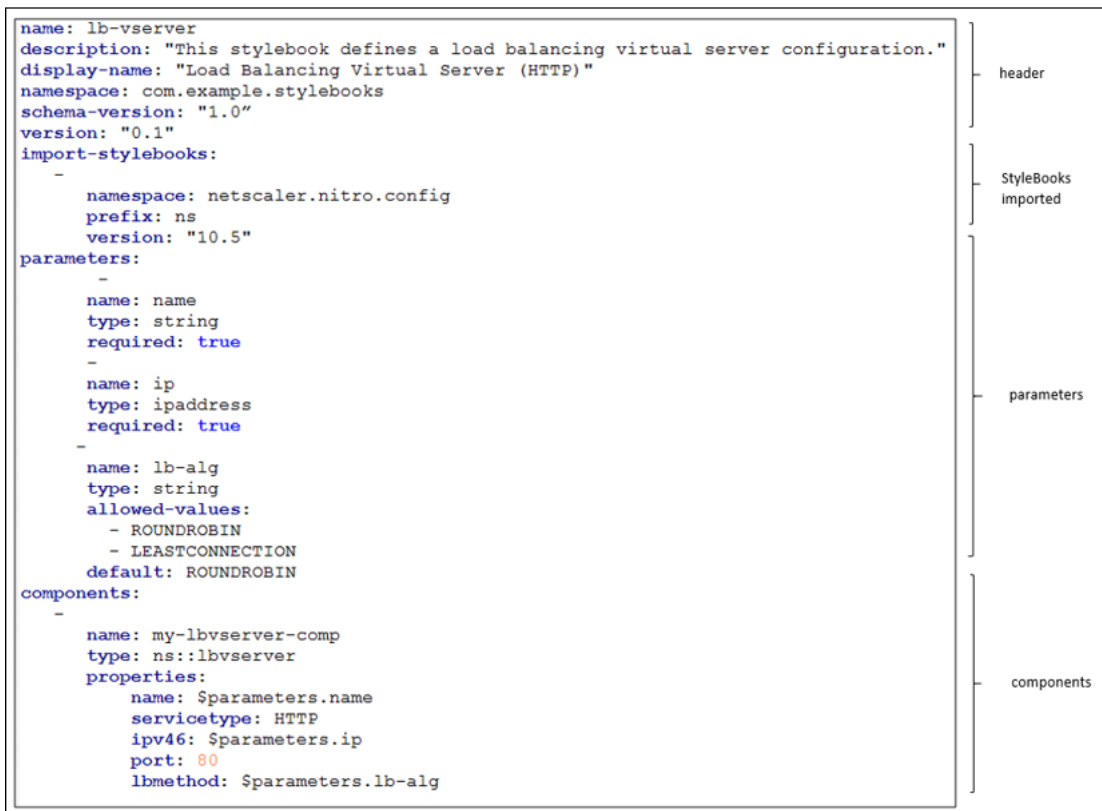
注:

スタックのデプロイが成功すると、テナントはスタック変更テンプレートを使用してスタックを更新できます。ただし、スタックの作成中に初回設定したサブネット情報と仮想 IP アドレス (VIP: Virtual IP Address) を変更することはできません。

テナントがスタックをデプロイしたら、NetScaler ADM で「オークストレーション」>「クラウドオークストレーション」>「**OpenStack**」>「リクエスト」の順に選択し、タスクのリストを確認します。また、NetScaler ADM の [アプリケーション] > [構成] の順に選択し、NetScaler ADC インスタンスが StyleBooks 構成パックの形式で正常に構成されていることを確認します。

**NetScaler ADM StyleBook** の例:

次の図は、NetScaler ADM StyleBook の構成例とコンポーネントを簡単に説明したものです。NetScaler ADM StyleBooks および同梱されている StyleBook の使用方法の詳細については、「[StyleBook](#)」を参照してください。



**Heat** テンプレートの例:

次の図は、YAML で定義されている Heat テンプレートの構造を示し、Heat リソースとしてインポートされる StyleBooks リソースおよび NetScaler ADC ネットワークリソースを示します。

```

heat_template_version: '2015-10-15'
parameter_groups:
- description: servers
  label: servers
  parameters: [server_ips, server_port]
- description: vip ip
  label: VIP IP
  parameters: [lb-virtual-ip, lb-virtual-port, lb-service-type]
- description: lb-appname
  parameters: [lb-appname]
parameters:
  lb-appname: {description: This is the lb-name, label: LB-NAME, type: string}
  lb-service-type:
    constraints:
      - allowed values: [HTTP, SSL, TCP, UDP, ANY]
      default: HTTP
      description: This is lb-service-type
      label: Service-type
      type: string
  lb-virtual-ip: {description: This is LB vip, label: VIP, type: string}
  lb-virtual-port: {description: This is virtual port, label: Virtual-port, type: string}
  server_ips: {description: Ip address of servers, label: IP of server, type: comma_delimited_list}
  server_port: {description: Port of server, label: Server port, type: string}
resources:
  sb_config:
    properties:
      lb-appname: {get_param: lb-appname}
      lb-service-type: {get_param: lb-service-type}
      lb-virtual-ip: {get_param: lb-virtual-ip}
      lb-virtual-port: {get_param: lb-virtual-port}
      mas_device_handle:
        get_attr: [network_resource_NS, mas_device_handle]
      svc-servers:
        repeat:
          for each:
            ipvar%: {get_param: server_ips}
            template:
              ip: ipvar%
              port: {get_param: server_port}
            type: Citrix::NetScaler::Stylebook_com_citrix_adc_stylebooks_1_0_lb
  network_resource_NS:
    properties:
      subnets: [c07d727c-37a6-493a-ab4e-b96d9ddab560]
    type: Citrix::NetScaler::NetscalerNetworkConfigurator

```

version of the Heat template

parameter groups - declares the input parameter groups and order

parameter groups - declares the input parameters

resources - declares template resources; in this example declares the StyleBook resources

resources - declares template resources; in this example declares the NetScaler network resources

Heat サービスの詳細とテンプレートの作成方法については、[OpenStack Heat のドキュメントを参照してください](#)。

## サービスパッケージの分離ポリシー

February 6, 2024

### 専用分離ポリシー

専用ポリシーの Citrix Application Delivery Management (ADM) サービスパッケージに関連付けられているすべてのテナントには、このサービスパッケージに含まれるインスタンスの中から Citrix ADC インスタンスが割り当てられます。この割り当てられた NetScaler ADC インスタンスは、他のテナントと共有されません。

## ← Service Package

### Service Level Agreement

Application Delivery Management allocates Citrix ADC Appliances for tenants

Name\*

Citrix ADC Instance Allocation\*

Dedicated     Partition     Shared    ?

Citrix ADC Instance Provisioning\*

Existing Instance     Create Instance OnDemand

Auto Provision Platform

CitrixADC SDX     OpenStack Compute

Citrix ADC Instance Type

**CitrixADC VPX**

### パーティション分離ポリシー

パーティションポリシーのサービスパッケージに関連付けられているすべてのテナントには、サービスパッケージの一部である NetScaler ADC インスタンスの専用の論理管理パーティションが割り当てられます。

## ← Service Package

### Service Level Agreement

Application Delivery Management allocates Citrix ADC Appliances for tenants

Name\*

Citrix ADC Instance Allocation\*

Dedicated  Partition  Shared

Citrix ADC Instance Provisioning\*

Existing Instance  Create Instance OnDemand

Citrix ADC Instance Type

CitrixADC VPX  CitrixADC MPX

### 共有分離ポリシー

サービスパッケージに関連付けられたテナントは、サービスパッケージの一部である Citrix ADC インスタンスを共有します。テナントのすべての構成は、1つの Citrix ADC インスタンスに割り当てられます。このモードでは、複数のテナントからの構成を同じ Citrix ADC インスタンスでホストできます。デバイスタイプとして **Citrix ADC VPX** または **Citrix ADC MPX** を選択できます。サービスパッケージには、Citrix ADC インスタンスを1つだけ割り当てることも、複数のインスタンスを割り当てることもできます。つまり、複数のテナントが Citrix ADC デバイスの1つまたは複数の仮想インスタンスを共有できます。

#### 注:

NetScaler ADC SDX インスタンスは、NetScaler ADC VPX インスタンスとしてのみサービスパッケージに追加してください。これは、NetScaler ADC SDX には NetScaler ADC VPX がプロビジョニングされているためです。

## ← Service Package

### Service Level Agreement

Application Delivery Management allocates Citrix ADC Appliances for tenants during their LB configuration. The following settings determine the SLA that is agreed for the tenants of this service package.

Name\*

Citrix ADC Instance Allocation\*

Dedicated     Partition     Shared

Citrix ADC Instance Type

CitrixADC VPX     CitrixADC MPX

Number of instances to allot per Policy/Tenant

Allot one instance     Allot many instances

Placement Method\*

 ⓘ

#### 注

また、ポリシーがテナント名や ID だけでなく、他のカスタム属性にも基づく柔軟な配置ポリシーを作成することもできます。柔軟な配置ポリシーについて詳しくは、「[柔軟なポリシーベースのデバイス割り当て](#)」を参照してください。

## 柔軟なポリシー・ベースのデバイス割り当て

February 6, 2024

Citrix Application Delivery Management (ADM) は、テナントと合意した SLA に基づいて、Citrix ADC 仮想インスタンスをテナントに割り当てます。テナントへの仮想インスタンス割り当てにおいて、インスタンスとテナントの関係は 1 対 1 です。データセンター内では、1 つのテナントを 1 つのサービスパッケージだけに割り当てることができます。



ただし、テナントが複数のインスタンスを必要とする場合や、テナントを基準にせず、ネットワーク ID やアプリケーションなどの要素に基づいてインスタンスを割り当てる場合も想定されます。このような場合、Citrix ADM では、ユーザー定義の式に基づいて配置ポリシーを正確に定義して、管理対象インスタンスの 1 つにロードバランサー構成を割り当てることができます。

配置ポリシーにより、ユーザーが作成した各ロードバランサー構成で使用される Citrix ADC インスタンスを柔軟に決定できます。Citrix ADM の柔軟な配置ポリシーは、テナントに基づいて Citrix ADC インスタンスを割り当てる既存の方法に追加のオプションを提供します。

### 注

手動でインスタンスをテナントに割り当てたり、作成された式に基づいてインスタンスを割り当てる配置ポリシーを使うことができます。1 つのサービスパッケージに対し、同時に両方の方法を使用することはできません。

配置ポリシーは、プールやロードバランサーなど、メインの LBaaS 構成のプロパティを通じて定義されたブール式に基づきます。Citrix ADM の配置ポリシーユーザーインターフェイスには、カスタマイズされたポリシーを定義するために選択できる定義済みの式が用意されています。さまざまな式に合わせて複数の配置ポリシーを作成できます。これにより、各テナントはテナントの要件で定義されている複数のデバイスを保有できます。

まずは、後で構成することとなるルートオブジェクトに適合する式を選択してください。ルートオブジェクトは、LBaaS V1 の場合はプールオブジェクト、LBaaS V2 の場合はロードバランサーオブジェクトです。そのため、Citrix ADM ポリシーベースのプレースメントは、LBaaS V1 API と V2 API の両方でサポートされています。その後、これらの配置ポリシーはサービスパッケージに割り当てられます。ルートオブジェクトがインスタンスに設定されると、モデルの後続のオブジェクトがインスタンスに追加されます。

たとえば、プール構成オブジェクトには次のプロパティがあります。

- tenant\_id
- name
- 説明
- protocol
- lb\_method
- subnet\_id
- subname\_name
- admin\_state\_up
- 状態
- network\_id
- network\_type
- segmentation\_id

- subnet\_cidr
- subnet\_gateway\_ip

次の例では、ポリシーの式を定義するプールプロパティを使用した式をいくつか示します。

1. プール名ベースのポリシー式

```
1 config["pools"]["name"] == "high-end-pool"
2 <!--NeedCopy-->
```

2. プールサブネット名ベースのポリシー式

```
1 config ["pools"]["subnet_name"] == "us-west-payment-subnet1"
2 <!--NeedCopy-->
```

3. ロードバランサーのサブネット名ベースのポリシー式

```
1 config["loadbalancers"]["subnet_name"] == "mas-subnet"
2 <!--NeedCopy-->
```

## 配置ポリシーの追加

1. Citrix ADM ホームページから、[オーケストレーション] > [クラウドオーケストレーション] > [配置ポリシー] に移動し、[追加] をクリックします。
2. **[Add Placement Policy]** ページで、次のパラメーターを設定します。
  - a) Name - 配置ポリシーの名前を入力します。
  - b) Frequently Used Expressions - ボックスの一覧から式を選択します。
  - c) Expression - 上のフィールドで選択した式に基づき、論理式（ブール式）がこのフィールドに表示されます。必要に応じてボックス名を編集します。

注:

複数のポリシーを作成する場合は、ポリシーが互いに排他的であることを確認してください。

## ← Add Placement Policy

Name\*

Sample Expressions\*

Expression\*

3. **[OK]** をクリックします。
4. **[\*\* オーケストレーション]** > **[クラウドオーケストレーション]** > **[OpenStack]** > **[サービスパッケージ]** に移動し、**[追加]** をクリックします。**\*\***
5. 「サービスパッケージ」 ページで、次のパラメータを設定します。

a) 名前-サービスパッケージの名前を入力します

b) 隔離ポリシー- 共有ポリシーを選択

共有分離ポリシーでは、テナントのロードバランサー構成は、テナントに割り当てられたデバイス中において、他のテナントのロードバランサー構成と共存します。

c) デバイスタイプ - 事前にプロビジョニングされた **Citrix ADC VPX** または **Citrix ADC MPX** を選択してください

テナントのすべてのロードバランサー構成を 1 つのデバイスに関連付ける場合は、**[Allot one device]** を選択します。テナントの各ロードバランサー構成を、配置ポリシーに基づいて複数のデバイスに配布する場合は、**[Allot many devices]** を選択します。

### 注

:Citrix ADC SDX には Citrix ADC VPX がプロビジョニングされているため、Citrix ADC SDX は Citrix ADC VPX インスタンスとしてのみサービスパッケージに追加する必要があります。

d) 配置方法- 「最小構成」を選択

「最小構成済み」を選択すると、その時点で構成されているプールメンバーの数が最も少ない NetScaler ADC インスタンスがテナントのデバイスとして選択されます。

## ← Service Package

### Service Level Agreement

Application Delivery Management allocates Citrix ADC Appliances for tenants

Name\*

Citrix ADC Instance Allocation\*

Dedicated   
  Partition   
  Shared

Citrix ADC Instance Type

CitrixADC VPX   
  CitrixADC MPX

Number of instances to allot per Policy/Tenant

Allot one instance   
  Allot many instances

Placement Method\*

Continue
Cancel

6. [続行] をクリックします。

7. [デバイスの割り当て] セクションで、使用可能な NetScaler ADC デバイスを構成済みのデバイスリストに追加します。

### Assign Devices

Available (1) Select All

10.102.31.138 +

▶

◀

Configured (1) Remove All

10.102.29.60 -

Continue
Cancel

8. [続行] をクリックします。
9. [ 配置ポリシーの割り当て ]/[OpenStack テナント] セクションで、前に作成した配置ポリシーを追加します。

**Assign Placement Policies/OpenStack Tenants**

Tenants assigned to one shared Service Package should not have overlapping IP addresses in their networks.

Placement Policies
  OpenStack Tenants

**Available (1)** Select All

http\_region\_pp +

**Configured (1)** Remove All

admin\_pp\_policy -

▶

◀

Continue

Cancel

注:

ポリシーが見つからない場合、フォールバックメカニズムが復活し、NetScaler ADM はテナントに基づいて NetScaler ADC インスタンスを割り当てます。テナントがどのサービスパッケージにも含まれていない場合、NetScaler ADM は

「テナント `admin` はどのサービスパッケージにも含まれておらず、デフォルトのサービスパッケージはありません」というエラーメッセージを表示します。

10. [Continue]、[Done] の順にクリックします。

## NSX Manager: NetScaler ADC インスタンスの手動 Provisioning

February 6, 2024

Citrix Application Delivery Management (ADM) は、VMware ネットワーク仮想化プラットフォームと統合して、Citrix ADC サービスの展開、構成、および管理を自動化します。この統合により、物理ネットワークポロジに関連する従来の複雑さが解消され、vSphere/vCenter 管理者は Citrix ADC サービスをプログラムにより迅速に展開できるようになります。

この記事では、VMware NSX Manager と Citrix ADM の両方で実行する必要があるタスクのリストを示します。

注:

VMware NSX for vSphere 6.2 以降がインストールおよび構成されていること、および負荷分散が必要なエッジゲートウェイ、分散論理ルーターおよび仮想マシンがすでに作成されていることを確認してください。

前提条件

- 最小要件を満たすハードウェアで VMware ESXi Version 4.1 以降をインストールします。
- 最小システム要件を満たす管理用のワークステーションに VMware Client をインストールします。
- 最小システム要件を満たす管理用のワークステーションに、VMware ESXi Version 4.1 に必要な VMware OVF Tool をインストールします。
- サポートされているハイパーバイザーのいずれかに NetScaler ADM をインストールします。

サポートされているハイパーバイザーに NetScaler ADM Build 13.0 をインストールするタスクについては、「[NetScaler ADM の展開](#)」を参照してください。

**VMware ESXi** のハードウェア要件

次の表は、Citrix ADM 仮想アプライアンスをインストールするために VMware ESXi サーバーに必要な仮想コンピューティングリソースを示しています。

---

コンポーネント	条件
RAM	8 GB
仮想 CPU	8
記憶域	500 GB
仮想ネットワーク インターフェイス	1
スループット	1Gbps

---

注

: 上記のメモリとハードディスクの要件は、ホスト上で他の仮想マシンが実行されていないことを考慮して、Citrix ADM を VMware ESXi サーバーに展開するためのものです。VMware ESXi サーバーのハードウェア要件は、サーバーで動作する仮想マシンの数によって異なります。

## VMware NSX の構成

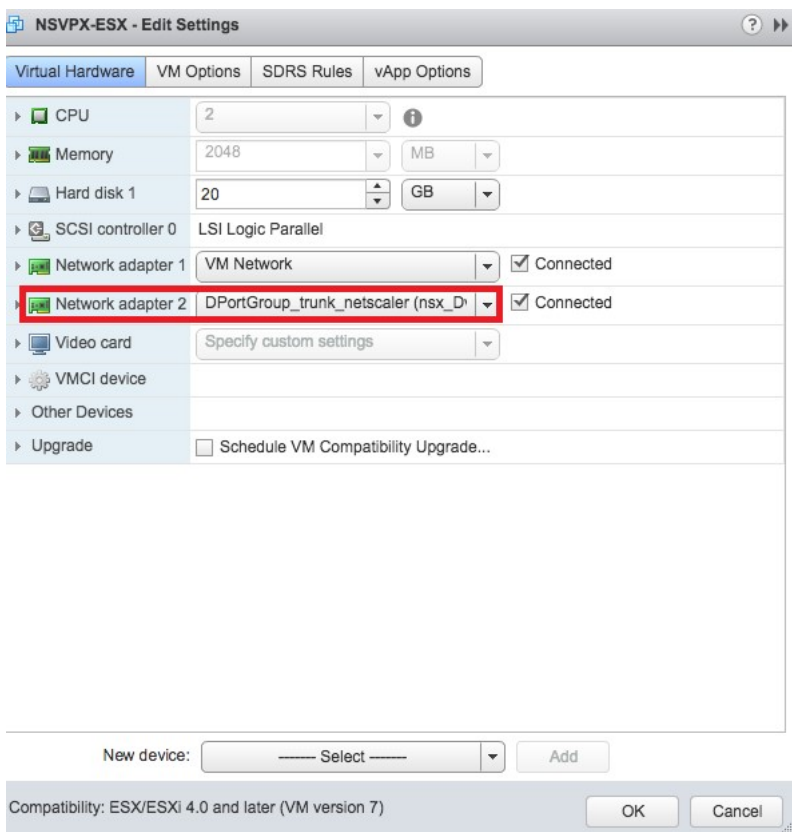
- 容量の異なる Citrix ADC VPX インスタンスのプールを作成し、さまざまなサービスパッケージに追加します。

次に例を示します：

- VPX1000 (1 Gbps) の Citrix ADC VPX インスタンスを 5 つ作成します。これらのインスタンスは Gold サービスパッケージに追加されます。
- VPX10 (10 Mbps) の Citrix ADC VPX インスタンスを 5 つ作成します。これらのインスタンスは Bronze サービスパッケージに追加されます。

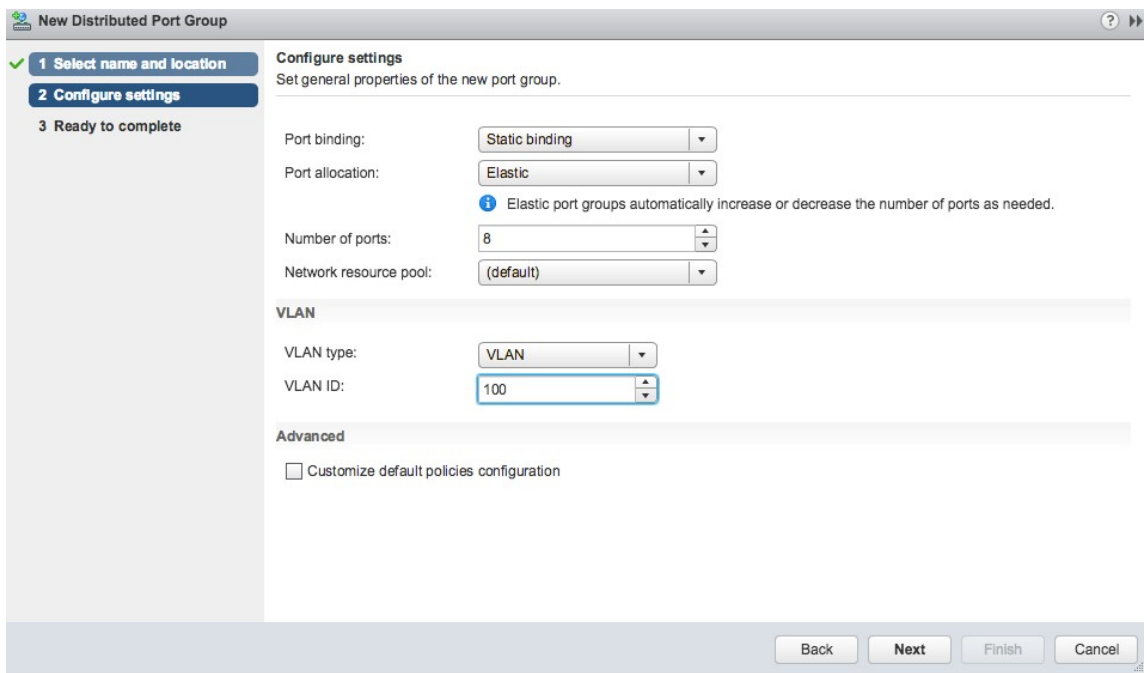
1. vSphere Client で **[Networking]** に移動し、たとえば「101-105」のように範囲を指定して、種類が VLAN トランク接続のポートグループを作成します（すべての範囲を設定することもできますが、必要な VLAN だけを対象として、種類が VLAN のポートグループを作成します）。

2. NetScaler ADC VPX インスタンスごとに新しいインターフェイスを作成し、上で作成した VLAN 範囲トランクポートグループに接続します。



3. vSphere Client で **[Networking]** に移動し、種類が VLAN のポートグループを作成します。

たとえば、最初のトランク接続のポートグループを 101 から 105 の範囲で作成した場合、VLAN ごとに1つずつ、合計 5 つの VLAN ポートグループを作成します。VLAN 101 のポートグループ、VLAN102 のポートグループというように、VLAN 105 まで作成します。





## NetScaler ADM での NetScaler ADC VPX インスタンスの追加

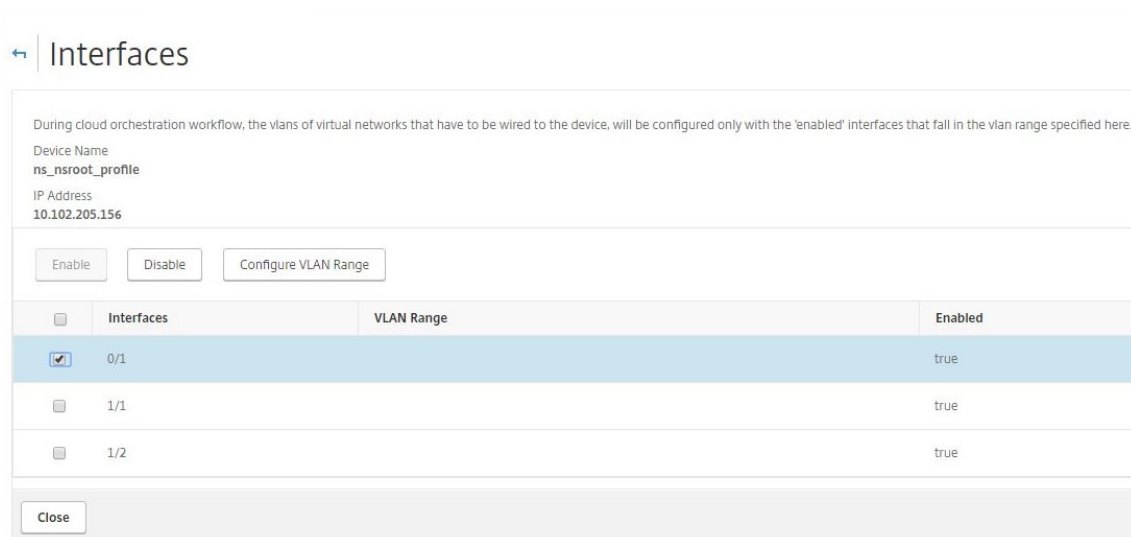
Citrix ADC VPX インスタンスを Citrix ADM に追加し、各デバイスのトランクグループの VLAN 範囲を指定します。

1. Citrix ADM で、[インフラストラクチャ]>[インスタンス]>[\*\*Citrix ADC VPX] に移動し、[追加 \*\*] をクリックします。
2. [Citrix ADC VPX の追加] ページで、インスタンスのホスト名、各インスタンスの IP アドレス、または IP アドレスの範囲を指定し、[プロファイル名] リストからインスタンスプロファイルを選択します。[+] をクリックして新しいインスタンスプロファイルを作成することもできます。
3. [OK] をクリックします。
4. Citrix ADC VPX ページのリストから新しく追加された **Citrix ADC VPX** インスタンスを選択し、アクションフィールドの下矢印ボタンをクリックします。[Configure Interfaces for Orchestration] を選択します。

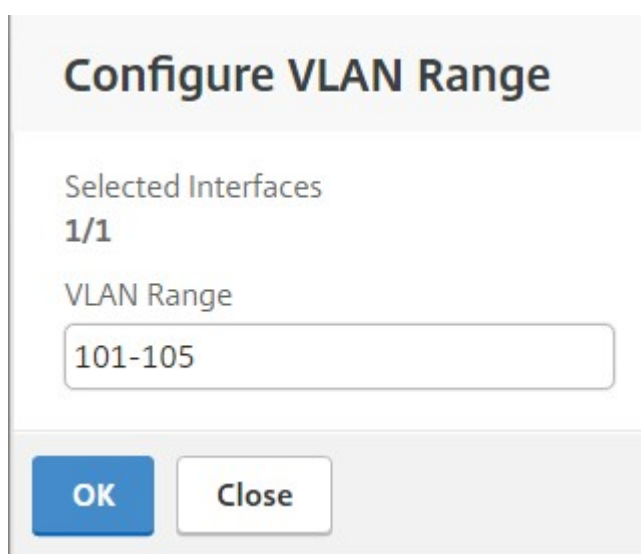
### Citrix ADC

	IP Address	Host Name	Instance State	Rx (Mbps)
<input checked="" type="checkbox"/>	10.102.29.60	--	● Up	
<input type="checkbox"/>	10.102.29.170	--	● Up	
<input type="checkbox"/>	10.102.29.175	--	● Up	
<input type="checkbox"/>	10.102.29.180	--	● Up	
<input type="checkbox"/>	10.102.29.200	--	● Up	
<input type="checkbox"/>	10.102.126.36	beta	● Out of Service	
<input type="checkbox"/>	10.102.166.4	10.102.166.4	● Down	
<input type="checkbox"/>	10.102.166.5	kranthi-2	● Down	
<input type="checkbox"/>	10.102.166.6	VPX03	● Down	

5. [Interfaces] ページで、管理インターフェイスを選択し、[Disable] をクリックして、VLAN が管理インターフェイスにバインドしないようにします。



6. [ **Inter** faces] ページで、必要なインターフェイスを選択し、[ **Configure VLAN Range**] をクリックします。
7. NSX Manager で設定された VLAN 範囲を入力し、[ **OK**]、[ 閉じる] の順にクリックします。

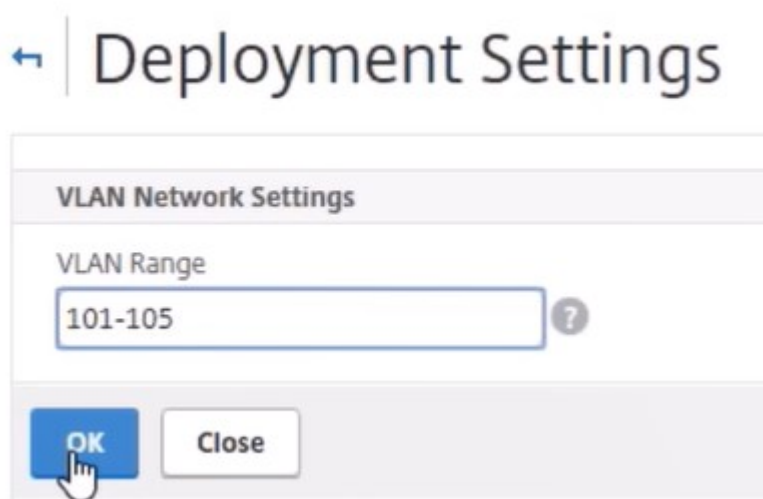


## VMware NSX マネージャーを NetScaler ADM に登録する

VMware NSX Manager を Citrix ADM に登録して、それらの間の通信チャンネルを作成します。

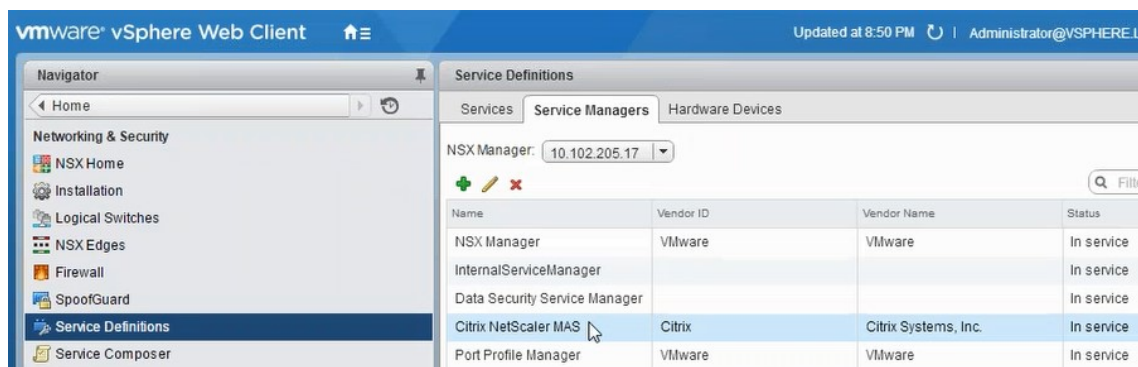
1. Citrix ADM で、ドロップダウンリストから [オーケストレーション] > [SDN オーケストレーション] > [VMware NSX Manager] に移動し、[NSX Manager 設定の構成] をクリック します。
2. **NSX Manager** の設定ページで、次のパラメータを設定します。
  - a) NSX Manager IP Address - NSX Manager の IP アドレス

- b) NSX Manager ユーザー名-NSX Manager の管理ユーザー名。
  - c) Password - NSX Manager の管理者ユーザーのパスワード
3. **[NSX マネージャーが使用する NetScaler ADM アカウント]**セクションで、**NSX** マネージャーの[NetScaler ADC ドライバのユーザー名とパスワード] を設定します。NetScaler ADM は、これらのログオン資格情報を使用して NSX Manager からのロードバランサー構成要求を認証します。
  4. **[OK]** をクリックします。
  5. **[オーケストレーション]>[システム]>[デプロイ設定]** に移動します。トランク接続のポートグループに構成されている VLAN の範囲を入力します。



6. vSphere Web Client で NSX Manager にログオンし、**[サービス定義]>[サービスマネージャ]** に移動します。

Citrix Citrix ADM をサービスマネージャの 1 人と見なすことができます。これは、登録が成功し、NSX Manager と NetScaler ADM の間に通信チャネルが確立されたことを示します。



## NetScaler ADM でのサービスパッケージの作成

1. Citrix ADM で、[オーケストレーション] > [SDN オーケストレーション] > [VMware NSX Manager] > [サービスパッケージ] に移動し、[追加] をクリックして新しいサービスパッケージを追加します。
2. 「サービスパッケージ」ページの「基本設定」セクションで、次のパラメータを設定します。

- a) Name - サービスパッケージの名前を入力します。
- b) Isolation Policy - デフォルトでは、分離ポリシーは [Dedicated] に設定されています。
- c) デバイスタイプ—デフォルトでは、デバイスタイプは Citrix ADC VPX に設定されています

注:

これらの値は、このバージョンではデフォルトで設定されており、変更することはできません。

- d) [続行] をクリックします。

### ← Service Package

**Service Level Agreement**

Application Delivery Management allocates Citrix ADC Appliances for tenants during their LB configuration.

Name\*

Citrix ADC Instance Allocation\*

Dedicated     Partition     Shared

Citrix ADC Instance Provisioning\*

Existing Instance     Create Instance OnDemand

Citrix ADC Instance Type

CitrixADC VPX     CitrixADC MPX

3. [デバイスの割り当て] セクションで、このパッケージ用に事前にプロビジョニングされた VPX を選択し、[続行] をクリックします。
4. [サービスパッケージの公開] セクションで、[続行] をクリックしてサービスパッケージを VMware NSX に公開し、[完了] をクリックします。

← Service Package

**Service Level Agreement**

Name <b>Platinum</b>	Citrix ADC Instance Allocation <b>dedicated</b>
	Citrix ADC Instance Type <b>CitrixADC VPX</b>
	Platform Type <b>CitrixADC VPX</b>

**Assign Instances**

Configured (0) Remove All

No items

+ Add

Continue
Cancel

## Publish ServicePackage

This Service Package is published to VMware NSX Manager.

Done

この手順により、NSX Manager にサービスパッケージが構成されます。サービスには複数のデバイスを追加でき、複数のエッジが同じサービスパッケージを使用して Citrix ADC VPX インスタンスを Citrix ADM にオフロードできます。

5. **vSphere Web Client** で **NSX Manager** にログインし、[ \*\* サービス定義 ] > [ サービス ] に移動します。 \*\*

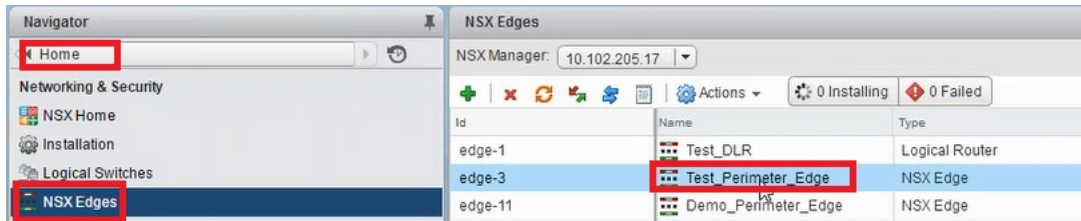
NetScaler ADM サービスパッケージが登録されていることがわかります。



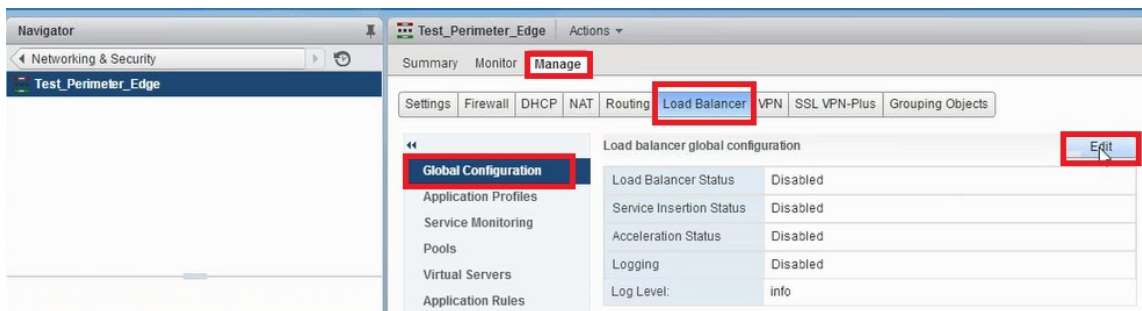
## Edge 向けのロードバランサーサービスの挿入の実行

以前に作成した NSX Edge ゲートウェイにロードバランサーサービスの挿入を実行します（ロードバランシング機能を NSX LB から Citrix ADC にオフロードします）。

1. NSX Manager で、[ホーム]>[NSX エッジ]に移動し、構成したエッジ Gateway を選択します。

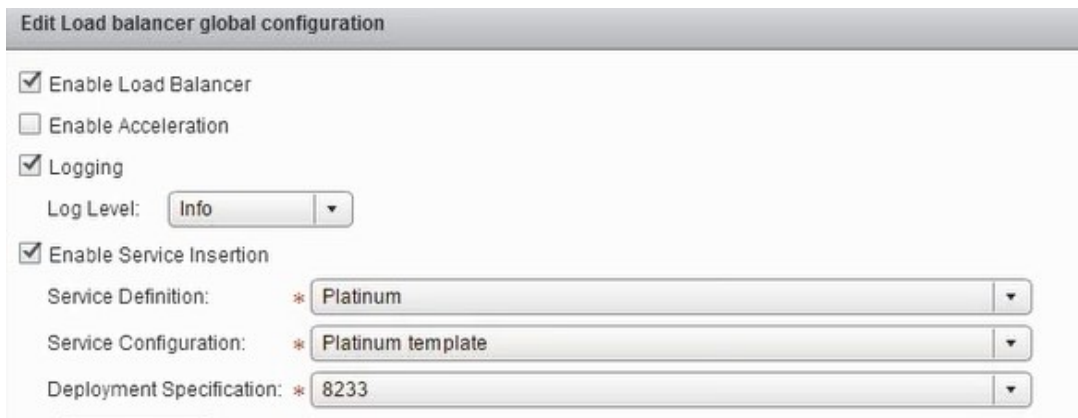


2. [管理] をクリックし、[ロードバランサ] タブで [グローバル構成] を選択し、[編集] をクリックします。



3. [ロードバランサを有効にする]、[ログ]、[サービス挿入を有効にする] の順に選択して有効にします。

- a) [サービス定義] で、NetScaler ADM で作成され、NSX Manager に公開されたサービスパッケージを選択します。



4. 既存のランタイム NIC を選択し、[編集] アイコンをクリックして、NetScaler ADC VPX が割り当てられているときに接続する必要があるランタイム NIC を編集します。

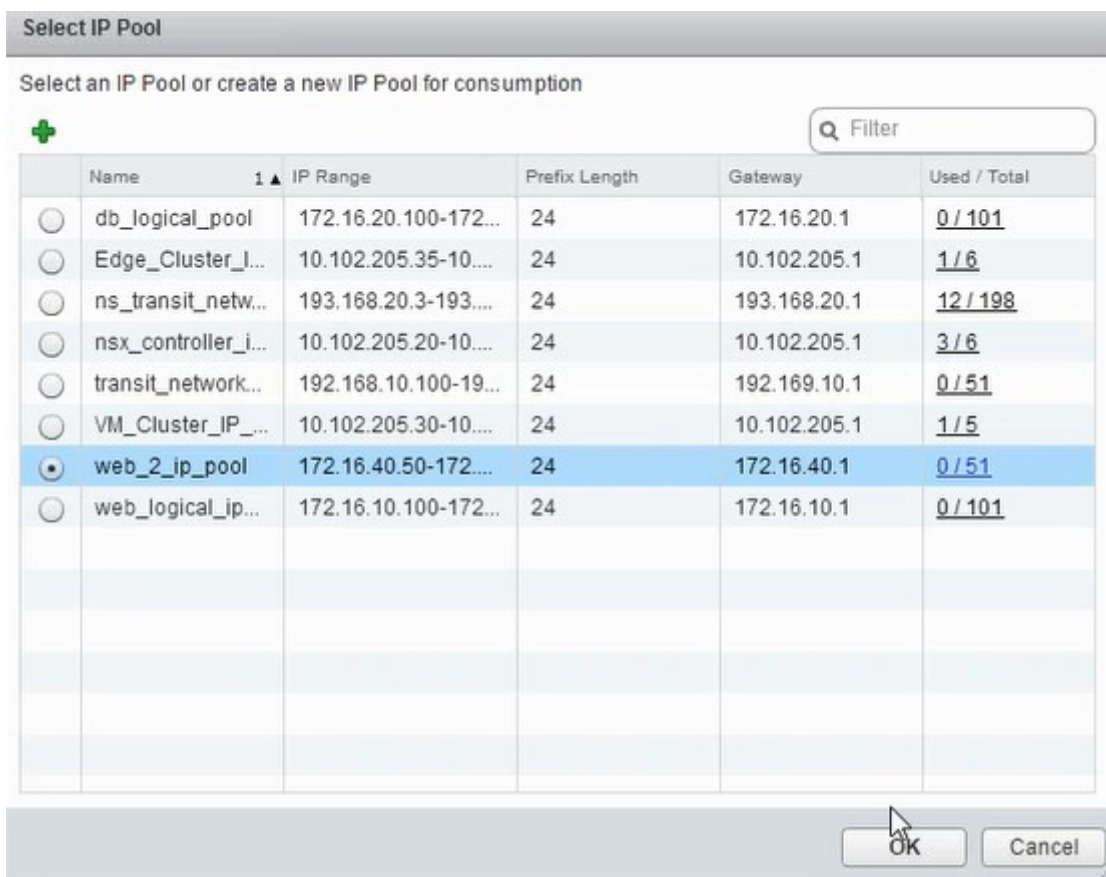
Name	Connected To	ConnectivityType	IP Address	Subnet Mask	Gateway Address
mgmt_if					10.102.205.102
transit_if	Web_2_logical_net	Data	172.16.40.102	255.255.255.0	172.16.40.102
vnic2					
vnic3					

5. NIC の名前を編集し、[接続タイプ] を [データ] に指定して、[変更] をクリックします。

6. 適切な Web 論理スイッチを選択します。

7. [プライマリ IP 割り当てモード] で、ドロップダウンリストから [IP Pool] を選択し、[IP Pool] フィールドの下矢印ボタンをクリックします。

8. [IP プールの選択] ウィンドウで、適切な IP プールを選択し、[OK] をクリックします。

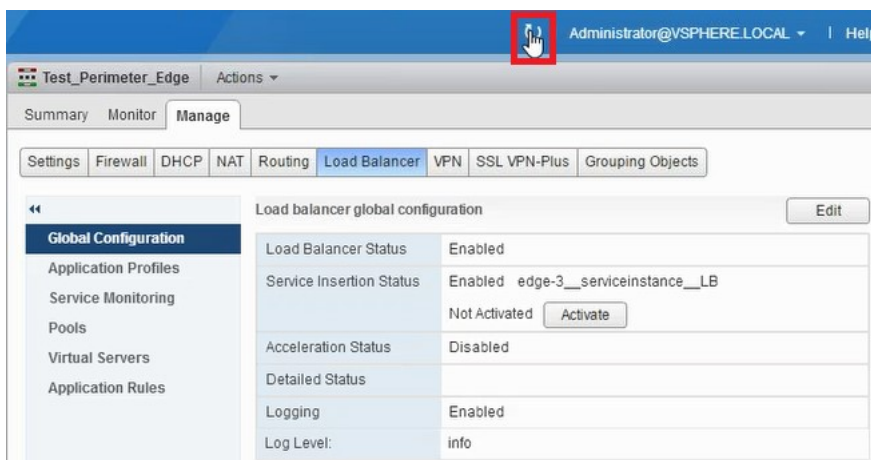


IP アドレスが取得され、NetScaler ADC VPX アプライアンスのソースネット IP アドレスとして設定されます。VXLAN を VLAN にマッピングするために、NSX Manager で L2 ゲートウェイが作成されます。

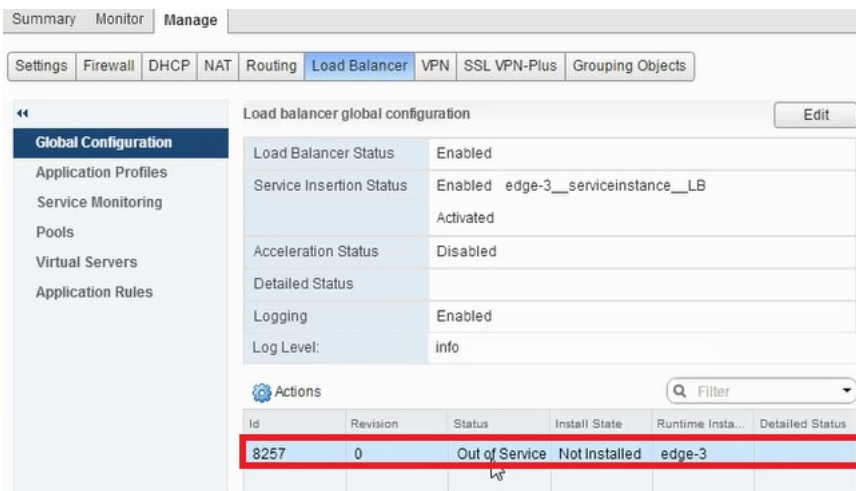
注:

すべてのデータインターフェイスは実行時 NIC として接続され、分散論理ルーター用のインターフェイスの一部です。

9. ビューを更新して、実行時の作成を確認します。







10. 仮想マシンの起動後、[状態]の値が[サービス中]に変わり、[インストール状態]の値が[有効]に変わります。

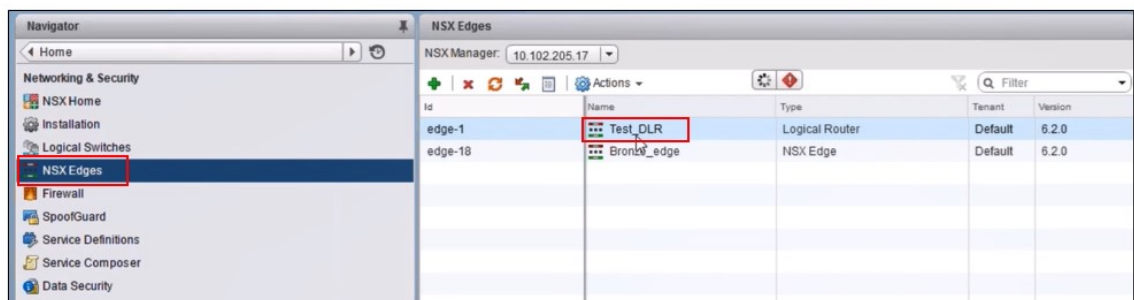
Id	Revision	Status	Install State	Runtime Insta...	Detailed Status
8257	2	In Service	Enabled	vm-267	

注:

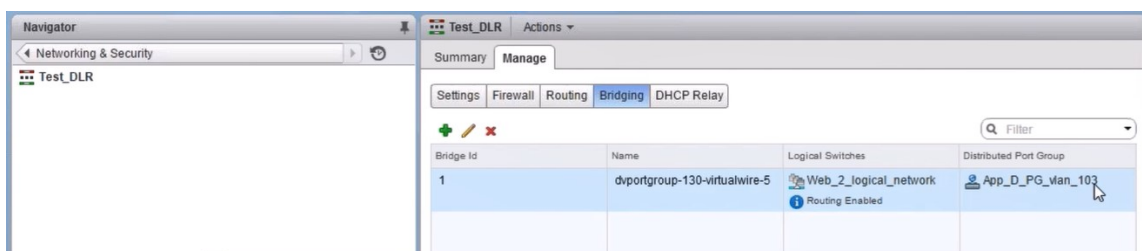
NetScaler ADM で、[オーケストレーション] > [リクエスト] に移動して、LB サービス挿入の完了の進行状況の詳細を確認します。

## NSX Manager での L2 ゲートウェイの表示

1. vSphere Web Client で NSX Manager にログオンし、[NSX エッジ]に移動し、作成した分散論理ルーターを選択します。



2. [分散論理ルーター] ページで、[管理] > [ブリッジ]に移動します。一覧に L2 ゲートウェイが表示されます。

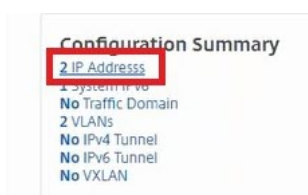


注:

L2 Gateway は、データインターフェイスごとに作成されます。

## 割り当てられた Citrix ADC の表示

1. Citrix ADM に表示されている IP アドレスを使用して Citrix ADC VPX インスタンスにログインします。次に、[構成] > [システム] > [ネットワーク] に移動します。2 つの IP アドレスが追加されていることが右ペインに表示されています。IP アドレスのハイパーリンクをクリックして詳細を表示します。



サブネット IP アドレスは、NSX に追加された Web インターフェイスの IP アドレスと同じです。

IPV4s 2		IPV6s 1					
	IP Address	State	Type	Mode	ARP	ICMP	Virtua
<input type="checkbox"/>	10.102.205.36	ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-N/A-
<input checked="" type="checkbox"/>	172.16.40.50	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-

2. [構成] > [システム] > [ライセンス] に移動し、このインスタンスに適用されているライセンスを表示します。

## StyleBook を使用した NetScaler ADC VPX インスタンスの構成

1. NetScaler ADM で、[オーケストレーション] > [SDN オーケストレーション] > [NSX Manager の構成] > [エッジゲートウェイ] に移動します。

StyleBooks による負荷分散構成を適用する必要があるそれぞれの Edge ゲートウェイに割り当てられる NetScaler ADC インスタンス IP を書き留めます。

2. 新しい StyleBook を作成します。「アプリケーション」 > 「設定」の順に選択し、StyleBook をインポートして、リストから StyleBook を選択します。

[新しい StyleBook を作成するには、独自の StyleBook を作成するを参照してください。](#)

3. すべての必須パラメーターに対して値を指定します。

The screenshot shows the 'Application Configuration / Choose StyleBook / Deploy Configuration' page. The left sidebar lists navigation options: Application Monitoring, Load Balancing, Content Switching, Cache Redirection, Authentication, GSLB, NetScaler Gateway, Auditing, Settings, Application Groups, and Application Configuration (selected). The main content area includes the following fields and sections:

- Load Balanced Application Name\*: web\_app
- Load Balanced App Virtual IP address\*: 172 . 16 . 40 . 100
- Application Servers IP Addresses\*: 172 . 16 . 40 . 21 and 172 . 16 . 40 . 22
- Application Server Port\*: 80
- Advanced Load Balancer Settings**
  - Load Balanced App Virtual Port\*: 80
  - Load Balanced App Persistence Type: SOURCEIP
  - Load Balanced App Algorithm: LEASTCONNECTION
  - Load Balanced App Client Timeout: (empty)
- Advanced Application Server Settings**
  - Service Group UseProxyPort: (empty)
  - Service Group CIP: (empty)
  - Preserve Client Source IP (USIP): (empty)
  - Service Group CIP Header: (empty)

4. これらの構成設定を実行する NetScaler ADC VPX インスタンスを指定します。

The screenshot shows the 'Advanced Configurations' dialog box. The 'Target Instance' field is a dropdown menu with the text 'Click to select' and a red box around it. Below the dropdown is a 'Dry Run' checkbox (unchecked) and 'Create' and 'Close' buttons.

5. 前述の IP インスタンスを選択し、[ **Select** ] をクリックします。

The screenshot shows the NetScaler instance management interface. At the top, there are buttons for 'Select', 'Add Instance', 'Delete', and 'Action'. Below is a table with the following data:

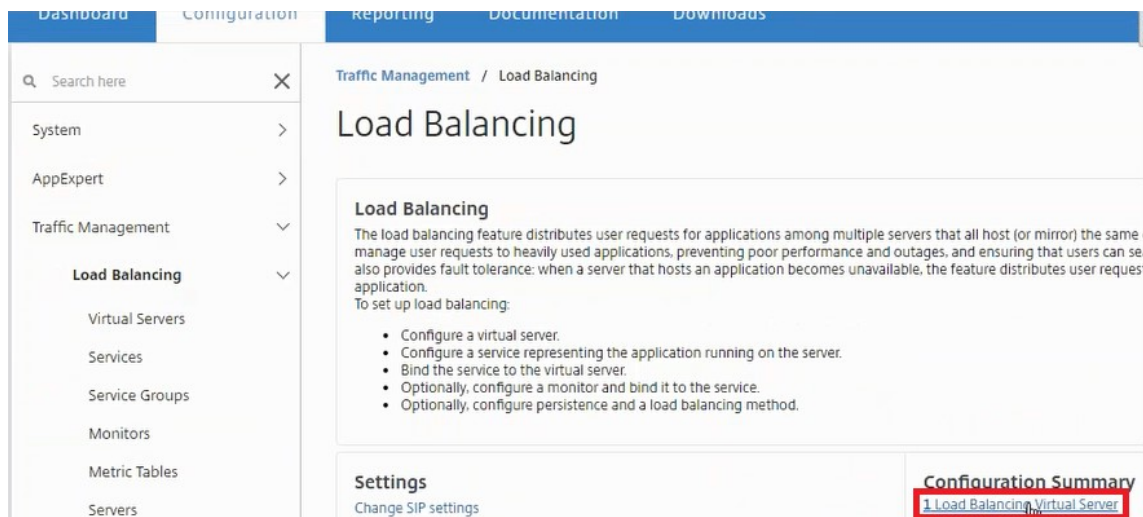
	IP Address	Host Name	State	Host IP Address	CPU Usage (%)	Memory Usage (%)	Build Version
<input checked="" type="radio"/>	10.102.205.36	--	<span style="color: green;">●</span>	--	0.6	11.85	11.1: Build 39.2.nc

6. [ **Create** ] をクリックして、選択したデバイスに設定を適用します。

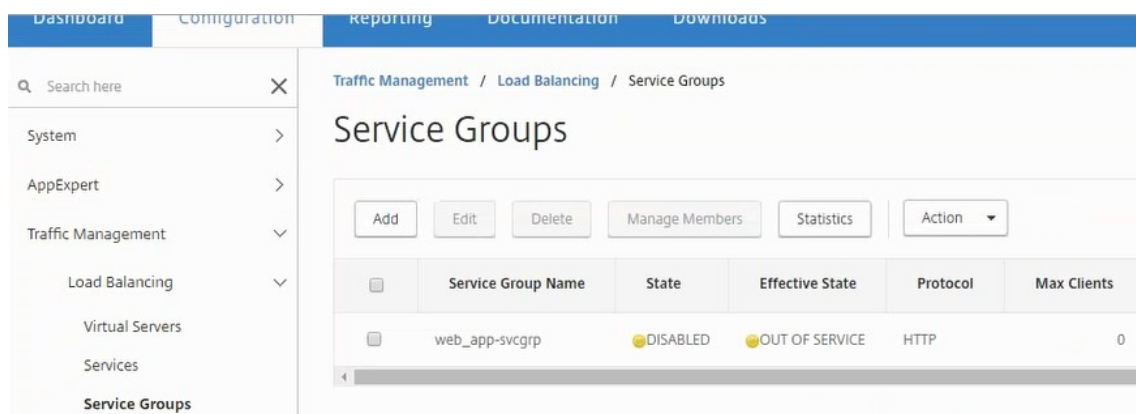
The screenshot shows the 'Advanced Configurations' dialog box. The 'Target Instance' field now contains the IP address '10.102.205.36'. The 'Create' button is highlighted with a red box.

ロードバランサー構成の表示

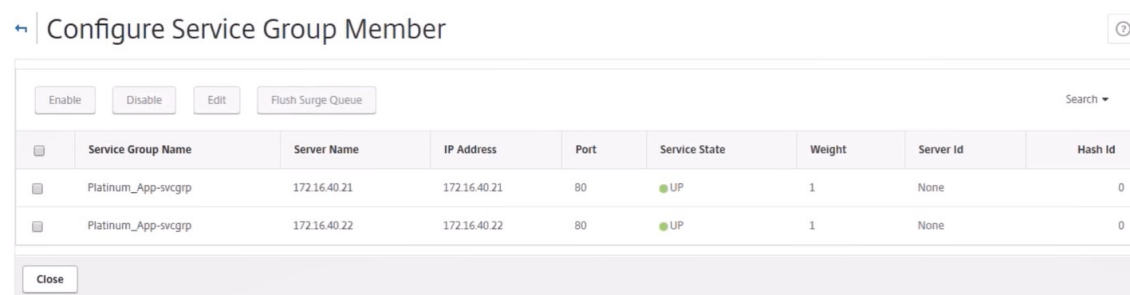
1. NetScaler ADC VPX インスタンスにログオンし、[構成] > [トラフィック管理] > [負荷分散] の順に選択し、作成された負荷分散仮想サーバーを表示します。



作成したサービスグループも表示できます。



2. サービスグループを選択し、[メンバーの管理] をクリックします。サービスグループに割り当てられたメンバーが [Configure Service Group Member] ページに表示されます。

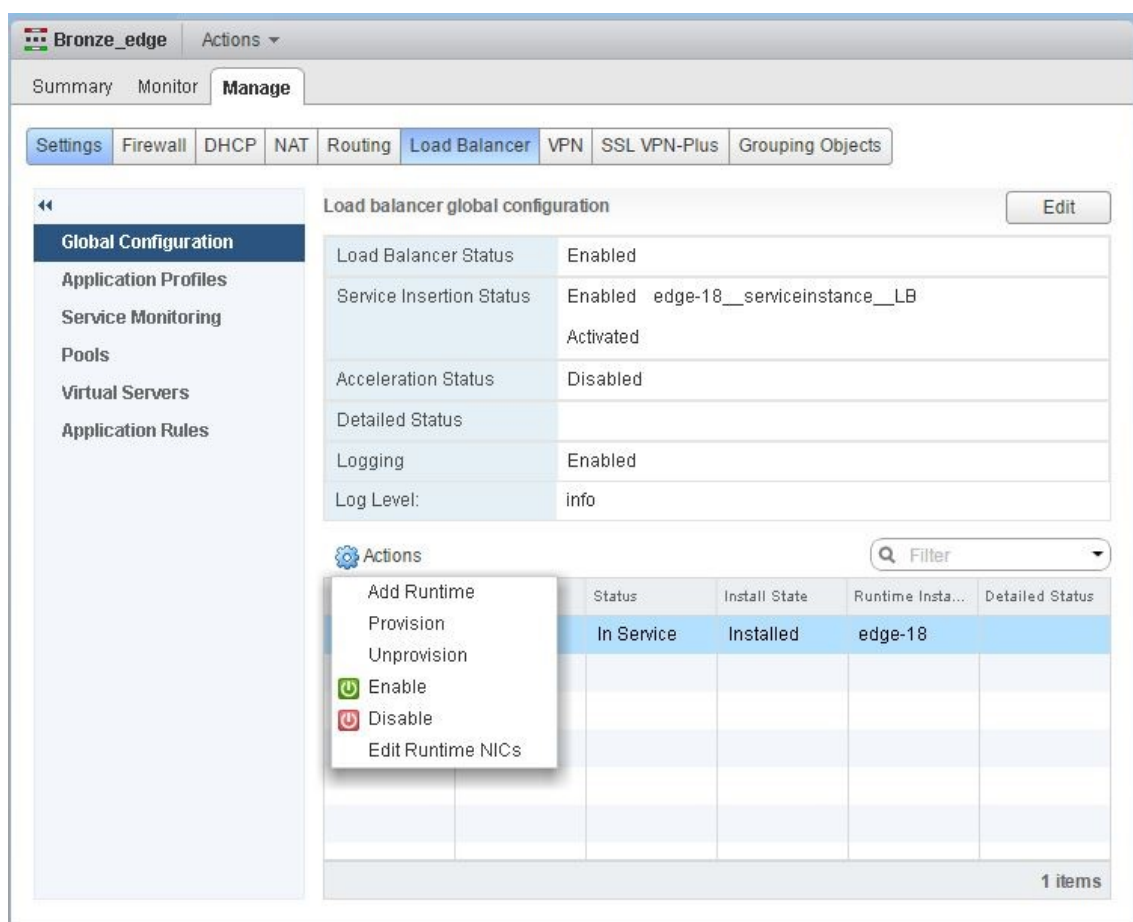


## ロードバランサーサービスの削除

1. Citrix ADM で、[アプリケーション] > [構成] に移動し、**[X]** アイコンをクリックしてアプリケーション構成を削除します。
2. vSphere Web Client で NSX Manager にログオンし、Citrix ADC VPX インスタンスが接続されているエッジゲートウェイに移動します。
3. [管理] > [ロードバランサー] > [グローバル設定] に移動し、ランタイムエントリを右クリックして、[プロビジョニング解除] をクリックします。

注:

NetScaler ADM のエッジゲートウェイは、NSX マネージャーの実行時エントリに対応します。



NetScaler ADC VPX インスタンスがサービス外になります。

4. NetScaler ADM で、[オーケストレーション] > **[SDN オーケストレーション]** > **[NSX Manager の構成]** > [エッジゲートウェイ] に移動します。削除されたインスタンスに対する Edge ゲートウェイの割り当てが存在しないことを確認します。

## NSX Manager: NetScaler ADC インスタンスの自動 Provisioning

February 6, 2024

### 概要

Citrix Application Delivery Management (ADM) は、VMware ネットワーク仮想化プラットフォームと統合して、Citrix ADC サービスの展開、構成、および管理を自動化します。この統合により、物理ネットワークポロジに関連する従来の複雑さが解消され、vSphere/vCenter 管理者は Citrix ADC サービスをプログラムにより迅速に展開できるようになります。

VMware NSX Manager での負荷分散サービスの挿入および削除中に、Citrix ADM は Citrix ADC インスタンスを動的にプロビジョニングおよび破棄します。この動的プロビジョニングでは、Citrix ADC VPX ライセンスの割り当てを Citrix ADM で自動化する必要があります。Citrix ADC ライセンスが Citrix ADM にアップロードされると、Citrix ADM はライセンスサーバーの役割を果たします。

### 前提条件

#### 注

この統合は、**vSphere 6.1** 以前の **VMware NSX** でのみサポートされます。

- Citrix ADM、バージョン 13.0 は高可用性でセットアップされ、ESX にインストールされています。
- Citrix ADC VPX、バージョン 13.0
- Citrix ADC VPX インスタンス用 Citrix ADC VPX ライセンス、バージョン 13.0
- 最小要件を満たすハードウェアで VMware ESXi Version 4.1 以降をインストールします。
- 最小システム要件を満たす管理用のワークステーションに VMware Client をインストールします。
- 最小システム要件を満たす管理用のワークステーションに、VMware ESXi Version 4.1 に必要な VMware OVF Tool をインストールします。

### Citrix ADM および Citrix ADC インスタンスの高可用性デプロイ

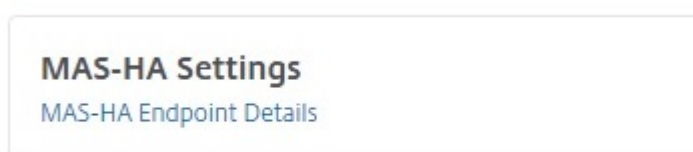
NetScaler ADM 高可用性セットアップをプロビジョニングするには、Citrix ダウンロードサイトからダウンロードした NetScaler ADM イメージファイルをインストールします。NetScaler ADM HA セットアップをプロビジョニングする方法の詳細については、「[NetScaler ADM を高可用性で展開する](#)」を参照してください。

## NetScaler ADM HA エンドポイントの詳細の設定

VMware NSX Manager を HA モードでデプロイされた Citrix ADM と統合するには、まず負荷分散 Citrix ADC インスタンスの仮想 IP アドレスを入力する必要があります。また、Citrix ADC 負荷分散仮想サーバーにある証明書ファイルを Citrix ADM ファイルシステムにアップロードする必要があります。

**Citrix ADM** で負荷分散構成情報を提供するには:

1. Citrix ADM HA ノードで、[システム]>[デプロイメント]に移動します。
2. 右上隅の [HA 設定] をクリックし、[MAS-HA 設定] ページで [MAS-HA エンドポイントの詳細] をクリックします。



3. **MAS-HA Endpoint Details** ページで、負荷分散 NetScaler ADC インスタンスにすでに存在する証明書と同じ証明書をアップロードします。
4. 負荷分散 NetScaler ADC インスタンスの仮想 IP アドレスを入力し、[OK] をクリックします。

### ← MAS-HA Endpoint Details

You can provide the LB configuration information (VIP and cert) which was configured in the NetScaler for Loadbalancing traffic to MAS nodes.

Certificate file\*

Choose File ▼ server\_cert3

Virtual IP\*

10 . 102 . 29 . 192

OK Close

## VMware NSX マネージャーを NetScaler ADM に登録する

2 台の Citrix ADM サーバーを高可用性に設定すると、2 台のサーバーノードはアクティブ/パッシブモードになります。プライマリ Citrix ADM サーバノードにログオンして VMware NSX Manager を HA の Citrix ADM に登録し、それらの間の通信チャンネルを作成します。

**VMware NSX Manager** を HA の **Citrix ADM** に登録するには:

1. プライマリ Citrix ADM サーバノードで、[オーケストレーション]> [SDN オーケストレーション]> [VMware NSX Manager] に移動します。

2. [ **NSX Manager** の設定を設定 ] をクリックします。
3. **NSX Manager** の設定ページで、次のパラメータを設定します。
  - a) NSX Manager IP Address - NSX Manager の IP アドレス
  - b) NSX Manager ユーザー名-NSX Manager の管理ユーザー名。
  - c) Password - NSX Manager の管理者ユーザーのパスワード
4. 「NSX Manager が使用する Citrix ADM アカウント」 セクションで、NSX Manager の Citrix ADC ドライバパスワードを設定します。
5. [ **OK** ] をクリックします。

### NetScaler ADM でのライセンスのアップロード

NetScaler ADC VPX ライセンスを NetScaler ADM にアップロードすると、NSX とのオーケストレーション中に NetScaler ADM がインスタンスにライセンスを自動的に割り当てられるようにします。

**NetScaler ADM** にライセンスファイルをインストールするには:

1. Citrix ADM で、[ ネットワーク ] > [ ライセンス ] に移動します。
2. [ ライセンスファイル ] セクションで、次のいずれかのオプションを選択します。
  - a) ローカルコンピュータからのライセンスファイルのアップロード-ローカルコンピュータに ライセンスファイルがすでに存在する場合は、NetScaler ADM にアップロードできます。ライセンスファイルを追加するには、[ **Browse** ] をクリックし、追加するライセンスファイル (.lic) を選択します。次に、[ 完了 ] をクリックします。
  - b) ライセンスアクセスコードを使用する -購入したライセンスのライセンスアクセスコードを電子メールで送信します。ライセンスファイルを追加するには、テキストボックスにライセンスアクセスコードを入力し、[ **Get Licenses** ] をクリックします。

注:

[ ライセンス設定 ] から、いつでも NetScaler ADM にライセンスを追加できます。



License Server Port Settings

Proxy Server Port <b>0</b>	License Server Port <b>27000</b>
-------------------------------	-------------------------------------

License Files

You must upload the license files to this license server. If a license file is already present on your local computer, you can upload it to this license server, allocate licenses from the Citrix licensing portal.

Upload license files from a local computer  
 Use license access code

License Expiry Information

Feature	Count	Days To Expiry
<i>No items</i>		

## NetScaler ADM での NetScaler ADC VPX イメージのアップロード

NetScaler ADC イメージを NetScaler ADM に追加すると、NetScaler ADM がサービスパッケージで定義されているとおりにこれらのイメージを使用するようになります。

**Citrix ADC VPX** イメージを **Citrix ADM** にアップロードするには:

1. NetScaler ADM で、[オーケストレーション] > [SDN オーケストレーション] > [VMware NSX マネージャー] > [ESX NSVPX イメージ] に移動します。
2. [アップロード] をクリックし、ローカルストレージフォルダーから NetScaler ADC VPX zip パッケージを選択します。

## Citrix ADM でのサービスパッケージの作成

NetScaler ADM でサービスパッケージを作成して、NetScaler ADC リソースの割り当て方法を示す SLA のセットを定義します。

**Citrix ADM** でサービスパッケージを作成するには:

1. Citrix ADM で、[オーケストレーション] > [SDN オーケストレーション] > [VMware NSX Manager] > [サービスパッケージ] に移動し、[追加] をクリックして新しいサービスパッケージを追加します。
2. 「サービスパッケージ」ページの「基本設定」セクションで、次のパラメータを設定します。
  - a) Name - サービスパッケージの名前。
  - b) 隔離ポリシー- 「専用」を選択
  - c) Citrix ADC インスタンス Provisioning- 「インスタンスをオンデマンドで作成」を選択します

- d) 自動プロビジョニングプラットフォーム- **CitrixADC SDX** を選択
  - e) [**Continue**] をクリックします
3. [自動プロビジョニング設定] セクションで、最近アップロードした Citrix ADC VPX zip パッケージを選択して NSX プラットフォームにデプロイし、対応するライセンスを選択して、[続行] をクリックします。

注:

[高可用性] セクションで、NetScaler ADC インスタンスを高可用性用にプロビジョニングするチェックボックスをオンにします。

### Auto Provision Settings

---

#### Resources

Netscaler VPX Package for ESX\*

NSVPX-ESX-11.1-49.81\_nc.zip ▼

License\*

VPX8000\_Enterprise, 2number ▼

vCPUs\*

2

Memory in MB\*

2048

---

#### High Availability

A high availability (HA) deployment can provide uninterrupted operation

Provision pair of NetScaler appliances for High Availability.

Continue

Cancel

注

上記の図に示したリストボックスに表示されたライセンスの名前、VPX8000\_Advanced、2 番号の例を次に示します。

- VPX-ライセンスは NetScaler ADC VPX インスタンスを展開することです
- 8000 - 使用可能な帯域幅は 8GB です。
- 詳細-Citrix には、スタンダード、アドバンスト、プレミアムの 3 種類のライセンスが用意されています
- 2 番号-このライセンスを使用して 2 つの NetScaler ADC VPX インスタンスを展開可能

[ライセンス] リストボックスに表示されるライセンスの名前は、Citrix から購入したライセンスによって異なります。

4. [続行] をクリックします。
5. サービスパッケージが NSX Manager に公開されます。NSX Manager で、[サービス定義] > [\*\* サービスマネージャ \*\*] に移動します。Citrix ADM をサービスマネージャの 1 人と見なすことができます。これは、登録が成功し、NSX Manager と Citrix ADM 間で双方向通信が確立されたことを示しています。

注

: 高可用性展開の Citrix ADM では、ライセンスは Citrix ADM ライセンスサーバーノードにのみアップロードされます。NetScaler ADM ノードはアクティブ/パッシブモードです。

## Edge 向けのロードバランサーサービスの挿入の実行

既存の NSX Edge Gateway でロードバランサーサービスの挿入を実行します。つまり、NSX ロードバランサから NetScaler ADC に負荷分散機能をオフロードします。

**NSX Edge** ゲートウェイにロードバランシングサービスを挿入するには:

1. NSX Manager で、[ホーム] > [ネットワークとセキュリティ] > [NSX Edge] に移動し、設定した Edge ゲートウェイをダブルクリックして選択します。
2. [管理] をクリックし、[ロードバランサ] タブで [グローバル構成] を選択し、[編集] をクリックします。
3. [ロードバランサーを有効にする] と [サービス挿入を有効にする] を選択して有効にします。
4. サービス定義で、NSX Manager に公開されたサービスパッケージを選択します。
5. 管理インターフェイス用に 1 つの仮想 NIC を、データインターフェイス用に 1 つ以上の仮想 NIC を設定します。構成に応じて、管理用およびデータ用のネットワークを選択します。

注:

プライマリ IP 割り当てモードで IP プールオプションを選択します。Citrix ADM は、IP アドレスの手動割り当てまたは DHCP 割り当てをサポートしていません。

6. 更新アイコンをクリックすると、ランタイムの作成が表示されます。

注

: 高可用性デプロイでは 2 つの Citrix ADCVFX インスタンスをデプロイするため、NSX Manager には 2 つのランタイムが作成されます。

画面に表示される実行時間を確認するには、画面の更新が必要な場合があります。

7. ランタイムを選択し、「アクション」をクリックして、ポップアップメニューから「インストール」を選択します。高可用性展開であるため、同じことをもう 1 つのランタイムについても実行します。

8. 両方の仮想マシンが起動すると、[ステータス] の値が [サービス中] に変わり、[インストール状態] の値は [有効] に変わります。

注:

ステータスの変化を確認するには、画面の更新が必要な場合があります。

9. Citrix ADM で、[オーケストレーション] > [リクエスト] に移動して、サービス挿入完了の進行状況の詳細を確認します。ランタイムを作成および更新するリクエストが Citrix ADM に送信されたことがわかります。ランタイムが更新されたら、リクエストを選択して [タスク] ボタンをクリックすると、Citrix ADM が NSX Manager に追加されたことがわかります。

HA の場合、Citrix ADM で 2 つのランタイムを作成して更新するリクエストが 2 回送信されます。両方のランタイムが更新されたら、両方のリクエストを選択して [タスク] ボタンをクリックすると、NSX Manager に 2 つの Citrix ADM HA ノードが追加されたことがわかります。

10. Citrix ADM で、[オーケストレーション] > [SDN オーケストレーション] > [VMware NSX Manager] > [エッジゲートウェイ] に移動します。右側のパネルでは、Citrix ADC VPX が NSX Edge ゲートウェイに追加されていることを確認できます。

高可用性の場合、高可用性モードの 2 つの NetScaler ADC VPX インスタンスが NSX Edge Gateway に追加されていることがわかります。

11. Citrix ADM で、[ネットワーク] > [ライセンス] > [VPX ライセンス] に移動します。NetScaler ADC VPX ライセンスとインストールしたエディションを選択します。

高可用性モードの NetScaler ADC VPX インスタンスは 2 つのライセンスを消費し、ステータスは以下のよう  
に画面に表示されます。



サービスの挿入が完了したら、StyleBook を使用して、次のいずれかの方法で NetScaler ADC インスタンスを構成できます。

- VMware NSX Manager GUI での Citrix ADC VPX のロードバランシングサービスの設定
- NetScaler ADM GUI での NetScaler ADC VPX での負荷分散サービスの構成

### VMware NSX Manager GUI での Citrix ADC VPX のロードバランシングサービスの設定

組み込みの StyleBook を使用して NSX Edge ゲートウェイデバイスの負荷分散サービスの構成を有効化するには、以下のタスクを実行します。

NSX Manager で、[ホーム] > [ネットワークとセキュリティ] > [NSX Edge] に移動し、設定した Edge ゲートウェイをダブルクリックして選択します。

プールおよびプールメンバーの作成

キャパシティが異なるサーバーおよびメンバーで構成されたプールを作成します。

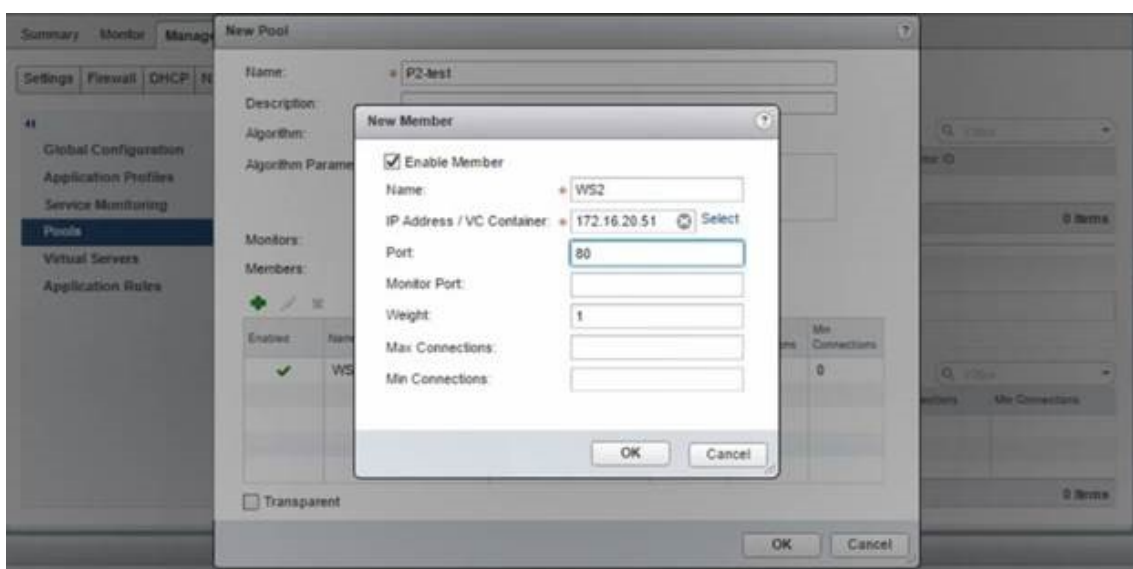
1. [管理] をクリックし、[ロードバランサー] タブで [プール] を選択し、[+] アイコンをクリックして新しいプールを追加し、次のパラメータを設定します。

a) Name - 新しいプールの名前。

- b) Algorithm - プールを選択するアルゴリズムをボックスの一覧から選択します。
- c) Monitors - サービスモニターを default\_http\_monitor に設定します。
- d) Members - [+] をクリックしてプールにメンバーを追加し、[New Member] ウィンドウで必須パラメーターを入力します。
  - i. Name - メンバーの名前。
  - ii. IP Address/ VC Container - [Select] をクリックして利用可能なオブジェクトの一覧からオブジェクトを選択するか、オブジェクトの IP アドレスを入力します。

2. [OK] をクリックします。

必要な数のメンバーを追加します。



## 仮想サーバーの作成

仮想サーバーのセットを作成し、各仮想サーバーにプールを割り当てます。

1. 「管理」をクリックし、「ロードバランサー」タブで「仮想サーバー」を選択し、「+」アイコンをクリックして仮想サーバーを追加し、次のパラメーターを設定します。
  - a) アプリケーションプロファイル-デフォルトでは、Citrix ADM で作成したサービスプロファイルが表示されます。
  - b) Name - 仮想サーバーの名前。
  - c) IP Address - [Select] をクリックして既存の IP アドレスのプールを選択するか、新しい IP のプールを作成します。
  - d) Default pool - ボックスの一覧でデフォルトのプールを選択します。

2. **[OK]** をクリックします。
3. NetScaler ADM で、[オーケストレーション] > [リクエスト] に移動して、選択した 1 つ以上の NetScaler ADC インスタンスでのサービス作成完了の進行状況の詳細を確認します。
4. NetScaler ADM で、[アプリケーション] > [構成] の順に選択し、**nsx-lb-mon** 構成パックが作成されたことを確認します。



## NetScaler ADM GUI での NetScaler ADC VPX での負荷分散サービスの構成

NetScaler ADM StyleBook を使用して、NetScaler ADC インスタンスにロードバランサー構成を展開します。HA の場合、構成は HA にある両方の Citrix ADC インスタンスにデプロイされます。

**StyleBooks** を使用して構成パックを作成するには：

1. Citrix ADM で、[アプリケーション] > [構成] > **[\*\* 新規作成]** に移動し、リストから [HTTP/SSL 負荷分散 (モニター付き)] StyleBook\*\* を選択します。StyleBook でユーザーインターフェイスページが表示されます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。
2. すべての必須パラメーターに対して値を指定します。
3. NSX 環境でプロビジョニングされているターゲットの Citrix ADC VPX インスタンスを選択し、「作成」をクリックして、選択したデバイスに構成を適用します。高可用性展開であるため、高可用性モードのインスタンスを選択します。

## Citrix ADC VPX インスタンスでの仮想サーバーとサービスグループの作成の検証

Citrix ADC VPX インスタンスにログインすると、サービスグループと仮想サーバーが作成されていることを確認できます。

サービスグループと仮想サーバを表示するには、次の手順で行います。

1. NetScaler ADC VPX インスタンスにログオンします。高可用性を導入するには、高可用性環境にある両方の Citrix ADC インスタンスにログオンする必要があります。
2. [構成] > [システム] > [ネットワーク] に移動します。右側のペインで、追加された IP アドレスを確認できます。IP アドレスのハイパーリンクをクリックして詳細を表示します。NSX に追加された Web インターフェイスの IP アドレスと同じサブネット IP アドレスが表示されます。

3. 次に、[トラフィック管理] > [負荷分散] > [仮想サーバー] に移動し、仮想サーバーの詳細を表示します。
4. 次に、サービスグループに移動して、サービスグループの詳細を表示します。
5. 最後に、[構成] > [システム] > [ライセンス] に移動し、このインスタンスに適用されているライセンスを表示します。

### 負荷分散サービスの削除

NSX Manager にデプロイされた NetScaler ADC VPX インスタンスで負荷分散サービスが不要になった場合は、以前に実行したサービスの挿入を削除できます。

構成とサービス挿入を削除するには：

1. Citrix ADM で、[アプリケーション] > [構成] に移動し、作成したアプリケーション構成を選択し、[X] アイコンをクリックして構成を削除します。
2. NSX Manager で、Citrix ADC VPX インスタンスが接続されているエッジゲートウェイに移動します。[\*\*管理] > [ロードバランサー] > [グローバル設定] に移動し、ランタイムエントリを右クリックして [プロビジョニング解除] をクリックします。\*\* 仮想マシンの表示が非稼働状態になります。
3. NetScaler ADM で、[オーケストレーション] > [クラウドオーケストレーション] > [エッジゲートウェイ] に移動します。削除されたインスタンスへの Edge ゲートウェイの対応するマッピングがないことを確認します。

## Cisco ACI ハイブリッドモードで NetScaler ADM を使用する NetScaler ADC オートメーション

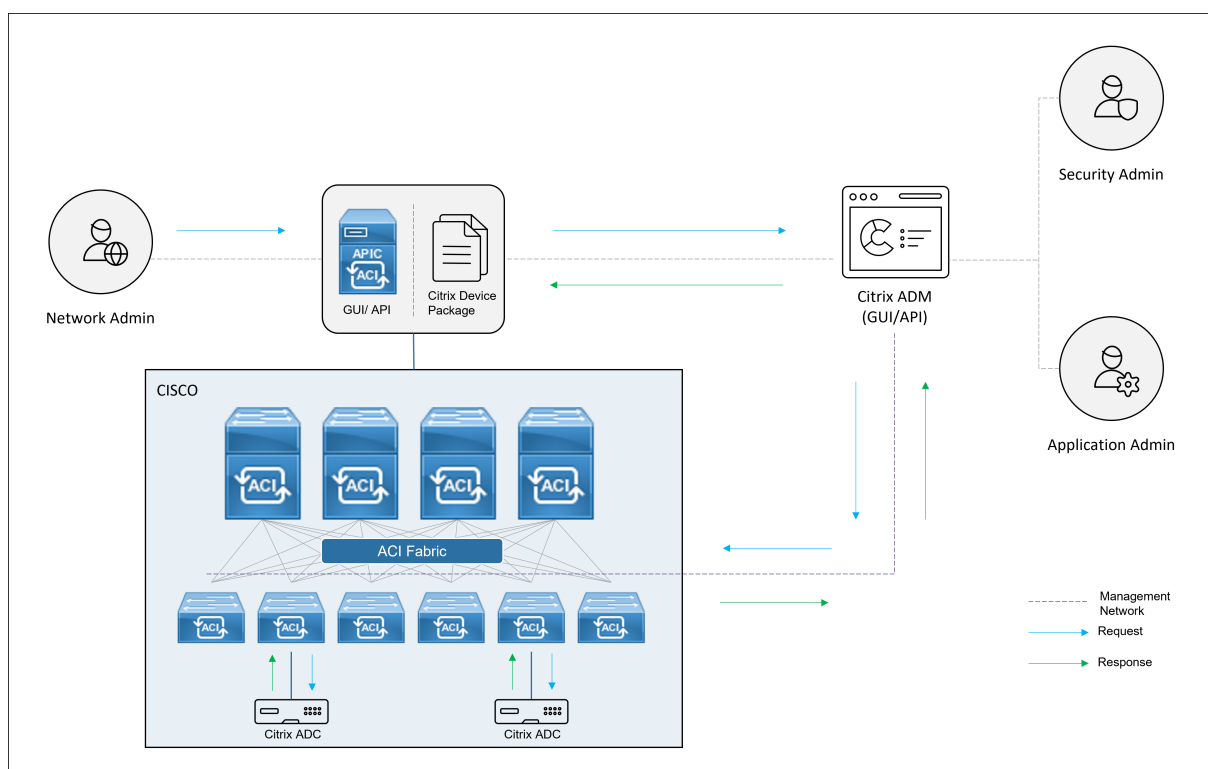
February 6, 2024

Cisco ACI では、バージョン 1.3 (2f) でハイブリッドモードのサポートが導入されています。ハイブリッドモードでは、アプリケーションポリシーインフラストラクチャコントローラー (APIC) を使用してネットワーク自動化を実行し、L4-L7 構成を APIC のデバイスマネージャーとして機能する Citrix Application Delivery Management (ADM) に委任できます。

Citrix ADC ハイブリッドモードソリューションは、ハイブリッドモードのデバイスパッケージと Citrix ADM でサポートされています。APIC のハイブリッドモードデバイスパッケージをアップロードする必要があります。このパッケージは、Citrix ADC のすべてのネットワーク L2-L3 構成可能なエンティティを提供します。アプリケーションパリティは、StyleBook によって Citrix ADM から APIC にマッピングされます。つまり、StyleBook は、特定のアプリケーションの L2~L3 構成および L4~L7 構成間の参照として機能します。APIC for Citrix ADC からネットワークエンティティを設定する際には、StyleBook 名を指定する必要があります。

次の図は、ハイブリッドモードソリューションにおける NetScaler ADC 概要を示しています。



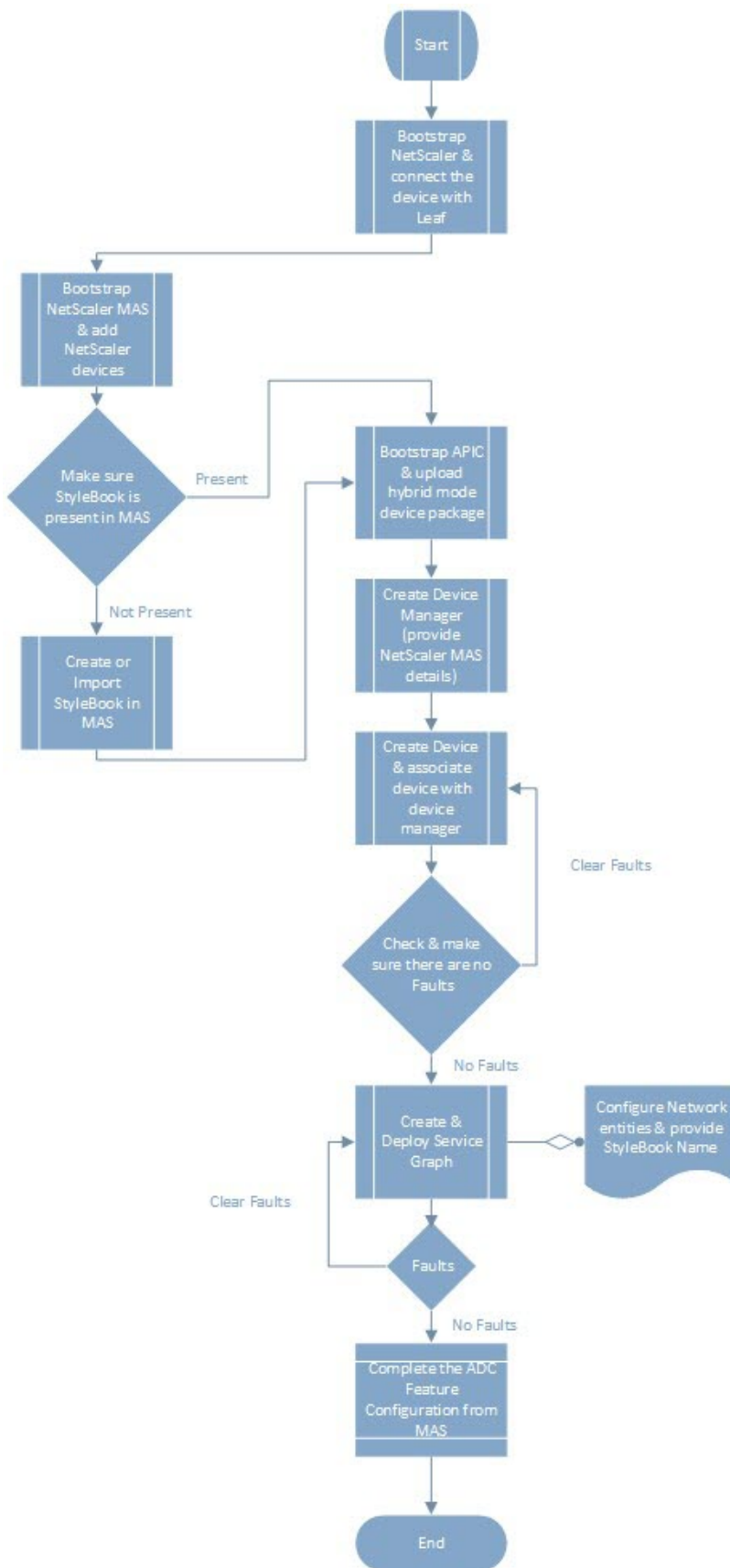


ハイブリッドモードでは、NetScaler ADC 構成は次の 2 つのフェーズで実行されます。

1. Cisco APIC からネットワーク切り替えを実行する。
2. 構成は Citrix ADM から行います

どのアプリケーションの場合も、ネットワーク管理者は、Cisco APIC でサービスグラフを作成および展開するときに、IP アドレス、ポート、VLAN (自動) などの特定の情報を指定する必要があります。これらの構成の詳細は、デバイスパッケージを介して Citrix ADM にプッシュされ、Citrix ADM がそれらを内部で処理して Citrix ADC を構成します。アプリケーション管理者は、Citrix ADM の StyleBook を使用してアプリケーションの ADC 関連の構成を作成し、これらの構成が Citrix ADM から Citrix ADC にプッシュされます。Cisco APIC と Citrix ADM は、管理ネットワークを介して ADC と通信します。

次の図は、ハイブリッドソリューションにおける NetScaler ADC ワークフローを示しています。



## 前提条件

February 6, 2024

以下の点を確認してください。

- Cisco ACI コンポーネントと NetScaler の概念知識があります。
  - Cisco ACI とそのコンポーネントの詳細については、次の URL にある製品マニュアルを参照してください。 <http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>
  - NetScaler ADC の詳細については、次の NetScaler ADC 製品ドキュメントを参照してください <http://docs.citrix.com/>。
- データセンターの Cisco APIC を含む、Cisco ACI のすべての必須コンポーネントのセットアップと構成が完了している。Cisco ACI とそのコンポーネントの詳細については、次の URL にある製品マニュアルを参照してください。 <http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>
- Citrix ADC 11.1 以降がインストールされています。
- Cisco ACI で Citrix ADC を設定して、Cisco APIC を使用して管理できるようにしました。
- 環境内に NetScaler Application Delivery Management (ADM) を展開しました。詳しくは、「[NetScaler ADM 13.0](#)」を参照してください。
- APIC から NetScaler ADM および ADC への管理接続が確立されます。
- また、次について書き留めておきます。
  - 管理およびデータパス接続に使用される接続インターフェイスと IP アドレス
  - リーフスイッチの詳細: Citrix ADC IP アドレス、ポート、インターフェイスなど。

### 注

このリリースでは、ハイブリッドモードソリューションは単一コンテキストで NetScaler ADC をサポートします。つまり、管理パーティションはサポートされていません。

## Cisco APIC および NetScaler ADM を使用して NetScaler ADC をハイブリッドモードで構成します

February 6, 2024

Cisco APIC と Citrix Application Delivery Management (ADM) を使用してハイブリッドモードで Citrix ADC を設定するには、次のタスクを実行します。

1. ファブリック内の NetScaler ADC インスタンスを NetScaler ADM に追加します。手順については、「[NetScaler ADM へのインスタンスの追加](#)」を参照してください。
2. NetScaler ADM を使用して、アプリケーションの StyleBook を作成します。手順については、「[NetScaler ADM を使用したアプリケーションの StyleBook の作成](#)」を参照してください。
3. NetScaler ADC ハイブリッドモードデバイスパッケージを Cisco APIC にインポートします。手順については、「[Citrix ADC ハイブリッドモードデバイスパッケージの Cisco APIC へのインポート](#)」を参照してください。
4. Cisco APIC で Device Manager として NetScaler ADM を追加します。手順については、「[Cisco APIC で Device Manager として NetScaler ADM を追加する](#)」を参照してください。
5. Cisco APIC を使用して、Cisco ACI に NetScaler ADC デバイスを追加します。手順については、「[Cisco ACI でデバイスとしての Citrix ADC の追加](#)」を参照してください。
6. サービスグラフテンプレートを作成して、展開します。手順については、「[サービスグラフの作成とデプロイ](#)」を参照してください。
7. NetScaler ADM で StyleBook を使用して L4-L7 パラメーターを構成します。手順については、「[NetScaler ADM の StyleBook を使用した L4-L7 パラメーターの構成](#)」を参照してください。
8. Cisco APIC のエンドポイントイベントが接続または接続解除されます。詳細については、「[APIC からのエンドポイントイベントのアタッチまたはデタッチ](#)」を参照してください。

## NetScaler ADM を使用したアプリケーションの StyleBook の作成

February 6, 2024

StyleBook は、あらゆるアプリケーションの Citrix ADC 構成を作成および管理するために使用できる構成テンプレートです。StyleBook を作成して、負荷分散、SSL オフロード、コンテンツスイッチなどの特定の Citrix ADC 機能を構成できます。StyleBook を設計することで、Microsoft Exchange や Microsoft Lync などのエンタープライズアプリケーション展開環境を構成できます。詳しくは、「[StyleBook](#)」を参照してください。

アプリケーション用に独自の StyleBook を作成することも、NetScaler Application Delivery Management (ADM) に付属の APIC-HTTP-LBStyleBook を変更して使用することもできます。

NetScaler ADM でアプリケーション用に独自の StyleBook を作成するには、「[独自の StyleBook を作成する方法](#)」を参照してください。

StyleBook を作成するときには、StyleBook の APIC サービスグラフモデルに従ってください。言い換えると、アプリケーションの APIC サービスグラフは、ADC 機能を介して接続されるコンシューマーモデルとプロバイダーモデルに従います。コンシューマーとプロバイダーは、エンドポイントグループ (EPG) として表され、1 対 1 の関係を

持ちます。StyleBook でも同じモデルに従う必要があります。つまり、プロバイダー EPG はサービスグループとして、各エンドポイントはサービスグループのメンバーとして表す必要があります。ADC 機能ノードは仮想サーバーによって表す必要があります（たとえば、負荷分散仮想サーバー）、仮想サーバーとサービスグループは 1 対 1 の関係である必要があります。

これは基本的にサービスグラフの本質をとらえるもので、これにより APIC に対するイベントの接続または接続解除を処理できます。接続イベントはエンドポイントに対応するサービスグループにバインドし、接続解除イベントはエンドポイントをバインド解除します。ネットワーク L2-L3 から ADC-feature L4-L7 構成へのシームレスな自動化を実現するには、サービスグラフと StyleBook が同等であることを確認する必要があります。

## NetScaler ADC ハイブリッドモードデバイスパッケージを Cisco APIC にインポート

February 6, 2024

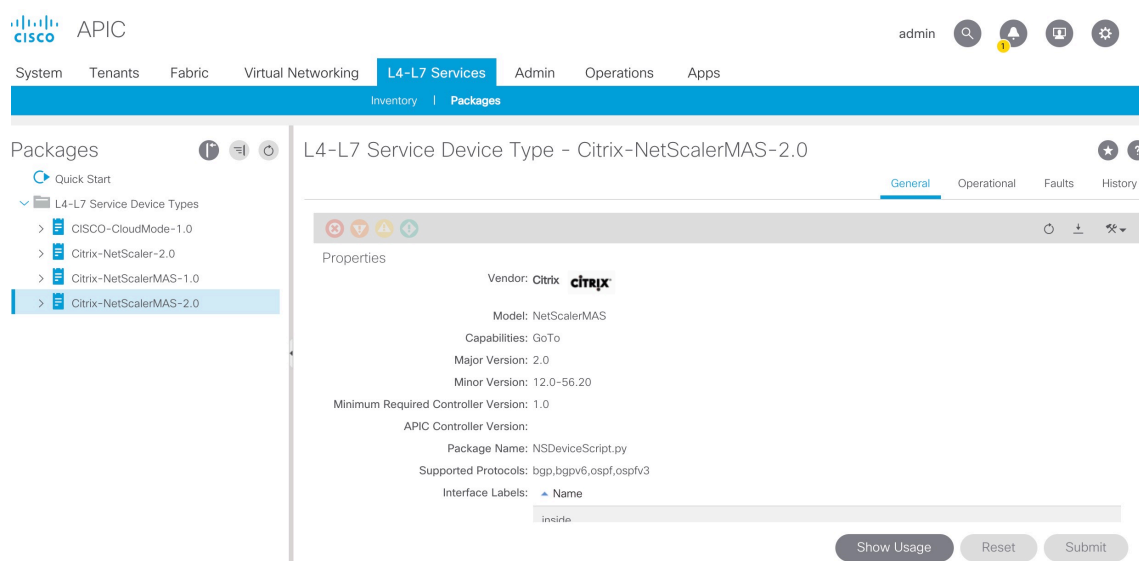
ハイブリッドモードのデバイスパッケージは、フルマネージモードと比べると軽量のパッケージです。このデバイスモデルで使用できるのは、L2-L3 ネットワークパラメーターのみです。デバイスモデルには、汎用 ADC 機能が 1 つだけ定義されており、ファブリック内の Citrix ADC の展開に基づく 4 つの機能プロファイル（たとえば、片腕と 2 腕、RHI と同じ）があります。ハイブリッドモードデバイスパッケージ名は、**NetScaler** ハイブリッドモードデバイスパッケージ **12.0** ビルド **56.20** です。[Citrix ダウンロードサイトでハイブリッドモードデバイスパッケージを検索してダウンロードし](#)、デバイスパッケージを APIC にインポートします。

### 注

ハイブリッドモードのデバイスパッケージは、フルマネージモードデバイスパッケージと混在させることができます。

**APIC GUI** を使用してハイブリッドモードのデバイスパッケージを **APIC** にインポートするには:

1. メニューバーの L4-L7 サービスタブをクリックし、パッケージパネルを選択します。
2. ナビゲーションペインで、**L4-L7** デバイスタイプを右クリックし、「デバイスパッケージのインポート \*\*」を選択します。
3. [デバイスパッケージのインポート] ダイアログボックスで、[参照] をクリックして、ダウンロードした Citrix ADC ハイブリッドモードのデバイスパッケージを選択します。
4. [**Submit**] をクリックします。  
デバイスパッケージが APIC に正常にインポートされたら、ナビゲーションペインでデバイス名をクリックしてデバイスパッケージの詳細を表示できます。



## 重要

デバイスパッケージをインポートしたら、APIC で問題が発生していないことを確認します。障害を表示するには、[Device Types] ウィンドウで **[Faults]** タブをクリックします。

## Cisco APIC の Device Manager として NetScaler ADM を追加します

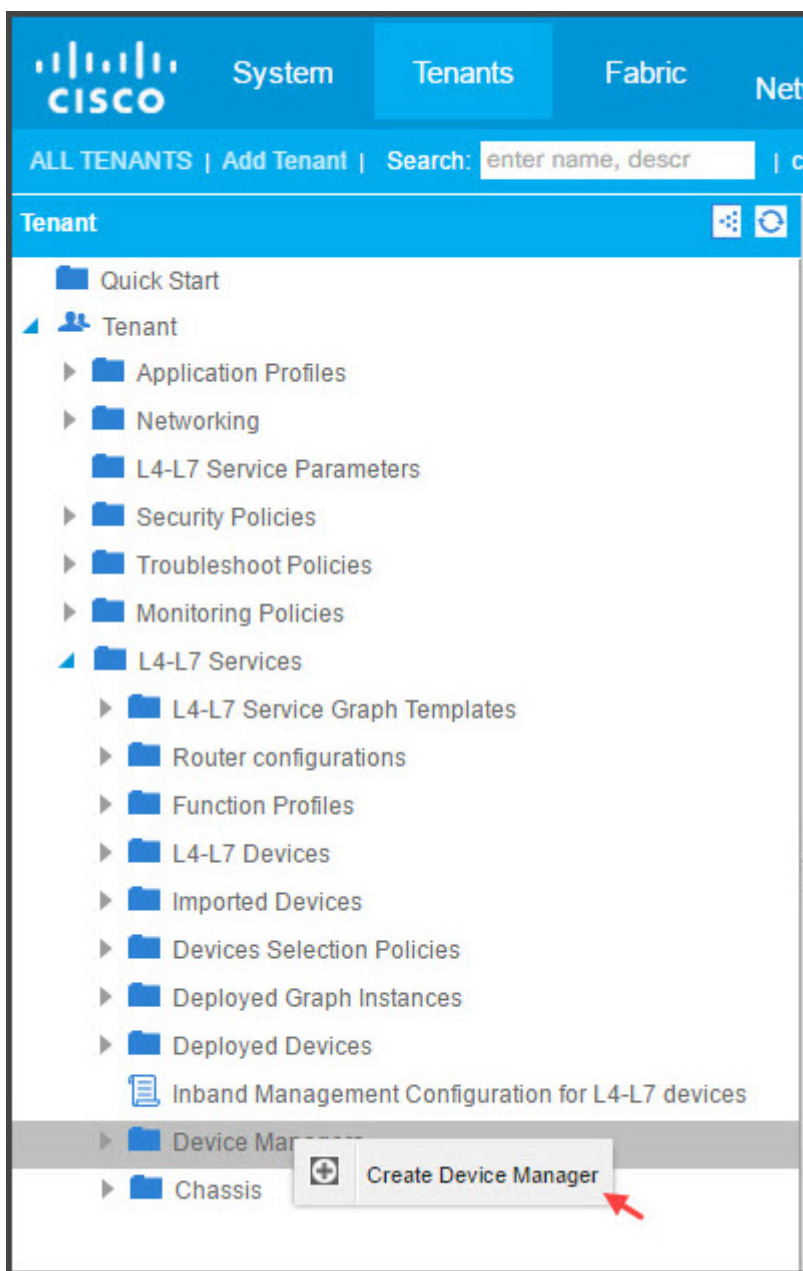
February 6, 2024

2018 年 5 月 24 日

Citrix Application Delivery Management (ADM) は、Cisco ACI に導入された Citrix ADC の一元化されたデバイスマネージャとして機能します。Citrix ADM をデバイスマネージャとして Cisco APIC に追加する必要があります。

**APIC GUI** を使用して **Citrix ADM** をデバイスマネージャとして **APIC** に追加するには:

1. メニューバーで [テナント] > [すべてのテナント] に移動します。
2. 作業ウィンドウで、テナントの名前をダブルクリックします。
3. ナビゲーションペインで、[\* テナント名 \*] > [L4-L7 サービス] を選択します。
4. [デバイスマネージャ] を右クリックし、[デバイスマネージャの作成] をクリックします。



5. [デバイスマネージャの作成] ダイアログボックスで、次の操作を行います。

- 「デバイスマネージャー名」フィールドに、デバイスマネージャーとして登録する Citrix ADM 展開の名前を入力します。
- [**Management EPG**] ボックスの一覧で、管理 EPG を選択します。
- [**Device Manager Type**] ボックスの一覧で、[**Citrix-DevMgr-1.0**] を選択します。
- [管理] フィールドで [+ ] をクリックし、Citrix ADM 展開の IP アドレスとポートの詳細を追加します。
- 「ユーザー名」フィールドに、Citrix ADM にアクセスするためのユーザー名を入力します。

- f) [パスワード] フィールドと [パスワードの確認] フィールドに、Citrix ADM にアクセスするためのパスワードを入力します。
- g) **[SUBMIT]** をクリックします。

**Create Device Manager**

Please enter device manager info below.

Device Manager Name:

Management EPG:  This is required only for inband management.

Device Manager Type:

Management

Host	Port
10.102.102.21	80

Username:

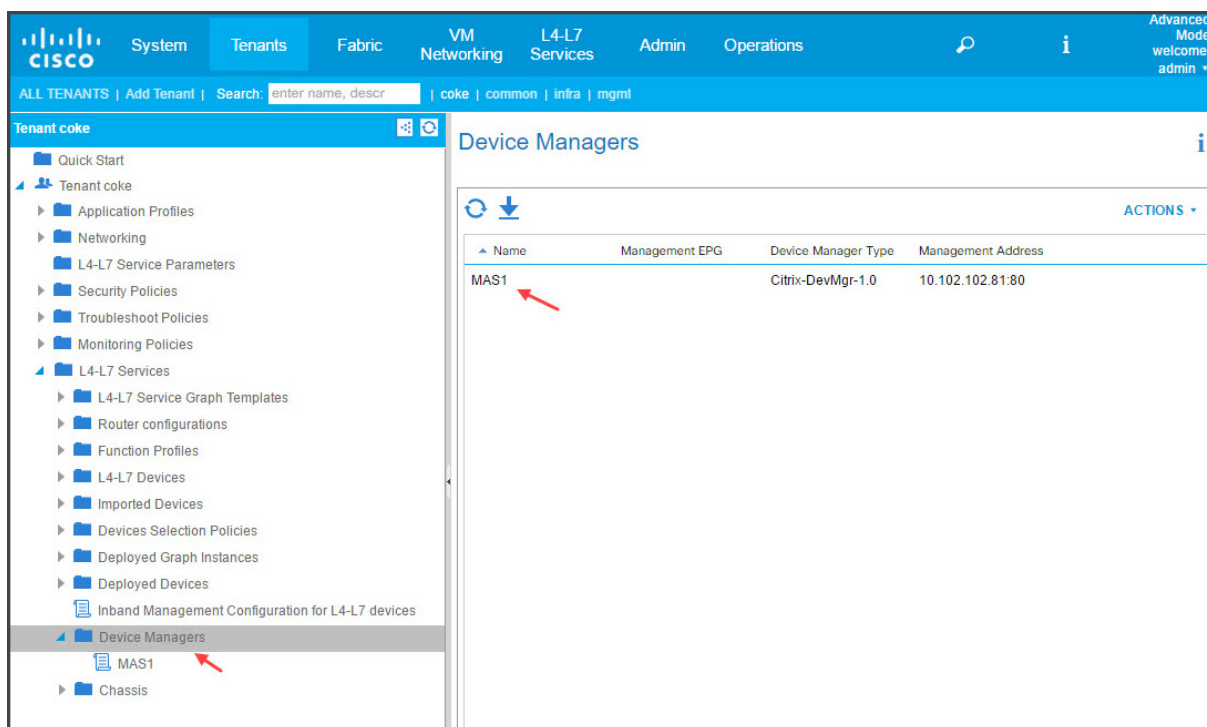
Password:

Confirm Password:

**SUBMIT** **CANCEL**

Citrix ADM がデバイスマネージャとして APIC に正常に登録されると、デバイスマネージャが追加され、ナビゲーションペインに表示されます。登録済みのデバイスマネージャを表示するには、ナビゲーションペインで [**\*tenant\_name\***] > [L4-L7 サービス] > [デバイスマネージャ] に移動します。





注

Cisco APIC と Citrix ADM の間に接続上の問題がないことと、Citrix ADM へのアクセスに使用するのと同じ認証情報を入力していることを確認してください。また、アカウントに管理者権限があることも確認します。

重要

デバイスパッケージをインポートしたら、APIC で問題が発生していないことを確認します。障害を表示するには、[Device Types] ウィンドウで **[Faults]** タブをクリックします。

API を使用して Citrix ADM をデバイスマネージャーとして登録することもできます。次に、API を使用して NetScaler ADM をデバイスマネージャーとして追加する方法を示す XML ペイロードのサンプルを示します。

```

1 <polUni>
2   <fvTenant name="coke">
3     <vnsDevMgr name="MAS1">
4       <vnsRsDevMgrToMDevMgr tDn="uni/infra/mDevMgr-Citrix-DevMgr
-1.0" />
5       <vnsCMgmts name="devMgmt" host="10.102.102.81" port="80"/>
6       <vnsCCred name="username" value="nsroot"/>
7       <vnsCCredSecret name="password" value="*****"/>
8     </vnsDevMgr>
9   </fvTenant>
10 </polUni>

```

## APIC を使用して Cisco ACI にデバイスとして NetScaler ADC を追加します

February 6, 2024

ネットワークを自動化するには、Citrix ADC を L4-L7 デバイスとして APIC に追加する必要があります。APIC は、デプロイされたサービスグラフに基づいて、リーフと Citrix ADC デバイス間のネットワークステッチを実行します。更新管理 IP アドレス、デバイスマネージャー、資格情報など、デバイス構成の基本設定を行う必要があります。

**APIC GUI** を使用して **Citrix ADC** を **APIC** のデバイスとして登録するには:

1. メニューバーで [テナント] > [すべてのテナント] に移動します。
  2. 作業ウィンドウで、テナントの名前をダブルクリックします。
  3. ナビゲーションペインで、\* テナント名 \* > **L4-L7** サービス > **L4-L7** デバイスを選択します。
  4. 作業ペインで、[アクション] > [**L4-L7** デバイスの作成] を選択します。
  5. **L4-L7** デバイスの作成ダイアログボックスの「一般」セクションで、次の操作を行います。
    - a) 「管理対象」チェックボックスを選択します。
    - b) 「名前」フィールドに、デバイスの名前を入力します。
    - c) [**Service Type**] ボックスの一覧で、[**ADC**] を選択します。
    - d) [**Device Type**] フィールドで、[**Physical**] を選択します。
- 注:
- VMware ESX の場合は、必ず [仮想] を選択し、それぞれの仮想マシンマネージャ (VMM) ドメインを関連付けてください。
- e) [**Physical Domain**] ボックスの一覧で、物理ドメインを選択します。
  - f) [モード] フィールドで、要件に応じて [シングルノード] または [**HA** クラスター] を選択します。
  - g) デバイスパッケージドロップダウンリストで、**Citrix-NetScalerMAS-1.0** を選択します。
  - h) 「モデル」ドロップダウンリストで、デバイスモデルを選択します。たとえば、Citrix ADC-MPX、または Citrix ADC-VPX。
6. [接続] セクションの [**APIC** からデバイス管理への接続] フィールドで、Citrix **ADC** がファブリック内でどのように設定されているかに応じて、[アウトオブバンド] または [インバンド] を選択します。
7. 認証情報セクションで、デバイスにアクセスするためのユーザー名とパスワードを指定します。
8. 「デバイス **1**」セクションと「デバイス **2**」セクションで、それぞれ管理関連の設定を完了します。

9. [ **Cluster** ] セクションで、クラスタの管理関連の設定を完了します。[ **Device Manager** ] ドロップダウンリストで、「Cisco APIC での Device Manager としての NetScaler ADM の追加」で作成したデバイスマネージャを選択していることを確認します。

STEP 1 > General

1. General 2. Device Configuration

Please select device package and enter connectivity information.

**General**

Managed:

Name: ADCCluster

Service Type: ADC

Device Type: PHYSICAL VIRTUAL

Physical Domain: phys

Mode:  Single Node  HA Cluster

Device Package: Citrix-NetScalerMAS-1.0

Model: NetScaler-SDXContext

**Connectivity**

APIC to Device:  Out-Of-Band

Management Connectivity:  In-Band

**Credentials**

Username: nsroot

Password: .....

Confirm Password: .....

**Device 1**

Management IP Address: 10.102.102.62 Management Port: http

Chassis: select a value

Device Interfaces:

Name	Path
0_1	Node-101/eth1/12
0_2	Node-101/eth1/14

**Device 2**

Management IP Address: 10.102.102.63 Management Port: http

Chassis: select a value

Device Interfaces:

Name	Path
0_1	Node-101/eth1/19
0_2	Node-101/eth1/20

**Cluster**

Management IP Address: 10.102.102.62 Management Port: http

Device Manager: coke/MAS1

Cluster Interfaces:

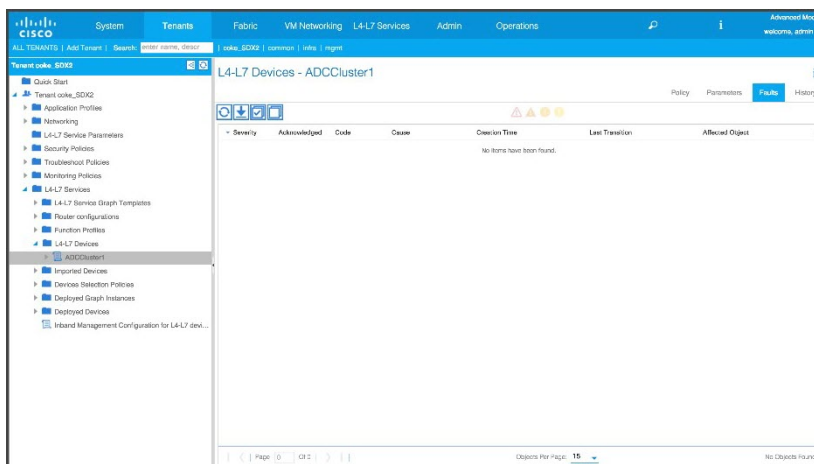
Type	Name	Concrete Interfaces
------	------	---------------------

PREVIOUS NEXT CANCEL

10. [ 次へ ] をクリックします。[ Device Configuration ] ページが開きます。ハイブリッドモードデバイスのパッケージには、高可用性、機能とモードの有効化/無効化、NTP、SNMP、SNMP アラームなど、デバイスおよびクラスター固有の詳細な構成は用意されていません。これらの構成は、Citrix ADM を使用して行う必要があります。
11. 「完了」をクリックします。APIC へのデバイスの登録に成功すると、そのデバイスが追加され、ナビゲーションペインに表示されます。登録されたデバイスを表示するには、ナビゲーションペインで [ \*tenant\_name\* ] > [ L4-L7 サービス ] > [ L4-L7 デバイス ] > [ device\_name ] に移動します。

#### 重要

デバイスを登録したら、APIC で問題が発生していないことを確認します。障害を確認するには、作業ペインの [ 障害 ] タブをクリックします。



API を使用して Citrix ADC デバイスを登録することもできます。以下に、L4-L7 デバイスを追加するための XML ペイロードの例を示します。

```

1  <polUni>
2
3      <fvTenant name="coke">
4
5          <vnsLDevVipname="ADCCluster1"funcType="GoTo" svcType="ADC">
6
7              <vnsRsMDevAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0" />
8
9              <vnsRsALDevToPhysDomP tDn="uni/phys-phys"/>
10
11             <vnsCMgmt name="devMgmt"host="10.102.102.67"port="80"/>
12
13             <vnsCCred name="username" value="nsroot"/>
14
15             <vnsCCredSecret name="password" value="****"/>
16
17             <vnsRsALDevToDevMgr tnVnsDevMgrName="MAS1"/>
18
19             <vnsCDev name="ADC1" devCtxLbl="C1">
20
21                 <vnsCIIf name="1_1">
22
23                     <vnsRsCIIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
24                         /33]"/>
25
26                 </vnsCIIf>
27
28                 <vnsCIIf name="1_2">
29
30                     <vnsRsCIIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
31                         /35]"/>
32
33                 </vnsCIIf>
34
35             <vnsCMgmt name="devMgmt" host="10.102.102.65" port="80"/>

```

```
34
35     <vnsCCred name="username" value="nsroot"/>
36
37     <vnsCCredSecret name="password" value="****"/>
38
39 </vnsCDev>
40
41 <vnsCDev name="ADC2" devCtxLbl="C1">
42
43     <vnsCIIf name="1_1">
44
45         <vnsRsCIIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
46             /34]"/>
47     </vnsCIIf>
48
49     <vnsCIIf name="1_2">
50
51         <vnsRsCIIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
52             /36]"/>
53     </vnsCIIf>
54
55     <vnsCMgmt name="devMgmt" host="10.102.102.66" port="80"/>
56
57     <vnsCCred name="username" value="nsroot"/>
58
59     <vnsCCredSecret name="password" value="****"/>
60
61 </vnsCDev>
62
63 <vnsLIIf name="outside">
64
65     <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
66         mIfLbl-outside"/>
67
68     <vnsRsCIIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
69         cIf-1_1"/>
70
71     <vnsRsCIIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
72         cIf-1_1"/>
73 </vnsLIIf>
74
75 <vnsLIIf name="inside">
76
77     <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
78         mIfLbl-inside"/>
79
80     <vnsRsCIIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
81         cIf-1_2"/>
82
83     <vnsRsCIIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
```

```
80         cIf-1_2"/>
81     </vnsLIIf>
82
83     </vnsLDevV
84
85     </fvTenant>
86
87     </polUni>
```

## サービスグラフの作成とデプロイ

February 6, 2024

Citrix ADC を作成してデプロイするには、APIC の Cisco APIC サービスグラフテンプレートを使用する必要があります。サービスグラフを作成および展開する場合、必ず ADC 機能プロファイルを使用してください。

APIC でグラフを構成すると、機能定義、デバイスのファブリックへの接続、グラフ展開環境の一部として設定されたエンティティに基づき、APIC により自動的にデバイスが構成されます。VLAN の割り当てとバインドなどのネットワーク構成も、サービスグラフの作成処理の一部として APIC により自動的に行われます。また、APIC からグラフを削除すると、構成も削除されます。

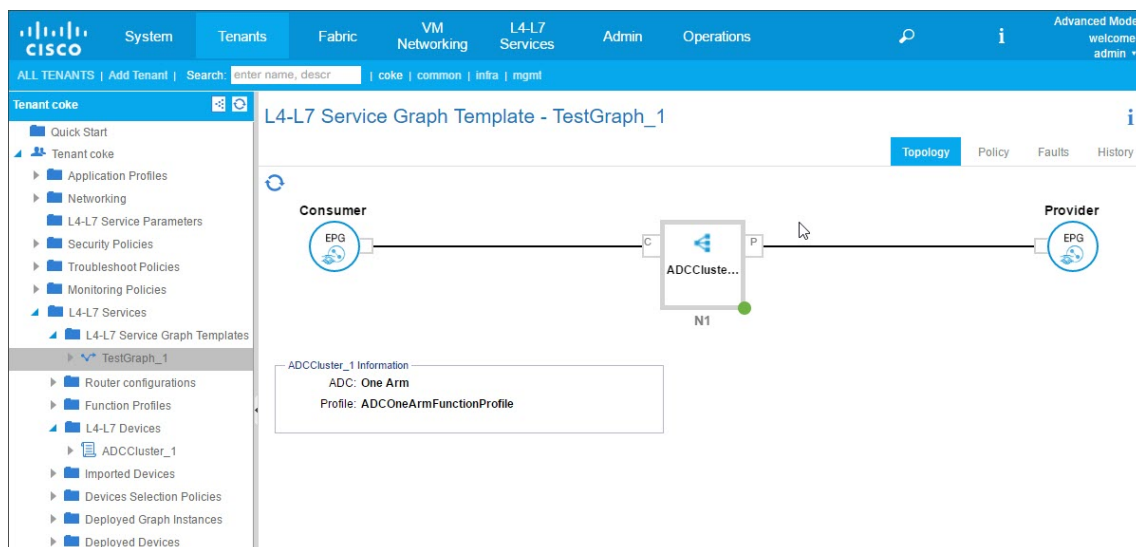
サービスグラフは、間に適切なサービス機能が挿入された 2 つ以上のアプリケーション階層によって表されます。サービスグラフは、契約により、送信元 EPG と送信先 EPG の間に挿入されます。

**APIC GUI** を使用してサービスグラフを作成するには:

1. メニューバーで [テナント] > [すべてのテナント] に移動します。
2. 作業ウィンドウで、テナントの名前をダブルクリックします。
3. ナビゲーションペインで、**\*tenant\_name\*** > **L4-L7 サービス** > **L4-L7 サービスグラフテンプレート** を選択します。
4. 作業ペインで、[アクション] > [**L4-L7 サービスグラフテンプレートの作成**] を選択します。
5. [**L4-L7 サービスグラフテンプレートの作成**] ダイアログボックスの [デバイスクラスタ] セクションで、デバイスクラスタを選択し、次の操作を行います。
  - a) [**Graph Name**] ボックスに、サービスグラフテンプレートの名前を入力します。
  - b) [**Graph Type**] フィールドで、[**Create A New One**] を選択します。
  - c) [**Device Cluster**] セクションからデバイスをドラッグし、コンシューマーエンドポイントグループとプロバイダーエンドポイントグループの間にドロップしてサービスノードを作成します。



ンバウンドトラフィックおよびアウトバウンドトラフィックに使用される個別のインターフェイスにバインドされます。



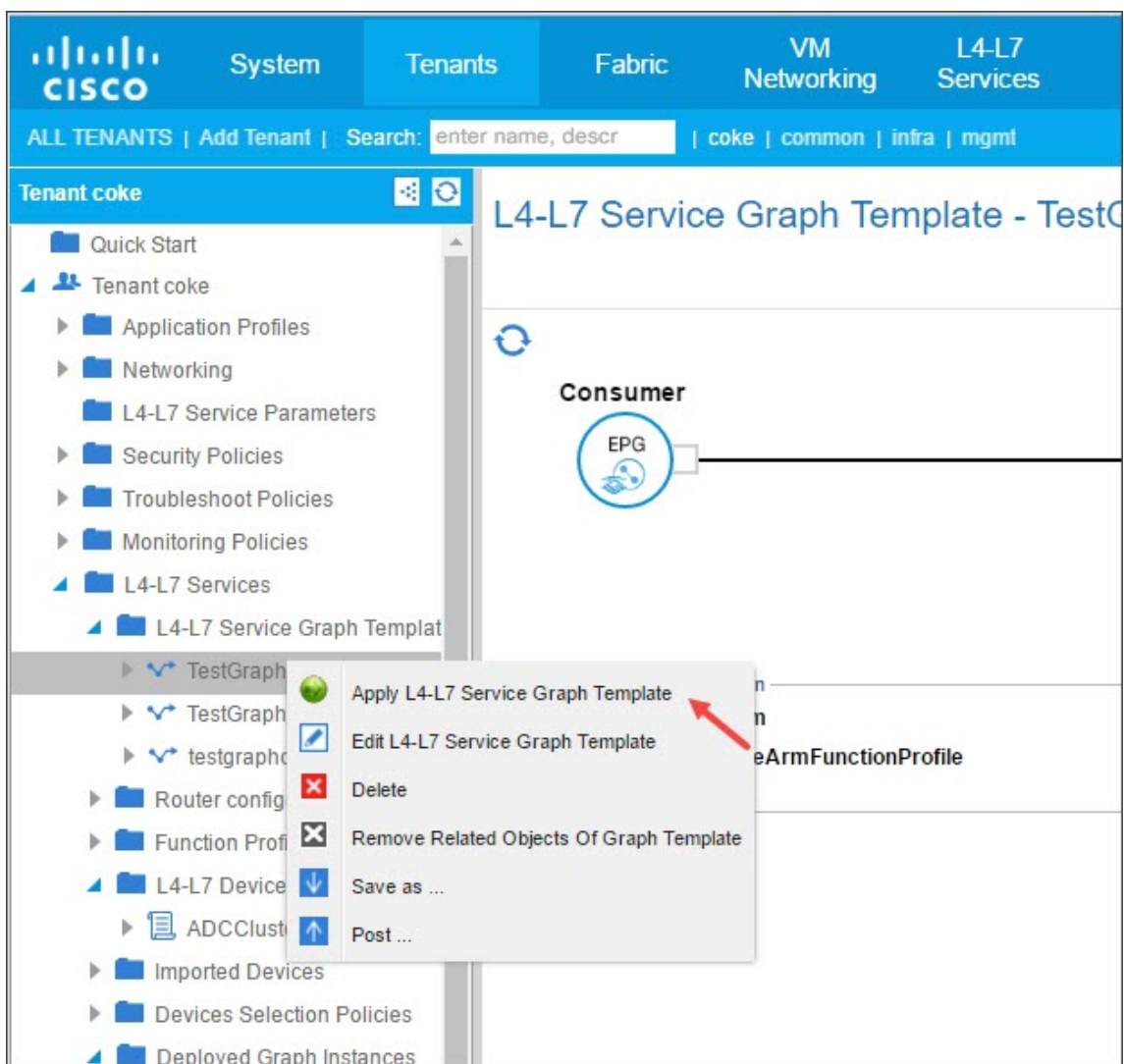
## サービスグラフテンプレートのエンドポイントグループへの適用

作成したサービスグラフテンプレートは、APIC GUI を使用して適用する必要があります。

サービスグラフテンプレートを適用するには:

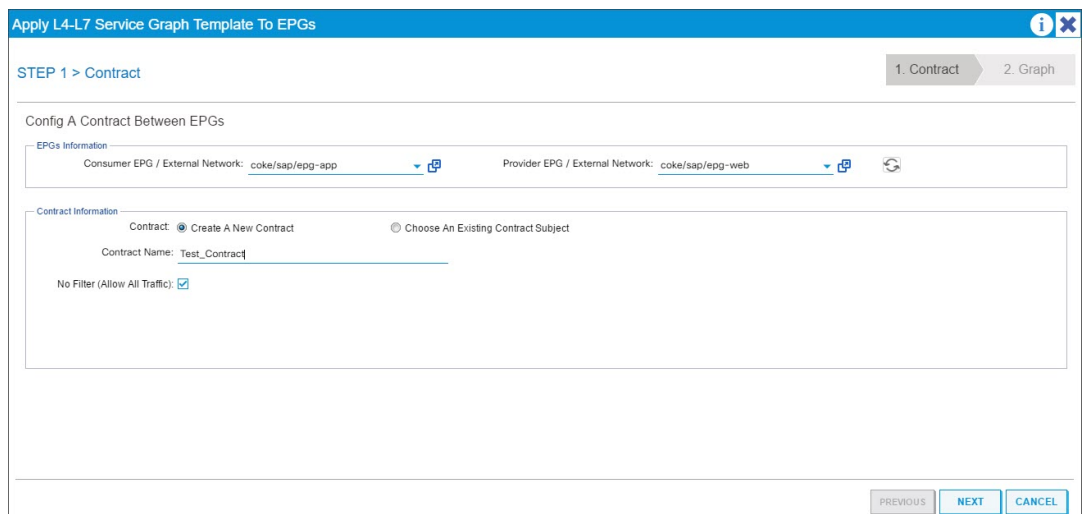
1. メニューバーで [テナント] > [すべてのテナント] に移動します。
2. 作業ウィンドウで、テナントの名前をダブルクリックします。
3. ナビゲーションペインで、 **\*tenant\_name\*** > **L4-L7 サービス** > **L4-L7 サービスグラフテンプレート** を選択します。
4. **template\_name** を右クリックして、「**L4-L7 サービスグラフテンプレートを適用**」をクリックします。





5. 「**L4-L7 サービスグラフテンプレートを EPG に適用**」ダイアログボックスの「**EPG 情報**」セクションで、次のフィールドに値を入力します。

- a) [**Consumer EPG/External Network**] ボックスの一覧で、コンシューマーエンドポイントグループを選択します。
- b) [**Provider EPG/External Network**] ボックスの一覧で、提供されているエンドポイントグループを選択します。
- c) [**Contract Information**] セクションで、適切なボックスに入力します。契約情報は、Cisco APIC に固有の情報であり、EPG に関連付けられたセキュリティポリシーの一部として構成されます。



d) [次へ] をクリックします。

e) 「グラフテンプレート」ドロップダウンリストで、作成したサービスグラフテンプレートを選択します。

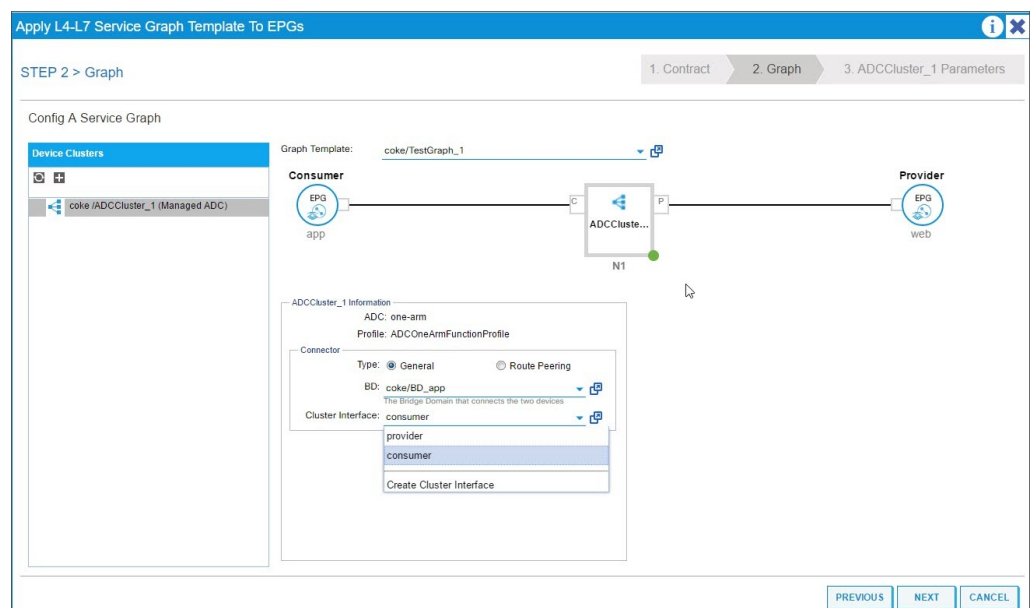
f) コネクタセクションで、次の操作を行います。

i. 「タイプ」フィールドで「一般」を選択します。

ii. **BD** ドロップダウンリストで、ブリッジドメインを選択します。コネクタの詳細はブリッジドメインの一部であり、ブリッジドメインは Cisco APIC インフラストラクチャモデルの一部です。

iii. **[Cluster Interface]** ボックスの一覧で、選択したブリッジドメインの適切なクラスターインターフェイスを選択します。

Cisco APIC は、選択したサービスグラフテンプレートの要件に応じて、Citrix ADC デバイスとファブリック間のデータパストラフィックに選択したブリッジドメインを使用します。

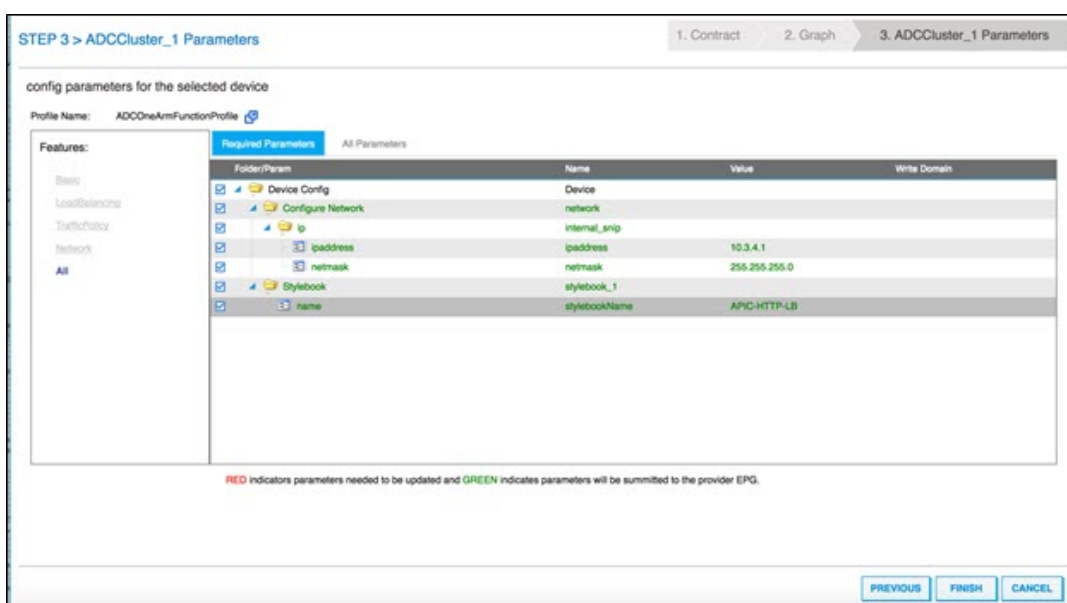


iv. [次へ] をクリックします。

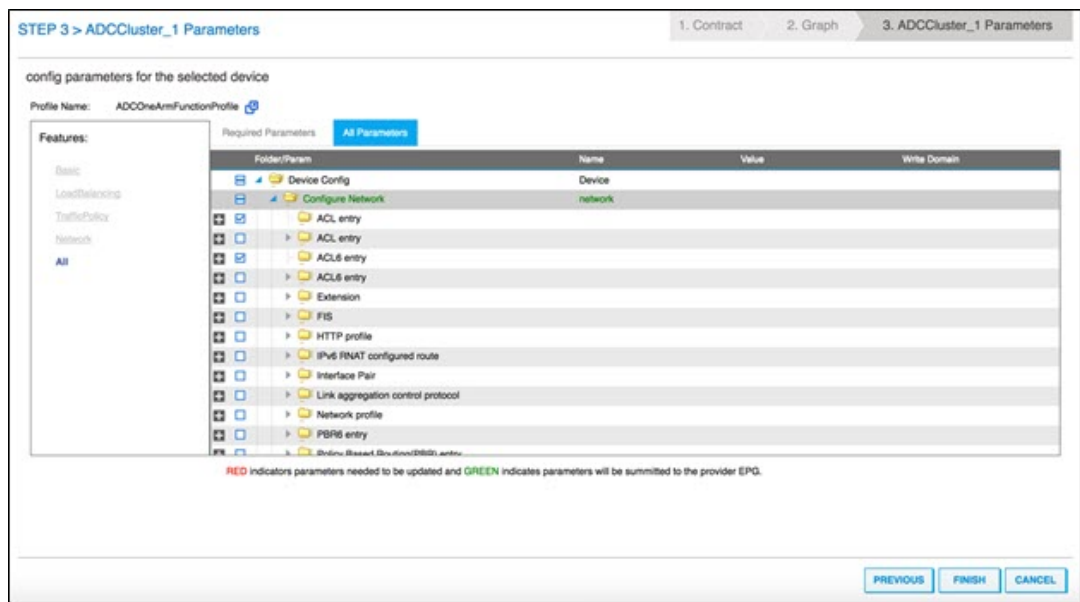
[パラメータ] 画面の [必須パラメータ] タブに、プロファイルで指定されている IP アドレスなど、L2-L3 固有の詳細を入力します。その他の主要パラメータとして StyleBook 名があります。NetScaler Application Delivery Management (ADM) で提供される組み込みの StyleBook **APIC-HTTP-LB**、または NetScaler ADM を使用したアプリケーションの StyleBook の作成で作成した StyleBook の名前を指定できます。

注

StyleBook の名前は、サービスグラフの詳細を、特定のアプリケーション用に Citrix ADM で作成された L4-L7 構成にリンクします。



Cisco APIC GUI を使用すると、機能（たとえば、負荷分散）に基づいてパラメーターを絞り込むことができます。すべての必須パラメーターを確認および設定するには [Required Parameters] タブを、特定の機能に関連する、その他のすべてのパラメーターを確認および設定するには [All Parameters] タブを使用します。



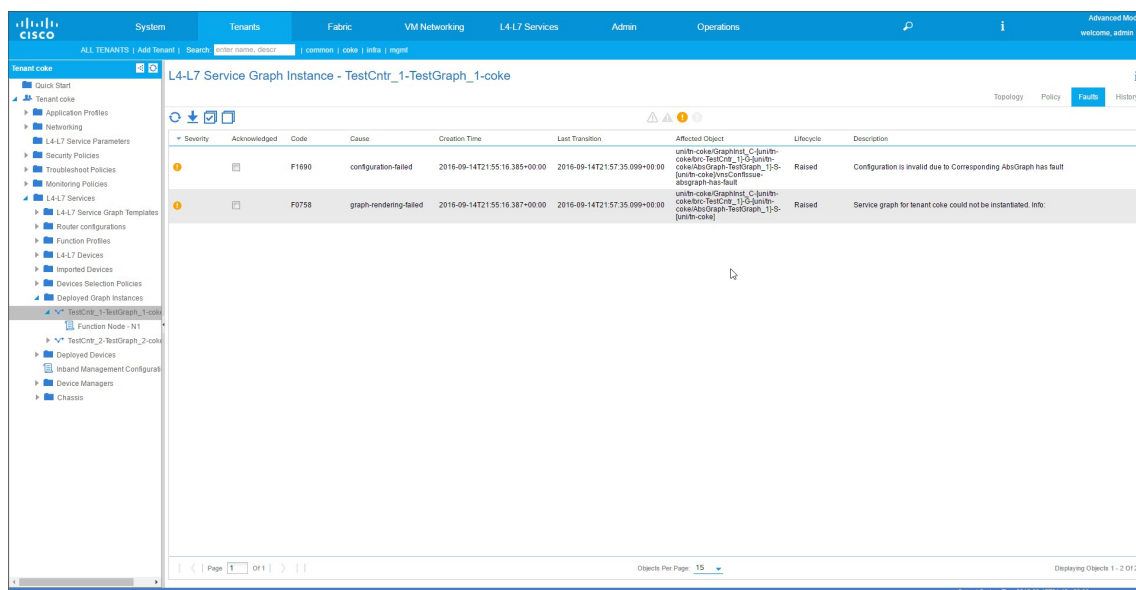
注

デフォルトでは、組み込みのワンアームプロファイルで SNIP の詳細（IP アドレスやネットマスクなど）を指定する必要があります。その他のネットワークパラメーターを確認するには、**[All Parameters]** をクリックして、Cisco APIC GUI で **[Configure Network]** ツリーを展開します。これには、Citrix ADC でサポートされているすべてのネットワークパラメーターが一覧表示されます。Cisco APIC GUI から任意のエントティティをインスタンス化して、リスト表示された各属性の値を指定できます。

6. **[完了]** をクリックします。

重要

サービスグラフテンプレートを適用したら、展開したグラフに問題がないことを確認してください。障害を確認するには、作業ペインの **[障害]** タブをクリックします。



サービスグラフの導入の一環として、ハイブリッドモードデバイスパッケージは構成の詳細を Cisco APIC から Citrix ADM にプッシュします。Citrix ADM はこれらの構成をそれぞれの Citrix ADC に内部的に処理し、応答を APIC に返します。グラフの展開が成功しても障害は発生せず、Citrix ADC は対応するグラフのファブリックと正常にネットワーク化されます。

APIC では、API を使用してグラフを構成および展開するためのさまざまな方法を用意しています。グラフの展開には、一部の APIC 固有の構造体（テナント、契約、VLAN、名前空間など）に対するさまざまな依存関係が含まれています。

次のアプローチ例は、APIC の API を使用して L4-L7 グラフを作成および展開する方法の 1 つを示しています。この例では、APIC 固有のアーティファクトが APIC 内に既に設定されているものとします。

**重要**

ここに示した XML ペイロードは参考用です。本番環境でこれらのペイロードを使用する場合は、事前に XML を適宜変更するようにしてください。

以下に、API を使用して、サービスグラフを作成および展開する例を示します。

- a) AppProfile の作成
- b) サービスグラフの詳細部分の作成
- c) 契約へのサービスグラフの接続

以下に、AppProfile を作成するための XML ペイロードの例を示します。AppProfile には EPG が含まれ、プロバイダー EPG には Citrix ADC 固有のエンティティ、属性、およびそれらの値が含まれます。次のサンプル XML ペイロードでは、NSIP などの Citrix ADC 固有のネットワークエンティティが、一連の属性と StyleBook 名を使用して作成されます。

```
1 <polUni>
```

```

2   <fvTenant name="coke">
3     <!-- Application Profile -->
4     <fvAp dn="uni/tn-coke/ap-sap" name="sap">
5       <!-- EPG 1 -->
6       <fvAEPg dn="uni/tn-coke/ap-sap/epg-web" name="web">
7         <fvRsBd tnFvBDName="BD_web" />
8         <!-- ----- CONFIG PAYLOAD ----- -->
9         <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Network" name=
"Network">
10          <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="
snip1">
11            <vnsParamInst key="ipaddress" name="ip1"
value="110.110.110.2"/>
12            <vnsParamInst key="netmask" name="netmask1
" value="255.255.255.0"/>
13            <vnsParamInst key="type" name="tye" value=
"SNIP"/>
14            <vnsParamInst key="dynamicrouting" name="
dynamicrouting" value="DISABLED"/>
15            <vnsParamInst key="hostroute" name="
hostroute" value="DISABLED"/>
16          </vnsFolderInst>
17          <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="
snip2">
18            <vnsParamInst key="ipaddress" name="ip2"
value="220.220.220.2"/>
19            <vnsParamInst key="netmask" name="netmask2
" value="255.255.255.0"/>
20            <vnsParamInst key="type" name="tye" value=
"SNIP"/>
21            <vnsParamInst key="dynamicrouting" name="
dynamicrouting" value="DISABLED"/>
22            <vnsParamInst key="hostroute" name="
hostroute" value="DISABLED"/>
23          </vnsFolderInst>
24        </vnsFolderInst>
25        <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Stylebook"
name="stylebook_1">
26          <vnsParamInst name="stylebookName" key="name"
value="APIC-HTTP-LB"/>
27        </vnsFolderInst>
28        <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="
internal_network" name="internal_network">
29          <vnsCfgRelInst name="internal_network_key" key
="internal_network_key" targetName="Network/snip1"/>
30        </vnsFolderInst>
31        <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="

```

```

external_network" name="external_network">
32     <vnsCfgRelInst name="external_network_key" key
="external_network_key" targetName="Network/snip2"/>
33     </vnsFolderInst>
34     <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="mFCngStylebook
" name="mFCngStylebook_1">
35         <vnsCfgRelInst name="Stylebook_key" key="
Stylebook_key" targetName="stylebook_1"/>
36         </vnsFolderInst>
37         <!-- ----- END CONFIG PAYLOAD ----- -->
38         <fvSubnet ip="110.110.110.110/24" scope="shared"/>
39         <fvRsProv tnVzBrCPName="Ctrct1"></fvRsProv>
40         <fvRsDomAtt tDn="uni/phys-sepg" />
41         <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
-[eth1/38]" encap="vlan-3703" instrImedcy="immediate"/>
42         </fvAEPg>
43         <!-- EPG 2 -->
44         <fvAEPg dn="uni/tn-coke/ap-sap/epg-app" name="app">
45             <fvRsCons tnVzBrCPName="Ctrct1"/>
46             <fvRsBd tnFvBDName="BD_app" />
47             <fvSubnet ip="220.220.220.220/24" scope="shared"/>
48             <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
-[eth1/37]" encap="vlan-3704" instrImedcy="immediate"/>
49             <fvRsDomAtt tDn="uni/phys-sepg" />
50         </fvAEPg>
51     </fvAp>
52 </fvTenant>
53 </polUni>
54 <!--NeedCopy-->

```

以下に、サービスグラフの詳細を作成するためのXML ペイロードの例を示します。

```

1 <polUni>
2   <fvTenant name="coke">
3     <vnsAbsGraph name = "Graph1">
4       <vnsAbsTermNodeProv name = "Input1">
5         <vnsAbsTermConn name = "C1"></vnsAbsTermConn>
6       </vnsAbsTermNodeProv>
7       <vnsAbsNode name="ADC" funcType="GoTo">
8         <vnsAbsFuncConn name = "outside" attNotify="true">
9           <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-
NetScalerMAS-1.0/mFunc-ADCFunction/mConn-external" />
10          </vnsAbsFuncConn>
11          <vnsAbsFuncConn name = "inside" attNotify="true">
12            <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-
NetScalerMAS-1.0/mFunc-ADCFunction/mConn-internal" />
13            </vnsAbsFuncConn>
14            <vnsRsNodeToMFunc tDn="uni/infra/mDev-Citrix-
NetScalerMAS-1.0/mFunc-ADCFunction"/>
15            <vnsRsDefaultScopeToTerm tDn="uni/tn-coke/AbsGraph
-Graph1/AbsTermNodeProv-Input1/outtmnl"/>
16            <vnsRsNodeToAbsFuncProf tDn="uni/infra/mDev-Citrix

```

```

-NetScalerMAS-1.0/absFuncProfContr/absFuncProfGrp-
ADCCluster1"/>
17 DCCluster1"/>
18     <vnsRsNodeToLDev tDn="uni/tn-coke/lDevVip-
ADCCluster1"/>
19     </vnsAbsNode>
20     <vnsAbsTermNodeCon name = "Output1">
21         <vnsAbsTermConn name = "C6"></vnsAbsTermConn>
22     </vnsAbsTermNodeCon>
23     <vnsAbsConnection name = "CON1">
24         <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
-Graph1/AbsTermNodeCon-Output1/AbsTConn" />
25         <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
-Graph1/AbsNode-ADC/AbsFConn-outside" />
26     </vnsAbsConnection>
27     <vnsAbsConnection name = "CON2">
28         <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
-Graph1/AbsNode-ADC/AbsFConn-inside" />
29         <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
-Graph1/AbsTermNodeProv-Input1/AbsTConn" />
30     </vnsAbsConnection>
31 </vnsAbsGraph>
32 </fvTenant>
33 </polUni>
34 <!--NeedCopy-->

```

以下に、サービスグラフを契約に接続するための XML ペイロードの例を示します。

```

1 <polUni>
2     <fvTenant name="coke">
3         <vzBrCP name="Ctrct1">
4             <vzSubj name="http">
5                 <vzRsSubjGraphAtt tnVnsAbsGraphName="Graph1"/>
6             </vzSubj>
7         </vzBrCP>
8     </fvTenant>
9 </polUni>
10 <!--NeedCopy-->

```

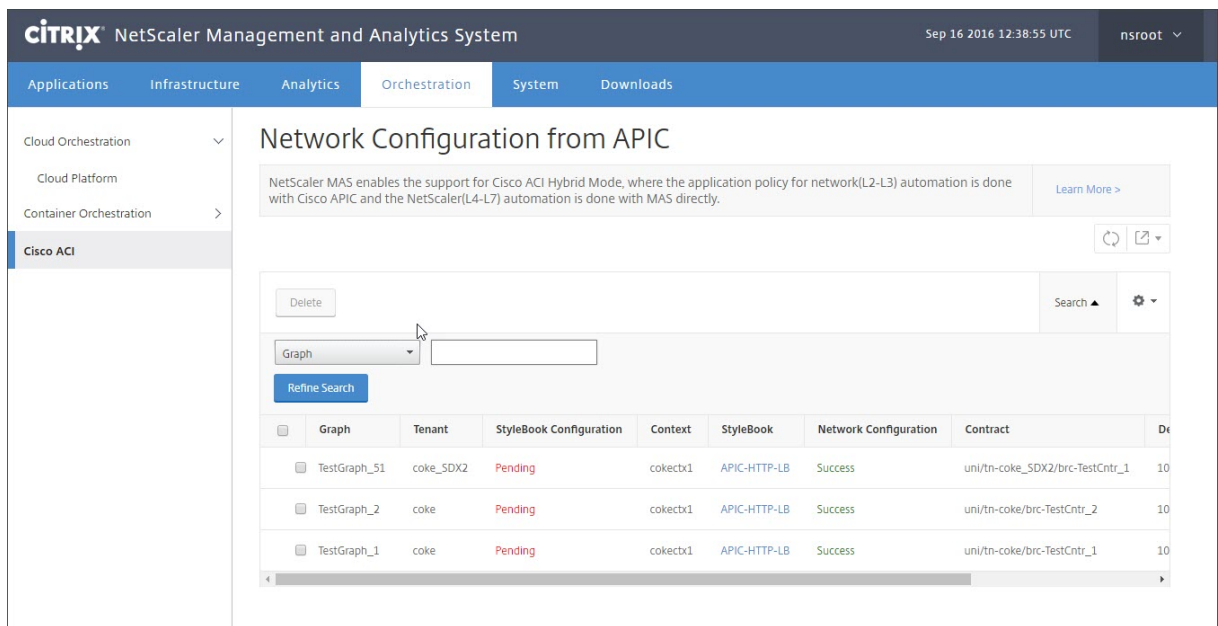
## StyleBook を使用して NetScaler ADM から L4-L7 パラメータを構成する

February 6, 2024

2018年5月24日

Citrix Application Delivery Management (ADM) では、展開されたサービスグラフの詳細を **Cisco ACI** の [オーケストレーション] タブで確認できます。表形式ビューに、グラフ名、テナント名、コンテキスト、StyleBook 名、ネットワーク構成の状態などのサービスグラフの詳細が表示されます。

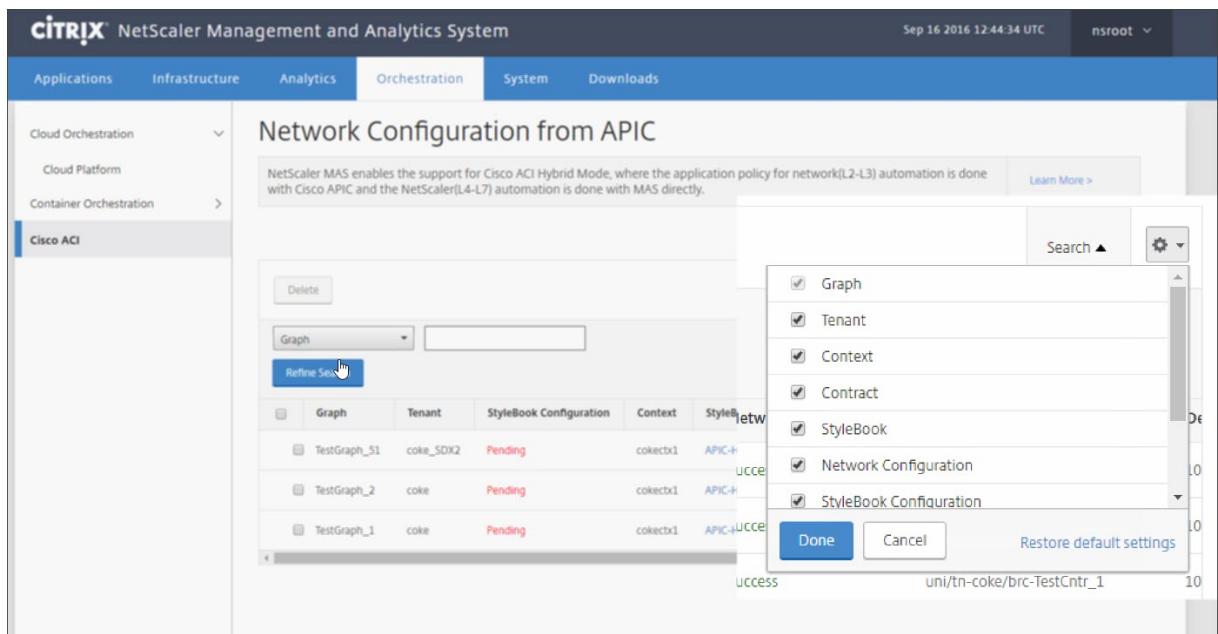




注

Cisco APIC からグラフが削除された場合、L4-L7 構成を含む対応する構成が、デバイスから削除されます。

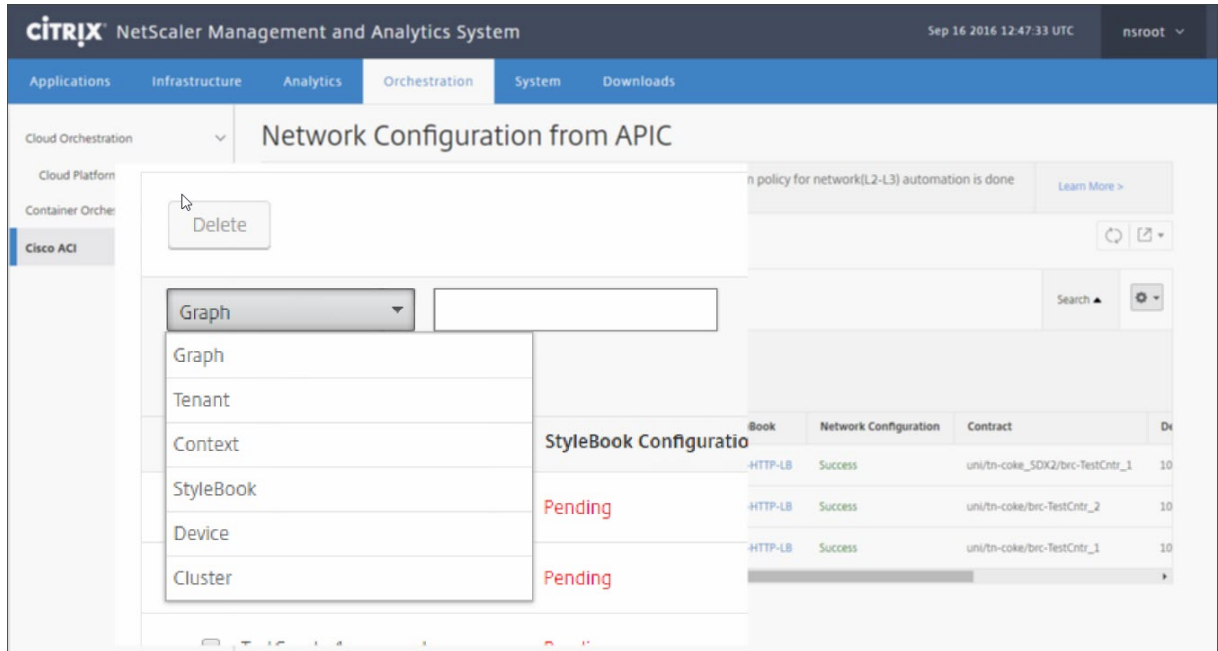
さらに、表形式ビューでは、表の列に合わせて並べ替えを行ったり、[Search] を使用してデータにフィルターを適用したりできます。また、次のように、ボックスで列名のチェックボックスをオンまたはオフにして、列の詳細をカスタマイズできます。



また、[Search] をクリックして検索オプションを使用し、データにフィルターを適用できます。ボックスから列を選択して、対応する値を入力すると、表のデータにフィルターを適用できます。

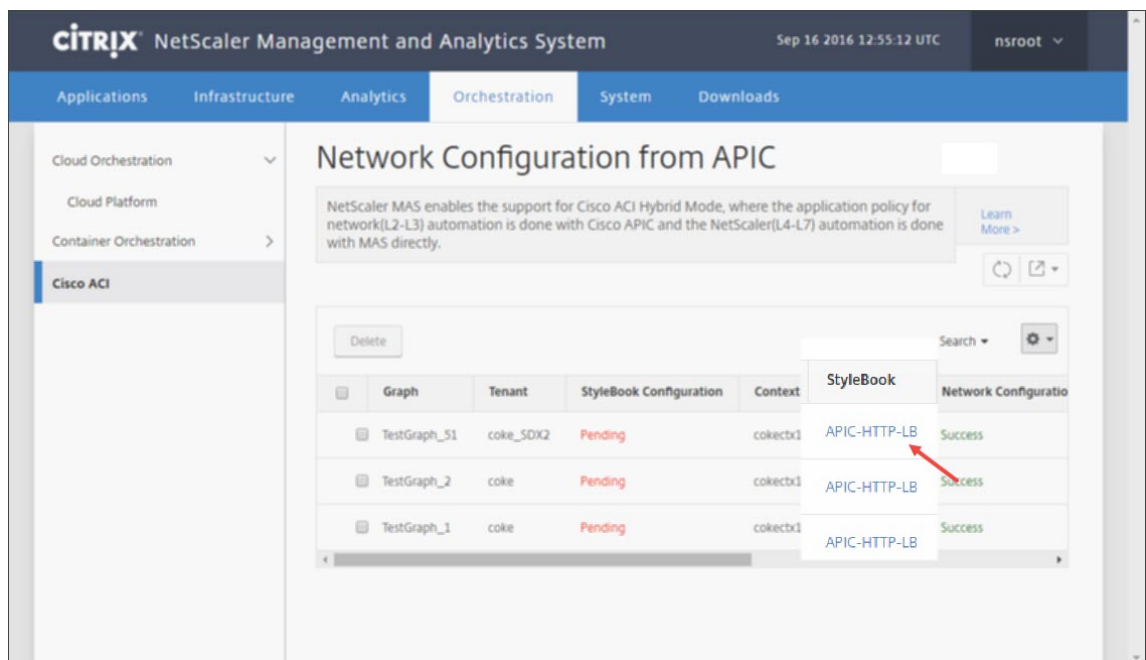
注

検索機能では大文字と小文字が区別されるので、正確な検索条件を入力してください。

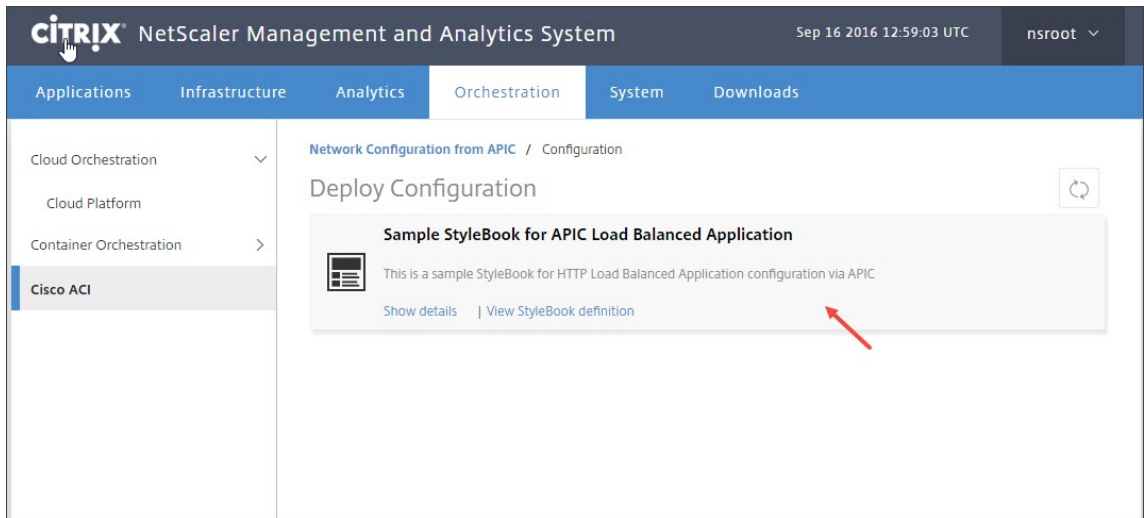


Citrix ADM で StyleBook を使用して L4-L7 構成を展開するには：

1. 表形式ビューで URL として表示されている StyleBook の名前をクリックします。

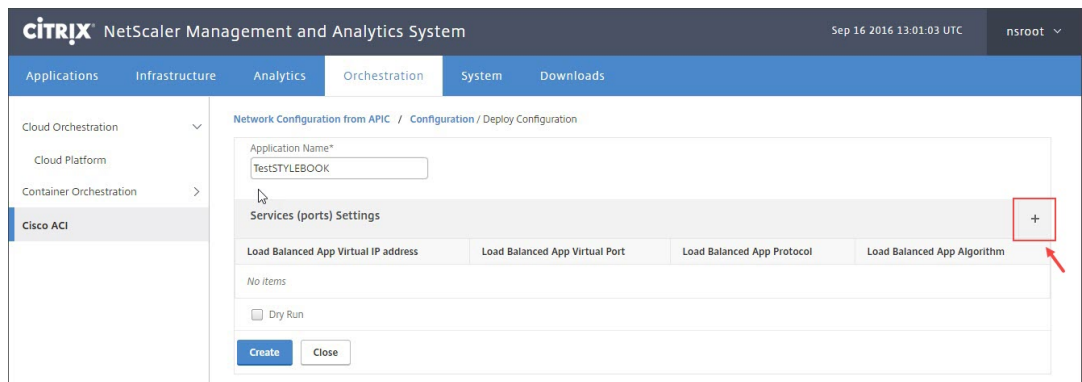


2. 設定ウィンドウで **StyleBook** をダブルクリックします。

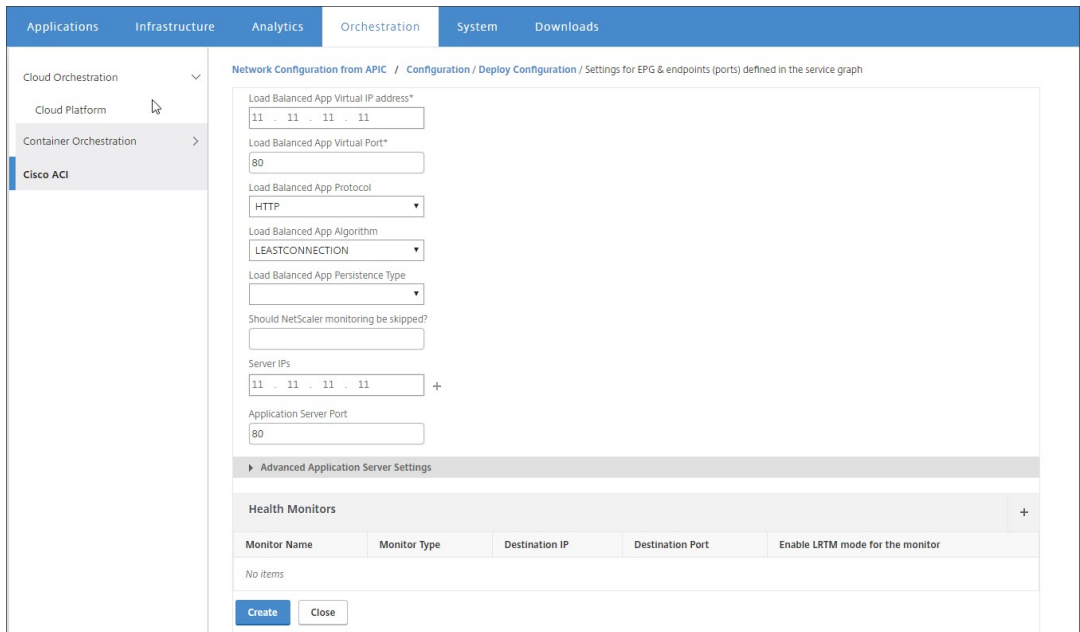


3. [Deploy Configuration] ウィンドウで次の操作を行います。

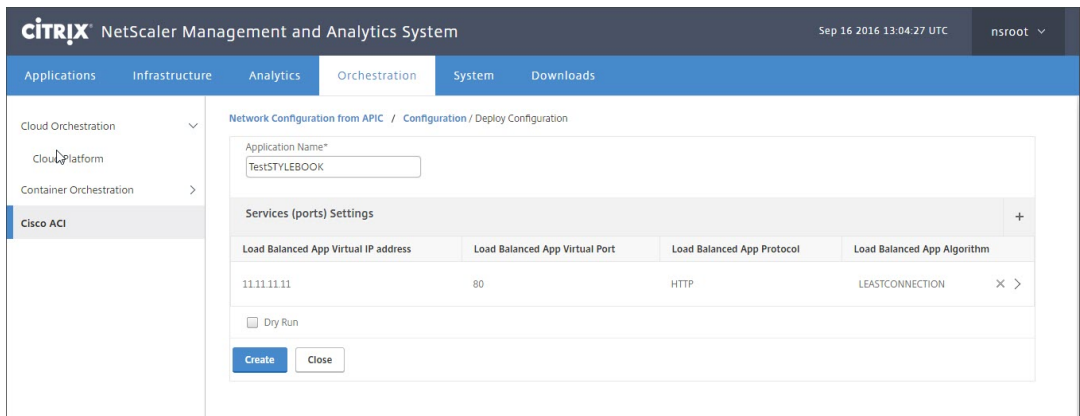
- a) APIC のアプリケーションのサービスグラフに対応する ADC の機能構成の名前を [Application Name] フィールドに入力します。
- b) [Service (ports) Settings] セクションで [+] をクリックします。



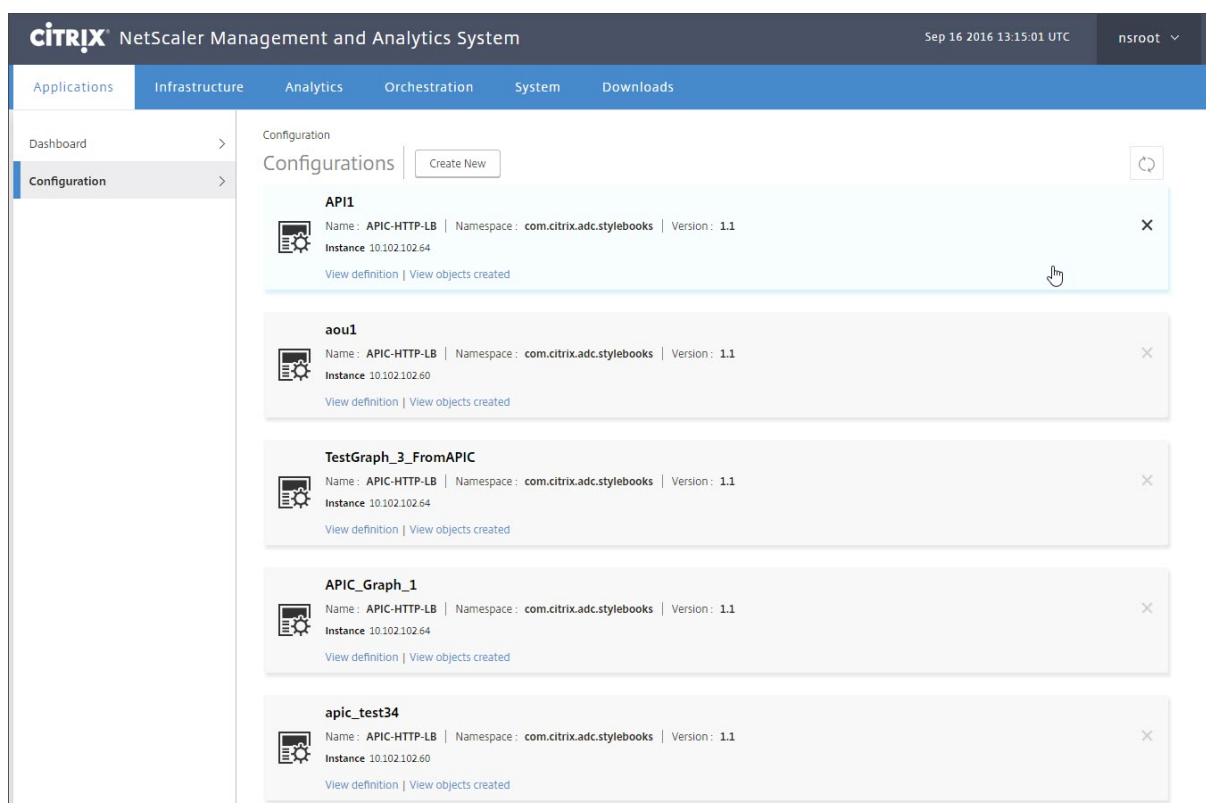
- c) サービスグラフウィンドウで定義されている EPG とエンドポイント（ポート）の設定で、StyleBook から入力されたパラメータの値を入力し、「作成」をクリックします。



d) [作成] をクリックします。



StyleBook で指定されている L4-L7 構成が Citrix ADM にデプロイされます。StyleBook 構成を表示するには、[Application] タブで [Application] > [Configuration] の順に選択します。



## APIC からのエンドポイントイベントのアタッチとデタッチ

February 6, 2024

ハイブリッドモードソリューションでは、Cisco APIC からの接続/接続解除エンドポイントイベントを暗黙的に処理します。Cisco APIC がエンドポイント接続イベントをトリガーすると、Citrix Application Delivery Management (ADM) の StyleBook によって `servicegroup_servicegroupmember_binding` が自動的にトリガーされ、エンドポイントのデタッチイベント中にエンドポイントのバインドが解除されます。

さらに、Cisco APIC でエンドポイントの接続または切断イベントがトリガーされる前に Citrix ADM に L4-L7 構成を展開していない場合、ソリューションは接続 IP アドレスをデータベースに保持します。これらの IP アドレスは、StyleBook 経由でサービスグループが作成された後、対応するサービスグループにバインドされます。

## APIC 障害レポート

February 6, 2024



```

6  'ADCHybridMode_1_Device_1': '1_1' }
7  , 'ackedstate': 0 }
8  , (7, '', '2129920_32778'): {
9  'state': 1, 'tag': 273, 'type': 1, 'ackedstate': 0, 'transaction': 0 }
10 , (1, '', 5790): {
11 'transaction': 0, 'ackedstate': 0, 'value': {
12 (3, 'ADCFunction', 'N1'): {
13 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
14 (4, 'mFCngNetwork', 'mFCngnetwork'): {
15 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
16 (6, 'Network_key', 'network_key'): {
17 'state': 1, 'transaction': 0, 'target': 'network', 'ackedstate': 0 }
18 }
19 }
20 , (4, 'internal_network', 'internal_network'): {
21 'connector': 'provider', 'state': 1, 'transaction': 0, 'ackedstate':
22 0, 'value': {
23 (6, 'internal_network_key', 'internal_network_key'): {
24 'state': 1, 'transaction': 0, 'target': 'network/internal_snip', '
25  ackedstate': 0 }
26 }
27 }
28 , (2, 'external', 'consumer'): {
29 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
30 (9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
31 'state': 1, 'transaction': 0, 'target': '
32  ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
33 }
34 }
35 , (4, 'mFCngStylebook', 'mFCngStylebook'): {
36 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
37 (6, 'Stylebook_key', 'Stylebook_key'): {
38 'state': 1, 'transaction': 0, 'target': 'stylebook_1', 'ackedstate': 0
39 }
40 }
41 }
42 , (2, 'internal', 'provider'): {
43 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
44 (9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
45 'state': 1, 'transaction': 0, 'target': '
46  ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
47 }
48 }
49 , 'state': 1, 'absGraph': 'HybridModeGraph_1', 'rn': u'vGrp-[uni/tn-
50 coke_SDx2/GraphInst_C-[uni/tn-coke_SDx2/brc-TestCntr_3]-G-[uni/tn-
51 coke_SDx2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDx2]]' }
52 , (4, 'Network', 'network'): {
53 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
54 (4, 'nsip', 'internal_snip'): {
55 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {

```

```

52 (5, 'type', 'type'): {
53 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'SNIP' }
54 , (5, 'hostroute', 'hostroute'): {
55 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'DISABLED' }
56 , (5, 'ipaddress', 'ipaddress'): {
57 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '10.1.1.1' }
58 , (5, 'dynamicrouting', 'dynamicRouting'): {
59 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'ENABLED' }
60 , (5, 'netmask', 'netmask'): {
61 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '255.255.255.0
    ' }
62 }
63 }
64 }
65 }
66 , (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
67 'state': 1, 'transaction': 0, 'vif': 'ADCHybridMode_1_Consumer_1', '
    ackedstate': 0, 'encap': '2129920_32778' }
68 , (4, 'Stylebook', 'stylebook_1'): {
69 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
70 (5, 'name', 'stylebookName'): {
71 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'
    }
72 }
73 }
74 }
75 , 'txid': 10000 }
76 }
77
78 2016-06-29 10:58:33,816 DEBUG get Graph Return details = {
79 'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[
    uni/tn-coke_SDX2]-ctx-cokectx1', (1, '', 5790): {
80 'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-
    coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-
    HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
81 , 'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB', '
    graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', '
    graphInstanceId': 5790 }
82
83 2016-06-29 10:58:33,827 DEBUG SUCCESS created track 2.0
84 2016-06-29 10:58:33,833 DEBUG SUCCESS updated track with new task 2
85 2016-06-29 10:58:33,851 DEBUG SUCCESS updated track with new task 1
86 2016-06-29 10:58:33,867 DEBUG fn_wrapper:long_operation_thread_id:<
    eventlet.greenthread.GreenThread object at 0x80aa5c7d0>
87 2016-06-29 10:58:33,867 DEBUG ++++++ Service Audit Call for Device
    Details = 10.102.102.62 ++++++
88 2016-06-29 10:58:33,867 DEBUG Inside APIC Cred Col If = 2
89 2016-06-29 10:58:33,867 DEBUG Host name from device =
    ADCHybridMode_1
90 "InProgress","message":null,"replication_status":"","target":
    "10.102.102.81","operation":"POST","entity_type":"apic",
    "entity_id":null }
91 }

```



```
92
93     2016-06-29 10:58:44,141 DEBUG Save config Response = {
94     "errorcode": 0, "message": "Done", "severity": "NONE" }
95
96     2016-06-29 10:58:44,141 DEBUG ++++++++ getContextAwareFlag = True
97     2016-06-29 10:58:44,141 DEBUG +++++ get context tenant name from
          Config ++++++
98     2016-06-29 10:58:44,141 DEBUG +++++ getContextTenantName = {
99     'state': 1, 'ctxName': 'coectx1', 'tenant': 'coke_SDx2', 'vdev': 5230
          }
100    ++++++
101     2016-06-29 10:58:44,142 DEBUG Service health details = {
102    }
103    collection length = 0
104     2016-06-29 10:58:44,142 DEBUG Count details Total = 0 Up = 0 Down =
          0
105     2016-06-29 10:58:44,142 DEBUG Health Score details Up = 0
106     2016-06-29 10:58:44,142 DEBUG Service HEALTH final collection = {
107    ((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')): {
108    'faults': [], 'state': 0, 'health': (((0, '', 5230), (1, '', 5790),
          (3, 'ADCFunction', 'N1')), 0) }
109    }
110
111     2016-06-29 10:58:44,142 DEBUG +++++getServiceHealth Fault List =
          []
112     2016-06-29 10:58:44,142 DEBUG Service HEALTH final response = {
113    'devs': 'ADCHybridMode_1_Device_1', 'faults': [], 'state': 0, 'health'
          : (((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')), 0) }
114
115     2016-06-29 10:58:44,236 DEBUG RESPONSE from NSLOGOUT = {
116     "errorcode": 0, "message": "Done", "severity": "NONE" }
117    , sessionId = ##
          D2EAF7CFCD73119E6C5E78D8BCB2E842829C971C1DC7E99850949DAE0029F2191B5E7EDF2764
118
119     2016-06-29 10:58:44,237 DEBUG +++++ Faults respCol = {
120     '10.102.102.62': {
121     u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
          u'NONE', 'operation_name': 'add_op' }
122    }
123    , (7, '', '2129920_32778'): {
124    'vlan': {
125    u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
          u'NONE', 'operation_name': 'add_op' }
126    }
127    , (((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1'), (2, '
          internal', 'provider')), 'nsip'): {
128    'vlan_nsip_binding': {
129    u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
          u'NONE', 'operation_name': 'bind_op' }
130    }
131    , (((0, '', 5230), (4, 'Network', 'network')), (4, 'nsip', '
          internal_snip')): {
```

```
132 'nsip': {
133   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
     u'NONE', 'operation_name': 'add_op' }
134 }
135 , (): {
136 }
137 , (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
138   'vlan_interface_binding': {
139     u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
       u'NONE', 'operation_name': 'bind_op' }
140   }
141 }
142
143   2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
     = Done, statusCode = add_op
144   2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
     = Done, statusCode = add_op
145   2016-06-29 10:58:44,237 DEBUG Fault details oprName = bind_op,
     erMsg = Done, statusCode = bind_op
146   2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
     = Done, statusCode = add_op
147   2016-06-29 10:58:44,238 DEBUG Fault details oprName = bind_op,
     erMsg = Done, statusCode = bind_op
148   2016-06-29 10:58:44,238 DEBUG ++++++ ServiceAudit response
     = {
149   'faults': [], 'state': 0, 'health': [] }
150
151   2016-06-29 10:58:44,238 DEBUG APIC Graph Details = {
152   'graphDN': u'uni/vDev-[uni/tn-coke_SDx2/lDevVip-ADCHybridMode_1]-tn-[
     uni/tn-coke_SDx2]-ctx-cokectx1', (1, '', 5790): {
153   'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDx2/GraphInst_C-[uni/tn-
     coke_SDx2/brc-TestCntr_3]-G-[uni/tn-coke_SDx2/AbsGraph-
     HybridModeGraph_1]-S-[uni/tn-coke_SDx2]]' }
154   , 'tenantName': 'coke_SDx2', 'StyleBookName': 'APIC-HTTP-LB', '
     graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', '
     graphInstanceId': 5790 }
155
156   2016-06-29 10:58:44,242 DEBUG Journal Processing: Database task:
     create apic_graph
157   2016-06-29 10:58:44,264 DEBUG SUCCESS created task 2
158   2016-06-29 10:58:44,269 DEBUG SUCCESS updated track with new task 2
159   2016-06-29 10:58:44,308 DEBUG ++++++ get IP and Connector
     collection from Config with type 22 for attach & detach event
     ++++++
160   2016-06-29 10:58:44,308 DEBUG ----- connector with IP List = {
161   0: [], 1: [], 3: [] }
162
163   2016-06-29 10:58:44,308 DEBUG ----- attachIpList = [] dettatchIpList
     = []
164   2016-06-29 10:58:44,308 DEBUG ----- In _attachDettachIps
     attachIpList = [] dettatchIpList = []
165   2016-06-29 10:58:44,312 DEBUG ----- In _attachDettachIps row = {
166   'deviceIP': u'10.102.102.62', 'responseToAPIC': None, 'graphDN': u'uni
```

```

/vDev-[uni/tn-coke_SDx2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-
coke_SDx2]-ctx-cokectx1', 'apicGraphState': None, 'serviceGroupName
': None, 'configPackId': None, 'tenantName': u'coke_SDx2', '
styleBookName': u'APIC-HTTP-LB', 'graphInstanceName': u'
HybridModeGraph_1', 'context': u'cokectx1', 'serviceGroupPort':
None, 'graphInstanceId': 5790, 'createDate': None, 'serviceGroupIP'
: None }

```

167

168 &lt;!--NeedCopy--&gt;

## ハイブリッドモードデバイスパッケージによって生成されるログ

February 6, 2024

Citrix ADC ハイブリッドモードデバイスパッケージは、構成関連のログと監視関連のログを生成します。生成されたログは、**/data/devicesscript/ Citrix.NetScalerMAS.1.0/logs** にあります。

Cisco APIC の **debug.log** のスニペットの例を次に示します。

```

1      2016-06-28 03:06:53.879767 DEBUG Thread-20 18723 [10.102.102.62,
      24063] Device manager details ip = 10.102.102.81, port = 80
2      2016-06-28 03:06:53.879856 DEBUG Thread-20 18724 [10.102.102.62,
      24063] ++++++ serviceAudit request ++++++
3      2016-06-28 03:06:53.879929 DEBUG Thread-20 18725 [10.102.102.62,
      24063] ++++++ getStyleBookObjects ++++++
4      2016-06-28 03:06:53.879995 DEBUG Thread-20 18726 [10.102.102.62,
      24063] NMAS collection A3 = (4, 'Stylebook', 'stylebook_1') B3 =
      {
5      'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
6      (5, 'name', 'stylebookName'): {
7      'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'
      }
8      }
9      }
10
11     2016-06-28 03:06:53.880045 DEBUG Thread-20 18727 [10.102.102.62,
      24063] NMAS collection styleBookName= APIC-HTTP-LB
12     2016-06-28 03:06:53.880093 DEBUG Thread-20 18728 [10.102.102.62,
      24063] NMAS collection retCol= {
13     'Stylebook': 'APIC-HTTP-LB', 'tuple': ((0, '', 5230), (4, 'Stylebook',
      'stylebook_1')) }
14
15     2016-06-28 03:06:53.880140 DEBUG Thread-20 18729 [10.102.102.62,
      24063] +++++ devMgrStyleBookUrl = http://10.102.102.81/stylebook
      /nitro/v1/config/stylebooks/com.citrix.adc.stylebooks/1.1/APIC-
      HTTP-LB
16     2016-06-28 03:06:54.135240 DEBUG Thread-20 18730 [10.102.102.62,
      24063] +++++ Response from styleBookresCode serviceAudit = {
17     u'stylebook': {

```

```

18 u'uses_built_in_namespaces': {
19 u'netScaler.nitro.config': u'10.5' }
20 , u'name': u'APIC-HTTP-LB', u'used_by_stylebooks': [], u'namespace': u
  'com.citrix.adc.stylebooks', u'source': u'---\nname: APIC-HTTP-LB\
  namespace: com.citrix.adc.stylebooks\nversion: "1.1"\ndisplay-name
  : "Sample StyleBook for APIC Load Balanced Application"\
  ndescription: "This is a sample StyleBook for HTTP Load Balanced
  Application configuration via APIC"\nschema-version: "1.0"\nimport-
  stylebooks: \n - \n namespace: netScaler.nitro.config\n
  prefix: ns\n version: "10.5"\n - \n namespace: "com.citrix.
  adc.stylebooks"\n prefix: "stlb"\n version: "1.1"\nparameters
  -default-sources:\n - stlb::APIC-ROOT\nsubstitutions:\n lb-name(
  appname, port): $appname + "-" + str($port) + "-lb"\n sg-name(
  appname, port): $appname + "-" + str($port) + "-sg"\n
  healthmonitor[]:\n true: "NO"\n false: "YES"\ncomponents: \n
  - \n name: lbvserver\n type: ns::lbvserver\n repeat:
  $parameters.app-services\n repeat-item: app\n properties: \n
  name: $substitutions.lb-name($parameters.appname, $app.
  virtual-port)\n ipv46: $app.virtual-ip\n port: $app.
  virtual-port\n servicetype: $app.protocol\n lbmethod?:
  $app.algorithm\n persistencetype?: $app.persistence\n - \n
  name: svcgrp\n type: ns::servicegroup\n repeat: $parameters.
  app-services\n repeat-item: app\n properties: \n name:
  $substitutions.sg-name($parameters.appname, $app.virtual-port)\n
  servicetype: $app.protocol\n useproxyport?: $app.sg-
  advanced.useproxyport\n usip?: $app.sg-advanced.usip\n
  cip?: $app.sg-advanced.cip\n cipheader?: $app.sg-advanced.
  cipheader\n healthmonitor?: $substitutions.healthmonitor($app.
  skip_healthmonitor)\n components: \n -\n name:
  lbvserver-svg-binding\n type: ns::
  lbvserver_servicegroup_binding\n properties: \n
  name: $substitutions.lb-name($parameters.appname, $app.virtual-port
  )\n servicegroupname: $parent.properties.name\n - \n
  name: svg-members\n type: ns::
  servicegroup_servicegroupmember_binding\n condition: $app.
  server-ips\n repeat: $app.server-ips\n repeat-item:
  serverip\n properties: \n ip: $serverip\n
  port: $app.server-port\n servicegroupname: $parent.
  properties.name\noutputs: \n - \n name: lbvservers\n value:
  $components.lbvserver\n - \n name: servicegroups\n value:
  $components.svcgrp', u'version': u'1.1', u'uses_stylebooks': [{
21 u'version': u'1.1', u'namespace': u'com.citrix.adc.stylebooks', u'name
  ': u'APIC-ROOT' }
22 ] }
23 }
24
25 2016-06-28 03:06:54.359142 DEBUG Thread-20 18731 [10.102.102.62,
  24063] +++ Dev Mgr request details devMgrUrl = http://
  10.102.102.81/admin/v1/apic
26 2016-06-28 03:06:54.359221 DEBUG Thread-20 18732 [10.102.102.62,
  24063] +++ Response from Device Mgr serviceAudit = {
27 "APIC": [] }
28

```

```
29     2016-06-28 03:06:54.359266 DEBUG Thread-20 18733 [10.102.102.62,
      24063] ++++++ serviceAudit response = {
30     "APIC":[] }
31
32     2016-06-28 03:06:54.359306 DEBUG Thread-20 18734 [10.102.102.62,
      24063] ++++++ serviceAudit response headers content type
      = application/json; charset=utf-8
33     2016-06-28 03:06:54.359394 DEBUG Thread-20 18735 [10.102.102.62,
      24063] ++++++ serviceAudit response headers = {
34     'content-length': '11', 'job_id': 'ctxt-f4db2883-e42c-4262-a35f-04628
      c4ad5ea', 'x-content-type-options': 'nosniff', 'transfer-encoding':
      'chunked', 'connection': 'close', 'date': 'Wed, 29 Jun 2016
      10:58:33 GMT', 'x-frame-options': 'SAMEORIGIN', 'content-type': '
      application/json; charset=utf-8' }
35
36     2016-06-28 03:06:54.359480 DEBUG Thread-20 18736 [10.102.102.62,
      24063] ++++++ pollingURL = http://10.102.102.81/admin/v1
      /journalcontexts/ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea
37     2016-06-28 03:06:54.359713 DEBUG Thread-20 18737 [10.102.102.62,
      24063] ++++++ pollingStatus = True, pollingTime = 0
38     2016-06-28 03:06:54.483228 DEBUG Thread-20 18738 [10.102.102.62,
      24063] ++++++ pollingResponse json = {
39     u'journalcontext': {
40     u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name':
      u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
      service_name': u'admin', u'start_time': u'2016-06-29T10
      :58:33.760565', u'is_default': u'false', u'end_time': None, u'
      target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883
      -e42c-4262-a35f-04628c4ad5ea', u'replication_status': u'' }
41     }
42
43     2016-06-28 03:07:04.493074 DEBUG Thread-20 18739 [10.102.102.62,
      24063] ++++++ pollingStatus = True, pollingTime = 1
44     2016-06-28 03:07:04.587595 DEBUG Thread-20 18767 [10.102.102.62,
      24063] ++++++ pollingResponse json = {
45     u'journalcontext': {
46     u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name':
      u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
      service_name': u'admin', u'start_time': u'2016-06-29T10
      :58:33.760565', u'is_default': u'false', u'end_time': None, u'
      target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883
      -e42c-4262-a35f-04628c4ad5ea', u'replication_status': u'' }
47     }
48
49     2016-06-28 03:07:14.597812 DEBUG Thread-20 18790 [10.102.102.62,
      24063] ++++++ pollingStatus = True, pollingTime = 2
50     2016-06-28 03:07:14.692590 DEBUG Thread-20 18791 [10.102.102.62,
      24063] ++++++ pollingResponse json = {
51     u'journalcontext': {
52     u'status': u'Finished', u'scopes': [], u'entity_id': None, u'name': u'
      Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
      service_name': u'admin', u'start_time': u'2016-06-29T10
      :58:33.760565', u'is_default': u'false', u'end_time': u'2016-06-29
```

```

T10:58:44.486919', u'target': u'10.102.102.81', u'message': u'Done'
, u'id': u'ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea', u'
replication_status': u'' }
53 }
54
55 2016-06-28 03:07:14.692932 DEBUG Thread-20 18793 [10.102.102.62,
24063] Attempts 1
56 2016-06-28 03:07:14.693031 DEBUG Thread-20 18794 [10.102.102.62,
24063] Cluster (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1', (0,
'', 5230)), transaction: 0
57 2016-06-28 03:07:14.693147 DEBUG Thread-20 18795 [10.102.102.62,
24063] Attempts for {
58 'name': 'ADCHybridMode_1', 'host': '10.102.102.62', 'virtual': False,
'devs': {
59 'ADCHybridMode_1_Device_1': {
60 'state': 0, 'virtual': False, 'manager': {
61 'hosts': {
62 '10.102.102.81': {
63 'port': 80 }
64 }
65 , 'name': 'NMAAS_1', 'creds': {
66 'username': 'nsroot', 'password': '<hidden>' }
67 }
68 , 'version': '11.0', 'host': '10.102.102.62', 'port': 80, 'creds': {
69 'username': 'nsroot', 'password': '<hidden>' }
70 }
71 }
72 , 'manager': {
73 'hosts': {
74 '10.102.102.81': {
75 'port': 80 }
76 }
77 , 'name': 'NMAAS_1', 'creds': {
78 'username': 'nsroot', 'password': '<hidden>' }
79 }
80 , 'contextaware': True, 'port': 80, 'creds': {
81 'username': 'nsroot', 'password': '<hidden>' }
82 }
83 is 0
84 2016-06-28 03:07:14.693339 DEBUG Thread-20 18796 [10.102.102.62,
24063] Deleting (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1',
(0, '', 5230))
85 2016-06-28 03:07:14.693379 DEBUG Thread-20 18797 [10.102.102.62,
24063] pending: False, delete: False, txId: None
86 2016-06-28 03:07:14.693517 DEBUG Thread-20 18798 [10.102.102.62,
24063] Faults: []
87 2016-06-28 03:07:14.693558 DEBUG Thread-20 18799 [10.102.102.62,
24063] Health: []
88 2016-06-28 03:07:14.693914 DEBUG Thread-20 18800 [10.102.102.62,
24063] Send num: 761, type: 220, len: 382
89 <!--NeedCopy-->

```

## Cisco ACI のクラウドオーケストレータモードの NetScaler ADC デバイスパッケージ

February 6, 2024

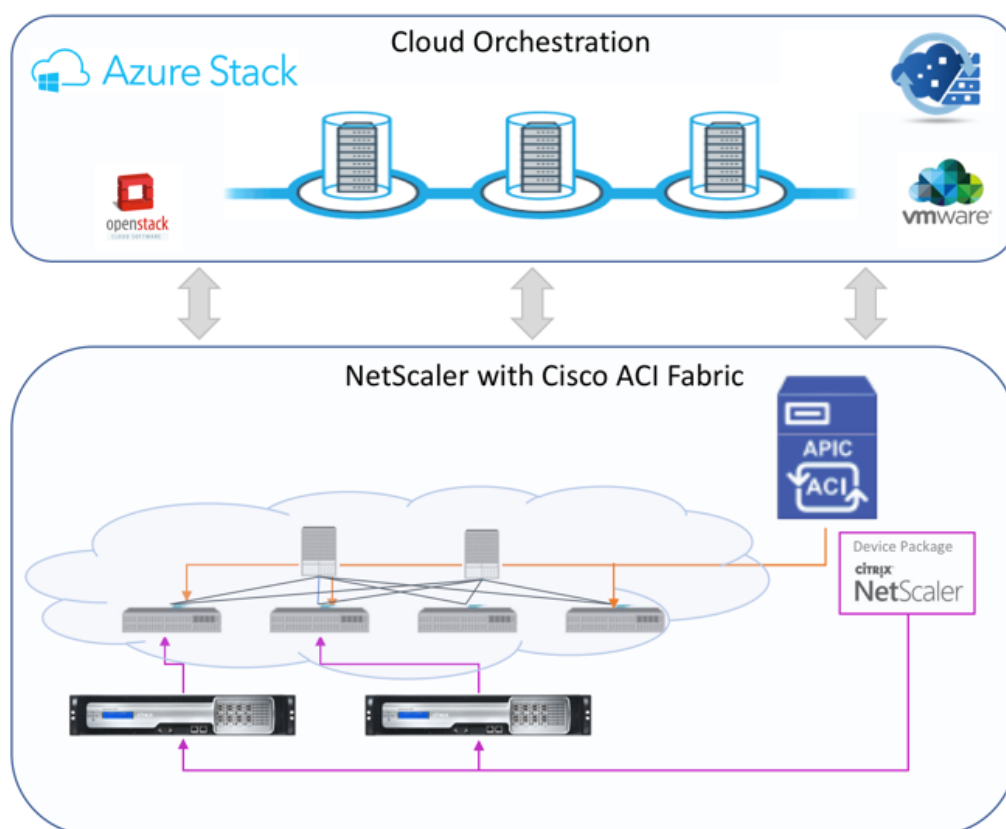
アプリケーションポリシーインフラストラクチャコントローラ (APIC) バージョン 3.1 により、Citrix ADC と Cisco ACI は共同統合ポートフォリオを拡大し、お客様のニーズに対応する新しいソリューションを提供します。新しい統合モードである ACI Cloud Orchestrator Mode\* は、標準化されたパラメーターによって構成の複雑さを抽象化することで、L4-L7 の統合を簡素化します。このソリューションはシームレスに動作し、L4-L7 サービスを自動化し、アジャイルなアプリケーション展開、運用の柔軟性、シンプルさという目標を達成します。

NetScaler ADC ソリューションを使用した Cisco ACI クラウドオーケストレータモードには、次の利点があります。

- L4-L7 サービスの自動化により、ヒューマンエラーが減少します。
- 事前に構築された Cisco ACI ソリューションの統合により、導入時間を短縮し、Web アプリケーション、仮想マシン、SQL などのアプリケーションのパフォーマンスを向上させることができます。
- 物理ネットワークコンポーネントと仮想ネットワークコンポーネント全体で、Web アプリケーション、仮想マシン、SQL などのアプリケーションの健全性を完全に統合して可視化します。

ACI クラウドオーケストレータモードでは、新しい簡略化された APIC GUI を直接使用するか、Cisco Cloud Center、Windows Azure Pack、OpenStack、vRealize などの任意のクラウドオーケストレータを好みに応じて選択して、より多くの選択肢が提供されます。この新しい変更は、一連の ADC 属性を ADC スキーマとして公開することで実現されます。これらの属性は、デバイスパッケージの機能プロファイルにマッピングされます。クラウドオーケストレータ (Cisco Cloud Center またはワイヤレスアプリケーションプロトコル (WAP)) による ADC サービスのプロビジョニング中に、これらの属性の値を指定できます。

次の図に、クラウドオーケストレーションソリューションにおける NetScaler ADC 概要を示します。



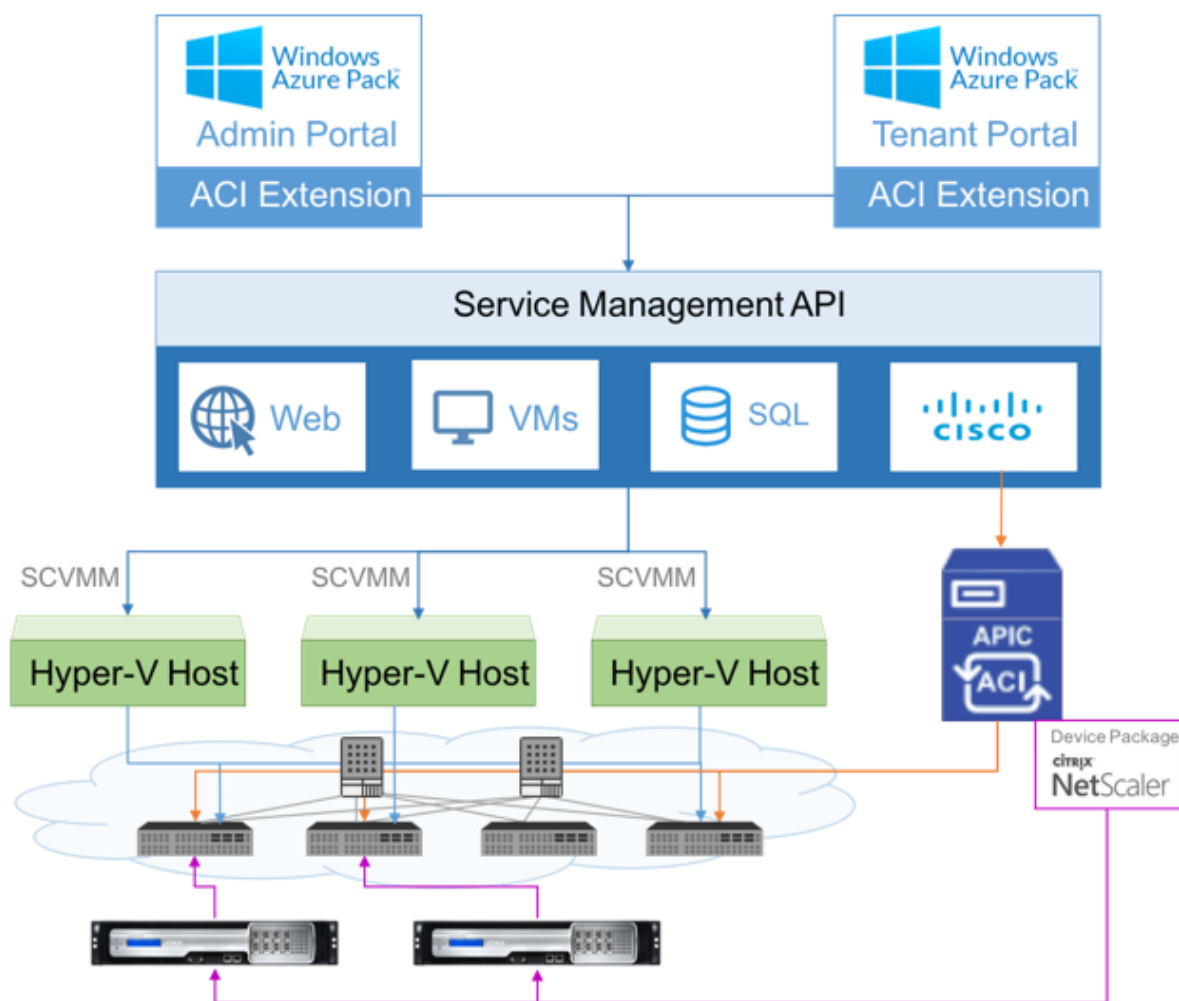
Microsoft Azure パックを使用するクラウドオーケストレーターモードソリューションには、Azure Pack から Cisco APIC、Cisco APIC からシステムセントラルのバーチャルマシンマネージャー (SCVMM)、Cisco APIC から NetScaler ADC への統合など、多くのポイントが含まれます。プライベートクラウドのテナントとして、NAT の有効化、ネットワークサービスのプロビジョニング、ロードバランサーの追加を行うことができます。

Azure Pack はテナントポータルと管理者ポータルをサポートし、それぞれに実行可能な独自の操作セットがあります。

- 管理者は、ACI 登録、VIP 範囲、NetScaler ADC デバイスと仮想マシンクラウドとの関連付け、テナントユーザーアカウントの作成などの管理タスクを実行できます。
- テナントは、Azure Pack テナントポータルへのログオンや、ネットワーク、ブリッジドメイン、仮想ルーティングおよび転送 (VRF) の構成などのタスクを実行でき、NetScaler ADC 負荷分散および RNAT 機能を使用できます。

次の図は、クラウドモードソリューションにおける Azure Pack の概要を示しています。





重要

- クラウド管理者は APIC でサポートされている L4-L7 スキーマを使用でき、追加の変更は APIC 管理者が直接 APIC で実行できます。これにより、サポートされている機能セットと同等の NetScaler ADC を構成および展開できます。
- テナントは、同じネットワークに対して異なるポートを持つ複数の VIP アドレスを展開できます。IP とポートの組み合わせが一意であることを確認する必要があります。
- NetScaler ADC デバイスパッケージは、単一コンテキスト展開のみをサポートします。各テナントは専用の NetScaler ADC インスタンスを取得します。
- ワイヤレスアプリケーションプロトコル (WAP) は、NetScaler ADC MPX アプライアンスおよび NetScaler ADC VPX アプライアンス (NetScaler ADC SDX プラットフォームにデプロイされた NetScaler ADC VPX インスタンスを含む) をサポートします。

クラウドオーケストレーターモードのデバイスパッケージは、完全マネージドモードとサービスマネージャモードの両

方をサポートしています。完全マネージドモードパッケージは、単純な負荷分散、コンテンツスイッチング、SSL オフロード、その他のプロファイルなど、さまざまな機能プロファイルをサポートします。これらの関数プロファイルは、NetScaler ADC の完全な機能セットと展開モードをカバーします。同様に、サービスマネージャモードのデバイスパッケージでは、APIC を使用した NetScaler ADC のワンアームおよびツアーム構成と展開がサポートされます。NetScaler Application Delivery Management (ADM) は APIC のサービスマネージャとして機能し、NetScaler ADM を使用して NetScaler ADC L4-L7 パラメーターを構成できます。

### 注

サービスマネージャモード（ハイブリッドモード）では、NetScaler ADC アプライアンスにすでに存在する同じサーバー IP アドレスを再利用または再割り当てすることはできません。

クラウドオーケストレータモード機能プロファイルには、APIC ADC スキーマにマッピングされた一連のパラメータがあり、オーケストレータはこれらのパラメータを使用します。クラウドオーケストレータは ADC パラメーター (VIP、APIC を介した NetScaler ADC のプロビジョニング中) の値を提供します。オーケストレータは APIC の API と通信し、特定の機能プロファイルのペイロードの一部として ADC 固有の詳細を渡します。内部的に、APIC は値を抽出し、NetScaler ADC を内部的に構成するデバイスパッケージに渡します。

Cisco APIC でサポートされている ADC スキーマの完全なリストについては、『[Cisco APIC レイヤ 4～レイヤ 7 サービス導入ガイド、リリース 3.x 以前](#)』を参照してください。

フルマネージドモードデバイスパッケージは、次の機能プロファイルをサポートします。

1. LB-HTTP-One-Arm-ProfileCM
2. LB-HTTP-Two-Arm-ProfileCM
3. LB-HTTP-Two-Arm-ServiceBackendProfileCM
4. CS-HTTP-LB-Service-ProfileCM
5. CS-SSL-LB-Service-ProfileCM
6. LB-SSL-ProfileCM
7. SSLVServerProfileInlineModeCM
8. WebVServerProfileWithRHICM
9. WebInlineVServerProfileWithRHICM
10. WebAnywhereVServerProfileWithRHIC
11. SSLVServerProfileForAnywhereModeCM
12. SSLAnywhereServerProfileCM
13. WebVServerProfileCM
14. WebInlineVServerProfileCM
15. WebAnywhereVServerProfileCM

16. CSLBServerProfileCM
17. GSLBServerProfileCM
18. CMPServerProfileCM
19. CRServerProfileC
20. DNSServerProfileCM
21. DSServerProfileCM
22. ICServerProfileCM
23. SSLVPNServerProfileCM
24. AppFWServerProfileCM
25. AAAServerProfileCM
26. AAASyslogServerProfileCM
27. IPv6WebInlineVServerProfileCM

サービス管理モードのデバイスパッケージでは、次のクラウドモード機能プロファイルがサポートされています。

1. ADCOneArmFunctionProfileCM
2. AADCTwoArmFunctionProfileCM
3. RHI-ADCOneArmFunctionProfileCM
4. RHI-ADCTwoArmFunctionProfileCM

NetScaler ADC は上記の機能プロファイルをサポートしています。APIC では、ADC スキーマでこれらのパラメータのサブセットがサポートされています。Cisco ACI でサポートされていない属性が機能プロファイルに存在する場合は、クラウドオーケストレータモードの機能プロファイルのクローンを作成し、APIC でサポートされていないすべての属性の値を指定し、その属性を保存する必要があります。その後、オーケストレータは新しくクローンされた機能プロファイルを使用できます。

Citrix Cloud モードデバイスパッケージは NetScaler ADC 12.0 をサポートし、サービスマネージャーモードでは NetScaler ADM 12.0 も使用されます。デバイスパッケージのモデルバージョンが 1.0 から 2.0 に変更され、新規インストールとして使用できるようになりました。Cloud Orchestrator モードデバイスパッケージは、モデルバージョンが変更されたため、以前のデバイスパッケージバージョンからアップグレードできません。

Cloud Orchestrator モードのデバイスパッケージは、通常の展開でも使用できます。このパッケージでは、クラウドオーケストレータを介して NetScaler ADC をプロビジョニングすることをユーザーに義務付けるものではありません。デバイスパッケージは APIC と APIC とクラウドオーケストレータとのみ互換性があります。

## NetScaler ADM で Kubernetes 入力構成を管理する

February 6, 2024

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。

Kubernetes は、クラスター外のクライアントトラフィックが Kubernetes クラスター内で実行されているアプリケーションのマイクロサービスにアクセスできるようにする Ingress 機能を提供します。ADC インスタンスは、Kubernetes クラスター内で実行されているアプリケーションの Ingress として機能します。ADC インスタンスは、クライアントから Kubernetes クラスター内の任意のマイクロサービスに North-South トラフィックをロードバランシングし、コンテンツルーティングできます。

### 注

- Citrix ADM は、Kubernetes バージョン 1.14 以降を搭載したクラスターのインGRESS機能をサポートしています。
- NetScaler ADM は、入力デバイスとして NetScaler ADC VPX および MPX アプライアンスをサポートしています。
- Kubernetes 環境では、NetScaler ADC インスタンスは「nodePort」サービスタイプのみを負荷分散します。

複数の ADC インスタンスを、同じクラスターまたは異なるクラスターまたは名前空間上で入力デバイスとして動作するように設定できます。インスタンスを構成したら、Ingress ポリシーに基づいて各インスタンスを異なるアプリケーションに割り当てることができます。

Kubernetes `kubectl` または API を使用して Ingress 設定を作成してデプロイできます。NetScaler ADM から Ingress を構成して展開することもできます。

ADM では、Kubernetes 統合の次の側面を指定できます。

- **クラスター**—ADM が Ingress 設定をデプロイできる Kubernetes クラスターを登録または登録解除できます。NetScaler ADM にクラスターを登録するときは、Kubernetes API サーバー情報を指定します。次に、Kubernetes クラスターにアクセスして Ingress 設定をデプロイできる ADM エージェントを選択します。
- **Policies**—Ingress ポリシーは、Ingress 設定をデプロイするクラスターまたは名前空間に基づいて ADC インスタンスを選択するために使用されます。ポリシーを追加するときに、クラスター、サイト、およびインスタンスの情報を指定します。
- **入力設定**: この設定は Kubernetes 入力設定です。この設定には、コンテンツスイッチングルールと、マイクロサービスとそのポートの対応する URL パスが含まれます。Kubernetes シークレットリソースを使用して SSL/TLS 証明書を指定することもできます (ADC インスタンスの SSL 処理をオフロードするため)。

NetScaler ADM は、入力ポリシーを使用して、入力構成を ADC インスタンスに自動的にマッピングします。

Ingress 構成が成功するたびに、NetScaler ADM は StyleBook ConfigPack を生成します。ConfigPack は、入力設定に対応する ADC インスタンスに適用される ADC 設定を表します。ConfigPack を表示するには、[アプリケーション] > [StyleBook] > [構成] に移動します。

はじめに

NetScaler ADC インスタンスを Kubernetes クラスターで Ingress デバイスとして使用するには、次のものがあることを確認します。

- Kubernetes クラスターが存在する。
- NetScaler ADM に登録された Kubernetes クラスター。

秘密トークンを使用して **NetScaler ADM** を構成し、**Kubernetes** クラスターを管理する

NetScaler ADM が Kubernetes からイベントを受信できるようにするには、Kubernetes で NetScaler ADM 用のサービスアカウントを作成する必要があります。また、クラスターに必要な RBAC アクセス許可を使用してサービスアカウントを構成します。

1. NetScaler ADM 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` になります。サービスアカウントを作成するには、「[複数のサービスアカウントを使用する](#)」を参照してください。
2. `cluster-admin` ロールを使用して、NetScaler ADM サービスアカウントをバインドします。このバインドにより、クラスター全体にわたって `ClusterRole` がサービスアカウントに付与されます。`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を次に示します。

```
1 kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole
   =cluster-admin --serviceaccount=default:citrixadm-sa
2 <!--NeedCopy-->
```

NetScaler ADM サービスアカウントを `cluster-admin` ロールにバインドすると、そのサービスアカウントはクラスター全体にアクセスできるようになります。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、以下のコマンドを実行して、`citrixadm-sa` サービスアカウントのトークンを表示します。

```
1 kubectl describe sa citrixadm-sa
2 <!--NeedCopy-->
```

4. 次のコマンドを実行して、トークンのシークレット文字列を取得します。

```
1 kubectl describe secret <token-name>
2 <!--NeedCopy-->
```

## NetScaler ADM に Kubernetes クラスタを追加する

NetScaler ADM エージェントを構成して静的ルートを構成したら、Kubernetes クラスタを NetScaler ADM に登録する必要があります。

Kubernetes クラスタを登録するには、次の手順を実行します。

1. 管理者の資格情報を使用して NetScaler ADM にログインします。
2. オーケストレーション > **Kubernetes** > クラスタに移動します。  
[クラスタ] ページが表示されます。
3. [追加] をクリックします。
4. [クラスタの追加] ページで、次のパラメータを指定します。
  - a) [名前]: 任意の名前を指定します。
  - b) **API サーバー URL** -Kubernetes メインノードから API サーバーの URL の詳細を取得できます。

- i. Kubernetes メインノードで、`kubectl cluster-info`コマンドを実行します。

```
root@kmaster: ~ # kubectl cluster-info
Kubernetes master is running at https://10.10.10.10:6443
KubeDNS is running at https://10.10.10.10:6443/api/v1/namespaces/kube-system/
services/kube-dns:dns/proxy

To further debug and diagnose cluster problems, use 'kubectl cluster-info dump'.
```

- ii. 「**Kubernetes** マスターが実行中です。」と表示される **URL** を入力します。

- c) 認証トークン - Kubernetes クラスタを管理するように NetScaler ADM を構成するとき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 クラスタと NetScaler ADM 間の通信へのアクセスを検証するために必要です。認証トークンを生成する手順は、次のとおりです。

- i. Kubernetes メインノードで、次のコマンドを実行します。

```
1 kubectl describe secret <token-name>
2 <!--NeedCopy-->
```

- ii. 生成されたトークンをコピーし、認証トークンとして貼り付けます。

詳細については、[Kubernetes](#) ドキュメントを参照してください。

- d) リストからエージェントを選択します。
  - e) [作成] をクリックします。

Orchestration > Kubernetes > Clusters

## ← Add Cluster

Name \*

API Server URL \*

Authentication Token \*

Requires secret token for a service-account with cluster-wide access control.

Agent

Create Close

### 入力ポリシーの定義

Ingress ポリシーは、Ingress クラスターまたは名前空間に基づいて、Ingress 構成の展開に使用される NetScaler ADC を決定します。

1. [オーケストレーション] > [Kubernetes] > [ポリシー] に移動します。
2. [Add] をクリックしてポリシーを作成します。
  - a) ポリシー名を指定します。
  - b) Kubernetes クラスターに Ingress 設定をデプロイするための条件を定義します。これらの条件は通常、Ingress クラスターと名前空間に基づいています。
  - c) [インフラストラクチャ] パネルで、

- サイト -リストからサイトを選択します。
- [インスタンス]-リストから ADC インスタンスを選択します。

[サイト] リストと [ インスタンス] リストには、[ 条件] パネルで選択したクラスタに基づいてオプションが入力されます。

これらのリストには、Kubernetes クラスタで構成された NetScaler ADM エージェントに関連付けられているサイトまたはインスタンスが表示されます。

- d) [ **Choose Network**] で、ADM が仮想 IP アドレスを入力構成に自動的に割り当てるネットワークを選択します。

このリストには、[ネットワーク] > [IPAM] で作成されたネットワークが表示されます。

- e) [作成] をクリックします。

## Ingress 設定をデプロイする

`kubectl`、Kubernetes API または他のツールを使用して、Kubernetes から Ingress 設定をデプロイできます。Ingress 構成を NetScaler ADM から直接展開することもできます。

1. オーケストレーション > **Kubernetes** > イングレスに移動します。

2. [追加] をクリックします。

3. 「**Create Ingress**」フィールドで、次の詳細を指定します。

- a) Ingress の名前を指定します。

- b) [クラスター] で、Ingress をデプロイする Kubernetes クラスターを選択します。

- c) リストから [クラスタ名前空間] を選択します。このフィールドには、指定した Kubernetes クラスターに存在する名前空間が一覧表示されます。

- d) 必要に応じて、[フロントエンド IP アドレスの自動割り当て] を選択します。

- e) リストから [入力プロトコル] を選択します。**HTTPS** を選択した場合は、**TLS** シークレットを指定します。

このシークレットには、HTTPS 証明書とプライベートキーを埋め込む Kubernetes シークレットリソースが埋め込まれます。

HTTPS Ingress には、Kubernetes クラスターに設定された TLS ベースのシークレットが必要です。

`tls.crt`および`tls.key`フィールドを指定して、サーバ証明書と証明書キーをそれぞれ含めます。

- f) コンテンツルーティングでは、次の詳細を指定します。

- **URL** パス -Kubernetes サービスとポートに関連付けられているパスを指定します。
- **Kubernetes** サービス -目的のサービスを指定します。



- [ポート]-サービスポートを指定します。
- **LB** メソッド -選択した Kubernetes サービスに優先する負荷分散方法を選択します。

選択したメソッドは、Ingress 仕様を適切なアノテーションで更新します。たとえば、**ROUNDROBIN** メソッドを選択すると、Citrix アノテーションは次のように表示されます。

```
1 "lbmethod":"ROUNDROBIN"
2 <!--NeedCopy-->
```

- パーシステンスタイプ -選択した Kubernetes サービスに優先する負荷分散パーシステンスタイプを選択します。

選択した永続性タイプは、Ingress 仕様を適切な注釈で更新します。たとえば、**COOKIEINSERT** を選択すると、Citrix 注釈は次のように表示されます。

```
1 "persistenceType":"COOKIEINSERT"
2 <!--NeedCopy-->
```

[ **Add** ] をクリックして、Ingress 設定に URL パスとポートを追加します。

The screenshot shows a configuration window for a default Ingress rule. It includes a toggle for the rule, a hostname input field, and a table of paths. The 'default' path is selected, showing its URL Path, Kubernetes Service, Service Port, LB Method, and Persistence Type. An 'Add Path' button is visible at the bottom.

デプロイ後、Ingress 設定は以下に基づいてクライアントトラフィックを特定のサービスにリダイレクトします。

- 要求された URL パスとポート。
- 定義された LB メソッドと永続性タイプ。

(注)

イングレス構成で使用される Kubernetes サービスは NodePort タイプであることが想定されます。

- g) オプションで、[ イングレス説明 ] を指定します。
- h) [ 展開 ] をクリックします

デプロイする前に設定を確認する場合は、[ **Ingress Spec** の生成 ] をクリックします。指定された Ingress 設定は YAML 形式で表示されます。設定を確認したら、[ **Deploy** ] をクリックします。

(注)

Ingress 構成を使用して作成された仮想サーバーにライセンスを適用します。ライセンスを適用するには、次の手順に従います。

1. [ システム ] > [ ライセンスと分析 ] 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 ] を有効にします。

## NetScaler ADC プール容量

February 6, 2024

NetScaler ADC プール容量により、異なる ADC フォームファクタ間で帯域幅またはインスタンスライセンスを共有できます。仮想 CPU サブスクリプションベースのインスタンスの場合、仮想 CPU ライセンスをインスタンス間で共有できます。このプールされたキャパシティーは、データセンターまたはパブリッククラウドにあるインスタンスに使用します。インスタンスがリソースを必要としなくなると、割り当てられたキャパシティーを共通プールにチェックインし直します。解放された容量を、リソースを必要とする他の ADC インスタンスに再利用します。

プールされたライセンスを使用して、必要な帯域幅をインスタンスに割り当てて、必要量を超え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ずに、実行時にインスタンスに割り当てられる帯域幅を増減します。プール容量ライセンスを使用すると、インスタンスの Provisioning を自動化できます。

### NetScaler ADC プール容量ライセンスの仕組み

NetScaler ADC プール容量には、次のコンポーネントがあります。

- NetScaler ADC インスタンス。次のものに分類できます。
  - ゼロキャパシティーハードウェア
  - スタンドアロン VPX インスタンス、CPX インスタンスまたは BLX インスタンス
- 帯域幅プール
- インスタンスプール
- NetScaler ADM がライセンスサーバーとして構成されている

### ゼロキャパシティハードウェア

NetScaler ADC プール容量で管理する場合、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。これらのインスタンスは、帯域幅とインスタンスプールからリソースをチェックアウトするまで機能しないためです。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には、共通プールから帯域幅をチェックアウトできるプラットフォームライセンスと、インスタンスライセンスが必要です。

#### 注

MPX インスタンスには、インスタンスライセンスのサブスクリプションは必要ありません。MPX および SDX インスタンスでサポートされるプール容量については、このページの表 1 を参照してください。MPX および SDX フォームファクタのライセンス要件については、表 5 を参照してください。

### プラットフォームライセンスの管理とインストール

プラットフォームライセンスは、ハードウェアシリアル番号またはライセンスアクセスコードを使用して手動でインストールする必要があります。プラットフォームライセンスがインストールされると、そのライセンスはハードウェアにロックされ、NetScaler ADC ハードウェアインスタンス間でオンデマンドで共有できなくなります。ただし、プラットフォームライセンスを別の NetScaler ADC ハードウェアインスタンスに手動で移動することはできます。

ADC ソフトウェアリリース 11.1 ビルド 54.14 以降を実行する ADC MPX インスタンスと 11.1 ビルド 58.13 以降を実行する ADC SDX インスタンスは、ADC プールされた容量をサポートします。詳細については、表 1 を参照してください。MPX および SDX インスタンスのプール容量をサポートしました。

### スタンドアロン NetScaler ADC VPX インスタンス

次のハイパーバイザーで NetScaler ADC ソフトウェアリリース 11.1 Build 54.14 以降を実行している NetScaler ADC VPX インスタンスは、プール容量をサポートします。

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

次のハイパーバイザーおよびクラウドプラットフォームで NetScaler ADC ソフトウェアリリース 12.0 Build 51.24 以降を実行している NetScaler ADC VPX インスタンスは、プール容量をサポートします。

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

### 注

NetScaler ADM と Microsoft Azure または AWS 間の通信を有効にするには、IPSEC トンネルを構成する必要があります。詳細については、「[クラウドにデプロイされた NetScaler ADC VPX インスタンスを NetScaler ADM に追加する](#)」を参照してください。

ゼロキャパシティハードウェアとは異なり、VPX にプラットフォームライセンスは必要ありません。VPX では、トラフィック処理のためにプールから帯域幅とインスタンスライセンスをチェックアウトする必要があります。

### スタンドアロン **NetScaler ADC CPX** インスタンス

Docker er ホストにデプロイされた NetScaler ADC CPX インスタンスは、プール容量をサポートします。ゼロキャパシティハードウェアとは異なり、CPX にはプラットフォームライセンスは必要ありません。最大 1 Gbps のスループットを消費する単一の CPX インスタンスでは、インスタンスが 1 つだけチェックアウトされ、ライセンスプールからの帯域幅はありません。たとえば、20 Gbps の帯域幅プールを持つ 20 の CPX インスタンスがあるとします。CPX インスタンスの 1 つが 500 Mbps のスループットを消費する場合、残りの 19 個の CPX インスタンスの帯域幅プールは 20 Gbps のままになります。

同じ CPX インスタンスが 1500 Mbps のスループットを消費し始めた場合、残りの 19 個の CPX インスタンスに対して帯域幅プールは 19.5 Gbps になります。

プールライセンスの場合、10 Mbps の倍数でのみ帯域幅を追加できます。

### スタンドアロンの **NetScaler ADC BLX** インスタンス

NetScaler ADC BLX インスタンスは、プール容量ライセンスをサポートします。NetScaler ADC BLX インスタンスには、プラットフォームライセンスは必要ありません。トラフィックを処理するには、NetScaler ADC BLX インスタンスが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、NetScaler ADC インスタンス（物理および仮想の両方）で共有できる合計帯域幅です。帯域幅プールは、ソフトウェアエディション（スタンダード、アドバンス、プレミアム）ごとに個別のプールで構成されます。特定の NetScaler ADC インスタンスでは、異なるプールの帯域幅を同時にチェックアウトすることはできません。インスタンスが帯域幅をチェックアウトできる帯域幅プールは、ライセンスが割り当てられているソフトウェアエディションによって決まります。

### インスタンスプール

インスタンスプールは、NetScaler ADC プール容量を介して管理できる VPX インスタンス、CPX インスタンスまたは BLX インスタンスの数、または SDX-Z インスタンス内の VPX インスタンスの数を定義します。

プールからチェックアウトされると、ライセンスは MPX-Z、SDX-Z、VPX、CPX、および BLX インスタンスのリソース (CPU/PE、SSL コア、1 秒あたりのパケット数、帯域幅など) のロックを解除します。

注

SDX-Z の管理サービスでインスタンスが消費されることはありません。

### NetScaler ADM ライセンスサーバー

NetScaler ADC プール容量は、ライセンスサーバーとして構成された NetScaler ADM を使用して、プール容量ライセンス (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。NetScaler ADM ソフトウェアを使用すると、ADM ライセンスがなくてもプールされたキャパシティライセンスを管理できます。

帯域幅とインスタンスプールからライセンスをチェックアウトする場合、容量ゼロのハードウェア上の NetScaler ADC フォームファクタとハードウェアモデル番号によって、

- NetScaler ADC 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 ADC がチェックアウトできる最大帯域幅とインスタンス数。
- 帯域幅チェックアウトごとの最小帯域幅単位。最小帯域幅単位は、NetScaler ADC がプールからチェックアウトする必要がある最小帯域幅単位です。チェックアウトは、最小帯域幅単位の整数倍で行う必要があります。たとえば、NetScaler ADC 最小帯域幅単位が 1Gbps の場合、100Gbps をチェックアウトできますが、200Mbps または 150.5Gbps はチェックアウトできません。最小帯域幅の単位は、最小帯域幅の要件とは異なります。NetScaler ADC インスタンスは、少なくとも最小帯域幅でライセンスされた後のみ動作します。最小帯域幅が満たされると、インスタンスは最小帯域幅単位でより多くの帯域幅をチェックアウトできます。

表 1、2、3、4 は、サポートされているすべての NetScaler ADC インスタンスの最大帯域幅/インスタンス、最小帯域幅/インスタンス、最小帯域幅単位をまとめたものです。表 5 は、サポートされているすべての NetScaler ADC インスタンスについて、さまざまなフォームファクタのライセンス要件をまとめたものです。

表 1. MPX および SDX インスタンスでサポートされるプール容量

製品ライン	最大帯域幅 (Gbps)	最小帯域幅 (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
<b>MPX 5900Z</b>	10	1	-	-	1Gbps
<b>MPX 8005Z</b>	15	5	-	-	1Gbps
<b>MPX 8900Z</b>	33	5	-	-	1Gbps
<b>MPX 8900Z</b>	33	5	-	-	1Gbps
<b>FIPS</b>					

製品ライン	最大帯域幅 (Gbps)	最小帯域幅 (Gbps)	最小インスタ ス数	最大インスタ ス数	最小帯域幅単位
<b>MPX 14000Z</b> シリーズ	100	20	-	-	1Gbps
<b>MPX 14000Z</b> <b>40G</b> シリーズ	100	20	-	-	1Gbps
<b>MPX 14000Z</b> <b>FIPS</b> シリーズ	100	20	-	-	1Gbps
<b>MPX 14000Z</b> <b>40S</b> シリーズ	100	20	-	-	1Gbps
<b>MPX 15000Z</b> シリーズ	120	20	-	-	1Gbps
<b>MPX 15000Z</b> <b>FIPS</b> シリーズ	120	20	-	-	1Gbps
<b>MPX 15000Z</b> <b>50G</b> シリーズ	120	20	-	-	1Gbps
<b>MPX 115XX</b> シ リーズ	42	15	-	-	1Gbps
<b>MPX 22000Z</b> シリーズ	120	40	-	-	1Gbps
<b>MPX 24000Z</b> シリーズ	150	100	-	-	1Gbps
<b>MPX 25000Z</b> <b>40G</b>	200	100	-	-	1Gbps
<b>MPX 25000ZA</b>	200	100	-	-	1Gbps
<b>MPX 26000Z</b> シリーズ	200	100	-	-	1Gbps
<b>MPX 26000Z</b> <b>100G</b> シリーズ	200	100	-	-	1Gbps
<b>MPX 26000Z</b> <b>50S</b> シリーズ	200	100	-	-	1Gbps
<b>SDX 8015Z</b>	15	7	1	5	1Gbps
<b>SDX 8900Z</b>	33	10	2	7	1Gbps

製品ライン	最大帯域幅 (Gbps)	最小帯域幅 (Gbps)	最小インスタ ス数	最大インスタン ス数	最小帯域幅単位
<b>SDX 115XX</b> シ リーズ	42	8	2	20	1Gbps
<b>SDX 14000Z</b> シリーズ	100	10	2	25	1Gbps
<b>SDX 14000Z</b> <b>40G</b> シリーズ	100	10	2	25	1Gbps
<b>SDX 14000Z</b> <b>40S</b> シリーズ	100	20	10	25	1Gbps
<b>SDX 14000Z</b> <b>FIPS</b> シリーズ	100	10	2	25	1Gbps
<b>SDX 15000Z</b> <b>50G</b>	120	10	2 (注:13.0 47.x より低いバージ ョンの場合は5 インスタンス)	55	1Gbps
<b>SDX 15000Z</b>	120	10	2 注:13.0 47.x より低いバージ ョンの場合は5 つのインスタン ス)	55	1Gbps
<b>SDX 22000Z</b> シリーズ	120	20	20	80	1Gbps
<b>SDX 25000Z</b> <b>40G</b>	200	50	10	115	1Gbps
<b>SDX 25000ZA</b>	200	50	10	115	1Gbps
<b>SDX 26000Z</b> <b>100G</b>	200	50	10	115	1Gbps
<b>SDX 26000Z</b>	200	50	10	115	1Gbps
<b>SDX 26000Z</b> <b>50S</b>	200	50	10	115	1Gbps
<b>SDX 24000Z</b> シリーズ	150	50	10	80	1Gbps

注 最小帯域幅とインスタンスは、11.1 64.x、12.0 63.x、12.1 54.x、および 13.0 41.x のリリースを実行している SDX インスタンスに適用されます。

最小購入数量は、最小システム要件とは異なります。

表 2. CPX インスタンスでサポートされるプール容量

製品ライン	最大帯域幅 (Gbps)	最小帯域幅 (Mbps)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
<b>CPX</b>	10	10	1	1	10Mbps

表 3. ハイパーバイザーおよびクラウドサービス上の VPX インスタンス用にプールされた容量をサポート

ハイパーバイザ/クラウドサービス	最大帯域幅 (Gbps)	最小帯域幅 (Mbps)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
<b>Citrix Hypervisor</b>	40 Gbps	10Mbps	1	1	10Mbps
<b>VMware ESXi</b>	100 Gbps	10Mbps	1	1	10Mbps
<b>Linux KVM</b>	100 Gbps	10Mbps	1	1	10Mbps
<b>Microsoft Hyper-V</b>	3Gbps	10Mbps	1	1	10Mbps
<b>AWS</b>	30 Gbps	10Mbps	1	1	10Mbps
<b>Azure</b>	10 Gbps	10Mbps	1	1	10Mbps
<b>Google Cloud</b>	10 Gbps	10Mbps	1	1	10Mbps

注

最小購入数量は、最小システム要件とは異なります。

表 4. BLX インスタンスでサポートされるプール容量



製品ライン	最大帯域幅 (Gbps)	最小帯域幅 (Mbps)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
<b>BLX</b>	100	10	1	1	10Mbps

表 5. さまざまなフォームファクタのライセンス要件

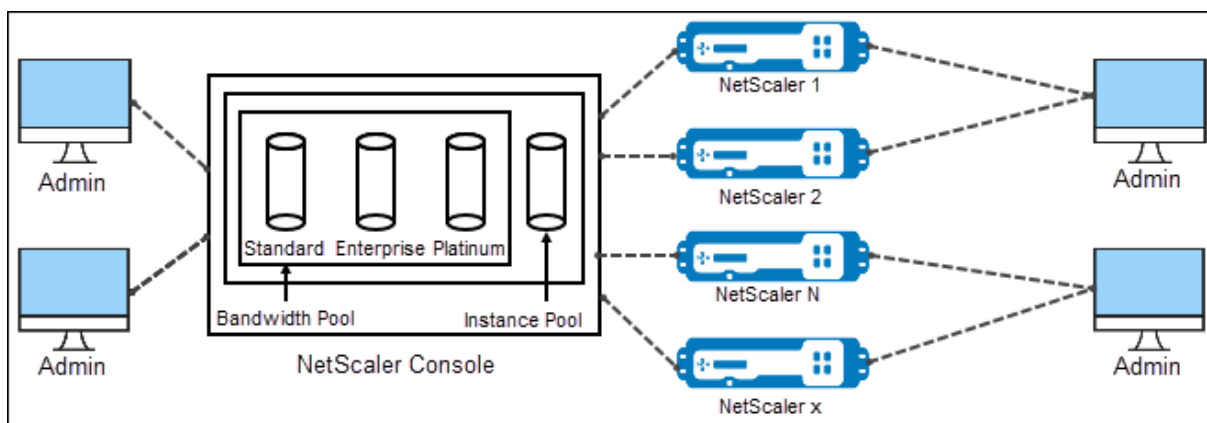
製品ライン	ゼロキャパシティハードウェアの購入	帯域幅およびエディションのサブスクリプション	インスタンスのサブスクリプション
<b>MPX</b>	ライセンスが必要です	ライセンスが必要です	-
<b>SDX</b>	ライセンスが必要です	ライセンスが必要です	ライセンスが必要です
<b>VPX</b>	-	ライセンスが必要です	ライセンスが必要です
<b>CPX</b>	-	-	ライセンスが必要です
<b>BLX</b>	-	ライセンスが必要です	ライセンスが必要です

## NetScaler ADC プール容量を構成する

February 6, 2024

ADC プール容量を使用するには、NetScaler ADM を必要な ADC インスタンスのライセンスサーバーとして構成します。ADC インスタンスは ADM からライセンスをチェックインおよびチェックアウトします。ADM GUI では、次のタスクを実行できます。

- プールされた容量ライセンスファイル（帯域幅とインスタンスプール）をライセンスサーバーにアップロードします。
- 必要に応じて、ライセンスプールから NetScaler ADC インスタンスにライセンスを割り当てます。
- インスタンスの最小容量と最大容量に基づいて、NetScaler ADC インスタンス（MPX-Z /SDX-Z/VPX/CPX/BLX）からライセンスを確認します。
- NetScaler ADC FIPS インスタンスがライセンスをチェックインまたはチェックアウトできるように、プールされた容量を構成します。



サポートされているハードウェアおよびソフトウェアのバージョン

プールされた容量でサポートされているハードウェアとソフトウェアのバージョンについては、「[NetScaler ADC プール容量](#)」を参照してください。

### ADC プール容量状態

プール容量状態は、ADC インスタンスのライセンス要件を示します。プールされたキャパシティで構成された ADC インスタンスは、次のいずれかの状態を表示します。

- **Optimum:** インスタンスは適切なライセンス容量で実行されています。
- **Capacity Mismatch:** インスタンスは、ユーザーが設定した容量よりも少ない容量で実行されています。
- **Grace:** インスタンスは猶予ライセンスで実行されています。
- **Grace & Mismatch:** インスタンスは猶予期間で実行されていますが、ユーザーが設定した容量よりも容量が少なくなっています。
- **利用不可:** インスタンスが管理用に ADM に登録されていないか、ADM からインスタンスへの NITRO 通信が機能していません。
- **未割り当て:** インスタンスにライセンスが割り当てられていません。

### ステップ 1-ADM でライセンスを適用する

1. NetScaler ADM で、[ネットワーク] > [ライセンス] に移動します。
2. [ライセンスファイル] セクションで、[ライセンスファイルの追加] を選択し、次のいずれかのオプションを選択します。
  - ローカルコンピュータからライセンスファイルをアップロードします。ローカルコンピュータにライセンスファイルがすでに存在する場合は、ADM にアップロードできます。

- ライセンスアクセスコードを使用します。Citrix から購入したライセンスのライセンスアクセスコードを指定します。次に、[ライセンスの取得] を選択します。次に、[完了] を選択します。

注:

[ライセンス設定] からいつでも **ADM** にライセンスを追加できます。

3. [完了] をクリックします。

ライセンスファイルが ADM に追加されます。[ライセンスの有効期限情報] タブには、ADM に存在するライセンスと有効期限までの残り日数が一覧表示されます。

4. [ライセンスファイル] で、適用するライセンスファイルを選択し、[ライセンスの適用] をクリックします。

この操作により、ADC インスタンスは選択したライセンスをプール容量として使用できます。

## 手順 2-NetScaler ADM をライセンスサーバーとして登録する

ADM をライセンスサーバーとして NetScaler ADC インスタンスに登録するには、次のいずれかの手順に従います。

- GUI を使用する
- CLI を使用

### GUI を使用して ADM をライセンスサーバーとして登録する

ADC GUI で、ADM サーバーをライセンスサーバーとして登録します。

1. NetScaler ADC GUI にログインします。
2. [システム] > [ライセンス] > [ライセンスの管理] に移動します。
3. [新規ライセンスの追加] をクリックします。
4. [リモートライセンスを使用する] を選択し、リストからリモートライセンスモードを選択します。
5. [サーバー名/IP アドレス] フィールドで、ADM サーバーの IP アドレスを指定します。
6. [NetScaler ADM に登録] を選択します。
7. ADM 認証情報を入力して NetScaler ADM にインスタンスを登録し、[続行] をクリックします。

## Licenses

If a license is already present on your local computer, you can upload it to this Citrix ADC appliance. If you have a license access code emailed by Citrix, to allocate licenses from the Citrix licensing portal.

To use pooled capacity, select Use pooled capacity and allocate licenses from a shared license server.

Upload license files

Use License Access Code

Use remote licensing

Remote Licensing Mode

Pooled Licensing ▾

Server Name/IP Address\*

License Port\*

27000

Citrix ADM access credentials to register

Username\*

nsroot

Password\*

.....

[Continue](#) [Back](#)

8. [ライセンスの割り当て] で、ライセンスエディションを選択し、必要な帯域幅を指定します。

初めて、NetScaler ADC でライセンスを割り当てます。ADM GUI からライセンス割り当てを後で変更または解放できます。

9. [**Get Licenses**] をクリックします。

### 重要

ライセンスエディションを変更した場合は、インスタンスをウォームリスタートします。設定の変更は、インスタンスを再起動するまで有効になりません。

**CLI** を使用して **ADM** をライセンスサーバーとして追加する

ADC インスタンスに GUI がない場合は、次の CLI コマンドを使用して ADM サーバーをライセンスサーバーとして追加します。

1. ADC コンソールにログインします。
2. ADM サーバの IP アドレスを追加します。

```
1 > add ns licenseserver <adm-server-IP-address> -port <adm-server-  
port-number>  
2 <!--NeedCopy-->
```

3. ライセンスサーバーで使用可能なライセンス帯域幅を表示します。

```
1 > sh ns licenseserverpool  
2 <!--NeedCopy-->
```

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。

```
1 > set ns capacity -unit gbps -bandwidth <specify-license-bandwidth  
> edition <specify-license-edition>  
2 <!--NeedCopy-->
```

ライセンスエディションには、スタンダード、エンタープライズ、プラチナがあります。

**重要:**

ライセンスエディションを変更する場合は、インスタンスをウォーム再起動します。

```
reboot -w
```

設定の変更は、インスタンスを再起動するまで有効になりません。

**ステップ 3-プールのライセンスを ADM インスタンスに割り当てる**

ADM GUI からプールキャパシティライセンスを割り当てるには、次の手順を実行します。

1. NetScaler ADM にログインします。
2. [ネットワーク] > [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 ADM にアップロードする場合にだけ表示されません。

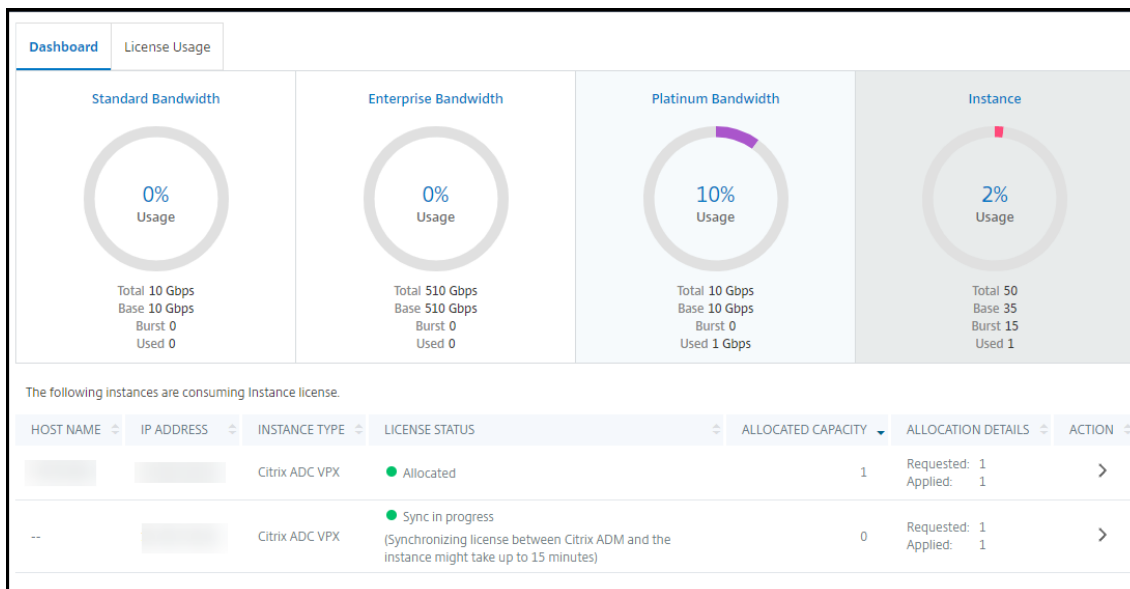
3. 管理するライセンスプールをクリックします。

(注)

[割り当てられたキャパシティ] フィールドには、変更された帯域幅がすぐには反映されません帯域幅の変更は、ADC のウォームリスタート後に有効になります。

[ 割り当ての詳細 ] の [ **Requested** ] および [ **Applied** ] フィールドは、インスタンスの帯域幅割り当てを変更すると更新されます。

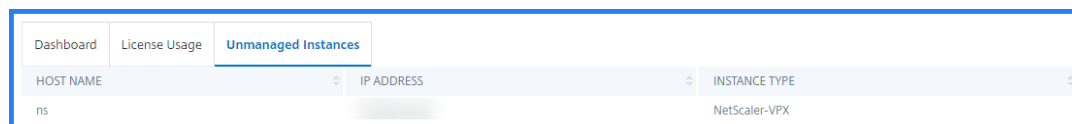
4. [ > ] ボタンをクリックして、使用可能なインスタンスのリストから ADC インスタンスを選択します。



ライセンスステータス列には、対応するライセンス割り当てステータスメッセージが表示されます。

注:

[管理対象外のインスタンス] タブには、NetScaler ADM で検出され管理されていないインスタンスが表示されます。



5. [ 割り当ての変更 ] または [ 割り当ての解除 ] をクリックして、ライセンスの割り当てを変更します。
6. ライセンスサーバーで使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。
7. [Allocate] リストオプションを設定することで、インスタンスへの帯域幅またはインスタンスの割り当てを選択できます。選択後、[ 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。

Change License Allocation
✕

License edition

Advanced ▾

TYPE	TOTAL	AVAILABLE	ALLOCATE
Instances	50	49	1
Bandwidth	510 Gbps	500 Gbps	<input style="width: 60px;" type="text" value="10000"/> <span style="font-size: 1.2em;">↕</span>

Mbps

Allocate

Cancel

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ます。

### ADC インスタンスでプールされたキャパシティを構成する

次の ADC インスタンスでプールキャパシティライセンスを設定できます。

- ADC MPX-Z インスタンス
- ADC VPX インスタンス
- ADC の高可用性ペア

### NetScaler ADC MPX-Z インスタンス

MPX-Z はプール容量対応の ADC MPX アプライアンスです。MPX-Z は、プレミアム、アドバンスト、またはスタンダードエディションのライセンスの帯域幅プーリングをサポートします。

MPX-Z をライセンスサーバーに接続するには、プラットフォームライセンスが必要です。MPX-Z プラットフォームライセンスは、次のいずれかでインストールできます。

- ローカルコンピュータからライセンスファイルをアップロードする。
- インスタンスのハードウェアシリアル番号を使用する。
- インスタンスの GUI の [システム] > [ライセンス] セクションにあるライセンスアクセスコード。

MPX-Z プラットフォームライセンスを削除すると、プールキャパシティ機能は無効になります。インスタンスライセンスがライセンスサーバーに解放されます。

MPX-Z インスタンスの帯域幅は、再起動せずに動的に変更できます。再起動が必要になるのは、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、構成済みの容量に必要なプールされたライセンスが自動的にチェックアウトされます。

### NetScaler ADC VPX インスタンス

プールキャパシティが有効な ADC VPX インスタンスは、帯域幅プール (プレミアム/アドバンス/スタンダードエディション) からライセンスをチェックアウトできます。ADC GUI を使用して、ライセンスサーバーからライセンスをチェックアウトできます。

VPX インスタンスの帯域幅は、再起動しなくても動的に変更できます。再起動が必要になるのは、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、構成済みのプールキャパシティライセンスは ADM サーバーから自動的にチェックアウトされます。

### NetScaler ADC の高可用性ペア

開始する前に、ADM サーバがライセンスサーバとして設定されていることを確認します。詳しくは、「ADM をライセンスサーバーとして構成する」を参照してください。

高可用性モードで構成された ADC インスタンスでは、高可用性ペアの各ノードでプールされた容量を構成する必要があります。プライマリノードとセカンダリノードの両方に、同じ容量のライセンスを割り当てる必要があります。たとえば、HA ペアの各インスタンスから 1 Gbps の容量が必要な場合は、共通プールから 2 倍の容量 (2 Gbps) が必要です。その後、各ノードに 1 Gbps の容量を割り当てることができます。

ペアの各ノードにプールライセンスを割り当てるには、プールされたライセンスを ADC インスタンスに割り当てるに記載されている手順に従います。最初に最初のノードにライセンスを割り当ててから、同じ手順を繰り返して 2 番目のノードにライセンスを割り当てます。

### ADM サーバーをプールされたライセンスサーバーとしてのみ構成する

February 6, 2024

管理者は、プールされたライセンスサーバーとしてのみ ADM サーバーを構成できます。この設定では、ADM サーバは ADC インスタンスからライセンスデータのみを受信します。

場合によっては、ADC インスタンスのデータを規制区域から退出することを制限する必要がある規制要件がある場合があります。このような状況では、規制区域に ADM オンプレムサーバーのローカルインスタンスをデプロイして、



管理、監視、および分析機能を使用できます。同じ方法でプールライセンス機能を使用する場合は、プールされたライセンスをさまざまな ADM ライセンスサーバー間で分割する必要があります。この方法では、グローバルにデプロイされた ADC インスタンスにプールされたライセンスを柔軟に割り当てることはできません。

したがって、ADM サーバはプールされたライセンスサーバとしてのみ構成します。ADM サーバは、すべての ADC インスタンスからライセンスデータのみを受信します。そのため、規制要件を遵守し、グローバルにデプロイされた ADC インスタンスにプールされたキャパシティーライセンスを動的に割り当てることができます。

このドキュメントでは、ADM サーバをプールされたライセンスサーバとしてだけ設定する方法について説明します。

### ADM サーバをプールされたライセンスサーバとしてのみ構成する方法

開始する前に、ADC インスタンスが ADM サーバに追加されていないことを確認してください。ステップ 4 を完了した後にはのみ、ADC インスタンスを追加します。

プールされたライセンスサーバだけの ADM サーバを構成するには、次の手順を実行します。

1. [システム] > [管理] に移動します。
2. [システム構成] セクションで、[システムの展開] を選択します。
3. [ADM 展開] で、プールされたライセンスサーバとして [ADM のみ] を選択します。

4. [OK] をクリックします。

このアクションでは、プールされたライセンス機能のみが保持され、次の ADM 機能が無効になります。

- ADM バックアップ
- イベントの管理
- SSL 証明書の管理
- ネットワークレポート作成
- ネットワーク機能
- 構成監査

注:

既定では、ADM 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。

ADM GUI には、プールされたライセンス機能だけが表示されます。また、残りのフィーチャは表示されません。

5. ライセンス機能だけに ADM を設定したら、[ネットワーク] > [インスタンス] ページで **ADC** インスタンスを追加します。

注

- ADC インスタンスは、1 つ以上の ADM サーバに追加できます。このような ADC インスタンスのパスワードを変更する場合は、インスタンスが検出されたすべての ADM サーバでパスワードを更新してください。
- ユーザーは、ADM GUI で無効化された機能の一部の操作を実行できます。たとえば、イベントポーリングや ADC バックアップなどです。スーパー管理者として、このような操作を制限する場合は、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ます。詳しくは、「[NetScaler ADM のアクセスポリシーの構成](#)」を参照してください。

## NetScaler ADC VPX の永続ライセンスを NetScaler ADC プール容量にアップグレードする

February 6, 2024

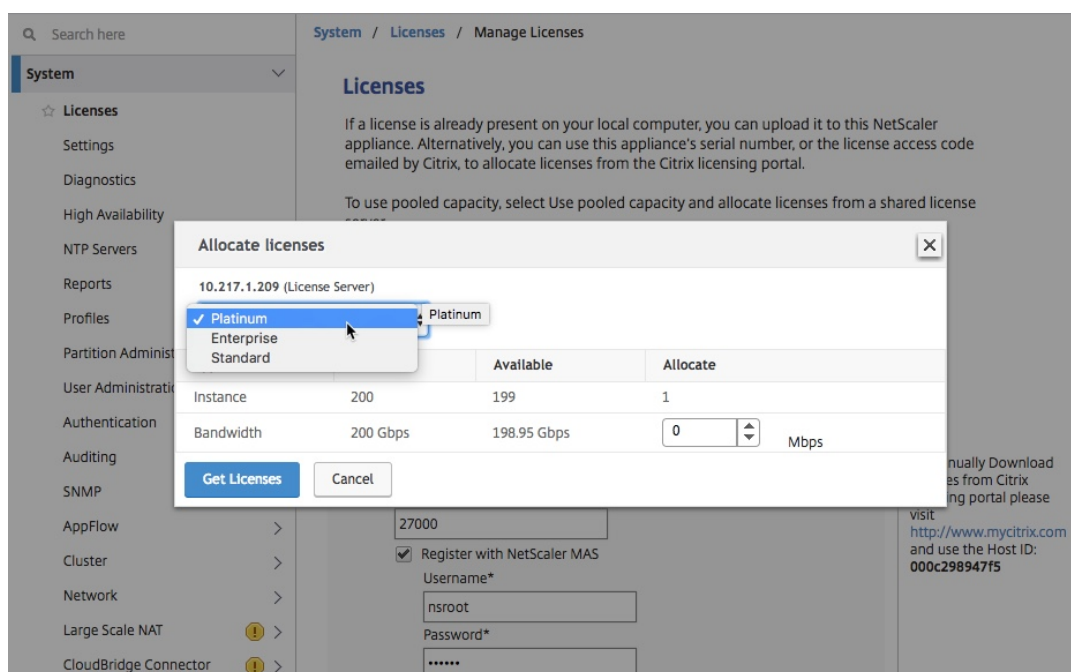
永続ライセンスを持つ NetScaler ADC VPX インスタンスは、ADC プール容量ライセンスにアップグレードできます。プールキャパシティライセンスにアップグレードすると、ライセンスプールから VPX インスタンスにオンデマンドでライセンスを割り当てることができます。高可用性モードで構成された ADC インスタンスに対して、プールされたキャパシティライセンスを構成することもできます。高可用性モードの VPX インスタンスのプール容量ライセンスを構成するには、NetScaler ADC VPX 高可用性ペアの永続ライセンスを NetScaler ADC プール容量にアップグレードするを参照してください。

### 前提条件

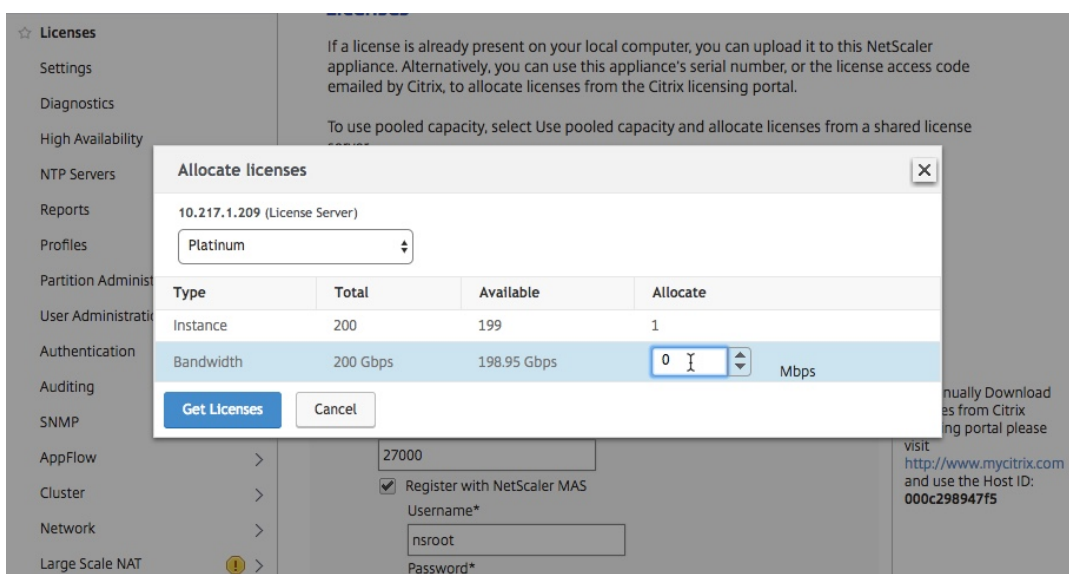
VPX インスタンスをバージョン 12.0.56.x にアップグレードしてください。

**NetScaler ADC** プール容量にアップグレードするには:

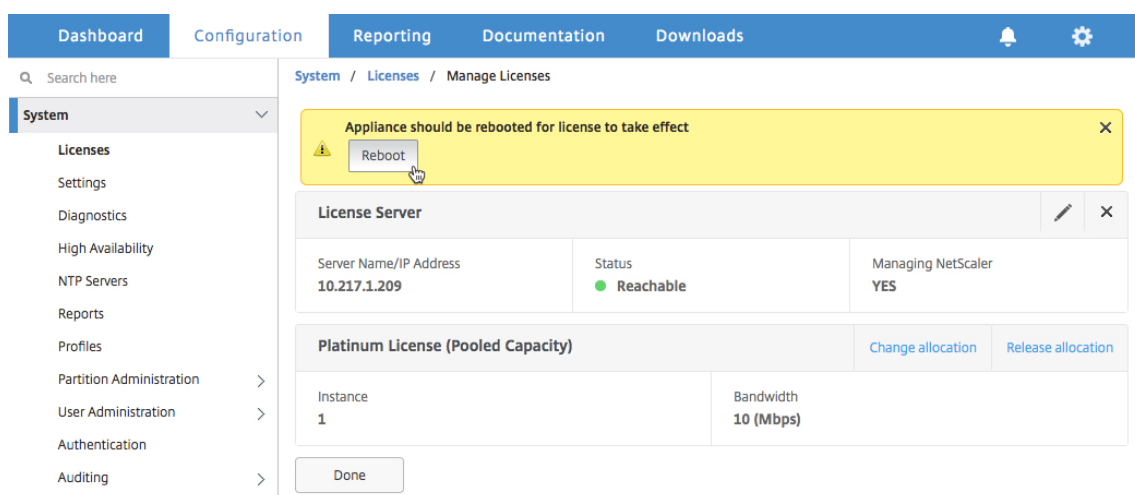
1. Web ブラウザで、VPX インスタンスの IP アドレス (<http://192.168.100.1>など) を入力します。
2. [ユーザー名] フィールドと [パスワード] フィールドに、管理者の資格情報を入力します。
3. [ようこそ] ページで、[続行] をクリックします。
4. [構成] タブで、[システム] > [ライセンス] に移動し、[ライセンスの管理] をクリックします。
5. [ライセンス] ページで、[新しい \*\* ライセンスの追加 \*\*] をクリックします。
6. [ライセンス] ページで、[リモートライセンスを使用する] を選択し、次の操作を行います。
  - a) [リモートライセンスモード] ドロップダウンリストで、[プールライセンス] を選択します。
  - b) [サーバ名/IP アドレス] フィールドに、ライセンスサーバの詳細を入力します。
  - c) **ADM** を使用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、[NetScaler ADM に登録] チェックボックスがオンになっていることを確認し、NetScaler ADM 資格情報を入力します。
  - d) [続行] をクリックします。
7. [ライセンスの割り当て] 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) [割り当て] メニューから NetScaler ADC アプライアンスに帯域幅を割り当てて、[ライセンスの取得] をクリックします。



8. プロンプトが表示されたら、[ **Reboot** ] をクリックしてアプライアンスを再起動します。



9. 確認ダイアログボックスで、「はい」をクリックします。

10. VPX インスタンスが再起動したら、インスタンスにログオンします。[ 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、NetScaler ADC VPX アプライアンスでライセンスされているすべての機能が表示されます。[ **X** ] をクリックします。

11. [ システム ] > [ ライセンス ] に移動し、[ ライセンスの管理 ] をクリックします。

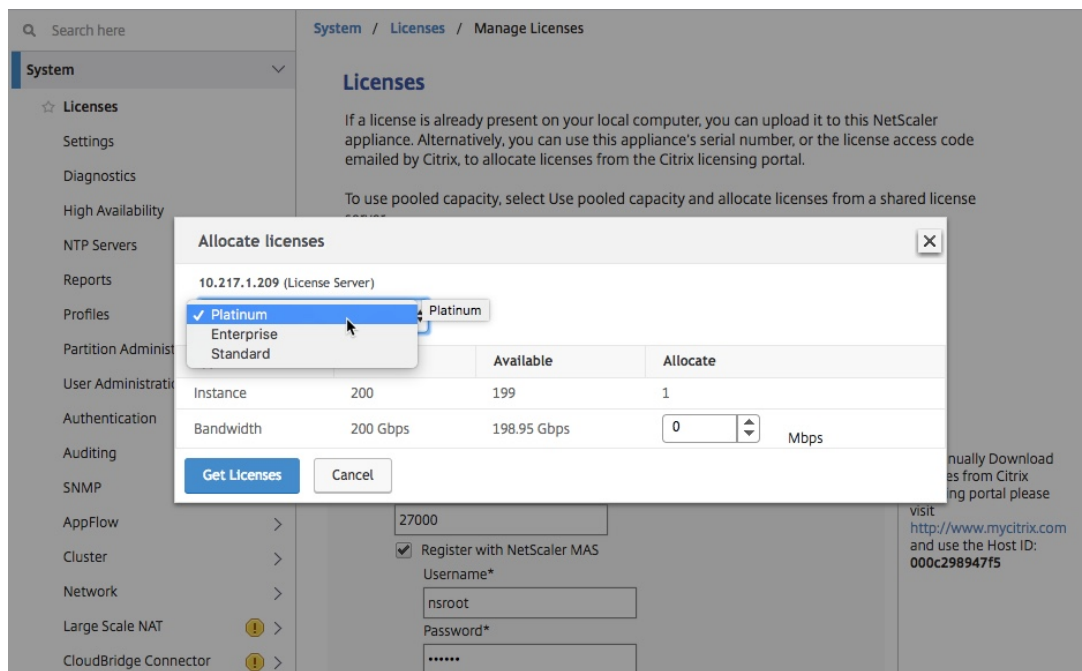
[ ライセンスの管理 ] ページでは、ライセンスサーバー、ライセンスエディション、および割り当てられた帯域幅の詳細を表示できます。

## NetScaler ADC VPX 高可用性ペアの永続ライセンスを NetScaler ADC プール容量にアップグレードする

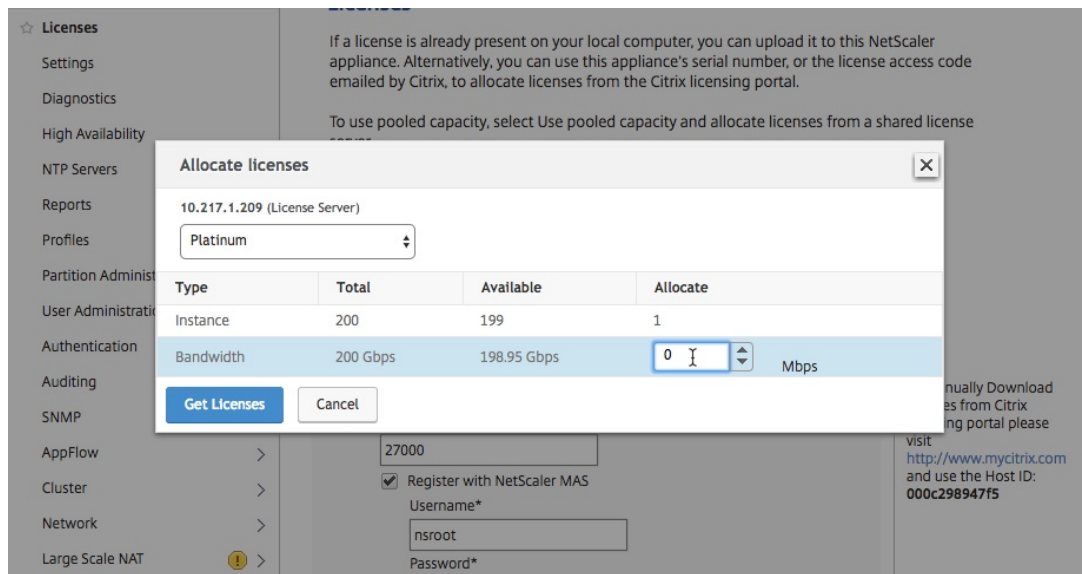
高可用性モードで構成された VPX インスタンスの場合、HA ペアのプライマリインスタンスとセカンダリインスタンスの両方にプールされた容量を構成する必要があります。プライマリインスタンスとセカンダリインスタンスの両方で、同じ容量のライセンスを割り当てる必要があります。たとえば、HA ペアの各インスタンスから 1 Gbps の容量が必要な場合は、共通プールから 2 倍の容量 (2 Gbps) が必要です。その後、HA ペアのプライマリインスタンスとセカンダリインスタンスにそれぞれ 1 Gbps の容量を割り当てることができます。

既存の **NetScaler ADC VPX HA** セットアップを **NetScaler ADC** プール容量にアップグレードするには:

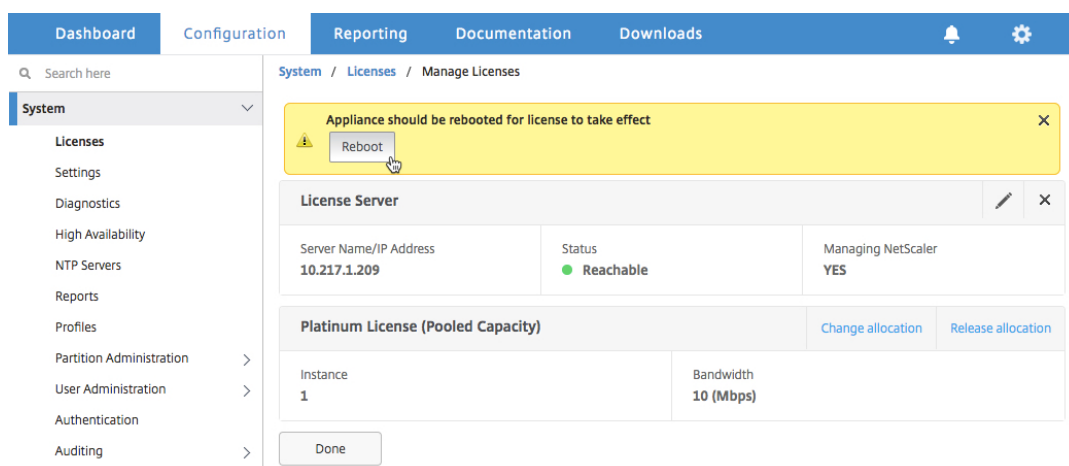
1. セカンダリ VPX (ノード 2) インスタンスにログオンします。Web ブラウザーで、NetScaler ADC アプリケーションの IP アドレス (<http://192.168.100.1> など) を入力します。
2. [ユーザー名] フィールドと [パスワード] フィールドに、管理者の資格情報を入力します。
3. [ようこそ] ページで、[続行] をクリックします。
4. [構成] タブで、[システム] > [ライセンス] に移動し、[ライセンスの管理] をクリックします。
5. [ライセンス] ページで、[新しい \*\* ライセンスの追加 \*\*] をクリックします。
6. [ライセンス] ページで、[リモートライセンスを使用する] を選択し、次の操作を行います。
  - a) [リモートライセンスモード] ドロップダウンリストで、[プールライセンス] を選択します。
  - b) [サーバ名/IP アドレス] フィールドに、ライセンスサーバの詳細を入力します。
  - c) **NetScaler ADM** を使用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、**[NetScaler ADM に登録]** チェックボックスがオンになっていることを確認し、ADM 資格情報を入力します。
  - d) [続行] をクリックします。
7. [ライセンスの割り当て] 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) [割り当て] メニューから NetScaler ADC アプライアンスに帯域幅を割り当てて、[ライセンスの取得] をクリックします。



c) プロンプトが表示されたら、[ **Reboot** ] をクリックしてインスタンスをウォームリスタートします。



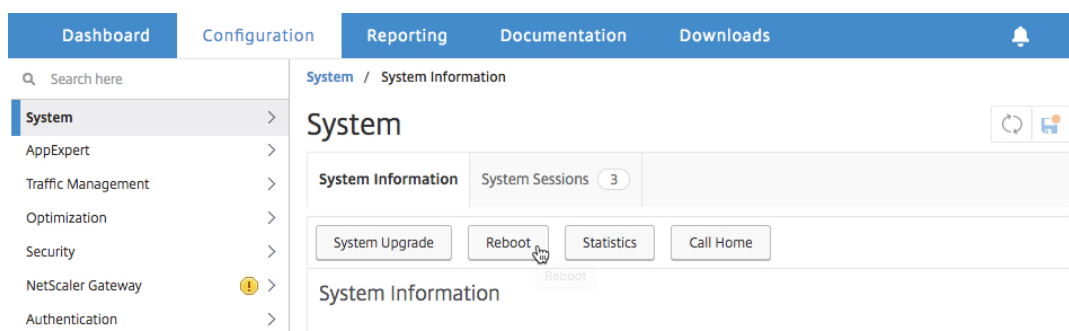
8. [確認] ダイアログボックスで、[はい] をクリックします。

VPX インスタンスが再起動します。

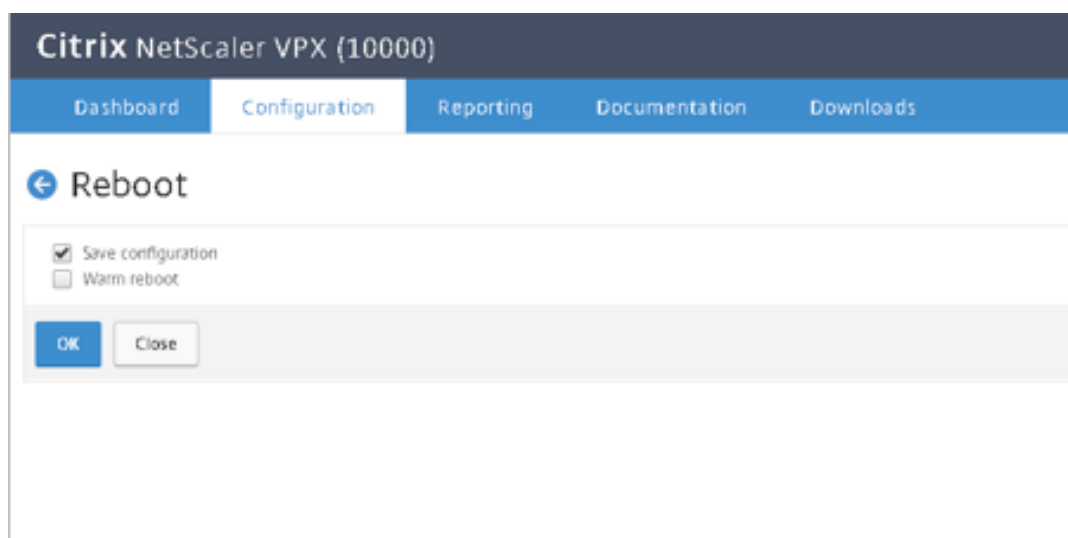
プロンプトが表示されたら、[ Reboot ] をクリックしてアプライアンスを再起動します。アプライアンスが新しいライセンスで起動して実行されたら、次のように入力してフェイルオーバーを強制します。  
`force ha failover` このフェイルオーバーにより、HA ペアの正常な状態が保証されます。

9. 既存のプライマリ VPX インスタンス (ノード 1) にログオンし、再起動します。以下のステップを完了します。

- a) Web ブラウザーで、NetScaler ADC 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) [ユーザー名] フィールドと [パスワード] フィールドに、管理者の資格情報を入力します。
- c) [ようこそ] ページで、[続行] をクリックします。
- d) [構成] タブで [システム] をクリックします。
- e) [システム] ページで、[再起動] をクリックします。



f) [再起動] ページで、[ウォーム再起動] を選択し、[OK] をクリックします。



ノード 1 が再起動すると、HA ペアのセカンダリインスタンスになります。HA ペアのプライマリインスタンスとセカンダリインスタンスを元の HA ペア設定に変更する場合は、フェイルオーバーを強制します。HA ペアの任意のインスタンスで次のコマンドを実行します。

“

強制フェイルオーバー

10. VPX インスタンスがプールキャパシティライセンスにアップグレードされたことを確認するには、プライマリインスタンスとセカンダリインスタンスにログオンし、次の手順を完了します。
  - a) [ ようこそ ] ページで、[ 続行 ] をクリックします。
  - b) [ 構成 ] タブで、[ システム ] > [ ライセンス ] に移動し、[ ライセンスの管理 ] をクリックします。[ ライセンスの管理 ] ページでは、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 ADC MPX の永続ライセンスを NetScaler ADC プール容量にアップグレードする

February 6, 2024

永続ライセンスを持つ NetScaler ADC MPX アプライアンスは、NetScaler ADC プール容量ライセンスにアップグレードできます。NetScaler ADC 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 ADC アプライアンスにライセンスをオンデマンドで割り当てることができます。高可用性モードで構成された NetScaler ADC インスタンスの NetScaler ADC プールキャパシティ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 ADC MPX インスタンスの NetScaler ADC プール容量ライセンスを構成するに



は、NetScaler ADC MPX 高可用性ペアの永続ライセンスを NetScaler ADC プール容量にアップグレードするを参照してください。

注

永久ライセンスからプールされたキャパシティライセンスへの移行は、ライセンスの権利付与のための一方向のプロセスです。プールされたキャパシティライセンスを永久ライセンスに戻すことはできません。

重要

Citrix ADC MPX アプライアンスを Citrix ADC プールキャパシティ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。

**Citrix ADC** プール容量にアップグレードするには:

1. Web ブラウザーで、NetScaler ADC アプライアンスの IP アドレス (<http://192.168.100.1>など) を入力します。
2. [ユーザー名] フィールドと [パスワード] フィールドに、管理者の資格情報を入力します。
3. [ようこそ] ページで、[続行] をクリックします。
4. ゼロキャパシティライセンス (MPX-Z ライセンス) をアップロードします。[構成] タブで、[システム] > [ライセンス] に移動します。
5. 詳細ペインで、[ライセンスの管理] をクリックし、[\*\*新しいライセンス\*\*の追加] をクリックします。
6. [ライセンス] ページで、[ライセンスファイルのアップロード] を選択し、[参照] をクリックして、ローカルマシンからゼロキャパシティライセンスを選択します。
7. ライセンスがアップロードされたら、[Reboot] 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、アプライアンスの SSL オフロードを含む機能のライセンスが解除されます。アプライアンスは HTTPS 要求の処理を停止します。

アップグレード前にアプライアンスで [セキュアアクセスのみ] オプションが有効になっている場合、HTTPS を使用して NetScaler ADM GUI 経由でアプライアンスに接続することはできません。

8. 「確認」 ページで、「はい」 をクリックします。
9. アプライアンスが再起動したら、アプライアンスにログオンします。
10. 「ようこそ」 ページで、「ライセンス」 セクションをクリックします。

**Dashboard** Configuration Reporting Documentation Downloads

**Welcome!**

Use this wizard for initial configuration of your NetScaler appliance. To configure or to change a previously configured setting, click each of the sections below. If a parameter has already been configured, a check mark appears within a green circle. An orange circle containing a dash indicates that you have chosen to skip this section.

	<b>NetScaler IP Address</b> IP address at which you access the NetScaler for configuration, monitoring, and other management tasks. NetScaler IP Address: <b>10.217.1.231</b>   Netmask: <b>255.255.255.0</b>	
	<b>Subnet IP Address</b> Specify an IP address for your NetScaler to communicate with the backend servers. Subnet IP Address: <i>Not configured</i>	
	<b>Host Name, DNS IP Address, and Time Zone</b> Specify a host name to identify your NetScaler, an IP address for a DNS server to resolve domain names, and the time zone in which your NetScaler is located. Host Name: <i>undefined</i>   DNS IP Address: <i>Not configured</i>   Time Zone: <b>CoordinatedUniversalTime</b>	
	<b>Licenses</b> Upload licenses from your local computer or allocate licenses from the Citrix licensing portal. You can also allocate pooled capacity from an on-premise license server. There are <b>3</b> license file(s) present on this NetScaler.	

**Continue**

11. [ライセンスサーバー] セクションで、次の操作を行います。

- a) [サーバ名/IP アドレス] フィールドに、ライセンスサーバの詳細を入力します。
- b) [ **License Port** ] フィールドに、ライセンスサーバのポートを入力します。デフォルト値: 27000。
- c) NetScaler ADM を使用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、[管理しやすくするためにライセンスサーバーに登録する] チェックボックスをオンにして、ADM 資格情報を入力します。
- d) [続行] をクリックします。

12. [ライセンスの割り当て] 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。

	Instance	Available	Allocate
Instance	200	197	1
Bandwidth	0 Mbps	0 Mbps	0 Gbps

- b) [割り当て] メニューから NetScaler ADC アプライアンスに帯域幅を割り当てて、[ライセンスの取得] をクリックします。

Type	Total	Available	Allocate
Instance	200	197	1
Bandwidth	200 Gbps	178.95 Gbps	50 Gbps

- c) プロンプトが表示されたら、[ **Reboot** ] をクリックしてアプライアンスを再起動します。

13. NetScaler ADC MPX アプライアンスが再起動したら、NetScaler ADC MPX アプライアンスにログインします。[ 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 ] > [ 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。

[ **Manage Licenses** ] ページでは、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 ADC MPX 高可用性ペアの永続ライセンスを NetScaler ADC プール容量にアップグレードする

高可用性モードで構成された MPX アプライアンスでは、HA ペアのプライマリ ADC インスタンスとセカンダリ ADC インスタンスの両方でプールされた容量を構成する必要があります。HA ペアのプライマリ NetScaler ADC インスタンスとセカンダリ NetScaler ADC インスタンスの両方に同じ容量のライセンスを割り当てます。たとえば、HA ペアの各インスタンスから 1 Gbps の容量が必要な場合は、共通プールから 2 Gbps の容量を割り当てる必要があります。2 Gbps の容量で、HA ペアのプライマリおよびセカンダリ NetScaler ADC インスタンスにそれぞれ 1 Gbps を割り当てることができます。

### 重要

NetScaler ADC MPX アプライアンスをアップグレードして NetScaler ADC プールキャパシティライセンスを使用するには、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

MPX-Z ライセンスを HA ペアのプライマリインスタンスとセカンダリインスタンスの両方にアップロードしてください。

**MPX-Z** ライセンスを **HA** ペアの **NetScaler ADC MPX** インスタンスに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 (<http://192.168.100.1>など) 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、管理者の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。[**Configuration**] タブで、[**System**] > [**Licenses**] の順に移動します。
5. 詳細ウィンドウで、[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、アプライアンスを再起動するように求められます。
7. [**Reboot**] 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。

既存の高可用性セットアップを **NetScaler ADC** プール容量にアップグレードするには:

1. セカンダリ NetScaler ADC MPX インスタンスにログオンします。Web ブラウザーで、NetScaler ADC アプライアンスの IP アドレス (<http://192.168.100.1>など) を入力します。
2. [ユーザー名] フィールドと [パスワード] フィールドに、管理者の資格情報を入力します。

3. 「ようこそ」 ページで、「ライセンス」 セクションをクリックします。

**Dashboard** Configuration Reporting Documentation Downloads

**Welcome!**

Use this wizard for initial configuration of your NetScaler appliance. To configure or to change a previously configured setting, click each of the sections below. If a parameter has already been configured, a check mark appears within a green circle. An orange circle containing a dash indicates that you have chosen to skip this section.

	<b>NetScaler IP Address</b> IP address at which you access the NetScaler for configuration, monitoring, and other management tasks. NetScaler IP Address: <b>10.217.1.231</b> Netmask: <b>255.255.255.0</b>	
	<b>Subnet IP Address</b> Specify an IP address for your NetScaler to communicate with the backend servers. Subnet IP Address: <i>Not configured</i>	
	<b>Host Name, DNS IP Address, and Time Zone</b> Specify a host name to identify your NetScaler, an IP address for a DNS server to resolve domain names, and the time zone in which your NetScaler is located. Host Name: <i>undefined</i> DNS IP Address: <i>Not configured</i> Time Zone: <b>CoordinatedUniversalTime</b>	
	<b>Licenses</b> Upload licenses from your local computer or allocate licenses from the Citrix licensing portal. You can also allocate pooled capacity from an on-premise license server. There are <b>3</b> license file(s) present on this NetScaler.	

**Continue**

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。

The screenshot shows the 'Configuration' tab in the NetScaler ADM interface. At the top, there are navigation tabs: Dashboard, Configuration, Reporting, Documentation, and Downloads. Below these, there are buttons for 'Add New License' and 'Delete'. A table lists licenses with columns for a checkbox and 'Name'. One license is listed: 'CNS\_MPX-Z\_1SERVER\_Retail.lic'. Below the table is the 'License Server' configuration section. It includes input fields for 'Server Name/IP Address\*' (10.217.1.209), 'License Port\*' (27000), a checked checkbox for 'Register with Licensing Server for manageability', 'User Name\*' (nsroot), and 'Password\*' (masked with dots). At the bottom of the form are 'Continue' and 'Cancel' buttons.

- a) [サーバ名/**IP** アドレス] フィールドに、ライセンスサーバの詳細を入力します。
  - b) [**License Port**] フィールドに、ライセンスサーバのポートを入力します。デフォルト値: 27000。
  - c) Citrix ADM を使用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、[管理しやすいようにライセンスサーバーに登録する] チェックボックスを選択し、ADM 認証情報を入力します。
  - 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。

The screenshot shows the 'Allocate licenses' dialog box. At the top, it says '10.217.1.209 (License Server)'. A dropdown menu is open, showing three options: 'Platinum' (selected with a checkmark), 'Enterprise', and 'Standard'. A tooltip 'Platinum' is visible next to the selected option. Below the dropdown is a table with columns for 'Instance', 'Available', and 'Allocate'. The table has two rows: 'Instance' with values 200, 197, and 1; and 'Bandwidth' with values 0 Mbps, 0 Mbps, and a spinner set to 0 Gbps. At the bottom are 'Get Licenses' and 'Cancel' buttons.

	Instance	Available	Allocate
	200	197	1
Bandwidth	0 Mbps	0 Mbps	0 Gbps

- b) [割り当て] メニューから NetScaler ADC アプライアンスに帯域幅を割り当てて、[ライセンスの取得] をクリックします。

Type	Total	Available	Allocate
Instance	200	197	1
Bandwidth	200 Gbps	178.95 Gbps	50 Gbps

- c) プロンプトが表示されたら、[ **Reboot** ] をクリックしてアプライアンスを再起動します。アプライアンスが新しいライセンスで起動して実行されたら、次のように入力してフェイルオーバーを強制します。  
`force ha failover` このフェイルオーバーにより、HA ペアの正常な状態が保証されます。

6. 既存のプライマリ NetScaler ADC 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。以下の手順に従います：

- Web ブラウザーで、NetScaler ADC 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。
- [ユーザー名] フィールドと [パスワード] フィールドに、管理者の資格情報を入力します。
- [ようこそ] ページで、[続行] をクリックします。
- [構成] タブで [システム] をクリックします。
- [システム] ページで、[再起動] をクリックします。
- [再起動] ページで、[ウォーム再起動] を選択し、[ **OK** ] をクリックします。

プライマリ NetScaler ADC 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 ADC MPX アプライアンスになります。HA ペアのプライマリインスタンスとセカンダリインスタンスを元の HA ペア設定に変更する場合は、フェイルオーバーを強制します。HA ペアの任意のインスタンスで次のコマンドを実行します。



```
1 > force ha failover
2 <!--NeedCopy-->
```

## NetScaler ADC SDX で永続ライセンスを NetScaler ADC プール容量にアップグレードする

February 6, 2024

永続ライセンスを持つ NetScaler ADC SDX アプライアンスは、NetScaler ADC プール容量ライセンスにアップグレードできます。NetScaler ADC 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 ADC アプライアンスにライセンスをオンデマンドで割り当てることができます。また、高可用性モードで構成された NetScaler ADC インスタンスに対して、ADC プール容量ライセンスを構成することもできます。

### 注

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、一方向のライセンスエンタイトルメントプロセスです。プールされたキャパシティライセンスを永続に戻すことはできません。

### 重要

- SDX アプライアンスを NetScaler ADC プール容量ライセンスにアップグレードするには、SDX-Z ライセンスをアプライアンスにアップロードする必要があります。
- ADM に ADC インスタンスを追加する権限があることを確認してください。

### Citrix ADC 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 (<http://192.168.100.1>など) 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、管理者の資格情報を入力します。
3. [ようこそ] ページで、[続行] をクリックします。
4. ゼロキャパシティライセンスをアップロードします。[構成] タブで、[システム]>[ライセンス] に移動します。
5. [ライセンスの管理] ページで、[ライセンスファイルの追加] をクリックします。
6. [ライセンス] ページで、[ローカルコンピュータ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、ローカルコンピュータからキャパシティゼロのライセンスを選択します。その後、[Finish] をクリックします。

### Licenses

If a license is already present on your local computer, you can upload it to this Citrix ADC SDX appliance. Alternatively, you can use this appliance's serial number, or the license access code emailed by Citrix, to allocate licenses from the Citrix licensing portal.

Upload license files from a local computer  
 Use license access code  
 Use hardware serial number(

To manually Download licenses from Citrix licensing portal please visit <http://www.mycitrix.com> and use the Host ID: 02c47a7a7ca0

容量ゼロのライセンスが正常に適用されると、[ライセンス] ページに [プールライセンス] セクションが表示されます。

7. [プールライセンス] セクションで、次の操作を行います。

#### Pooled licenses

You must now add a license server to this Citrix ADC SDX appliance and allocate the licenses from the license server.

Licensing Server Name or IP Address\*

Port Number\*

User Name\*

Password\*

Device Profile Name

- a) [ライセンスサーバ名] または [IP アドレス] フィールドに、ライセンスサーバの詳細を入力します。  
 ADM サーバをライセンスサーバとして設定する場合は、ADM サーバの IP アドレスを指定します。  
 エージェントを使用して ADM サーバと通信する場合は、ADM エージェントの IP アドレスを指定します。
  - b) 「ポート番号」フィールドに、ライセンスサーバのポートを入力します。デフォルト値: 27000。
  - c) [**Get Licenses**] 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。

**Allocate Licenses**
✕

(Licensing Server)

TYPE	TOTAL	AVAILABLE	ALLOCATE
Instances	35	35	2
Premium Bandwidth	0 (Gbps)	0 (Gbps)	0
Advanced Bandwidth	500 (Gbps)	500 (Gbps)	80
Standard Bandwidth	0 (Gbps)	0 (Gbps)	0

Allocate
Cancel

[ **Manage Licenses** ] ページでは、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。

License Server
✕

IP Address
Status  
● Reachable

Modify Allocation						Change Allocation	Release Allocation
Instance		Premium Bandwidth (Gbps)		Advanced Bandwidth (Gbps)		Standard Bandwidth (Gbps)	
2	0	0	0	80	0	0	0
Total	Used	Total	Used	Total	Used	Total	Used

#### 注

永続ライセンスをプールされた容量にアップグレードする場合、SDX アプライアンスを再起動する必要はありません。

## クラスターモードの **NetScaler ADC** インスタンス上の **NetScaler ADC** プール容量

February 6, 2024

クラスターとして構成された NetScaler ADC インスタンスで、NetScaler ADC プール容量を構成できます。クラスターモードで NetScaler ADC インスタンスでプール容量を構成するための前提条件は次のとおりです。

- インスタンスは、プールキャパシティライセンスモードで個別に実行され、クラスターを形成します。
- すべてのインスタンスが同じ帯域幅で実行されている必要があります。
- すべてのインスタンスが、同じ NetScaler Application Delivery Management (ADM) からプールされた容量をチェックアウトしました。

- 容量と NetScaler ADM 構成がクラスター内の既存のインスタンスの構成と同じでない限り、新しいインスタンスを既存の NetScaler ADC クラスターに追加することはできません。

Citrix ADC クラスターから容量をチェックアウトすると、すべてのクラスターノードに同じ容量が割り当てられ、チェックアウト帯域幅 = 提供された帯域幅 x ノード数が割り当てられます。

たとえば、NetScaler ADC クラスターから 50 Mbps の帯域幅をチェックアウトし、クラスターに 12 個のインスタンスが含まれている場合、各インスタンスは自動的に 50 Mbps を受け取ります。また、600 Mbps はプールからチェックアウトされています。

注

クラスター内の 1 つ以上のインスタンスが応答しなくなった場合、クラスターは残りのインスタンスの容量でトラフィックを処理し続けます。

### ADC プール容量を ADC クラスターに割り当てる

各クラスターノードに個別にライセンスを割り当てます。これは、クラスターノード間でライセンスを伝達および同期するコマンドが無効になっているためです。

各クラスターノードで以下の手順を繰り返します。

1. ウェブブラウザで、Citrix ADC IP アドレス (NSIP) を入力します。例: <http://192.168.100.1>。
2. [User Name] と [Password] の各フィールドに管理者の資格情報を入力します。
3. [設定] タブで、[システム] > [ライセンス] > [ライセンスの管理] に移動し、[新しいライセンスを追加] をクリックして、[プールライセンスを使用する] を選択します。
4. 「サーバー名/IP アドレス」フィールドにライセンスサーバーの名前またはアドレスを入力します。
5. Citrix ADM を使用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、[管理しやすくするために Citrix ADM に登録する] チェックボックスを選択し、ADM 認証情報を入力します。
6. ライセンスエディションと必要な帯域幅を選択し、[Get Licenses] をクリックします。

**Allocate licenses**
✕

10.102.29.55 (License Server)

Platinum ▼

Pool	Total	Available	Allocate
Instance	200	198	1
Bandwidth	500 Gbps	490 Gbps	<input style="width: 40px; text-align: center;" type="text" value="50"/> <span style="font-size: 0.8em;">Mbps</span>

Get Licenses

Cancel

7. [割り当ての変更] または [割り当ての解除] を選択すると、\*\* ライセンスの割り当てを変更または解除できません\*\*。

System / Licenses / Manage Licenses

License Server		
Server Name/IP Address 10.102.29.55	Status ● Reachable	Managing NetScaler YES
Platinum License (Pooled License)		Change allocation Release allocation
Instance 1	Bandwidth 90 (Mbps)	
Reboot		

8. [割り当ての変更] をクリックすると、ポップアップウィンドウに、ライセンスサーバで使用可能なライセンスが表示されます。

注

帯域幅の割当量は、対応するフォームファクターの最小帯域幅単位の整数倍にする必要があります。

**Allocate licenses** ✕

10.102.29.55 (License Server)

Platinum ▼

Pool	Total	Available	Allocate
Instance	200	197	1
Bandwidth	500 Gbps	489.9 Gbps	0 <input type="text"/> Mbps

Get Licenses Cancel

9. [割り当て] ドロップダウンリストから、帯域幅またはインスタンスを NetScaler ADC インスタンスに割り当てることができます。次に [ライセンスを取得] をクリックします。
10. ポップアップウィンドウのボックスの一覧で、ライセンスのエディションと必要な帯域幅を選択できます。

注

帯域幅の割り当てを変更する場合再起動は必要ありませんが、ライセンスのエディションを変更する場合はウォーム再起動が必要になります。

**CLI** を使用して **ADC** プール容量を **ADC** クラスターに割り当てる

各クラスターノードに個別にライセンスを割り当てます。これは、クラスターノード間でライセンスを伝達および同期するコマンドが無効になっているためです。

各クラスターノードで以下の手順を繰り返します。

1. SSH クライアントで、Citrix ADC IP アドレス (NSIP) を入力し、管理者の資格情報を使用してログインします。
2. ライセンスサーバーを追加するには、次のコマンドを入力します。

```
1 add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
  port number >]
2 <!--NeedCopy-->
```

```
> add ns licenseserver 10.102.29.97 -port 27000
Done
```

3. ライセンスサーバーで使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。

```
1 sh licenseserverpool
2 <!--NeedCopy-->
```

```
> sh licenseserverpool
Instance Total           : 0
Instance Available      : 0
Standard Bandwidth Total : 0 Mbps
Standard Bandwidth Availabe : 0 Mbps
Enterprise Bandwidth Total : 0 Mbps
Enterprise Bandwidth Available : 0 Mbps
Platinum Bandwidth Total : 0 Mbps
Platinum Bandwidth Available : 0 Mbps
VPX25S Total            : 1
VPX25S Available       : 1
VPX200E Total          : 1
VPX200E Available      : 1
VPX1000S Total         : 1
VPX1000S Available     : 1
VPX8000E Total         : 2
VPX8000E Available     : 1
Done
```

4. NetScaler ADC VPX アプライアンスにライセンスを割り当てるには、次のコマンドを入力します。

```
1 set capacity -platform V[S/E/P][Bandwidth]
2 <!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

## サーバーヘルス監視

February 6, 2024

ライセンスサーバーは、Citrix ADC プールキャパシティ対応インスタンスの状態を継続的に監視します。そのインスタンスは定期的なメッセージングによってライセンスサーバーと通信しています。連続してメッセージが受信されなければ、ライセンスサーバーは接続が切れたとレポートします。

デフォルトのアラームを補足するカスタムの通知を作成することができます。

### 猶予期間

Citrix ADC プールキャパシティ対応インスタンスが正常な状態にあり、ライセンスサーバーが応答を停止しても、インスタンスは現在の容量で 30 日間動作し続けます。30 日後もライセンスサーバーへの接続が回復していない場合、インスタンスはキャパシティを失ってトラフィック処理を停止します。

### 通知とアラーム

インスタンスで実行されるすべてのアクションについて、Citrix Application Delivery Management (ADM) から通知を有効にできます。カスタム通知設定とは別に、デフォルトで構成されているアラームもあります。たとえば、容量の一定割合が枯渇したプールを補充するためのアラームを設定するには、[インフラストラクチャ] > [ライセンス] > [設定] > [通知 \*\* 設定 \*\*] の順に選択し、[編集] ボタンをクリックします。

### Notification Settings

What would you like to be notified about?

Notify me on license usage  
To replenish a pool that has reached  % of its capacity

How would you like to be notified?

Email

SMS (Text Message)

Slack  
 PagerDuty  
 ServiceNow

Expiry of licenses  
How many days before the license expires do you want to be notified?

## 問題が発生したときに予想される動作

February 6, 2024

説明されている問題が発生した場合に、ライセンスサーバーと Citrix ADC インスタンスで予想される動作は次のとおりです。

ライセンスサーバーの応答停止



#### 警告

ライセンスサーバーが応答していません。NetScaler ADC は、30 日間現在の容量で動作し続けます。30 日後、ライセンスサーバーへの接続が復元されない場合、NetScaler ADC は現在の容量を失い、トラフィックの処理を停止します。

ライセンスサーバーが応答しなくなった場合、NetScaler ADC インスタンスは接続が回復するまで猶予期間に入ります。

#### **Citrix ADC** プールキャパシティ対応インスタンスが応答を停止する

NetScaler ADC プールキャパシティ対応インスタンスが応答を停止し、ライセンスサーバーが正常な状態にある場合、ライセンスサーバーは 10 分後にすべての NetScaler ADC インスタンスのライセンスをチェックインします。インスタンスが再起動すると、ライセンスサーバーからすべてのライセンスをチェックアウトする要求が送信されます。

#### ライセンスサーバーと **NetScaler ADC** プール容量が有効なインスタンスの両方が応答を停止する

ライセンスサーバーと NetScaler ADC プール容量対応インスタンスの両方が再起動して接続を再確立すると、ライセンスサーバーは 10 分後にすべてのライセンスをチェックインし、再起動の完了後に NetScaler ADC プール容量対応インスタンスによってライセンスが自動的にチェックアウトされます。

#### **NetScaler ADC** プールキャパシティが有効なインスタンスは正常にシャットダウンする

正常なシャットダウンの際には、このシャットダウンの前に割り当てられていたライセンスをチェックインするか保持するかを選択できます。ライセンスをチェックインすることを選択した場合、NetScaler ADC プールキャパシティが有効なインスタンスは、再起動後にライセンスが解除されます。ライセンスを保持する場合、インスタンスのシャットダウン時にそれらのライセンスがライセンスサーバーにチェックインされます。インスタンスは再起動後にライセンスサーバーとの接続を再確立し、保存済みの構成での指定されているとおりにライセンスをチェックアウトします。

システムが再起動し、プールに利用可能な容量がないためにチェックアウトが失敗した場合、NetScaler ADC は NetScaler Application Delivery Management (ADM) プールライセンスのインベントリをチェックし、使用可能な容量をチェックアウトします。NetScaler ADC がフルキャパシティで実行されていない場合、構成ごとに SNMP アラームが発生し、この状態をユーザーに通知します。帯域幅プールで使用可能な容量がない場合、プール容量が有効なインスタンスはライセンスされません。

#### ネットワーク接続の喪失

#### エラーメッセージ (syslog)

ライセンスサーバーが応答していません。

ライセンスサーバーと NetScaler ADC プールキャパシティ対応インスタンスが正常な状態にあるものの、ネットワーク接続が失われた場合、インスタンスは現在の容量で 30 日間稼働し続けます。30 日後もライセンスサーバーへの接続が回復していない場合、インスタンスはキャパシティを失ってトラフィック処理を停止し、ライセンスサーバーはライセンスすべてをチェックインします。ライセンスサーバーが NetScaler ADC インスタンスとの接続を再確立した後、インスタンスはライセンスを再度チェックアウトします。

### プール容量ライセンスの有効期限チェックの構成

February 6, 2024

NetScaler ADC プールキャパシティライセンスのライセンス有効期限のしきい値を設定できるようになりました。しきい値を設定することで、CitrixApplication Delivery Management (ADM) は、ライセンスの有効期限が切れるときに電子メールまたは SMS で通知を送信します。NetScaler ADM でライセンスの有効期限が切れた場合も、SNMP トラップと通知が送信されます。

ライセンス有効期限の通知が送信されると、イベントが生成され、このイベントは NetScaler ADM で表示できません。

ライセンスの有効期限チェックを構成するには、次の手順に従います。

1. [ネットワーク] > [ライセンス] に移動します。
2. [ライセンス設定] ページの [ライセンスの有効期限情報] セクションに、有効期限が切れるライセンスの詳細が表示されます。
  - 機能: 有効期限が切れる予定のライセンスのタイプ。
  - **Count**: 影響を受ける仮想サーバーまたはインスタンスの数。
  - 有効期限までの日数: ライセンスの有効期限までの日数。
3. [通知設定] セクションで、[編集] アイコンをクリックし、アラートのしきい値を指定します。プールされたライセンス容量の割合を設定して、管理者に通知することができます。
4. 適切なチェックボックスを選択して、送信する通知の種類を選択します。通知の種類を次に示します。
  - a) メールプロファイル: メールサーバーとプロファイルの詳細を指定します。ライセンスの有効期限が近づくと、メールがトリガーされます。
  - b) **SMS** プロファイル: ショートメッセージサービス (SMS) サーバーとプロファイルの詳細を指定します。ライセンスの有効期限が近づくと、SMS メッセージがトリガーされます。
5. 次に、ライセンスの有効期限が切れるまでの日数で通知を送信するタイミングを指定します。

6. [保存] をクリックします。

注

プールに新しいライセンスを追加すると、NetScaler ADC インスタンスは既存のライセンスの有効期限が切れた時点で新しいライセンスを使用します。

## NetScaler ADC VPX および BLX ライセンスのチェックインとチェックアウト

February 6, 2024

VPX および BLX ライセンスは、NetScaler Application Delivery Management (ADM) からオンデマンドで NetScaler ADC インスタンスに割り当てることができます。ADM ソフトウェアはライセンスを保存および管理します。ライセンスは、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を備えています。インスタンスは、プロビジョニング時に NetScaler ADM からライセンスをチェックアウトできます。インスタンスが削除または破棄されると、インスタンスは NetScaler ADM ソフトウェアにライセンスをチェックインします。

### 前提条件

次の前提条件が満たされていることを確認してください。

- ソフトウェアバージョン 12.0 を実行している Citrix ADC VPX イメージを使用しています。  
例: NSVPX-ESX-12.0-xx.xx\_nc.zip
- バージョン 12.0 を実行している Citrix ADM をインストールしました。  
例: MAS-ESX-12.0-xx.xx.zip

注

Citrix ADM で既存の VPX ライセンスを管理するには、ライセンスを Citrix ADM に再ホストする必要があります。

### Citrix ADM へのライセンスのインストール

注

: ソフトウェアのエディションまたは帯域幅を変更した場合は、ライセンスをインストールする前に、Citrix ADM 仮想アプライアンスを再起動してください。

**NetScaler ADM** にライセンスファイルをインストールするには:

1. Web ブラウザで、Citrix ADM IP アドレス (例: <http://192.168.100.1>) を入力します。

2. [User Name] と [Password] に管理者の資格情報を入力します。
3. [ネットワーク] > [ライセンス] に移動します。
4. 「ライセンスファイル」セクションで、次のオプションのいずれかを選択します。
  - ローカルコンピュータからのライセンスファイルのアップロード-ローカルコンピュータにライセンスファイルがすでに存在する場合は、NetScaler ADM にアップロードできます。  
ライセンスファイルを追加するには、[ **Browse** ] をクリックし、追加するライセンスファイル (.lic) を選択します。次に、[ 完了 ] をクリックします。
  - ライセンスアクセスコードを使用する -購入したライセンスのライセンスアクセスコードを電子メールで送信します。  
ライセンスファイルを追加するには、テキストボックスにライセンスアクセスコードを入力し、[ **Get Licenses** ] をクリックします。

注:

ライセンスアクセスコードを使用してライセンスをインストールする前に、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。

[ライセンス設定] からいつでも NetScaler ADM にライセンスを追加できます。

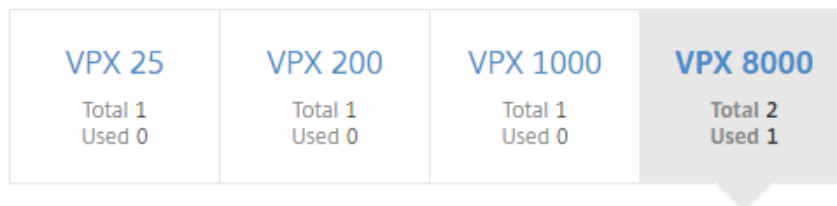
## 確認

Citrix ADM GUI で、使用可能なライセンスと割り当てられたライセンスを表示できます。

ライセンスを表示するには:

1. Web ブラウザで、Citrix ADM IP アドレス (例: <http://192.168.100.1>) を入力します。
2. [User Name] と [Password] に管理者の資格情報を入力します。
3. [構成] タブで、[ネットワーク] > [ライセンス] > [VPX ライセンス] に移動します。

## VPX Licenses



VPX <b>8000</b>	Enterprise Edition Total 2 Used 1		
The following instances are consuming VPX 8000 Enterprise Edition license.			
Name	IP Address	Allocation Status	Running
--	10.102.29.99	● Optimum	

4. 割り当て済みのライセンスは、利用可能なライセンスのセクションの下の表で表示できます。

### NetScaler ADC GUI を使用して VPX および BLX ライセンスを ADC インスタンスに割り当てる

1. Web ブラウザで、NetScaler ADC インスタンスの IP アドレス（例: <http://192.168.100.1>）を入力します。
2. [User Name] と [Password] の各フィールドに管理者の資格情報を入力します。
3. [構成] タブで、[システム] > [ライセンス] > [ライセンスの管理] に移動し、[ \*\* 新しいライセンスの追加 ] をクリックして、[ リモートライセンスを使用する ] > [ CICO ライセンス \*\* ] を選択します。
4. 「サーバー名/IP アドレス」フィールドにライセンスサーバーの詳細を入力します。
5. 上の画面の「ユーザー名」フィールドと「パスワード」フィールドに、Citrix ADM 資格情報を入力し、「続行」をクリックします。

## Licenses

If a license is already present on your local computer, you can upload it to this Citrix ADC appliance. Alternatively, you can use the license access code emailed by Citrix, to allocate licenses from the Citrix licensing portal.

To use pooled capacity, select Use pooled capacity and allocate licenses from a shared license server.

- Upload license files
- Use License Access Code
- Use remote licensing

Remote Licensing Mode

CICO Licensing ▾

Server Name/IP Address\*

License Port\*

27000

Citrix ADM access credentials to register

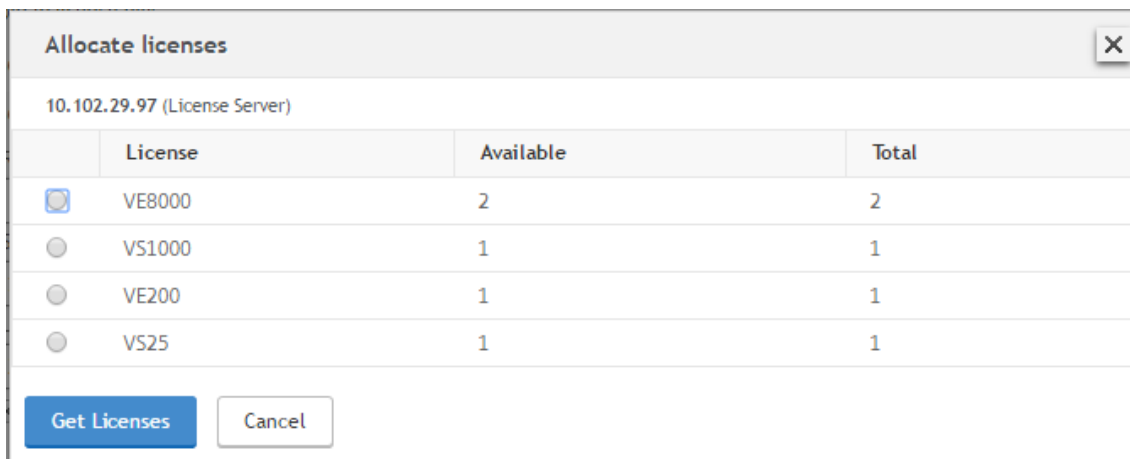
Username\*

Password\*

Continue

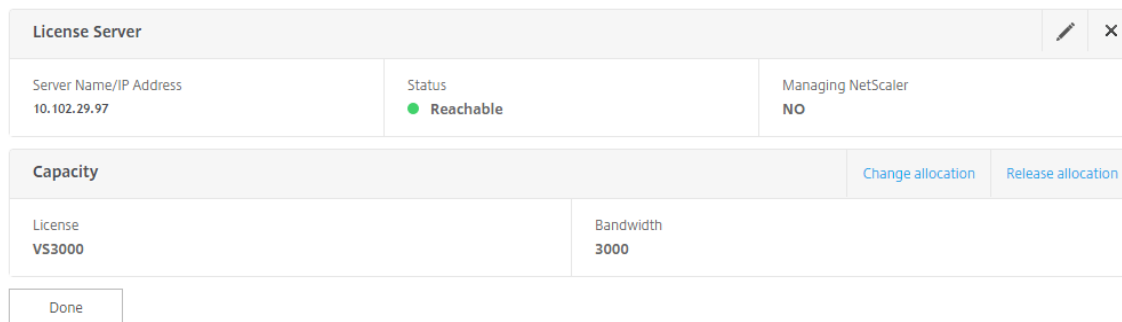
Back

6. 必要な帯域幅のライセンスエディションを選択し、[ **Get Licenses** ] をクリックします。

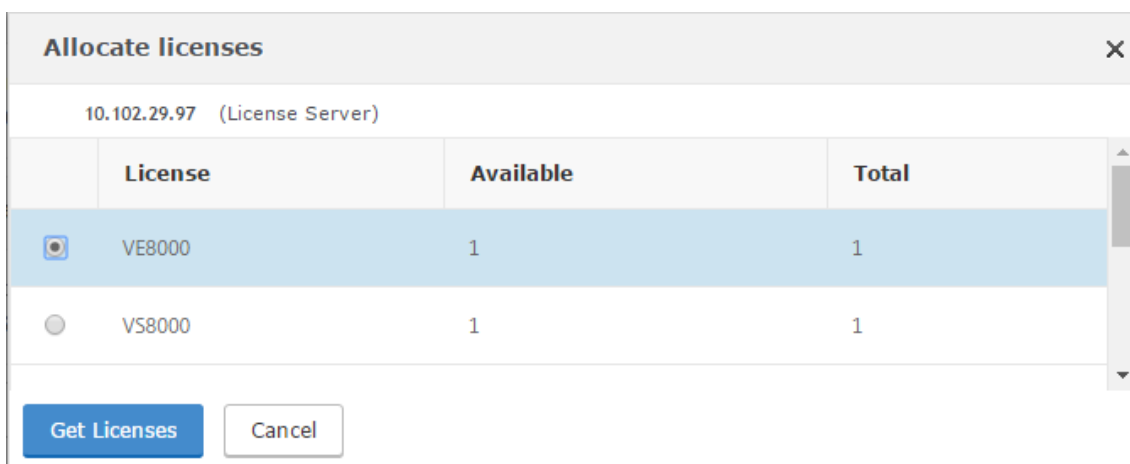


- [再起動] をクリックすると、NetScaler ADC インスタンスが再起動します。
- ライセンス割り当てを変更または解除するには、[システム] > [ライセンス] > [ライセンスの管理] に移動し、[割り当ての変更] または [割り当ての解除] を選択します。

System / Licenses / Manage Licenses



- [割り当ての変更] をクリックすると、ポップアップウィンドウに、ライセンスサーバで使用可能なライセンスが表示されます。必要なライセンスを選択し、[ライセンスを取得] をクリックします。



**NetScaler ADC CLI** を使用して **VPX** および **BLX** ライセンスを **ADC** インスタンスに割り当てる

1. SSH クライアントで、NetScaler ADC インスタンスの IP アドレスを入力し、管理者の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。

```
1 add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
  port number >]
2 <!--NeedCopy-->
```

```
> add ns licenseserver 10.102.29.97 -port 27000
Done
```

3. ライセンスサーバで使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。

```
1 sh licenseserverpool
2 <!--NeedCopy-->
```

```
> sh licenseserverpool
Instance Total           : 0
Instance Available      : 0
Standard Bandwidth Total : 0 Mbps
Standard Bandwidth Availabe : 0 Mbps
Enterprise Bandwidth Total : 0 Mbps
Enterprise Bandwidth Available : 0 Mbps
Platinum Bandwidth Total : 0 Mbps
Platinum Bandwidth Available : 0 Mbps
VPX25S Total            : 1
VPX25S Available       : 1
VPX200E Total           : 1
VPX200E Available      : 1
VPX1000S Total          : 1
VPX1000S Available     : 1
VPX8000E Total          : 2
VPX8000E Available     : 1
Done
```

4. NetScaler ADC アプライアンスにライセンスを割り当てるには、次のコマンドを入力します。

```
1 set capacity -platform V[S/E/P][Bandwidth]
2 <!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

**API** を使用して **VPX** および **BLX** ライセンスを **ADC** インスタンスに割り当てる

Web ブラウザーまたは API クライアントで、管理者の資格情報を使用して NetScaler ADC インスタンスにログオンします。

ライセンスサーバーを追加するには、次の手順に従います。

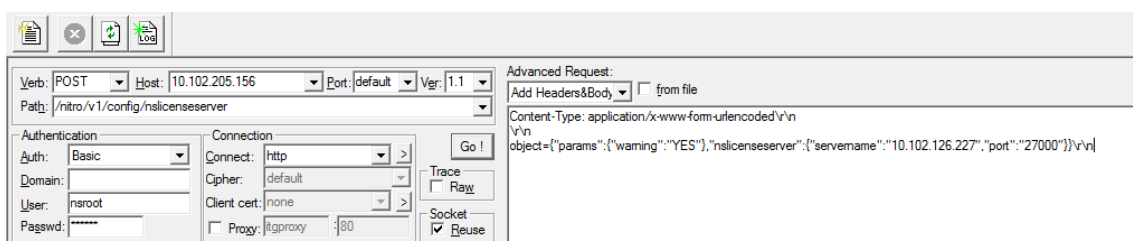


1. 要求タイプを「転記」に設定します。
2. パスに/nitro/v1/config/nslicensingserverを設定します。
3. ペイロードを次のように設定します。

```

1 content-type: application/x-www-form-urlencoded\r\n
2 \r\n
3 object= {
4   "params" ;{
5     warning : " yes" }
6   , " nslicensing server" ;{
7     servename : " <Citrix ADM IP>" , " port" : " 27000" }
8   }
9 \r\n
10 <!--NeedCopy-->

```



NetScaler ADM は要求に応答します。次のサンプル応答は、成功を示しています。

```

I RESPONSE: *****\n
H HTTP/1.1 201 Created\r\n
H Date: Fri, 06 Jan 2017 19:03:21 GMT\r\n
H Server: Apache\r\n
H Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
H Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
H Pragma: no-cache\r\n
H Content-Length: 57\r\n
H Content-Type: application/json; charset=utf-8\r\n
H \r\n
D { "errorcode": 0, "message": "Done", "severity": "NONE" }
finished.

```

ライセンスサーバで使用可能なライセンスを表示するには、次の手順を実行します。

1. リクエストタイプを **Get** に設定します。
2. パスに/nitro/v1/config/nslicenseserverpoolを設定します。

NetScaler ADM は要求に応答します。次のサンプル応答は成功と、ライセンスサーバーで利用可能なライセンスの一覧を示しています。

```

RESPONSE: *****\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:18:54 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 1874\r\n
Content-Type: application/json; charset=utf-8\r\n
\n
{ "errorCode": 0, "message": "Done", "severity": "NONE", "nslicenserverpool": { "instancetotal": 0, "instanceavailable": 0, "standardbandwidthtotal": 0, "standardbandwidthavailable": 0, "enterprisebandwidthtotal": 0, "enterprisebandwidthavailable": 0, "platinumbandwidthtotal": 0, "platinumbandwidthavailable": 0, "cpxinstanttotal": 0, "cpxinstantavailable": 0, "vpx1stotal": 0, "vpx1savailable": 0, "vpx1ptotal": 0, "vpx1pavailable": 0, "vpx5stotal": 0, "vpx5savailable": 0, "vpx5ptotal": 0, "vpx5pavailable": 0, "vpx10stotal": 0, "vpx10savailable": 0, "vpx10ptotal": 0, "vpx10pavailable": 0, "vpx10stotal": 0, "vpx10pavailable": 0, "vpx25stotal": 0, "vpx25savailable": 0, "vpx25ptotal": 0, "vpx25pavailable": 0, "vpx25stotal": 0, "vpx25pavailable": 0, "vpx50stotal": 0, "vpx50savailable": 0, "vpx50ptotal": 0, "vpx50pavailable": 0, "vpx50stotal": 0, "vpx50pavailable": 0, "vpx100stotal": 0, "vpx100savailable": 0, "vpx100ptotal": 0, "vpx100pavailable": 0, "vpx100stotal": 0, "vpx100pavailable": 0, "vpx200stotal": 0, "vpx200savailable": 0, "vpx200ptotal": 0, "vpx200pavailable": 0, "vpx200stotal": 0, "vpx200pavailable": 0, "vpx500stotal": 0, "vpx500savailable": 0, "vpx500ptotal": 0, "vpx500pavailable": 0, "vpx500stotal": 0, "vpx500pavailable": 0, "vpx1000stotal": 0, "vpx1000savailable": 0, "vpx1000ptotal": 0, "vpx1000pavailable": 0, "vpx1000stotal": 0, "vpx1000pavailable": 0, "vpx2000stotal": 0, "vpx2000savailable": 0, "vpx2000ptotal": 0, "vpx2000pavailable": 0, "vpx2000stotal": 0, "vpx2000pavailable": 0, "vpx3000stotal": 0, "vpx3000savailable": 0, "vpx3000ptotal": 0, "vpx3000pavailable": 0, "vpx3000stotal": 0, "vpx3000pavailable": 0, "vpx4000stotal": 0, "vpx4000savailable": 0, "vpx4000ptotal": 0, "vpx4000pavailable": 0, "vpx4000stotal": 0, "vpx4000pavailable": 0, "vpx5000stotal": 0, "vpx5000savailable": 0, "vpx5000ptotal": 0, "vpx5000pavailable": 0, "vpx5000stotal": 0, "vpx5000pavailable": 0, "vpx8000stotal": 1, "vpx8000savailable": 1, "vpx8000ptotal": 1, "vpx8000pavailable": 1 } }
finished.

```

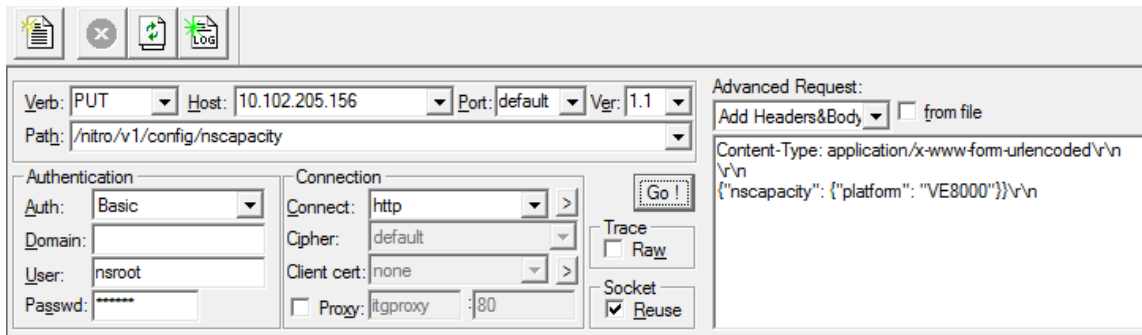
### NetScaler ADC アプライアンスにライセンスを割り当てるには:

1. 要求タイプを「転記」に設定します。
2. パスに/nitro/v1/config/nscapacityを設定します。
3. ペイロードを次のように設定します。

```

1 content-type: application/x-www-form-urlencoded\r\n
2 \r\n
3 {
4   "nscapacity":{
5     "platform" : " VE8000 " }
6   }
7 \r\n
8 <!--NeedCopy-->

```



NetScaler ADM は要求に応答します。次のサンプル応答は、成功を示しています。

```

1 RESPONSE: *****\n
2 HTTP/1.1 200 OK\r\n
3 Date: Fri, 06 Jan 2017 19:16:21 GMT\r\n
4 Server: Apache\r\n
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
7 Pragma: no-cache\r\n
8 Content-Length: 57\r\n
9 Content-Type: application/json; charset=utf-8\r\n
10 \r\n
11 { "errorcode": 0, "message": "Done", "severity": "NONE" }
12 finished.
    
```

#### ライセンスサーバーの IP アドレスを更新する

VPX および BLX インスタンスのライセンスサーバーの IP アドレスは、インスタンスに割り当てられたライセンス帯域幅に影響を与えたり、データを損失したりすることなく更新できます。

**CLI** を使用した更新:**CLI** を使用してライセンスサーバーの IP アドレスを更新するには、インスタンスで次のコマンドを入力します。

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

このコマンドは、新しいサーバーに接続し、以前のライセンスサーバーに関連付けられたリソースを解放します。

**GUI** を使用した更新: **GUI** を使用してライセンスサーバーの IP アドレスを更新するには、[システム] > [ライセンス] > [ライセンスの管理] に移動し、[新しいライセンスの追加] をクリックします。詳細については、「NetScaler ADC GUI を使用して VPX および BLX ライセンスを ADC インスタンスに割り当てる」を参照してください。

#### NetScaler ADC VPX および BLX チェックインおよび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 ADC VPX および BLX ライセンスのライセンス有効期限の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切れると、NetScaler ADM が電子メールまたは SMS で通知を送信します。NetScaler ADM でライセンスの有効期限が切れると、SNMP トラップと通知も送信されます。

ライセンス有効期限の通知が送信されると、イベントが生成され、このイベントは NetScaler ADM で表示できません。

ライセンスの有効期限チェックを構成するには、次の手順に従います。

1. [ネットワーク] > [ライセンス] に移動します。
2. ライセンス設定 ページの「ライセンス 有効期限情報」セクションで、有効期限が切れるライセンスの詳細を確認できます。
  - 機能: 有効期限が切れる予定のライセンスのタイプ。
  - 数: 影響を受ける仮想サーバーまたはインスタンスの数。
  - 有効期限までの日数: ライセンスの有効期限までの日数。
3. [通知設定] セクションで、[編集] アイコンをクリックし、アラートのしきい値を指定します。プールされたライセンス容量の割合を設定して、管理者に通知することができます。
4. 適切なチェックボックスを選択して、送信する通知の種類を選択します。通知の種類を次に示します。
  - a) メールプロファイル: メールサーバーとプロファイルの詳細を指定します。ライセンスの有効期限が近づくと、メールがトリガーされます。
  - b) **SMS** プロファイル: ショートメッセージサービス (SMS) サーバーとプロファイルの詳細を指定します。ライセンスの有効期限が近づくと、SMS メッセージがトリガーされます。
5. 次に、ライセンスの有効期限が切れるまでの日数で通知を送信するタイミングを指定します。
6. [保存] をクリックします。

## NetScaler ADC 仮想 CPU ライセンス

February 6, 2024

皆さんのようなデータセンターの管理者は、ネットワーク機能を簡素化すると同時に、コスト削減と拡張性の向上を実現する新しいテクノロジーに移行しています。新しいデータセンターのアーキテクチャには、少なくとも次の機能が含まれている必要があります。

- ソフトウェア定義ネットワーク (SDN)
- ネットワーク機能仮想化 (NFV)
- ネットワーク仮想化 (NV)
- マイクロサービス

このような動きには、絶え間なく変化するビジネスニーズを満たすために、ソフトウェア要件が動的、柔軟かつ機敏であることも必要です。ライセンスは、使用状況を完全に把握できる中央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。

## Citrix ADC VPX の仮想 CPU ライセンス

以前は、NetScaler ADC 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 ADC 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、特定の帯域幅や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。使用可能な帯域幅を増やすには、より多くの帯域幅を提供するライセンスエディションにアップグレードする必要があります。特定のシナリオでは、帯域幅要件は小さくても、SSL TPS、圧縮スループットなど、他の L7 パフォーマンスの要件はより高くなる場合があります。このような場合、NetScaler ADC VPX ライセンスのアップグレードは適切ではない可能性があります。ただし、CPU 負荷の高い処理に必要なシステムリソースのロックを解除するには、帯域幅が大きいライセンスを購入する必要があります。NetScaler ADM は、仮想 CPU 要件に基づく NetScaler ADC インスタンスへのライセンスの割り当て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、特定の NetScaler ADC VPX が資格を持つ CPU の数がライセンスに指定されます。そのため、NetScaler ADC VPX は、ライセンスサーバー上で実行されている仮想 CPU の数だけライセンスをチェックアウトできます。NetScaler ADC 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 ADC VPX は、ライセンスのチェックアウト中にアイドル状態の 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 ADM ライセンスサーバーは個別の仮想 CPU ライセンスを管理します。また、仮想 CPU ライセンスで管理されているエディションは、スタンダード、アドバンス、プレミアムの 3 つです。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でロック解除された機能と同じ機能のセットをロック解除します。

仮想 CPU の数に変更されたり、ライセンスエディションが変更されたりする場合があります。このような場合、新しいライセンスのセットのリクエストを開始する前に、常に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 ADC VPX を再起動します。

**GUI** を使用して **NetScaler ADC VPX** でライセンスサーバーを構成するには：

1. NetScaler ADC VPX で、[システム] > [ライセンス] に移動し、[ライセンスの管理] をクリックします。
2. ライセンスページで、「新規ライセンスを追加」をクリックします。
3. ライセンスページで、「リモートライセンスを使用する \*\*」オプションを選択します。
4. \*\* リモートライセンスモードリストから CPU\*\* ライセンスを選択します。
5. ライセンスサーバーの IP アドレスとポート番号を入力します。
6. [続行] をクリックします。

Upload license files  
 Use License Access Code  
 Use remote licensing

Remote Licensing Mode

CPU Licensing

Server Name/IP Address\*

10.217.220.60

License Port\*

27000

Register with NetScaler MAS

注:

NetScaler ADC VPX インスタンスは常に NetScaler ADM に登録する必要があります。まだ行っていない場合は、[NetScaler ADM に登録] を有効にして、NetScaler ADM のログイン資格情報を入力します。

- [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、使用可能な仮想 CPU の合計数と割り当て可能な CPU が表示されます。[Get Licenses] をクリックします。
- 次のページで [Reboot] をクリックして、ライセンスを申請します。

Appliance should be rebooted for license to take effect

Reboot

License Server	
Server Name/IP Address	Status
10.217.220.60	● Reachable

CPU Capacity		Change allocation	Release allocation
Edition	Count		
Platinum	16		

注:

現在のライセンスをリリースして、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 ライセンスをすでに実行しているとします。そのライセンスをリリースしてから、Advanced Edition からチェックアウトできます。

## CLI を使用した NetScaler ADC VPX ライセンスでのライセンスサーバーの構成

NetScaler ADC VPX コンソールで、次のコマンドを入力して次の 2 つのタスクを実行します。

- ライセンスサーバーを NetScaler ADC VPX に追加するには:

```
1 add licenseserver <IP address of the license server>
2 <!--NeedCopy-->
```

2. ライセンスを申請するには:

```
1 set capacity -vcpu - edition premium
2 <!--NeedCopy-->
```

プロンプトが表示されたら、次のコマンドを入力してインスタンスを再起動します。

```
1 reboot -w
2 <!--NeedCopy-->
```

ライセンスサーバーの **IP** アドレスを更新する

VPX インスタンスのライセンスサーバーの IP アドレスを更新できます。インスタンスに割り当てられたライセンス帯域幅に影響を与えたり、データを失ったりすることはありません。ライセンスサーバーの IP アドレスを更新するには、VPX インスタンスで次のコマンドを入力します。

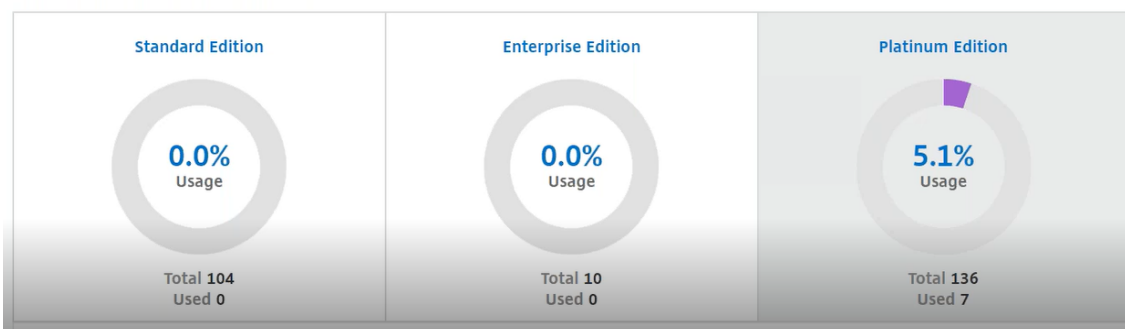
```
add licenseserver <licensing server IP address> -forceUpdateIP
```

このコマンドは、新しいサーバーに接続し、以前のライセンスサーバーに関連付けられたリソースを解放します。

## NetScaler ADM での仮想 CPU ライセンスの管理

1. Citrix ADM で、[ネットワーク] > [ライセンス] > [仮想 CPU ライセンス] に移動します。
2. このページには、各ライセンスエディションに割り当てられたライセンスが表示されます。
3. 各ドーナツ内の番号をクリックすると、このライセンスを使用している NetScaler ADC インスタンスが表示されます。

### Virtual CPU Licenses



## NetScaler ADC CPX 用の仮想 CPU ライセンス

NetScaler ADC CPX インスタンスをプロビジョニングするときに、インスタンスの CPU 使用率に応じて、ライセンスサーバーからライセンスをチェックアウトするように NetScaler ADC CPX インスタンスを構成できます。

NetScaler ADC CPX は、NetScaler ADM 上で稼働するライセンスサーバーを利用してライセンスを管理します。NetScaler ADC CPX は、起動時にライセンスサーバーからライセンスをチェックアウトします。NetScaler ADC CPX がシャットダウンすると、ライセンスはライセンスサーバーにチェックインされます。

NetScaler ADC CPX は、Docker アプリストアからダウンロードできます。Docker ホストで、NetScaler ADC CPX をダウンロードするには、次のコマンドを実行します。

```
docker pull store/citrix/netscalercpx: [version]
```

CPX ライセンスには、次の 3 つのライセンスタイプがあります。

1. CPX と VPX でサポートされる仮想 CPU サブスクリプションライセンス
2. プールキャパシティライセンス
3. CPX のみの単一または複数の vCPU をサポートする CP1000 ライセンス

**NetScaler ADC CPX** インスタンスの **Provisioning** 中に **vCPU** サブスクリプションライセンスを構成するには:

NetScaler ADC CPX インスタンスが使用する vCPU ライセンスの数を指定します。

- この値は、Docker、Kubernetes、または Mesos/Marathon を通じて環境変数として入力されます。
- ターゲット変数は「CPX\_CORES」です。CPX は 1 から 16 コアまでサポートできます。

2 つのコアを指定するには、次のように docker run コマンドを実行します。

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
   -e EULA=yes -e CPX_CORES=2
2 <!--NeedCopy-->
```

NetScaler ADC CPX インスタンスをプロビジョニングする際には、次に示すように、**docker run** コマンドで **Citrix** ADC ライセンスサーバーを環境変数として定義します。

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
   -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
   LS_PORT> cpx:11.1
2 <!--NeedCopy-->
```

各項目の意味は次のとおりです。

- <LS\_IP\_ADDRESS> は NetScaler ADC ライセンスサーバーの IP アドレスです。
- <LS\_PORT> は Citrix ADC ライセンスサーバーのポートです。デフォルトのポートは 27000 です。



## 注:

デフォルトでは、NetScaler ADC CPX インスタンスは vCPU サブスクリプションプールからライセンスをチェックアウトします。インスタンスが「n」個の CPU で実行されている場合、CPX インスタンスは「n」個のライセンスをチェックアウトします。

**NetScaler ADC CPX** インスタンスの **Provisioning** 時に **NetScaler ADC** プールキャパシティまたは **CP1000** ライセンスを構成するには:

プールライセンス (帯域幅ベース) または CPX プライベートプール (CP1000 またはプライベートプールベース) を使用して CPX インスタンスのライセンスをチェックアウトする場合は、それに応じて環境変数を指定する必要があります。

## 例:

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
  -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
    LS_PORT> -e PLATFORM=CP1000 cpx:11.1
2 <!--NeedCopy-->
```

**CP1000.** このコマンドは、CP1000 プール (CPX プライベートプール) からのチェックアウトをトリガーします。次に、NetScaler ADC CPX インスタンスは、CPX\_CORES に指定された「n」個のコアに対して「n」個のインスタンスを取得します。最も一般的な使用例は、1つのインスタンスのチェックアウトに  $n=1$  を指定することです。マルチコア CPX のユースケースでは、「n」個の vCPU (「n」は 1~7) をチェックアウトします。

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
  -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
    LS_PORT> -e BANDWIDTH=2000 cpx:11.1
2 <!--NeedCopy-->
```

プールされた容量。このコマンドは、インスタンス・プールから 1つのライセンスをチェックアウトし、プレミアム帯域幅プールから 1000 Mbps の帯域幅を消費しますが、CPX は最大 2000Mbps まで稼働できます。プールライセンスでは、最初の 1000 Mbps は課金されません。

## 注

: 次の表に示すように、帯域幅プールからチェックアウトするときに、目的のターゲット帯域幅に対応する vCPU の数を指定します。

コア数 (vCPU)	最大帯域幅
1	1000Mbps
2	2000 Mbps
3	3500 メガビット/秒
4	5000Mbps

5	6500 メガビット/秒
6	8000Mbps
7	9300 メガビット/秒

## Citrix SD-WAN インスタンスの管理

February 6, 2024

Citrix ADM を使用すると、ネットワーク内の Citrix SD-WAN アプライアンスの分析を監視、管理、および表示できます。次の相互運用性表は、Citrix SD-WAN プラットフォームの各エディションで現在サポートされている Citrix ADM の機能に関する情報を示しています。

### Citrix SD-WAN プラットフォームエディションと NetScaler ADM 機能の操作性マトリックス

プラットフォーム版	検出中	構成	監視	レポート (ネットワークレポート)	イベント管理	HDX Insight	WAN Insight
Citrix SD-WAN WANOP	はい	はい	はい	はい	はい	はい	はい
Citrix SD-WAN SE	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
Citrix SD-WAN PE	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ

### Citrix ADM がサポートする Citrix SD-WAN バージョン

プラットフォーム版	Citrix SD-WAN バージョン	Citrix ADM バージョン
Citrix SD-WAN WANOP	Citrix CloudBridge 7.4 以降	Citrix ADM 11.0 以降
Citrix SD-WAN SE	Citrix SD-WAN 9.3.0 以降のバージョンでは、	NetScaler ADM 12.0.53.8 以降

プラットフォーム版	Citrix SD-WAN バージョン	Citrix ADM バージョン
Citrix SD-WAN PE	Citrix SD-WAN 9.3.0 以降のバージョンでは、	NetScaler ADM 12.0.53.8 以降

---

Citrix SD-WAN WANOP アプライアンスを管理インスタンスとして NetScaler ADM に追加できます。詳しくは、「[NetScaler ADM へのインスタンスの追加](#)」を参照してください。Citrix SD-WAN WANOP インスタンスの WAN Insight、HDX Insight、ネットワークレポート、イベントレポートを表示できます。

NetScaler ADM では、Citrix SD-WAN スタンダードエディション (SE) およびエンタープライズエディション (EE) アプライアンスが自身を NetScaler ADM で管理対象インスタンスとして登録できます。

Citrix SD-WAN SE/PE/AE アプライアンスを NetScaler ADM に追加するには、Citrix SD-WAN SE/PE/AE アプライアンスで NetScaler ADM を AppFlow コレクタとして構成します。Citrix SD-WAN SE/PE/AE アプライアンスは、それ自身を NetScaler ADM 上で管理対象インスタンスとして追加します。SD-WAN SE/PE/AE アプライアンスは、分析データを NetScaler ADM に送信します。

NetScaler ADM は、各 SD-WAN SE/PE/AE デバイスの AppFlow コレクタとして個別に設定することも、Citrix SD-WAN Center を使用して構成を管理アプライアンスにエクスポートすることもできます。

詳細については、「[NetScaler ADM での Citrix SD-WAN SE/PE/AE インスタンスの追加](#)」を参照してください。

Citrix SD-WAN PE アプライアンスの場合、AppFlow の構成に応じて、HDX データレコードまたはマルチホップデータを表示できます。Citrix SD-WAN SE アプライアンスは、マルチホップデータのみを提供します。詳しくは、[HDX \[Insight のレポートとメトリクスの表示およびマルチホップ展開用の Analytics データの表示を参照してください\]\(/ja-jp/netscaler-application-delivery-management-software/13/manage-sd-wan-wo-instances/view-sd-wan-analytics-data-multi-hop-deployment.html\)](#)。

このページでは、NetScaler ADM をセットアップし、NetScaler ADM を使用して SD-WAN WANOP アプライアンスを管理するために参照できるトピックへのクイックアクセスリンクを提供します。

### **Citrix ADM** の概要

[Citrix ADM について](#)

[アーキテクチャ](#)

[Citrix ADM がインスタンスを検出する方法](#)

[Citrix ADM が管理対象インスタンスと通信する方法](#)

### **Citrix ADM** デプロイメント

[Citrix Hypervisor で Citrix ADM をデプロイする](#)

[Microsoft Hyper-V を使用して NetScaler ADM を展開する](#)

[VMware ESXi で Citrix ADM をデプロイする](#)

[Linux KVM サーバーを使用した NetScaler ADM デプロイ](#)

[Citrix ADM を高可用性モードでデプロイする](#)

[NetScaler Insight Center から NetScaler ADM への移行](#)

[Citrix ADM を Director と統合](#)

## インスタンス管理

[Citrix ADM にインスタンスを追加する方法](#)

[Citrix ADM でインスタンスグループを作成する方法](#)

[Citrix ADM を使用してインスタンスをバックアップおよび復元する方法](#)

## 構成管理

[Citrix ADM の修正コマンドから構成ジョブを作成する方法](#)

[Citrix ADM の組み込みテンプレートを使用して作成されたジョブをスケジュールする方法](#)

[Citrix ADM 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](#)

[実行済みの構成ジョブを再使用する方法](#)

## 分析

[WAN Insight](#)

[HDX Insight](#)

[Citrix SD-WAN WANOP インスタンスのネットワークレポートを表示する方法](#)

[アダプティブしきい値を構成する方法](#)

[分析用のデータベースの概要を構成する方法](#)

[Citrix ADM を使用してしきい値とアラートを作成する方法](#)

## イベント管理

[Citrix ADM でイベントのイベント経過時間を設定する方法](#)

[Citrix ADM を使用してイベントフィルターをスケジュールする方法](#)

[Citrix ADM からのイベントに繰り返し電子メール通知を設定する方法](#)

[Citrix ADM を使用してイベントを抑制する方法](#)

[Citrix SD-WAN WANOP インスタンスのイベントレポートを表示する方法](#)

[Citrix ADC インスタンスで発生するイベントの報告された重要度を変更する方法](#)

[NetScaler ADM でイベントの概要を表示する方法](#)

[Citrix ADM のインフラストラクチャダッシュボードに 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](#)

## 認証

[外部認証サーバーをカスケードする方法](#)

[RADIUS 認証サーバーを追加する方法](#)

[LDAP 認証サーバーを追加する方法](#)

[TACACS 認証サーバーを追加する方法](#)

[Citrix ADM で認証サーバーグループを抽出する方法](#)

[ローカル認証のフォールバックを有効にする方法](#)

## NetScaler ADM システム

[Citrix ADM システムの管理](#)

[Citrix ADM をアップグレードする方法](#)

[Citrix ADM のテクニカルサポートファイルを生成する方法](#)

[単一サーバー展開で Citrix ADM サーバーをバックアップおよび復元する方法](#)

[高可用性ペアの Citrix ADM 構成をバックアップおよび復元する方法](#)

[Citrix ADM でデフォルト以外のユーザーのシェルアクセスを有効にする方法](#)

[Citrix ADM で NTP サーバーを構成する方法](#)

[Citrix ADM の SSL 設定を構成する方法](#)

[Citrix ADM のシスログ消去間隔を構成する方法](#)

[NetScaler ADM 監査情報を表示する方法](#)

[NetScaler ADM システム通知設定を構成する方法](#)

[Citrix ADM の CPU、メモリ、およびディスクの使用状況を監視する方法](#)

[Citrix ADM の暗号グループを構成する方法](#)

[Citrix ADM で SNMP トラップ、マネージャー、およびユーザーを作成する方法](#)

[Citrix ADM サーバーにホスト名を割り当てる方法](#)

[Citrix ADM のシステムブルーニング設定を構成する方法](#)

[Citrix ADM を使用してシステムバックアップ設定を構成する方法](#)

[NetScaler ADM でシステムアラームを構成および表示する方法](#)

## Citrix SD-WAN インスタンスの追加

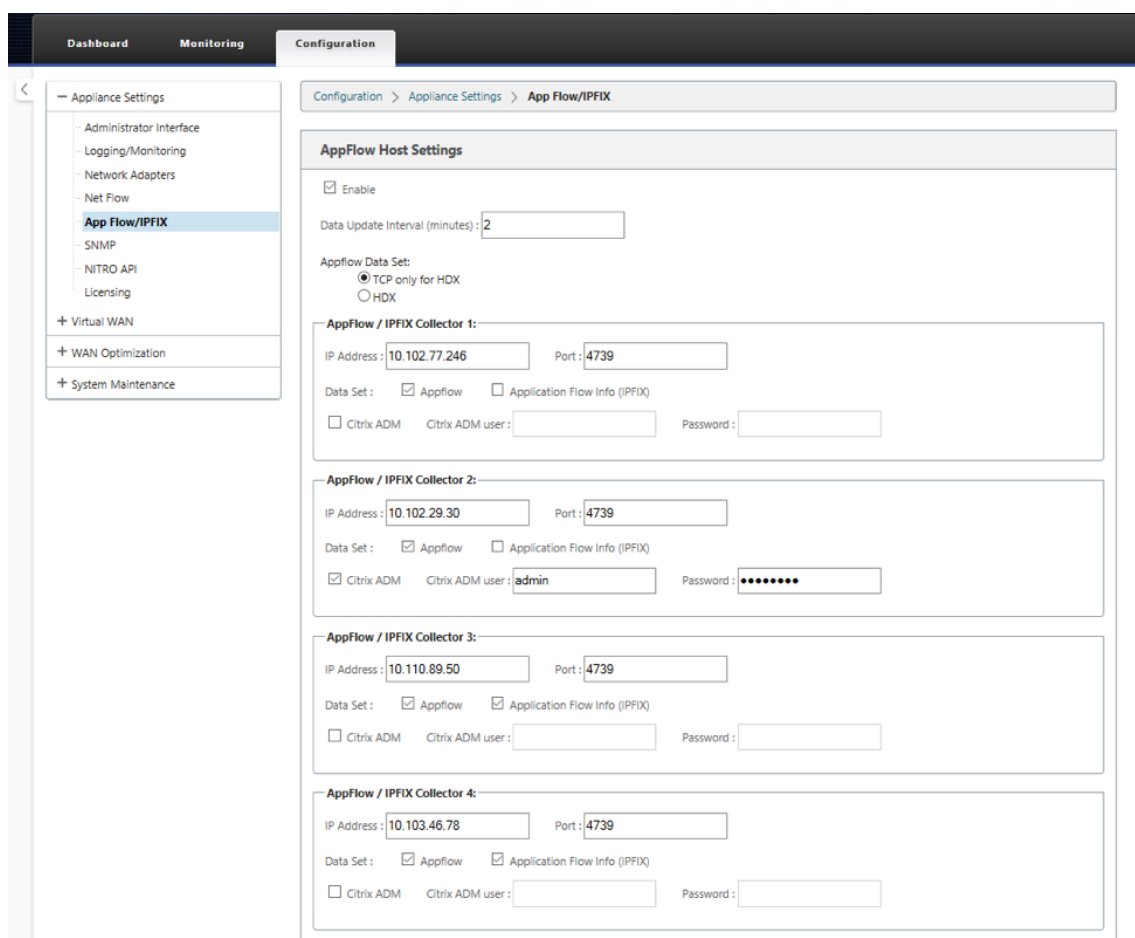
February 6, 2024

NetScaler ADM にこれらのインスタンスを追加するには、Citrix SD-WAN SE/PE アプライアンスの AppFlow コレクターとして NetScaler ADM を構成します。Citrix SD-WAN SE/PE/AE アプライアンスは、NetScaler ADM で管理されたインスタンスとして登録され、AppFlow レコードが収集されます。**Citrix SD-WAN PE** アプライアンスの場合、**HDX** テンプレートのみの TCP または HDX テンプレートのいずれかを有効にできます。**HDX 専用 TCP** テンプレートはマルチホップデータを提供します。**HDX** テンプレートは HDX データを提供します。データセンター アプライアンスでのみ有効にしてください。

NetScaler ADM は、個々の SD-WAN SE/PE/AE アプライアンス上で AppFlow コレクタとして構成できます。または、SD-WAN Center を使用して NetScaler ADM を AppFlow コレクタとして構成し、その構成を管理しているアプライアンスにエクスポートできます。

**Citrix SD-WAN SE/PE/AE** アプライアンスで、**NetScaler ADM** を **AppFlow ow** コレクタとして構成するには:

1. SD-WAN SE/PE/AE Web インターフェイスで、[設定] > [**AppFlow/IPFIX**] に移動します。
2. [有効] を選択します。



3. 「データ更新間隔」フィールドで、AppFlow レポートが AppFlow コレクターにエクスポートされる時間間隔を分単位で指定します。

注

Citrix ADM が AppFlow コレクターの場合、データ更新間隔は 1 分である必要があります。

4. 次のいずれかを行います：

- **HDX** を選択して、HDX インサイトデータを AppFlow コレクターに送信します。これは、ブランチャアプライアンスで有効にする必要があります。
- マルチホップデータを AppFlow コレクターに送信するには、**HDX** 用の **TCP** のみを選択します。

注

**HDX** テンプレートオプションは Citrix SD-WAN PE アプライアンスでのみ使用でき、データセンターアプライアンスで有効にする必要があります

5. 「IP アドレス」フィールドに、外部 AppFlow コレクターシステム（Citrix ADM サーバー）の IP アドレスを入力します。

6. 「ポート」フィールドに、外部 AppFlow コレクターシステムがリスンするポート番号を入力します。デフォルト値は 4739 です。

7. **Citrix ADM** チェックボックスを選択して、Citrix ADM が AppFlow コレクターであることを指定します。

注

- NetScaler ADM は現在、IPFIX 収集をサポートしていません。
- 最大 4 つの AppFlow コレクターを追加できます。Citrix ADM または IPFIX プロトコルをサポートする任意の AppFlow コレクターのいずれか。

8. Citrix ADM サーバーの認証情報を入力します。

9. [ 設定の適用 ] をクリックします。

Citrix SD-WAN SE/PE アプライアンスが検出され、Citrix ADM に一覧表示されます。Citrix SD-WAN SE/PE アプライアンスは、分析データを NetScaler ADM に送信します。詳細については、「[AppFlow と IPFIX](#)」を参照してください。

**Citrix SD-WAN** センターを使用して **NetScaler ADM** を **AppFlow** コレクターとして構成するには:

1. Citrix SD-WAN Center 管理 UI で、[ 構成 ] > [ アプライアンス設定 ] に移動します。
2. **AppFlow/IPFIX** セクションに移動し、「ファイルに含める」を選択します。
3. [ **IPFIX /AppFlow** 収集を有効にする ] を選択します。

4. 「データ更新 間隔」フィールドで、AppFlow レポートが AppFlow コレクターにエクスポートされる間隔を分単位で指定します。

注

Citrix ADM が AppFlow コレクターの場合、データ更新間隔は 1 分である必要があります。

5. 次のいずれかを行います:



- **HDX** を選択して、HDX インサイトデータを AppFlow コレクターに送信します。
- マルチホップインサイトデータを **AppFlow** コレクターに送信するには、**HDX** 用の **TCP** を選択します。これは、ブランチアプライアンスで有効にする必要があります。

注

**HDX** テンプレートオプションは Citrix SD-WAN PE アプライアンスでのみ使用でき、データセンターアプライアンスで有効にする必要があります。

6. **IPFIX/AppFlow Collector** フィールドに、外部の AppFlow コレクターシステム (Citrix ADM サーバー) の IP アドレスを入力します。
7. 「ポート」フィールドに、外部 AppFlow コレクターシステムがリスンするポート番号を入力します。デフォルト値は 4739 です。
8. **Citrix ADM** チェックボックスを選択して、Citrix ADM が AppFlow コレクターであることを指定します。
9. Citrix ADM サーバーの認証情報を入力します。

注

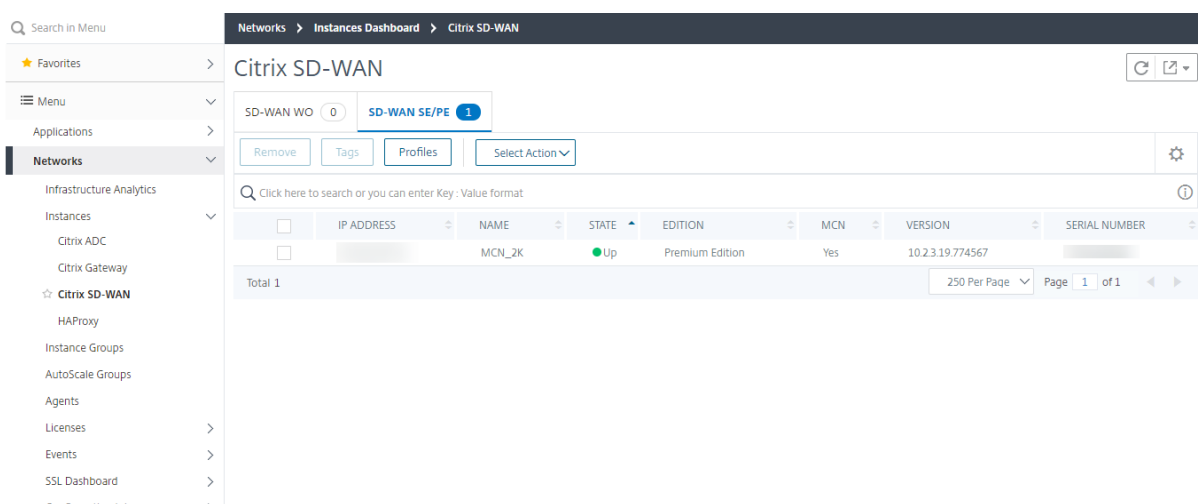
最大 4 つの AppFlow コレクターを追加できます。Citrix ADM または IPFIX プロトコルをサポートする任意の AppFlow コレクターのいずれか。

10. 構成を保存して、管理対象アプライアンスにエクスポートします。

詳細については、「[アプライアンス設定を構成して管理アプライアンスにエクスポートする方法](#)」を参照してください。

Citrix SD-WAN センター、AppFlow、および IPFIX を使用して NetScaler ADM を AppFlow コレクターとして構成する方法の詳細については、

Citrix SD-WAN SE/PE アプライアンスが検出され、NetScaler ADM によってリストされます。Citrix SD-WAN SE/PE アプライアンスが検出され、NetScaler ADM に表示されます。検出された Citrix SD-WAN SE/PE アプライアンスを表示するには、NetScaler ADM Web インターフェイスで [ネットワーク] > [インスタンス] > [**Citrix SD-WAN**] の順に選択し、[**SD-WAN SE/PE/AE**] を選択します。



検出されたアプライアンスの IP アドレス、名前、現在の状態、ソフトウェアエディション、およびバージョンを確認できます。アプライアンスがマスターコントローラーノード（MCN）かどうかを確認できます。

次の操作を実行できます。

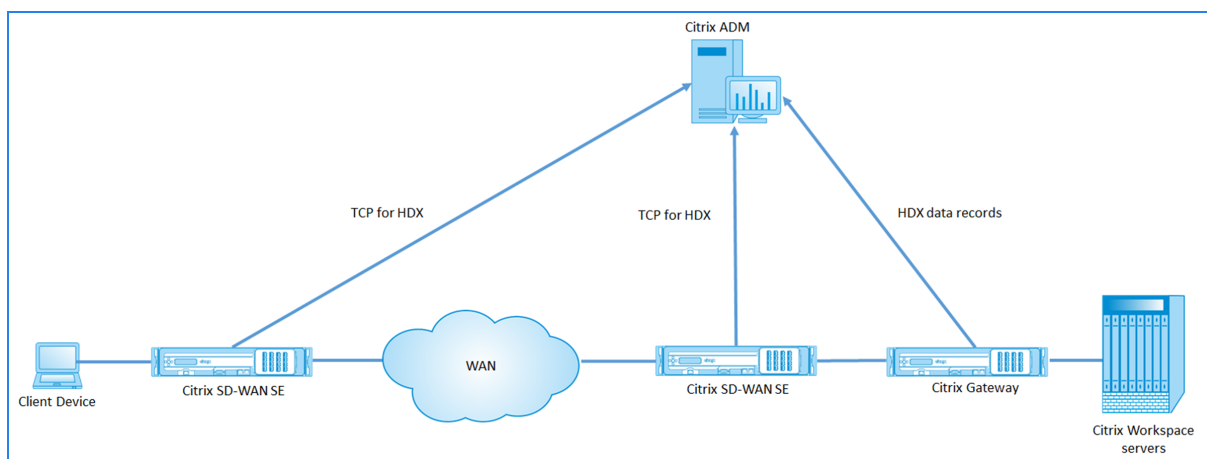
- インスタンスプロファイルの表示と削除。
- Citrix ADM からインスタンスを削除します。
- インスタンスの再検出。

Citrix SD-WAN PE アプライアンスの場合、AppFlow の構成に応じて、HDX データレコードまたはマルチホップデータを表示できます。Citrix SD-WAN SE アプライアンスは、マルチホップデータのみを提供します。詳しくは、「[HDX Insight レポートとメトリックの表示](#)」および「[マルチホップ展開用の Citrix SD-WAN Analytics データの表示](#)」を参照してください。

## マルチホップ展開のための **Citrix SD-WAN** 分析データの表示

February 6, 2024

マルチホップネットワーク展開では、次の図で示すように、クライアントとサーバー間にデバイスが複数存在します。このタイプの展開では、Citrix SD-WAN SE アプライアンスと Citrix ゲートウェイが Citrix ADM に追加され、AppFlow が有効になります。



Citrix ADM は、ホップカウントと接続チェーン ID に基づいて、データを受信するアプライアンスを識別します。ホップ数は、トラフィックがクライアントからサーバーへ流れるときに通過する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。

Citrix ADM は、ホップカウントと接続チェーン ID を使用してアプライアンスからのデータを関連付けて、レポートを生成します。

Citrix SD-WAN SE アプライアンスが分析データを Citrix ADM に送信するには、Citrix Gateway の仮想 IP アドレスを DPI ICA IP として構成し、DPI ICA のポート番号を 443 に設定する必要があります。

**ICA DPI** の設定を構成するには次の手順を実行します。

1. **Citrix SD-WAN SE** アプライアンスの **UI** で、[構成エディタ] > [詳細設定] > [グローバル] > [アプリケーション] > [設定] に移動します。
2. [ディープパケットインスペクションを有効にする] > [Citrix ICA アプリケーションのディープパケットインスペクションを有効にする] > [マルチストリーム ICA を有効にする \*\*] を選択します

## Settings

Enable Deep Packet Inspection

Enable Deep Packet Inspection for Citrix ICA Applications

Citrix ICA Deep Packet Inspection Settings

Enable Multi-Stream ICA

DPI ICA IP and Port List

DPI ICA IP-1:	DPI ICA Port-1:
<input type="text" value="192.168.29.2/4"/>	<input type="text" value="2599"/>
DPI ICA IP-2:	DPI ICA Port-2:
<input type="text" value="192.170.29.3/5"/>	<input type="text" value="2600"/>
DPI ICA IP-3:	DPI ICA Port-3:
<input type="text" value="192.170.100.3/5"/>	<input type="text" value="2601"/>
DPI ICA IP-4:	DPI ICA Port-4:
<input type="text" value="192.160.23.3/5"/>	<input type="text" value="8008"/>
DPI ICA IP-5:	DPI ICA Port-5:
<input type="text"/>	<input type="text"/>

3. 「**DPI ICA IP-1**」フィールドに、Citrix Gateway の仮想 IP アドレスとプレフィックスを入力します。

4. **DPI ICA** ポート-**1** フィールドに、ポート番号 443 を入力します。

5. 「適用」をクリックし、変更管理プロセスを使用して構成をアプライアンスにエクスポートします。

Citrix ADM では、アクティブな ICA セッションごとに、HDX Insight でセッション図を表示できます。セッションダイアグラムには、接続パスにあるデバイスの詳細が表示されます。また、ネットワークデバイスと直近のホップ間におけるクライアント側/サーバー側の遅延も詳細に確認できます。こうした情報により、遅延の根本原因を特定し、パフォーマンスの問題を解決することができます。


Citrix SD-WAN SE は HDX データレコードを送信しません。NetScaler SD-WAN SE で提供されるのは、HDX 情報の TCP のみです。HDX Insight データは、ネットワーク内の HDX Insight 対応デバイス（NetScaler ADC や NetScaler Gateway など）によって提供されます。

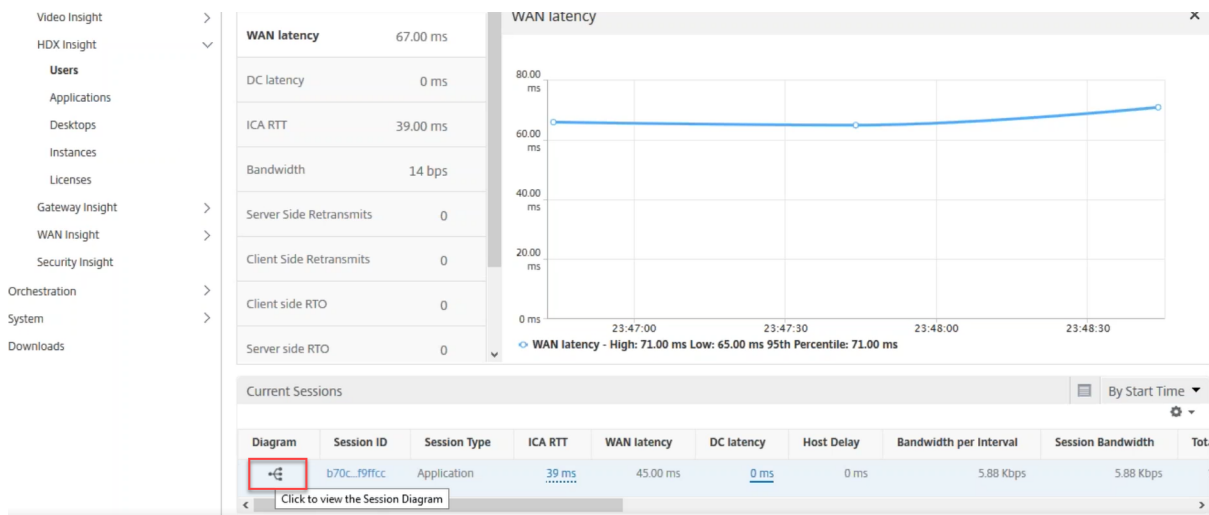
Citrix SD-WAN PE アプライアンスは、アプライアンスの AppFlow 構成に応じて、HDX データまたは HDX Insight データの TCP を送信できます。データセンターアプライアンスでは HDX テンプレートを有効にする必要があります。

注

マルチホップ展開では、ネットワークデバイスのうち 1 つのみから HDX Insight データが送信されるようにしてください。残りのネットワークデバイスでは、HDX データの TCP を送信できます。


マルチホップデータを表示するには:

**Citrix ADM Web** インターフェイスで、[HDX Insight] > [ユーザー] > [現在のセッション] または [HDX Insight] > [アプリケーション] > [現在のセッション] に移動し、 アイコンをクリックします。

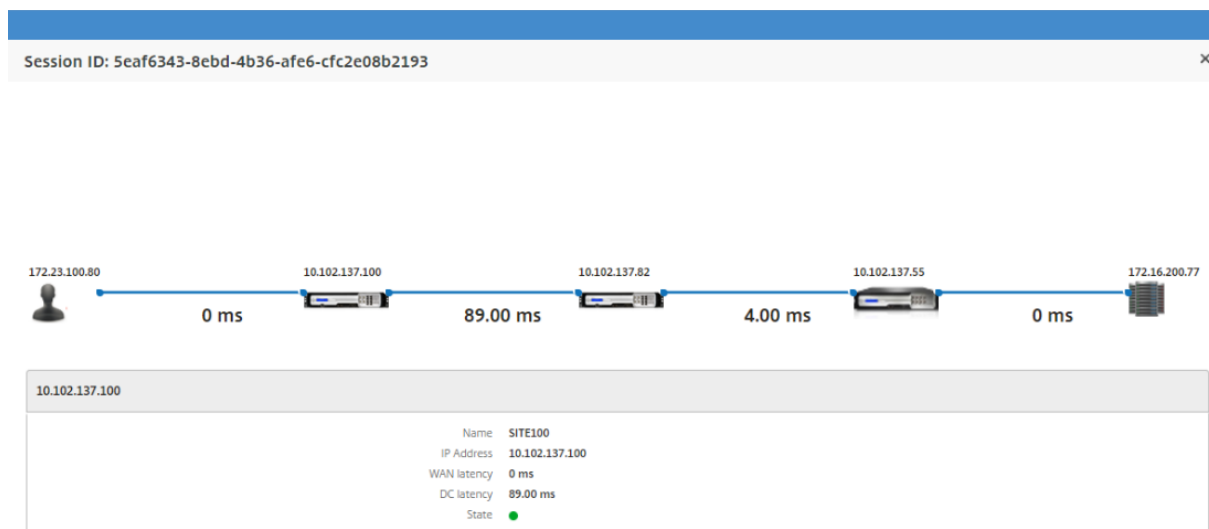


WAN latency	67.00 ms
DC latency	0 ms
ICA RTT	39.00 ms
Bandwidth	14 bps
Server Side Retransmits	0
Client Side Retransmits	0
Client side RTO	0
Server side RTO	0

WAN latency - High: 71.00 ms Low: 65.00 ms 95th Percentile: 71.00 ms

Diagram	Session ID	Session Type	ICA RTT	WAN latency	DC latency	Host Delay	Bandwidth per Interval	Session Bandwidth	Tot
	b70c_f9ffc	Application	39 ms	45.00 ms	0 ms	0 ms	5.88 Kbps	5.88 Kbps	

ネットワークポロジダイアグラムが表示されます。



Session ID: 5eaf6343-8ebd-4b36-afe6-cfc2e08b2193

172.23.100.80 — 0 ms — 10.102.137.100 — 89.00 ms — 10.102.137.82 — 4.00 ms — 10.102.137.55 — 0 ms — 172.16.200.77

10.102.137.100	
Name	SITE100
IP Address	10.102.137.100
WAN latency	0 ms
DC latency	89.00 ms
State	●

ネットワーク要素をクリックすると、詳細が表示されます。

注

表示される情報は、選択したネットワーク要素によって異なります。

Citrix アプライアンスには次のパラメータが表示されます。

- 名前: Citrix アプライアンスの名前。
- IP アドレス: アプライアンスの IP アドレス。
- **WAN** 遅延: ネットワークのクライアント側による遅延。つまり、Citrix アプライアンス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る遅延。つまり、Citrix アプライアンスからバックエンドサーバーまでです。
- 状態: デバイスの到達可能性ステータス。

## Citrix SD-WAN WANOP インスタンスのイベントレポートを表示する

February 6, 2024

[ ネットワーク ] > [ イベント ] > [ レポート ] に移動し、[ **Citrix SD-WAN WO** ] を選択すると、上位 **10** の **SD-WAN WANOP** インスタンスのイベントをグラフィカルに表示できます。

インスタンスごとにイベントが重要度に応じて表示され、各イベントをクリックするとイベント数、発生時期、イベントのカテゴリに関する詳細を確認できます。



## Citrix SD-WAN WANOP インスタンスのネットワークレポートの表示

February 6, 2024

Citrix ADM で WAN 最適化ネットワーク関連のレポートを表示できます。このデータを使用して、ネットワークの問題のトラブルシューティングや、Citrix SD-WAN WANOP デバイスの動作の分析を行うことができます。WAN 最適

化デバイスについて、過去 1 時間、過去 1 日、過去 1 週間、または過去 1 ヶ月のネットワーク統計情報に関するレポートを表示できます。

次のレポートを表示できます。

レポート	説明
アクセラレーション	このレポートを使用して、高速トラフィックのパターン（サービスクラス別の KBPS）と、WAN 最適化アプライアンスを通過する高速 TCP 接続の数を分析します。これには、WAN 最適化デバイスを通してアクセラレーションが行われる TCP 接続の数、アクセラレーション対象として選択されたオープン接続とハーフクローズ接続の数、アクセラレーションの対象となるハーフオープン接続の数が含まれます。
パススルー接続	このレポートでは、WAN 最適化デバイスの非アクセラレーション対象接続を確認できます。
サービスクラス	このレポートを使用すると、WAN 最適化デバイスに定義されているサービスクラスタイプに基づく送受信帯域幅の削減量を確認できます。
アプリケーション	このレポートを使用して、WAN 最適化デバイスで実行されているアプリケーションの送受信データ量をビット/秒単位で表示します。
CPU 使用率	このレポートでは、WAN 最適化デバイスの CPU 使用率 (%) を確認できます。
増加容量	このレポートでは、WAN 最適化デバイスの累積送信圧縮率を確認できます。
データ削減率	このレポートでは、送受信帯域幅の節約率 (%) を確認できます。また、WAN 最適化デバイスの送信帯域幅と受信帯域幅の節約値を個別に分析することもできます。
リンク使用率	このレポートを使用して、WAN 最適化の送信リンク使用率と受信リンク使用率をパーセンテージで表示します。
プラグイン使用状況	このレポートでは、WAN 最適化デバイスに接続されているプラグインの数を確認できます。
パケット損失	このレポートを使用して、WAN 最適化デバイスで定義されているリンクについて、リンクがドロップした送信パケットとリンク ドロップされた受信パケットを表示します。
スループット	このレポートを使用して、WAN 最適化デバイスのリンク送信量とリンク受信量をビット/秒単位で表示します。

レポート	説明
QoS	このレポートを使用して、WAN 最適化デバイスの QoS 送信量と QoS 受信量（ビット/秒）を表示します。

---

**Citrix SD-WAN WANOP** ネットワークレポートを表示するには：

1. Citrix ADM で、[ネットワーク] > [ネットワークレポート] > [ **Citrix SD-WAN WO** ] に移動します。
2. [レポート名] ドロップダウンリストから、表示するレポートを選択します。
3. インスタンスドロップダウンリストから、レポートを表示する Citrix SD-WAN WANOP インスタンスを選択します。
4. 「期間」ドロップダウンリストから、時間間隔を選択します。
5. [実行] をクリックします。

## Citrix SD-WAN WANOP インスタンスのバックアップ

February 6, 2024

インスタンスの現在の状態をバックアップし、後でバックアップしたファイルを使用して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上の理由から、インスタンスをバックアップすることをお勧めします。安定したシステムをバックアップしておく、システムが不安定になった場合にシステムを安定した状態に復元できます。Citrix SD-WAN WANOP 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 を使用してインスタンスを手動でバックアップおよび復元するか、Citrix ADM を使用してバックアップを実行できます。Citrix ADM は、NITRO コール、Secure Shell (SSH) プロトコル、およびセキュアコピー (SCP) プロトコルを使用して、管理対象 Citrix SD-WAN WANOP インスタンスの現在の状態をバックアップします。

### インスタンスバックアップ設定の構成

Citrix ADM で Citrix SD-WAN WANOP インスタンスのバックアップを作成する前に、Citrix ADM でインスタンスのバックアップ設定を構成する必要があります。

インスタンスのバックアップ設定を構成するには：

1. NetScaler ADM で、[システム] > [システム管理] に移動します。右側のペインの [バックアップ設定] で、[インスタンスバックアップ設定] を選択します。
2. [インスタンスバックアップを有効にする] を選択します。このオプションは、デフォルトで有効になっています。

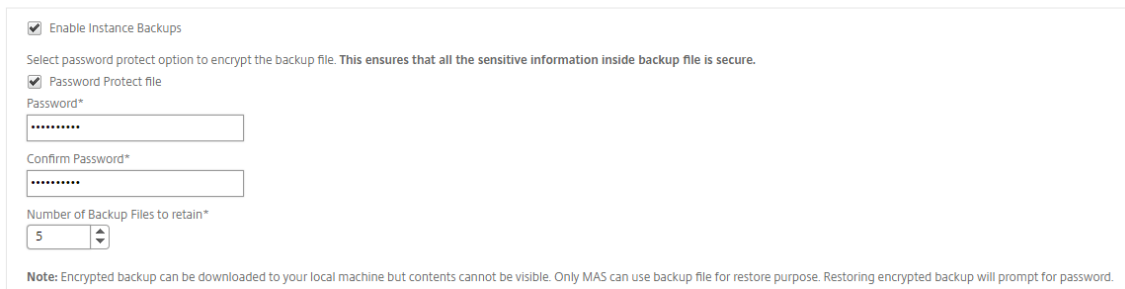


3. バックアップファイルを暗号化するには、「パスワード保護ファイル」を選択します。バックアップファイルを暗号化することで、バックアップファイル内の機密情報の安全性が確保されます。
4. [保持するバックアップファイルの数] フィールドで、Citrix ADM に保持するバックアップファイルの数を指定します。最大 50 個のバックアップファイルを保持できます。

### 注

各バックアップファイルには、ある程度のストレージ要件が必要です。Citrix ADM には、要件に応じて最適な数のバックアップファイルを保存することをお勧めします。

### ← Configure Instance Backup Settings



Enable Instance Backups

Select password protect option to encrypt the backup file. This ensures that all the sensitive information inside backup file is secure.

Password Protect file

Password\*

Confirm Password\*

Number of Backup Files to retain\*

5

Note: Encrypted backup can be downloaded to your local machine but contents cannot be visible. Only MAS can use backup file for restore purpose. Restoring encrypted backup will prompt for password.

5. バックアップスケジュール設定を設定します。ここでは、次のいずれかオプションを選択できます：
  - 間隔ベース - 指定した間隔が経過すると、NetScaler ADM で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 - バックアップを実行する時間を「時間: 分」形式で指定できます。Citrix ADM では、インスタンスで毎日最大 4 回のバックアップを実行できます。

▼ Backup Scheduling Settings

Scheduling Option

Interval Based  Time Based

Specify time for daily Backup (Maximum-limit: 4)

Add Time

00:00	×	
06:00	×	
12:00	×	
18:00	×	+

注

**Citrix ADC** 設定セクションは無視してください。これらの設定は Citrix SD-WAN WANOP インスタンスには適用されません。

6. [外部転送を有効にする] を選択して、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します。次のフィールドに値を入力します。

- サーバー: 外部サーバーの IP アドレス。
- ユーザー名: 外部サーバーのユーザー名
- パスワード: 外部サーバーのパスワード。
- ポート: 外部サーバーとの通信に使用されるポート番号。
- 転送プロトコル: Citrix ADM から外部サーバーにバックアップファイルを転送するために使用されるプロトコル。

バックアップファイルを外部サーバーに転送した後、Citrix ADM から削除することもできます。

▼ External Transfer

Enable External Transfer

Server\*

192 . 10 . 10 . 1

User Name\*

davidT

Password\*

.....

Port\*

-1

Transfer Protocol

SCP  SFTP  FTP

Directory Path\*

/test/nsbackups/

Delete file from NetScaler Management and Analytics System after transfer

7. **[OK]** をクリックします。

注

Citrix ADM は、選択した Citrix SD-WAN WANOP インスタンスのいずれかでバックアップが失敗すると、SNMP トラップまたは Syslog 通知をそれ自体に送信します。

### Citrix SD-WAN WANOP インスタンスのバックアップの作成

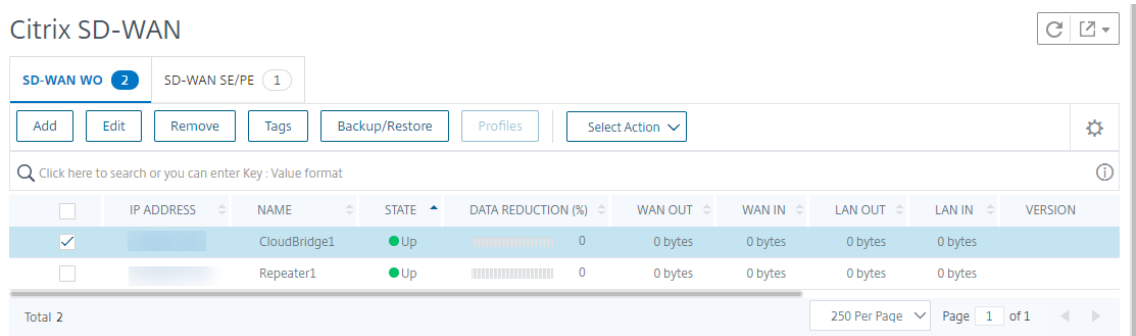
Citrix SD-WAN WANOP インスタンスのバックアップを作成する手順は、デフォルトの nsroot プロファイルを使用して管理者ユーザーにも適用できます。

カスタムユーザーが Citrix SD-WAN WANOP インスタンスのバックアップを作成する方法については、このトピックの「カスタムユーザー用の Citrix SD-WAN WANOP インスタンスのバックアップを作成する」を参照してください。

Citrix SD-WAN WANOP インスタンスが NetScaler ADM に追加されていることを確認します。詳細については、「[NetScaler ADM へのインスタンスの追加](#)」を参照してください。

**Citrix SD-WAN WANOP** インスタンスのバックアップを作成するには:

1. Citrix ADM で、[ネットワーク]>[インスタンス]>[\*\*Citrix SD-WAN\*\*] に移動します。
2. [**SD-WAN WO**] で、バックアップする Citrix SD-WAN OP インスタンスを選択し、[バックアップと復元] をクリックします。



3. 「バックアップファイル」 ページで、「バックアップ」 をクリック します。
4. 以下のオプションのいずれかを使用してバックアップファイルを暗号化します。
  - [パスワードで保護されたファイル] を選択し、パスワードを入力してバックアップファイルを暗号化します。
  - インスタンスバックアップ設定ページで指定したグローバルパスワードを使用するには、「グローバルパスワードを使用」を選択します。
5. 「バックアップを作成」 を  
クリックします

カスタムユーザー向けの **Citrix SD-WAN WANOP** インスタンスのバックアップの作成

Citrix SD-WAN WANOP インスタンスで管理者権限を持つカスタムユーザーを作成した場合は、次の手順を使用してインスタンスを追加し、Citrix ADM を使用してそのインスタンスをバックアップします。

カスタムユーザーによるバックアップ操作は、400/800/1000WS/2000WS/3000/4000/5000/4100/5100 SD-WAN WANOP プラットフォームではサポートされていません。

注

Citrix ADM で Citrix SD-WAN アドバンスドプラットフォームのバックアップを作成するには、デフォルトの nsroot プロファイルを使用することをお勧めします。

**Citrix SD-WAN WANOP** インスタンスを追加し、カスタムユーザーのバックアップを作成するには:

1. Citrix ADM で、[ネットワーク ]>[インスタンス]>[ **\*\*Citrix SD-WAN** ] に移動し、[ **SD WAN WO\*\*** ] を選択します。
2. [追加] をクリックします。
3. 「IP アドレス」フィールドに、Citrix SD-WAN WANOP インスタンスの IP アドレスを入力します。
4. 「プロファイル名」フィールドの横にある「追加」をクリックして、新しいプロファイルを作成します。[ **Citrix SD-WAN WO** プロファイルの作成] ウィンドウが表示されます。



← Create Citrix SD-WAN WO Profile

Profile Name\*

New-admin-profile

User Name\*

nsroot

Password\*

\*\*\*\*\*

Community\*

\*\*\*\*\*

Protocol for Citrix SD-WAN WO communication is https.

Create Close

5. 「プロファイル名」フィールドに、プロファイルの名前を入力します。
6. [ユーザー名]フィールドに、SD-WAN WANOP インスタンスで作成したカスタムユーザーのユーザー名を入力します。
7. [パスワード]フィールドに、SD-WAN WANOP インスタンスでカスタムユーザーに設定したパスワードを入力します。
8. コミュニティフィールドに、SD-WAN WANOP アプライアンスで構成されている SNMP 通信文字列を入力します。(例: パブリック)
9. [作成] をクリックします。

10. 「プロファイル名」フィールドで、新しく作成したプロファイルを選択して「OK」をクリックします。

11. [ネットワーク] > [インスタンス] > [\*\*Citrix SD-WAN\*\*] に移動します。

12. **SD-WAN WO** で、追加した Citrix SD-WAN OP インスタンスを選択し、[バックアップと復元] をクリックします。

Citrix SD-WAN

SD-WAN WO 2 SD-WAN SE/PE 1

Add Edit Remove Tags Backup/Restore Profiles Select Action

Click here to search or you can enter Key : Value format

	IP ADDRESS	NAME	STATE	DATA REDUCTION (%)	WAN OUT	WAN IN	LAN OUT	LAN IN	VERSION
<input checked="" type="checkbox"/>		CloudBridge1	Up	0	0 bytes	0 bytes	0 bytes	0 bytes	
<input type="checkbox"/>		Repeater1	Up	0	0 bytes	0 bytes	0 bytes	0 bytes	

Total 2 250 Per Page Page 1 of 1

13. 「バックアップファイル」 ページで、「バックアップ」 をクリック します。

14. 以下のオプションのいずれかを使用してバックアップファイルを暗号化します。

- ・ [パスワードで保護されたファイル] を選択し、パスワードを入力してバックアップファイルを暗号化します。
- ・ インスタンスバックアップ設定ページで指定したグローバルパスワードを使用するには、「グローバルパスワードを使用」 を選択します。

注

暗号化されたバックアップファイルをローカルマシンにダウンロードすることはできますが、その内容を表示することはできません。これらのバックアップファイルを復元目的で使用できるのは Citrix ADM だけです。暗号化されたバックアップを復元すると、パスワードの入力を求められます。

15. 「バックアップを作成」をクリックします。

重要

1 1. Citrix SD-WAN WANOP VPX アプライアンスの場合、Citrix ADM は CB ブローカー構成ファイルのみをバックアップします。

a) 高度な Citrix SD-WAN WANOP プラットフォームの場合、Citrix ADM は次のものをバックアップします。

- CB ブローカー設定ファイル
- NTP 設定ファイル
- DNS
- SNMPD コンフィギュレーションファイル
- シスログ設定ファイル
- SSL 証明書、キー、ポリシー
- SVM データベースファイル
- コンポーネント (XML 形式)
- リソース (XML フォーマット)

各フォルダーでバックアップされるファイルは、以下の表に一覧表示されています。フォルダー名に「\*」が続いている場合は、そのフォルダーのすべてのファイルがバックアップされることに注意してください。

ディレクトリ	サブディレクトリまたはファイル
/br_broker/	CB-6BBB660A/ ws.conf
/など/	resolv.conf
/mps/	mps_devices.xml
/mpsconfig/	ssl/*、ntp.conf、snmpd.conf、syslog.conf
/mpsdb/	mpsdb_dump.sql
/ns/	ns-6cbb660a/*
/var/	mps/policy/, mps/ssl_certs/ sdx_default_ssl_cert, mps/ssl_keys/ sdx_default_ssl_key, mps/tenants/

## HAProxy インスタンスの管理

February 6, 2024

HAProxy、すべての TCP サービスおよび HTTP サービスの負荷を分散させることができるオープンソースのロードバランサーです。HAProxy の詳細については、を参照してください <http://www.haproxy.org/>。

Application Delivery Management (Citrix ADM) は HAProxy バージョン 1.4.24 以降をサポートしています。HAProxy インスタンスをプロビジョニングしたホストを Citrix ADM に追加すると、Citrix ADM はホスト上の HAProxy インスタンスを検出し、それらを監視できるようにします。NetScaler MAS には、各インスタンスの HAProxy 構成について以下の種類の情報が表示されます。

- Frontend -バックエンドへの要求の転送方法
- Backend -転送された要求を受信するサーバー
- Servers -HAProxy によりトラフィックの負荷分散が行われるサーバー

詳しくは、<http://www.haproxy.org/download/1.7/doc/configuration.txt>を参照してください。

また、NetScaler ADM には、フロントエンドをリアルタイムで監視できる HAProxy アプリダッシュボードが用意されています。詳細については、[HAProxy アプリダッシュボード](#)を参照してください。

## HAProxy インスタンスを NetScaler ADM に追加する

February 6, 2024

Citrix Application Delivery Management (Citrix ADM) では、HAProxy インスタンスをプロビジョニングしたホストの詳細を手動で追加する必要があります。これらの詳細を追加すると、NetScaler ADM はホストでプロビジョニングされた HAProxy インスタンスを自動的に検出し、NetScaler ADM インベントリに追加します。また、HAProxy インスタンス上に構成されているすべてのフロントエンド、バックエンド、およびサーバーを検出し、フロントエンドを検出されたアプリケーションとして扱います。

### 前提条件

以下の点について確認してください。

- 展開環境に HAProxy インスタンスを展開済みであること。詳しくは、<http://www.haproxy.org/#docs>を参照してください。
- HAProxy アプリケーションダッシュボードでアプリケーション統計を表示するフロントエンドの数を特定し、決定しました。デフォルトでは、検出された 30 アプリケーションの統計情報が HAProxy App ダッシュボードに表示されます。HAProxy アプリダッシュボードの詳細については、[HAProxy アプリダッシュボード](#)を参



照してください。検出された 30 を超えるアプリケーションの統計を表示するには、別途ライセンスを購入する必要があります。詳しくは、「[サードパーティライセンス](#)」を参照してください。

#### 重要

NetScaler ADM では、ホスト内の HAProxy インスタンスを検出するために、ホストへのアクセスが必要です。NetScaler ADM へのアクセスを提供するには、ホストの SSH キーペアを指定するか、ホストのパスワードを使用します。SSH キーペアを使用してアクセスを提供する場合は、秘密キーと公開キーの SSH キーペアをホストで生成して、公開キーをホスト上で承認されたキーに追加するようにします。また、SSH ユーザーアカウントにはスーパーユーザー権限が必要です。

**HAProxy** インスタンスを **NetScaler ADM** に追加するには:

1. [ネットワーク]>[インスタンス]に移動します。「インスタンス」で「**HAProxy**」を選択し、「追加」をクリックします。
2. [**HAProxy** ホストの追加] ダイアログボックスで、次の操作を行います。

## ← Add HAProxy Host

IP Address\*  
10 . 102 . 29 . 234 ?

HAProxy Profile\*  
HAproxy1 Add Edit ?

Site\*  
Default Add Edit

Agent  
Click to select >

Tags  
location Bangalore +

OK Close

1. [**IP Address**] フィールドに、HAProxy インスタンスをプロビジョニングしたホストの IP アドレスを入力します。
  - a) **HAProxy** プロファイルメニューで、既存の HAProxy プロファイルを選択するか、新しい HAProxy プロファイルを作成して選択します。HAProxy プロファイルを作成するには、「追加」をクリックします。

- i. [ **HAProxy** プロファイルの追加] ダイアログボックスで、次の操作を行います。

- i. [ プロファイル名] フィールドに、プロファイル名を入力します。  
 ii. 「ユーザー名」フィールドと「パスワード」フィールドに、ホストのユーザー認証情報を入力します。  
 iii. [作成] をクリックします。

2. 「サイト」メニューから、HAProxy サイトを選択します。新しいサイトを作成してメニューに追加するには、「追加」をクリックします。  
 3. [エージェント]メニューから [エージェント] を選択します。  
 4. 「タグ」フィールドに、適切な値を入力します。  
 5. [OK] をクリックします。

NetScaler ADM は、ホスト上でプロビジョニングされた HAProxy インスタンスを検出し、[インスタンス] タブですべての HAProxy インスタンスを表示できます。

HAProxy

HAProxy Hosts 2 Instances 5

View Configuration View Backup Dashboard Hard Restart Soft Restart Search ▾

<input type="checkbox"/>	Host IP Address	Configuration Path	State	Version	CPU Usage (%)	Memory Usage (%)
<input type="checkbox"/>	10.102.205.59	lb_testportal3.cfg	● Up	1.4.24	0	0.10
<input type="checkbox"/>	10.102.205.59	lb_testportal1.cfg	● Up	1.4.24	0	0.10
<input type="checkbox"/>	10.102.205.59	lb_testportal4.cfg	● Up	1.4.24	0	0.10
<input type="checkbox"/>	10.102.205.178	lb_mas.cfg	● Up	1.4.24	0	0.10
<input type="checkbox"/>	10.102.205.59	lb_testportal2.cfg	● Up	1.4.24	0	0.10

## HAProxy インスタンスの設定の表示

NetScaler ADM で HAProxy インスタンスの構成を表示するには、[ネットワーク] > [インスタンス] > [HAProxy] に移動し、[インスタンス] タブで HAProxy インスタンスを選択し、[構成の表示] をクリックします。

```
Configuration ×
global
    log /dev/log      local0
    log /dev/log      local1 notice
    chroot /var/lib/haproxy
    user haproxy
    group haproxy
    daemon

    stats socket /var/run/haproxy.sock mode 600 level admin

defaults
    log      global
    mode     http
    option   httplog
    option   dontlognull
    contimeout 5000
    clitimeout 50000
    srvtimeout 50000
    errorfile 400 /etc/haproxy/errors/400.http
    errorfile 403 /etc/haproxy/errors/403.http
    errorfile 408 /etc/haproxy/errors/408.http
    errorfile 500 /etc/haproxy/errors/500.http
    errorfile 502 /etc/haproxy/errors/502.http
    errorfile 503 /etc/haproxy/errors/503.http
    errorfile 504 /etc/haproxy/errors/504.http

frontend http-in_1
    bind 10.102.205.59:8061
    acl host_api hdr(host) -i 10.102.205.59
    default_backend api_backend1

frontend http-in_2
    bind 10.102.205.59:8062
    acl host_api hdr(host) -i 10.102.205.59
```

## HAProxy アプリのダッシュボード

February 6, 2024

アプリケーションダッシュボードは、NetScaler ADM (NetScaler Application Delivery Management ADM) によって監視されるすべての HAProxy フロントエンドのリアルタイム統計を提供します。フロントエンドを個別のアプリケーションとして一覧表示し、アプリケーションに関するトランザクション、スループット、セッション情報を提供します。

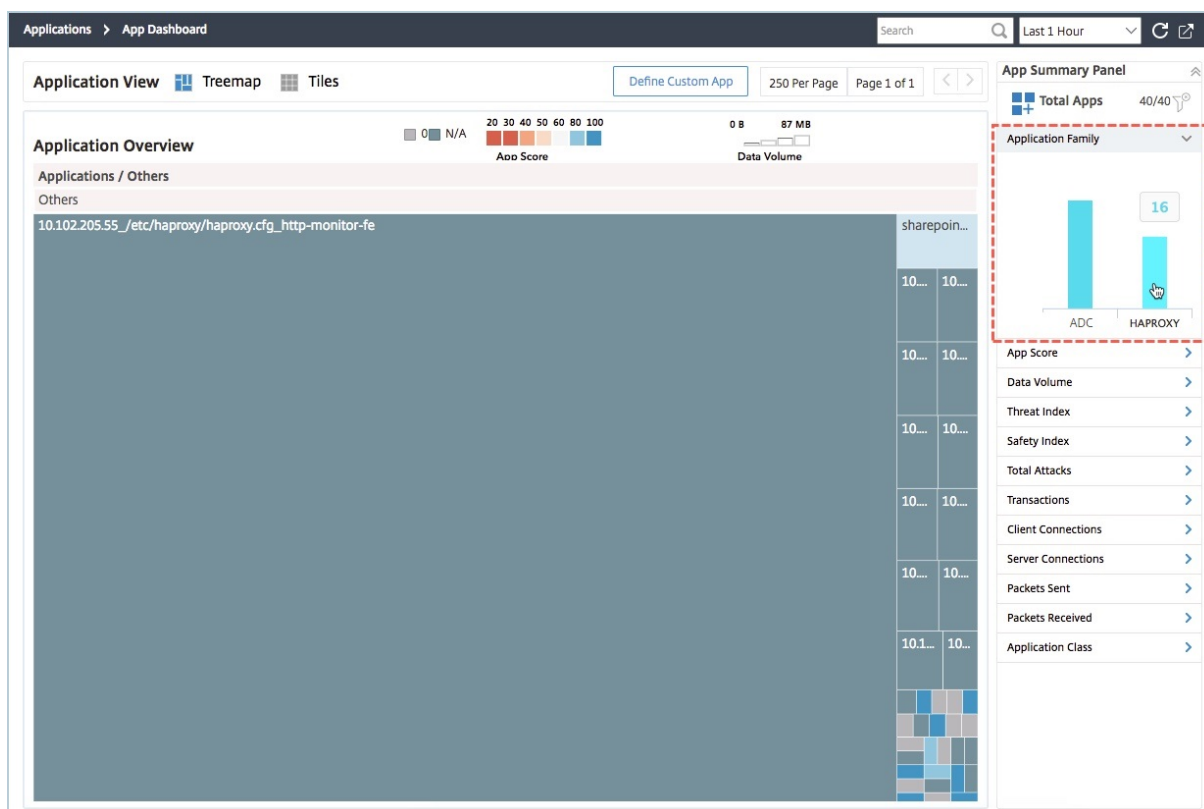
### 重要

必ず HAProxy インスタンス設定ファイルで **stats** を有効にしてください。統計情報を有効にするには、HAProxy 設定ファイルを編集し、default セクションの後に、次のサンプルのようなエントリを追加します。

```

1 listen stats :9000 # Listen on localhost:9000
2 mode http
3 stats enable # Enable stats page
4 stats hide-version # Hide HAProxy version
5 stats realm Haproxy\ Statistics # Title text for popup window
6 stats uri /haproxy_stats # Stats URI
7 stats auth Username:Password # Authentication credentials
8 <!--NeedCopy-->
    
```

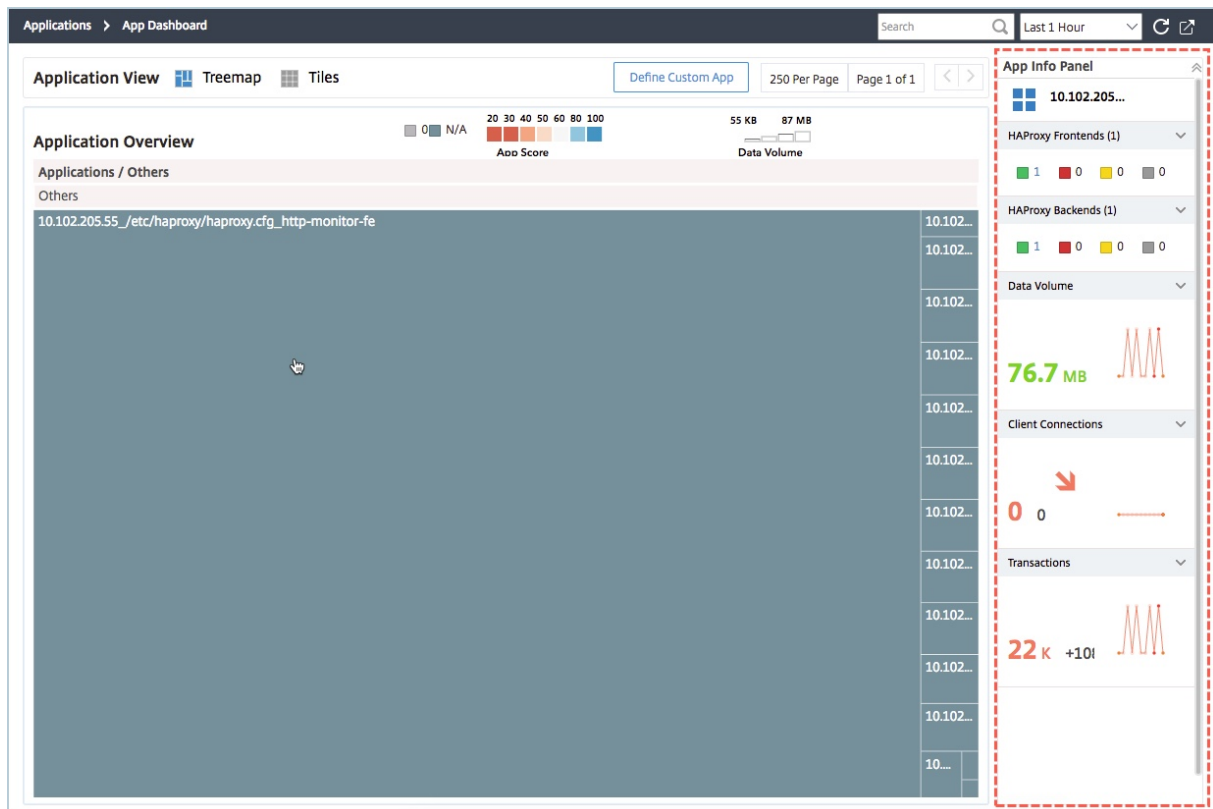
Citrix ADM のアプリケーションダッシュボードで HAProxy アプリケーションにアクセスするには、HAProxy インスタンスを Citrix ADM に追加した後、[アプリケーション] > [ダッシュボード] に移動します。HAProxy アプリケーションのみを表示するようにダッシュボードをフィルタリングできます。ダッシュボードをフィルタリングするには、「App Summary Info」パネルの「アプリケーションファミリー」セクションに表示される「**HAPROXY**」を選択します。



## HAProxy アプリケーションの主要なメトリックの表示

アプリケーション情報パネルは、HAProxy アプリケーションをドリルダウンすると、最初のレベルになります。アプリケーションの状態とともに、主要な測定基準とコンポーネントが表示されます。たとえば、選択した HAProxy アプリケーションについて、アプリケーション情報パネルには HAProxy フロントエンドの総数、HAProxy バックエンドの総数、データ量、クライアント接続の傾向、トランザクションが表示されます。HAProxy アプリケーションの主要なメトリックを表示するには、アプリケーションダッシュボードで **HAProxy** アプリケーションタイルをクリック

ックします。その後、アプリ情報パネルがアプリ概要パネルに置き換わります。

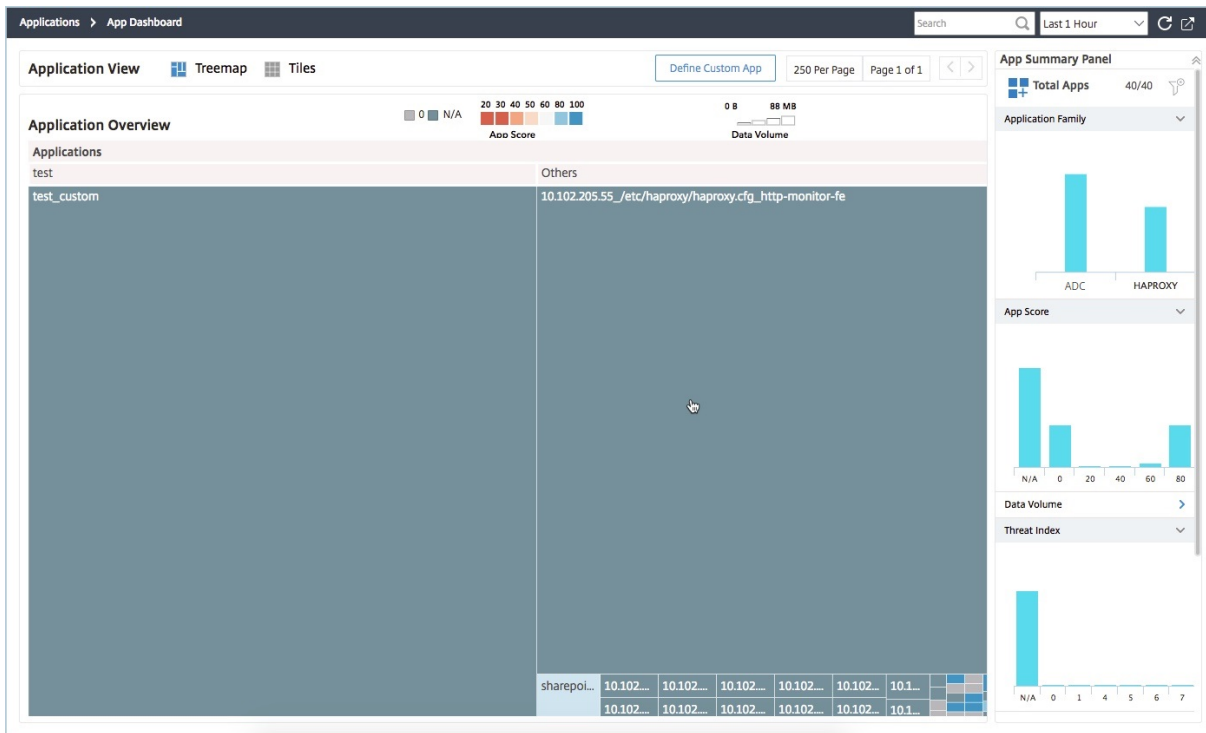


## HAProxy アプリケーションのリアルタイムパフォーマンスを表示

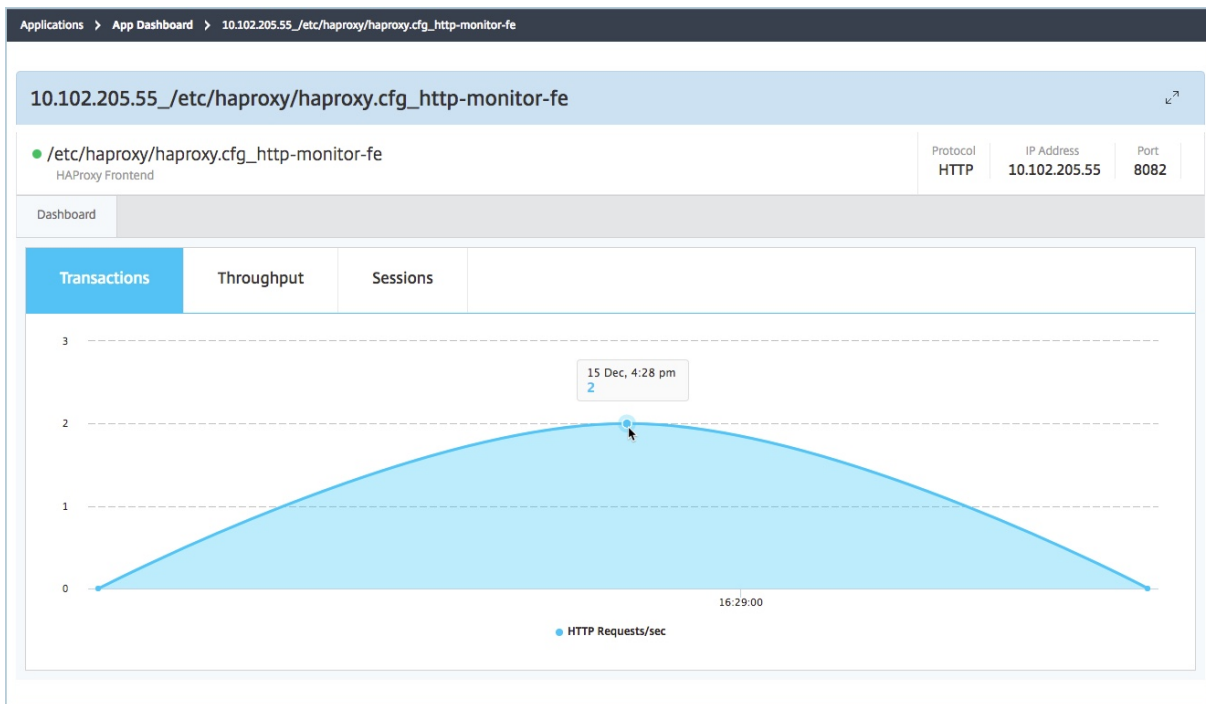
Citrix ADM では、HAProxy アプリケーションのパフォーマンスをリアルタイムで表示できます。選択した HAProxy アプリケーションの以下の詳細がリアルタイムで表示されます。

- 取引。アプリケーションが実行したトランザクション。
- スループット。アプリケーションのスループット。
- セッション。アプリケーションによって確立されたセッションの数。

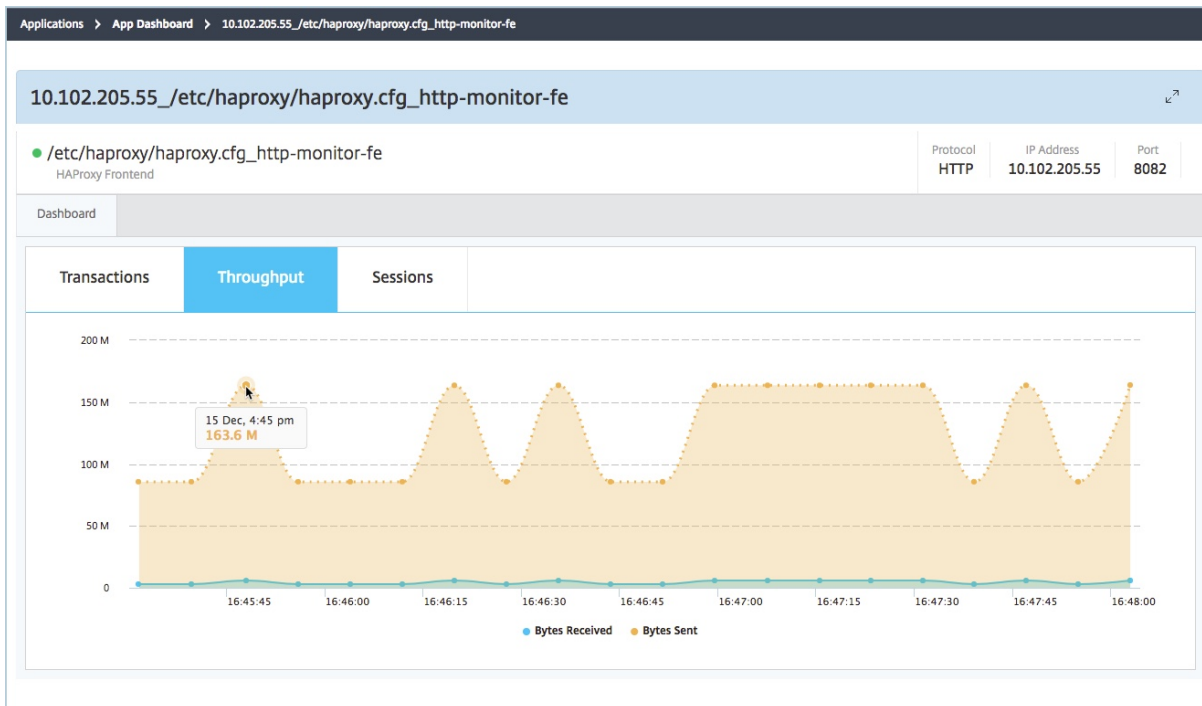
HAProxy アプリケーションのリアルタイムパフォーマンスを表示するには、アプリケーションダッシュボードで HAProxy アプリケーションタイルをダブルクリックします。



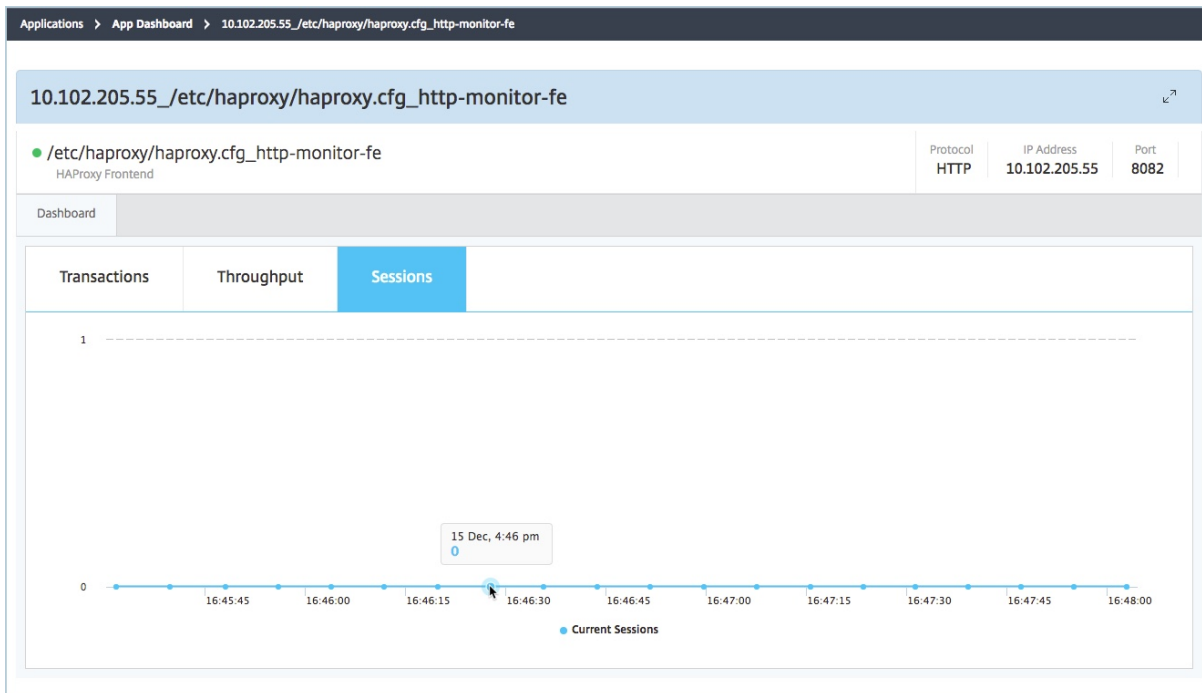
デフォルトでは、「トランザクション」タブが選択され、アプリケーションによって実行されたリアルタイムのトランザクションが表示されます。



アプリケーションのリアルタイムスループットを表示するには、[スループット] タブをクリックします。



[ **Sessions** ] タブをクリックすると、アプリケーションによって確立されたセッション数をリアルタイムで表示できます。



## サードパーティライセンス

February 6, 2024

ホストを NetScaler Application Delivery Management (NetScaler ADM) に追加すると、NetScaler ADM はホスト上でプロビジョニングされた HAProxy インスタンスを自動的に検出し、NetScaler ADM インベントリに追加します。また、HAProxy インスタンス上に構成されているすべてのフロントエンド、バックエンド、およびサーバーを検出し、フロントエンドを検出されたアプリケーションと見なします。

検出されたすべてのアプリケーションを管理、監視できますが、デフォルトでは、HAProxy App ダッシュボードには検出された 30 のアプリケーションのアプリケーション統計が表示されます。HAProxy App ダッシュボードについて詳しくは、「HAProxy App ダッシュボード」を参照してください。検出されたアプリケーションのアプリケーション統計を 30 を超えて表示する場合は、ライセンスを別途購入する必要があります。

The screenshot shows the 'Managed Third Party licensed Virtual Servers' page in the NetScaler ADM GUI. At the top, there is a navigation breadcrumb: 'Networks > License Settings > Managed Third Party licensed Virtual Servers'. The main heading is 'Managed Third Party licensed Virtual Servers' with a 'Modify Third party licensed Virtual Servers' button and a refresh icon. Below the heading, there are two summary cards: 'Third Party Licenses' with 'Allowed Virtual Servers Equivalent' and 'Total Managed Virtual Servers Equivalent', both showing the value '30'. Underneath, there is a table titled 'Managed Third Party Virtual Servers' with one entry: 'HAProxy Frontend' with a count of '30'. This entry is highlighted with a red rectangular box.

より多くのフロントエンドのライセンスは、100 の仮想サーバーパックで利用できます。有効なライセンスを取得し、NetScaler ADM GUI を使用してライセンスをインストールできます。

### サードパーティライセンスをインストールする

NetScaler ADM にライセンスをインストールすると、検出された 30 を超えるアプリケーションのアプリケーション統計を表示できます。

ライセンスをインストールするには以下を行います。

1. [ネットワーク]>[ライセンス]に移動します。
2. 「ライセンスファイル」セクションで、次のオプションのいずれかを選択します。
  - ローカルコンピューターからライセンスファイルをアップロードします。ライセンスが既にローカルコンピューターに存在する場合は、[Browse] をクリックし、ライセンスの割り当てに使用するライセンスファイル (.lic) を選択します。[完了] をクリックします。
  - ライセンスアクティベーションコードを使用する - 購入したライセンスのライセンスキーを電子メールで送信します。テキストボックスにライセンスキーを入力し、[ **Get Licenses** ] をクリックします。



注

このオプションを選択する場合は、NetScaler ADM がインターネットに接続されていないか、プロキシサーバーが使用可能である必要があります。

Networks > License Settings

License Server Port Settings

Proxy Server Port 0	License Server Port 27000	Vendor Daemon Port 7279
------------------------	------------------------------	----------------------------

License Files

You must upload the license files to this license server. If a license file is already present on your local computer, you can upload it to this license server. Alternatively, you can use the license access code emailed by Citrix to allocate licenses from the Citrix licensing portal.

Upload license files from a local computer  
 Use license access code

[Browse](#) [Finish](#)

To manually Download licenses from Citrix licensing portal please visit <http://www.mycitrix.com> and use the Host ID: **000c29ceda11**

License Expiry Information

Feature	Count	Days To Expiry
No items		

Notification Settings

Email Profile No Email profile is configured	SMS Profile No SMS profile is configured	Alert Threshold 90%	Days To Expiry 30
---	---	------------------------	----------------------

NetScaler ADM にインストールされているライセンスを確認するには、[ネットワーク] > [ライセンス] > [サードパーティライセンス \*\*] の順に選択します。

Networks > License Settings > Managed Third Party licensed Virtual Servers

Managed Third Party licensed Virtual Servers [Modify Third party licensed Virtual Servers](#) [Refresh](#)

Third Party Licenses

Allowed Virtual Servers Equivalent 30	Total Managed Virtual Servers Equivalent 30
--	--

Managed Third Party Virtual Servers

HAProxy Frontend 30
------------------------

### サードパーティライセンスの管理

NetScaler ADM は、HAProxy インスタンスで検出されたアプリケーションをランダムに選択し、自動的にライセンスを取得します。選択された検出済みアプリケーションを変更する場合は、手動で、ライセンス許可された検出済みアプリケーションのライセンスを取り消してから、ライセンス許可する検出済みアプリケーションにライセンスを割り当てる必要があります。

サードパーティライセンスを管理するには、以下を行います。

1. [ネットワーク]>[ライセンス]>[サードパーティライセンス]に移動し、[サードパーティライセンス仮想サーバーの変更]をクリックします。ダッシュボードには、管理されたフロントエンドが表示されます。

HAProxy Frontends

Add the HAProxy Frontends that you want to manage

Add HAProxy Frontends    Mark Unlicensed    Search    ⚙

<input type="checkbox"/>	Host IP Address	Bind Host	Name	Configuration Path
<input type="checkbox"/>	10.106.101.10	10.106.101.10	t_http36	/etc/haproxy/haproxy2.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http21	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http8	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http23	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http17	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http13	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http3	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http29	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http1	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http6	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http27	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http16	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http2	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http5	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http20	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http25	/etc/haproxy/haproxy.cfg

2. リストからフロントエンドを選択し、[ライセンスなし]を選択し、[完了]をクリックしてライセンスを解放します。

HAProxy Frontends

Add the HAProxy Frontends that you want to manage

Add HAProxy Frontends    Mark Unlicensed    Search    ⚙

<input type="checkbox"/>	Host IP Address	Bind Host	Name	Configuration Path
<input checked="" type="checkbox"/>	10.106.101.10	10.106.101.10	t_http36	/etc/haproxy/haproxy2.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http21	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http8	/etc/haproxy/haproxy.cfg
<input checked="" type="checkbox"/>	10.106.101.10	10.106.101.10	http23	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http17	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http13	/etc/haproxy/haproxy.cfg
<input checked="" type="checkbox"/>	10.106.101.10	10.106.101.10	http3	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http29	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http1	/etc/haproxy/haproxy.cfg
<input checked="" type="checkbox"/>	10.106.101.10	10.106.101.10	http6	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http27	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http16	/etc/haproxy/haproxy.cfg

3. ライセンスを解放した後、または使用可能なライセンスをすでに持っている場合は、「HAProxy フロントエンドを追加」をクリックします。

← Choose Virtual Servers Equivalent

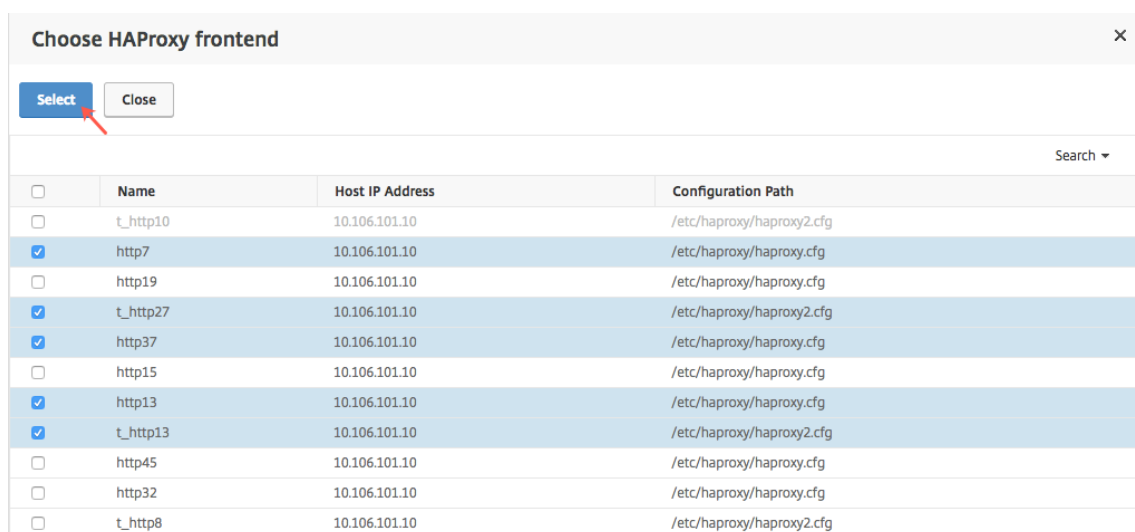
HAProxy Frontends

Add the HAProxy Frontends that you want to manage

Add HAProxy Frontends    Mark Unlicensed    Search    ⚙

<input type="checkbox"/>	Host IP Address	Bind Host	Name	Configuration Path
<input type="checkbox"/>	10.106.101.10	10.106.101.10	t_http36	/etc/haproxy/haproxy2.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http21	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http8	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http23	/etc/haproxy/haproxy.cfg

4. [ **HAProxy** フロントエンドを選択] ダイアログボックスで、リストからライセンスされていないフロントエンドを選択し、[ 選択 ] をクリックします。



5. [ 今すぐ終了 ] をクリックします。

## HAProxy インスタンスのロールベースのアクセス制御

February 6, 2024

Citrix Application Delivery Management (Citrix ADM) は、きめ細かなロールベースのアクセス制御 (RBAC) を使用して構成オブジェクトへのアクセスを制御します。たとえば、ユーザーを作成して特定の HAProxy インスタンスへのアクセスを与えることができます。また [HAProxy App] ダッシュボードの表示/読み取り専用権限を指定できます。詳しくは、「[NetScaler ADM の役割ベースのアクセス制御](#)」を参照してください。

## HAProxy インスタンスの監視

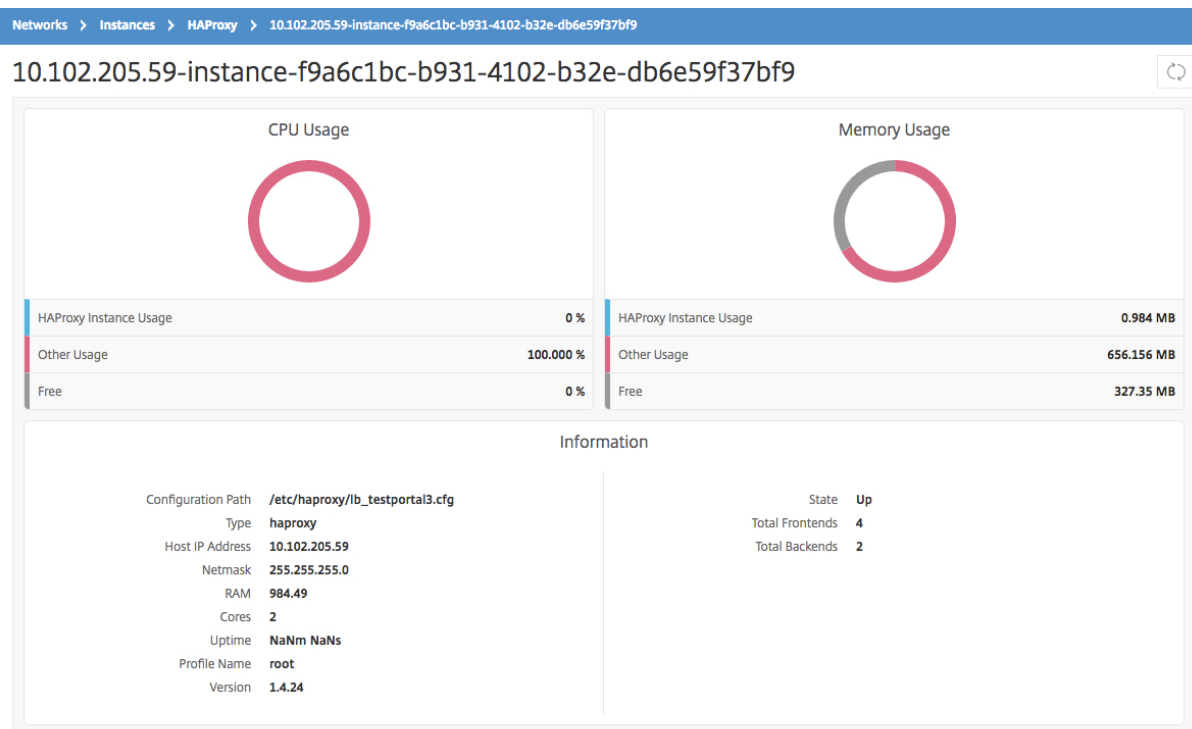
February 6, 2024

Citrix Application Delivery Management (Citrix ADM) の HAProxy ダッシュボードには、HAProxy インスタンスの CPU とメモリの使用状況を追跡するのに役立つグラフが表示されます。このダッシュボードには、次の内容を示すグラフも表示されます。

- ホスト上の HAProxy インスタンスによって使用されている CPU の割合
- ホスト上の他のエンティティによって使用されている CPU の割合
- ホスト上の残りの CPU の割合

- ホスト上の HAProxy インスタンスによって使用されているメモリの割合
- ホスト上の他のエンティティによって使用されているメモリの割合
- ホスト上の残りのメモリの割合

NetScaler ADM で HAProxy インスタンスを監視するには、[ネットワーク] > [インスタンス] > [HAProxy] > [インスタンス] タブに移動し、HAProxy インスタンスを選択し、[ダッシュボード] をクリックします。



## HAProxy インスタンスで構成されたフロントエンドの詳細を表示する

February 6, 2024

NetScaler Application Delivery Management (NetScaler ADM) は、HAProxy インスタンス上で構成されたフロントエンドの次の詳細を報告します。

- ホストの **IP** アドレス。ホストの IP アドレス
- 設定パス。ホスト上の HAProxy インスタンスの絶対設定パス。
- 名前。着信トラフィックを処理するフロントエンドの名前。
- [ホストのバインド]。フロントエンドがバインドされている IP アドレス。
- バインドポート。フロントエンドがバインドされているポート。

HAProxy インスタンスで構成されたフロントエンドを表示するには、次の手順を実行します。

NetScaler ADM で、[ネットワーク] > [ネットワーク機能] > [HAProxy] > [フロントエンド] に移動します。

## Frontends



<input type="checkbox"/>	Host IP Address	Configuration Path	Name	Bind Host	Bind Port
<input type="checkbox"/>	10.102.205.132	haproxy.cfg	http-in	*	80
<input type="checkbox"/>	10.102.205.132	haproxy7.cfg	http-i21n	*	820
<input type="checkbox"/>	10.102.205.132	haproxy4.cfg	http-in	*	80
<input type="checkbox"/>	10.102.205.132	haproxy9.cfg	http-in	*	820
<input type="checkbox"/>	10.102.205.132	haproxy11.cfg	http-i22n	*	8014
<input type="checkbox"/>	10.102.205.132	haproxy6.cfg	http-i22n	*	8014
<input type="checkbox"/>	10.102.205.132	haproxy8.cfg	http-in	*	810
<input type="checkbox"/>	10.102.205.132	haproxy1.cfg	http-in	*	80
<input type="checkbox"/>	10.102.205.132	haproxy6.cfg	http-i1n	*	8025
<input type="checkbox"/>	10.102.205.132	haproxy7.cfg	http-i11	*	8011
<input type="checkbox"/>	10.102.205.132	haproxy6.cfg	http-i1	*	8051
<input type="checkbox"/>	10.102.205.132	haproxy7.cfg	http-i11n	*	8021

## HAProxy インスタンスで設定されたバックエンドの詳細を表示する

February 6, 2024

NetScaler Application Delivery Management (NetScaler ADM) は、HAProxy インスタンス上で構成されたバックエンドアプリケーションの次の詳細を報告します。

- ホストの **IP** アドレス。ホストの IP アドレス。
- 設定パス。ホスト上の HAProxy インスタンスパス。
- 名前。トラフィックの転送先となるバックエンドの名前。
- アルゴリズム。トラフィックを分散させるために使用する負荷分散アルゴリズムです。

**HAProxy** インスタンスで設定されたバックエンドを表示するには、次の手順を実行します。

NetScaler ADM で、[ネットワーク] > [ネットワーク機能] > [**HAProxy**] > [バックエンド] に移動します。

## Backends

<input type="checkbox"/>	Host IP Address	Configuration Path	Name	Algorithm
<input type="checkbox"/>	10.102.205.59	lb_testportal4.cfg	api_backend2	roundrobin
<input type="checkbox"/>	10.102.205.59	lb_testportal3.cfg	api_backend2	roundrobin
<input type="checkbox"/>	10.102.205.59	lb_testportal2.cfg	api_backend1	roundrobin
<input type="checkbox"/>	10.102.205.178	lb_mas.cfg	api_backend2	roundrobin
<input type="checkbox"/>	10.102.205.59	lb_testportal4.cfg	api_backend1	roundrobin
<input type="checkbox"/>	10.102.205.59	lb_testportal1.cfg	api_backend2	roundrobin
<input type="checkbox"/>	10.102.205.178	lb_mas.cfg	api_backend1	roundrobin
<input type="checkbox"/>	10.102.205.59	lb_testportal1.cfg	api_backend1	roundrobin
<input type="checkbox"/>	10.102.205.59	lb_testportal2.cfg	api_backend2	roundrobin
<input type="checkbox"/>	10.102.205.59	lb_testportal3.cfg	api_backend1	roundrobin

## HAProxy インスタンスで設定されたサーバーの詳細の表示

February 6, 2024

Citrix Application Delivery Management (Citrix ADM) は、HAProxy インスタンス上に構成されたサーバーに関する以下の詳細を報告します。

- ホストの **IP** アドレス。ホストの名前です。
- 設定パス。ホスト上の HAProxy インスタンス構成ファイルの絶対パスです。
- バックエンド名。HAProxy 設定のバックエンドの名前。
- 名前。HAProxy 構成内のサーバーの名前です。
- サーバーアドレス。サーバーの IP アドレスです。
- サーバーポート。サーバーによって使用されるポートです。

**HAProxy** インスタンス上で構成されているサーバーを表示するには、次の手順に従います。

NetScaler ADM で、[ ネットワーク ] > [ \*\* ネットワーク 機能 \*\* ] > [ **HAProxy** ] > [ サーバー ] に移動します。

## Servers

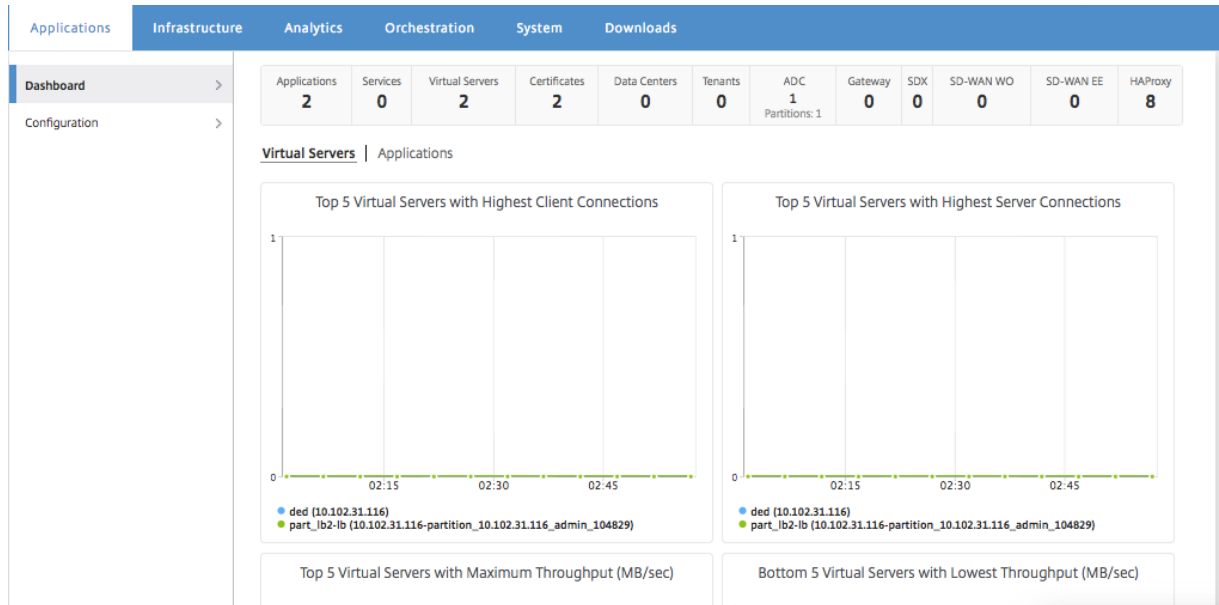
<input type="checkbox"/>	Host IP Address	Configuration Path	Backend Name	Name	Server Address	Server Port
<input type="checkbox"/>	10.102.205.178	lb_mas.cfg	api_backend1	api_machine_1	10.102.31.178	80
<input type="checkbox"/>	10.102.205.59	lb_testportal3.cfg	api_backend1	api_machine_1	10.102.31.178	80
<input type="checkbox"/>	10.102.205.59	lb_testportal4.cfg	api_backend1	api_machine_1	10.102.31.178	80
<input type="checkbox"/>	10.102.205.59	lb_testportal2.cfg	api_backend1	api_machine_1	10.102.31.178	80
<input type="checkbox"/>	10.102.205.59	lb_testportal1.cfg	api_backend1	api_machine_1	10.102.31.178	80

フロントエンドまたはサーバーの数が最も多い **HAProxy** インスタンスを表示する

February 6, 2024

[アプリケーションダッシュボード] に、NetScaler Application Delivery Management (NetScaler ADM) によって検出された HAProxy インスタンスの数が表示され、フロントエンドまたはサーバーの数が最も多く構成されている HAProxy インスタンスの上位 5 つが一覧表示されます。

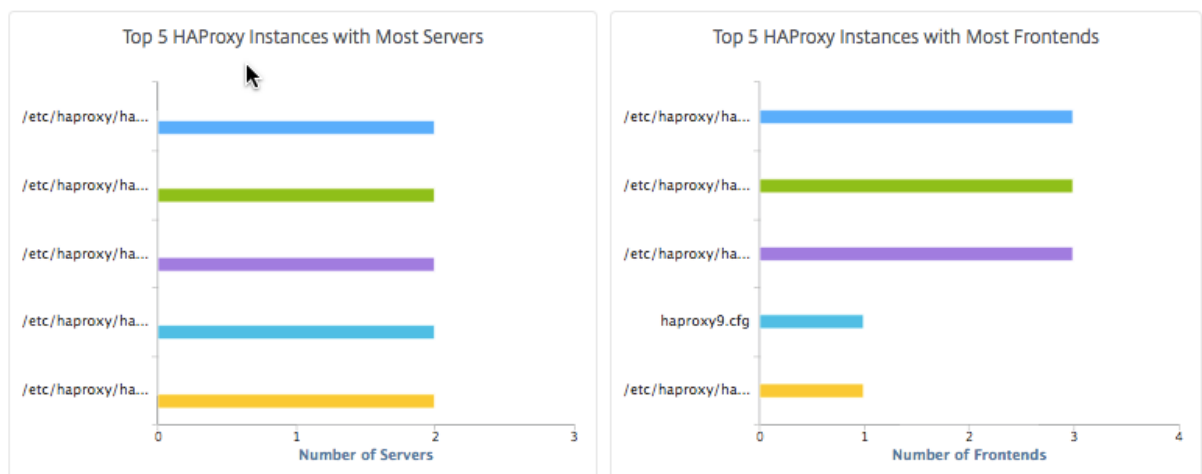
アプリケーションダッシュボードを表示するには、NetScaler ADM で [アプリケーション] > [ダッシュボード] に移動します。



NetScaler ADM によって検出された HAProxy インスタンスの数が、一番上の行に表示されます。



フロントエンドの最大数または最大数のサーバーで構成された上位 5 つの HAProxy インスタンスのリストを表示するには、ダッシュボードを下にスクロールします。



## HAProxy インスタンスを再起動する

February 6, 2024

Citrix Application Delivery Management (Citrix ADM) GUI から HAProxy インスタンスを再起動するには、ハードリスタートまたはソフトリスタートを選択できます。

### ハードリスタート

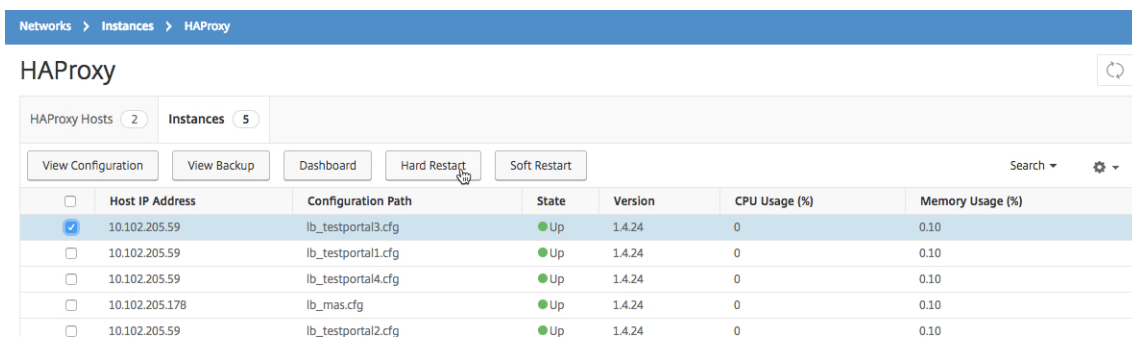
ハード再起動では、インスタンス上の HAProxy プロセスが終了され、確立されている接続がすべて閉じられます。再起動後、新しい HAProxy プロセスが作成され、後続の新しい接続が新しい HAProxy プロセスによって処理されます。

### ソフト再起動

ソフト再起動では、HAProxy プロセスがリスナーポートからバインド解除されますが、既存の接続は、閉じられるまで HAProxy プロセスによって引き続き処理されます。新しい接続を処理するために新しい HAProxy プロセスが作成されます。

HAProxy インスタンスを再起動するには、次の手順に従います。

1. [ネットワーク]>[インスタンス]>[\*\*HAProxy\*\*] に移動し、[インスタンス] タブをクリックします。
2. [インスタンス] タブで、再起動する HAProxy インスタンスを選択します。
3. 「ハード再起動」をクリックして HAProxy インスタンスをハード再起動するか、「ソフト再起動」をクリックして HAProxy インスタンスをソフト再起動します。



The screenshot shows the Citrix ADM GUI for HAProxy instances. The breadcrumb navigation is 'Networks > Instances > HAProxy'. The page title is 'HAProxy'. There are two tabs: 'HAProxy Hosts' (2) and 'Instances' (5). Below the tabs are buttons for 'View Configuration', 'View Backup', 'Dashboard', 'Hard Restart', and 'Soft Restart'. A table lists five instances with columns for Host IP Address, Configuration Path, State, Version, CPU Usage (%), and Memory Usage (%). The 'Hard Restart' button is highlighted with a mouse cursor.

	Host IP Address	Configuration Path	State	Version	CPU Usage (%)	Memory Usage (%)
<input checked="" type="checkbox"/>	10.102.205.59	lb_testportal3.cfg	● Up	1.4.24	0	0.10
<input type="checkbox"/>	10.102.205.59	lb_testportal1.cfg	● Up	1.4.24	0	0.10
<input type="checkbox"/>	10.102.205.59	lb_testportal4.cfg	● Up	1.4.24	0	0.10
<input type="checkbox"/>	10.102.205.178	lb_mas.cfg	● Up	1.4.24	0	0.10
<input type="checkbox"/>	10.102.205.59	lb_testportal2.cfg	● Up	1.4.24	0	0.10

## HAProxy インスタンスのバックアップと復元

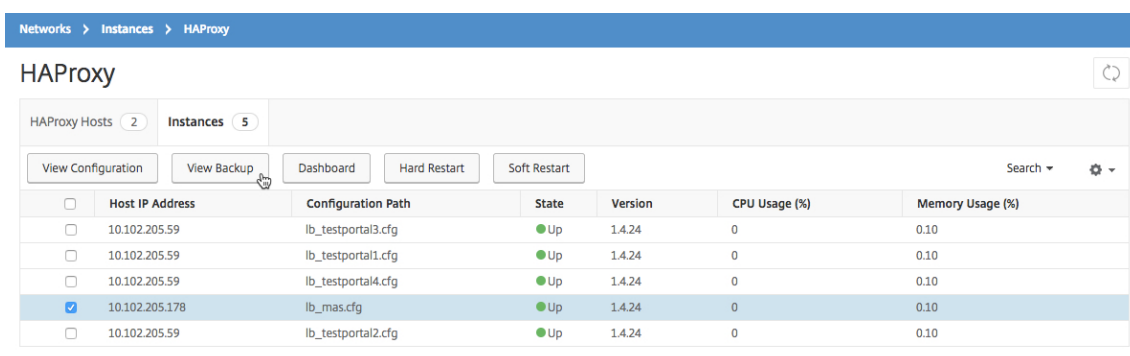
February 6, 2024



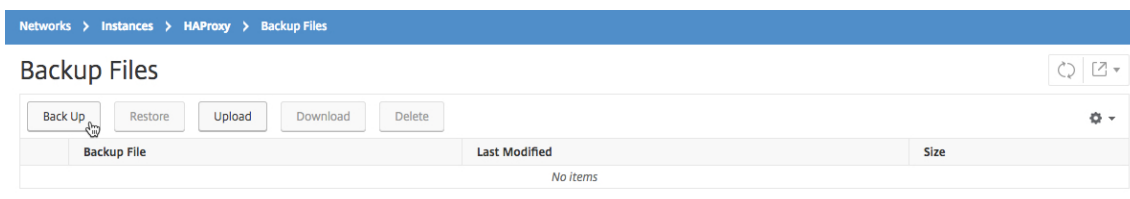
HAProxy 構成ファイルの HAProxy インスタンスの現在の状態をバックアップすることができます。インスタンスが不安定になった場合は、バックアップファイルを使用して、インスタンスを安定した状態に復元できます。

**NetScaler ADM** を使用して **HAProxy** インスタンスをバックアップするには:

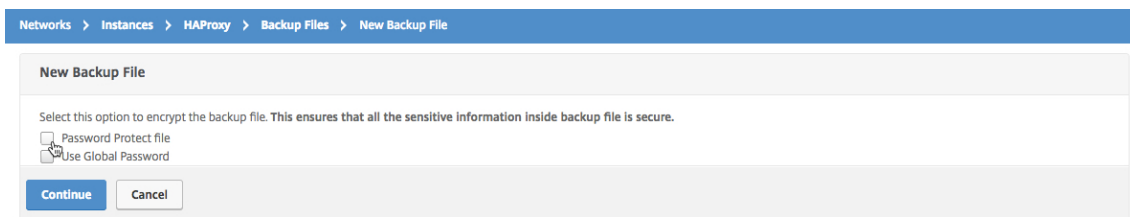
1. Citrix Application Delivery Management (Citrix ADM) で、[ ネットワーク ] > [ インスタンス ] > [ **HAProxy** ] に移動します。
2. **HAProxy** ページで、「インスタンス」タブをクリックします。
3. バックアップする HAProxy インスタンスを選択し、[ バックアップの表示 ] をクリックします。



4. 「バックアップファイル」ページで、「バックアップ」をクリックします。



5. 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こともできます。



6. [ 続行 ] をクリックします。

**NetScaler ADM** を使用してインスタンスを復元するには:

1. [ ネットワーク ] > [ インスタンス ] > [ **\*\*HAProxy\*\*** ] に移動します。
2. **HAProxy** ページで、「インスタンス」タブをクリックします。
3. 復元するインスタンスを選択し、[ **View Backup** ] をクリックします。

Networks > Instances > HAProxy

### HAProxy

HAProxy Hosts 2 Instances 5

View Configuration View Backup Dashboard Hard Restart Soft Restart Search ⌵ ⚙

<input type="checkbox"/>	Host IP Address	Configuration Path	State	Version	CPU Usage (%)	Memory Usage (%)
<input type="checkbox"/>	10.102.205.59	lb_testportal3.cfg	● Up	1.4.24	0	0.10
<input type="checkbox"/>	10.102.205.59	lb_testportal1.cfg	● Up	1.4.24	0	0.10
<input type="checkbox"/>	10.102.205.59	lb_testportal4.cfg	● Up	1.4.24	0	0.10
<input checked="" type="checkbox"/>	10.102.205.178	lb_mas.cfg	● Up	1.4.24	0	0.10
<input type="checkbox"/>	10.102.205.59	lb_testportal2.cfg	● Up	1.4.24	0	0.10

4. **[Backup Files]** ページで、復元するバックアップファイルを選択し、**[Restore]** をクリックします。

Networks > Instances > HAProxy > Backup Files

### Backup Files

Back Up Restore Upload Download Delete Search ⌵ ⚙

<input checked="" type="checkbox"/>	Backup File	Last Modified	Size
<input checked="" type="checkbox"/>	backup_10.102.205.59-instance-e4f6ca3f-02eb-4643-bd77-13b1b8531931_21Apr2017_01_52_03.conf	Fri, 21 Apr 2017 01:52:05 GMT	1.78 KB

注

インスタンスを復元すると、NetScaler ADM ソフトは HAProxy インスタンスを再起動します。

## HAProxy 設定ファイルを編集します

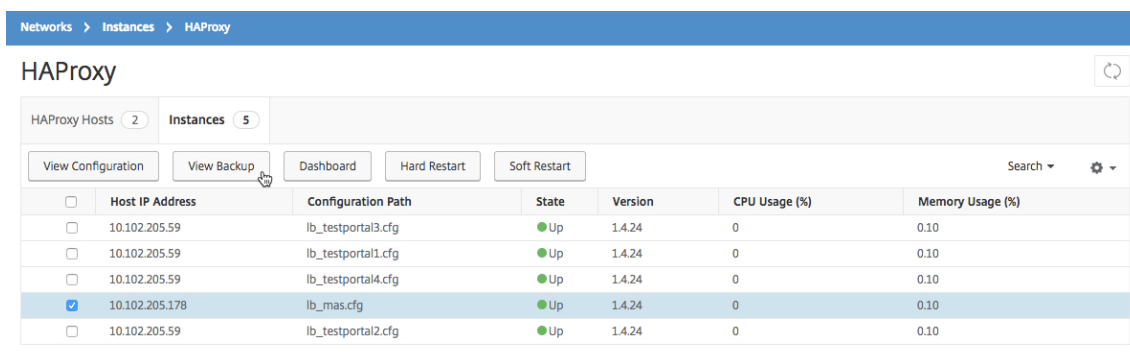
February 6, 2024

既存の HAProxy 設定ファイルのフロントエンド、バックエンド、サーバー、およびその他の設定を更新できます。HAProxy 構成ファイルを編集するには、次の手順に従います。

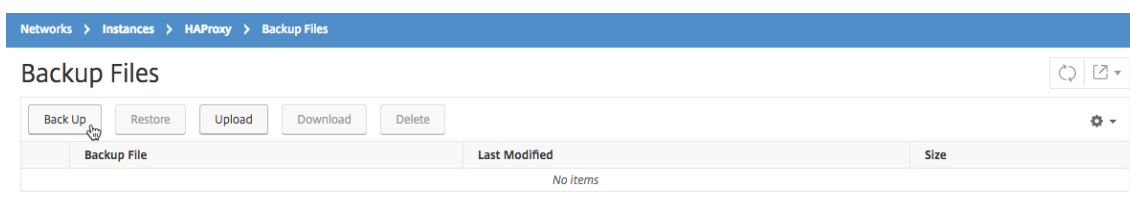
- HAProxy 設定ファイルをバックアップします。
- バックアップの HAProxy 構成ファイルをダウンロードし、オフラインで編集します。
- 更新された HAProxy 構成ファイルを Citrix Application Delivery Management (Citrix ADM) にアップロードします
- 更新したバックアップファイルを使用して HAProxy インスタンスを復元します。

**NetScaler ADM** を使用して **HAProxy** 構成ファイルを編集するには：

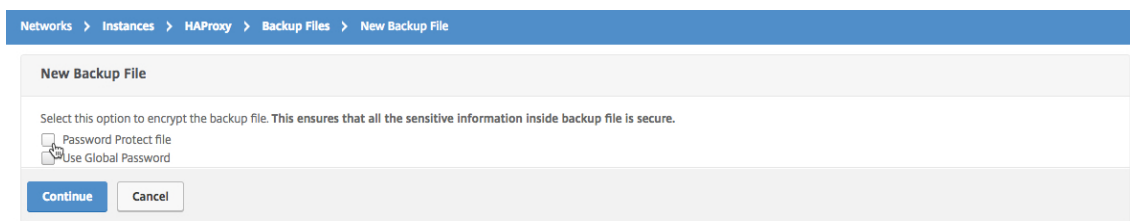
1. Citrix ADM で、[ネットワーク]>[インスタンス]>[\*\*HAProxy\*\*] に移動します。
2. **HAProxy** ページで、「インスタンス」タブをクリックします。
3. バックアップする HAProxy インスタンスを選択し、[バックアップの表示]をクリックします。



4. [Backup Files] ページで [Back Up] をクリックします。



5. [続行] をクリックします。



注

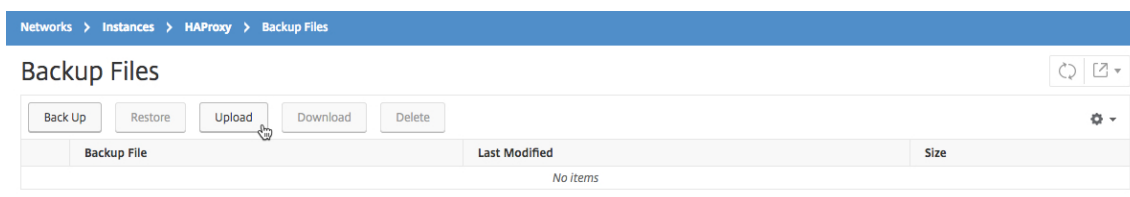
バックアップファイルを暗号化しないでください。

6. [バックアップファイル] ページで、バックアップファイルを選択し、[ダウンロード] をクリックします。



7. テキストエディターを使用して、HAProxy 構成ファイルを編集します。

8. 「バックアップファイル」 ページで 「アップロード」 をクリックして、更新された HAProxy 設定ファイルを参照して選択します。



更新された HAProxy 設定ファイルがアップロードされると、[バックアップファイル] ページに表示されま  
す。

- 更新された HAProxy 設定ファイルを選択し、「復元」をクリックします。

## システム設定の管理

February 6, 2024

次の表では、[システム] > \*\*[\*\* 管理] で使用できるオプションのリストをまとめています。

### ネットワーク構成

ネットワーク構成	オプション	説明
IP アドレス、2 番目の NIC、ホスト 名、プロキシサーバ	IP アドレス	NetScaler ADM の展開に使用され る NetScaler ADM ネットワーク構 成の IP アドレスの詳細を表示します NetScaler ADM 管理アクセスを分 離するように 2 つ目の NIC を構成で きます。詳しくは、「 <a href="#">NetScaler ADM にアクセスするためのデュア ル NIC の構成</a> 」を参照してください。
	2 つ目の NIC	NetScaler ADM にホスト名を割り 当てることができます。詳しく は、「 <a href="#">NetScaler ADM サーバーにホ スト名を割り当てる</a> 」を参照してく ださい。
	プロキシサーバ	ADM をプロキシサーバとして設定 できます。詳しくは、「 <a href="#">API プロキシ サーバとしての NetScaler ADM</a> 」 を参照してください。
静的ルート		静的ルートを構成して、NetScaler ADM と NetScaler ADC VPX イン スタンス間の接続を確立できます

ネットワーク構成	オプション	説明
NTP サーバー		NetScaler ADM クロックが、ネットワーク上の他のサーバーと同じ日付と時刻の設定を持つようにします。詳細については、「 <a href="#">NTP サーバーの構成</a> 」を参照してください。
ADM ポート情報		ADM インスタンスと ADC インスタンスまたは SD-WAN インスタンス間の通信にどのポートを開く必要があるかを理解できます。詳細については、「 <a href="#">サポートされるポート</a> 」を参照してください。

## システム構成

システム構成	オプション	説明
システム、タイムゾーン、許可された URL、今日のメッセージ	基本設定	<code>nsrecover</code> ログインの有効化、セッションタイムアウトの有効化などのシステム設定を変更できます。
	タイムゾーン	NetScaler ADM で使用するタイムゾーンを変更できます。デフォルトのタイムゾーンは UTC です
	許可された URL リスト	ADM に中断のない要求を送信するように URL を設定できます。URL を追加しない場合は、値「none」で設定できます
	今日のメッセージ	NetScaler ADM でウェルカムメッセージを作成できます。この機能を使用して、自分または NetScaler ADM にログオンするユーザーに対するリマインダーメッセージを設定できます。「メッセージを有効にする」をクリックし、メッセージボックスにメッセージを入力して、「保存」をクリックします。

システム構成	オプション	説明
ADM フィンガープリントを表示		一意の NetScaler ADM フィンガープリント ID をコピーして、サービスグラフを使い始めることができます
カスタマー ID の設定		認証された顧客またはユーザだけがネットワークにアクセスできるようにすることで、ネットワークリソースを保護できます。詳しくは、「 <a href="#">データガバナンス</a> 」を参照してください。
CUXIP 設定		このチェックボックスを選択すると、GUI の改善のみを目的として使用統計が収集されます。受信したデータは Citrix のエンジニアのみが使用し、誰とも共有されません。

## システムメンテナンス

システムメンテナンス	説明
NetScaler ADM アップグレード	GUI を使用して NetScaler ADM をアップグレードできます。詳細については、「 <a href="#">アップグレード</a> 」を参照してください。
NetScaler ADM の再起動	NetScaler ADM を再起動できます
NetScaler ADM をシャットダウン	NetScaler ADM をシャットダウンできます
障害回復	災害復旧ノード情報を表示できます。詳細については、「 <a href="#">ディザスタリカバリを構成する</a> 」を参照してください。

## データプルーニング

データブリーニング	オプション	説明
システムとインスタンスのデータブリーニング	システム	NetScaler ADM サーバーデータベースに保存されるレポートデータの量を制限できます。詳細については、「 <a href="#">システム削除設定の構成</a> 」を参照してください。
	インスタンスイベント	NetScaler ADM に保存されるイベントメッセージレポートデータを制限できます。
	インスタンス Syslog	データベースに格納される syslog データの量を制限できます。詳細については、「 <a href="#">インスタンスの Syslog ブリーニング設定の構成</a> 」を参照してください。
	ネットワークレポート作成	NetScaler ADM に保存されるネットワークレポートデータを制限できます。

## バックアップ

バックアップ	オプション	説明
システムとインスタンスのバックアップの設定	システム	システムバックアップを実行する前に、初期バックアップ設定を構成できます。詳細については、「 <a href="#">システムバックアップ設定</a> 」を参照してください。
	インスタンス	NetScaler ADM の設定を構成して、選択した NetScaler ADC 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できます。詳細については、「 <a href="#">インスタンスバックアップ設定の構成</a> 」を参照してください。

## イベント通知





機能の構成	説明
機能の無効化または有効化	NetScaler ADM の機能を有効または無効にすることができます。詳しくは、「 <a href="#">ADM 機能の有効化または無効化</a> 」を参照してください。

## システムバックアップの設定を構成する

February 6, 2024

NetScaler Application Delivery Management (ADM) システムをバックアップおよび復元する前に、初期システムバックアップ設定を設定します。

1. [システム] > [システム管理] に移動します。[バックアップ設定] で、[システムバックアップ設定] をクリックします。
2. 「システムバックアップ設定の構成」 ページで、次の項目を指定します。
  - 保持するバックアップの数。保持できるバックアップは 10 個までです。
  - バックアップファイルの暗号化。
  - 外部転送の有効化。通常の前防措置として、バックアップファイルのコピーのコピーを他のシステムに転送することができます。構成を復元する場合は、まずファイルを Citrix ADM サーバーにアップロードしてから、復元操作を実行する必要があります。サーバー、ユーザー名とパスワード、ポート、使用する転送プロトコル、およびディレクトリパスを指定します。外部転送について詳しくは、「[NetScaler ADM バックアップファイルの外部システムへの転送](#)」を参照してください。
3. **[OK]** をクリックします。

## ← Configure System Backup Settings

Previous backups to retain\*

Encrypt Backup File

Enable External Transfer

Backup happens everyday at 00:30.

### NTP サーバの構成

February 6, 2024

NetScaler Application Delivery Management (ADM) でネットワークタイムプロトコル (NTP) サーバーを構成して、そのクロックを NTP サーバーと同期させることができます。NTP サーバーを構成すると、NetScaler ADM クロックは、ネットワーク上の他のサーバーと同じ日付と時刻の設定になります。

Citrix ADM で NTP サーバーを構成するには:

1. **[System]** > **[NTP Servers]** の順に選択して、**[Add]** をクリックします。
2. **[Create NTP Server]** ページで、次の詳細情報を入力します。
  - **Server Name/IP Address** -NTP サーバーのドメイン名と IP アドレスを入力します。ここで入力したドメイン名と IP アドレスは、NTP サーバーを追加した後は変更できません。
  - **Minimum Poll Interval** -NTP メッセージの送信間隔の最小値を秒数 (2 のべき乗) で指定します。たとえば、最小ポーリング間隔を 64 秒 (2<sup>6</sup> で表すことができる) にするには、6 を入力します。
  - **Maximum Poll Interval** -NTP メッセージの送信間隔の最大値を秒数 (2 のべき乗) で指定します。たとえば、最大ポーリング間隔を 256 秒にする場合、256 は 2 の 8 乗であるため、「8」と入力します。
  - **Key Identifier** - NTP サーバーとの対称キー認証に使用するキー識別子を入力します。Autokey を選択する場合は、キー識別子を追加しないでください。
  - **Autokey** - NTP サーバーとの公開キー認証を使用する場合は、**[Autokey]** を選択します。キー識別子を追加する場合は、Autokey を選択しないでください。
  - **Preferred** -この NTP サーバーをクロック同期の優先サーバーとして指定する場合に、このオプションを選択します。2 台以上のサーバーを構成する場合のみ適用されます。

3. [作成] をクリックします。

← Create NTP Server

Server Name / IP Address\*

Minimum Poll Interval

Maximum Polling Interval

Key Identifier

Autokey  
 Preferred

**NetScaler ADM** で **NTP** 同期を有効にするには:

1. [System] > [NTP Servers] の順に選択します。
2. [NTP 同期化] をクリックし、[NTP 同期を有効にする] チェックボックスをオンにします。
3. [OK] をクリックします。

← NTP Synchronization

Enable NTP Synchronization

注: NTP ログメッセージは、`/var/log/ntpd.log` ファイル内の `/var/log` ディレクトリにあります。

## NetScaler Application Delivery Management (ADM) のアップグレード

February 6, 2024

NetScaler ADM の各リリースでは、機能が強化された新機能および更新された機能が提供されます。機能拡張についてはすべて、リリース発表に付属のリリースノートに記載されています。ソフトウェアをアップグレードする前に、リリースノートをご一読ください。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について理解することが重要です。

**Citrix ADM** をアップグレードするには:

1. [System]>[System Administrations] の順に選択します。[システム管理] サブヘッダーで、[NetScaler ADM のアップグレード] をクリックします。

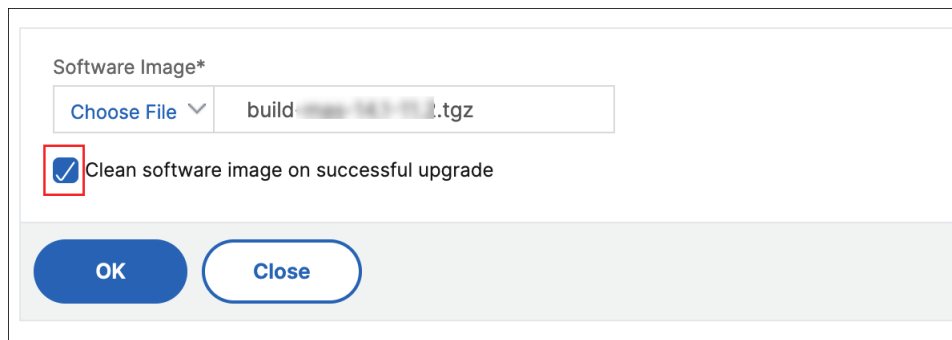
2. [NetScaler ADM のアップグレード] ページで、[ローカル] (ローカルコンピューター) または [アプライアンス] を選択して、新しいイメージファイルをアップロードします。

注

アプライアンスを選択するときは、アップグレードイメージが NetScaler ADM の `/var/mps/mps_images`にあることを確認してください。

デフォルトでは、アップグレードが成功すると、ソフトウェアイメージがクリーンアップされます。

3. **[OK]** をクリックします。



Software Image\*

Choose File

Clean software image on successful upgrade

OK Close

## NetScaler ADM パスワードをリセットする方法

February 6, 2024

NetScaler ADM のパスワードをリセットする手順は、ホストされているハイパーバイザーによって異なる場合があります。デフォルトのパスワードを変更し、デフォルトのパスワードにリセットしたい場合は、NetScaler ADM ノードを再起動してパスワードをリセットできます。

### XenCenter を使用する Citrix Hypervisor:

1. XenCenter を使用して Citrix Hypervisor にログオンします。
2. NetScaler ADM ノードを選択して右クリックし、「再起動」を選択します。
3. \*\* コンソールタブで **CTL+C** を押してブートシーケンスを中断します \*\*。

```
iPXE (http://ipxe.org) 00:04.0 C900 PCI2.10 PMM+00100010+00111020 C900
Press F12 for boot menu.

Boot device: CD-Rom - failure: could not read boot disk

Boot device: Hard Disk - success.

BTX loader 1.00 BTX version is 1.02
Consoles: internal video/keyboard
BIOS drive C: is disk0
BIOS 632kB/3931136kB available memory

FreeBSD/x86 bootstrap loader, Revision NS1.2
Loading /boot/defaults/loader.conf
/mas-12.1-50.28 text=0x9aac71 data=0x1cf79e30+0x4db1d0 syms=[0x8+0xc59a0+0x8+0xb
7421]

Press [Ctrl-C] for command prompt, or any other key to boot immediately.
Booting [/mas-12.1-50.28] in 2 seconds...
```

4. OK プロンプトで **boot-s** コマンドを実行します。

```
iPXE (http://ipxe.org) 00:04.0 C900 PCI2.10 PMM+00100010+00111020 C900
Press F12 for boot menu.

Boot device: CD-Rom - failure: could not read boot disk

Boot device: Hard Disk - success.

BTX loader 1.00 BTX version is 1.02
Consoles: internal video/keyboard
BIOS drive C: is disk0
BIOS 632kB/3931136kB available memory

FreeBSD/x86 bootstrap loader, Revision NS1.2
Loading /boot/defaults/loader.conf
/mas-12.1-50.28 text=0x9aac71 data=0x1cf79e30+0x4db1d0 syms=[0x8+0xc59a0+0x8+0xb
7421]
\
Press [Ctrl-C] for command prompt, or any other key to boot immediately.
Booting [/mas-12.1-50.28] in 1 second...

Type '?' for a list of commands, 'help' for more detailed help.
OK _
```

NetScaler ADM が再起動し、次のメッセージが表示されます。

```

talk_to_backend: xn_num_q 1 max_q 16 err 0
xn0: backend features:xbd0: 122880MB <Virtual Block Device> at device/vbd/768 on
xenbusb_front0
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usb0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usb0
ugen0.2: <QEMU 0.10.2> at usb0
ums0: <Endpoint1 Interrupt Pipe> on usb0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
MS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh: █

```

5. **Enter** キーを押して /u @ プロンプトを表示します。

```

xn0: backend features:xbd0: 122880MB <Virtual Block Device> at device/vbd/768 on
xenbusb_front0
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usb0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usb0
ugen0.2: <QEMU 0.10.2> at usb0
ums0: <Endpoint1 Interrupt Pipe> on usb0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
MS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh:
\u@ █

```

6. 次のコマンドを使用して、フラッシュパーティションをマウントします。

```
mount dev/ad0s1a /flash
```

```

xenbusb_front0
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label (16h,63s != 255h,63s) (proceeding anyway)
Root mount waiting for: usb0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usb0
ugen0.2: <QEMU 0.10.2> at usb0
ums0: <Endpoint1 Interrupt Pipe> on usb0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibility
Enter full pathname of shell or RETURN for /bin/sh:
\nu@mount dev/ad0s1a /flash
\nu@

```

7. 次のコマンドを使用してファイルを作成します。

```
touch /flash/mpsconfig/.recover
```

これで、パスワードがデフォルトのパスワードにリセットされます。

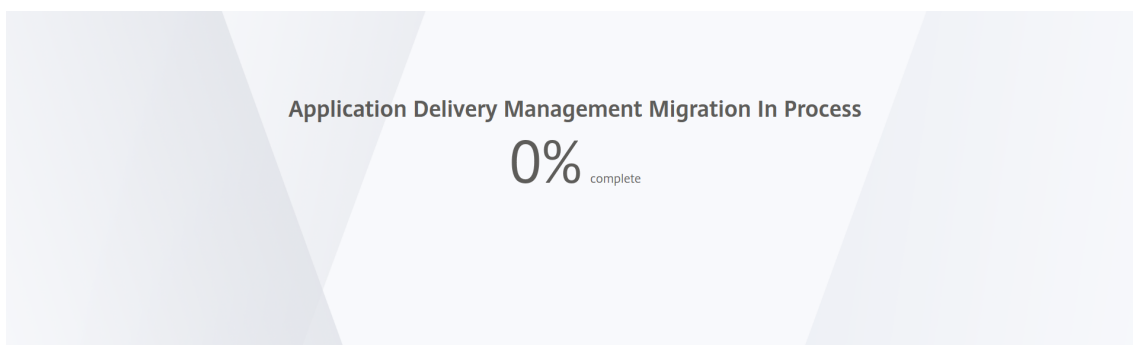
8. 再起動コマンドを実行して **Citrix ADM** を再起動します。

```

xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label (16h,63s != 255h,63s) (proceeding anyway)
Root mount waiting for: usb0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usb0
ugen0.2: <QEMU 0.10.2> at usb0
ums0: <Endpoint1 Interrupt Pipe> on usb0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibility
Enter full pathname of shell or RETURN for /bin/sh:
\nu@mount dev/ad0s1a /flash
\nu@touch /flash/mpsconfig/.recover
\nu@reboot

```

9. NetScaler ADM GUI にアクセスし、再起動が完了するまで待ちます。



nsroot/nsroot 認証情報を使用して GUI からログオンし、nsrecover/nsroot を使用して Hypervisor からログオンできるようになりました。

注

再起動後、パスワードがデフォルトパスワードにリセットされない場合は、同じ手順（手順 1～7）を繰り返します。次に、次のコマンドを実行して NetScaler ADM を再起動します。

- `rm /flash/mpsconfig/master.passwd`
- `rm -rf /etc/passwd`

#### vSphere を使用する ESX:

1. vSphere を使用して ESX にログオンします。
2. NetScaler ADM ノードを選択して右クリックし、[再起動] を選択します。
3. \*\* コンソールタブで **CTL+C** を押してブートシーケンスを中断します \*\*。

```
iPXE (http://ipxe.org) 00:04.0 C900 PCI2.10 PMM+00100010+00111020 C900
Press F12 for boot menu.
Boot device: CD-Rom - failure: could not read boot disk
Boot device: Hard Disk - success.
BTX loader 1.00 BTX version is 1.02
Consoles: internal video/keyboard
BIOS drive C: is disk0
BIOS 632kB/3931136kB available memory
FreeBSD/x86 bootstrap loader, Revision NS1.2
Loading /boot/defaults/loader.conf
/mas-12.1-50.28 text=0x9aac71 data=0x1cf79e30+0x4db1d0 syms=[0x8+0xc59a0+0x8+0xb7421]
press [Ctrl-C] for command prompt, or any other key to boot immediately.
booting [/mas-12.1-50.28] in 2 seconds...
```

4. OK プロンプトで **boot-s** コマンドを実行します。

NetScaler ADM が再起動します。



5. **Enter** キーを押して /u @ プロンプトを表示します。
6. 次のコマンドを使用して、フラッシュパーティションをマウントします。

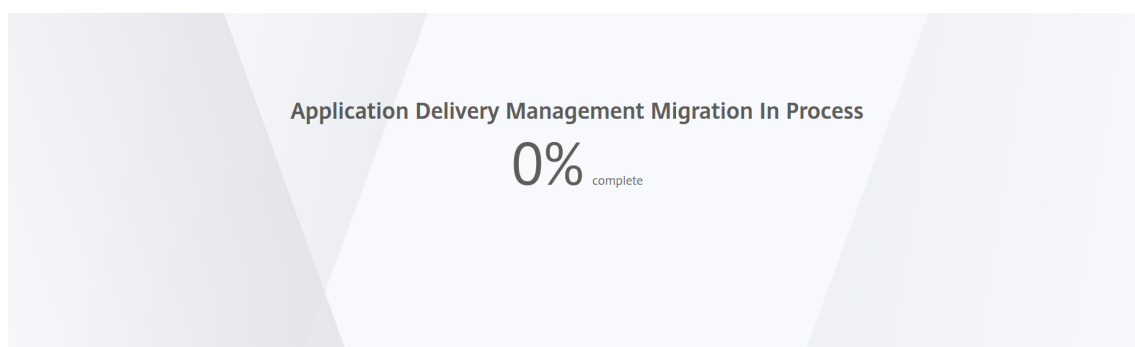
```
mount dev/da0s1a /flash
```

7. 次のコマンドを使用してファイルを作成します。

```
touch /flash/mpsconfig/.recover
```

これで、パスワードがデフォルトのパスワードにリセットされます。

8. 再起動コマンドを実行して **Citrix ADM** を再起動します。
9. NetScaler ADM GUI にアクセスし、再起動が完了するまで待ちます。



nsroot/nsroot 認証情報を使用して GUI からログオンし、nsrecover/nsroot を使用して ESX サーバからログオンできるようになりました。

注

再起動後、パスワードがデフォルトパスワードにリセットされない場合は、同じ手順（手順 1～7）を繰り返します。次に、次のコマンドを実行して NetScaler ADM を再起動します。

- `rm /flash/mpsconfig/master.passwd`
- `rm -rf /etc/passwd`

### Hyper-V マネージャーを使用する **Hyper-V**:

1. hyper-v マネージャーを使用して hyper-v にログオンします。
2. NetScaler ADM ノードを選択して右クリックし、[再起動] を選択します。
3. \*\* コンソールタブで **CTL+C** を押してブートシーケンスを中断します \*\*。

```

iPXE (http://ipxe.org) 00:04.0 C900 PCI2.10 PMM+00100010+00111020 C900
Press F12 for boot menu.

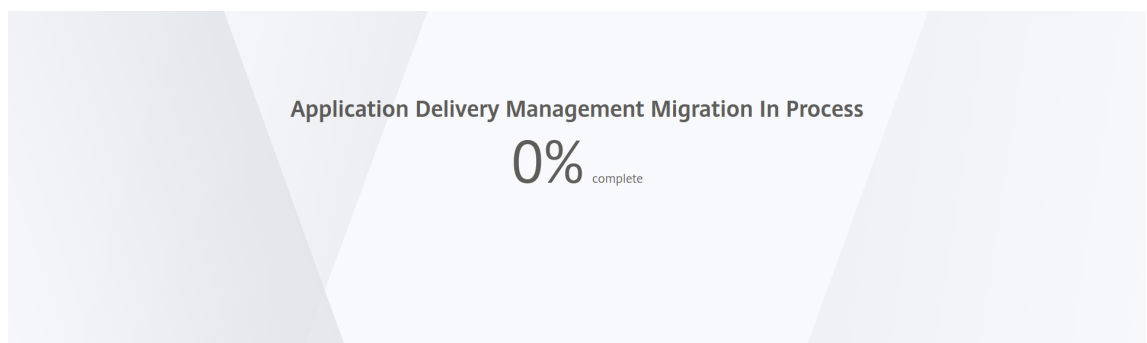
Boot device: CD-Rom - failure: could not read boot disk
Boot device: Hard Disk - success.

BTX loader 1.00 BTX version is 1.02
Consoles: internal video/keyboard
BIOS drive C: is disk0
BIOS 632kB/3931136kB available memory

FreeBSD/x86 bootstrap loader, Revision NS1.2
Loading /boot/defaults/loader.conf
/mas-12.1-50.28 text=0x9aac71 data=0x1cf79e30+0x4db1d0 syms=[0x8+0xc59a0+0x8+0xb
7421]

Press [Ctrl-C] for command prompt, or any other key to boot immediately.
booting [/mas-12.1-50.28] in 2 seconds...
    
```

4. OK プロンプトで **boot-s** コマンドを実行します。  
NetScaler ADM が再起動します。
5. **Enter** キーを押して /u @ プロンプトを表示します。
6. 次のコマンドを使用して、フラッシュパーティションをマウントします。  
`mount dev/ad0s1a /flash`
7. 次のコマンドを使用してファイルを作成します。  
`touch /flash/mpsconfig/.recover`  
これで、パスワードがデフォルトのパスワードにリセットされます。
8. 再起動コマンドを実行して **Citrix ADM** を再起動します。
9. NetScaler ADM GUI にアクセスし、再起動が完了するまで待ちます。



nsroot/nsroot 認証情報を使用して GUI からログオンし、nsrecover/nsroot を使用して Hyper-V マネージャからログオンできるようになりました。

## 注

再起動後、パスワードがデフォルトパスワードにリセットされない場合は、同じ手順（手順 1～7）を繰り返します。次に、次のコマンドを実行して NetScaler ADM を再起動します。

- `rm /flash/mpsconfig/master.passwd`
- `rm -rf /etc/passwd`

**Linux KVM サーバー (SSH クライアントを使用して KVM サーバーに SSH):**

1. SSH クライアントを使用して NetScaler ADM に KVM サーバーにログオンします。
2. NetScaler ADM を再起動します。
3. `/boot/default/loader.conf` のメッセージが表示された直後にブートシーケンスを中断するには、**CTL** キーを押しながら **C** キーを押します。
4. OK プロンプトで、次のコマンドを実行します。

```
set console='comconsole,vidconsole'
```

5. **boot-s** コマンドを実行して、NetScaler ADM を再起動します。
6. 「シェルのフルパスを入力してください」または「**/bin/sh:**」というメッセージが表示されたら、**Enter** キーを押して `/u @` プロンプトを表示します。
7. 次のコマンドを使用して、フラッシュパーティションをマウントします。

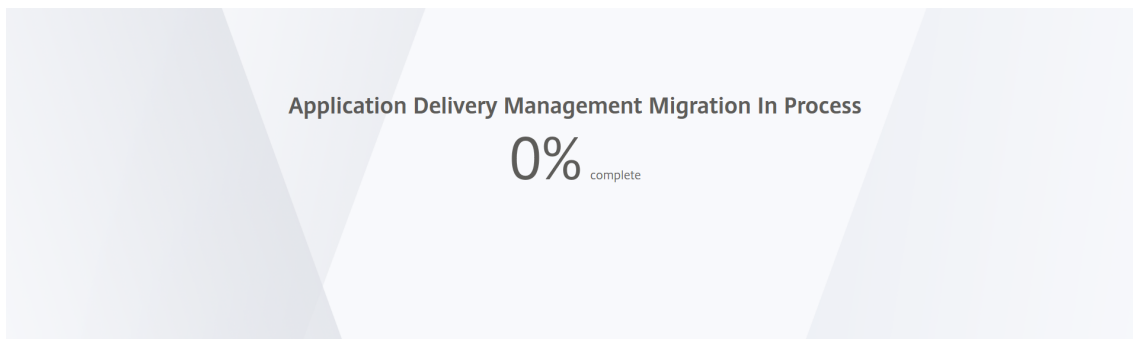
```
mount dev/vtbd0s1a /flash
```

8. 次のコマンドを使用してファイルを作成します。

```
touch /flash/mpsconfig/.recover
```

これで、パスワードがデフォルトのパスワードにリセットされます。

9. 再起動コマンドを実行して **Citrix** ADM を再起動します。
10. NetScaler ADM GUI にアクセスし、再起動が完了するまで待ちます。



`nsro ot/nsroot` 認証情報を使用して GUI からログオンし、`nsrecover/nsroot` を使用して SSH コンソールからログオンできるようになりました。

注

再起動後、パスワードがデフォルトパスワードにリセットされない場合は、同じ手順（手順 1～7）を繰り返します。次に、次のコマンドを実行して NetScaler ADM を再起動します。

- `rm /flash/mpsconfig/master.passwd`
- `rm -rf /etc/passwd`

## NetScaler ADM にアクセスするためのデュアル NIC の構成

February 6, 2024

NetScaler ADM への管理アクセスを分離するために、2 つ目の NIC を構成できます。この 2 つ目の NIC 機能を使用すると、要件に応じて、NetScaler ADM を介して送受信されるトラフィックをどのように分離するかを選択できます。

トラフィックを次のように分離したいシナリオを考えてみましょう。

- NetScaler ADM とその管理対象 NetScaler ADC インスタンス間のすべての通信を 1 つのネットワーク内で実現します。
- 別のネットワークにある NetScaler ADM への管理アクセス権を持っている。

このシナリオでは、管理者は次のことができます。

- NetScaler ADM とその管理対象 NetScaler ADC インスタンス間のトラフィック用に 1 つの IP アドレスを設定します。
- NetScaler ADM ソフトウェアを管理するための別の IP アドレスを設定して、ソフトウェア内のすべての管理タスクを実行します。

注

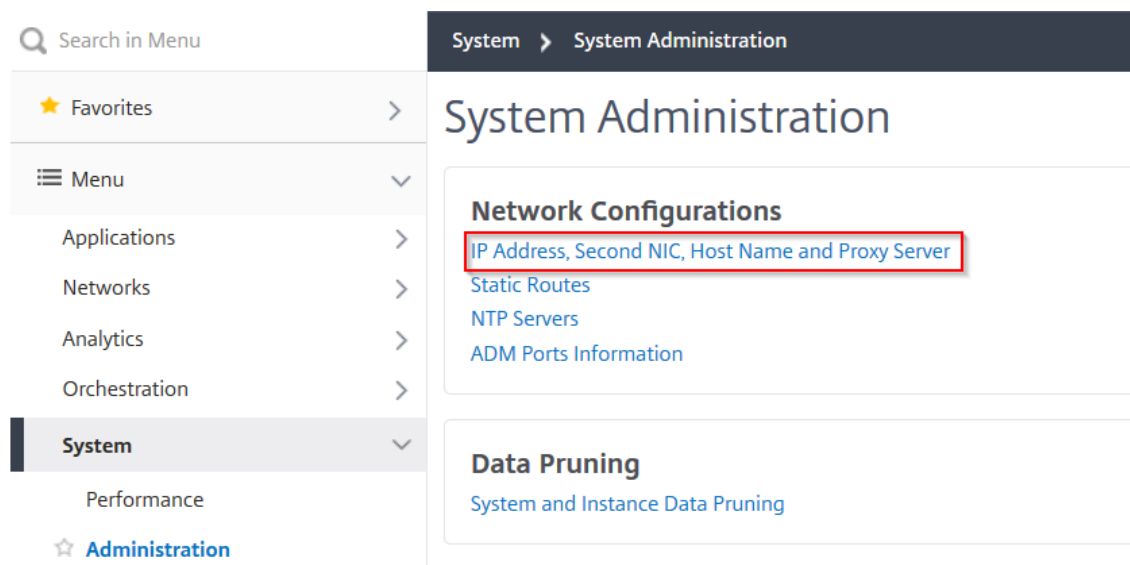
NetScaler ADM が HA ペアとして構成されている場合、2 番目の NIC で構成された管理 IP アドレスはプライマリノードに関連付けられます。

### 前提条件

- ハイパーバイザー（**Citrix Hypervisor**、**Microsoft Hyper-V**、**Linux KVM**、または **VMware ESXi**）に **NetScaler ADM 13.0** ビルド **47.x** 以降を展開して構成していることを確認します。
- ハイパーバイザー（Citrix Hypervisor、Microsoft Hyper-V、Linux KVM、または VMware ESXi）に 2 つ目の NIC が追加されていることを確認します。

## NetScaler ADM で 2 つ目の NIC を設定します

1. ADM GUI にログインします。
2. [システム] > [管理] に移動します。
3. [ネットワーク構成] で、[IP アドレス]、[2 番目の NIC]、[ホスト名]、[プロキシサーバー] の順にクリックします。



「ネットワーク構成」ページが表示されます。

4. Second NIC タブをクリックし、次のパラメータを設定します。
  - a) アプリケーション配信管理 **IP** アドレス—NetScaler ADM にアクセスするための有効な IP アドレスを入力します。既存の管理 IP アドレスとは別に、この IP アドレスを使用して NetScaler ADM にアクセスできます。
  - b) **Netmask** —ネットワークホストを指定するネットマスクアドレスを入力します。デフォルトのアドレスは 255.255.255.0 です。
  - c) ネットワークアドレス—IP アドレスを入力して、NetScaler ADM のルートエントリを追加します。+ をクリックして IP アドレスをさらに追加します。この情報は入力しなくても構いません。
  - d) [保存] をクリックします。

## ← Network Configuration

IP Address	>
<b>Second NIC</b>	>
Host Name	>
Proxy Server	>

### Configure Second NIC

Application Delivery Management IP Address\*

 ⓘ

Netmask\*

 ⓘ

Network Address

 + ⓘ

**Save**

## syslog パージ間隔の設定

February 6, 2024

Syslog は、ログ記録用の標準プロトコルです。これには、Citrix Application Delivery Controller (ADC) インスタンスで実行される Syslog 監査モジュールと、Citrix ADC インスタンスの基盤となる FreeBSD オペレーティングシステム (OS) またはリモートシステムのいずれかで実行できる Syslog サーバーの 2 つのコンポーネントがあります。Syslog は、データ転送に UDP (User Datagram Protocol: ユーザーデータグラムプロトコル) を使用します。

Syslog によって、情報を生成するシステムと、情報を保存するシステムを分離できます。ログ情報を統合して、集められたデータから詳細な情報を得られます。Syslog を構成して、さまざまな種類のイベントをログ記録することもできます。

データベースに保存される syslog データの量を制限するには、syslog データを削除する間隔を指定できます。次の syslog データが NetScaler Application Delivery Management (ADM) から削除されるまでの日数を指定できます。

- 汎用 Syslog データ
- AppFirewall データ
- NetScaler Gateway データ

Citrix Gateway プルーニング間隔を syslog タイプごとに構成することもできます。このプルーニング間隔は、Citrix Gateway データを保持するように構成された実行間隔よりも優先されます。

**NetScaler ADM syslog** プルーニング間隔設定を構成するには：

1. [システム] > [管理] に移動します。[データのプルーニング] で、[システムとインスタンスのデータのプルーニング] をクリックし、[インスタンスの **Syslog**] をクリックします。
2. インスタンスの **Syslog** プルーニング設定ページで、「**Syslog** 汎用データの保持 (日数)」を指定します。NetScaler ADM が汎用 syslog メッセージを保持する日数を入力します。

## ← Configure Instance Syslog Prune Settings

You can specify the number of days after which the following syslog data will be deleted from the Citrix ADM server.

Retain Syslog Generic Data\*

 ?

OK

Close

## システムプルーニングとイベントプルーニングの設定

February 6, 2024

NetScaler Application Delivery Management (ADM) ソフトウェアデータベースに格納されるレポートデータの量を制限するには、そのデータをプルーニングできます。NetScaler ADM でネットワークレポートデータ、イベント、監査ログ、タスクログを保持する間隔を指定できます。デフォルトでは、これらのデータは 24 時間ごとに (00:00 の時刻に) 削除されます。

注

指定する値は 30 日を超えることも、15 日未満にすることもできません。

**NetScaler ADM** を使用してパフォーマンスレポートのシステム削除設定を構成するには：

1. [システム] > [管理] に移動します。[データプルーニング] で、[システムとインスタンスのデータプルーニング] をクリックします。
2. [システム削除設定の構成] ページで、データを保持する日数を指定し、[ **OK** ] をクリックします。

### Configure System Prune Settings

Data to keep (days)\*  
 ⓘ

Pruning happens every day at 00:00

Auto Prune Details:

Enable Automatic Data Prune

Pruning starts when any one of the criteria is met – data prune threshold value or data to keep (days). Whichever is met first, takes precedence over the other.

Data Prune Threshold Value (%)

[Save](#)

自動プルーニングを有効にするには、[自動データプルーニングを有効にする] チェックボックスをオンにします。ディスク使用量が設定されたデータプルーニングしきい値を超えると、アラームがトリガーされ、電子メールが送信されます。ディスク領域の割合（プルーニングしきい値）を変更するには、[編集] をクリックします。

#### 注

: プルーニングは、データプルーニングのしきい値または保持するデータ（日数）のいずれかの基準が満たされたときに開始されます。どちらが先に満たされたかが、他方より優先されます。

**diskutilizationHigh** アラームを設定および有効にし（デフォルト）、次の項目を指定できます。

- 重大度（クリティカルなど）。
- アラームしきい値。イベントの重要度を計算する基準となる値を入力します。
- 時間。アラームをトリガーするまでの時間（分単位）。



## Configure Alarm

Alarm Name

diskUtilizationHigh

Enable Alarm

Severity

Critical

Alarm Threshold

80

Time (minutes)

5

OK Close

### NetScaler ADM を使用してイベントプールの設定を構成する

NetScaler ADM データベースに格納されるイベントメッセージデータの量を制限するには、NetScaler ADM がネットワークレポートデータ、イベント、監査ログ、およびタスクログを保持する間隔を指定できます。デフォルトでは、これらのデータは 24 時間ごとに (00:00 の時刻に) 削除されます。

- [システム] > [管理] > [データプルーニング] に移動し、[システムとインスタンスデータのプルーニング] をクリックします。[インスタンスイベント] をクリックします。
- NetScaler ADM サーバーでデータを保持する間隔を日単位で入力し、[保存] をクリックします。

### デフォルト以外のユーザーのシェルアクセスを有効にする

February 6, 2024

Citrix Application Delivery Management (ADM) では、デフォルト以外のユーザーのシェルアクセスを有効にできます。この機能を使用し、インスタンスとの通信モードを有効にして、セットアップできます。

注

特に指定しない限り、デフォルト以外のユーザーに対してシェルアクセスは無効になっています。

**Citrix ADM** でデフォルト以外のユーザーのシェルアクセスを有効にするには:

1. NetScaler ADM で、[システム] > [システム管理] に移動します。
2. [System Settings] の [Change System Settings] をクリックします。
3. [Modify System Settings] ページで次のパラメーターを構成します。
  - **Communication with instances** - 通信プロトコルを選択します。
  - 安全なアクセス-Citrix ADM の安全なアクセスを有効にします。
  - **Enable Session Timeout** - 非アクティブなセッションを保持する期間を指定します。
  - **Allow Basic Authentication** - 基本認証プロトコルを使用して提供された資格情報を管理サービスが受け入れられるようにします。
  - **nsrecover nsrecover** ログインを有効にする -管理サービスでログインを有効にします。
  - 証明書のダウンロードを有効にする -追加した NetScaler ADC から証明書をダウンロードできます。
  - **nsroot** 以外のユーザーのシェルアクセスを有効にする-Citrix ADM のデフォルト以外のユーザーのシェルアクセスを有効にします。
  - インスタンスログインのユーザー資格情報を要求する -Citrix ADM からインスタンスにログオンするときに、ユーザーがユーザー資格情報を入力できるようにします。
4. [OK] をクリックします。

## アクセスできない **NetScaler ADM** サーバーをリカバリする

February 6, 2024

Citrix Application Delivery Management (ADM) には、システムデータベースのクリーンアップを実行するデータベースメンテナンスツールが提供されるようになりました。これで、Citrix ADM ユーティリティツールを起動してファイルシステムに接続し、いくつかのコンポーネントを削除して、データベースにアクセスできるようになります。Citrix ADM リカバリスクリプトは、古いデータベーステーブルや未使用のデータベーステーブルやファイルを消去することで、ファイルシステム内のスペースを回復するのに役立つツールです。このツールを使用すると、データベーステーブルやファイル間を連続してナビゲートでき、ファイルシステム上で現在占められているスペースが各項目ごとに表示されます。削除するデータベーステーブルとファイルを選択すると、ツールは確認後にそれらをファイルシステムから削除します。

## Citrix ADM スタンドアロン展開で Citrix ADM データベース回復スクリプトを使用する方法

単一サーバーの NetScaler ADM 展開環境で次の手順を使用して、ファイルシステムに接続し、いくつかのコンポーネントを削除し、データベースにアクセスできるようにしてから、リカバリ操作を実行します。

1. SSH クライアントまたはハイパーバイザーのコンソールを使用して NetScaler ADM にログオンし、次のコマンドを入力します。

```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

2. いくつかの NetScaler ADM プロセスを停止するための注意メッセージが画面に表示されたら、「y」と入力して **Enter** キーを押します。

次の画面が表示され、システムのコアファイルに影響を与えずに削除できるデータベースのコンポーネントが決定されます。

```
-----
***** Citrix ADM Cleanup Utility *****
-----

This utility helps you gain disk space by performing cleanup.

Checking whether DB is accessible...

DB is accessible.

Please wait. Gathering data. This will take some time.

<----->
```

3. 画面に、データベース内のファイルのリストが表示されます。「y」と入力し、Enter キーを押してクリーンアッププロセスを開始します。

```

----- SUMMARY -----
DB component                Current size
-----
Analytics ----- 184.58 MB
Perf Reports ----- 43.73 MB
App Summary ----- 12.03 MB
App Health Summary ----- 6.33 MB
App Counter Data ----- 5.30 MB
Device Syslogs ----- 56.00 KB
Device Events ----- 40.00 KB

Filesystem component        Current size
-----
Citrix ADM Images ----- 15.51 GB
Core Files ----- 718.37 MB
Citrix ADC Images ----- 453.32 MB
Techsupport Bundles ----- 439.35 MB
Device Backup ----- 131.79 MB
Citrix ADM Backup ----- 35.21 KB
Citrix ADC VPX ESXi Images ----- 0.00 B
Citrix ADC SDX Images ----- 0.00 B
Citrix ADC CPX images ----- 0.00 B

-----

Do you wish to proceed with cleanup?
[y/n]: 

```

4. クリーニングが必要な特定のデータベースコンポーネントを選択し、対応する番号を入力できます。**Enter** キーを押します。

たとえば、システムカタログのクリーンアップを実行するには、**DB** コンポーネント選択メニューでオプション 8 を選択し、「y」と入力して **Enter** キーを押してシステムカタログのクリーンアップを続行します。

#### 注

: Citrix ADM には、システムカタログと呼ばれるユーザーテーブルが含まれています。システムカタログは、Citrix ADM データベース内の場所であり、リレーショナルデータベース管理システムは、テーブルや列、内部レコードに関する情報などのスキーマメタデータを格納します。システムカタログのテーブルは通常のテーブルに似ており、時間が経つにつれて膨張した行や使用されなくなった行が蓄積されることがあるため、最適なパフォーマンスを得るには定期的なクリーンアップが必要です。これらのテーブルは定期的に管理することをお勧めします。このアクティビティにより、ディスク容量が解放されるだけでなく、データベース全体、ひいては Citrix ADM のパフォーマンスも向上します。

```
***** Citrix ADM Cleanup Utility *****
-----
                                DB components
                                -----

Enter the number corresponding to the menu entry.
You can input multiple space separated numbers.
E.g. '1 2 4' will select entries numbered 1, 2, and 4.

[0] Go back and start again
[1] Analytics ----- 184.58 MB
[2] Perf Reports ----- 41.84 MB
[3] App Summary ----- 11.84 MB
[4] App Health Summary ----- 6.09 MB
[5] App Counter Data ----- 5.09 MB
[6] Device Syslogs ----- 56.00 KB
[7] Device Events ----- 40.00 KB
[8] Clean System Catalog
[9] Select all
[10] Continue without selecting

Your input: 8
Are you sure you want to CLEAN SYSTEM CATALOG tables?

[y/n]: y
```

クリーンアップユーティリティには、データベースコンポーネントとファイルコンポーネントをクリーンアップするオプションがあります。「1」から「9」までの数字を入力して任意のファイルコンポーネントを選択するか、「11」と入力して Enter キーを押してデータベースコンポーネントをクリーンアップできます。

注:

「11」という数字は、クリーンアップするファイルコンポーネントを何も選択しておらず、以前に選択していたデータベースコンポーネントのクリーンアップを続行していることを示します。この例では、「システムカタログ」です。

```

***** Citrix ADM Cleanup Utility *****
-----
                        Filesystem components
                        -----

Enter the number corresponding to the menu entry.
You can input multiple space separated numbers.
E.g. '1 2 4' will select entries numbered 1, 2, and 4.

[0] Go back and start again
[1] Citrix ADM Images ----- 15.51 GB
[2] Core Files ----- 718.37 MB
[3] Citrix ADC Images ----- 453.32 MB
[4] Techsupport Bundles ----- 439.35 MB
[5] Device Backup ----- 131.79 MB
[6] Citrix ADM Backup ----- 35.21 KB
[7] Citrix ADC VPX ESXi Images 0.00 B
[8] Citrix ADC SDX Images --- 0.00 B
[9] Citrix ADC CPX images --- 0.00 B
[10] Select all
[11] Continue without selecting

Your input: 11
    
```

5. 最終確認画面で「y」と入力し、**Enter** キーをもう一度押します。

```

***** Citrix ADM Cleanup Utility *****
-----
                        FINAL CONFIRMATION

                        These components will be cleaned.

                        DB components
                        -----

                        >> System Catalog

No data has been deleted yet.

If you choose to proceed, all ADM processes will be stopped
for the remainder of the cleanup.

Do you wish to proceed with cleanup?
[y/n]:
    
```

システムカタログはクリーンアップされます。システムカタログのテーブルのサイズによっては、時間がかかる場合があります。プロセスが完了すると、概要画面が表示されます。

```
-----
***** Citrix ADM Cleanup Utility *****
-----
                          SUMMARY
-----
                          DB components
-----

Component name           Present size           Size cleared
-----
System Catalog ----- 189.15 MB ----- 0.00 B
Cleanup complete.
Note that even empty tables in DB may appear to occupy some
space, this is expected.

To prevent potential unpredictable behavior, we STRONGLY recommend
rebooting the ADM now.

Do you want to REBOOT the ADM?
[y/n]: 
```

6. 「y」と入力し、**Enter** キーを押して Citrix ADM を再起動します。

システムのクリーンアップ後は、必ず Citrix ADM を再起動してください。NetScaler ADM が再起動した後、内部データベース操作が完了するまで約 30 分間待ちます。これで、Citrix ADM データベースに接続できるようになります。そうでない場合は、回復スクリプトを再度実行して空き領域を増やします。Citrix ADM が起動して実行されると、期待どおりに動作するはずです。

注:

システムカタログテーブルの現在のサイズは、クリーンアップ後ゼロに等しくなることはありません。これは、テーブルから空の行だけが削除され、クリーンアップされた後でもテーブルに有効なエントリがある可能性があるためです。

### Citrix ADM 高可用性展開で Citrix ADM データベースリカバリスクリプトを使用する方法

高可用性環境の Citrix ADM サーバーのデータベースシステムは、連続同期モードになっています。新しいデータベース回復ツールを使用している間は、両方の Citrix ADM サーバーで手順を複製する必要はありません。

1. SSH クライアントまたはハイパーバイザーのコンソールを使用して、プライマリノードにログオンします。
2. 次のコマンドを実行します:

```
/mps/mas_recovery/mas_recovery.py
```

3. NetScaler ADM スタンドアロン展開回復スクリプトで利用可能な手順 2 の手順に従います。

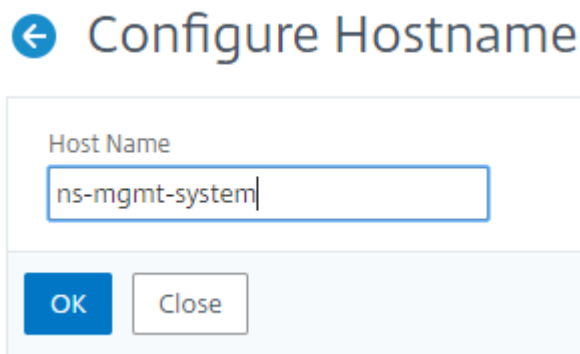
## NetScaler ADM サーバーへのホスト名の割り当て

February 6, 2024

NetScaler Application Delivery Management (ADM) サーバーを識別するために、サーバーにホスト名を割り当てることができます。ホスト名は、NetScaler ADM のユニバーサルライセンスに表示されます。

**NetScaler ADM** サーバーにホスト名を割り当てるには:

1. NetScaler ADM で、[システム] > [システム管理] に移動します。
2. [System Settings] の [Change Hostname] をクリックします。
3. [ホスト名の構成] ページで、ホスト名を入力し、[OK] をクリックします。



## NetScaler ADM サーバーのバックアップと復元

February 6, 2024

Citrix ADM サーバーの定期的なバックアップを作成できます。設定ファイル、インスタンスの詳細、システムデータなどをバックアップおよび復元できます。

### 重要

: 同じバージョンのバックアップを使用して ADM サーバーを復元することをお勧めします。たとえば、ADM バージョンが 13.0 の場合は、13.0 ADM バックアップを使用してサーバーを復元します。

ADM サーバーをバックアップおよび復元するためのユーザーアクセスは制限されています。[システム] > [バックアップファイル] ページは、すべての ADM 機能にアクセスできるユーザーのみ表示されます。ユーザーは、アクセスポリシーにすべての権限がある場合にのみ、このページにアクセスできます。通常、スーパーユーザーはすべての ADM 機能にアクセスできます。



← Create Access Policies

Policy Name\*  
 ⓘ

Policy Description  
 ⓘ

Permissions

- All
  - Tasks
  - Overview
  - Applications
  - Security
  - Gateway
  - Infrastructure
  - Settings

、「[アクセスポリシーの構成](#)」を参照してください。

アップグレードする前に、予防的な理由により ADM サーバの構成ファイルをバックアップしてください。

バックアップには次のコンポーネントが含まれます。

- Citrix ADM 設定ファイル:
  - SNMP
  - Syslog サーバ構成ファイル
  - NTP ファイル
  - SSL 証明書
  - Control Center ファイル
- Citrix ADM サーバが管理する Citrix ADC インスタンスのバックアップ。
- 構成監査テンプレート
- データベースに格納されているシステムデータ:
  - 作成されたテナントとユーザーの一覧
  - 外部認証サーバの構成 (LDAP、RADIUS など)

- 作成された構成ジョブとジョブテンプレート
- データベースに格納されているインフラストラクチャとアプリケーションのデータ：
  - 追加および管理された Citrix ADC インスタンスからのデータ。
  - インスタンスプロファイルの詳細、バージョンの詳細、インスタンスグループの詳細など
  - 管理者が作成した静的アプリケーション（仮想サーバーのグループ）
- SNMP の設定

注:

Analytics データ、イベント、ADM ライセンス、および syslog メッセージは、バックアップから除外されません。

## NetScaler ADM 構成のバックアップ

デフォルトでは、Citrix ADM サーバーは 24 時間ごと（00 時 30 分）に構成をバックアップします。バックアップの時間をスケジュールして選択することもできます。さらに、バックアップしたファイルのコピーを別のシステムに移動できます。

バックアップは暗号化もできる圧縮 TAR ファイルとして格納されます。デフォルトでは、3 つのバックアップファイルがサーバーに保持されます。ディスク容量不足の問題を回避するには、NetScaler ADM サーバー上に最大 10 個のバックアップファイルを保存できます。ただし、予防策として、バックアップファイルのコピーをサーバーに保存するか、別のシステムに転送することをお勧めします。

**NetScaler ADM 構成をバックアップするには:**

1. [システム] > [バックアップファイル] に移動し、[バックアップ] をクリックします。
2. バックアップファイルを暗号化するには、[ファイルをパスワードで保護する] チェックボックスをオンにし、ファイルを暗号化するためのパスワードを指定します。

New Backup File

Select password protect option to encrypt the backup file. This ensures that all the sensitive information inside backup file is secure.

Password Protect file

Password\*

Confirm Password\*

Continue Cancel

## NetScaler ADM バックアップファイルを外部システムに転送する

通常の予防措置として、バックアップファイルのコピーを他のシステムに転送することができます。構成を復元する場合は、まずファイルを NetScaler ADM サーバーにアップロードしてから、復元操作を実行します。

**Citrix ADM** バックアップファイルを転送するには：

1. [システム] > [バックアップファイル] に移動します。
2. 別のシステムに移動するバックアップファイルを選択し、[転送] をクリックします。
3. 「バックアップファイル」 ページで、次のパラメータを指定します。
  - **Server** -バックアップファイルを転送するシステムの IP アドレス。
  - ユーザー名とパスワード -バックアップファイルをコピーする新しいシステムのユーザー認証情報。
  - **Port** - ファイルの転送先システムのポート番号。
  - **Transfer Protocol** - バックアップファイルの転送に使用するプロトコル。バックアップファイルの転送には SCP、SFTP、FTP のいずれかのプロトコルを選択できます。
  - ディレクトリパス：バックアップファイルが新しいシステム上で転送される場所。
4. 転送後に NetScaler ADM からバックアップファイルを削除するには、[転送後に アプリケーション配信管理 からファイルを削除 する] チェックボックスをオンにします。
5. 「OK」 をクリックして転送を行います。

← Backup Files

Backup File  
Backup\_... .tgz

Server\*  
backup server

Username\*  
admin

Password\*  
.....

Port\*  
22

Transfer Protocol  
 SCP  SFTP  FTP

Directory Path\*  
/example/filebackup

Delete file from Console after transfer

OK Close

注

バックアップファイルのコピーをローカルシステムに保存するには、[システム] > [バックアップファイル] に移動し、コピーするファイルを選択して [ダウンロード] をクリックします。

### バックアップファイルから **NetScaler ADM** 構成を復元する

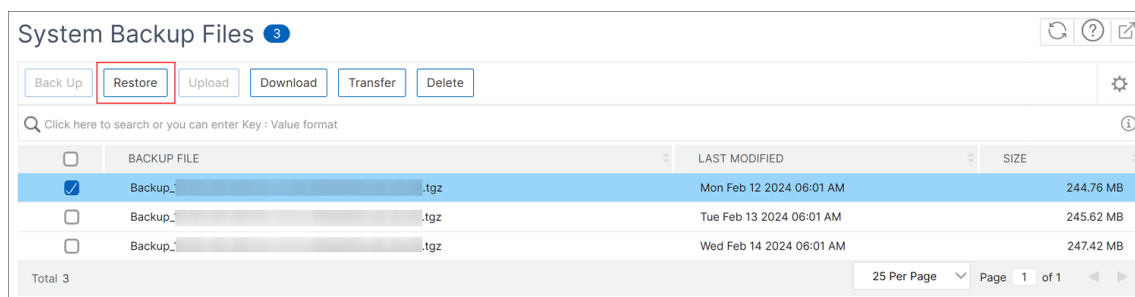
以前にバックアップしたファイルから Citrix ADM 構成を復元すると、復元操作によってバックアップファイルが解凍され、構成が復元されます。復元操作は既存の構成を削除し、バックアップファイルの構成で置き換えます。

注

バックアップファイルの名前が変更されたり、バックアップファイルの内容が変更されたりすると、復元操作は失敗します。

バックアップファイルから **NetScaler ADM** 構成を復元するには:

1. [システム] > [バックアップファイル] に移動します。
2. 復元するバックアッププロファイルを選択して、[Restore] をクリックします。



3. 確認ダイアログボックスで、[Yes] をクリックします。

注

外部システムに格納されているバックアップファイルから設定を復元するには、復元操作を実行する前に、バックアップファイルを ADM サーバにアップロードします。ファイルをアップロードするには、[システム] > [バックアップファイル] に移動し、[アップロード] をクリックします。

### 監査情報の表示

January 29, 2024

Syslog は、ログ記録用の標準プロトコルです。これには、Citrix Application Delivery Controller (ADC) インスタンスで実行される Syslog 監査モジュールと、Citrix ADC インスタンスの基盤となる FreeBSD オペレーティング

グシステム (OS) またはリモートシステムのいずれかで実行できる Syslog サーバーの 2 つのコンポーネントがあります。Syslog は、データ転送に UDP (User Datagram Protocol: ユーザーデータグラムプロトコル) を使用します。

Syslog によって、情報を生成するシステムと、情報を保存するシステムを分離できます。ログ情報を統合して、集められたデータから詳細な情報を得られます。Syslog を構成して、さまざまな種類のイベントをログ記録することもできます。

Syslog メッセージを Citrix Application Delivery Management (ADM) にリダイレクトするようにデバイスを構成すると、Citrix ADC デバイスが生成する syslog メッセージを監視できます。Citrix ADM の組み込みテンプレート機能を使用して、さまざまな種類の Syslog データを生成する Syslog サーバーを作成するジョブをスケジュールできます。

まず、インスタンスがログ情報を送信する対象の Syslog サーバーを構成します。次に、ログメッセージを記録する日時形式を指定します。

**Citrix ADM** でシスログサーバーを構成するには:

1. [システム] > [監査] に移動します。「構成の概要」で、「**Syslog** サーバー」を選択します。または、[システム] > [監査] > [**Syslog** サーバー] に移動することもできます。
2. 「**Syslog** サーバー」ページで、「追加」をクリックします。
3. [**Create Syslog Server**] ページで、次の値を入力します。
  - **Name** - Syslog サーバーの名前
  - **IP Address** - Syslog サーバーの IP アドレス
  - **Port** - Syslog サーバーのポート
4. ログレベルを選択します (All、None、または Custom)。それに応じて重要度レベルを選択します。
5. [**Create**] をクリックします。

**Citrix ADM** でシスログの日付と時刻の形式を設定するには:

1. [システム] > [監査] に移動します。「構成の概要」で、「**Syslog** サーバー」を選択します。
2. 「**Syslog** サーバー」ページで、Syslog サーバーを選択し、「**Syslog** パラメータ」をクリックします。
3. [**Configure Syslog Parameters**] ページで日時形式を指定します。
4. [**OK**] をクリックします。

**Citrix ADM** でシステムログメッセージを表示するには:

Syslog メッセージを Citrix ADM サーバーにリダイレクトするようにインスタンスを構成している場合は、管理対象 Citrix ADC 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るようになりました。Syslog メッセージは Citrix ADM サーバーのデータベースに一元的に保存され、監査目的で Syslog ビューアで利用できるようになります。こうしたログ情報を統合し、集められたデータからレポートを作成できます。

これらの情報は、モジュール、イベントタイプ、および重要度でフィルタリングできます。Syslog を構成して、さまざまな種類のイベントをログ記録することもできます。

**Syslog** ビューアを表示するには、[システム]>[監査]に移動します。「監査」ページの「監査メッセージ」で、「Syslog メッセージ」を選択します。適切なフィルターを選択して、システムのログメッセージを表示します。

## Syslog Messages

The screenshot shows the Syslog Viewer interface with the following details:

- Header:** Syslog Viewer (4 results), Sort: Newest first, and a refresh icon.
- Search:** A search bar with a 'Go' button.
- Filter By:** A sidebar with expandable sections for Module, Event Type, and Severity, and an 'Apply' button.
- Log Entries:**
  - Entry 1:** Dec 03 2018 11:21:13, Info, 10.102.29.190. Message: GUI: CMD\_EXECUTED: User nsroot - Remote\_ip 10.252.240.142 - Command "login login tenant\_name=Owner,password=\*\*\*\*\*,Secret=\*\*\*\*\*,challenge\_response=\*\*\*\*\*,token=878335e13d869b7,client\_port=-1,cert\_verified=false,sessionid=\*\*\*\*\*,session\_timeout=900,permission=superuser" - Status "Done"
  - Entry 2:** Dec 03 2018 10:49:57, Info, 10.102.29.190. Message: GUI: CMD\_EXECUTED: User nsroot - Remote\_ip 10.252.240.227 - Command "login login tenant\_name=Owner,password=\*\*\*\*\*,Secret=\*\*\*\*\*,challenge\_response=\*\*\*\*\*,token=2f8ac227524a8ed,client\_port=-1,cert\_verified=false,sessionid=\*\*\*\*\*,session\_timeout=900,permission=superuser" - Status "Done"
  - Entry 3:** Dec 03 2018 09:46:04, Info, 10.102.29.190. Message: GUI: CMD\_EXECUTED: User nsroot - Remote\_ip 10.252.240.97 - Command "login login tenant\_name=Owner,password=\*\*\*\*\*,Secret=\*\*\*\*\*,challenge\_response=\*\*\*\*\*,token=b3bc0b4cfad71ff,client\_port=-1,cert\_verified=false,sessionid=\*\*\*\*\*,session\_timeout=900,permission=superuser" - Status "Done"
  - Entry 4:** Nov 21 2018 10:24:26, Info, 10.102.29.190. Message: GUI: CMD\_EXECUTED: User nsroot - Remote\_ip 10.252.241.240 - Command "login login tenant\_name=Owner,password=\*\*\*\*\*,Secret=\*\*\*\*\*,challenge\_response=\*\*\*\*\*,token=4d381cfb98db967,client\_port=-1,cert\_verified=false,sessionid=\*\*\*\*\*,session\_timeout=900,permission=superuser" - Status "Done"

## SSL 設定の構成

February 6, 2024

SSL (Secure Socket layer) と TLS (Transport Layer Security) は、ユーザーとサーバー間の暗号化通信を実現する、広く使用されているセキュリティネットワークプロトコルです。Citrix Application Delivery Management (ADM) で SSL 設定を構成し、システムに接続するクライアントの種類を指定できます。

**Citrix ADM の SSL 設定を構成するには:**

1. **[System] > [System Administrations]** の順に選択します。**[System Settings]** で **[Configure SSL Settings]** を選択します。
2. **SSL 設定** ページで、現在のプロトコル設定とシステムに適用されている暗号スイートを確認します。
3. プロトコル設定を変更するには、**[Edit Settings] > [Protocol Settings]** の順に選択して、必要な変更を行います。
4. 適用されている暗号の組み合わせを変更するには、**[Edit Settings] > [Cipher Suites]** の順に選択して、必要な変更を行います。
5. 「**OK**」をクリックし、「閉じる」をクリックします。

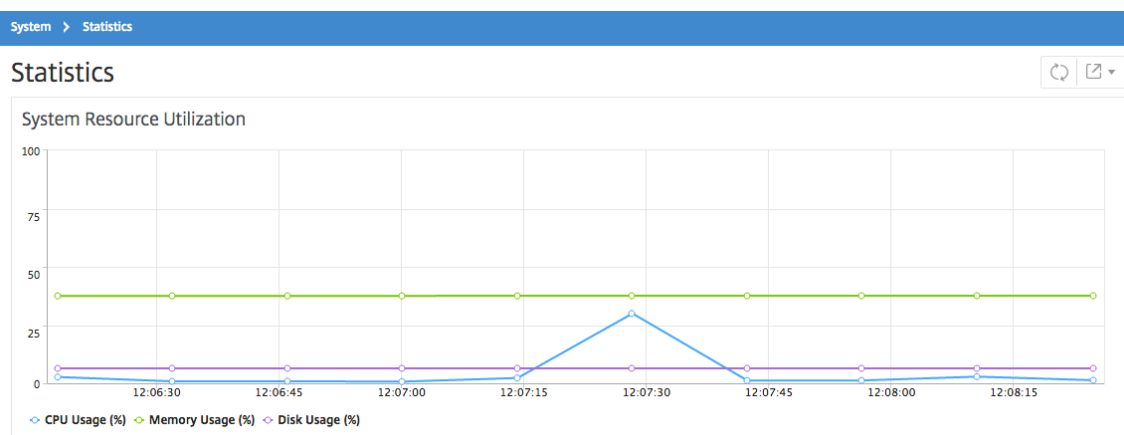
## CPU、メモリ、ディスク使用率の監視

January 29, 2024

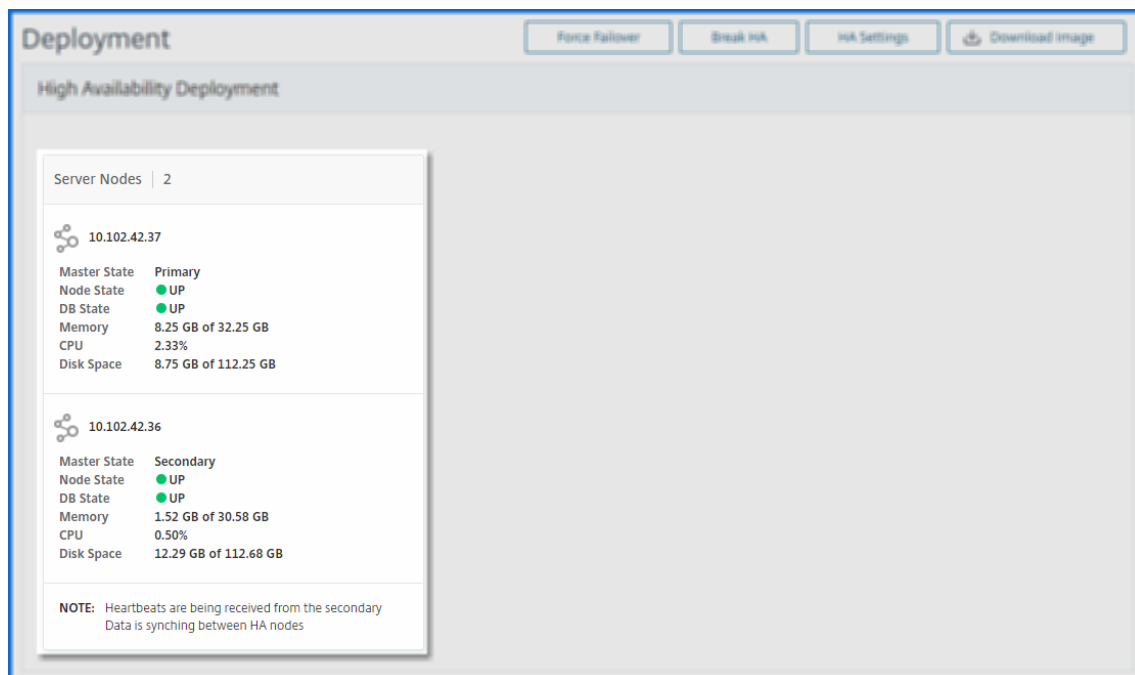
ログと統計に保持されている情報を使用できます。この情報は、Citrix Application Delivery Management (ADM) の構成と保守に役立つレポートにも表示されます。

CPU、メモリ、ディスクの使用状況を監視するには、

- スタンドアロンデプロイメント。[システム]>[統計]に移動します。CPU、メモリ、ディスク使用率のグラフをリアルタイムで表示できます。



- 高可用性導入。[システム]>[展開]に移動します。メモリ、CPU、ディスク領域、および管理対象インスタンスの統計は、次の図のように数値で表示されます：



## 通知設定の構成

January 29, 2024

通知タイプを選択して、次の機能の通知を受け取ることができます:

- イベント—NetScaler ADC インスタンスに対して生成されるイベントのリスト。詳細については、「[イベントルールのアクションを追加する](#)」を参照してください。
- **[Licenses]**: 現在アクティブで、間もなく期限切れになるなどのライセンスのリスト。詳しくは、「[NetScaler ADM ライセンスの有効期限](#)」を参照してください。
- **SSL 証明書**—NetScaler ADC インスタンスに追加される SSL 証明書のリスト。詳しくは、「[SSL 証明書の有効期限](#)」を参照してください。

ADM では、次の通知タイプがサポートされています。

- メール
- SMS
- Slack
- PagerDuty
- ServiceNow

ADM GUI には、通知タイプごとに、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。ADM は、選択した配布リストまたはプロファイルに通知を送信します。

### メール配布リストを作成する

ADM 機能の電子メール通知を受信するには、電子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。

電子メール同報リストを作成するには、次の手順を実行します。

1. **[System] > [Notifications]** の順に選択します。
2. [電子メール] で、[追加] をクリックします。
3. 「電子メール配布リストの作成」で、次の詳細を指定します。
  - [名前]-配布リスト名を指定します。
  - メールサーバー -メール通知を送信するメールサーバーを選択します。メールサーバーを追加する場合は、「追加」をクリックします。
  - 送信者 -ADM がメッセージを送信する電子メールアドレスを指定します。
  - 宛先-ADM がメッセージを送信する電子メールアドレスを指定します。



- **Cc** -ADM がメッセージのコピーを送信する電子メールアドレスを指定します。
- **Bcc** -ADM がメッセージのコピーを送信する電子メールアドレスを指定します。アドレスは表示されません。

### Create Email Distribution List

Name\*

Email Servers\*

From

To\*

Cc

Bcc

4. [作成] をクリックします。

この手順を繰り返して、複数の電子メール配布リストを作成します。「電子メール」タブには、ADM に存在するすべての電子メール配布リストが表示されます。

### SMS 配布リストを作成する

ADM 機能の SMS 通知を受信するには、SMS サーバーと電話番号を追加する必要があります。

SMS 通知設定を構成するには、次の手順を実行します。

1. [System] > [Notifications] の順に選択します。
2. SMS で、[追加] をクリックします。
3. 「SMS 配布リストの作成」で、次の詳細を指定します。
  - [名前]-配布リスト名を指定します。
  - SMS サーバー -SMS 通知を送信する SMS サーバーを選択します。
  - 宛先 -ADM がメッセージを送信する先の電話番号を指定します。
4. [作成] をクリックします。

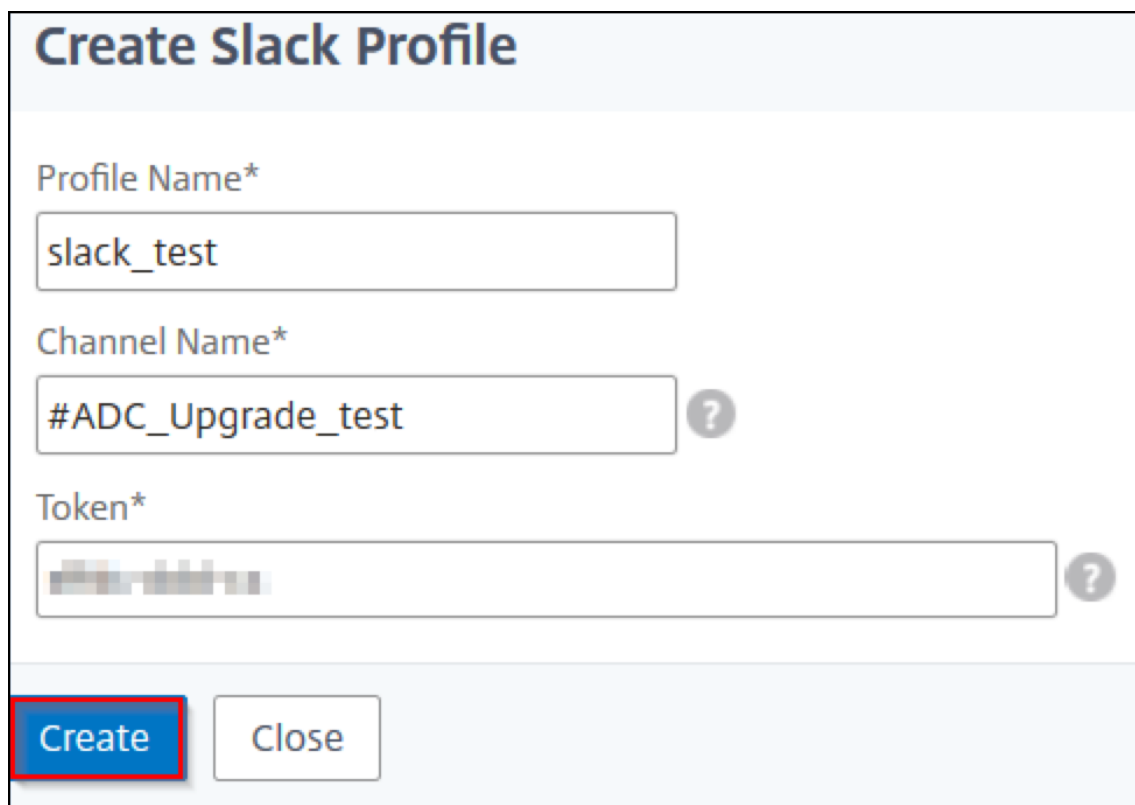
この手順を繰り返して、複数の SMS 配布リストを作成します。SMS タブには、ADM にあるすべての SMS 配布リストが表示されます。

### Slack プロファイルの作成

ADM 機能の Slack 通知を受け取るには、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、次の手順に従います。

1. [System] > [Notifications] の順に選択します。
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、次の詳細を指定します。
  - プロファイル名 -プロフィール名を指定します。この名前は Slack のプロフィールリストに表示されます。
  - チャンネル名 -ADM が通知を送信する Slack チャンネル名を指定します。
  - ウェブフック URL -チャンネルのウェブフック URL を指定します。受信ウェブフックは、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 は内部的にチャンネル名にリンクされています。また、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 チャンネルに投稿されます。ウェブフックの例は次のとおりです。[https://hooks.slack.com/services/T0\\*\\*\\*\\*\\*E/B9X55DUMQ/c4tewWaiGVTT51Fl6oEOVirK](https://hooks.slack.com/services/T0*****E/B9X55DUMQ/c4tewWaiGVTT51Fl6oEOVirK)



**Create Slack Profile**

Profile Name\*  
slack\_test

Channel Name\*  
#ADC\_Upgrade\_test ?

Token\*  
[Blurred Token] ?

Create Close

4. [作成] をクリックします。

この手順を繰り返して、複数の Slack プロファイルを作成します。**Slack** タブには、ADM に存在するすべての Slack プロファイルが表示されます。

### PagerDuty プロファイルを作成する

PagerDuty プロファイルを追加すると、PagerDuty 設定に基づいてインシデント通知を監視できます。PagerDuty では、電子メール、SMS、プッシュ通知、および登録番号への電話による通知を設定できます。

NetScaler ADM で PagerDuty プロファイルを追加する前に、PagerDuty で必要な構成が完了していることを確認します。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. **[System] > [Notifications]** の順に選択します。
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 ポータルから入手できます。

4. [作成] をクリックします。

詳しくは、PagerDuty ドキュメントの「[サービスと統合](#)」を参照してください。

この手順を繰り返して、複数の PagerDuty プロファイルを作成します。**PagerDuty** タブには、ADM に存在するすべての PagerDuty プロファイルが表示されます。

### ServiceNow のプロフィールを表示する

NetScaler ADC イベントおよび ADM 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 ADM を ServiceNow と統合する必要があります。詳しくは、「[NetScaler ADM と ServiceNow インスタンスの統合](#)」を参照してください。

ServiceNow プロファイルを表示して確認するには、次の手順を実行します。

1. **[System] > [Notifications]** の順に選択します。
2. **[ServiceNow]** で、リストから **Citrix\_Workspace\_sn** プロファイルを選択します。
3. 「テスト」をクリックして ServiceNow チケットを自動生成し、構成を確認します。

NetScaler ADM GUI で ServiceNow チケットを表示する場合は、**[ServiceNow チケット]** を選択します。

### テクニカルサポートファイルを生成する

February 6, 2024

Citrix は、問題をデバッグするためにテクニカルサポートに連絡する前に、NetScaler Application Delivery Management (ADM) のデータと統計のアーカイブを生成することをお勧めします。テクニカルサポートチームに送信できるアーカイブは、TAR ファイルです。

#### 注

高可用性モードの Citrix ADM サーバーでは、どちらのサーバーからでもテクニカルサポートファイルを生成できます。Citrix では、テクニカルサポートファイルを生成する場合に負荷分散仮想サーバーの IP アドレスを使用しないことをお勧めしています。

**NetScaler ADM** からテクニカルサポートファイルを構成して送信するには：

1. **[システム] > [診断] > [テクニカルサポート]** に移動し、**[テクニカルサポートファイルの生成]** をクリックします。
2. **[サポートファイルを生成]** ページで、次のオプションを選択します。
  - 「デバッグログの収集」 — **afdecoder** ログを収集するには、このオプションを選択します。

- 「期間」—デバッグログを収集する必要がある期間を入力します。このオプションは、[デバッグログの収集] オプションを有効にした場合にのみ表示されます。
- **Collect Data Distribution** - このオプションは、データベースからさまざまなログを収集する場合に選択します。

```

1 The archive file is created as a TAR file.
2
3 For example, the archive file that is created might be named as
  follows: Citrix_ADM_<ADM_IP_address>_<DDMMYY>_<time_stamp>.
  tar.gz
  
```

1. テクニカルサポートファイルは、次の 2 つの方法でサポートチームに送信できます。
  - a) ADM GUI からローカルストレージにファイルをダウンロードし、Web ブラウザを使用して CIS にアップロードできます。
  - b) ADM コンソールでスクリプトを実行して、テクニカルサポートファイルを Citrix Insight Services (CIS) Web サイトにアップロードすることもできます。
    - i. SSH を使用して、ADM コンソールにログオンします。
    - ii. シェルプロンプトに切り替えて、次のように入力します。

```
/mps/collector_upload.pl
```

コマンド全体を、指定する必要がある属性とともに以下に示します。

```

1 /mps/collector_upload.pl [-proxy [<proxy_user>:<proxy_password>@]<
  proxy_host>:<proxy_port>] [-user <user>] [-password <password>] [-sr
  <sr>] [-description <description>] [-debug] <file>
2 <!--NeedCopy-->
  
```

Perl スクリプトを実行する利点は、テクニカルサポートファイルを ADM からローカルシステムにダウンロードして CIS にアップロードする必要がないことです。オプションとして、ADM コンソールからプロキシを使用してファイルを CIS に直接アップロードできます。

CIS のアカウントを持っていることを確認してください。Citrix アカウントの認証情報を使用して CIS にファイルをアップロードできます。

プロキシサーバーがない場合はどうなりますか？ それとも、SSL フォワードプロキシで何らかの問題に直面している場合はどうでしょうか？ (これは、Perl スクリプトがプロキシサーバーのルート証明書を信頼していない場合に発生する可能性があります)

。ADM シェルから CIS にファイルを直接アップロードすることは引き続き可能です。

注:

ADM がコンソールから CIS にファイルをアップロードできない場合でも、ファイルをダウンロードして Citrix

テクニカルサポートチームに電子メールで送信できます。または、ADM からローカルストレージにファイルをダウンロードし、Web ブラウザを使用して CIS にアップロードすることもできます。

## 暗号グループの構成

January 29, 2024

暗号グループは、Citrix Application Delivery Controller (ADC) インスタンス上の SSL 仮想サーバー、サービス、またはサービスグループにバインドする暗号スイートのセットです。暗号スイートは、プロトコル、鍵交換 (Kx) アルゴリズム、認証 (Au) アルゴリズム、暗号化 (Enc) アルゴリズム、およびメッセージ認証コード (Mac) アルゴリズムで構成されています。

**NetScaler ADM** で暗号グループを追加するには:

1. [システム] > [管理] に移動します。
2. [SSL 設定] で [暗号グループ] をクリックします。
3. [追加] をクリックします
4. [Create Cipher Group] ページで、次の情報を入力します。
  - **Group Name** - 暗号化グループの名前。
  - **Cipher Group Description** - 暗号化グループの説明を入力します。
  - **Cipher Suites** - [Add] をクリックして [Available] 一覧から暗号の組み合わせを選択した後、選択した (またはすべての) 暗号の組み合わせを [Configured] 一覧に移動します。
5. [作成] をクリックします。

← Create Cipher Group

Group Name\*  
Cipher Group Test

Cipher Group Description\*  
Cipher Group Test

Cipher Suites\*

Available (55)	Select All	Configured (2)	Remove All
TLS1-AES-256-CBC-SHA	+	TLS1.2-AES-128-SHA256	-
TLS1-AES-128-CBC-SHA	+	TLS1.2-AES-256-SHA256	-
TLS1.2-AES256-GCM-SHA384	+		
TLS1.2-AES128-GCM-SHA256	+		
TLS1-ECDHE-RSA-AES256-SHA	+		
TLS1-ECDHE-RSA-AES128-SHA	+		
TLS1.2-ECDHE-RSA-AES-256-SHA384	+		
TLS1.2-ECDHE-RSA-AES-128-SHA256	+		
TLS1.2-ECDHE-RSA-AES256-GCM-SHA3...	+		
TLS1.2-ECDHE-RSA-AES128-GCM-SHA2...	+		
TLS1.2-DHE-RSA-AES-256-SHA256	+		

Create Close

## SNMP トラップの宛先、マネージャコミュニティ、およびユーザーの作成

February 6, 2024

Citrix ADM で異常な状態が発生するたびに、SNMP トラップが生成されます。次に、トラップは、トラップ宛先サーバーまたは SNMP トラップ宛先と呼ばれるリモートデバイスに送信されます。ここでは、Citrix ADM がトラップの送信先として構成されています。SNMP マネージャと呼ばれるリモートデバイスから、システム固有の情報について SNMP エージェントに問い合わせることができます。エージェントは、要求されたデータを MIB (Management Information Base: 管理情報ベース) で検索して、データを SNMP マネージャーに送信します。

**Citrix ADM** で **SNMP** トラップの送信先を作成するには:

1. **[System]** > **[SNMP]** > **[Trap Destinations]** の順に選択します。
2. 「**SNMP** トラップ」で、「追加」をクリックして SNMP トラップを作成し、次の詳細を指定します。
  - バージョン。使用する SNMP バージョンを選択します。
  - 送信先サーバー。トラップ宛先の名前または IP アドレス。
  - ポート。トラップ先のポートを入力します。デフォルトでは、ポートは 162 に設定されています。
  - コミュニティ。トラップリスナーにトラップを送信するときに使用するコミュニティストリングを指定します。
3. [作成] をクリックします。

### 注

SNMP v3 トラップの宛先を作成する場合は、トラップをバインドする SNMP ユーザー認証情報を指定します。SNMP ユーザー認証情報を追加するには、「挿入」をクリックし、利用可能な SNMP ユーザーのリストからユーザーを追加します。

**SNMP** マネージャーコミュニティを作成するには:

1. **[System]** > **[SNMP]** > **[Managers]** の順に選択します。
2. 「**SNMP** マネージャー」で、「追加」をクリックして SNMP マネージャーコミュニティを作成し、次の詳細を指定します。
  - **SNMP** マネージャ。SNMP マネージャーの名前または IP アドレスを入力します。
  - コミュニティ。トラップリスナーにトラップを送信するときに使用するコミュニティストリングを指定します。
3. オプションで、「管理ネットワークを有効にする」チェックボックスを選択して、**SNMP** マネージャーネットワークのサブネットマスクであるネットマスクを指定できます。
4. [作成] をクリックします。

**SNMP** ユーザーを作成するには、次の手順を実行します。

1. **[System]** > **[SNMP]** > **[Users]** の順に選択します。
2. 「**SNMP** ユーザー」で、「追加」をクリックします。
3. ユーザー名を入力し、メニューからユーザーにセキュリティレベルを割り当てます。
4. ユーザーに割り当てたセキュリティレベルに基づいて、認証プロトコル、プライバシーパスワードなどの追加の認証プロトコルを指定し、SNMP ビューの割り当てを行います。

## システムアラームの設定と表示

February 6, 2024

一連のアラームを有効にして構成して、NetScaler Application Delivery Management (ADM) サーバーの正常性を監視できます。システムアラームを設定して、システムの重大な問題または重大な問題を認識する必要があります。たとえば、CPU 使用率が高い場合や、サーバーへのログインに複数回失敗した場合に、管理者に通知が送信されるようにします。cpuUsageHigh や memoryUsageHigh などの一部のアラームカテゴリでは、しきい値を設定してそれぞれの重要度 (Critical や Major など) を定義できます。inventoryFailed や loginFailure などのカテゴリについては、重要度のみを定義できます。アラームカテゴリ (MemoryUsageHigh など) のしきい値を超えた場合、またはアラームカテゴリに対応するイベント (**LoginFailure** など) が発生すると、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、アラーム設定に対応した電子メールや SMS を受信する通知を設定することもできます。

アラームの重要度を割り当て、または変更することができます。割り当てることができる重要度レベルは、「緊急」、「メジャー」、「マイナー」、「警告」、および「情報」です。

バックアップに失敗した場合に、常に監視するシナリオを考えてみましょう。BackupFailed アラームを有効にして、メジャーなどの重大度を割り当てることができます。NetScaler ADM がシステムファイルのバックアップを試行し、失敗するとアラームがトリガーされます。Citrix ADM でメッセージを表示したり、電子メールや 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。このアラームはデフォルトで有効化されています。

**NetScaler ADM** を使用してシステムアラームを構成および表示するには:

1. **[System]** > **[SNMP]** の順に選択します。右上隅の [アラーム] をクリックします。



Name	Status	Severity	Threshold	Time (minutes)
backupFailed	Enabled	Major	-NA-	-NA-
cpuUsageHigh	Enabled	--	80	0
cpuUsageNormal	Enabled	--	-NA-	-NA-
dataStorageExceeded	Enabled	--	-NA-	-NA-
dataStorageNormal	Enabled	--	-NA-	-NA-
devicebackupFailed	Enabled	--	-NA-	-NA-
diskUtilizationHigh	Enabled	--	80	0
diskUtilizationNormal	Enabled	--	-NA-	-NA-
haDatabaseOutOfSync	Enabled	--	-NA-	-NA-

2. 設定するアラーム（BackupFailed など）を選択し、[ **Edit** ] をクリックして設定を変更します。
3. このアラームはデフォルトで有効化されています。重要度レベル（例: メジャー）を割り当て、「**OK**」をクリックします。

**注**

一部のアラームでは、しきい値を設定できません。

このアラームが発生すれば、生成されたイベントが syslog メッセージとして表示されます。

**Citrix ADM** を使用してバックアップ失敗アラームによって生成されたイベントを表示するには:

1. [システム] > [監査] に移動します。
2. 「監査」ページの「監査メッセージ」で、「Syslog メッセージ」を選択します。
3. 検索フィールドに、アラームの名前を入力します。

この例では、失敗したバックアップ試行に対してイベントが生成されていることがわかります。

Log Messages (2 results)	Sort: Newest first	Filter By
Jul 17 2018 23:04:37 10.102.29.55 GUI: CMD_EXECUTED: User nsroot - Remote_ip 10.252.241.91 - Command "modify snmp_alarm_config enable=true,name=backupfailed,severity=Major" - Status "Done"		Module Event Type Severity Apply
Jul 17 2018 23:05:56 10.102.29.55 GUI: CMD_EXECUTED: User nsroot - Remote_ip 10.252.241.91 - Command "modify snmp_alarm_config enable=true,name=backupfailed,severity=Major" - Status "Done"		

アラームが発生したときに、電子メールか SMS（Short Message Service）テキストのいずれかを送る通知を設定することもできます。システム通知の構成方法については、「[NetScaler ADM のシステム通知設定を構成する方法](#)」を参照してください。

## API プロキシサーバーとしての NetScaler ADM

February 6, 2024

Application Delivery Management (Citrix ADM) は、独自の管理および分析機能に対する NITRO REST API リクエストを受信できるだけでなく、マネージドインスタンスの REST API プロキシサーバーとしても機能します。

REST API クライアントは、API リクエストを管理対象インスタンスに直接送信する代わりに、API リクエストを Citrix ADM に送信できます。Citrix ADM は、応答する必要がある API リクエストと、変更されずにマネージドインスタンスに転送する必要がある API リクエストを区別できます。

API プロキシサーバーとして、Citrix ADM には次の利点があります。

- **API 要求の検証:** Citrix ADM は、すべての API リクエストを、構成済みのセキュリティおよびロールベースのアクセス制御 (RBAC) ポリシーと照合して検証します。Citrix ADM はテナント対応でもあり、API アクティビティがテナントの境界を越えないようにします。
- **集中監査:** Citrix ADM は、管理対象インスタンスに関連するすべての API アクティビティの監査ログを保持します。
- **セッション管理:** NetScaler ADM は、API クライアントを管理対象インスタンスとのセッションを維持するタスクから解放します。

### Citrix ADM が API プロキシサーバーとして機能する仕組み

NetScaler ADM で管理対象インスタンスにリクエストを転送する場合は、API リクエストに次の HTTP ヘッダーのいずれかを含めるように API クライアントを構成します。

ヘッダー値	説明
<code>_MPS_API_PROXY_MANAGED_INSTANCE_NAME</code>	管理対象インスタンスの名前。
<code>_MPS_API_PROXY_MANAGED_INSTANCE_IP</code>	管理対象インスタンスの IP アドレス。
<code>_MPS_API_PROXY_MANAGED_INSTANCE_ID</code>	管理対象インスタンスの ID。
<code>MPS_API_PROXY_TIMEOUT</code>	NITRO API 要求のタイムアウト値。タイムアウト値を秒単位で設定します。プロキシタイムアウトを設定すると、ADM は要求がタイムアウトするまで指定された期間待機します。
<code>_MPS_API_PROXY_MANAGED_INSTANCE_USERNAME</code>	管理対象 ADC インスタンスにアクセスするためのユーザー名。
<code>MPS_API_PROXY_MANAGED_INSTANCE_PASSWORD</code>	管理対象の ADC インスタンスにアクセスするためのパスワード。
<code>MPS_API_PROXY_MANAGED_INSTANCE_SESSID</code>	管理対象インスタンスにアクセスするためのセッション ID。

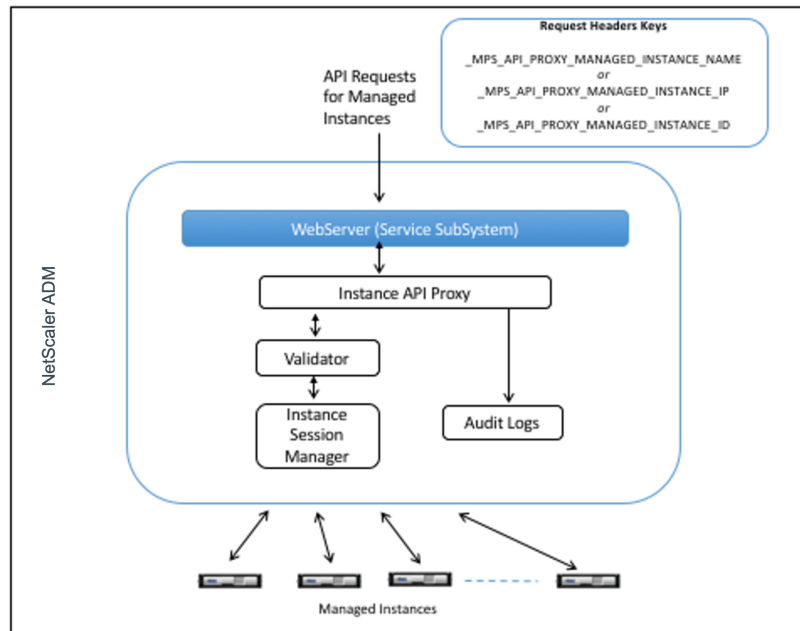
注:

[システム] > [管理] > [システム構成] > [基本設定] で、[インスタンスログインの認証情報を確認する] を選

択した場合は、マネージドインスタンスのユーザー名とパスワードを設定してください。または、インスタンスセッション ID を指定することもできます。

これらの HTTP ヘッダーが存在すると、NetScaler ADM は API リクエストを管理対象インスタンスに転送する必要がある API リクエストとして識別するのに役立ちます。ヘッダーの値は、Citrix ADM がリクエストを転送する必要がある管理対象インスタンスを識別するのに役立ちます。

次の図はこのフローを示しています。



上記の図に示すように、これらの HTTP ヘッダーの 1 つが要求に表示されると、NetScaler ADM は要求を次のように処理します。

1. Citrix ADM は、リクエストを変更せずに、リクエストをインスタンス API プロキシエンジンに転送します。
2. インスタンス API プロキシエンジンは API 要求を検証ツールに転送し、API 要求の詳細を監査ログに記録します。
3. 検証ツールは、要求が構成されているセキュリティポリシー、RBAC ポリシー、テナント境界などに違反がないことを確認します。管理対象インスタンスが利用可能かどうかを判断するチェックなど、追加のチェックを実行します。

API リクエストが有効で、管理対象インスタンスに転送できる場合、NetScaler ADM はインスタンス Session Manager によって維持されるセッションを識別し、そのリクエストを管理対象インスタンスに送信します。

注:

[インスタンスログインの認証情報をプロンプト] オプションが無効になっていることを確認します。必要な操作:

1. [システム] > [管理] に移動します。
2. [システム構成] で、[システム]、[タイムゾーン]、[許可された URL]、[今日のメッセージ] の順に選択します。

## NetScaler ADM を API プロキシサーバーとして使用する方法

次の例は、API クライアントが IP アドレス 192.0.2.5 の Citrix ADM サーバーに送信する REST API リクエストを示しています。Citrix ADM は、リクエストを変更せずに IP アドレス 192.0.2.10 の管理対象インスタンスに転送する必要があります。すべての例で `_MPS_API_PROXY_MANAGED_INSTANCE_IP` ヘッダーを使用します。

Citrix ADM に API リクエストを送信する前に、API クライアントは次のことを行う必要があります。

- Citrix ADM にログインする
- セッション ID を取得
- 後続の API リクエストにはセッション ID を含めてください。

ログオン API 要求の形式は次のとおりです。

```
1  POST /nitro/v1/config/login
2  Content-Type: application/json
3
4  {
5
6      "login": {
7
8          "username": "nsroot",
9          "password": "nsroot"
10     }
11 }
12
13
14 <!--NeedCopy-->
```

Citrix ADM は、セッション ID を含む応答でログオン要求に応答します。次のサンプル応答本文は、セッション ID を示しています。

```
1  {
2
3
4      "errorCode": 0,
5
6      "message": "Done",
7
8      "operation": "add",
9
10     "resourceType": "login",
11
12     "username": "*****",
13 }
```

```
14  "tenant_name": "Owner",
15
16  "resourceName": "nsroot",
17
18  "login": [
19
20    {
21
22      "tenant_name": "Owner",
23
24      "permission": "superuser",
25
26      "session_timeout": "36000",
27
28      "challenge_token": "",
29
30      "username": "",
31
32      "login_type": "",
33
34      "challenge": "",
35
36      "client_ip": "",
37
38      "client_port": "-1",
39
40      "cert_verified": "false",
41
42      "sessionid": "##
43      D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",
44
45      "token": "b2f3f935e93db6a"
46    }
47
48  ]
49
50 }
51
52
53 <!--NeedCopy-->
```

**例 1:** 負荷分散仮想サーバーの統計情報の取得

クライアントは、NetScaler ADM に次の形式の API 要求を送信する必要があります。

```
1  GET /nitro/v1/stat/lbvserver
2  Content-type: application/json
3  _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4  SESSID: ##
5  D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
6  <!--NeedCopy-->
```

クッキーヘッダーの値は、ログイン API 呼び出しから返されたセッション ID です。そして、\_MPS\_API\_PROXY\_MANAGED\_INSTANCE\_IP の値は、ADC の IP アドレスです。

### 例 2: 負荷分散仮想サーバーの作成

クライアントは、NetScaler ADM に次の形式の API 要求を送信する必要があります。

```
1   POST /nitro/v1/config/lbserver/sample_lbserver
2   Content-type: application/json
3   Accept-type: application/json
4   _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5   SESSID: ##
      D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
6
7   {
8
9       "lbserver":{
10
11           "name":"sample_lbserver",
12           "servicetype":"HTTP",
13           "ipv46":"10.102.1.11",
14           "port":"80"
15       }
16   }
17
18
19 <!--NeedCopy-->
```

### 例 3: 負荷分散仮想サーバーの変更

クライアントは、NetScaler ADM に次の形式の API 要求を送信する必要があります。

```
1   PUT /nitro/v1/config/lbserver
2   Content-type: application/json
3   Accept-type: application/json
4   _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5   SESSID: ##
      D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
6
7   {
8
9       "lbserver":{
10
11           "name":"sample_lbserver",
12           "appflowlog":"DISABLED"
13       }
14   }
15
```

```
16
17 <!--NeedCopy-->
```

**例 4:** 負荷分散仮想サーバーを削除する

クライアントは、NetScaler ADM に次の形式の API 要求を送信する必要があります。

```
1 DELETE /nitro/v1/config/lbvserver/sample_lbvserver
2 Accept-type: application/json
3 _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4 SESSID: ##
   D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5
6 <!--NeedCopy-->
```

**例 5: ADC** での設定実行中の **CLI** のダウンロード

クライアントは、NetScaler ADM に次の形式の API 要求を送信する必要があります。

```
1 GET /nitro/v1/config/nsrunningconfig
2 Accept-type: application/json
3 _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4 SESSID: ##
   D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5
6 <!--NeedCopy-->
```

## インフラストラクチャ分析を使用して問題を視覚化

February 6, 2024

ネットワーク管理者の主な目標は、NetScaler ADC インスタンスを監視することです。ADC インスタンスは、それを介してアクセスされるアプリケーションとデスクトップの使用状況とパフォーマンスに関する興味深い洞察を提供します。管理者は、ADC インスタンスを監視し、各 ADC インスタンスによって処理されるアプリケーションフローを分析する必要があります。アプリケーションの使用状況やパフォーマンスに影響を与える可能性のある構成、セットアップ、接続、証明書など、考えられる問題を修復できます。たとえば、アプリケーショントラフィックパターンの急激な変化は、SSL プロトコルの無効化などの SSL 設定の変更が原因である可能性があります。管理者は、次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は最適な状態にあります
- リソース消費、ハードウェア、容量、構成変更の問題はありません

- 未使用のインベントリはありません
- 期限切れの証明書はありません

Infrastructure Analytics 機能では、複数のデータソースを相互に関連付け、インスタンスの状態を定義する測定可能なスコアに定量化することで、データ分析のプロセスを簡略化します。この機能により、管理者は 1 つのタッチポイントで、問題があるかどうか、問題の原因および実行可能な改善策を把握できます。

### インフラストラクチャ分析

Citrix Application Delivery Management (ADM) インフラストラクチャ分析機能は、Citrix ADC インスタンスから収集されたすべてのデータを照合し、それをインスタンスの状態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。Infrastructure Analytics 機能は、インスタンスで問題が発生した、または発生する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判断するのにも役立ちます。

### インスタンススコア

インスタンススコアは、ADC インスタンスの状態を示します。スコアが 100 の場合、インスタンスは問題なく正常に動作していることを意味します。インスタンススコアは、インスタンス上のさまざまなレベルの潜在的な問題を把握します。これはインスタンスの状態を定量化できる測定値であり、複数の「ヘルスインジケータ」がスコアに影響します。

ヘルスインジケータはインスタンススコアの構成要素であり、スコアは、その時間枠で検出されたすべてのインジケータに基づいて、事前に定義された「モニタリング期間」にわたっ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では、インスタンスから収集されたデータに基づいて、1 時間に 1 回インスタンススコアを計算しています。

インジケータは、インスタンス上の次のカテゴリのいずれかに属する任意のアクティビティ (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
- クリティカルイベントインジケータ
- SSL 設定インジケータ
- 構成偏差インジケータ

### 健康指標

- システムリソースインジケータ

以下は、NetScaler ADC インスタンスで発生し、NetScaler ADM によって監視される可能性のある重大なシステムリソースの問題です。



- **CPU** 使用率が高い。CPU 使用率が、NetScaler ADC インスタンスの上限しきい値を超えました。
- メモリ使用量が高い。メモリ使用量が NetScaler ADC インスタンスの上限しきい値を超えました。
- ディスク使用率が高い。ディスク使用量が NetScaler ADC インスタンスの上限しきい値を超えました。
- ディスクエラー。ADC インスタンスがインストールされているハイパーバイザーのハードディスク 0 またはハードディスク 1 にエラーがあります。
- 電源障害。電源が故障したか、ADC インスタンスから切断されました。
- **SSL** カードに障害が発生しました。インスタンスにインストールされている SSL カードに障害が発生しました。
- フラッシュエラー。NetScaler ADC インスタンスでコンパクトフラッシュエラーが表示される。
- **NIC** は破棄します。NIC カードによって破棄されたパケットが、NetScaler ADC インスタンスのより高い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。

- クリティカルイベントインジケータ

ADM のイベント管理機能で「クリティカル」に設定されているイベントによって、次のクリティカルイベントが識別されます。

- **HA** 同期失敗。高可用性の ADC インスタンス間の構成同期がセカンダリサーバーで失敗しました。
- ハートビートはありません。高可用性のペアの ADC インスタンスのプライマリサーバーは、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** セカンダリステートが不良です高可用性の ADC インスタンスのペアのセカンダリサーバーが Down、Unknown、または Stay セカンダリの状態にあります。
- **HA** バージョンの不一致。高可用性のペアの ADC インスタンスにインストールされている ADC ソフトウェアイメージのバージョンが一致しません。
- クラスタ同期失敗。クラスタモードの ADC インスタンス間の設定の同期が失敗しました。
- クラスタのバージョンが一致しません。クラスタモードで ADC インスタンスにインストールされている ADC ソフトウェアイメージのバージョンが一致しません。
- クラスタの伝播に失敗。クラスタ内のすべてのインスタンスへの構成の伝達が失敗しました。

注:

重要な SNMP イベントのリストを表示するには、イベントの重大度を変更します。重要度レベルの変更方法の詳細については、「[NetScaler ADC インスタンスで発生するイベントの報告された重要度を変更する](#)」を参照してください。

Citrix ADM のイベントについて詳しくは、「[イベント](#)」を参照してください。

- SSL 設定インジケータ
  - キーの強度は推奨されません。SSL 証明書の主な強度は Citrix の標準とは異なります
  - 推奨発行者ではありません。SSL 証明書の発行者は Citrix では推奨されていません。
  - **SSL** 証明書の有効期限が切れました。ADC インスタンスにインストールされている SSL 証明書の有効期限が切れています。
  - **SSL** 証明書の有効期限が切れず。ADC インスタンスにインストールされている SSL 証明書は、今後 1 週間で期限切れになりそうです。
  - 推奨されないアルゴリズム。ADC インスタンスにインストールされる SSL 証明書の署名アルゴリズムは、Citrix 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。

- 構成偏差インジケータ
  - 設定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設定で作成した監査テンプレートから、設定がずれ（保存されていない変更）している。
  - 設定ドリフトデフォルト。デフォルト設定ファイルからの設定にドリフト（保存されていない変更）があります。

構成の逸脱の詳細と、監査レポートを実行して構成の逸脱を確認する方法については、「[監査レポートを表示する](#)」を参照してください。

## ADC の容量に関する問題の表示

ADC インスタンスが使用可能な容量の大半を消費した場合、クライアントトラフィックの処理中にパケット廃棄が発生することがあります。この問題は、ADC インスタンスのパフォーマンスが低下します。このような ADC の容量問題を理解することで、ADC の性能を安定させるために積極的にライセンスを割り当てることができます。

ADC の容量に関する問題を確認するには、

1. [ネットワーク] > [インフラストラクチャ分析] に移動します。
2. 容量の問題を表示するインスタンスを展開します。

ADM は、ADC インスタンスから 5 分ごとにこれらのイベントをポーリングし、パケットドロップまたはレート制限カウンタが存在する場合は、その増加を表示します。問題は次の容量パラメータに分類されます。

- スループット制限に達しました—スループット制限に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** の上限に達した—PE CPU の制限に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** の上限に達しました—PPS の上限に達した後にインスタンスでドロップされたパケットの数。
- **SSL** スループットレート制限—SSL スループット制限に達した回数。
- **SSL TPS** レート制限—SSL TPS 制限に達した回数。

ADM は、定義された容量しきい値に基づいてインスタンススコアを計算します。

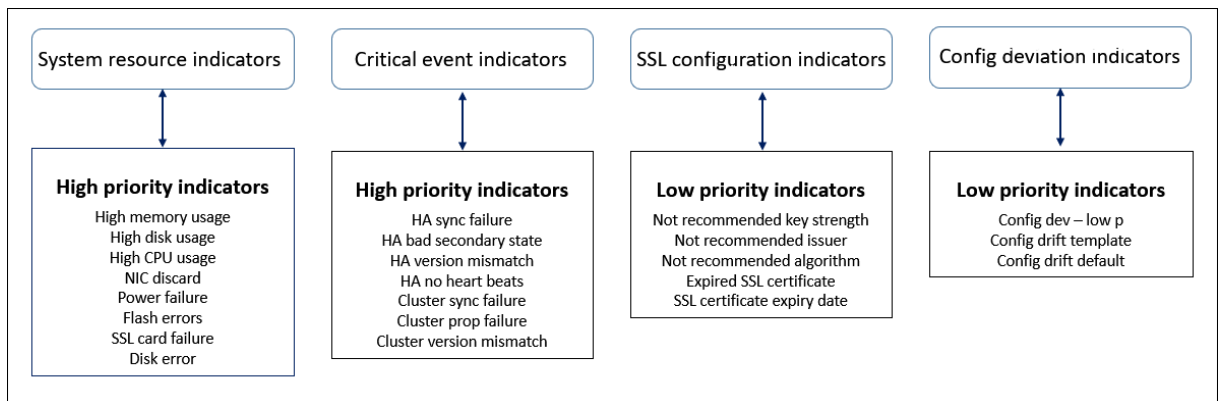
- 低いしきい値: 1 パケットドロップまたはレート制限カウンタ増分
- 高いしきい値: 10000 パケットのドロップまたはレート制限カウンタ増分

そのため、ADC インスタンスが容量しきい値を超えると、インスタンスのスコアが影響を受けます。

パケットがドロップまたはレート制限カウンタが増加すると、**ADCCapacityBreach** カテゴリの下にイベントが生成されます。これらのイベントを表示するには、[アカウント]>[システムイベント]に移動します。

### 健康指標の価値

指標は、その値に基づいて高優先度指標と低優先度指標に分類される。



同じ指標グループ内の健全性指標には、それぞれ異なる重みが割り当てられています。ある指標が他の指標よりもインスタンススコアの低下に寄与している場合があります。たとえば、メモリ使用率が高いと、ディスク使用率が高く、CPU 使用率が高く、NIC の破棄率よりもインスタンスのスコアが下がります。インスタンスで検出されたインジケータの数が多ければ、インスタンスのスコアは低くなります。

指標の価値は、以下のルールに基づいて計算されます。このインジケータは、次の 3 つの方法のいずれかで検出されると言われています。

1. アクティビティに基づく。たとえば、インスタンスで停電が発生するたびにシステムリソースインジケータがトリガーされ、このインジケータはインスタンススコアの値を減らします。インジケータがクリアされると、ペナルティがクリアされ、インスタンスのスコアが上がります。
2. 閾値違反に基づく。たとえば、NIC カードがパケットを破棄し、しきい値レベルを超えると、システムリソースインジケータがトリガーされます。
3. 低い閾値と高い閾値の違反に基づく。ここでは、インジケータは次の 2 つの方法でトリガーできます。
  - 指標の値が低い閾値と高い閾値の間にある場合、インスタンススコアに部分的なペナルティが課されます。
  - 値が高いしきい値を超えると、インスタンススコアに全額のペナルティが課されます。

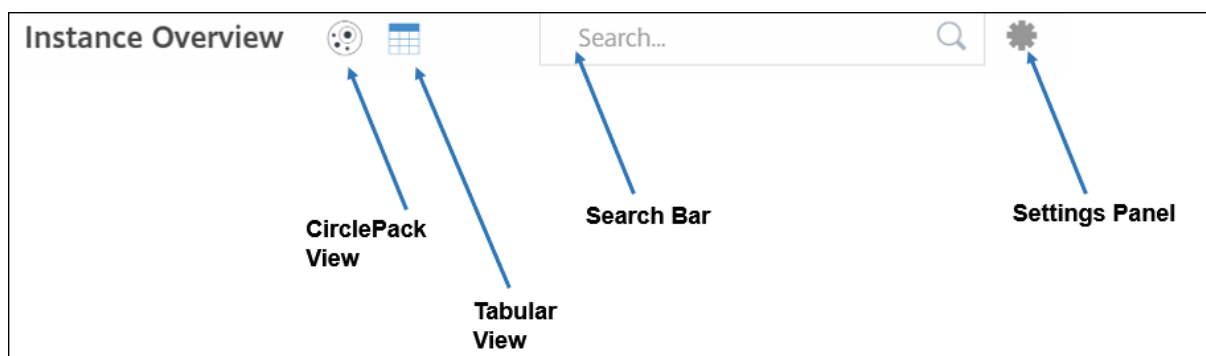
- 値が低いしきい値を下回っても、インスタンススコアにペナルティは課されません。

たとえば、CPU 使用率は、使用量が下限しきい値を超えたとき、および値が上限しきい値を超えたときにトリガーされるシステムリソースインジケータです。

### インフラストラクチャ分析ダッシュボード

[ネットワーク]>[インフラストラクチャ分析]に移動します。

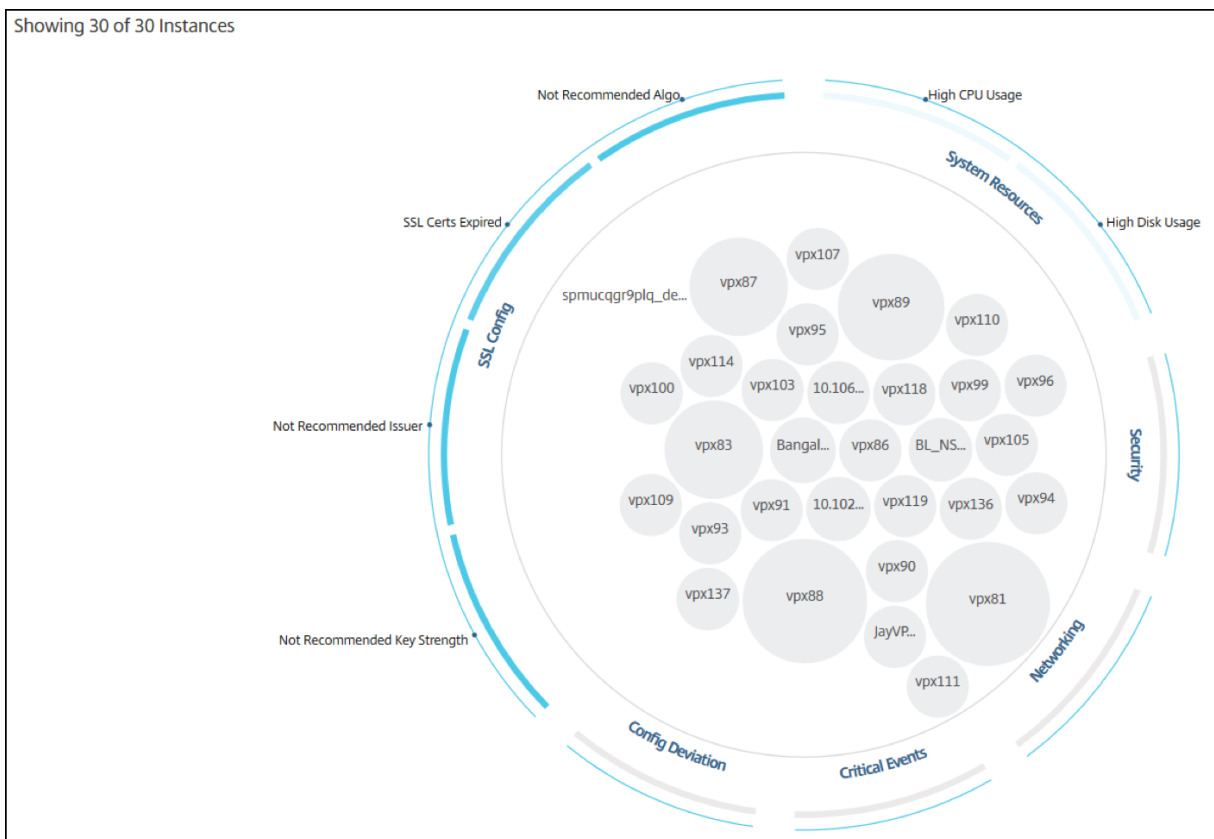
インフラストラクチャ分析は、サークルパック形式または表形式で表示できます。2つの形式を切り替えることができます。



- [Tabular] 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、Summary Panel 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せん。

### サークル・パックの表示

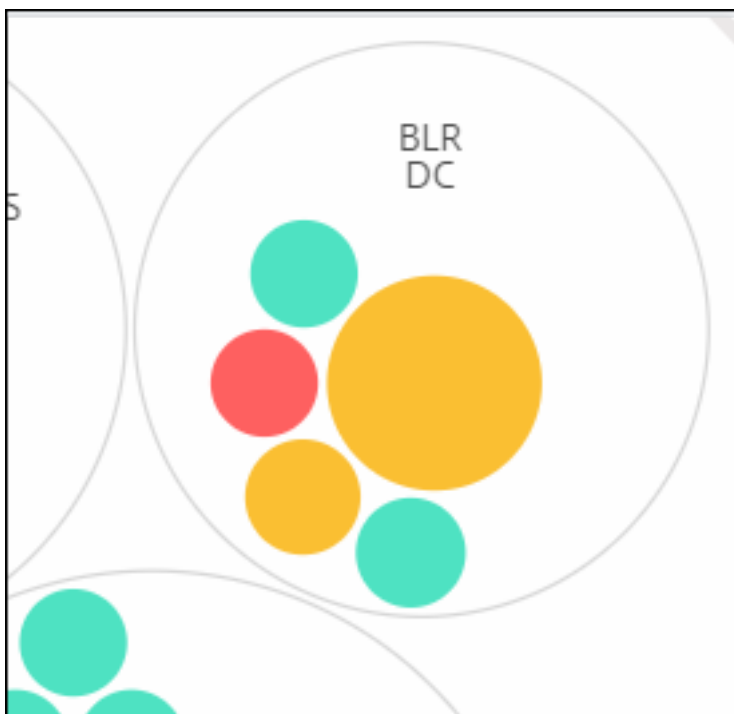
円のパッキング図は、インスタンスグループを密に構成された円として示しています。多くの場合、小さなインスタンスグループが同じカテゴリの他のグループと同様に色付けされているか、大きなグループ内にネストされている階層が表示されます。サークルパックは階層データセットを表し、階層内の異なるレベルと、それらが相互にどのように相互作用するかを示します。



インスタンス円

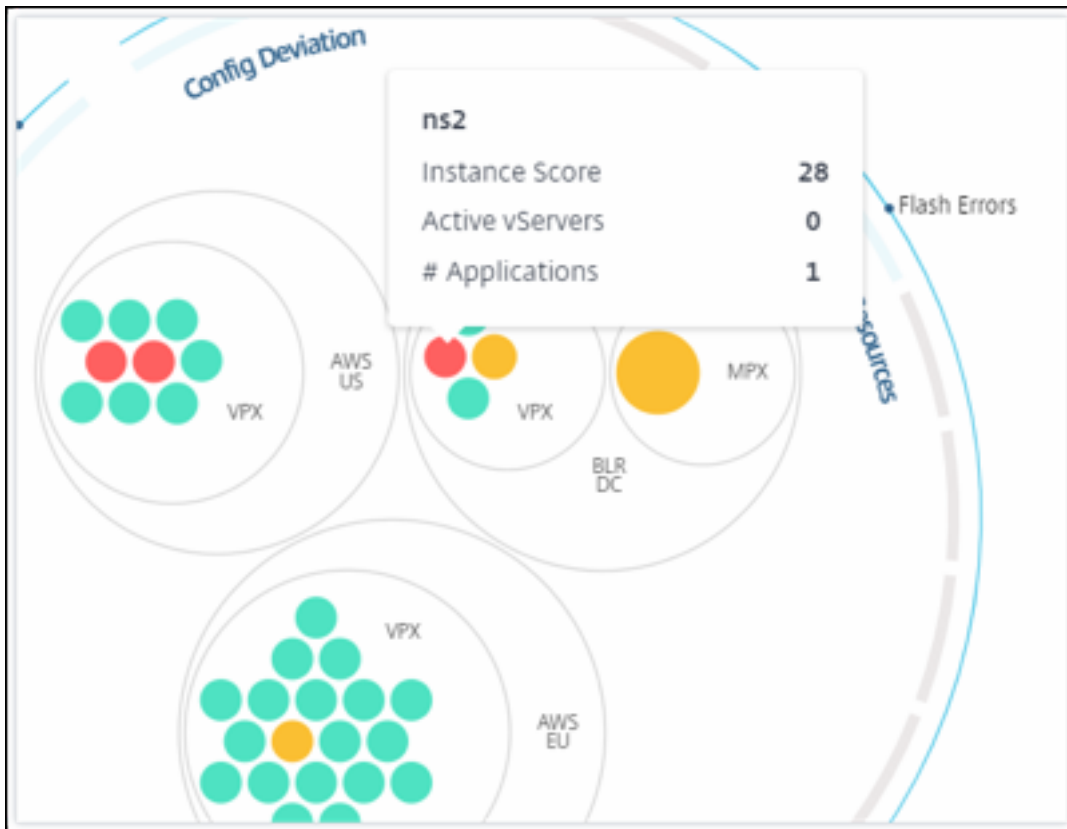
色。Circle Pack では、各インスタンスは色付きの円で表されます。円の色はそのインスタンスの状態を示します。

- 緑 -インスタンスのスコアは 100 から 80 の間です。インスタンスは正常です。
- 黄色 -インスタンスのスコアは 80 ~50 です。いくつかの問題が確認されており、確認が必要です。
- 赤 -インスタンスのスコアが 50 を下回っています。インスタンスは複数の問題に気づいているため、インスタンスは重要な段階にあります。



**【サイズ】**。これらの色付きの円のサイズは、そのインスタンスに構成されている仮想サーバーの数を示します。円が大きいほど、仮想サーバーの数が多いことを示します。

各インスタンスの円 (色付きの円) にマウスポインタを置くと、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、そのインスタンスに構成されているアプリケーションの数が表示されます。

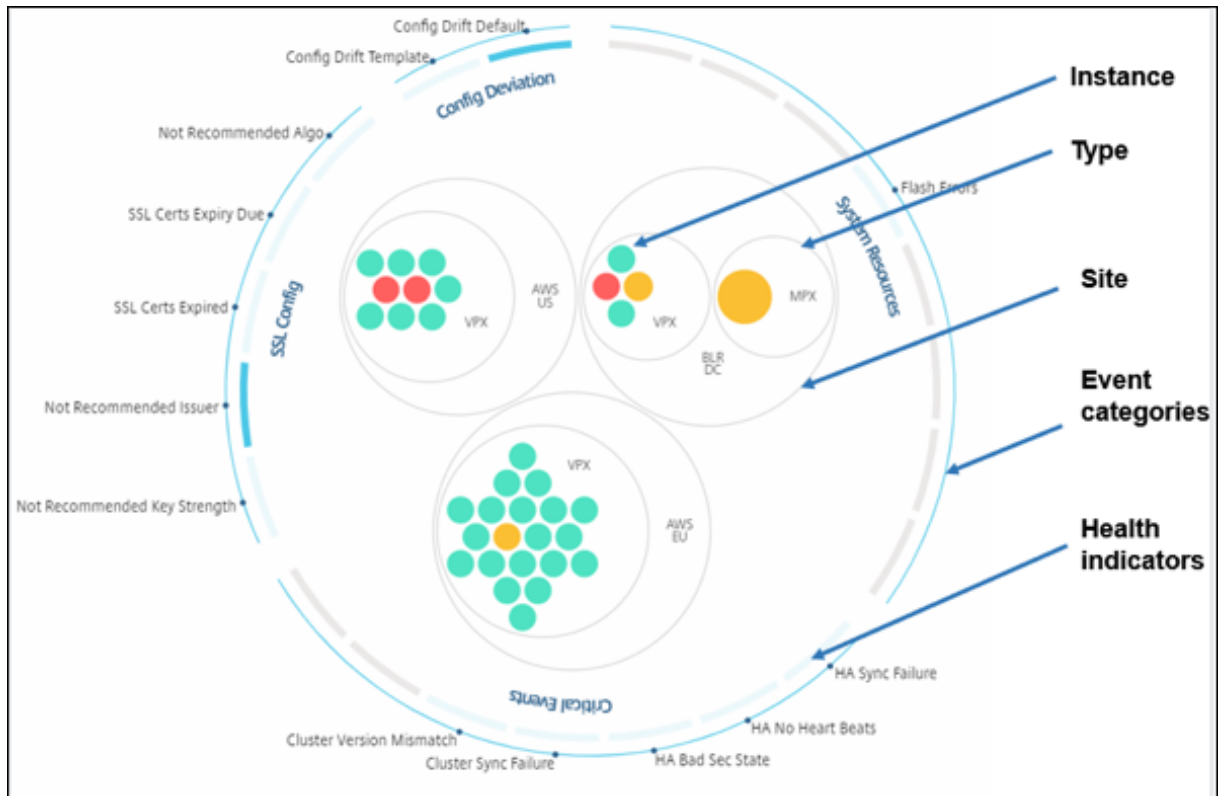


#### グループ化されたインスタンス円

最初の Circle Pack は、次の基準に基づいて別のサークルの中にグループ化、ネスト、またはパックされたインスタンスサークルで構成されます。

- それらがデプロイされているサイト
- デプロイされたインスタンスのタイプ (VPX、MPX、SDX、CPX)
- ADC インスタンスの仮想モデルまたは物理モデル
- インスタンスにインストールされている ADC イメージバージョン

次の図は、Circle Pack を示しています。この Circle Pack では、インスタンスがデプロイされるサイトまたはデータセンター別にグループ化され、次にそのタイプ (VPX、MPX) に基づいてさらにグループ化されます。



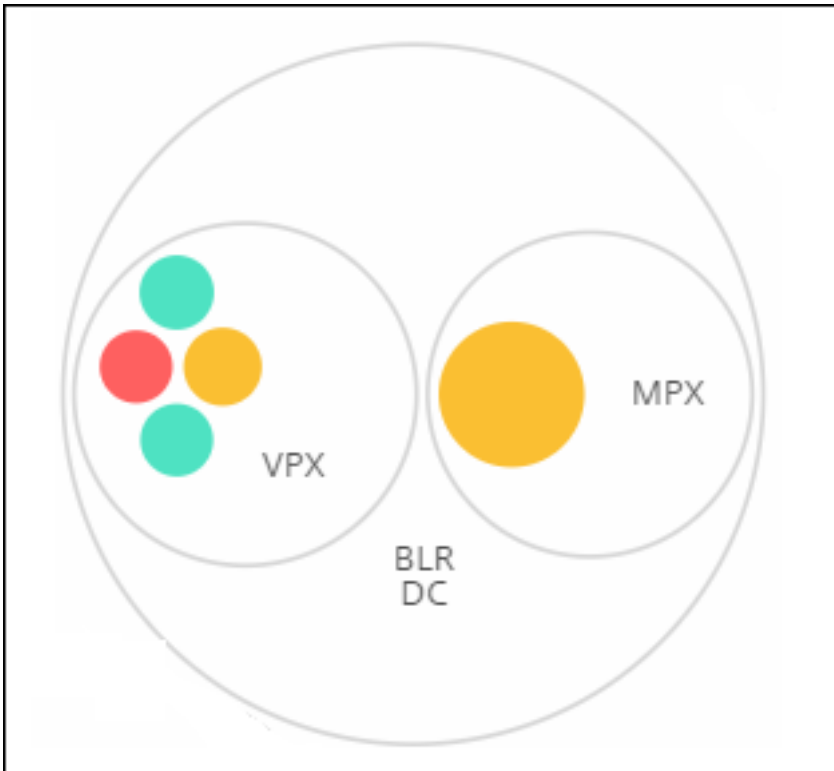
これらのネストされた円はすべて、最も外側の 2 つの円で囲まれています。外側の 2 つの円は、NetScaler ADM によって監視されるイベントの 4 つのカテゴリ（システムリソース、重要なイベント、SSL 構成、および構成の逸脱）とそれに寄与する正常性指標を表しています。

#### クラスター化されたインスタンス円

NetScaler ADM は多くのインスタンスを監視します。これらのインスタンスのモニタリングとメンテナンスを容易にするために、Infrastructure Analytics ではインスタンスを 2 つのレベルでクラスター化できます。つまり、インスタンスグループを別のグループにネストできます。

たとえば、BLR データセンターには VPX と MPX の 2 種類の ADC インスタンスが導入されています。最初に ADC インスタンスをタイプ別にグループ化し、次にグループ化されたサイトごとにすべてのインスタンスをグループ化できます。管理しているサイトにデプロイされているインスタンスの種類を簡単に特定できるようになりました。

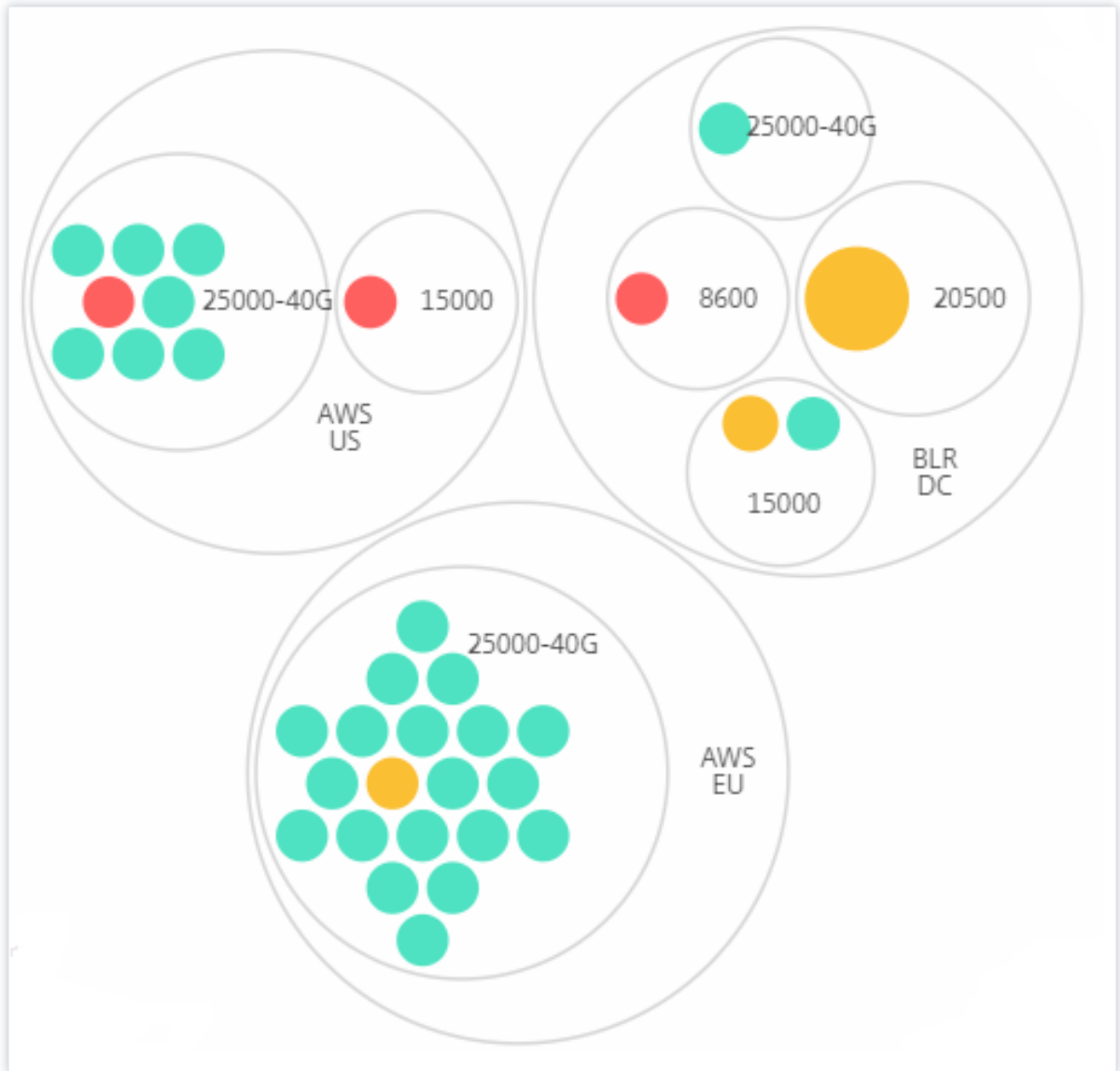




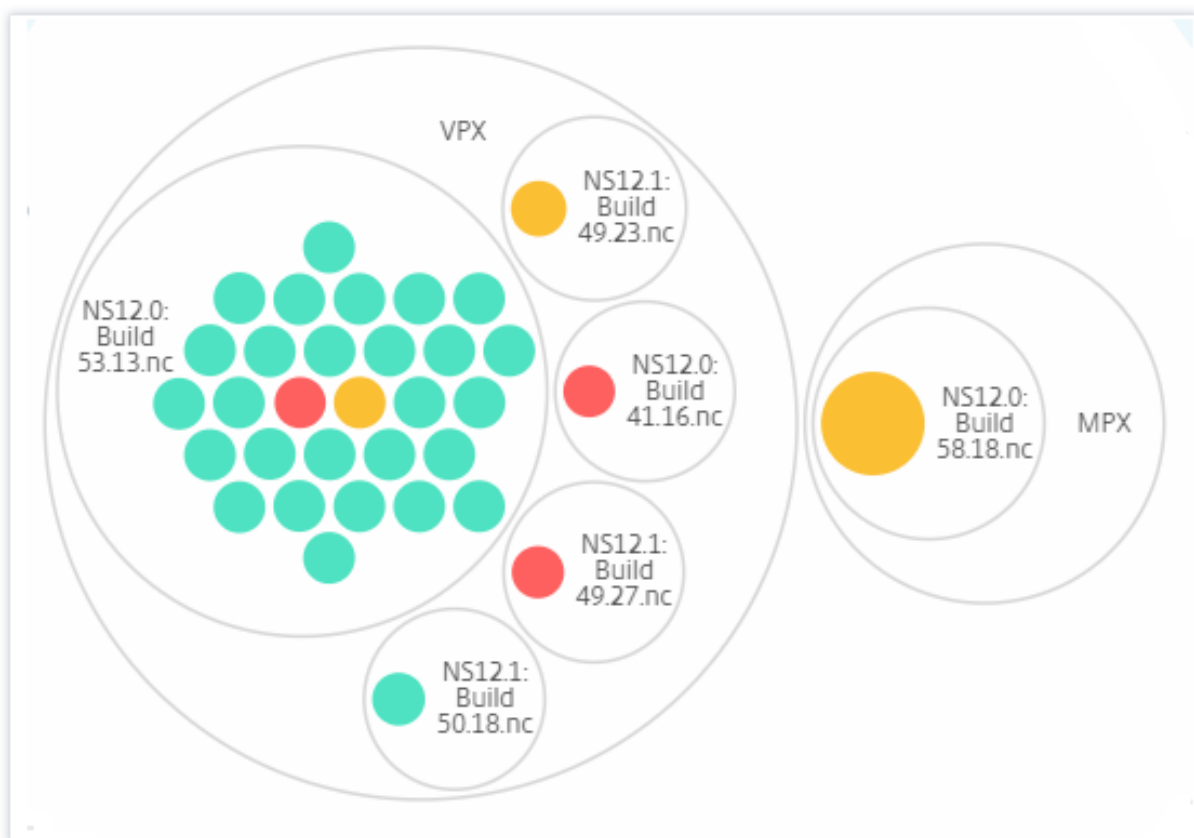
The screenshot shows the 'Infrastructure > Infrastructure Analytics' interface. The main area displays a circle pack visualization of 14 instances. The visualization includes labels for various metrics: 'Not Recommended Algorithm', 'SSL Certs Expiry Due', 'SSL Certs Expired', 'Not Recommended issuer', 'Not Recommended Key Strength', 'Config Drift', 'Config Deviation', and 'Critical Events'. The circle pack shows a hierarchy with a 'VPX' node containing several smaller nodes (e.g., 'Azu...', 'OnP...', '4500', '2000') and an 'MPX' node. A configuration panel on the right is open, showing settings for 'CIRCLE PACK - INSTANCE SIZE' (set to '# Virtual Servers') and 'CIRCLE PACK - CLUSTER BY' (Level 1: 'Type', Level 2: 'Model').

2 レベルクラスタリングのさらにいくつかの例を次に示します。

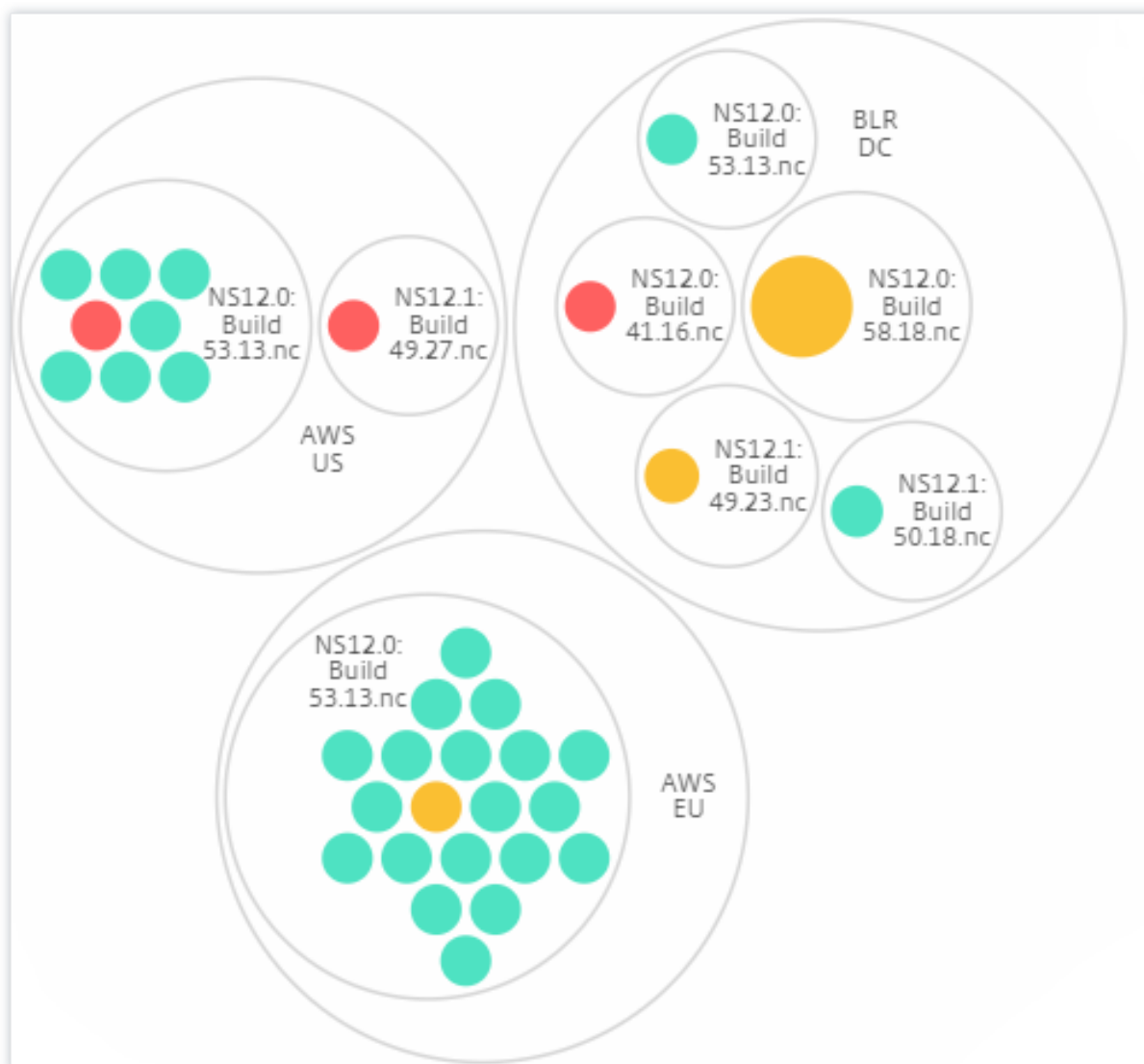
サイトとモデル:



タイプとバージョン:



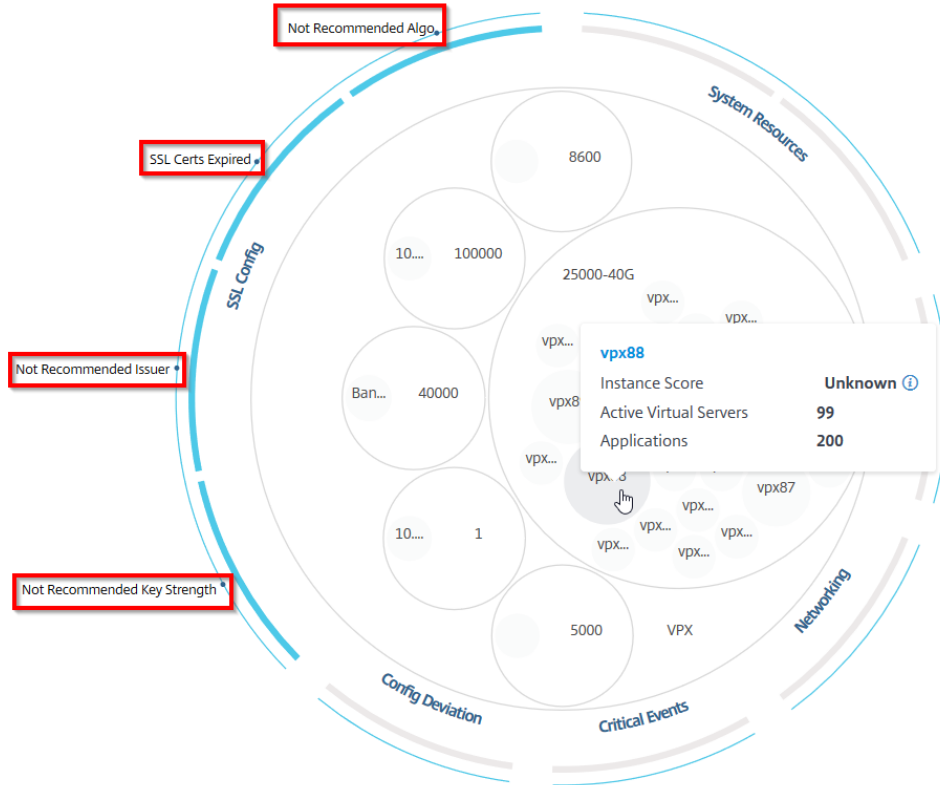
サイトとバージョン:



### サークルパックの使用方法

色付きの円をそれぞれクリックして、そのインスタンスをハイライト表示します。

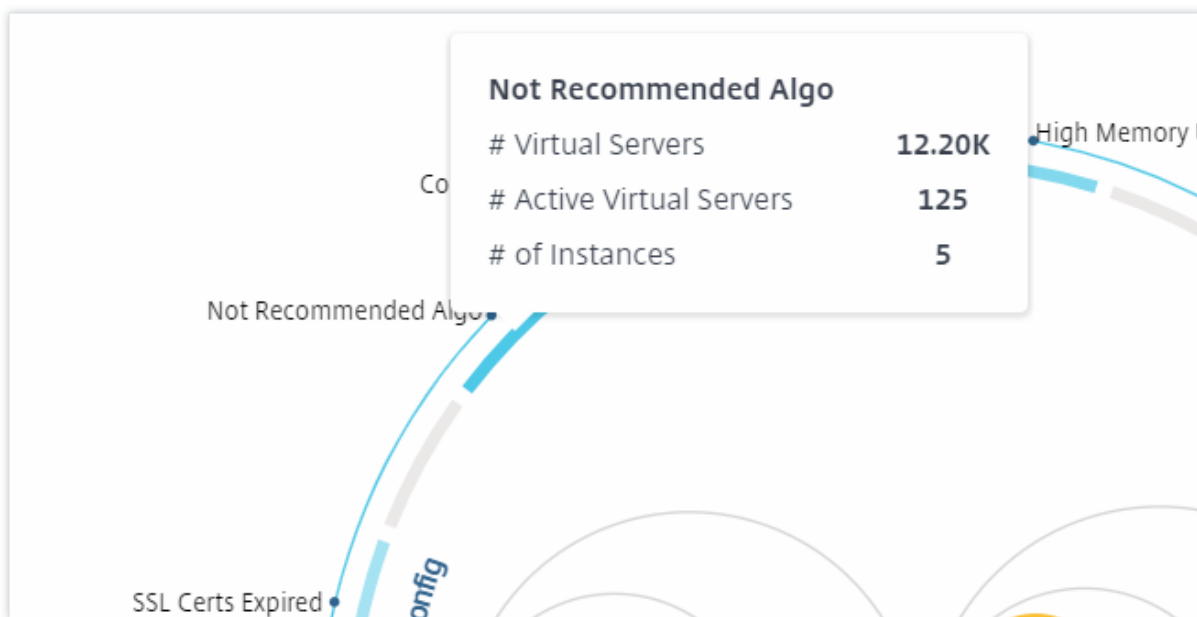
Showing 30 of 30 Instances



そのインスタンスで発生したイベントに応じて、それらの健全性インジケータだけが外側の円で強調表示されます。たとえば、次の2つのサークルパックの画像は、両方のインスタンスがクリティカル状態にあるにもかかわらず、異なるリスク指標のセットを示しています。



また、健全性インジケータをクリックして、そのリスクインジケータを報告したインスタンスの数に関する詳細を表示することもできます。たとえば、**Not recommended Algo**をクリックすると、そのリスクインジケータのサマリレポートが表示されます。



### 表形式ビュー

表形式ビューには、インスタンスとインスタンスの詳細が表形式で表示されます。表示される詳細は次のとおりです。

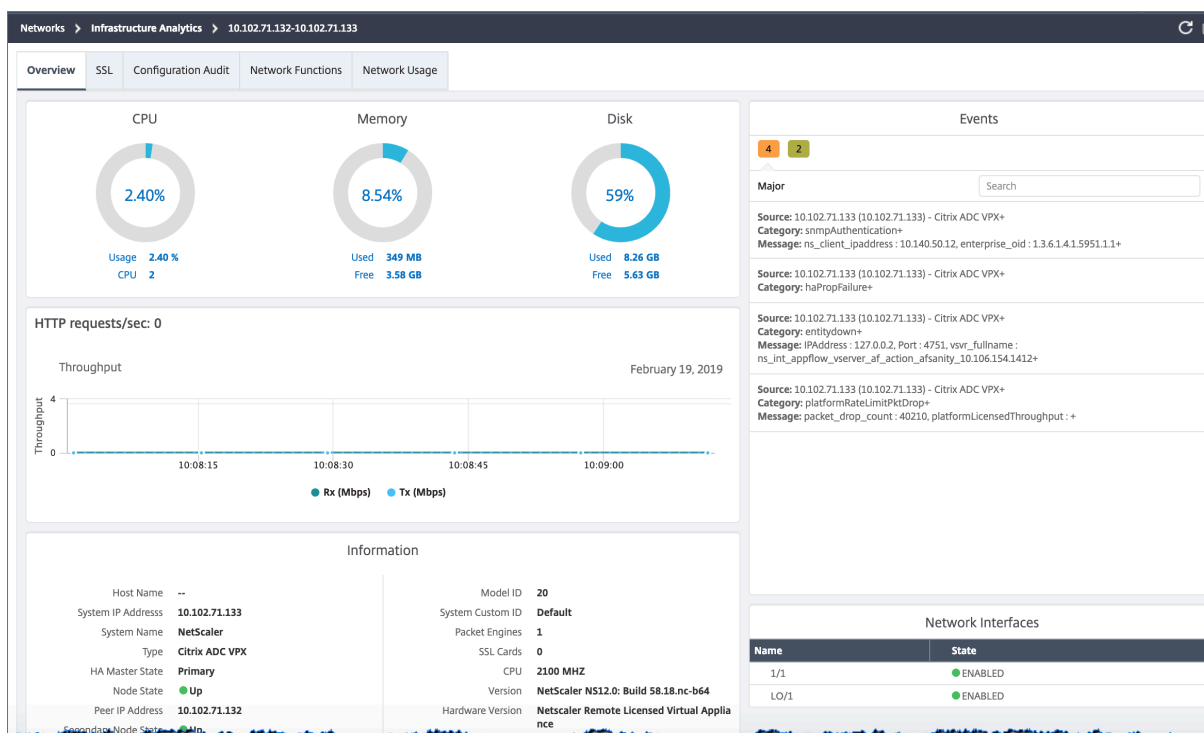
- インスタンスのホスト名
- インスタンスの IP アドレス
- インスタンスの状態
- インスタンススコア
- そのインスタンスに設定されている仮想サーバーの数
- そのインスタンスに設定されているアプリケーションの数
- リスク指標の総数
- インスタンススコアの低下に大きく寄与しているイベント

重要な状態のインスタンスが表の一番上にあり、その後にレビューが必要なインスタンス、そしてより正常なインスタンスが続きます。

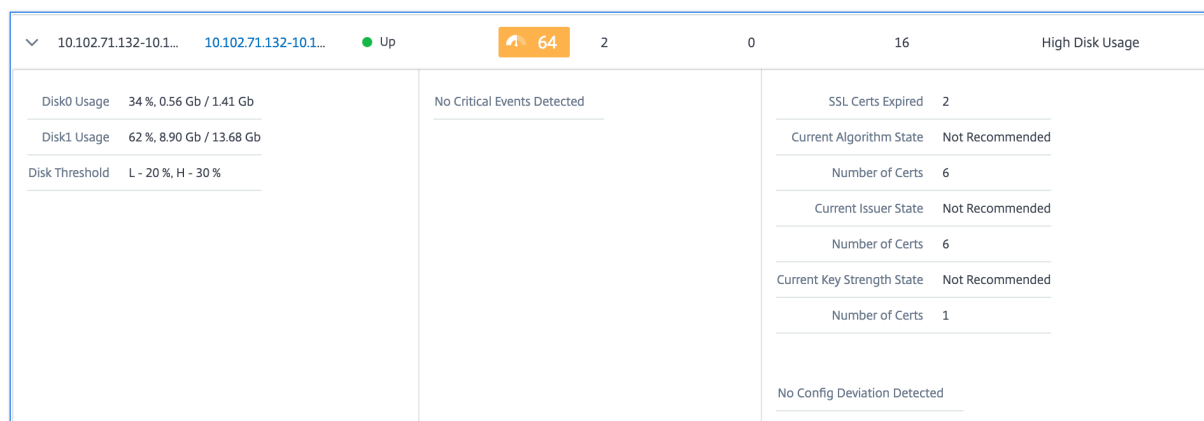
**Instance Overview** 🔍 📄  ⚙️ ?

	HOST NAME	IP ADDRESS	STATE	SCORE	# VSERVERS	# APPLICAT...	# TOTAL IN...	MAX CONT...
>	10.106.136...	<a href="#">10.106.136...</a>	● Up	90	0	0	2	High Memo...
>	10.102.126...	<a href="#">10.102.126...</a>	● Up	82	17	3	7	High Memo...
>	10.102.71.1...	<a href="#">10.102.71.1...</a>	● Up	64	2	0	16	High Disk U...
>	10.106.99.9...	<a href="#">10.106.99.9...</a>	● Up	63	2	1	8	High Disk U...
>	naresh_138	<a href="#">10.102.61.1...</a>	● Up	63	12	5	6	High Disk U...
>	10.106.136...	<a href="#">10.106.136...</a>	● Up	59	0	0	7	High Memo...
>	10.102.103...	<a href="#">10.102.103...</a>	● Up	51	3	0	6	High Memo...
>	10.102.29.1...	<a href="#">10.102.29.1...</a>	● Up	50	2	0	9	High Memo...
>	10.106.40.1...	<a href="#">10.106.40.1...</a>	● Up	48	2	0	8	High Memo...
>	10.102.60.1...	<a href="#">10.102.60.1...</a>	● Up	48	10000	44	6	High Memo...

表形式のビューでインスタンスの IP アドレスをクリックすると、そのインスタンスの詳細がダッシュボードに表示されます。インスタンスダッシュボードには、インスタンスの概要が表示され、インスタンスの CPU、メモリ、ディスク使用量を確認できます。SSL 証明書管理、設定監査、ネットワーク機能、およびインスタンスの詳細なネットワーク使用状況を示すネットワークレポートに関連する詳細も確認できます。さらに下にスクロールすると、このインスタンスで有効になっている機能とモードのリストが表示されます。



各行の先頭にある矢印をクリックして、行を展開して詳細を確認することもできます。



展開された表の行には、すべてのカテゴリのインスタンスで発生したエラーが表示されます。上の例では、システムリソース、SSL 構成、および設定ファイルにエラーがあったことがわかります。ただし、インスタンスから報告される重大なイベントはありません。

## サマリーパネルの使用方法

**Summary Panel** を使用すると、レビューやクリティカルな状態が必要なインスタンスに効率的かつ迅速に焦点を当てることができます。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により、Circle Pack と Tabular View フォーマットの両方での表示が変更されます。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。次のセクションの例は、さまざまな選択基準を使



用して、インスタンスによって報告された問題を効率的に分析するのに役立ちます。

概要:

概要タブでは、ハードウェアエラー、使用状況、期限切れの証明書、およびインスタンスで発生する可能性のある同様の指標に基づいてインスタンスを監視できます。ここで監視できる指標は次のとおりです。

- CPU 使用率
- メモリ使用率
- ディスク使用率
- システム障害
- クリティカルイベント
- SSL 証明書の有効期限

次の例は、[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:

「レビュー」(Review) チェックボックスを選択すると、重大なエラーは報告されていないが、まだ注意が必要なインスタンスのみが表示されます。

概要パネルのヒストグラムは、高 CPU 使用率、高メモリ使用量、および高ディスク使用率イベントに基づいて集計されたインスタンス数を表します。ヒストグラムは、10%、20%、30%、40%、50%、60%、70%、80%、90%、100%で等級分けされます。棒グラフのいずれかにマウスポインターを置きます。グラフ下部の凡例には、使用範囲とその範囲内のインスタンス数が表示されます。棒グラフをクリックして、その範囲内のすべてのインスタンスを表示することもできます。

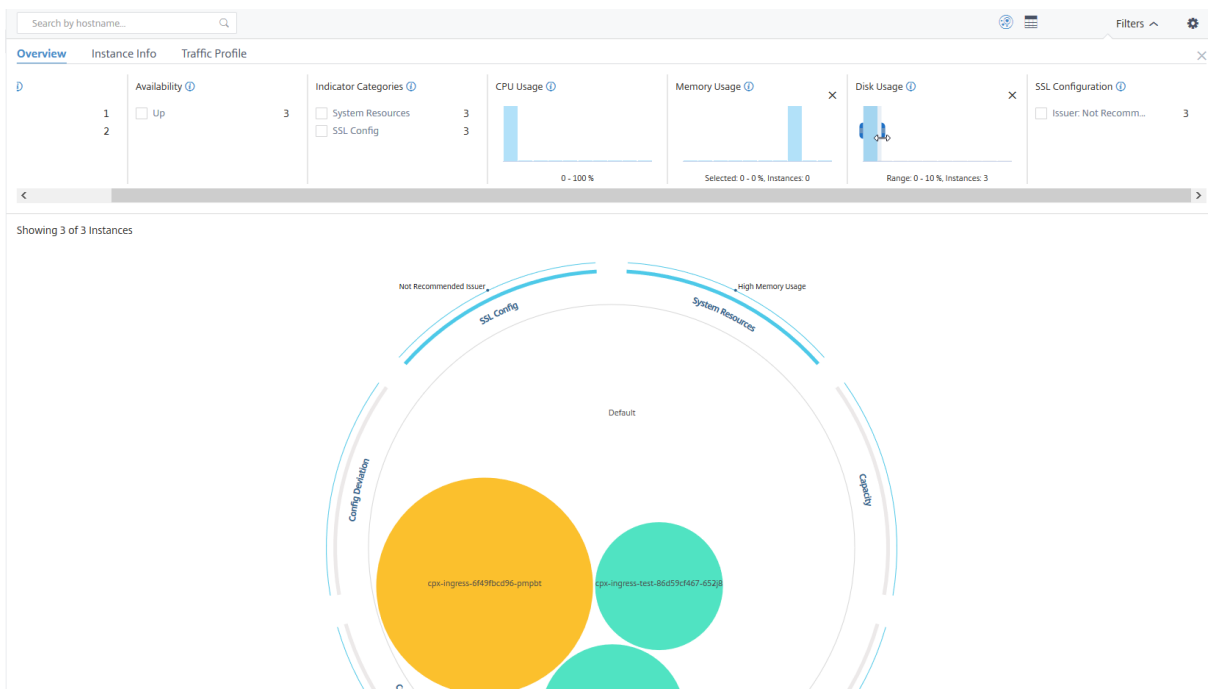
例 **2**: 割り当てられたメモリの **10%** から **20%** を消費しているインスタンスを表示する:

メモリ使用量セクションで、棒グラフをクリックします。凡例によると、選択された範囲は 10 ~20% で、その範囲で動作しているインスタンスが 29 個あります。

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**: 複数の範囲で大量のディスク容量を消費しているインスタンスを表示する:

0 ~10% のディスク容量を消費したインスタンスを表示するには、マウスポインタを 2 つの範囲にドラッグします。

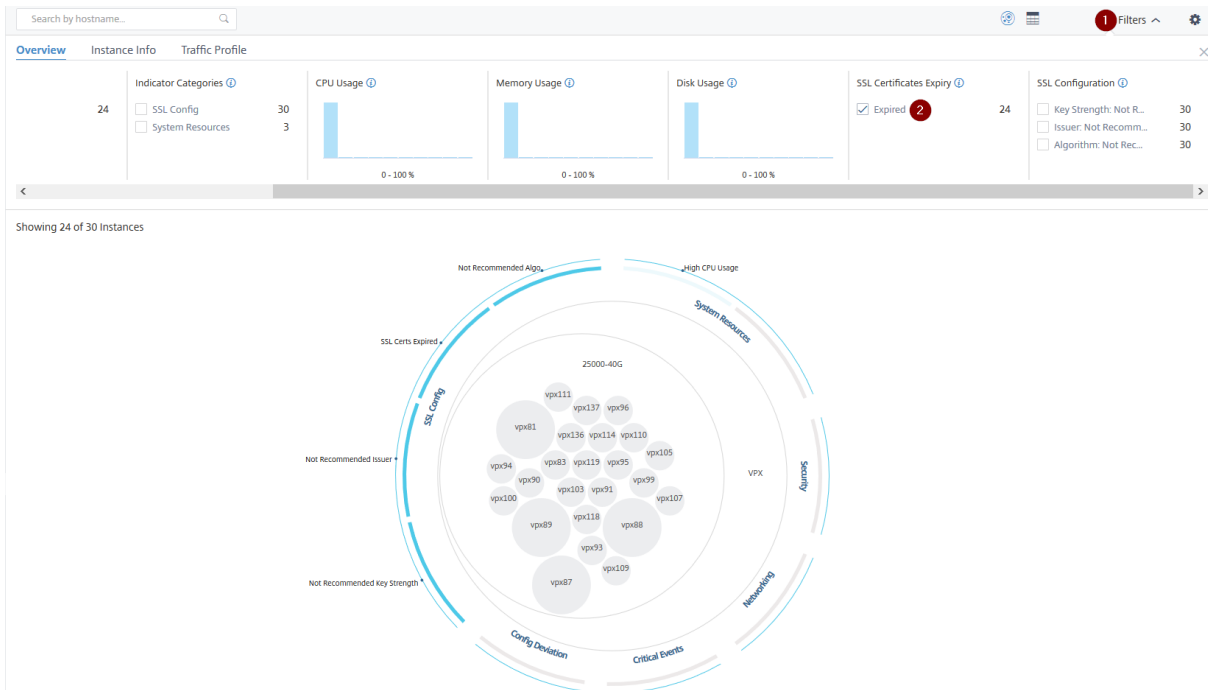


注:

[X] をクリックして選択を解除します。[リセット] をクリックして複数の選択を削除することもできます。

概要パネルの横棒グラフには、システムエラー、重大なイベント、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が表示されます。チェックボックスを選択すると、それらのインスタンスが表示されます。

例 4: 有効期限が切れた SSL 証明書のインスタンスの表示:



1 - [フィルタ] リストをクリックします。

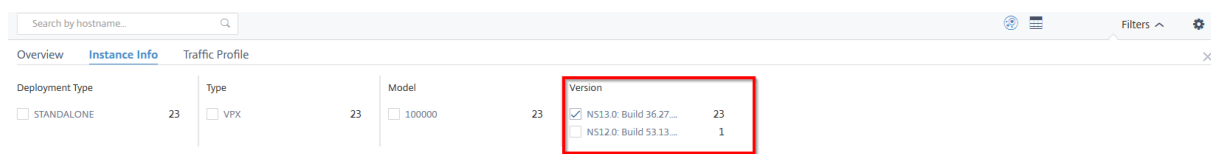
2 - **SSL** 証明書の有効期限セクションで、[期限切れ] チェックボックスを選択してインスタンスを表示します。

### インスタンス情報

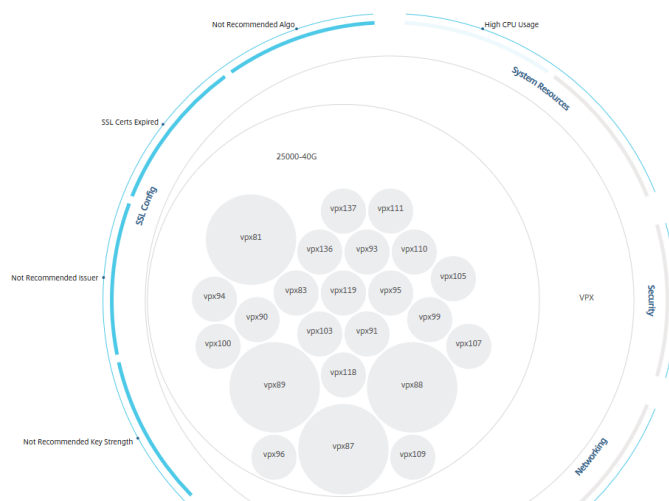
インスタンス情報パネルでは、デプロイのタイプ、インスタンスタイプ、モデル、およびソフトウェアバージョンに基づいてインスタンスを表示できます。複数のチェックボックスを選択して、選択を絞り込むことができます。

例 **5**: 特定のビルド番号の **ADC VPX** インスタンスを表示する:

表示するバージョンを選択します。



Showing 23 of 30 Instances



### 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、リクエスト数、接続数、インスタンスが処理した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数を表します。棒グラフを選択すると、その範囲のインスタンスが表示されます。

例 **6**: **TCP** 接続をサポートするインスタンスの表示:

次の図は、TCP 接続をサポートするインスタンスの数を示しています。



## 設定パネルの使い方

設定パネルでは、インフラストラクチャー分析のデフォルトビューを設定できます。また、CPU 使用率が高い、ディスク使用量が多い、メモリ使用量が多い場合に、しきい値の下限值と上限値を設定することもできます。設定パネルは、「表示」と「スコアしきい値」の2つのタブに分かれています。

## 表示

- デフォルトビュー。分析ページのデフォルトビューとして「サークルパック」または「表形式」を選択します。選択した形式は、NetScaler ADM のページにアクセスしたときに表示される形式です。
- サークルパック-インスタンスサイズ。インスタンスサークルのサイズは、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なります。
- サークルパック-**Cluster By**。インスタンスサークルの2レベルのクラスタリングを決定します。インスタンスのクラスタリングについて詳しくは、「クラスター化されたインスタンスの円」を参照してください。

### Settings Panel

Apply Settings 
Reset Settings

---

View    Score Thresholds

---

**DEFAULT VIEW**

Circle Pack View  
 Tabular View

---

**CIRCLE PACK - INSTANCE SIZE**

# Virtual Servers  
 # Active Virtual Servers

---

**CIRCLE PACK - CLUSTER BY**

Level 1	Site
Level 2	Type

#### スコア閾値


組織内のトラフィック要件に応じて、CPU、メモリ、およびディスク使用率の上限と下限を変更できます。各選択ヒストグラムのハンドルをドラッグして、値を設定します。

### Settings Panel

Apply Settings     Reset Settings

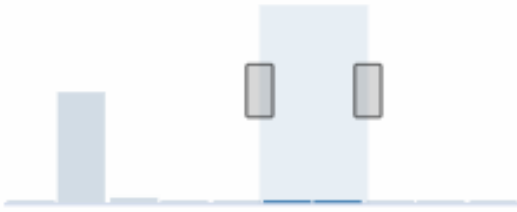
View [Score Thresholds](#)

#### HIGH CPU USAGE




Selected: 80 - 90 %, # Instances: 0

#### HIGH MEMORY USAGE



Selected: 50 - 70 %, # Instances: 0

#### HIGH DISK USAGE



Selected: 80 - 90 %, # Instances: 0

注:

[設定の適用] をクリックしてこれらの変更を適用するか、[リセット] をクリックしてすべての変更を削除します。

## ダッシュボードでデータを視覚化する方法

Infrastructure Analytics を使用して、ネットワーク管理者は数秒以内に最も注意が必要なインスタンスを特定できるようになりました。データビジュアライゼーションをより詳細に理解するために、ExampleCompany のネットワーク管理者である Chris の場合を考えてみましょう。

クリスは組織内で多くの Citrix ADC インスタンスを管理しています。一部のインスタンスは大量のトラフィックを処理しているため、Chris はそれらを注意深く監視する必要があります。Chris は、トラフィックの多いインスタンスが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がきました。この減少を分析するために、以前、クリスはさまざまなソースから届いた複数のデータレポートを読む必要がありました。Chris は、データを手動で関連させ、どのインスタンスが最適な状態にないか、注意が必要かを確かめるために、より多くの時間を費やす必要がありました。

Chris はインフラストラクチャ分析機能を使用して、すべてのインスタンスの状態を視覚的に確認しています。

次の 2 つの例は、Infrastructure Analytics が Chris のメンテナンスアクティビティ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には:

Chris が Circle Pack で、1 つのインスタンスのスコアが低く、そのインスタンスが「Critical」状態になっていることに気がきます。Chris はそのインスタンスをクリックして、問題が何であるかを確認します。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、インスタンスが SSL トラフィックを処理できない (SSL トラフィックが減少した) ことが表示されます。Chris はその情報を抽出し、問題をすぐに調査するレポートをチームに送信します。

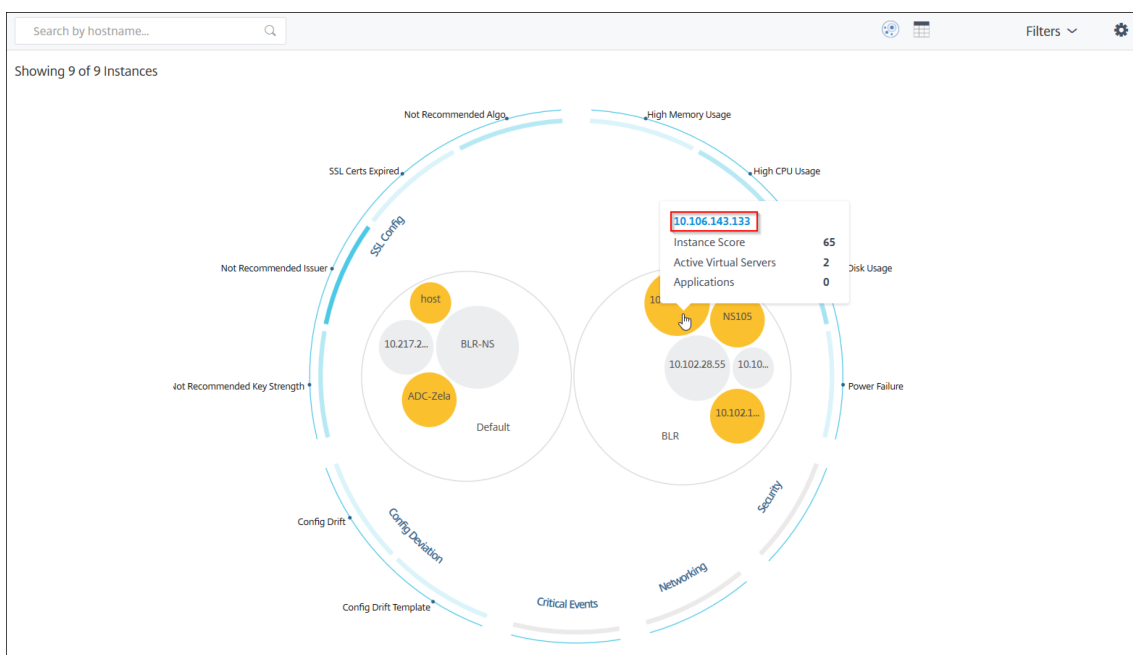
### 例 2-構成の変更を監視するには:

Chris は、別のインスタンスが「Review」状態にあり、最近設定偏差があることに気がきます。Chris が構成逸脱リスクインジケータをクリックすると、Chris は RC4 Cipher、SSL v3、TLS 1.0、TLS 1.1 に関連する構成変更が行われたことに気がきますが、これはセキュリティ上の懸念によるものと考えられます。Chris は、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ダウンしていることにも気がきました。Chris はこのレポートをエクスポートし、管理者に送信してさらに問い合わせます。

## インフラストラクチャ分析でのインスタンスの詳細の表示

February 6, 2024

1. [ ネットワーク ] > [ インフラストラクチャ分析 ] に移動します
2. サークルバックビューをクリックし、IP アドレスを選択します。



テーブルビューから IP アドレスをクリックすることもできます。

HOST NAME	IP ADDRESS	SCORE	AVAILABILITY	MAX CONT...	CPU USAGE	MEMORY USA...	DISK USAGE	SYSTEM FAILU...	CRITICAL EVE...	SSL EXPIRY	TYPE	DEPI
> 10.217.24.1...	10.217.24.1...	Unknown	Out of Serv	NA	1.39%	0%	0%	Power Failure	NA	Expired	MPX	STAI
> 10.102.28.55	10.102.28.55	Unknown	Out of Serv	NA	2.85%	0%	0%	NA	NA	NA	VPX	STAI
> 10.106.136...	10.106.136...	Unknown	Out of Serv	NA	2.07%	0%	0%	NA	NA	NA	VPX	STAI
> BLR-NS	10.102.60.28	Unknown	Out of Serv	NA	2.05%	0%	0%	NA	NA	NA	VPX	STAI
> 10.102.126...	10.102.126...	55 Review	Up	High Memo...	0.6%	213.8%	0%	NA	NA	NA	BLX	STAI
> NS105	10.102.126...	61 Review	Up	High CPU U...	5%	17.16%	92.21%	NA	NA	NA	VPX	STAI
> 10.106.143...	10.106.143...	65 Review	Up	High Disk U...	1%	19.91%	51.96%	NA	NA	NA	VPX	STAI
> ADC-Zela	10.221.37.67	67 Review	Up	High Disk U...	0.3%	5.35%	48.88%	NA	NA	NA	MPX	STAI
> host	10.102.126...	67 Review	Up	High Disk U...	1%	17.36%	66.03%	NA	NA	NA	VPX	STAI

- ホスト名—ADC インスタンスに割り当てられたホスト名を示します
- **IP** アドレス—ADC インスタンスの IP アドレスを示します。
- スコア—ADC インスタンスのスコアと、クリティカル、グッド、フェアなどのステータスを示します。
- 可用性—ADC インスタンスのステータス（稼働中、停止中、\*\* サービス停止など \*\*）を示します。
- 最大寄与度—ADC インスタンスのエラー数が最大である問題のカテゴリを示します。
- **CPU** 使用率—インスタンスが現在使用している CPU% を示します

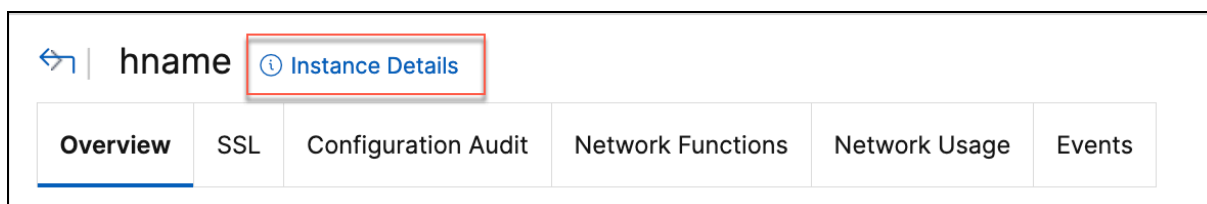


- メモリ使用量—インスタンスが現在使用しているメモリ (%) を示します
- **Disk usage** —インスタンスが現在使用しているディスク (%) を示します
- システム障害—インスタンス・システムのエラーの総数を示します
- 「クリティカルイベント」—NetScaler ADC インスタンスに最大イベントがあるイベントカテゴリを示します。
- **SSL** 有効期限—ADC インスタンスにインストールされている SSL 証明書のステータスを示します
- タイプ: VPX、SDX、MPX、CPX などの ADC インスタンスタイプを示します。
- デプロイ—ADC インスタンスがスタンドアロンインスタンスとしてデプロイされているか、HA ペアとしてデプロイされているかを示します
- モデル—ADC インスタンスのモデル番号を示します
- バージョン—ADC インスタンスのバージョンとビルド番号を示します
- スループット—ADC インスタンスからの現在のネットワークスループットを示します
- **HTTPS** リクエスト/秒—ADC インスタンスが受信した現在の HTTPS リクエスト/秒を示します
- **TCP** 接続—現在確立されている TCP 接続を示します
- **SSL** トランザクション—ADC インスタンスが現在処理している SSL トランザクションを示します
- サイト—ADC インスタンスがデプロイされているサイトの名前を示します。

注

5 分ごとに、CPU 使用量、メモリ使用量、ディスク使用量、スループットなどの現在の値が更新されます。

[インスタンスの詳細] をクリックして詳細を表示します。



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。

- Details			
<b>Information</b>			
HOST NAME	[REDACTED]	MODEL ID	2000
SYSTEM IP ADDRESS	[REDACTED]	SYSTEM CUSTOM ID	Default
SYSTEM NAME	NetScaler	PACKET ENGINES	1
TYPE	NetScaler CPX	SSL CARDS	0
HA MASTER STATE	Primary	CPU	3501MHZ
NODE STATE	<span style="color: green;">↑</span> Up	VERSION	NS13.1: Build 49.13.nc
PEER IP ADDRESS	--	HARDWARE VERSION	ADC CPX
SECONDARY NODE STATUS	--	LOM VERSION	-NA-
HA SYNC STATUS	ENABLED	HOST ID	nscpx-netscal
SYSTEM SERVICES	72	SERIAL NUMBER	-ingress-controller-[REDACTED]-:-
NETMASK	[REDACTED]	ENCODED SERIAL NUMBER	-ingress-controller-[REDACTED]-
GATEWAY	[REDACTED]	NetScaler ADC UUID	a48d554d-9082-4899-bb59-[REDACTED]
ADMIN PROFILE	10.128.3.202_cpx_profile	LOCATION	POP (default)
HEALTH	--	CONTACT PERSON	WebMaster (default)
MAINTENANCE TYPE	--	MAINTENANCE END DATE	0
UPTIME	--		
DESCRIPTION	--		

- 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。[ライセンス機能]をクリックすると、ライセンスされている機能が表示されます。

Features			
All features are licensed except the following:			
License Type	Advanced	Licensing Mode	Pooled
Model ID	2000	Web Interface	×
Integrated Caching	×	Application Firewall	×
CloudBridge	×	Priority Queuing	×
Sure Connect	×	DoS Protection	×
Content Accelerator	×	vPath	×
RISE	×	Reputation	×
Delta Compression	×	URL Filtering	×
Video Optimization	×		
<a href="#">Licensed Features &gt;</a>			

- 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。「有効化されたモードを表示」をクリックすると、インスタンスで有効になっているモードが表示されます。

### Modes

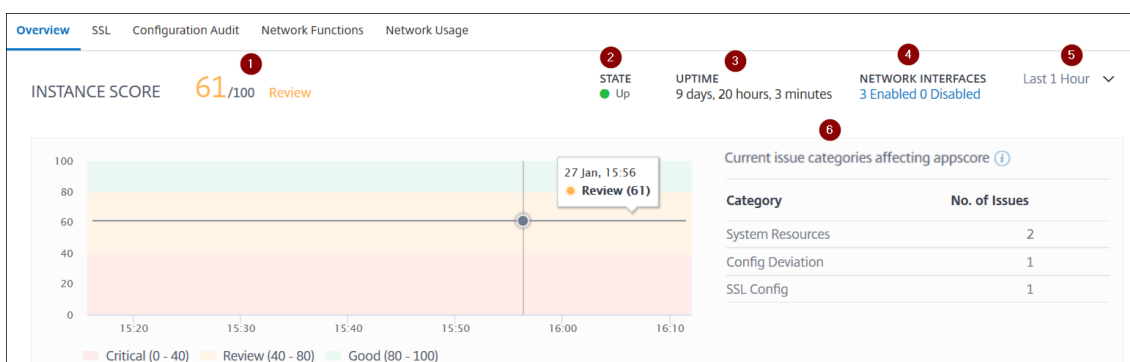
All modes are enabled except the following:

Bridge BPDUs	×	Client side Keep Alive	×
Direct Route Advertisement	×	IPv6 Direct Route Advertisement	×
Intranet Route Advertisement	×	Layer 2 Mode	×
MAC based forwarding	×	Media Classification	×
RISE APBR	×	RISE RHI	×
Static Route Advertisement	×	IPv6 Static Route Advertisement	×
TCP Buffering	×	Use Source IP	×
Unified Logging Format	×		

[View Enabled Modes](#) ▼

インスタンスダッシュボードにはインスタンスの概要が表示され、次の詳細を確認できます。

- インスタンススコア



**1**—選択した期間における現在の NetScaler ADC インスタンスのスコアを示します。最終スコアは、**100** から合計ペナルティを引いたもの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**—Citrix ADC インスタンスのステータス（稼働中、停止中、\*\* サービス \*\* 停止など）を示します。

**3**—NetScaler ADC インスタンスが起動して実行されている期間を示します。

**4**—インスタンスで有効化されているネットワークインタフェースと無効化されているネットワークインタフェースの合計数を示します。クリックすると、ネットワークインターフェ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。

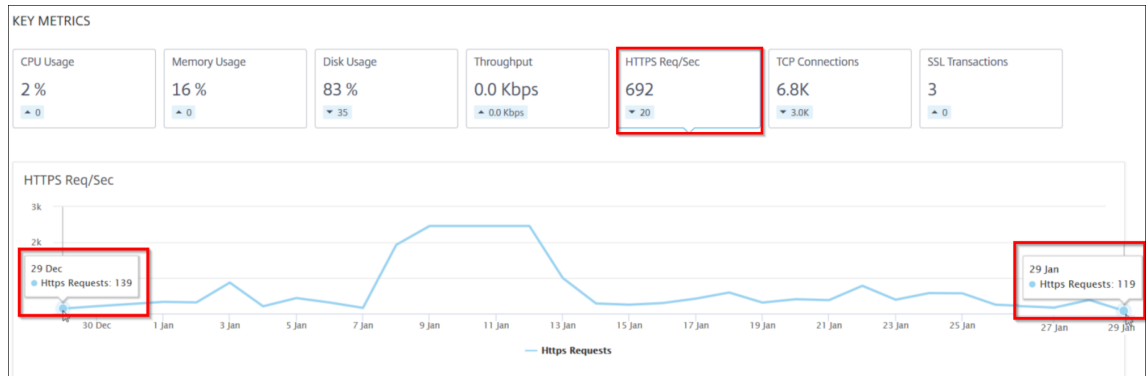
**5**—インスタンスの詳細を表示する期間をリストから選択します。

**6**—ADC インスタンスの全問題と問題カテゴリを表示します。

- 主要指標

各タブをクリックすると、詳細が表示されます。各指標で、選択した時間の平均値と差分値を表示できます。

次の画像は HTTPS Req/Sec の例で、選択した期間は 1 時間です。692 は 1 か月間の平均 HTTPS 要求/秒で、20 は差異値です。グラフでは、最初の値は 139、最後の値は 119 です。差の値は  $139 - 119 = 20$  です。



選択した期間について、次のインスタンスメトリックスをグラフ形式で表示できます。

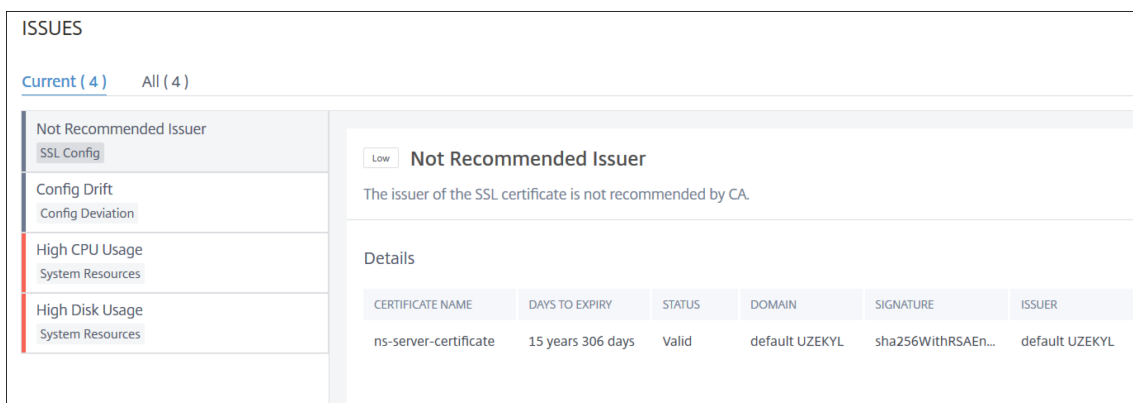
- CPU 使用率—選択した期間におけるインスタンスの平均 CPU% (パケット CPU と管理 CPU の両方で表示)。
  - Memory Usage —選択した期間におけるインスタンスの平均メモリ使用率 (%)。
  - ディスク使用量—選択した期間におけるインスタンスの平均ディスク容量 (%)。
  - スループット—選択した期間にインスタンスが処理した平均ネットワークスループットです。
  - HTTPS リクエスト/秒—選択した期間にインスタンスが受信した HTTPS リクエストの平均。
  - TCP 接続—選択した期間にクライアントとサーバーによって確立された TCP 接続の平均値。
  - SSL トランザクション—選択した期間にインスタンスが処理した SSL トランザクションの平均です。
- 問題点

NetScaler ADC インスタンスで発生する次の問題を確認できます。

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、Citrix ADC システムリソースに関連するすべての問題が表示されます。	<ul style="list-style-type: none"> <li>- 高い CPU 使用率</li> <li>- 高いメモリ使用量</li> <li>- 高いディスク使用量</li> <li>- SSL カード障害</li> <li>- 停電</li> <li>- ディスクエラー</li> <li>- フラッシュエラー</li> </ul>

問題カテゴリ	説明	問題
SSL 設定	NetScaler ADC インスタンスの SSL 構成に関連するすべての問題を表示します。	<ul style="list-style-type: none"> <li>- NIC 廃棄</li> <li>-SSL 証明書の有効期限切れ</li> <li>- 推奨されない発行者</li> <li>- 推奨されないアルゴリズム</li> <li>- 推奨キーストレングスではありません</li> </ul>
設定偏差	NetScaler ADC 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。	<ul style="list-style-type: none"> <li>-構成ドリフト</li> <li>- 実行とテンプレート</li> </ul>
クリティカルイベント	HA ペアとクラスタで構成された NetScaler ADC インスタンスに関連するすべての重要なイベントを表示します。	<ul style="list-style-type: none"> <li>- クラスタブロック障害</li> <li>- クラスタ同期失敗</li> <li>- クラスタバージョンの不一致</li> <li>- HA セカンダリステートが不良です</li> <li>- HA ノーヒートビート</li> <li>- HA 同期失敗</li> <li>- HA バージョンの不一致</li> </ul>
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、「 <a href="#">新しい指標によるインフラストラクチャ分析の強化</a> 」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に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し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ストラクチャの問題が表示されます。

## ADC インスタンスの容量に関する問題の表示

February 6, 2024

ADC インスタンスが使用可能な容量の大半を消費した場合、クライアントトラフィックの処理中にパケット廃棄が発生することがあります。この問題は、ADC インスタンスのパフォーマンスが低下します。このような ADC 容量の問題を理解することで、ADC の性能を安定させるために事前に追加ライセンスを割り当てることができます。

**Circle Pack** ビューでは、ADC インスタンスのキャパシティの問題が存在する場合は、その問題を表示できます。

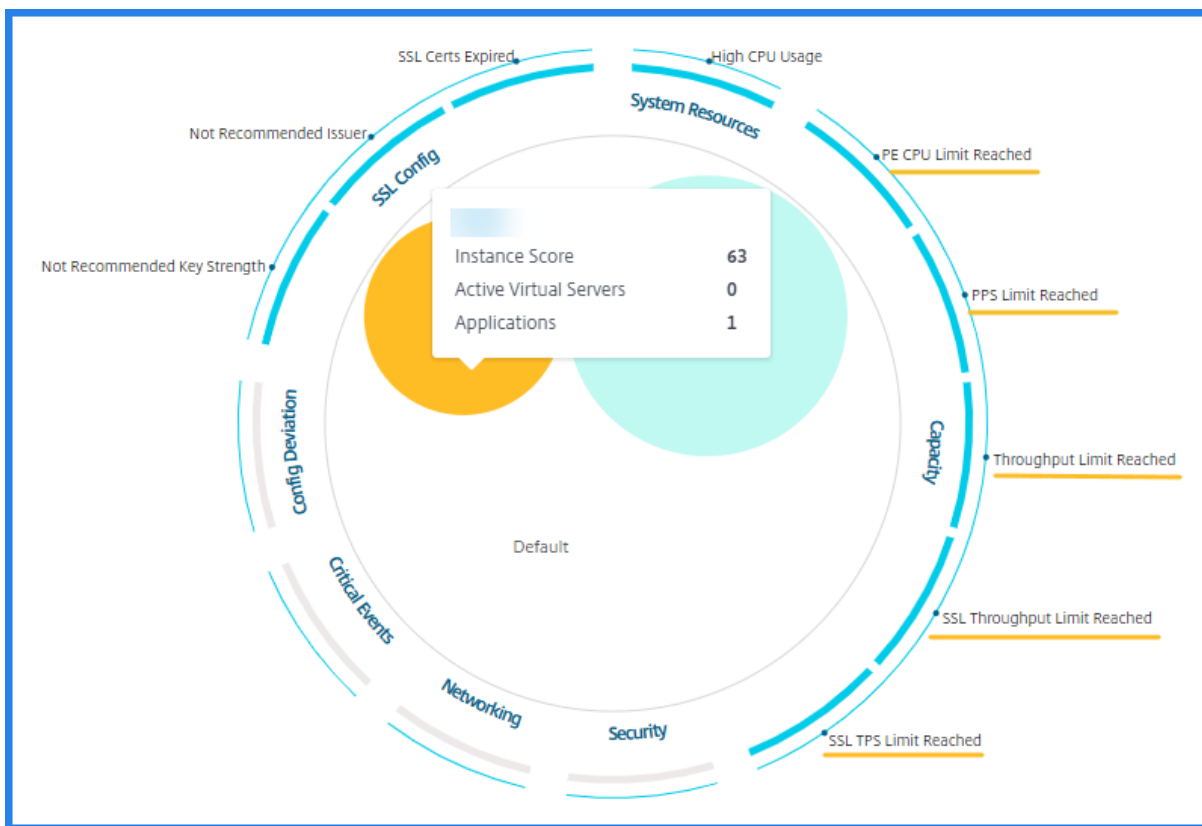
ADC の容量に関する問題を確認するには、

1. [ネットワーク] > [インフラストラクチャ分析] に移動します。
2. 円パックビューを選択します。

注:

**Infrastructure Analytics** では、サークルパックビューと表形式ビューに、過去 1 時間に発生したイベントと問題が表示されます。

次の図は、選択したインスタンスにキャパシティの問題が存在することを示しています:



問題は次の容量パラメータに分類されます。

- スループット制限に達しました—スループット制限に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** の上限に達した -PE CPU の制限に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** 制限に達しました—PPS 制限に達した後にインスタンスでドロップされたパケット数。
- **SSL** スループットレート制限—SSL スループット制限に達した回数。
- **SSL TPS** レート制限—SSL TPS 制限に達した回数。

キャパシティの問題を解決するための推奨アクションを表示

ADM は、容量の問題を解決できるアクションを推奨しています。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. [ネットワーク] > [インフラストラクチャ分析] で、表形式のビューを選択します。
2. 容量に問題があるインスタンスを選択し、[ **Details** ] をクリックします。

HOST NAME	IP ADDRESS	SCORE	INSTANCE STATE	MAX CONT...	CPU USAGE	MEMORY U...	DISK USAGE	SYSTEM FAL...	CRITICAL E...
▼		63 Review	● Up	High CPU U...	4.20%	19.91%	34.44%	NA	NA
System Resources						SSL Config			
Packet CPU Usage 4.20 %						SSL Certs Expired 2			
Management CPU Usage 100 %						Current Issuer State Not Recommended			
CPU Threshold L - 80 % H - 90 %						Number of Certs 3			
						Current Key Strength State Not Recommended			
						Number of Certs 1			

3. インスタンスページで、**Issues** セクションまでスクロールします。
4. 各問題を選択し、キャパシティの問題を解決するための推奨アクションを表示します。

The screenshot shows the 'Issues' section in the NetScaler ADM interface. On the left, a list of issues is displayed, including 'PE CPU Limit Reached', 'FPS Limit Reached', 'Throughput Limit Reached', 'SSL Throughput Limit Reach...', 'SSL TPS Limit Reached', 'Not Recommended Key Stre...', 'Not Recommended Issuer', 'SSL Certs Expired', and 'High CPU Usage'. The 'PE CPU Limit Reached' issue is selected, and its details are shown on the right. The details include a description: 'Aggregate (all nics) packet drops after PE CPU limit was reached'. Below this, there are 'Recommended Actions' with two bullet points: 'If you are a pooled license customer, then allocate more throughput to the ADC.' and 'If you are not a pooled license customer, talk to your sales executive for upgrading your existing license/model.' At the bottom, there is a 'Details' section with a bar chart showing the 'PE CPU Limit Reached' event occurring between 15:30 and 16:20. The chart has a y-axis labeled 'PE CPU Limit Reached' and an x-axis labeled 'TIMESTAMP' with values 15:30, 15:40, 15:50, 16:00, 16:10, and 16:20. Below the chart is a table with columns 'TIMESTAMP' and 'MESSAGE'.

ADM は、ADC インスタンスから 5 分ごとにこれらのイベントをポーリングし、パケットドロップまたはレート制限カウンタが存在する場合は、その増加を表示します。

ADM は、定義された容量しきい値に基づいてインスタンススコアを計算します。

- 低いしきい値: 1 パケットドロップまたはレート制限カウンタの増分
- 高いしきい値: 10000 パケットのドロップまたはレート制限カウンタ増分

したがって、ADC インスタンスがキャパシティしきい値を超えると、インスタンスのスコアが影響を受けます。

パケットがドロップまたはレート制限カウンタが増加すると、**ADCCapacityBreach** カテゴリの下にイベントが生成されます。これらのイベントを表示するには、[アカウント] > [システムイベント] に移動します。



## 新しいインジケータによるインフラストラクチャ分析の強化

February 6, 2024

Citrix ADM インフラストラクチャ分析を使用すると、次のことができます。

- NetScaler ADC インスタンスで発生する新しい運用上の問題をご覧ください。
- エラーメッセージを表示し、推奨事項を確認して問題をトラブルシューティングします。

管理者は、問題の根本原因分析をすばやく特定できます。

## 注

ルールインジケータは次の場合はサポートされていません。

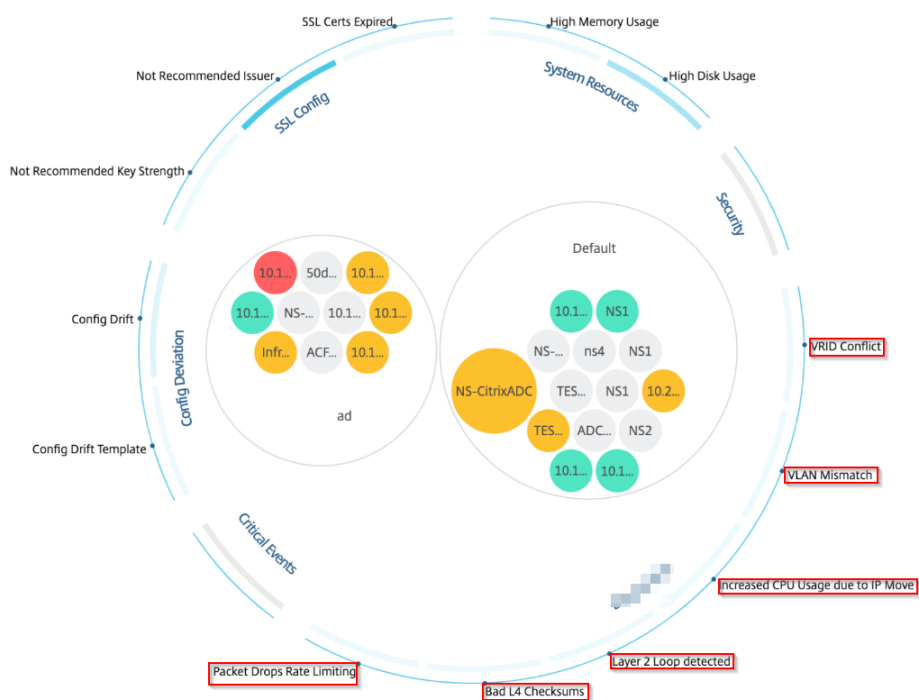
- クラスターモードで構成された NetScaler ADC インスタンス。
- 管理パーティションで構成された NetScaler ADC インスタンス。

NetScaler ADM で、[ネットワーク]&gt;[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名	説明
ポート割り当ての失敗	NetScaler ADC が SNIP を使用して新しいサーバー接続と通信し、その SNIP で使用可能なポートの合計が使い果たされたことを検出します。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。
デフォルトのルート設定なし	ルートが使用できないためにトラフィックがドロップされたことを検出します。
<b>IP</b> の競合	ネットワーク内の複数のインスタンスに同じ 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。
<b>VRID</b> の競合	指定した VRID で断続的なアクセスの問題が発生したことを検出します。
<b>VLAN</b> の不一致	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。
<b>TCP</b> 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。ADC はすでにこの攻撃を軽減しているため、このアラートは情報提供のみを目的としています。
レートコントロールしきい値	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ことを検出します。
パーシスタンス制限	NetScaler ADC メモリに最大ヒットが発生したことを検出します。

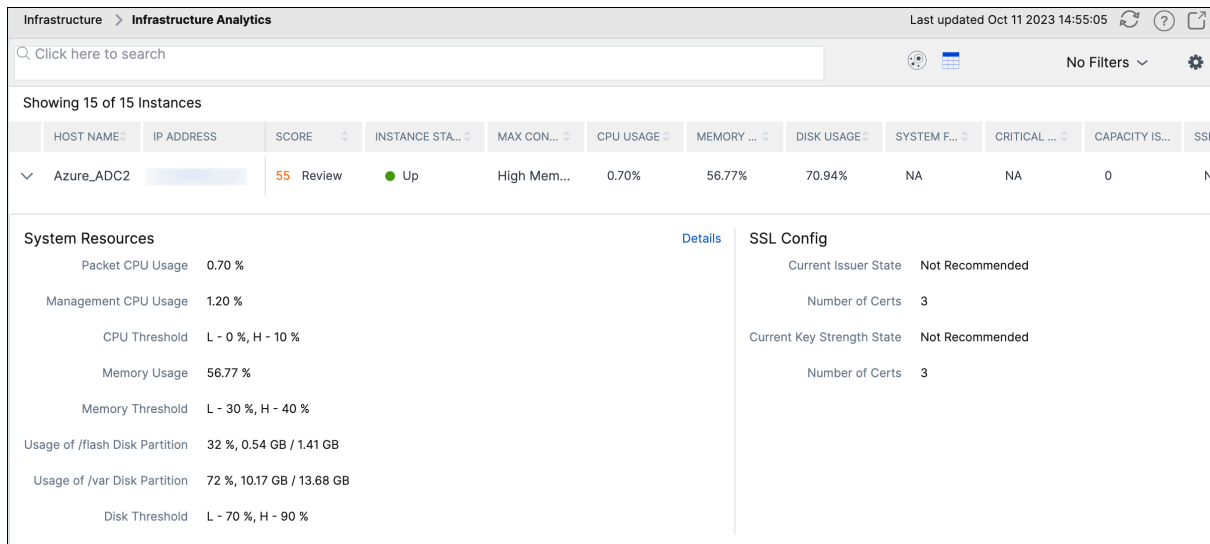
インフラストラクチャ分析のインジケータ名	説明
<b>GSLB</b> サイト名の不一致	サイト名の不一致が原因で GSLB 構成の同期エラーが発生したことを検出します。
不正な <b>IP</b> ヘッダー	IPv4 パケットのサニティチェックが失敗したことを検出します。
不正な <b>L4</b> チェックサム	TCP パケットのチェックサム検証が失敗したことを検出します。
<b>IP</b> 移動による <b>CPU</b> 使用率の向上	多数の Mac を更新する必要があるかどうかを検出します。
過剰なパケットステアリング	非対称 RSS キータイプの使用による高レベルのソフトウェアパケットステアリングを検出します。
レイヤ <b>2</b> ループ	ネットワーク内のレイヤ 2 ループの存在を検出します。
タグ付き <b>VLAN</b> 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ことを検出します。

Showing 24 of 24 Instances



表形式ビュー

Inf **rastructure Analytics** の表形式表示オプションを使用して、異常を表示することもできます。[ ネットワーク ] > [ インフラストラクチャ分析 ] に移動し、[  ] をクリックしてすべてのマネージドインスタンスを表示します。[  ] をクリックして展開すると、詳細が表示されます。



The screenshot shows the 'Infrastructure Analytics' page with a table of instances. The instance 'Azure\_ADC2' is selected, and its details are expanded. The details are split into two panels: 'System Resources' and 'SSL Config'.

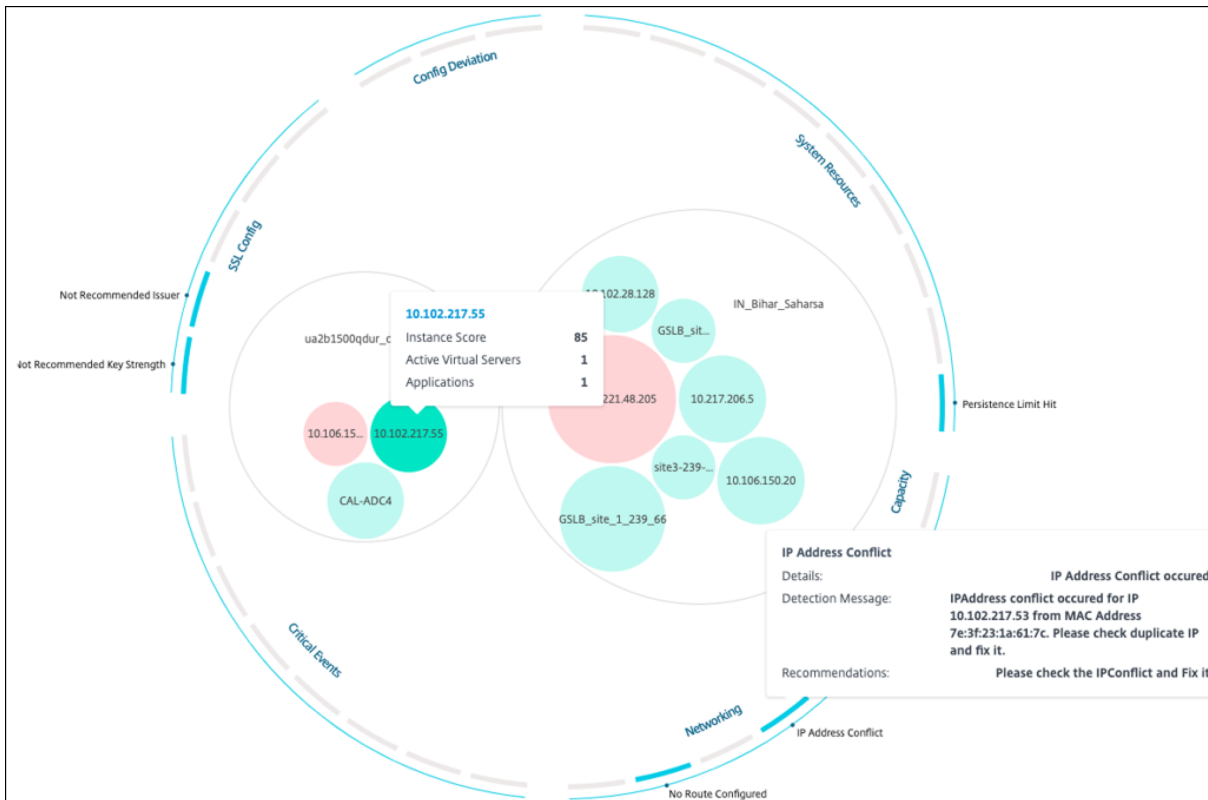
HOST NAME	IP ADDRESS	SCORE	INSTANCE STA...	MAX CON...	CPU USAGE	MEMORY ...	DISK USAGE	SYSTEM F...	CRITICAL ...	CAPACITY IS...	SSL
Azure_ADC2		55 Review	Up	High Mem...	0.70%	56.77%	70.94%	NA	NA	0	NA

System Resources		SSL Config	
Packet CPU Usage	0.70 %	Current Issuer State	Not Recommended
Management CPU Usage	1.20 %	Number of Certs	3
CPU Threshold	L - 0 %, H - 10 %	Current Key Strength State	Not Recommended
Memory Usage	56.77 %	Number of Certs	3
Memory Threshold	L - 30 %, H - 40 %		
Usage of /flash Disk Partition	32 %, 0.54 GB / 1.41 GB		
Usage of /var Disk Partition	72 %, 10.17 GB / 13.68 GB		
Disk Threshold	L - 70 %, H - 90 %		

異常の詳細を表示する

たとえば、ネットワーク内の **IP** アドレス競合の詳細を表示する場合は、IP アドレスの競合について表示されている異常をクリックして詳細を表示します。



- **Details** -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アクション項目を示します。

よくある質問

February 6, 2024

このセクションでは、以下の NetScaler Application Delivery Management (NetScaler ADM) 機能に関する FAQ について説明します。次の表の機能名をクリックすると、その機能に関する FAQ のリストが表示されます。

分析	認証	構成管理
証明書管理	展開	展開 (災害復旧)
イベント管理	インスタンス管理	StyleBook
システム管理		

## 分析

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

EUEM 仮想チャネルデータは、NetScaler ADM がゲートウェイインスタンスから受信する HDX Insight データの一部です。EUEM 仮想チャネルは、ICA RTT に関するデータを提供します。EUEM 仮想チャネルが有効になっていない場合でも、残りの HDX Insight データは NetScaler ADM に表示されます。

EUEM 仮想チャネルは、Citrix 仮想デスクトップアプリケーション (VDA) 上で実行されるデフォルトのサービスです。実行されていない場合は、VDA サービスで「Citrix エンドユーザーエクスペリエンス監視」プロセスを開始します。

**NetScaler ADM** が **Web** アプリケーションと仮想デスクトップのトラフィックを監視できるようにするにはどうすればよいですか

1. [インフラストラクチャ] > [インスタンス] > [ **CitrixADC** ] に移動し、分析を有効にする NetScaler ADC インスタンスを選択します。
2. [アクションの選択] リストから、[ **Analytics** の設定 ] を選択します。
3. 表示された [分析の設定] ページで、分析を有効にするすべての仮想サーバーを選択し、[ **AppFlow** の有効化 ] をクリックします。詳しくは、「[インスタンスの分析を有効にする方法](#)」を参照してください。

### 注

11.0 リリース、65.30 ビルド以降の NetScaler ADC インスタンスの場合、NetScaler ADM では Security Insight を明示的に有効にするオプションはありません。NetScaler ADC インスタンスで AppFlow パラメータを構成して、NetScaler ADM が Web Insight トラフィックとともに Security Insight トラフィックの受信を開始するようにします。NetScaler ADC インスタンスで AppFlow パラメーターを設定する方法について詳しくは、「[構成ユーティリティを使用して AppFlow パラメーターを設定するには](#)」を参照してください。

**NetScaler ADC** インスタンスを追加すると、**NetScaler ADM** は自動的に分析情報の収集を開始しますか？

なし NetScaler ADM によって管理されている NetScaler ADC インスタンスでホストされている仮想サーバーで分析を有効にします。詳しくは、「[インスタンスの分析を有効にする方法](#)」を参照してください。

分析を有効にするには、個々の **NetScaler ADC** アプライアンスにアクセスする必要がありますか

いいえ。すべての構成は、特定の NetScaler ADC インスタンスでホストされている仮想サーバーを一覧表示する NetScaler ADM ユーザーインターフェイスから行います。詳細については、「[インスタンスでアナリティクスを有効にする方法](#)」を参照してください。

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

現在、NetScaler ADM ユーザーインターフェイスには、分析を有効にするための次の仮想サーバーが一覧表示されます。

- 負荷分散仮想サーバー
- コンテンツスイッチ仮想サーバー
- VPN 仮想サーバー
- キャッシュリダイレクト仮想サーバー

追加のディスクを **NetScaler ADM** に接続するにはどうすればよいですか

追加のディスクを NetScaler ADM に接続するには：

1. NetScaler ADM 仮想マシンをシャットダウンします。
2. ハイパーバイザーで、必要なディスクサイズの追加のディスクを NetScaler ADM 仮想マシンに接続します。  
たとえば、120GB の NetScaler ADM 仮想マシンで 200GB にディスク容量を増やすことを考えてみましょう。このシナリオでは、80 GB ではなく 200 GB のディスク領域を接続する必要があります。新しく接続された 200 GB のディスク容量は、データベースデータ、NetScaler ADM ログファイルの保存に使用されます。既存の 120 GB のディスク領域は、コアファイル、オペレーティングシステムのログファイルなどを格納するために使用されます。
3. NetScaler ADM 仮想マシンを起動します。

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

コレクターは、NetScaler ADC アプライアンスによって生成された AppFlow レコードを受信します。

AppFlow 機能が有効になっている場合、NetScaler ADM は NetScaler ADC インスタンスから Security Insight サイトと Web インサイトのトラフィックを受信します。NetScaler ADC インスタンスで AppFlow 機能を有効にする場合は、AppFlow レコードの送信先となるコレクターを少なくとも 1 つ指定する必要があります。NetScaler ADC インスタンスでコレクターが構成されていない場合、NetScaler ADM はインスタンスからのトラフィックを受信しません。

たとえば、5 つの NetScaler ADC インスタンスが NetScaler ADM に追加されます。コレクターが 2 つのインスタンスに指定されていない場合、トラフィックは NetScaler ADM に流れません。セルフサービス診断で問題が検出され、「コレクターが 2 つのインスタンスに構成されていません。」

AppFlow 機能の構成方法の詳細については、「[AppFlow 機能の構成](#)」を参照してください。

クライアント側の測定を有効にするにはどのような機能がありますか

クライアント側の測定を有効にすると、ADM は HTML インジェクションを通じて HTML ページのロード時間とレンダリング時間メトリックをキャプチャします。管理者は、これらのメトリックスを使用して、L7 レイテンシーの問題を特定できます。

### 認証

認証要求の負荷分散とは何ですか

認証サーバーの負荷分散機能により、NetScaler ADM は外部認証サーバーに送信される認証要求の負荷を分散できます。認証サーバーの負荷分散により、認証の負荷が複数の認証サーバーに分散されるようになるので、認証サーバーが過負荷状態になるのを防ぐことができます。LDAP、RADIUS、TACACS などの認証プロトコルを使用して既存の外部認証サーバーに接続し、そのサーバーからユーザー情報を取得する認証サービスを作成できます。

外部認証サーバーをカスケードする必要があるのはなぜですか

カスケードされた外部認証サーバーでは、認証を中断なしで処理でき、いずれかの認証サーバーで障害が発生した場合でも正規ユーザーにアクセスを許可できます。カスケードできる認証サーバーの種類に制限はありません。すべて RADIUS サーバーにすることも、すべて LDAP サーバーにすることも、RADIUS サーバーと LDAP サーバーを組み合わせてカスケードすることもできます。

何台の外部認証サーバーをカスケードできますか

NetScaler ADM では、最大 32 台の外部認証サーバーをカスケードできます。

外部認証に失敗した場合の代替手段はありますか

複数のサーバーをカスケード接続した場合でも、外部認証が完全に失敗することがあります。たとえば、外部サーバーに到達できなくなったり、新しいユーザーの資格情報が外部認証サーバーのいずれにも入力されていない可能性があります。このような状況でユーザーがロックアウトされないようにするには、ローカル認証のフォールバックを有効にします。詳しくは、「[ローカル認証のフォールバックを有効にする方法](#)」を参照してください。

ローカル認証のフォールバックとは何ですか

ローカル認証のフォールバックとは、外部認証に失敗したときにユーザーをローカルで認証するオプションです。外部認証に失敗すると、NetScaler ADM はローカルユーザーデータベースにアクセスしてユーザーを認証します。

Citrix ADM で、[システム] > [認証] > [認証構成] に移動します。このページでは、複数の外部認証サーバーをカスケードに追加したり、**[Enable fallback local authentication]** をオンにできます。

外部ユーザーグループの抽出は何ですか

ユーザーを認証するために外部サーバーを追加した場合は、既存のユーザーグループを NetScaler ADM にインポート（抽出）できます。個々のユーザーをインポートして個々の権限を付与するのではなく、ユーザーグループを一度インポートしてユーザーグループにグループ権限を割り当てるだけで済みます。NetScaler ADM でユーザーを再作成する必要はありません。

グループ権限を割り当てる必要があるのはなぜですか

NetScaler ADC の負荷分散機能を使用する場合は、NetScaler ADM を外部認証サーバーと統合し、認証サーバーからユーザーグループ情報をインポートできます。NetScaler ADM にログインし、NetScaler ADM で同じグループ情報を手動で作成し、それらのグループに権限を割り当てます。ユーザーおよびユーザーグループの権限は、外部サーバーではなく、NetScaler ADM で管理されます。ユーザーは、外部サーバーでさまざまな役割ベースのアクセス権限を持っています。NetScaler ADM のユーザーにも同じ権限を構成します。権限をユーザーごとに個別に構成するのではなく、グループレベルの権限を構成できます。これにより、ユーザーグループのメンバーが負荷分散された仮想サーバー上の特定のサービスにアクセスできるようになります。割り当てることができる一般的な権限は、NetScaler ADC インスタンス、Citrix SDX インスタンス、仮想サーバーなどを管理する権限です。これにより、そのグループのユーザーはそれらのインスタンスまたは仮想サーバーのみを管理できます。ユーザーにグループレベルで付与した権限は、後で編集できます。1 つ以上のユーザーグループを削除することもできますが、他のグループユーザーは引き続き NetScaler ADM で機能します。

構成管理

**NetScaler ADM** を使用して、複数の **NetScaler ADC** インスタンスにまたがって構成を同時に実行できますか

はい。構成ジョブを使用して、複数の NetScaler ADC インスタンスにわたって構成を実行できます。

**NetScaler ADM** の構成ジョブは何ですか？

ジョブとは、管理対象インスタンスに対して作成および実行できる構成コマンドのセットです。ジョブを作成してインスタンス間で構成を変更したり、ネットワーク上の複数のインスタンスに構成を複製したり、NetScaler ADM GUI を使用して構成タスクを記録して再生したりできます。記録したタスクを CLI コマンドに変換することもできます。

NetScaler ADM 構成ジョブ機能を使用して、構成ジョブの作成、電子メール通知の送信、および作成されたジョブの実行ログの確認を行うことができます。



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

はい! 組み込みテンプレートオプションを使用して、ジョブにスケジュールを指定できます。ジョブとは、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のことです。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にスケジュールを指定できます。ジョブをすぐに実行するか、後で実行するようにジョブをスケジュールするかを選択できます。

作成済みのジョブの構成を保存して、コマンド、パラメーター、構成ソース、ターゲットインスタンスを変更してから、そのジョブを再実行できます。これは、同じ一連のコマンドを別のインスタンスで実行する必要がある場合や、ジョブでエラーが発生してそれ以降の実行を停止する場合に便利です。

## 証明書管理

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

いいえ

## 展開

### デフォルトのユーザー名とパスワードは何ですか?

- 初期ネットワーク構成が完了したら、デフォルトのユーザー名とパスワード (nsrecover/nsroot) を使用して、ハイパーバイザーまたは SSH コンソールから NetScaler ADM にログオンできます。
- GUI からログオンするデフォルトのユーザー名とパスワードは、*nsroot/nsroot* です。

デフォルトパスワードを変更するにはどうすればいいですか

パスワードを変更するには、次の手順に従います。

1. NetScaler ADM で、[システム] > [ユーザー管理] > [ユーザー] に移動します。

「ユーザー」ページが表示されます。

2. ユーザー名 **nsroot** を選択し、[編集] をクリックします。



[システムユーザーの構成] ページが表示されます。

3. [パスワードの変更] を選択し、任意のパスワードを作成します。

User Name\*

 ?

Password\*

 ?

Confirm Password\*

 ?

4. [OK] をクリックします。

これで、新しいパスワードを使用して GUI、ハイパーバイザー、または SSH コンソールからログオンできます。

注

ユーザー名は変更できません。

パスワードをリセットするには?

[このドキュメントを参照して](#)、パスワードをリセットできます。

**HA** ペアで、プライマリノードでパスワードを変更し、後で [ **Break HA pair** ] オプションを選択した場合、どのような動作になりますか

新しいパスワードを使用して、両方のスタンドアロンノードにログオンできます。

**2** 台のスタンドアロンサーバーでパスワードが異なる場合、これら **2** 台のサーバーを **HA** ペアで展開するとどのような影響がありますか

2 台のスタンドアロンサーバーを **HA** ペアに展開する場合は、両方のサーバーにデフォルトパスワードを設定することをお勧めします。

高可用性構成は完了しましたが、プライマリノードの **GUI** にはアクセスできません。理由は何でしょうか?

設定が有効になるまでに数分かかります。数分後にもう一度アクセスしてみることができます。

**HA** 設定は完了しましたが、フローティング IP アドレス **GUI** にはアクセスできません。理由は何でしょうか？

HA の設定が完了したら、まずプライマリノードの GUI にアクセスし、展開を完了する必要があります。詳細については、「[プライマリノードとセカンダリノードを高可用性ペアとしてデプロイする](#)」を参照してください。展開が完了すると、サーバは再起動し、高可用性展開の準備が整います。その後、フローティング IP アドレス GUI にアクセスできます。

**NetScaler ADM** スタンドアロンと **NetScaler ADM HA** ではどのデータベースがサポートされていますか？

NetScaler ADM スタンドアロンと NetScaler ADM HA はどちらも PostgreSQL をサポートしています。

セカンダリノードへの潜在的なデータ損失は何ですか？

セカンダリノードは、プライマリノードが NetScaler ADM データベースを介して送信するハートビートメッセージをリッスンします。セカンダリノードが 180 秒を超えてハートビートを受信しない場合、セカンダリノードはプライマリノードで SSH ベースのチェックを実行します。ハートビートと SSH ベースのチェックが失敗した場合、プライマリノードはダウンしていると見なされます。

このシナリオでは、セカンダリノードがプライマリノードを引き継ぎ、180 秒の時間枠は、セカンダリノードへのデータ損失の可能性と見なすことができます。

プライマリノードがダウンした場合はどうなりますか

セカンダリノードが引き継ぎ、プライマリノードになります。

障害が発生したノードを再インストールするにはどうすればいいですか

新しい VM ビルドをインストールすることが推奨されます。再インストールするには:

1. HA ペアを解除します。[システム]>[展開]に移動します  
配置ページが表示されます。**HA** ブレークをクリックします
2. Hypervisor から障害が発生したノードを削除します。
3. .XVA イメージファイルをハイパーバイザーにインポートします。
4. [コンソール] タブで、NetScaler ADM を初期ネットワーク構成で構成します。詳細については、「[1 番目のサーバー \(1 次ノード\) の登録と展開](#)」および「[2 番目のサーバー \(2 次ノード\) の登録と展開](#)」を参照してください。
5. **HA** ペアを再展開します。

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

NetScaler ADM VHD をローカルストレージでホストすることをお勧めします。SAN 内のストレージデバイスでホストされている場合、NetScaler ADM が期待どおりに動作しないことがあります。そのため、SAN への ADM の導入はサポートされていません。

**NetScaler ADM は余分なディスクをサポートしていますか**

はい。NetScaler ADM HA ペアの新規インストールでは、デフォルトで 120 GB のストレージが割り当てられます。120 GB を超えるストレージでは、最大 3 TB のストレージに 1 つのディスクを追加できます。複数のディスクの追加はサポートされていません。

**HA ペアを無効にすると、設定された Floating IP アドレスはどうなりますか**

フローティング IP アドレスにアクセスできなくなり、高可用性ペアを再デプロイする必要があります。

**再デプロイ中に別のフローティング IP アドレスを指定できますか？**

はい。新しい Floating IP アドレスを設定できます。

**セカンダリノードの GUI にアクセスできないのはなぜですか？**

セカンダリノードは読み取りレプリカサーバーであり、何らかの理由でプライマリノードがダウンした場合にのみプライマリノードとして機能します。プライマリノード GUI またはフローティング IP アドレス GUI にアクセスすることをお勧めします。

プライマリノードが長時間ダウンしている場合でも、フローティング IP アドレス GUI を使用して設定を行うことはできますか

はい。引き続き設定を行うことができ、設定はセカンダリノードに保存されます。プライマリノードが復帰すると、すべての構成が同期されます。

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

HA ペアの IP アドレスの変更は、HA ペアを壊さない限りサポートされません。

プライマリノードまたはセカンダリノードの IP アドレスを更新するには、次の手順を実行します。

1. HA ペアを解除します。[システム]>[展開]に移動します。

「配置」ページが表示されます。**HA** ブレークをクリックします

- a) SSH クライアントを使用するか、ハイパーバイザーからプライマリノードにログオンします。
- b) `nsrecover` をユーザー名として使用し、設定したパスワードを入力します。
- c) **networkconfig** と入力します。[最初のサーバ \(プライマリノード\) の登録と展開にあるステップ3](#)の手順を実行します。

初期ネットワーク構成では、別の IP アドレスを指定できます。

- d) セカンダリノードについても同じ手順を実行し、[2 番目のサーバ \(セカンダリノード\) の登録と展開にあるステップ3](#)の手順に進みます。

フローティング IP アドレスを更新するには:

1. [システム]>[展開]に移動します。

「配置」ページが表示されます。

- a) **HA** 設定をクリックします。
- b) [高可用性モードの **Floating IP** アドレスの設定] をクリックします。
- c) フローティング IP アドレスを入力し、[**OK**] をクリックします。

**ADM** は **AMD** プロセッサをサポートしていますか

なし ADM は、AMD プロセッサをサポートしていません。

導入 (災害復旧)

プライマリサイトとディザスタリカバリサイトの間でレプリケーションが行われる頻度はどれくらいですか

プライマリサイトとディザスタリカバリサイト間のレプリケーションはリアルタイムです。

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

いいえ。これで、DR サイトがプライマリサイトになります。HA ペアをプライマリサイトに戻すには、「[構成を元のプライマリサイトに戻す](#)」を参照してください。

**[Break HA pair]** オプションを選択すると、両方のノードがスタンドアロンサーバとして動作します。**DR** サポートはスタンドアロンサーバには適用されないため、ブレイク **HA** ペアを選択した場合、**DR** サイトはどうなりますか

[Break HA pair] オプションを選択すると、プライマリサイトと DR サイト間のレプリケーションが終了します。高可用性ペアの再展開の一環として DR サイトを再構成する必要があります。

## イベント管理

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

ネットワーク管理者は、NetScaler ADC インスタンスの構成変更、ログオン条件、ハードウェア障害、しきい値違反、エンティティ状態の変化などの詳細を、特定のインスタンスでのイベントとその重大度とともに表示できます。NetScaler ADM イベントダッシュボードを使用して、すべての NetScaler ADC インスタンスに関する重大なイベントの重大度の詳細について生成されたレポートを表示できます。

イベント規則とは何ですか

NetScaler ADM を使用して、特定のイベントを監視するルールを構成できます。イベントルールを使用すると、Citrix ADM インフラストラクチャ全体で生成される多数のイベントを簡単に監視できます。

特定の条件で規則を構成し、規則にアクションを割り当てることで、一連のイベントにフィルターを適用できます。生成されたイベントがルール内のフィルタ条件を満たすと、そのルールに関連付けられたアクションが実行されます。

フィルタを作成できる条件は、重大度、NetScaler ADC インスタンス、カテゴリ、および障害オブジェクトです。イベントに割り当てることができるアクションは、電子メール通知の送信、管理対象 NetScaler ADC インスタンスから NetScaler ADM への SNMP トラップの転送、SMS 通知の送信です。

## インスタンス管理

**NetScaler ADC** プール容量ライセンスを使用しているときに、帯域幅割り当て後に **ADC** インスタンスが **ADM** に接続できない場合はどうなりますか

ADC インスタンスと ADM 間のハートビートが失敗した場合、インスタンスは 30 日間の猶予期間に入ります。通信が再確立されると、プールされたキャパシティライセンスが機能し始めます。猶予期間内では、ADC 機能は影響を受けません。猶予期間が 30 日経過すると、ADC インスタンスはウォームリスタートを開始し、ライセンスは取得されません。

### NetScaler ADM のデータセンターとは何ですか？

NetScaler ADM データセンターは、特定の地理的場所にある NetScaler ADC インスタンスの論理グループです。各サーバーは、データセンター内の複数の NetScaler ADC インスタンスを監視および管理できます。Citrix ADM サーバーを使用して、管理対象インスタンスからの Syslog、アプリケーショントラフィックフロー、SNMP トラップなどのデータを管理できます。データセンターの構成の詳細については、「Citrix ADM でジオマップ用にデータセンターを構成する方法」を参照してください。

### NetScaler ADM でサポートされているさまざまな Citrix アプライアンスは何ですか？

インスタンスは、NetScaler ADM から検出、管理、監視する Citrix 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は NetScaler ADM サーバーに追加する必要があります。以下の Citrix アプライアンスと仮想アプライアンスを NetScaler ADM に追加できます。

- Citrix MPX
- Citrix VPX
- Citrix SDX
- Citrix CPX
- NetScaler Gateway
- Citrix SD-WAN WO
- Citrix SD-WAN PE

インスタンスは、NetScaler ADM サーバーの初回セットアップ時に追加することも、後で追加することもできます。

### インスタンスプロファイルとは何ですか？

インスタンスプロファイルは、NetScaler ADM がインスタンスにアクセスするために使用されます。

インスタンスプロファイルには、インスタンスにアクセスするためのユーザー名とパスワードが含まれています。インスタンスの種類ごとにデフォルトのプロファイルが用意されています。たとえば、ns-root-profile は、NetScaler ADC インスタンスのデフォルトプロファイルです。これには、デフォルトの NetScaler ADC 管理者資格情報が含まれています。インスタンスへのアクセスに必要な資格情報を変更する場合は、それらのインスタンスのカスタムのインスタンスプロファイルを定義できます。

### NetScaler ADM に無制限の SD-WAN インスタンスを追加できますか？ NetScaler ADM は、SD-WAN のすべてのスカラーおよびベクトルカウンターを処理できますか

現在、NetScaler ADM に追加できる SD-WAN インスタンスにはライセンス制限はありません。NetScaler ADM には、スカラーカウンターとベクトルカウンターの両方を内部的にポーリングする一連の組み込みレポートがあります。

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

はい。NetScaler ADM で複数の Citrix VPX インスタンスを再検出して、インスタンスの最新の状態と構成を確認することができます。

[ネットワーク] > [インスタンス] > [NetScaler ADC] > [VPX] の順に選択し、再検出するインスタンスを選択し、[操作] リストで [再検出] をクリックします。詳細については、「[複数の VPX インスタンスを再検出する方法](#)」を参照してください。

### NetScaler ADM を Citrix の SDX にインストールすることはできますか？

いいえ

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

はい、ネットワークアドレス変換 (NAT) を使用できます。

- 単一インスタンスを追加する場合:ADC インスタンスのパブリック IP アドレスの NAT IP を使用します。
- ADC HA ペアを追加するには、HA ペアの NAT IP アドレスを次の形式で追加します。

<NAT **public** IP of the primary instance>#<NAT **public** IP of the secondary instance>

- ADC クラスタを追加するには、クラスタ内のすべてのインスタンスのすべての NAT パブリック IP アドレスをそれぞれカンマで区切って追加し、括弧または丸括弧内に CLUSTER IP の NAT IP を追加します。フォーマットの例: NAT1、NAT2、NAT3、(クラスタ IP の NATIP)。

詳しくは、次のトピックを参照してください:

- [NetScaler ADM へのインスタンスの追加](#)
- [ネットワークアドレス変換の構成](#)

**DR** ノードの認証情報が変更された場合に、ディザスタリカバリノードを登録する方法を教えてください

次のコマンドを使用して、災害復旧 (DR) ノードの資格情報を `nsrecover/nsroot` にリセットします。

```
1 ./mps/change_freebsd_password.sh <username> <password>
2 <!--NeedCopy-->
```

DR ノードを登録するには、[DR コンソール](#)を使用して NetScaler ADM DR ノードを展開および登録するの順に従います。



## StyleBook

**StyleBooks** を使用して、異なるバージョンの **NetScaler ADC** ソフトウェアで実行する異なる **NetScaler ADC** インスタンスを構成できますか

はい。異なるバージョンのコマンド間に矛盾がない場合は、**StyleBooks** を使用して、異なるバージョンで実行する異なる **NetScaler ADC** インスタンスを構成できます。

**StyleBook** を使用して複数の **NetScaler ADC** インスタンスを同時に構成し、**1** つの **NetScaler ADC** インスタンスの構成に失敗した場合、どうなりますか？

**NetScaler ADC** インスタンスへの構成の適用に失敗すると、構成はこれ以上インスタンスに適用されず、すでに適用されている構成がロールバックされます。

**NetScaler ADC** を介して作成された **NetScaler ADC** バックアップには、**StyleBooks** を通じて適用された構成が含まれていますか

はい

## システム管理

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

はい。ホスト名を割り当てて、**NetScaler ADM** サーバーを識別できます。ホスト名を割り当てるには、**[System]** > **[System Administration]** > **[System Settings]** の順に選択し、**[Change Hostname]** をクリックします。

ホスト名は、**NetScaler ADM** のユニバーサルライセンスに表示されます。詳しくは、「[NetScaler ADM サーバーにホスト名を割り当てる方法](#)」を参照してください。

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

はい。設定ファイル (NTP ファイルと SSL 証明書)、システムデータ、インフラストラクチャとアプリケーションデータ、すべての **SNMP** 設定をバックアップできます。**NetScaler ADM** が不安定になった場合は、バックアップファイルを使用して **NetScaler ADM** を安定した状態に復元できます。

**NetScaler ADM** 構成をバックアップおよび復元するには、**[システム]** > **[詳細設定]** > **[バックアップファイル]** の順に選択し、**[バックアップ]** または **[復元]** をクリックします。詳しくは、「[NetScaler ADM で構成をバックアップおよび復元する方法](#)」を参照してください。

この機能は、アップグレードの実行前に、または予防手段として使用することをお勧めします。

### NetScaler ADM のしきい値とアラートとは何ですか？

しきい値とアラートを設定して、NetScaler ADC インスタンスの状態を監視し、管理対象インスタンスのエントリを監視できます。

カウンターの値がしきい値を超えると、NetScaler ADM はパフォーマンス関連の問題を示すアラートを生成します。カウンターの値がしきい値で指定されているクリア値に戻るとイベントは消去されます。

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

はい。問題のデバッグについてテクニカルサポートに連絡する前に、NetScaler ADM のデータと統計のアーカイブを生成することをお勧めします。テクニカルサポートチームに送信できるアーカイブは、TAR ファイルです。

NetScaler ADM データベースからデバッグログ、デバッグログが収集された期間、および異なる多様なログを含むテクニカルサポートファイルを生成できます。

テクニカルサポートファイルを構成して送信するには、[システム] > [診断] > [テクニカルサポート] の順に選択し、[テクニカルサポートファイルの生成] をクリックします。詳しくは、「[NetScaler ADM のテクニカルサポートファイルを生成する方法](#)」を参照してください。

### Syslog のページとは何ですか

Syslog は、ログ記録用の標準プロトコルです。Syslog によって、情報を生成するシステムと、情報を保存するシステムを分離できます。ログ情報を統合して、集められたデータから詳細な情報を得られます。Syslog を構成して、さまざまな種類のイベントをログ記録することもできます。

データベースに保存される Syslog データの量を制限するために、Syslog データをページする間隔を指定できます。すべての汎用 Syslog データ、AppFirewall データ、および Citrix Gateway データが Citrix ADM から削除されるまでの日数を指定できます。

### NetScaler ADM で NTP サーバーを構成できますか？

NetScaler ADM ネットワークタイムプロトコル (NTP) サーバーを構成して、NetScaler ADM 時計を NTP サーバーと同期させることができます。NTP サーバーを構成すると、NetScaler ADM クロックは、ネットワーク上の他のサーバーと同じ日付と時刻の設定になります。

NTP サーバーを設定するには、[システム] > [NTP サーバー] に移動し、[追加] をクリックします。詳しくは、「[NetScaler ADM で NTP サーバーを構成する方法](#)」を参照してください。

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

NetScaler ADM アクティブ/パッシブ HA 展開モードは、NetScaler ADM バージョン 12.0 ビルド 51.24 からサポートされています。

**NetScaler ADM** アクティブ-アクティブ **HA** セットアップを行い、統合 **GUI** アクセス用に負荷分散仮想サーバーを備えた **NetScaler ADC** アプライアンスを構成しました。この構成をどうすればアップグレードできますか

NetScaler ADM HA ペアをアクティブ/パッシブモードにアップグレードした後、NetScaler ADC アプライアンスで次のコマンドを実行して、負荷分散構成を更新する必要があります。

```
lb モニターを追加 MAS_Monitor TCP-ECV-送信「GET /mas_health HTTP/1.1\r\n 受け入れエンコーディング: アイデンティティ\r\n ユーザーエージェント: NetScaler-Monitor\r\n 接続: 閉じる\r\n\r\n” -recv “{”ステータスコード” : 0, “is_passive” : 0} -LRTM DISABLED
```

ポート **443** を使用して **NetScaler ADC** インスタンスで **NetScaler ADM HA** ペアの負荷分散を構成できますか

いいえ。ポート 443 を使用して NetScaler ADC インスタンス上で NetScaler ADM HA ペアの負荷分散を構成することはできません。

NetScaler ADC で `http-ecv` および `https-ecv` モニタを構成すると、NetScaler ADM HA ノードが正しく監視されません。

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

はい

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

はい。Citrix ADM バックアップファイルをダウンロードし、別の Citrix ADC インスタンスのバックアップリポジトリにアップロードして、そのインスタンスを復元します。ネットワーク情報と認証情報が競合しないようにしてください。たとえば、IP アドレスやポートの競合、パスワードプロファイルの不一致をチェックします。また、復元された VPX インスタンスに、バックアップされた NSIP アドレスと NetScaler ADC ライセンスが同じであることを確認してください。

高可用性ペアのインスタンスを復元する前に、バックアップファイルに保存されている IP アドレスと状態 (プライマリまたはセカンダリ) が元の HA 構成の IP アドレスと状態 (プライマリまたはセカンダリ) と一致していることを確認してください。また、新しいプライマリとセカンダリに同じ種類の NetScaler ADC ライセンスがあることも確認します。

**Citrix ADM** サーバーの **NSIP** アドレスを使用する代わりに、**Citrix ADM** に **SNIP** アドレスを使用して **Citrix ADC** インスタンスと通信するように強制することはできますか？

はい。NetScaler ADC Citrix ADC インスタンスと通信するために、NetScaler ADM に SNIP アドレス（管理が有効になっている場合）を追加できます。

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

NetScaler ADM による NetScaler ADC インスタンスのバックアップは完全バックアップです。

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

はい。 <https://support.citrix.com/article/CTX224502> を参照してください。

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

ハートビートと SSH ベースのチェックが失敗した場合、プライマリノードはダウンしていると見なされ、セカンダリノードがプライマリノードとして引き継ぎます。デフォルトでは、すべての NetScaler ADC インスタンスは、SNMP トラップ宛先として最新のプライマリノードの詳細で更新されます。

新しいプライマリ（アクティブ）NetScaler ADM ノードは、以前にアクティブだったノードが AppFlow コレクターまたは Syslog サーバーとして構成されているかどうかを調べます。構成されている場合は、新しいプライマリによって、AppFlow コレクターまたは Syslog サーバーの詳細がインスタンスに送信される情報に追加されます。

syslog の場合、古いサーバの詳細が置き換えられます。

ダウンした **NetScaler ADM HA** ノードが復旧するとどうなりますか

サービスに戻った後、アクティブノードがフェイルオーバーしない限り、NetScaler ADM ノードはパッシブなままです

**NetScaler ADC** インスタンスは、**NetScaler ADM HA** ノード間でどのように分散されていますか

すべての NetScaler ADC インスタンスは、プライマリ NetScaler ADM ノードによって管理されます。

**NetScaler ADM HA** フェールオーバーがある場合、仮想サーバーライセンスはどのように管理されますか

仮想サーバーライセンスを適用する NetScaler ADM プライマリノードがダウンした場合、新しいプライマリノードは 30 日間の猶予期間仮想サーバーライセンスを管理します。猶予期間が終了する前に、新しいプライマリでライセンスを再適用します。別の方法については、Citrix サポートにお問い合わせください。

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

いいえ。ただし、ロードバランサーがない場合は、NetScaler ADM ノードには独自の IP アドレスを使用してアクセスする必要があります。パッシブノードには「パッシブ」というタグが付いています。パッシブノードには構成を作成しないことをお勧めします。

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

いいえ

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

はい

**NetScaler ADM HA** ノード間で同期されるデータは何ですか

NetScaler ADM データベース全体が同期され、次のフォルダーが同期されます。

- /var/mps/テナント/ルート/
- /var/mps/ns\_images/
- /var/mps/sdx\_images/
- /var/mps/xen\_nsvpx\_images/
- /var/mps/cbwanopt\_images/
- /var/mps/sdwanvw\_images/
- /var/mps/mps\_images/
- /var/mps/ssl\_certs/
- /var/mps/ssl\_keys/
- /mpsconfig/ssl/
- /var/mps/backup/
- /var/mps/esx\_nsvpx\_images/
- /var/mps/locdb/



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).

---