NetScaler Application Delivery Management 14.1

Machine translated content

Disclaimer

Contents

リリースノート

February 6, 2024

NetScaler Application Delivery Management（ADM）14.1 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。14.1 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。

> 注
>
> これらのリリースノートには、セキュリティ関連の修正は記載されていません。セキュリティ関連の修正と勧告のリストについては、セキュリティ速報を参照してください。

NetScaler ADM 14.1-12.34 ビルドのリリースノート

February 6, 2024

このリリースノートでは、NetScaler ADM リリース Build 14.1-12.34 の拡張機能や変更、修正された問題、既知の問題について説明します。

メモ

- このリリースノートには、セキュリティ関連の修正は含まれていません。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。
- ビルド 14.1-12.34 がビルド 14.1-12.30 に取って代わります。
- ビルド 14.1-12.34 には、新機能 NSADM-98483 と既知の問題である NSADM-106497 のほか、ビルド 14.1-12.30 で利用できるすべての拡張機能とバグ修正が含まれています。

新機能

ビルド 14.1-12.34 で利用できる機能強化と変更点

ライセンス

NetScaler フレックスライセンス　NetScaler Flexed ライセンスは、ライセンス管理プロセスを簡素化することを目的とした新しいライセンスフレームワークです。フレックスライセンスには、ソフトウェアインスタンスライセンス（VPX/CPX/BLX、SDX、MPX、VPX FIPS）と帯域幅容量ライセンスが含まれます。フレックスライセンスは、NetScaler コンソールサービスまたはオンプレミスの NetScaler ADM で適用する必要があります。また、MPX Z-Cap ライセンスと SDX Z-Cap ライセンスを、それぞれ NetScaler MPX ハードウェアと NetScaler SDX ハードウェアに適用する必要があります。その後、クラウドまたはオンプレミスに展開されているすべての NetScaler フォームファクターにそれらを割り当てることができます。

詳しくは、「
フレックスライセンス」を参照してください。

フレックスライセンスは、NetScaler ADM オンプレミス 14.1 および 13.1 リリースで正式にサポートされています。リリース ADM オンプレミス 14.1-12.x 以降では、分析用に無制限の ADM VIP がバンドルされており、Flexed ダッシュボード UI（**NetScaler** ライセンス **> Flexed Licensing**）から **Flexed** ライセンスを管理できます。

14.1-12.x より前の ADM オンプレミスリリース 13.1 および 14.1 ビルドでは、フレックスライセンスを適用すると、ADM はそれらをプールライセンスと同じように扱い、プールダッシュボード UI（インフラストラクチャ **>** プールライセンス）に詳細を表示します。これらのリリースでは、分析用の無制限の ADM VIP のバンドル利用はできません。

Flexed GUI を紹介し、バンドルエンタイトルメントを提供する製品エクスペリエンスを向上させるには、オンプレミスの ADM をリリース 14.1-12.x 以降にアップグレードすることをお勧めします。

> 注:
>
> 現在のFlexed ライセンス要件に準拠するには、ADM オンプレミスの Cloud Connector を有効にしてください。この機能は、オンプレミスの ADM を ADM サービスに接続してテレメトリを収集します。Flexed ライセンスを使用している場合は、テレメトリ収集を有効にすることをお勧めします。ADM オンプレミ Cloud Connector を有効にするには、「ADM オンプレミ Cloud Connector」を参照してください。

[NSADM-98483]

分析

アプリケーション・キー・メトリクスの異常検出　管理者は、優先順位付けとトラブルシューティングに役立つ洞察を得るために、アプリケーションが効率的に管理されていることを確認する必要があります。シナリオによっては、特定の期間に発生する可能性のある異常なアプリケーションパフォーマンスの偏差を表示して分析したい場合もあります。

App Dashboard では、アプリケーションを選択すると、「**Key Metrics** 」タブにアプリケーションの使用状況が表示されます。NetScaler ADM はトラフィックパターンを監視し、主要なメトリックが予想される範囲内にあるかどうかを分析します。予想範囲から逸脱した場合に、以下の主要指標の異常を表示できるようになりました:

- 応答時間
- スループット
- データ量
- 1 秒あたりのリクエスト数

詳細については、「アプリケーションの使用状況と異常」を参照してください

[NSADM-97531]

選択したインスタンスからのみ **Splunk** と **New Relic** にデータをエクスポートする　Splunk と New Relic にデータをエクスポートするサブスクリプションを作成するときに、インスタンスを選択できるようになりました。特定のインスタンスでサブスクリプションを作成した場合、データは選択したインスタンスからのみ Splunk と New Relic にエクスポートされます。

詳細については、「Splunk との統合 」および「New Relic との統合」を参照してください。

[NSADM-94371]

実行可能なタスクと推奨事項　タスク機能に次の拡張機能が追加されました:

- 新しい [タスク] タブが導入されました。このタブでは、すぐに対処する必要のあるアクション可能なタスクを表示できます。これらのタスクは、現在の使用状況に基づいて表示されます。管理者は、これらの実行可能なタスクを完了することで、NetScaler の導入環境が安全で、コンプライアンスに準拠し、効率的であることを保証します。これらの実行可能なタスクは、問題の重大度（重大および中）に基づいています。
- 「**To Do**」タブの名前が「推奨事項」に変更されました。レコメンデーションでは、引き続き既存のタスクを確認し、「ガイドする」をクリックしてタスクを完了できます。
- [アーカイブ] タブは使用できなくなりました。代わりに、リストからレコメンデーションを却下することもできます。

詳細については、「実行可能なタスクと推奨事項」を参照してください。

[NSADM-91870]

インフラストラクチャ

証明書ストアを使用して **SSL** 証明書を更新する　[インフラストラクチャ**] > [SSL** ダッシュボード**] > [**更新**]** で **SSL** 証明書を更新するときに、証明書ストアから証明書を選択できるようになりました。以前は、SSL 証明書を更新するには、証明書ファイルとキーファイルをアップロードする必要がありました。

詳細については、「インストールされた証明書を更新する方法」を参照してください。

[NSADM-101303]

セキュリティアドバイザリでのスキャンログのサポート　セキュリティアドバイザリで、スキャンログと呼ばれる新しいオプションを表示できるようになりました。スキャンログを使用すると、次のことができます。

- 直近の 5 回の CVE スキャンのレポートを表示します。レポートには、デフォルトのシステムスキャンとユーザーが開始するオンデマンドスキャンの両方が含まれます。
- 各スキャンのレポートを CSV および PDF 形式でダウンロードします。
- 現在進行中のオンデマンドスキャンの状態を表示します。

詳細については、「セキュリティアドバイザリ」を参照してください。

[ナダム-10142]

SNMP トラップのリストが更新されました　SNMP トラップのリストは、新しいトラップと以前に存在しなかったトラップで更新されました。完全なリストを表示するには、[インフラストラクチャ**] > [**イベント**] > [**イベント設定**] > [NetScaler**] に移動します。

[NSADM-99798]

HA 展開におけるデータベースのカスタム証明書と暗号の管理　NetScaler ADM では、デフォルトの組み込みデータベース証明書を、信頼できる認証局からの独自の証明書に置き換えることができるようになりました。ADM データベース用に独自の暗号スイートを設定することもできます。この機能を使用するには、[設定**] > [HA** 展開**] > [**データベース証明書] に移動します。

詳細については、「高可用性展開におけるデータベースのカスタム証明書と暗号の管理」を参照してください。

[NSADM-96583]

オンプレミスの **ADM** と **ADM** サービス間のサブスクリプションライセンス情報の共有　ADM オンプレミスサーバーは、ADM オンプレミ Cloud Connector を介して NetScaler サブスクリプションライセンス情報を ADM サービスに送信するようになりました。

[NSADM-93820]

オンプレミスの **ADM** と **ADM** サービス間のプールライセンス情報の共有　ADM オンプレミスサーバーは、NetScaler プールライセンス情報を ADM オンプレミス Cloud Connector を介して ADM サービスに送信するようになりました。

[NSADM-93812]

[セキュリティ**]**

統合セキュリティダッシュボード　NetScaler ADM では、単一ペインのダッシュボードを使用して保護の設定、分析の有効化、アプリケーションへの展開が可能になりました。[セキュリティ] **> [**セキュリティダッシュボード] に移

動し、[アプリケーションの管理] をクリックして次の操作を行います:

- セキュリティで保護されたアプリケーションとセキュリティで保護されていないアプリケーションをすべて表示します。
- セキュリティで保護されていないアプリケーションを選択し、さまざまなテンプレートオプションから保護を設定し、保護の分析を有効にして、アプリケーションにデプロイしてアプリケーションを保護します。

以前は、NetScaler インスタンスですべての保護を構成する必要があり、NetScaler ADM では、構成された保護の分析のみを表示できました。管理者は、この単一ペインのダッシュボードにより、単一のワークフローでアプリケーションの保護を設定できます。

詳細については、「統合セキュリティダッシュボード」を参照してください。

[NSADM-92678]

StyleBook

StyleBook の **NetScaler ADM** 証明書ストアにある証明書を使用する　NetScaler ADM 証明書ストアの証明書を使用するように StyleBook を定義できるようになりました。構成パックを作成するときに、証明書ストアに既に存在する証明書を選択するか、新しい証明書を証明書ストアに追加できます。

詳しくは、「StyleBooks を使用して証明書ストアから SSL 証明書を管理する」を参照してください。

[NSADM-101515]

StyleBook でドロップダウンメニューを定義する　NetScaler ADM では、StyleBook 定義の「パラメータ-条件」にドロップダウンメニューを定義できるようになりました。

詳細については、「パラメーター条件」を参照してください。

[NSADM-99543]

StyleBook と構成パックのサポートバンドルをダウンロードする　構成パックや StyleBook の操作をトラブルシューティングするためのサポートバンドルをダウンロードできるようになりました。StyleBooks のサポートチケットを開くときに、これらのサポートバンドルを NetScaler チームと共有できます。サポートバンドルをダウンロードするには、[アプリケーション] **>** [構成] **>** [構成パック] **>** [サポートバンドル] に移動します。

詳細については、「サポートバンドルのダウンロード」を参照してください。

[NSADM-97838]

StyleBooks の仮想サーバーの状態と **ARP** ステータスを変更する　[アプリケーション] **>** [構成] **>** [構成パック] **>** [**NetScaler** 構成の移行] で、新しい **NetScaler** に移行された仮想サーバーの状態（有効/無効）と ARP ステータスを表示および編集できるようになりました。

詳しくは、「NetScaler アプリケーション構成を移行するための StyleBook の作成」を参照してください。

[NSADM-97827]

構成パックなしで構成を移行　NetScaler ADM では、NetScaler ADM で構成パックを作成せずに、NetScaler 間でアプリケーション構成を移行するオプションが提供されるようになりました。デフォルトでは、移行によって ADM に設定パックが作成され、StyleBooks による構成の詳細な管理に使用されます。アプリケーション構成をある NetScaler から別の NetScaler にのみ移行し、後で StyleBooks で管理しない場合は、移行中に [アプリケーション**] > [** 構成] > [**構成パック**] > [NetScaler** 構成の移行**] > [**移行**]** で **[ADM** による構成の管理 **] チェックボックスをオフにします。

詳しくは、「StyleBooks 構成ビルダーを使用した NetScaler アプリケーション構成の移行」を参照してください。

[NSADM-97802]

解決された問題

ビルド 14.1-12.34 で対処されている問題。

分析

- NetScaler ADM エージェントは、アップグレード後にクラッシュしてコアダンプファイルを生成することがあります。

  [NSHELP-36428]

インフラストラクチャ

- 特定の条件下では、一部のユーザーグループに適用された正規表現の設定が失われる可能性があります。

  [ナダム-104565]

- [インフラストラクチャ**] > [**インスタンスアドバイザリ**] > [**セキュリティアドバイザリ] で、**CVE** のある脆弱な **NetScaler** インスタンスを選択して **[**アップグレードワークフローに進む] をクリックすると、次のエラーメッセージが表示されます:

  「選択した NetScaler インスタンスには、この修復ワークフローは必要ありません」

  [NSADM-103649]

- [インフラストラクチャ] **>** [イベント] **>** [イベントメッセージ] では、NetScaler ADM は、NetScaler CPU 使用率トラップがパケット CPU 用か管理 CPU 用かを表示しません。

  [NSADM-103391]

- NetScaler ADM を Kubernetes クラスターにインストールすると、インフラストラクチャ分析、イベント、****Syslog** イベント、****** データストレージ管理などの特定のページが **NetScaler**ADM GUI に表示されないことがあります。

  [NSADM-103180]

- NetScaler ADM のスクロール可能なページのレポートをエクスポートすると、エクスポートされたレポートでは、表示されているウィンドウの高さを超えるコンテンツが切り捨てられることがあります。

  [NSADM-102765]

- 大規模デプロイメントでは、mas_service サブシステムのクラッシュが発生しています。

  この問題は、RBAC 権限があり、[設定] > [ユーザーとロール**] > [**グループ**] > [**認証設定**]** で次の構成になっているグループに属している場合に発生します。

  - 特定のインスタンスが **[**インスタンス**]** で選択されている
  - 「アプリケーション」で「すべてのアプリケーション **」が選択されています

  [NSADM-99873]

- ルート管理者として、デフォルトの資格情報を使用して NetScaler ADM GUI または API に初めてログオンすると、デフォルトのパスワードを変更するように求められます。

  [NSADM-95328]

管理とモニタリング

- RBAC ユーザーが NetScaler ADM に NITRO API リクエストを送信して NetScaler サーバーのリストを取得しようとすると、応答には使用可能なサーバーがゼロであることが誤って示されます。ただし、NetScaler ADM GUI（[インフラストラクチャ］**>**［ネットワーク機能］**>**［負荷分散］**>**［サーバー]）に移動すると、そのユーザーにリンクされているすべての NetScaler サーバーが表示されます。

  [NSHELP-36645]

- **[**設定**] > [**バックアップファイル**] > [**復元**]** の **NetScaler ADM** 復元操作が断続的に完了しない。

  [NSHELP-36527]

- NetScaler ADM は特定のコアファイルの圧縮に失敗するため、ディスク容量の消費が増加します。

  [NSHELP-36434]

- 管理者がすべてのアプリケーションにアクセスできるグループを作成し、そのグループに属するユーザーが [インフラストラクチャ**] > [**ネットワーク機能**] > [**負荷分散**] > [**サーバー] ページにアクセスしようとすると、NetScaler ADM GUI にアクセスできなくなります。

  [NSHELP-36426]

- NetScaler ADM HA セットアップのプライマリノードとセカンダリノード間のファイルの同期中に、インベントリサブシステムが断続的にクラッシュします。

  [NSHELP-36357]

- NetScaler の組み込みエージェントでは、イベントの経過時間が [インフラストラクチャ**] > [**イベント**] > [**ルール**] > [**追加**]** で設定された期間を超えても、イベントアラートまたはメッセージは生成されません

  [NSHELP-35706]

- **[** インフラストラクチャ**] > [**インスタンス**] > [NetScaler] > [SDX] > [**アクションの選択**] > [VPX** のプロビジョニング**]** で SDX に VPX インスタンスをプロビジョニングすると、**[**ネットワーク経由で管理**]** オプションが表示されません。

  [NSHELP-36328]

StyleBook

- NetScaler ADM StyleBook のログファイルは、ファイルサイズの制限を超えても自動的に圧縮されないため、ディスク容量の消費量が増加します。

  [NSHELP-36680]

- パラメーターに特殊文字を含む構成パックが更新または削除されると、NetScaler ADM は NetScaler での更新または削除操作が不完全であっても成功メッセージを表示します。今回の修正により、NetScaler ADM は、構成パック定義の特殊文字が原因で発生した不完全な構成のエラーを正確に表示するようになりました。

  [NSADM-104423]

既知の問題

リリース 14.1-12.34 に存在する問題。

分析

- [アプリケーション**] > [**ダッシュボード] で、NetScaler HA ペアでホストされているアプリケーションをクリックすると、アプリケーション詳細ページの [パフォーマンス] タブに [すべてのサービス] にデータが表示されません。

  回避策：ページを更新するか、アプリケーション詳細ページ内の別のタブに移動してから、[パフォーマンス] タブに戻って、負荷分散仮想サーバーに関連するサービスを表示します。

  [NSADM-105613]

インフラストラクチャ

- フレックスライセンスダッシュボードには、プレミアム帯域幅ライセンスプールから少なくとも 1 つの NetScaler がチェックアウトされた後にのみ NetScaler の詳細が表示されます。

  [ナダム-106497]

- NetScaler ADM for VMware ESXi からライセンスを削除すると、**[**設定**] > [**ライセンスと分析の構成**]** のライセンス数に、更新された数がすぐに反映されない場合があります。

  [NSADM-105851]

- 差分レポートは、[インフラストラクチャ**] > [**アップグレードジョブ**] > [**差分レポート] のアップグレードジョブでは生成されません。

  [ナダム-10677]

- 新しい NetScaler ADM を構成すると、次のエラーメッセージが表示される場合があります。「操作中にエラーが発生しました-メトリックが見つかりません。」

  この問題は、自動データ消去ジョブがまだ実行されておらず、データが存在しないために発生します。ジョブは 3 時間実行するようにスケジュールされており、実行後に必要なデータが生成され、エラーメッセージは表示されなくなります。

  [NSADM-103157]

- NetScaler BLX インスタンスに証明書をインストールしようとすると、インストールが失敗し、［インフラストラクチャ］**>**［**SSL** ダッシュボード］**>**［**SSL** 監査ログ］ページに次のエラーメッセージが表示されます:

  「SCP: IP アドレスでパスワードによる認証が失敗します。」

  [NSADM-102202]

- いずれかのパスワードに「#」記号が付いている場合、NetScaler エージェントは NetScaler ADM に登録されません。

  [NSADM-100613]

ライセンス

- Flexed ライセンスまたは Pooled ライセンスを適用しても、**Analytics** 設定ページ ([設定**] > [Analytics** 設定]) は正しい情報で更新されません。

  回避策: ページを更新して正しい詳細情報を確認してください。

  [NSADM-106665]

- ［**NetScaler** ライセンス］**>**［フレックスライセンス］**>**［ダッシュボード］のフレックスライセンスダッシュボードが空白で表示されます。

回避策: プレミアム帯域幅ライセンスを適用してください。

[NSADM-106561]

管理とモニタリング

- NetScaler ADM エージェントは「NetScaler ログイン失敗」SNMP トラップを生成します。この問題は、ADM エージェントが NetScaler へのログインに使用する資格情報が改行文字が原因で切り捨てられるために発生します。

  [NSHELP-36804]

- ADM HA ペアでは、GUI の Sync Database オプションを何回か試しても、データベースステータスがダウン状態で、同期していないことが確認されました。

  [NSHELP-29626]

NetScaler ADM 14.1—8.50 リリースのリリースノート

February 6, 2024

このリリースノートドキュメントでは、NetScaler ADM リリースビルド 14.1～8.50 の機能強化と変更、修正された問題と既知の問題について説明します。

メモ

- このリリースノートには、セキュリティ関連の修正は含まれていません。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。

新機能

ビルド 14.1—8.50 で利用できる機能強化と変更。

管理とモニタリング

CVE-2023-4966 と **CVE-2023-4967** の特定と是正のサポート

> 注:
>
> CVE-2023-4966 と CVE-2023-4967 の詳細は、ADM オンプレミ Cloud Connector を通じてセキュリティア

> ドバイザリを有効にしている場合にのみ表示できます。詳細については、「ADM オンプレミ CloudConnector」を参照してください

NetScaler ADM セキュリティアドバイザリは、CVE-2023-4966 と CVE-2023-4967 の識別と修復をサポートするようになりました。

- 識別には、バージョンスキャンと構成スキャンの組み合わせが必要です。
- 修正するには、脆弱な NetScaler インスタンスを、修正された推奨ビルドにアップグレードする必要があります。

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

NetScaler ADM を使用して NetScaler インスタンスをアップグレードする方法について詳しくは、「ジョブを使用して NetScaler インスタンスをアップグレードする」を参照してください。

詳細については、「セキュリティ情報」を参照してください。

[NSADM-101092]

分析

StyleBook を介した **NetScaler** から **Prometheus** へのメトリックのエクスポートの設定のサポート NetScaler から Prometheus にメトリックをエクスポートするには、NetScaler で分析プロファイルを作成し、スキーマファイルを指定する必要があります。詳しくは、「Prometheus による NetScaler、アプリケーション、およびアプリケーションセキュリティの監視」を参照してください。

[アプリケーション] **> [**構成] **> [StyleBook] > [**デフォルト **StyleBook **]** で、****Prometheus TimeSeries Analytics** 構成 **StyleBook** を使用して、すべての管理対象インスタンスに対して構成を実行できるようになりました。

詳細については、「Prometheusアナリティクス StyleBook 」を参照してください。

[NSADM-97698]

アプリケーション遅延の根本原因を表示する　アプリケーションの遅さは、ビジネスへの影響や生産性につながるため、あらゆる組織にとって大きな懸念事項です。[アプリケーション] **> [Web Insight**] に、「応答時間異常のあるアプリケーション」という新しい指標が表示されるようになりました。このメトリックを使用すると、管理者はアプリケーションの遅延が以下の原因で発生しているかどうかを分析できます。

- クライアントネットワーク遅延
- サーバーネットワークの待ち時間
- サーバー処理時間

詳細については、「アプリケーション遅延の根本原因の表示」を参照してください。

[NSADM-97530]

構成ジョブ**-NetScaler** から **Prometheus** へのメトリックのエクスポートを構成するためのジョブの作成をサポート　NetScaler から Prometheus にメトリックをエクスポートするには、NetScaler で分析プロファイルを作成し、スキーマファイルを指定する必要があります。詳しくは、「Prometheus による NetScaler、アプリケーション、およびアプリケーションセキュリティの監視」を参照してください。

設定ジョブでは、**** 組み込みテンプレートの **NSConfigurePrometheusAnalyticsProfile** テンプレートを使用してジョブを作成し **、必要なパラメータを指定して、すべての管理対象インスタンスに対してジョブを実行できるようになりました。

詳細については、「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」を参照してください。

[NSADM-97251]

NetScaler ADM から管理対象ネットスケーラーのネットプロファイルを割り当てます　NetScaler ADM で仮想サーバーの分析を有効にすると、NetScaler からの AppFlow データが NetScaler サブネット IP アドレス（SNIP）を介して NetScaler ADM にエクスポートされます。シナリオによっては、ネットワーク内のファイアウォールが原因で SNIP がブロックされることがあります。このようなシナリオでは、SNIP とは異なる IP アドレスを使用する必要がある場合があります。ネットプロファイルの詳細については、「指定されたソース IP をバックエンド通信に使用する」を参照してください。

NetScaler ADM を使用してネットプロファイルを NetScaler インスタンスに割り当てることができるようになりました。［インフラストラクチャ］**>**［インスタンス］**>**［**NetScaler ADC**］に移動してインスタンスを選択し、［アクションの選択］リストから［ネットプロファイルの設定］をクリックしてインスタンスにネットプロファイルを割り当てます。

> 注:
>
> インスタンスにネットプロファイルを割り当てる前に、すべての仮想サーバーで分析を無効にしていることを確認してください。

この機能強化により、NetScaler から NetScaler ADM に AppFlow データをエクスポートするためのネットプロファイルを割り当てることができます。

[NSADM-91836]

インフラストラクチャ

アップグレード失敗シナリオの改善　アップグレードジョブ (**[**インフラストラクチャ**] > [**アップグレードジョブ]) が失敗すると、ビルドファイルやその他の抽出されたファイルが存在するため、失敗したジョブによってディスクスペースの問題が発生します。その結果、次のアップグレードジョブも失敗します。

アップグレードジョブの失敗シナリオが改善されました。アップグレードジョブが失敗した場合、NetScaler ADM は NetScaler インスタンスから古いビルドファイルを削除します。

[NSADM-97383]

リブランディングの変更　NetScaler ADM は NetScaler ADM にリブランドされました。新しいブランドに合わせて、ADM GUI も更新されました。

[NSADM-97365]

オンプレミスエージェントのアクセスポリシー　[設定**] > [**ユーザーと役割**] > **[**** アクセスポリシー] で ADM エージェントの編集アクセス権を持つアクセスポリシーを作成すると **、このポリシーに関連付けられているユーザーは、自分の認証情報を使用してエージェントを登録できるようになりました。

[NSADM-97337]

NetScaler ADM GUI で使用可能なデータストレージ管理ダッシュボード　設定 **>** データストレージ管理で、現在の環境内のさまざまな機能にわたるデータストレージ情報を表示および管理できるようになりました。データストレージ管理ダッシュボードは、機能全体のストレージ消費状況を視覚化し、ストレージ消費量が指定されたしきい値内かどうかを監視するのに役立ちます。

ダッシュボードには以下の機能があります:

- データ取り込み、ストレージ消費、アクションタイル: タイルには次の機能があります:
  - データ取り込みアクティビティのステータス
  - 消費したデータと利用可能な総ディスク容量に関する情報
  - データ保持ポリシーの見直し、データプルーニングの実行、システム通知の確認を行うオプション
- ストレージ消費トレンド: ある期間におけるさまざまな機能間でのデータの保存状況を視覚化できます
- 機能別のストレージ消費量:
  - さまざまな機能によるデータストレージの分布を表示します
  - データプルーンを実行したり、データプルーンの履歴を表示したり、各データプルーンで削除された機能を表示したりできます。

詳細については、「データストレージダッシュボードの使用」を参照してください。

[NSADM-97320]

NetScaler ADM での **SSL** 証明書ストアのサポート　インフラストラクチャ **> SSL** ダッシュボード **>** 証明書ストアで **SSL** 証明書を管理できるようになりました。

証明書ストアを使用して次のことを行います。

- 証明書の追加、更新、削除
- NetScaler インスタンスへの証明書のインストール
- NetScaler インスタンスから証明書をインポートする

詳細については、「証明書ストアの使用方法」を参照してください。

[NSADM-97257]

ユーザーセッションの制限が **40** に変更　**[設定] > [**ユーザーと役割**] > [**グループ] では、最大 40 のユーザーセッションを設定できます。デフォルトでは、20 のユーザーセッションが割り当てられます。ただし、管理者および読み取り専用ユーザーグループに属している場合、デフォルトで 40 ユーザーセッションが割り当てられ、この値は変更できません。

[NSADM-95314]

失敗したアップグレードジョブを再試行　[インフラストラクチャ**] > [**アップグレードジョブ] で、失敗したアップグレードジョブを選択し、次のいずれかのアクションを実行できるようになりました。

- 失敗したアップグレードジョブの横にある **[**再試行] をクリックします。
- 「アクションの選択」**>**「アップグレードジョブの再試行」に進みます

詳細については、「失敗したアップグレードジョブを再試行する」を参照してください。

[NSADM-93439]

ADM オンプレミ **Cloud Connector**　Cloud Connector 機能を使用して、ADM オンプレミスと ADM サービス間の接続を確立できます。この接続により、ADM On-Prem のセキュリティアドバイザリ機能を活用できます。セキュリティアドバイザリを利用すると、新しい一般的な脆弱性と露出 (CVE) を追跡し、CVE の影響を評価し、修復方法を理解し、脆弱性を解決することができます。管理者は、定期スキャンまたは手動スキャンによって NetScaler インスタンスに新しい CVE がないか監視し、修正に必要なアクションを実行できます。

詳細については、「ADM オンプレミ CloudConnector」を参照してください。

[NSADM-92204]

NetScaler ADM に関するセキュリティアドバイザリ　ADM オンプレミス Cloud Connector を設定し、セキュリティアドバイザリを有効にして、ADM オンプレミスのセキュリティアドバイザリ機能のフルバージョンを使用できます。以前は、セキュリティアドバイザリはプレビュー版でのみ利用可能でした。

詳細については、「セキュリティアドバイザリ」を参照してください。

> 注**:**

> ADM オンプレミ Cloud Connector を設定していない場合、または無効にしている場合は、セキュリティアドバイザリをプレビューバージョンとしてのみ使用できます。

ADM オンプレミ Cloud Connector の詳細については、「ADMオンプレミ Cloud Connector」を参照してください。

[NSADM-91726]

管理とモニタリング

StyleBook の操作で **NetScaler** インスタンスにアクセスするには認証が必要です　管理者は、NetScaler インスタンスで実行されるすべての StyleBook および構成パック操作の資格情報の提供をユーザーに要求できるようになりました。この機能を有効にするには、次の手順に従います。

- [設定] **>** [管理] **>** [システム、タイムゾーン、許可する **URL**、およびエージェントの設定] **>** [基本設定] に移動します。-インスタンスログイン用のプロンプト認証情報の選択
- **Stylebook** 操作用のプロンプト認証情報の選択

または、「インスタンスログインの資格情報を要求する」を選択し、「**Stylebook** 操作用の資格情報を要求する」を選択解除した場合、NetScaler インスタンスで実行される StyleBook および構成パックの操作では、ユーザー名とパスワードの入力を求められません。

詳細については、「デフォルト以外のユーザーのシェルアクセスを有効にする方法」を参照してください。

[NSHELP-35432]

NetScaler ADM バックアップファイルおよびユーザーセッションへの読み取り専用アクセス　読み取り専用アクセス権を持つユーザーは、[設定] > [ユーザーと役割] > [** セッション *
**] > [設定] >
[バックアップファイル] ページを表示できるようになりました。

[NSHELP-35431]

データ取り込みのしきい値を設定　[設定] > [データストレージ管理] **>** [データ保持ポリシー] **>** [システム] **>** [データ取り込み設定] でデータ取り込みしきい値を設定できるようになりました。この設定では、データストレージがしきい値に達したときにシステムレベルのプロセスを停止するように構成できます。許容されるしきい値は 50% ～80% です。

詳細については、「データ保持ポリシー」を参照してください。

[NSHELP-35237]

テクニカルサポートファイラーで確認できる **ADM** バージョンと **IP** アドレス　ADM バージョンと IP アドレスは、**[**設定**] > [**診断**] > [**テクニカルサポートファイルを生成**]** のテクニカルサポートファイルで確認できるようになりました。

[NSHELP-33551]

StyleBook

StyleBooks では以下の機能を利用できるようになりました。

- データソース: NetScaler ADC インスタンスをデータソースとして使用するか、カスタムデータソースを作成します。
- GitHub Enterprise: GitHub Enterprise サーバーから StyleBook と設定パックをインポートして同期します。
- 組み込み関数: 次の組み込み関数が追加されました。
  - `match()`
  - `contains()`
  - `select()`
  - `hash_sha256()`
  - `relate()`
  - `splat()`
- StyleBook 定義: NetScaler ADM GUI からカスタム StyleBook 定義を直接更新します。
- GitHub リポジトリからの設定パック:GitHub リポジトリから設定パックをインポートして同期します。以前は、StyleBook のみが許可されていました。
- `botinsight`属性: StyleBook の`insights`セクションで`botinsight`タイプを設定します。

[NSADM-97841]

StyleBooks アナリティクスにおける追加属性のサポート　StyleBooks の分析セクションが次のように拡張されました。
- パラメータを受け入れてトランスポートモードを設定する (`transport-mode`)
- さまざまな種類のトラフィック用に HDX Insight を設定 (`enable-hdxinsight-for`)
- HTTP X-Forwarded-For オプションを有効にする (`http-x-forwarded-for`)
- クライアント側の測定を有効にする (`client-side-measurements`)

詳しくは、「StyleBooks の文法」を参照してください。

[NSADM-97839]

解決された問題

ビルド 14.1—8.50 で対処されている問題。

分析

- App Dashboard データの定期的なプルーニングが期待どおりに機能しませんでした。その結果、NetScaler ADM はより多くのディスク容量を消費しました。

  [NSHELP-36184]

- NetScaler ADM が仮想サーバーライセンスを失うと、それらのライセンスを使用する仮想サーバーの分析ステータスは無効になると予想されます。このシナリオは、VPN 仮想サーバーでは期待どおりに機能しませんでした。

  [NSHELP-36183]

インフラストラクチャ

- [ゲートウェイ**] > [HDX Insight**] と [ゲートウェイ] **> [Gateway Insight**] では、グラフの X 軸に時間ではなく日付が表示されます。

  [NSHELP-36043]

- NetScaler ADM HA ペアは、ハートビート通信の同期障害により、スプリットブレインシナリオからの回復に失敗します。

  [NSHELP-35934]

- 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）機能はユーザーに対して有効になっており、管理者が [設定] > [管理**] > [CUXIP** 設定**]** で CUXIP を無効にした後でも、その使用状況データは収集されます。

  [NSADM-101771]

- ルート管理者として、デフォルトの資格情報を使用して NetScaler ADM GUI または API に初めてログオンしたときに、デフォルトのパスワードを変更するように求められませんでした。この修正により、デフォルトパスワードの変更が強制されます。

  [NSADM-95328]

- スクリプトを使用して複数の SNMP ユーザーを同時に作成すると、ADM への SNMP 要求が失敗します。

  [NSADM-83924]

管理とモニタリング

- NetScaler ADM バックアップディレクトリ内に作成されたフォルダーは、2 時間ごとにスケジュールされているバックアップ削除操作では削除されません。

  [ヘルプ-35911]

- 外部 LDAP による認証は NetScaler ADM で断続的に失敗し、NetScaler ADM を再起動することによってのみ解決されます。

  [NSHELP-35733]

- ADM mas_perf サブシステムがクラッシュし、**[**設定**] > [ADM** システムイベント**]** にイベントメッセージが表示されます。

  [NSHELP-35711]

- ユーザーは、[アプリケーション] **> [**アプリダッシュボード**]** で承認済みアプリケーションを表示できません。この問題は、ユーザーが多数のグループに属していて、各グループに多数のアプリケーションがある場合に発生します。

  [NSHELP-35165]

- NetScaler ADM で実行された Qualys スキャンにより、PostgreSQL ポートに脆弱な SSL/TLS キー交換のアクティブな脆弱性が報告されました。

  [NSHELP-34487]

- NetScaler がライセンスサーバーとの接続を切断し、10 分以内に接続し直すと、NetScaler によってチェックアウトされたライセンスがライセンスサーバーに 2 回表示されることがあります。ライセンスサーバーを再起動して、この古いエントリを解放します。

  [NSHELP-35420]

プロビジョニング

- ESXi または VMware vCenter を使用して NetScaler VPX をクラウドにプロビジョニング (インフラストラクチャ **>** インスタンス **> NetScaler > VPX >** プロビジョニング) すると、ライセンス構成は無視されます。

  [NSHELP-35984]

- VMware vCenter での NetScaler VPX のプロビジョニング（[インフラストラクチャ］**>**［インスタンス］**>**［**NetScaler**］**>**［**VPX**］**>**［プロビジョニング］）は、以前に削除された **VPX** インスタンスで使用されていたのと同じ名前が原因で失敗します。

  [NSHELP-35983]

StyleBook

- 認証仮想サーバーと組み込みのキャッシュポリシーバインディングを含む StyleBook 定義から構成パックを作成し、構成パックを削除すると、削除は成功します。ただし、同じパラメーターを使用して構成パックを再度作成しようとすると、次のエラーメッセージが表示され `Resource already exists`ます。

  [NSHELP-35646]

- [アプリケーション] **>** [構成] **>** [構成パック] **>** [**ADC** の移行] **>** [はじめに] **>** [構成の指定] で、**ADC** 構成をソース **ADC** インスタンスからターゲットインスタンスに移行しようとし、[次へ] をクリックすると、次のエラーメッセージが断続的に表示されます。

  `No Job found`。

  [NSADM-97948]

既知の問題

リリース 14.1 ～8.50 に存在する問題。

インフラストラクチャ

- [インフラストラクチャ] **>** [インスタンスアドバイザリ] **>** [セキュリティアドバイザリ] で、**CVE** のある脆弱な **NetScaler** インスタンスを選択して [アップグレードワークフローに進む] をクリックすると、次のエラーメッセージが表示されます:

  「選択した NetScaler インスタンスには、この修復ワークフローは必要ありません」

  回避策:［インフラストラクチャ］［アップグレードジョブ］から NetScaler インスタンスを手動でアップグレードします。

  [NSADM-103649]

- 新しい NetScaler ADM を構成すると、次のエラーメッセージが表示される場合があります。`Error in operation - Metrics not found.`

  この問題は、自動データ消去ジョブがまだ実行されておらず、データが存在しないために発生します。ジョブは 3 時間実行するようにスケジュールされており、実行後に必要なデータが生成され、エラーメッセージは表示されなくなります。

  [NSADM-103157]

- NetScaler ADM のスクロール可能なページのレポートをエクスポートすると、エクスポートされたレポートでは、表示されているウィンドウの高さを超えるコンテンツが切り捨てられることがあります。

  [NSADM-102765]

- NetScaler BLX インスタンスに証明書をインストールしようとすると、インストールが失敗し、［インフラストラクチャ］**>**［**SSL** ダッシュボード］**>**［**SSL** 監査ログ］ページに次のエラーメッセージが表示されます:

  `SCP: Authentication by password fails on _<ip-address>_.`

  [NSADM-102202]

- いずれかのパスワードに%23 の記号が付いている場合、NetScaler エージェントは NetScaler ADM に登録されません。

  [NSADM-100613]

管理とモニタリング

- ADM HA ペアでは、GUI の Sync Database オプションを何回か試しても、データベースステータスがダウン状態で、同期していないことが確認されました。

  [NSHELP-29626]

NetScaler ADM 14.1-4.42 リリースのリリースノート

February 6, 2024

このリリースノートドキュメントでは、NetScaler ADM リリース Build 14.1-4.42 の強化と変更、修正された問題と既知の問題について説明します。

メモ

- このリリースノートには、セキュリティ関連の修正は含まれていません。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。

新機能

ビルド 14.1-4.42 で利用できる機能強化と変更。

分析

Web Insight-リクエストに基づくパーセンテージ分布の表示をサポート　**Web Insight** では、次の指標に基づいてリクエストごとのパーセンテージ分布を表示できるようになりました。

- クライアント

- サーバー
- 地理的場所
- URL

この機能強化により、管理者は選択した期間の合計リクエスト数に基づいて受け取った分配率を把握できるようになります。たとえば、選択した期間にサーバーがどのようにリクエストを受信しているかを比較できます。

詳細については、「Web Insight」を参照してください。

[NSADM-96158]

Web Insight の各ウィジェットからのエクスポートをサポート　**Web Insight** では、すべてのウィジェットにエクスポートオプションが導入され、データを表形式でエクスポートできるようになりました。この拡張機能を使用すると、次のことが可能になります。

- 任意のウィジェットから必要なデータを個別にエクスポートします。
- 任意の指標をドリルダウンし、任意のウィジェットから必要なデータをエクスポートできます。

以前は、エクスポートデータには統合レポートのみが提供されていました。

> 注:
>
> 既存のエクスポートオプションを引き続き使用して、統合レポートを生成することもできます。

[NSADM-94140]

インスタンスの主要メトリックの詳細を表示する統合ダッシュボード　管理者は、以下に基づいて主要な指標の詳細の概要を示すダッシュボードを視覚化できるようになりました。

- アプリケーション
- ADC インフラストラクチャ
- アプリケーションセキュリティ
- Gateway

この単一ペインのダッシュボードでは、詳細を表示して、インスタンスの使用状況とパフォーマンスをよりよくモニタリングできます。

詳しくは、「統合ダッシュボード」を参照してください。

[NSADM-94137]

ADM イベントとメトリクスデータを **Splunk** と **New Relic** にエクスポートする　**NetScaler ADM** を **Splunk** および **New**Relic と統合するための新しいサブスクリプションを [設定] > [エコシステム統合 **] で作成すると、[**ADM** イベントと **ADM** メトリックス] オプションを選択できるようになりました。** これらのオプションのいずれ

かまたは両方でサブスクリプションを設定すると、Splunk と New Relic のダッシュボードで対応するデータを表示できます。

詳細については、「Splunk との統合 」および「New Relic との統合」を参照してください。

[NSADM-93765]

アプリケーションの **SSL** 評価を表示する　[アプリケーション**] > [**ダッシュボード] で、アプリケーションの SSL 評価を表示できるようになりました。SSL の問題を確認し、アプリケーションをアップグレードして A+ 評価を取得できます。ただし、このアップグレードによってトラフィックがいくらか低下した場合は、アプリケーションに設定されているセキュアフロントエンドプロファイルをロールバックできます。このアクションにより、A+ レーティングは以前のレーティングに戻ります。

詳細については、「A+ SSL 評価分析」を参照してください。

[NSADM-92025]

Web インサイト**-nil** 値のグラフ表示をサポート　**Web Insight** では、[アプリケーション]、[クライアント]、[URL]、または [インスタンス] でメトリクスをドリルダウンすると、選択した期間のグラフに nil 値 (たとえば、0 ms と 0 リクエスト) が表示されるようになりました。

以前は、選択した期間にトラフィックやトランザクションが受信されなかった場合、Web Insight はこれらの nil 値をスキップしてグラフを表示していました。管理者は、これらの nil 値を含むグラフ全体を表示できるようになりました。

[NSADM-88686]

インフラストラクチャ

NetScaler の高可用性展開における **RPC** ノードパスワードのサポート　HA 展開でプライマリノードとセカンダリノードを作成するときに RPC ノードパスワードを設定できるようになりました。[インフラストラクチャ**] > [**ジョブのアップグレード**] > [**ジョブの作成**] > [NetScaler** インスタンスの **HA** ペアの構成] に移動して、高可用性ノードの RPC ノードパスワードを入力します。

詳しくは、「NetScaler インスタンスの HA ペア構成のスケジュール」を参照してください。

[NSADM-93912]

NetScaler ADM エージェントは **NetScaler** イメージをキャッシュします　NetScaler イメージはダウンロード後に NetScaler ADM エージェントにキャッシュされるため、NetScaler のアップグレードにかかる時間が大幅に短縮されました。したがって、以降のアップグレードジョブでイメージをダウンロードする必要はありません。

> 注:
>
> これは、NetScaler ADM エージェントを使用して追加された ADC にのみ適用されます。

詳細については、「ADC アップグレードジョブの作成」を参照してください。

[NSADM-76343]

証明書チェーン全体を表示　これで、中間証明書からルート CA 証明書までの証明書のリンクチェーン全体を表示できるようになりました。

証明書チェーンを表示するには、[インフラストラクチャ**] > [SSL** ダッシュボード] に移動し、SSL 証明書を選択して [詳細] をクリックします。

詳細については、「SSL 証明書チェーンを表示する」を参照してください。

[NSADM-52467]

StyleBook

replace () 関数におけるその他の引数タイプのサポート　「replace ()」組み込み関数は、以下の組み込み型のリストも受け付けることができます。

- `string`
- `ipaddress`
- `tcp-port`
- `number`
- **`boolean`**

詳細については、「組み込み関数」を参照してください。

[NSADM-96802]

複数 **()** 関数のサポート　StyleBooks の組み込み関数が multiple () 関数をサポートするようになりました。multiple (argument1, argument2) 関数は 2 つの引数を取り、引数 1 のコピーを多数含むリストを返します。コピーの数は、引数 2 に渡された数と同じです。

詳細については、「組み込み関数」を参照してください。

[NSADM-95973]

StyleBook 設定パックのオプションセクションのサポート　設定パックの`targets`ペイ`stylebook`ロードでは、とセクションがオプションになりました。構成パックを更新するためにこれらのセクションを指定しない場合、

最後に使用`targets`されたセクションと`stylebook`セクションが NetScaler ADM データベースから取得され、構成パックが更新されます。

[NSADM-92377]

構成パックへのユーザーグループアクセスを指定　管理者は、他のユーザーグループが作成した構成パックにユーザーグループがアクセスできないように制限できるようになりました。このオプションを選択するには、[設定] **>** **[**ユーザーとロール**]** **>** **[**グループ**]** **>** **[**認証設定**]** **>** **[**構成パック**]** **>** **[**ユーザーグループが作成したすべての構成] に移動します。

詳しくは、「ユーザーグループの作成」の「構成パック」セクションを参照してください。

[NSADM-92374]

解決された問題

ビルド 14.1-4.42 で対処されている問題。

分析

- NetScaler ADM HA ペアが原因で、断続的にスプリットブレインのシナリオが発生することがあります。

  [NSHELP-35430]

- URL にクエリパラメータ値がない HTTP Web トランザクションは、NetScaler ADM Web Insight ダッシュボード（「アプリケーション」「Web Insight」）には表示されません。

  たとえば、URL `https://www.google.com/search?q=abstract%20api` にクエリパラメータ値がなく、`https://www.google.com/search?q=`として利用できる場合、HTTP トランザクションは削除され、ダッシュボードに表示されません。

  [NSADM-9948]

- **Web Insight** では、任意のメトリックをドリルダウンして詳細を表示し、さらに任意のメトリックをドリルダウンすると、グラフは前のビューのままですが、その他の詳細はすべて期待どおりに表示されます。

  その結果、それ以降のドリルダウンが期待どおりに機能していないという仮定が生まれます。

  [NSADM-9895]

インフラストラクチャ

- [インフラストラクチャ] **>** [**NetScaler** インベントリ] **>** [**NetScaler**]（**MPX/VPX/CPX/BLX**）ページに **MPX** インスタンスが表示されません。

  [NSHELP-35593]

- LDAP ユーザー認証を使用して NetScaler ADM GUI にログオンし、「ドメイン\ ユーザー名」を使用すると、ユーザー設定は保存されません。

  [NSADM-10095]

- 構成ジョブのパーティションでコマンドを実行すると、「管理パーティションデバイスのコマンドがブロックされました」というエラーメッセージが表示されます。

  この問題は、NetScaler 13.1-42.47 以降のビルドで発生しています。

  [NSADM-100416]

- [設定] > [展開 **] > [**強制フェールオーバー**]** で **ADM HA** ペアのフェイルオーバーを実行すると、**[**設定 ****]**> [展開 **] ページにセカンダリノードの詳細は表示されません。

  [NSADM-98674]

- **[**設定**] > [**通知**] > [Slack] > [**追加**]** で **Slack** プロファイルを追加しようとすると、プロファイルが追加されず、次のエラーメッセージが表示されます。

  `Please check internet connectivity`。

  [NSADM-9863]

- ルート管理者として、デフォルトの資格情報を使用して NetScaler ADM GUI または API に初めてログオンしたときに、デフォルトのパスワードを変更するように求められませんでした。この修正により、デフォルトパスワードの変更が強制されます。

  [NSADM-95328]

管理とモニタリング

- NetScaler インスタンスをバックアップまたはリストアする場合、/var/metrics_conf ディレクトリはバックアップされません。

  [NSHELP-35724]

- [インフラストラクチャ**] > [SSL** ダッシュボード**] > [SSL** 証明書**] > [**レポートのエクスポート**]** から週、**30** 日、または **90** 日間の **SSL** 有効期限レポートをエクスポートし、[表形式] を選択すると、結果のレポートには空のドメイン列が表示されます。

  [NSHELP-35592]

- インフラストラクチャ **> SSL** ダッシュボード **> SSL** 証明書では、NetScaler の高可用性ペアには、プライマリデバイスとセカンダリデバイスの「P」と「S」の上付き文字は表示されません。

  [NSHELP-35523]

- NetScaler ADM のステータスは、すべてのプロセスが起動して実行された後でも断続的に停止中と表示されます。

  [NSHELP-35408]

- クラスター内に複数のクラスター IP アドレス（CLIP）がある場合、［インフラストラクチャ］**>**［インスタンス］**>**［**NetScaler**］**>**［追加］で括弧内に **CLIP** を追加すると、構成が失敗し、CLIP が NetScaler ADM に追加されません。

  [NSHELP-35323]

- **[** インフラストラクチャ**] > [**構成**] > [**構成ジョブ**] > [**ジョブの作成**] > [**構成の選択**]** で、パスワード変数（`$password$`）を入力し、**[** パスワードフィールド**]** ではなく **[** タイプ**]** を **[**テキストフィールド**]** のままにして **[** 次へ**]** をクリックすると、ページが読み込まれません。

  [NSHELP-35266]

- 要求が他の ADM プロセスに送信されると、NetScaler ADM インベントリプロセスが断続的にクラッシュします。

  [NSHELP-35048]

- 複数のサブシステムがクラッシュしたため、NetScaler ADM が応答しません。

  [NSHELP-3463]

- プライマリサイト（NetScaler ADM HA ペア）は、NetScaler ADM 災害復旧ノードとのデータの同期を再試行し続け、失敗します。
  この問題は、プライマリサイトのデータが大きい (1 GB を超える) 場合に発生します。

  [NSHELP-32750]

プロビジョニング

- SDX（インフラストラクチャ **>** インスタンス **> NetScaler ADC > VPX**）で **NetScaler VPX** をプロビジョニングすると、**NetScaler ADM** で失敗します。

  [NSHELP-35347]

StyleBook

- StyleBook 定義に`operations`セクションが含まれていると、構成パックのデプロイが失敗することがあります。

  [NSHELP-35588]

- [設定**] > [IPAM] > [**追加**]** で一部のバージョンの **Infoblox** を **IP** アドレス管理プロバイダとして追加すると、次のエラーメッセージが表示されます。

  `Invalid provider information: Invalid attributes for registering provider`。

  [NSHELP-35302]

既知の問題

リリース 14.1-4.42 に存在する問題。

インフラストラクチャ

- いずれかのパスワードに記号が付いていると、NetScaler エージェントは NetScaler ADM に登録されません。#

  [NSADM-100613]

- ［設定］**>**［管理］**>**［**SSL** 証明書のインストール］で、アップロードする証明書ファイルの名前に括弧が付いていると、NetScaler への SSL 証明書のインストールは失敗します。次のエラーメッセージが表示されます：

  「POST リクエストが無効です。ペイロードは object= で始まるはずです。」

  [NSADM-9531]

管理とモニタリング

- ADM HA ペアでは、GUI の Sync Database オプションを何回か試しても、データベースステータスがダウン状態で、同期していないことが確認されました。

  [NSHELP-29626]

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。

> 注：
>
> NetScaler ADM サービスは、NetScaler コンソールサービスに名前が変更されました。当社の製品 UI とドキュメントは、これらの変更を反映するように現在更新中です。この間、古い名前と新しい名前が同じ意味で参照されていることに気付くかもしれません。この移行の間、ご理解いただきますようお願いいたします。

Citrix Cloud を介した NetScaler コンソールサービスにより、次のことが可能になります。

- 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分析、アプリケーションセキュリティとボットのため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 NetScaler Console サービスでのみサポートされているその他のさまざまな機能。

移行を成功させるには、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
- NetScaler エージェントを設定する
- 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
- NetScaler コンソールのライセンスを検証してください
- スクリプトを使用して移行する

オンプレミスの ADM から NetScaler Console サービスに移行した後、オンプレミスの ADM を再び使用したい場合は、ロールバックスクリプトを使用できます。詳しくは、「オンプレミス ADM へのロールバック」を参照してください。

NetScaler エージェントを設定する

NetScaler インスタンスと NetScaler ADM 間の通信を有効にするには、エージェントを構成する必要があります。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構成されていない場合は、NetScaler Console サービス用に少なくとも 1 つのエージェントを構成する必要があります。
- 既存のオンプレミス 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、NetScaler Console サービスにも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。

NetScaler コンソールのサービスライセンスを検証してください

NetScaler サービスのライセンスを取得する必要があります。

- NetScaler Console サービスの VIP ライセンスは、オンプレミスの VIP ライセンスと同じかそれ以上である必要があります。

  > 注
  >
  > ：VIP ライセンスの方が少ない場合、仮想サーバーはランダムに選択され、NetScaler Console サービスの VIP レベルの構成は失敗します。

- ADM オンプレミス展開をライセンスサーバーとして使用する場合は、移行前にライセンスを NetScaler Console サービスに再割り当てしてください。詳細については、「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 でプールライセンスを使用している場合は、NetScaler Console サービスのプールライセンスを取得してから、ADC インスタンスにライセンスを割り当てる必要があります。詳細については、「プールライセンスの構成」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 SDX：13.0 74.11 またはそれ以降のバージョン。
  - NetScaler 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。

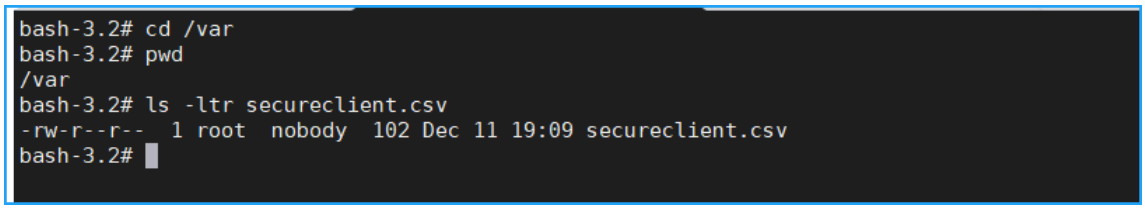
> 注
>
> 移行中は、オンプレミスの ADM にインターネット接続があることを確認します。

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

   > 注
   >
   > ADM HA ペアの場合は、プライマリノードにログオンします。

2. **shell** と入力して **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 NetScaler 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
```

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

この例では、オプション 1 が選択されています。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 SDWANOPs 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']"}
1620286058


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



--------------------------------------------------------------------------------
ADM On-rem 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、データプルーニング設定。
- 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。
> - プールライセンスを移行すると、仮想サーバーを含むすべてのタイプが移行されます。

5. ADM **13.0 76.xx** バージョンの場合は、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 NetScaler 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

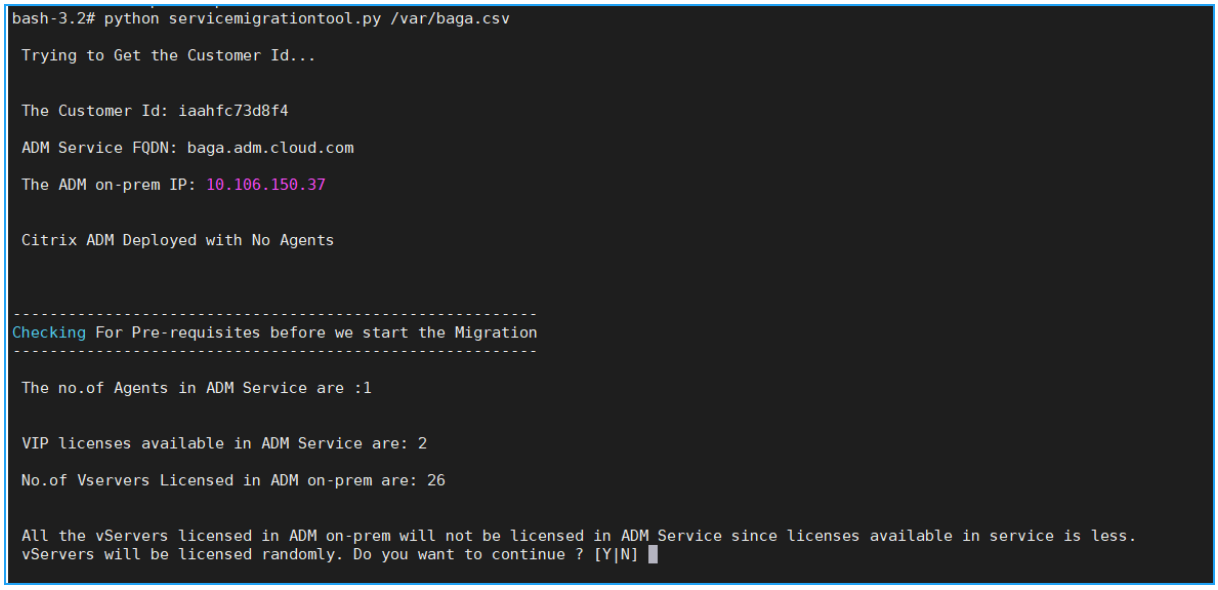
   c) 以下のコマンドを実行して移行します。

      i. `cd /var`

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

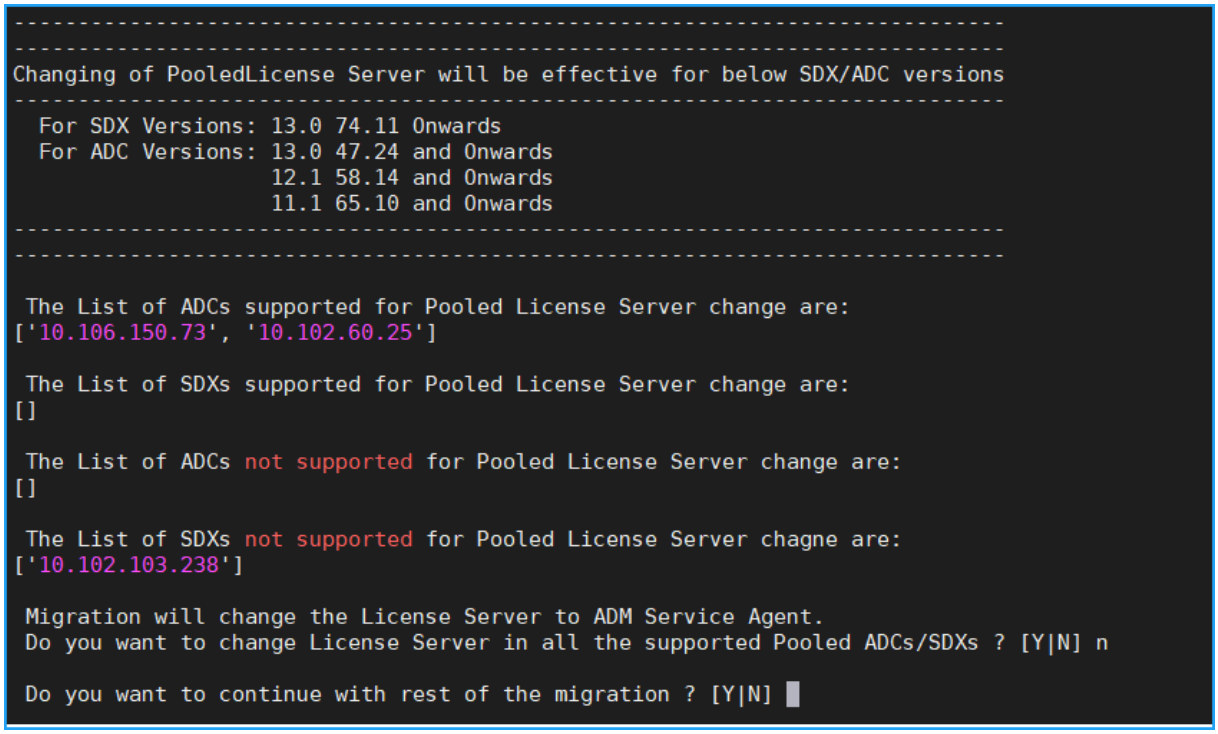
      たとえば、`python servicemigrationtool_27.py /var/secureclient.csv`

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、NetScaler Console のサービスライセンスがオンプレミスライセンスよりも低い場合にのみ表示されます。



[**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。



[**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 インスタンスとそれぞれの構成が NetScaler Console サービスに正常に移動されると、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 ADM（NetScaler Console 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。

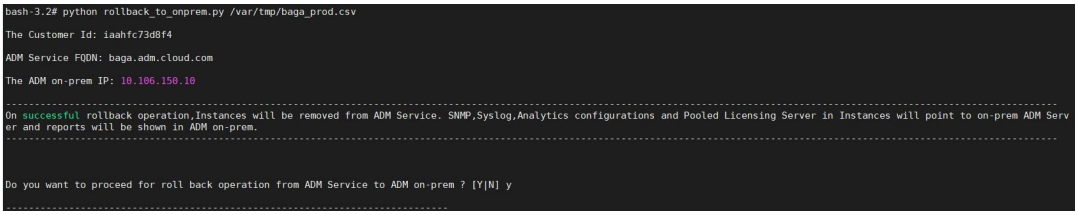
1. SSH クライアントを使用して、オンプレミスの ADM にログオンします。
2. shell と入力して Enter キーを押すと、bash モードに切り替わります。
3. ADM **13.0 82.xx** ビルドでは、以下のコマンドを実行してロールバックを完了します。

   a) cd /mps/script

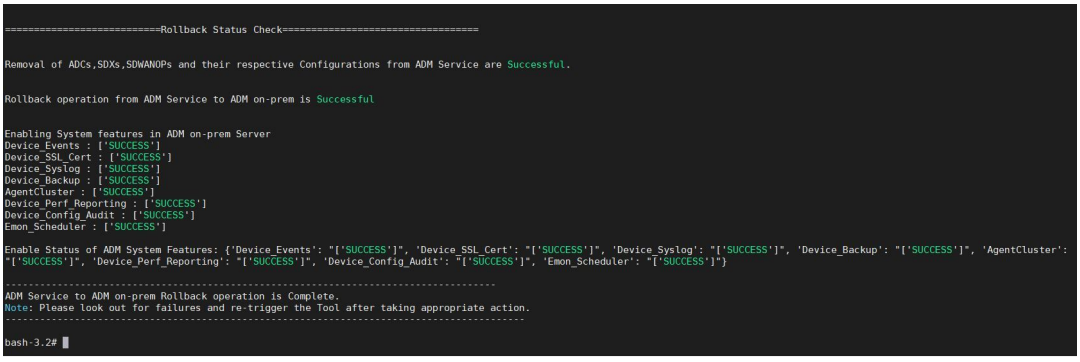
   b) python rollback_to_onprem.py <path of ClientID/Secret File in ADM on-prem VM>

   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。



   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。



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ン期間分析、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://www.citrix.com/events/2022/whats-new-with-citrix-application-delivery-management.html

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す。

移行スクリプトで **ADC** 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 インスタンスは引き続きオンプレミスの ADM セットアップで動作します。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。

いくつかの **ADC** インスタンスが **ADM** サービスへの移行に失敗した場合はどうなりますか。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` はログファイルをとして持ち、Python 2.7 の ADM はログファイルを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 サービスのエクスプレスアカウントには、仮想サーバーライセンスが 2 つ、StyleBook 構成パックが 2 つ、構成ジョブが 2 つしかありません。オンプレミスの ADM にこれら以上の構成があり、Express Account で移行を開始した場合、スクリプトは Express アカウントに適用できる上記の構成（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。

ADM サービスに追加された構成ジョブ

```
==============Config Jobs Addition to ADM Service====================

config_job2_show_ns_ip : FAILURE : Express user can have maximum 2 config jobs

ConfigJob1_show_ha_node : FAILURE : Express user can have maximum 2 config jobs

 The config jobs status is :
{'config_job2_show_ns_ip': 'FAILURE', 'ConfigJob1_show_ha_node': 'FAILURE'}
```

回避策：このエラーは、Express アカウントに登録していて、3 つ以上の構成ジョブがある場合に発生します。すべての構成ジョブを移行するには、有効なサブスクリプションを取得する必要があります。

ADM サービスに追加された **IP** ブロック

```
====================IP Blocks Addition in ADM Service======================

ipblock1 : FAILURE : IP Block Name ipblock1 already exists

ipblock3 : FAILURE : IP Block Name ipblock3 already exists

test : FAILURE : IP Block Name test already exists
```

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

ネットワークダッシュボードレポートの追加ステータス

```
================Network Dashboard Reports Addition to ADM Service=================

new456 : FAILURE : Dashboard new456 already exists

new123 : FAILURE : Dashboard new123 already exists

 The network dashoard reports addition status is:
{'new456': "['FAILURE']", 'new123': "['FAILURE']"}
```

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

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
	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 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 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 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 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 インスタンスに複製する方法

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 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

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 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 インスタンスから SSL 証明書をポーリングする方法

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

ADM は、Citrix Hypervisor、VMware ESXi、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

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

インスタンスグループ

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 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、NetScaler 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で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 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 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。

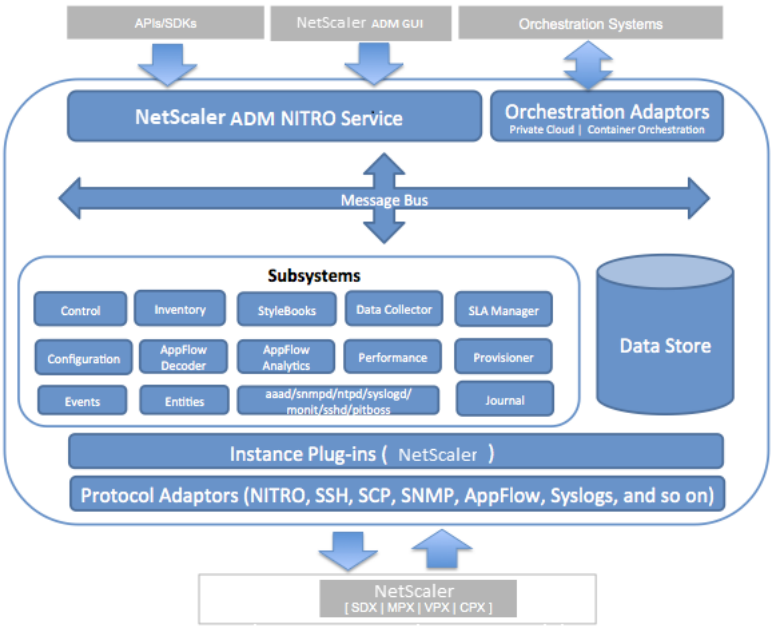
アーキテクチャ

February 6, 2024

NetScaler Application Delivery Management（ADM）データベースはサーバーと統合され、サーバーはデータ収集、NITRO 呼び出しなどの主要なプロセスをすべて管理します。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 ADC アプライアンスまたは NetScaler Application Delivery Management（ADM）から検出、管理、監視したい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 NetScaler ADC 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。

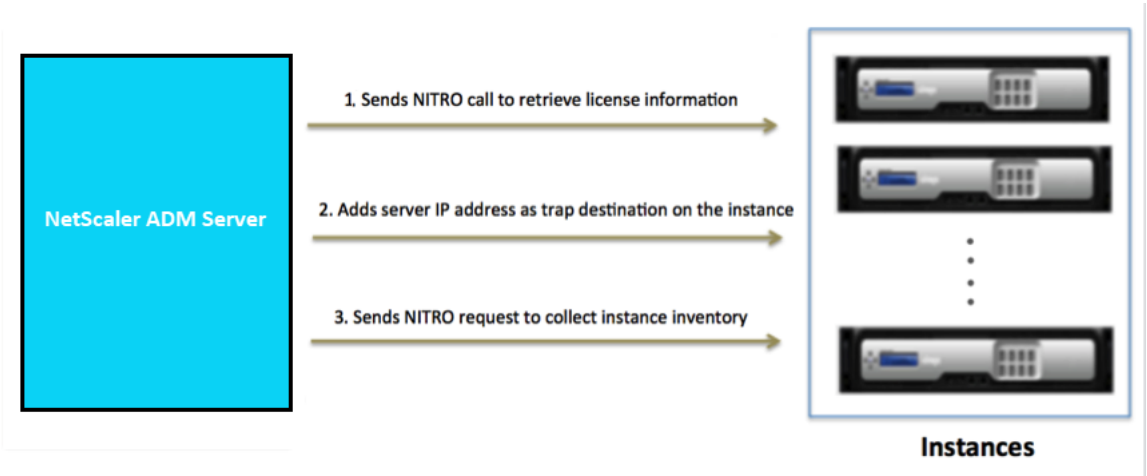
- NetScaler インスタンス
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
  - NetScaler CPX
  - NetScaler BLX
- NetScaler Gateway インスタンス

インスタンスは、NetScaler ADM サーバー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。

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 MPX、NetScaler VPX、NetScaler SDX、NetScaler BLX、NetScaler Gateway）が判断されます。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。

   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。NetScaler MPX、NetScaler VPX、NetScaler SDX、NetScaler BLX、および NetScaler Gateway インスタンスの場合、ライセンスがインスタンスに適用されていないと、このステップが失敗することもあります。

   > 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値を超えると失敗します。インスタンスの上限は 20 です。

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、NetScaler Application Delivery Management （ADM）が NetScaler インスタンスから特定の情報を収集するプロセスです。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。NetScaler ADM を使用してインスタンスを監視するには、NetScaler 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、ライセンスの種類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 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

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。[インフラストラクチャ**] > [**インスタンス**] > [NetScaler**] に移動します。インスタンスを選択し、[**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。[インフラストラクチャ**] > [**構成監査] に移動します。[構成監査] ページで、[設定] をクリックし、[構成監査ポーリング] のポーリング間隔を構成します。

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
				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、[インフラストラクチャ**] > [**構成監査] に移動し、[今すぐポーリング] をクリックします。[**Poll Now**] ページでは、ネットワーク内のすべてのインスタンスまたは選択したインスタンスをポーリングできます。
SSL 証明書のポーリング	24 時間ごと (デフォルト)	NetScaler インスタンスにインストールされている SSL 証明書。	NITRO コールと SCP	はい。インフラストラクチャ **> SSL** ダッシュボードに移動します。[SSL ダッシュボード] ページで、[設定] をクリックしてポーリング間隔を設定します。

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、[インフラストラクチャ] > **[SSL** ダッシュボード] に移動し、[今すぐポーリング] をクリックします [**Poll Now**] ページでは、ネットワーク内のすべてのインスタンスまたは選択したインスタンスをポーリングできます。
エンティティのポーリング	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、ADM 機能の有効化または無効化を参照してください。	NITRO 呼び出し	はい。ただし、10 分未満に設定することはできません。構成するには、[インフラストラクチャ] > **[**ネットワーク機能] に移動します。[ネットワーク機能] ページで、[設定] をクリックしてポーリング間隔を構成します。

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。そのためには、[インフラストラクチャ] > [ネットワーク機能] に移動し、[今すぐポーリング] をクリックします。[**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。

> 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、[インフラストラクチャ**] > [**ネットワーク機能**] ****[設定]** の順に移動して、要件に応じて間隔を設定できます。

インスタンスの手動ポーリング

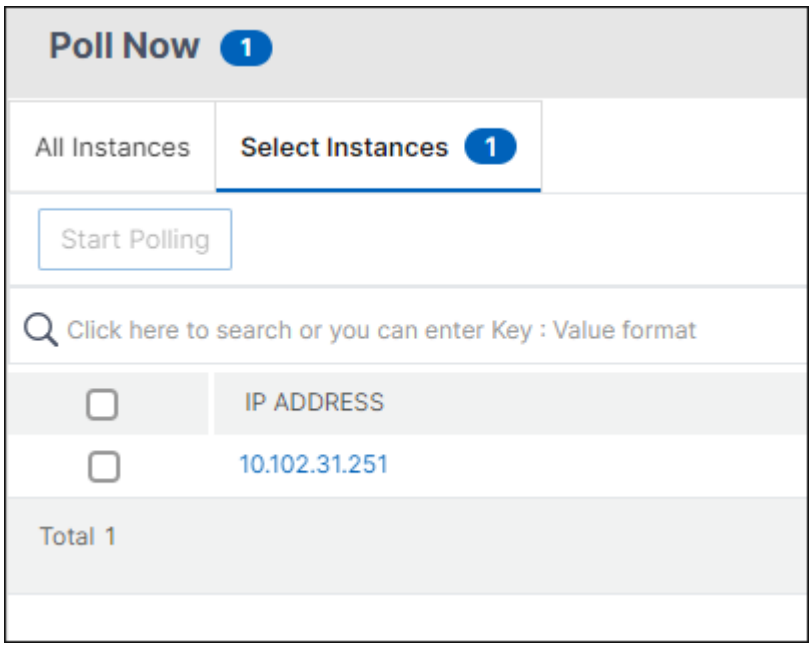
NetScaler ADM が多数のエンティティを管理している場合、ポーリングサイクルでレポートの生成に時間がかかり、画面が空白になったり、システムが以前のデータを表示したりする可能性があります。

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、［インフラストラクチャ］**>**［ネットワーク機能］に移動します。
2. [ネットワーク機能] ページの右上隅にある [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。



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

エンティティの手動ポーリング

NetScaler ADM では、特定のインスタンスにバインドされている一部の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. NetScaler ADM で、［インフラストラクチャ］**>**［ネットワーク機能］**>**［負荷分散］**>**［仮想サーバー］に移動します。
2. 状態が DOWN と表示されている仮想サーバを選択し、[**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。

データガバナンス

February 6, 2024

ADM On-Prem Cloud Connector を使用すると、Citrix Cloud はライセンスコンプライアンスのためのライセンス、構成、使用状況データを収集し、サービスの管理、測定、改善を行うことができます。14.1 8.x 以降のリリース以降では、ADM サービスと ADM オンプレミス間の接続を有効にするように Cloud Connector を設定できます。ADM オンプレミ Cloud Connector を有効にすると、

- Flexed Licensing コンプライアンスの必須ライセンスおよび使用状況データが収集されます。
- セキュリティアドバイザリ機能は **ADM** オンプレミスで利用できます。詳細については、「ADM オンプレミ CloudConnector」を参照してください。

Cloud Connector を有効にすると、データメトリックの収集が有効になります。

データカテゴリ

次の表は、Cloud Connector を有効にした後に収集されるパラメータの詳細を示しています。

カテゴリ	説明	使用目的
NetScaler の導入と機能の使用状況	顧客名、顧客 ID、管理対象デバイスの総数、アクティブな管理対象デバイスの合計数など、NetScaler の展開と使用に関する情報。	サービスの管理、測定、改善のため。
NetScaler ADM デプロイ	NetScaler に関する情報	サービスの管理、測定、改善のため。
NetScaler と NetScaler ADM のライセンス、エンタイトルメント、および使用状況	資格、ライセンス	ライセンスコンプライアンス、およびサービスの管理、測定、改善。

NetScaler と **NetScaler ADM-**デプロイメントパラメーターと機能使用パラメーター

パラメーター	説明
onprem_ip	ADM の IP アドレス
t_ten	ADM に接続されているテナントの総数
deploy	ADM デプロイメントタイプがスタンドアロンか HA ペアかを確認します
is_dr	ディザスタリカバリノードが構成されているかどうかをチェックします
is_agt	ADM オンプレミスエージェントが設定されているかどうかを確認します
is_cloud	ADM デプロイメントが ADM サービスか ADM オンプレミスかを確認します
is_cntr	ADM デプロイメントが Kubernetes クラスタ内にあるかどうかをチェックします
platform	ADM がホストされているプラットフォーム。たとえば、Citrix Hypervisor
total_users	ADM ローカルユーザーの総数
total_gui_requests	過去 24 時間に ADM GUI にログインしたユーザーの総数
total_api_requests	過去 24 時間の API 経由の ADM へのリクエストの合計数。これには、リモートプロキシユーザ (エージェントからの要求) も含まれます。
total_api_external_requests	API から ADM へのリクエストのうち、エージェントからのリクエストを除外したリクエストの合計数
total_custom_apps	ADM のカスタムアプリケーションの総数
total_managed_apps	ADM の管理対象アプリケーションの総数
total_apps	ADM のアプリケーション総数
total_custom_sites	ADM で設定されているカスタムサイトの総数
total_managed_devices	ADM 内のマネージド NetScaler インスタンスの総数
total_active_managed_devices	稼働状態にある NetScaler インスタンスの総数
total_ns_device	ADM の管理対象 MPX インスタンスの総数
total_ngvpx_device	ADM 内のマネージドゲートウェイ VPX インスタンスの総数
total_nswg_device	ADM の管理対象 Web ゲートウェイインスタンスの総数
total_nswgvpx_device	ADM の管理対象 Web ゲートウェイ VPX インスタンスの総数

パラメーター	説明
total_nsvpx_device	ADM の管理対象 VPX インスタンスの総数
total_cpx_device	ADM の管理対象 CPX インスタンスの総数
total_nsap_device	ADM の管理パーティションインスタンスの総数
total_nssdx_device	ADM 内のマネージド SDX インスタンスの総数
total_agents	設定された ADM オンプレミスエージェントの合計数
total_active_agents	UP 状態の ADM オンプレミスエージェントの合計
total_custom_event_rules	ADM で作成されたカスタムイベントルールの総数
total_event_rules	ADM で作成されたイベントルールの総数
total_stylebook_config_store_count	ADM で作成された構成パックの総数
total_user_sb_stylebook_count	ADM で作成されたカスタム構成パックの総数
total_waf_devices	WAF 違反が有効になっている NetScaler インスタンスの総数
total_gw_devices	SSL VPN が有効になっている NetScaler インスタンスの総数
total_icaproxy_devices	ADM の HDX Insight が有効になっている NetScaler インスタンスの総数
total_bot_devices	ボット違反が有効になっている NetScaler インスタンスの総数
total_pooled_devices	ライセンスをプールした NetScaler インスタンス（管理対象と管理対象外の両方）の合計
total_config_audit	ADM で設定された設定監査テンプレートの合計
total_config_job	ADM で作成された設定ジョブの総数
total_ssl_certs	ADM から作成、変更、削除された SSL 証明書の合計
total_network_report	ADM で作成されたネットワークレポートの合計
total_k8s	Kubernetes クラスターでホストされている NetScaler ADM。Kubernetes クラスターの合計です。
total_ipam	ADM に追加された IP アドレス管理プロバイダーの総数
total_rbac_groups	ADM で設定されている RBAC グループの総数
total_ingress_deployed	Kubernetes のイングレスコントローラーの総数。
total_ipam_configured	ADM に追加された IP アドレス管理ネットワークの総数
total_web_transaction_analytics	Web トランザクション分析が有効になっている NetScaler インスタンスの総数

パラメーター	説明
total_pager_duty_profile	ADM に追加された PagerDuty プロファイルの総数
total_slack_profile	ADM に追加された Slack プロファイルの総数
total_api_discovery	API リクエストを受信する NetScaler インスタンスの総数
total_lb_devices	負荷分散仮想サーバーで構成された NetScaler インスタンスの総数
total_lb_devices_http	負荷分散 HTTP 仮想サーバーで構成された NetScaler インスタンスの総数
total_lb_devices_ssl	負荷分散 SSL 仮想サーバーで構成された NetScaler インスタンスの総数
total_cs_devices	コンテンツスイッチ仮想サーバーで構成された NetScaler インスタンスの総数
total_gslb_devices	グローバルサーバー負荷分散仮想サーバーで構成された NetScaler インスタンスの総数
total_aaa_devices	AAA 仮想サーバーで構成された NetScaler インスタンスの総数
t_radius_svr	ADM で設定されている RADIUS 認証サーバーの総数
t_ldap_svr	ADM で設定されている LDAP 認証サーバーの総数
t_tacacs_svr	ADM に設定されている TACACS 認証サーバの総数
agent_id	デプロイされたエージェントの固有 ID
platform	エージェントがホストされているプラットフォーム。たとえば、Citrix Hypervisor
version	ADM エージェントのバージョン
city	ADM エージェントが導入されている都市
country	ADM エージェントが展開されている国
region	ADM エージェントがデプロイされているリージョン
device_id	VPX インスタンスのユニーク ID
version	VPX インスタンスのビルドバージョン
state	VPX インスタンスの現在のステータス (稼働中または停止中)
device_platform	VPX インスタンスがホストされているプラットフォーム
root	/var、/root、/flash、/var/mps ディレクトリにある ADM ディスク使用率の詳細
total	ADM ディスクの総容量 (単位: バイト)

パラメーター	説明
used	使用されている ADM ディスクの合計容量
free	使用可能な ADM ディスクの合計容量
Adm_analt_dx - Feature	問題が特定される分析タイプ (ボット、WAF、Web Insight、サービスグラフなど)。
Adm_analt_dx - issue_type	特定された問題が属する問題カテゴリ。たとえば、ライセンス、構成
Adm_analt_dx - sub_issue_type	特定された問題のサブ課題カテゴリ。サブ問題としては、NO_VIPS_LICENSED、BOT_IN_ACTION_DISABLED、NS_FEATURE_DISABLED、VSERVER_WITHOUT_BOT_POLICY_BINDING、APPFLOWPARAM_DISABLED、ICA_APPFLOW_POLICY_BINDING、SECURITY_INSIGHT_IN_ACTION_DISABLED、SECURITY_INSIGHT_ACTION_DISABLED、CPX_VIPS_PRESENT、VSERVER 内のコレクタバインド解除、APPFLOW_POLICY_BINDING
feature	負荷分散/コンテンツスイッチ仮想サーバーで有効になっている分析機能
total_lbvserver_ft_enabled	少なくとも 1 つの分析機能が有効になっている負荷分散仮想サーバーの総数
total_csvserver_ft_enabled	少なくとも 1 つの分析機能が有効になっているコンテンツスイッチ仮想サーバーの総数
feature_enabled_on_vpn	VPN 仮想サーバーで有効になっている分析機能
total_vpnvserver_ft_enabled	少なくとも 1 つの分析機能が有効になっている VPN 仮想サーバーの総数

NetScaler および **NetScaler ADM** のライセンス、エンタイトルメント、および使用状況に関するデータ要素

パラメーター	説明
pool_instances_entitled	資格が付与されたプールインスタンスの総数
pool_instances_used	使用済みプールインスタンスの総数
pool_fips_instances_entitled	資格が付与されたプール FIPS インスタンスの総数
pool_fips_instances_used	使用済みプール FIPS インスタンスの総数

パラメーター	説明
pool_entvpu_entid	対象となるエンタープライズ vCPU の合計プール
pool_entvpu_used	使用済みプールエンタープライズ vCPU の合計使用量
pool_entbw_entitled	[MBps] という表題のプールのエンタープライズ帯域幅の合計
pool_entbw_used	プールのエンタープライズ帯域幅の合計使用量 [MBps]
pool_pltbw_entitled	[MBps] という表題のプールプラチナ帯域幅の合計
pool_pltbw_used	プールプラチナ帯域幅の合計使用量 [MBps]
pool_pltvcpu_entitled	対象となるプラチナ vCPU プールの総数
pool_pltvcpu_used	使用されたプラチナ vCPU プールの総数
pool_stdbw_entitled	プールに付与された標準帯域幅の合計
pool_stdbw_used	使用されたプールの標準帯域幅の合計
pool_stdvcpu_entitled	使用資格のあるスタンダード vCPU プールの総数
pool_stdvcpu_used	使用済みの標準 vCPU プールの総数
pool_cpxvcpu_entitled	使用資格のあるプール CPX vCPU の合計数
pool_cpxvcpu_used	使用されたプール CPX vCPU の合計数
pool_perc_instances_used	使用済みインスタンスの割合
pool_perc_vcpu_used	使用済みの vCPU の割合
pool_perc_bw_used	使用済み帯域幅の割合
total_entitled_vservers	資格のある仮想サーバーの総数
total_used_vservers	使用された仮想サーバーの総数
total_discovered_vservers	検出された仮想サーバーの総数
perc_used_vservers	使用済み/使用資格のある仮想サーバーの割合
perc_discovered_vservers	検出された/使用資格のある仮想サーバの割合
is_local_license	ライセンスが NetScaler ADM でホストされているかどうかを確認します
license_edition	ライセンスの種類 (プラチナ/スタンダード/エンタープライズ)
is_pooled_license	ライセンスがプールライセンスかどうかをチェックします
model_id	インスタンスのモデル ID
plt_license_allocation	プラチナライセンスの割り当て

パラメーター	説明
ent_license_allocation	エンタープライズライセンスの割り当て
std_license_allocation	標準ライセンス割り当て
ライセンス終了日	ライセンスの有効期限が切れるまでの合計日数
platform	デバイスタイプ
instance_id	インスタンスの一意の識別子
instance_mode	インスタンスがスタンドアロンか HA ペアかを確認します
instance_state	インスタンスのステータス (Up/Down)
flex_vpx_inst_enabled	資格のある VPX インスタンスの総数
inst_flex_vpx	割り当てられた VPX インスタンスの総数
flex_sdx_inst_enabled	資格が付与された SDX インスタンスの総数
splex_inst_allocated	割り当てられた SDX インスタンスの総数
「flex_mpx_inst_itred_	資格が付与された MPX インスタンスの総数
inst_flex_mpx	割り当てられた MPX インスタンスの総数
flex_plt_bw_itled	対象となるプラチナ帯域幅
flex_plt_bw_allocated	割り当てられたプラチナ帯域幅
flex_ent_bw_entited	対象となるエンタープライズ帯域幅
bw_flex_ent_allocated	割り当てられた企業帯域幅
flex_std_bw_enabled	対象となる標準帯域幅
flex_std_bw_allocated	割り当てられた標準帯域幅
flex_vpx_fips_inst_redit_	資格が付与された FIPS インスタンスの総数
flex_vpx_fips_inst_allocated	割り当てられた FIPS インスタンスの総数

NetScaler ADM のバージョンが 14.1 4.x 以前の場合は、Citrix Cloud 上でカスタマー ID を作成して、ADM の状態、ステータス、およびその他のメトリック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 アカウントに送信できます。Citrix は、NetScaler ADM の使用状況を把握するために統計情報を収集します。詳細については、「顧客 ID のデータガバナンス」を参照してください。

ライセンス

February 6, 2024

NetScaler Application Delivery Management（ADM）では、NetScaler 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 ライセンスが必要です。

NetScaler ADM は、次のライセンスエディションをサポートしています。NetScaler の営業担当者またはパートナーに連絡して、ADM ライセンスを購入してください。

Express Edition —Express Edition のライセンスでは、任意の数のインスタンスを管理および監視できます。既定では、Express Edition のライセンスが適用されます。

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

注意すべき点:

- **13.1** ～**9.x** 以前のビルドでは、検出されたアプリケーションまたは仮想サーバーを最大 30 個管理し、分析を表示できます。検出された 30 個のアプリケーションまたは 30 台の仮想サーバを超える場合は、Advanced ライセンスを購入して適用する必要があります。たとえば、100 個の仮想サーバライセンスを購入した場合、最大 130 個の仮想サーバライセンスを使用できます。
- ビルド **13.1** ～**12.x** 以降では、検出されたアプリケーションまたは仮想サーバを最大 2 つ管理し、分析を表示できます。検出された 2 つのアプリケーションまたは 2 つの仮想サーバ以外に、Advanced ライセンスを購入して適用する必要があります。たとえば、100 個の仮想サーバライセンスを購入した場合、最大 102 個の仮想サーバライセンスを使用できます。

ビルド **13.1-12.x** へのアップグレード後:

- Express のデフォルトの無料仮想サーバーはすべて、30 日間機能します。2 つの仮想サーバを選択し、30 日間の猶予期間内に 2 つのデフォルトライセンスを適用できます。アップグレードの 30 日後にユーザーアクションを実行しなかった場合、ADM は 2 台の仮想サーバーにライセンスをランダムに適用し、残りの仮想サーバーのライセンスを解除します。これらの仮想サーバを有効にするには、新しい Advanced ライセンスを購入して適用する必要があります。
- アップグレード後、ADM の動作に以下の変更が加えられました。
  - ADM は 30 日間の猶予期間を強制します。
  - 30 日間の猶予期間内に、30 台の Express Free 仮想サーバーに対する新しい仮想サーバーの割り当てはブロックされます。
    * たとえば、12.x にアップグレードする前に使用可能な仮想サーバライセンスの数が 30 で、ライセンスされた仮想サーバが 20 台のみ使用されていた場合、30 日間の猶予期間内に 20 台の仮想サーバのみを使用でき、残りの 10 台の仮想サーバにはライセンスが付与されません。

- ただし、30 日間の猶予期間内であれば、管理者は Advanced ADM ライセンスを適用し、新しい仮想サーバーを割り当てることができます。

機能	オプション	Express Edition	Advanced Edition	NetScaler ライセンス
アプリケーション	アプリケーションダッシュボード	最大 2 つの仮想サーバー。	購入したすべての仮想サーバーライセンスと、追加の仮想サーバー 2 台分の資格があります。	アプリダッシュボードの NetScaler Web App Firewall 関連情報には、App Firewall ライセンスを使用したプレミアム（または）アドバンストが必要です。
		Web Insight	最大 2 つの仮想サーバー。	購入したすべての仮想サーバーライセンスと、追加の仮想サーバー 2 台分の資格があります。
		サービスグラフ	最大 2 つの仮想サーバー。	購入したすべての仮想サーバーライセンスと、追加の仮想サーバー 2 台分の資格があります。
		構成 > StyleBooks	無制限	無制限
[セキュリティ]	セキュリティダッシュボード	最大 2 つの仮想サーバー。	購入したすべての仮想サーバーライセンスと、追加の仮想サーバー 2 台分の資格があります。	セキュリティダッシュボードの NetScaler Web App Firewall 関連情報には、App Firewall ライセンスを使用したプレミアム（または）アドバンストが必要です。
		セキュリティ違反	最大 2 つの仮想サーバー。	購入したすべての仮想サーバーライセンスと、追加の仮想サーバー 2 台分の資格があります。

機能	オプション	Express Edition	Advanced Edition	NetScaler ライセンス
		ユーザーとエンドポイント	最大 2 つの仮想サーバー。	購入したすべての仮想サーバーライセンスと、追加の仮想サーバー 2 台分の資格があります。
Gateway	HDX Insight	最大 2 つの仮想サーバー。	購入したすべての仮想サーバーライセンスと、追加の仮想サーバー 2 台分の資格があります。	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）
		Gateway Insight	最大 2 つの仮想サーバー。	購入したすべての仮想サーバーライセンスと、追加の仮想サーバー 2 台分の資格があります。
インフラ	インフラストラクチャ分析	無制限	無制限	-
		インスタンス	無制限	無制限
		SSL ダッシュボード	無制限	無制限
		イベント	無制限	無制限
		ネットワーク機能	無制限	無制限
		ネットワークレポート作成	無制限	無制限
		プールライセンス	無制限	無制限
		構成 > 構成ジョブ、構成テンプレート、および構成アドバイス	無制限	無制限
		ジョブのアップグレード	無制限	無制限
		オーケストレーション	無制限	無制限
		WAN Insight	無制限	無制限
設定	RBAC および外部認証（インスタンスレベル）	無制限	無制限	-

機能	オプション	Express Edition	Advanced Edition	NetScaler ライセンス
		RBAC および外部認証	無制限	無制限

*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のライセンスは、10 個の仮想サーバ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。

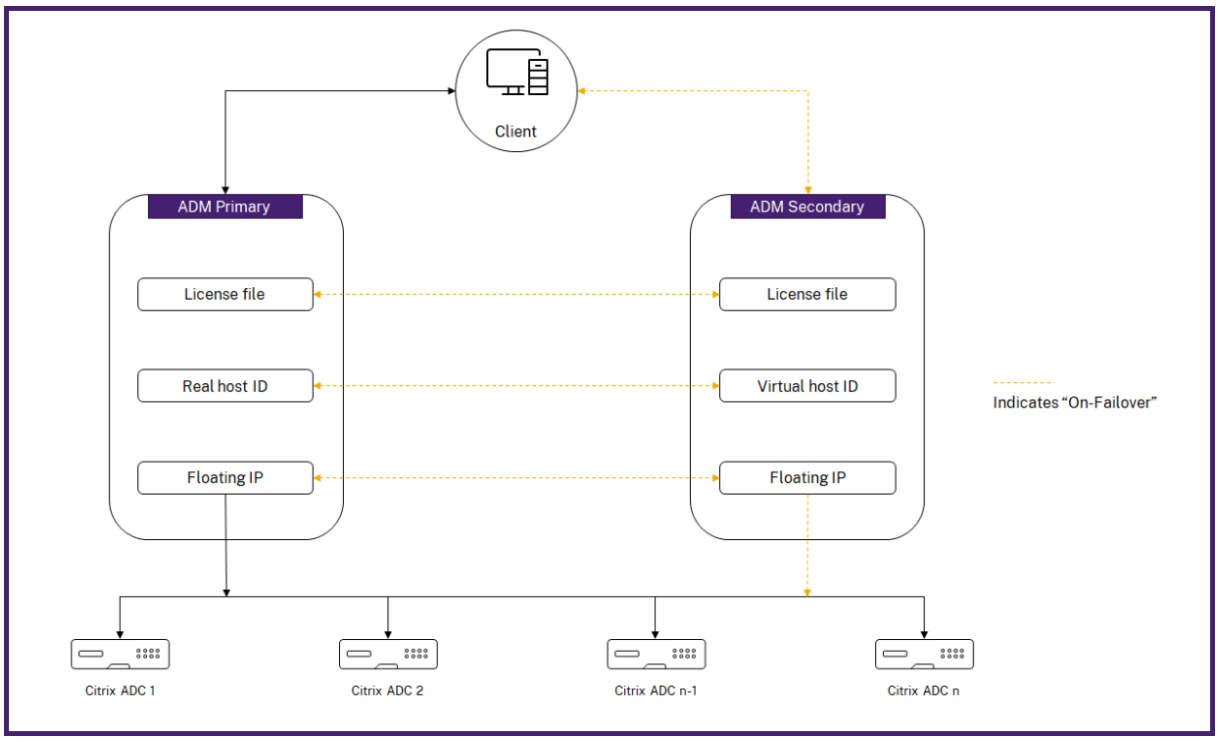
> 注
>
> - NetScaler ADM 12.1.49.x 以前のリリースをインストールしている場合、セカンダリノードでライセンスを維持するために 30 日間の猶予期間があります。猶予期間の後、Citrix に連絡して元のライセンスを再ホストする必要があります。
> - 12.1.50.x 以降のリリースでは、NetScaler ADM ライセンスは自動的にセカンダリノードに同期されます。
> - プールされたライセンスは、12.1.50.x 以降のリリースからセカンダリノードに自動的に同期されます。

ADM 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 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。ライセンスを管理するプライマリサーバーでライセンスを適用すると、そのインスタンスに今後のすべてのライセンスが適用されます。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。

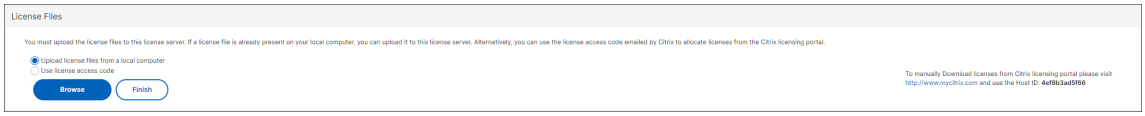
仮想サーバーライセンスをアップグレードする

NetScaler ADM でライセンスをアップグレードして、NetScaler 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。

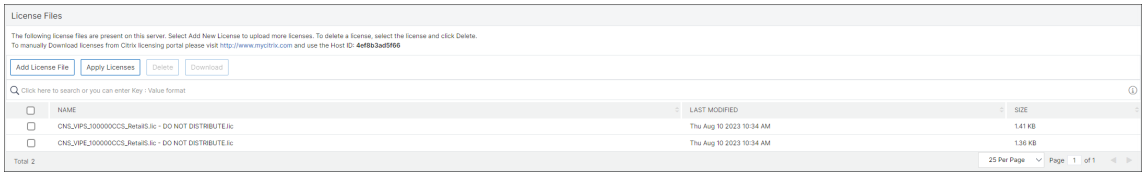
アプライアンスライセンスをアップグレードするには**:**

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. [インフラストラクチャー**] > [**プールライセンス] に移動します。
3. [ライセンスファイル] に移動し、次のいずれかのオプションを選択します。
   - ローカルコンピュータ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。



確認

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、**[**設定**] > [**ライセンスと分析の構成] の順に移動します。

仮想サーバの管理

NetScaler ADM で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。

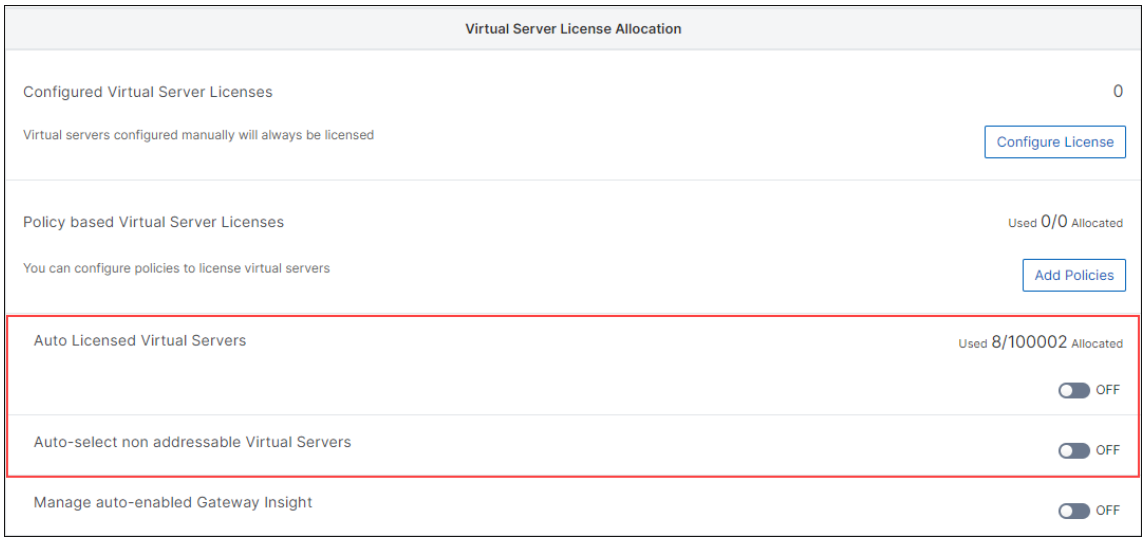
仮想サーバーを手動で選択するかライセンスの割り当て対象を一部の仮想サーバーのみに制限するには、まず仮想サーバーへの自動ライセンス割り当てを無効化してから、管理する仮想サーバーを選択する必要があります。

仮想サーバーの自動ライセンス認証を無効にする

1. [設定] **>** [ライセンスと分析の設定] に移動します。

   ダッシュボードには、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。

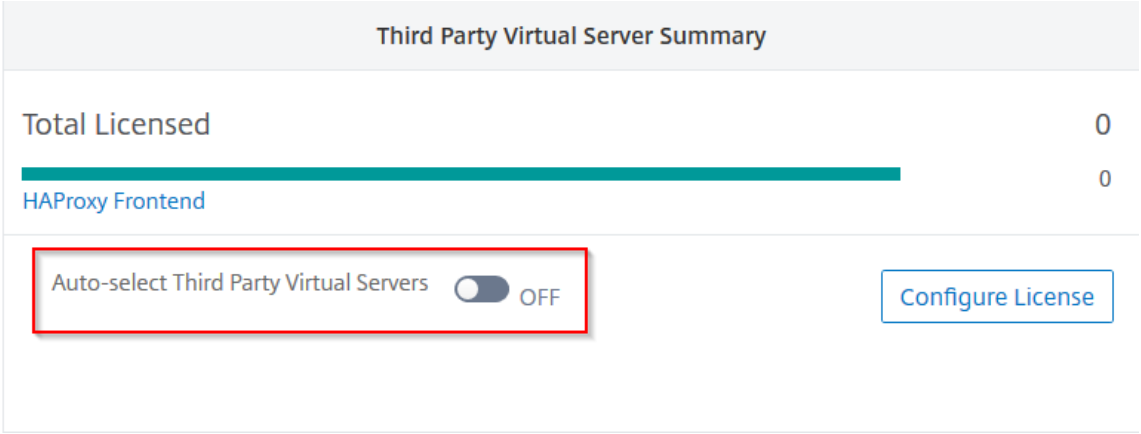


ライセンス供与するサードパーティ仮想サーバーを選択する

1. [設定] **>** [ライセンスと分析の設定] に移動します。

ダッシュボードには、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。



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. [仮想サーバー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ー] 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ーを選択します。
4. **[**ライセンス**]** をクリックします。

ポリシーベースの仮想サーバーライセンスを構成する

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

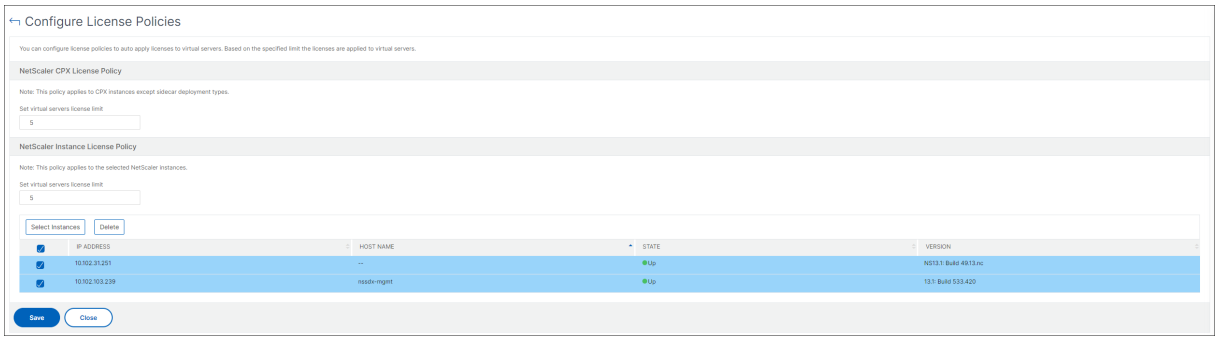
[ポリシーの編集] をクリックすると、次の項目を指定できます:

- CPX インスタンスに仮想サーバー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ーにライセンスを適用します。

  > 重要
  >
  > : この制限は、サイドカーデプロイタイプを除く 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ー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）に仮想サーバーの制限を設定します。ADM は、指定された制限まで ADC インスタンス上の仮想サーバーにライセンスを適用します。
- 仮想サーバーライセンスを適用する優先 ADC インスタンスを選択します。したがって、ADM は、選択したインスタンスの仮想サーバーにのみライセンスを適用できます。



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表示できます。

1. [設定**] > [**ライセンスと分析の設定] に移動します。
2. 仮想サーバライセンスの 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ー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ーにライセンスを自動的に適用しません。アドレス指定不可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ー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 [仮想サーバーライセンスの割り当て] のオプションがあります。アドレス指定不可能な仮想サーバを自動選択オプションを有効にすると、アドレス指定不可能な仮想サーバのライセンスが自動的に適用されます。

> 注
>
> - NetScaler ADM は、デフォルトでは、アドレス指定不可能な仮想サーバー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. インフラストラクチャ **>** プールライセンス **>** 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. インフラストラクチャ **>** プールライセンス **>** 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 ADM をインストールする前に、ソフトウェア要件、ブラウザー要件、ポート情報、ライセンス情報、および制限を理解する必要があります。

NetScaler ADM の要件

コンポーネント	条件
RAM	32 GB
仮想 CPU	8 基の CPU 注：NetScaler ADM の展開には、ソリッドステートドライブ（SSD）テクノロジーを使用することをお勧めします。
記憶域	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 のサイズ見積もりによって異なります。サイズ計算ツールを使用して、ストレージの見積もりを計算します。サイズ計算ツールにアクセスするには、NetScaler の担当者に問い合わせてください。 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。 初期導入時にストレージを見積もり、追加のディスクを取り付けることをお勧めします。 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。
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

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

コンポーネント	条件
スループット	1Gbps

> 注
>
> AMD プロセッサーは以下でサポートされています。
>
> - **NetScaler ADM 13.1** ビルド **4.43** 以降。
> - **NetScaler ADM** エージェント **13.1** ビルド **17.42** 以降。

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、使用している NetScaler のバージョン とビルドと同じかそれ以上である必要があります。たとえば、NetScaler ADM 12.1 ビルド 50.39 をインストールしている場合は、NetScaler 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 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、10.1 以降の場合
	NetScaler SDX、11.0 以降の場合
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
WAF セキュリティ違反	11.0.65.31 以降
Gateway Insight	11.0.65.31 以降
Cache Insight	10.5 以降 *

NetScaler ADM 機能	NetScaler ソフトウェアのバージョン
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 を実行する NetScaler インスタンスを搭載した NetScaler ADM ではサポートされません。

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

HDX Insight でサポートされているシンクライアント

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

HDX 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 アプライアンスに対してのみ表示されます。

NetScaler 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、RHEL 8.0、Ubuntu 16.04、および Ubuntu 18.04

サポート対象のオペレーティングシステムと **Workspace** バージョン

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

オペレーティングシステム	Workspace 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
Chrome アプリ	1.5

サポートされているブラウザー

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。

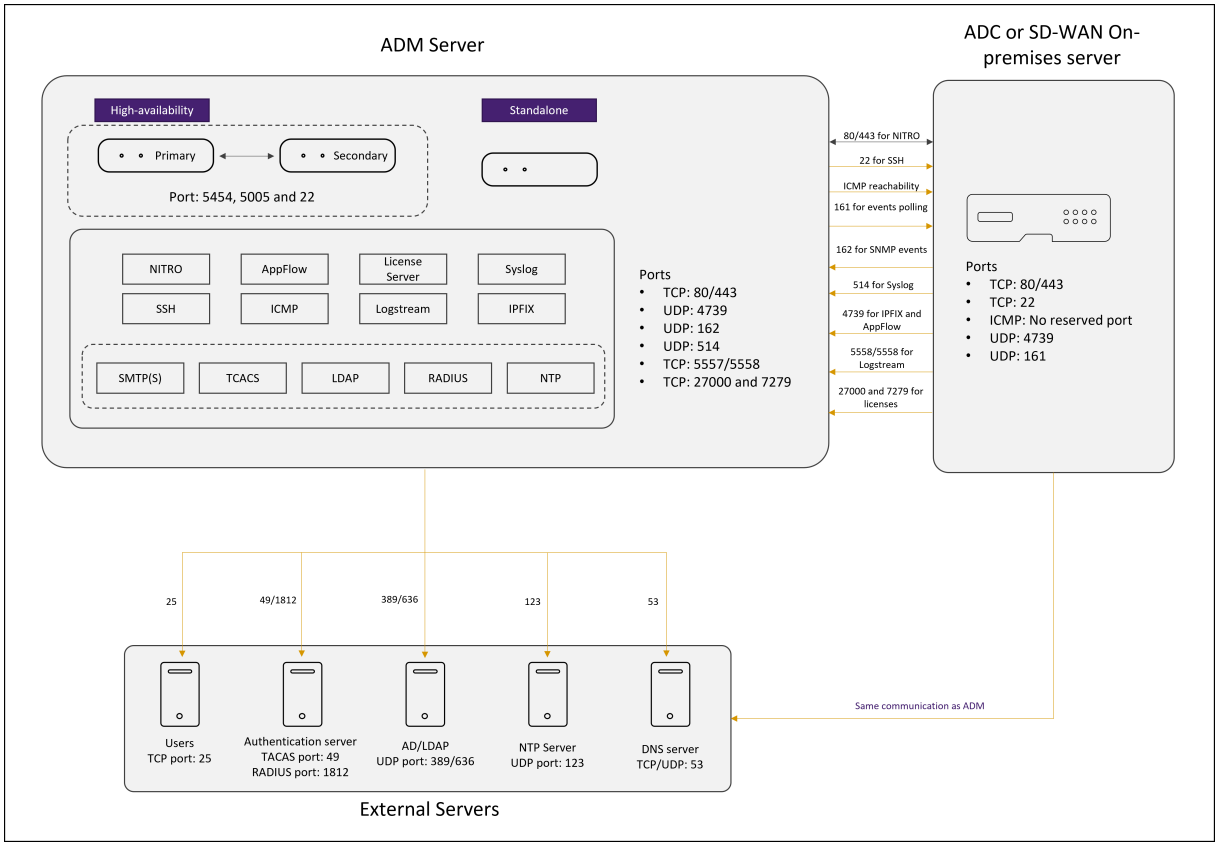
ウェブブラウザ	バージョン
Microsoft Edge	79 以降
Google Chrome	51 以降
Safari	10 以降
Mozilla Firefox	52 以降

サポートされるポート

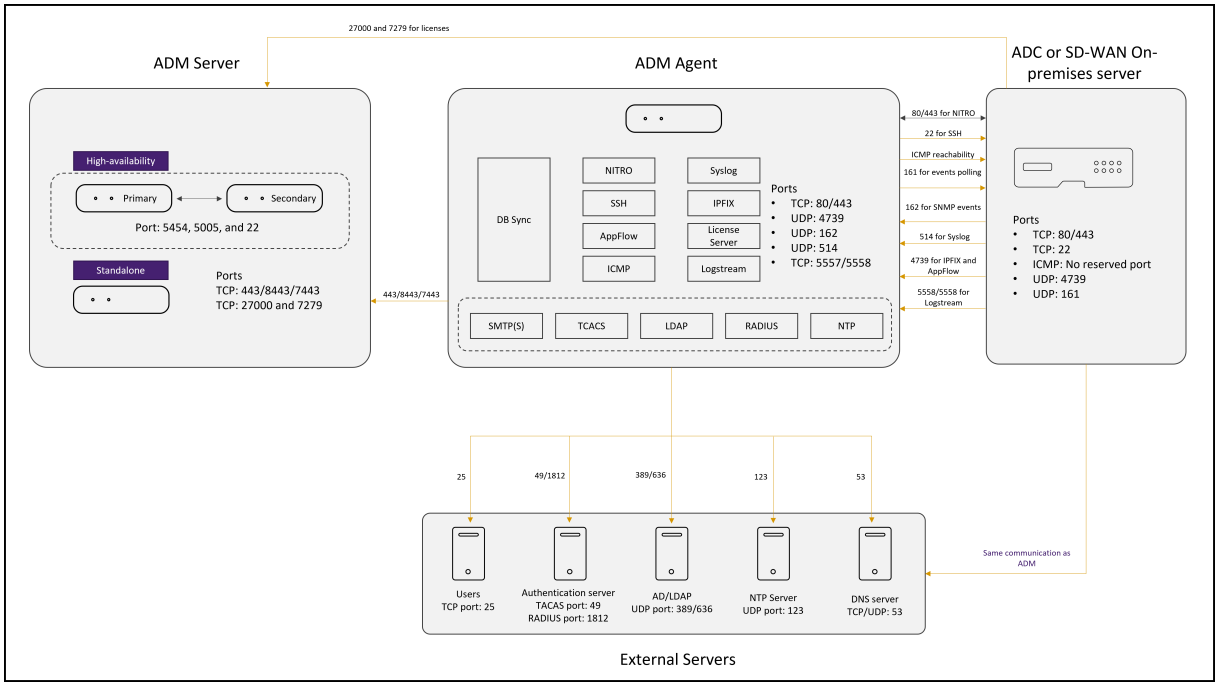
NetScaler ADM は、NetScaler IP（NSIP と呼ばれる）アドレスを使用して NetScaler ADC と通信します。ADC インスタンスと ADM の間の仲介者としてエージェントを使用できます。これらのサーバーとの通信を確立するには、必要なポートを開きます。

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



NetScaler ADM 高可用性展開環境のネットワークポート図:

2 台の NetScaler 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、インスタンスを追加すると、次

のようになります。

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

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 インスタンス
- 外部サーバ

ADM サーバのポート

次の表は、ADM サーバ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
80/443/5454/22	TCP	高可用性モードの NetScaler ADM ノード間の通信およびデータベース同期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、NetScaler ADM とエージェントは相互に対話します。
27000 と 7279	TCP	NetScaler ADM ライセンスサーバーと ADC インスタンス間の通信用のライセンスポート。これらのポートは、ADC プールされたライセンスにも使用されます。	NetScaler から NetScaler ADM へ

ポート	種類	詳細	コミュニケーションの方向
5005	UDP	HA ノード間でハートビートを交換するためのポート。	NetScaler ADM プライマリノードからセカンダリノードへ。NetScaler ADM セカンダリノードからプライマリノードへ。

NetScaler ADM インスタンスと NetScaler インスタンスが通信にエージェントを使用しない場合は、NetScaler ADM サーバー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 インスタンスへの NITRO 通信用。	NetScaler ADM エージェントから NetScaler に、NetScaler から NetScaler ADM エージェントへの Citrix
4739	UDP	NetScaler インスタンスから Citrix NetScaler ADM への AppFlow 通信用。	NetScaler から NetScaler ADM エージェントへ
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 から NetScaler ADM エージェントへ
514	UDP	NetScaler インスタンスから NetScaler ADM に Syslog メッセージを受信すること。	NetScaler から NetScaler ADM エージェントへ
5557/5558	TCP	NetScaler ADC から NetScaler ADM へのログストリーム通信（WAF セキュリティ違反、Web Insight サイト、および HDX Insight 用）。	NetScaler から NetScaler ADM へ

ポート	種類	詳細	コミュニケーションの方向
5563	TCP	NetScaler ADC インスタンスから NetScaler ADM に ADC メトリック（カウンタ）、システムイベント、監査ログメッセージを受信するには	NetScaler から NetScaler ADM へ

ADM エージェントのポート

次の表は、ADM エージェント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 インスタンスへの NITRO 通信用。	NetScaler ADM エージェントから NetScaler に、NetScaler から NetScaler ADM エージェントへの Citrix
4739	UDP	NetScaler インスタンスから Citrix NetScaler ADM への AppFlow 通信用。	NetScaler から NetScaler ADM エージェントへ
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 から NetScaler ADM エージェントへ
514	UDP	NetScaler インスタンスから NetScaler ADM に Syslog メッセージを受信すること。	NetScaler から NetScaler ADM エージェントへ
5557/5558	TCP	NetScaler ADC から NetScaler ADM へのログストリーム通信（WAF セキュリティ違反、Web Insight サイト、および HDX Insight 用）。	NetScaler から NetScaler ADM へ

ADC インスタンスのポート

次の表では、NetScaler 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 インスタンスへの NITRO 通信用。高可用性モードの NetScaler ADM サーバー間の NITRO 通信用。	NetScaler ADM から NetScaler へ、NetScaler から NetScaler ADM へ
22	TCP	NetScaler ADM から NetScaler インスタンスへの SSH 通信用。高可用性モードで展開された NetScaler ADM サーバー間の同期用。また、このポートは、ADM エージェントと NetScaler 間の SSH 通信に必要です。	NetScaler ADM から NetScaler 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	NetScaler ADM インスタンスと NetScaler インスタンス間、または高可用性モードでデプロイされたセカンダリ NetScaler ADM サーバー間のネットワーク接続性を検出します。	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

ADC ビルトインエージェント用ポート

次の表では、NetScaler 組み込みエージェントで開く必要がある必須ポートについて説明します。

ポート	種類	詳細	コミュニケーションの方向
443	TCP	NetScaler ADM から NetScaler 組み込みエージェントへのすべての通信用	NetScaler ADM から NetScaler への組み込みエージェントおよび NetScaler 組み込みエージェントから NetScaler ADM

> 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

次の表は、外部サーバー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
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
123	UDP	複数のタイムソースと同期するためのデフォルトの NTP サーバポート。	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ています。

1. NetScaler ADM GUI の管理アクセス
2. NetScaler 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. ネットスケーラーからの 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 のネットワークデバイス（NetScaler ADC および NetScaler Gateway）を管理するネットワーク管理者およびアプリケーション管理者を対象としています。NetScaler ADM を使用して管理するデバイスの種類に関係なく、このドキュメントの手順に従います。

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/current-release/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。ライセンスなしで、インスタンスとエンティティをいくつでも追加できます。ただし、ライセンスを適用せずに分析情報を表示できるのは 2 つの仮想サーバーだけです。3 台以上の仮想サーバーの分析を表示するには、適切なライセンスを購入する必要があります。詳細情報。
- 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 インスタンスと通信するために必要なポートが開いていることを確認します。詳細情報。
- **NetScaler** 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 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。

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 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

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

- NetScaler
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
  - NetScaler CPX
  - NetScaler BLX
  - NetScaler Gateway

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）サーバーの時計を NTP サーバーと同期するように構成する必要があります。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 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プル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。次のシスログデータが NetScaler 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 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 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 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。

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 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 NetScaler Application Delivery Management （ADM）を仮想アプライアンス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 NetScaler ADM をインストールする詳細な手順については、次のトピックを参照してください。

- Citrix Hypervisor を使用した NetScaler ADM
- MicrosoftHyperV 搭載 NetScaler ADM
- VMware ESXi を使用した NetScaler ADM
- Linux KVM サーバーを使用した NetScaler ADM

NetScaler 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	Citrix では、NetScaler ADM の導入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推奨しています。

コンポーネント	条件
	必要なデフォルトのストレージ容量は 120 GB です。実際のストレージ要件は、NetScaler ADM のサイズ設定の見積もりによって異なります。NetScaler ADM HA 展開ガイドの 「最大制限」セクション（7 ページ）に記載されているサイジング計算ツールを使用します。このガイドは、ダウンロードサイトの [**NetScaler MAS** リリース **12.1] > [**以前のバージョン] 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 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。 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。
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。NetScaler ADM のインストールを実行するには、Citrix XenCenter を使用する必要があります。

> 注:
>
> NetScaler ADM は XenMotion をサポートしていません。

前提条件

NetScaler ADM をインストールする前に、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。NetScaler 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。
- NetScaler ADM .XVA イメージファイルがダウンロードされました。

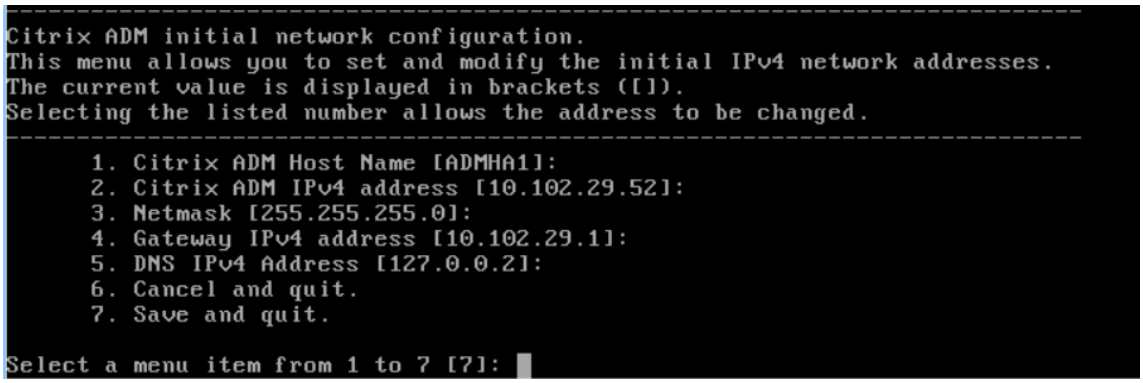
XenCenter のシステム要件

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

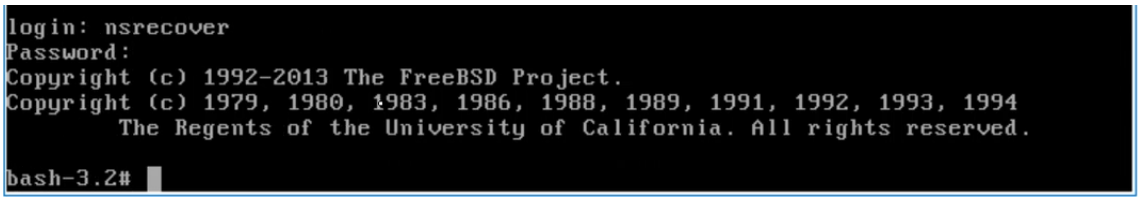
NetScaler Application Delivery Management のインストール

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



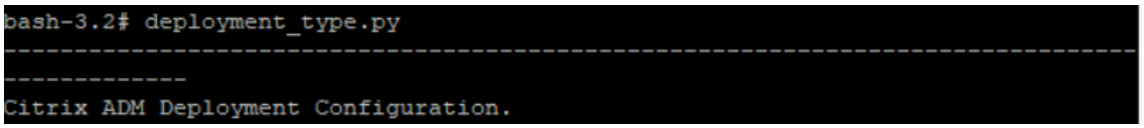
2. 必要な IP アドレスを指定したら、構成設定を保存します。

3. プロンプトが表示されたら、nsrecover/nsroot 認証情報を使用してログオンします。



> 注
>
> ログオン後、初期ネットワーク構成を更新する場合は、networkconfig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



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。

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

NetScaler 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。
- NetScaler ADM イメージファイルがダウンロードされました。

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。

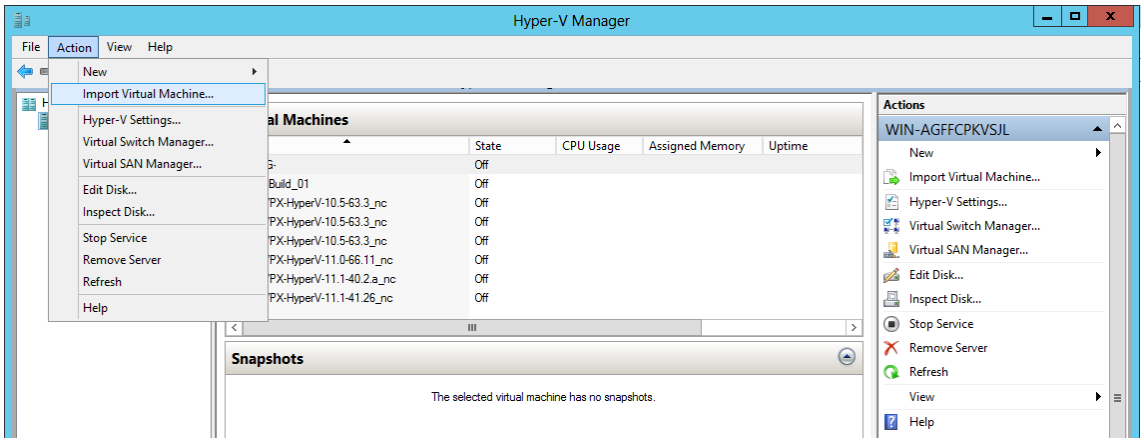
コンポーネント	条件
オペレーティングシステム	Windows Server 2012 R2
.NET Framework	バージョン 2.0 以降
CPU	750 MHz (MHz)、推奨:1 ギガヘルツ (GHz) またはそれより高速
RAM	1GB。推奨：2GB
NIC	100Mbps 以上の NIC

NetScaler Application Delivery Management インストール

インストールできる NetScaler 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。

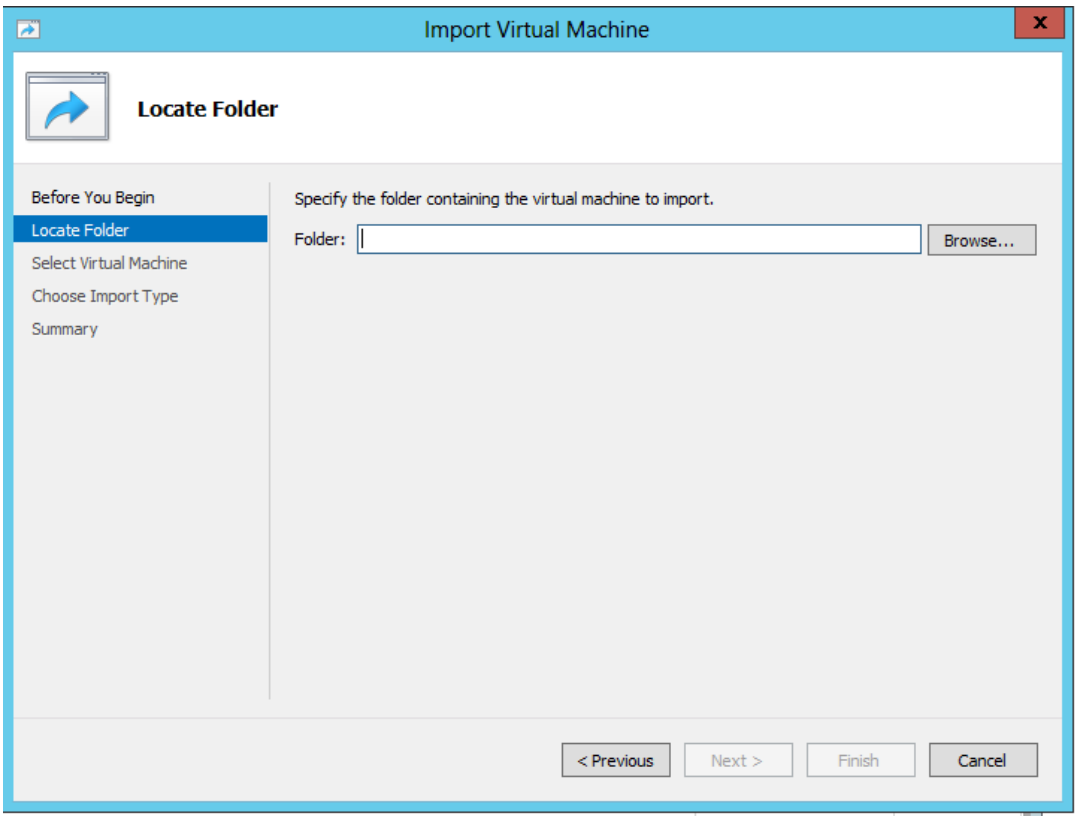
   a) ［仮想マシンのインポート］ダイアログボックスの［フォルダーの検索］セクションで、**NetScaler ADM Hyper-V** イメージを保存したフォルダーを参照してフォルダーを選択し、［次へ］をクリックします。

   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。

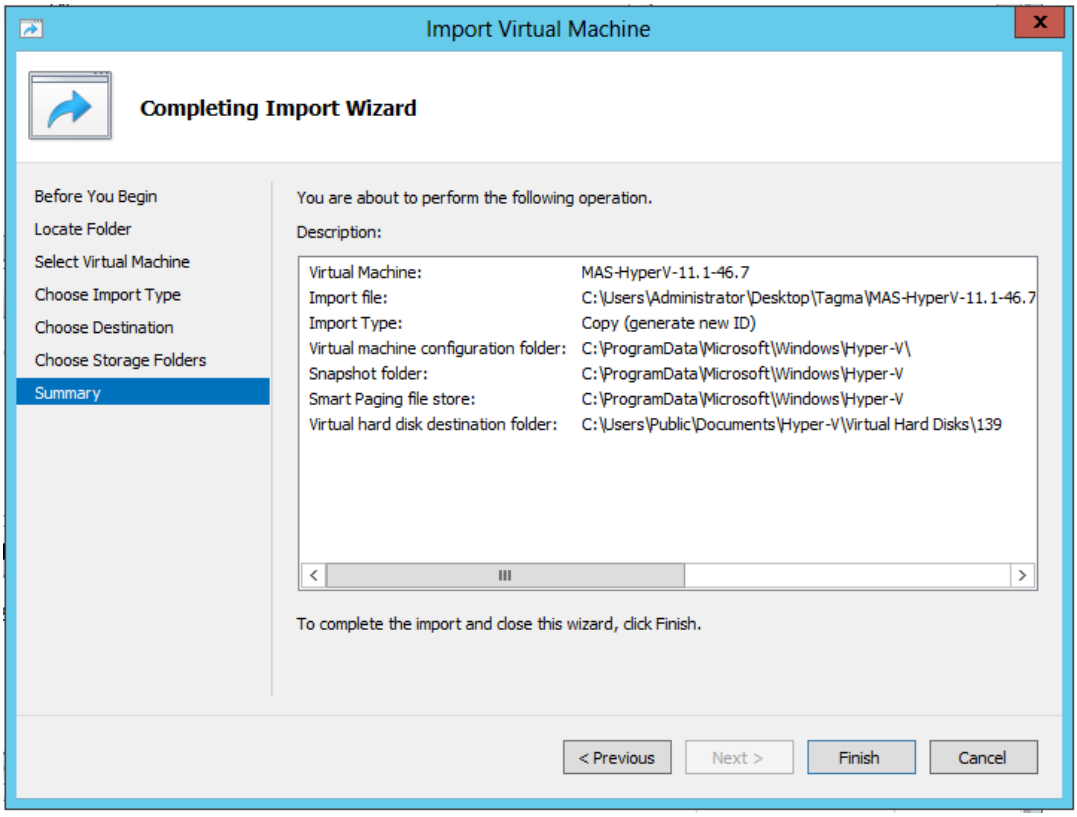
   d) ［**Choose Destination**］セクションで、仮想マシンファイルを格納するフォルダーを指定します。

   > 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。



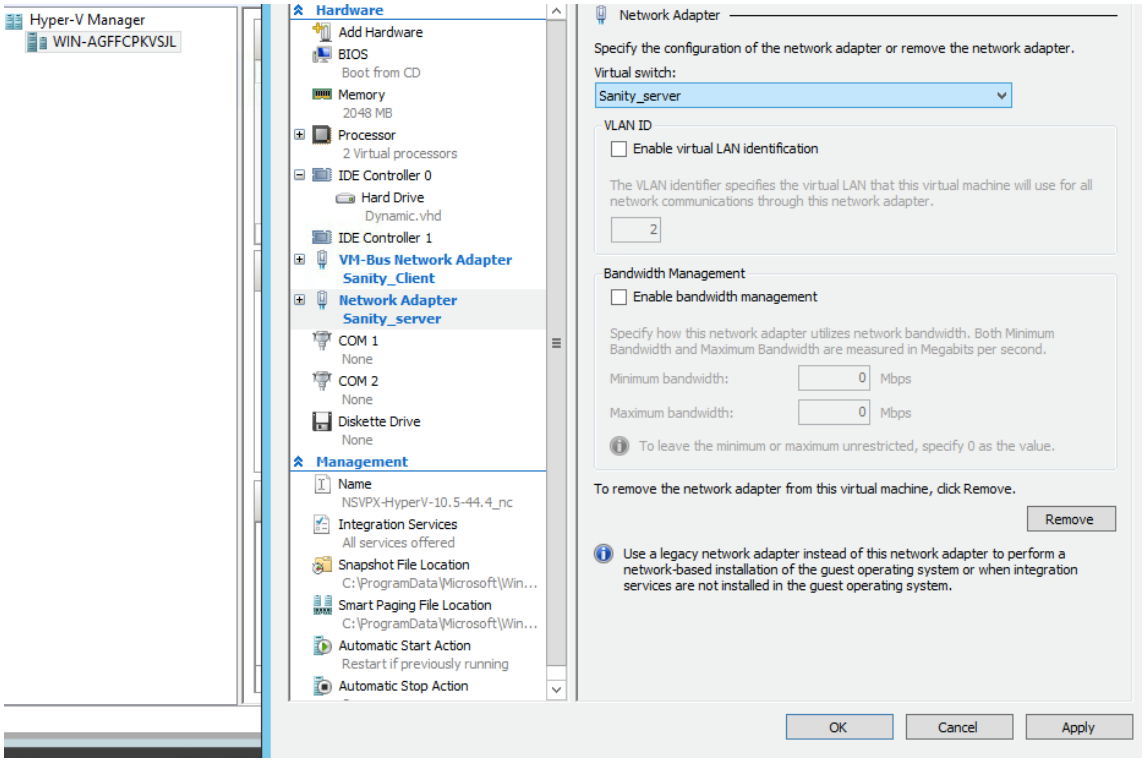
e) [**Choose Storage Folders**] セクションで、仮想ハードディスクを保存する場所を選択し、[**Next**] をクリックします。

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。



NetScaler 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. **NetScaler ADM Hyper-V** イメージを右クリックし、**[接続]** をクリックします。
8. 「コンソール」ウィンドウで、「開始」ボタンをクリックします。
9. 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。

```
deployment_type.py
<!--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 deplo
yment.
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. 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。
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

このドキュメントでは、VMware vSphere クライアントを使用して、VMware ESXi に NetScaler ADM 仮想アプライアンスをインストールする方法について説明します。

前提条件

仮想アプライアンスのインストールを開始する前に、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 用 VMware Tools はソフトウェアビルドの一部として提供され、個別にアップグレードまたは変更することはできません。

NetScaler ADM をインストールするには

ADM 仮想アプライアンスを VMware ESXi にインストールするには、次の手順に従います。

> 注
>
> 手順とスクリーンキャプチャは、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。

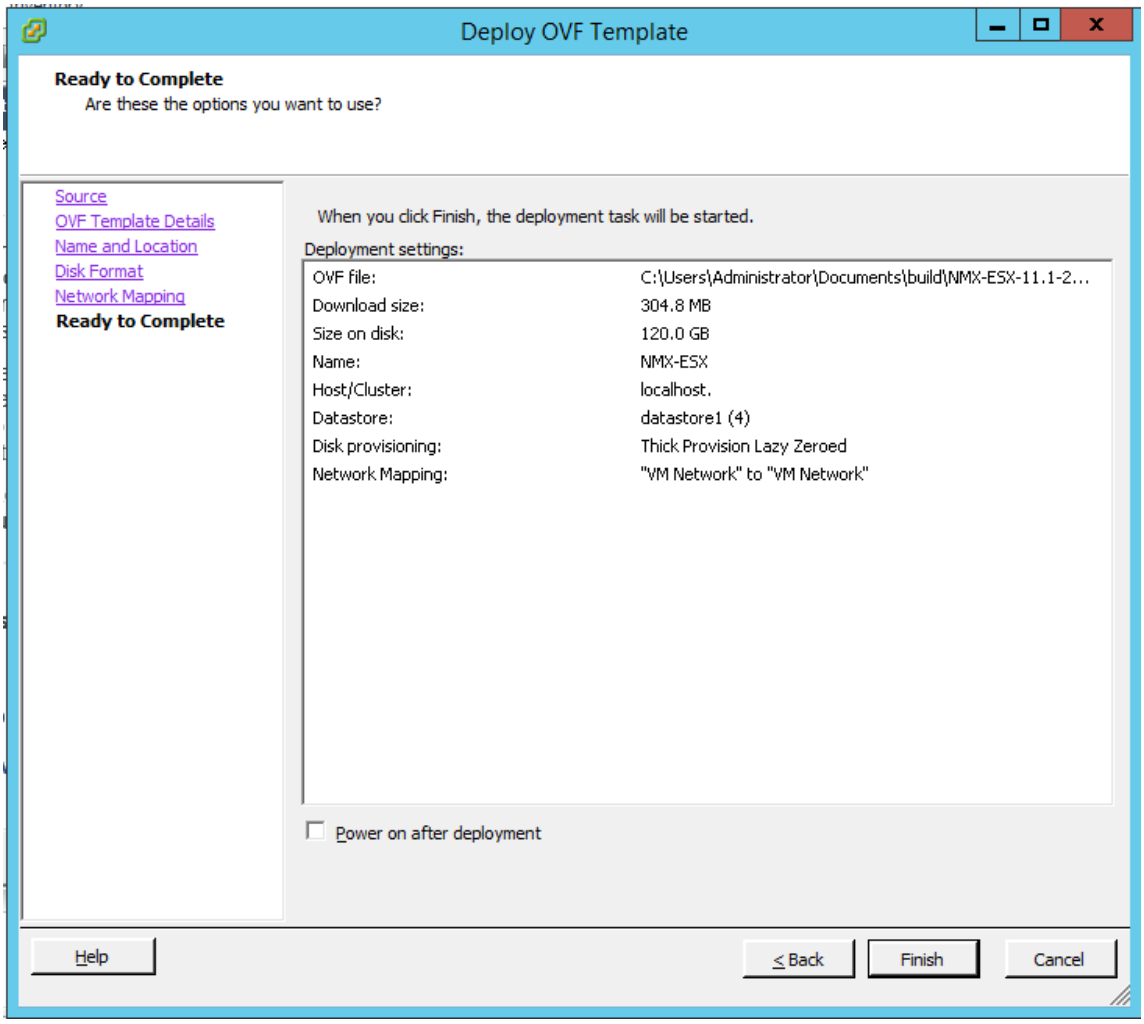
5. [**OVF** テンプレートのデプロイ] ダイアログボックスの [ファイルまたは **URL** からのデプロイ] で、.ovf ファイルを選択し、[次へ] をクリックします。

   > 注
   >
   > 「オペレーティングシステム識別子は選択したホストではサポートされていません」という警告メッセージが表示された場合は、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確認してください。[はい] をクリックします。

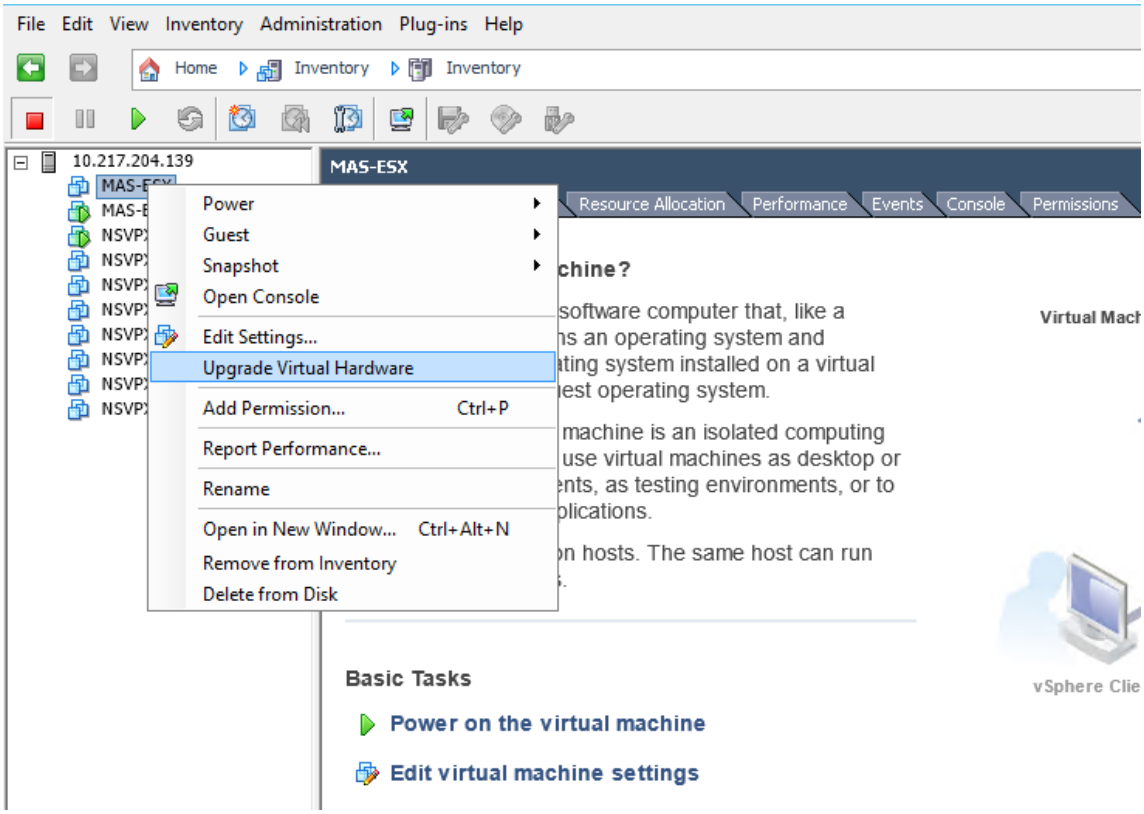
6. [**OVF** テンプレートの詳細] ページで、[次へ] をクリックします。
7. NetScaler ADM 仮想アプライアンスの名前を入力し、[次へ] をクリックします。
8. [Disk Format] で [Thin provisioned format] または [Thick provisioned format] を選択し、ディスク形式を指定します。

   > 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。

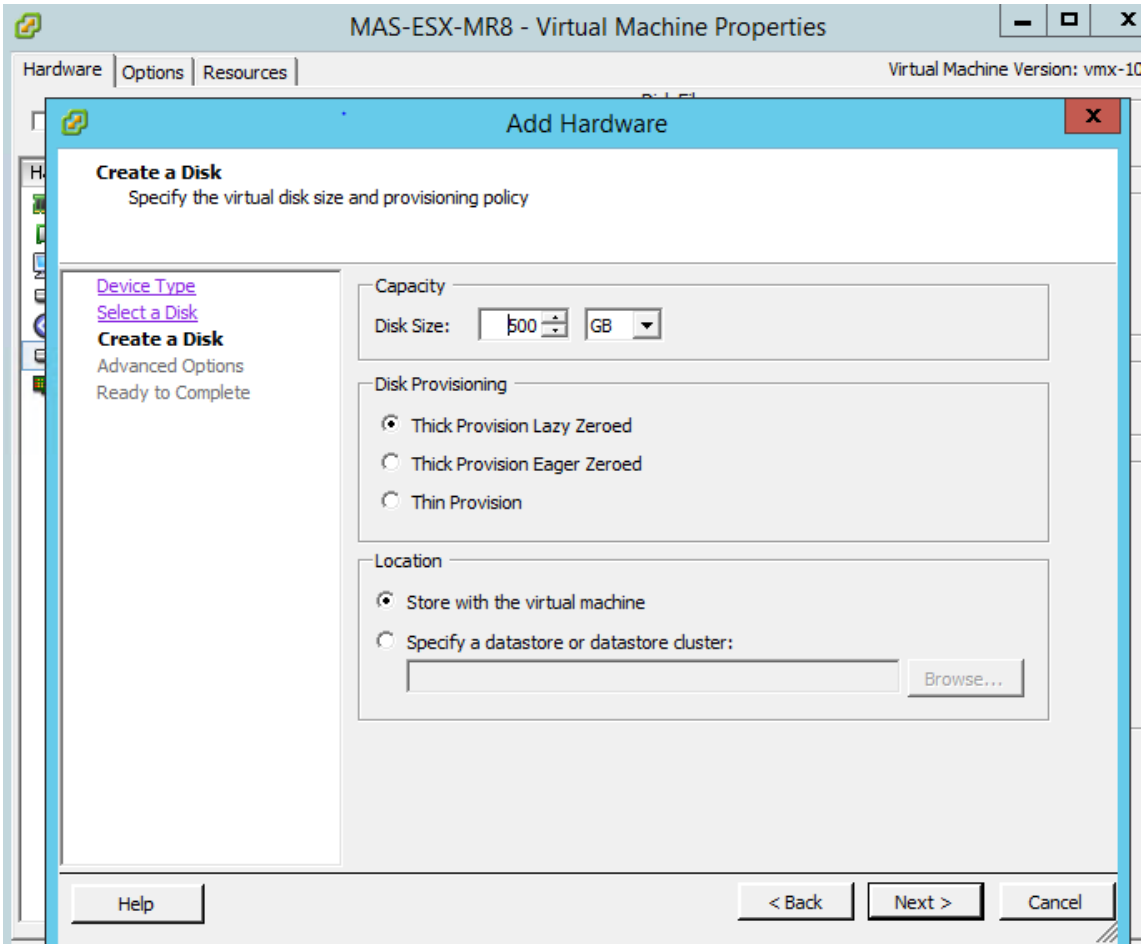
9. [完了] をクリックして、インストールプロセスを開始します。



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

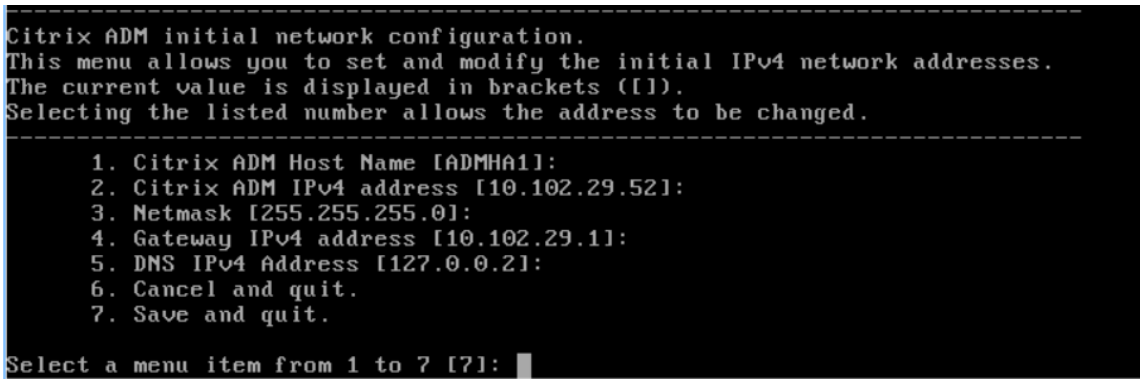


12. [インベントリ] メニューで、[仮想マシン] をクリックし、[設定の編集] をクリックします。
13. [仮想マシンのプロパティ] ダイアログボックスの [ハードウェア] タブで [メモリ] をクリックし、右側のペインで [メモリサイズ] に 32 GB を指定します。
14. [**CPU**] をクリックし、右側のペインで CPU を 8 と指定します。[**OK**] をクリックします。
15. 要件に応じて余分なディスクを追加します。



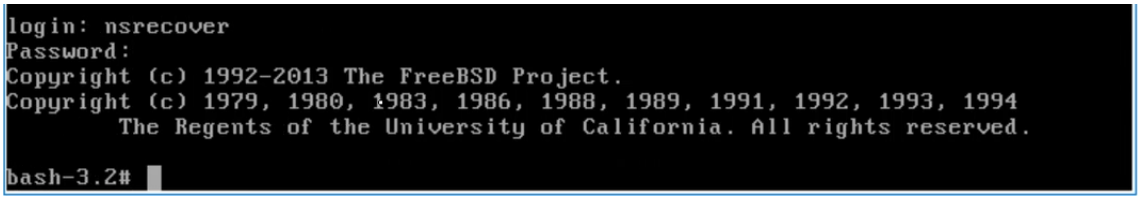
16. ナビゲーションペインで、インストールした仮想アプライアンスを選択します。[インベントリ] メニューから、[仮想マシン]、[パワー]、[パワーオン] の順にクリックします。

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。



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。

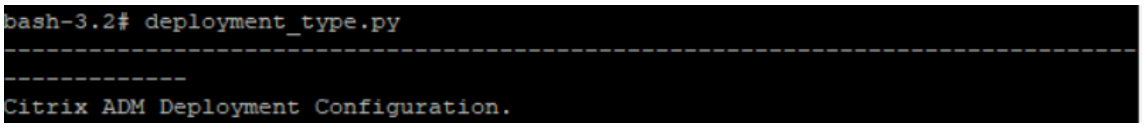
19. プロンプトが表示されたら、nsrecover/nsroot 認証情報を使用してログオンします。



> 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。

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



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。

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:
>
> 通常 ADM のインストール時間は VMware ESXi では約 10 分ですが、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。

VMware ESXi への NetScaler ADM エージェントのデプロイを自動化します

February 6, 2024

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

管理者は、次のアクションを自動化できます。

- NetScaler ADM エージェントの構成
- NetScaler ADM エージェントを登録し、エージェントのデフォルトパスワードを変更します。

NetScaler ADM エージェントの構成

エージェントの設定を自動化するには、.ovf ファイルに次のパラメータの値を追加します。

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

> 注:
>
> .ovf ファイルはエージェントイメージファイルにあります。NetScaler ADM エージェントファイルをダウンロードするには、https://www.citrix.com/downloads/citrix-application-management/を参照してください。エージェントイメージファイルの命名パターンは次のとおりです。**MASAGENT-ESX-releasenumber-buildnumber.zip**

NetScaler ADM エージェントの登録とデフォルトパスワードの変更

> 注
>
> デフォルトパスワードを登録して変更する前に、NetScaler ADM エージェントの構成で指定されているパラメーターを追加していることを確認してください。

NetScaler ADM エージェントの登録とデフォルトパスワードの変更を自動化するには、同じ.ovf ファイルに次のパラメーターの値を追加します。

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

前提条件

仮想アプライアンスのインストールを開始する前に、次のことを確認してください。

- 最小システム要件を満たす管理ワークステーションに VMware vSphere 8.x をインストールします。
- NetScaler ADM セットアップファイルをダウンロードします。

NetScaler ADM エージェントを構成して登録する方法

1. .OVF ファイルのダウンロードと編集
2. NetScaler ADM 仮想アプライアンスを VMware ESXi にインストール
3. 確認

.OVF ファイルのダウンロードと編集

1. MASAGENT-ESX-releasenumber-buildnumber.zip から目的の場所にファイルを抽出します。次のファイルを使用できます。
    - .ovf ファイル
    - .vmdk ファイル
    - .ova ファイル
    - .mf ファイル
2. 任意のエディターで.ovf ファイルを開き、</VirtualHardwareSection>タグの後に次の <ProductSection>..</ProductSection >サンプルコードを追加します

```
<ProductSection>
    <Info>Information about the installed software</Info>
    <Product>Application Delivery management</Product>
    <Vendor>Citrix</Vendor>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
       string"
    ovf:key="eth0.ip">
    <Label>IPAddress</Label>
    </Property>

```

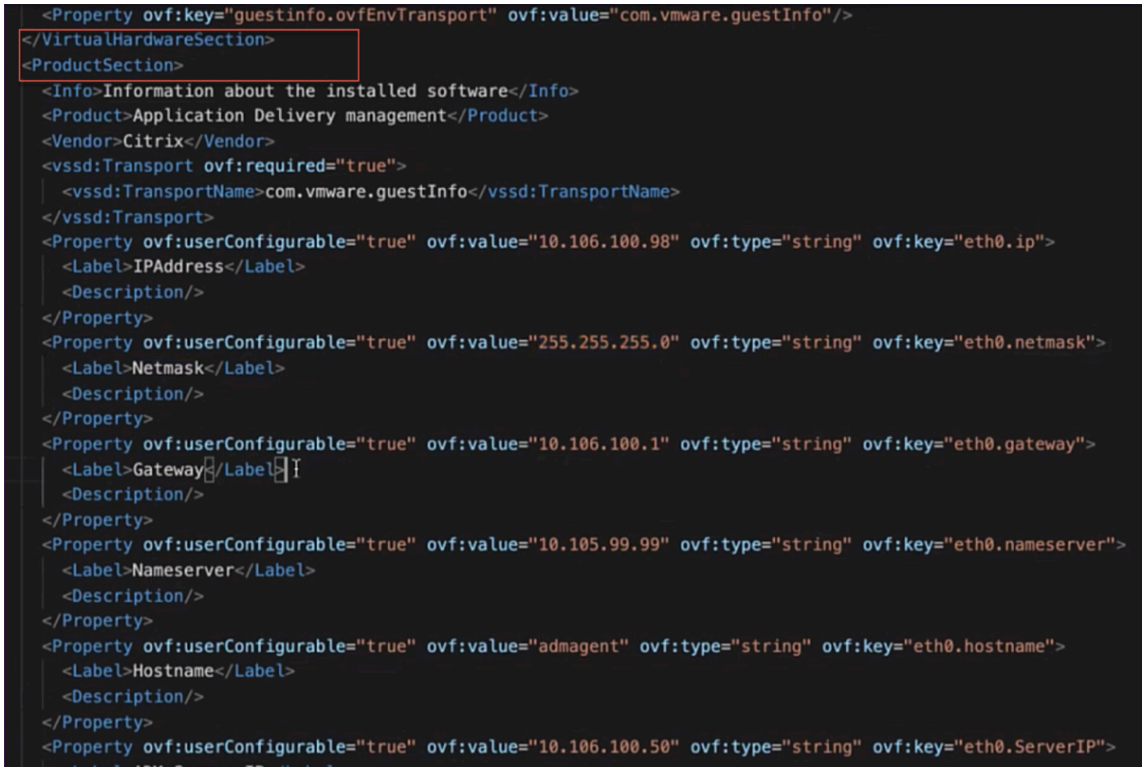


```
11      <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
            string"
12      ovf:key="eth0.netmask">
13      <Label>Netmask</Label>
14      </Property>
15
16      <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
            string"
17      ovf:key="eth0.gateway">
18      <Label>Gateway</Label>
19      </Property>
20
21      <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
            string"
22      ovf:key="eth0.nameserver">
23      <Label>Nameserver</Label>
24      </Property>
25
26      <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
            string"
27      ovf:key="eth0.hostname">
28      <Label>Hostname</Label>
29      </Property>
30
31      <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
            string"
32      ovf:key="eth0.ServerIP">
33      <Label>ADM Server IP</Label>
34      </Property>
35
36      <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
            string"
37      ovf:key="eth0.ServerUname">
38      <Label>ADM Username</Label>
39      </Property>
40
41      <Property ovf:userConfigurable="true" ovf:password="true" ovf:value
            ="VALUE"
42      ovf:type="string" ovf:key="eth0.ServerPassword">
43      <Label>ADM Password</Label>
44      </Property>
45
46      <Property ovf:userConfigurable="true" ovf:password="true" ovf:value
            ="VALUE"
47      ovf:type="string" ovf:key="eth0.NewPassword">
48      <Label>Agent New Password</Label>
49      </Property>
50
51  </ProductSection>
52  <!--NeedCopy-->
```

1. 設定したいパラメータについては、対応する値を OVF: value= “value” に追加します。

- NetScaler ADM エージェントを構成するには、次のパラメーターに値を追加します。
  - IP アドレス
  - ネットマスク
  - Gateway
  - ネームサーバー
  - ホスト名
- NetScaler ADM エージェントのデフォルトパスワードを登録して変更するには、次のパラメーターに値を追加します。
  - ADM サーバー IP
  - ADM ユーザー名
  - ADM パスワード
  - エージェントの新しいパスワード

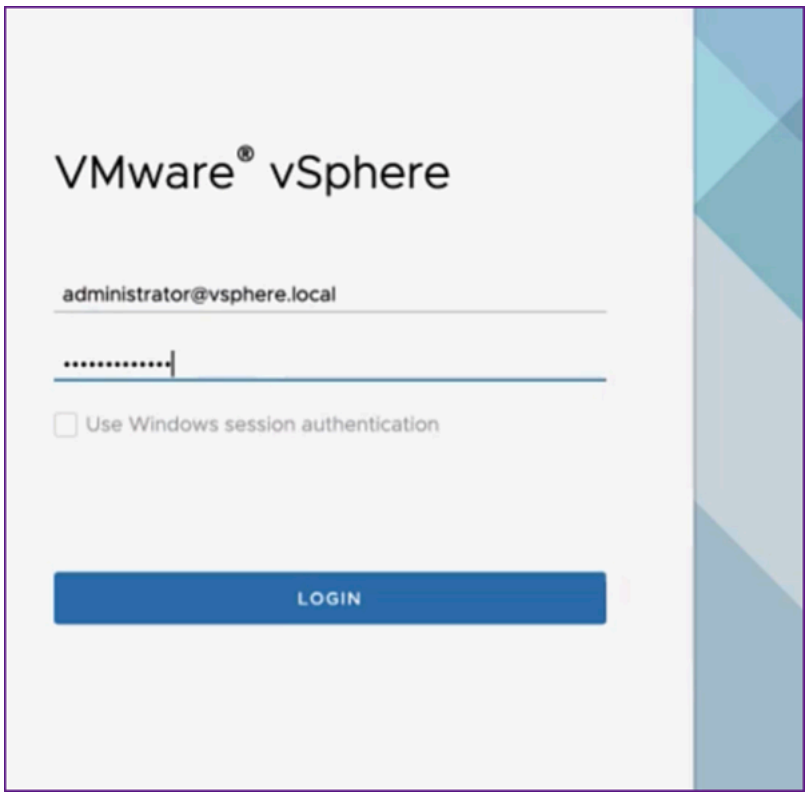
> 注
>
> - エージェントのデフォルトパスワードを登録して変更する前に、NetScaler ADM エージェントを構成する必要があります。
> - .ovf ファイルにデフォルトパスワードを登録および変更しない場合は、仮想マシンをデプロイした後にこれらのアクションを手動で実行する必要があります。



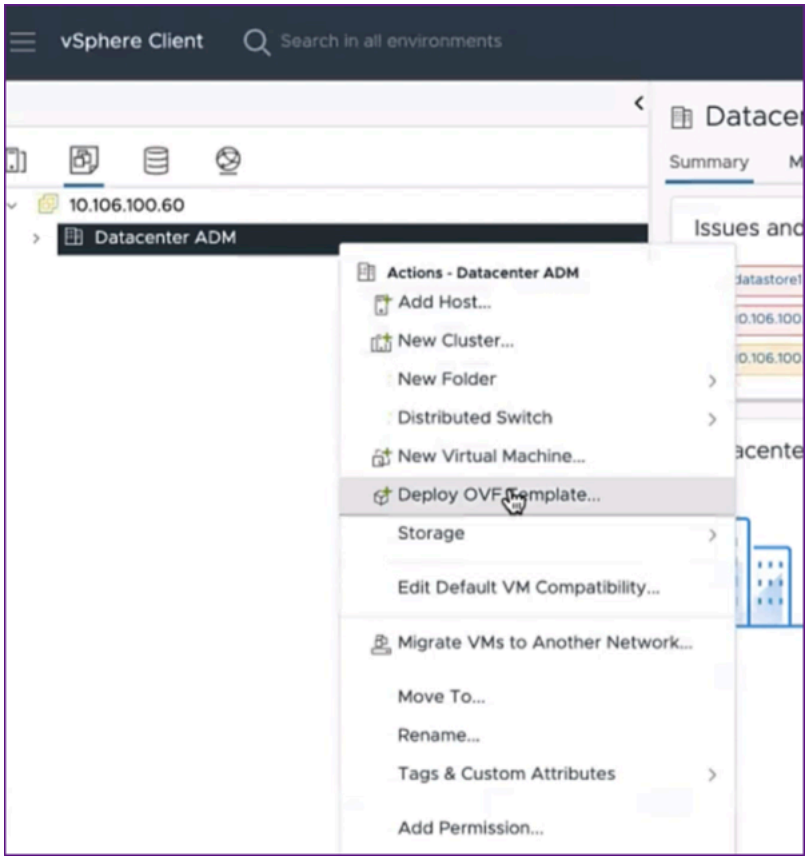
2. パラメータとその値を追加したら、.ovf ファイルを保存します。

NetScaler ADM 仮想アプライアンスを **VMware ESXi** にインストール

1. **VMware vSphere** クライアントにログインし、管理者の認証情報を入力します。[ログイン] をクリックします。

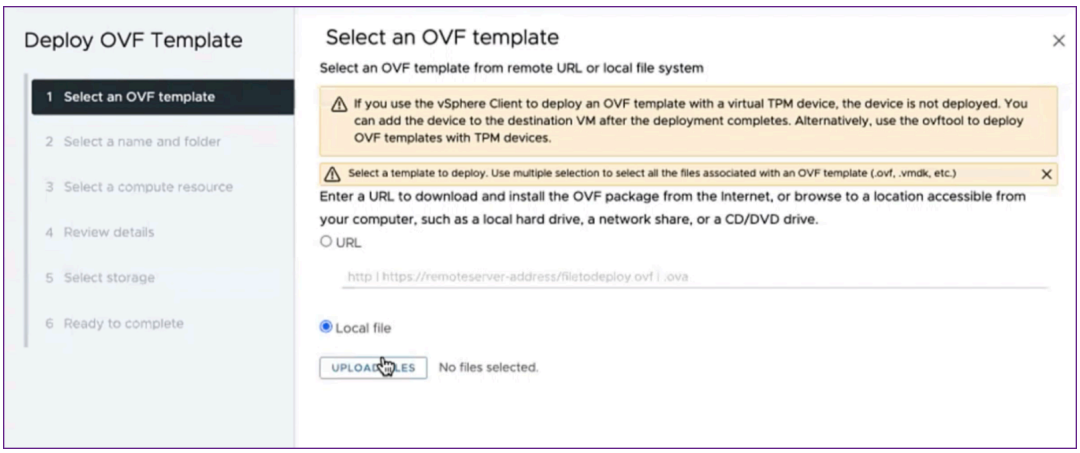


2. ESXi サーバを選択し、右クリックして [**OVF** テンプレートのデプロイ] を選択します。

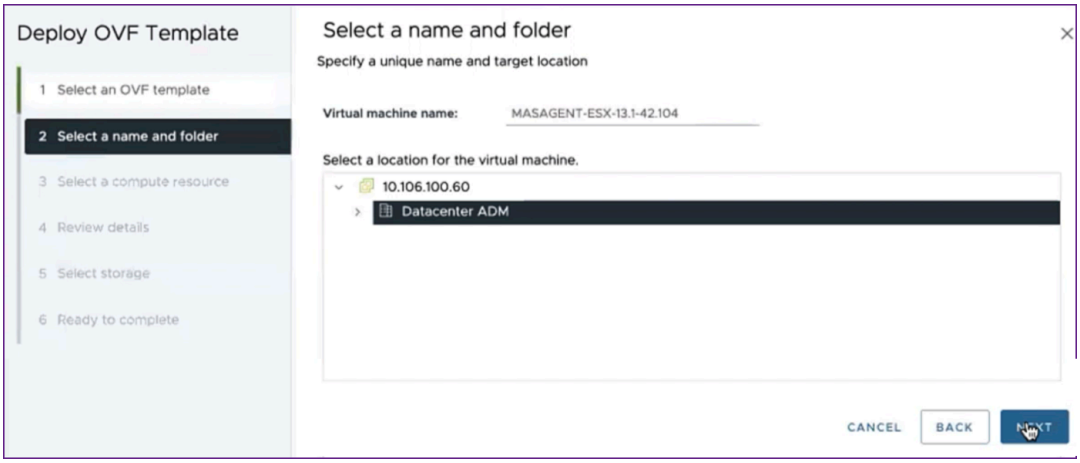


3.「**OVF** テンプレートのデプロイ」ページで:

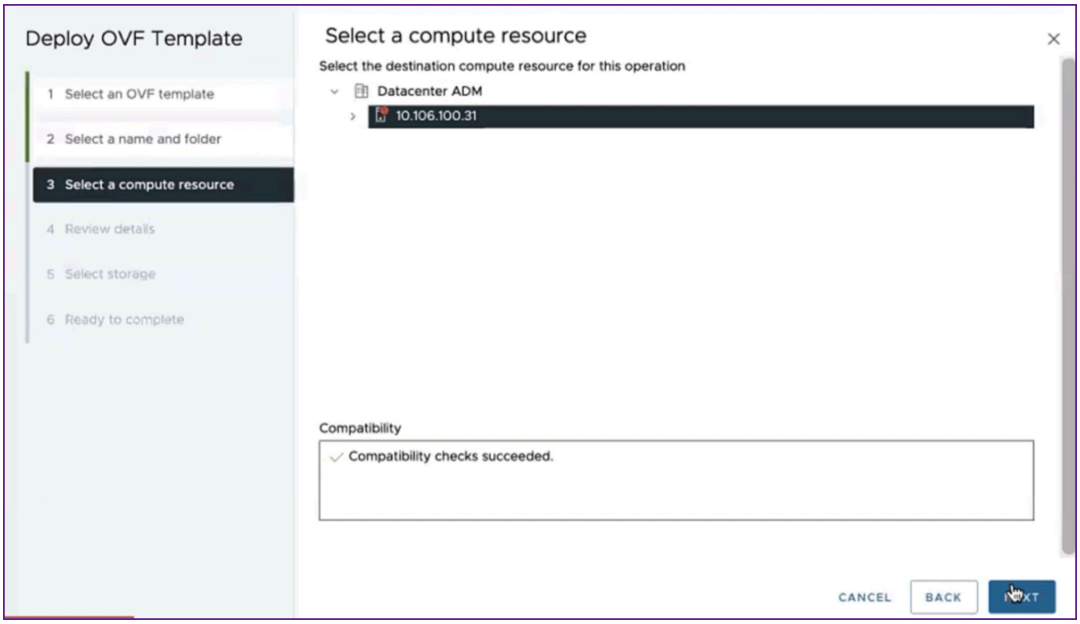
a) **OVF** テンプレートを選択:「ローカルファイル」を選択し、編集した.ovf ファイルと.vmdk ファイルを保存した場所に移動します。ファイルを選択して [開く] をクリックしてアップロードします。[次へ] をクリックします。



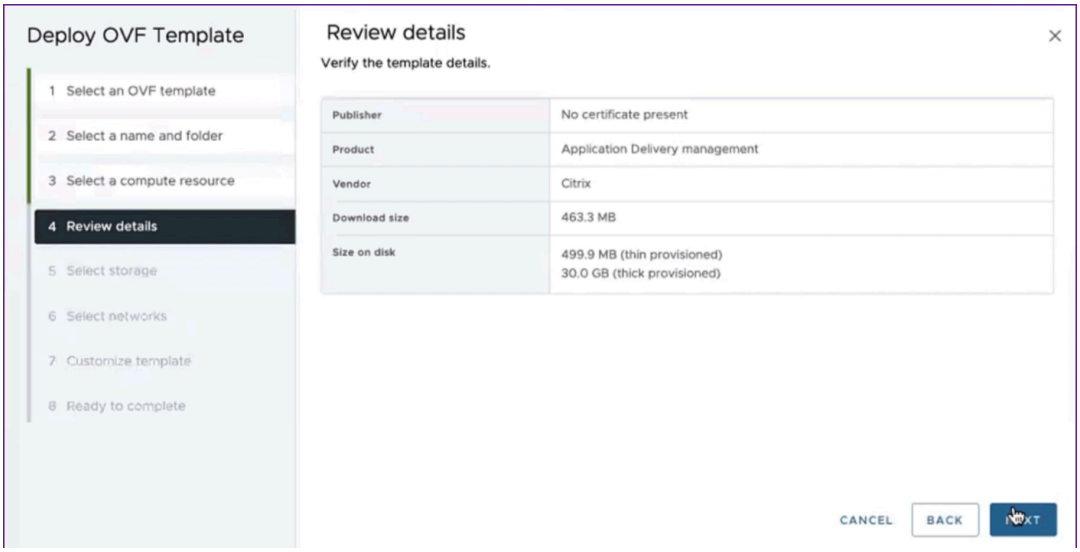
b) 名前とフォルダを選択: 仮想アプライアンスの名前を追加し、仮想マシンをデプロイする ESXi 上の場所を選択します。[次へ] をクリックします。



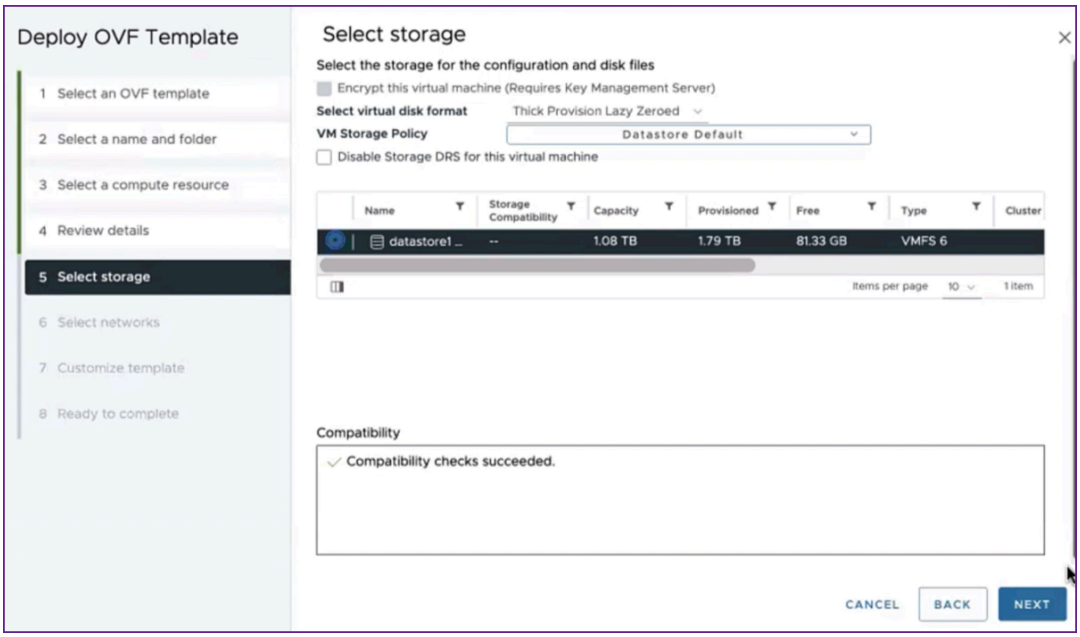
c) コンピュートリソースの選択: デプロイ後にテンプレートを実行するリソースを選択します。［次へ］をクリックします。



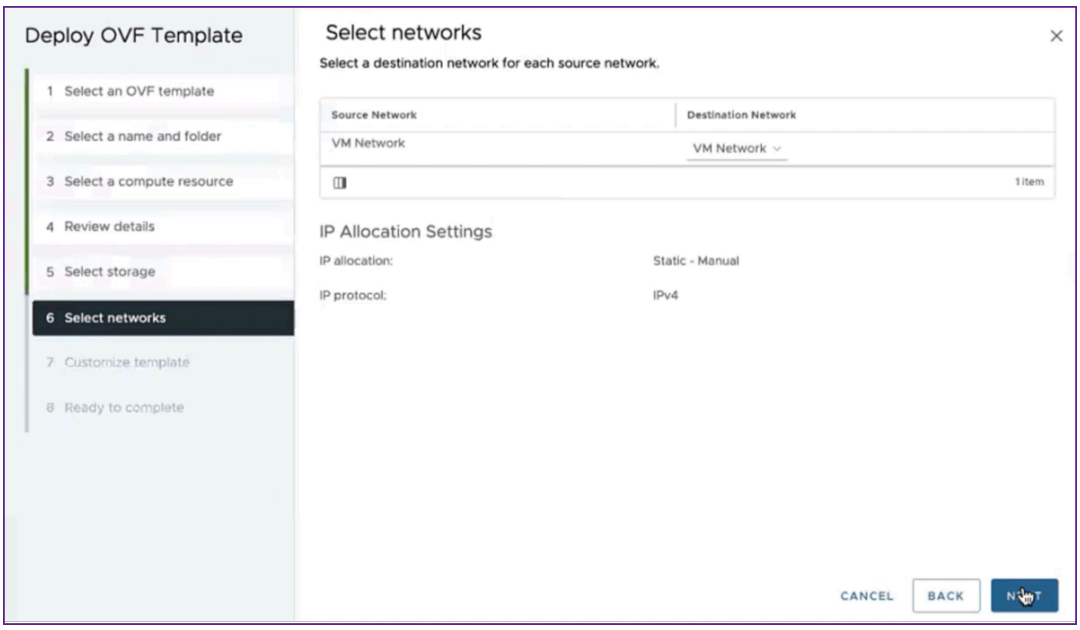
d) 詳細を確認:OVF テンプレートの詳細を確認します。［次へ］をクリックします。



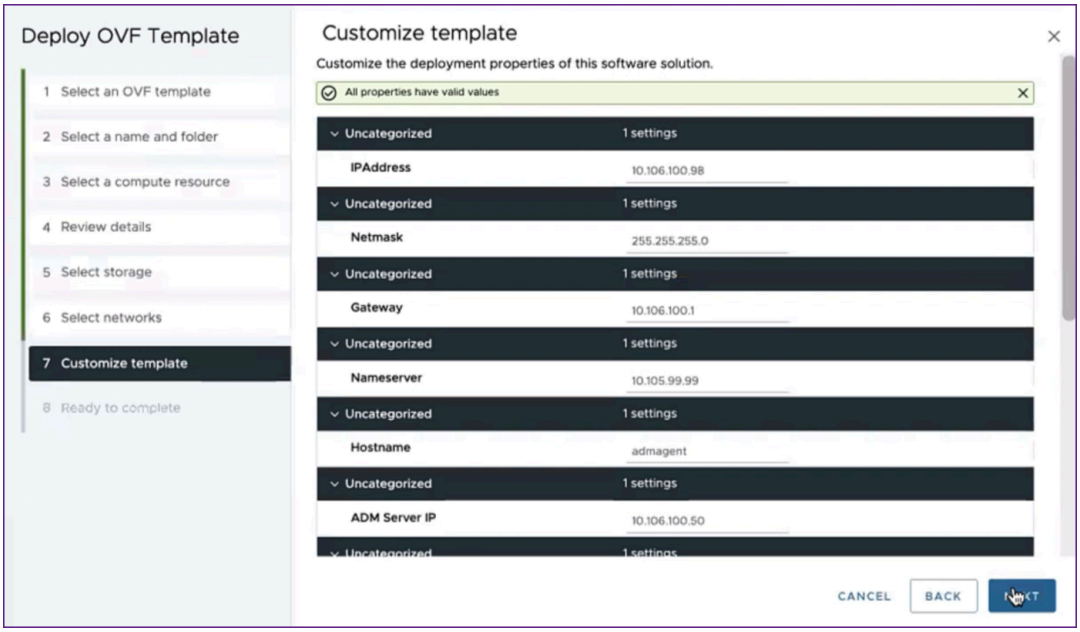
e) ストレージの選択:OVF テンプレートを保存するデータストアを選択します。［次へ］をクリックします。



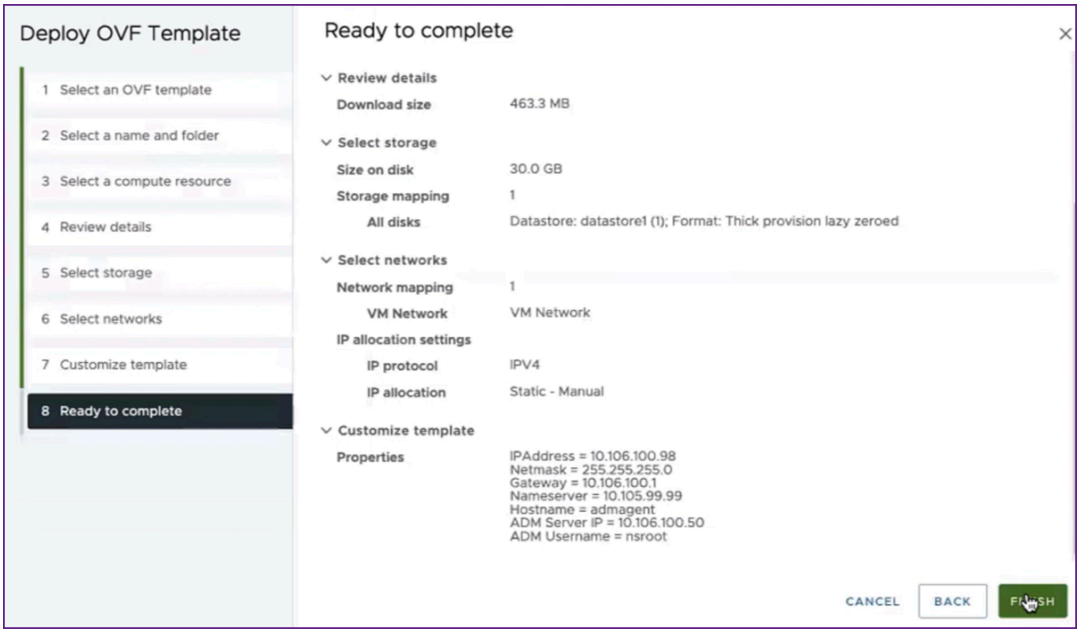
f) ネットワークの選択: デフォルト設定で続行します。［次へ］をクリックします。



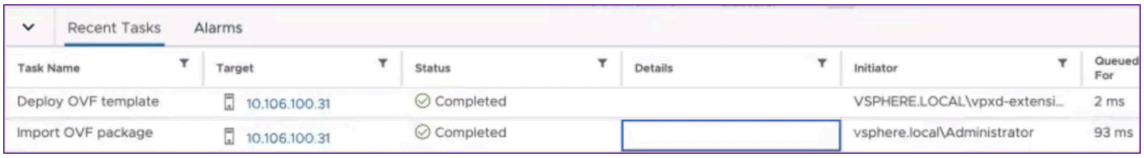
g) テンプレートのカスタマイズ:OVF テンプレートのすべてのプロパティを確認します。「.OVF ファイルのダウンロードと編集」セクションの.ovf ファイルに追加したすべてのパラメータと値が表示されます。



h) 準備完了: 設定を保存してデプロイプロセスを開始するには、「完了」をクリックします。

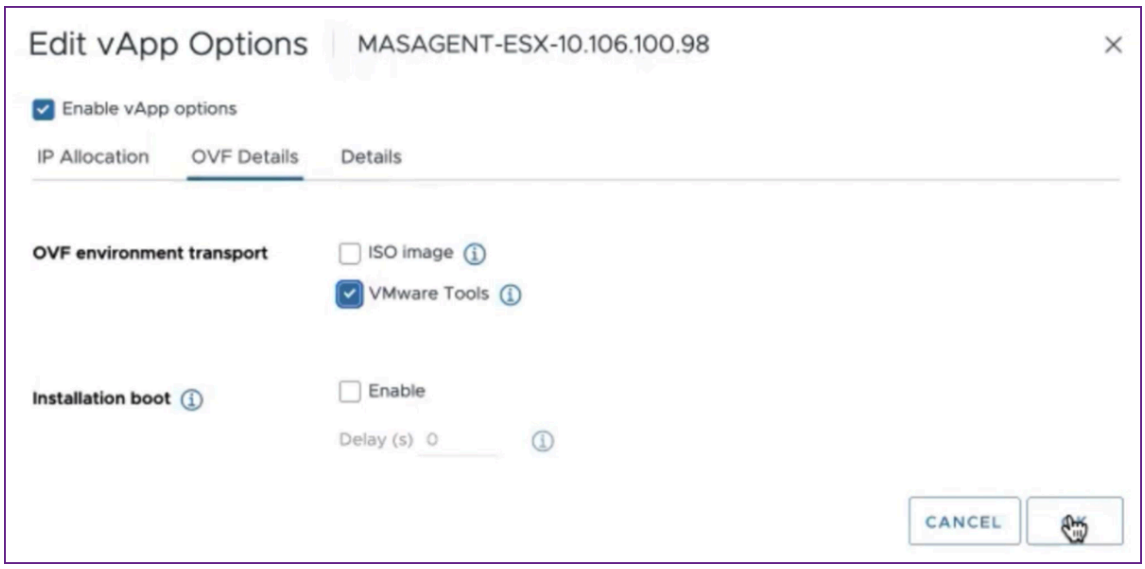


デプロイが完了するまでお待ちください。**Deploy OVF** テンプレート操作のステータスが 100% 完了すると、エージェントがデプロイされます。

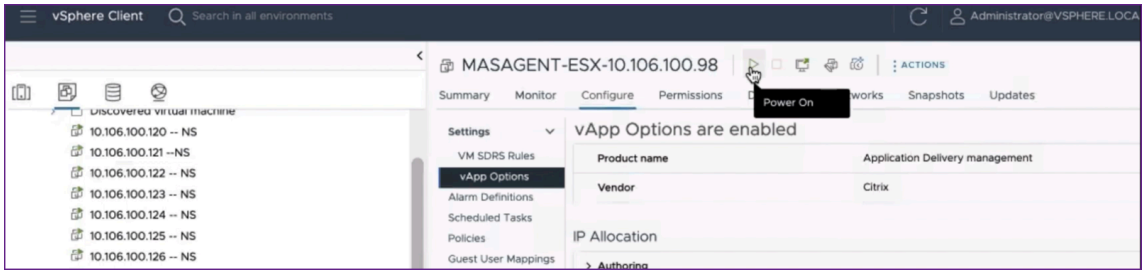


> 重要
>
> 設定を編集する前に仮想アプライアンスをパワーオンしないでください。

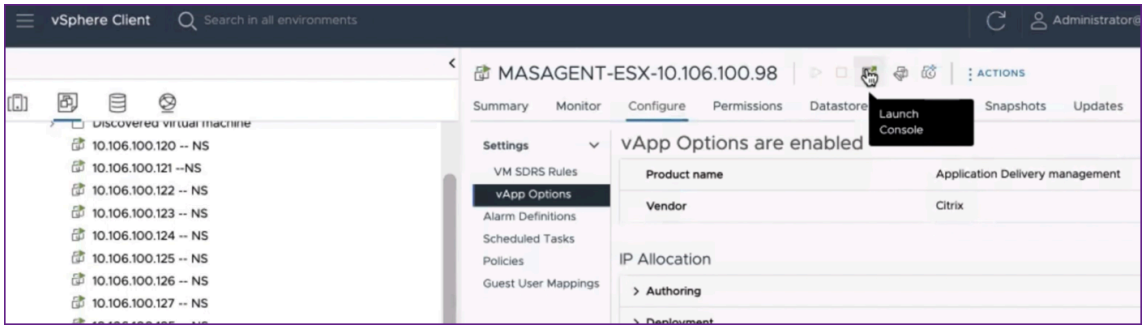
4. インストールした新しい仮想アプライアンスをクリックし、[構成] **> [**設定**] > [vApp** オプション**] > [**編集] に移動します。
5. [**vApp** オプションの編集] ウィンドウで、[**OVF** 詳細**] > [OVF** 環境トランスポート] に移動し、[**VMware Tools**] を選択します。[**OK**] をクリックします。

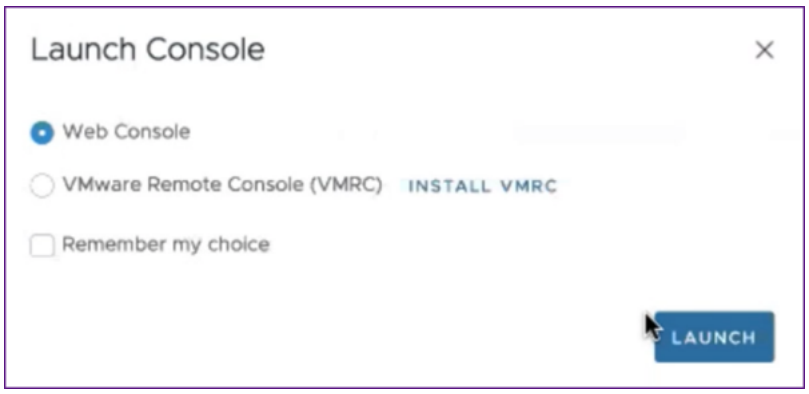


6. 仮想マシンを右クリックして、[パワーオン] をクリックします。別の方法として、仮想マシンの [サマリ] タブを選択し、[パワーオン] をクリックすることもできます。

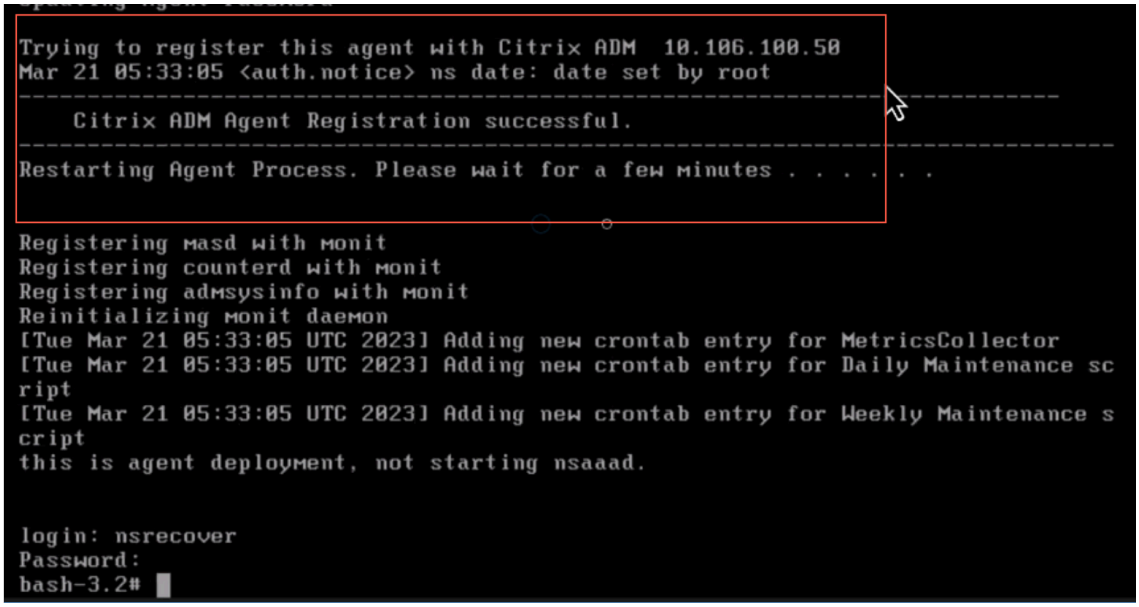


7. 「概要」タブで、「**Web** コンソールを起動」を選択します。
「コンソールの起動」ウィンドウで、「**Web** コンソール」を選択します。[**Launch**] をクリックします。





8. NetScaler ADM エージェントが NetScaler ADM サーバーに登録されると、コンソールに正常に登録されたことを示すメッセージが表示されます。NetScaler ADM エージェントが展開され、デフォルトのパスワードが変更されたことを確認するには、NetScaler
   ADM エージェントのユーザー名と新しいパスワードでログインします。



確認

NetScaler ADM エージェントが展開されていることを確認するには:

1. NetScaler ADM エージェントが展開されたら、ブラウザに NetScaler
   ADM サーバーの IP アドレスを入力して NetScaler ADM GUI にアクセスします。
2. 認証情報を使用してサーバーにログインします。
3. インフラストラクチャ **>** インスタンス **>** エージェントに移動します。
   新しくデプロイされたエージェントが ESX Platform に表示されます。

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 クラスター

- 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 v1.20
  - クライアントバージョン v1.20

  `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ている Helm アプリケーションは、クライアントバージョンが v3.4.0 以上である必要があります。

  `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 v3.21.1 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があるデータの量によって異なります。最小サイズは 100 GB です。
本番環境では、本番グレードの NFS ソリューションを使用することをお勧めします。

NetScaler アプライアンス

NetScaler アプライアンスは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 クラスタに ADM をインストールする

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

1. NetScaler サイトにアクセスして 、Kubernetes 用 NetScaler ADM Helm チャートのファイルをダウンロードしてください。
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` ディレクトリの下の `/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 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 で構成された仮想 IP。
    - `applicationID`: NetScaler 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 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 アプライアンスにアクセスするためのユーザー名。このユーザーは書き込み権限を持っている必要があります。
- `ingressADCPassword`: ユーザー名のパスワード。

```
# 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"

# ingressADCUsername is the password for above username
ingressADCPassword: "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ー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、NetScaler ADM を Linux-KVM プラットフォームにインストールし、ネットワークに合わせて構成します。

前提条件

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

ハードウェア要件

コンポーネント	条件
CPU	インテル VT-X プロセッサー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 プロセッサー。ホスト Linux-KVM に 2 つ以上の CPU コアを指定します。注：CPU が Linux ホストをサポートしているかどうかをテストするには、ホスト Linux シェルプロンプトで次のコマンドを入力します。*. egrep'^flags .* (vmx | svm)'/proc/cpuinfo*拡張機能の BIOS 設定が無効になっている場合は、BIOS で有効にする必要があります。プロセッサ速度に関する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。
メモリ (RAM)	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。
ハード ディスク	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 NetScaler ADM 仮想マシンには 120 GB のディスク容量が必要です。

> 注
>
> ここで指定するメモリとハードディスクの要件は、ホスト上で他の仮想マシンが実行されていないことを考慮して、OpenStack プラットフォームに NetScaler ADM を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

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

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

2. ［サインイン］オプションに カーソルを合わせ、［**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、**NetScaler Application Delivery Management** を選択します。
5. ［**NetScaler Application Delivery Management** ］ページで、リリースを選択します。たとえば、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、NetScaler 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. NetScaler ADM 属性を指定するドメイン XML ファイル

      ii. ドメインディスクイメージのチェックサム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

```
tar -xvfz MAS-KVM.tgz
MAS-KVM.xml
MAS-KVM.qcow2
checksum.txt
<!--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。

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

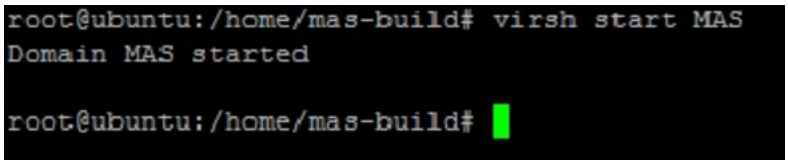
vi. 次のコマンドを使用して、MAS1-KVM.xml ファイルの仮想マシンの属性を定義します。`virsh define \<FileName\>.xml`

```
virsh define MAS-KVM.xml
Domain MAS defined from MAS-KVM.xml
<!--NeedCopy-->
```

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

root@ubuntu:~/mas-build#
```

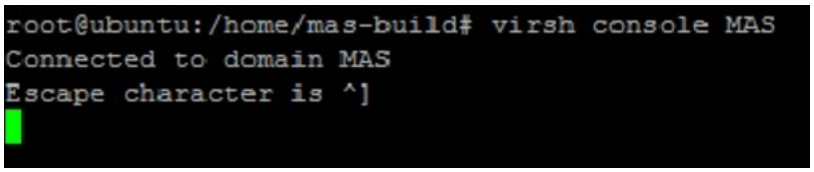
vii. 次のコマンドを入力して、NetScaler ADM を起動します。`virsh start \[\<DomainName\> | \<DomainUUID\>\]`


```
virsh start MAS
Domain MAS started
<!--NeedCopy-->
```



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

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



Citrix Application 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。NetScaler ADM 仮想アプライアンスを再起動すると、NetScaler 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。NetScaler ADM ホームページから、［設定］**>**［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。

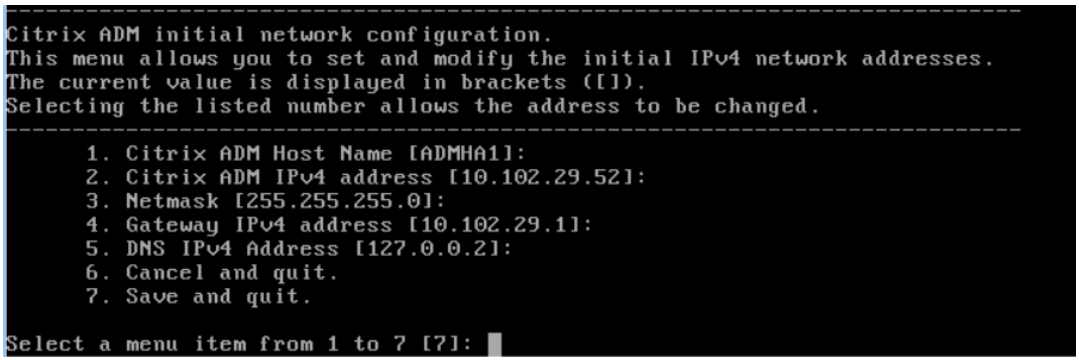
2. プロンプトで、「*shell*」と入力します。
3. **networkconfig** と入力して、NetScaler ADM の初期ネットワーク構成メニューに入ります。管理 IP アドレスを構成します。
4. NetScaler ADM の初期ネットワーク構成を完了するには、プロンプトに従います。コンソールには、NetScaler ADM の次のパラメーターを設定するための NetScaler ADM の初期ネットワーク構成オプションが表示されます。ホスト名は、デフォルトで設定されています。

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

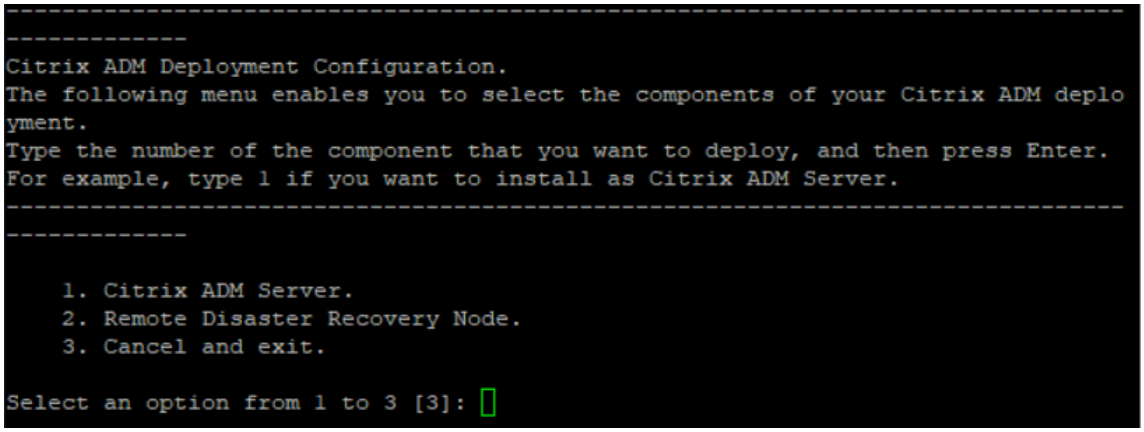
   b)「**3** 」を入力してネットマスク-管理 IP アドレスに関連付けられたサブネットマスクを更新します。

   c) **4** を入力してゲートウェイ **IPv4** アドレス（NetScaler ADM の管理 IP アドレスのサブネットのデフォルトゲートウェイ IP アドレス）を更新します

   d) 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。



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。



7. 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。
8. 「はい」と入力して NetScaler ADM サーバーを再起動します。
9. NetScaler ADM サーバーが再起動したら、コマンドラインまたは GUI からデフォルトの管理者資格情報（nsroot/nsroot）を使用して NetScaler ADM にログオンします。

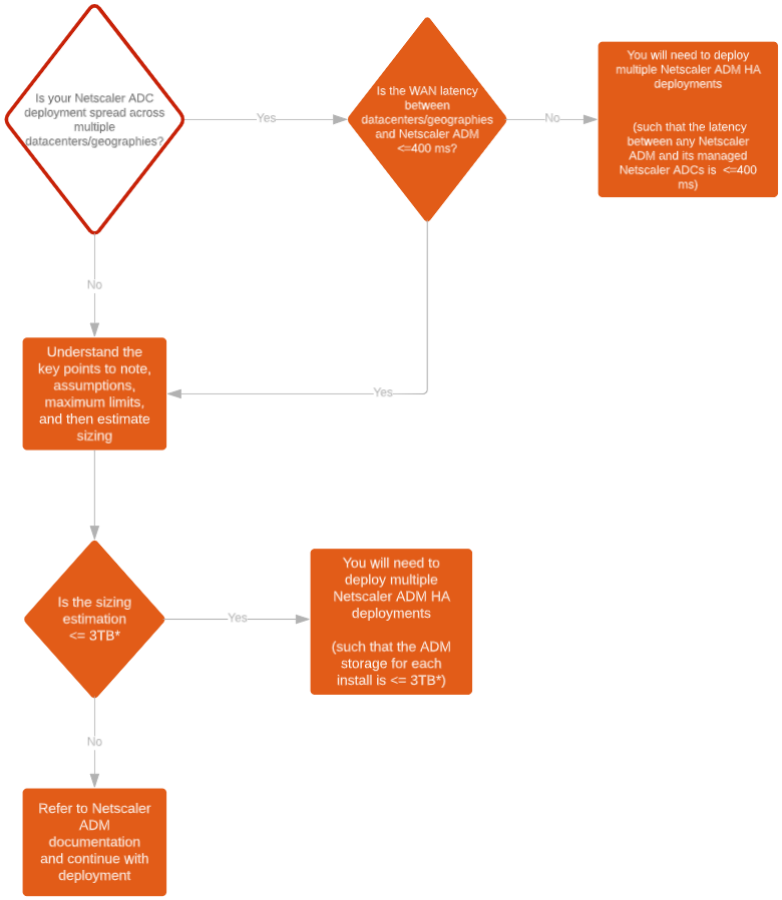
   ブラウザのアドレスバーに NetScaler ADM サーバーの IP アドレスを入力することで、後で NetScaler ADM にアクセスできます。サーバにログオンするためのデフォルトの管理者認証情報は *nsroot/nsroot* です。

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 2 つの NetScaler ADM ノードをアクティブ/パッシブモードで高可用性展開すると、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 **NetScaler ADM 12.1** ビルド **48.18** 以降のバージョンにアクセスするには:
>
> NetScaler ADM を高可用性モードで負荷分散するように NetScaler インスタンスを構成している場合は、まず NetScaler インスタンスを削除します。次に、高可用性モードで NetScaler ADM にアクセスするようにフローティング IP アドレスを構成します。

NetScaler ADM で高可用性を導入するメリットは次のとおりです。

- 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。

- プライマリノードでフローティング IP アドレスを構成できるため、個別の NetScaler ロードバランサーが不要になります。
- フローティング IP アドレスを使用して NetScaler ADM ユーザーインターフェイスに簡単にアクセスできます。
- NetScaler ADM ユーザーインターフェイスは、プライマリノードでのみ提供されます。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。

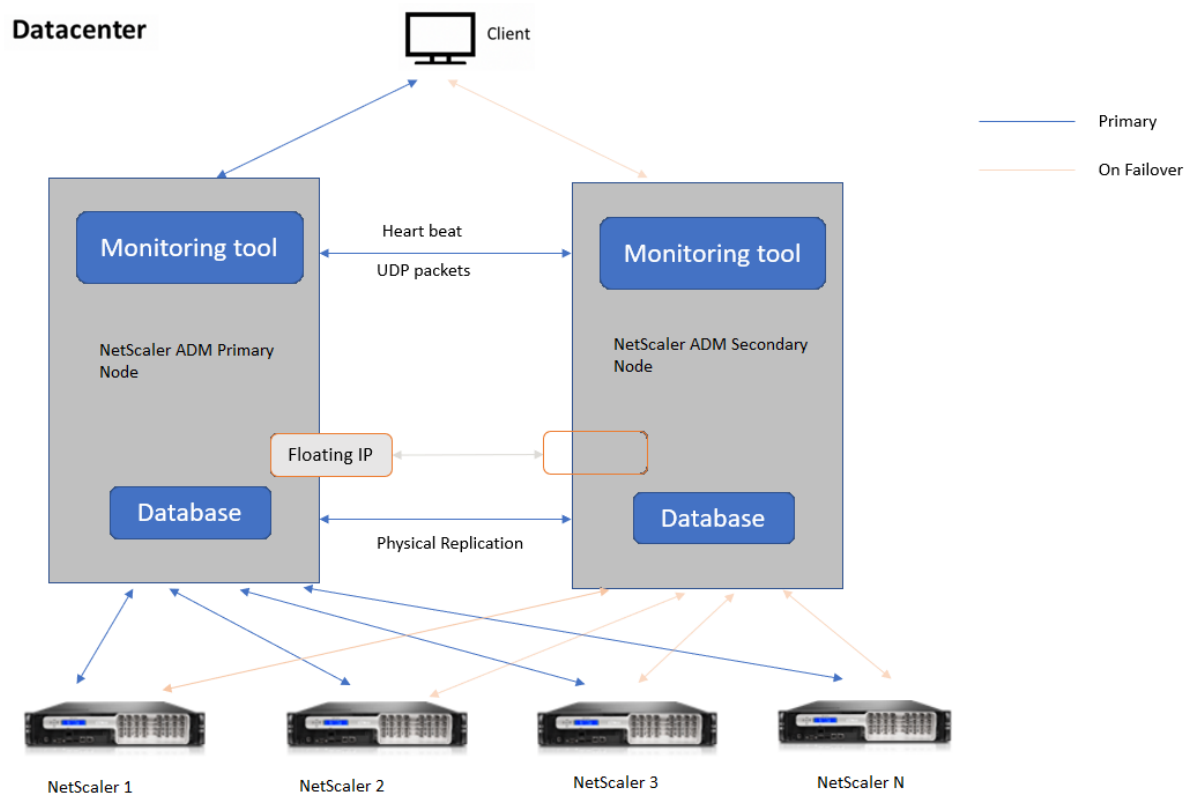
次の表は、高可用性導入で使用される用語をまとめたものです。

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。NetScaler ADM ユーザーインターフェイスにはプライマリノードからアクセスできます。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 NetScaler 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。NetScaler ADM のすべてのサブシステムとデータベースを監視して、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 アドレスに付けられたエイリアスで、クライアントはプライマリノードの NetScaler ADM に接続するために使用できます。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

- 高可用性セットアップでは、両方の NetScaler ADM ノードがアクティブ/パッシブモードで展開されます。これらは同じサブネット上にあり、同じソフトウェアバージョンとビルドを使用し、同じ構成で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。

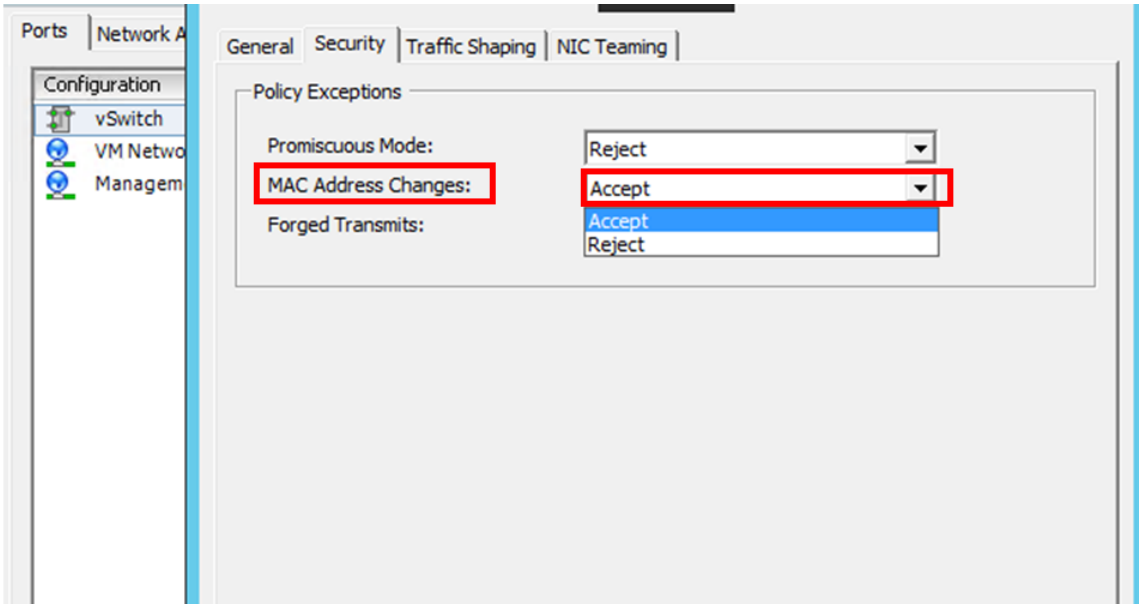
> 注
>
> Citrix では、ユーザーインターフェイスへのアクセスにはフローティング IP アドレスを使用することをお勧めします。

- 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:
  - 内部プロセスにより、NetScaler ADM が以前のバージョンから暗黙的にアップグレードされます。

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

- 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、NetScaler ADM を VMware ESXi の高可用性上に展開する場合は、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** に展開されている **NetScaler ADM** では、MAC アドレスの変更オプションを「拒否」に設定することもできます。フェールオーバー後、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

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

- NetScaler ADM の高可用性展開は、NetScaler ADM バージョン 12.0 ビルド 51.24 でサポートされています。
- NetScaler のサイトから NetScaler Application Delivery Management イメージファイル（.xva）をダウンロードします。https://www.citrix.com/downloads/

Citrix 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	**32 GB**
仮想 CPU	**8** 基の **CPU**

コンポーネント	条件
記憶域	Citrix では、NetScaler ADM の導入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推奨しています。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。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。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、「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。
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

NetScaler 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

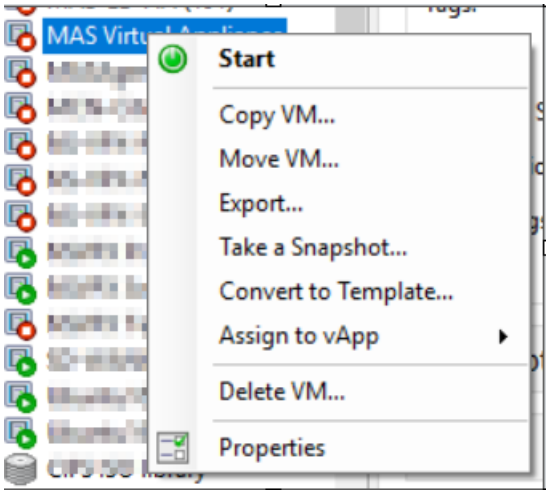
最初のノードを登録するには:

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

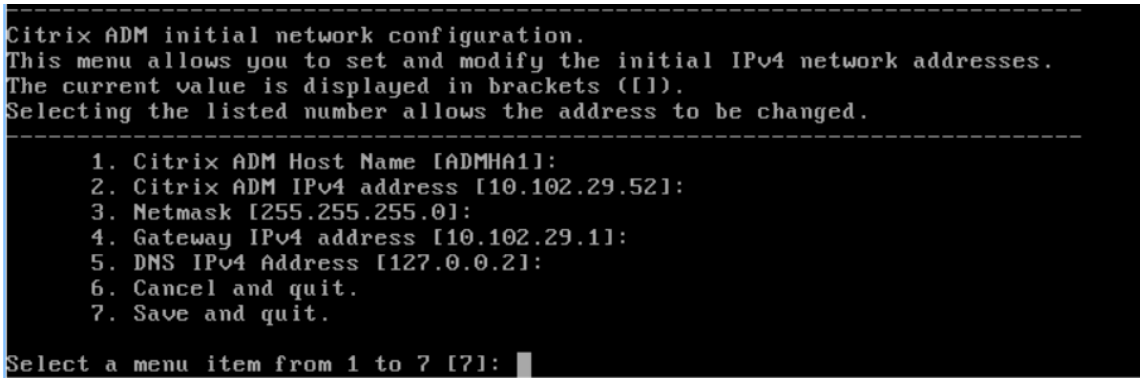
   > 注**:**
   >
   > .xva イメージファイルをインポートして開始するまでに数分かかる場合があります。画面下部にステー

> 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］タブで、NetScaler ADM を初期ネットワーク構成で構成します。



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。NetScaler 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 deplo
yment.
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]:
```

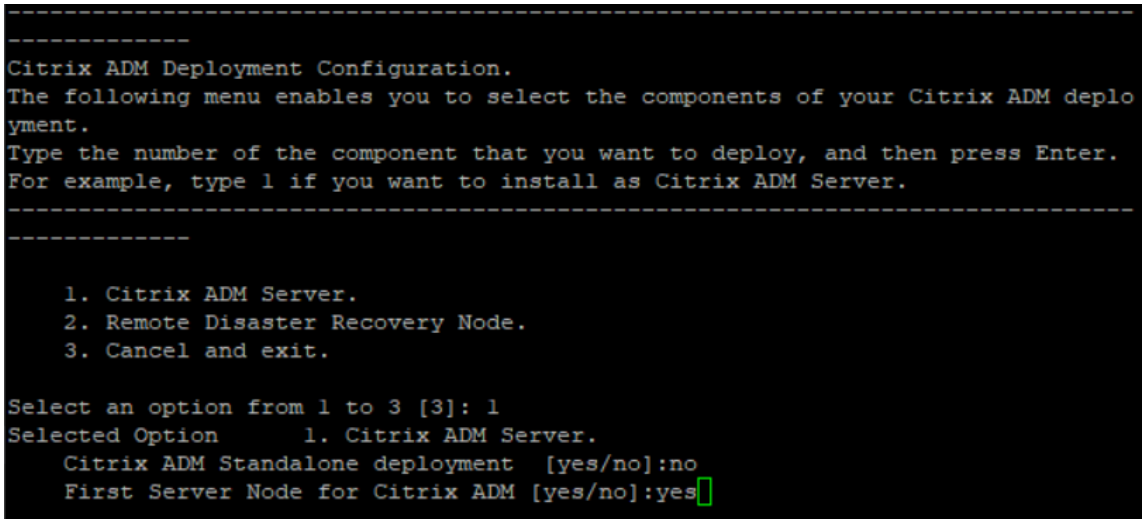
6. **1** を選択して、NetScaler ADM サーバーをプライマリノードとして登録します。

```
bash-3.2# /mps/deployment_type.py
--------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
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]:
```

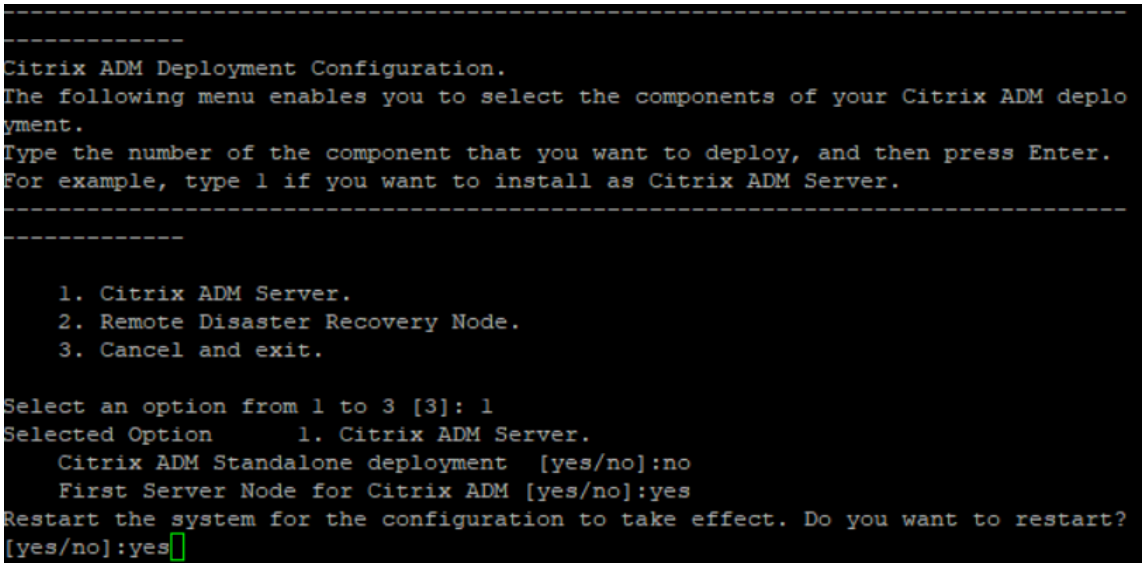
7. コンソールで、NetScaler ADM スタンドアロン展開を選択するように求められます。**No** と入力して、展開を高可用性として確認します。

```
--------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
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。



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。



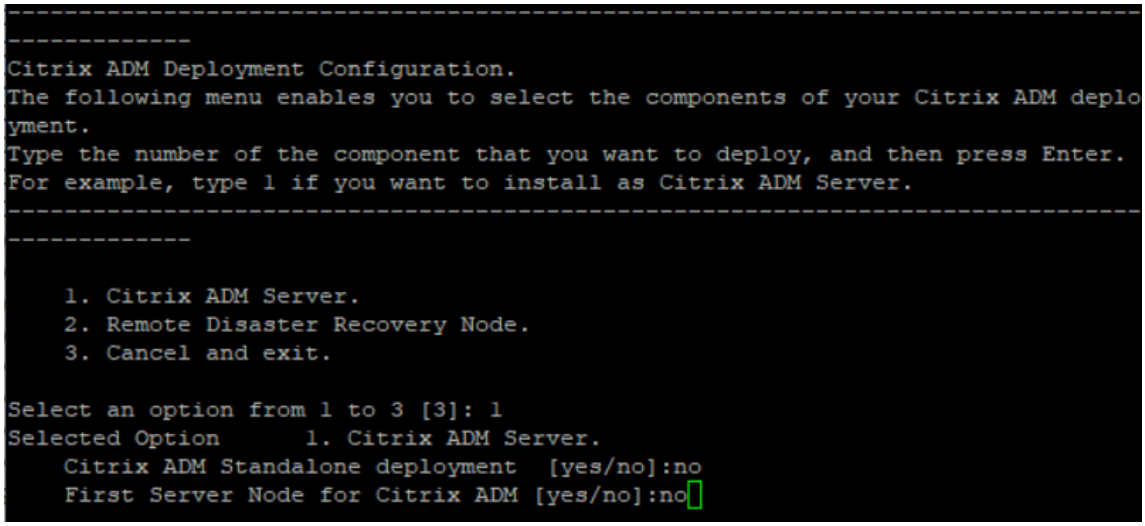
システムが再起動し、NetScaler ADM ユーザーインターフェイスにプライマリノードとして表示されます。

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

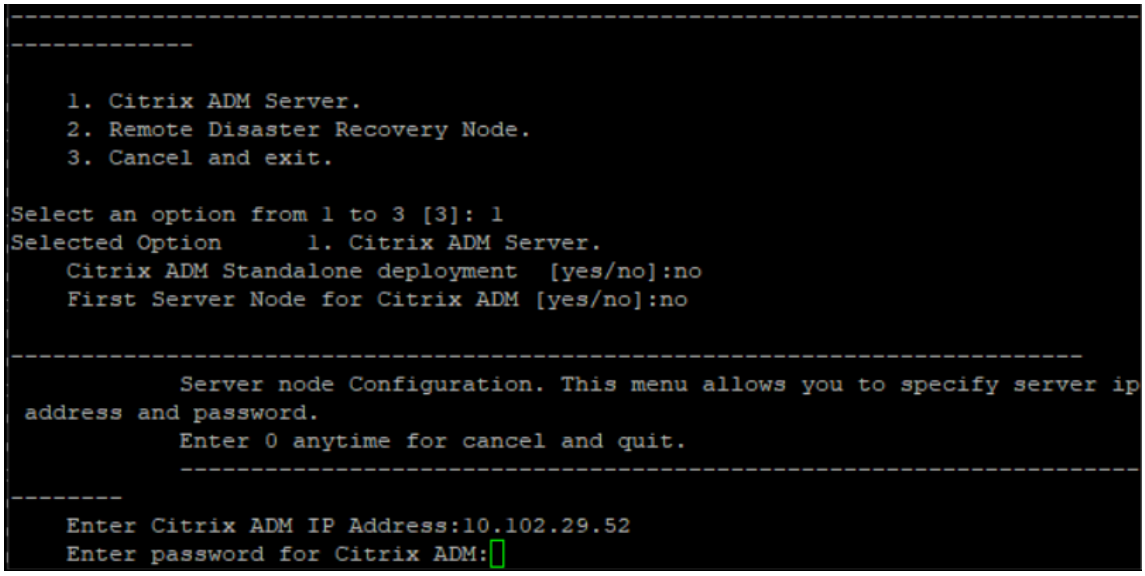
1. **NetScaler** サイトからダウンロードした**.xva** イメージファイルを使用して、ハイパーバイザーにインポートします。
2. [コンソール] タブから、次の図に示す初期ネットワーク構成で NetScaler ADM を構成します。
3. 初期ネットワーク設定が完了すると、システムはログインを要求します。次の認証情報（*nsrecover/nsroot*）を使用してログオンします。

> 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。

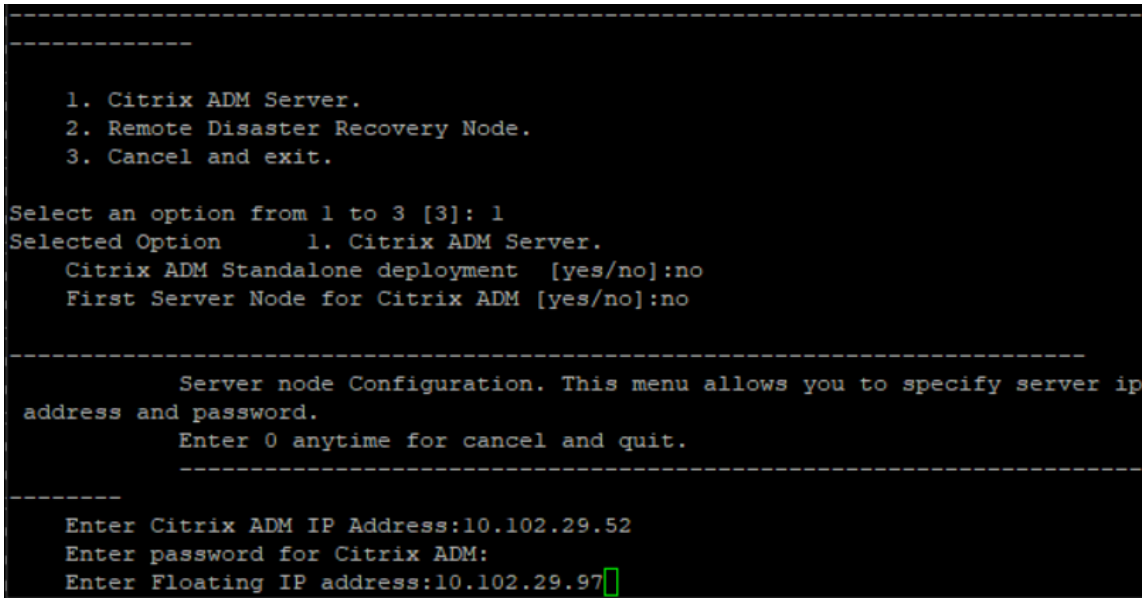
4. セカンダリノードをデプロイするには、**/mps/deployment_type.py** と入力します。NetScaler ADM 展開構成メニューが表示されます。
5. NetScaler ADM サーバーをセカンダリノードとして登録するには、**1** を選択します。
6. コンソールでは、NetScaler ADM をスタンドアロン展開として選択するように求められます。**No** と入力して、展開を高可用性として確認します。
7. コンソールでは、最初のサーバーノードを選択するように求められます。**No** を入力して、ノードを 2 番目のサーバとして確認します。



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に求められます。



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。



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 NetScaler ADM ユーザーインターフェイスに表示されます。これらのノードを高可用性ペアにデプロイします。

> 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 NetScaler ADM ユーザーインターフェイスにアクセスします。

ノードを高可用性ペアとしてデプロイするには**:**

1. Web ブラウザーを開き、最初の NetScaler ADM サーバーノードの IP アドレスを入力します。
2. 「ユーザー名」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. 管理者の資格情報を使用して NetScaler ADM にログオンし、ホームページの「はじめに」をクリックし、オプションで以下を完了します。

   a) NetScaler 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. [設定**] > [**展開**]** に移動し、展開を検証します。

   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

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

> 注
>
> プライマリノードから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、NetScaler ADM サーバーのプライマリノードの IP アドレスを入力します。
2. [ユーザー名] 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

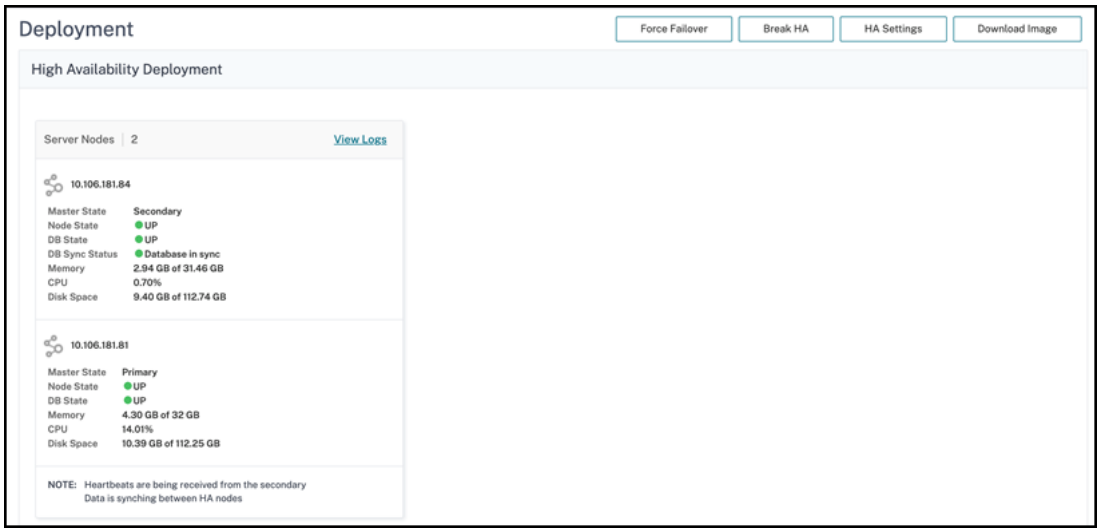
フェールオーバーが実行されるのは、次のいずれかの状態が検出された場合です。

- 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。

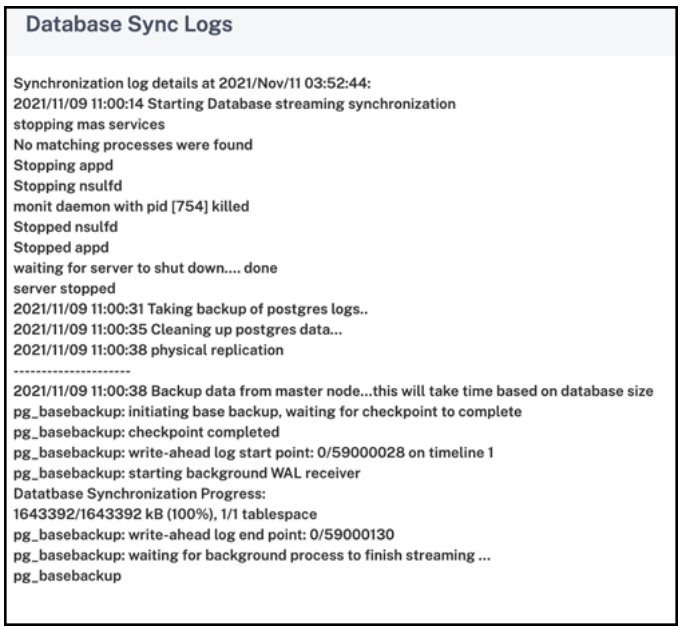
データベース同期ログメッセージの表示

NetScaler ADM HA ペアでは、構成ファイルがプライマリノードからセカンダリノードに自動的に同期され、データベースの物理ストリーミングレプリケーションが行われます。

ただし、ストリーミングレプリケーションエラーが発生した場合は、[**Sync Database**] ボタンが表示されます。[**Sync Database**] ボタンをクリックすると、データベース同期プロセスを開始できます。



データベース同期の進行状況を表示するには、[ログの表示] をクリックします。[**Database Sync Logs**] メッセージが表示され、同期の進行状況の詳細をリアルタイムで表示できます。



スプリットブレインシナリオ

ネットワークリンクのダウンタイム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 NetScaler ADM ノードがプライマリとセカンダリとして展開されています。ネットワークリンクのダウンタイムが発生する可能性があるため、2 つの NetScaler ADM ノード間の通信は完全に中断されます。180 秒以上ハートビートの交換が行われないため、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。

NetScaler ADM 12.1 以降のリリースでは、ネットワークリンクとハートビートが復元された後でも、このスプリットブレインの状態は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。

次の表は、NetScaler ADM でディザスタリカバリを構成する際に使用される用語をまとめたものです。

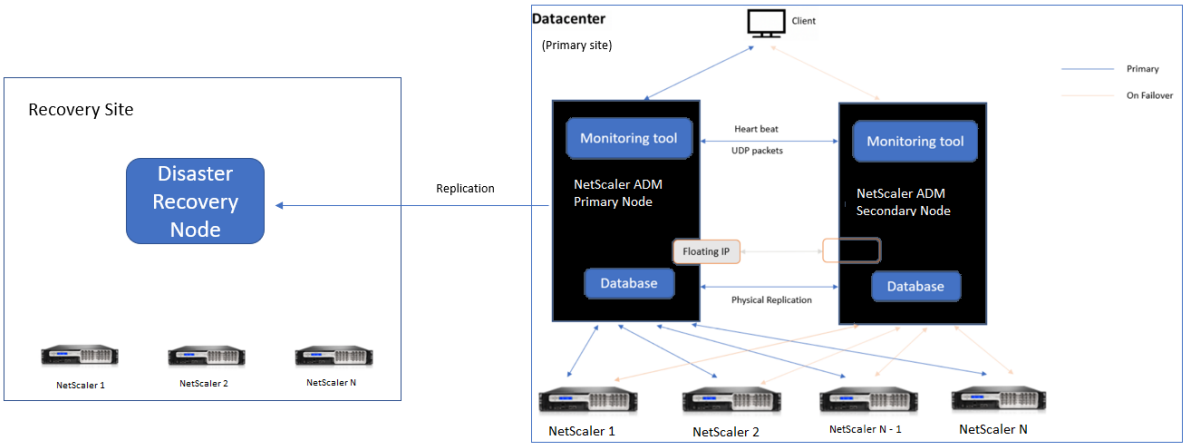
利用規約	説明
プライマリサイト (データセンター A)	プライマリサイトには、高可用性モードで展開された NetScaler ADM ノードがあります。
リカバリサイト (データセンター B)	リカバリ・サイトには、スタンドアロン・モードで展開された災害復旧ノードがあります。このノードは読み取り専用モードで、プライマリサイトがダウンするまで動作しません。
災害復旧ノード	リカバリ・ノードは、リカバリ・サイトにデプロイされたスタンドアロン・ノードです。このノードは、プライマリ・サイトで災害が発生し、それが機能しない場合に備えて、新しいプライマリに対して動作可能になります。

> 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、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 NetScaler インスタンスも検出されますが、トラフィックは流れていません。バックアッププロセス中、すべてのデータ、ファイル、および構成は、プライマリノードからディザスタ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:

- ディザスタリカバリ設定を有効にするには、プライマリサイトの NetScaler 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 NetScaler ADM のスタンドアロン展開では、災害復旧機能はサポートされません。
- NetScaler ADM HA ペア（プライマリサイト）とスタンドアロンノード（DR サイト）のソフトウェアバージョン、ビルド、および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

コンポーネント	条件
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。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。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、「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。
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

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
>
> - 高可用性モードで展開された NetScaler ADM は、NetScaler ADM リリースバージョン 13.1 にアップ

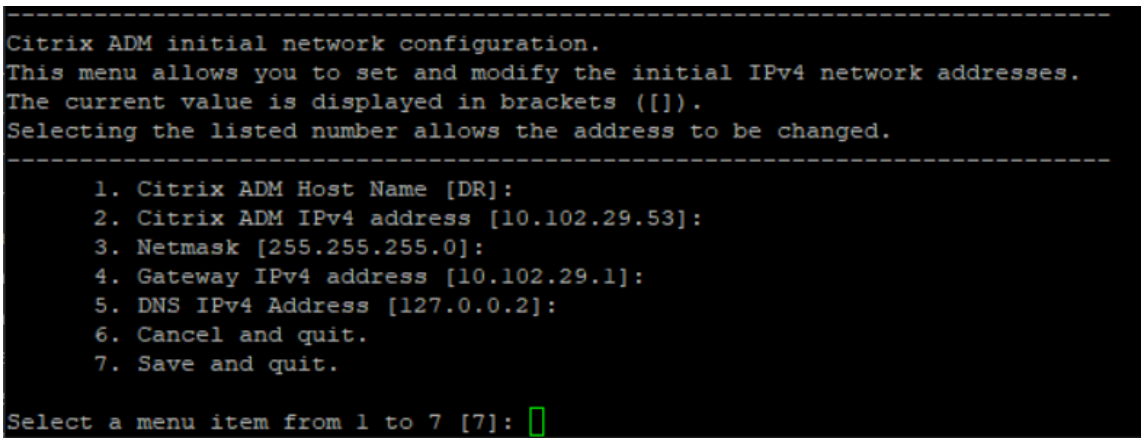
> グレードする必要があります。
>
> - 障害復旧ノードをプライマリノードに登録するには、**Floating IP** アドレスが必須 です。

DR コンソールを使用して **NetScaler ADM** ディザスタリカバリノードをデプロイして登録する

NetScaler ADM 災害復旧ノードを登録するには:

1. `.xva` NetScaler サイトから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］タブで、NetScaler ADM を初期ネットワーク構成で構成します。

   > 注
   >
   > 災害復旧ノードは、別のサブネット上に配置できます。

3. 初期ネットワーク設定が完了すると、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オンします—`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。

4. 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。NetScaler 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 deplo
yment.
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. 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 deplo
yment.
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
>
> - ディザスタリカバリノードには GUI がありません。
> - 登録が成功すると、サーバにログオンするためのデフォルトの管理者資格情報は`nsroot`/`nsroot`になります。

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

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

例:

```
/mps/change_freebsd_password.sh nsroot new_password
<!--NeedCopy-->
```

NetScaler ADM GUI を使用して災害復旧ノードを展開する

災害復旧ノードが DR コンソールを使用して正常に登録されたら、NetScaler ADM GUI から DR ノードをデプロイします。このステップにより、NetScaler ADM プライマリサイトからのディザスタリカバリ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。

NetScaler 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** ノードの削除] を選択します。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。

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:

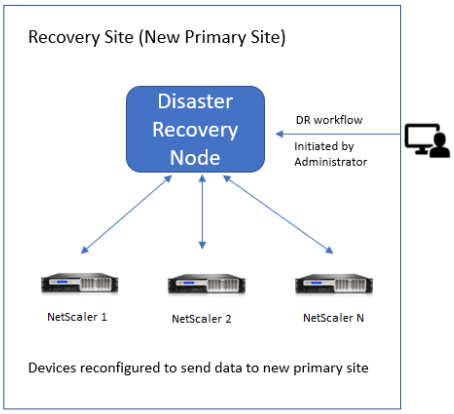
     ```
     /mps/scripts/pgsql/pgsql_restore_remote_backup.sh

     <!--NeedCopy-->
     ```

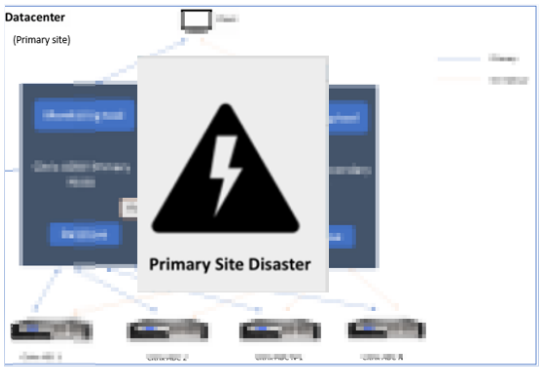
   - DR ノードをライセンスサーバとしても設定します:

     ```
     /mps/scripts/pgsql/pgsql_restore_remote_backup.sh -reconfig-
        ls <IP-address-of-the-primary-site>

     <!--NeedCopy-->
     ```

4. 内部的には、NetScaler インスタンスは、新しいプライマリサイト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

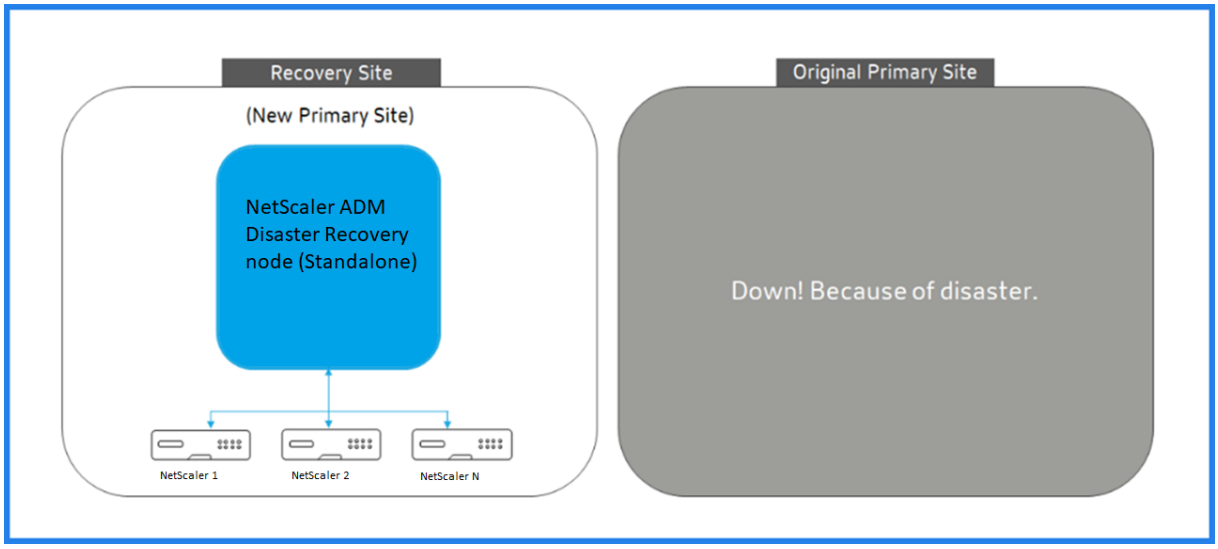
災害が発生し、管理者がリカバリ・スクリプトを開始すると、DR サイトが新しいプライマリ・サイトになります。

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
>
> - 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は、30 日間の猶予期間が与えられます。Citrix に連絡して、元のライセンスを NetScaler ADM（DR サイト）で再ホストするように依頼してください。
> - 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 DR サイトに同期されます（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）。
> - インスタンスにプールライセンスを適用した場合、バージョン 11.1 65.x 以降、12.1 58.x 以降、13.0 47.x 以降の NetScaler**、および NetScaler SDX 13.0 76.x 以降の NetScaler**SDX では、**DR** サイトでの自動ライセンスサーバー更新がサポートされます。その他のバージョンでは、インスタンスを DR サイトに手動で再構成する必要があります。

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。

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

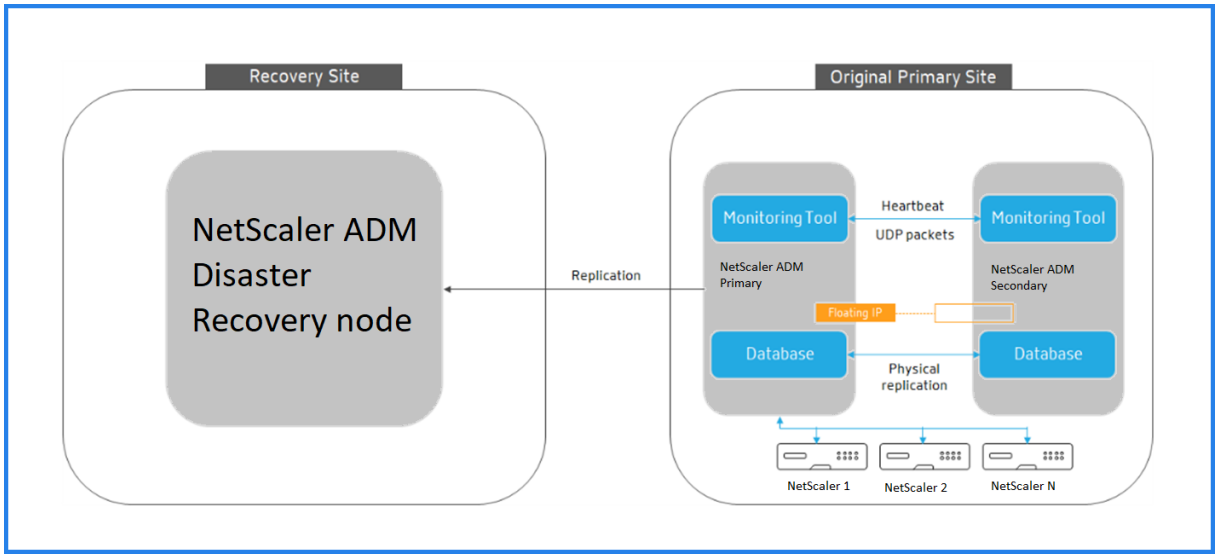
このコマンドは、プライマリサイトに Syslog、SNMP、Analytics のみを設定します。

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。

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

> 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 オンプレミスエージェントはプールライセンスをサポートしていません。

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

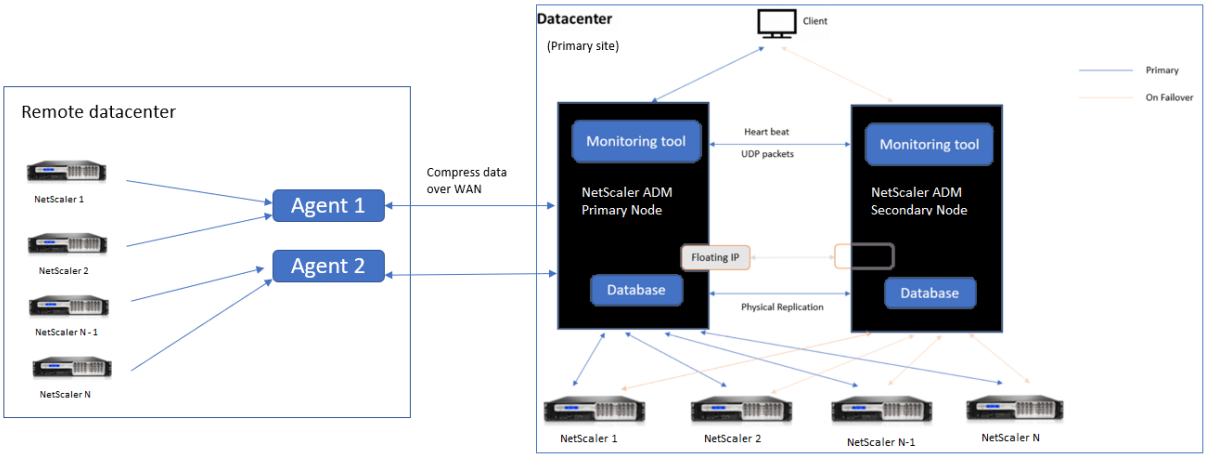
エージェントは、プライマリ NetScaler ADM と、異なるデータセンターで検出されたインスタンスの間の仲介者として動作します。エージェントをインストールする利点は次のとおりです。

- 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 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 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 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 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 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ネルを介して NetScaler ADM サーバーと通信し、チャネルを介して送信されるデータは帯域幅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 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 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アウトバウンドおよびインバウンド通信用。	NetScaler ADM エージェントから NetScaler ADM への接続

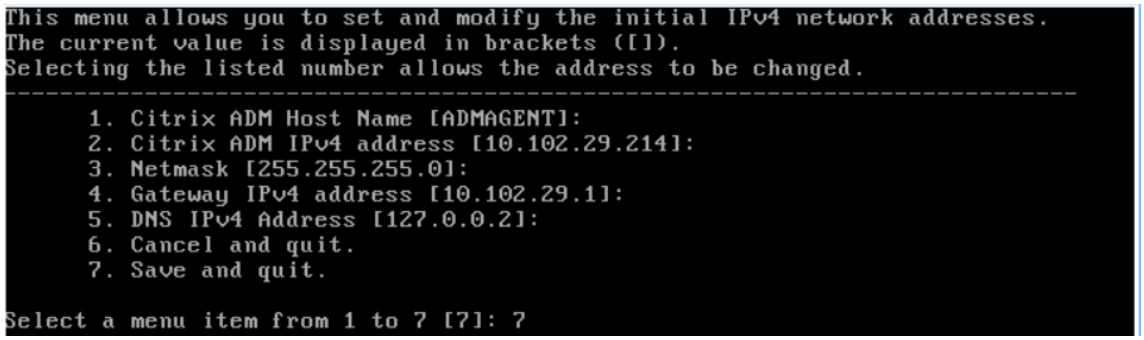
エージェントと NetScaler インスタンスの間で次のポートが開いている必要があります。

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 インスタンス間の NITRO 通信用。	NetScaler ADM から NetScaler へ、NetScaler から NetScaler ADM へ
TCP	22	エージェントと NetScaler インスタンス間の SSH 通信用。高可用性モードで展開された NetScaler ADM サーバー間の同期用。	NetScaler ADM から NetScaler に、NetScaler ADM エージェントは NetScaler に
UDP	4739	エージェントと NetScaler インスタンス間の AppFlow 通信用。	NetScaler から NetScaler ADM へ

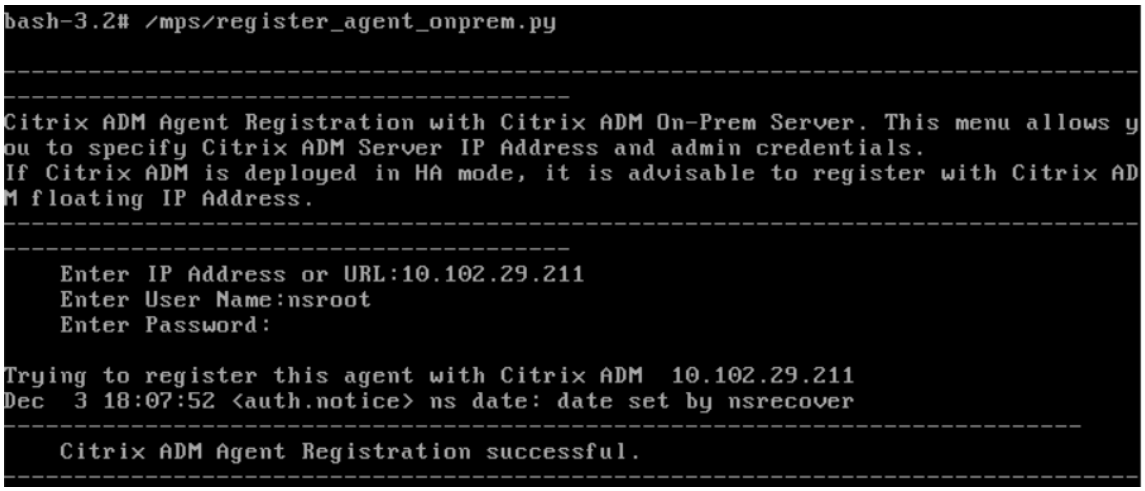
種類	ポート	詳細	コミュニケーションの方向
ICMP	予約されているポートなし	NetScaler ADM インスタンスと NetScaler インスタンス間、または高可用性モードでデプロイされたセカンダリ NetScaler ADM サーバー間のネットワーク接続性を検出します。	
UDP	161, 162	NetScaler インスタンスからエージェントに SNMP イベントを受信する。	ポート 161 -NetScaler ADM から NetScaler へ ポート 162 -NetScaler から NetScaler ADM へ
UDP	514	NetScaler インスタンスからエージェントに syslog メッセージを受信するため。	NetScaler から NetScaler ADM へ
TCP	5557	エージェントと NetScaler インスタンス間のログストリーム通信用。	NetScaler から NetScaler ADM へ

エージェントを登録する

1. NetScaler サイトからダウンロードしたエージェントイメージファイルを使用して、ハイパーバイザーにインポートします。エージェントイメージファイルの命名パターンは、**MASAGENT-\ <HYPERVISOR\ >-\ <Version.no\ >** です。例：**MASAGENT-XEN-13.0-xy.xva**
2. ［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。
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。



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。NetScaler ADM エージェントの登録資格情報が、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。



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 [インフラストラクチャ**] > [**インスタンス**] > [**エージェント] ページに移動して、エージェントのステータスを確認します。新しく追加されたエージェントは **Up** 状態で表示されます。

> 注
>
> NetScaler ADM はエージェントのバージョンを表示し、エージェントが最新バージョンであるかどうかも確認します。ダウンロードアイコンは、エージェントが最新バージョンではなく、アップグレードが必要であることを示します。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 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

[インフラストラクチャ] **>** [エージェント] **>** [アクションの選択] でエージェントにさまざまなアクションを適用できます

[アクションの選択] では、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 インスタンスの追加

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

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway
- Citrix の SSL 転送プロキシ

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. [インフラストラクチャー**] > [**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 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. 「エージェント」ページで、インスタンスを関連付けるエージェントを選択し、「**OK**」をクリックします。

> 注**:**
>
> インスタンスを関連付ける 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。

NetScaler ADM で、[インフラストラクチャ] > [インスタンス] に移動します。[インスタンス] で、アクセスするインスタンスの種類（NetScaler 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 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時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ールオーバーは、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。

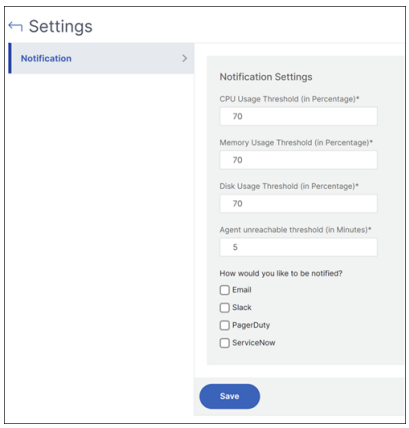
たとえば、バンガロールのサイトで、10.106.1xx.2x と 10.106.1xx.3x の 2 つのエージェントが接続され、動作しているとします。1 つのエージェントが非アクティブになると、NetScaler ADM はエージェントを検出し、その状態を down と表示します。

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。

エージェント到達不能しきい値と通知を構成する

エージェントがダウンしているか、一定期間到達できない場合、メール、Slack、PagerDuty、ServiceNow を通じてエージェントのステータスに関する通知を受け取ることができます。[インフラストラクチャ] > [インスタンス] > [エージェント] で、[設定] をクリックし、5 分から 60 分の期間を指定し、通知を受け取る通知方法を選択します。



Kubernetes クラスターに **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 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にのみ適用されます。このシナリオでは、Kubernetes クラスターがホストされている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、インフラストラクチャ **>** インスタンス **>** エージェントの順に移動します。
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

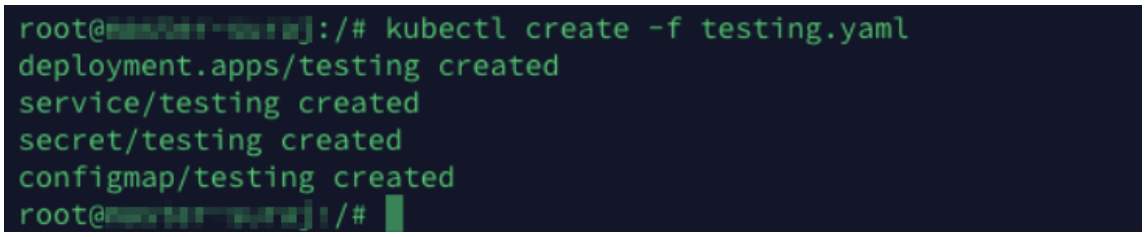
Kubernetes メインノードで以下を実行します。

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。



NetScaler ADM で、[インフラストラクチャ] **>** [インスタンス] **>** [エージェント] に移動し、エージェントのステータスを確認します。

エージェントを構成したら、NetScaler CPX インスタンスを追加し、サービスグラフで分析を表示できます。詳しくは、次のトピックを参照してください:

- NetScaler CPX インスタンスを NetScaler ADM に追加する。
- サービスグラフを設定します。

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

NetScaler ADM 単一サーバーを、2 台の NetScaler ADM サーバーで構成される高可用性環境にアップグレードできます。NetScaler ADM サーバーの高可用性ペアはアクティブ/パッシブモードになっており、両方のサーバーは同じ構成になっています。このタイプのアクティブ/パッシブ展開では、一方の NetScaler ADM サーバーがプライマリノードとして構成され、もう一方がセカンダリノードとして構成されます。何らかの理由でプライマリノードがダウンした場合、セカンダリノードが引き継ぎます。

NetScaler ADM 単一サーバーを高可用性ペアに移行するには、新しい NetScaler ADM サーバーノードをプロビジョニングし、それを 2 番目の NetScaler ADM シングルサーバーとして構成し、両方の NetScaler ADM サーバーを高可用性ペアとして展開する必要があります。

NetScaler ADM 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 **NetScaler ADM** サーバーノードを変更します

NetScaler 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 NetScaler ADM サーバーノードのコンソールを開きます。たとえば、IP アドレスが 10.106.171.17 の NetScaler ADM をスタンドアロンサーバーとして展開したとします。
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 NetScaler 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 deplo
yment.
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。最初のサーバーのインストールに使用したのと同じイメージファイルを使用するか、NetScaler サイトから同じバージョンのイメージファイルを入手

します。

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]:
```

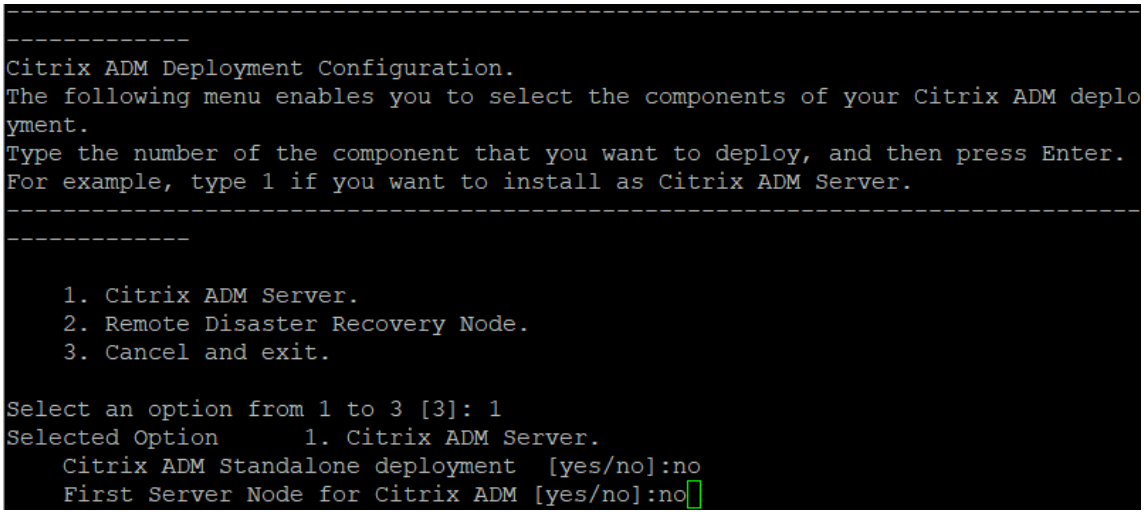
2. 必要な IP アドレスを指定した後、シェルプロンプトで /mps/deployment_type.py と入力し、Enter キーを押します。

3. 展開タイプを **NetScaler ADM** サーバーとして選択します。

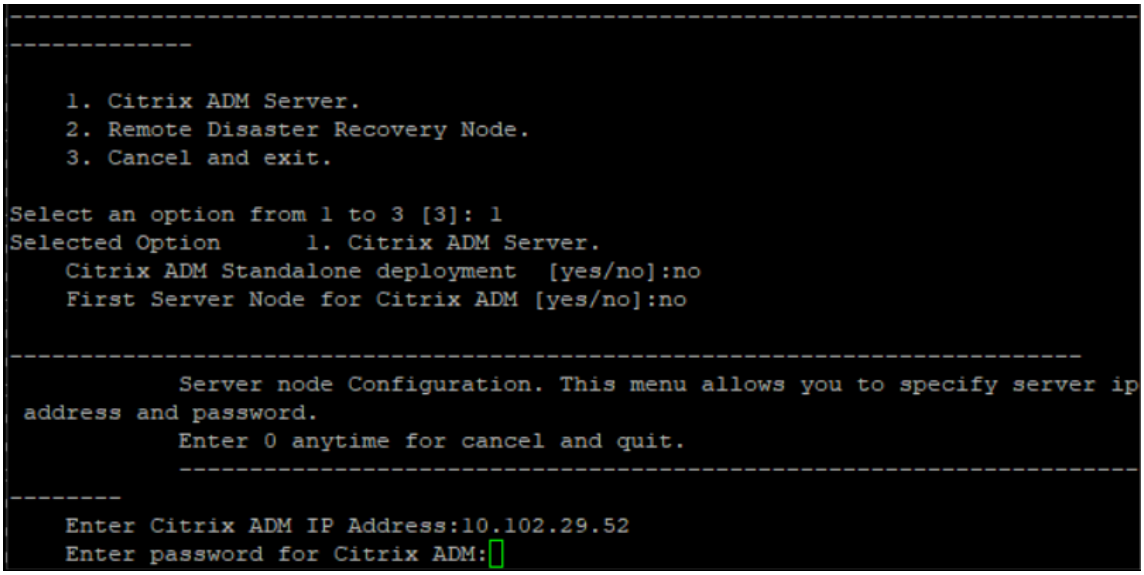
4. デプロイメントコンソールで、サーバーデプロイメントを選択するよう求められます（スタンドアロンとして）。「**No** 」と入力して、展開を高可用性ペアとして確認します。

```
bash-3.2# /mps/deployment_type.py
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
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
```

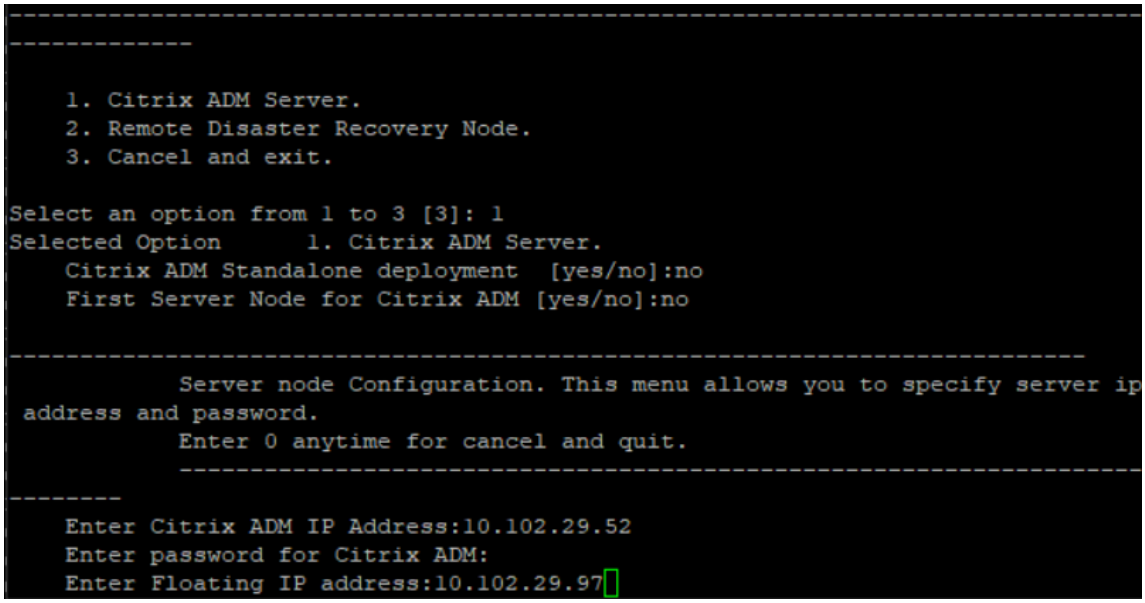
5. （最初のサーバーノード）を選択するかどうかを尋ねるメッセージがコンソールに表示されます。「**No** 」と入力して、ノードを 2 番目のサーバ・ノードとして確認します。



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。



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。



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 NetScaler ADM サーバーノードの GUI からこれらのノードをデプロイ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
   >
   > NetScaler 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 NetScaler 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。NetScaler ADM を使用すると、アプリケーションに関連する NetScaler インスタンスによって生成されたさまざまな分析を表示できるだけでなく、単一の統合コンソールからグローバル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。

> 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 NetScaler ADM に移行する前に、次の要件が満たされていることを確認してください。

- NetScaler Insight Center 11.1 Build 47.14 以降がインストールされている。
- 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 をインストールしてから、最新の NetScaler ADM 13.1 ビルドにアップグレードする必要があります。詳しくは、「アップグレード」を参照してください。

- NetScaler ADM 13.1 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 では NetScaler ADM の導入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推奨しています。

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_imag* es 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ら、上記の手順を実行して最新の NetScaler ADM 13.1 ビルドにアップグレードする必要があります。

移行後、NetScaler Insight Center インベントリで検出されたすべての NetScaler ADC インスタンスが、**NetScaler ADM** の［インフラストラクチャ］**>**［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
>
> NetScaler ADM では、デフォルトでは、検出された NetScaler インスタンス内に作成された 2 つの仮想サーバーを管理および監視するためのライセンスコストは発生しません。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

最低限の要件

ネットワーク統合を設定する前に、HDX Insights にアクセスできる RBAC ユーザーを作成してください。

ソフトウェア要件

NetScaler ADM 仮想アプライアンスに移行する前に、次の要件が満たされていることを確認します。

- 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 Workspace for Mac バージョン 11.8 以降、および Windows Citrix Workspace for Windows 14.0 以降で正確な ICA RTT メトリックが表示されることを確認してください。
- NetScaler ADM バージョン 11.0 以降がインストールされます。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 セッションのラウンドトリップ時間（RTT）には、Windows 3.4 以降の Citrix Workspace および Mac 11.8 以降の Citrix Workspace のデータが正しく表示されます。これらの Workspaces の以前のバージョンでは、データは正しく表示されません。
- [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/citrix-virtual-apps-desktops/director/install-and-configure/hdx-insight.htmlを参照してください。
> - HDX Insight の詳細については、http://docs.citrix.com/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:
>
> - ストレージ要件を見積もり、サーバーに追加のディスクを接続します。
> - 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なければなりません。
> - 容量の小さい外部ディスクが既に存在する場合は、新しいディスクを接続する前にそのディスクを取り外す必要があります。
> - NetScaler ADM の導入には、ソリッドステートドライブ（SSD）テクノロジーを使用することをお勧めします。

このドキュメントでは、追加の新しいディスクの接続、パーティションの作成、および追加ディスクのサイズ変更に関する次のシナリオについて説明します:

1. スタンドアロンの NetScaler ADM に追加ディスクを接続する
2. ディスクパーティションツールを起動する
3. 新しい追加ディスクにパーティションを作成する
4. 既存の追加ディスク内のパーティションのサイズを変更する
5. 追加のディスクのパーティションを削除します

スタンドアロンの **NetScaler ADM** に追加ディスクを接続する

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。

   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。現在、コアファイルやオペレーティングシステムのログファイルなどの保存には、既存のデフォルトディスクである 120 GB が使用されています。
3. NetScaler ADM 仮想マシンを起動します。

ディスクパーティションツールを起動する

NetScaler 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。

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. ツールを使用して、既存の追加ディスクのサイズを変更することもできます。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:
   >
   > - 既存のディスクのサイズが 2 TB を超えると、データが失われる可能性があります。これは、プラットフォーム上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、ディスク上の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) ディスクにパーティションを作成することはできません。

ディスクパーティションツールを起動するには:

1. PuTTY などの SSH クライアントを使用して、NetScaler ADM への SSH 接続を開きます。
2. `nsrecover`/`nsroot` 資格情報を使用して NetScaler ADM にログオンします。
3. シェルプロンプトに切り替えて、次のように入力します。

```
/mps/DiskPartitionTool.py
<!--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:
>
> この処理には数秒かかることがあるため、処理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 interrup 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:
>
> このツールは、パーティションが作成された後に仮想マシンを再起動します。

既存の追加ディスク内のパーティションのサイズを変更する

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 TB 未満でなければなりません。

> 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、サイズを変更する前に、このディスク内の重要なデータを外部ストレージにバックアップすることをお勧めします。データバックアップは、サイズ変更操作中にディスクデータが破損する可能性がある場合に役立ちます。
> - パーティションのサイズを変更するときは、必ず 100 GB ずつディスク容量を増やしてください。このような段階的な増加により、頻繁にサイズ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 capcity 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、およびサイズ変更に同意した後に処理を続行します。NetScaler ADM サブシステム、PostgreSQL DB プロセス、および NetScaler ADM 監視プロセスを含むディスクにアクセスするプロセスを停止します。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増加」プロセスが完了するまでに時間がかかる場合があり、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
 interrup 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確認できます。サイズを大きくしたときの、変更前と変更後の詳細は次のとおりです:

```
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/da1s1a   152329216 3082226 137060654     2%    /var/mps
```

```
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/da1s1a   304651668 3137954 277141582     1%    /var/mps
```

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。この問題は、パーティションの既知の制限が原因です。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。

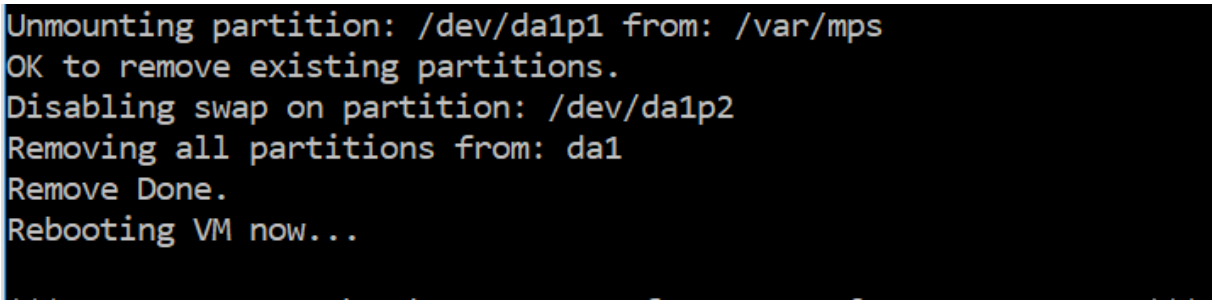
> 注:
>
> 既存のパーティションを削除すると、既存のデータはすべて削除されます。したがって、このコマンドを使用する前に、重要なデータを外部ストレージにバックアップする必要があります。

```
(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を求められ、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
```

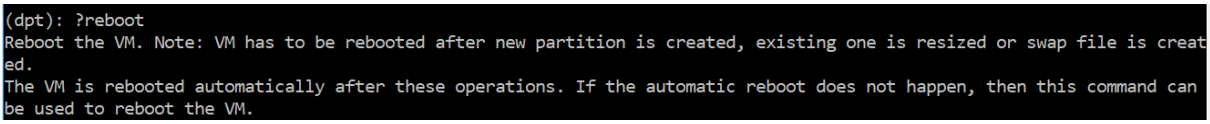
「y」と入力すると、ディスクがアンマウントされ、ディスク上のすべてのパーティションが削除されます。



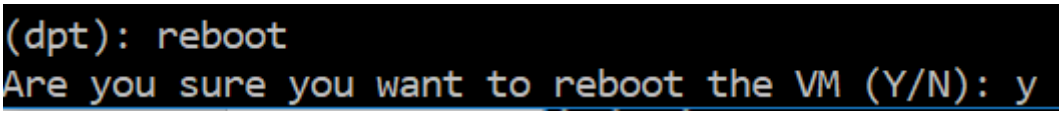
> 注:
>
> パーティションを削除すると、仮想マシンが再起動されます。

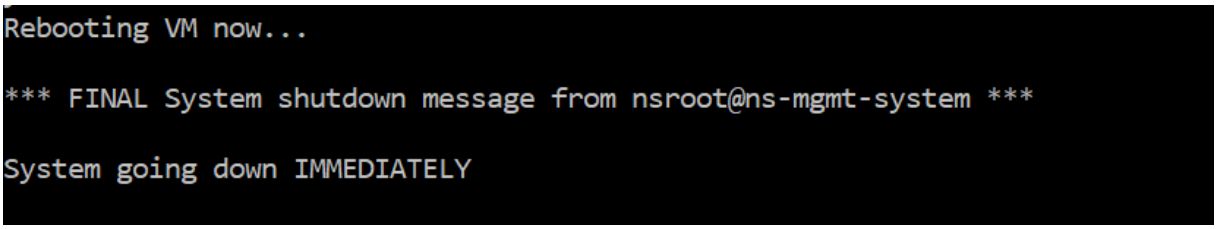
仮想マシンの再起動

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。



確認を求められ、確認後、すべてのプロセス (ADM サブシステム、PostgreSQL プロセス、ADM モニターなど) が停止します。その後、仮想マシンが再起動されます。





ディスクデータのバックアップファイルを作成する

> 注:
>
> バックアップファイルの作成にはディスク容量が必要です。バックアップコマンドを実行する前に、十分なディスク容量 (50% 以上) があることを確認してください。

パーティションのサイズを変更または削除する前に、NetScaler ADM データをバックアップするには:

1. ADM を停止します。


```
/mps/masd stop
<!--NeedCopy-->
```

2. PostgreSQL を停止します。

```
su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh
<!--NeedCopy-->
```

3. ADM モニタを停止します。

```
/mps/scripts/stop_mas_monit.sh
<!--NeedCopy-->
```

4. tarball を作成します。

```
cd /var
tar cvfz /var/mps/mps_backup.tgz mps
<!--NeedCopy-->
```

> 注:
>
> バックアップするデータのサイズによっては、操作に時間がかかります。

5. チェックサムを生成します。

```
md5 /var/mps/mps_backup.tgz > /var/mps/mps_backup_checksum
<!--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。

```
cd /var/mps/
rm mps_backup.tgz  mps_backup_checksum
<!--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。各コマンドについてさらにヘルプを参照するには、[ヘルプ] または [**?**] を押してください。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、ディスクが以前のバージョンの NetScaler ADM バージョンを使用して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、作成時は 2 テラバイトを超えることがあります。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。この問題は、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上のデフォルトのスワップパーティションは 4 GB なので、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) 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 以上の場合にのみ役立ち、メモリが少ないときには役立ちません。そのため、このコマンドは、スワップファイルの作成に進む前にメモリの有無もチェックします。

```
(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 n
ot 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

セカンダリディスクを使用しない高可用性セットアップで、2 台の NetScaler ADM サーバーを構成したとします。また、2 つ以上の NetScaler インスタンスを追加し、すべてのプロセスが実行されていることを確認したとします。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. セカンダリノードをシャットダウンします。
2. ハイパーバイザーを介してディスクを追加します。

   > 注:
   >
   > セカンダリノードのメインディスクを拡張しないようにしてください。

3. セカンダリノードを起動します。
4. セカンダリノードでパーティションツールを実行します。
5. ディスクが追加されると、セカンダリノードが再起動します。
6. 再起動後、セカンダリノードをシャットダウンします。
7. プライマリノードをシャットダウンします。
8. ハイパーバイザーを介してディスクを追加します。

   > 注:
   >
   > プライマリノードのメインディスクを拡張しないように注意してください。

9. プライマリノードを起動します。
10. プライマリノードでパーティションツールを実行します。
11. ディスクが追加されると、プライマリノードが再起動します。
12. プライマリノードが起動して実行されたら、セカンダリノードを起動します。
13. セカンダリノードが稼働していて、データベースが同期していることを確認します。
14. すべてのデータがまだ存在することを確認します。

両方のノードの **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、それがプライマリノードかどうかを確認します。
5. ADM_ セカンダリノードを起動します。再起動後、セカンダリとして起動し、DB 同期が機能していることを確認します。
6. すべてのデータがまだ存在することを確認します。

   > 注:
   >
   > セカンダリディスクを追加した後、プライマリノードが起動するまでにしばらく時間がかかります。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。

ADM オンプレミ Cloud Connector

February 6, 2024

ADM オンプレミ Cloud Connector 機能を使用して、ADM オンプレミスと NetScaler Console サービス間の接続を確立できます。

> 注:
>
> NetScaler ADM サービスは、NetScaler コンソールサービスに名前が変更されました。当社の製品 UI とドキュメントは、これらの変更を反映するように現在更新中です。この間、古い名前と新しい名前が同じ意味で参照されていることに気付くかもしれません。この移行の間、ご理解いただきますようお願いいたします。

この接続により、ADM On-Prem で使用する次の機能を選択できます。

セキュリティアドバイザリ—セキュリティアドバイザリは、脆弱な NetScaler の自動識別をサポートし、修復ワークフローの利点を提供します。セキュリティアドバイザリを利用すると、新しい一般的な脆弱性と露出 (CVE) を追跡し、CVE の影響を評価し、修復方法を理解し、脆弱性を解決することができます。管理者は、定期スキャンまたは手動スキャンによって NetScaler インスタンスに新しい CVE がないか監視し、修正に必要なアクションを実行できます。詳細については、「セキュリティアドバイザリ」を参照してください。

自動テレメトリ収集—Flexed ライセンスを使用している場合は、テレメトリデータ収集の自動モードである Cloud Connector を有効にすることをお勧めします。詳しくは、「フレキシブルキャパシティライセンス」を参照してください。

> 注:
>
> - NetScaler インスタンスを NetScaler コンソールサービスに追加または移行する必要はありません。
> - ADM オンプレミ Cloud Connector では、NetScaler Console サービスアカウントを設定して NetScaler Console サービスに接続する必要があります（まだ作成されていない場合）。
> - 14.1 8.x ビルド以降、ADM オンプレミ Cloud Connector はカスタマー ID 機能に取って代わります。
> - ADM On-Prem Cloud Connector を構成すると、Citrix Cloud がライセンスコンプライアンスのためのライセンス、構成、使用状況データを収集し、サービスを管理、測定、改善できるようになります。詳しくは、「データガバナンス」を参照してください。

前提条件

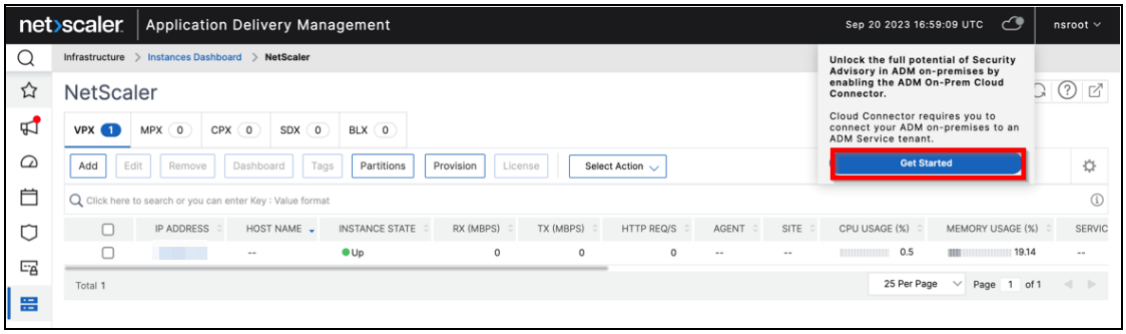
ADM オンプレミ Cloud Connector を設定する前に、次の前提条件を満たしていることを確認してください。

- Citrix Cloud にアクセスできるようにするには、インターネット接続があるか、ADM オンプレミスにプロキシサーバーが設定されていることを確認してください。
- 次のエンドポイント URL へのアクセスが許可されていることを確認します。
  - ダウンロードサービス:
    `https://download.citrixnetworkapi.net`
  - 信頼サービス:
    `*.citrixnetworkapi.net`
  - サービス URL
    - `*.agent.adm.cloud.com`
    - `*.adm.cloud.com`
    - `adm.cloud.com`
  - Citrix Cloud 接続:
    - `Citrix.cloud.com`
    - `Accounts.cloud.com`
- ADM オンプレミス GUI にアクセスするブラウザーのポップアップブロッカーを無効にしていることを確認してください。

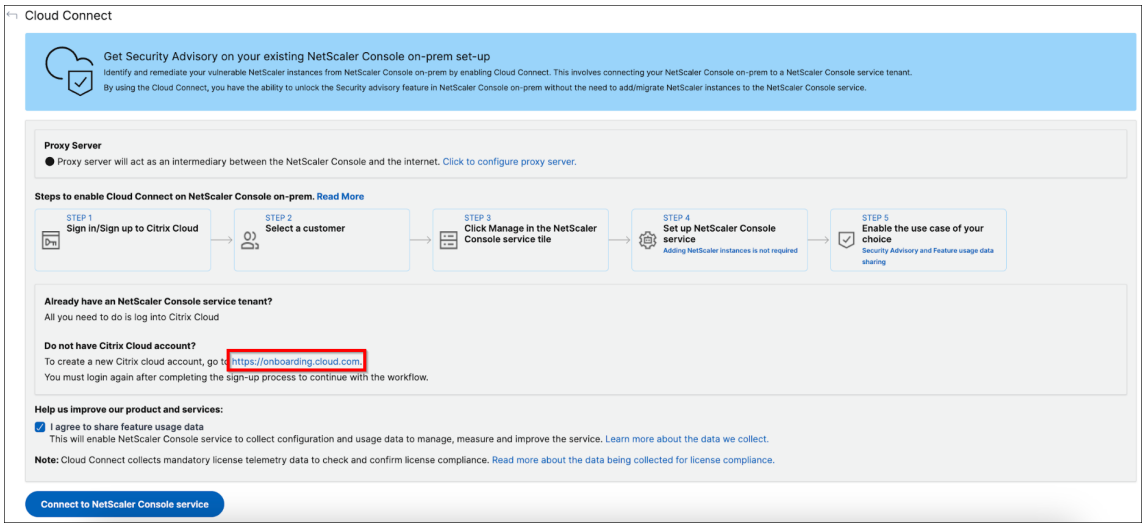
ADM オンプレミ Cloud Connector の設定

ワークフロー 1 —Citrix Cloud アカウントと NetScaler Console サービステナントを持たない新規ユーザーの場合

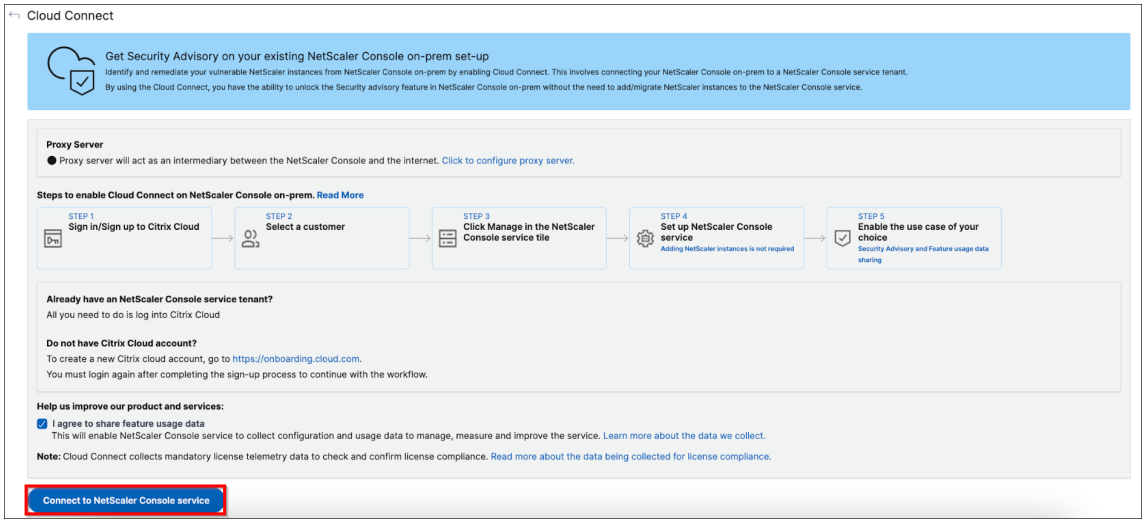
1. **NetScaler ADM** で、**[** クラウド**]** アイコン **>** **[**はじめに**]** をクリックします。**



2. ADM オンプレミ Cloud Connector 設定ページで、リンクをクリックします。`https://onboarding.cloud.com`



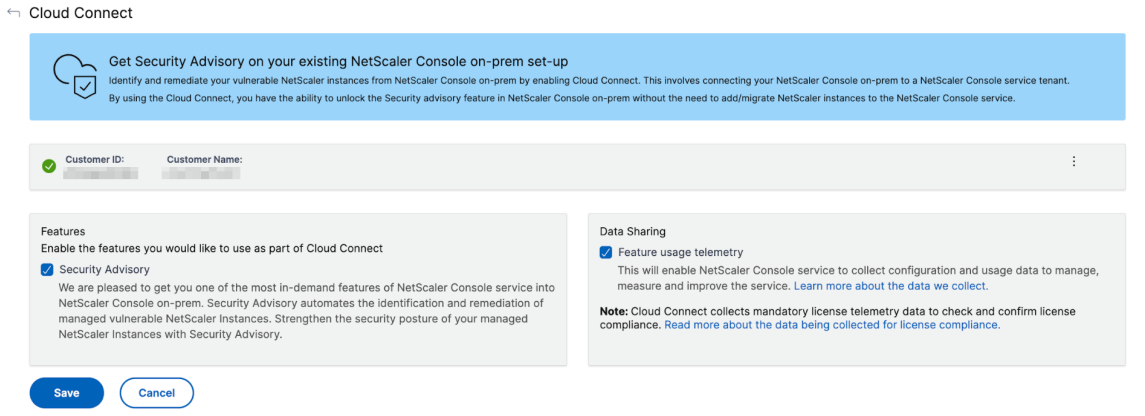
3. このドキュメントの手順に従って 、Citrix Cloud アカウントを作成します。
4. Citrix Cloud アカウントを作成したら、NetScaler ADM の［**NetScaler** コンソールサービスに接続］をクリックして再度ログインする必要があります。ログインに成功すると、ページは NetScaler Console のサービステナント作成手順にリダイレクトされます。



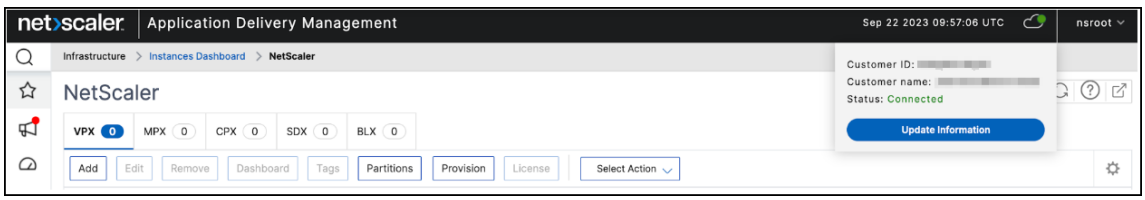
5. ビジネスニーズに合った地域を選択し、「完了」をクリックします。
6. ロールを選択し、セットアップを完了します。

   設定が完了するまでに数分かかる場合があります。ADM では、**ADM** オンプレミスクラウドコネクタの有効化が進行中であることを示す画面が表示されます。[**Refresh**] をクリックして更新された設定ページが表示されるまで待つか、[**Cancel**] をクリックしてこの画面をスキップし、後で更新された設定ページを確認することができます。

7. ADM オンプレミ Cloud Connector の設定が完了しました。さらに、ADM On-Prem Cloud Connector 設定ページからセキュリティアドバイザリを有効にできます。
8. 「セキュリティアドバイザリ」を選択し、「保存」をクリックします。

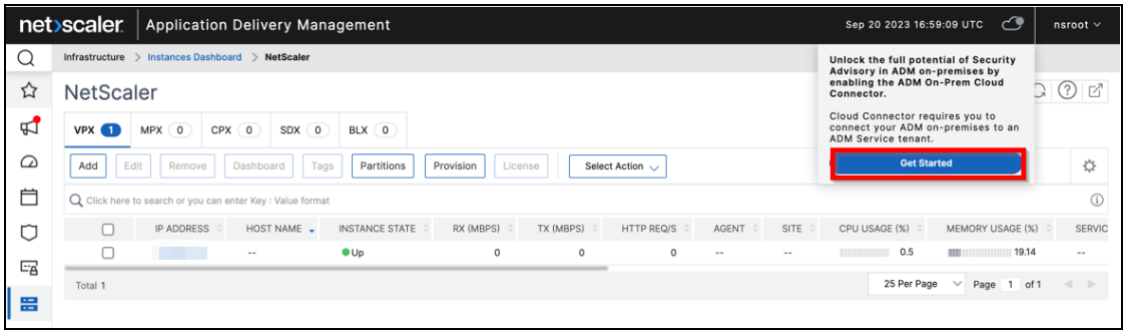


ステータスが「接続済み」と表示されます。

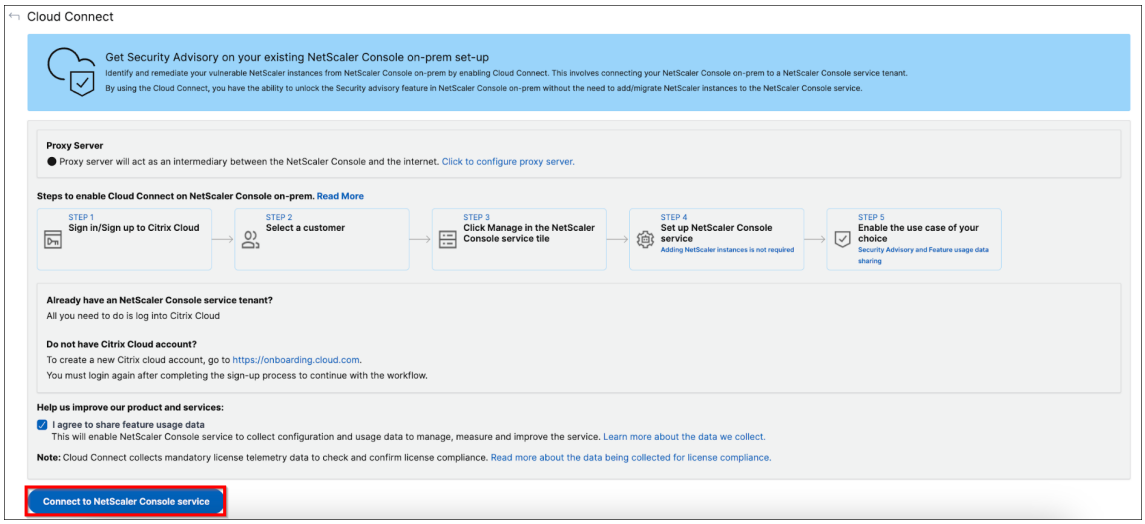


ワークフロー **2** —**Citrix Cloud** アカウントはあるが、**NetScaler Console** サービステナントを持っていない場合

1. **NetScaler ADM** で、**[**** クラウド**]** アイコン **> [**はじめに] をクリックします。******



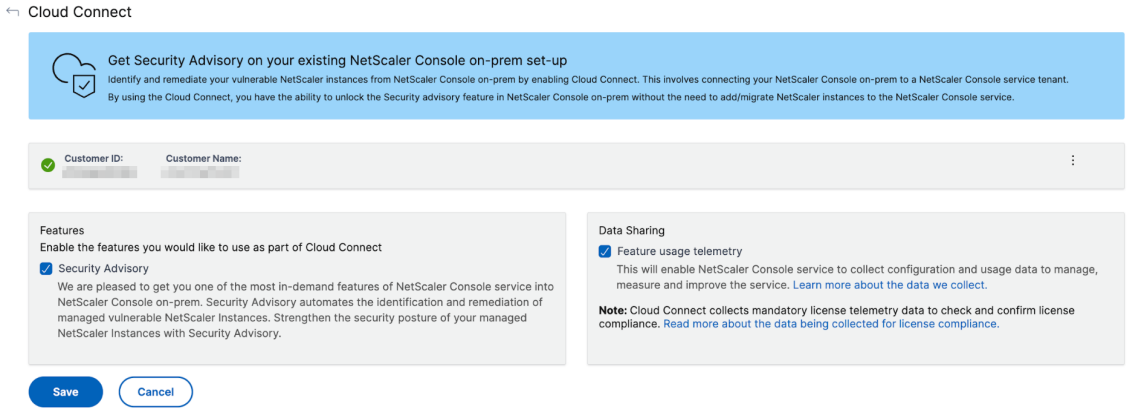
2.「**NetScaler** コンソールサービスに接続」をクリックします。



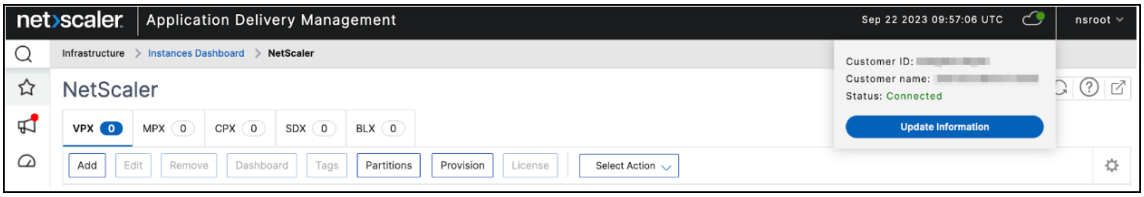
3. 新しいタブにリダイレクトされます。Citrix Cloud にサインインします。
4. ログイン成功のメッセージを受け取ると、ページは ADM のオンボーディング手順にリダイレクトされます。
5. ビジネスニーズに合った地域を選択し、「完了」をクリックします。
6. ロールを選択し、セットアップを完了します。

   設定が完了するまでに数分かかる場合があります。ADM では、**ADM** オンプレミスクラウドコネクタの有効化が進行中であることを示す画面が表示されます。[**Refresh**] をクリックして更新された設定ページが表示されるまで待つか、[**Cancel**] をクリックしてこの画面をスキップし、後で更新された設定ページを確認することができます。

7. ADM オンプレミ Cloud Connector の設定が完了しました。さらに、ADM On-Prem Cloud Connector 設定ページからセキュリティアドバイザリを有効にできます。
8.「セキュリティアドバイザリ」を選択し、「保存」をクリックします。

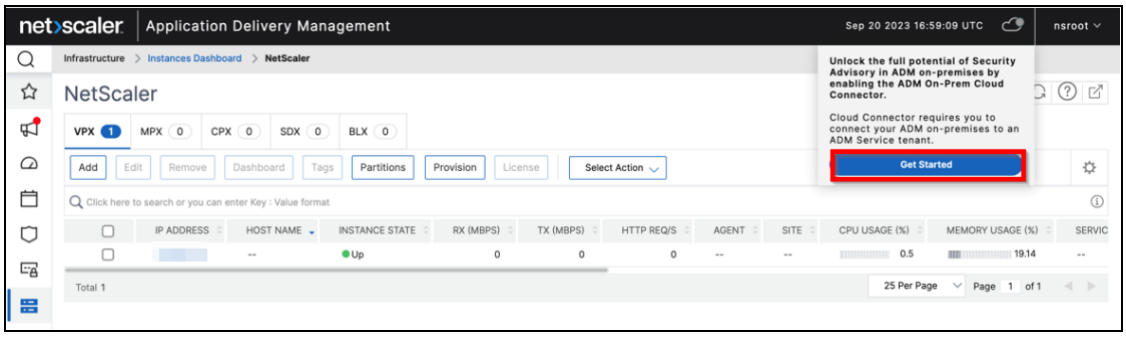


ステータスが「接続済み」と表示されます。

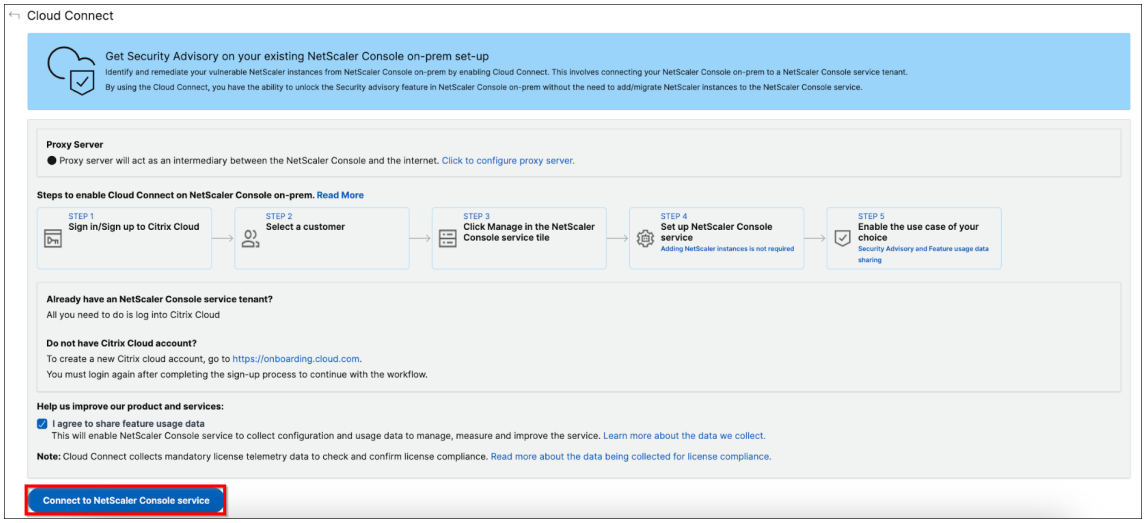


ワークフロー **3-Citrix Cloud** アカウントと **NetScaler Console** サービステナントの両方を持つ既存のユーザーの場合

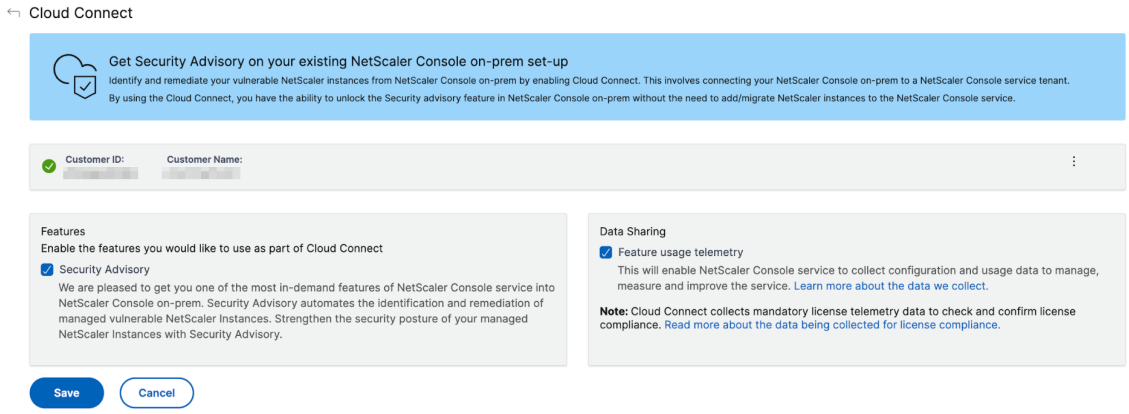
1. **NetScaler ADM** で、**[** クラウド]** アイコン **> [**はじめに] をクリックします。**



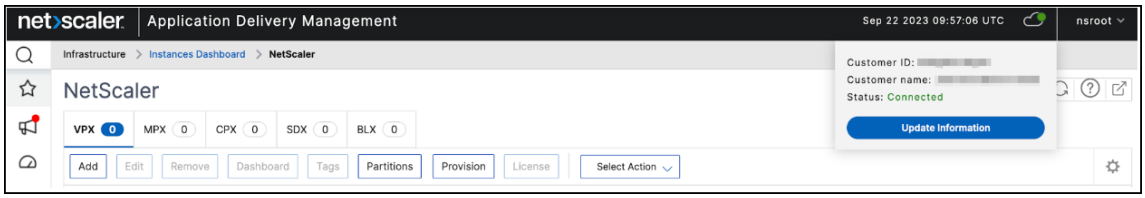
2. 「**NetScaler** コンソールサービスに接続」をクリックします。



3. 新しいタブにリダイレクトされます。Citrix Cloud にサインインし、テナントを選択します。テナントを選択すると、ログイン成功のメッセージが表示されます。
4. ADM オンプレミ Cloud Connector の設定が完了しました。さらに、ADM On-Prem Cloud Connector 設定ページからセキュリティアドバイザリを有効にできます。
5. 「セキュリティアドバイザリ」を選択し、「保存」をクリックします。



ステータスが「接続済み」と表示されます。

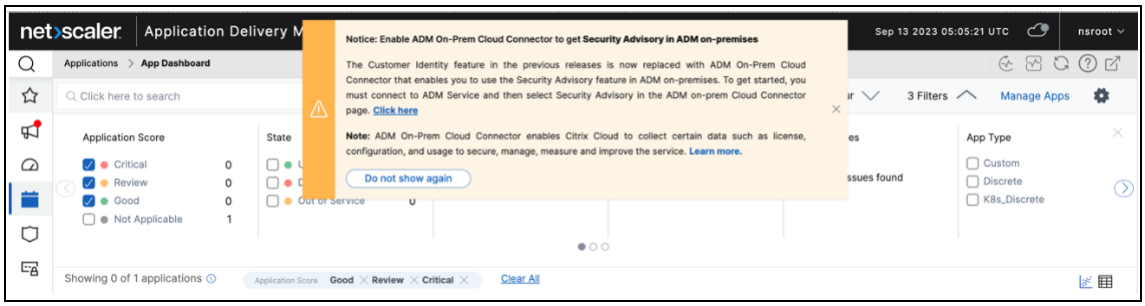


カスタマー **ID** がすでに有効になっている場合はどうなりますか**?**

Customer Identity を有効にし、データ共有を選択し、最新のビルド（14.1 8.x）にアップグレードした以前のビルドの既存のユーザーの場合、次のシナリオが適用されます。

- NetScaler Console サービステナントがある場合、ADM オンプレミス Cloud Connector は ADM オンプレミスで自動的に有効になります。これにより、Citrix Cloud はライセンス、構成、使用状況に関するデータを収集して、サービスの管理、測定、改善を行うことができます。詳しくは、「データガバナンス」を参照してください。Cloud Connector の設定ページから、セキュリティアドバイザリを選択して機能を使用できます。

  ADM オンプレミ Cloud Connector が NetScaler ADM で自動的に構成されている場合、次の通知が表示されます。

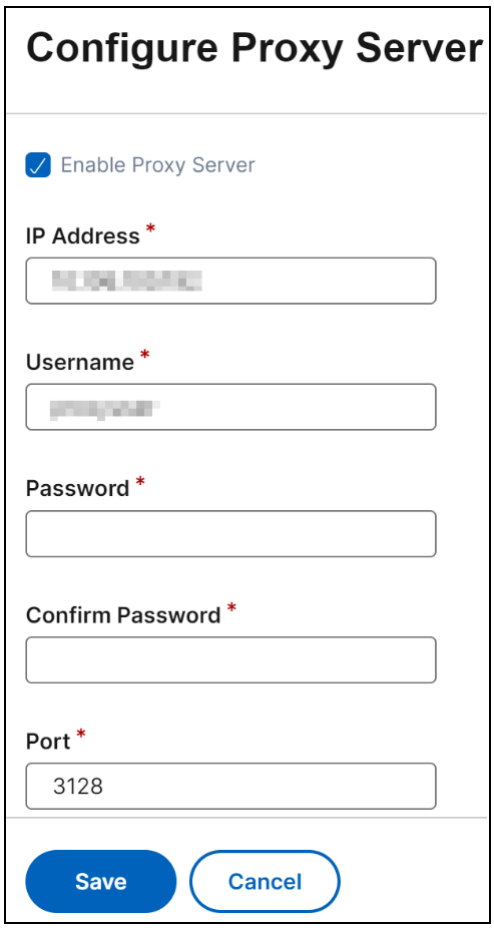


- NetScaler Console サービステナントがない場合、またはカスタマー ID の一部としてデータ共有が有効になっていない場合、ADM オンプレミスクラウドコネクタは自動的に有効にならないため、Cloud Connector を手動で構成する必要があります。設定が完了すると、Citrix Cloud はライセンス、構成、および使用状況データを収集して、サービスの管理、測定、改善を行うことができます。データ収集の詳細をご覧ください。

その他のオプション

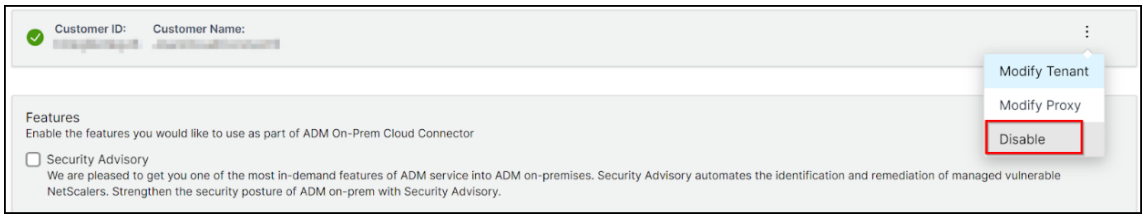
ADM オンプレミ Cloud Connector を有効にすると、次のオプションを使用できます。

- テナントの変更 -既存のテナントを変更できます。「テナントを変更」をクリックすると、新しいタブにリダイレクトされ、Citrix Cloud にサインインする必要があります。ログインに成功したら、別のテナントを選択できます。
- プロキシの変更 -ADM オンプレミスのプロキシ設定を構成できます。これは、NetScaler ADM 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です。リストから [プロキシの修正] をクリックし、詳細を更新して [保存] をクリックします。



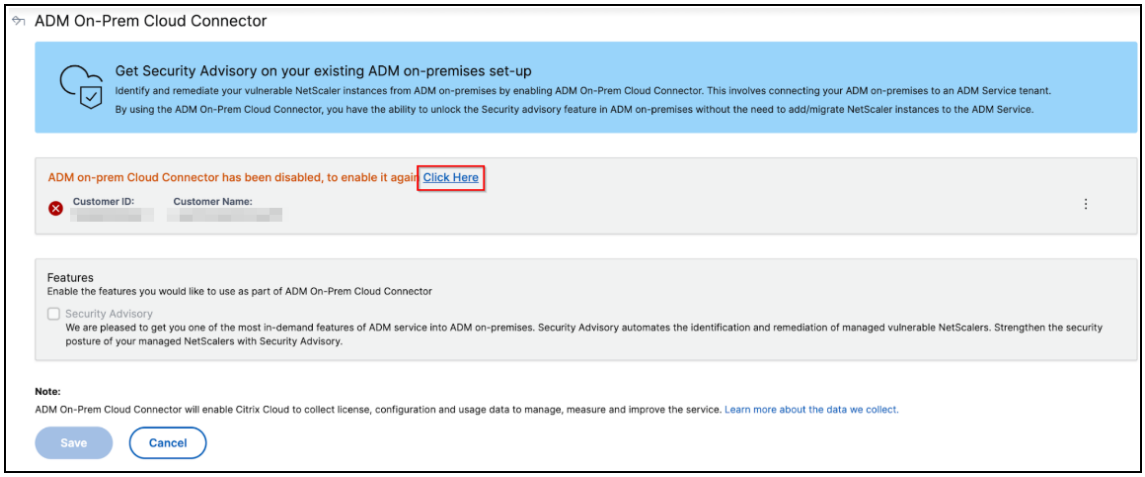
- 無効 -ADM オンプレミス Cloud Connector 機能を無効にします。無効にすることを選択した場合、データメトリックの収集は無効になり、セキュリティアドバイザリのフルバージョンは使用できなくなります。

  無効にするには、リストから [無効] をクリックします。



  確認メッセージが表示されます。[はい] をクリックして無効にします。

  ADM オンプレミス Cloud Connector は、追加の手順なしで後で再び有効にできます。



セキュリティアドバイザリを無効にする

ADM On-Prem Cloud Connector の設定ページから、セキュリティアドバイザリのチェックボックスをオフにしてセキュリティアドバイザリ機能を無効にすることもできます。データメトリクスは引き続き収集されます。

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。
- 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。NetScaler ADM でネットワークタイムプロトコル（NTP）サーバーの時計を NTP サーバーと同期するように構成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いくつかのシステム設定を構成することをお勧めします。

NetScaler ADM へのインスタンスの追加

February 6, 2024

インスタンスとは、NetScaler ADM から検出、管理、監視したい NetScaler アプライアンスまたは仮想アプライアンスです。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 NetScaler 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 MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- NetScaler Gateway

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 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。

> - NetScaler ADM がインスタンスを検出する方法については、「インスタンスの検出」を参照してください。

NetScaler プロファイルの作成方法

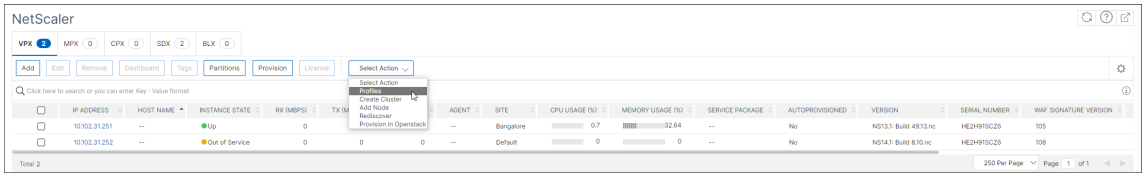
NetScaler プロファイルには、NetScaler ADM にインスタンスを追加するための資格情報、ポート、および認証タイプが含まれています。インスタンスの種類ごとにデフォルトのプロファイルが用意されています。たとえば、`nsroot` は NetScaler ADC インスタンスのデフォルトのプロファイルです。デフォルトのプロファイルは、デフォルトの NetScaler ADC 管理者の資格情報を使用して定義されます。インスタンスのデフォルトの管理者資格情報を変更した場合は、それらのインスタンスのカスタムのインスタンスプロファイルを定義できます。インスタンスが検出された後にインスタンス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 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を作成するには、必ずスーパー管理者アカウントを使用してください。

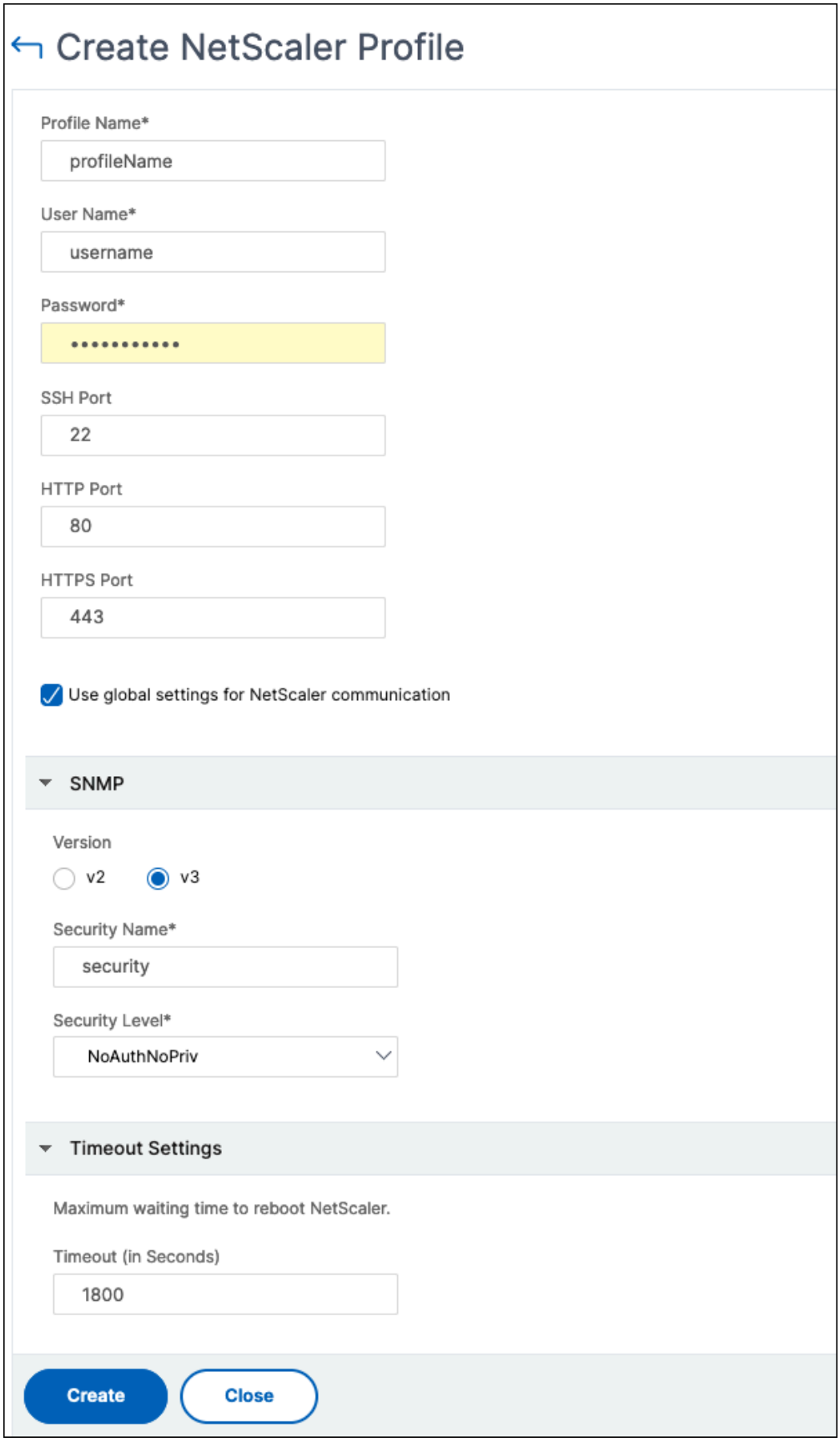
［インスタンス］ページから **NetScaler** プロファイルを作成するには:

1. ［**Infrastructure**］**>** ［**Instances**］の順に選択します。
2. インスタンスを選択します。たとえば、NetScaler などです。
3. ［NetScaler］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** プロファイルの作成ページで、次の操作を行います:



a) プロファイル名:NetScaler インスタンスのプロファイル名を指定します。

b) ユーザー名: NetScaler インスタンスにログオンするユーザー名を指定します。

c) パスワード:NetScaler インスタンスにログオンするためのパスワードを指定します。

d) **SSH** ポート:NetScaler ADM と NetScaler インスタンス間の SSH 通信用のポートを指定します。

e) **HTTP** ポート:NetScaler ADM と NetScaler インスタンス間の HTTP 通信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 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 CPX 間の通信にのみ使用できます。

f) **HTTPS** ポート:NetScaler ADM と NetScaler 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 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。

   > 注:
   >
   > NetScaler SDX では、**SNMPv2** のみがサポートされています。

i) タイムアウト設定: 再起動後、NetScaler 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。

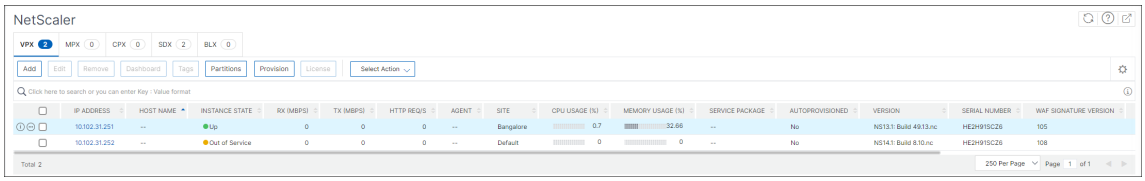
インスタンスを追加するには、各 NetScaler ADC インスタンスのホスト名または IP アドレス、または IP アドレスの範囲を指定する必要があります。

> 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。

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 にログオンします。
2. [インフラストラクチャ**] > [**インスタンス**] > [NetScaler**] に 移動します。追加するインスタンスのタイプ（NetScaler VPX など）を選択し、「追加」をクリック します。



3. 次のいずれかのオプションを選択します:

   - デバイス **IP** アドレスの入力-NetScaler 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。

     ```
     <SNIP of primary instance>#<SNIP of secondary instance>
     <!--NeedCopy-->
     ```

     たとえば、`10.10.10.11#10.10.10.12`

   - **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プロファイルを 作成します。
5. 「サイト」から、インスタンスを追加する場所を選択するか、「**+** 」アイコンをクリックして場所を作成します。
6. 「**OK** 」をクリック して、NetScaler ADM にインスタンスを追加するプロセスを開始します。

> 注:
>
> インスタンスを再検出する場合は、[インフラストラクチャ**] > [**インスタンス**] > [NetScaler**] に移動します。インスタンスタイプ（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。

NetScaler CPX インスタンスを **NetScaler ADM** に追加する

NetScaler ADM は、CPX 機能で達成された機能強化をサポートするように拡張されました。NetScaler 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 ホストからは検出されなくなりました。

1. [インフラストラクチャ**] > [**インスタンス**] > [NetScaler**] に移動し、[**CPX**] 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 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:

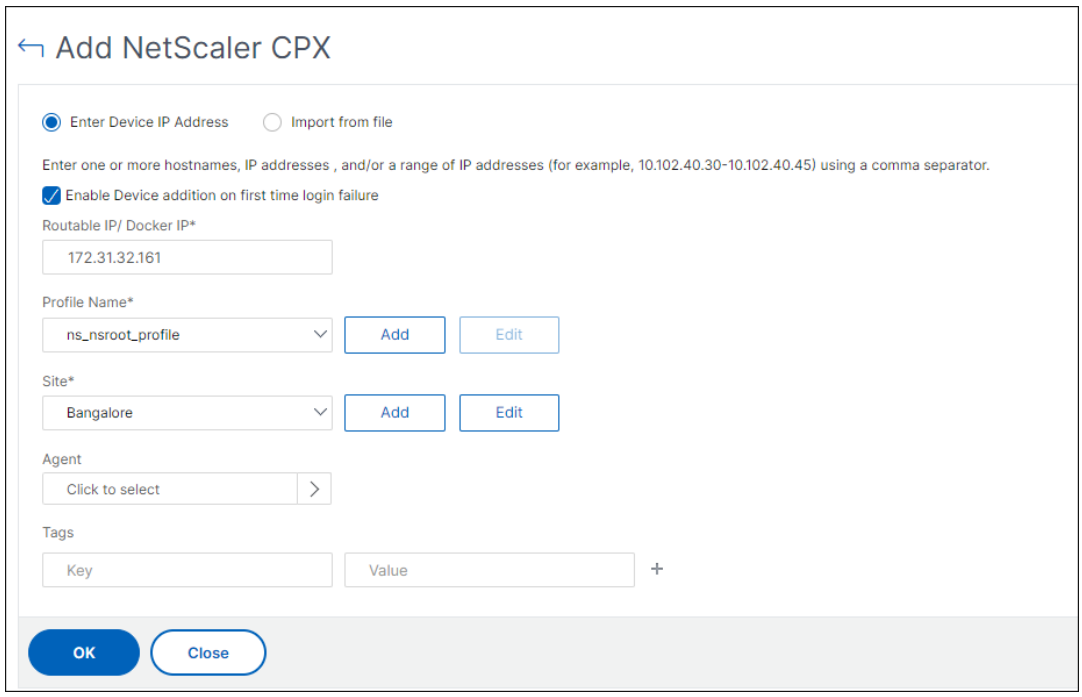
    a) CPX インスタンスの到達可能な IP アドレス、または CPX インスタンスがホストされている Docker コンテナの IP アドレスのいずれかを指定することにより、CPX インスタンスを追加できます。

    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、後で簡単にインスタンスを検索できます。



> 注:
>
> NetScaler CPX インスタンスの場合、CPX インスタンスプロファイルを作成するときに、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 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. [インフラストラクチャ] **>** [インスタンス] **>** [**NetScaler**] に移動します。
2. [**BLX**] タブで、[追加] をクリックします。
3. [インスタンスタイプ] リストから [スタンドアロン] オプションを選択します。
4. **IP** アドレスフィールドに、BLX インスタンスの IP アドレスを指定します。
5. ホスト **IP** アドレスフィールドに、BLX インスタンスがホストされている Linux サーバーの IP アドレスを指定します。
6. プロファイル名リストで、BLX インスタンスの適切なプロファイルを選択するか、プロファイルを作成します。

   プロファイルを作成するには、[追加] をクリックします。

> 重要:
>
> プロファイルに Linux サーバーの正しいホストユーザー名とパスワードを指定していることを確認してください。

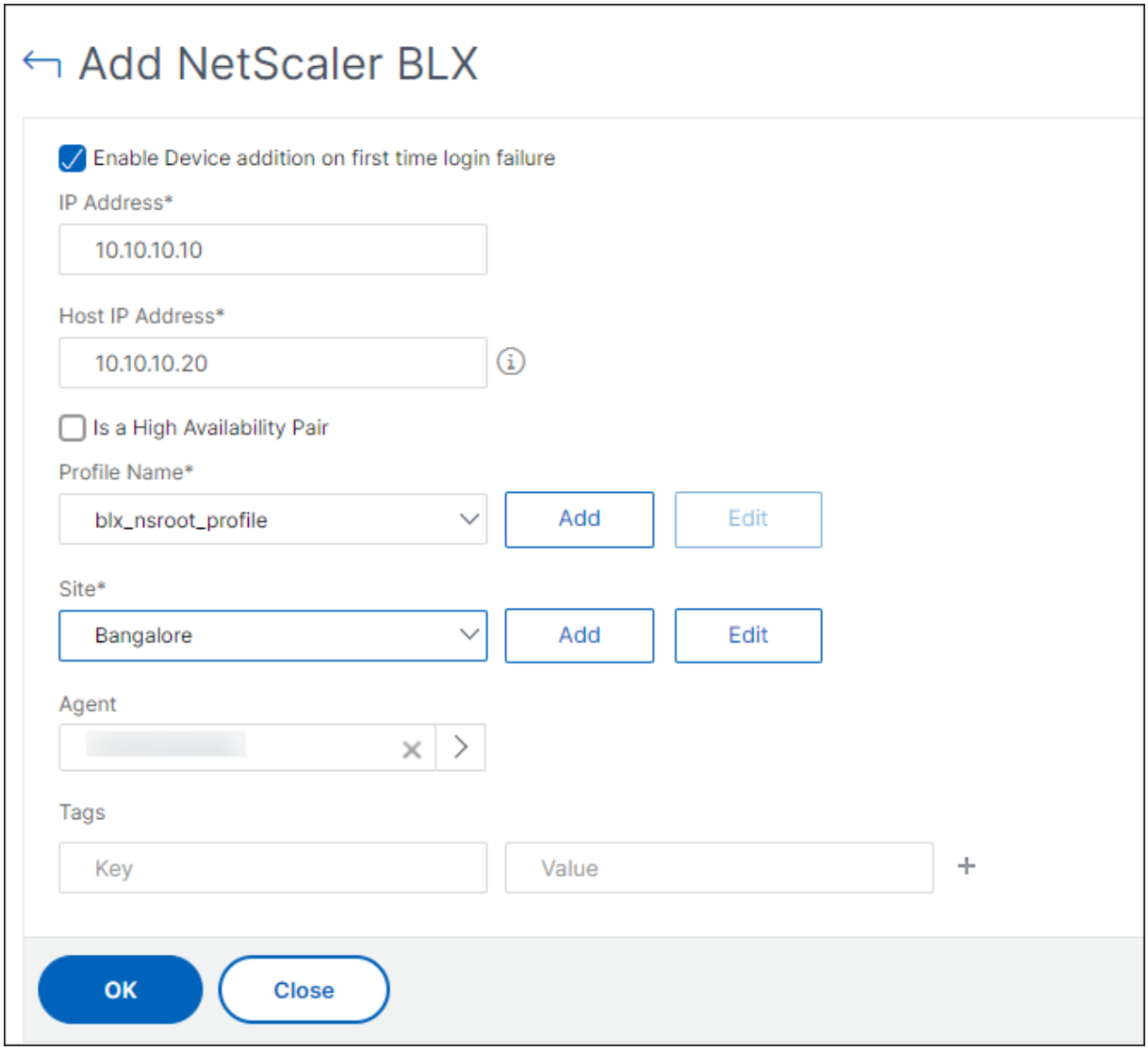
7. サイトリストで、インスタンスを追加するサイトを選択します。

   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。



NetScaler ADM に高可用性の **NetScaler 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**:**
   >
   > プロファイルに Linux サーバーの正しいホストユーザー名とパスワードを指定してください。

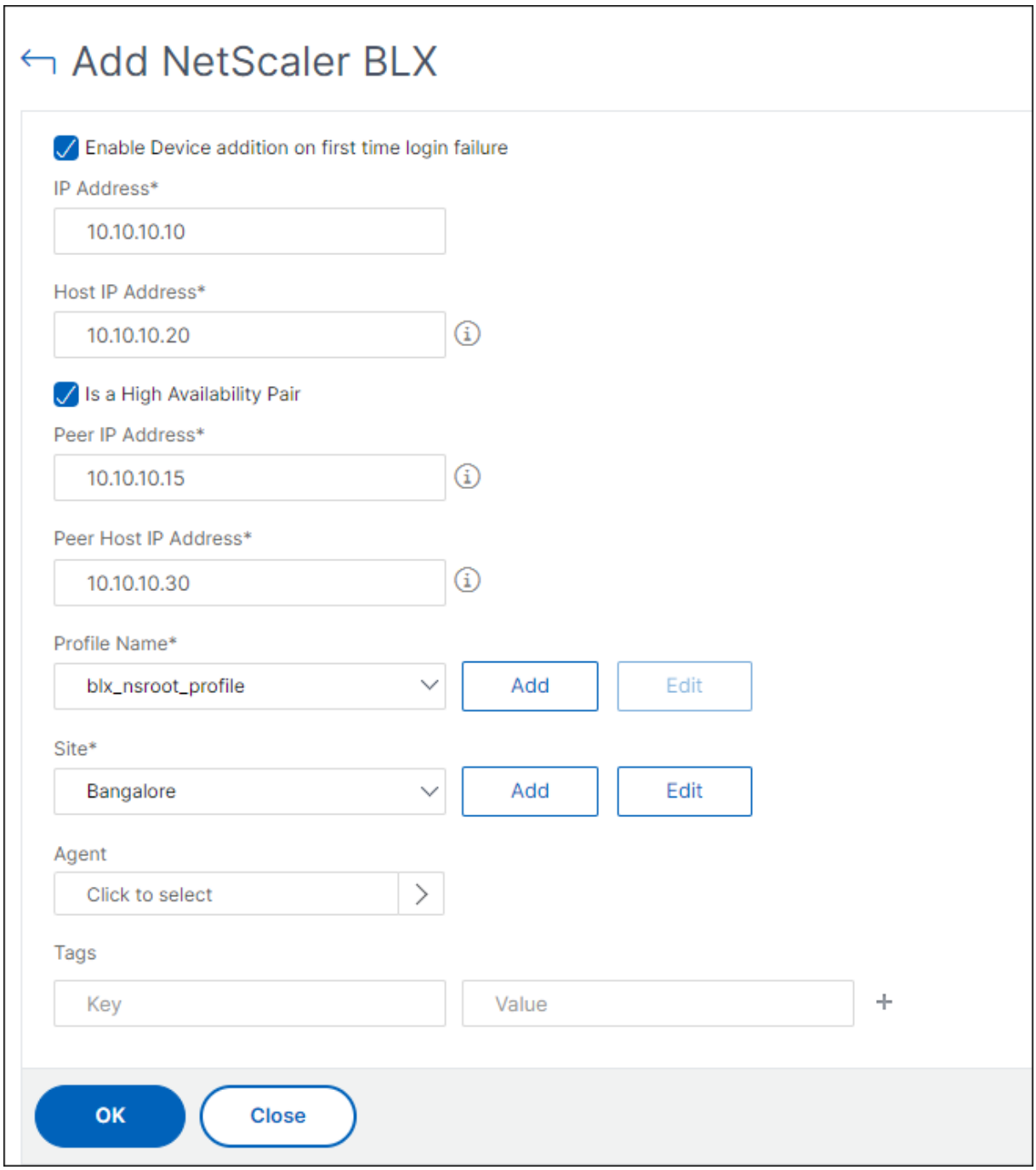
8. サイトリストで、インスタンスを追加するサイトを選択します。

   サイトを追加する場合は、[追加] をクリックします。

9. エージェントリストで、インスタンスを関連付ける NetScaler ADM エージェントを選択します。

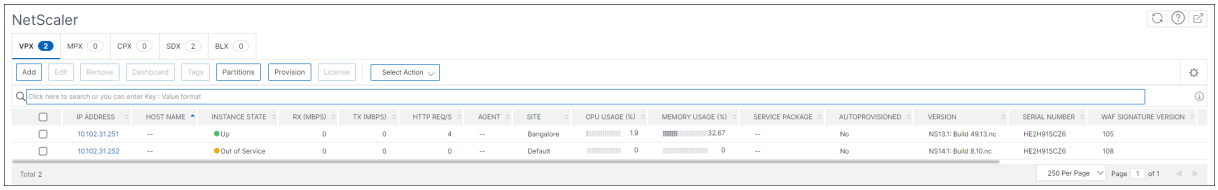
   NetScaler ADM にエージェントが 1 つしか構成されていない場合、そのエージェントはデフォルトで選択されます。

10. [**OK**] をクリックします。



NetScaler ADM からインスタンス **GUI** にアクセスする

1. [インフラストラクチャ**] >** [インスタンス] [**NetScaler**] に移動します。
2. アクセス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。



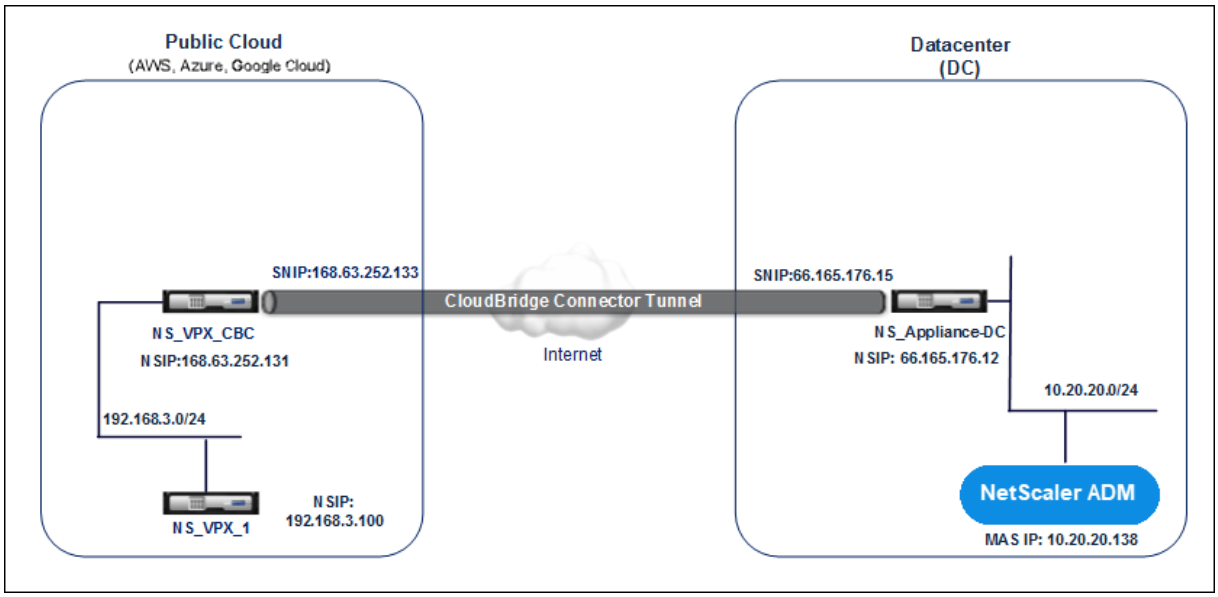
選択したインスタンスの GUI がポップアップウィンドウに表示されます。

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

NetScaler ADM を使用して、Amazon Web Services（AWS）、Microsoft Azure、Google Cloud などのパブリッククラウドにデプロイされた NetScaler 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、AWS への直接接続、Azure の VPN、または Equinix などのサードパーティコネクタなどのソリューションを使用できます。

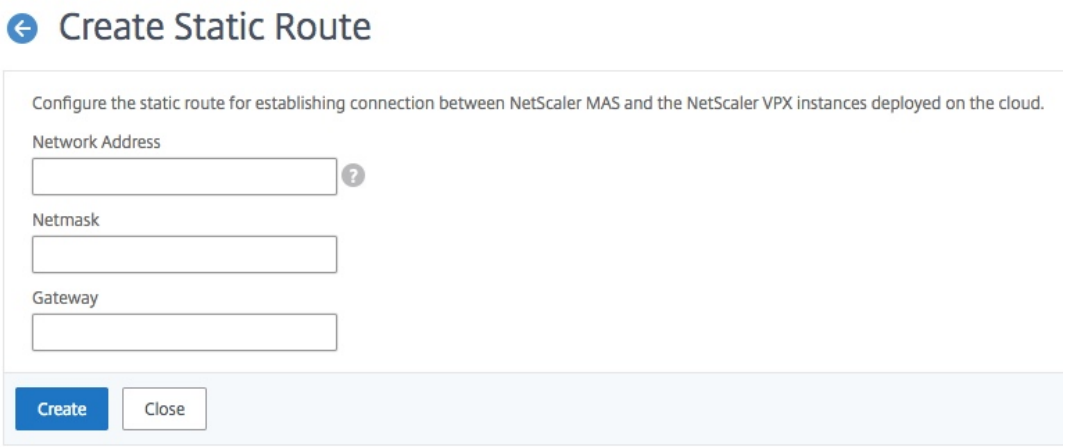
次のトポロジ例では、NetScaler ADM とクラウドにデプロイされた NetScaler ADC VPX インスタンス間のレイヤー 3 接続に Citrix CloudBridge Connector を使用しています。



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内の NetScaler ADC 仮想アプライアンス（VPX）NS_VPX_CBC の間に設定されます。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 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 VPX を Microsoft Azure 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 VPX を Google クラウド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。



   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立するネットワークのアドレスを入力します。
   d) [**Netmask**] フィールドに、ネットワークのネットマスクを入力します。
   e)「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 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

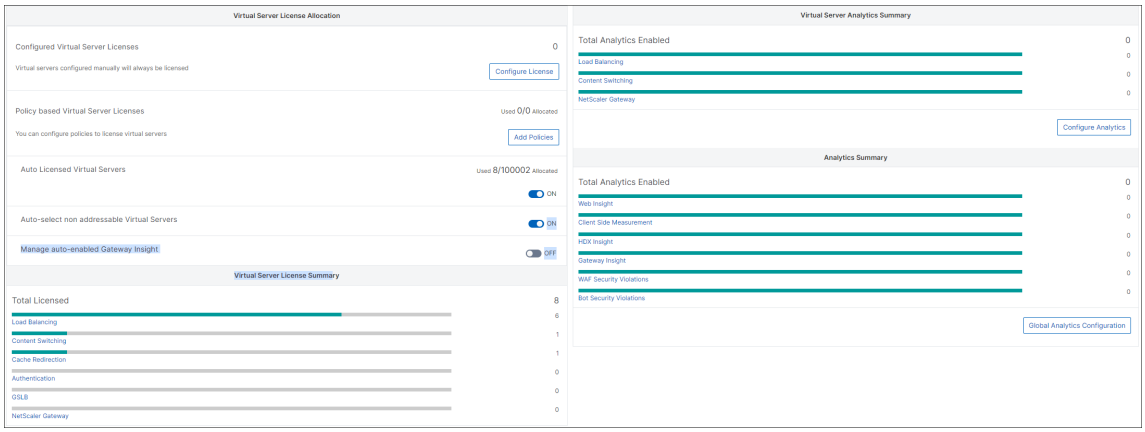
February 6, 2024

> 注
>
> - 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。[設定] **>** [ライセンスと分析の設定] 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。

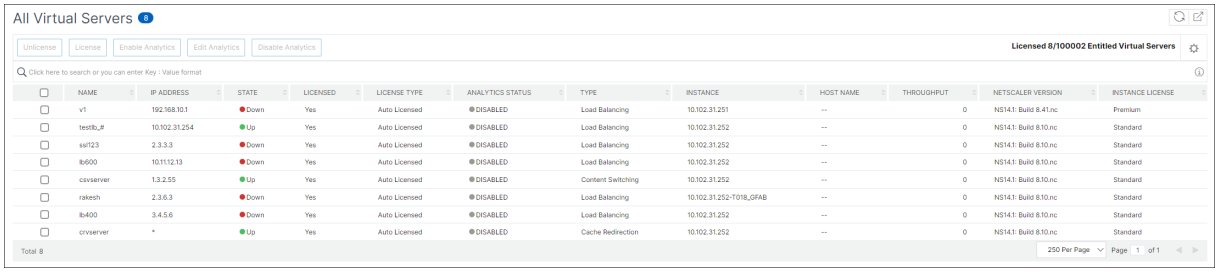
分析を有効にするプロセスが簡素化されます。仮想サーバーのライセンスを取得し、1 つのワークフローで分析を有効にできます。

[設定] **>** [ライセンスとアナリティクスの設定] に移動して

- 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。



[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。

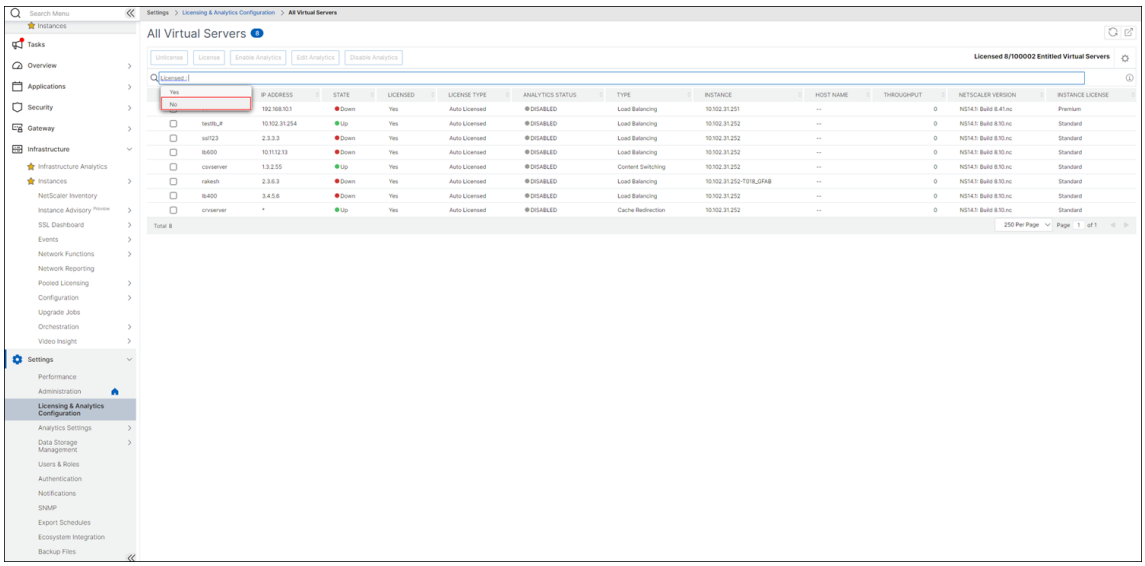
- ライセンスのない仮想サーバーにライセンスを適用
- ライセンスされた仮想サーバーのライセンスを削除
- ライセンスされた仮想サーバーで分析を有効にする
- 分析の編集
- 分析を無効にする

> 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

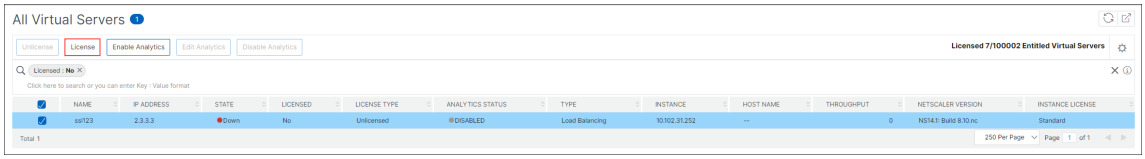
仮想サーバーのライセンスを取得するには、「すべての仮想サーバー」ページから：

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。

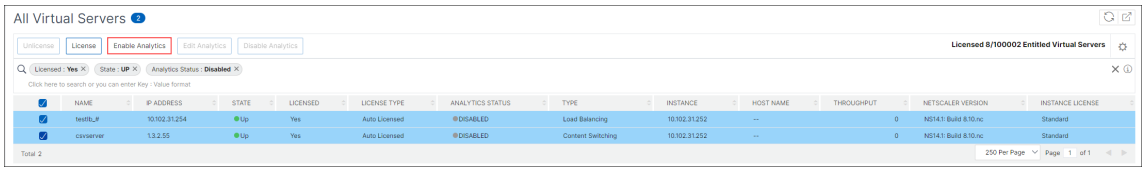
分析を有効にする

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. [ **インフラストラクチャ] > [インスタンス] > [NetScaler**
>    ] に移動し、インスタンスタイプを選択します。たとえば、VPX
>    です。
> 2.
> 3. 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. 「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) インサイトの種類 (Web Insight または WAF セキュリティ違反) を選択します。

b) **Logstream** をトランスポートモードとして選択

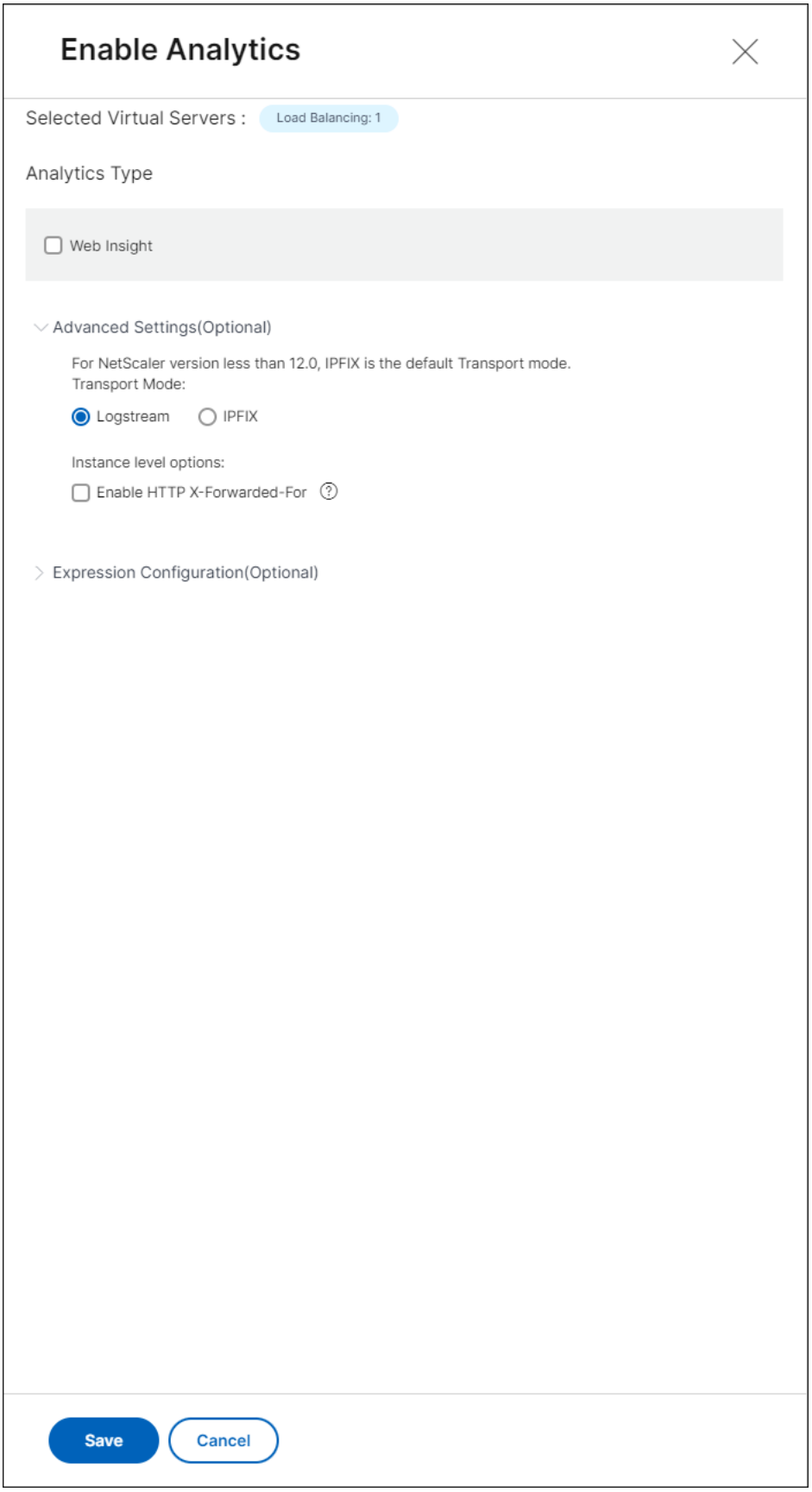
> 注
>
> NetScaler 12.0 以前の場合、**IPFIX** はトランスポートモードのデフォルトのオプションです。NetScaler 12.0 以降では、トランスポートモードとして［ログストリーム］または［**IPFIX** ］を選択できます。
>
> IPFIX とログストリームの詳細については、「ログストリームの概要」を参照してください。

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



> 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
>
> NetScaler ADM は、ログストリームには NetScaler SNIP を使用し、IPFIX には NSIP を使用します。NetScaler ADM エージェントと NetScaler インスタンスの間でファイアウォールが有効になっている場合は、必ず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. [**インフラストラクチャ] > [インスタンス] > [NetScaler**] に移動し、インスタンスタイプを選択します。たとえば、VPX です。
   2.
   3. 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	•	•
WAF セキュリティ違反	•	•
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	•	•

仮想サーバーでの分析を可能にする統一されたプロセス

February 6, 2024

アナリティクスを有効にする既存のプロセスとは別に、単一ペインのワークフローを使用して次の項目についてアナリティクスを構成することもできます。

- ライセンスされた既存の仮想サーバすべて
- それ以降にライセンスされた仮想サーバー

この機能を設定すると、既存および後続の仮想サーバーで分析を手動で有効にする必要がなくなります。

注意すべき点:

分析を構成する前に、NetScaler ADM の次の動作を理解しておく必要があります。

- この機能を初めて設定するときは、このドキュメントに記載されている前提条件が満たされていることを確認する必要があります。
- アナリティクスの設定を後で変更します。

  Web Insight、HDX Insight、および Gateway Insight を選択して、初めて分析設定を構成したとします。分析設定を後で変更し、Gateway Insight の選択を解除する場合、その変更は分析ですでに有効になっている仮想サーバーには影響しません。
- アナリティクスがすでに有効になっている仮想サーバー。

  ライセンスされた仮想サーバーが 10 台あり、そのうちの 2 台はすでに分析が有効になっているとします。このシナリオでは、この機能により、残りの 8 台の仮想サーバーについてのみ分析が有効になります。
- Analytics で手動で無効にされた仮想サーバー。

  ライセンスされた仮想サーバが 10 台あり、2 台の仮想サーバの分析を手動で無効にしているとします。このシナリオでは、この機能により、残りの 8 台の仮想サーバーについてのみ分析が有効になり、分析で手動で無効にされた仮想サーバーはスキップされます。
- **Bot Security Violations** および **WAF Security Violations** オプションは、プレミアムライセンスの仮想サーバーでのみサポートされます。仮想サーバーがプレミアムライセンスではない場合、ボットセキュリティ違反と **WAF** セキュリティ違反は有効になりません。

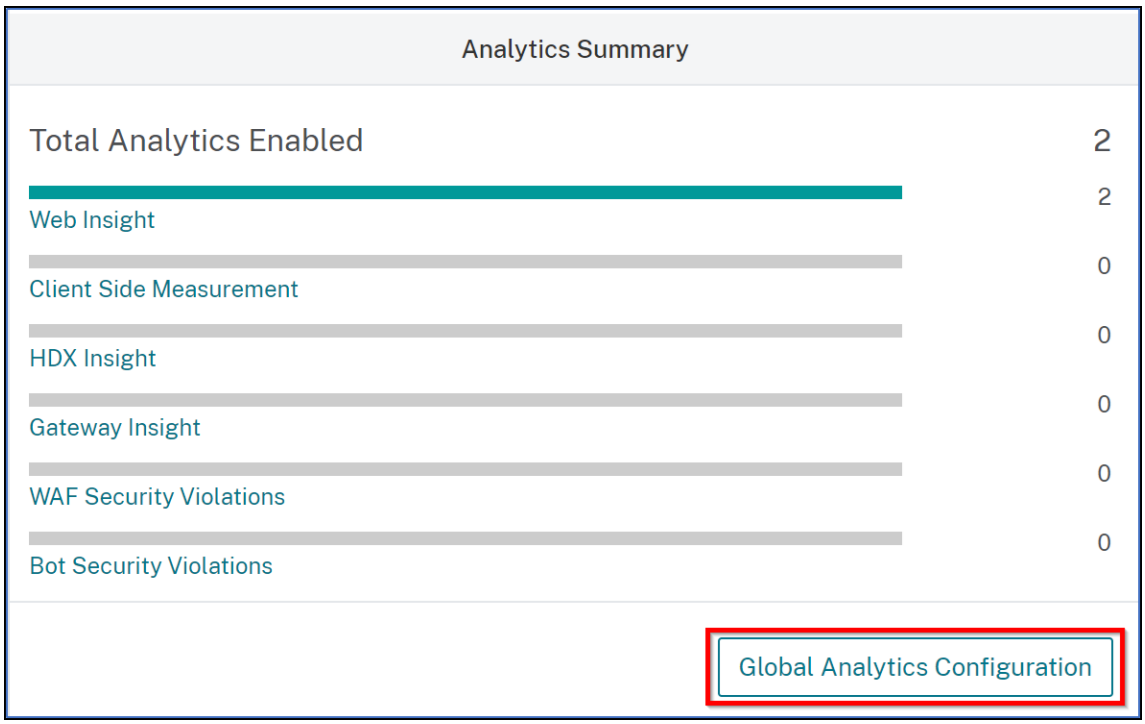
前提条件

以下の点を確認してください。

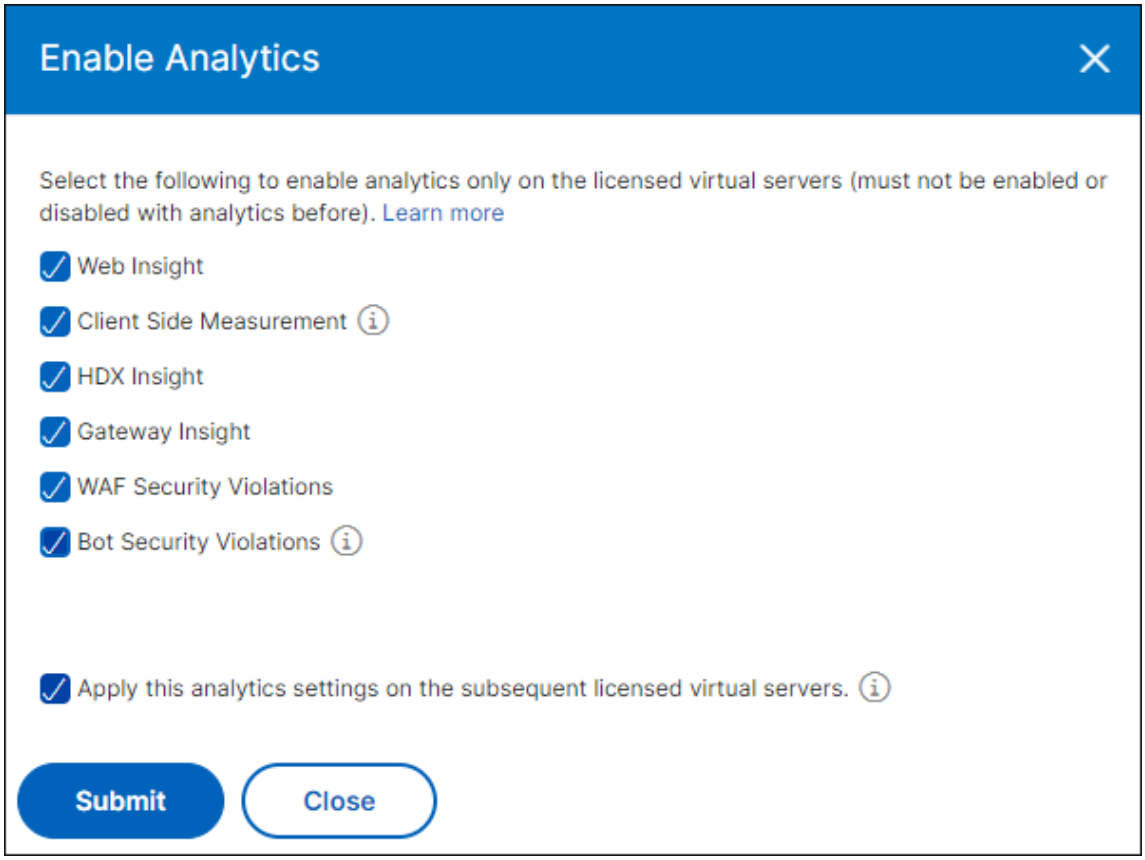
- 既存のすべての仮想サーバにライセンスが付与されます。
- 自動ライセンスオプションを有効にすると、後続のすべての仮想サーバにライセンスが付与されます。[設定**] > [**ライセンス **&** 分析設定**]** に移動し、[仮想サーバーライセンスの割り当て] で [自動ライセンス仮想サーバー] オプションをオンにします。

分析を有効にする

1. [設定**] > [**ライセンスと分析の設定**]** に移動します。
2. [**Analytics** サマリー] で、[グローバル分析設定



3. 仮想サーバーで分析を有効にする分析機能を選択します。
4. 後続の仮想サーバーで分析を有効にするには、[この分析設定を後続のライセンス仮想サーバーに適用する] チェックボックスをオンにします。
5. [**Submit**] をクリックします。



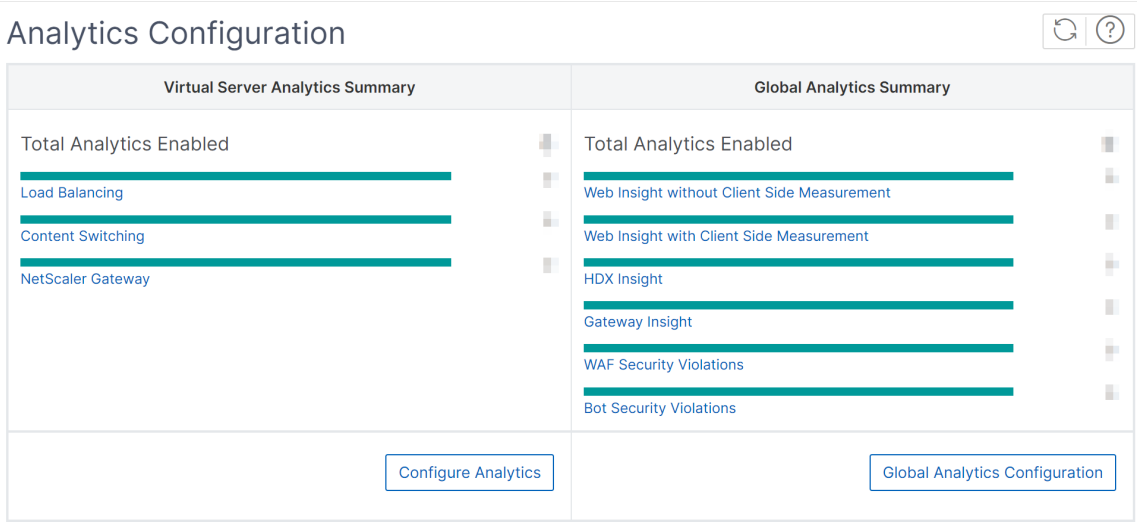
フレキシブルライセンス仮想サーバーで分析を設定

February 6, 2024

分析を有効にするための前提条件は、仮想サーバーにライセンスが必要であることです。フレックスライセンスを使用する場合、既存のすべての仮想サーバーとそれ以降の仮想サーバーには自動的にライセンスが付与されます。分析の設定に進むことができます。

分析は 2 つの方法で設定できます。[設定] **> [**アナリティクス設定] に移動すると、以下が表示されます。

- 仮想サーバー分析の概要-既存の仮想サーバーで分析を設定できます。
- グローバル分析サマリー-既存の仮想サーバーと後続の仮想サーバーの両方で分析を設定できます。



既存の仮想サーバーで分析を設定

> 注:
>
> 分析を有効にする仮想サーバーが **UP** 状態であることを確認します。

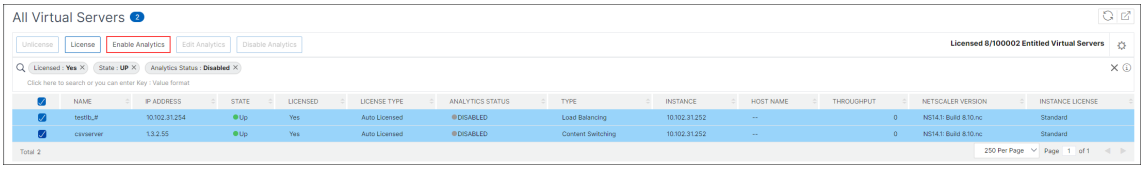
1. 「仮想サーバー分析の概要」で、「分析の設定」をクリックします。

   [すべての仮想サーバー] ページが表示されます。次の操作を実行できます:

   - 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。

2. 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、インスタンスのアナリティクスを有効にすることもできます。

```
1. [ **インフラストラクチャ] > [インスタンス] > [NetScaler**
   ] に移動し、インスタンスタイプを選択します。たとえば、VPX
```



```
です。
2
3 1. インスタンスを選択し、「 **アクションを選択**」 リストから「 **アナリティクスの設定** 」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。
```

3.「アナリティクスを有効にする」ウィンドウで:

a) インサイトタイプを選択します。

b) トランスポートモードとして [ログストリーム] を選択します。

> 注:
>
> NetScaler 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 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) デフォルトでは、エクスプレッションは true です。

e) ［**OK**］をクリックします。

> 注:
>
> - 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
>
> NetScaler ADM は、ログストリームには NetScaler SNIP を使用し、IPFIX には NSIP を使用します。NetScaler ADM エージェントと NetScaler インスタンスの間でファイアウォールが有効になっている場合は、必ず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. 仮想サーバーを選択します。

   注:

   または、インスタンスのアナリティクスを編集することもできます。

   ```
   1. [ **インフラストラクチャ] > [インスタンス] > [NetScaler**] に移動し、インスタンスタイプを選択します。たとえば、VPX です。
   2
   3. 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. 仮想サーバーを選択します。
2. 「アナリティクスを無効にする」をクリックします。

NetScaler ADM は、選択した仮想サーバーの分析を無効にします。

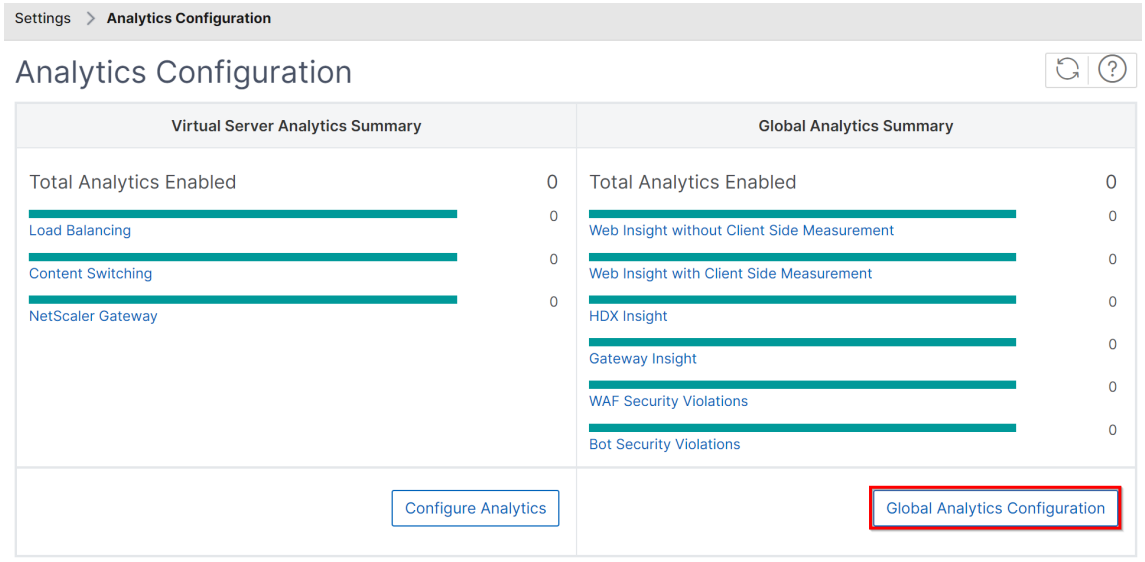
次の表では、IPFIX および Logstream をトランスポートモードとしてサポートする NetScaler ADM 機能を説明します。

機能	IPFIX	Logstream
Web Insight	•	•
WAF セキュリティ違反	•	•

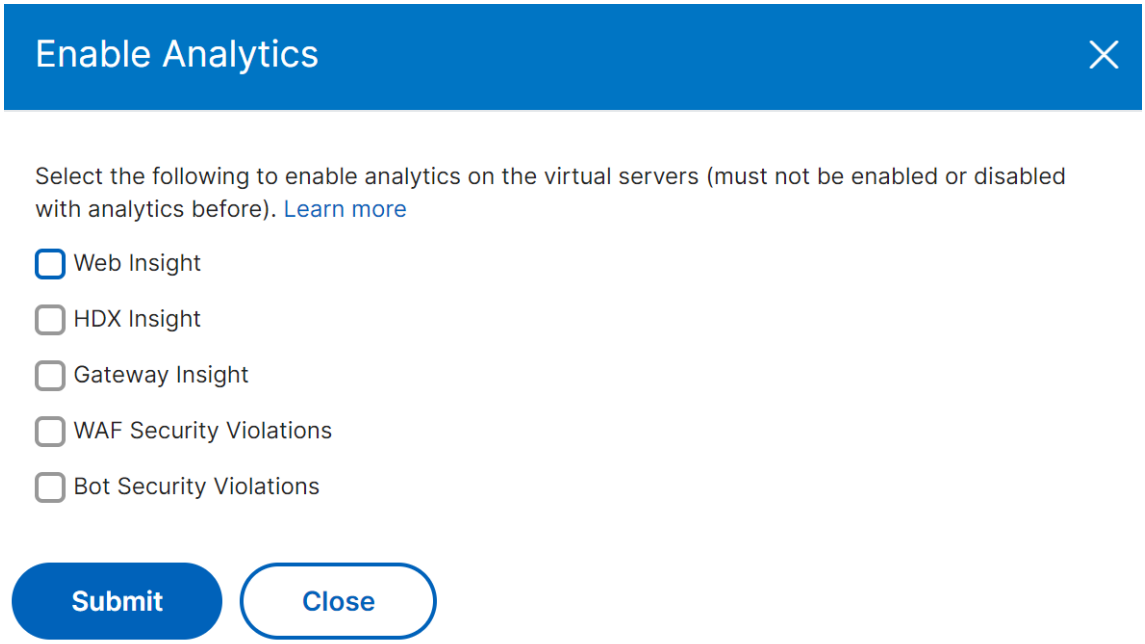
機能	IPFIX	Logstream
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	未サポート	•
CR Insight	•	•
IP レピュテーション	•	•
AppFirewall	•	•
クライアント側の測定	•	•
Syslog/Auditlog	•	•

アナリティクスをグローバルに設定

1. 「グローバルアナリティクスの概要」で、「グローバルアナリティクスの設定」をクリックします。



2. 仮想サーバーで分析を有効にする分析機能を選択します。
3. [Submit] をクリックします。



構成後、分析は既存の仮想サーバーと後続の仮想サーバーの両方で有効になります。

注意事項

- Web Insight、HDXInsight、GatewayInsight を選択して、グローバル分析構成を初めて構成したとします。後で分析設定を再度変更して Gateway Insight を選択解除しても、その変更は、すでに分析が有効になっている仮想サーバーには影響しません。
- ライセンスされた仮想サーバーが 10 台あり、そのうち 2 台が **Configure Analytics** オプションを使用して既に分析を有効にしているとします。このシナリオでは、グローバル分析設定を構成すると、分析は残りの 8 台の仮想サーバーにのみ適用されます。
- ライセンスされた仮想サーバが 10 台あり、2 台の仮想サーバの分析を手動で無効にしているとします。このシナリオでは、グローバル分析構成を構成すると、分析は残りの 8 台の仮想サーバーにのみ適用され、分析で手動で無効化された仮想サーバーはスキップされます。

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

February 6, 2024

NetScaler ADM で仮想サーバーの分析を有効にすると、NetScaler からの AppFlow データが NetScaler サブネット IP アドレス（SNIP）を介して NetScaler ADM にエクスポートされます。シナリオによっては、ネットワーク内のファイアウォールが原因で SNIP がブロックされることがあります。このようなシナリオでは、SNIP とは異な

る IP アドレスを使用する必要がある場合があります。ネットプロファイルの詳細については、「指定されたソース IP をバックエンド通信に使用する」を参照してください。

NetScaler ADM を使用してネットプロファイルを NetScaler インスタンスに割り当てて、NetScaler から NetScaler ADM に AppFlow データをエクスポートできます。

前提条件

以下の点を確認してください。

- **NetScaler** インスタンスのバージョンは **13.0-48.4** 以降です。
- ネットプロファイルは NetScaler インスタンスで構成されます。

NetScaler ADM でネットプロファイルを割り当てるには:

1. [インフラストラクチャ**] > [**インスタンス**] > [NetScaler**] に移動します。
2. インスタンスを選択し、「アクションの選択」リストから「ネットプロファイルの設定」をクリックして、インスタンスにネットプロファイルを割り当てます。
3. リストからネットプロファイルを選択し、[適用] をクリックします。

> 注:
>
> インスタンスにネットプロファイルを割り当てる前に、必ずすべての仮想サーバーの分析を無効にしてください。

NTP サーバーの構成

February 6, 2024

NetScaler ADM のネットワークタイムプロトコル（NTP）サーバーは、その時計を NTP サーバーと同期するように構成できます。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。

NetScaler ADM で NTP サーバーを構成するには:

1. ADM GUI から、[設定**] > [**管理**]** に移動します。[システム管理] ページの [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。
- **Minimum 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

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. [設定**] > [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、[設定**] > [**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. [設定**] >** [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. [設定**] > [**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. [設定**] > [**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. [設定**] > [**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、**NetScaler ADM** サーバー上のデータを保持する期間を日単位で入力し、「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. [設定**] > [**管理] に移動します。
2. [バックアップ] で、[システムとインスタンスのバックアップの設定] 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

NetScaler インスタンスの現在の状態をバックアップすると、インスタンスが不安定になった場合に、バックアップファイルを使用して安定性を回復できます。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. [設定] **>** [管理] に移動します。
2. [バックアップ] で、[システムとインスタンスのバックアップの設定] 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、[設定] **> [**管理] **> [**構成可能な機能] 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 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 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。NetScaler ADM で受信したイベントは [イベントの概要] ページ（[インフラストラクチャ] **>** [イベント]）に表示され、すべてのアクティブなイベントは [イベントメッセージ] ページ（[インフラストラクチャ] **>** [イベント] **>** [イベントメッセージ]）に表示されます。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。

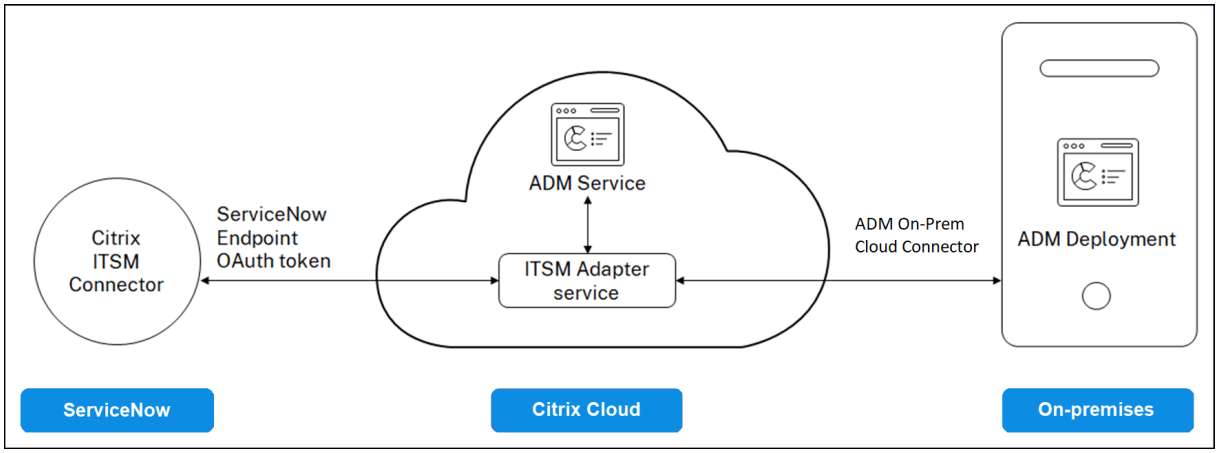
> 重要:
>
> 機能が無効になっている場合、ユーザーはその機能に関連付けられた操作を実行できません。

NetScaler ADM を ServiceNow インスタンスと統合する

February 6, 2024

NetScaler 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 オンプレミスデプロイを ITSM アダプターに接続するには、ADM オンプレミ Cloud Connector が設定されていることを確認してください。詳細については、「ADM オンプレミ CloudConnector」を参照してください。

ServiceNow を ADM ビルド 14.1 4.x 以前と統合する場合は、必ずカスタマー 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。

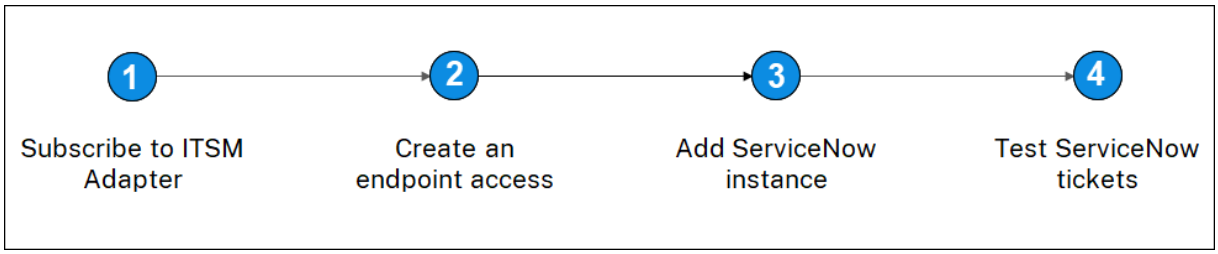
前提条件

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

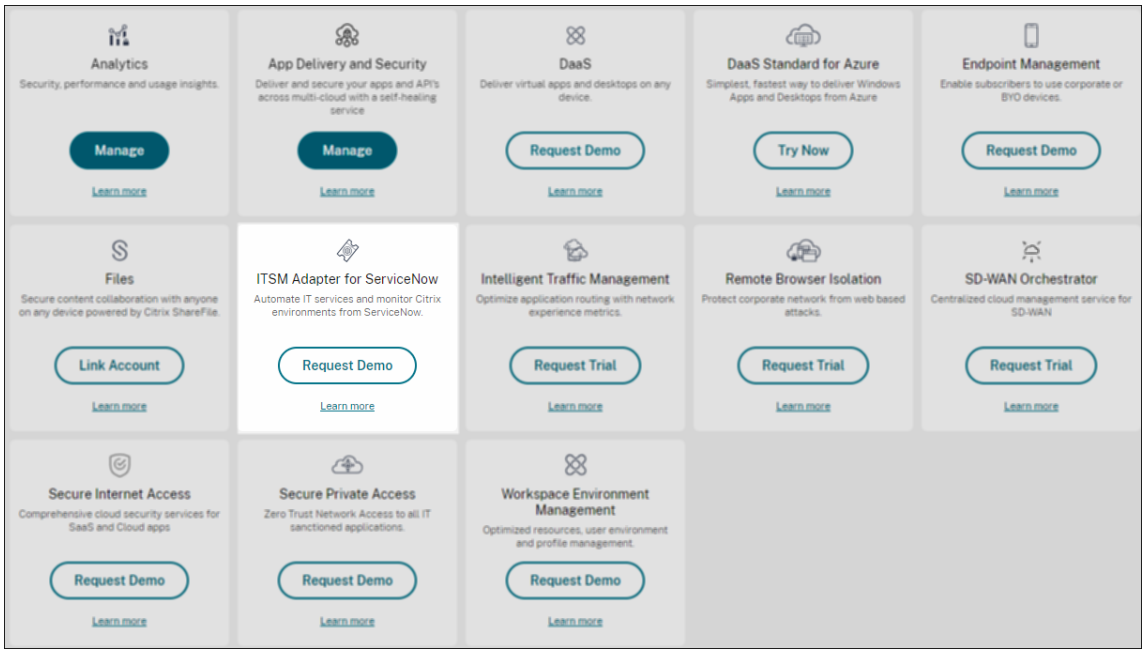
ITSM コネクタを使用して NetScaler ADM と ServiceNow を統合するには、次の手順を実行します。



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

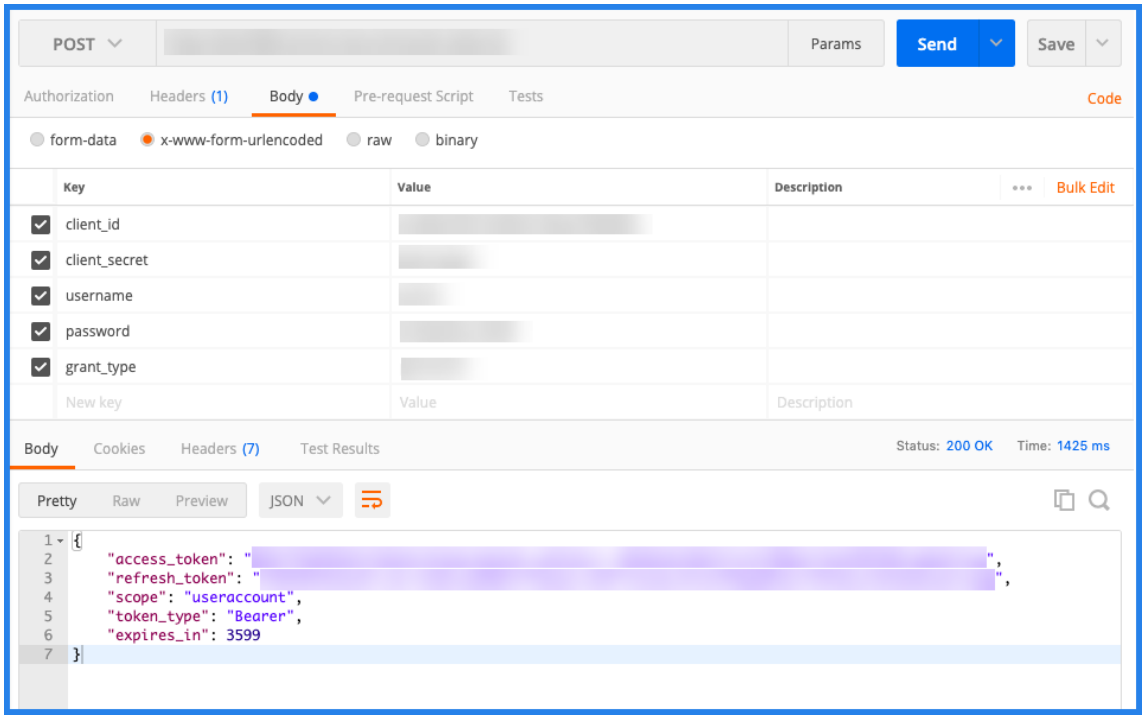
1. [**ITSM** アダプタ] タイルで、[試用版の要求] をクリックします。



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。

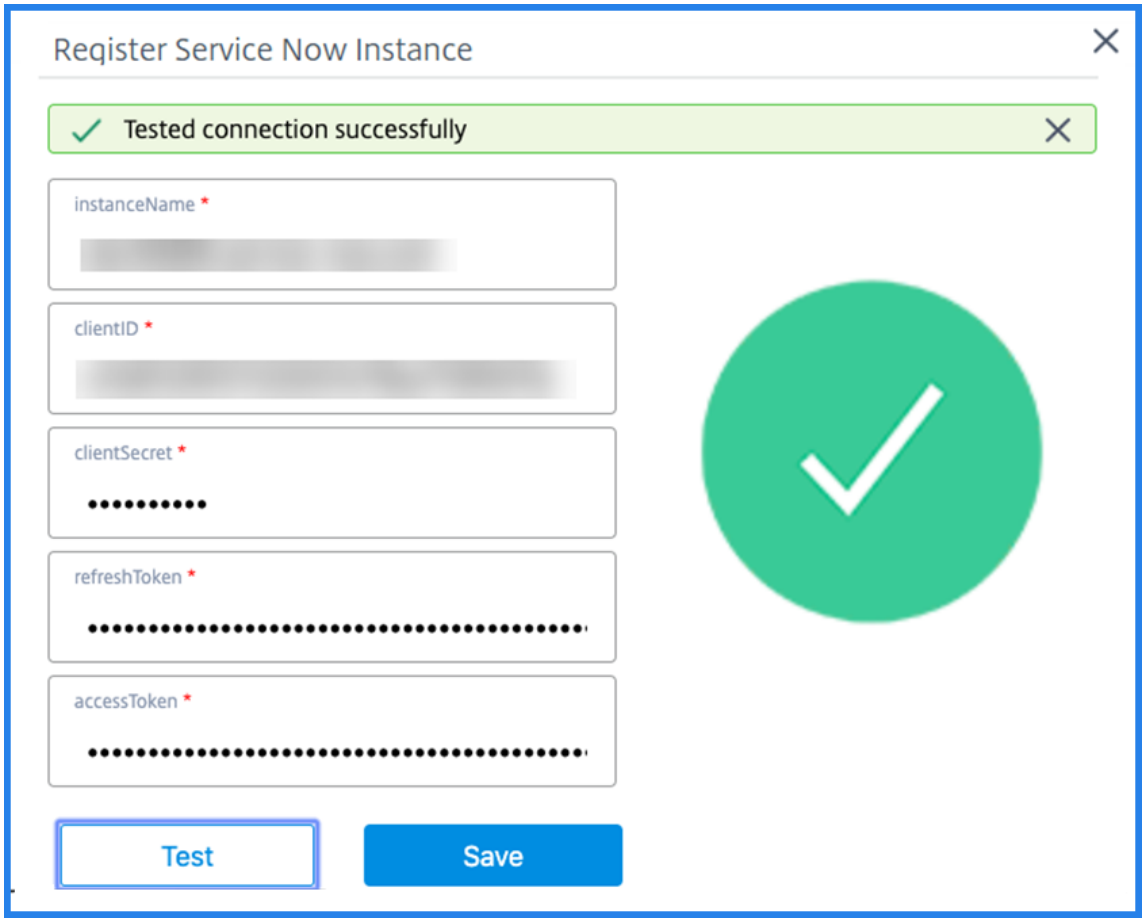
ステップ **2-ServiceNow** インスタンスでエンドポイントアクセスを作成する

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。

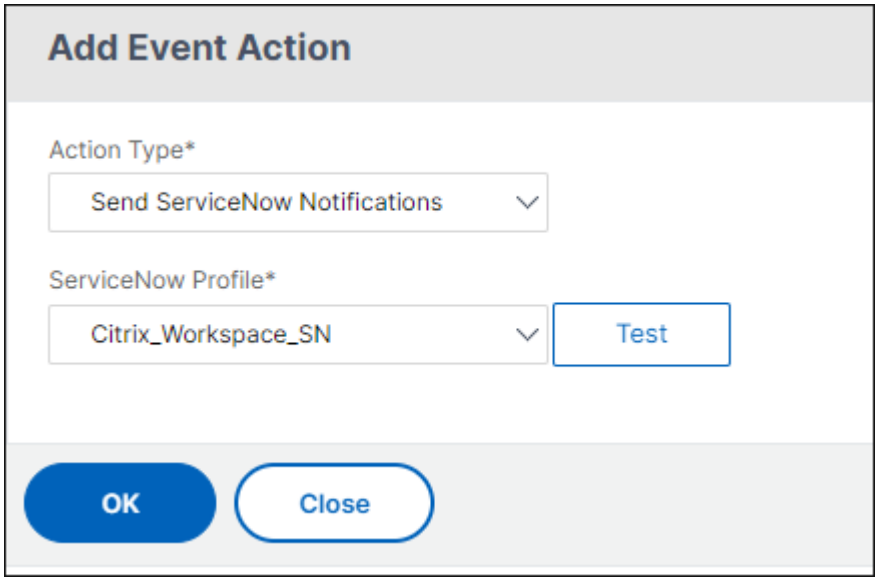
> 重要:
>
> この機能は、ServiceNow クラウドでサポートされています。

- **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。

  ADM でイベントルールを作成するには、[インフラストラクチャ] > [イベント] > [ルール] の順に移動します。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。



  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 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**］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。

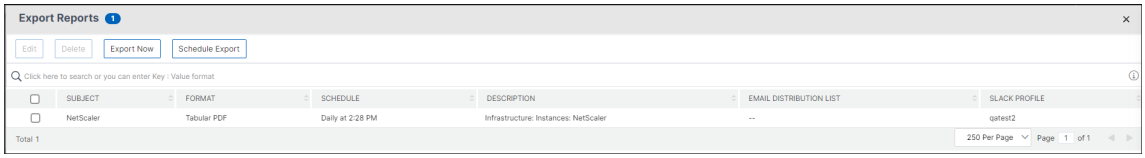
「レポートのエクスポート」では、次のアクションを実行できます。

- 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。

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

NetScaler ADM Downloads 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 14.1 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、NetScaler ADM はアップグレードが完了するまでデータを処理しません。

> 重要
>
> NetScaler ADM のバージョンとビルドは、NetScaler のバージョン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 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。

14.1 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。
    1. 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。
    2. バージョン 12.1 の最新ビルドにアップグレードします。
    3. バージョン 13.1 にアップグレードしてください。
    4. バージョン 14.1 にアップグレードしてください。
- 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、次に 13.1 にアップグレードし、次に 14.1 にアップグレードします。
- 12.1 からアップグレードする場合は、まず 13.0 64.xx にアップグレードしてから、直接 14.1 にアップグレードする必要があります。
- 13.0 64.xx より前のバージョンからアップグレードする場合は、ユーザーエクスペリエンスを向上させるために、まず 13.0 64.xx にアップグレードしてから 14.1 にアップグレードしてください。
- 14.1 へのアップグレードが成功して GUI にログインすると、デフォルトパスワードを使用している場合はパスワードを変更することを推奨します。

14.1 xx.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 14.1 xx.xx にアップグレードすると、ADM データベースも移行されます。このデータ移行は、ADM が PostgreSQL バージョン 10.11 を使用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:

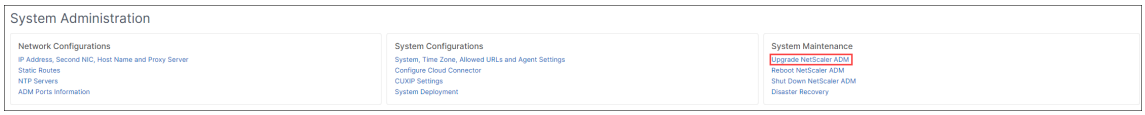
- 14.1 xx.xx 以降にアップグレードする場合は、アップグレードごとに NetScaler ADM サーバーのスナップショットを作成します。
- アップグレードする前に、NetScaler ADM サーバーをバックアップしてください。
- アップグレード後、NetScaler ADM サーバーと管理対象インスタンス間の接続の再確立が必要になる場合があります。「続行すると接続に失敗する可能性がある」という旨を警告する確認メッセージが表示されます。
- 13.1.9.x から 13.1.30.x までのいずれかのバージョンにアップグレードすると、NetScaler ADM は既存の StyleBook 構成パックを以前のバージョンにロールバックします。

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

単一の **NetScaler ADM** サーバーを **14.1 4.x** にアップグレードします

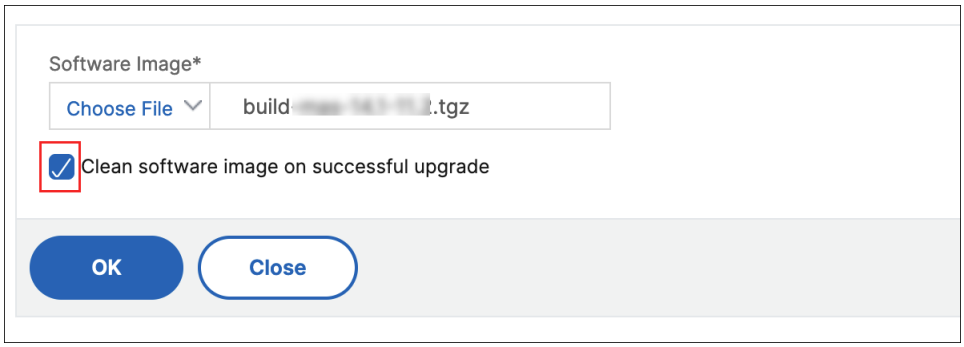
1. 管理者の資格情報を使用して NetScaler ADM にログオンします。
2. [設定] > **[**** 管理**]** に移動します。**[**** システムメンテナンス] で、[**NetScaler ADM** のアップグレード] をクリックします。



3. [**NetScaler ADM** のアップグレード] ページで、[アップグレード成功時にソフトウェアイメージを消去する] 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選択しない場合は、イメージを手動で削除する必要があります。

4. 次に、ローカル（ローカルマシン）またはアプライアンスのいずれかを選択して、新しいイメージファイルをアップロードできます。ビルドファイルは、NetScaler ADM 仮想アプライアンス上に存在する必要があります。



5. [**OK**] をクリックします。
   [確認] ダイアログボックスが表示されます。[はい] をクリックします。

   アップグレードプロセスが開始されます。

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。

高可用性ペアを **14.1** リリースにアップグレードする

高可用性モードの NetScaler 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。

NetScaler ADM ディザスタリカバリ展開のアップグレード

> 注:
>
> HA ペアとディザスタリカバリノードの両方でパスワードが同じであることを確認してください。

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。
- 障害回復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た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. NetScaler ADM アップグレードイメージファイルを NetScaler サイトから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. 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 NetScaler サイトから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。

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 12.1～13.10 からアップグレードしても、以前のバージョンで追加ディスクに作成したパーティションは同じままです。パーティションは削除もサイズ変更もされません。

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。

認証

February 6, 2024

ユーザーは、NetScaler ADM による内部認証、認証サーバーによる外部認証、またはその両方で認証できます。ローカル認証を使用する場合、ユーザーは NetScaler ADM セキュリティデータベースに存在する必要があります。ユーザーが外部で認証される場合、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、およびアカウンティング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 NetScaler ADM 実装にユーザーがアクセスしようとすると、要求されたアプリケーションサーバーは、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 NetScaler ADM へのアクセス権が付与されます。

外部認証サーバ

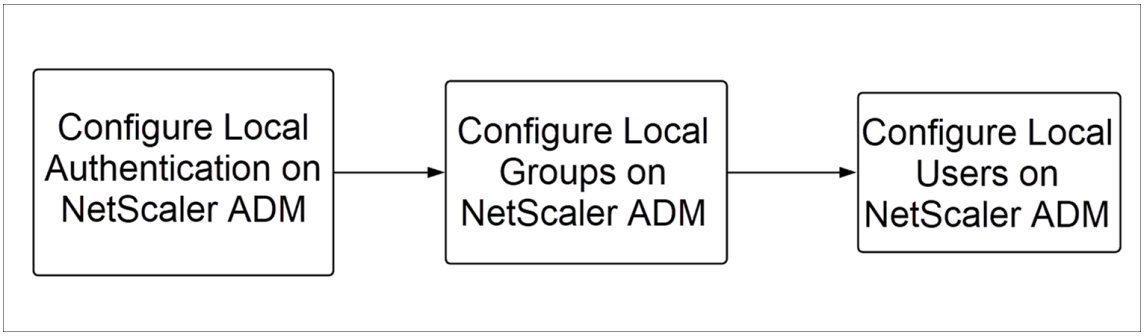
NetScaler ADM は、すべての認証、承認、および監査サービス要求をリモート RADIUS、LDAP、または TACACS サーバーに送信します。リモート認証、承認、および監査サーバーは、要求を受信し、要求を検証し、NetScaler ADM に応答を送信します。認証にリモート RADIUS、TACACS、または LDAP サーバーを使用するように構成すると、NetScaler ADM は RADIUS、TACACS、または LDAP クライアントになります。これらのいずれの構成でも、認証記録はリモートホストサーバーのデータベースに格納されます。アカウント名、割り当てられたアクセス許可、および時間アカウンティングレコードは、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。

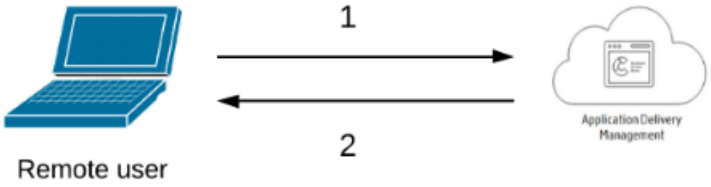
NetScaler ADM でユーザーを認証する

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。

- NetScaler ADM で構成されたローカルユーザー



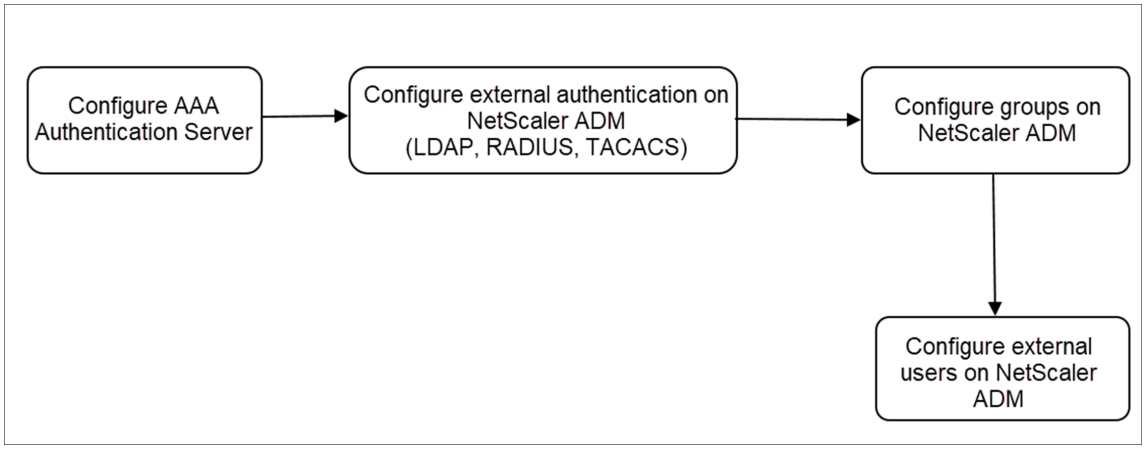
設定後、ローカルサーバでのユーザ認証のワークフローを次に示します。



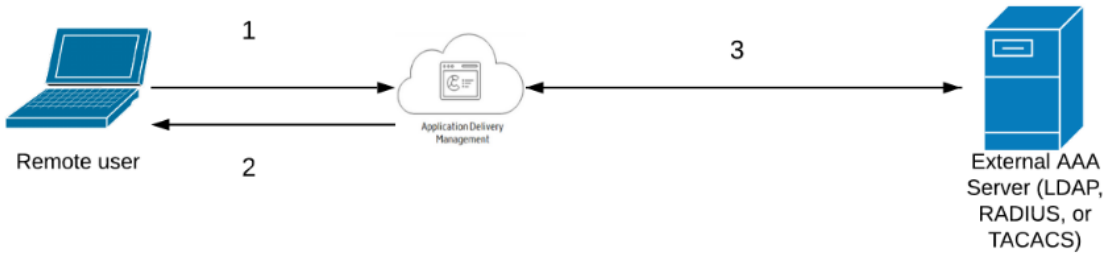
1 —ユーザーは NetScaler ADM にログオンします

2 —NetScaler ADM は、認証用の資格情報の入力をユーザーに求め、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 NetScaler ADM に接続します

2 —NetScaler ADM がユーザーに資格情報の入力を求めます

3 -NetScaler ADM は、外部認証、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。

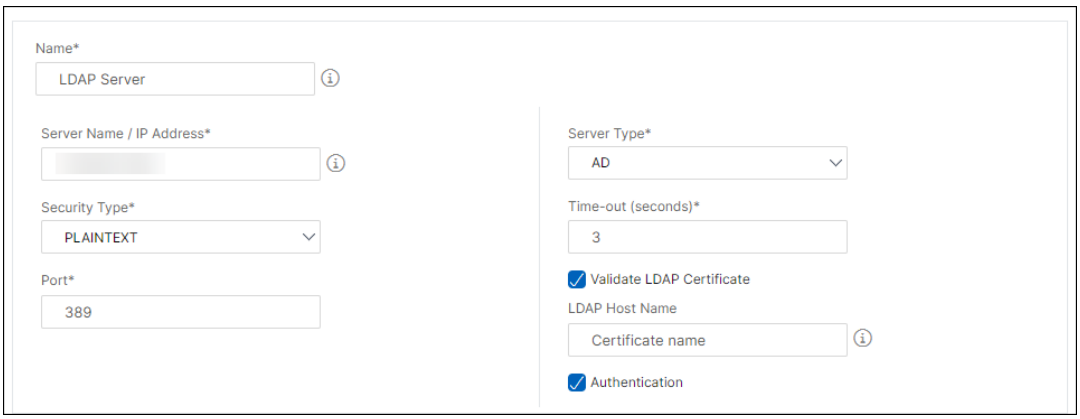
LDAP 認証サーバーの追加

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クレデンシャルを検索および認証できます。

1. [設定**] > [**認証**]** に移動します。
2. [**LDAP**] タブを選択し、[追加] をクリックします。
3.「**LDAP** サーバーの作成」ページで、次のパラメータを指定します。
    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**)** —NetScaler 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。



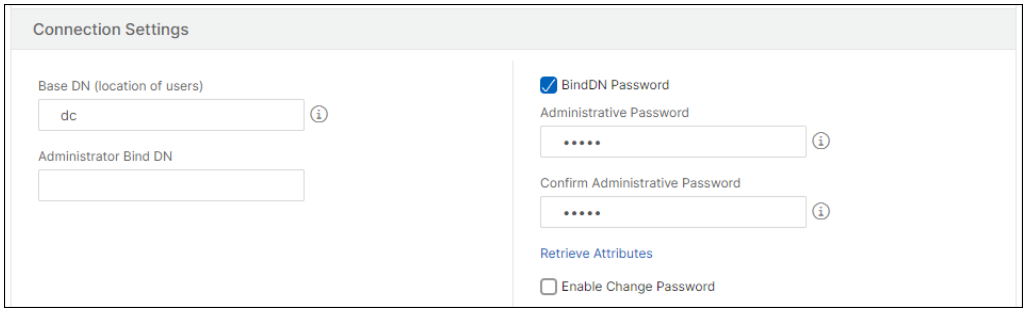
[接続設定] で、次のパラメータを指定します。

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。

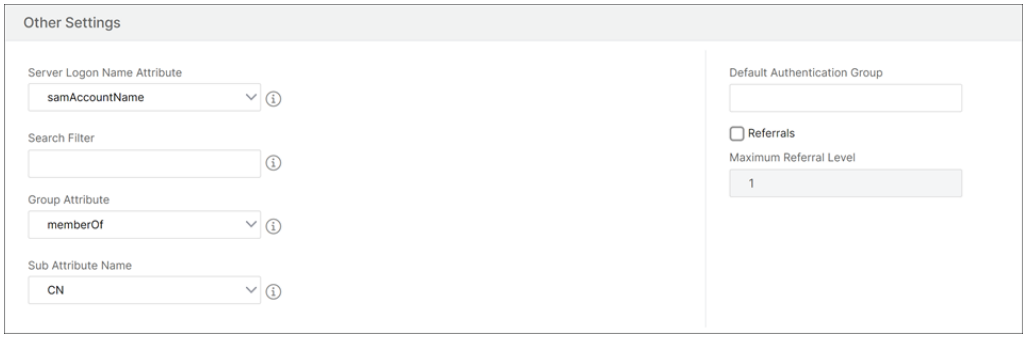
ii. 「検索フィルタ」—LDAP サーバーで構成された検索フィルタに従って、2 要素認証用に外部ユーザーを設定します。たとえば、ldaploginame `samaccount` を指定した vpnallowed=true、ユーザーが指定したユーザー名 bob を指定すると、LDAP 検索文字列が返されます: &(`vpnallowed=true`)(`samaccount=bob`)。

> 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。

   > 注記:
   >
   > 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。

5. 外部認証サーバーを有効にします。

   外部認証サーバーを有効にする方法の詳細については、「外部認証サーバーとフォールバックオプションを有効にする」を参照してください。

RADIUS 認証サーバーの追加

February 6, 2024

1. [設定] **>** [認証] に移動します。
2. [**RADIUS**] タブを選択し、[追加] をクリックします。

   「**RADIUS** サーバーの作成」ページで、次のパラメータを指定します。

   a) 名前—RADIUS サーバー名を指定します。

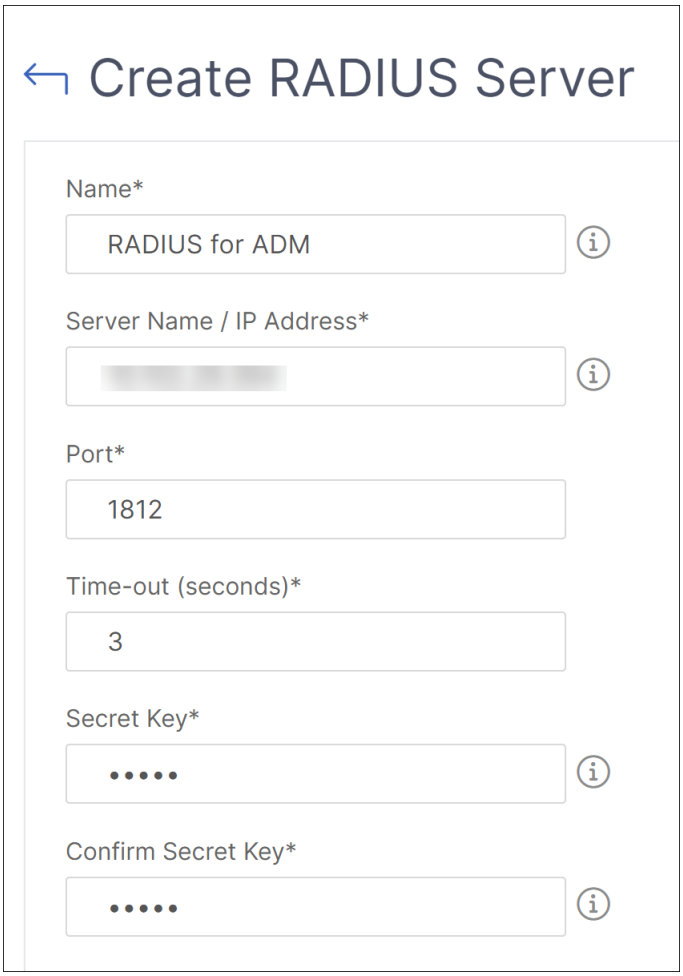
   b) サーバー名**/IP** アドレス—RADIUS サーバーの IP アドレスを指定します

   c) ポート—RADIUS サーバ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**)** —NetScaler 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



「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。

4. 外部認証サーバーを有効にします。

外部認証サーバーを有効にする方法の詳細については、「外部認証サーバーとフォールバックオプションを有効にする」を参照してください。

TACACS 認証サーバーの追加

February 6, 2024

1. [設定] **>** [認証] に移動します。
2. [**TACACS**] タブを選択し、[追加] をクリックします。
3. **TACACS** の作成ページで、次のパラメータを指定します。

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**)** —NetScaler ADM システムが LDAP サーバーからの応答を待つ時間 (秒単位)

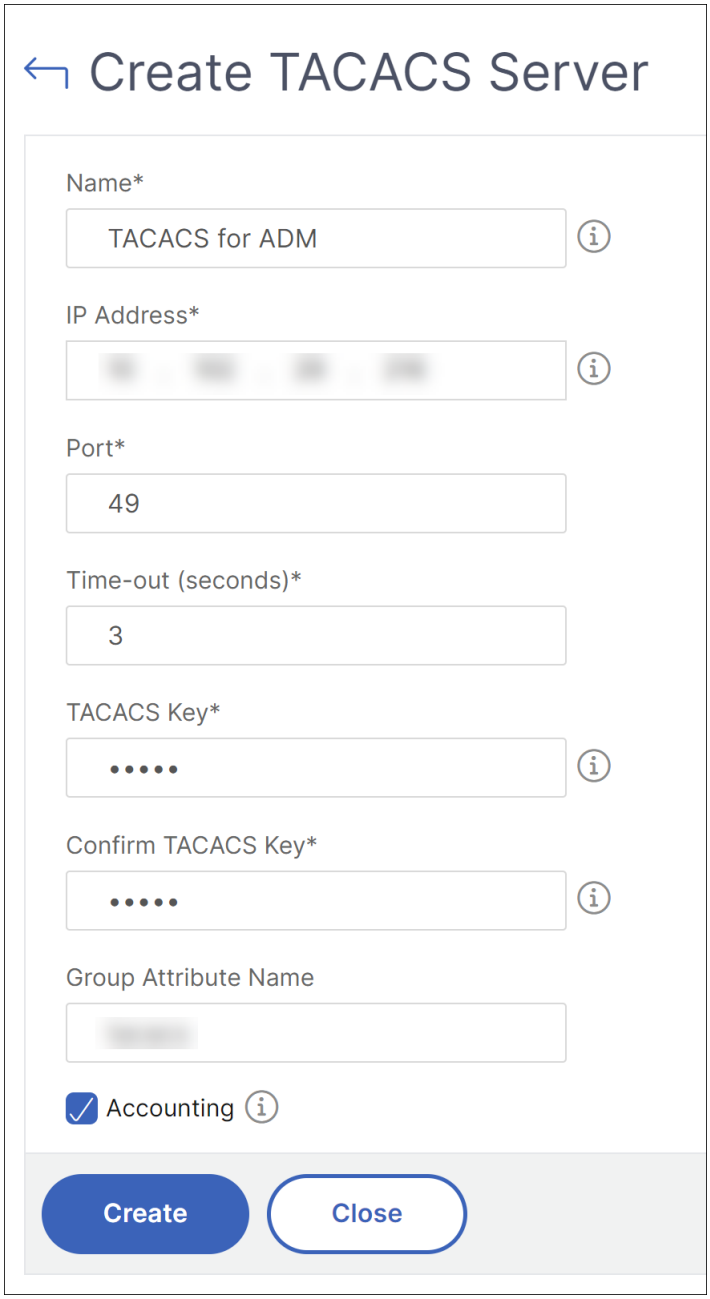
e) **TACACS** キー—認証用の TACACS キーを指定します

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、「アカウンティング」を選択します。

4. ［作成］をクリックします。



5. 外部認証サーバーを有効にします。

   外部認証サーバーを有効にする方法の詳細については、「外部認証サーバーとフォールバックオプションを有効にする」を参照してください。

NetScaler ADM 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、NetScaler 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。

NetScaler 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。

NetScaler 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、NetScaler ADM のグループを、内部ネットワークの認証サーバーで構成されているグループと一致するように構成します。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、NetScaler 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詳しくは、「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** サーバー抽出は **NetScaler**ADM 13.0 からサポートされています。

NetScaler 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。

外部認証サーバーとフォールバックオプションを有効にする

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。NetScaler 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たり接続できない場合でも、NetScaler 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場合や接続できない場合、NSroot 以外のユーザーは NetScaler ADM にアクセスできる必要があります
- 少なくとも 1 つの外部サーバーを追加する必要があります

NetScaler ADM は、ローカル認証に加えて、認証、承認、アカウンティング（AAA）プロトコル（LDAP、RADIUS、TACACS）の統合システムもサポートしています。この統合サポートにより、システムにアクセスするすべてのユーザと外部 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、NetScaler ADM に外部認証サーバーを追加する必要があります。サポートされている外部認証サーバー（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 サーバを設定するとします。NetScaler 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、NetScaler ADM は次のことを試みます。

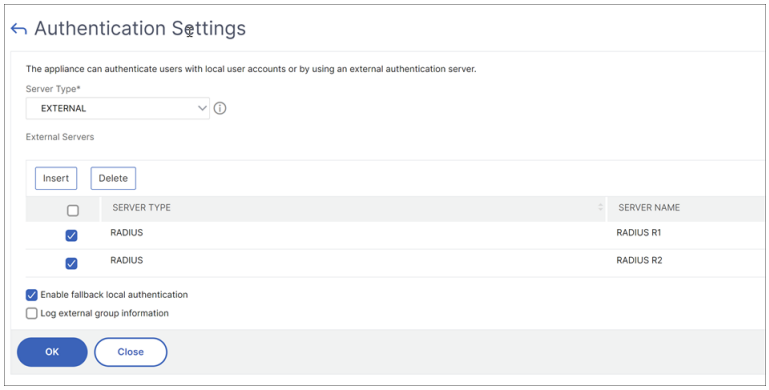
- 最初の RADIUS サーバに接続
- 1 台目の RADIUS サーバで認証に失敗した場合は、2 番目の RADIUS サーバに接続する
- 両方の RADIUS サーバで認証に失敗した場合は、LDAP サーバに接続する
- RADIUS サーバと LDAP サーバの両方で認証に失敗した場合は、TACACS サーバに接続します。

> 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. [設定] **>** [認証] に移動します。
2. [認証] ページで、[設定] をクリックします。
3. 「認証設定」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。



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、NetScaler ADM は RADIUS、LDAP、および TACACS プロトコルによる外部認証をサポートしています。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と、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 NetScaler ADM 上のユーザーが識別されます。

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。NetScaler ADM では、管理者が企業内の個々のユーザーの役割に基づいてユーザーにアクセス権限を与えることができる、きめ細かな役割ベースのアクセス制御（RBAC）が可能です。NetScaler 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

NetScaler 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ることもできます。

グループとは、共通の権限を持つユーザーの集まりです。たとえば、特定のデータセンターを管理している複数のユーザーを 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。

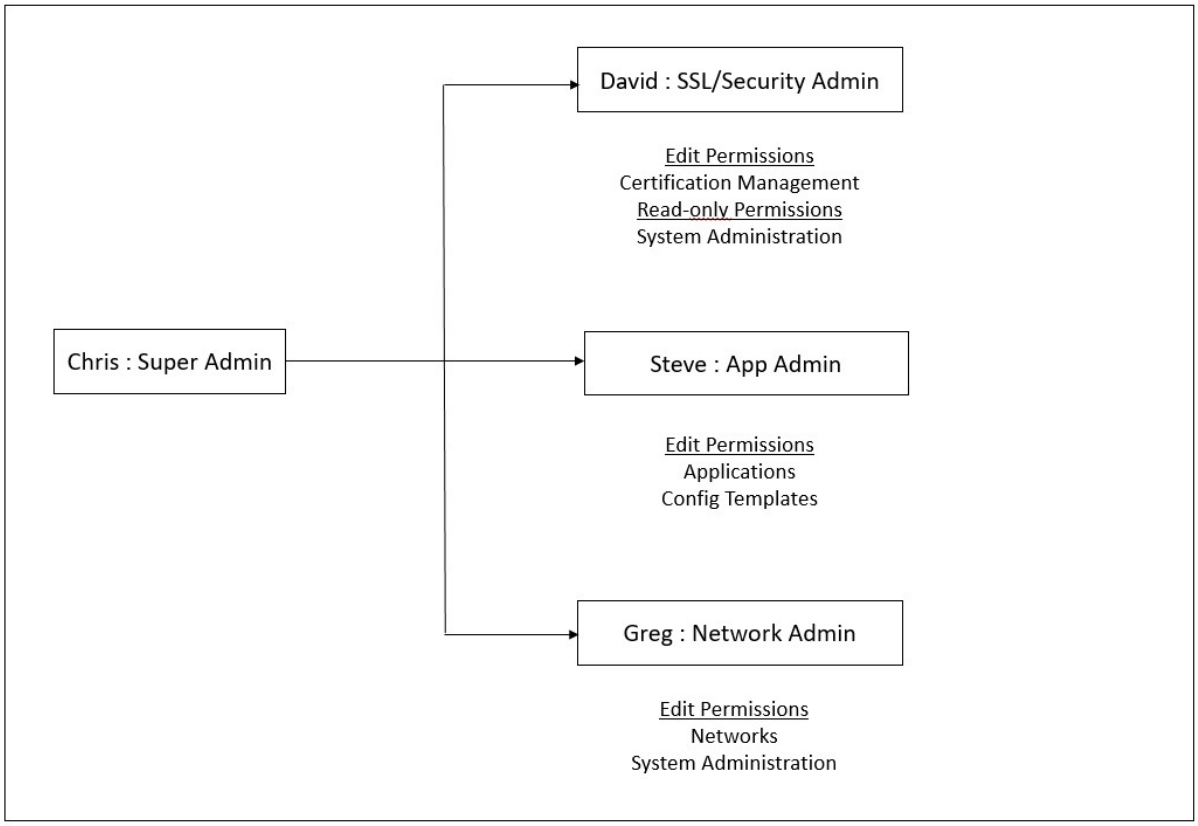
アプリケーション管理者のスティーブは、特定のアプリケーションと特定の構成テンプレートのみのアクセスが必要です。

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、次の NetScaler ADM 機能で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制限されており、Web Insight、SSL Insight、Gateway Insight、HDX Insight、WAF セキュリティ違反の各分析モジュールでは、アプリケーションレベルでは適用されません。次に例を示します:

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、StyleBook とコンフィグパックは個別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、個別に、または同時に提供できます。構成パックの表示または編集権限により、ユーザーは StyleBooks を閲覧することが暗黙的に許可されます。これは、構成パックの詳細を取得して構成パックを作成するために不可欠です。
  - 特定の StyleBook または構成パックへのアクセス権限はサポート
    されていません。例：インスタンスに構成パックが既に存在する場合、ユーザーは、そのインスタンスにアクセスできなくても、ターゲット NetScaler 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。NetScaler Application Delivery Management （ADM）には、4 つの定義済みアクセスポリシーが用意されています。

1. 管理ポリシー。NetScaler 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 NetScaler 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. NetScaler ADM で、[設定**] > [**ユーザーと役割**] > [**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。

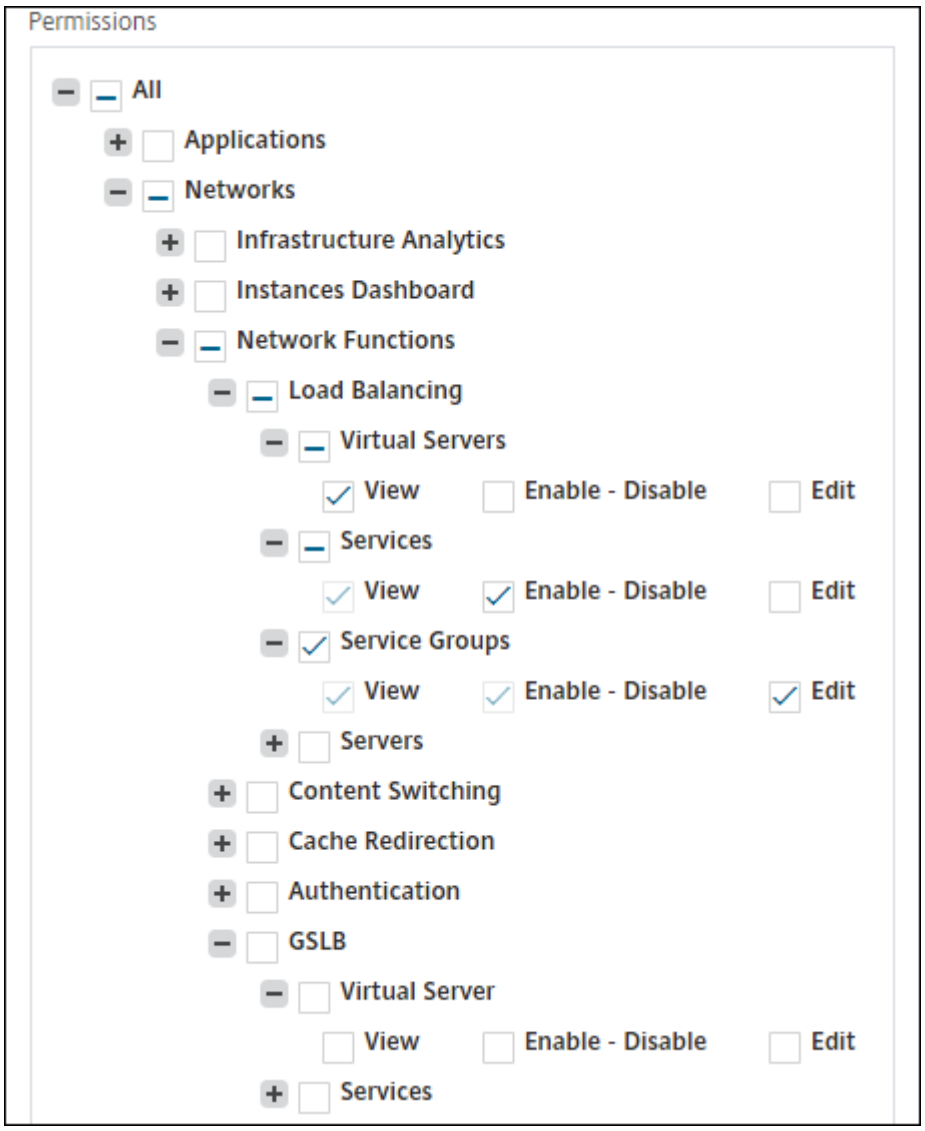
     ユーザーに「有効/無効化」権限を付与すると、「表示」権限も付与されます。このオプションの選択を解除することはできません。
   - 編集**:** このオプションはユーザーにフルアクセスを許可します。ユーザーは機能とその機能を変更できます。

     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**:**
>
> その他の設定オプションを表示するには、負荷分散と GSLB を展開してください。

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：



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、[インフラストラクチャ**] > [**ネットワーク機能**] > [**負荷分散] に移動し、[仮想サーバー] タブを選択します。

サービス 機能の 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、[インフラストラクチャ**] > [**ネットワーク機能**] > [**負荷分散] に移動し、[サービス] タブを選択します。

> 注**:**
>
> ユーザーに有効化/無効化権限がある場合、サービスの有効化または無効化操作は次のページで制限されます。
>
> a) [インフラストラクチャー**] > [**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、**[** インフラストラクチャ] > [**ネットワーク機能**] > [**負荷分散] に移動し、[サービスグループ] タブを選択します。

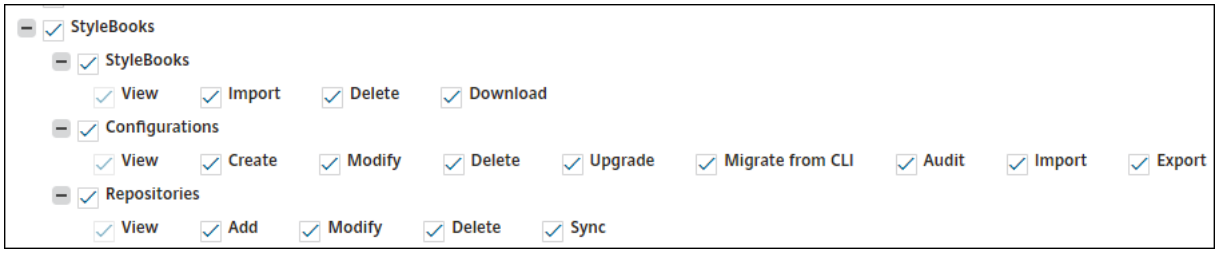
5. ［作成］をクリックします。

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、表示権限が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 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（)、NetScaler Gateway（VPNAuth）
- 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、[設定**] > [**ユーザーとロール**] > [**グループ] に移動します。
2. [追加］をクリックします。

   「システムグループの作成」ページが表示されます。
3. [グループ名] フィールドに、グループの名前を入力します。最大許容長は 64 文字です。
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。

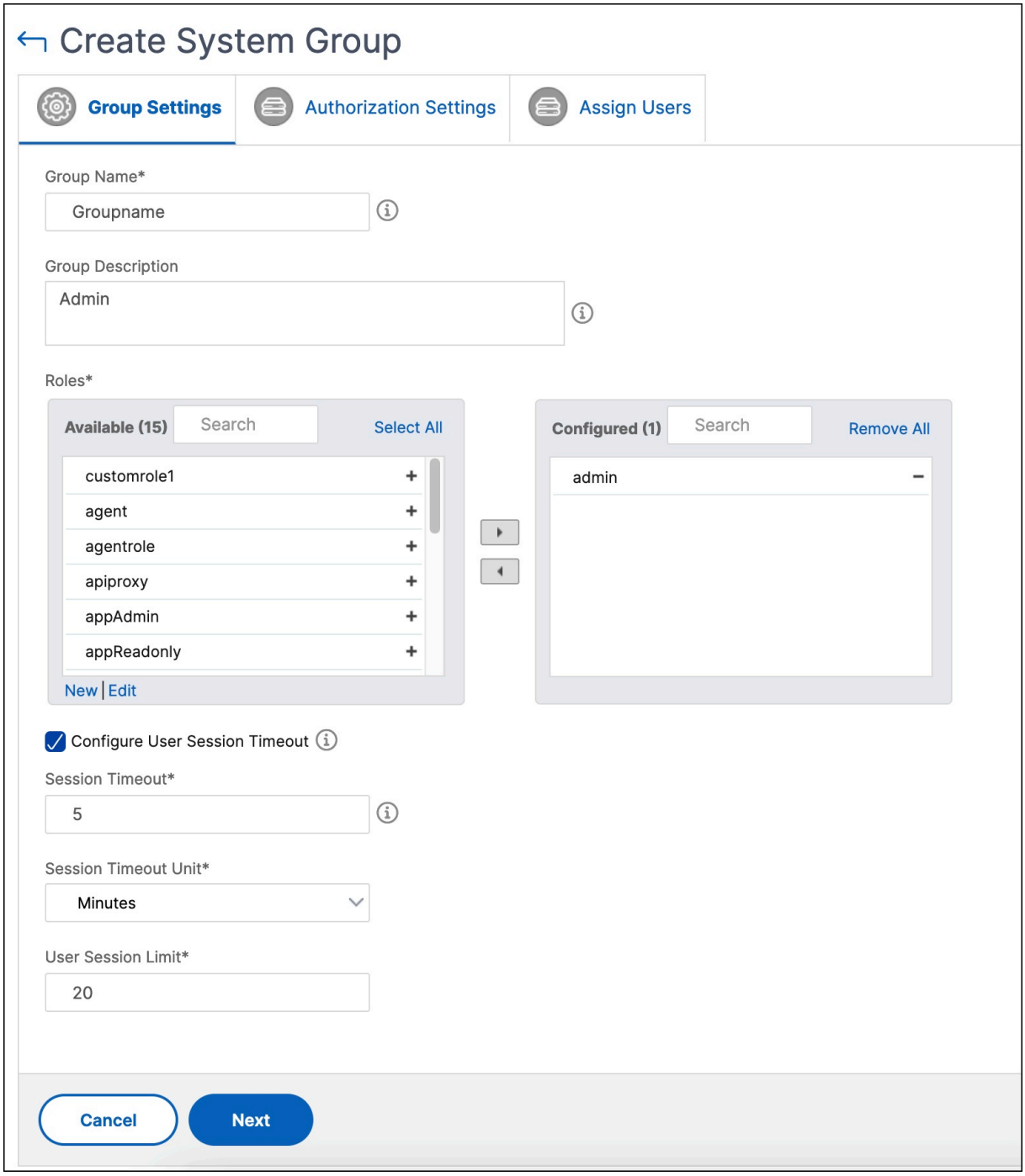
   > 注:
   >
   > 「使用可能」リストで、「新規」または「編集」をクリックしてロールを作成または変更できます。または、[設定**] > [**ユーザーとロール**] > [**ユーザー**]** に移動して、ユーザーを作成または変更することもできます。

6. ユーザーがアクティブな状態を維持する期間を設定するには、「ユーザーセッションタイムアウトの設定」を選択します。

   有効になっている場合は、次のパラメータを指定します:

   - セッションタイムアウト: ユーザーセッションをアクティブに保つ必要がある時間を入力します。デフォルト値は 15 です。
   - セッションタイムアウト単位: 一覧からタイムアウト単位を分単位または時間単位で選択します。デフォルト値は分です。
7.「ユーザーセッション制限」フィールドに、ユーザーごとに許可される最大セッション数を入力します。

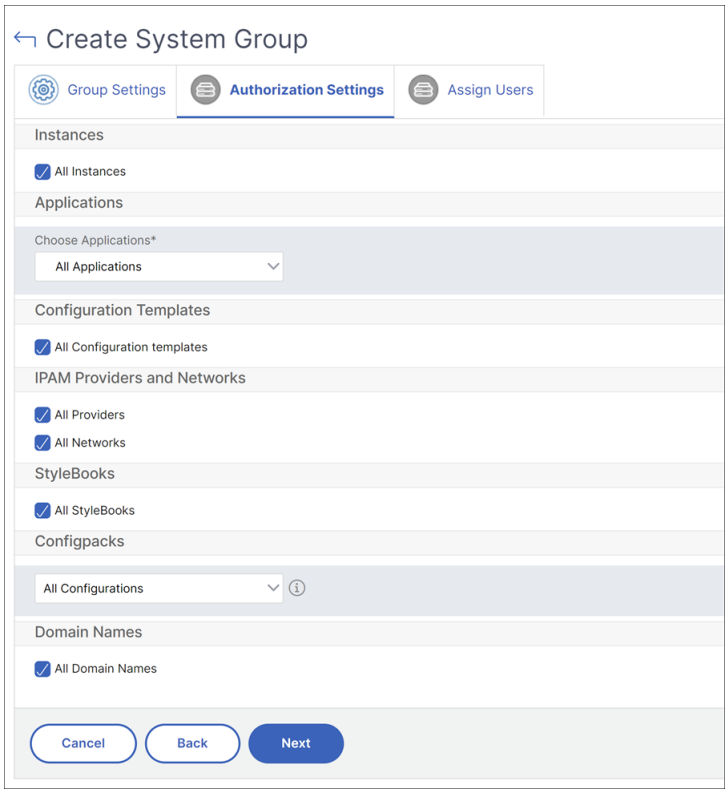
> 注**:**
>
> 最大 40 のユーザーセッションを設定できます。デフォルトでは、20 のユーザーセッションが割り当てられます。ただし、管理者および読み取り専用ユーザーグループに属している場合、デフォルトで 40 ユーザーセッションが割り当てられ、この値は変更できません。



1. ［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



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** グループの追加] をクリックします。

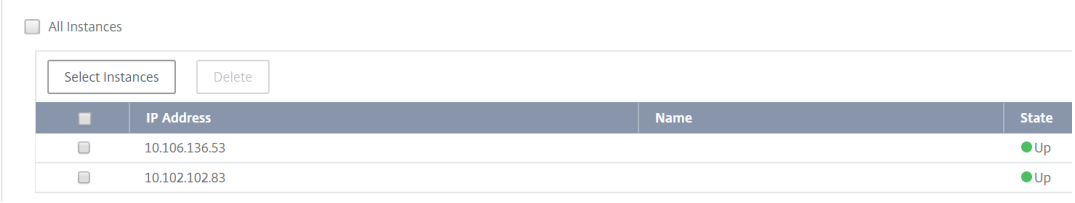
b) リストから必要な Autoscale グループを選択し、「**OK**」をクリックします。

インスタンス**:**

ユーザーが表示または管理できる特定のインスタンスを選択するには、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。



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。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。

次のオプションを使用できます。

- 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、NetScaler ADM は選択したアプリケーションにバインドされているすべてのエンティティを承認します。

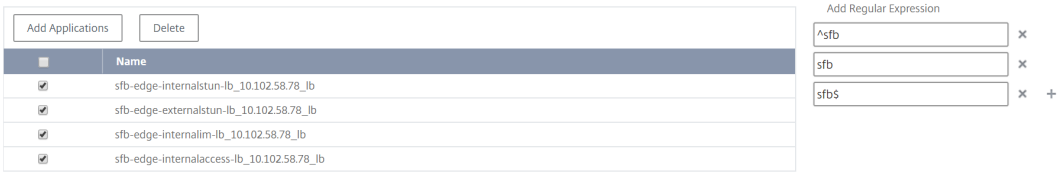
  > 注**:**
  >
  > バインドされたエンティティを承認するには、エンティティタイプを 1 つだけ選択します。

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:

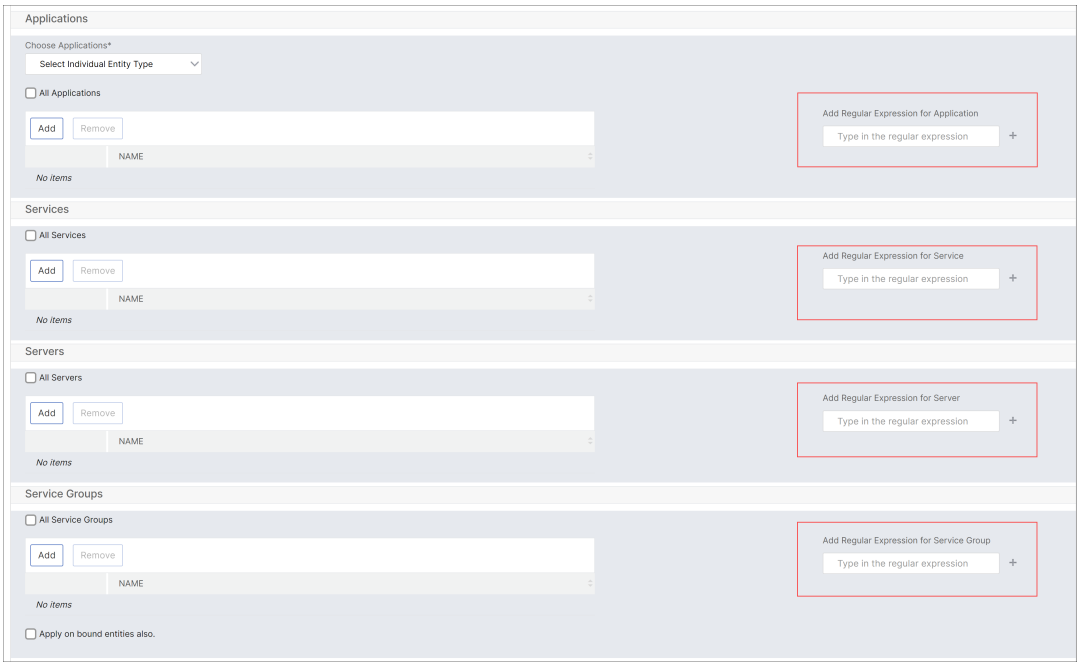
a)「正規表現を追加」をクリックします。

b) テキストボックスに正規表現を指定します。

以下の画像は、「Specific Applications」オプションを選択したときに、正規表現を使用してアプリケーションを追加する方法を示しています:



次の図は、[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 **Servers** エンティティタイプのサーバー名にのみ一致し、サーバー IP アドレスとは一致しません。

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、[構成テンプレートの追加] 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、「StyleBook をグループに追加 **」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。クエリーは、`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:

```
name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
    version=1.0
<!--NeedCopy-->
```

このクエリは、次の条件を満たす StyleBook をリストします。

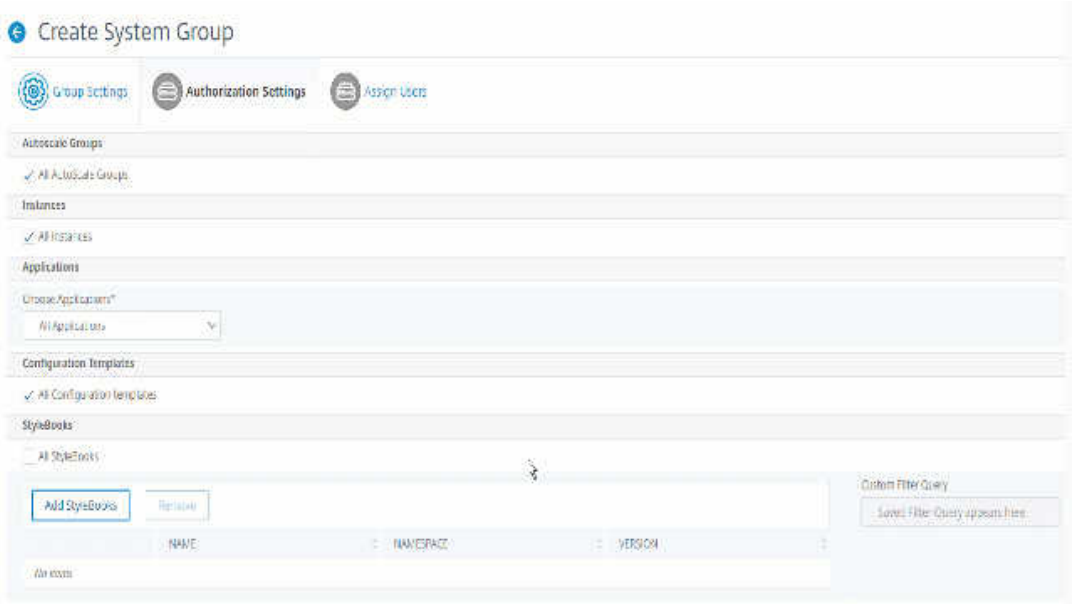
- StyleBook 名は`lb-mon`または`lb`のいずれかです。
- StyleBook の名前空間は`com.citrix.adc.stylebooks`です。
- StyleBook 版は `1.0`です。

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ー] 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。

構成パック**:**

設定パックで、次のオプションのいずれかを選択します。

- すべての構成: このオプションはデフォルトで選択されています。これにより、ユーザーは ADM にあるすべての構成を管理できます。
- 選択した StyleBook のすべての構成: このオプションは、選択した StyleBook のすべての構成パックを追加します。
- 特定の構成：このオプションでは、任意の StyleBook の特定の構成を追加できます。
- ユーザーグループによって作成されたすべての構成: このオプションにより、ユーザーは同じグループのユーザーによって作成された構成のみにアクセスできます。

  グループを作成してユーザーをそのグループに割り当てるときに、適切な構成パックを選択できます。

ドメイン名**:**

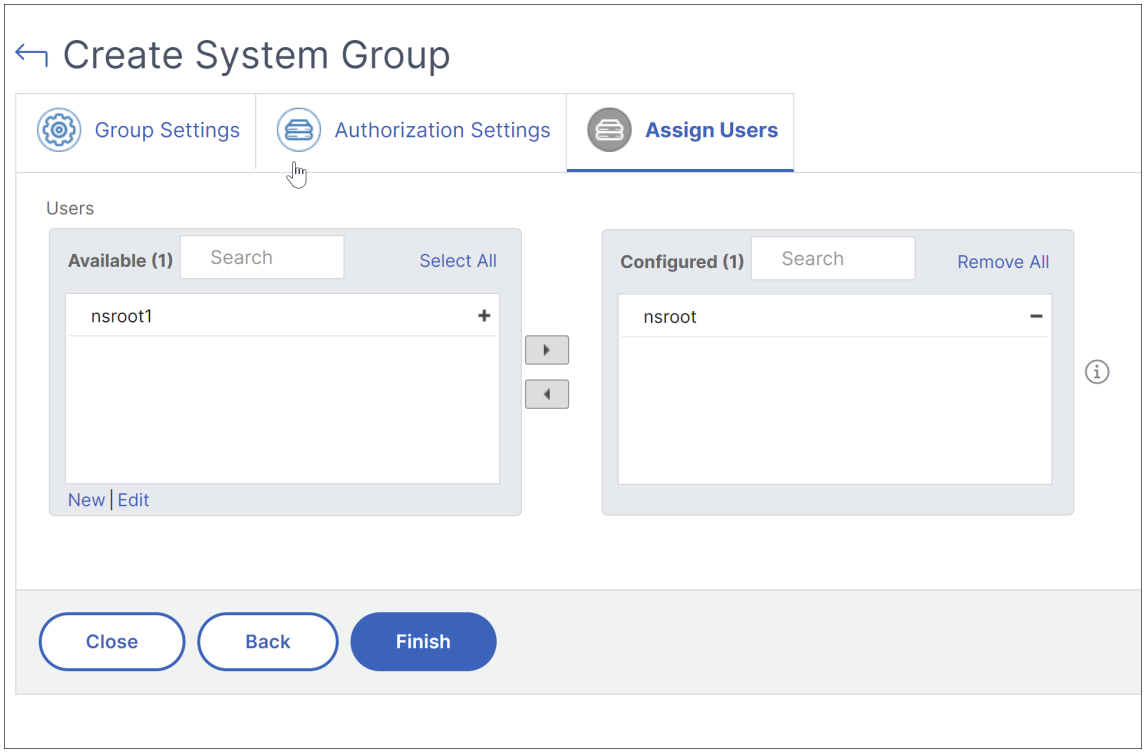
ユーザーが表示または管理できる特定のドメイン名を選択するには、次の手順を実行します。

a) [すべてのドメイン名] チェックボックスをオフにし、[ドメイン名の追加] をクリックします。

b) リストから必要なドメイン名を選択し、**OK** をクリックします。

2. [**Create Group**] をクリックします。
3. 「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。



4. [完了] をクリックします。

複数のネットワーク機能エンティティにわたるユーザーアクセスを管理

管理者は、NetScaler ADM のネットワーク機能エンティティの個々のレベルでユーザーアクセスを管理できます。また、正規表現フィルターを使用して、エンティティレベルで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:
>
> NetScaler ADM は、仮想サーバー、サービス、サービスグループ、およびサーバーをネットワーク機能エンティティとして扱います。エンティティタイプ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。

> 注意**:**
>
> 「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、NetScaler ADM は App-1 にバインドされているすべてのネットワーク機能エンティティへのアクセスを許可します。その結果、ホスティングサーバーへのアクセスも許可されます。

スーパー管理者は、エンティティタイプごとに正規表現 (regex) を指定できます。正規表現は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エンティティタイプの正規表現と一致すると、NetScaler ADM はユーザーに特定のネットワーク機能エンティティへのアクセスを動的に許可できます。

ユーザー権限を動的に付与するために、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。

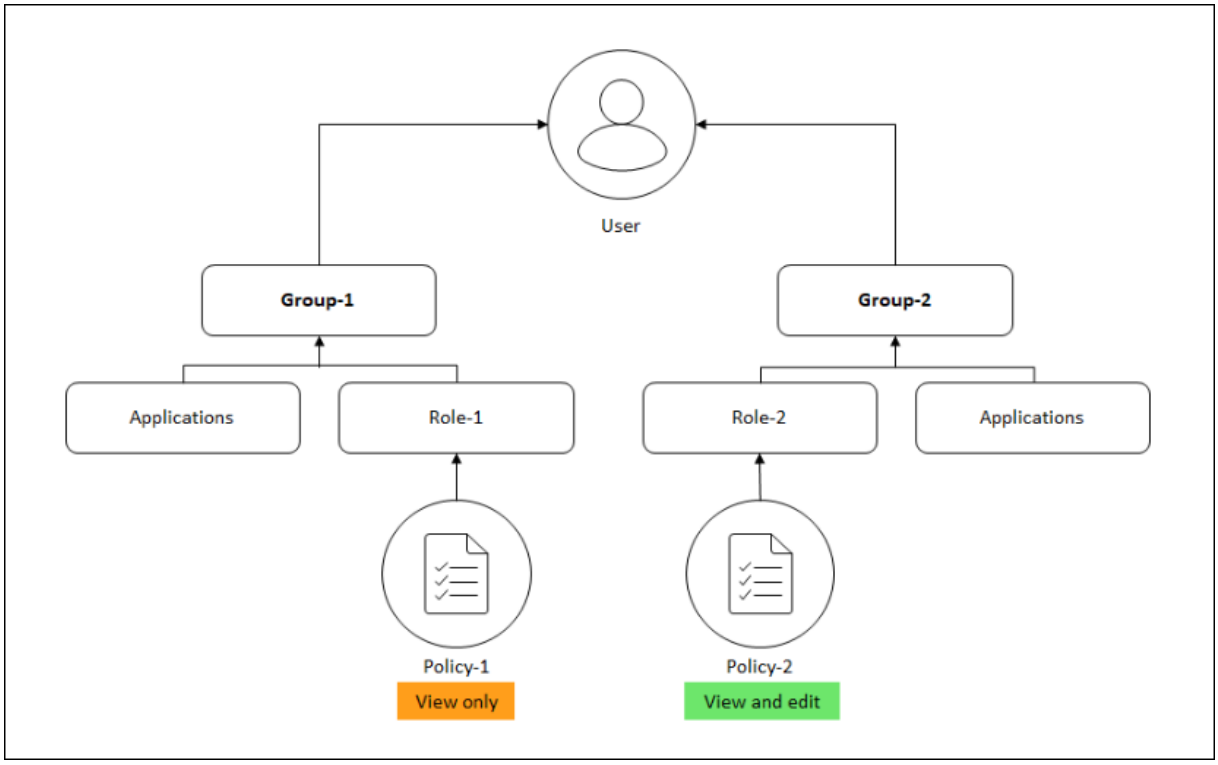
承認スコープに基づくユーザーアクセスの変更方法

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

NetScaler ADM を 12.0 から 13.1 にアップグレードすると、グループの作成時に「読み取り/書き込み」または「読み取り」権限を付与するオプションは表示されません。これらの権限は「ロールとアクセスポリシー」に置き換えら

れました。これにより、ロールベースの権限をより柔軟にユーザーに提供できます。次の表に、リリース 12.0 の権限がリリース 13.1 にどのようにマッピングされるかを示します。

12.0	アプリケーションのみ許可	13.1
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

NetScaler 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。1 つのポリシーでは NetScaler ADM に NetScaler インスタンスを追加する権限を付与し、別のポリシーでは StyleBook を作成および展開し、NetScaler インスタンスを構成する権限を付与する場合があります。

複数のポリシーで 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。

NetScaler ADM には、次の 4 つの定義済みロールが用意されています。

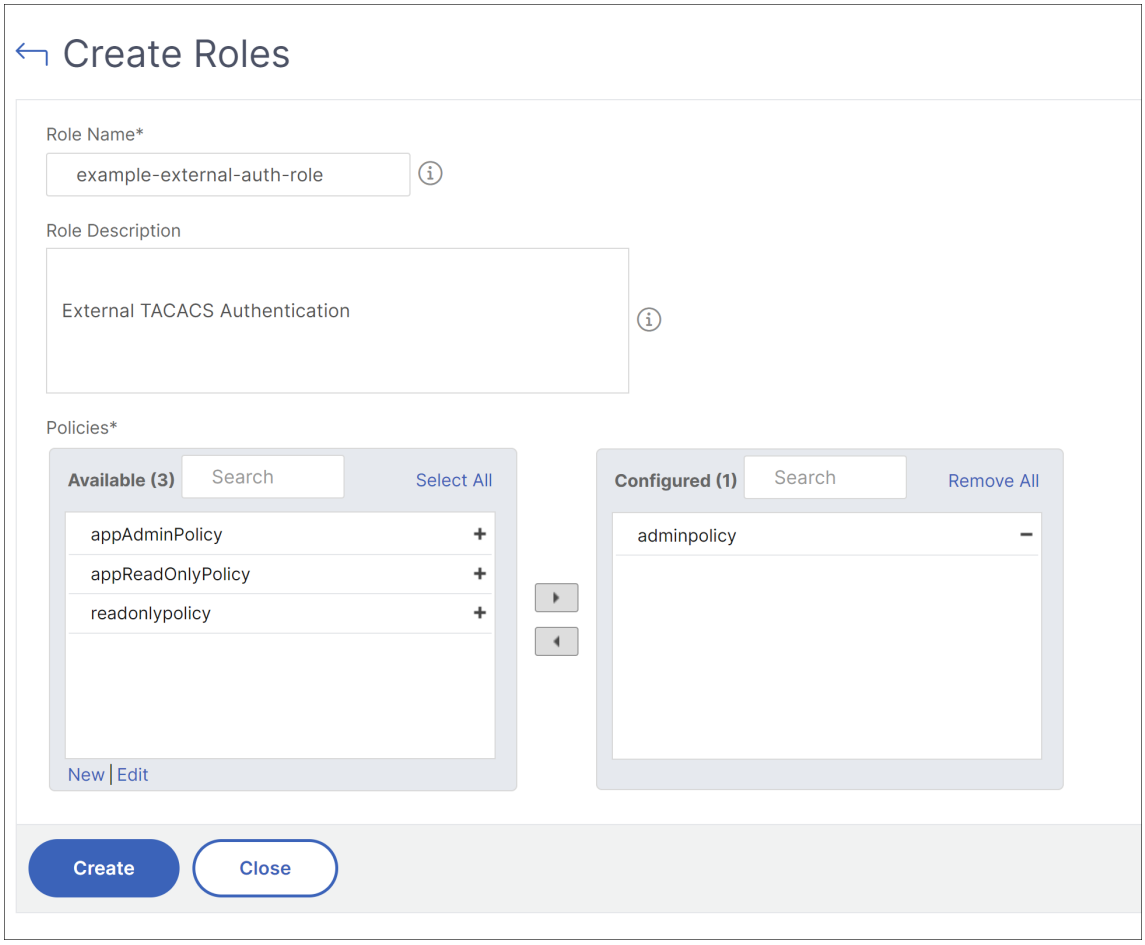
- 管理者。すべての NetScaler ADM 機能にアクセスできます。（この役割は adminpolicy にバインドされています）。
- 読み取り専用。読み取り専用アクセスが設定されています（この役割は readonlypolicy にバインドされています）。
- **appAdmin**。NetScaler ADM アプリケーション機能にのみ管理者権限が付与されます。（この役割は appAdminPolicy にバインドされています）。
- **appReadonly**。アプリケーション機能に対する読み取り専用アクセス権が設定されています（この役割は appReadOnlyPolicy 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. NetScaler ADM で、[設定] **>** [ユーザーとロール] に移動します。
2. ［追加］をクリックします。
3. 「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。



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、NetScaler Application Delivery Management （ADM）には 1 人のユーザーがいます。

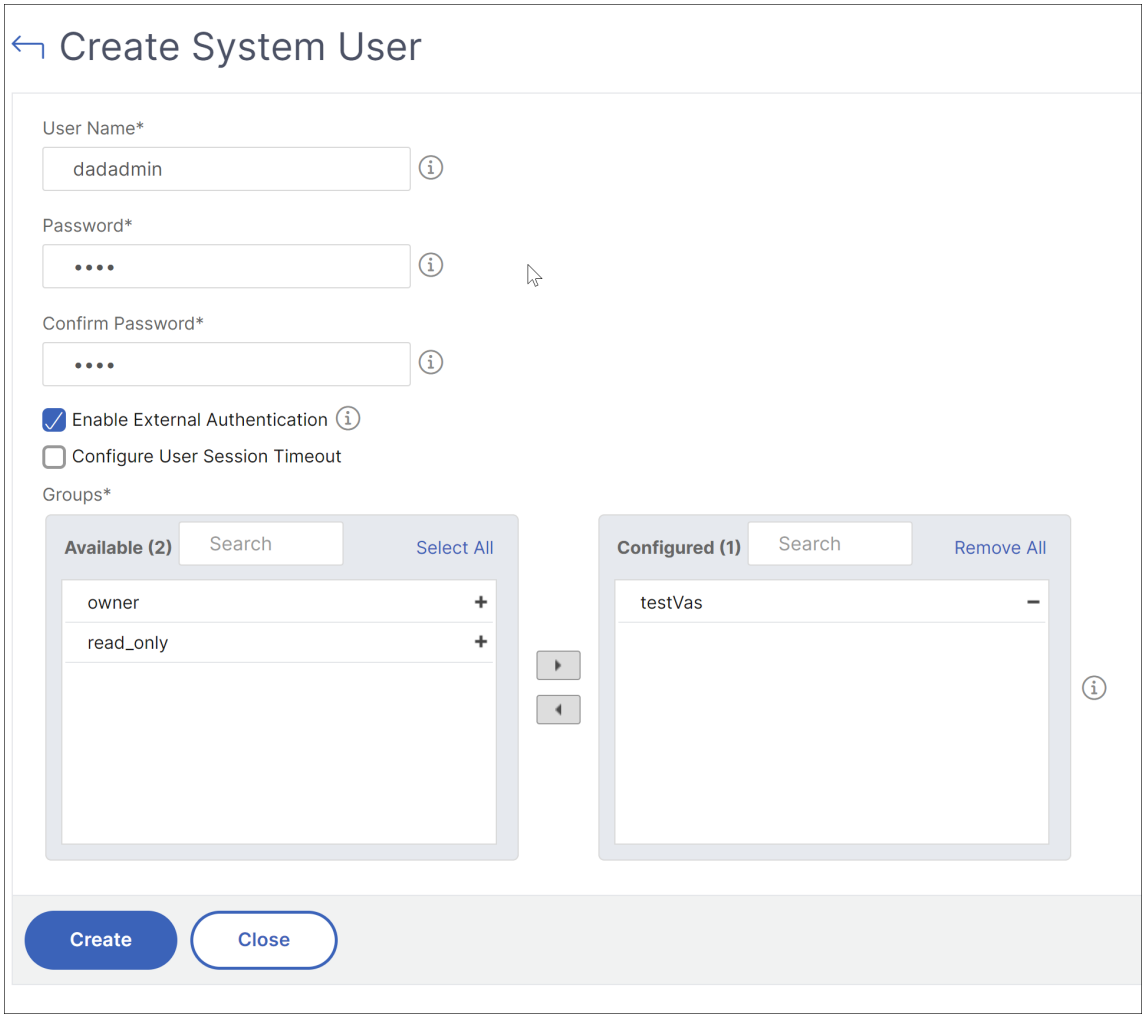
nsroot - ルートユーザー（nsroot）は、アプライアンスに対するすべての管理権限を持ちます。nsroot ユーザーは NetScaler ADM のスーパー管理者です。

ユーザーは、アカウントを構成することで追加できます。NetScaler ADM に新しいユーザーを追加するときに、適切なグループ、ロール、およびポリシーを割り当てること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、[設定**] > [**ユーザーとロール**]** に移動します。
2. ［追加］をクリックします。
3. 次の詳細情報を入力します：
    a) ユーザー名。ユーザーの名前
    b) パスワード。ユーザーが NetScaler 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。



6. [作成] をクリックします。

実行可能なタスクと推奨事項

February 6, 2024

> 注:
>
> - 「**To Do**」タブの名前が「推奨事項」に変更されました。レコメンデーションでは、引き続き既存のタスクを確認し、「ガイドする」をクリックしてタスクを完了できます。
> - [アーカイブ] タブは使用できなくなりました。代わりに、リストからレコメンデーションを却下することもできます。

何百もの NetScaler インスタンスが検出され、各インスタンスから複数の仮想サーバー（アプリケーション）を構成

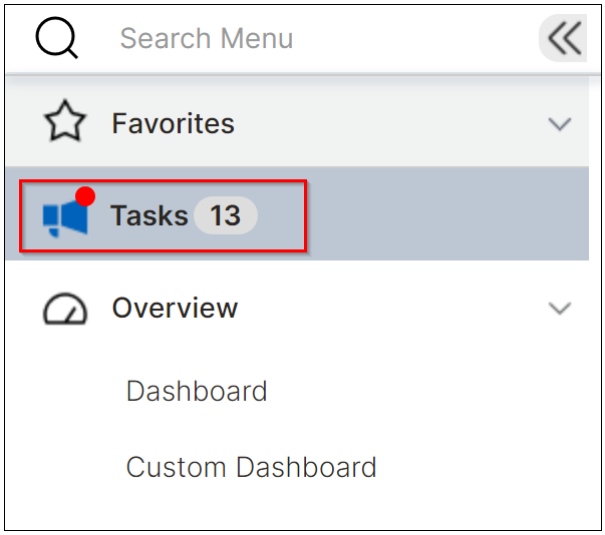
している場合があります。管理者は、すべての NetScaler インスタンスとアプリケーションを効率的に管理して、優先順位付けとトラブルシューティングに役立つ情報を得る必要があります。

インフラストラクチャをさらにスケールアップするにつれて、インスタンスやアプリケーションに影響を与える重大な問題に早急に対処する必要が生じる場合もあります。また、NetScaler ADM の導入が効率的で安全で、コンプライアンスに準拠していることを確認する必要があります。NetScaler **ADM** のタスク機能では、現在の使用状況とサブスクリプションに基づいて、すぐに実行する必要のある実行可能なタスクと、効率的な展開を実現するための推奨事項の両方を表示できます。

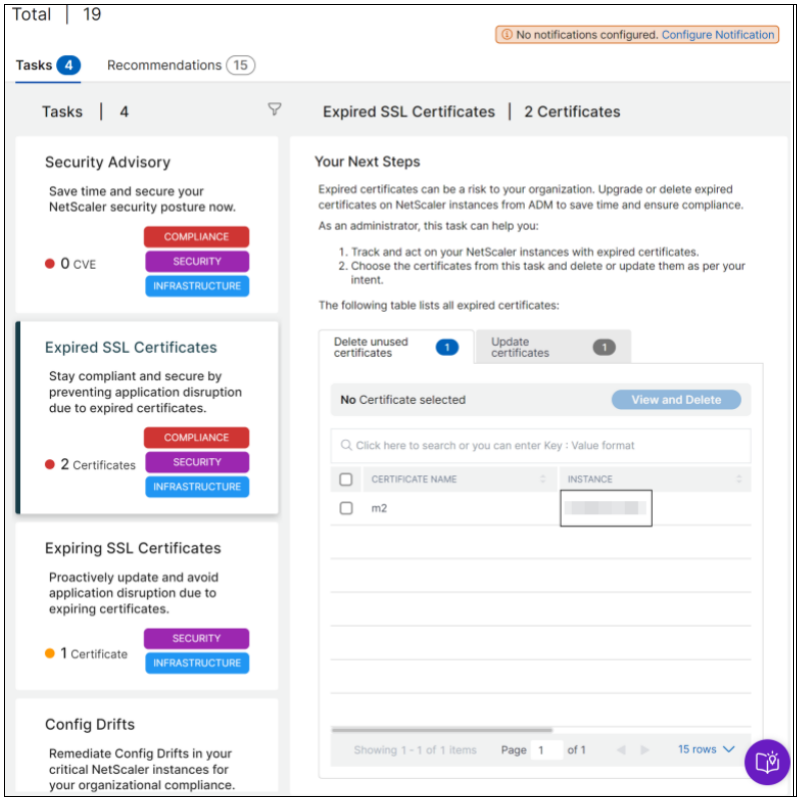
管理者は、** これらの実行可能なタスクと推奨事項を利用することで **、次のことが可能になります。

- 早急な対応が必要な観察結果や問題を、瞬時に把握できます。
- NetScaler ADM がタスクを検出し、事前にアクションを実行したときに通知を受け取るように通知を構成します。
- NetScaler ADM インスタンスと NetScaler インスタンスの効率的な導入を実現します。
- 重大な問題を特定するための重要な時間と労力を削減します。
- NetScaler ADM のすべての機能を活用していることを確認し、製品の検出と製品が推奨する機能を有効にして、展開を効率的に管理できるようにします。

NetScaler ADM GUI で［タスク］をクリックすると、［タスク］と［推奨事項］の両方が表示されます。

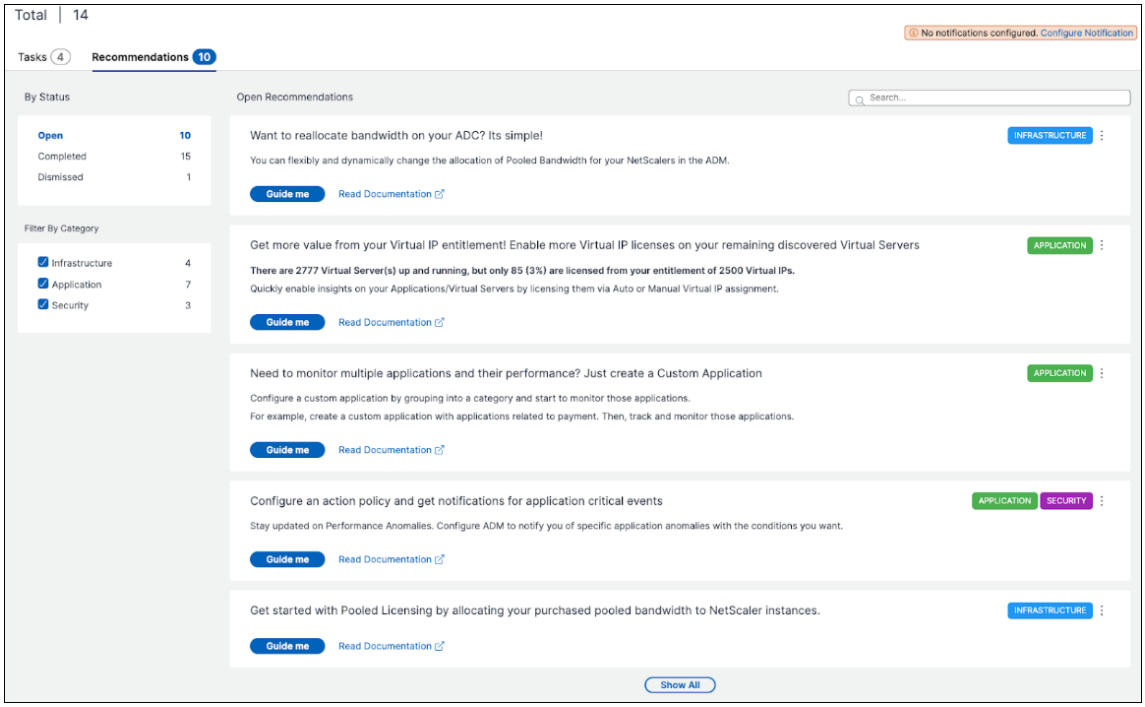


- タスク -早急な対応とアクションが必要なタスクのリストを表示できます。インフラストラクチャをスケールアップするにつれて、いくつかの重大な問題が見過ごされ、セキュリティ侵害につながる可能性があります。たとえば、CVE を使用する NetScaler インスタンスには早急に対応する必要があり、インスタンスが推奨ビルドとバージョンで実行されていることを確認するには、すぐに行動を起こす必要があります。タスクでは、それらのインサイトをすぐに得ることができます。現在の使用状況に基づいて、合計 4 つのタスクを表示できます。タスクは重要度 (クリティカルおよびミディアム) に基づいて表示されます。



- 推奨事項 -NetScaler ADM の導入環境を改善するために、現在の使用状況に基づいて特定の推奨事項を提示します。「**Guide Me** 」オプションを使用して、おすすめ情報を入力できます。「**Guide Me** 」オプションを使用して入力したレコメンデーションはすべて「完了」に移動されます。また、どのレコメンデーションも却下でき、そのレコメンデーションは「却下」カテゴリに移動されます。却下されたレコメンデーションを表示するには、「ステータス別」フィルターを使用し、「却下」を選択すると、却下されたレコメンデーションが表示されます。

  また、「カテゴリ別フィルター」を使用して、カテゴリ (インフラストラクチャ、アプリケーション、セキュリティ) に基づいて特定のレコメンデーションをフィルタリングすることもできます。または、検索バーを使用して最初の数文字を入力してタスクにドリルダウンすることもできます。



タスク

[タスク] には、現在の ADM 展開に応じて、次の 4 つのタスクが表示されます。

- 期限切れの **SSL** 証明書—NetScaler ADM にインストールされている期限切れの SSL 証明書に関する情報を提供します。このタスクを選択すると、次のタブが表示されます:
  - 未使用の証明書を削除: どの NetScaler インスタンスでも使用されていない証明書を表示します。タスクを完了するには、未使用の証明書を確認し、証明書を選択して [表示して削除] をクリックします。

    推奨処置:[インフラストラクチャ**] > [SSL** ダッシュボード**] > [SSL** 証明書**-**期限切れ] にリダイレクトされます。証明書を削除するには、[削除] をクリックします。証明書を更新する場合は、証明書を選択して [更新] をクリックします。詳細については、「インストールされた証明書を更新する方法」を参照してください。
  - 証明書の更新: すでに有効期限が切れている証明書を表示します。タスクを完了するには、証明書を確認し、証明書を選択して、[表示と更新] をクリックします。

    推奨処置:[インフラストラクチャ**] > [SSL** ダッシュボード**] > [SSL** 証明書**-**期限切れ] にリダイレクトされます。証明書を選択し、[更新] または [削除] をクリックします。詳細については、「インストールされた証明書を更新する方法」を参照してください。
- 期限切れ間近の **SSL** 証明書—期限切れ間近の SSL 証明書に関する情報を提供します。

  推奨処置**:** このタスクを選択すると、有効期限までの合計日数に基づいてタブが表示されます。タスクを完了するには、タブから証明書を選択し、「表示して更新」をクリックします。インフラストラクチャ **> SSL** ダッ

シュボードの関連ページにリダイレクトされます。証明書を選択し、「更新」をクリックします。詳細については、「インストールされた証明書を更新する方法」を参照してください。

- 構成ドリフト—**NetScaler** インスタンスの構成偏差（保存された差分と実行中の差分、テンプレートと実行中の差分）に関する情報を提供します。このタスクを選択すると、次のタブが表示されます：
  - 構成が保存されていないインスタンス**:** 構成が保存されていないインスタンスを表示できます。タスクを完了するには、インスタンスを選択し、[設定を表示して保存] をクリックします。

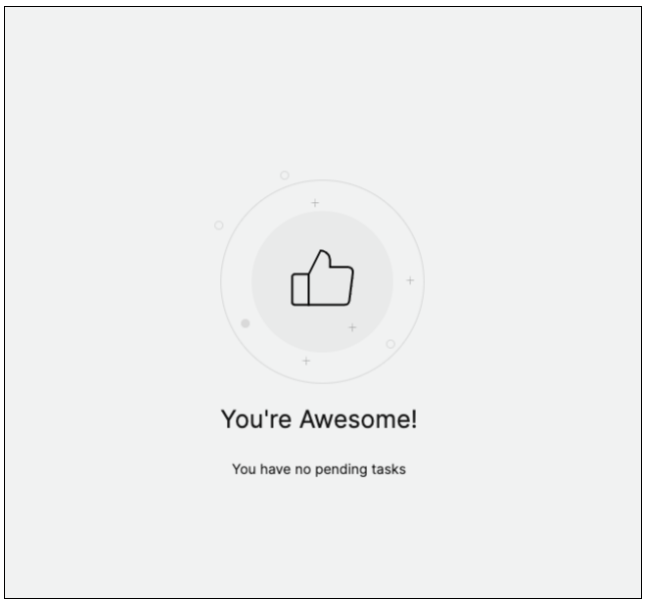
    推奨処置:[インフラストラクチャ**] > [**構成**] > [**構成監査**] > [**監査レポート] にリダイレクトされ、構成が保存されていないインスタンスを表示できます。[設定を保存] をクリックしてこのタスクを完了します。詳細については、ドキュメントを参照してください。
  - テンプレートからドリフトがあるインスタンス**:** テンプレートから逸脱しているインスタンスを表示できます。タスクを完了するには、インスタンスを選択し、[正しいコマンドを表示して実行] をクリックします。

    推奨処置:[インフラストラクチャ**] > [**構成**] > [**構成監査**] > [**監査レポート] にリダイレクトされ、テンプレートから逸脱しているインスタンスを表示できます。ドキュメントに従ってタスクを完了してください 。
- セキュリティアドバイザリ—NetScaler インスタンスに影響を与えている CVE に関する情報を提供します。このタスクを選択すると、次のタブが表示されます：
  - 検出された **CVE**：検出された CVE と、CVE に影響を与えている NetScaler インスタンスが表示されます。このタスクを完了するには、CVE を選択し、「表示して修正」をクリックします。

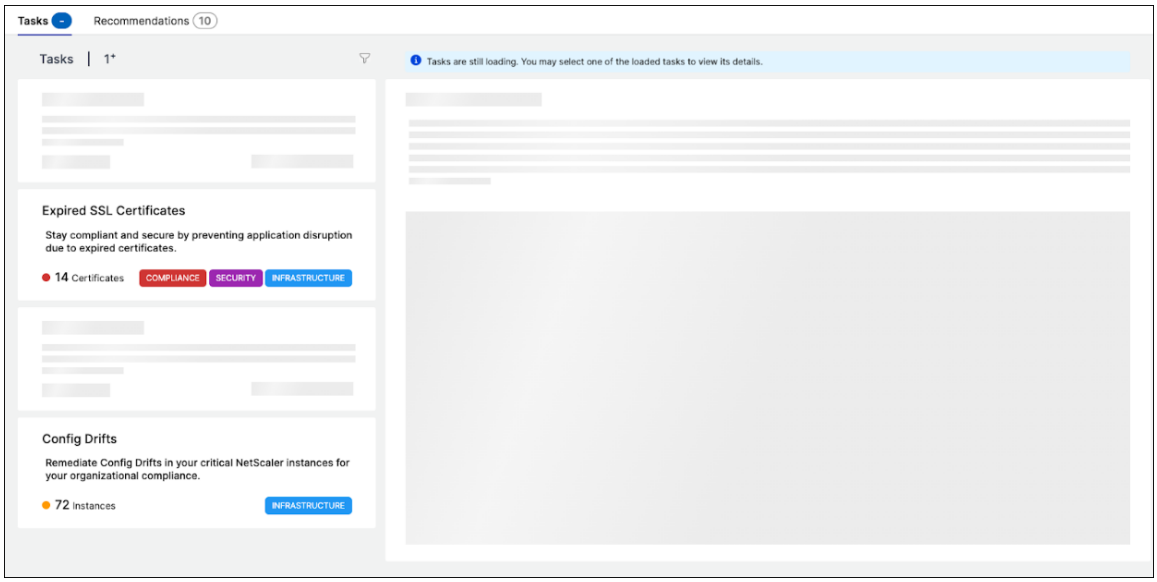
    推奨処置: インフラストラクチャ **>** インスタンスアドバイザリ **>** セキュリティアドバイザリのセキュリティアドバイザリページにリダイレクトされます **。ドキュメントに従ってタスクを完了してください 。
  - 影響を受けるインスタンス：CVE の影響を受ける NetScaler インスタンスが表示されます。タスクを完了するには、インスタンスを選択して [**View and Remediate**] をクリックします。

    推奨処置: インフラストラクチャ **>** インスタンスアドバイザリ **>** セキュリティアドバイザリのセキュリティアドバイザリページにリダイレクトされます **。ドキュメントに従ってタスクを完了してください 。

> 注：
>
> - NetScaler ADM に保留中のタスクがない場合は、次のページが表示されます。



- シナリオによっては、すべてのインスタンスでチェックが行われ、すべてのタスクをロードするのにさらに時間がかかる場合があります。



推奨事項

次の表は、NetScaler ADM GUI で表示できる推奨事項を示しています:

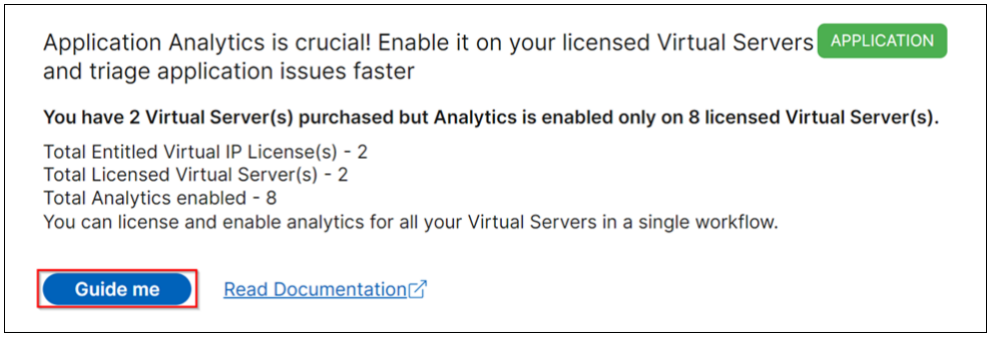
> 注
>
> プールライセンスの場合は、既存のプールライセンス資格に基づいて推奨事項が表示されます。

レコメンデーション名	タスクが GUI に表示されるのはいつですか?
ADC を追加	NetScaler ADM にオンボーディングした後、ADC インスタンスが検出されない場合。
NetScaler ADM の機能を最大限に活用するには、外部の ADM エージェントを追加してください	外部エージェントが設定されていない場合。組み込みのエージェントから始めることができます。ただし、分析、プールライセンスなどのすべての機能を使用するには、外部エージェントが必要です。
ADC をビルトインエージェントから外部エージェントに登録する	Service Connect ワークフローを使用して NetScaler ADM にオンボーディングすると、ADC インスタンスは組み込みエージェントを使用してオンボーディングされます。これらの ADC インスタンスを外部エージェントに登録して、分析、プールライセンスなどのすべての機能を使用できます。
アプリケーション分析は非常に重要です! ライセンスを取得した仮想サーバーで有効にして、アプリケーションの問題をより迅速にトリアージできます。	ライセンスを受けた仮想サーバーが複数あるが、分析が有効になっていない場合。
ADC の帯域幅を再割り当てしたいですか? シンプルです!	プールされたライセンスが ADC GUI で割り当てられ、それらの ADC インスタンスが NetScaler ADM で検出された場合は、NetScaler ADM を使用して再割り当てを行うことができます。
仮想 IP 資格からより多くの価値を引き出しましょう! 検出された残りの仮想サーバで、より多くの仮想 IP ライセンスを有効にします	必要なライセンスはあるが、すべての仮想サーバーにライセンスが付与されていない場合。
主要なエンタープライズユーザーに、きめ細かなロールベースのアクセスを実現	NetScaler ADM でロールベースのアクセス制御（RBAC）がまだ構成されていない場合。
ルールを設定して、ADC インスタンスの重要なイベントを見逃さないようにしましょう	カスタムイベントルールがまだ設定されていない場合。
複数のアプリケーションとそのパフォーマンスを監視する必要がありますか? カスタムアプリケーションを作成するだけ	カスタムアプリがまだ設定されていない場合。
アプリケーション内の重要なイベントを通知し、見逃さないようにしましょう	アクションポリシーがアプリスコア偏差、サーバー処理時間、クライアントネットワーク遅延、サーバーネットワーク遅延、または応答時間に設定されていない場合。
アプリケーションの停止を回避し、アプリケーション内の期限切れ間近の SSL 証明書を見逃さないようにしましょう	期限切れ間近の SSL 証明書に対してアラートまたは通知が設定されていない場合。
セキュリティ勧告-CVE と緩和策により ADC を最新の状態に保ちましょう	ADC インスタンスが CVE に影響を与える場合。

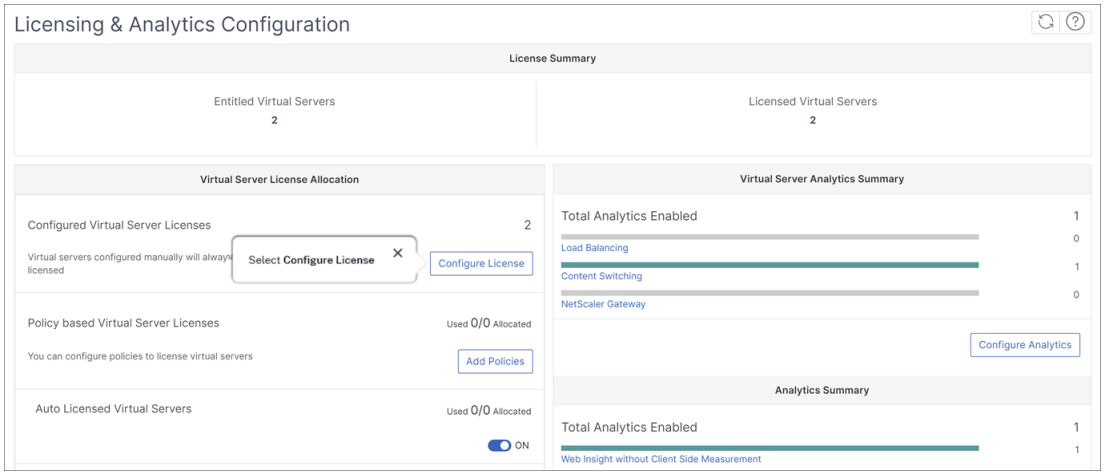
レコメンデーション名	タスクが GUI に表示されるのはいつですか?
企業ポリシーを設定し、逸脱がないか監視します	SSL エンタープライズ設定が変更されていないか、デフォルトのままである場合。
タスクを手動で繰り返す? 設定ジョブを作成して複数の ADC に適用する	**Config Job** タスクがまだ設定されていない場合。
任意のカスタム指標を選択して、インスタンススコアを管理および監視します。	インスタンススコア設定のデフォルト設定としきい値が変更されていない場合。
お好みのカスタム指標を選択して、アプリケーションスコアを追跡します。	アプリダッシュボードのアプリスコアコンポーネントがデフォルトで使用され、カスタマイズが行われていない場合。
プライベート IP ブロックを追加して、Geo Map でクライアントのリクエストを視覚化します	IP ブロックが設定されていない場合。プライベート IP/範囲に基づいて、クライアントリクエストをジオマップにマッピングおよび視覚化するための IP ブロックを作成できます。
AppSec 違反をサブスクライブして Splunk にリアルタイムでエクスポート	NetScaler ADM の Splunk インテグレーションがまだ設定されていない場合。
Kubernetes サービスのデフォルトのしきい値をカスタマイズするか、新しいしきい値を作成します	サービスグラフでデフォルトのしきい値のみが使用され、サービスには単一または二重のしきい値が適用されない場合。
通知プロファイルを事前に設定し、コミュニケーション先で通知を受け取る	通知プロファイルがまだ設定されていない場合。
定期的なエクスポートをスケジュールし、インフラストラクチャの詳細に関する通知を受け取る	[インフラストラクチャ**] > [**インスタンス**]** でエクスポートスケジュールがまだ設定されていない場合。
ServiceNow を利用していて、ADM との統合を検討していますか?	NetScaler ADM の ServiceNow 統合がまだ構成されていない場合。
Venafi と ADM を使用して SSL 証明書管理を自動化します	Venafi サーバーが NetScaler ADM でまだ構成されていない場合。
有効期限が切れる前にプールライセンスを更新してください。	既存のライセンスが 30 日後に期限切れになる場合。
購入したプール帯域幅を NetScaler インスタンスに割り当てて、プールライセンスを開始します。	プールライセンス資格の割り当てをまだ開始していない場合。
プール帯域幅の容量を増やすことを検討してください。	プールされた帯域幅使用率の 90% 以上を利用している場合。
現在のプール帯域幅の使用権限は十分に活用されていません。確認して、さらに割り当てることを検討してください	プールライセンス割り当ての使用率が 70% 未満の場合。

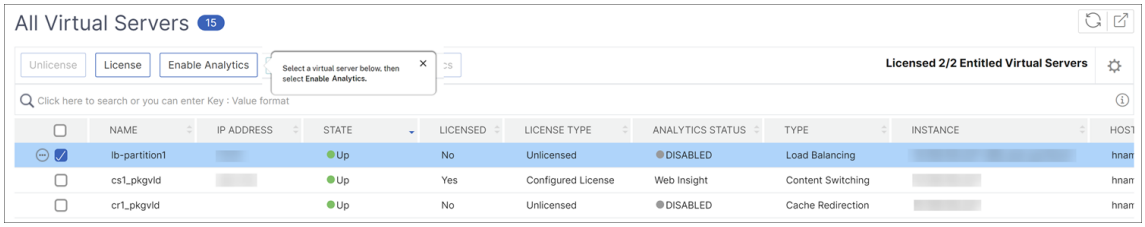
ガイドミーワークフローを使用してレコメンデーションを完了するにはどうすればいいですか

ライセンスを受けたすべての仮想サーバーの分析を有効にしたいと考えてください。「ガイドミー」をクリックして次のタスクを実行してください。

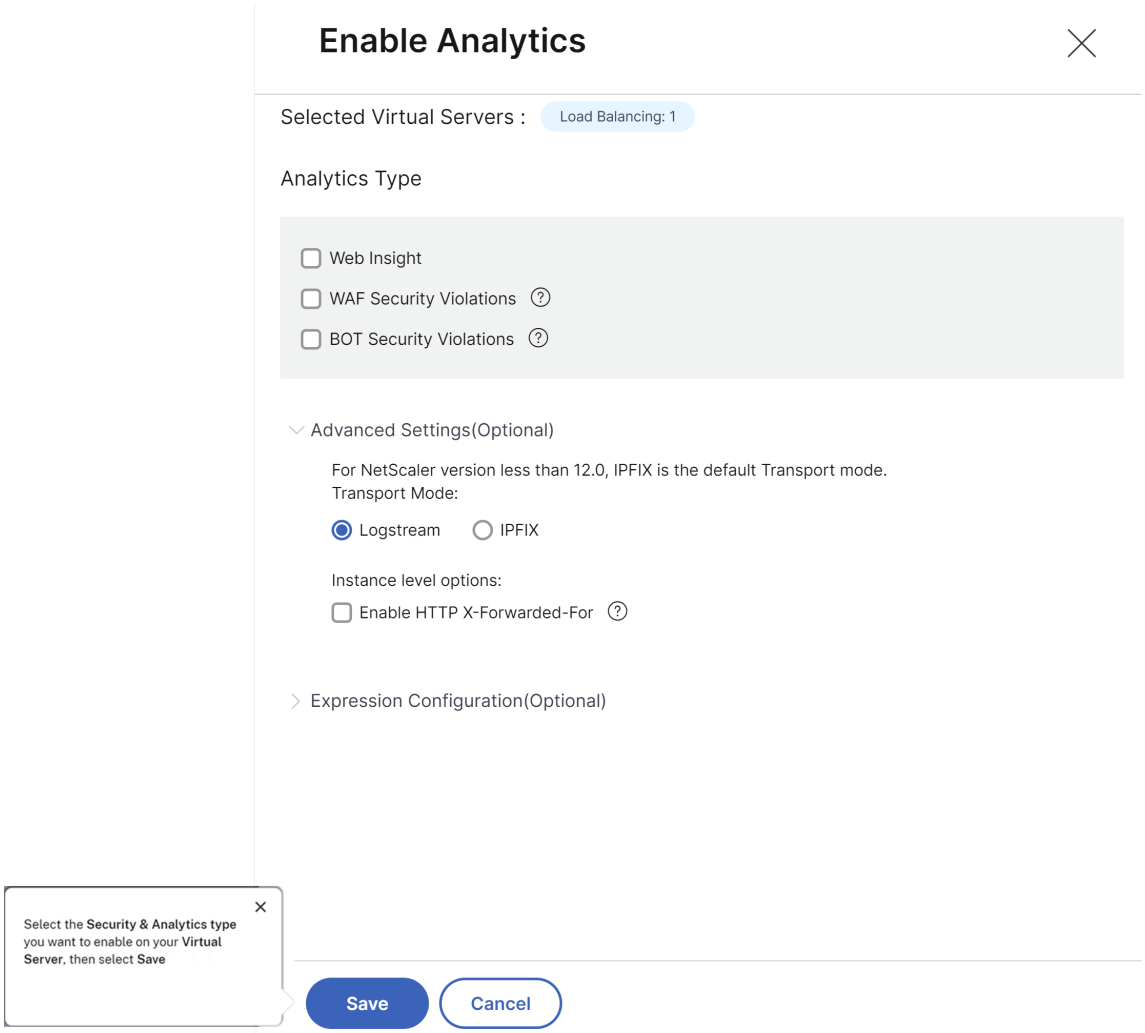


ワークフローには、タスクを完了するために必要な提案が表示されます。この例では、「**Guide me**」をクリックした後、表示されるツールチップの提案に従います：

1. 

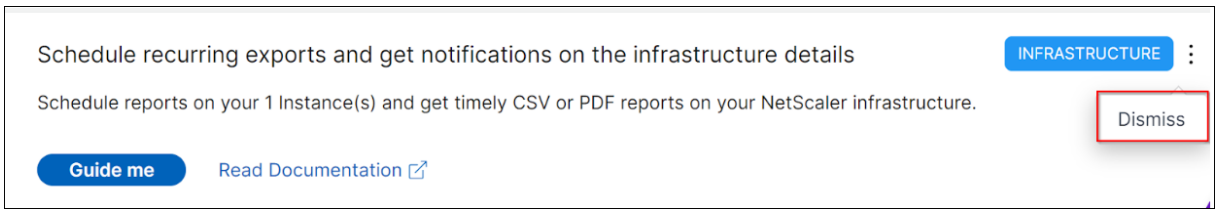
2. 

3.



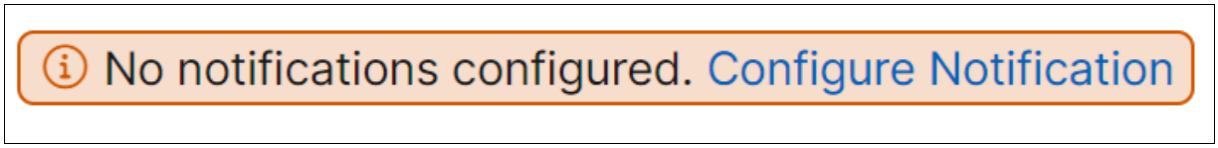
分析タイプを選択して [分析を保存] をクリックすると、レコメンデーションが完成し、[完了] に移動します。

同様に、レコメンデーションを後で完了したい場合は、リストから [却下] を選択すると [却下] に移動します。



通知の設定

NetScaler ADM が、すぐにアクションが必要な未解決のタスクを検出したときに、通知を構成して受け取ることができます。通知を設定していない場合は、右上隅にある [通知の設定] をクリックします。



通知ページでは、メールと **Slack** のプロファイルを設定し、「保存」をクリックして通知を受け取ることができます。通知の種類ごとに、NetScaler ADM GUI には構成済みの配布リストまたはプロファイルが表示されます。NetScaler 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。

よくある質問

1. 管理者にはなぜこのような推奨事項があるのでしょうか。

   現在のところ、推奨事項はデプロイメントに特化したもので、管理者がデプロイメントを効率的にするための構成やセットアップタスクについてさらに詳しく説明できるようになっています。また、製品を見つけやすくなり、管理者は事前に知識がなくても、その機能が ADM に存在するかどうかを知らなくても、タスクが何をし、どのように役立つかを知ることができます。

2. 推薦を却下した場合はどうなりますか?

   却下したレコメンデーションは「却下」に移動されます。これらの推奨事項は後で入力できます。

3. ガイドを始めて途中でそのままにしておくと、レコメンデーションは「完了」になりますか?

   いいえ、アクションが保存または完了しないかぎり、レコメンデーションは完了しません。

4. 検索やフィルタリングはできますか?

   はい！検索バーを使用するか、リストからカテゴリを選択して特定のタスクに絞り込むことができます。

5. 動的イベントに対してアクションを実行するためのタスクはもらえますか?

   はい！現在、合計 4 つの実行可能なタスクを表示できます。詳細については、「タスク」を参照してください。

6. NetScaler ADM に NetScaler インスタンスを追加していなくても、実行可能なすべてのタスクと 20 以上の推奨事項が表示されますか?

   いいえ。すべてのタスクと推奨事項を表示するには、NetScaler ADM で NetScaler インスタンスと仮想サーバーの両方を使用できる必要があります。

7. タスクはどのくらいの頻度で更新されますか?

   左側のナビゲーションペインで [タスク] をクリックすると、タスクが更新され、最新のステータスで使用できるようになります。詳細が取得され、更新されます。

インスタンスの主要メトリックの詳細を表示する統合ダッシュボード

February 6, 2024

NetScaler ADM では、アプリケーションの使用状況とパフォーマンス、ADC インフラストラクチャ、セキュリティ（ボットと WAF）違反などに関するさまざまな洞察を表示できます。管理者は、複数のインサイトを表示するために、ADM GUI のさまざまなオプションに移動する必要がある場合があります。たとえば、仮想サーバー (アプリケーション) と ADC インスタンスのインサイトを確認するには:

- アプリケーションのインサイトを表示するには、まず [アプリケーション**] > [**ダッシュボード] に移動する必要があります。
- 次に、インフラストラクチャ **>** インフラストラクチャ分析に移動して、ADC インスタンスのインサイトを表示する必要があります。

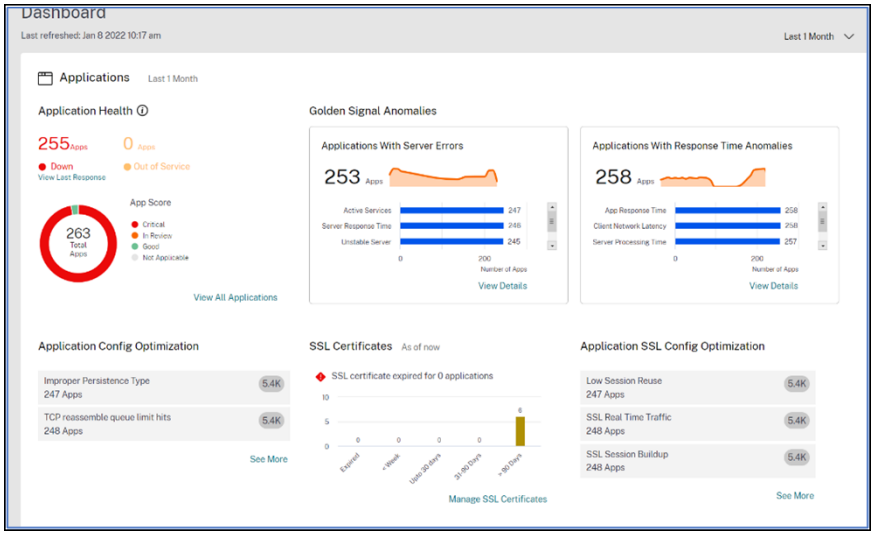
モニタリングをより快適に行うには、必要なすべてのインサイトの概要を含む権限が必要です。[概要**] > [**ダッシュボード] に移動すると、次のカテゴリに基づいて主要なメトリックの詳細の概要を示す単一ペインのダッシュボードが表示されます。

- アプリケーション
- ADC インフラストラクチャ
- アプリケーションのセキュリティ
- Gateway

アプリケーション

「アプリケーション」には、次の項目が表示されます。

- アプリケーションヘルス—****** 停止中およびサービス停止中のアプリケーションの概要を、「****** 緊急」、「レビュー中」、「良好」、「該当なし」などのステータスに基づいて表示します。「すべてのアプリケーションを表示」をクリックすると、アプリダッシュボードに詳細が表示されます。
- **Golden Signal Anomalies** —サーバーエラーと応答時間に異常があるアプリケーションの概要を提供します。詳細については、[詳細の表示] をクリックしてください。
- アプリケーション構成の最適化—パフォーマンスに問題があるアプリケーション全体の概要を示します。「もっと見る」をクリックすると、アプリダッシュボードに課題の詳細が表示されます。
- **SSL** 証明書—SSL 証明書の概要とその有効性について説明します。**SSL** 証明書の管理をクリックすると、SSL ダッシュボードに詳細情報が表示されます。
- アプリケーション **SSL** 構成の最適化—SSL 関連の問題があるアプリケーション全体の概要を提供します。「詳細を表示」をクリックすると、問題の詳細が表示されます。



ADC インフラストラクチャ

「**ADC** インフラストラクチャ」では、以下の ADC インスタンス関連の主要メトリックを表示できます。

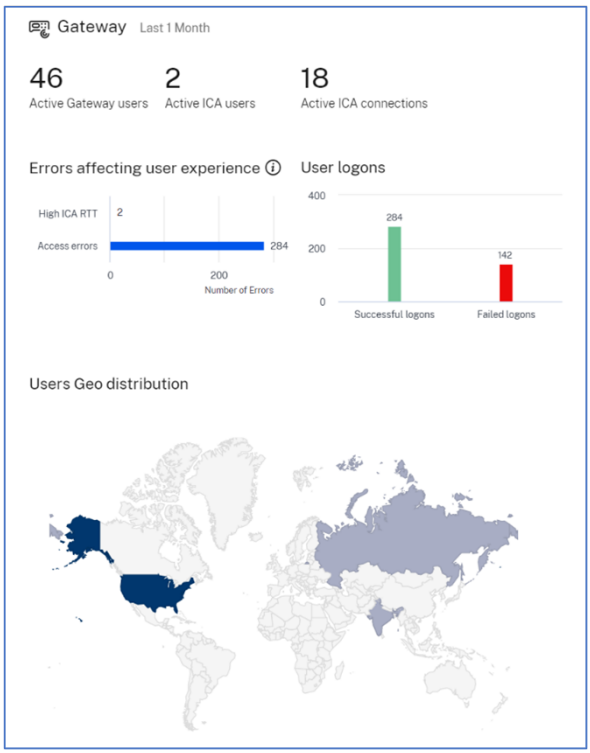
- **ADC** インスタンスの状態—インスタンスのスコアに基づいて、ADC インスタンスの合計数の概要が表示されます。
- **CVE** の影響を受ける **ADC** インスタンス—一般的な脆弱性と暴露 (CVE) の影響を受ける ADC インスタンスの総数の概要を示します。
- **ADC** インスタンスの問題—問題のカテゴリ別に、ADC インスタンスの問題の概要を示します。詳細については、「インフラストラクチャ分析」を参照してください。
- **ADC** インスタンスのアップグレードの概要—最新のビルドにない ADC インスタンスの総数の概要が表示されます。詳細については、「ADC インスタンスダッシュボードを表示」をクリックしてください。

アプリケーションセキュリティ

影響を受けたアプリケーションの合計数と、選択した期間に報告された違反（ボットと WAF）の合計の概要が表示されます。「セキュリティダッシュボードを表示」をクリックすると、セキュリティとボット違反の詳細が表示されます。

Gateway

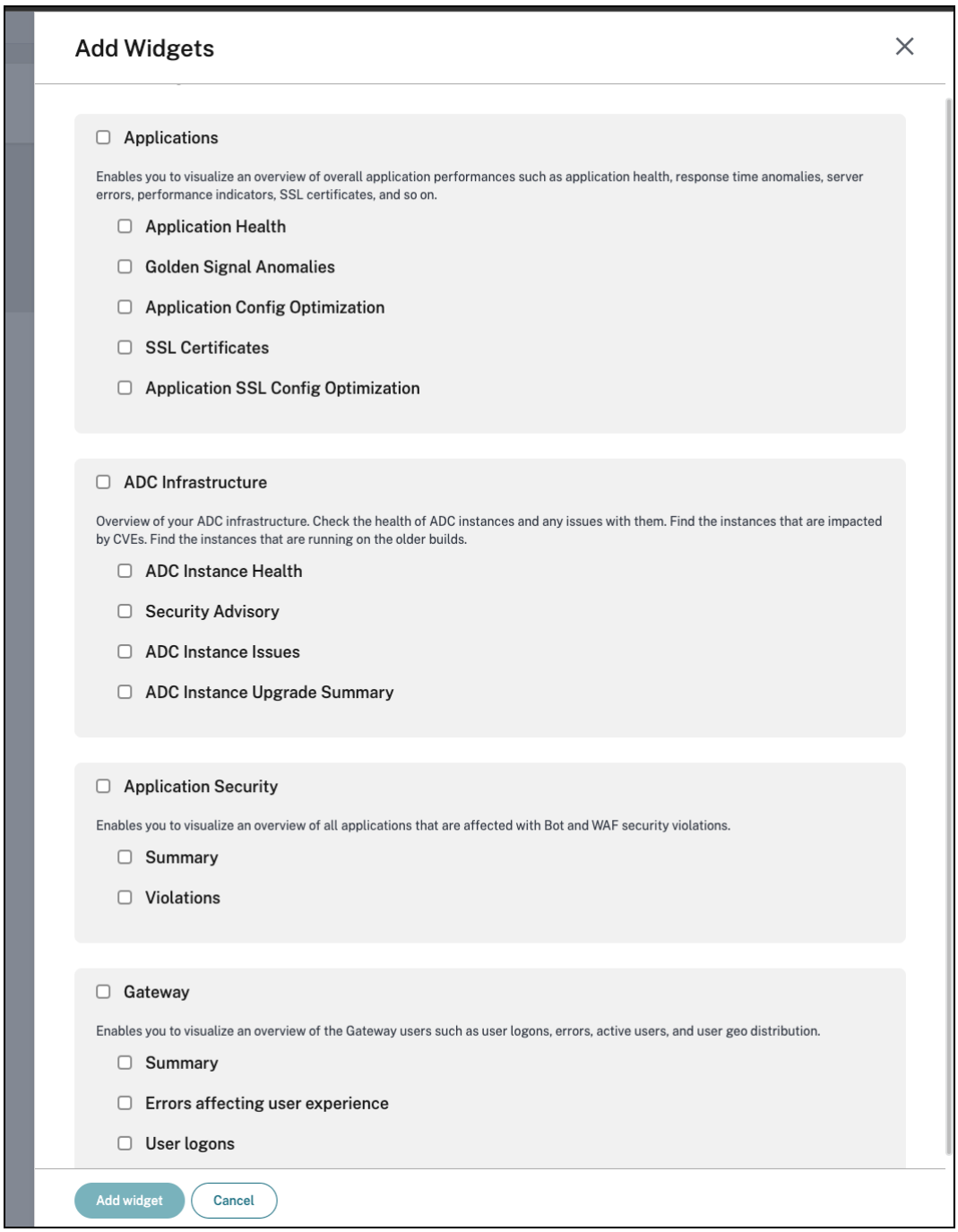
アクティブなゲートウェイユーザーの合計、アクティブな ICA ユーザーの総数、アクティブな ICA 接続の合計の概要を示します。エラー、ユーザーログオンの詳細、およびユーザーの場所の詳細を示すジオマップを表示することもできます。



ダッシュボードをカスタマイズ

[ダッシュボードの編集] オプションを使用して、選択に基づいてダッシュボードビューをカスタマイズできます。「ダッシュボードを編集」オプションを使用すると、次のことができます。

- ウィジェットをドラッグ
- ウィジェット全体 (アプリケーション、ADC インフラストラクチャ、ゲートウェイ、またはアプリケーションセキュリティ) を削除します。
- 各ウィジェットの下にある小さいウィジェットを削除します。
- 「ウィジェットを追加」をクリックし、各ウィジェットの下に表示したい必須の主要指標を選択します。



- デフォルトにリセット
- 最後に保存した内容にリセット

変更を加えたら、[保存] をクリックします。

> 注
>
> - デフォルトでは、すべてのウィジェットが表示されます。ダッシュボードをカスタマイズして変更を保存

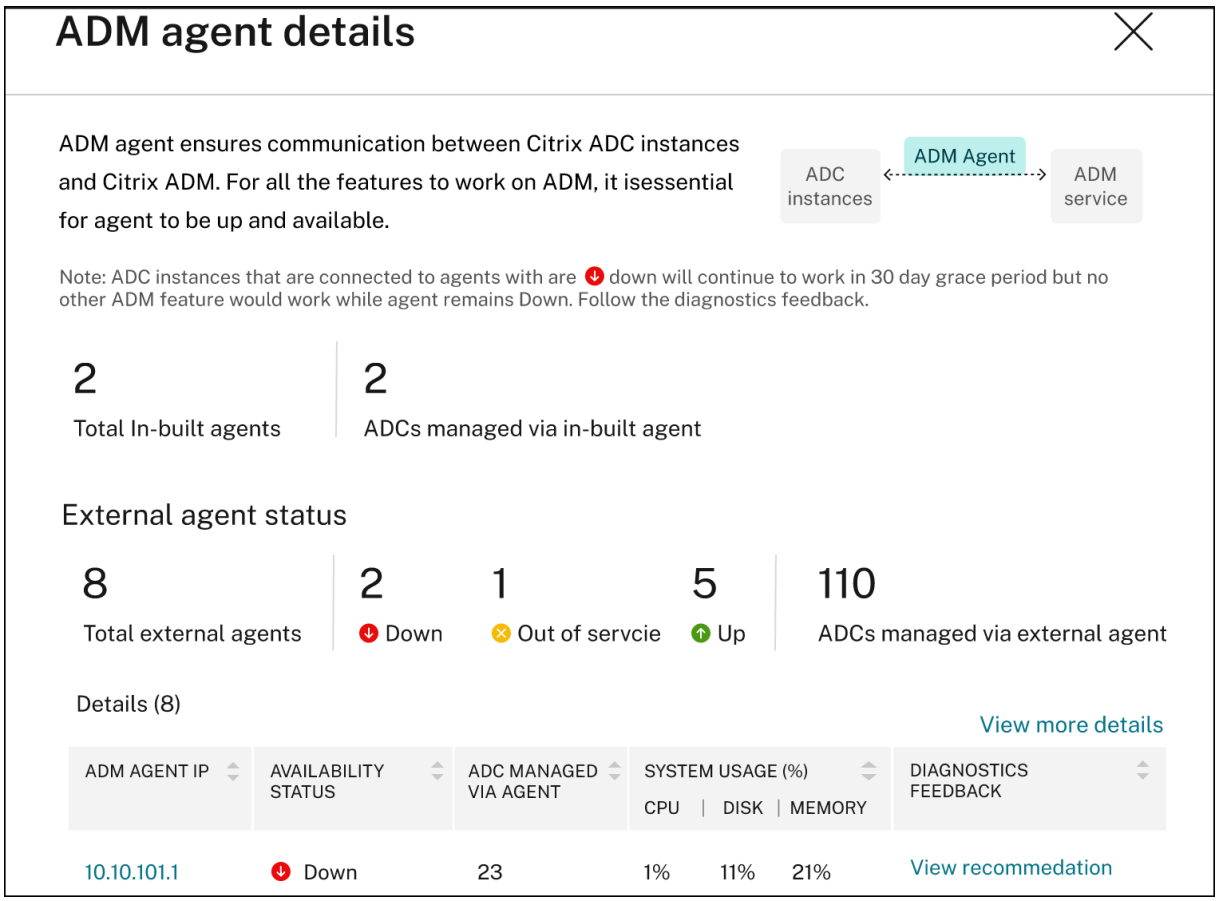
> し、再び [デフォルトにリセット] オプションを使用すると、すべてのウィジェットがダッシュボードに追加されます。
>
> • [最後に保存した設定にリセット] オプションを選択すると、以前に保存した構成がロードされます。

エージェントの詳細を表示

統合ダッシュボードでは、ADM エージェントの詳細の概要を視覚化できます。**[**概要**] > [**ダッシュボード**]** の **[ADM Agent**Status] の横に、次のステータスが表示され、エージェント全体の可用性を分析できます。

- すべてご利用いただけます。すべてのエージェントが稼働中であることを示します。
- すべて利用できません。すべてのエージェントがダウンしていてアクセスできないことを示します。
- **[**エージェント数**]** は利用できません。一部のエージェントがダウンしていてアクセスできないことを示します。
- すべてアウトオブサービス。すべてのエージェントがアウトオブサービスであることを示します。
- **[**エージェント数**]** はサービスを停止しています。サービス停止中のエージェントが数人いることを示します。
- 外部エージェントが見つかりません。エージェントが (どのハイパーバイザー経由でも) 構成されていないことを示します。

[詳細を表示] をクリックすると、組み込みエージェントの総数、外部エージェントの総数、エージェント IP、ステータス、システム使用状況、診断チェックなど、ADM エージェントの詳細の概要が表示されます。



フィルターの作成と適用

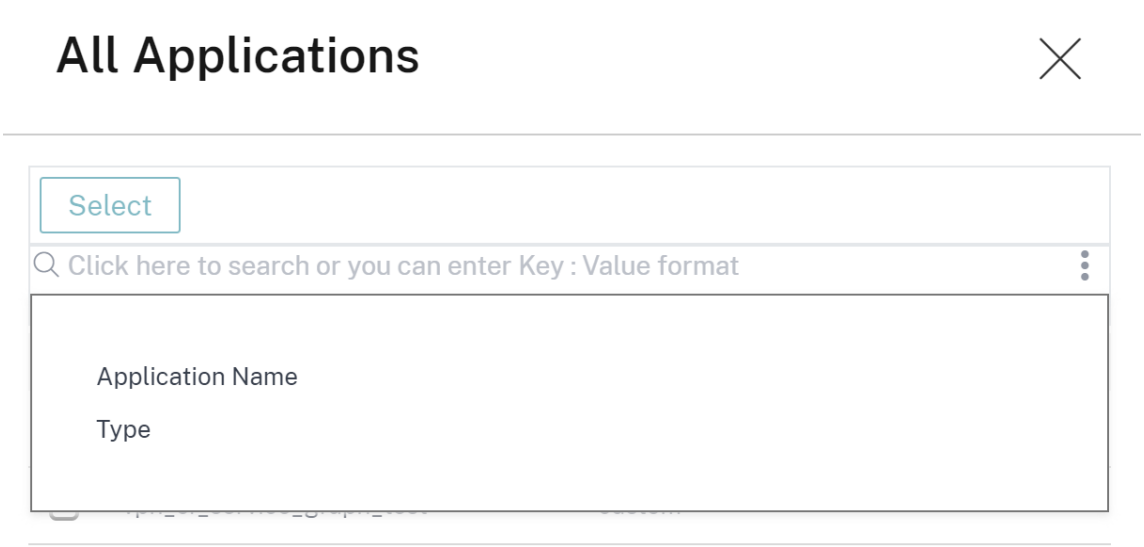
フィルターを適用してインサイトを表示できるのは、以下で選択したインスタンスまたはアプリケーションだけです。

- アプリケーション
- ADC インフラストラクチャ
- アプリケーションセキュリティ

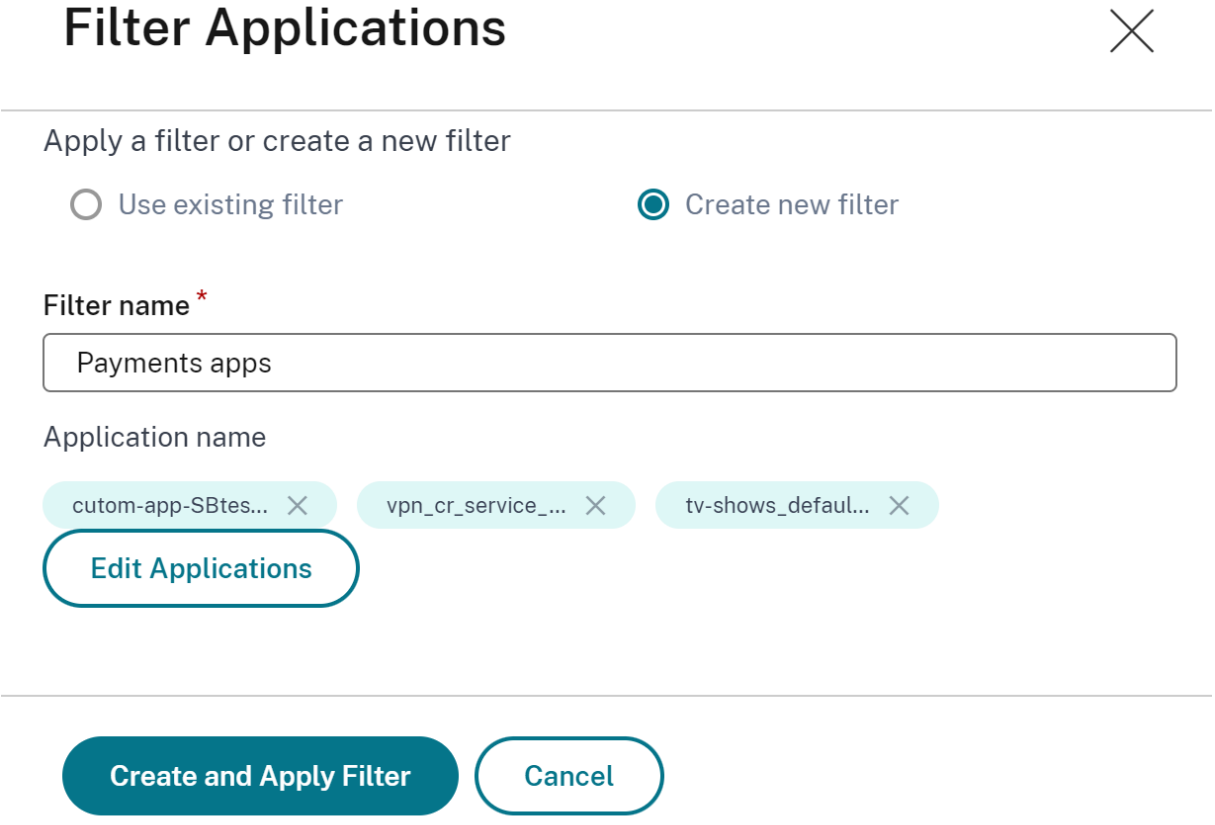
デフォルトでは、すべてのアプリケーションが選択されます。タイルにあるフィルターアイコンをクリックすると、ダッシュボードからカスタマイズされたフィルターを作成できます。

「アプリケーションのフィルタ」ウィンドウでは、

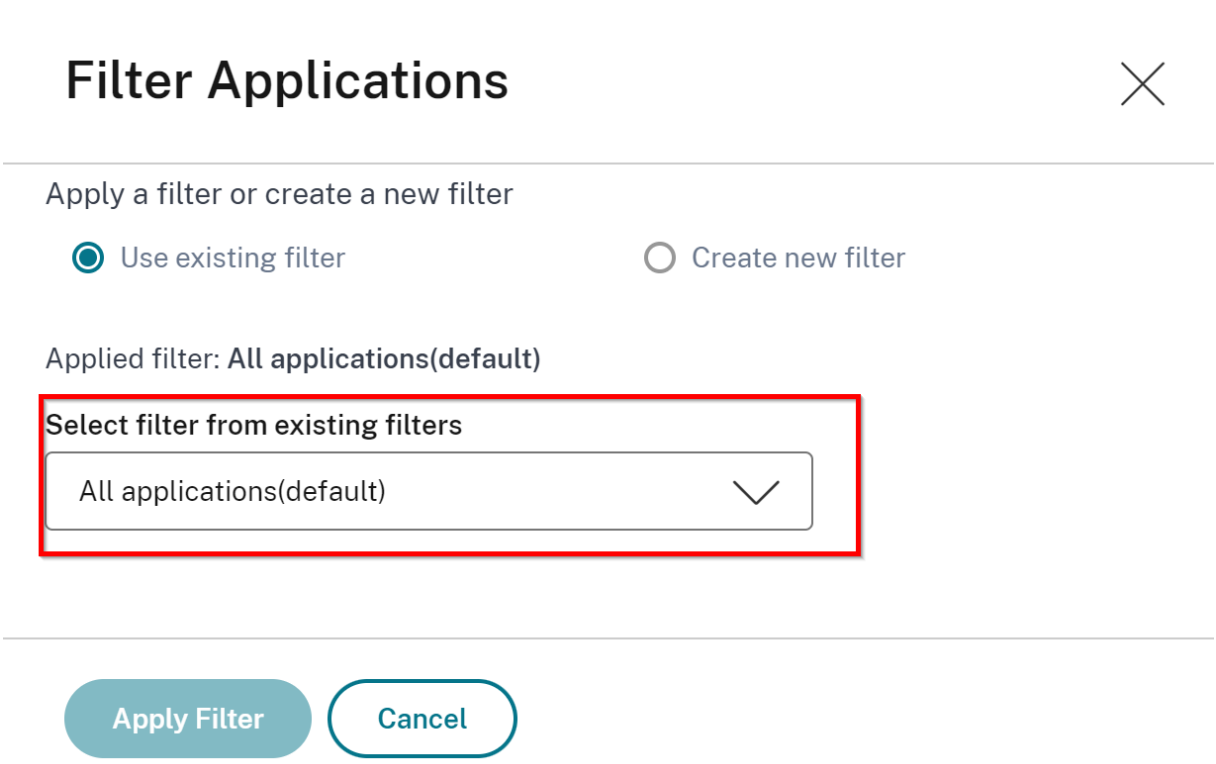
1. [新しいフィルターを作成] を選択します。
2. 選択に基づいてフィルター名を指定します。
3. 「アプリケーションを選択」をクリックし、フィルターに必要なアプリケーションをすべて追加します。アプリケーションを選択するときは、フィルター ([アプリケーション名] と [タイプ]) を使用してからアプリケーションを選択することもできます。



4. [フィルターを作成して適用] をクリックします。

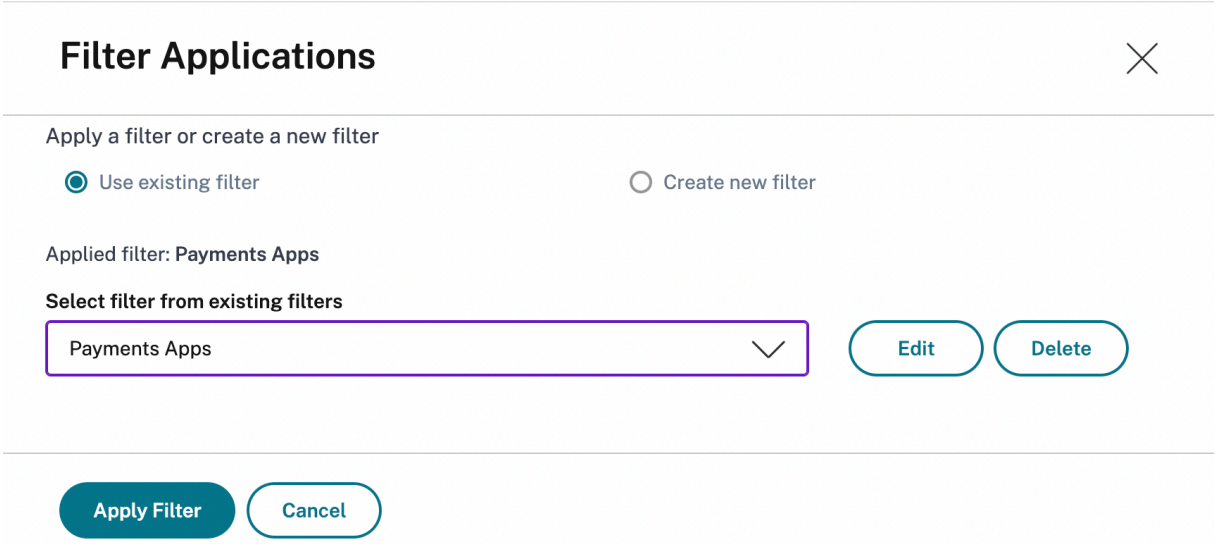


これで、フィルターが作成され、適用されました。同じ手順でさらにフィルターを作成できます。フィルターを作成したら、「既存のフィルターからフィルターを選択」リストからフィルターを選択して適用できます。



フィルターを編集

フィルターを編集するには、リストからフィルターを選択し、[編集] をクリックします。編集オプションを使用して、アプリケーションを追加または削除し、フィルターを更新できます。



フィルターを削除するには、リストからフィルターを選択し、[削除] をクリックします。

> 注
>
> アプリケーションを含むフィルターを作成し、アプリケーションダッシュボードでアプリケーションの 1 つを削除すると、アプリケーションの詳細が統合ダッシュボードからすぐに削除されます。

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）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 インスタンスを追加したことを確認してください
- NetScaler インスタンスの有効なライセンスがあることを確認してください。詳細については、「ライセンス」を参照してください。
- 仮想サーバ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。

- ディスクリー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)

ディスクリートアプリケーション

ライセンスが付与されているすべての仮想サーバは、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ーは、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 クラスターでは、NetScaler は NetScaler MPX（ハードウェア）、NetScaler VPX（仮想化）、および NetScaler CPX（コンテナ化）用の Ingress Controller を提供します。詳しくは、「NetScaler Ingress Controller」を参照してください。

NetScaler CPX インスタンスを使用して構成され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。

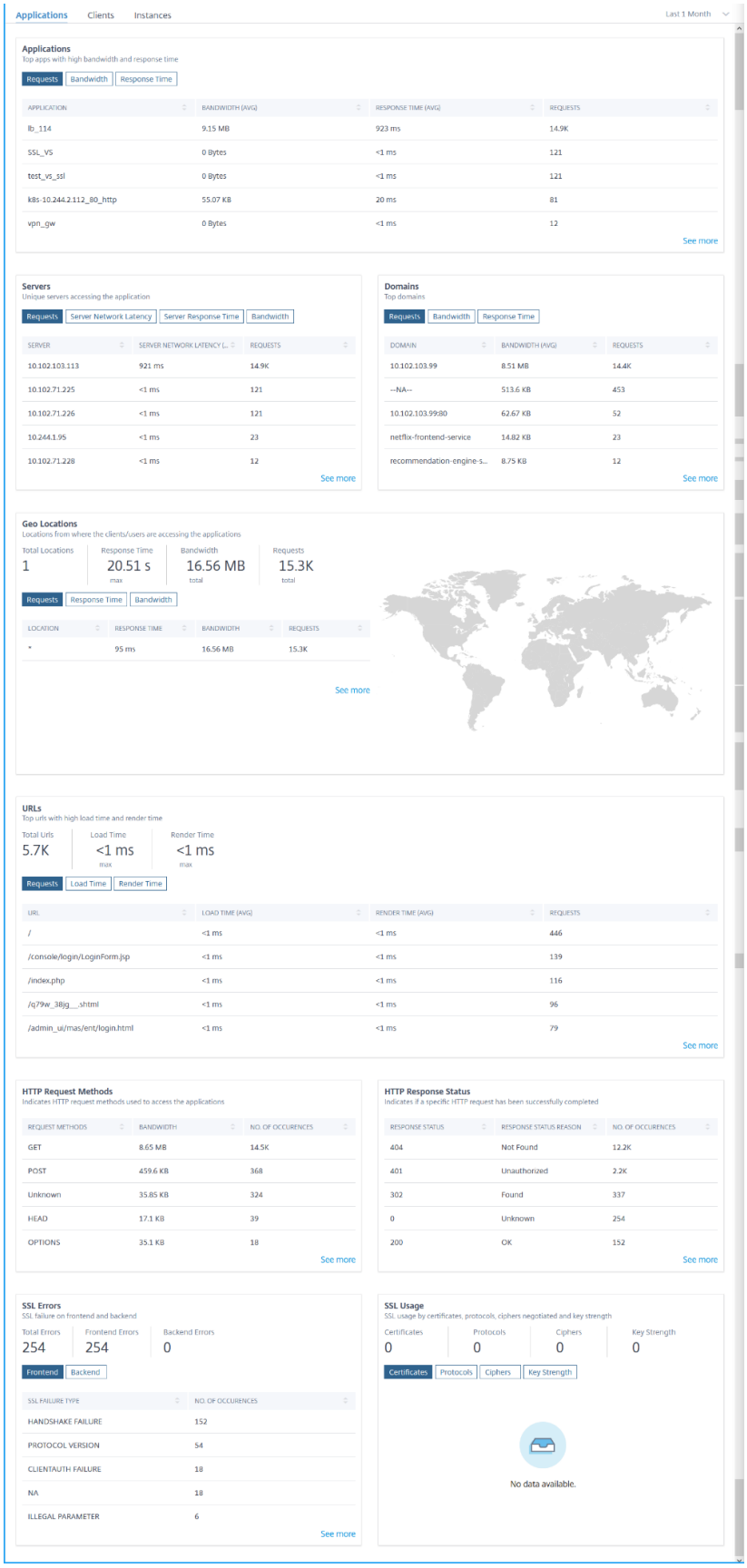
Web Insight ダッシュボード

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 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
		Web ブラウザー

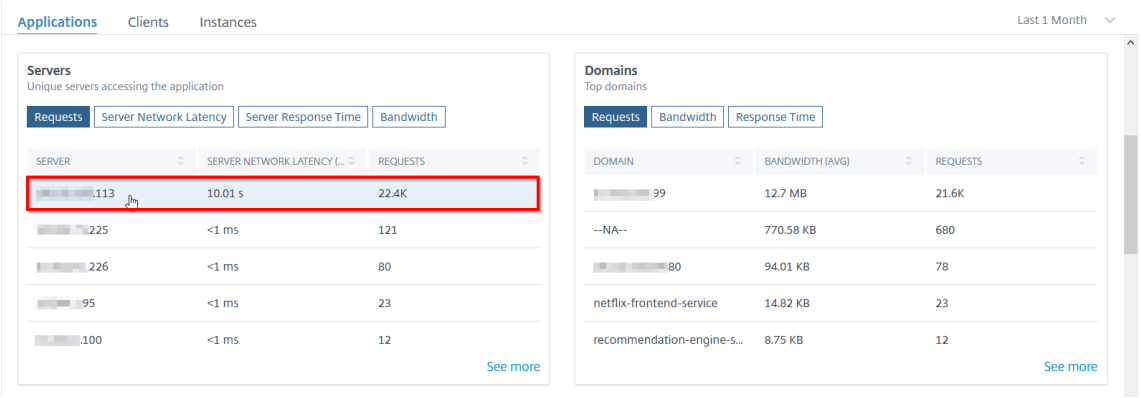


各指標で、上位 5 つの結果を表示できます。をクリックしてさらにドリルダウンして、問題を分析し、トラブルシューティングアクションを迅速に行うことができます。

> 注:
>
> - **14.1-4.x** リリース以降、メトリックスをドリルダウンすると、時系列グラフの分析ビューには、選択した期間のゼロ値（たとえば、0 ミリ秒と 0 リクエスト）が表示されます。以前は、選択した期間にトラフィックやトランザクションが受信されなかった場合、アナリティクスビューではこれらの nil 値をスキップしてグラフを表示していました。
> - シナリオによっては、NetScaler が一部のトランザクションの RTT 値を計算できない場合があります。このようなトランザクションの場合、NetScaler ADM は RTT 値を次のように表示します。
>
> - **NA** —ADC インスタンスが RTT を計算できない場合に表示されます。
> - **< 1ms** —ADC インスタンスが 0 ミリ秒から 1 ミリ秒の範囲の 10 進数で RTT を計算するときに表示されます。たとえば、0.22 ミリ秒です。

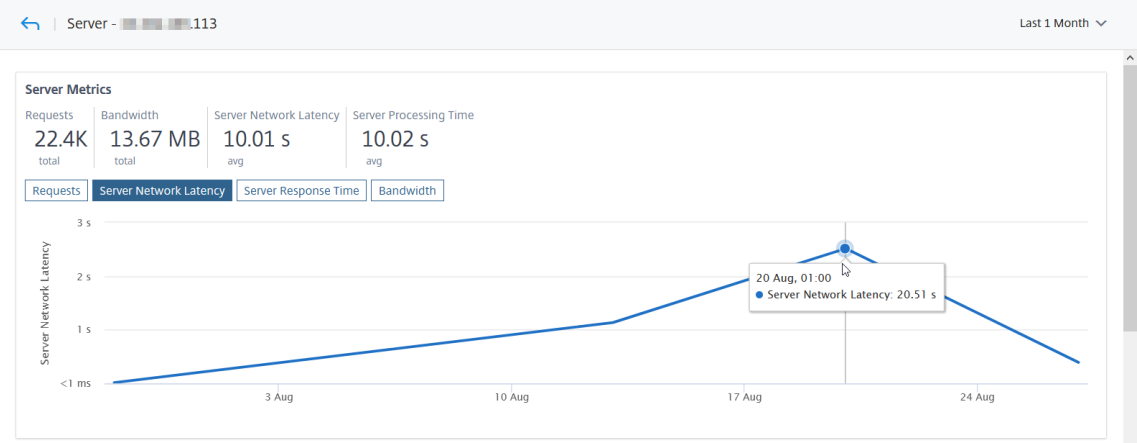
たとえば、1 か月間のサーバーネットワーク遅延を分析し、運用環境をスケールアップするかスケールダウンするかを決定するとします。これを分析するには:

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。

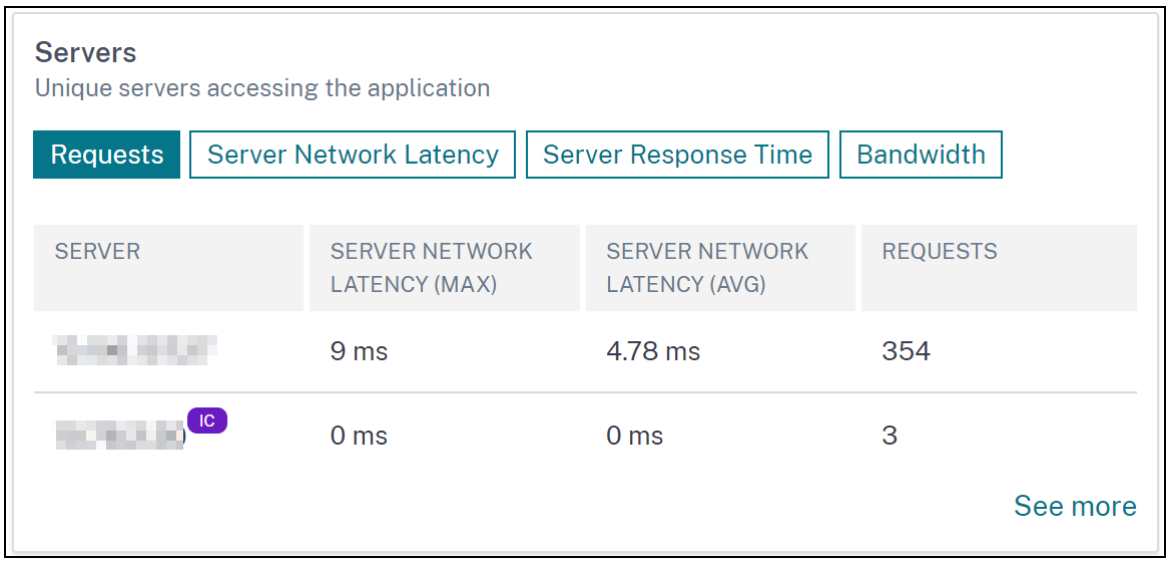


平均レイテンシーは 10.01 秒を示し、グラフから、過去 1 か月のサーバーネットワークのレイテンシーが高いと思われることを分析できます。管理者は、本番環境のスケールアップを決定できます。

統合キャッシュリクエスト

統合キャッシュは、NetScaler アプライアンスのメモリ内ストレージを提供し、オリジンサーバーへの往復を必要とせずにユーザーに Web コンテンツを提供します。

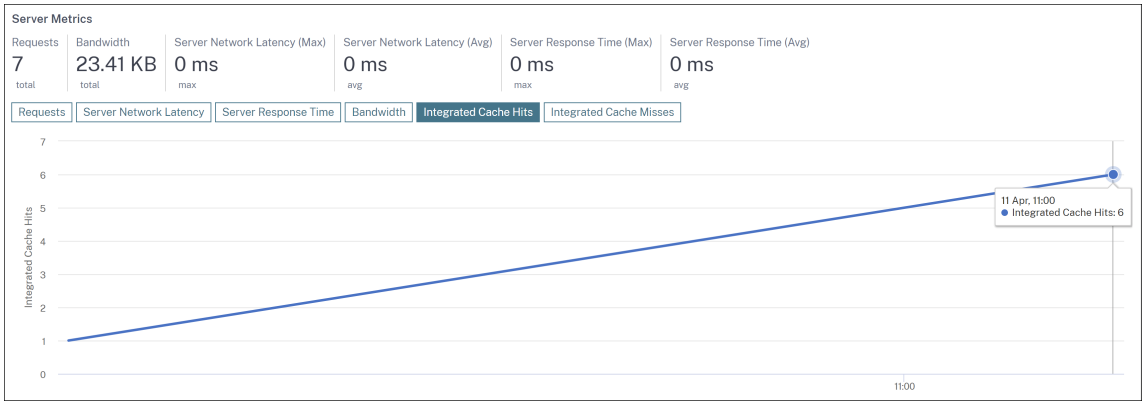
統合キャッシュリクエストは現在、**ADC** 仮想サーバーの **IP** アドレスの横に **IC** 通知が表示されているサーバーの下に表示されます。他のすべてのリクエストは、オリジンサーバーの IP アドレスで表示されます。



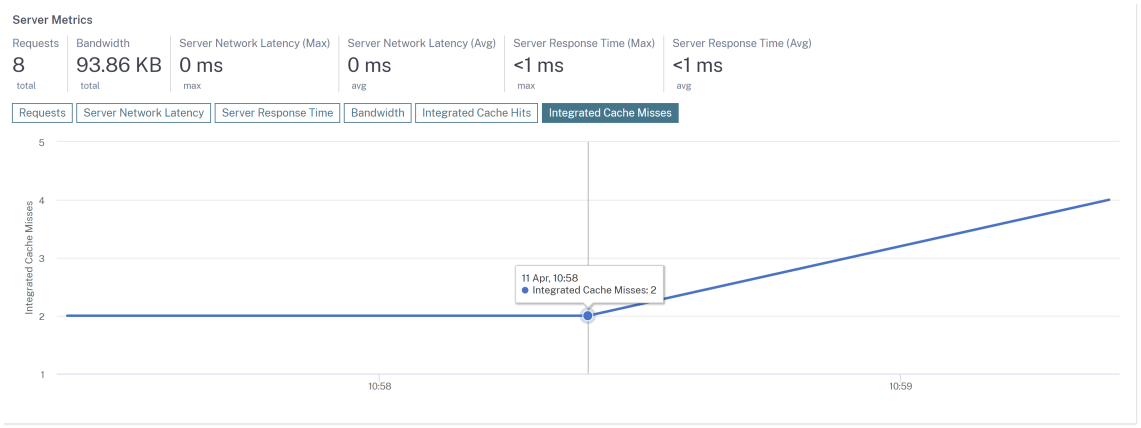
サーバーをドリルダウンして詳細を表示すると、サーバーメトリックには統合されたキャッシュヒットとミスのタブが表示されます。

グラフビューは以下のとおりです。

- 統合キャッシュヒットタブでは、NetScaler アプライアンスがキャッシュから処理する応答の総数を表示できます。



- 統合キャッシュミスタブでは、NetScaler アプライアンスがオリジンサーバーから処理した応答の合計を表示できます。



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。

アプリケーション遅延の根本原因を表示する

February 6, 2024

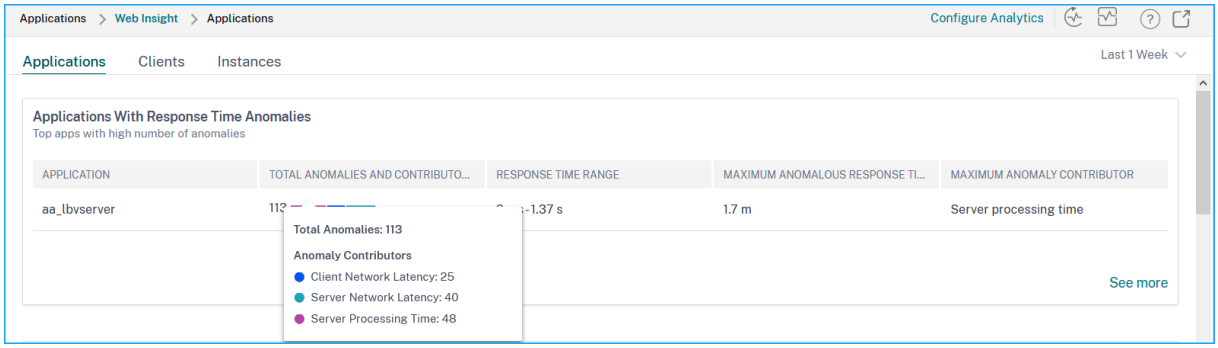
アプリケーションの遅さは、ビジネスへの影響や生産性につながるため、あらゆる組織にとって大きな懸念事項です。[アプリケーション] **> [Web Insight]** に、「応答時間異常のあるアプリケーション」という新しい指標が表示されるようになりました。このメトリックを使用すると、管理者はアプリケーションの遅延が以下の原因で発生しているかどうかを分析できます。

- クライアントネットワーク遅延

- サーバーネットワークの待ち時間
- サーバー処理時間

NetScaler ADM は、特定の前提条件に基づいて、1 時間ごとに異常チェックを実行し、過去 1 時間のトラフィックの異常を報告します。たとえば、偽陽性の結果を避けるために、応答時間が 1 ミリ秒未満の場合、これらの結果の異常チェックはスキップされます。

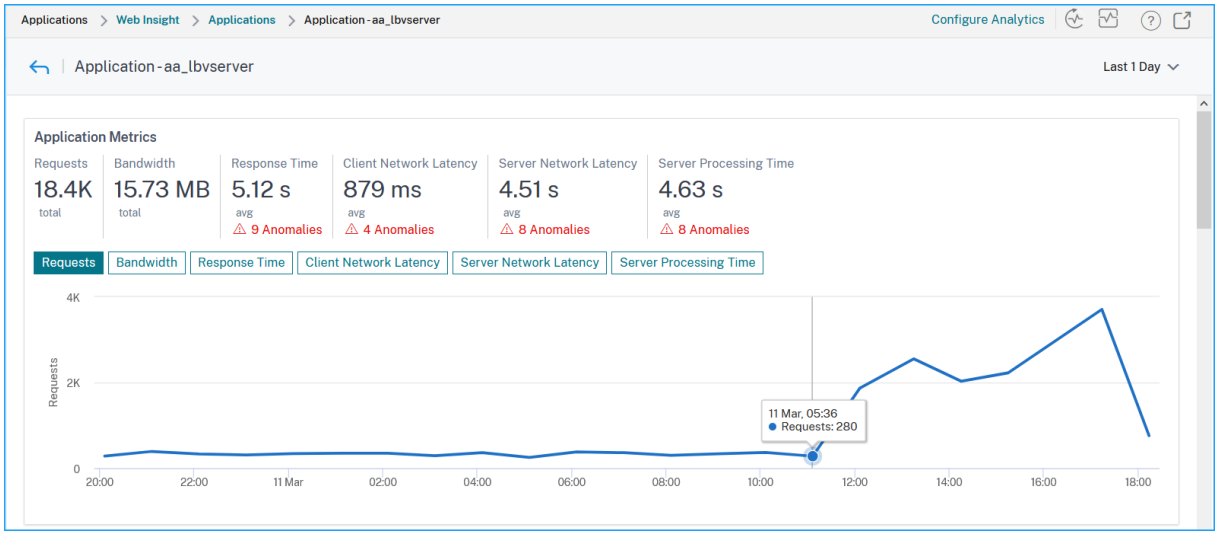
[アプリケーション**] > [Web Insight**] ページでは、選択した期間における応答時間の異常があるアプリケーションを表示できます。「応答時間異常のあるアプリケーション」メトリックには、異常合計に基づいて上位 5 つのアプリケーションが表示されます。[詳細を表示] をクリックして、すべてのアプリケーションを表示します。



- 「アプリケーション」-アプリケーション名を示します。
- [異常値の合計**]** と **[**コントリビュータ数] ―アプリケーションからの異常の総数を示します。マウスポインターを合わせると、クライアントネットワーク遅延、サーバーネットワーク遅延、およびサーバー処理時間の合計異常を表示できます。
- [**Response Time Range**]: アプリケーションからの予測応答時間の範囲を示します。
- **[** 最大異常応答時間]: アプリケーションからの応答時間が最大であることを示します。
- **[Maximum Anomaly Contributor**] ―アプリケーションの異常の最大数が、クライアントネットワーク遅延、サーバーネットワーク遅延、またはサーバー処理時間からのものかどうかを示します。

アプリケーションのドリルダウン

アプリケーションをクリックして、選択した期間の「アプリケーション・メトリック」の詳細を表示します。



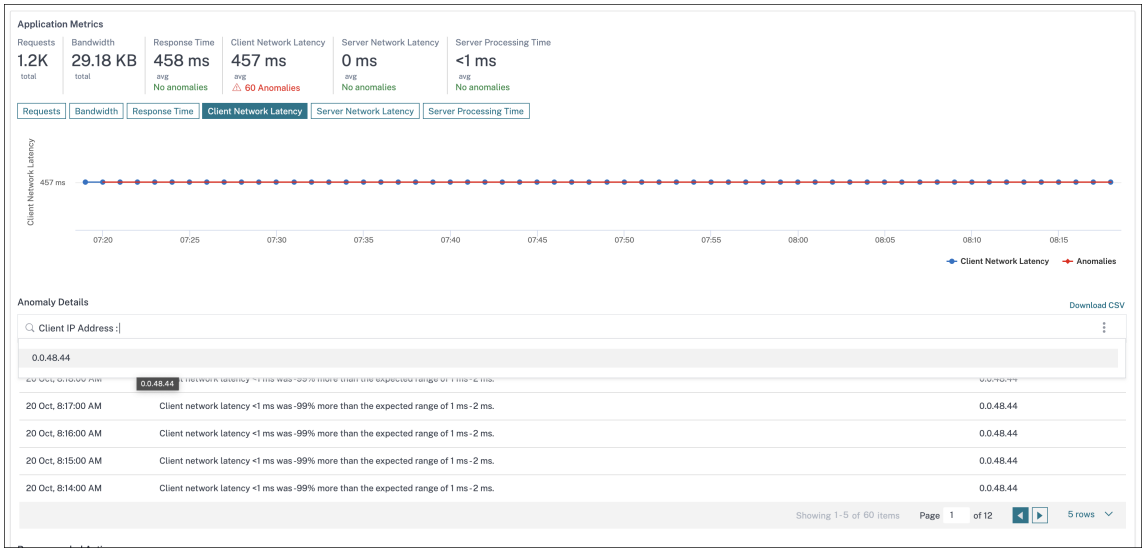
アプリケーション・メトリックを使用すると、次の項目を表示できます。

- 概要—応答時間、要求、帯域幅などのアプリケーションパフォーマンスを視覚化するための概要。
- リクエスト—アプリケーションが受信したリクエストの合計数です。リクエストの合計に基づいて、上位 5 つのクライアントからのリクエストを表示することもできます。
- 帯域幅—アプリケーションが処理した合計帯域幅。また、帯域幅の合計使用量に基づいて、上位 5 台のサーバーの帯域幅消費量を表示することもできます。
- 応答時間—クライアントネットワーク遅延、サーバーネットワーク遅延、サーバー処理時間を同じグラフで視覚化するための概要です。
- クライアントネットワーク遅延—クライアントネットワークの平均遅延 (クライアントから ADC まで)。
- サーバーネットワーク遅延—平均サーバーネットワーク遅延 (ADC からサーバーまで)。
- サーバー処理時間—サーバーの平均処理時間 (サーバーから ADC まで)。

アプリケーションに異常がある場合は、異常がクライアントネットワーク遅延、サーバーネットワーク遅延、またはサーバー処理時間のどちらから発生しているかを確認できます。各タブをクリックして詳細を表示します。

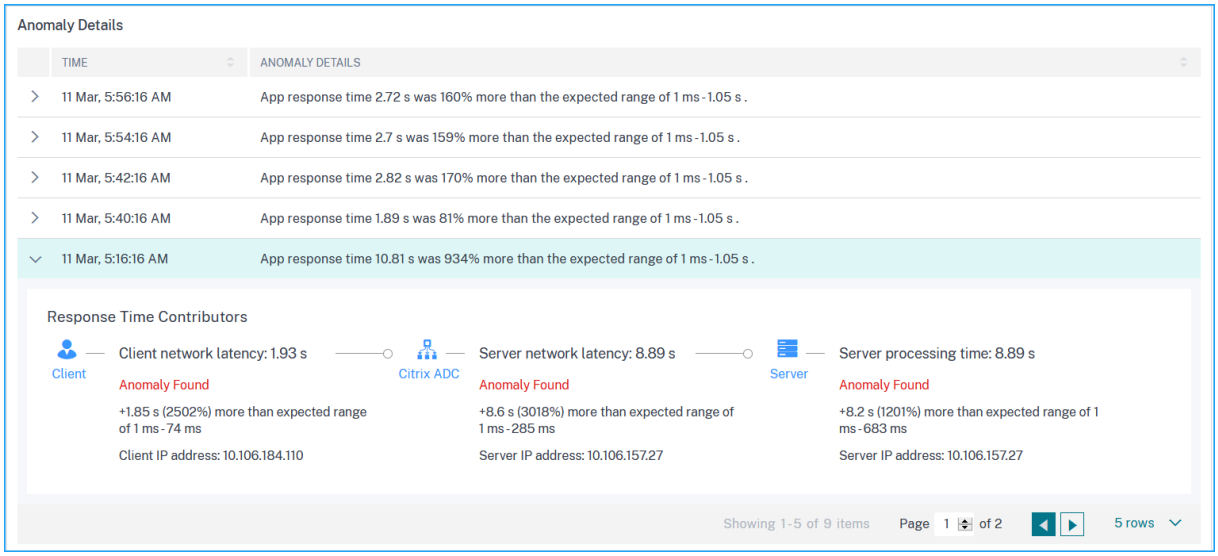
[クライアントネットワーク遅延] タブと [サーバーネットワーク遅延] タブでは、次の情報を確認できます。

- 検索バー -検索バーをクリックすると、すべてのクライアント ([クライアントネットワーク遅延]) とサーバー ([サーバーネットワーク遅延]) の IP アドレスが表示されます。IP アドレスを選択して結果をフィルタリングできます。
- エクスポートオプション-詳細を CSV 形式でエクスポートするには、[**CSV** をダウンロード] をクリックします。

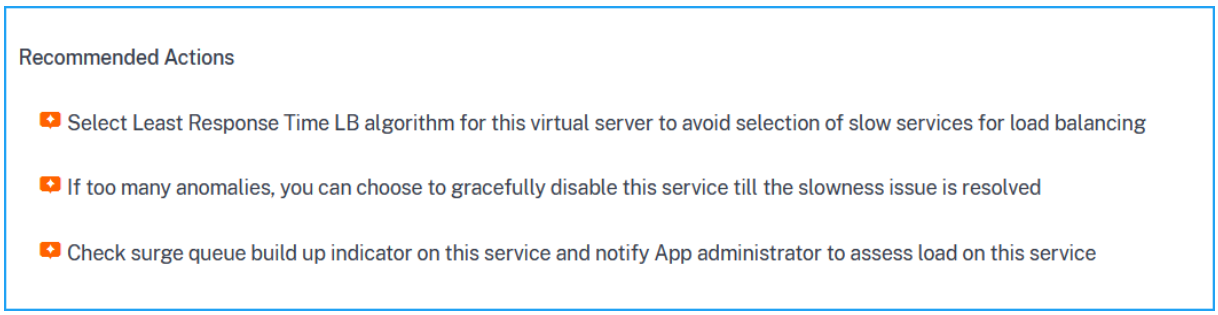


応答時間

[異常の詳細] で、をクリックして、応答時間のコントリビュータの詳細を表示します (クライアントからサーバーへ)。次の例では、クライアントネットワーク遅延、サーバーネットワーク遅延、およびサーバー処理時間の異常があります。また、期待される範囲および期待範囲を超えて発生した違反も表示できます。



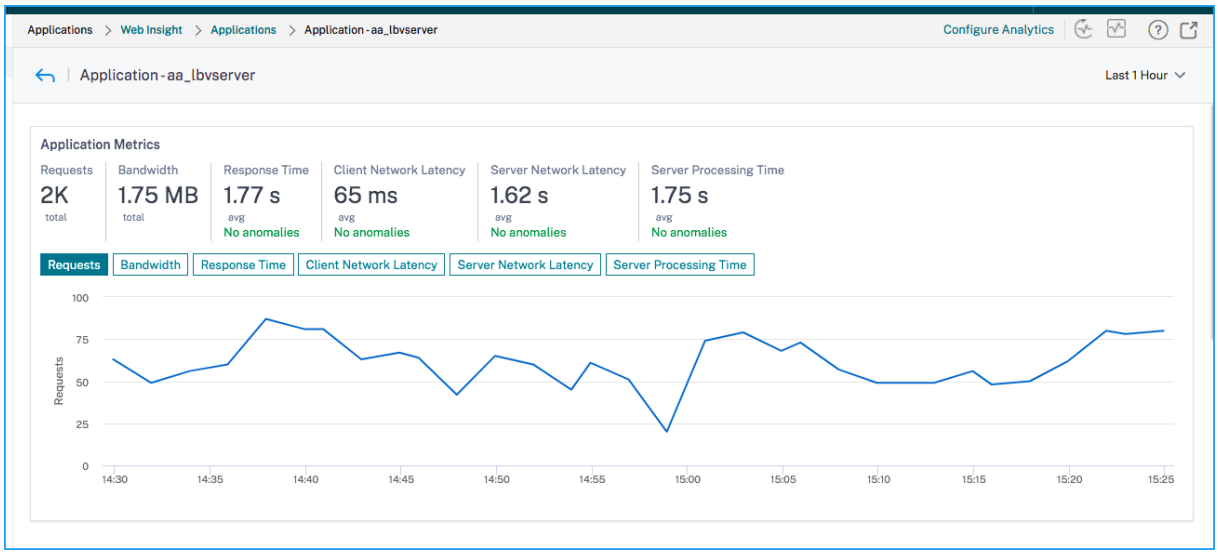
推奨アクションは、異常の解決方法を示します。



同様に、**[**クライアントネットワーク遅延**]**、**[** サーバーネットワーク遅延**]**、**[** サーバー処理時間**]** タブをクリックして、次の項目を表示できます。

- 期待範囲に違反した異常。
- 可能な解決策を示唆する推奨アクション。

アプリケーションのパフォーマンスが良好であれば、アプリケーションメトリックを異常なしとして表示できます。



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ー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 仮想サーバー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ーがない場合、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。
- 仮想サーバーと 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。
- 仮想サーバー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 仮想サーバー、サービスなどの構成データに基づいてサービスグラフで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。

StyleBook

February 6, 2024

StyleBook は、アプリケーションの複雑な NetScaler 構成の管理作業を簡素化します。StyleBook は、NetScaler 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。NetScaler Application Delivery Management （ADM）は、NetScaler 上の既存の状態と指定した希望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ので、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 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の入力で構成される単純なインターフェイスを使用して、複雑にもなり得る NetScaler 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。そのため、1 つの構成を 1 つまたは複数の NetScaler に展開したり、インスタンス間で移動したりすることもできます。
- 自動生成 **UI**：NetScaler ADM は、NetScaler ADM GUI を使用して構成を行うときに、StyleBook のパラメータ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を実現する構成を作成し、NetScaler インスタンスで実行できます。この構成は構成パックとして保存されます。同じ StyleBook を使用して値の異なる別の構成を作成し、それを同じ NetScaler インスタンスまたは異なる NetScaler 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、NetScaler ADM と構成が実行される NetScaler インスタンスの両方に保存されます。

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

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。

1. [セキュリティ] > [セキュリティダッシュボード] に移動します。
2. [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。

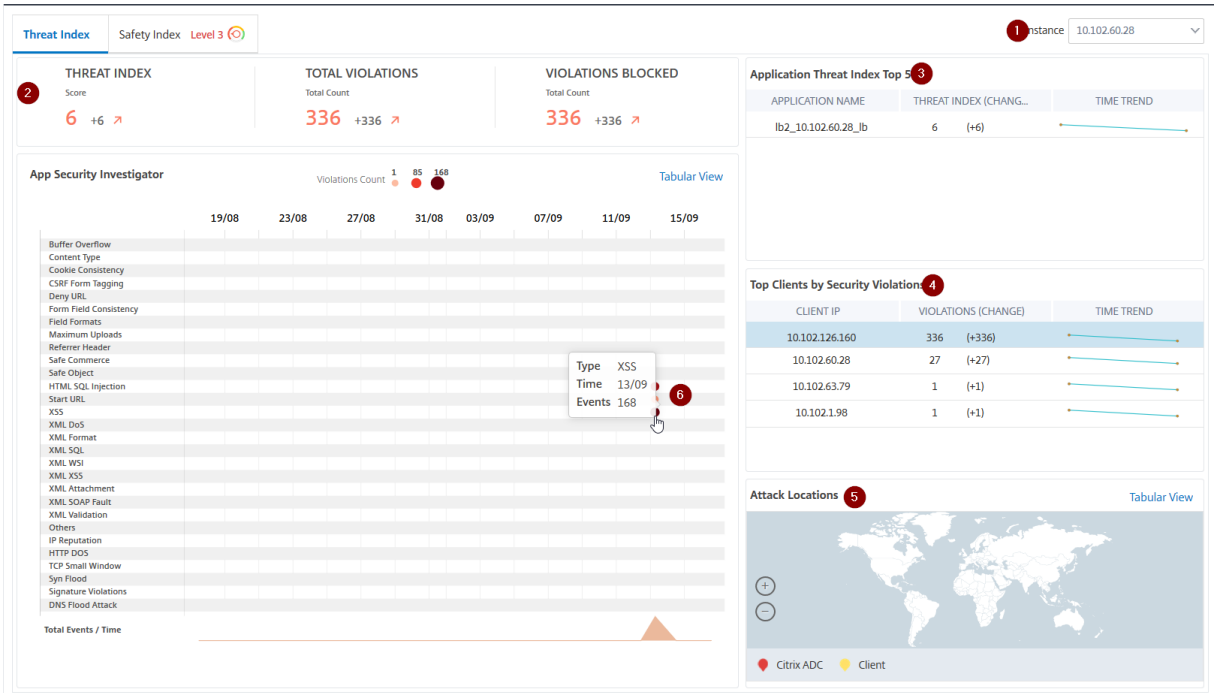
   - 安全指数。外部からの脅威や脆弱性からアプリケーションを保護するために、NetScaler インスタンスをどのように安全に構成したかを示す 1 桁の評価システム。アプリケーションのセキュリティリスクが小さいほど、安全性指数は高くなります。値の範囲は 1 ～7 です。

     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 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 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 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。

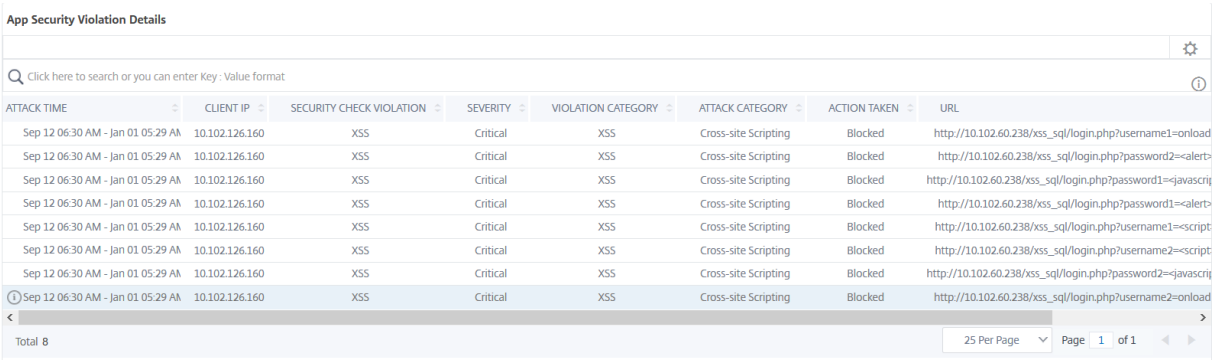
4 -クライアントに基づいてセキュリティ違反を表示します。App Security Investigator のグラフは、クライアントごとに表示されます。各クライアント IP をクリックすると、結果を表示できます。

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。



[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。

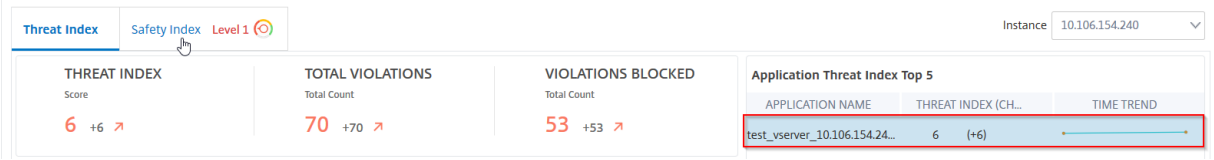
安全指数の詳細

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。

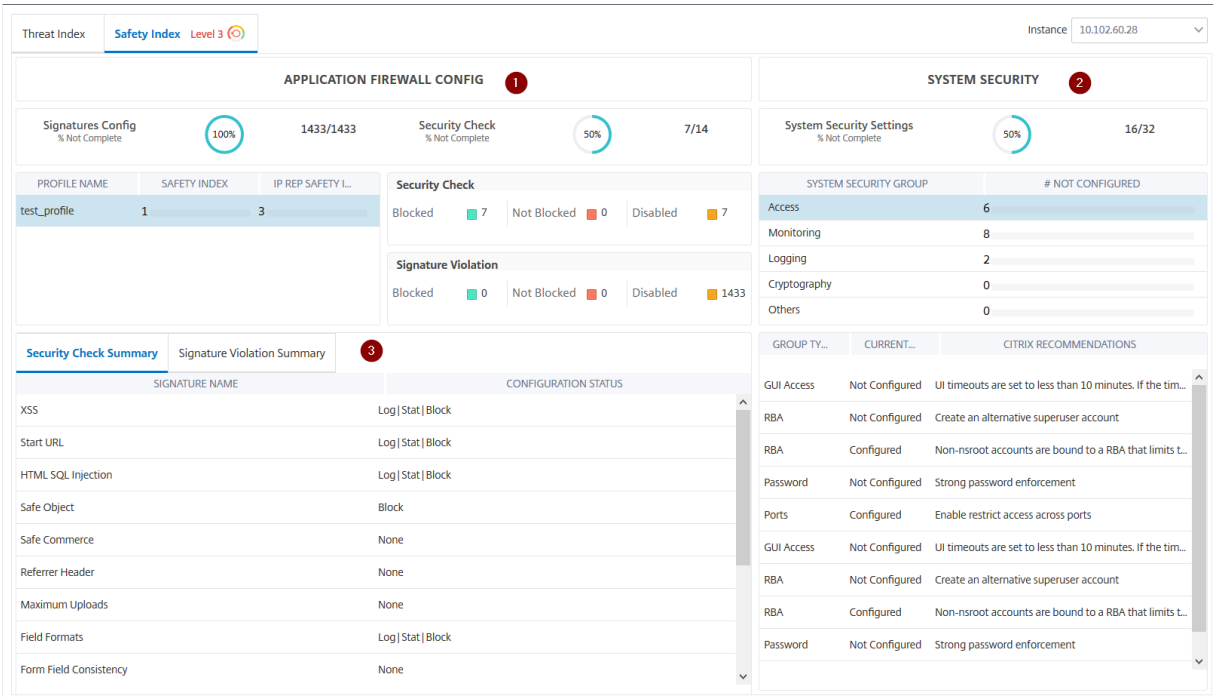
安全性指数概要には、次のセキュリティ構成の有効性に関する情報が表示されます。

- 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 **WAF** セキュリティ違反を有効にし、**[**セキュリティ**] > [**セキュリティ違反] に移動して、脅威環境の概要を表示することもできます。 **

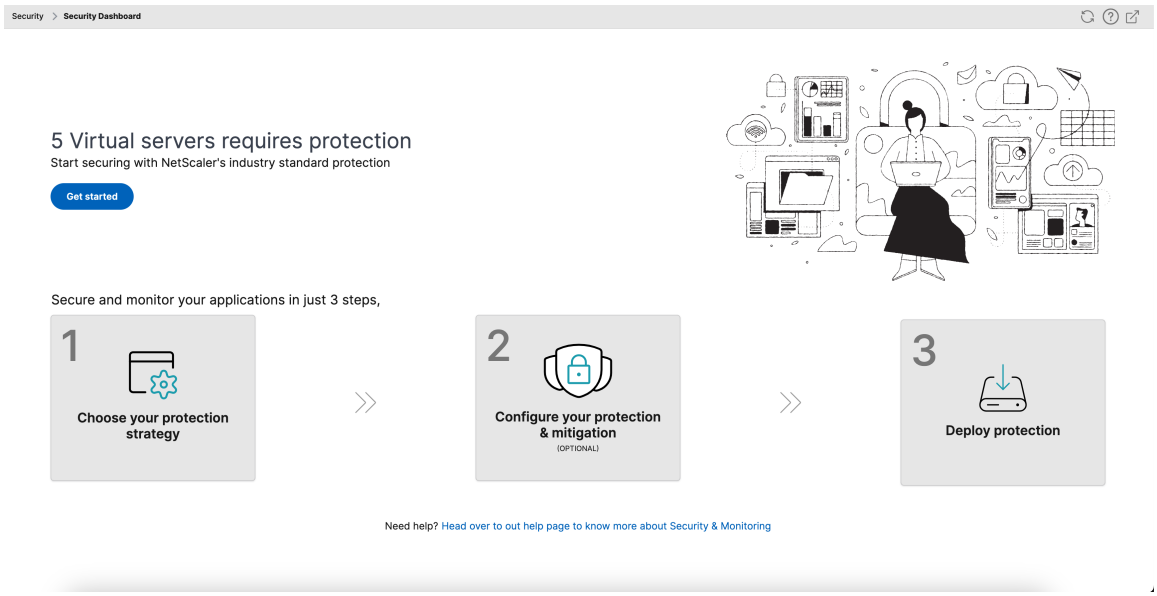
統合セキュリティダッシュボード

February 6, 2024

Unified Security ダッシュボードは、保護の設定、分析の有効化、およびアプリケーションへの保護の展開ができる単一ペインのダッシュボードです。このダッシュボードでは、さまざまなテンプレートオプションから選択して、構成プロセス全体を 1 つのワークフローで完了できます。開始するには、[セキュリティ] **> [**セキュリティダッシュボード] に移動し、[アプリケーションの管理] をクリックします。「アプリケーションの管理」ページでは、セキュリティで保護されたアプリケーションとセキュリティで保護されていないアプリケーションの詳細を表示できます。

> 注:
>
> - 新規ユーザーの場合、または **StyleBooks** または **NetScaler** インスタンスで直接保護を設定していない場合は、**[**セキュリティ**] > [**セキュリティダッシュボード] をクリックすると次のページが表示されま

す。

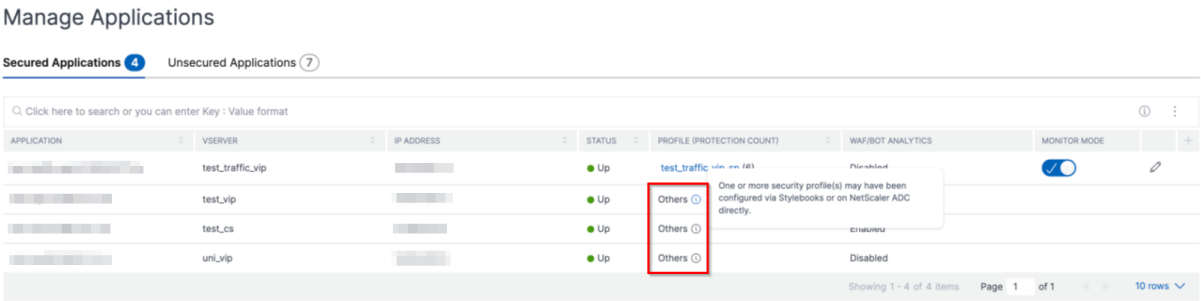


- 保護が必要な仮想サーバーの総数を表示できます。「はじめに」をクリックすると、「セキュリティで保護されていないアプリケーション」の詳細が表示されます。
- 保護を構成する対象となる仮想サーバーの種類は、負荷分散とコンテンツスイッチングです。

セキュリティで保護されたアプリケーション

統合セキュリティダッシュボードを使用して保護を設定すると、詳細を表示できます。詳細については、「セキュリティで保護されていないアプリケーションの保護の設定」を参照してください。

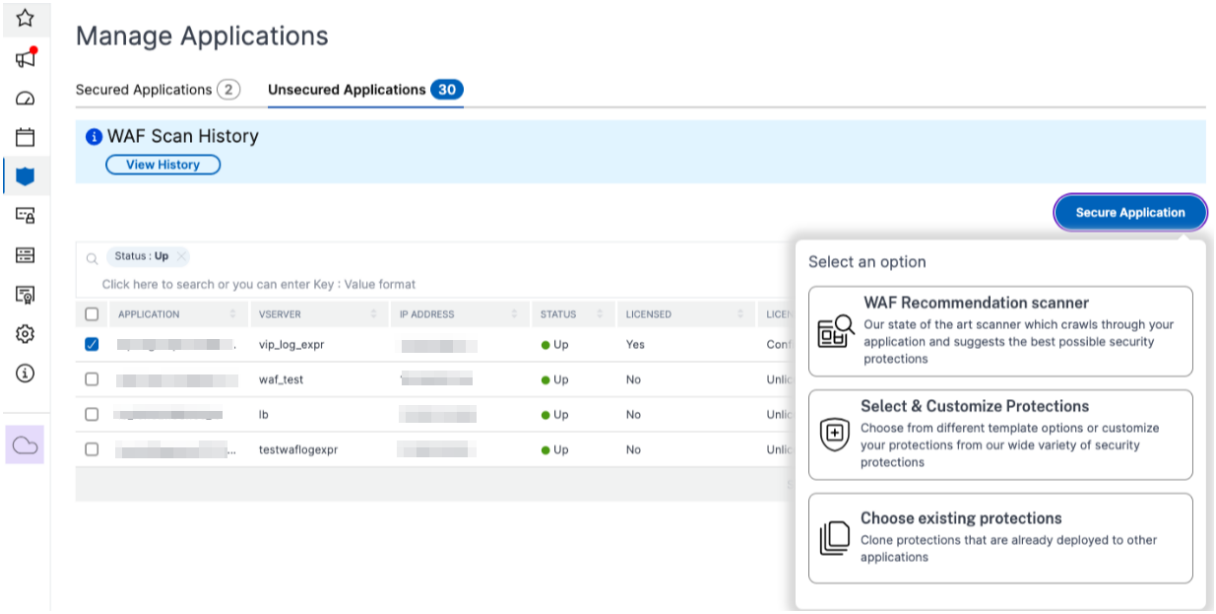
NetScaler インスタンスで直接、または StyleBook を通じて保護を既に設定している場合は、［プロファイル］の［その他］と表示されている［セキュリティで保護されたアプリケーション］タブにアプリケーションを表示できます。



セキュリティで保護されていないアプリケーションの保護を設定

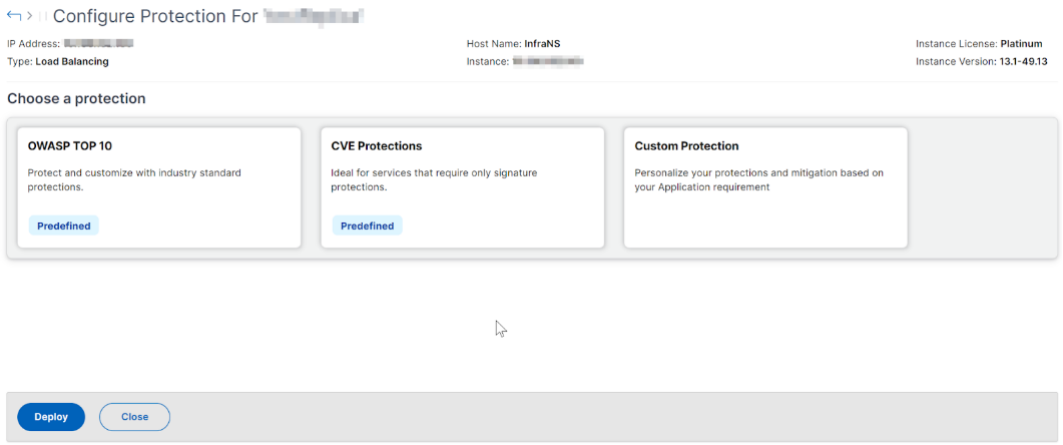
> 注:
>
> ブロックリストでサポートされる構成エンティティ (ルール) の最大数は 32 です。

「セキュリティで保護されていないアプリケーション」タブでアプリケーションを選択し、「セキュリティで保護されたアプリケーション」をクリックします。



アプリケーションを保護するには、次のオプションのいずれかを選択できます:

- **WAF** レコメンデーションスキャナー -このオプションでは、アプリケーションのスキャンを実行できます。スキャンの特定のパラメータに基づいて、結果からアプリケーションの保護が提案されます。これらの推奨事項を適用することを検討してください。
- 保護の選択とカスタマイズ -このオプションでは、さまざまなテンプレートオプションを選択したり、保護をカスタマイズして展開したりできます。



  - **OWASP** トップ **10** -OWASP トップ 10 のセキュリティリスクに対する業界標準の保護機能を備えた事

前定義されたテンプレート。詳しくは、https://owasp.org/www-project-top-ten/ を参照してください。

- **CVE Protections** -既知の脆弱性カテゴリに分類された事前設定されたシグニチャルールのリストからシグニチャセットを作成できます。シグニチャを選択して、シグニチャパターンが着信トラフィックと一致したときのログまたはブロックアクションを設定できます。ログメッセージには脆弱性の詳細が含まれます。
- カスタム保護 -保護を選択し、要件に基づいて導入します。

- 既存の保護を選択 -このオプションは、既存のアプリケーションにデプロイされている保護を複製します。同じ保護機能を別のアプリケーションに展開する場合は、このオプションを選択して、そのまま別のアプリケーションに展開できます。このオプションをテンプレートとして選択し、保護を変更してから展開することもできます。

WAF レコメンデーションスキャナー

> 注:
>
> - 1 つのアプリケーションに対して一度に実行できるスキャンは 1 つだけです。同じアプリケーションまたは別のアプリケーションに対して新しいスキャンを開始するには、前回のスキャンが完了するまで待つ必要があります。
> - [履歴を表示] をクリックすると、過去のスキャンの履歴とステータスを表示できます。[レポートを表示] をクリックして、後で推奨事項を適用することもできます。

前提条件:

- NetScaler インスタンスは 13.0 41.28 以降（セキュリティチェック用）および 13.0 以降（署名用）である必要があります。
- プレミアムライセンスが必要です。
- 負荷分散仮想サーバーでなければなりません。

WAF レコメンデーションスキャンを開始するには、次の情報を提供する必要があります:

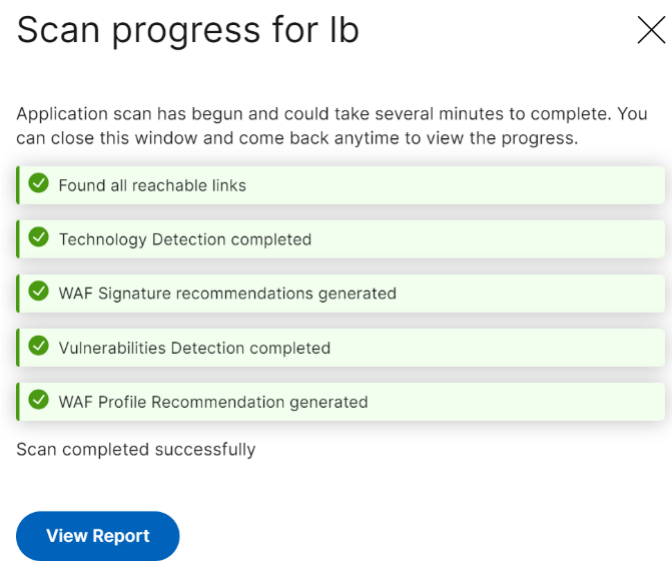
1. スキャンパラメータの下:
   - ドメイン名—アプリケーションに関連付けられている有効でアクセス可能な IP アドレスまたは一般にアクセス可能なドメイン名を指定します。例: www.example.com。
   - **HTTP/HTTPS** プロトコル—アプリケーションのプロトコルを選択します。
   - トラフィックタイムアウト—スキャン中の 1 つのリクエストの待機時間 (秒単位)。値は 0 より大きくなければなりません。

- スキャンを開始する **URL** —スキャンを開始するアプリケーションのホームページ。例: `https://www.example.com/home`。URL は有効な IPv4 アドレスでなければなりません。IP アドレスがプライベートの場合は、NetScaler ADM 管理 IP からプライベート IP アドレスにアクセスできることを確認する必要があります。
- ログイン **URL** —認証のためにログインデータが送信される URL。HTML では、この URL は一般にアクション URL と呼ばれます。
- 認証方法—アプリケーションでサポートされている認証方法 (フォームベースまたはヘッダーベース) を選択します。
  - フォームベース認証では、ログイン認証情報を使用してログイン URL にフォームを送信する必要があります。これらの認証情報は、フォームフィールドとその値の形式である必要があります。次に、アプリケーションは、スキャン中にセッションを維持するために使用されるセッション Cookie を共有します。
  - ヘッダーベースの認証では、ヘッダーセクションに Authentication ヘッダーとその値が必要です。Authentication ヘッダーには有効な値が必要で、スキャン中のセッションを維持するために使用されます。ヘッダーベースの場合、フォームフィールドは空のままにしてください。
- リクエストメソッド—フォームデータをログイン URL に送信するときに使用する HTTP メソッドを選択します。許可されているリクエストメソッドは、**POST**、**GET**、および **PUT** です。
- フォームフィールド—ログイン URL に送信するフォームデータを指定します。フォームフィールドは、フォームベース認証を選択した場合にのみ必須です。キーと値のペアで指定する必要があります。ここで、フィールド名はキー、フィールド値は値です。パスワードを含め、ログインに必要なすべてのフォームフィールドが正しく追加されていることを確認してください。値は、データベースに保存される前に暗号化されます。複数のフォームフィールドを追加するには、「追加」をクリックします。たとえば、フィールド名—ユーザー名、フィールド値—admin などです。
- ログアウト **URL** —アクセス後にセッションを終了する URL を指定します。例: `https://www.example.com/customer/logout`。

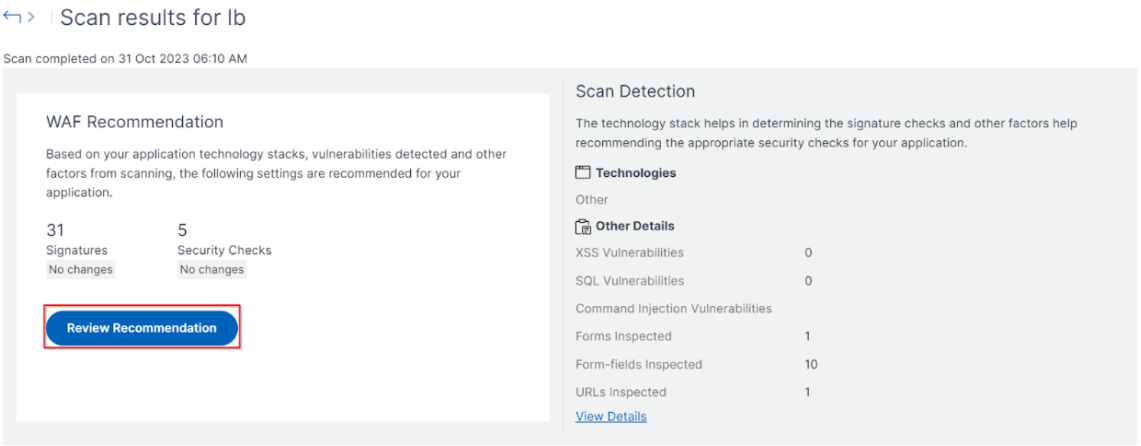
2. [スキャン設定] で:

- チェックする脆弱性—スキャナーが検出する脆弱性を選択します。現在、これは SQL インジェクション違反とクロスサイトスクリプティング違反に対して行われています。デフォルトでは、すべての違反が選択されます。脆弱性を選択した後、アプリケーションに対するこれらの攻撃をシミュレートして潜在的な脆弱性を報告します。実稼働環境以外ではこの検出を有効にすることをお勧めします。アプリケーションに対するこれらの攻撃をシミュレートせずに、他のすべての脆弱性も報告されています。
- レスポンスサイズの上限—レスポンスサイズの上限です。上記の値を超える応答はスキャンされません。推奨制限は 10 MB (1000000 バイト) です。
- 同時リクエスト数—ウェブアプリケーションに並行して送信されたリクエストの総数。

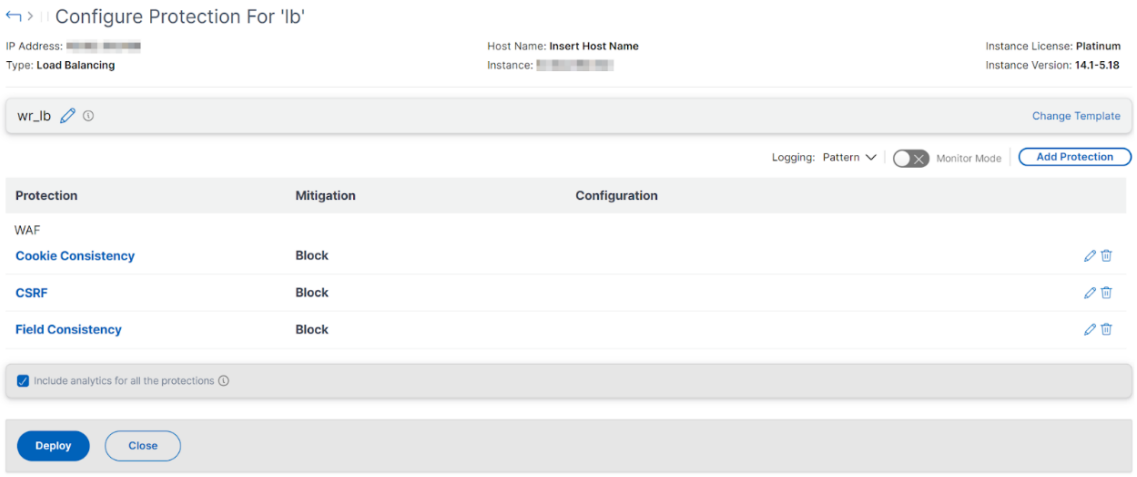
3. WAF スキャンの設定が完了しました。[スキャンの開始] をクリックしてスキャン処理を開始し、進行状況が完了するのを待つことができます。スキャンが完了したら、[レポートを表示] をクリックします。



4. スキャン結果ページで、「推奨内容を確認」をクリックします。



5. 保護を確認するか、他の保護を編集/追加して、「デプロイ」をクリックします。

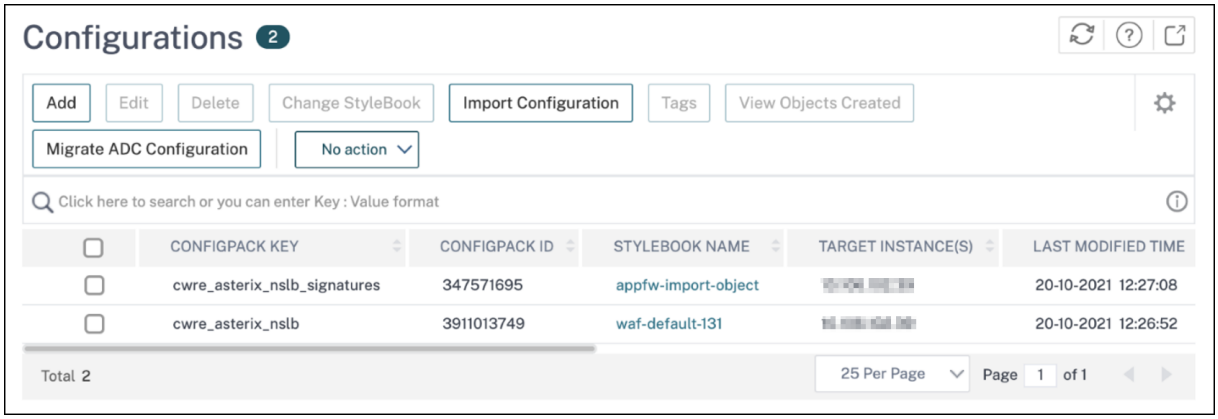


セキュリティーチェックを正常に適用すると：

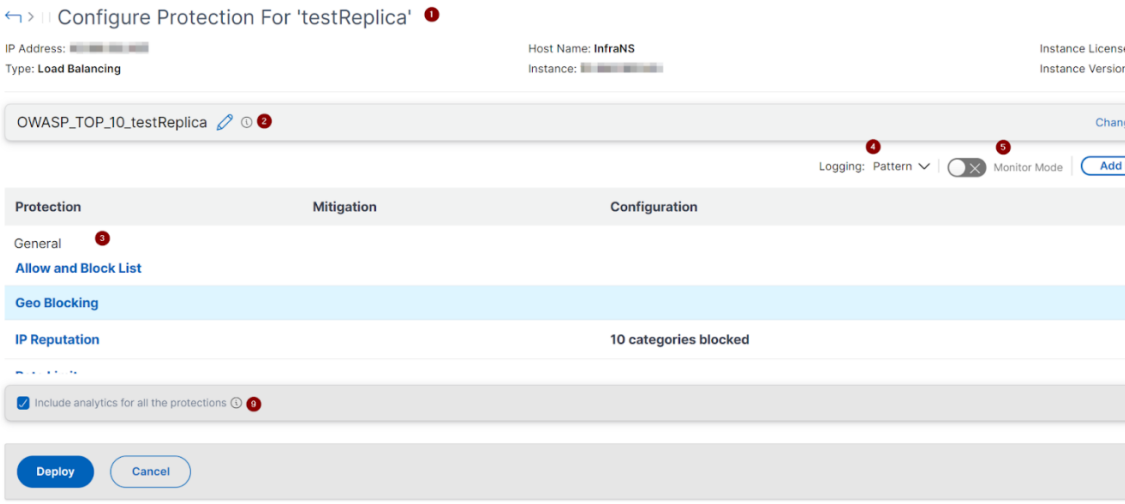
- 構成は、バージョンに応じて StyleBooks を介して NetScaler インスタンスに適用されます。
  - NetScaler 13.0 では、`unified-appsec-protection-130` StyleBook が使用されます。
  - NetScaler 13.1 では、`unified-appsec-protection-131` StyleBook が使用されています。
  - NetScaler 14.1 では、`unified-appsec-protection-141` StyleBook が使用されています。
- `Appfw`プロファイルは NetScaler で作成され、`policylabel`を使用してアプリケーションにバインドされます。
- 推奨シグニチャが既に適用されている場合、シグニチャは appfw プロファイルにバインドされます。

> 注
>
> セキュリティチェックは NetScaler 13.0 41.28 以降のバージョンでサポートされています。

WAF プロファイルと署名がデフォルトの StyleBooks で適用されていることを確認するには、「アプリケーション」**>**「構成」**>**「構成パック」に移動します。



保護機能の選択とカスタマイズ



OWASP トップ **10**

1 -IP アドレス、仮想サーバーのタイプ、ライセンスの種類、アプリケーションが構成されているインスタンスなど、アプリケーションに関する情報を提供します。

2 -選択したテンプレートを表示します。必要に応じて名前を変更できます。

3 -保護を表示します。一部の保護には追加情報が必要です。

4 -詳細ログタイプを表示します。次のオプションを選択できます:

- [パターン]。違反パターンのみをログに記録します。
- パターンペイロード。違反パターンと 150 バイトの余分な JSON ペイロードをログに記録します。
- パターン、ペイロード、ヘッダー。違反パターン、150 バイトの追加 JSON ペイロード、および HTTP ヘッダー情報をログに記録します。

5 -監視モードを有効にできます。監視モードを有効にすると、トラフィックは記録されるだけで、緩和策は有効になりません。

6 -保護機能をさらに追加できます。「保護を追加」をクリックし、内容を確認して追加してください。

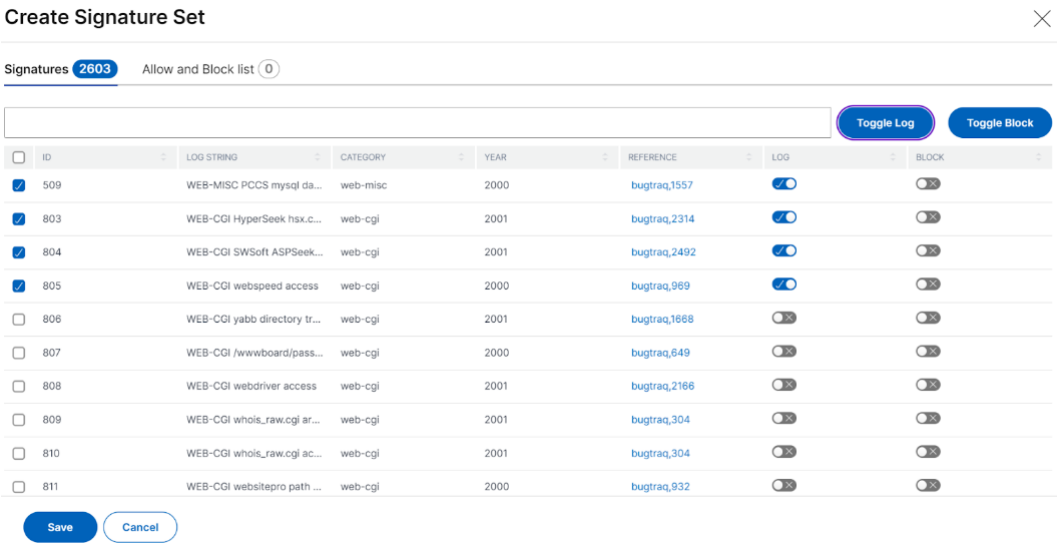
7 -「テンプレートの変更」オプションを使用して新しいテンプレートを選択できます。

8 -保護を編集または削除できます。

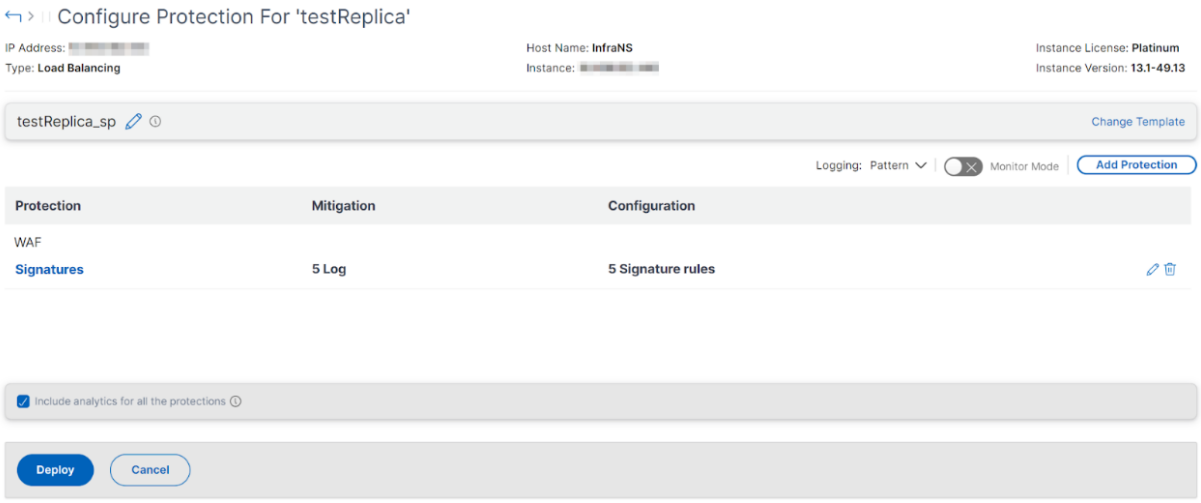
9 -選択した保護の分析を有効にします。このオプションはデフォルトで選択されています。設定された保護の分析は、[セキュリティ] **>** [セキュリティ違反] で確認できます。

保護を設定したら、「デプロイ」をクリックします。

CVE プロテクション　CVE 保護を展開するには、「CVE 保護の作成」をクリックします。「署名セットの作成」ページで、ログまたはブロックアクションを設定する署名をリストから選択し、「保存」をクリックします。

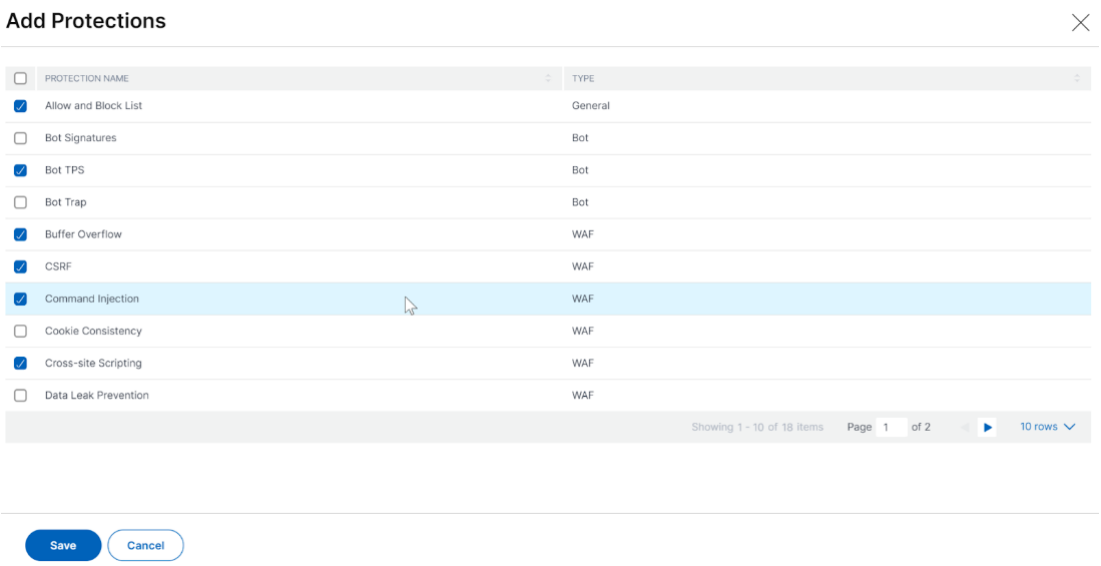


「保存」をクリックすると、設定ページに追加された署名が表示されます。



「保護を追加」をクリックして、アプリケーションにさらに保護を追加することもできます。すべての保護を設定したら、「デプロイ」をクリックします。

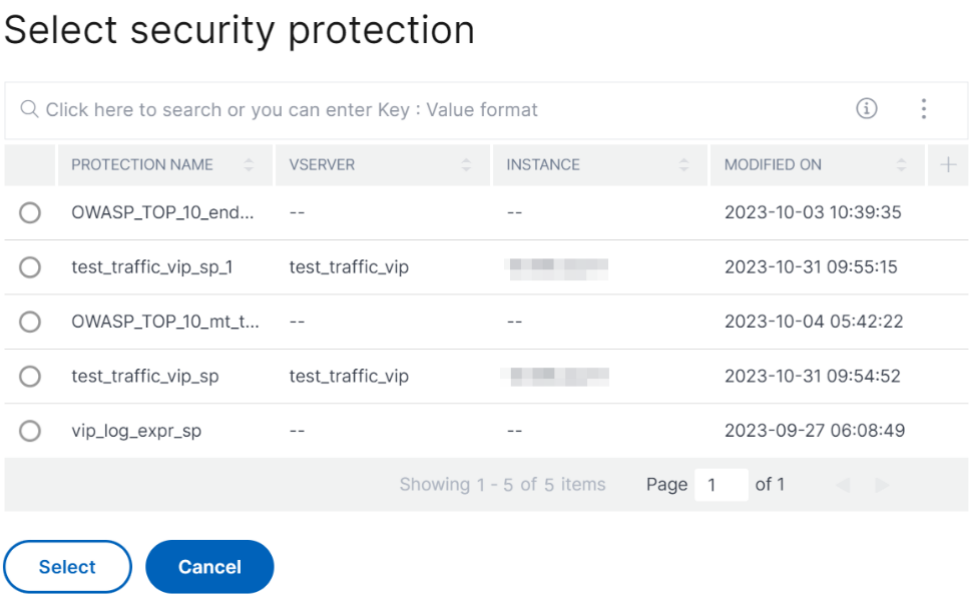
カスタム保護　要件に基づいて保護機能を導入するには、「新しい保護を作成」をクリックします。「保護の追加」ページで、導入する保護を選択し、「保存」をクリックします。



「保存」をクリックした後、構成ページで選択した保護を確認し、「デプロイ」をクリックします。

既存の保護を選択

あるアプリケーションから別のアプリケーションに既存の保護を展開するには、リストから既存の保護を選択します。



保護を選択すると、既存の保護が複製され、構成ページに表示されます。要件に基づいて変更し、「デプロイ」をクリックします。

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。単一ペインソリューションの [セキュリティ] **>** [セキュリティ違反] に移動し、次の操作を行います。

- WAF セキュリティ違反とボットセキュリティ違反の両方に関連する脅威の詳細を完全に可視化して、アプリケーションを視覚化
- 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、メトリックスコレクター 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。

Splunk との統合

February 6, 2024

NetScaler ADM を Splunk と統合して、以下の分析を表示できるようになりました。

- WAF 違反
- ボット違反
- SSL 証明書インサイト
- イベントと指標

Splunk アドオンにより、次のことが可能になります。

- 他のすべての外部データソースを結合します。
- 一元化された場所で分析の可視性を高めます。

NetScaler ADM はボット、WAF、SSL イベントを収集し、定期的に Splunk に送信します。Splunk 共通情報モデル (CIM) アドオンは、イベントを CIM 互換データに変換します。管理者は CIM 互換データを使用して、Splunk ダッシュボードでイベントを表示できます。

統合を成功させるには、次のことを行う必要があります。

- NetScaler ADM からデータを受信するように Splunk を設定
- データを Splunk にエクスポートするように NetScaler ADM を設定する
- Splunk のダッシュボードを表示する

NetScaler ADM からデータを受信するように **Splunk** を設定

Splunk では、次のことを行う必要があります。

1. Splunk HTTP イベントコレクターエンドポイントをセットアップしてトークンを生成する
2. Splunk 共通情報モデル (CIM) アドオンをインストールする
3. CIM ノーマライザーのインストール (WAF とボットインサイトにのみ適用)
4. Splunk でサンプルダッシュボードを用意する

Splunk HTTP イベントコレクターエンドポイントをセットアップしてトークンを生成する

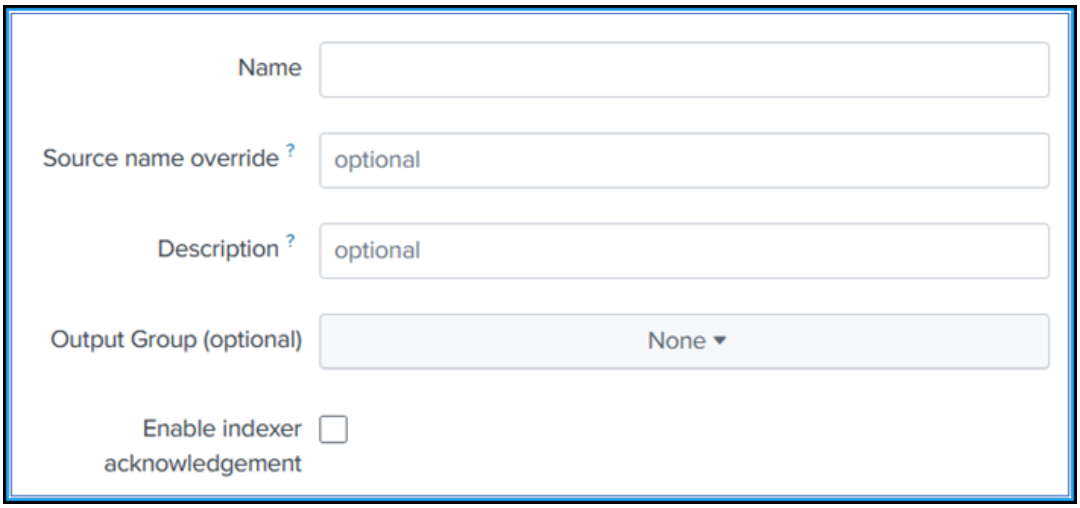
最初に Splunk で HTTP イベントコレクターを設定する必要があります。この設定により、ADM と Splunk を統合してデータを送信できます。次に、Splunk で次のことを行うためのトークンを生成する必要があります。

- ADM と Splunk 間の認証を有効にします。
- イベントコレクターエンドポイントを介してデータを受信します。

1. Splunk にログオンします。
2. [設定**] > [**データ入力**] > [HTTP** イベントコレクター] に移動し、[新規追加] をクリックします。
3. 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) ソース名の上書き **(**オプション**):** 値を設定すると、HTTP イベントコレクターのソース値が上書きされます。
    c) 説明 **(**オプション**):** 説明を指定します。

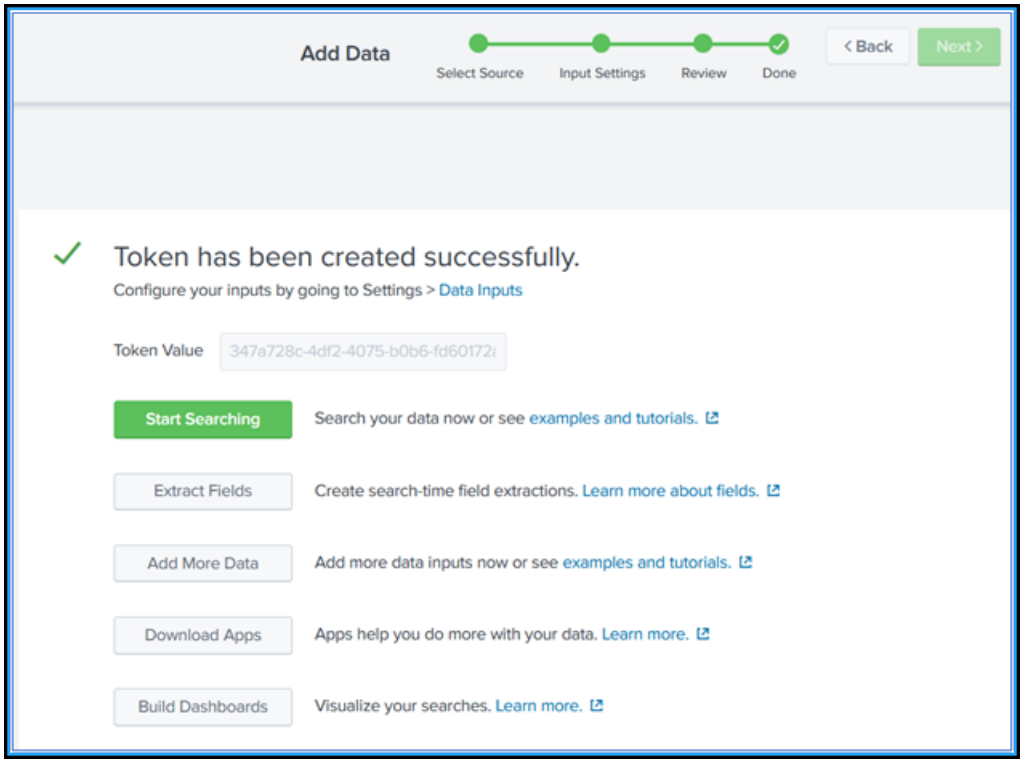
d) 出力グループ **(**オプション**)**: デフォルトでは、このオプションは「なし」に設定されています。

e) インデクサーの確認を有効にする: デフォルトでは、このオプションは選択されていません。



4. [次へ] をクリックします。
5. オプションで、入力設定ページで追加の入力パラメータを設定できます。
6. 「確認」をクリックして入力内容を確認し、「送信」をクリックします。

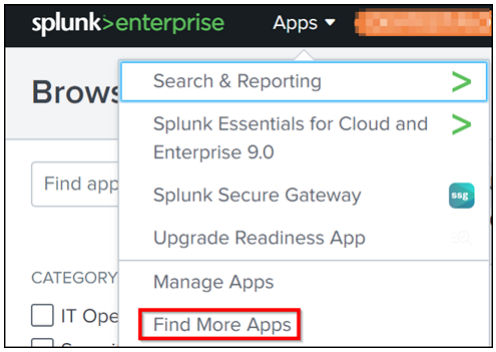
   トークンが生成されます。NetScaler ADM で詳細を追加するときは、このトークンを使用する必要があります。



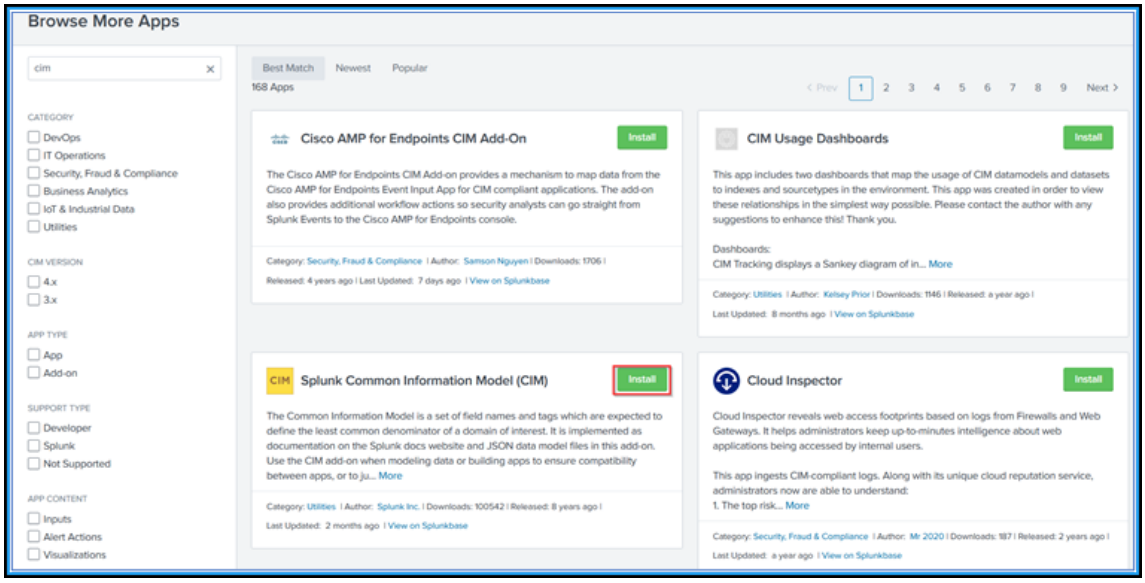
Splunk 共通情報モデルのインストール

Splunk では、Splunk CIM アドオンをインストールする必要があります。このアドオンにより、NetScaler ADM から受信したデータが取り込まれたデータを正規化し、同等のイベントに対して同じフィールド名とイベントタグを使用して共通の標準に一致するようにします。

1. Splunk にログオンします。
2. [アプリ] **>** [その他のアプリを検索] に移動します。



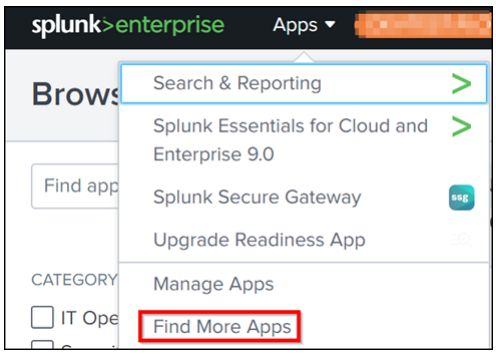
3. 検索バーに **CIM** と入力し、**Enter** キーを押して **Splunk** 共通情報モデル **(CIM)** アドオンを取得し、[インストール] をクリックします。



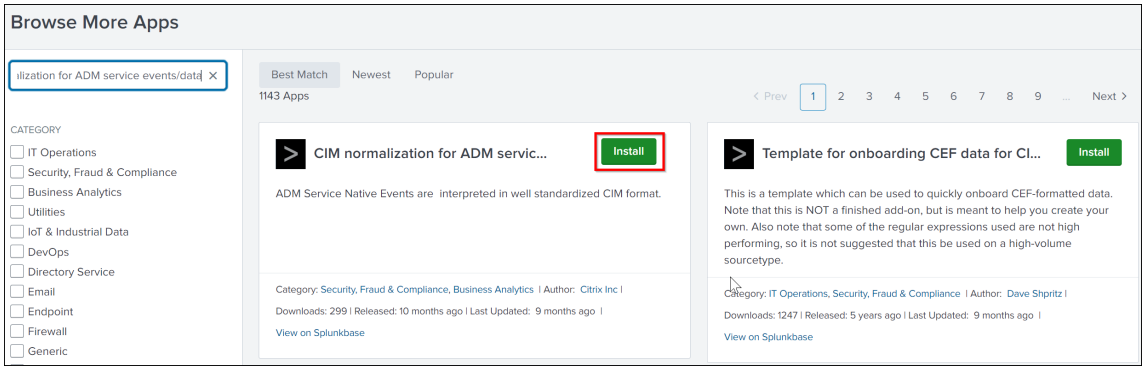
CIM ノーマライザーのインストール

CIM ノーマライザーは、Splunk で WAF とボットのインサイトを表示するためにインストールする必要がある追加プラグインです。

1. Splunk ポータルで、[アプリ] **>** [その他のアプリを検索] に移動します。



2. 検索バーに「ADM サービスイベント/データの CIM 正規化」と入力し、Enter キーを押してアドオンを入手し、**[インストール]** をクリックします。



Splunk でサンプルダッシュボードを用意する

Splunk CIM をインストールしたら、WAF と Bot、SSL 証明書のインサイト、イベントとメトリクスのテンプレートを使用してサンプルダッシュボードを準備する必要があります。ダッシュボードテンプレート (`.tgz`) ファイルをダウンロードし、任意のエディター (メモ帳など) を使用してその内容をコピーし、データを Splunk に貼り付けてダッシュボードを作成できます。

> 注:
>
> サンプルダッシュボードを作成する以下の手順は、すべてのユースケースに適用できます。必要な`json`ファイルを使用する必要があります。

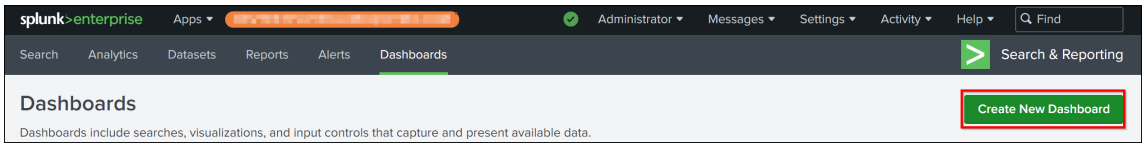
1. Citrix のダウンロードページにログオンし、「サードパーティ製エンドポイントのサンプルダッシュボード」にあるサンプルダッシュボードをダウンロードします。
2. `json`ファイルを抽出し、任意のエディターを使用してファイルを開き、ファイルからデータをコピーします。

   解凍すると、3 つの`json`ファイルが作成されます。以下を使用してください。

   - WAF と Bot のサンプルダッシュボードを作成するための`adm_splunk_security_violations.json`ファイル。
   - SSL 証明書インサイトサンプルダッシュボードを作成するための`adm_splunk_ssl_certificate.json`ファイル。

- ADM イベントとメトリクスダッシュボードを作成するための`adm_splunk_events_and_metrics_hist.json`ファイル。

3. Splunk ポータルで、[検索とレポート**] > [**ダッシュボード] に移動し、[新しいダッシュボードの作成] をクリックします。



4.「ダッシュボードの新規作成」ページで、次のパラメータを指定します。

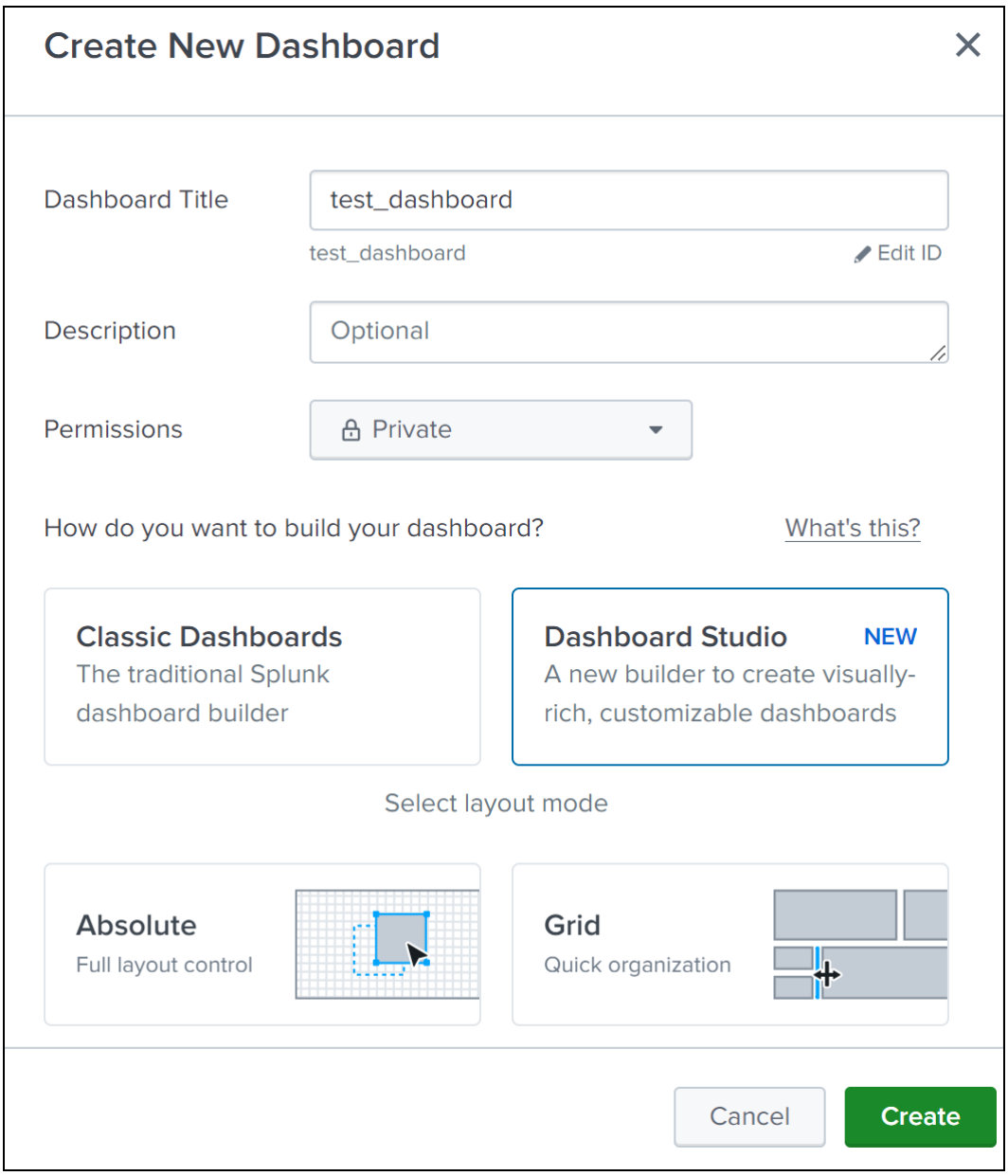
a) ダッシュボードタイトル -任意のタイトルを入力します。

b) 説明 -必要に応じて、参照用の説明を入力できます。

c) 権限 -要件に応じて [非公開] または [アプリ内で共有] を選択します。

d) [ダッシュボード **Studio**] を選択します。

e) 任意のレイアウト ([絶対] または [グリッド]) を選択し、[作成] をクリックします。

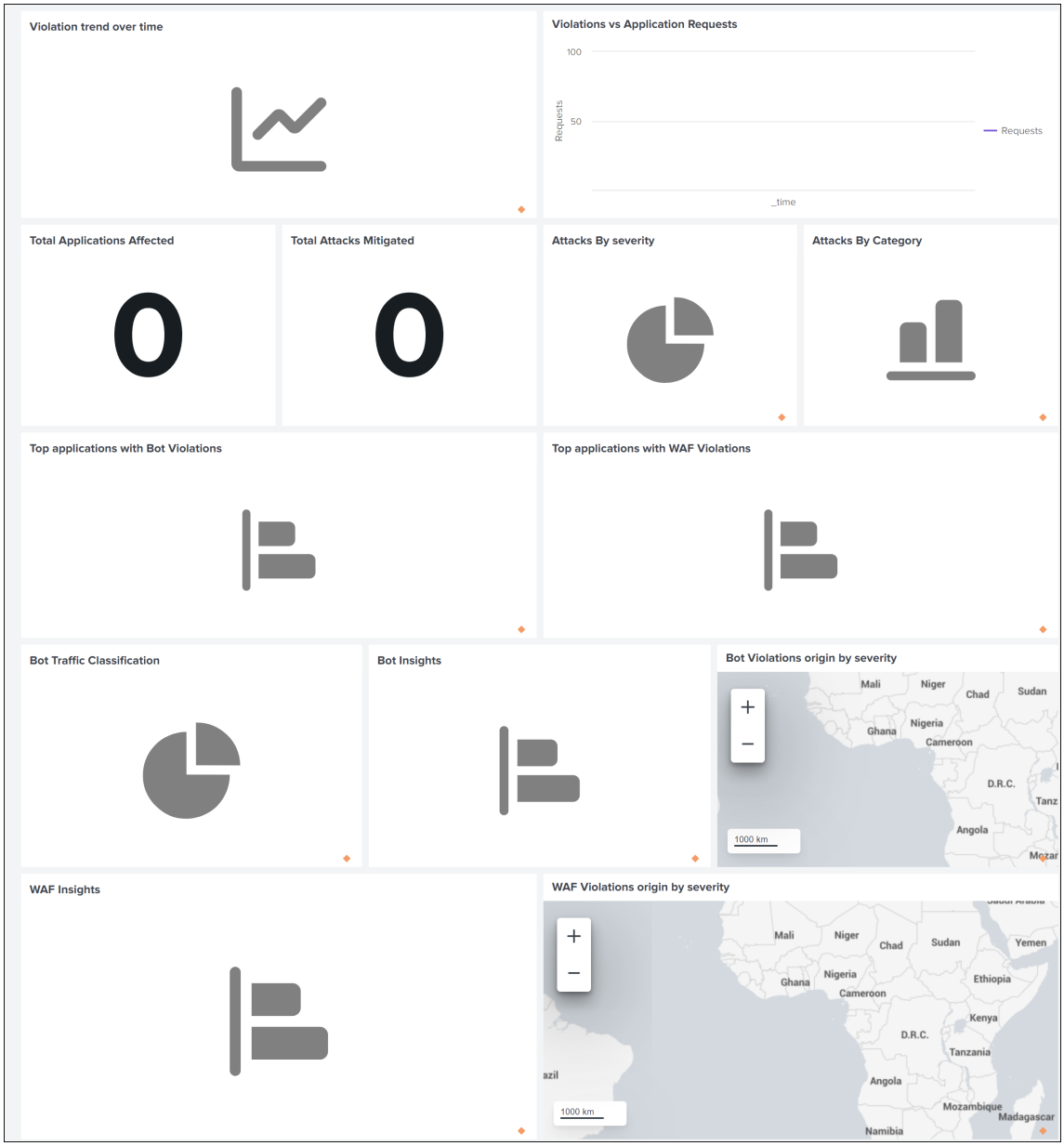


「作成」をクリックした後、レイアウトから「ソース」アイコンを選択します。

5. 既存のデータを削除し、ステップ 2 でコピーしたデータを貼り付けて、[戻る] をクリックします。
6. [保存] をクリックします。

   サンプルダッシュボードを表示できます。

   以下は、WAF と bot のサンプルダッシュボードの例です。



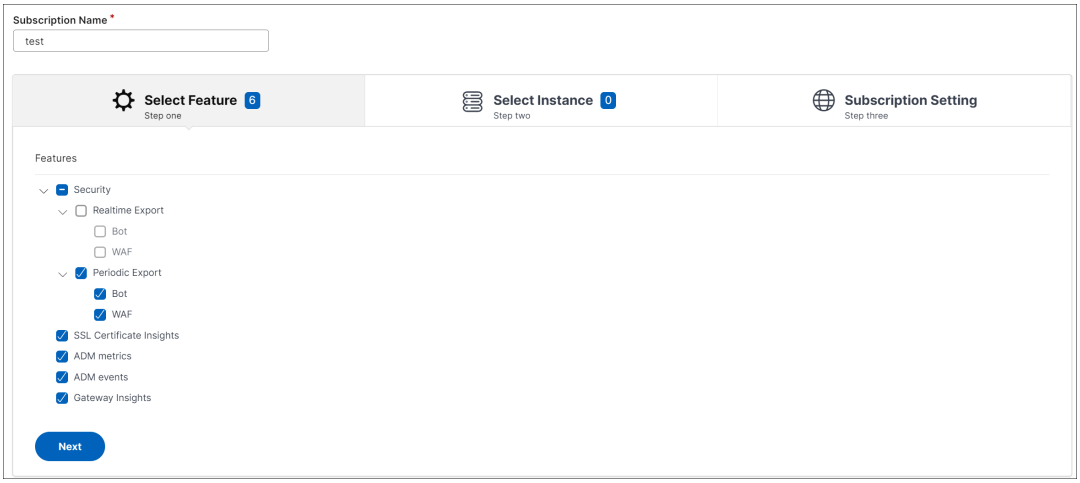
データを **Splunk** にエクスポートするように **NetScaler ADM** を設定する

これで、Splunk ですべての準備が整いました。最後のステップは、サブスクリプションを作成してトークンを追加することによって NetScaler ADM を構成することです。

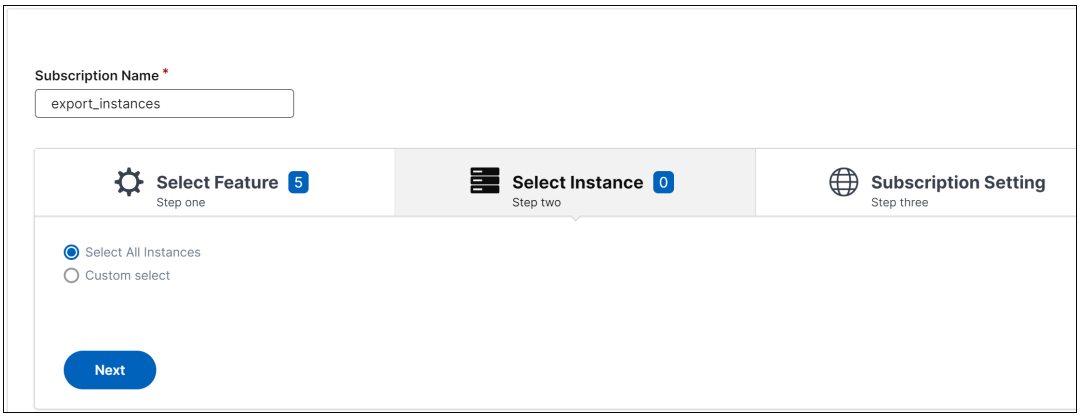
次の手順を完了すると、NetScaler ADM で現在使用可能な更新されたダッシュボードを Splunk で表示できます。

1. NetScaler ADM にログオンします。
2. [設定] **>** **[**エコシステム統合**]** に移動します。
3. 「購読」ページで、「追加」をクリックします。

4. [サブスクリプション名] フィールドに任意の名前を指定します。
5. [機能の選択] タブでは、エクスポートする機能を選択し、[次へ] をクリックできます。
   - リアルタイムエクスポート -選択した違反は直ちに Splunk にエクスポートされます。
   - 定期エクスポート -選択した違反が、選択した期間に従って Splunk にエクスポートされます。



6. [インスタンスの選択] タブでは、[すべてのインスタンスを選択] または [カスタム選択] を選択し、[次へ] をクリックします。
   - すべてのインスタンスを選択 -すべての NetScaler インスタンスから Splunk にデータをエクスポートします。
   - カスタム選択-一覧から **NetScaler** インスタンスを選択できます。リストから特定のインスタンスを選択した場合、データは選択した NetScaler インスタンスからのみ Splunk にエクスポートされます。



7. 「サブスクリプション設定」タブでは:
   a) エンドポイントタイプ—**Splunk** を選択します。
   b) エンドポイント **URL** —Splunk エンドポイントの詳細を指定します。終点はhttps://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/eventの形式でなければなりません。

> 注
>
> セキュリティ上の理由から HTTPS を使用することをお勧めします。

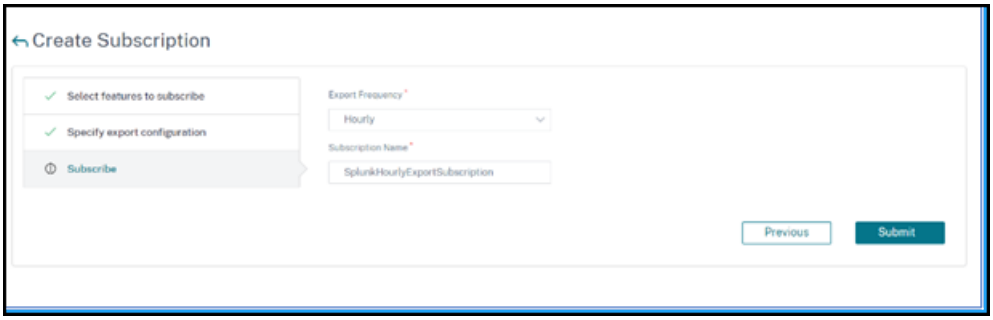
- **SPLUNK_PUBLIC_IP** —Splunk に設定された有効な IP アドレス。
- **SPLUNK_HEC_PORT** —HTTP イベントエンドポイントの設定時に指定したポート番号を示します。デフォルトのポート番号は 8088 です。
- サービス/コレクター/イベント—HEC アプリケーションのパスを示します。

c) 認証トークン—Splunk ページから認証トークンをコピーして貼り付けます。

d) 頻度を選択 -リストから「毎日」または「毎時」を選択します。選択内容に基づいて、NetScaler ADM は詳細を Splunk にエクスポートします。

> 注
>
> 定期エクスポートで違反を選択した場合にのみ適用されます。

e) [**Submit**] をクリックします。



> 注
>
> - **Periodic Export** オプションで初めて設定すると、選択した機能のデータが直ちに Splunk にプッシュされます。次のエクスポート頻度は、選択内容に基づいて行われます (毎日または毎時)。
> - リアルタイムエクスポートオプションで初めて構成すると、NetScaler ADM で違反が検出されるとすぐに、選択した機能のデータがすぐに Splunk にプッシュされます。

Splunk のダッシュボードを表示する

NetScaler ADM で構成を完了すると、データが NetScaler ADM からエクスポートされ、イベントが Splunk に表示されます。

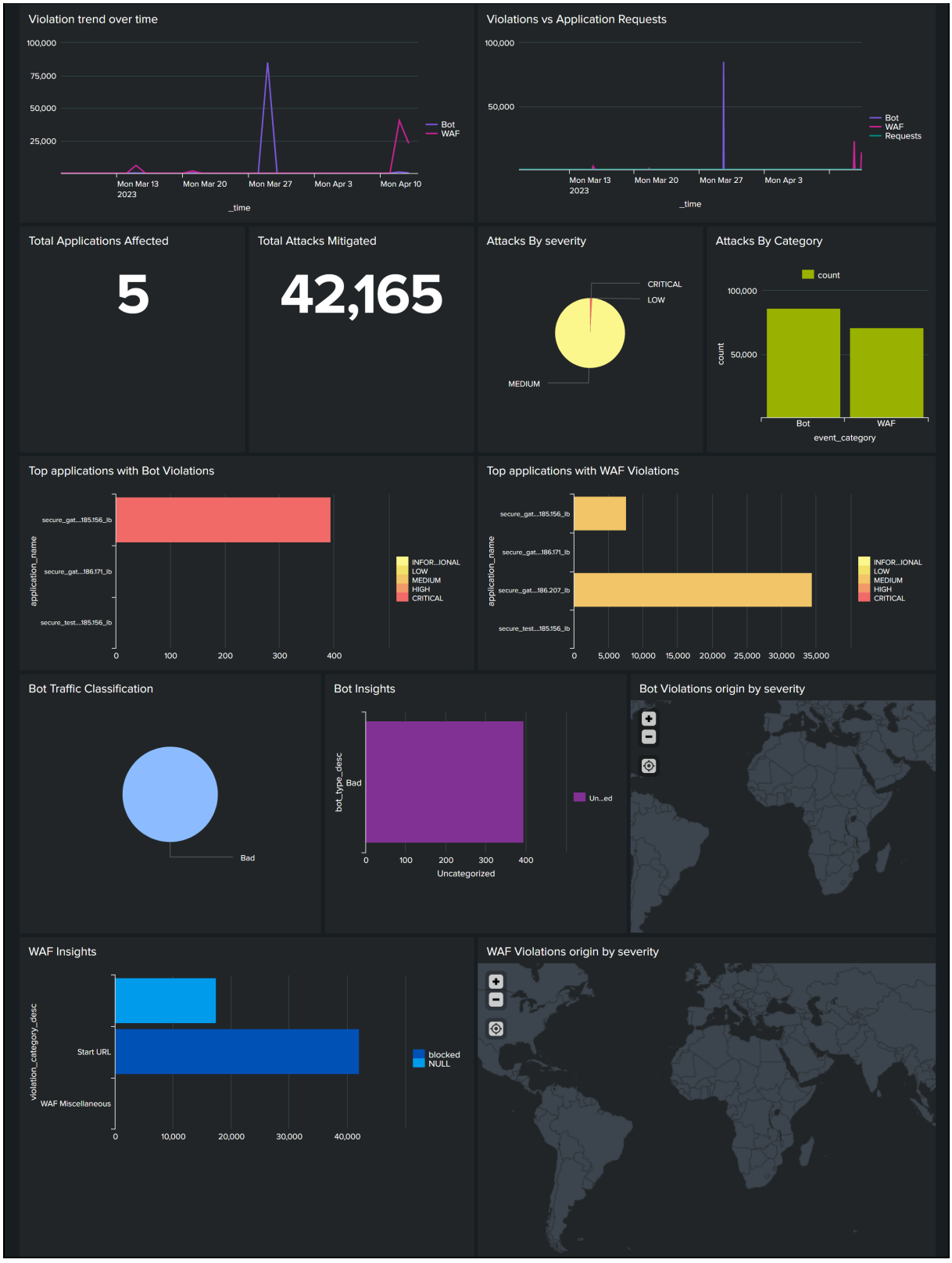
> 注:

> 更新された SSL 証明書インサイトデータを Splunk ですぐに表示するには、NetScaler ADM SSL ダッシュボード（インフラストラクチャ SSL ダッシュボード）で「今すぐ投票」をクリックします。

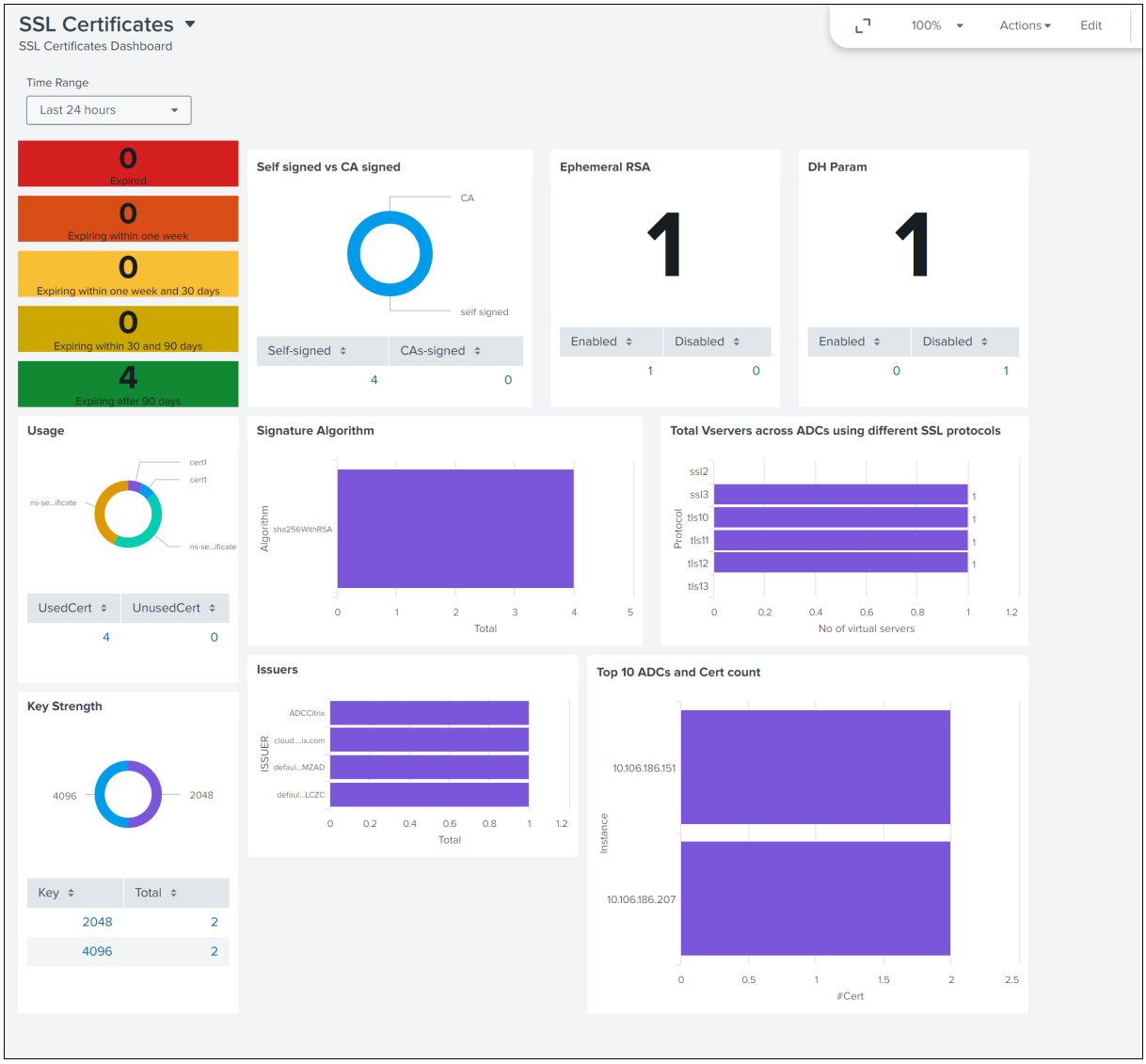
これで、追加の手順なしに、更新されたダッシュボードを Splunk で表示する準備が整いました。

Splunk に移動し、作成したダッシュボードをクリックすると、更新されたダッシュボードが表示されます。

以下は、更新された WAF とボットのダッシュボードの例です。

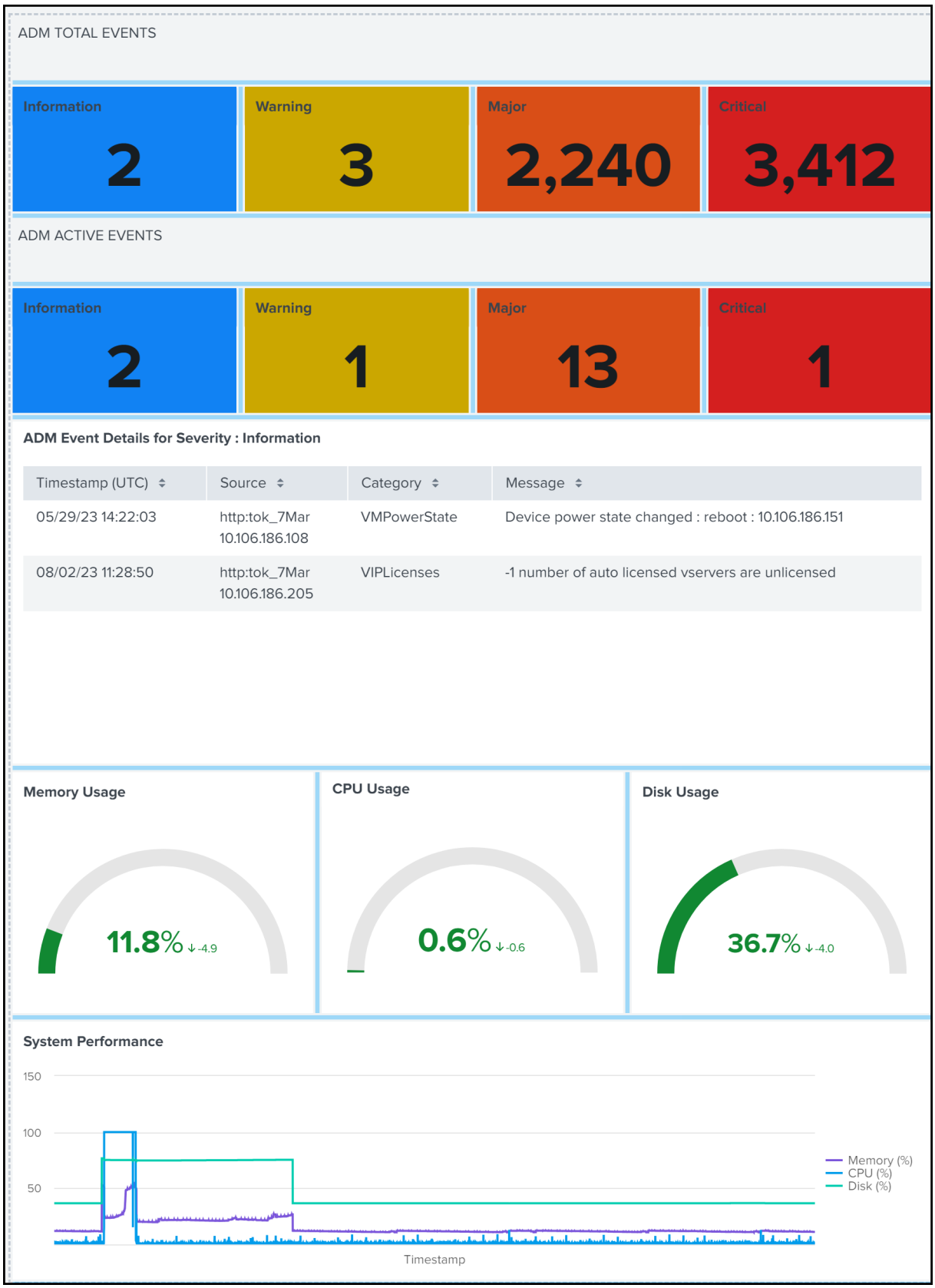


次のダッシュボードは、更新された SSL 証明書インサイトダッシュボードの例です。



次のダッシュボードは、更新されたイベントとメトリクスダッシュボードの例です。

> 注:
>
> メモリ、CPU、ディスクの使用状況データには、NetScaler ADM の現在の値が表示されます。これらの値の上昇傾向と下降傾向は、5 分ごとの前回の値の比較に基づいて表示されます。



ダッシュボードとは別に、サブスクリプションの作成後に Splunk でデータを表示することもできます。

1. Splunk で [検索とレポート] をクリックします。
2. 検索バーで:
    - `sourcetype="metrics"`を入力してリストから期間を選択すると、ADM メトリクスデータが表示されます。
    - ADM イベントデータを表示するには、`sourcetype="event"`を入力してリストから期間を選択します。
    - `sourcetype="bot"`または`sourcetype="waf"`を入力してリストから期間を選択すると、Bot/WAF データが表示されます。
    - SSL 証明書のインサイトデータを表示するには、`sourcetype="ssl"`を入力してリストから期間を選択します。

New Relic との統合

February 6, 2024

NetScaler ADM を New Relic と統合して、WAF および Bot 違反の分析を New Relic ダッシュボードに表示できるようになりました。この統合により、次のことが可能になります。

- New Relic ダッシュボードで他のすべての外部データソースを組み合わせます。
- アナリティクスを一元的に可視化できます。

NetScaler ADM はボットイベントと WAF イベントを収集し、リアルタイムで、またはお客様の選択に基づいて定期的に New Relic に送信します。管理者は、New Relic ダッシュボードで Bot イベントと WAF イベントを確認することもできます。

前提条件

統合を成功させるには、次のことを行う必要があります。

- New Relic のイベントエンドポイントを以下の形式で取得します。

  ```
  https://insights-collector.newrelic.com/v1/accounts/<account_id>/events
  ```

  イベントエンドポイントの設定の詳細については、New Relic のドキュメントを参照してください。

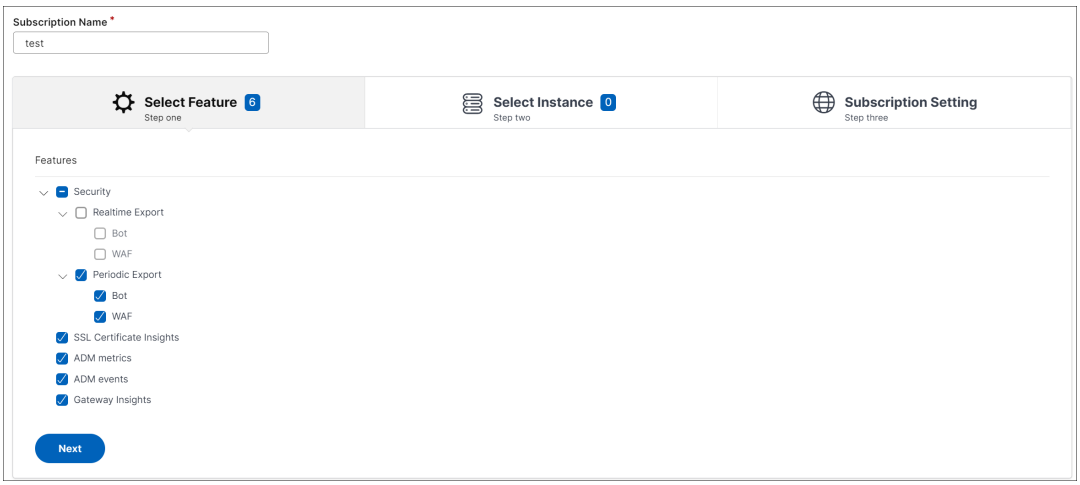
  アカウント ID の取得について詳しくは、New Relic のドキュメントを参照してください。

- New Relic キーを入手してください。詳細については、New Relic のドキュメントを参照してください。
- NetScaler ADM に重要な詳細情報を追加します

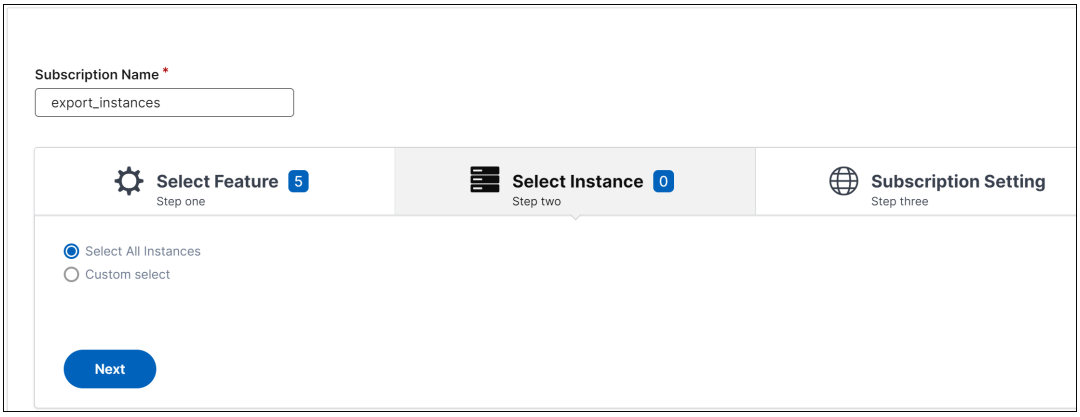
NetScaler ADM に重要な詳細情報を追加します

トークンを生成したら、NetScaler ADM に詳細を追加して New Relic と統合する必要があります。

1. NetScaler ADM にログオンします。
2. [設定] **>** **[**エコシステム統合**]** に移動します。
3. 「購読」ページで、「追加」をクリックします。
4. **[**機能の選択] タブで、エクスポートする機能を選択し、[次へ] をクリックします。
    - リアルタイムエクスポート -選択した違反はすぐに New Relic にエクスポートされます。
    - 定期エクスポート -選択した違反は、選択した期間に基づいて New Relic にエクスポートされます。



5. **[**インスタンスの選択] タブでは、[すべてのインスタンスを選択**]** または [カスタム選択**]** を選択し、[次へ] をクリックします。
    - すべてのインスタンスを選択 -すべての NetScaler インスタンスから New Relic にデータをエクスポートします。
    - カスタム選択**-**一覧から **NetScaler** インスタンスを選択できます。リストから特定のインスタンスを選択した場合、データは選択した NetScaler インスタンスからのみ New Relic にエクスポートされます。



6. 「サブスクリプション設定」タブでは:

   a) エンドポイントタイプ—**New Relic** を選択します。

   b) エンドポイント **URL** —New Relic エンドポイントの詳細を指定します。終点は`https://insights-collector.newrelic.com/v1/accounts/<account_id>/events`の形式でなければなりません。

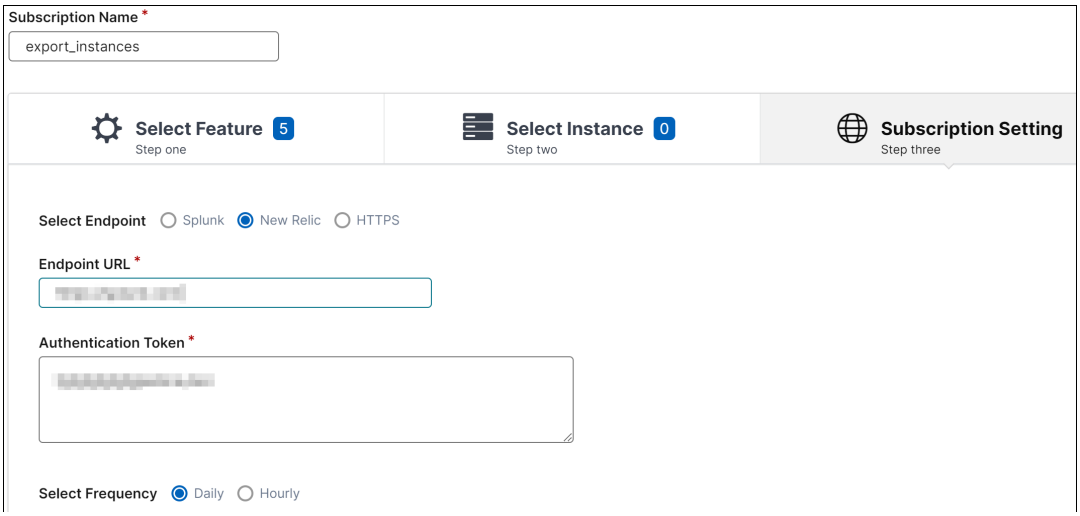
   > 注
   >
   > セキュリティ上の理由から HTTPS を使用することをお勧めします。

   c) 認証トークン—New Relic ページから認証トークンをコピーして貼り付けます。

   d) 頻度を選択 -リストから「毎日」または「毎時」を選択します。選択に基づいて、NetScaler ADM は詳細を New Relic にエクスポートします。

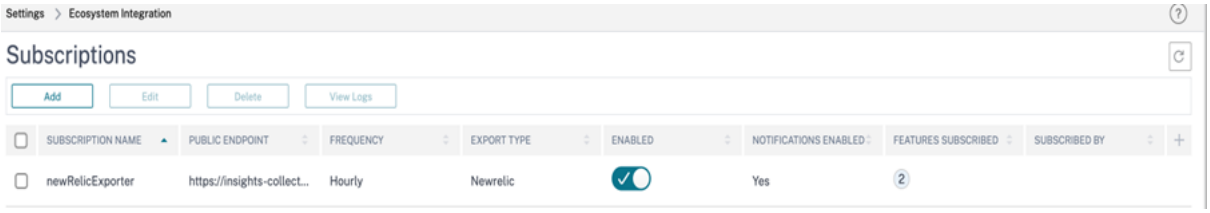
   > 注
   >
   > 定期エクスポートで違反を選択した場合にのみ適用されます。

   e) [**Submit**] をクリックします。



> 注
>
> - 定期エクスポートオプションを使用して初めて設定すると、選択した機能データがすぐに New Relic にプッシュ配信されます。次のエクスポート頻度は、選択内容に基づいて行われます (毎日または毎時)。
> - リアルタイムエクスポートオプションを使用して初めて設定する場合、NetScaler ADM で違反が検出されるとすぐに、選択した機能データが New Relic にプッシュ配信されます。

設定は完了です。詳細は「購読」ページで確認できます。

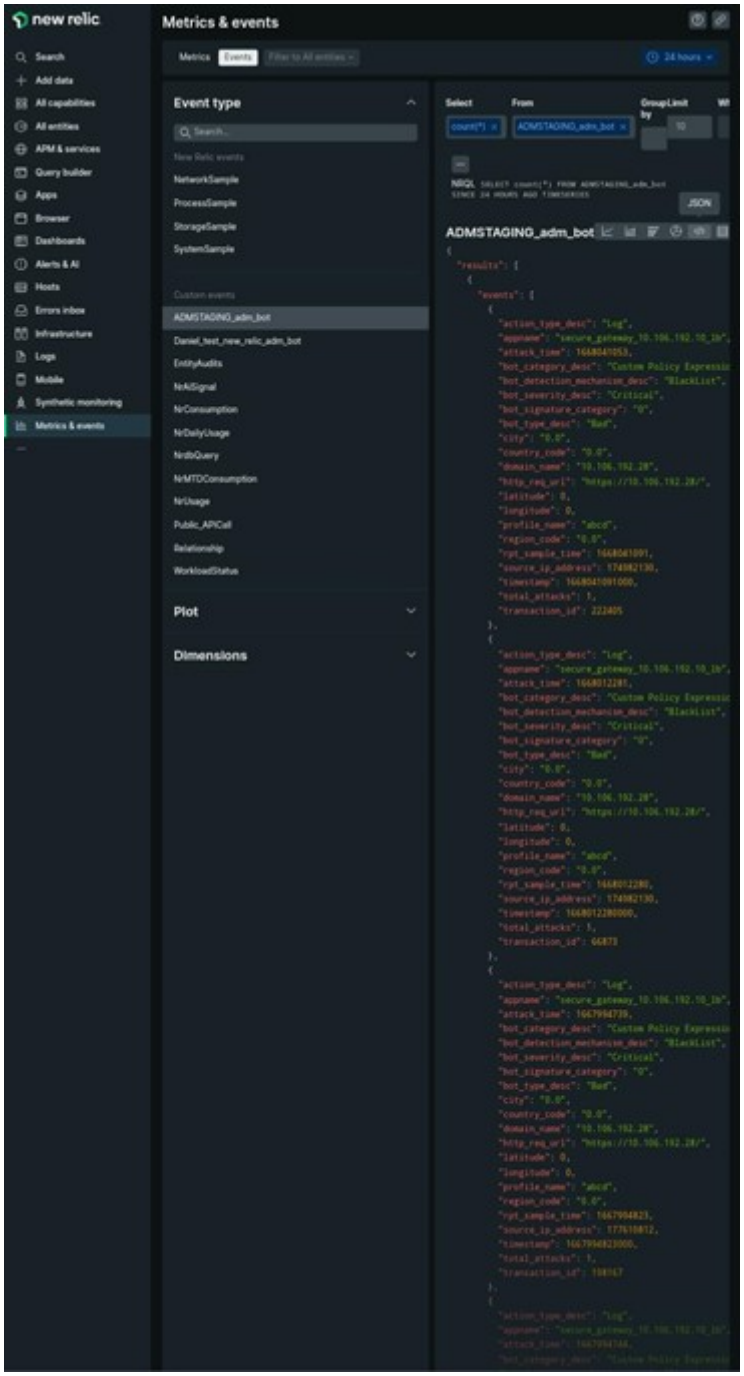


New Relic ダッシュボード

イベントが New Relic にエクスポートされると、次の JSON 形式でメトリクスとイベントの下にイベントの詳細が表示されます。

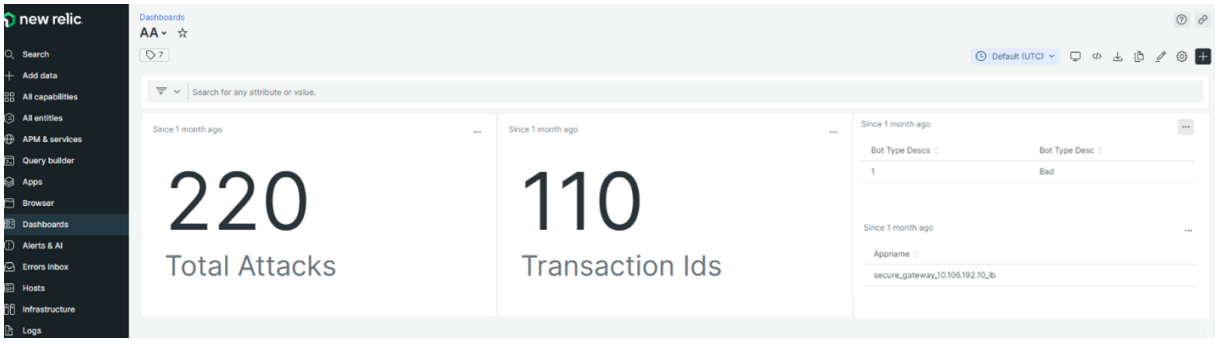
<subsription_name>_adm_<event name> イベント名には Bot、WAF などを使用できます。

次の例では、ADMSTAGING は<subscription_name>で、bot は<event_name>です。



JSON データを New Relic ダッシュボードに取り込んだら、管理者は NRQL (New Relic Query Language) を使用して、取り込んだデータに基づいてクエリを構築することで、選択したファセットとウィジェットを含むカスタムダッシュボードを作成できます。詳しくは、https://docs.newrelic.com/docs/query-your-data/nrql-new-relic-query-language/get-started/introduction-nrql-new-relics-query-language/を参照してください。

以下は、NRQL を使用して作成されたダッシュボードの例です。



このダッシュボードを作成するには、次のクエリが必要です。

- ウィジェット 1: イベント表のユニーク攻撃総数

  ```
  SELECT count(total_attacks)from <event_name> since 30 days ago
  ```

- ウィジェット 2: イベントテーブル内のユニークなトランザクション ID

  ```
  SELECT uniqueCount(transaction_id)from <event_name> since 30 days
   ago
  ```

- ウィジェット 3: ユニークボットタイプの総数とその数

  ```
  SELECT uniqueCount(bot_type_desc), uniques(bot_type_desc)from <
  event_name> since 30 days ago
  ```

- ウィジェット 4: ボット違反が発生しているユニークアプリ名の総数

  ```
  SELECT uniques(appname)from <event_name> since 30 days ago
  ```

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 NetScaler 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に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。

NetScaler Gateway アプライアンスに関連するすべての Gateway で使用されている Gateway 数、アクティブなセッション数、合計バイト数、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。
- アドバンストライセンスを持つ NetScaler 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 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、第 2 DMZ の NetScaler Gateway アプライアンスのエラーに関する情報を入手できません。
- 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
  - OAuth-OpenID コネクト

    OAuth-OpenID 接続認証の場合、NetScaler は OAuth-OpenID 接続依存パーティ（RP）または OAuth-OpenID 接続アイデンティティプロバイダー（IdP）として機能できます。認証が成功すると、Gateway Insight レポートの [Users] タブにユーザー名が報告されます。ただし、セッションが IdP と RP のどちらで作成されたかは識別できません。

    注： OAuth-OpenID 接続認証は、NetScaler ADM リリース 13.1 ビルド 4.xx 以降でサポートされています。

Gateway Insight の有効化

NetScaler Gateway アプライアンスの Gateway Insight を有効にするには、まず NetScaler Gateway アプライアンスを NetScaler ADM に追加する必要があります。次に、VPN アプリケーションを代表する仮想サーバー向けに AppFlow を有効にしてください。NetScaler 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. [インフラストラクチャ**] > [**インスタンス] に移動し、AppFlow を有効にするインスタンスを選択します。
2. **[** アクションの選択] リストから、[**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. [インフラストラクチャ**] > [**インスタンス] に移動し、インスタンスを選択します。
2. **[** 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) **NetScaler**Gateway を選択
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

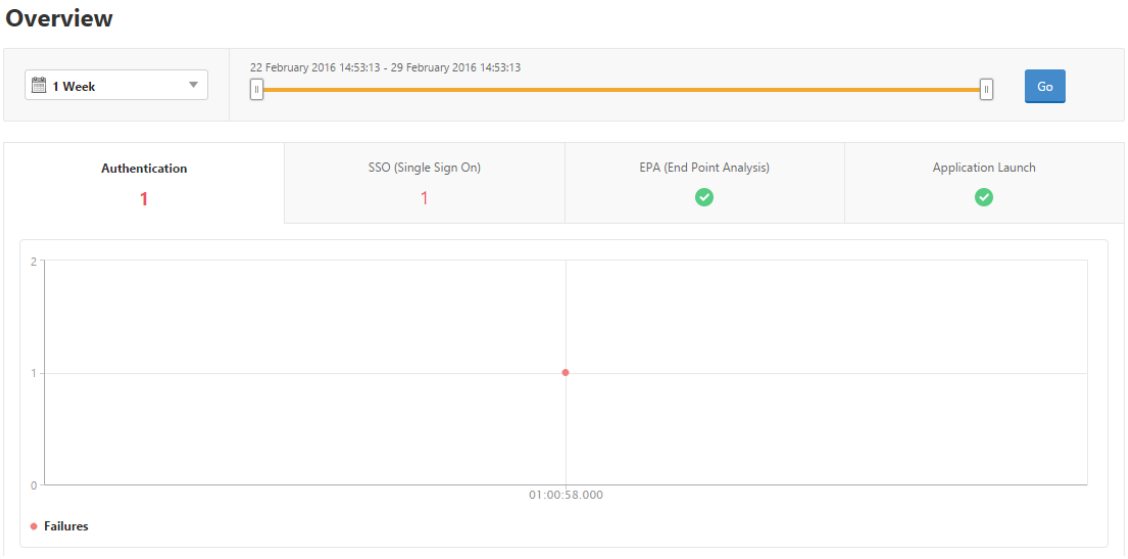
NetScaler ADM では、NetScaler Gateway アプライアンスに関連するすべてのユーザー、アプリケーション、および Gateway のレポートを表示でき、特定のユーザー、アプリケーション、または Gateway の詳細を表示できます。「概要」セクションでは、EPA、SSO、認証、およびアプリケーション起動の失敗を表示できます。ユーザーがログオンに使用したさまざまなセッションモードの概要、クライアントの種類、時間ごとのログオンしたユーザーの数を表示することもできます。

> 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。

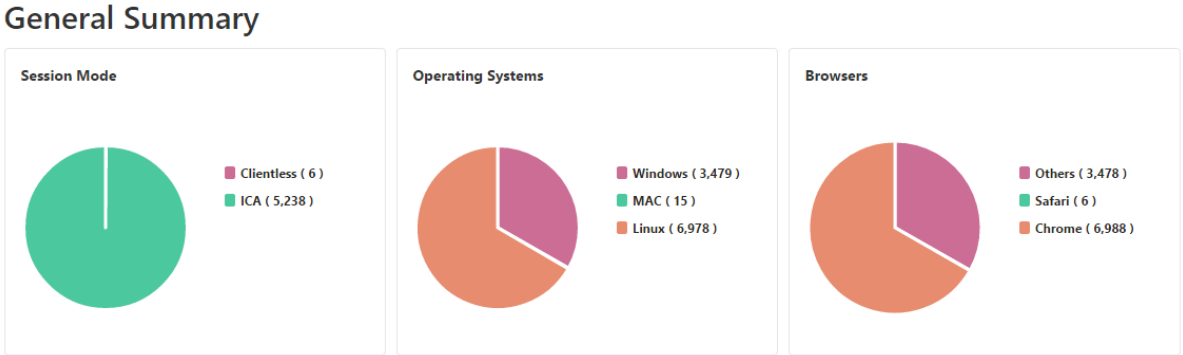
EPA、**SSO**、認証、承認、およびアプリケーションの起動の失敗を表示するには

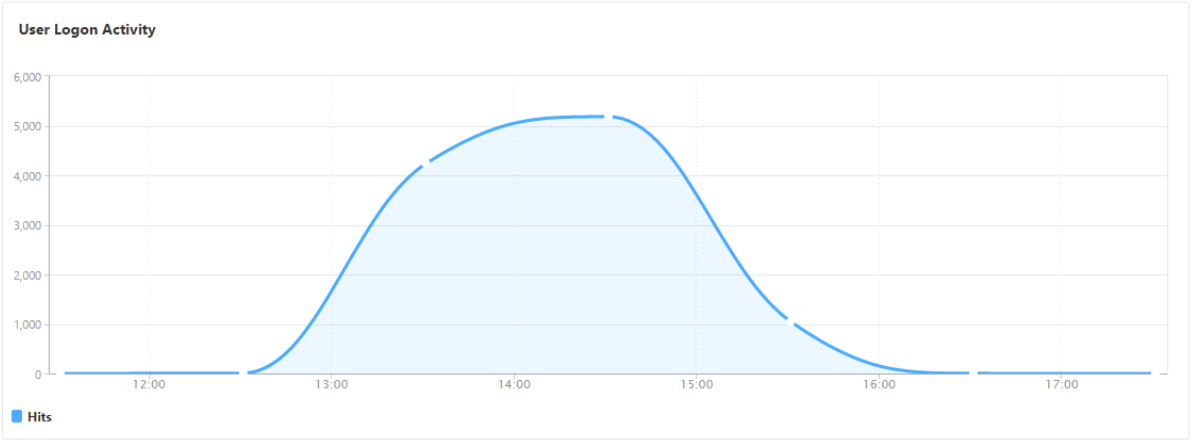
1. NetScaler ADM で、［Gateway ］**>**［**Gateway Insight**］に移動します。
2. ユーザーの詳細を表示する期間を選択します。時間スライダーを使用して選択する期間をカスタマイズできます。［**Go**］をクリックします。
3. ［EPA (End Point Analysis)］、［Authentication］、［Authorization］、［SSO (Single Sign On)］、［Application Launch］タブのいずれかをクリックして、エラーの詳細を表示します。



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、［**Gateway** ］**>**［**Gateway Insight**］に移動し、下にスクロールしてレポートを表示します。





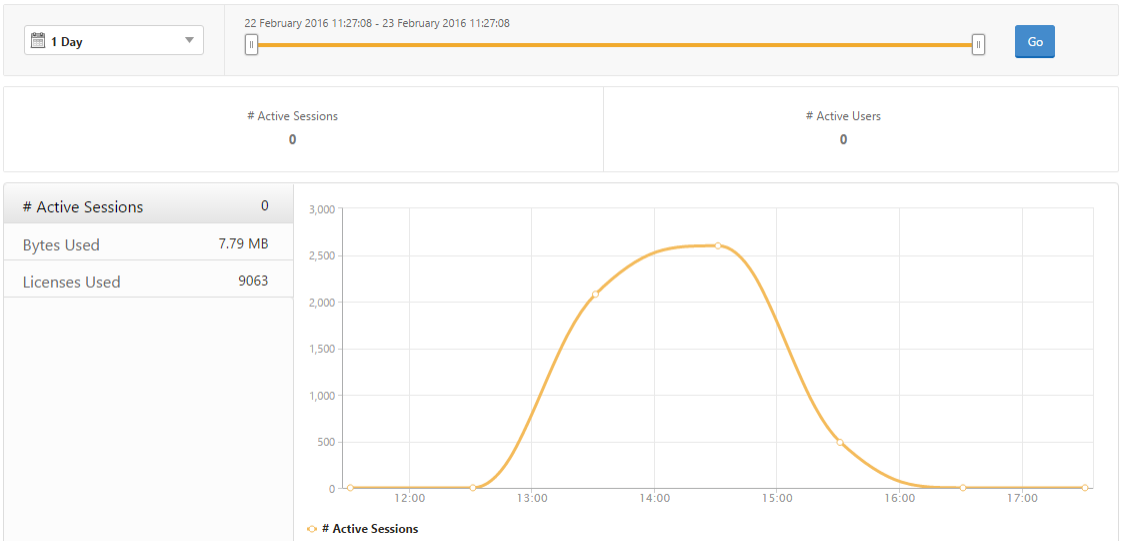
ユーザーの **Gateway Insight** レポートの表示

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. NetScaler ADM で、**Gateway > Gateway Insight >** 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。

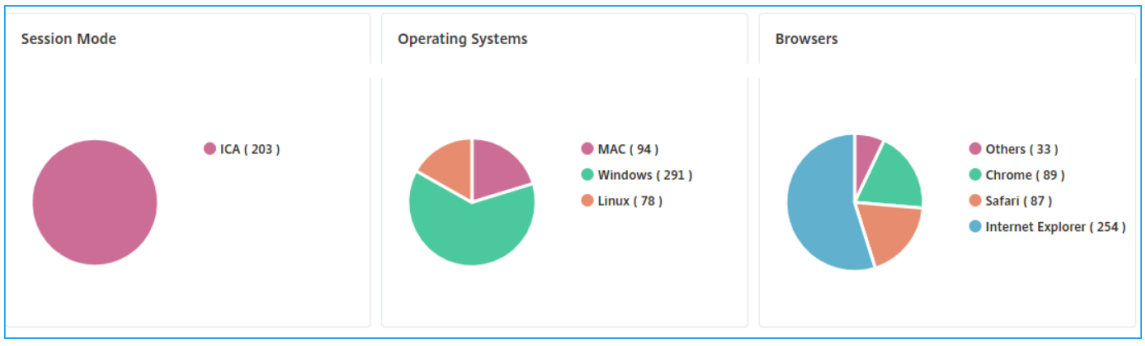


下にスクロールすると、有効なユーザーとアクティブユーザーの一覧が表示されます。

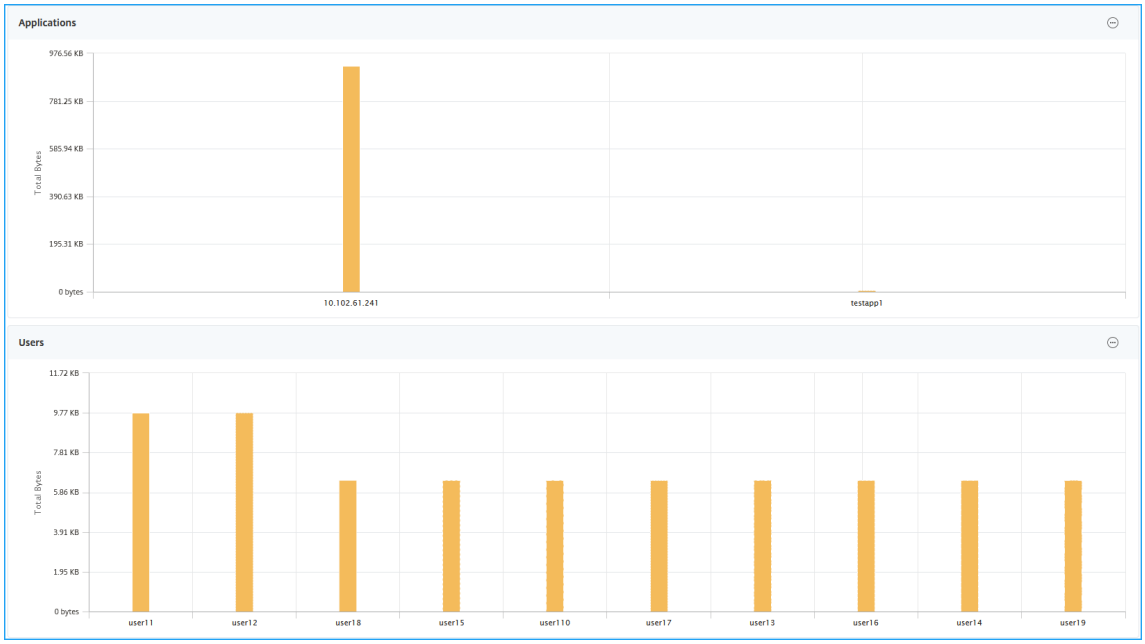
User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

[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。

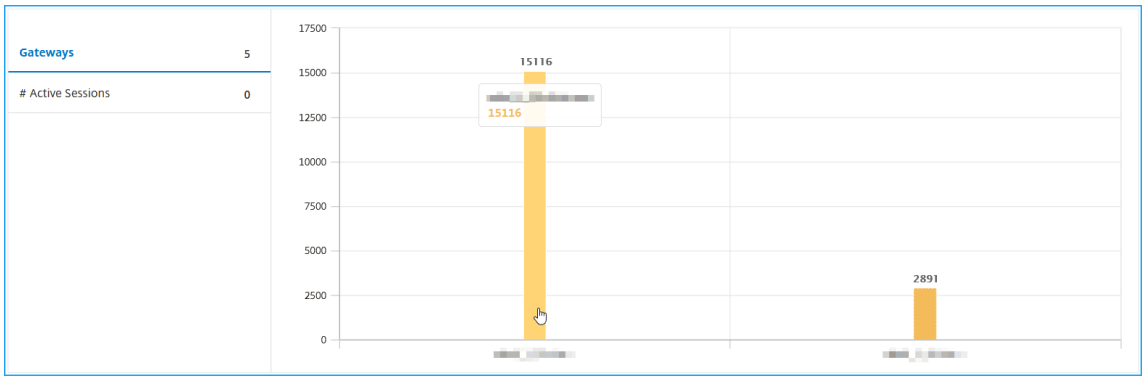
- ユーザーの詳細 -ADC Gateway アプライアンスに関連付けられた各ユーザーのインサイトを表示できます。[**Gateway **] > [**Gateway Insight**] > [**Users**] に移動し、ユーザーをクリックして、選択したユーザーのインサイト (セッションモード、オペレーティングシステム、ブラウザなど) を表示します。



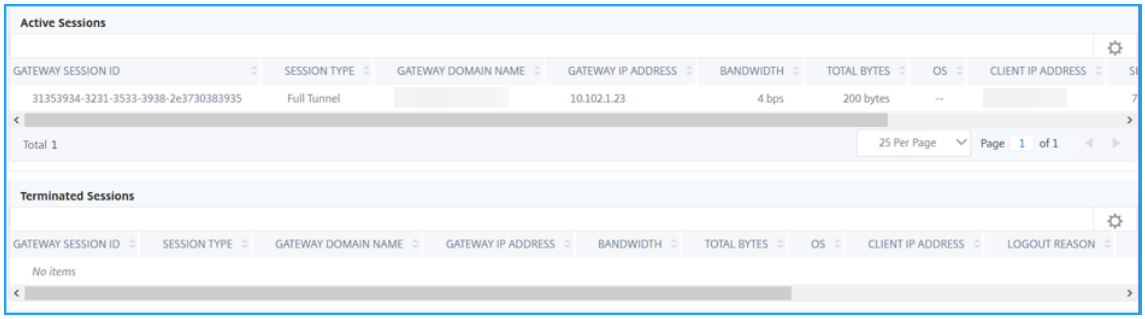
- 選択した **Gateway** のユーザーとアプリケーション -[Gateway] > [**GatewayInsight**] > [**Gateway**] に移動し、Gateway ドメイン名をクリックすると、選択した Gateway に関連付けられている上位 10 個のアプリケーションと上位 10 個のユーザーが表示されます。



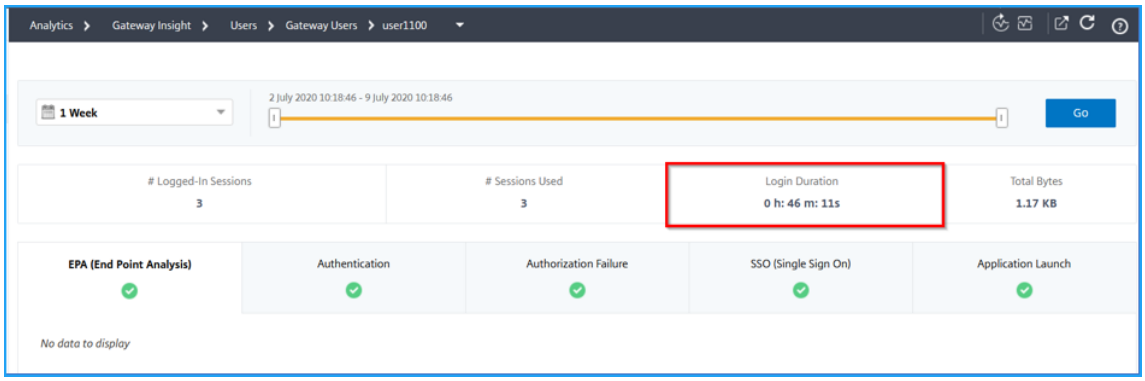
- アプリケーションとユーザーの表示オプション—10 を超えるアプリケーションおよびユーザーの場合、[アプリケーションとユーザー] の [詳細] アイコンをクリックすると、選択したゲートウェイに関連付けられているすべてのユーザーとアプリケーションの詳細を表示できます。
- 棒グラフをクリックして詳細を表示—棒グラフをクリックすると、関連する詳細を表示できます。たとえば、[**Gateway] > [Gateway Insight] ** [Gateway] に移動し、Gateway の棒グラフをクリックして Gateway の詳細を表示します。



- 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。



- 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

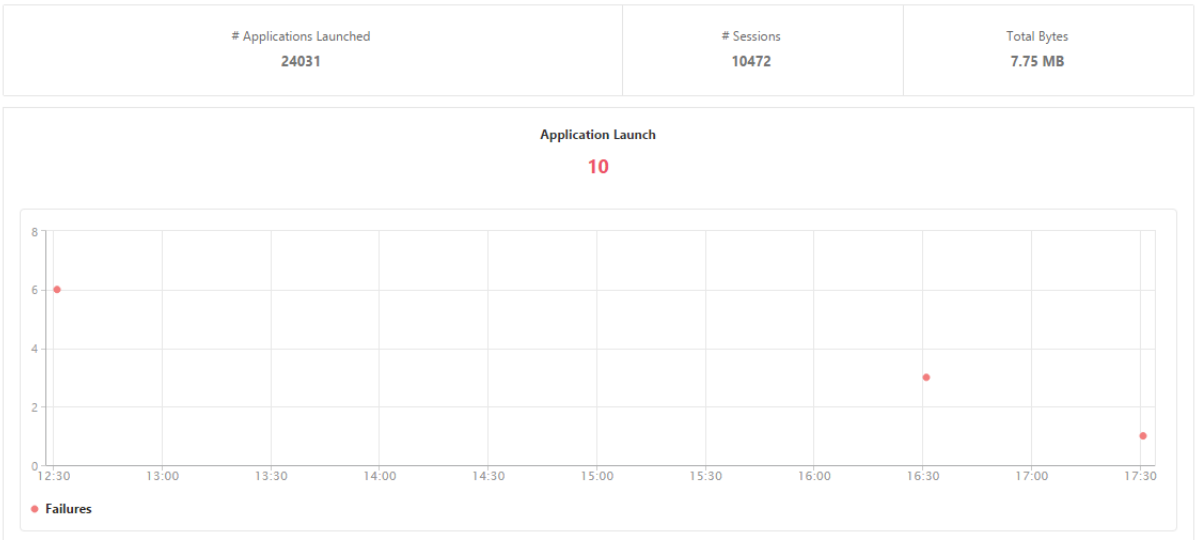
アプリケーションの **Gateway Insight** レポートの表示

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、[ゲートウェイ] **>** [ゲートウェイインサイト] **[**アプリケーション] に移動します。
2. アプリケーションの詳細を表示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。

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。

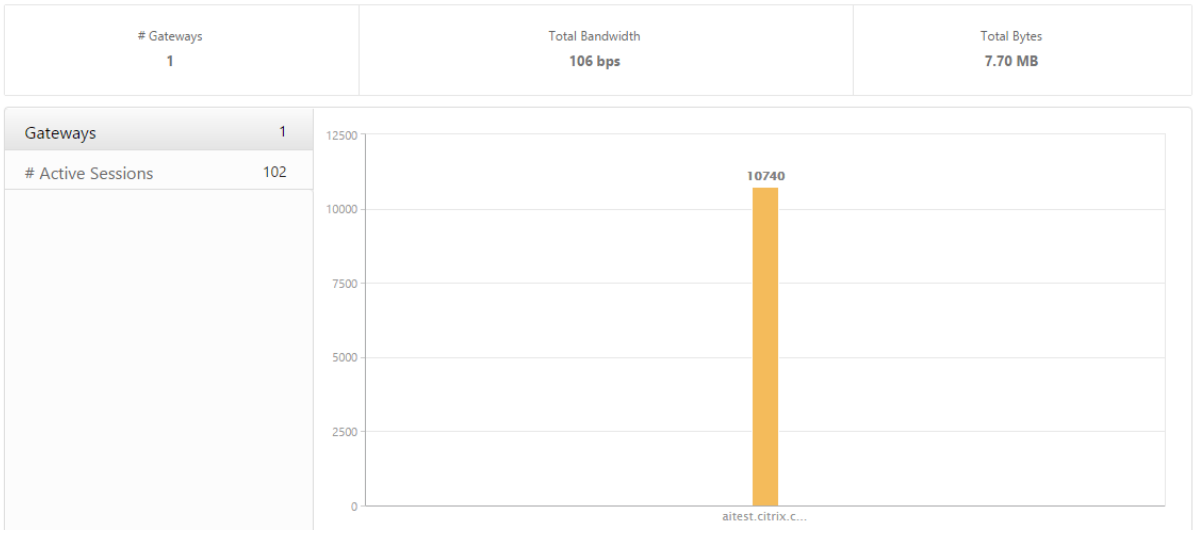
Gateway の **Gateway Insight** レポートの表示

NetScaler Gateway アプライアンスに関連するすべての Gateway で使用されている Gateway 数、アクティブなセッション数、合計バイト数、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。

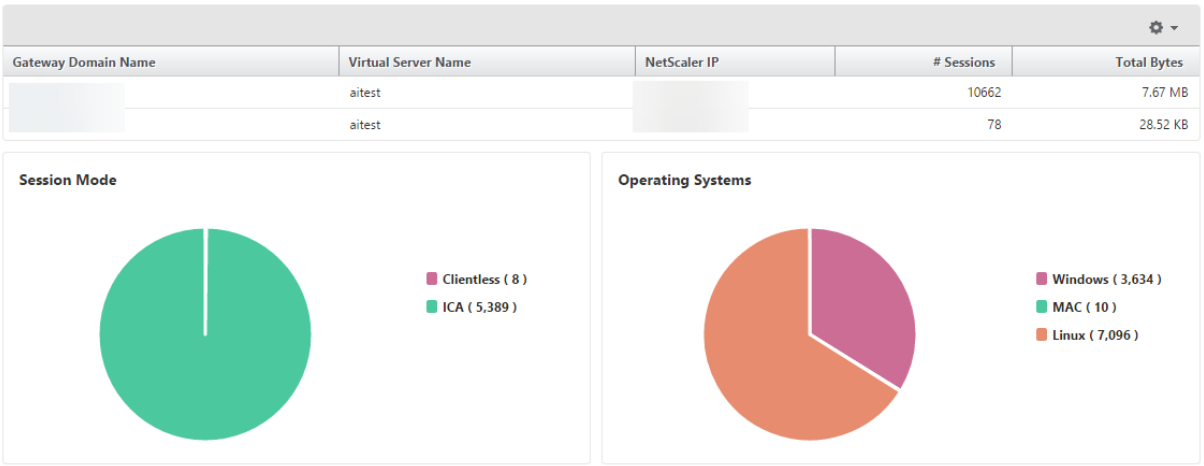
ゲートウェイの詳細を表示するには

1. **NetScaler ADM** で、[ゲートウェイ] **> [** ゲートウェイインサイト**] [**ゲートウェイ] 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

1. [ダッシュボード] タブの右ペインで、[エクスポート] ボタンをクリックします。
2. [今すぐエクスポート] で、必要な形式を選択し、[エクスポート] をクリックします。

エクスポートをスケジュールするには**:**

1. [ダッシュボード] タブの右ペインで、[エクスポート] ボタンをクリックします。
2. [エクスポートのスケジュール] で詳細を指定し、[スケジュール] をクリックします。

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。

1. [構成] タブで、[設定**] > [**通知**] > [**電子メール**]** に移動します。
2. 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

NetScaler ADM を使用して NetScaler Gateway アプライアンスを監視している NetScaler Gateway 管理者で、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。

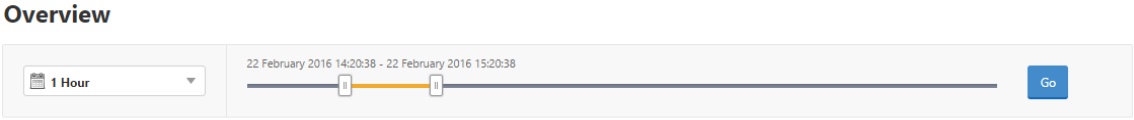
NetScaler ADM で、[**Gateway**] **>** [**Gateway Insight**] に移動し、[ユーザーの検索] テキストボックスで検索するユーザーを指定します。

認証の失敗

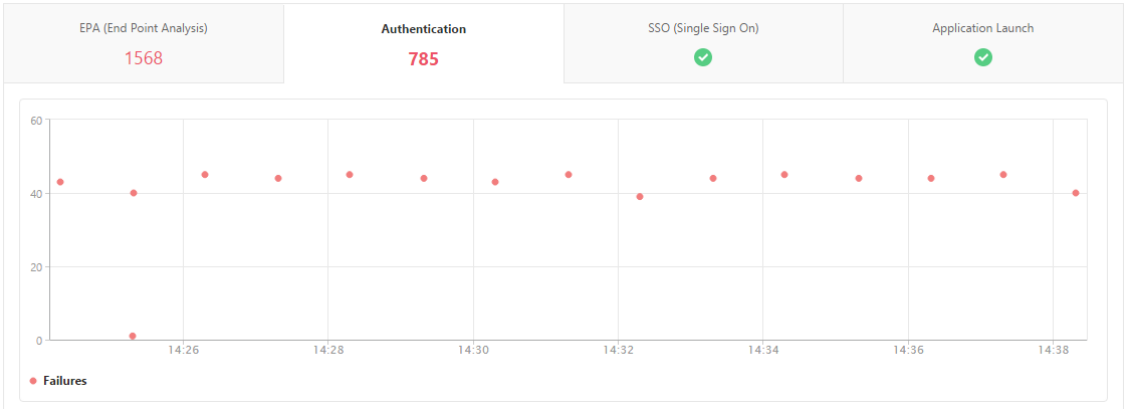
資格情報が正しくない、または認証サーバーから応答がないなどの認証エラーについて確認できます。認証が失敗した要因も確認できます。

認証失敗の詳細を表示する手順は、次のとおりです。

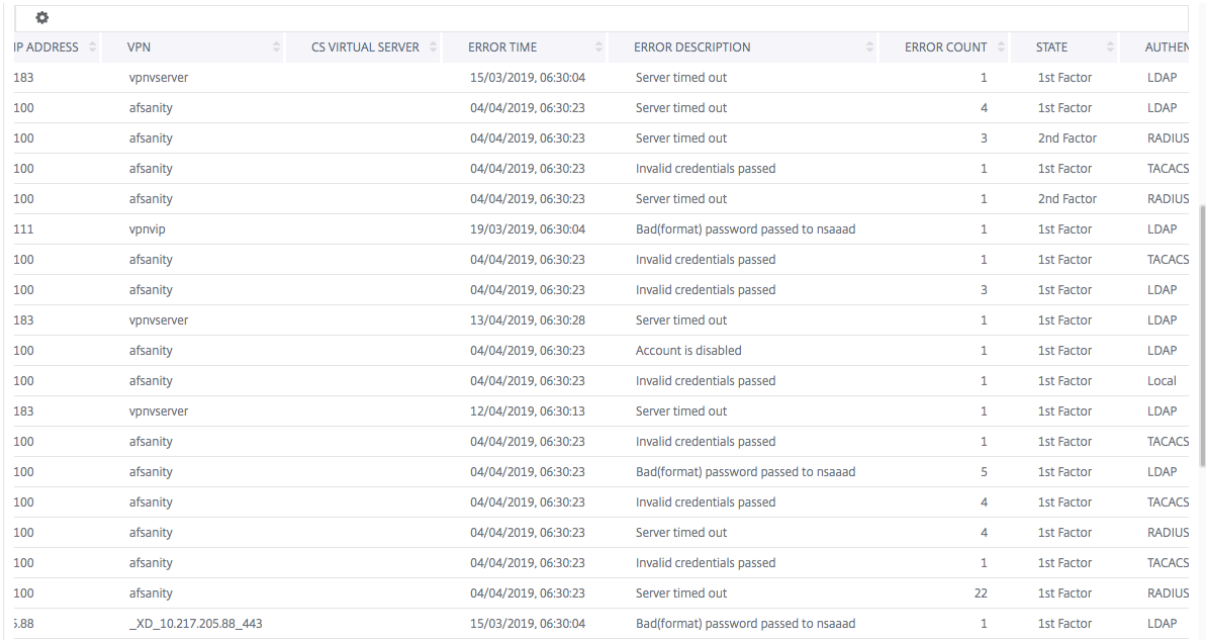
1. NetScaler ADM で、[Gateway] **>** [**Gateway Insight**] に移動します。
2. [概要] セクションで、認証エラーを表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。[**Go**] をクリックします。



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] 列にはログオ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	vpnvserver		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	vpnvserver		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	vpnvserver		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
.88	_XD_10.217.205.88_443		15/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP

[Us **ername**] 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。

> 重要:
>
> OAuth-OpenID Connect 認証が失敗した場合、「トークン検証の失敗」など、一部の障害について、Gateway Insight レポートでユーザー名が **NA** と表示されます。この失敗では、OAuth-OpenID 接続依存パーティでの「トークン検証の失敗」が原因で、ユーザー名を認証の失敗に使用できません。

USERNAME	CITRIX ADC IP ADDRESS	CLIENT IP ADDRESS	GATEWAY IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR DESCRIPTION
-NA-	[redacted]	[redacted]	[redacted]	gitest.citrix.com		Relying party: Token verification failed
-NA-	[redacted]	[redacted]	[redacted]	gitest.citrix.com		Relying party: Incoming URL query parameter from user agent is NULL in /nf/auth/doOAuth requ
-NA-	[redacted]	[redacted]	[redacted]	gitest.citrix.com		Relying party: Action query parameter isn't present in the URL from user agent in /nf/auth/doOA
-NA-	[redacted]	[redacted]	[redacted]	gitest.citrix.com		Relying party: Action query parameter isn't present in the URL from user agent in /nf/auth/doOA
-NA-	[redacted]	[redacted]	[redacted]	vpnvserver		Relying party: Token verification failed
-NA-	[redacted]	[redacted]	[redacted]	vpnvserver		Relying party: Token verification failed
-NA-	[redacted]	[redacted]	[redacted]	vpnvserver		Relying party: Token verification failed
-NA-	[redacted]	[redacted]	[redacted]	vpnvserver		Relying party: Token decryption failure

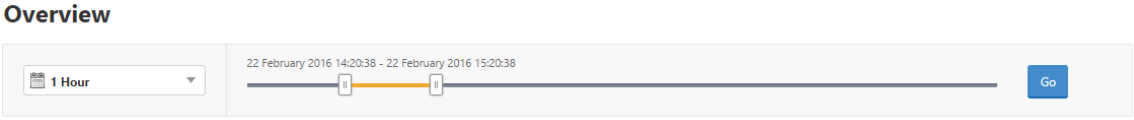
EPA エラー

EPA の失敗は、認証前または認証後の段階で表示できます。

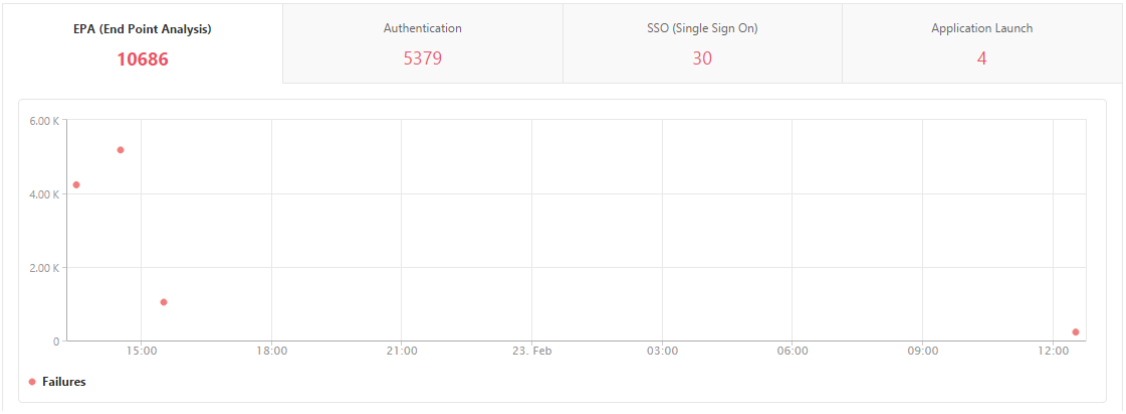
> 重要:
>
> NetScaler Gateway は、従来の表現と高度な表現の両方について、EPA の障害を NetScaler ADM に報告します。高度な式の場合、ポリシー名は Gateway Insight ダッシュボードに表示されません。EPA が nFactor 認証フローの要素の 1 つとして設定されている場合、障害が報告されます。

EPA 障害の詳細を表示するには、次の手順に従います。

1. NetScaler ADM で、[Gateway] **>** [**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。



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「エラーの説明」列には、EPA 障害の原因が表示されます。たとえば、nFactor EPA の障害により EPA チェックが失敗すると、「EPA 事前認証チェック失敗」というエラーメッセージが表示されます。

「ポリシー名」列には、障害の原因となったポリシーが表示されます。

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

[Us **ername**] 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。EPA が nFactor 認証フローの要素として使用されている場合、ユーザー名が割り当てられていないエントリにはケース ID が表示されます。

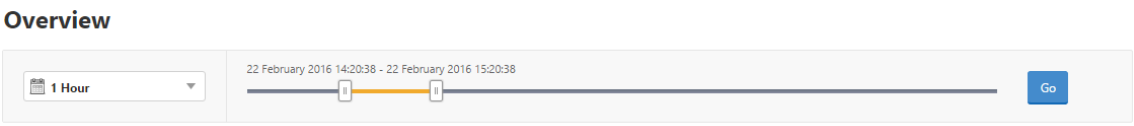
> 注
>
> 「ClientSecurity」式が VPN セッションポリシールールとして構成されている場合、NetScaler Gateway は EPA の失敗を報告しません。

SSO の障害

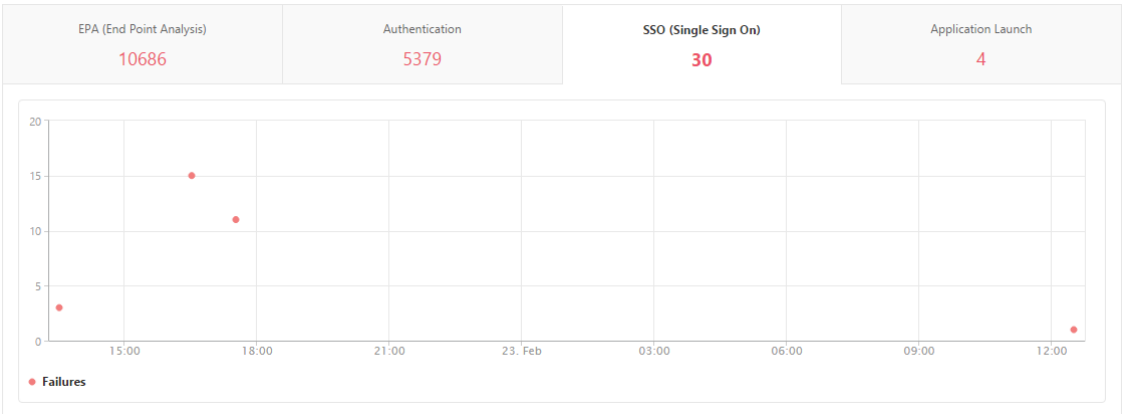
ユーザーが NetScaler Gateway アプライアンスを経由してアプリケーションにアクセスする中で、あらゆる段階の SSO エラーについて確認できます。

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、[Gateway] **>** [**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。



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

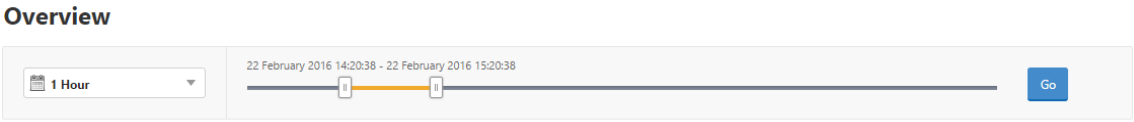
[Username] カラムで ユーザ をクリックすると、そのユーザの SSO エラーやその他の詳細を表示できます。下向きの矢印を使用して、テーブルをカスタマイズして列を追加または削除できます。

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

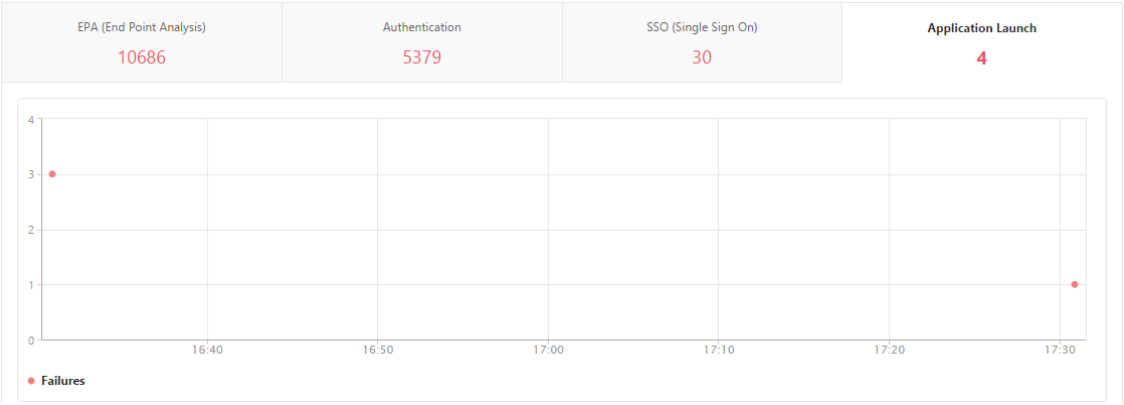
アプリケーションの起動に失敗した場合、Secure Ticket Authority（STA）または Citrix Virtual App Server にアクセスできない、または STA チケットが無効であるなどの原因を可視化できます。エラーの時間や詳細、STA 検証ができなかったリソースについて確認できます。

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、[Gateway] **>** [**Gateway Insight**] に移動します。
2. 「概要」セクションで、SSO エラーを表示する期間を選択します。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。



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。

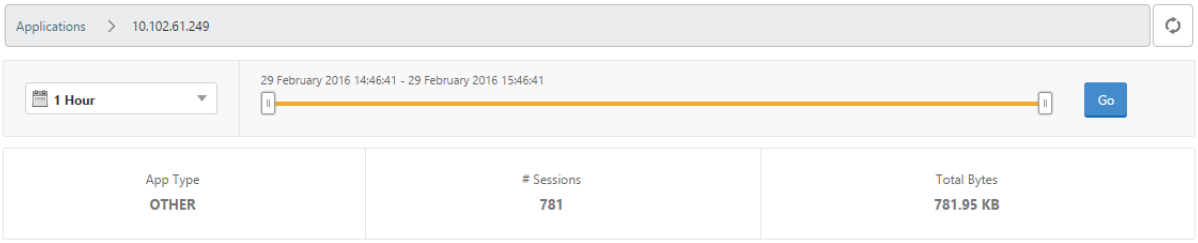
新しいアプリケーションを正常に起動した後、ユーザーは、そのアプリケーションによって消費された合計バイト数と帯域幅を表示したい

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。

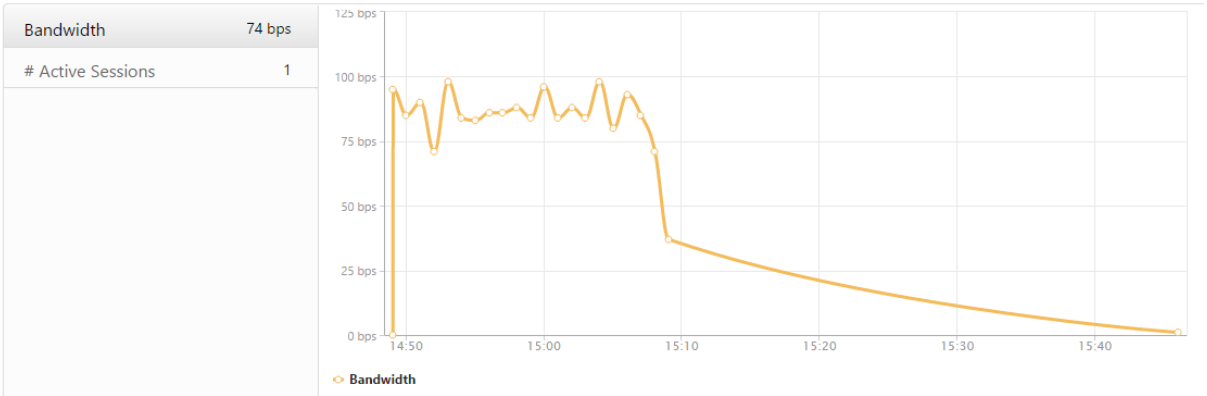
アプリケーションによって消費された合計バイト数と帯域幅を表示するには、次の手順を実行します。

NetScaler ADM で、[**Gateway] > [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。

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。

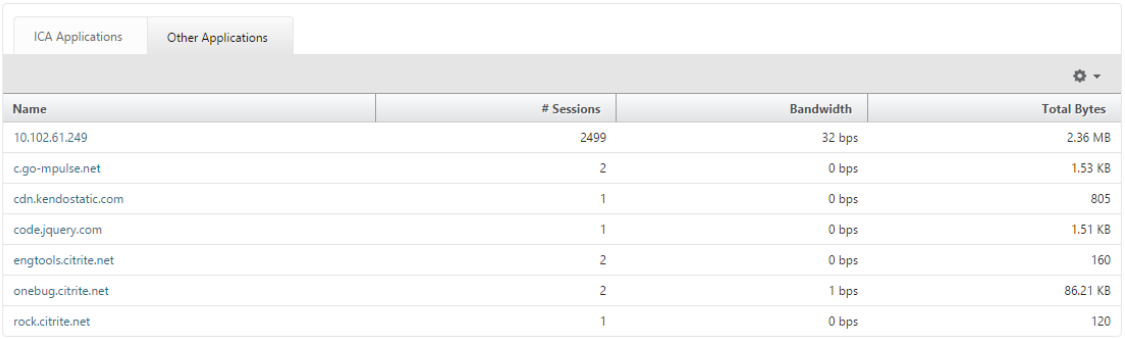


ユーザーが **NetScaler Gateway** に正常にログオンしたが、内部ネットワークの特定のネットワークリソースにアクセスできない

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. NetScaler ADM で、[**Gateway] > [Gateway Insight] > [**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。



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

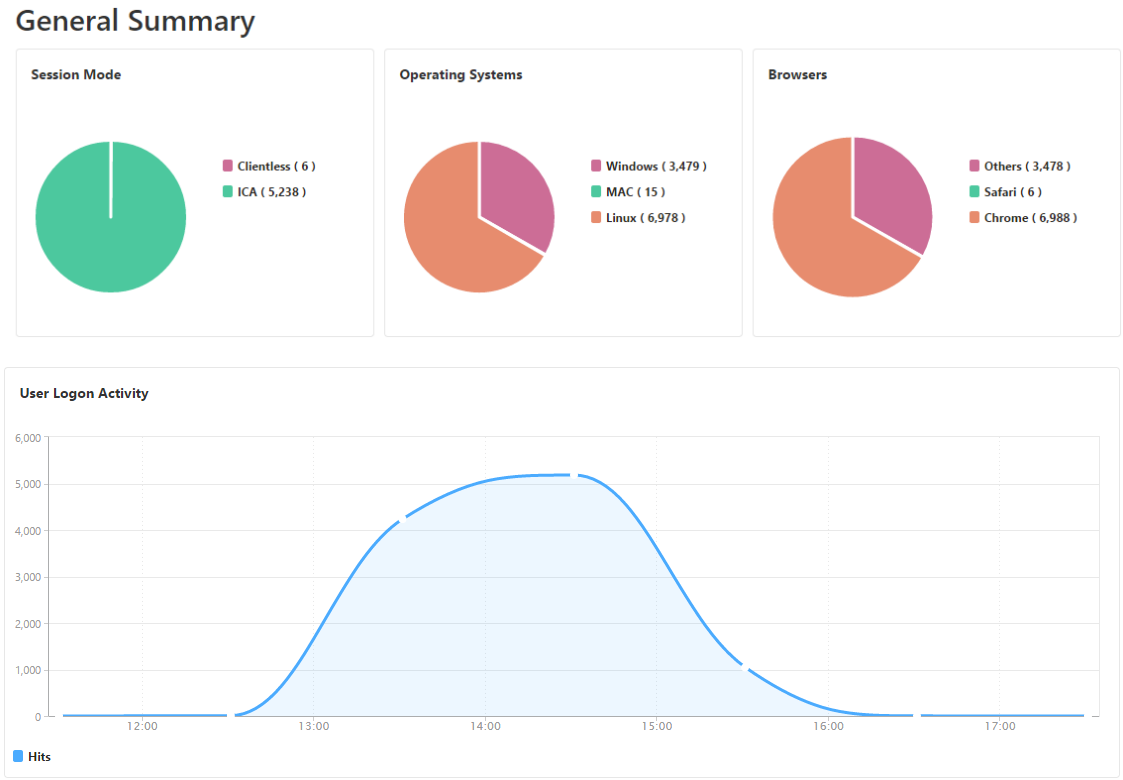
3. 下にスクロールすると、「ユーザー」テーブルに、そのアプリケーションにアクセスできるすべてのユーザーが表示されます。

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できる必要があります

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、[Gateway] **>** [**Gateway Insight**] に移動します。
2. [概要] セクションで、下にスクロールして、[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。



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 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、


```
bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
<!--NeedCopy-->
```

Gateway Insight には、バインドタイプ OTHERTCP_REQUEST も必要です。

```
bind vpn vserver afsanity -policy afp -priority 100 -type
   OTHERTCP_REQUEST
<!--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 と NetScaler ADM の間の接続チェックリスト

- NetScaler で AppFlow コレクタのステータスを確認します。詳しくは、「NetScaler 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 [設定] **> [AppFlow] > [**ポリシー**]** に移動して、AppFlow ポリシーヒットを確認することもできます。
- AppFlow ポート 4739 または 5557 をブロックしているファイアウォールを検証します。

NetScaler チェックリストでのレコード生成

- `nsconmsg -d stats -g ai_tot`コマンドを実行し、NetScaler 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、nsrace 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/ulflog/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

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 147 0 : "
    GwInsight: Sent auth record Func=ns_sslvpn_export_auth_data Username
    =<name> Clientip=<ip>:<port> Destip=0:80 SessSeq=0 Sessid=<sessid>
    Gwip=<ip>:443 StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<
    vpnfqdn> Authtype=3 EPAid=(null) AuthStage=1 AuthDuration=309
    AuthAgent=<auth_server_ip> Groupname= Policyname=<name>
    CurfactorPolname=<name> NextfactorPolname= CSecExpr= Devicetype
    =16777219 Deviceid=0 email="
<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 143 0 : "GwInsight
    : Func=ns_aaa_copy_email_id_to_vpn_record input hash_attrs_len is
    zero"
<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 148 0 : "GwInsight
    : Func=update_session_appflow_collector pcb or session is NULL"
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 165 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<> Clientip=<ip>:<port> Destip
    =<ip>:80 SessSeq=1 Sessid=<sessid> Gwip=<ip>:443 StatusCode=0
    CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=0 SessState
    =2 SessMode=2 IIP=0 AppByteCount=0 ReqURL=/Citrix/Store
Web BackendServername= SSOurl= email="
SSO logs:
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 463 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=1
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 582 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=3
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```



```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 513 0 : "
   GwInsight: Sent session update record Func=
   ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
   Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
   =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=2
   SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
   BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 29796 0 : "
   GwInsight: Sent session update record Func=
   ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
   Destip=<ip>:443 SessSeq=c Sessid=<sessid> Gwip=<ip>:443 StatusCode
   =155 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=6
   SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
   BackendServername=<> SSOurl= email="
<!--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トポロジの詳細。
- 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

Gateway Insight の既知の問題については、ADC リリースノートを参照してください。

HDX Insight

February 6, 2024

HDX Insight は、NetScaler を経由する 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、NetScaler Gateway 仮想サーバーで AppFlow を有効にする必要があります。AppFlow は、IPFIX プロトコルまたは LogStream メソッドによって配信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す。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。

Gateway ］**>** ［**HDX Insight**］**>** ［アプリケーション］に移動し、［起動時間］をクリックしてアプリケーションの起動にかかった時間を確認することもできます。[**Gateway] > [HDX Insight] > [**ユーザー**]** の順に移動して、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 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。

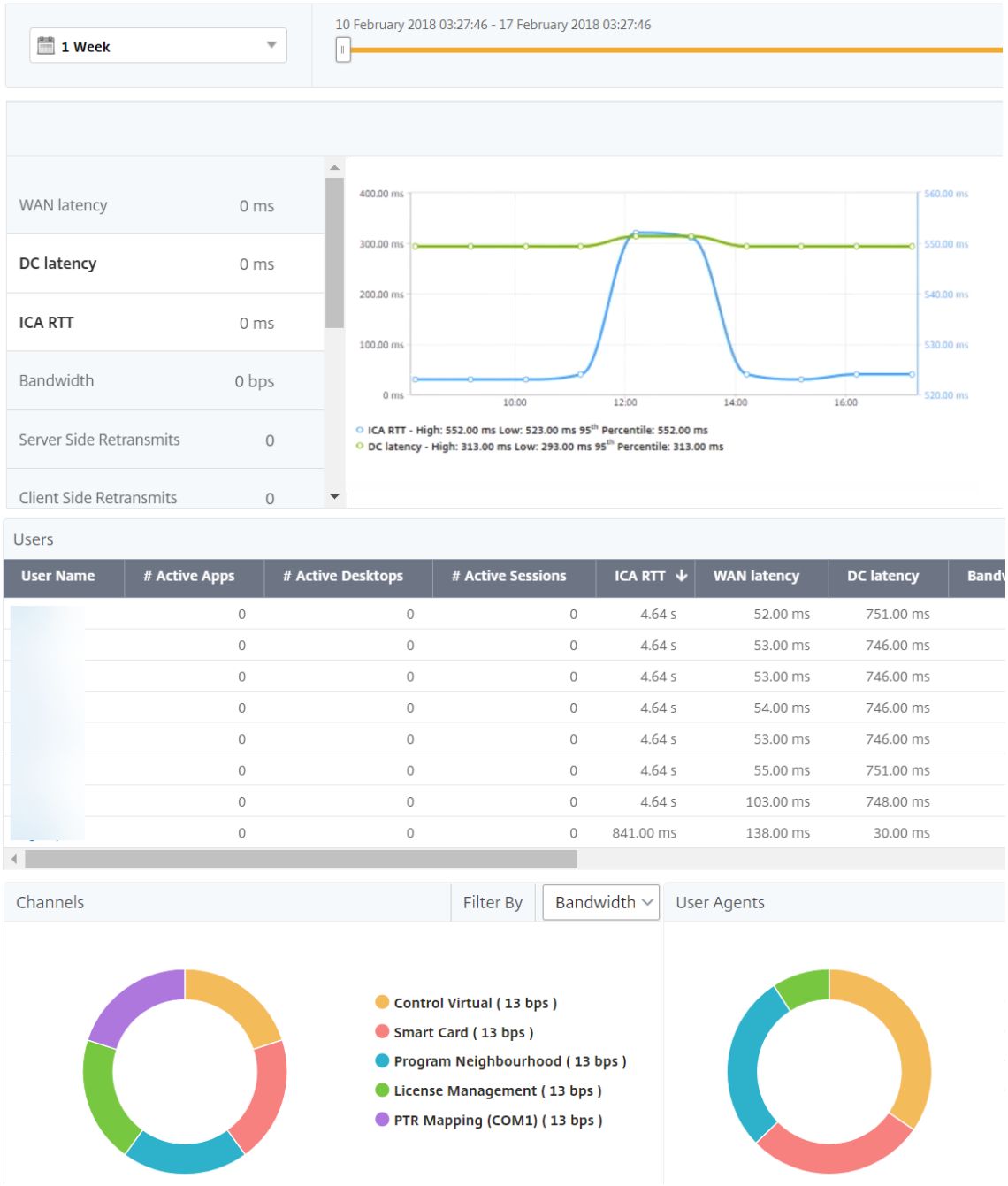
遅延の原因として考えられるのは、サーバーネットワークの遅延、サーバーネットワークに起因する ICA トラフィックの遅延、またはクライアントネットワークの遅延です。

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。

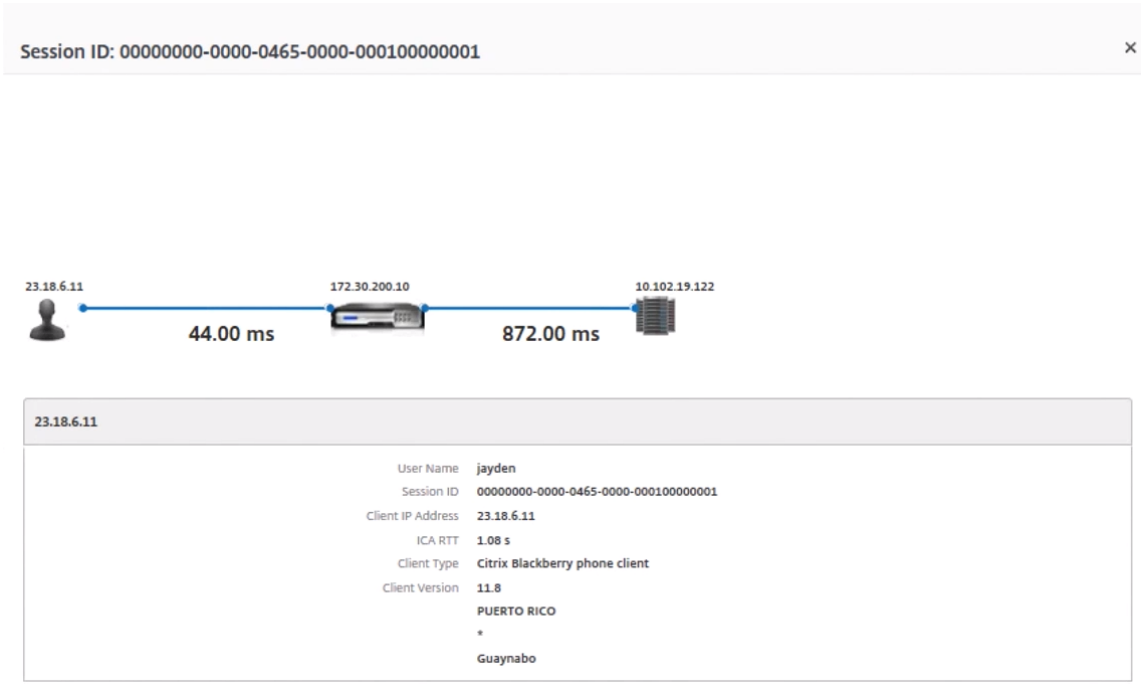
- WAN 遅延
- DC の遅延
- ホストの遅延

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. **Gateway > HDX Insight >** ユーザーの順に移動します。
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。



4. [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。
5. 「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。



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。

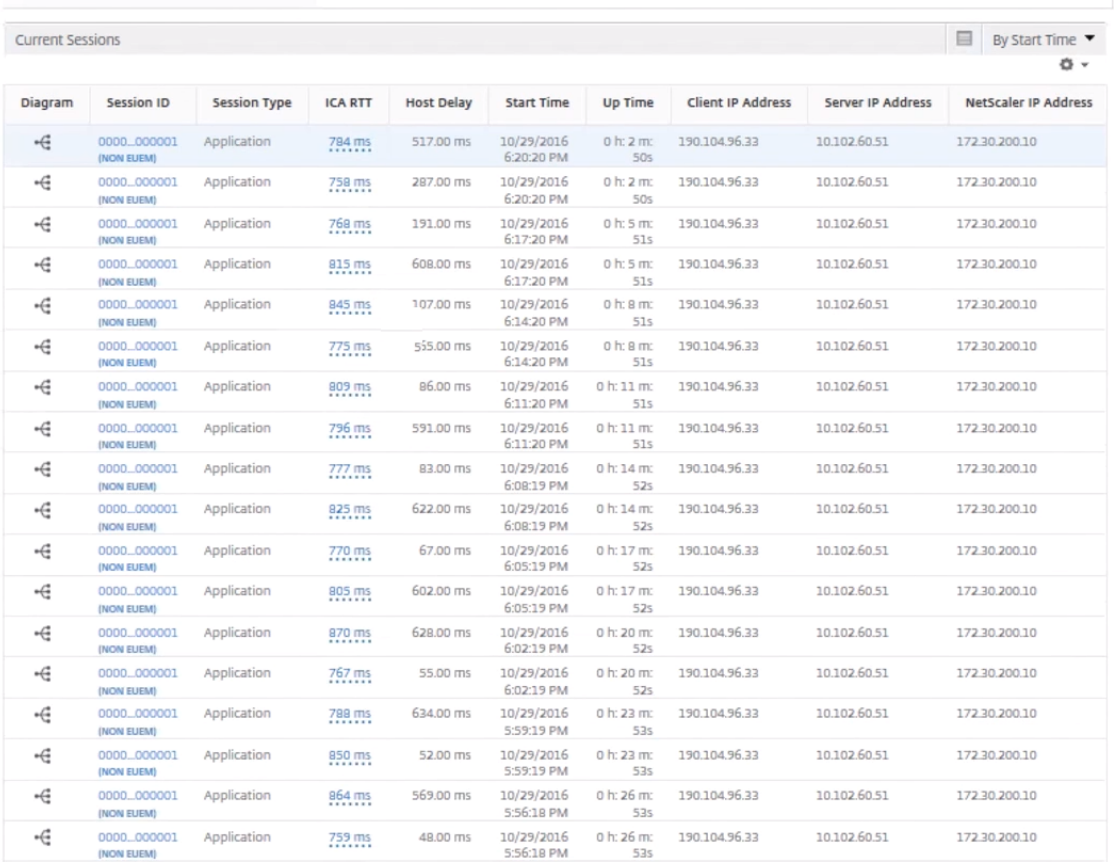
問題の根本原因を特定するために、次の測定基準を分析します。

- 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. [ゲートウェイ**] > [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。



Current Sessions — By Start Time

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	555.00 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。これらのメトリックを表示するには、[ゲートウェイ] **> [HDX Insight] > [**ユーザー] に移動し、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

NetScaler ADM のジオマップ機能は、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）を指定することで、NetScaler ADM を構成して特定の地理的場所または LAN のジオマップを表示できます。

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。[**Gateway] > [HDX Insight**] に移動し、マップの [世界] 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。

[設定**] > [Analytics** 設定**] > [IP** ブロック] に移動して、特定の場所のジオマップを構成します。

使用例

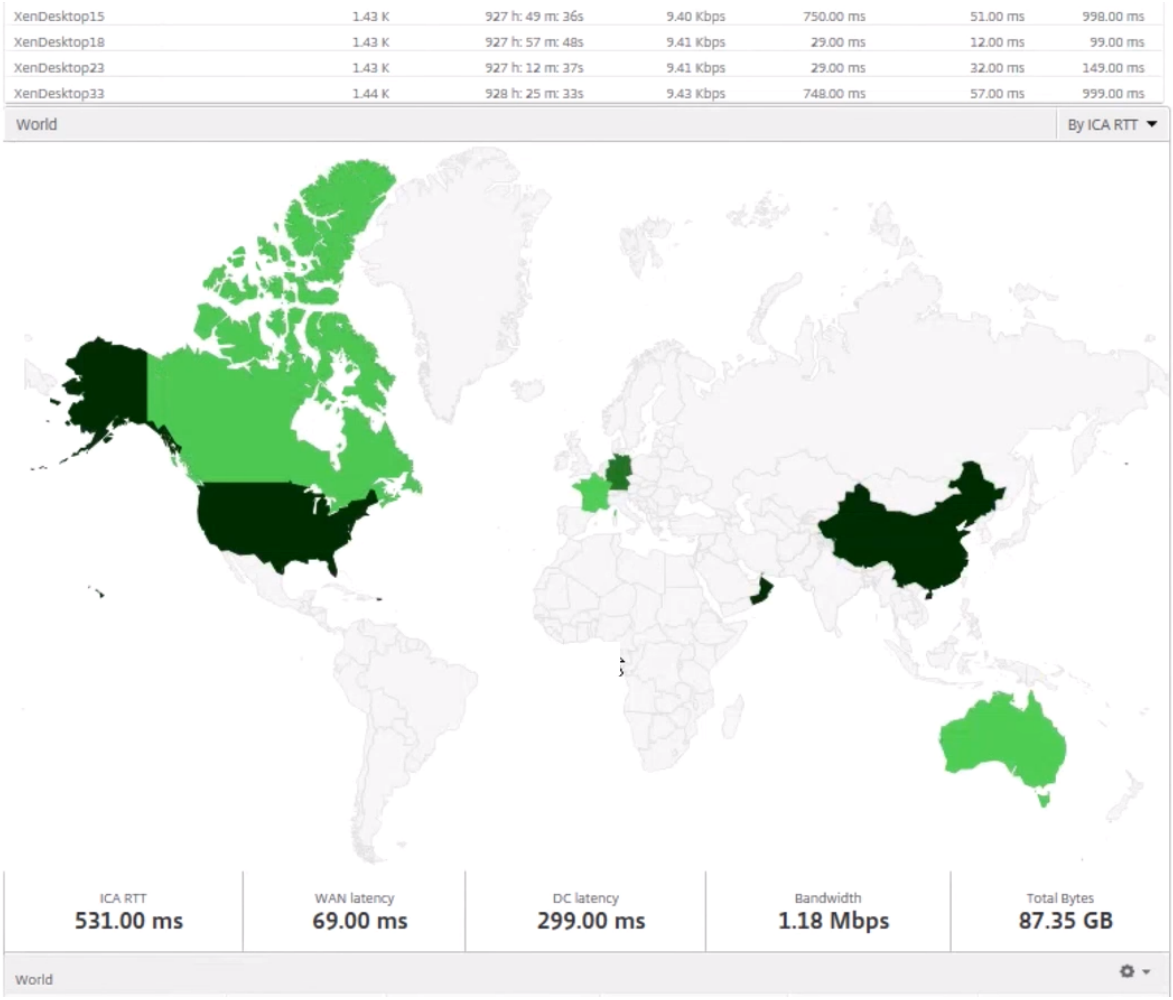
このシナリオでは 2 つのブランチオフィスを持つ ABC という名前の企業を扱います。ABC はサンタクララとインドにブランチオフィスがあります。

サンタクララのユーザーは、SClara.x.com の NetScaler Gateway アプライアンスを使用して、VPN トラフィックにアクセスしています。インドのユーザーは、India.x.com の NetScaler Gateway アプライアンスを使用して、VPN トラフィックにアクセスしています。

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 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 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 を使用すると、NetScaler インスタンスを通過する ICA トラフィックをこれまでになくエンドツーエンドで可視化でき、NetScaler Application Delivery Management（ADM）分析の一部となるため、IT 部門は優

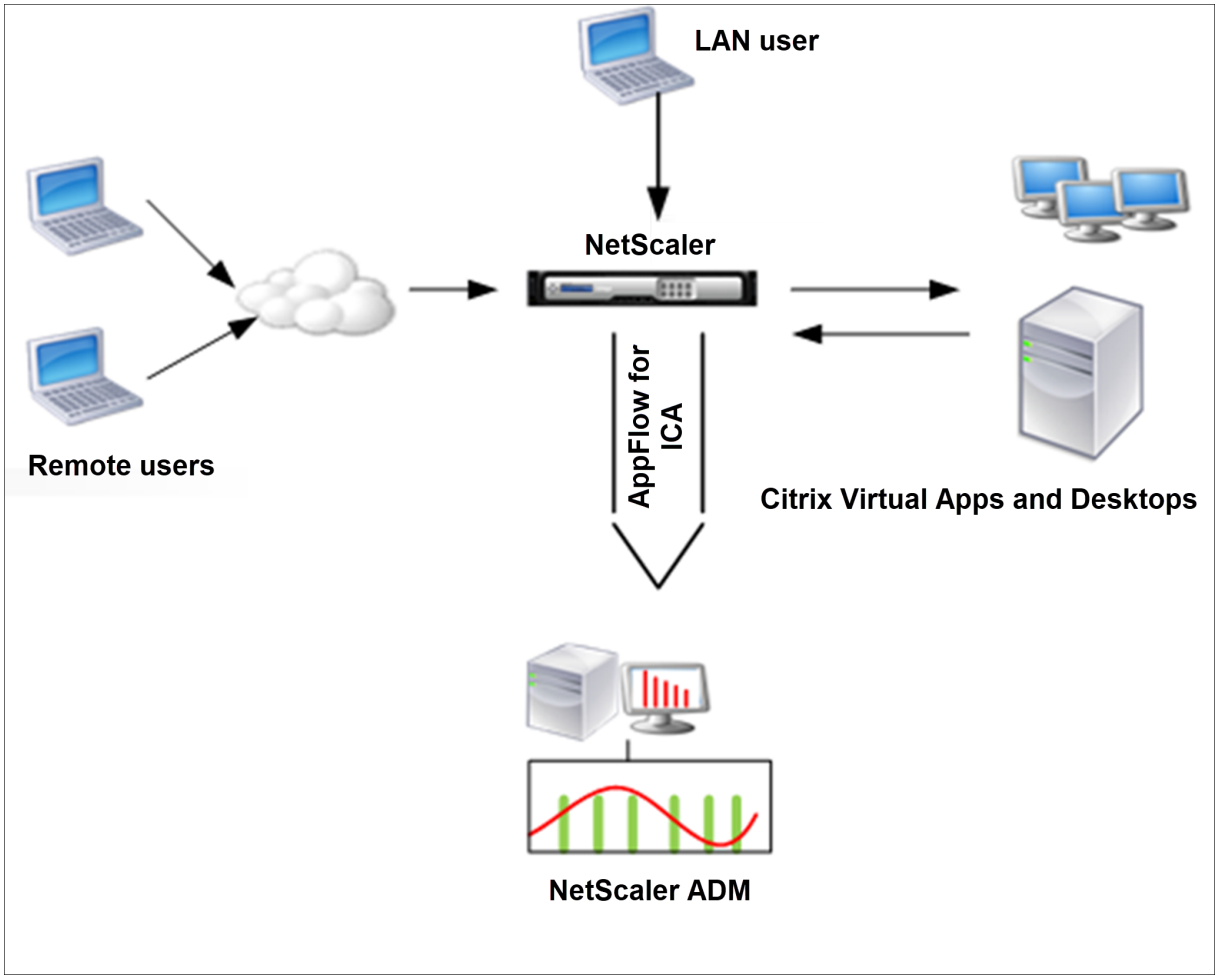
れたユーザーエクスペリエンスを提供できます。HDX Insight は、ネットワーク、仮想デスクトップ、アプリケーション、アプリケーションファブリックに対して、魅力的で強力なビジネスインテリジェンスと障害分析機能を提供します。HDX Insight はユーザーの問題を優先度によってすぐに選別すると同時に、仮想デスクトップ接続に関するデータを収集し、AppFlow レコードを生成して、それらをビジュアルレポートとして提示します。

NetScaler 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 ユーザーモードで導入された **NetScaler** 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、透過モードで展開する場合、管理者は、ルーティングポリシーを手動で適用して、要求を NetScaler アプライアンスにリダイレクト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 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 アプライアンスを監視するには、まず NetScaler アプライアンスを NetScaler Insight インベントリに追加し、AppFlow を有効にして、ダッシュボードにレポートを表示します。

NetScaler アプライアンスを NetScaler ADM インベントリに追加した後、データ収集のために AppFlow を有効にする必要があります。

> 注
>
> - ADC インスタンスでは、[設定] **> [AppFlow] > [**コレクター**]** に移動して、コレクター（NetScaler ADM）が稼働しているかどうかを確認できます。NetScaler インスタンスは、NSIP を使用して AppFlow レコードを NetScaler ADM に送信します。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 でデータ収集を有効にすることはできません。
> - コマンドとその使用法について詳しくは、「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** 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。

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
   cacheType <cachetype>] [ - cltTimeout <secs>]
<!--NeedCopy-->
```

例

```
add cr vserver cr1 HDX 10.12.2.2 443  - cacheType FORWARD  -
   cltTimeout 180
<!--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。

```
add vpn trafficAction <name> <qual> [-HDX ( ON or OFF )]

add vpn trafficPolicy <name> <rule> <action>
<!--NeedCopy-->
```

例


```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
<!--NeedCopy-->
```

3. NetScaler ADM を AppFlow コレクタとして NetScaler アプライアンスに追加します。

```
add appflow collector <name> -IPAddress <ip_addr>
<!--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。

```
add appflow action <name> -collectors <string>
```

例:

```
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。

```
add appflow policy <policyname> <rule> <action>
```

例:

```
add appflow policy pol true act
```

6. AppFlow ポリシーをグローバルバインドポイントにバインドします。

```
bind appflow global <policyname> <priority> -type <type>
```

例:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

> 注
>
> 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。

```
set appflow param -flowRecordInterval 60
```

例:


```
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の有効化

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 VPN（Virtual Private Network：仮想プライベートネットワーク）経由で NetScaler アプライアンスにアクセスします。

レポートの収集を開始するには、NetScaler Gateway アプライアンスを NetScaler Application Delivery Management（ADM）インベントリに追加し、ADM で AppFlow を有効にする必要があります。

NetScaler ADM から **AppFlow** 機能を有効にするには：

1. Web ブラウザーで、NetScaler ADM の IP アドレス（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. [インフラストラクチャ**] > [**インスタンス] に移動し、分析を有効にする NetScaler インスタンスを選択します。
4. **[** アクションの選択] リストから、[**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。

```
- 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>
```

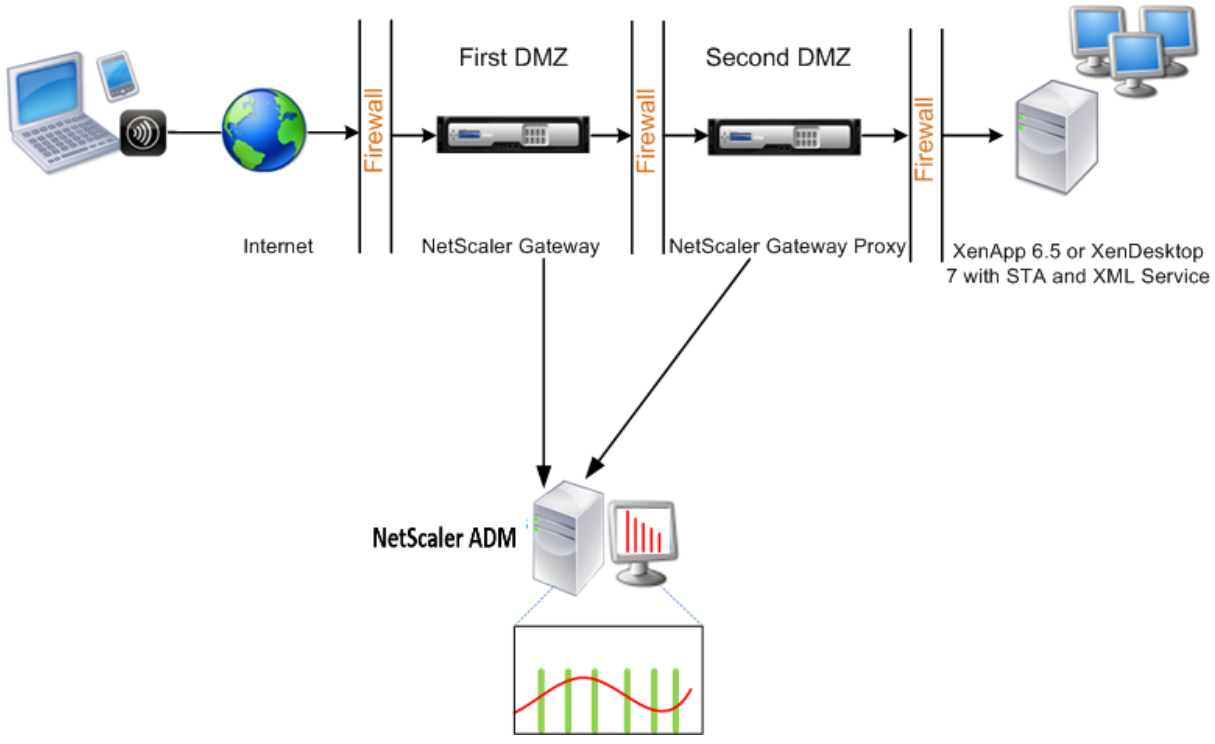


```
12
13  -  set appflow policy <name> -rule <expression>
14
15  -  bind vpn vserver <vsname> -policy <string> -type <type> -priority <
       positive_integer>
16
17  -  set vpn vserver <name> -appflowLog ENABLED
18
19  -  save ns config
```

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の有効化

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ー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、内部ネットワークのサーバーへのアクセスを制御します。

2 つ目の DMZ の NetScaler ゲートウェイは、NetScaler ゲートウェイのプロキシデバイスとして機能します。この NetScaler Gateway を使用すると、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 ゲートウェイアプライアンスに属するサブネット、または NetScaler ゲートウェイアプライアンスの 2 番目の DMZ 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、クライアントからサーバーへのトラフィックが流れる NetScaler Gateway アプライアンスの数を表します。接続チェーン ID は、クライアントとサーバー間のエンドツーエンド接続を表します。

NetScaler ADM は、ホップカウントと接続チェーン ID を使用して、NetScaler Gateway アプライアンス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 ゲートウェイを 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. [インフラストラクチャ**] > [**インスタンス] に移動し、分析を有効にする NetScaler インスタンスを選択します。
2. **[** アクションの選択] リストから、[**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 ブラウザーで、NetScaler ADM 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. [インフラストラクチャ**] > [**インスタンス] に移動し、分析を有効にする NetScaler インスタンスを選択します。
4. **[** アクションの選択] リストから、[**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 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。

- 最初の DMZ と 2 番目の DMZ の NetScaler Gateway アプライアンスの仮想サーバーを相互に通信するように構成します。
- 2 番目の DMZ の NetScaler ゲートウェイ仮想サーバーを最初の DMZ の NetScaler ゲートウェイ仮想サーバーにバインドします。
- 2 番目の DMZ の 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 ゲートウェイアプライアンスで ICA レコードをエクスポートできるようにする
- 他の NetScaler ゲートウェイアプライアンスを有効にして、TCP レコードをエクスポートします。
- 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 仮想サーバーを構成して、2 番目の DMZ の NetScaler Gateway 仮想サーバーと通信します。

```
add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (
    ON or OFF)] [-imgGifToPng]

add vpn nextHopServer nh1 10.102.2.33 8443  -secure ON
```

2. 2 番目の DMZ の NetScaler ゲートウェイ仮想サーバーを最初の DMZ の NetScaler ゲートウェイ仮想サーバーにバインドします。最初の DMZ の NetScaler ゲートウェイで次のコマンドを実行します。

```
bind vpn vserver <name> -nextHopServer <name>

bind vpn vserver vs1 -nextHopServer nh1
```

3. 2 つ目の DMZ の NetScaler ゲートウェイでダブルホップと AppFlow を有効にします。

```
set vpn vserver <name> [- doubleHop ( ENABLED or DISABLED )] [-
    appflowLog ( ENABLED or DISABLED )]

set vpn vserver vpnhop2  -doubleHop ENABLED  -appFlowLog ENABLED
```

4. 2 番目の DMZ の NetScaler Gateway 仮想サーバーでの認証を無効にします。

```
set vpn vserver <name> [-authentication (ON or OFF)]

set vpn vserver vs -authentication OFF
```

5. いずれかの NetScaler ゲートウェイアプライアンスで TCP レコードをエクスポートできるようにします。

```
bind vpn vserver <name> [-policy <string> -priority <
    positive_integer>] [-type <type>]

bind vpn vserver vpn1 -policy appflowpol1 -priority 101  -type
    OTHERTCP_REQUEST
```

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>]

bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
    ICA_REQUEST
```

7. NetScaler Gateway アプライアンスの両方の接続チェーンを有効にします：


```
set appFlow param [-connectionChaining (ENABLED or DISABLED)]

set appflow param -connectionChaining ENABLED
```

構成ユーティリティを使用して **NetScaler Gateway** を構成します。

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 「 **NetScaler 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 番目の NetScaler Gateway アプライアンスにバインドします。

2. 2 番目の DMZ の 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) 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 つ目の DMZ にある NetScaler Gateway の仮想サーバーでの認証を無効にします。

   a) [**Configuration**] タブで [**NetScaler Gateway**] を展開し、[**Virtual Servers**] をクリックします。

   b) 右側のペインで仮想サーバーをダブルクリックし、[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 ゲートウェイアプライアンスで TCP レコードをエクスポートできるようにします。

   a) [**Configuration**] タブで [**NetScaler Gateway**] を展開し、[**Virtual Servers**] をクリックします。

   b) 右側のウィンドウで、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) [**Configuration**] タブで [**NetScaler Gateway**] を展開し、[**Virtual Servers**] をクリックします。

b) 右側のペインで仮想サーバーをダブルクリックし、[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 番目の DMZ の 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 つ目の DMZ にある NetScaler Gateway の仮想サーバーでの認証を無効にします。

a)「構成」タブで 「 NetScaler Gateway 」を展開 し、「仮想サーバー」をクリック します。

b) 右側のペインで仮想サーバーをダブルクリックし、[基本設定] グループで編集アイコンをクリックします。

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 ゲートウェイアプライアンスで 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 「 **NetScaler 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。

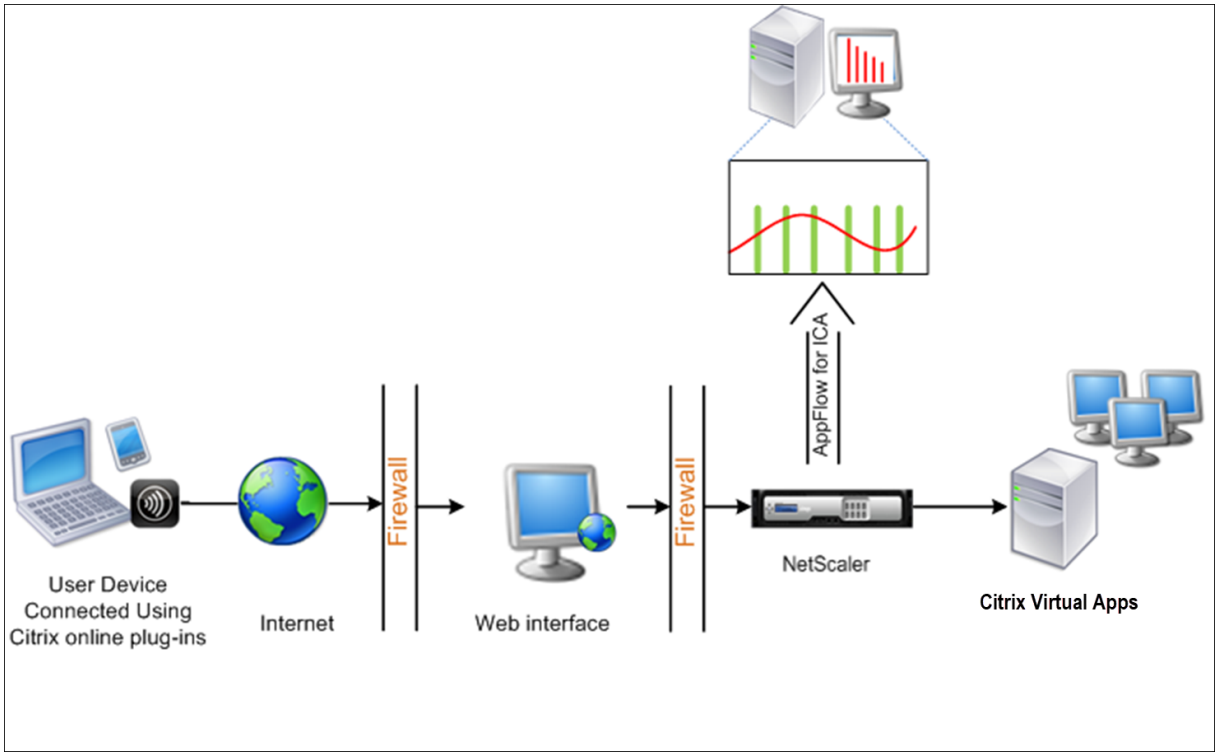
トランスペアレントモードで導入された **NetScaler** を監視するためのデータ収集を有効にする

NetScaler 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 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 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 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 でデータ収集を有効にすることはできません。
> - コマンドとその使用法について詳しくは、「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 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** アプライアンスでデータ収集を構成するには:

コマンドプロンプトで、次の操作を行います:

1. アプライアンスにログオンします。
2. NetScaler アプライアンスがトラフィックをリッスンする ICA ポートを指定します。

```
set ns param --icaPorts <port>...
```

例:

```
set ns param -icaPorts 2598 1494
```

> 注
>
> - このコマンドでは、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 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。

```
add appflow collector <name> -IPAddress <ip_addr>
```

例:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```


> 注: NetScaler アプライアンスで構成された 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。

```
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。

```
add appflow policy <policyname> <rule> <action>
```

例:

```
add appflow policy pol true act
```

6. AppFlow ポリシーをグローバルバインドポイントにバインドします。

```
bind appflow global <policyname> <priority> -type <type>
```

例:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

> 注
>
> ICA トラフィックに適用するには、**TYPE** の値は ICA_REQ_OVERRIDE または ICA_REQ_DEFAULT である必要があります。

7. AppFlow の flowRecordInterval パラメーターの値を 60 秒に設定します。

```
set appflow param -flowRecordInterval 60
```

例:

```
set appflow param -flowRecordInterval 60
```

8. 構成を保存します。種類: `save ns config`

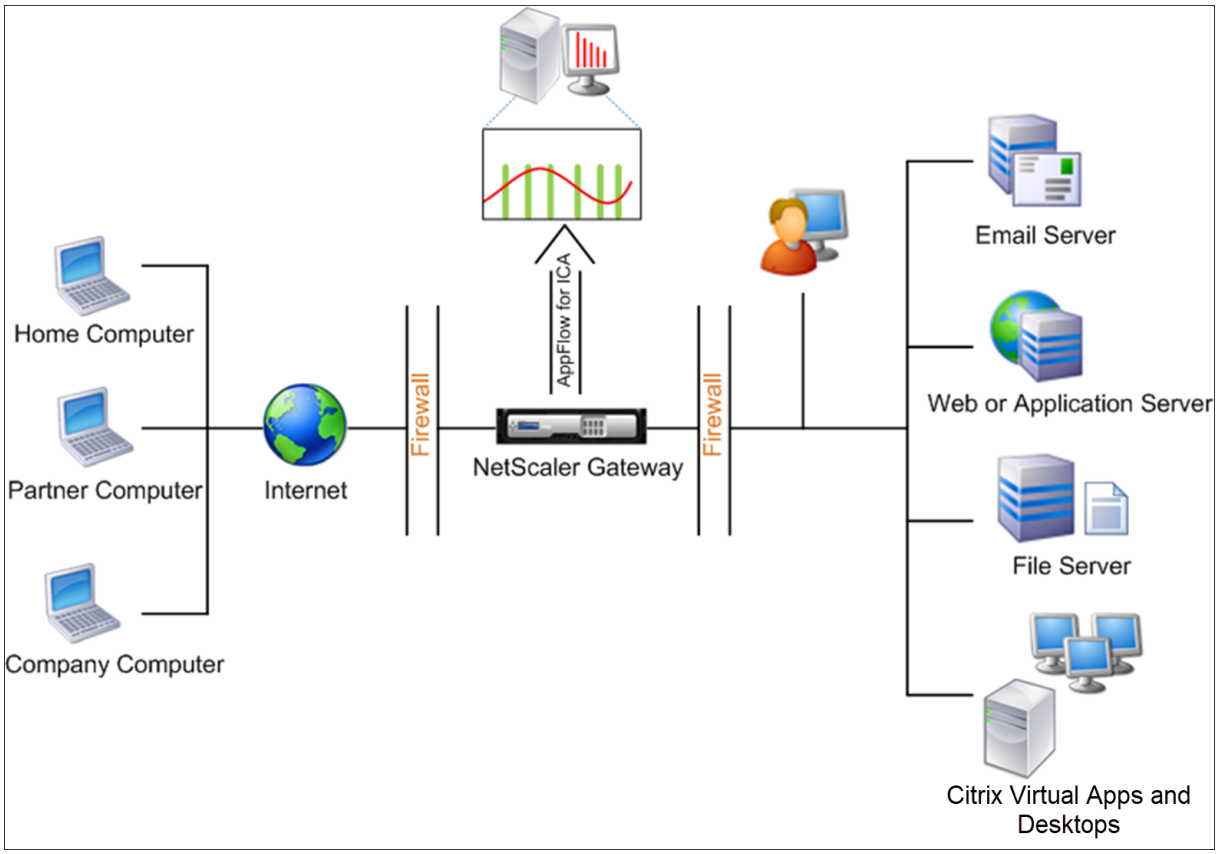
‘‘‘

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 VPN（Virtual Private Network：仮想プライベートネットワーク）経由で NetScaler アプライアンスにアクセスします。

レポートの収集を開始するには、NetScaler Gateway アプライアンスを NetScaler Application Delivery Management（ADM）インベントリに追加し、ADM で AppFlow を有効にする必要があります。



ADM から **AppFlow** 機能を有効にするには：

1. [インフラストラクチャ] > [インスタンス] に移動し、分析を有効にする NetScaler インスタンスを選択します。
2. 「アクション」リストから「**Insight** の有効化/無効化」を選択します。
3. **VPN** 仮想サーバーを選択し、「**AppFlow** 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。

データ収集を有効にして、透過モードで導入された **NetScaler** を監視できます

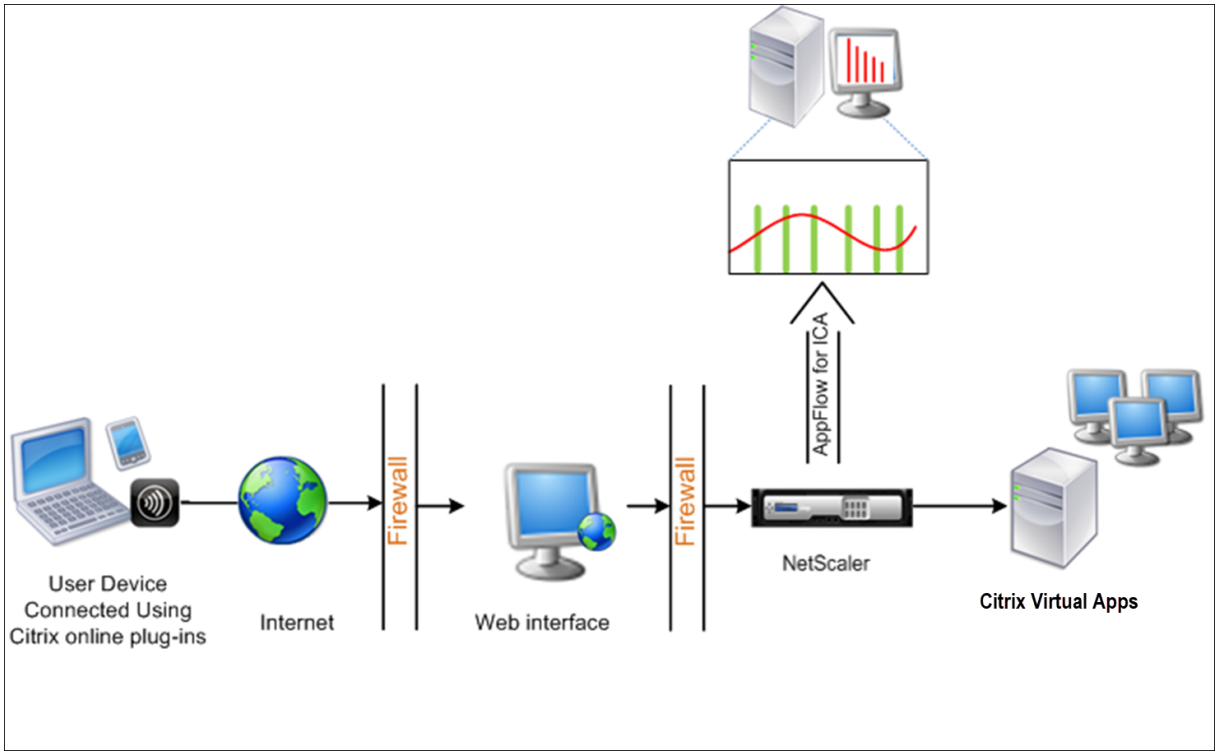
February 6, 2024

NetScaler 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 が Citrix Virtual Apps and Desktops 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 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 を各 NetScaler インスタンスの AppFlow コレクターとして追加する必要があります。また、アプライアンスを経由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 でデータ収集を有効にすることはできません。
> - コマンドとその使用法について詳しくは、「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 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** アプライアンスでデータ収集を構成するには:

コマンドプロンプトで、次の操作を行います:

1. アプライアンスにログオンします。
2. NetScaler アプライアンスがトラフィックをリッスンする ICA ポートを指定します。

```
set ns param --icaPorts \<port\>...
<!--NeedCopy-->
```

例:

```
set ns param -icaPorts 2598 1494
<!--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。

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

例:


```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--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。

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

例:

```
add appflow action act -collectors MyInsight
<!--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。

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

例:

```
add appflow policy pol true act
<!--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。

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```

例:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--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。

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. 構成を保存します。

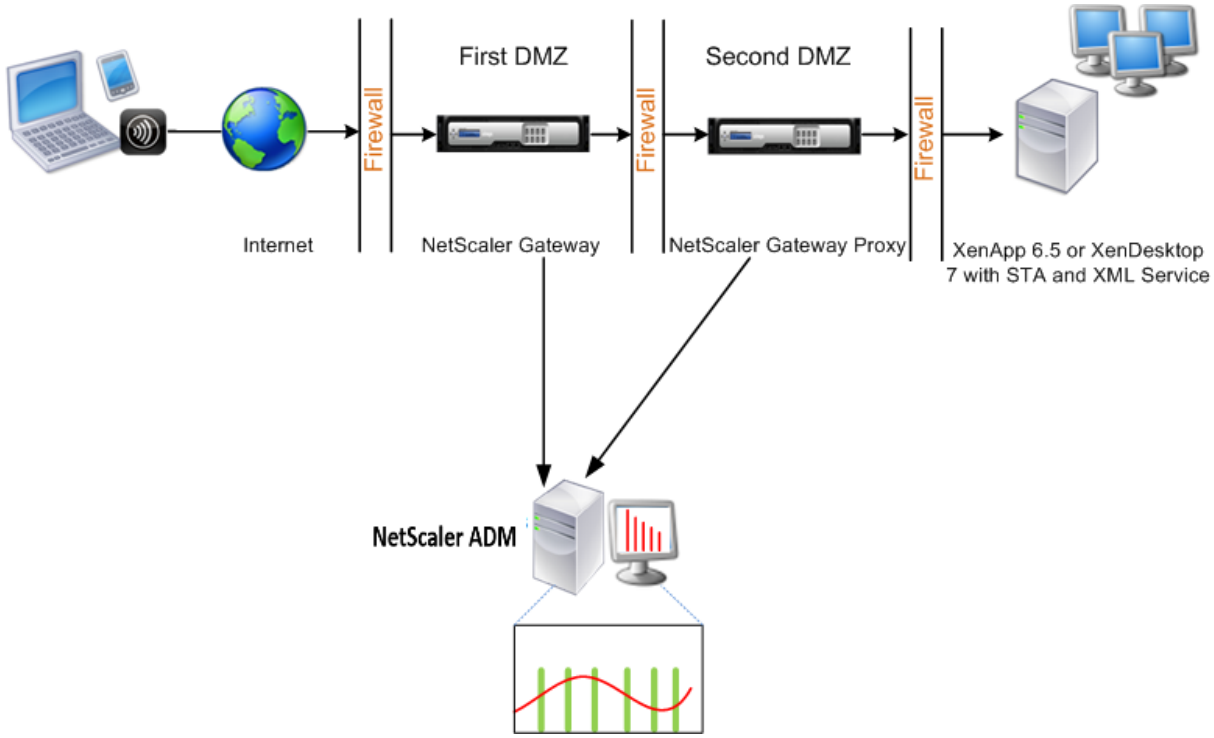
```
save ns config
<!--NeedCopy-->
```


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ー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、内部ネットワークのサーバーへのアクセスを制御します。

2 つ目の DMZ の NetScaler ゲートウェイは、NetScaler ゲートウェイのプロキシデバイスとして機能します。この NetScaler Gateway を使用すると、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 ゲートウェイアプライアンスに属するサブネット、または NetScaler ゲートウェイアプライアンスの 2 番目の DMZ 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、クライアントからサーバーへのトラフィックが流れる NetScaler Gateway アプライアンスの数を表します。接続チェーン ID は、クライアントとサーバー間のエンドツーエンド接続を表します。

NetScaler ADM は、ホップカウントと接続チェーン ID を使用して、NetScaler Gateway アプライアンス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 ゲートウェイを 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 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 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ように **NetScaler** ゲートウェイアプライアンスを構成する

NetScaler Gateway アプライアンスをインストールした後、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。

- 最初の DMZ と 2 番目の DMZ の NetScaler Gateway アプライアンスの仮想サーバーを相互に通信するように構成します。
- 2 番目の DMZ の NetScaler ゲートウェイ仮想サーバーを最初の DMZ の NetScaler ゲートウェイ仮想サーバーにバインドします。
- 2 番目の DMZ の 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 ゲートウェイアプライアンスで ICA レコードをエクスポートできるようにする
- 他の NetScaler ゲートウェイアプライアンスを有効にして、TCP レコードをエクスポートします。
- 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 仮想サーバーを構成して、2 番目の DMZ の NetScaler Gateway 仮想サーバーと通信します。

---

add vpn nextHopServer [**-secure**(ON OFF)] [**-imgGifToPng**] …

```
add vpn nextHopServer nh1 10.102.2.33 8443 -secure ON
<!--NeedCopy-->
```

2. 2 番目の DMZ の NetScaler ゲートウェイ仮想サーバーを最初の DMZ の NetScaler ゲートウェイ仮想サーバーにバインドします。最初の DMZ の NetScaler ゲートウェイで次のコマンドを実行します。

   bind vpn vserver <name> **-nextHopServer** <name>

```
bind vpn vserver vs1 -nextHopServer nh1
<!--NeedCopy-->
```

3. 2 つ目の DMZ の NetScaler ゲートウェイでダブルホップと AppFlow を有効にします。

---

set vpn vserver [**- doubleHop** (ENABLED DISABLED)] [**- appflowLog** (ENABLED DISABLED)]

```
set vpn vserver vpnhop2 -doubleHop ENABLED -appFlowLog ENABLED
<!--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)]

```
set vpn vserver vs -authentication OFF
<!--NeedCopy-->
```

5. いずれかの NetScaler ゲートウェイアプライアンスで TCP レコードをエクスポートできるようにします。

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
bind vpn vserver vpn1 -policy appflowpol1 -priority 101  - type
   OTHERTCP_REQUEST
<!--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>]

```
bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
   ICA_REQUEST
<!--NeedCopy-->
```

7. NetScaler Gateway アプライアンスの両方の接続チェーンを有効にします:

set appFlow DISABLED)]
param [**-connectionChaining** (ENABLED

```
set appflow param -connectionChaining ENABLED
<!--NeedCopy-->
```

構成ユーティリティを使用して **NetScaler** ゲートウェイを構成します。

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 「 **NetScaler 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 番目の NetScaler Gateway アプライアンスにバインドします。

2. 2 番目の DMZ の 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) [**More**] を展開し、[**Double Hop**] を選択して [**OK**] をクリックします。

3. 2 つ目の DMZ にある NetScaler Gateway の仮想サーバーでの認証を無効にします。

a) [**Configuration**] タブで [**NetScaler Gateway**] を展開し、[**Virtual Servers**] をクリックします。

b) 右側のペインで仮想サーバーをダブルクリックし、[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 ゲートウェイアプライアンスで TCP レコードをエクスポートできるようにします。

a) [**Configuration**] タブで [**NetScaler Gateway**] を展開し、[**Virtual Servers**] をクリックします。

b) 右側のウィンドウで、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) [**Configuration**] タブで [**NetScaler Gateway**] を展開し、[**Virtual Servers**] 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、[設定**] > [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。

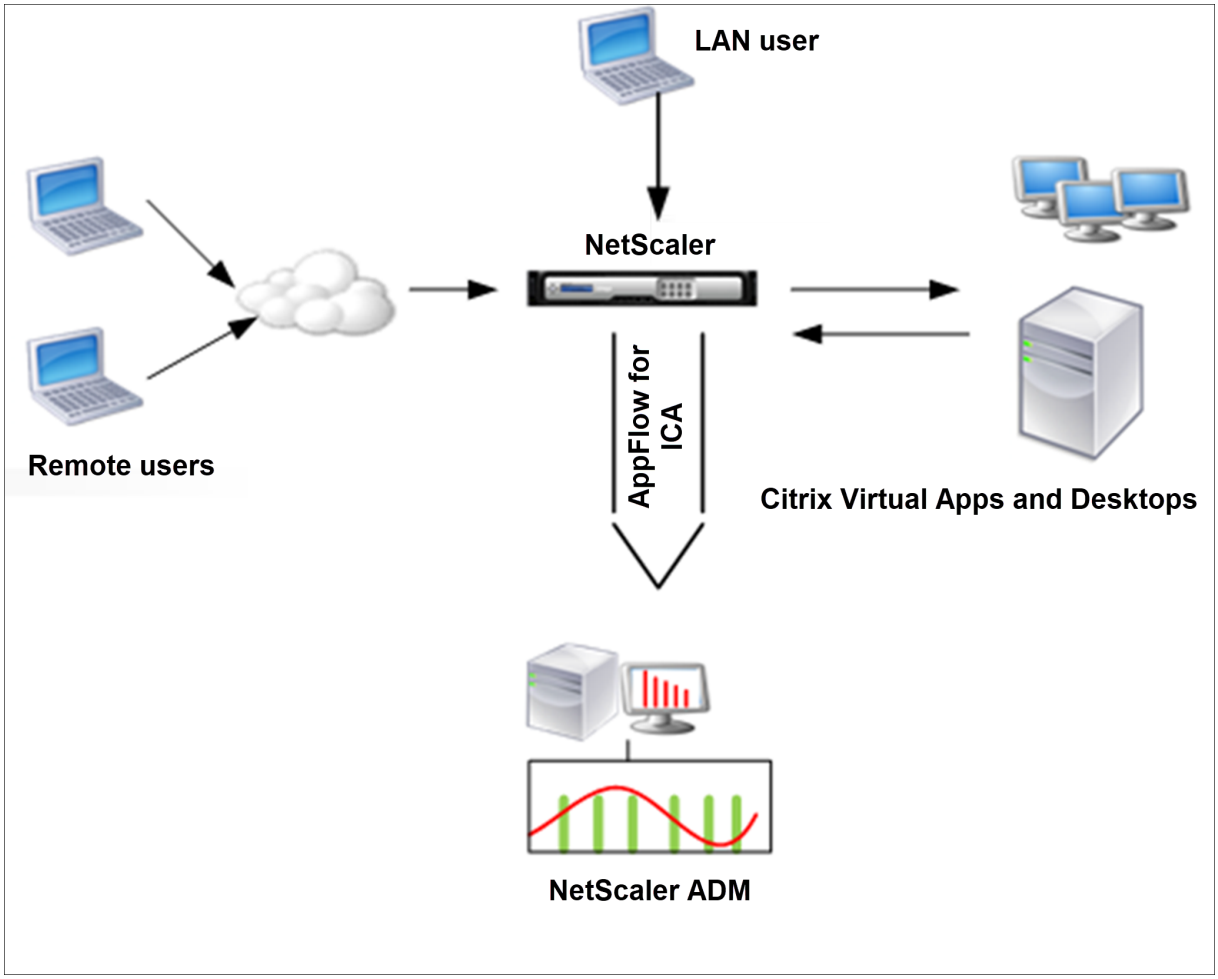
データ収集を有効にして、**LAN** ユーザーモードで展開された **NetScaler** を監視できます

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、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、透過モードで展開する場合、管理者は、ルーティングポリシーを手動で適用して、要求を NetScaler アプライアンスにリダイレクト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 アプライアンスを監視するには、まず NetScaler アプライアンスを NetScaler

Insight インベントリに追加し、AppFlow を有効にして、ダッシュボードにレポートを表示します。

NetScaler アプライアンスを NetScaler ADM インベントリに追加した後、データ収集のために AppFlow を有効にする必要があります。

> 注
>
> - NetScaler ADM 構成ユーティリティを使用して、LAN ユーザーモードで展開された NetScaler でデータ収集を有効にすることはできません。
> - コマンドとその使用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** 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。

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
    cacheType <cachetype>] [ - cltTimeout <secs>]
<!--NeedCopy-->
```

例:

```
add cr vserver cr1 HDX 10.12.2.2 443  - cacheType FORWARD  -
    cltTimeout 180
<!--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。

```
add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]

add vpn trafficPolicy** \<name\> \<rule\> \<action\>
<!--NeedCopy-->
```

例:

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
<!--NeedCopy-->
```

3. NetScaler ADM を AppFlow コレクタとして NetScaler アプライアンスに追加します。

```
add appflow collector** \<name\> \*\*-IPAddress\*\* \\<ip\\_addr
    \\>
<!--NeedCopy-->
```


例:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--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。

```
add appflow action** \<name\> \*\*-collectors\*\* \<string\> ...
<!--NeedCopy-->
```

例:

```
add appflow action act -collectors MyInsight
<!--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。

```
add appflow policy** \<policyname\> \<rule\> \<action\>
<!--NeedCopy-->
```

例:

```
add appflow policy pol true act
<!--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。

```
bind appflow global** \<policyname\> \<priority\> \*\*-type\*\* \<
   type\>
<!--NeedCopy-->
```

例:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--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。

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

例:

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. 構成を保存します。


```
save ns config
<!--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

NetScaler Application Delivery Management（ADM）上の HDX Insight を使用すると、NetScaler インスタンスを通過する HDX トラフィックを監視できます。NetScaler ADM では、Insight トラフィックの監視に使用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スを選択します。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 NetScaler ADM に表示したり、モバイルデバイスでメールまたは SMS としてアラートを受信したり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て、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. NetScaler ADM で、［設定］**>**［分析設定］**>**［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。

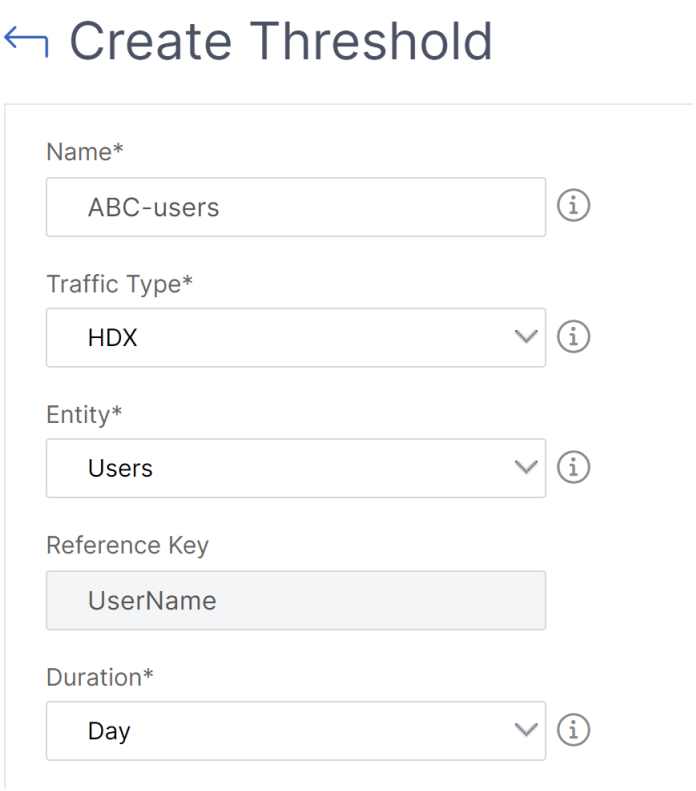
a) 名前。NetScaler ADM がアラートを生成するイベントを作成するための名前を入力します。

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。

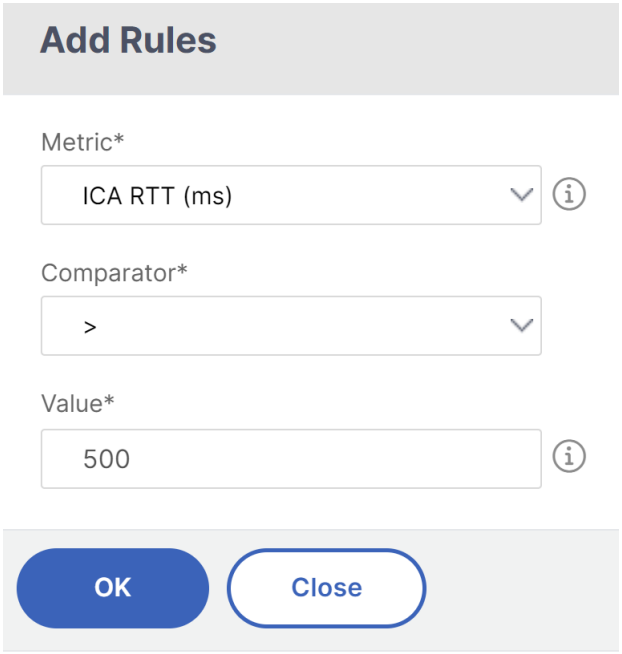
d) 参照キー。参照キーは、選択したトラフィックタイプとエンティティに基づいて自動的に生成されます。

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。

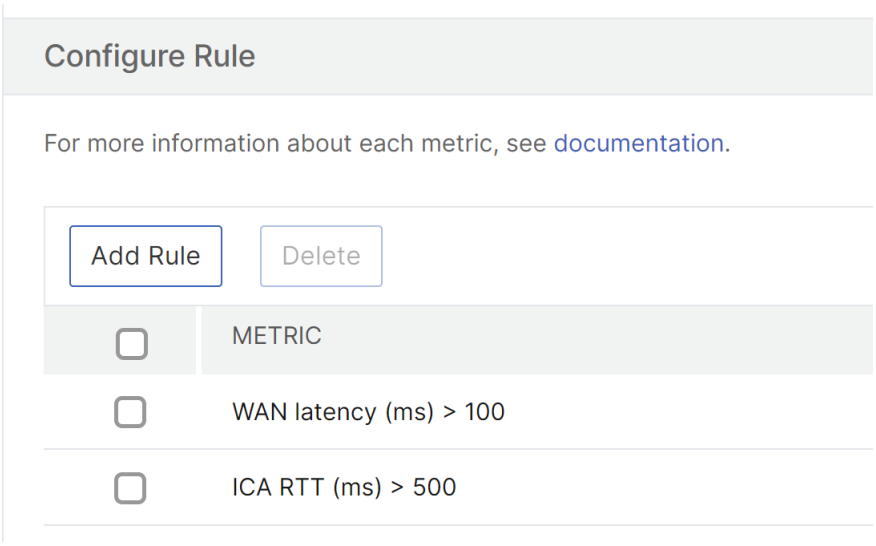


3. すべてのエンティティのしきい値ルールグループを作成しています。

   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。

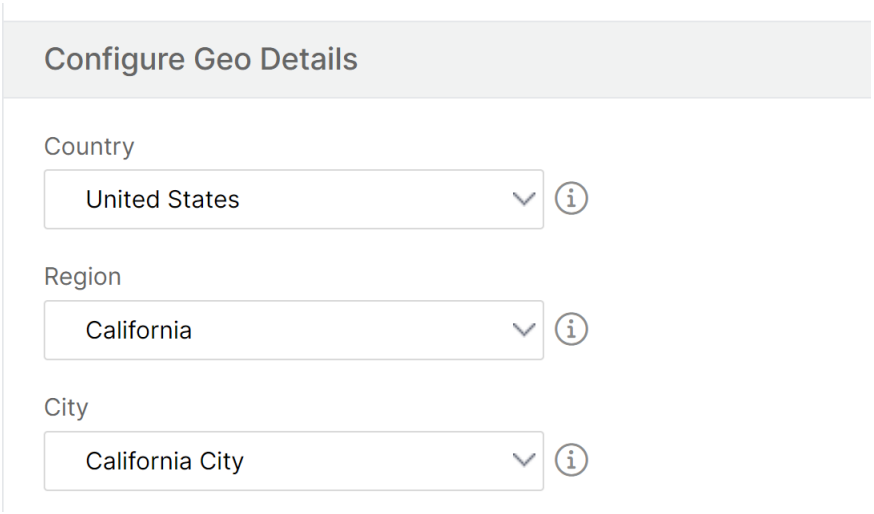


複数のルールを作成して、各エンティティを監視できます。1 つのグループに複数のルールを作成すると、個々のルールではなく、しきい値ルールのグループとしてエンティティを監視できます。[**OK**] をクリックしてウィンドウを閉じます。



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。



5. ［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。
6. オプションで、電子メール通知や SMS 通知などのアクションを構成します。
7. [**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。

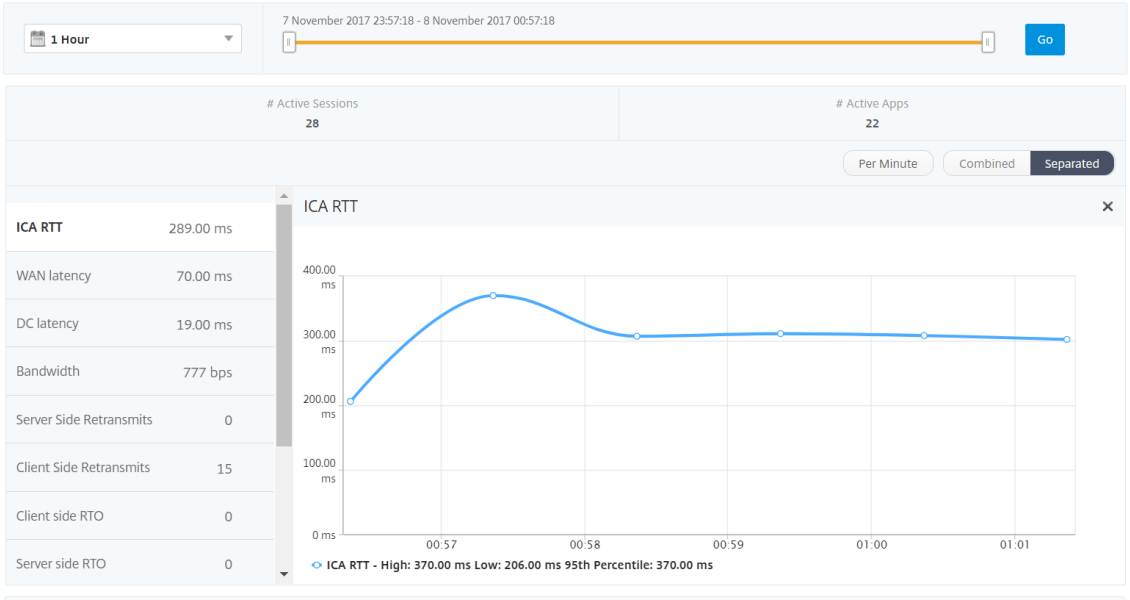
- ユーザー: 選択した時間間隔内に Citrix Virtual App または Desktop にアクセスするすべてのユーザーのレポートを表示します。
- アプリケーション**:** アプリケーションの総数のレポートと、指定された時間間隔内にアプリケーションが起動された合計回数など、関連するすべての情報を表示します。
- インスタンス: 着信トラフィックのゲートウェイとして機能する NetScaler ADC インスタンスに関するレポートを表示します。
- デスクトップ: 選択した期間内に使用されたデスクトップのレポートを表示します。
- ライセンス: 指定したタイムスロット内に使用された SSL VPN ライセンスの合計に関するレポートを表示します。

ユーザービューのレポートとメトリック

このビューのレポートとメトリックは、Citrix Virtual Apps and Desktops ユーザーごとに表示されます。

ユーザー・ビューに移動するには、次の手順に従います。

1. [ゲートウェイ**] > [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

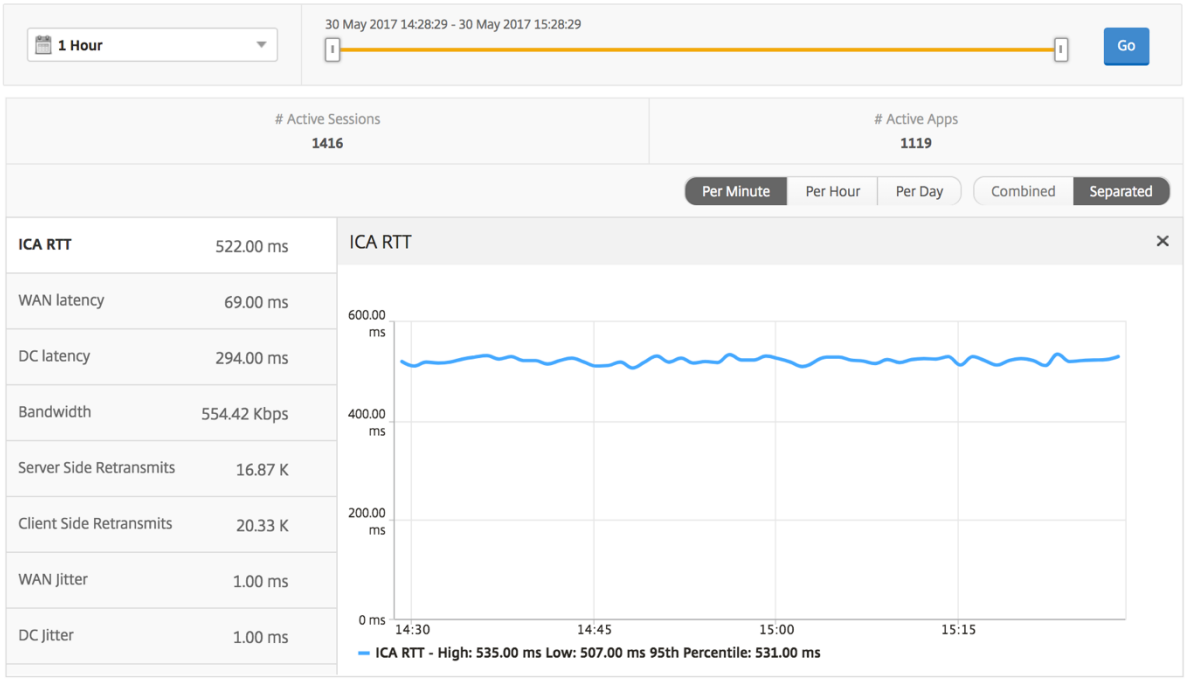
[Summary] ビューには、選択した期間中にログインしたすべてのユーザーのレポートが表示されます。このビューのすべての指標/レポートには、特に指定がない限り、選択した期間の対応する値が表示されます。

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	選択した期間中にエンドツーエンドの通信にかかった 1 秒あたりの合計バイト数。
サーバー側の再転送	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ド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ド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 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	選択した期間中にエンドツーエンドの通信にかかった 1 秒あたりの合計バイト数。
サーバー側の再転送	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。

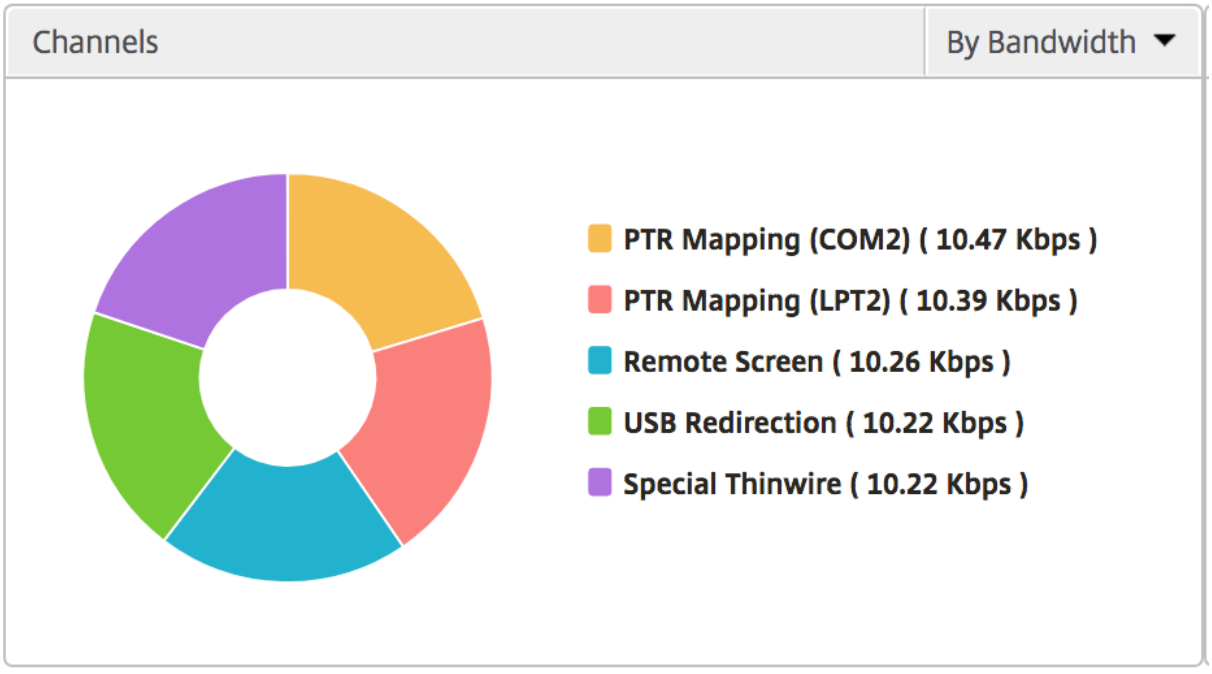
メトリックス	説明
クライアント側の再転送	NetScaler ADC とエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	NetScaler ADC とエンドユーザー間の接続で再送信タイムアウトが発生した回数。
Server side fast RTO	NetScaler ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。
クライアント側のゼロ ウィンドウ サイズ イベント	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ド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ド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。

Users

Search

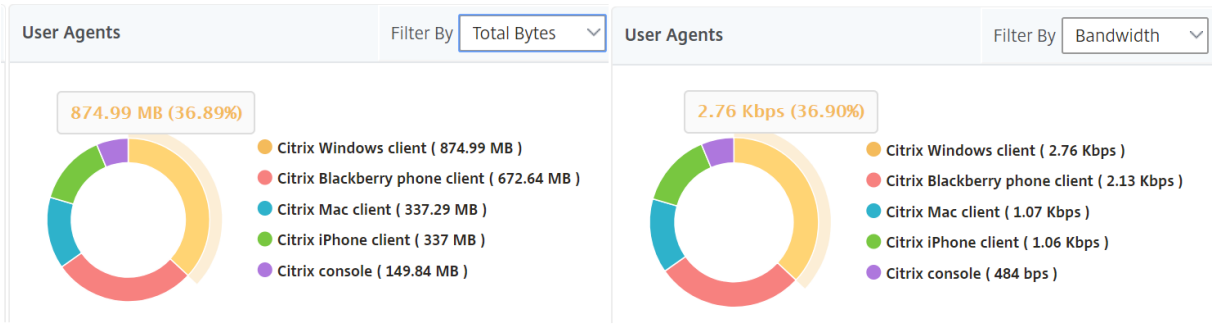
User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	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	
randyb	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	

チャネル　Channels では、各 ICA 仮想チャ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、各ワークスペースクライアントが消費する全体的な帯域幅/合計バイト数をドーナツグラフの形式で表します。グラフの各色付きセグメントは、1 つのワークスペースクライアント

を表します。セグメントの長さは、そのワークスペースクライアントでアプリケーションを起動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、そのワークスペースクライアントを使用しているユーザーの詳細が表示されます。

User Details

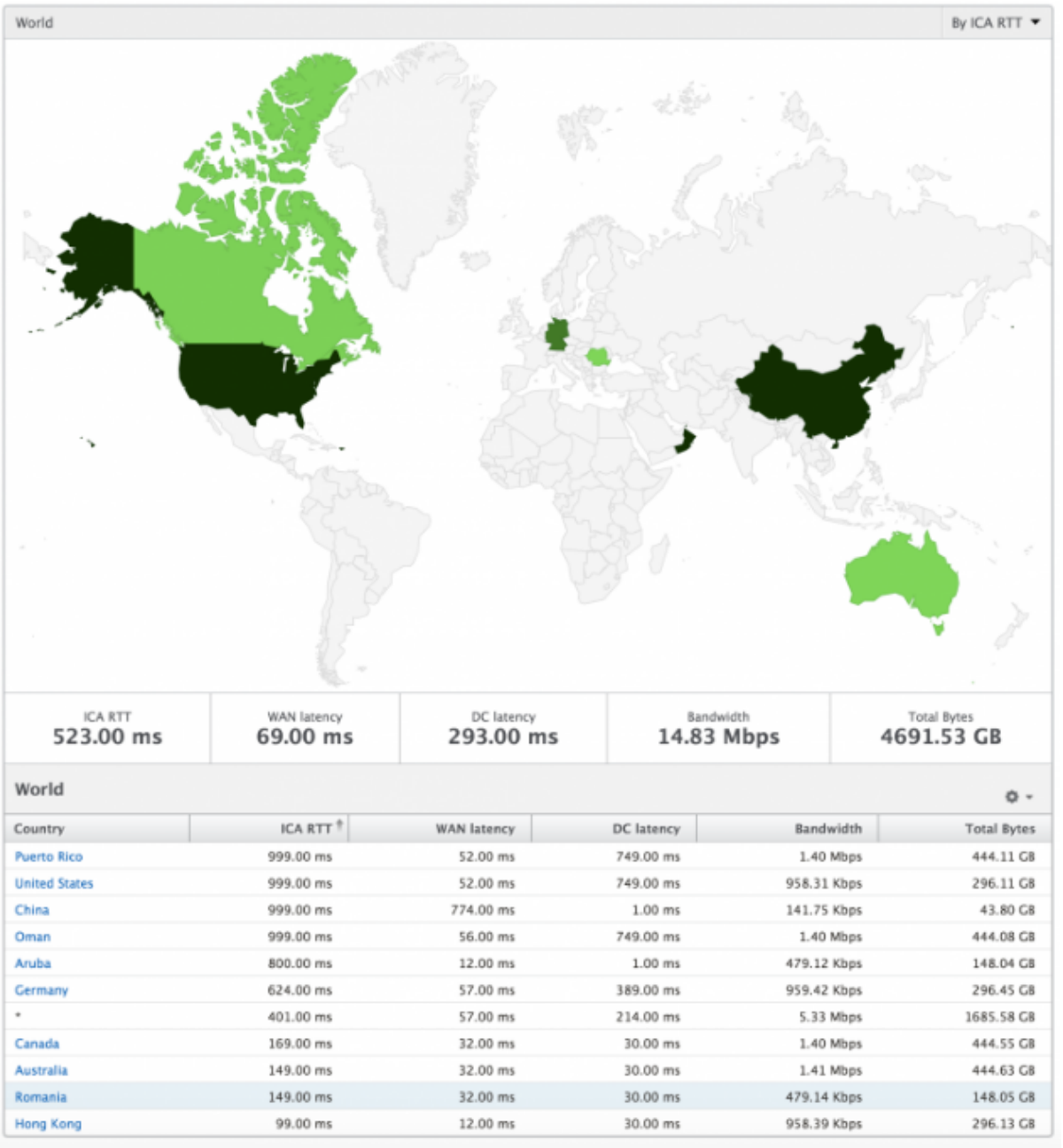
Name	Server Side Retransmits	ICA RTT	Client SRTT	Session Reconnect	Latency	Clientside zero window size event	Server SRTT
c1\daniel	0	149.44	1		149.44	0	
ryan	5071	4640	1		4640	0	
ramas	0	994.71	1		994.71	0	

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



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

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 にログオンします。
2. [**Gateway] > [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 を通過する ICA トラフィックの平均遅延時間。
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	ワークスペースタイプ-Citrix Windows クライアントなど
クライアントのバージョン	ワークスペースバージョン。
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 ユーザー/トランスペアレントモードなどです。

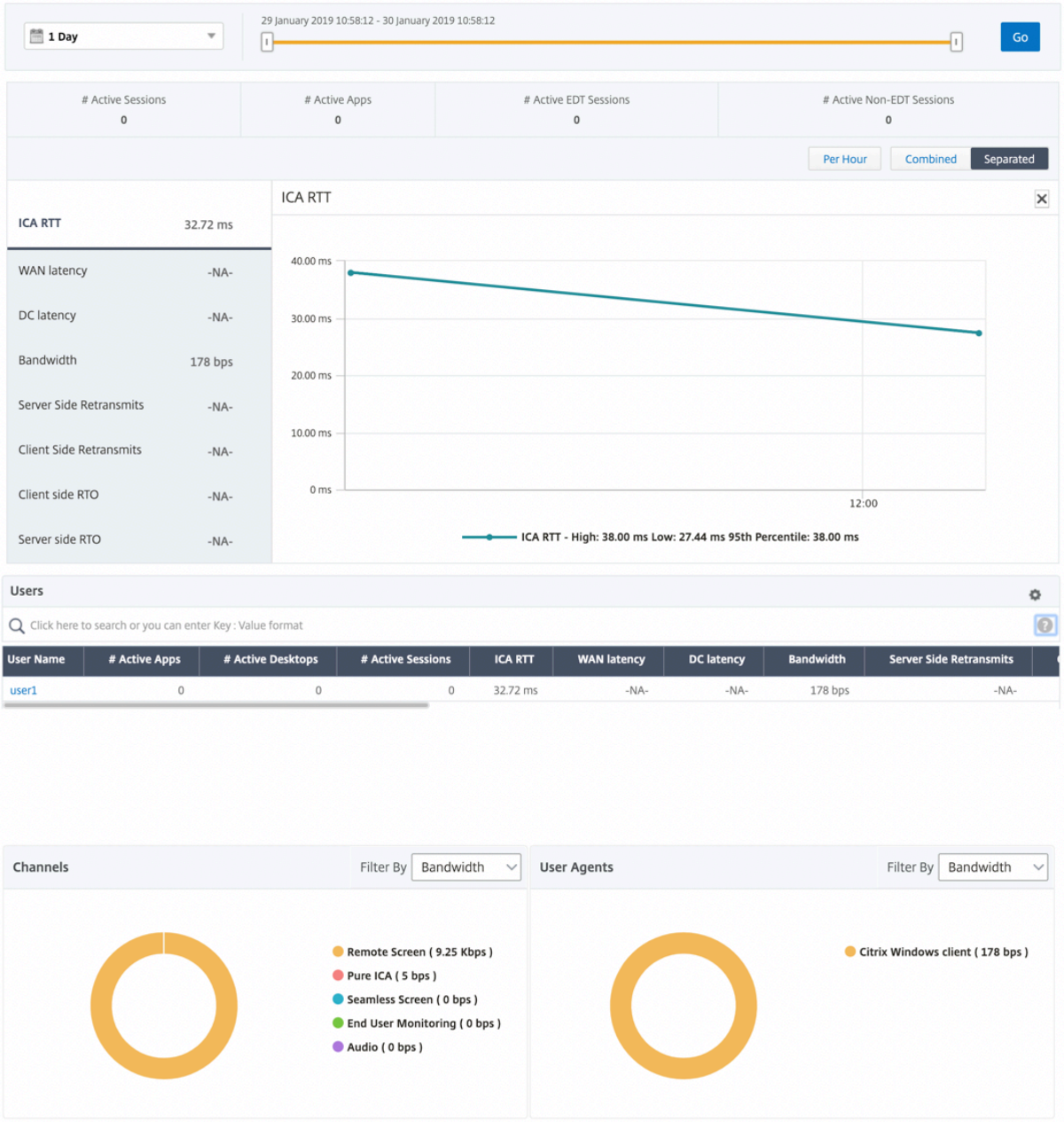
メトリックス	説明
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA 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。

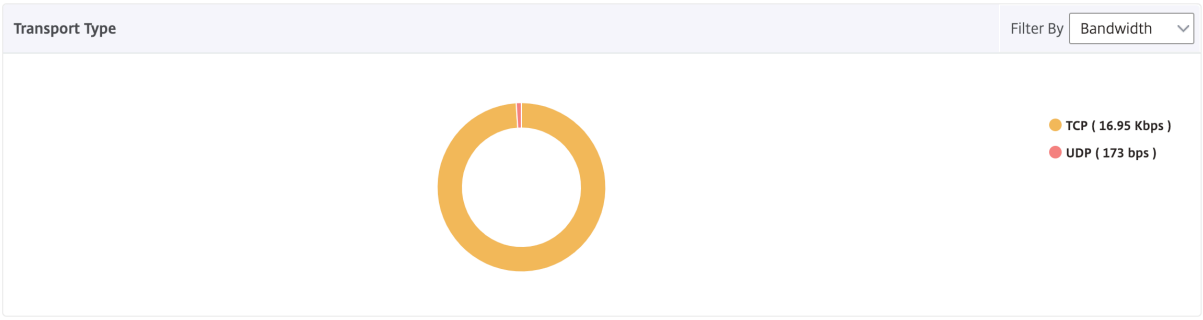
HDX Insight における **EDT** のサポート

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 Workspace を実行しているユーザーは、仮想デスクトップのセッション中の高解像度のユーザーエクスペリエンスを保証します。

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。



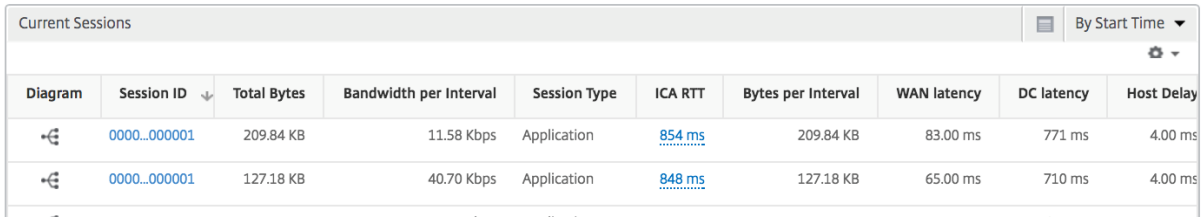
新しいドーナツグラフが導入され、ユーザーが使用したプロトコルの種類に基づいて、ユーザーが消費した帯域幅と合計バイト数を確認できるようになりました。

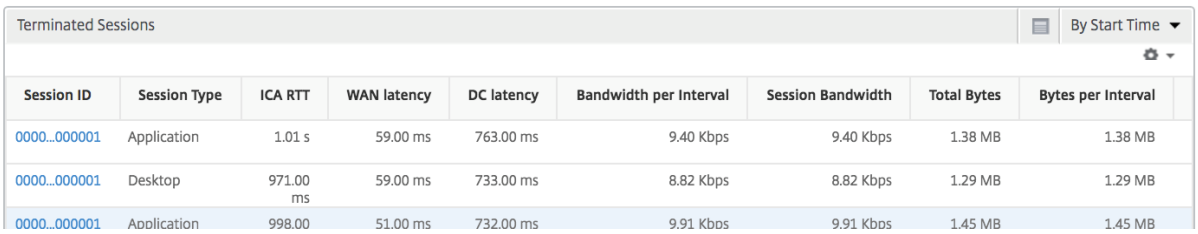


> 注
>
> HDX Insight の EDT は、リリース 12.1 ビルド 50.28 の NetScaler ADM でサポートされ、リリース 12.1 ビルド 49.23 の ADC インスタンスで使用できます。

NetScaler ADM 12.0 以降から入手可能な **HDX Insight** メトリック:

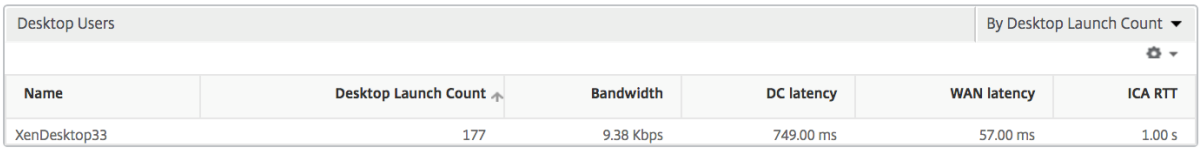
L7 Client-side Latency	ICA クライアントと NetScaler ADC インスタンスの間で観測された平均 L7 遅延時間。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。
L7 Server-side Latency	NetScaler ADC デバイスと Citrix Virtual Apps の間で観察された平均 L7 遅延。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。
違反の最大遅延	定義済みしきい値の違反が一定期間に発生した場合の、L7 遅延の最大値。
平均侵害待ち時間	システムが「L7 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。



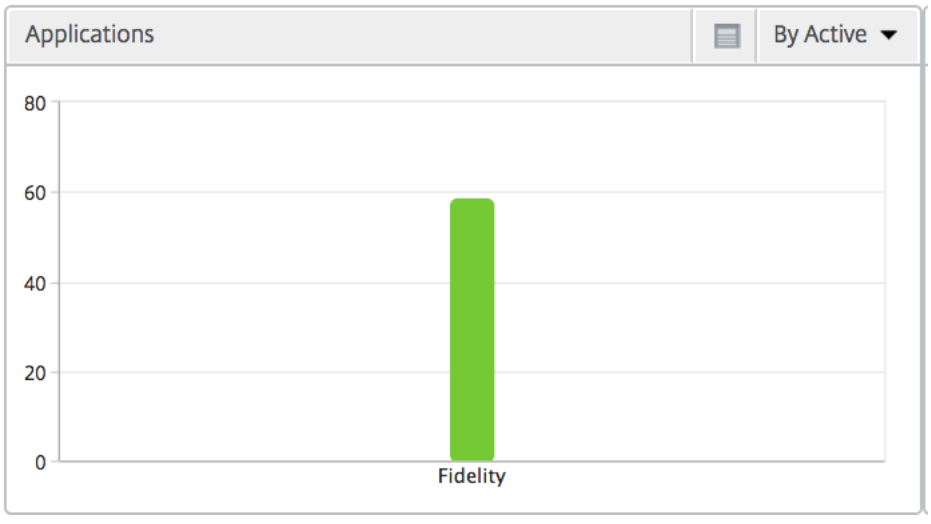


デスクトップユーザー　この表は、特定のユーザーの Citrix Virtual Desktop セッションに関する洞察を示しています。以下のメトリクスは［Desktop Launch Count］および［Bandwidth］を基準にしてソートできます。

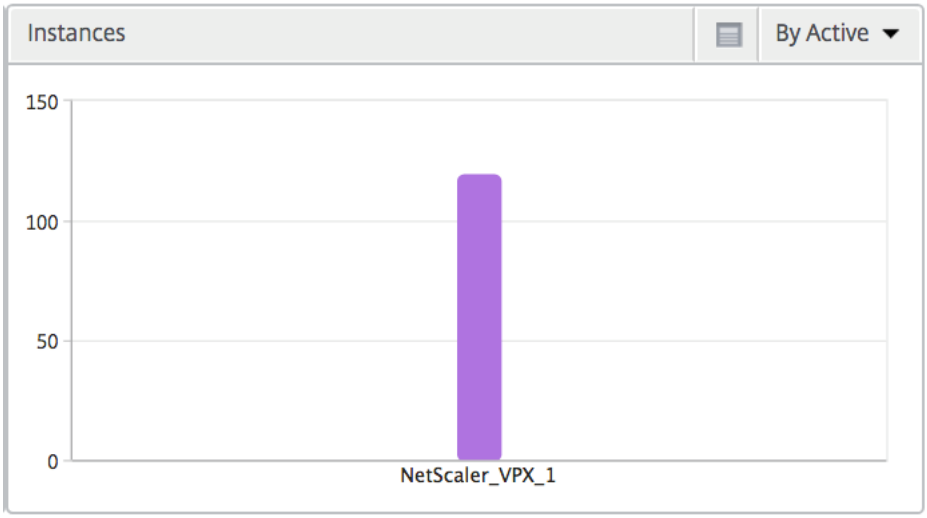
メトリックス	説明
名前	Citrix Virtual Desktops の名前。
デスクトップ起動回数	デスクトップが起動された回数です。
帯域幅	選択した期間中にエンドツーエンドの通信にかかった 1 秒あたりの合計バイト数。
DC 遅延	NetScaler Gateway と VDI、CVAD、または StoreFront サーバーとの間で、ネットワークのサーバー側で発生する遅延。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop 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。



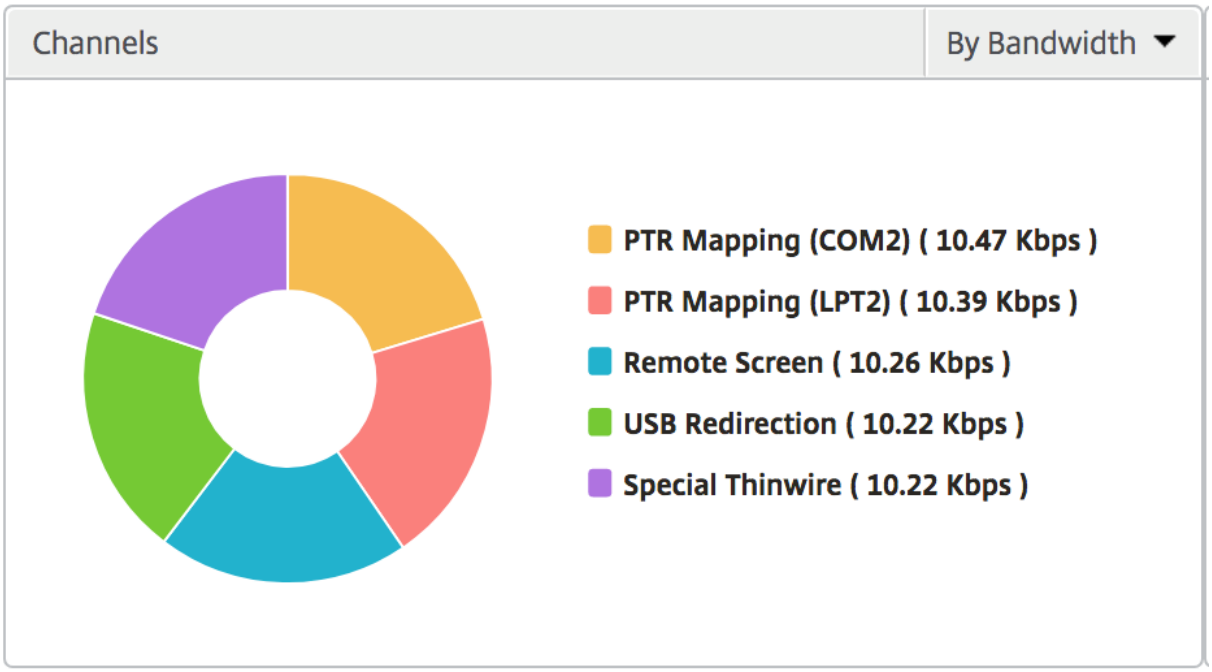
アプリケーション　アクティブでソートされたアプリ、合計セッション起動数、合計アプリ起動数、および起動期間を表す棒グラフ。



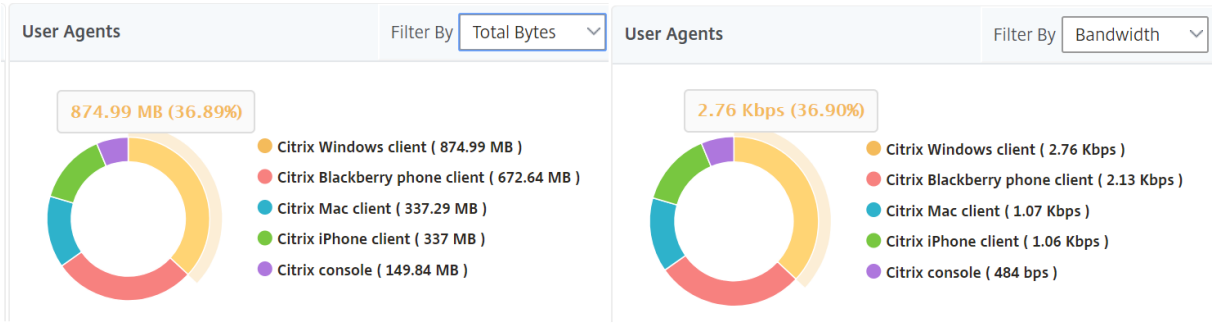
インスタンス　NetScaler インスタンスをアクティブおよび合計アプリでソートした棒グラフ



チャネル　Channels では、各 ICA 仮想チャ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。

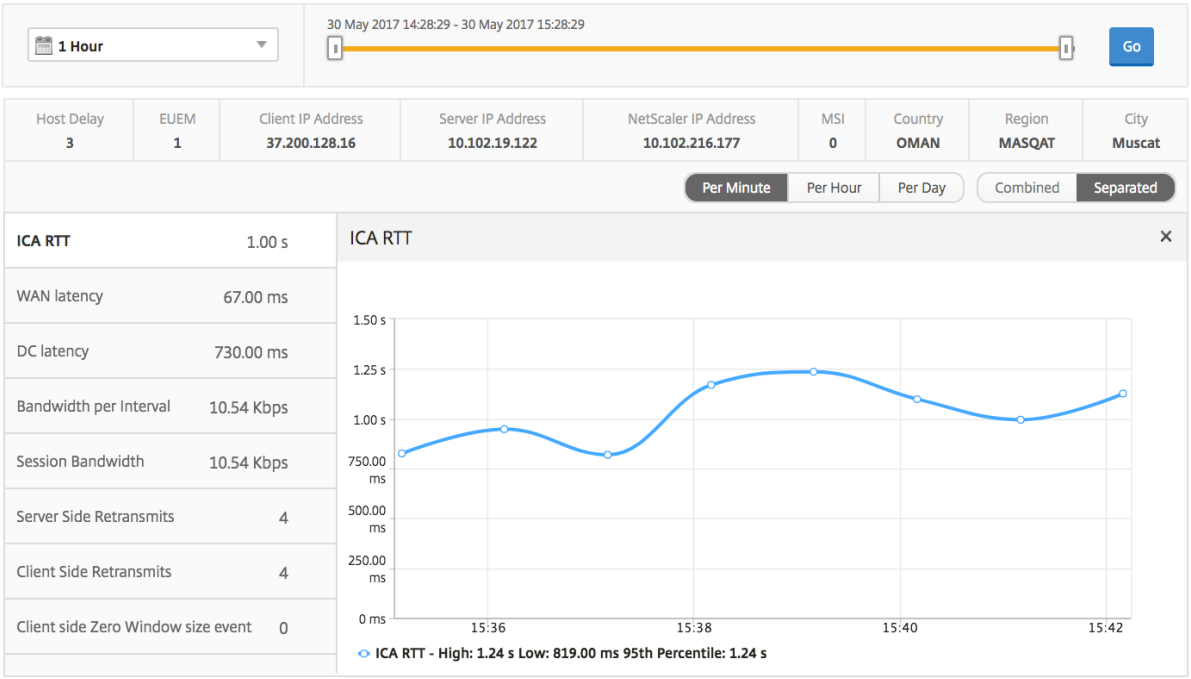
選択したユーザーのセッションのメトリックを表示する手順は、次のとおりです。

1. [**Gateway] > [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。

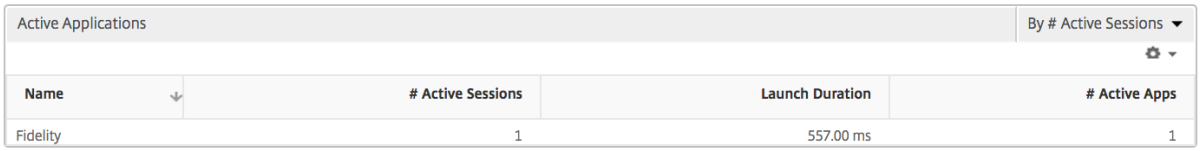
時系列グラフ

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	NetScaler Gateway と VDI、CVAD、または StoreFront サーバーとの間で、ネットワークのサーバー側で発生する遅延。
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。

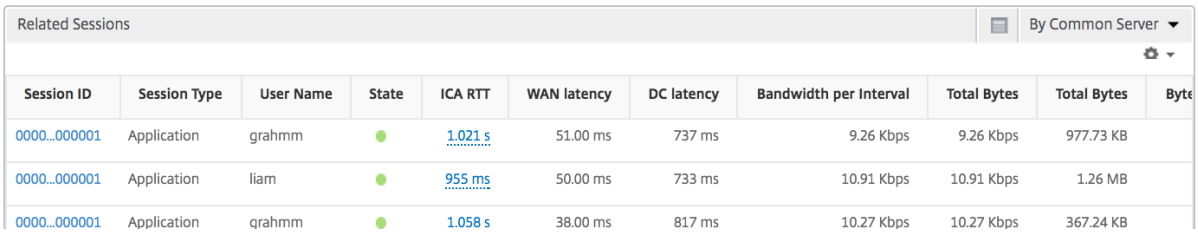
メトリックス	説明
クライアント側の再転送	NetScaler ADC とエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	NetScaler ADC とエンドユーザー間の接続で再送信タイムアウトが発生した回数。
Server side fast RTO	NetScaler ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。
間隔あたりの帯域幅	特定の期間にセッションで使用された帯域幅です。
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ドバ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ドバ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。



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。関係性は、共通サーバーと共通 NetScaler から選択できます。



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. ［ゲートウェイ**] > [HDX Insight] > [**アプリケーション］に移動します。

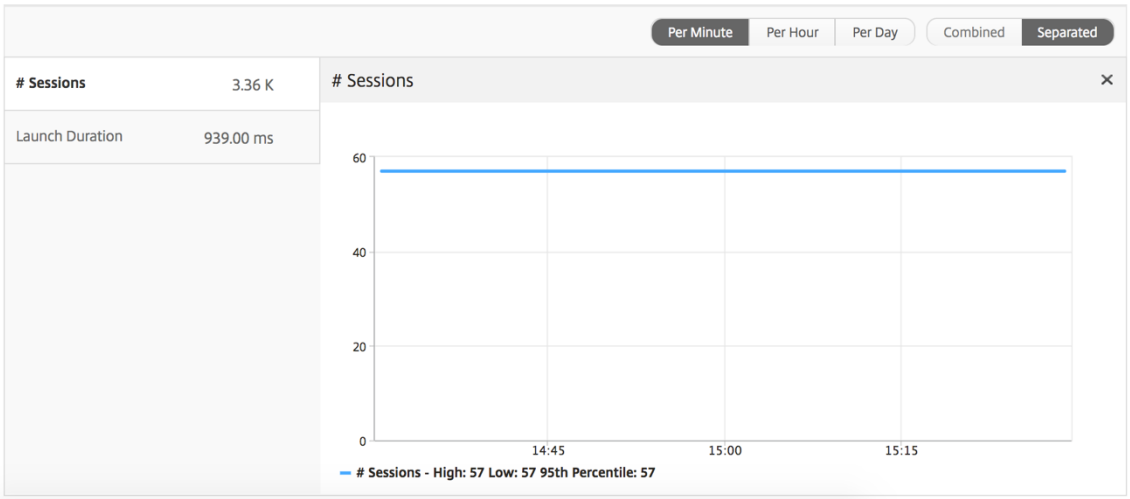
［**Summary**］ビュー

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。

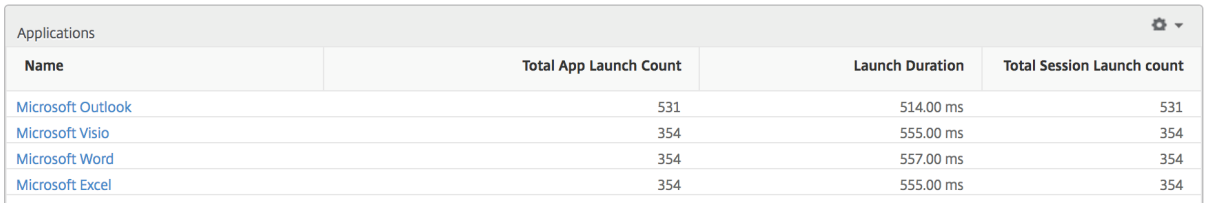
折れ線グラフ

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

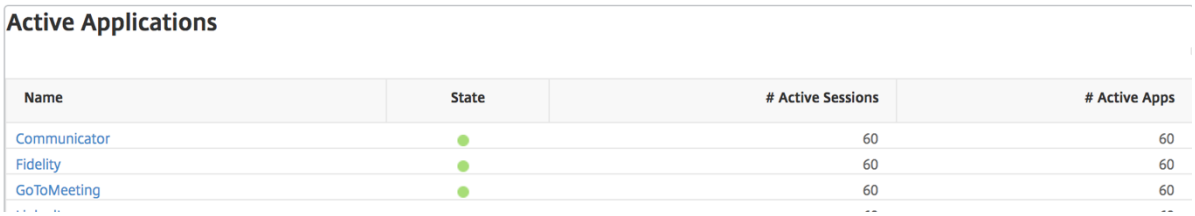
メトリックス	説明
名前	Citrix Virtual Apps の名前。
セッションの起動数合計	特定の時間間隔におけるアクティブな Citrix Virtual App セッションの総数。
アプリケーションの起動数合計	特定の期間中に起動された Citrix Virtual App アプリケーションの総数。
起動期間	Citrix Virtual App の起動に要した平均時間。



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。

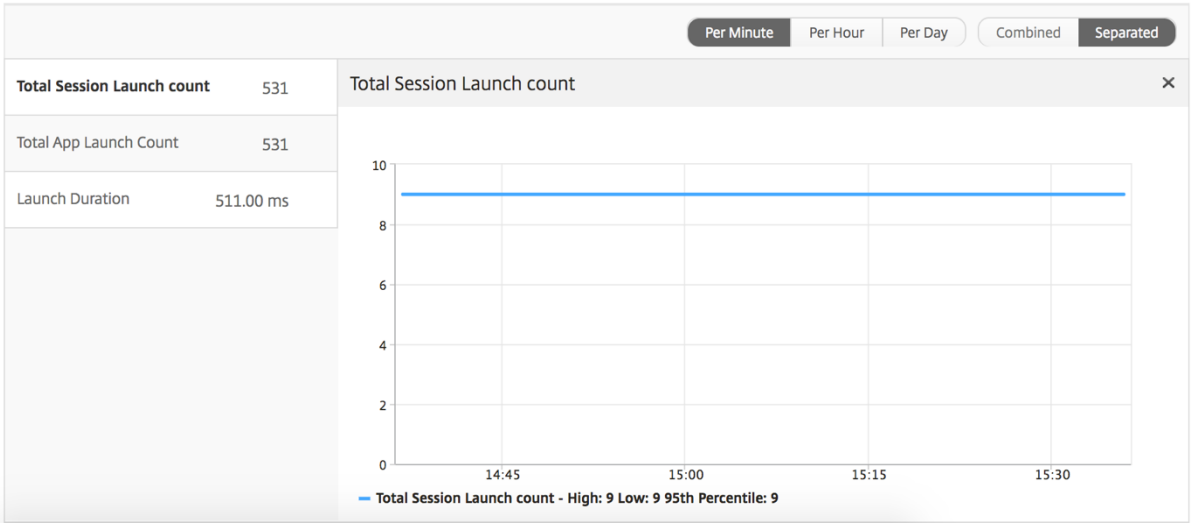
メトリックス	説明
アクティブなアプリケーション数	このアプリケーションのアクティブなセッション数。



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。

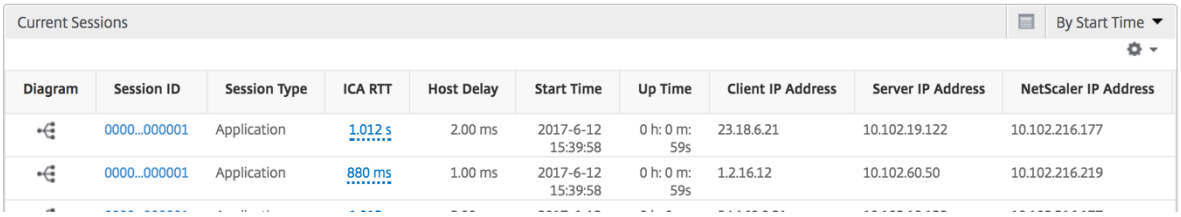


現在のセッションレポート

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 を通過する ICA トラフィックの平均遅延時間。
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	ワークスペースタイプ-Citrix Windows クライアントなど
クライアントのバージョン	ワークスペースバージョン。
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 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。

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。



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。

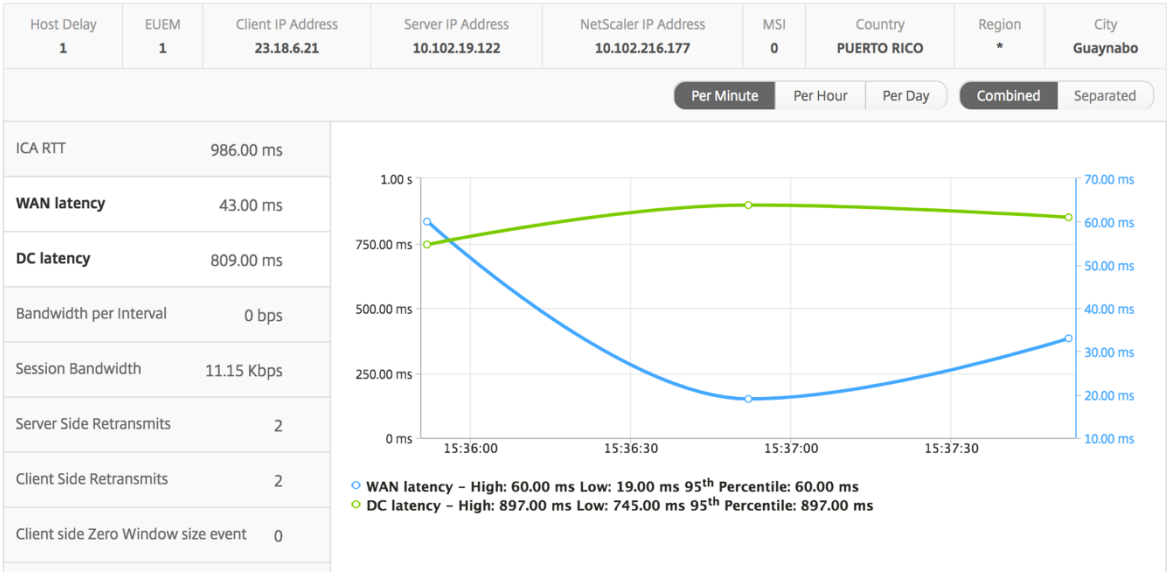
セッション・レポートを表示するには、次の手順に従います。

1. サポートされている Web ブラウザを使用して、NetScaler ADM にログオンします。
2. [ゲートウェイ**] > [HDX Insight] > [**アプリケーション] に移動します。
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。

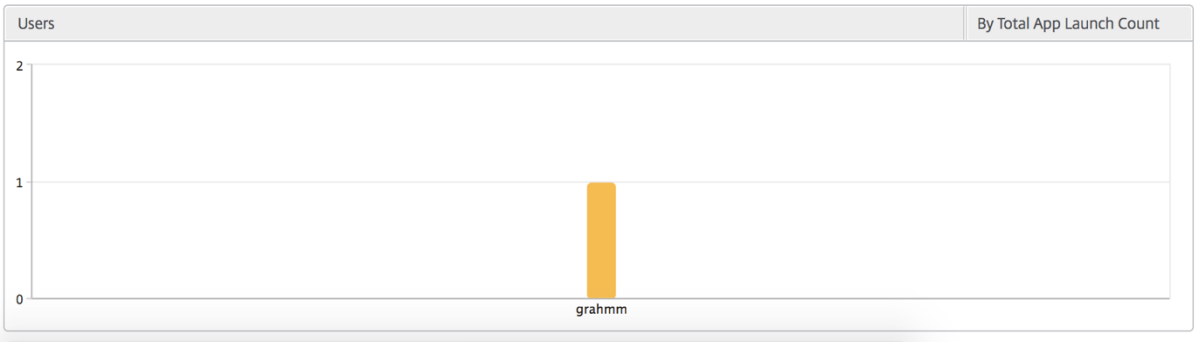
折れ線グラフ

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。
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ド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

このビューのレポートとメトリックは、Citrix Virtual Desktops に焦点を当てています。

デスクトップ・ビューに移動するには:

1. サポートされている Web ブラウザを使用して、NetScaler ADM にログオンします。
2. [ゲートウェイ] **> [HDX Insight] > [**デスクトップ] に移動します。

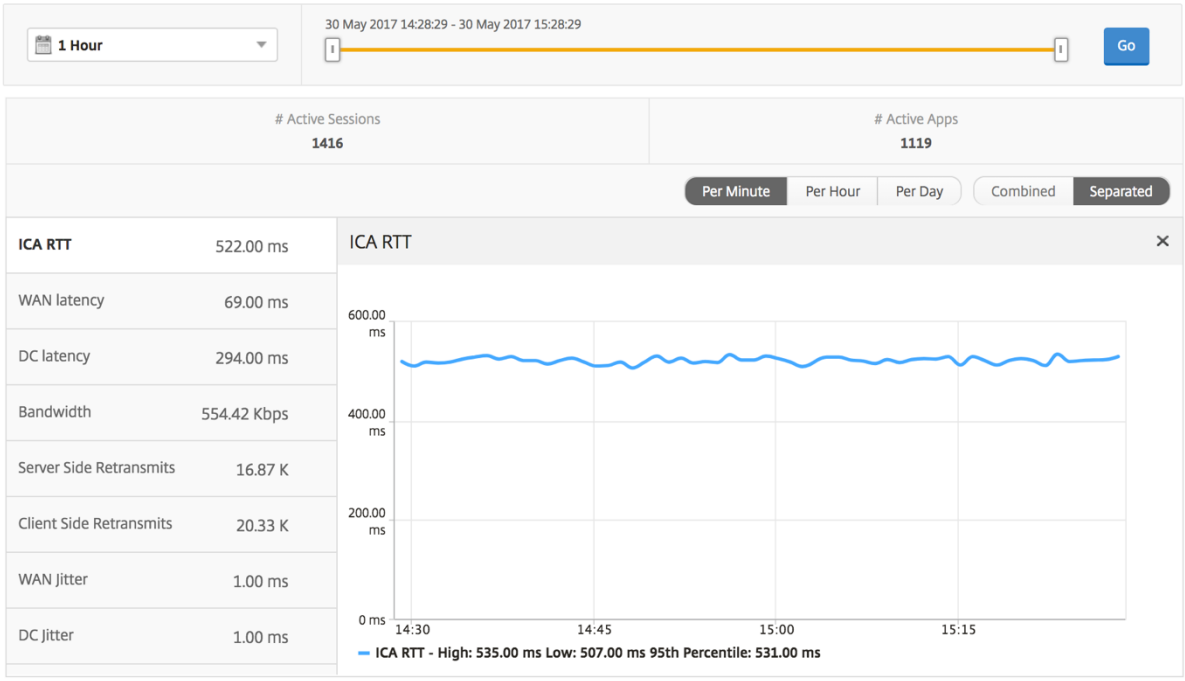
[**Summary**] ビュー

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。

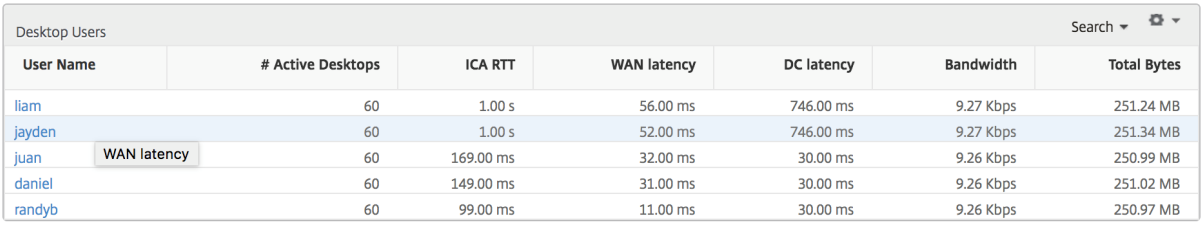
折れ線グラフ

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	選択した期間中にエンドツーエンドの通信にかかった 1 秒あたりの合計バイト数。
サーバー側の再転送	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ド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ドバ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	選択した期間中にエンドツーエンドの通信にかかった 1 秒あたりの合計バイト数。
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。



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。

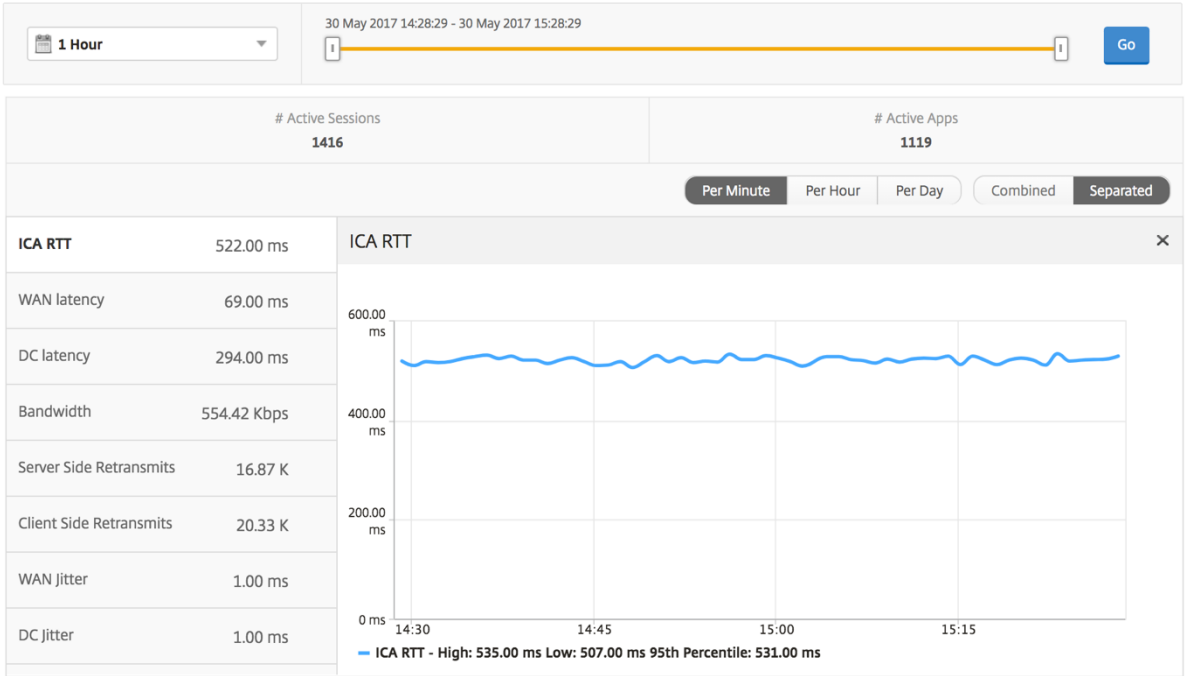
特定のデスクトップビューに移動するには**:**

1. サポートされている Web ブラウザを使用して、NetScaler 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

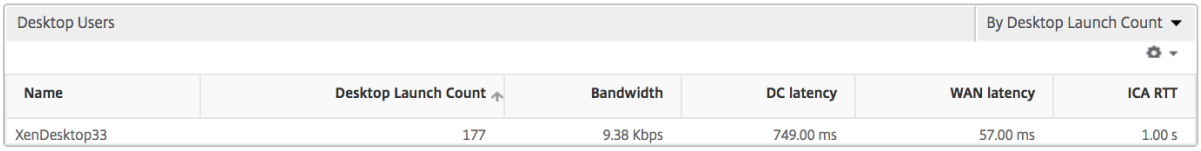
メトリック	説明
アクティブセッション	この数字は、アクティブな Citrix Virtual Apps and Desktops セッションの数を示します。
アクティブなアプリケーション数	この数字は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC から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	選択した期間中にエンドツーエンドの通信にかかった 1 秒あたりの合計バイト数。

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ド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ド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	選択した期間中にエンドツーエンドの通信にかかった 1 秒あたりの合計バイト数。
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。

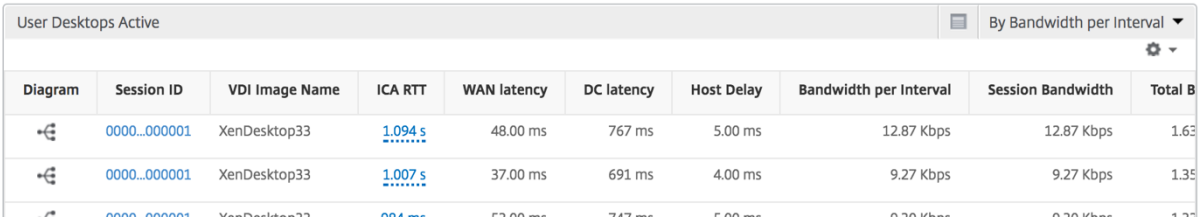


ユーザーデスクトップアクティブ/非アクティブレポート　以下のメトリクスは、[Bandwidth per Interval]、[Session Reconnects]、および［ACR Counts］を基準にしてソートできます。

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 を通過する ICA トラフィックの平均遅延時間。
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	ワークスペースタイプ-Citrix Windows クライアントなど
クライアントのバージョン	ワークスペースバージョン。
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 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 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。
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	



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、NetScaler 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。

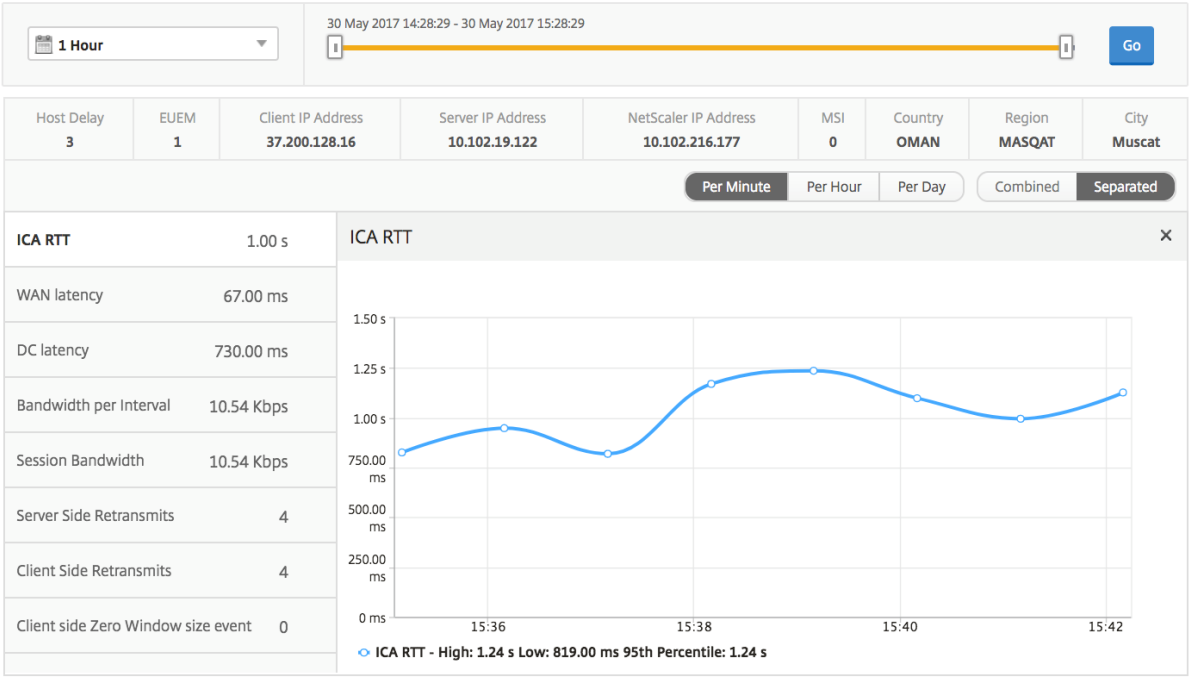
時系列グラフ　［Per User Session］ビューには、選択したユーザーのセッションに関するレポートが表示されます。

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. サポートされている Web ブラウザを使用して、NetScaler ADM にログオンします。
2. [**Gateway] > [HDX Insight] > [**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ドバ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ドバタイズした回数を表します。

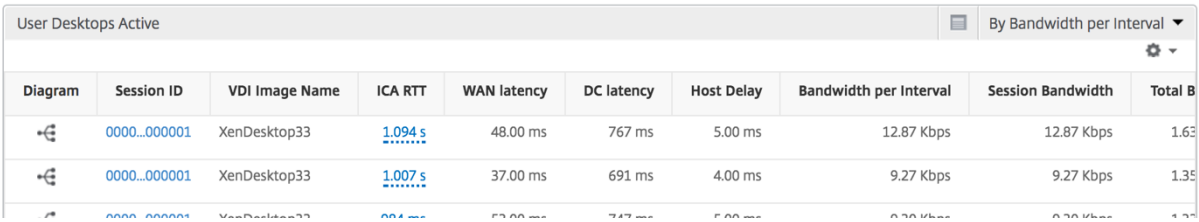


関連するデスクトップセッションレポート　以下のメトリクスは、［Bandwidth per Interval］、［Session Reconnects］、および［ACR Counts］を基準にしてソートできます。

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 を通過する ICA トラフィックの平均遅延時間。

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	ワークスペースタイプ-Citrix Windows クライアントなど
クライアントのバージョン	ワークスペースバージョン。
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 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。

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。



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 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 にログオンします。
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

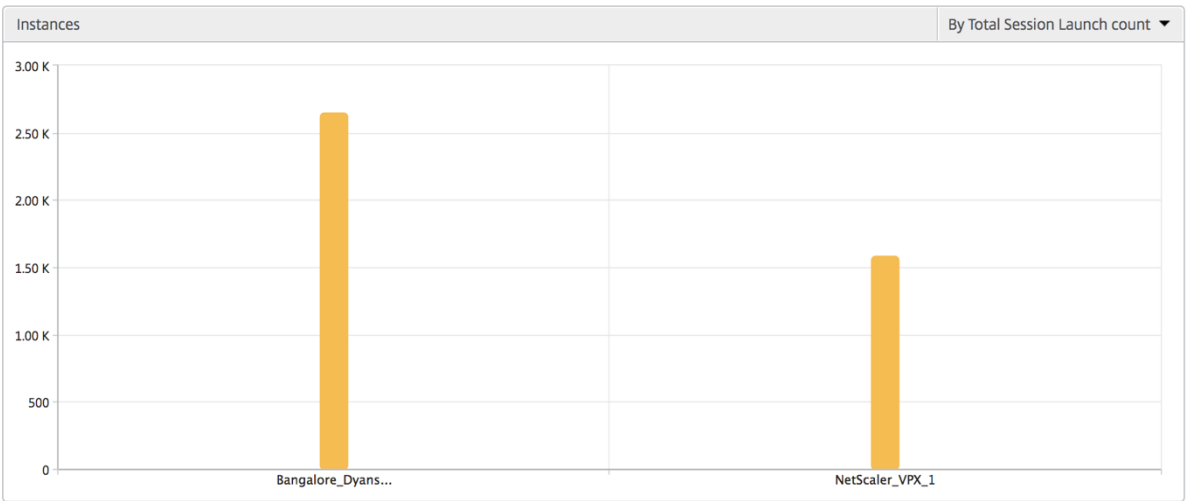
インスタンスの概要ビュー

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。

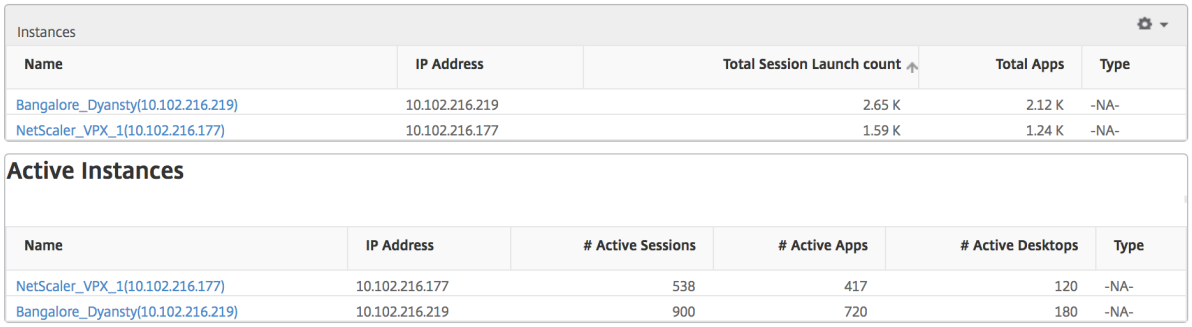
インスタンス棒グラフ

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 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	-



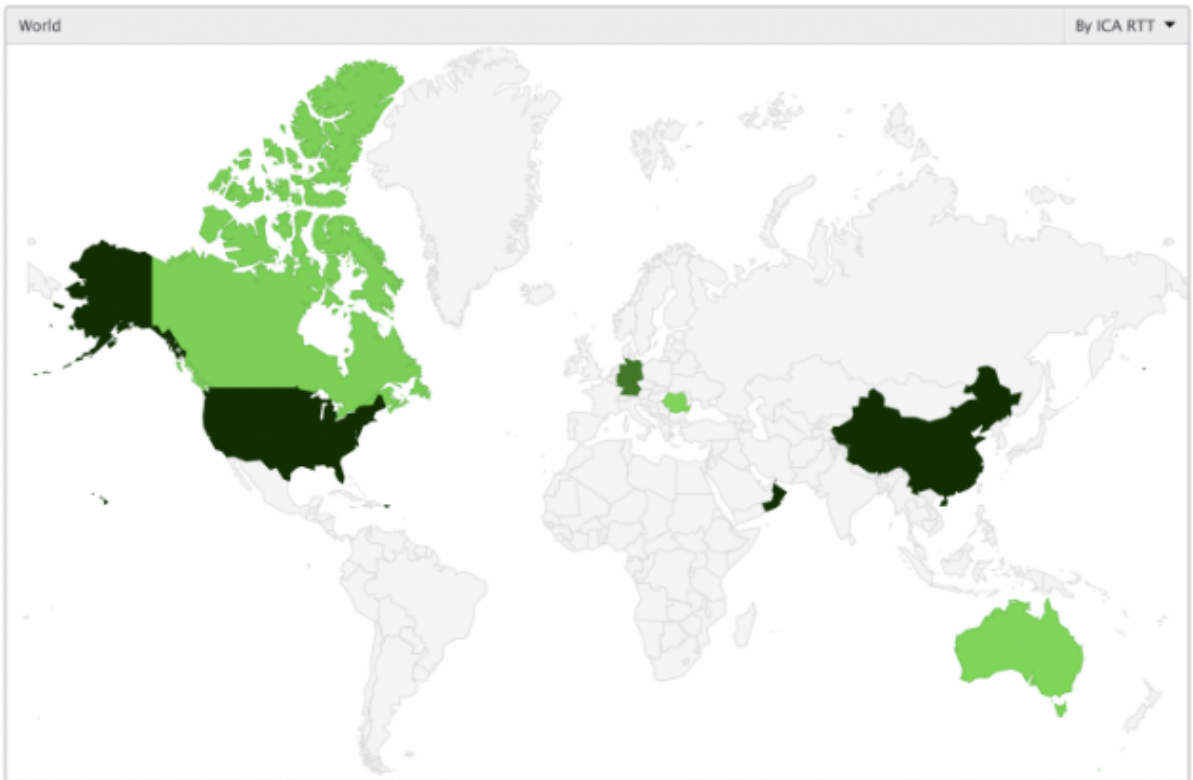
しきい値レポート　しきい値レポートは、選択した期間内に エンティティ がインスタンスとして選択された場合に、違反したしきい値の数を表します。詳細については、「しきい値の作成方法」を参照してください。

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バージョンの Citrix Virtual Apps and Desktops を使用している、サポートされていないバージョンのワークスペースまたはワークスペースタイプを使用しているなど、さまざまな理由で発生する可能性があります。この表には、IP アドレスとスキップされたフロー数が表示されます。これらのワークスペースは、ホワイトリストに登録されているワークスペースの一部ではない可能性があります。したがって、これらのセッションはモニタリングからスキップされます。

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



World

Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

インスタンスごとのビュー

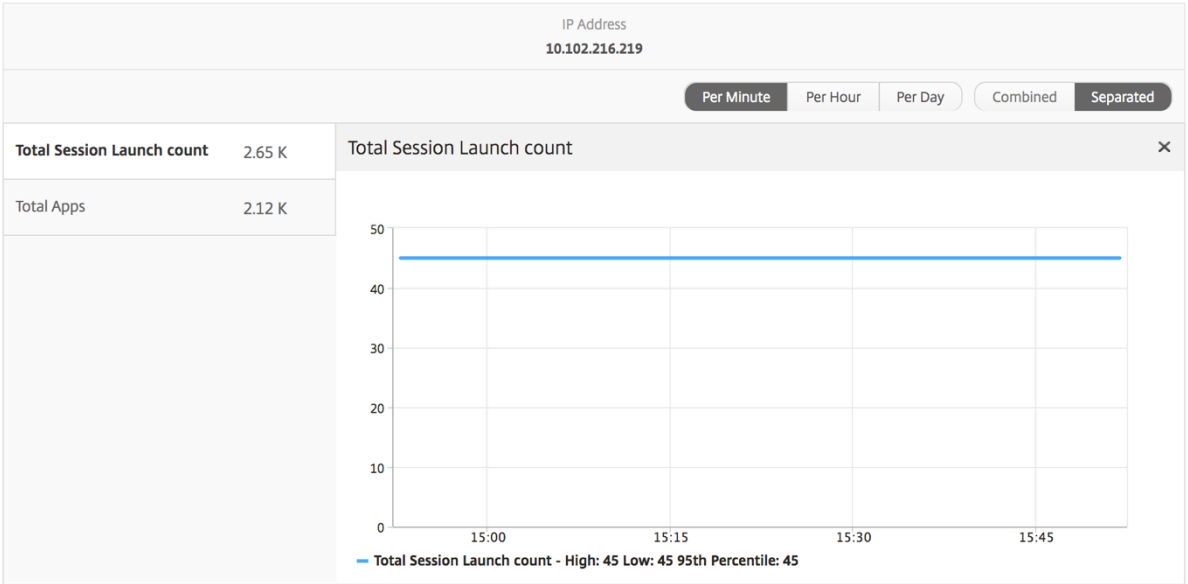
インスタンス別ビューには、選択した特定の NetScaler インスタンスの詳細なエンドユーザーエクスペリエンスに関するレポートが示されます。

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。

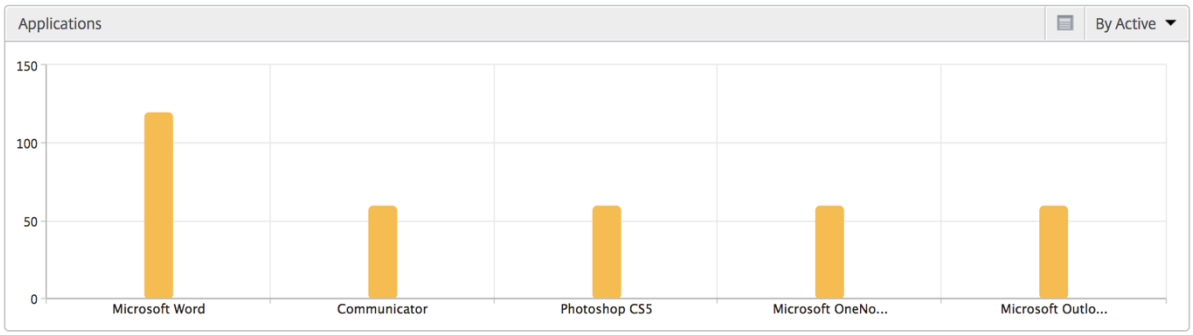
1. サポートされている Web ブラウザを使用して、NetScaler ADM にログオンします。
2. [分析] **> [HDX Insight] > [**インスタンス] に移動します。
3. インスタンス 概要レポートから特定のインスタンスを選択します。

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。

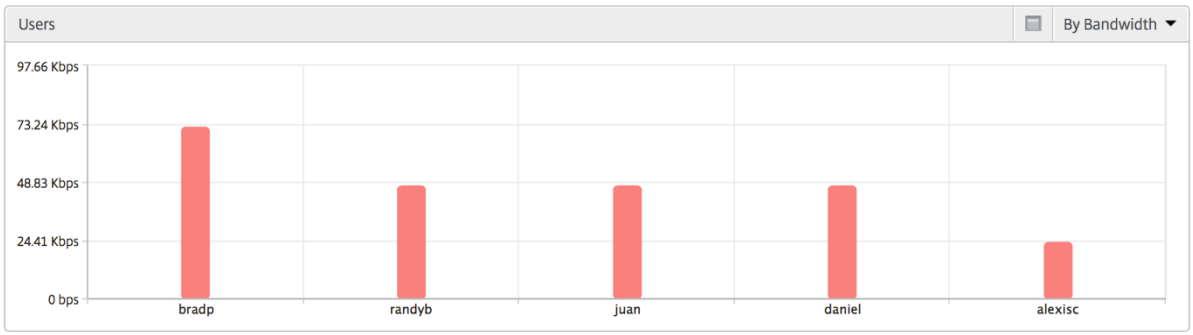


アプリケーション棒グラフ　アクティブなアプリ、セッションの合計起動数、アプリの合計起動数、起動時間などの条件に基づいて、上位 5 個のアプリケーションを表示します。



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。

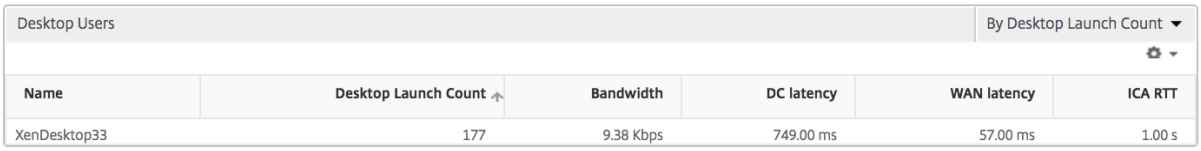
- 帯域幅
- WAN 遅延
- DC の遅延
- ICA 往復時間



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	選択した期間中にエンドツーエンドの通信にかかった 1 秒あたりの合計バイト数。
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。

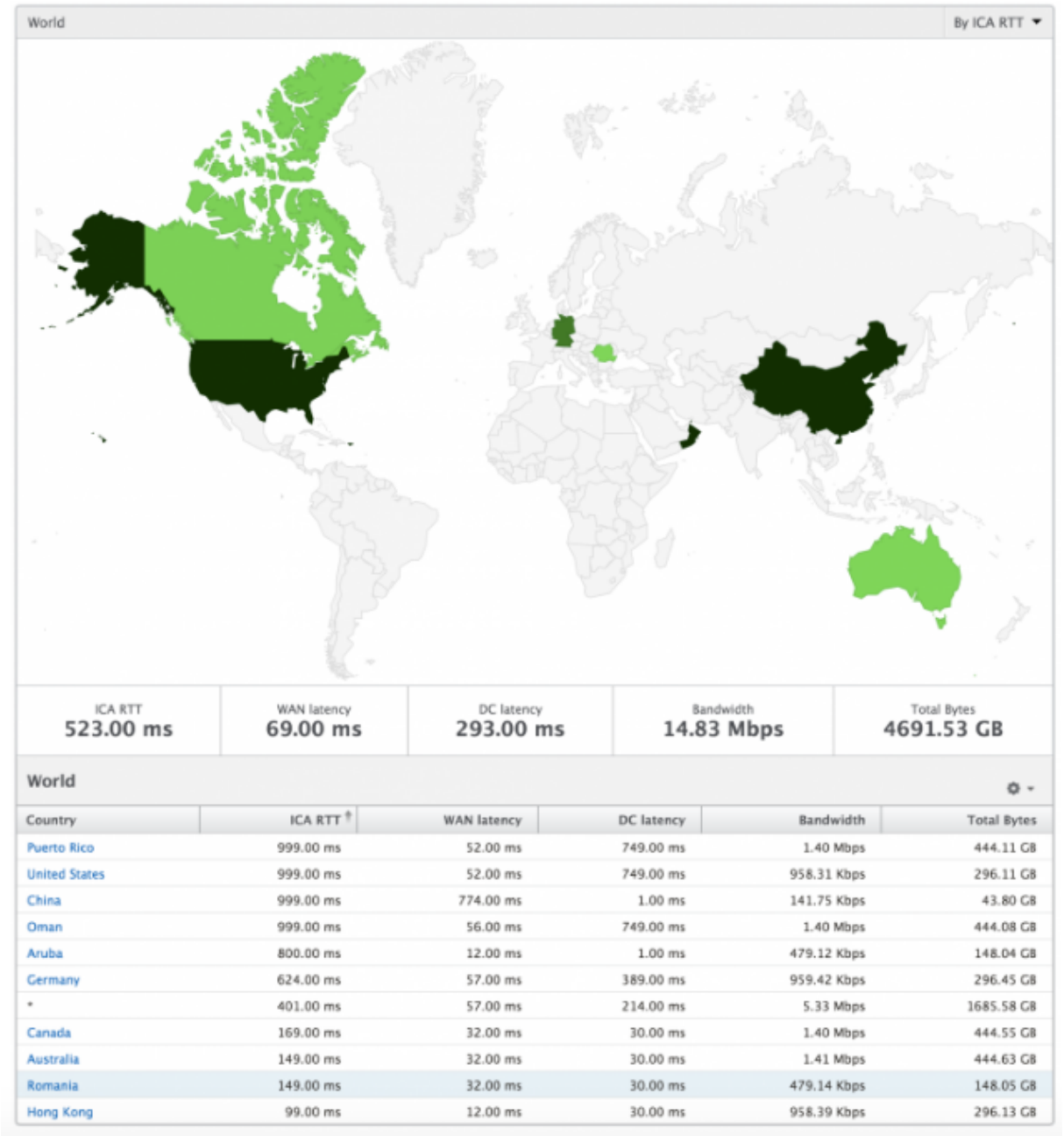
メトリックス	説明
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。



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



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

ライセンスビューのレポートとメトリック

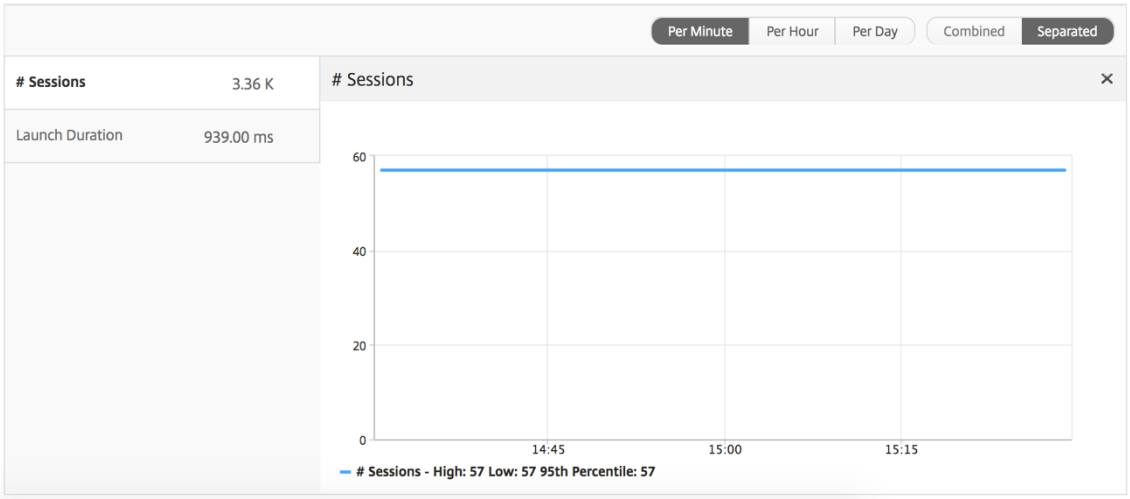
ライセンスビューには、NetScaler Gateway のライセンス情報が表示されます。

[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	選択したタイムラインで使用されている NetScaler ADC ゲートウェイ 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 ADC ゲートウェイ CCU ライセンスの総数。



しきい値レポート　しきい値レポートは、選択した期間内に 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. [ゲートウェイ**] > [HDX Insight] > [**アプリケーション] に移動します。

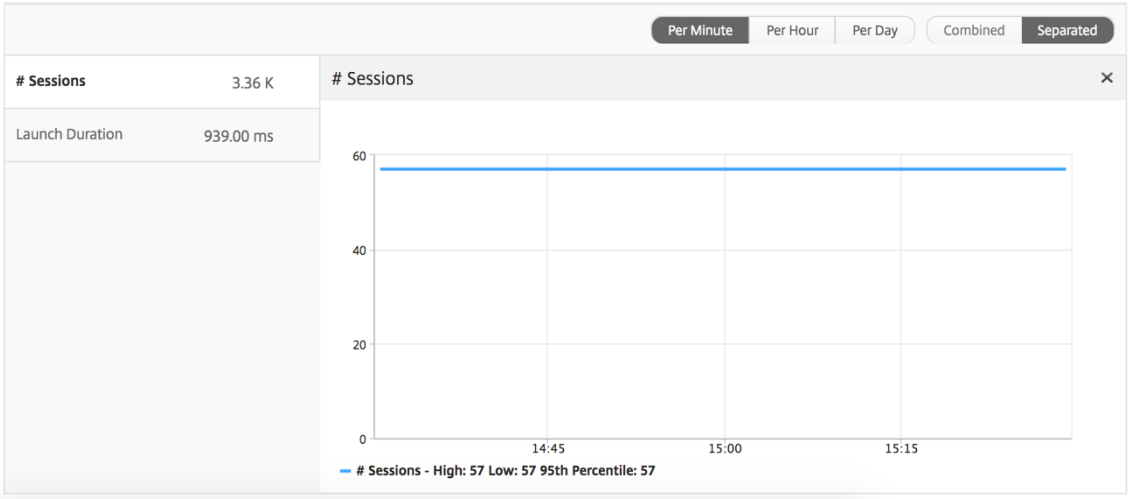
[**Summary**] ビュー

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。

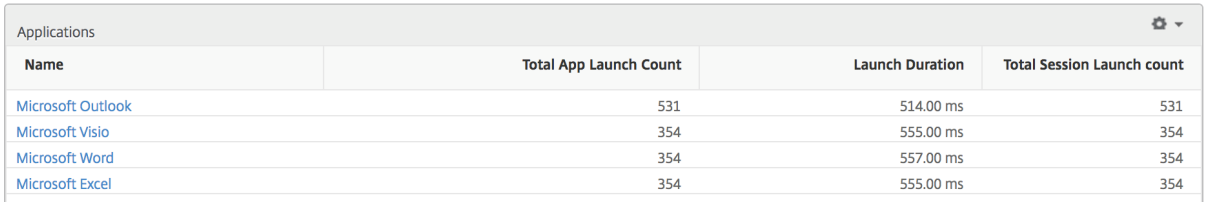
折れ線グラフ

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。



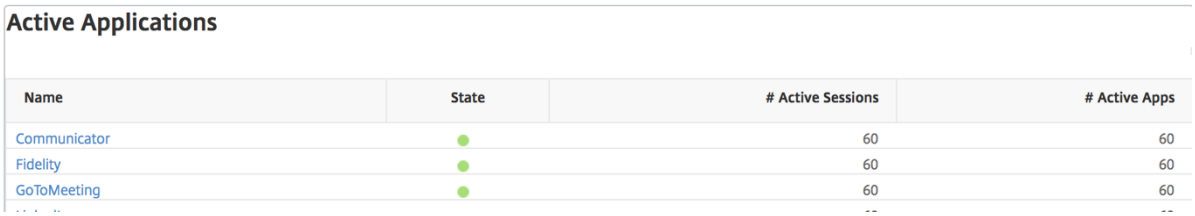
アプリケーション・サマリー・レポート

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。



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。

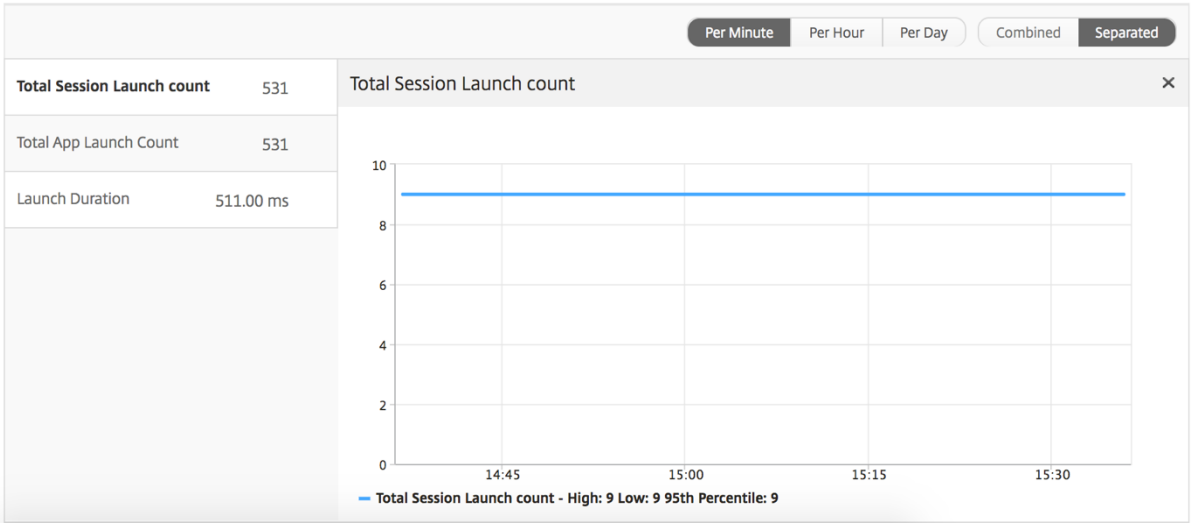


しきい値レポート

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。

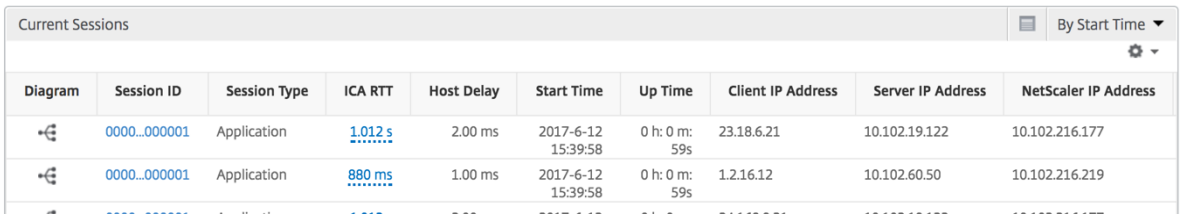


現在のセッションレポート

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 を通過する ICA トラフィックの平均遅延時間。
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	ワークスペースタイプ-Citrix Windows クライアントなど
クライアントのバージョン	ワークスペースバージョン。
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 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 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。
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。



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。

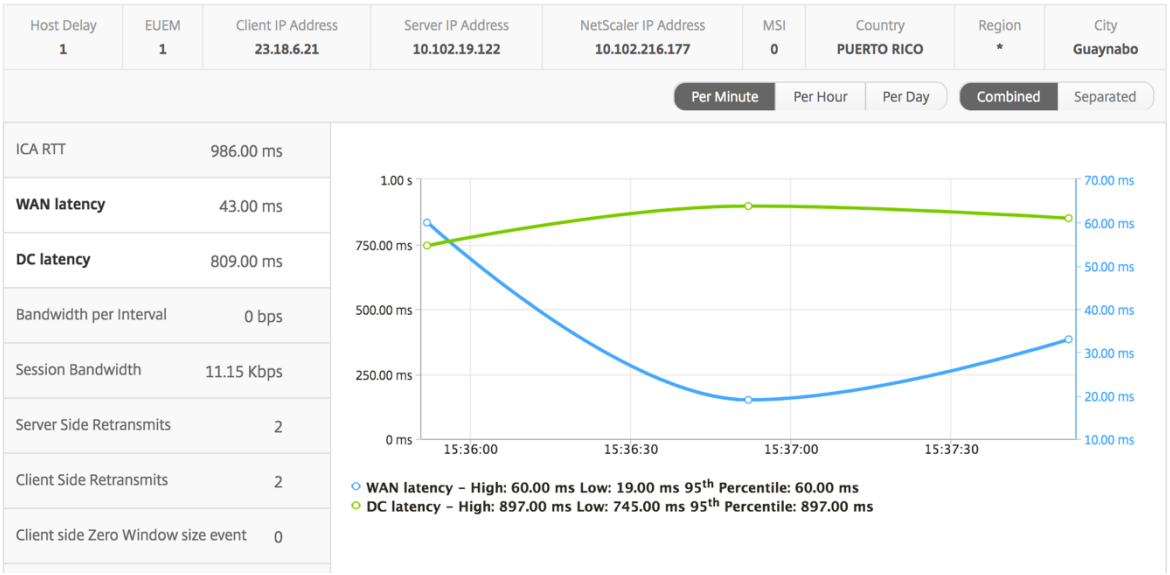
セッション・レポートを表示するには、次の手順に従います。

1. [ゲートウェイ**] > [HDX Insight] > [**アプリケーション] に移動します。
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

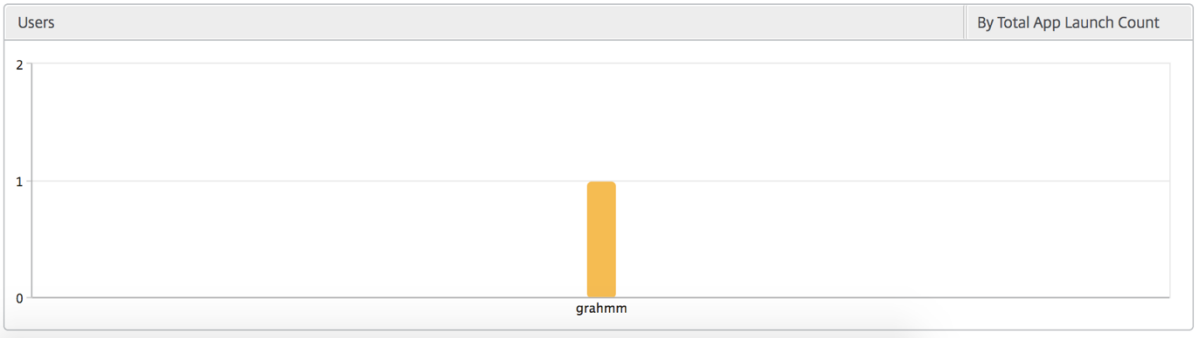
メトリック	説明
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
サーバー側のゼロ ウィンドウ サイズ イベント	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler 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。
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ド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. [ゲートウェイ**] > [HDX Insight] > [**デスクトップ] に移動します。

[**Summary**] ビュー

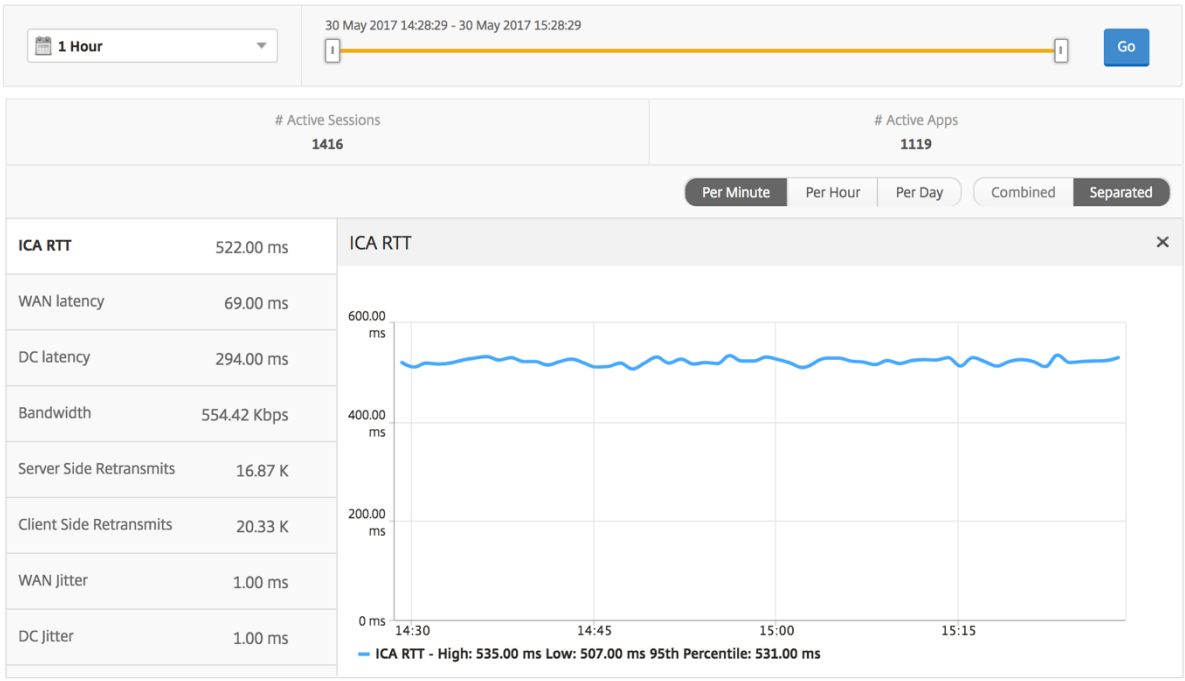
概要ビューには、選択したタイムライン中にログインしたすべての Citrix Virtual Desktops のレポートが表示されます。

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。

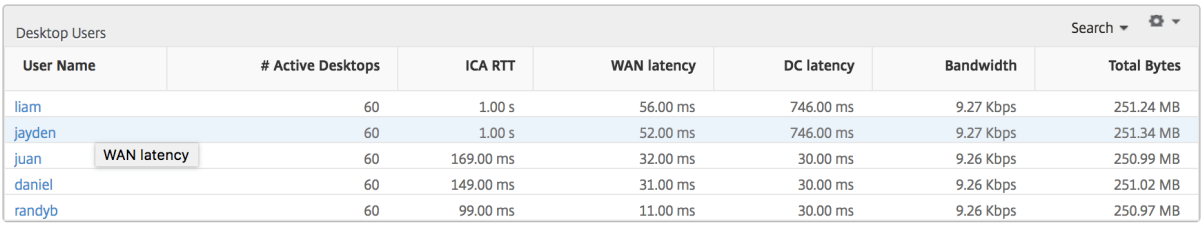
メトリック	説明
クライアント側のゼロ ウィンドウ サイズ イベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがアドバタイズした回数を表します。
サーバー側のゼロ ウィンドウ サイズ イベント	このカウンターは、TCP ウィンドウサイズがゼロであることをサーバーがアドバタイズした回数を表します。



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。



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。

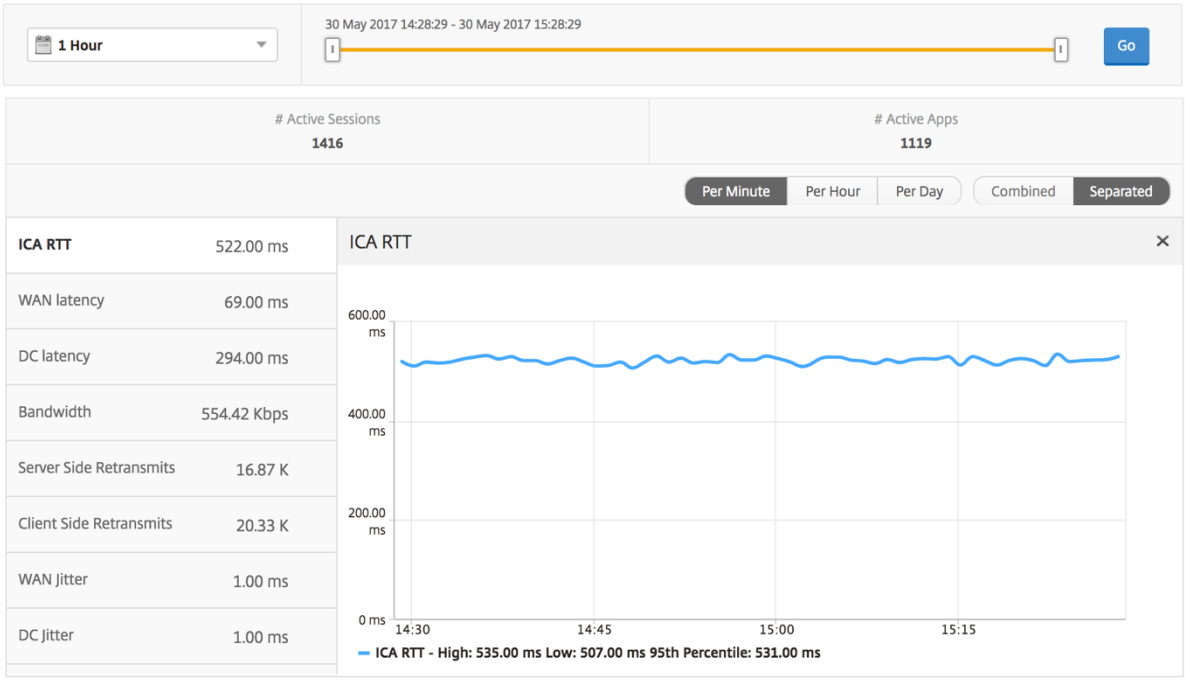
特定のデスクトップビューに移動するには**:**

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。

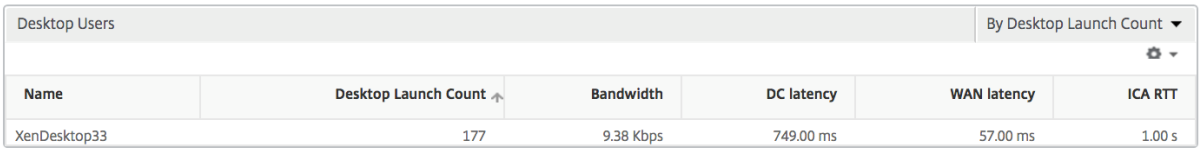
メトリック	説明
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler ADC からバックエンドサーバーまでです。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
サーバー側の再転送	NetScaler 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ド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ド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 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。



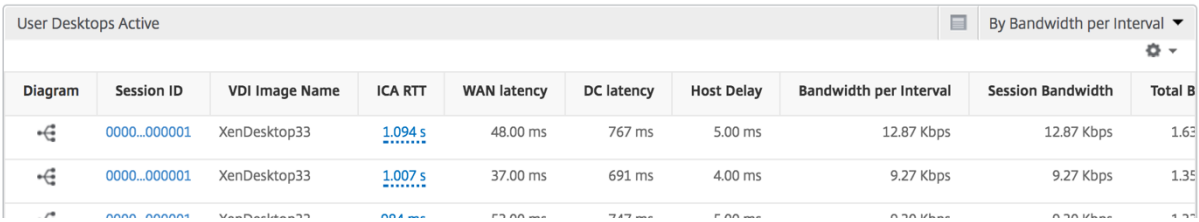
ユーザーデスクトップのアクティブ/非アクティブレポート

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起因する、NetScaler ADC を経由する ICA トラフィックの平均遅延時間。
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	ワークスペースタイプ-Citrix Windows クライアントなど
クライアントのバージョン	ワークスペースバージョン。
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 ユーザー/トランスペアレントモードなどです。

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。
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	



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. [ゲートウェイ**] > [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。

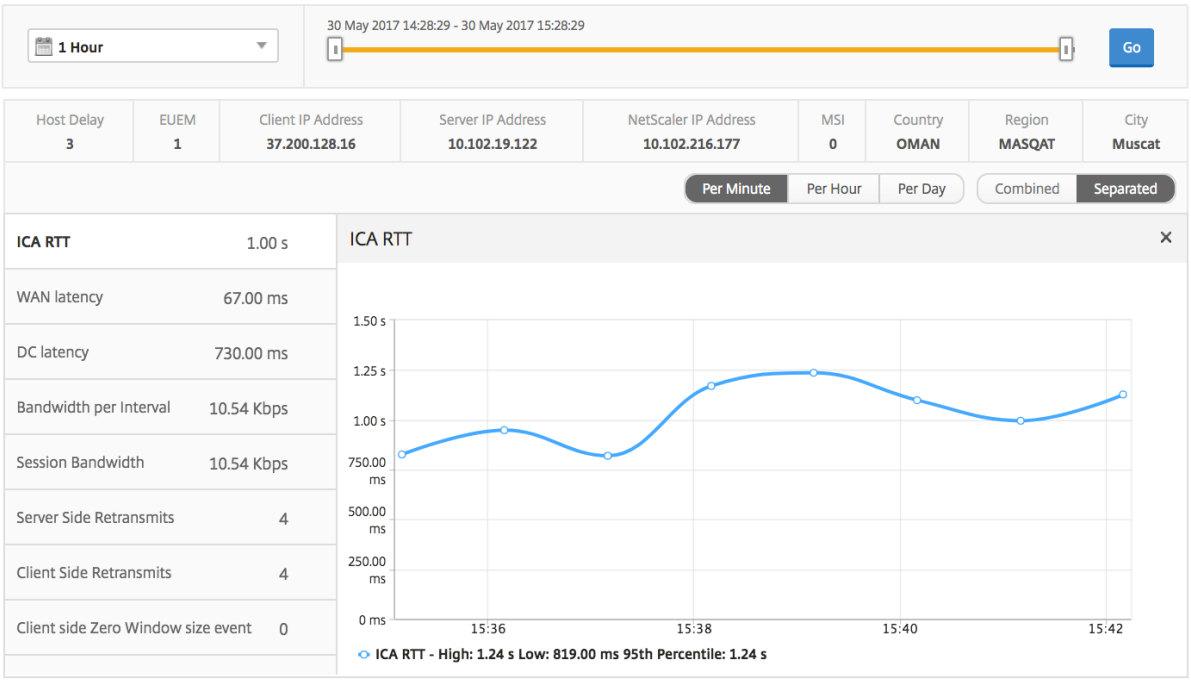
時系列グラフ

[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. [**Gateway] > [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ドバ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ドバタイズした回数を表します。



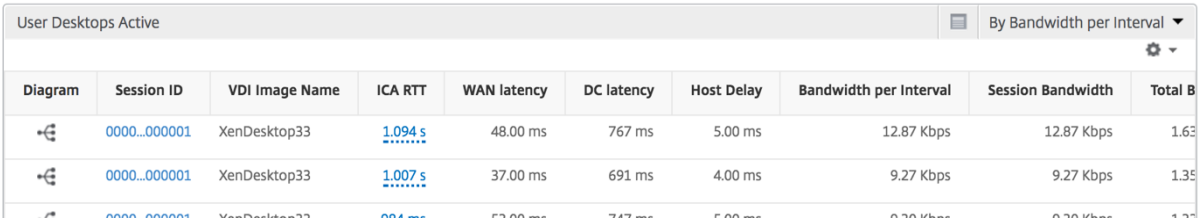
関連するデスクトップセッションレポート

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 を通過する ICA トラフィックの平均遅延時間。
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 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。
VDI イメージ名	ユーザーが接続している Citrix Virtual Desktop の名前



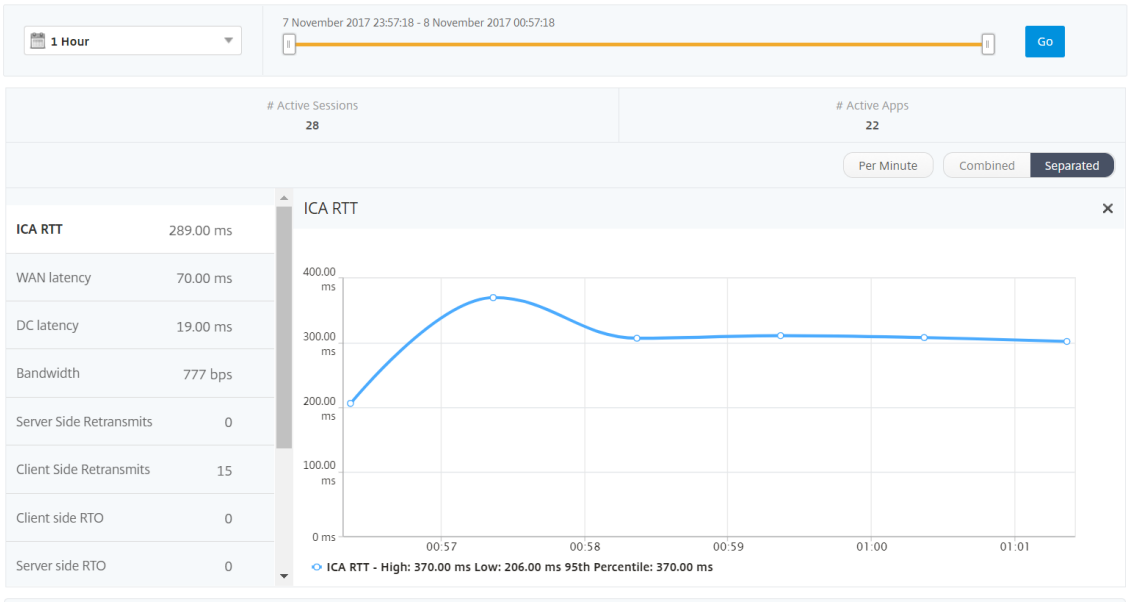
ユーザービューのレポートとメトリック

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。

「ユーザー」ビューに移動する手順は、次のとおりです。

1. [ゲートウェイ**] > [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。

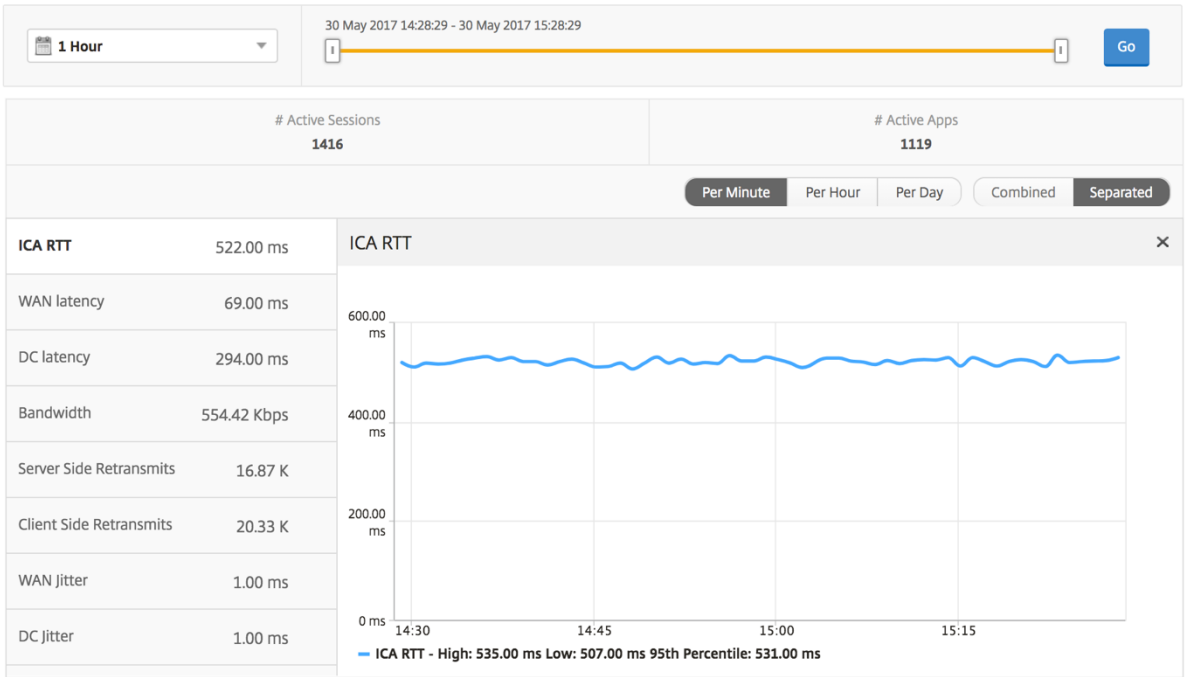
選択した期間を変更するには、次の手順に従います。

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 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 とバックエンドサーバー間の接続で発生した再送信タイムアウトの回数です。
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。
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。

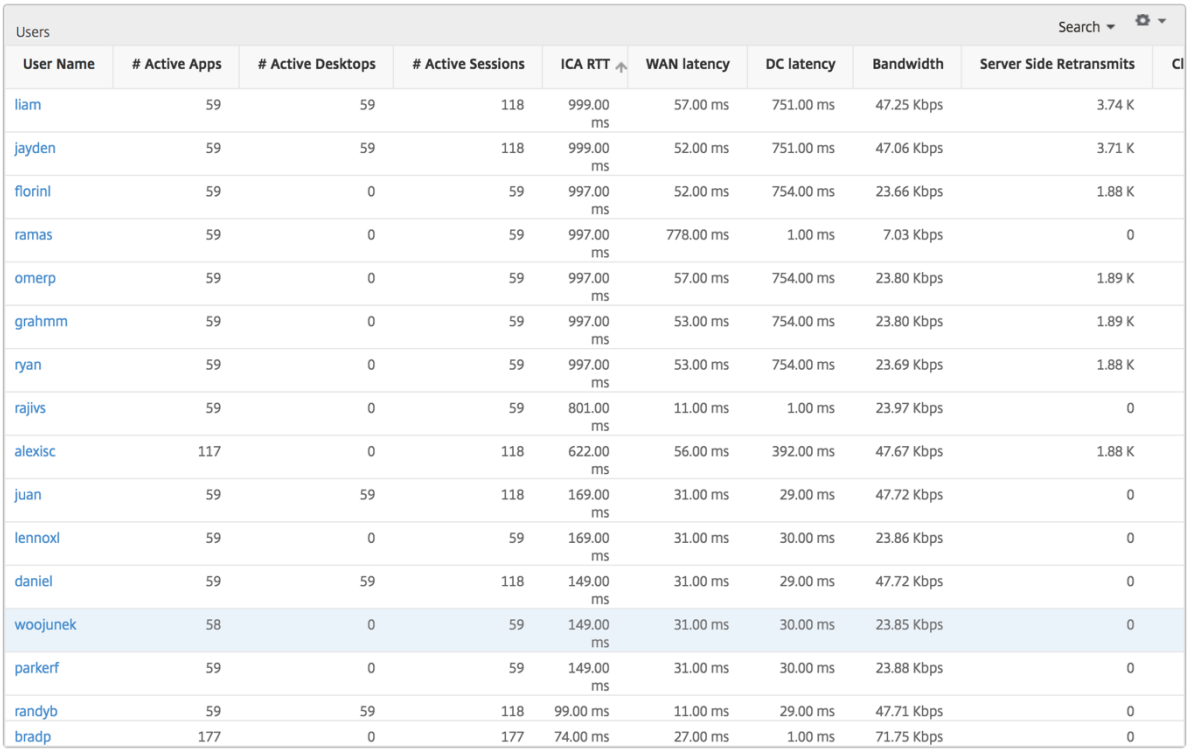


ユーザー概要レポート

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 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 とバックエンドサーバー間の接続で発生した再送信タイムアウトの回数です。
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。
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。
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。



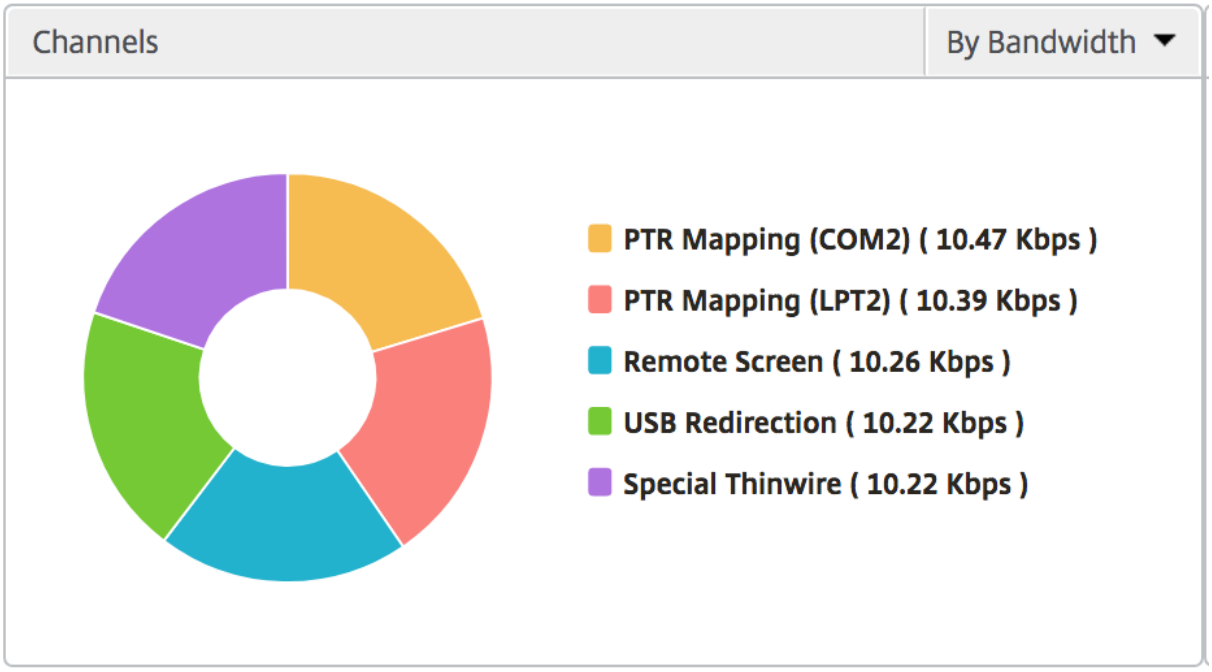
Users

Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
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	
randyb	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	

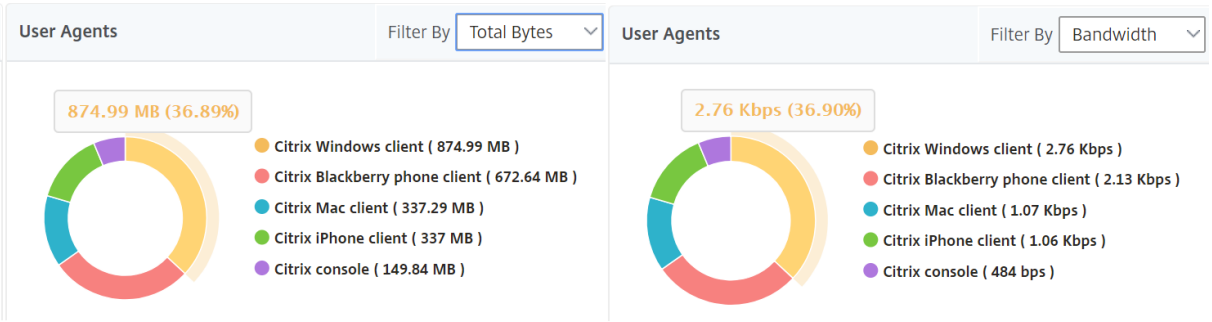
チャネル

Channels では、各 ICA 仮想チャ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。

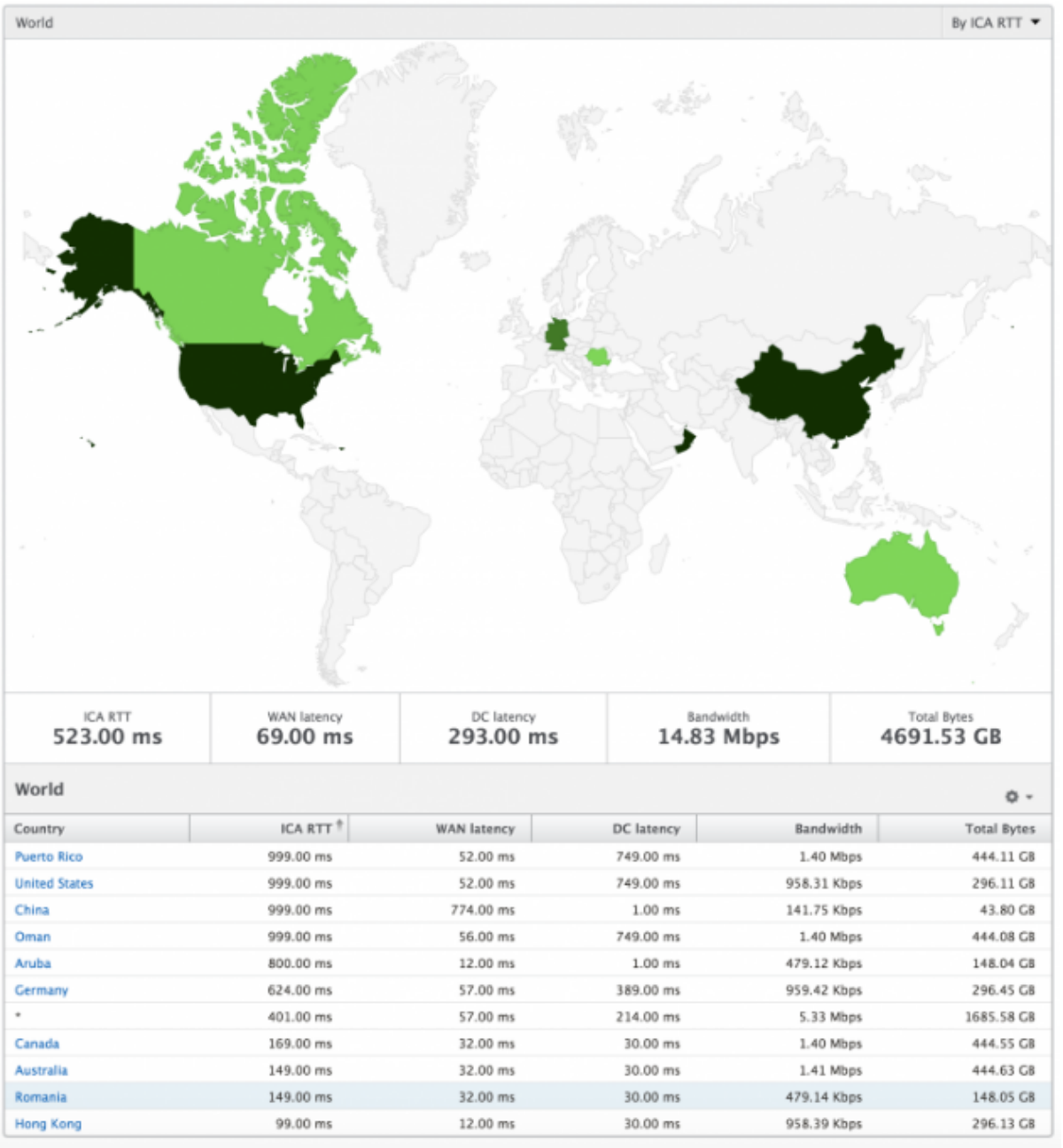
世界地図

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



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

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. [**Gateway] > [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起因する、NetScaler ADC を経由する ICA トラフィックの平均遅延時間。
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	ワークスペースタイプ-Citrix Windows クライアントなど
クライアントのバージョン	ワークスペースバージョン。
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 ユーザー/トランスペアレントモードなどです。

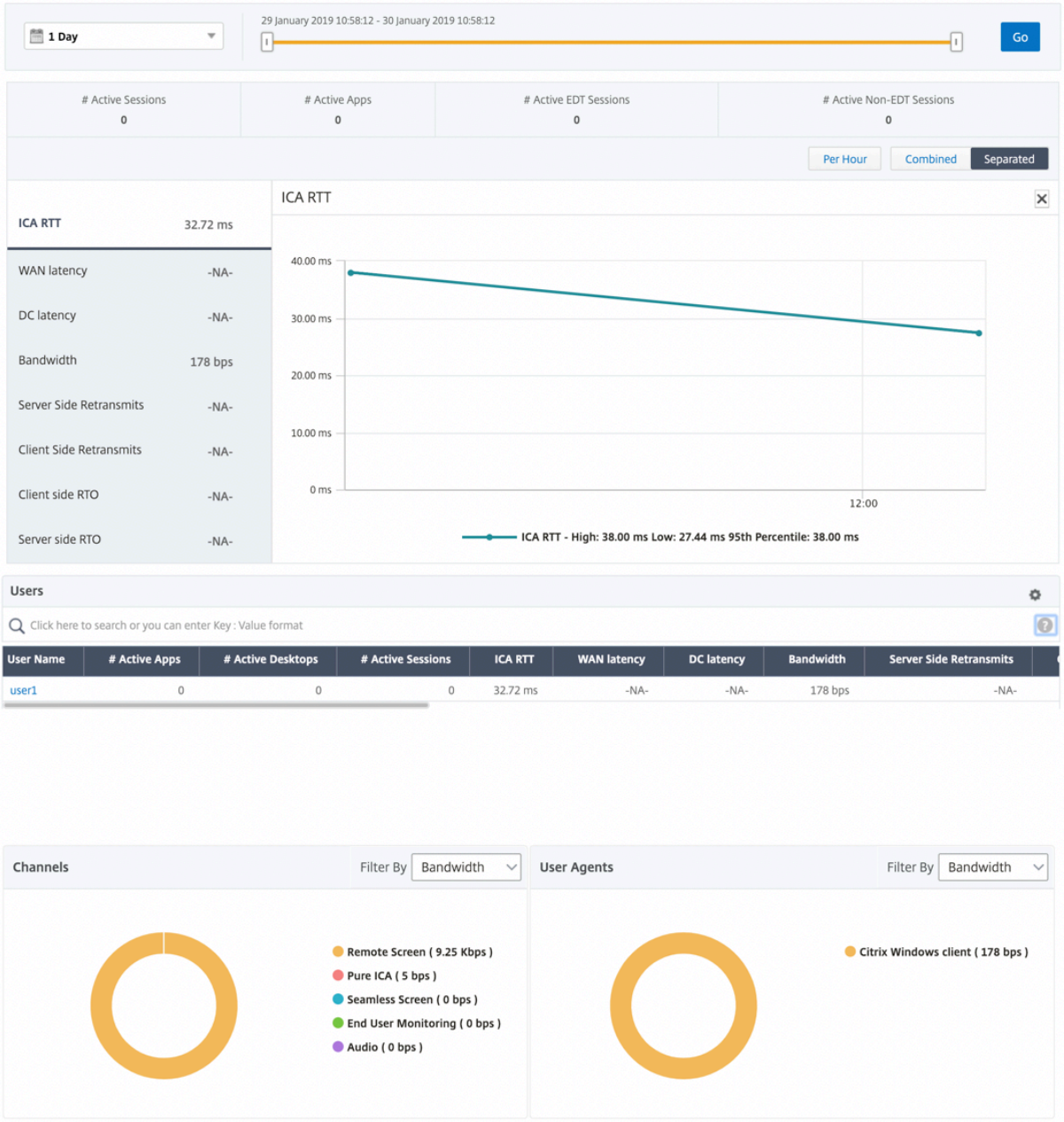
メトリックス	説明
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA 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 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ドバタイズした回数を表します。
Server side fast RTO	NetScaler とバックエンドサーバー間の接続で発生した再送信タイムアウトの回数です。

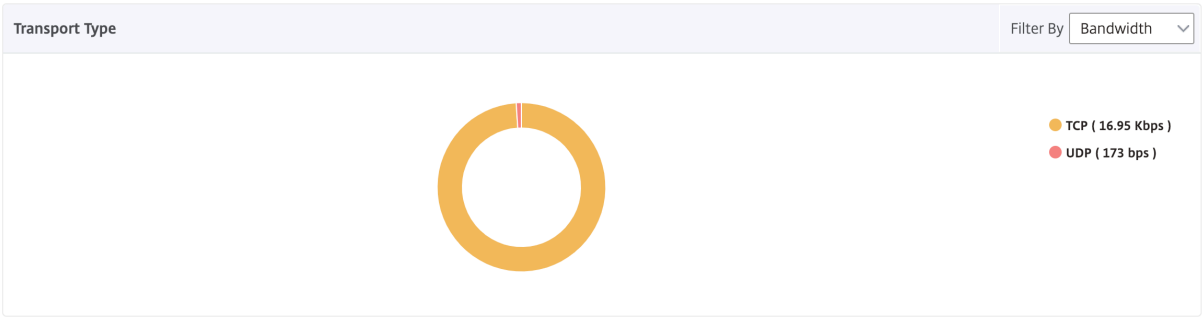
HDX Insight における **EDT** のサポート

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 Workspace を実行しているユーザーは、仮想デスクトップのセッション中の高解像度のユーザーエクスペリエンスを保証します。

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。

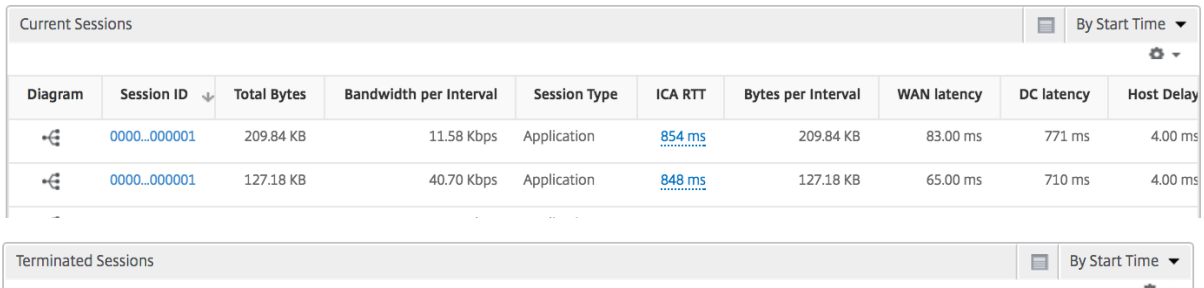


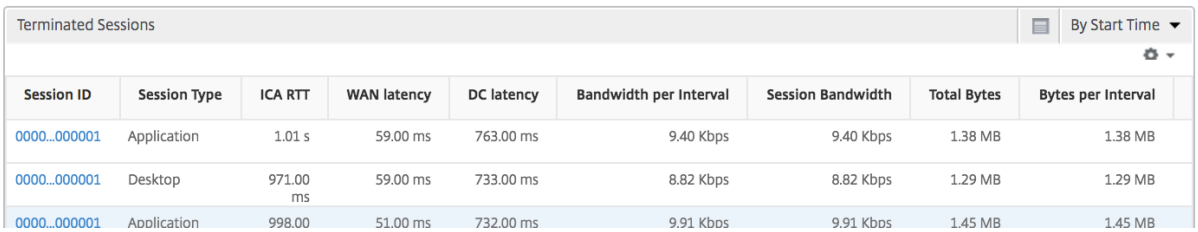
新しいドーナツグラフが導入され、ユーザーが使用したプロトコルの種類に基づいて、ユーザーが消費した帯域幅と合計バイト数を確認できるようになりました。



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。
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。

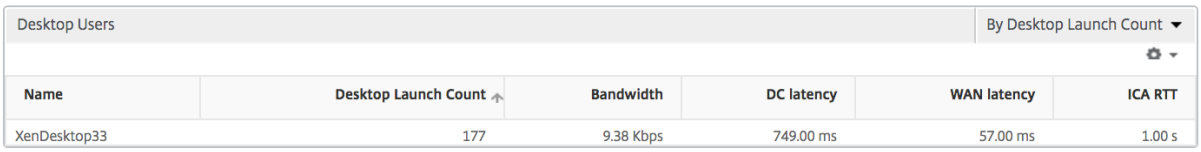




デスクトップ ユーザー

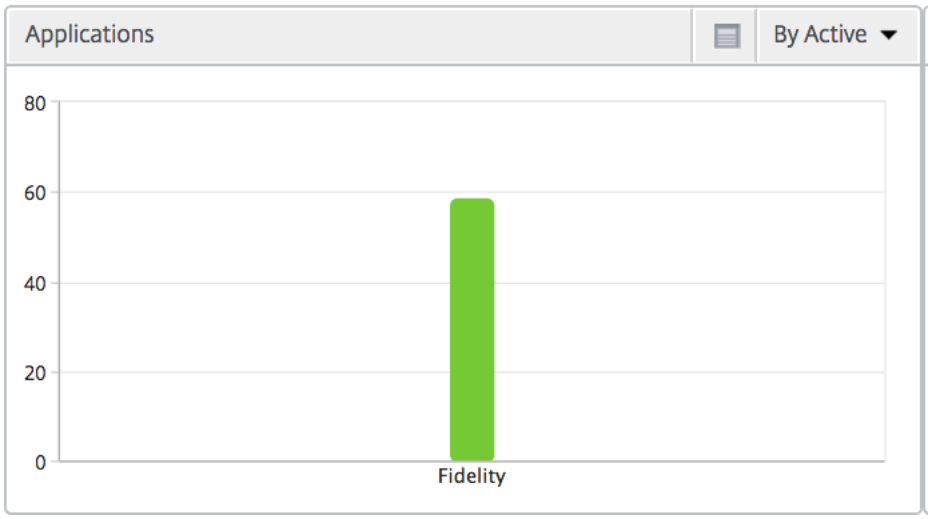
この表は、特定のユーザーの Citrix Virtual Desktop セッションに関する洞察を示しています。以下のメトリクスは［Desktop Launch Count］および［Bandwidth］を基準にしてソートできます。

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 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。



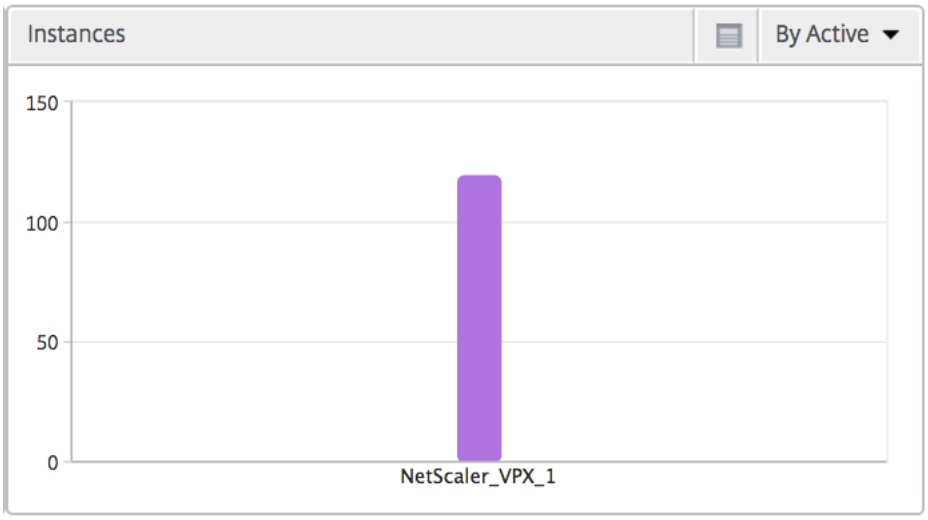
アプリケーション

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。



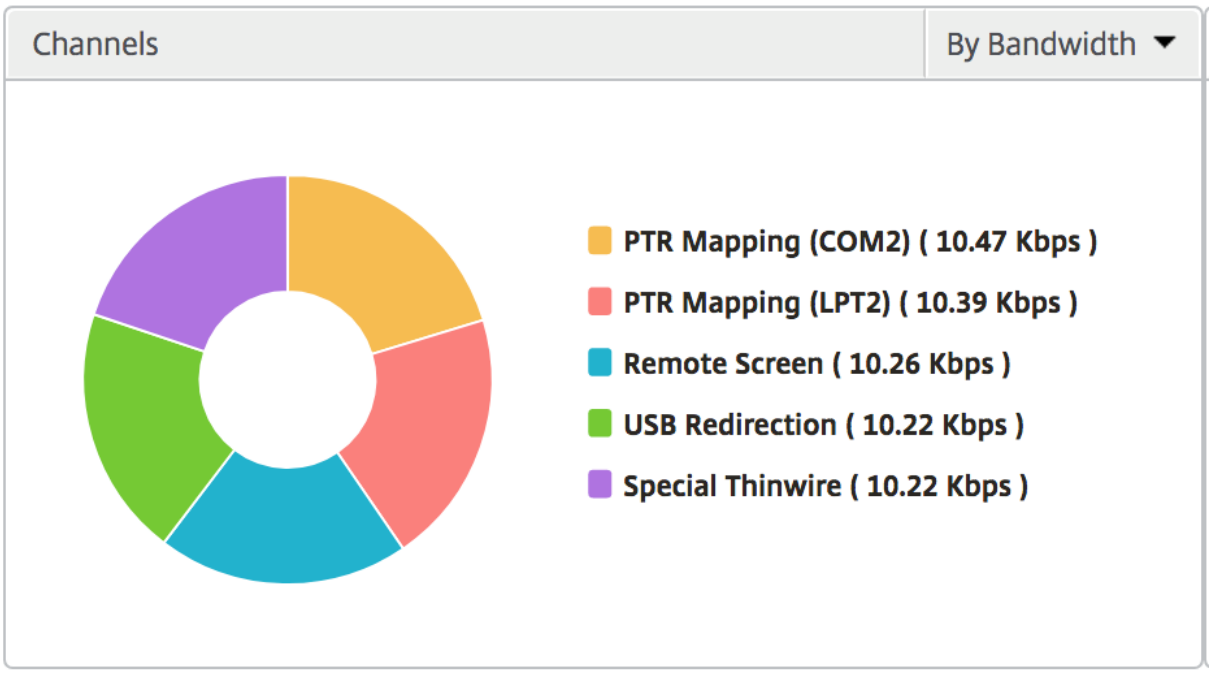
インスタンス

［Active］および［Total Apps］で並べ替えることができる、NetScaler インスタンスを表す棒グラフ



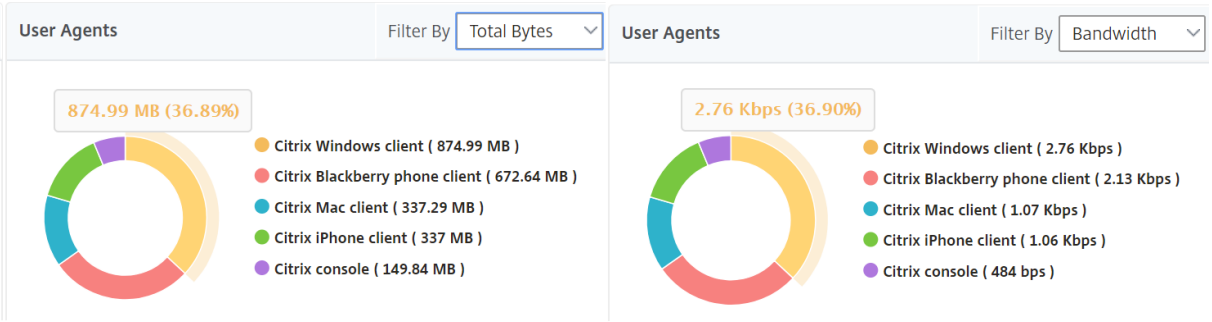
チャネル

Channels では、各 ICA 仮想チャ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。

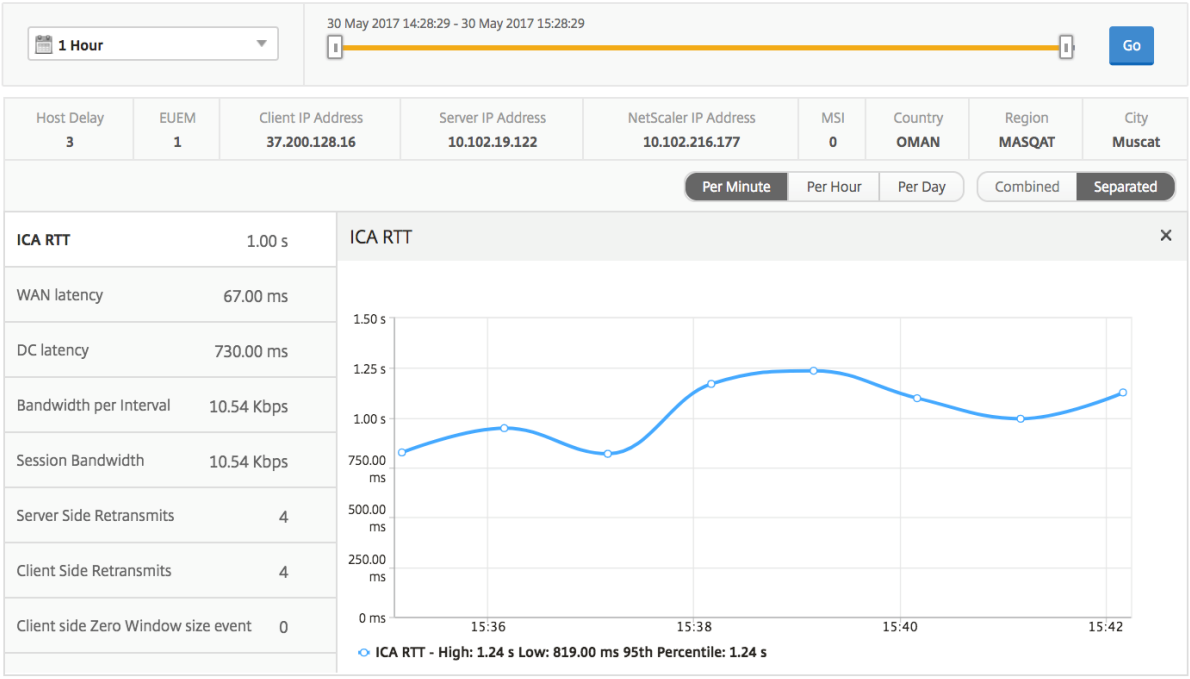
選択したユーザーのセッションのメトリックを表示する手順は、次のとおりです。

1. ［**Gateway] > [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

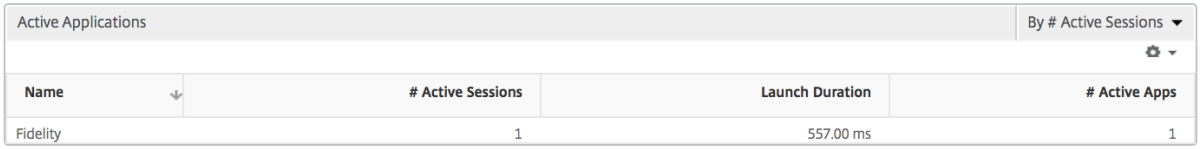
メトリックス	説明
セッション再接続	この数字は、アクティブな Citrix Virtual App and Desktop セッションの数を示します。
ACR 数	この数字は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 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 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 とバックエンドサーバー間の接続で発生した再送信タイムアウトの回数です。
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。
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。



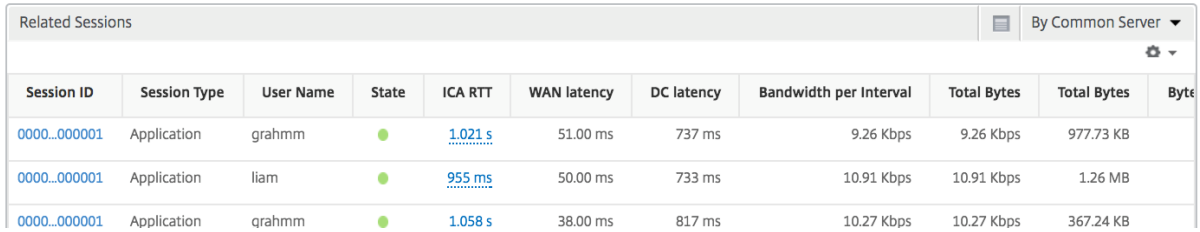
アクティブなアプリケーション

「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。



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。関係性は、共通サーバーと共通 NetScaler から選択できます。



インスタンスビューのレポートとメトリックス

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 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. [ゲートウェイ**] > [HDX Insight] > [**インスタンス**]** に移動します。

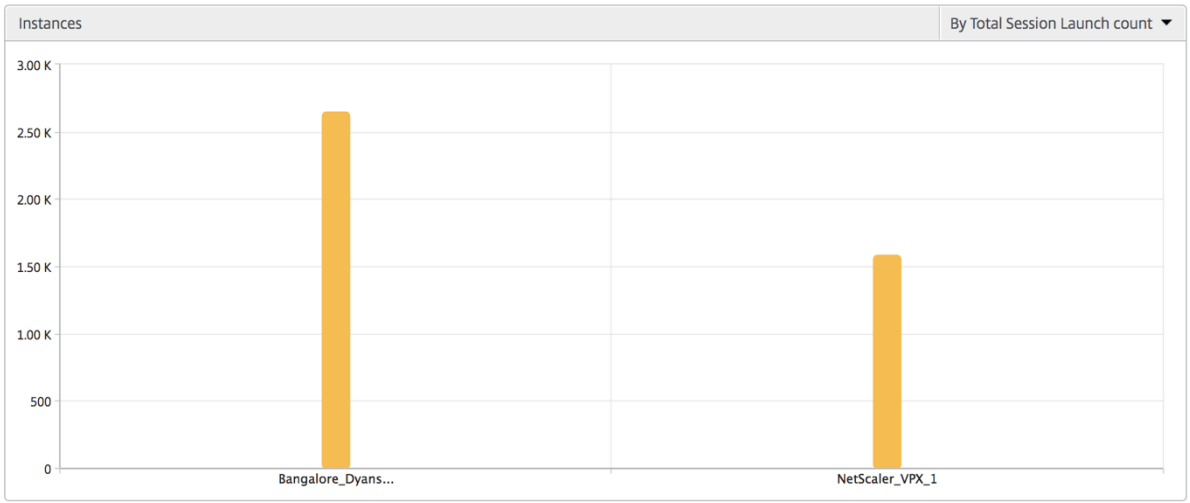
インスタンスの概要ビュー

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。

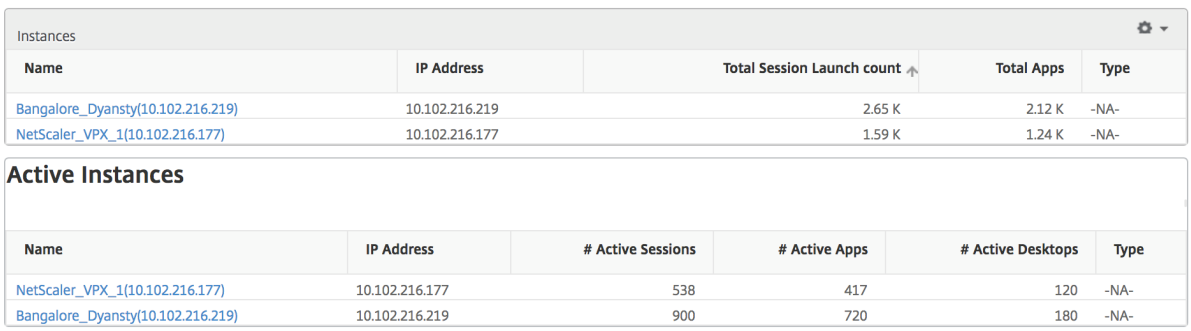
インスタンス棒グラフ

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 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バージョンの Citrix Virtual Apps and Desktops を使用している、サポートされていないバージョンのワークスペースまたはワークスペースタイプを使用しているなど、さまざまな理由により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。これらのワークスペースは、ホワイトリストに登録されているワークスペースの一部ではない可能性があります。したがって、これらのセッションは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

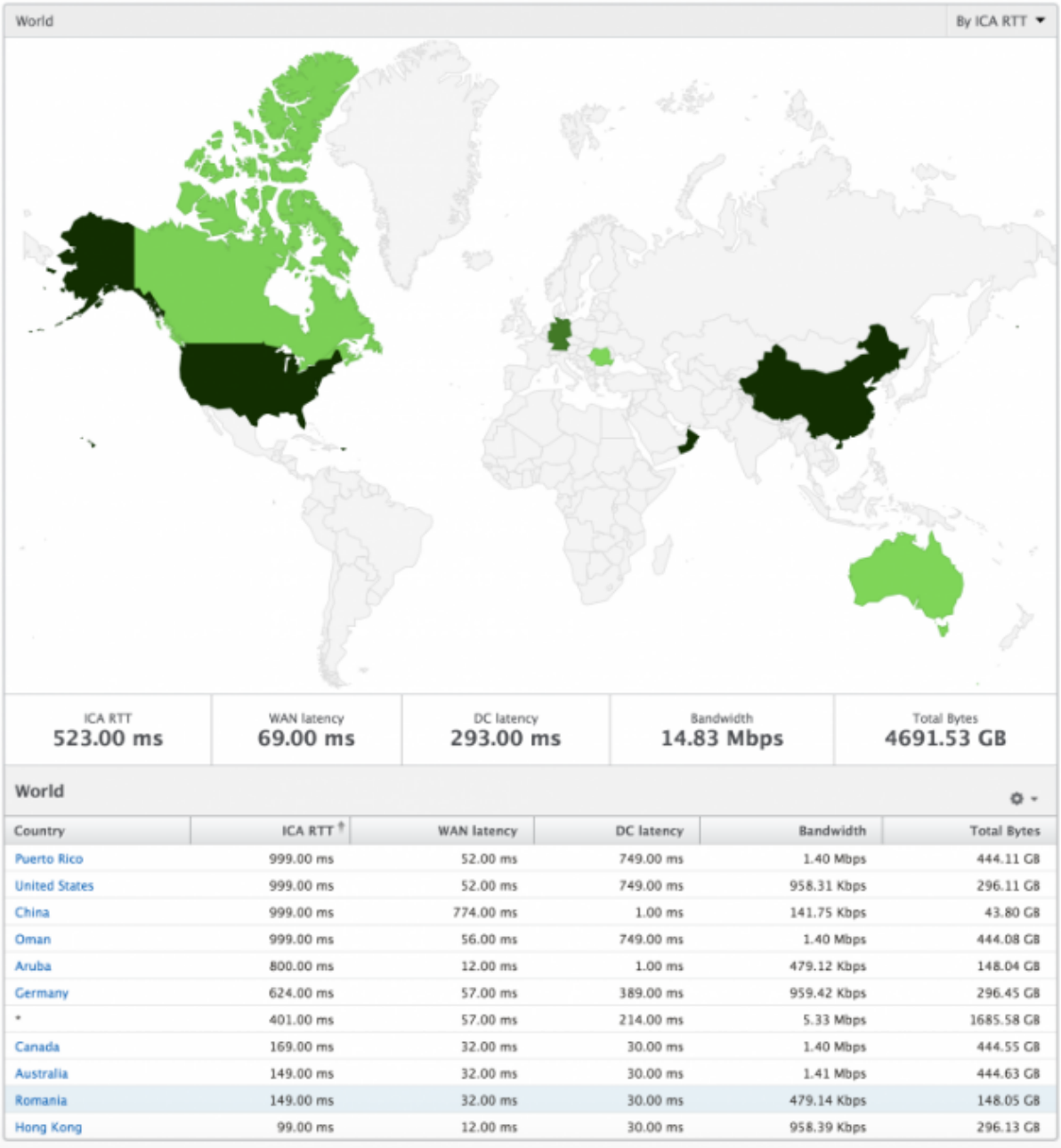
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

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



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

インスタンスごとのビュー

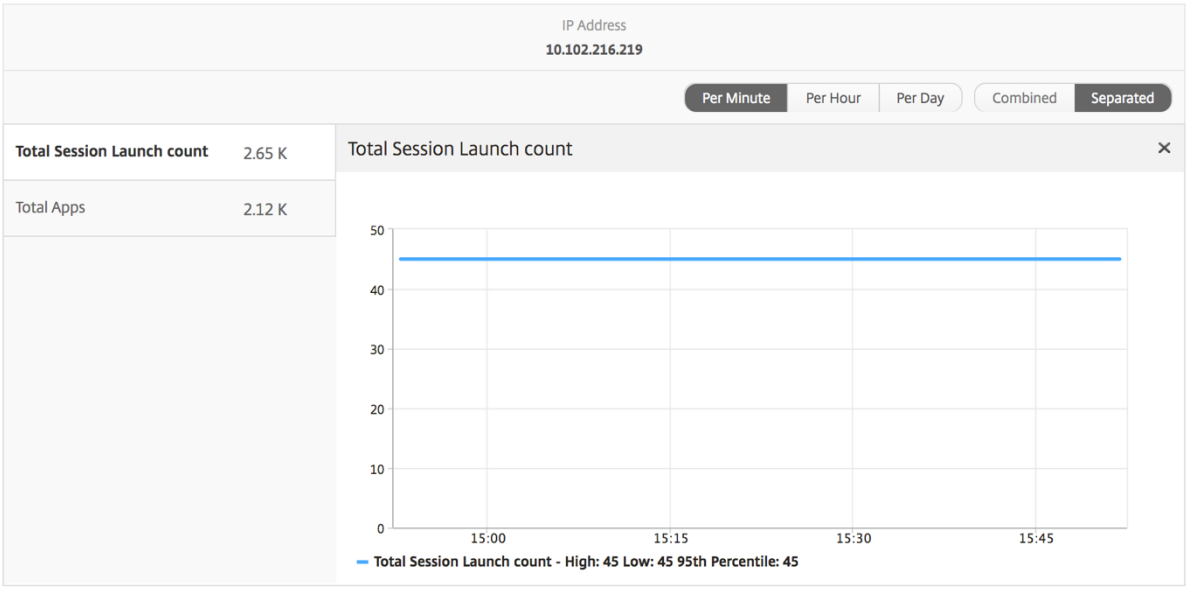
インスタンス別ビューには、選択した特定の NetScaler インスタンスの詳細なエンドユーザーエクスペリエンスに関するレポートが示されます。

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. [ゲートウェイ] **> [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。

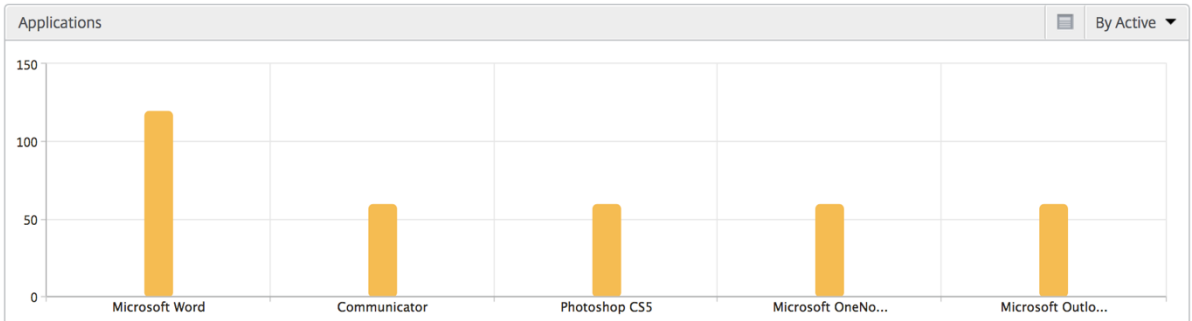
折れ線グラフ

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

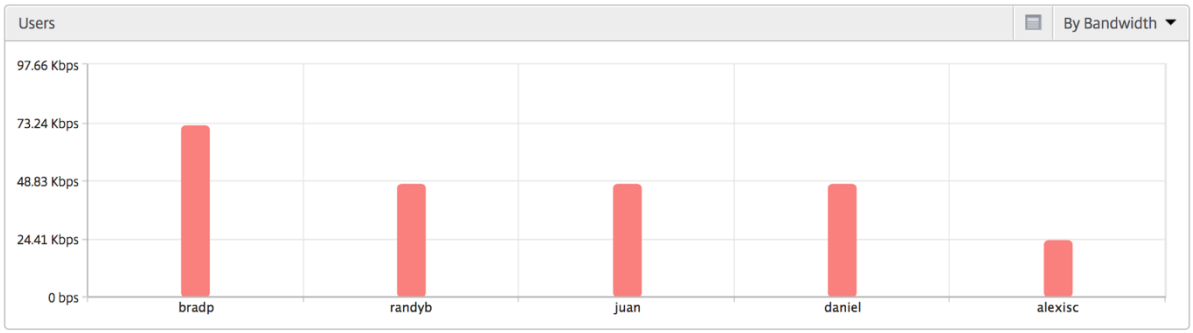
アクティブなアプリ、セッションの合計起動数、アプリの合計起動数、起動時間などの条件に基づいて、上位 5 個のアプリケーションを表示します。



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。

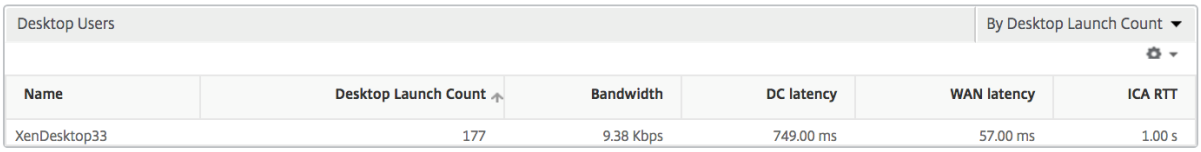
- 帯域幅
- WAN 遅延
- DC の遅延
- ICA 往復時間



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。

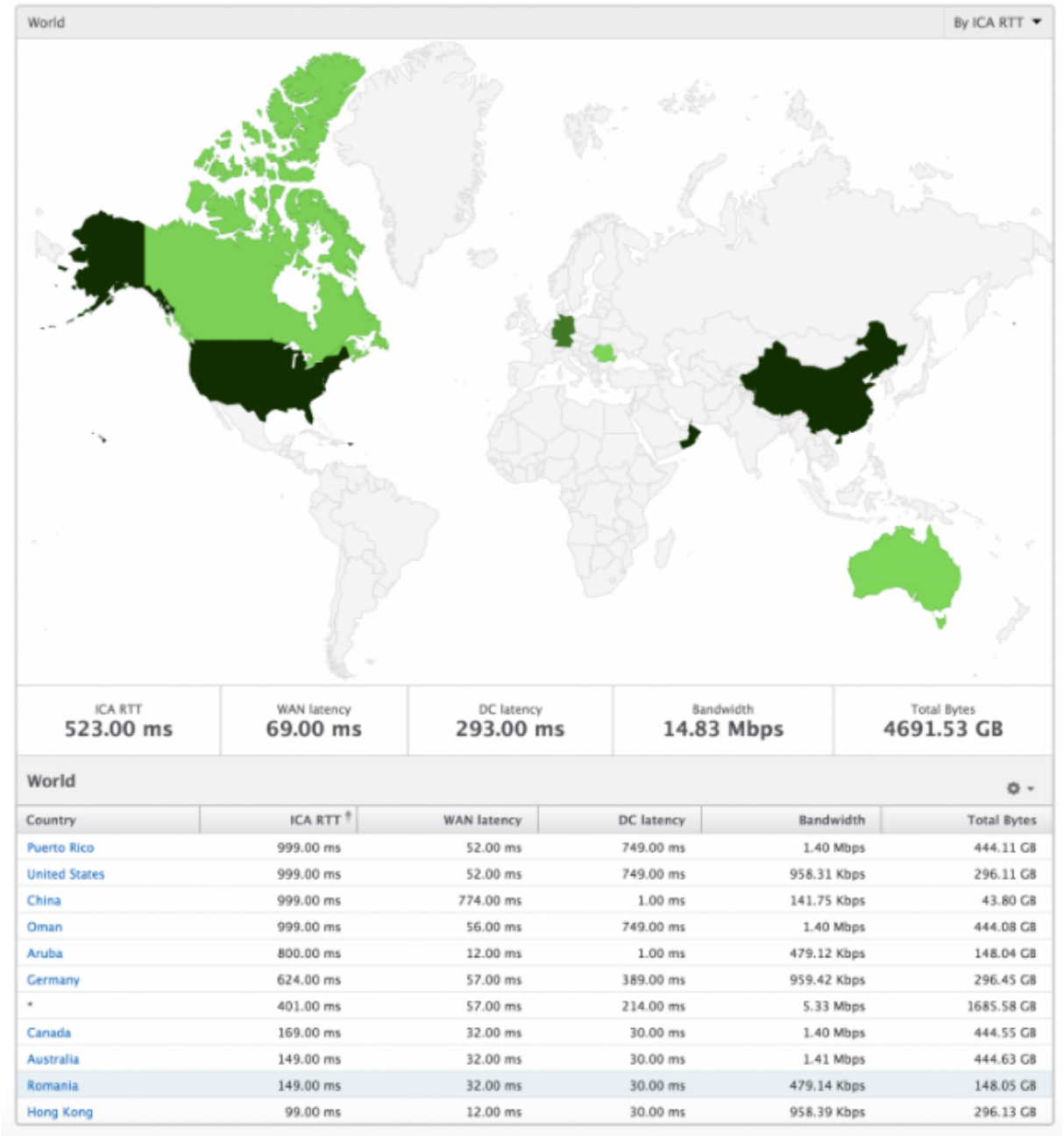


世界観

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



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

ライセンスビューのレポートとメトリック

February 6, 2024

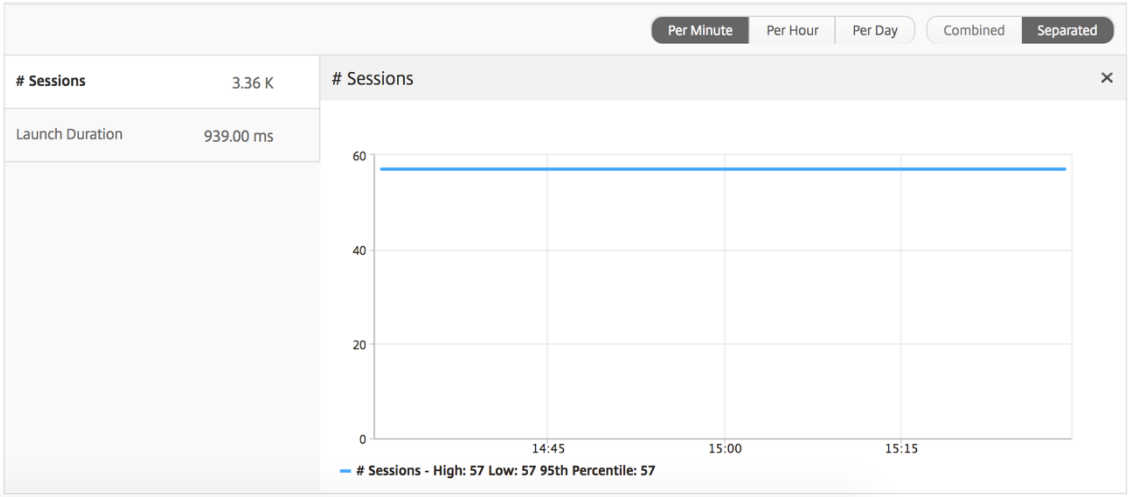
ライセンスビューには、NetScaler Gateway のライセンス情報が表示されます。

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. [ゲートウェイ] **> [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	選択したタイムラインで使用されている NetScaler ADC ゲートウェイ 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 ADC ゲートウェイ CCU ライセンスの総数。



しきい値レポート

しきい値レポートは、選択した期間内に 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 で AppFlow 機能が有効になっていることを確認します。詳細については、「AppFlow の有効化」を参照してください。
- NetScaler の実行構成で 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 ICA_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 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 と NetScaler ADM の間の接続チェックリスト

- NetScaler で AppFlow コレクタのステータスを確認します。詳しくは、「NetScaler 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 [設定] **> [AppFlow] > [**ポリシー**]** に移動して、AppFlow ポリシーヒットを確認することもできます。

- AppFlow ポート 4739 または 5557 をブロックしているファイアウォールを検証します。

NetScaler 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：無効なチャネルヘッダー

  原因：チャネルヘッダーを識別できません

解決策：新しいセッションが確立されるまで、この特定の ICA セッションのレポートは利用できません。

- ログ：スキップコード

スキップコードに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_CNT	V3 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	エンコーダーをチャ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 チャネル番号が無効です
106	NS_ICA_ERR_INVALID_DECODER	チャ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 チャネルに無効なパラメータ数が指定されました
108	NS_ICA_ERR_INVALID_TW_DECODER	Thinwire チャネルのデコーダーが無効です
109	NS_ICA_ERR_REDUC_NO_DECODER	チャネルにデコーダーが定義されていません
110	NS_ICA_ERR_REDUC_V3_EXPANDER	チャネルデータ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	未定義のエキ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_REDUC_CTX_ALLOC	リダクションパンダーコンテキストのメモリ割り当てエラー
117	NS_ICA_ERR_ICA_OLD_SERVER	古いサーバー - 機能ブロックはサポートされていません
118	NS_ICA_ERR_PIR_MANY_FRAG	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_INSUFFICENT_CHANNEL_BYTES	ヘッダーで不十分なバイト数
123	NS_ICA_ERR_CHANNEL_DATA	EUEM、CONTROL、または SEAMLESS チャネルのデータが正しくない
124	NS_ICA_ERR_INVALID_PURE_CMD	PURE ICA チャ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_LEN0	PURE ICA チャ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	無効なチャネルヘッダーが検出されました
130	NS_ICA_ERR_CGP_PARSE_RECONNECT_ID	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_NS_RECONNECT	SR レジストリの無効化中にエラーが発生しました
132	NS_ICA_ERR_REDUC_NOT_V3	サポートされていない ICA リデューサーバージョン
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	圧縮は無効で、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、誤ったワークスペースで表示される
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_RECEIVER_VERSION	ICA (クライアント) は許可リストにないため、ICA 解析をスキップしました
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	クライアント再接続 Cookie の解析状態を検出できません
144	NS_ICA_ERR_SYNCUP_RECONNECT_ID	クライアント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_ID	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ワークスペース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_LEN	最後のチャネル長が無効です
149	NS_ICA_ERR_SPECIAL_THINWIRE	解凍エラー
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	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 チャネル解析のイベントが無効です
153	NS_ICA_ERR_CTRL_INVALID_EVENT	CTRL チャネル解析のイベントが無効です
154	NS_ICA_ERR_EUEM_INVALID_EVENT	EUEM チャネル解析のイベントが無効です
155	NS_ICA_ERR_USB_INVALID_EVENT	USB チャネル解析のイベントが無効です
156	NS_ICA_ERR_PURE_INVALID_EVENT	PURE チャ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_INVALIDSTATE	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_INVALIDCRYPTCMD	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_INVALIDSTATE	RC5 暗号化の crypt コマンドの状態が無効です
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	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_REDUCER_V3	ICA 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_REDUCER_V3	ICA スペース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 チャネルデータからアプリの詳細を解析中にエラーが発生しました
173	NS_ICA_ERR_NSAP_ACR	Insight チャネルデータから ACR の詳細を解析中にエラーが発生しました
174	NS_ICA_ERR_NSAP_SESSION_END	Insight チャネルデータからセッション終了の詳細を解析中にエラーが発生しました
175	NS_ICA_ERR_NON_NSAP_SN	Insight チャネル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_FETCH	サービスノード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_RECONSEQ	サービスノードでより高い再接続シーケンス番号を受信するとエラーが発生しました
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NON_NSAP	NSAP 以外の接続で 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 カウンター名	目的	カテゴリ（統計/エラー/診断）
hdx_tot_ica_conn	NS によって検出されたピュア 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。	統計情報
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 (セッション画面の保持がオン)。クライアント PCB の CGP シグネチャに基づく CGP 接続が検出されるたびに増分されます。	統計情報
hdx_dbg_tot_udt_conn	NS によって検出された UDP ICA 接続の総数を示します	統計情報
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	統計情報
skip_conn	ICA または CGP 署名が無効な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。	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 がセッションから切り離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 カウンター名	目的	カテゴリ（統計/エラー/診断）
hdx_dbg_ag_user	アクセスゲートウェイ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
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	クライアントが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監視チャネルが使用可能な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ネルが必要です。	ステータス/診断
hdx_err_disabled_sr	セッション画面の保持は、`nsapimgr`ノブを使用して無効にします。このセッションではセッションは機能しません。	エラー
hdx_err_skip_no_msi	XA/XD サーバーに MSI 機能がありません。これは古いサーバーバージョンを示し、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	クライアントワークスペースが許可リストに含まれていません。HDX Insight はこの接続をスキップします	エラー
hdx_sm_ica_cam_channel_disabled	SmartAccess ポリシーによって無効化された NS_ICA_CAM_CHANNEL の総数	診断
hdx_sm_ica_usb_channel_disabled	SmartAccess ポリシーによって無効化された NS_ICA_USB_CHANNEL の総数	診断

HDX カウンター名	目的	カテゴリ（統計/エラー/診断）
hdx_sm_ica_clip_channel_disabled	SmartAccess ポリシーによって無効にされた NS_ICA_CLIP_CHANNEL の総数	診断
hdx_sm_ica_ccm_channel_disabled	SmartAccess ポリシーによって無効にされた NS_ICA_CCM_CHANNEL の総数	診断
hdx_sm_ica_cdm_channel_disabled	SmartAccess ポリシーによって無効にされた 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化された NS_ICA_COM1_CHANNEL の総数	診断
hdx_sm_ica_com2_channel_disabled	SmartAccess ポリシーによって無効化された NS_ICA_COM2_CHANNEL の総数	診断
hdx_sm_ica_cpm_channel_disabled	SmartAccess ポリシーによって無効化された 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化された NS_ICA_LPT2_CHANNEL の総数	診断
dx_dbg_sm_ica_msi_disabled	SmartAccess ポリシーによって MSI が無効になっているケースの総数	診断
hdx_sm_ica_file_channel_disabled	NS_ICA_FILE_CHANNEL の合計数は、SmartAccess ポリシーによって無効になっています	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_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 カウンター名	目的	カテゴリ（統計/エラー/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	消滅した USB デバイスの総数	診断
hdx_dbg_usb_device_stopped	停止した USB デバイスの総数	診断

nstrace 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 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トポロジの詳細。
- 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。
- クライアントワークスペースバージョン。
- 問題が発生したときのアクティブな ICA セッションの数。
- Citrix `show techsupport` ADC コマンドプロンプトで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、ADC リリースノートを参照してください。

インフラストラクチャ分析

February 6, 2024

ネットワーク管理者の主な目標は、NetScaler インスタンスを監視することです。ADC インスタンスは、それを介してアクセスされるアプリケーション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

NetScaler Application Delivery Management （ADM）インフラストラクチャ分析機能は、NetScaler インスタンスから収集されたすべてのデータを照合し、インスタンスの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ー」がスコアに影響します。

ヘルスインジケーターはインスタンススコアの構成要素であり、スコアは、その時間枠で検出されたすべてのインジケーターに基づいて、事前に定義された「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ー
- 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 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 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 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 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 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 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。
  - クラスター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 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。

  NetScaler 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 証明書の重要な強度が、NetScaler の標準に準拠していない
  - 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ます。ADC インスタンスにインストールされている SSL 証明書は、今後 1 週間で期限切れになりそうです。
  - 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ている SSL 証明書の署名アルゴリズムは、NetScaler 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. [インフラストラクチャー**] > [**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。

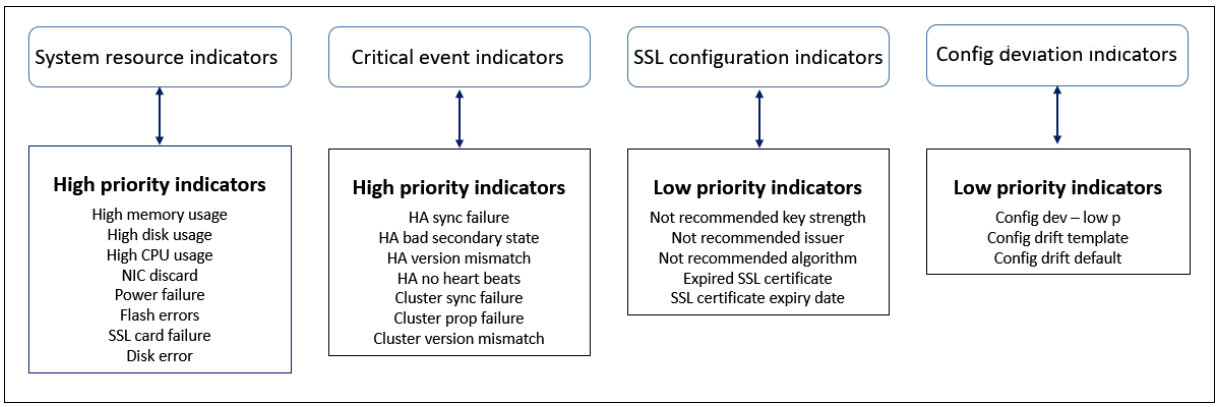
- 低しきい値：1 パケットドロップまたはレート制限カウンタ増分
- 高しきい値：10000 パケットのドロップまたはレート制限カウンタ増分

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ーの数が多いほど、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。このインジケーターは、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。

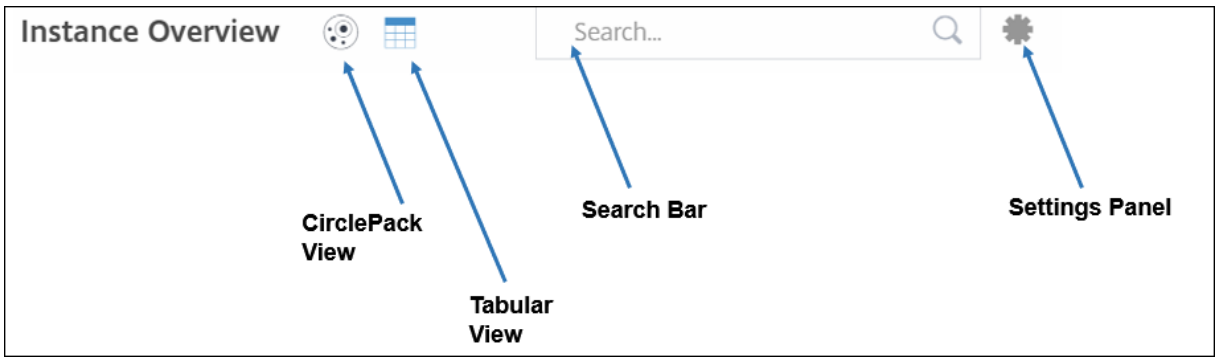
1. アクティビティに基づく。たとえば、インスタンスで停電が発生するたびにシステムリソースインジケーターがトリガーされ、このインジケーターはインスタンススコアの値を減らします。インジケーターがクリアされると、ペナルティがクリアされ、インスタンスのスコアが上がります。
2. 閾値違反に基づく。たとえば、NIC カードがパケットを破棄し、しきい値レベルを超えると、システムリソースインジケータがトリガーされます。
3. 低い閾値と高い閾値の違反に基づく。ここでは、インジケーターは次の 2 つの方法でトリガーできます。
    - 指標の値が低い閾値と高い閾値の間にある場合、インスタンススコアに部分的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ーです。

インフラストラクチャ分析ダッシュボード

[インフラストラクチャー**] > [**インフラストラクチャ分析] に移動します。

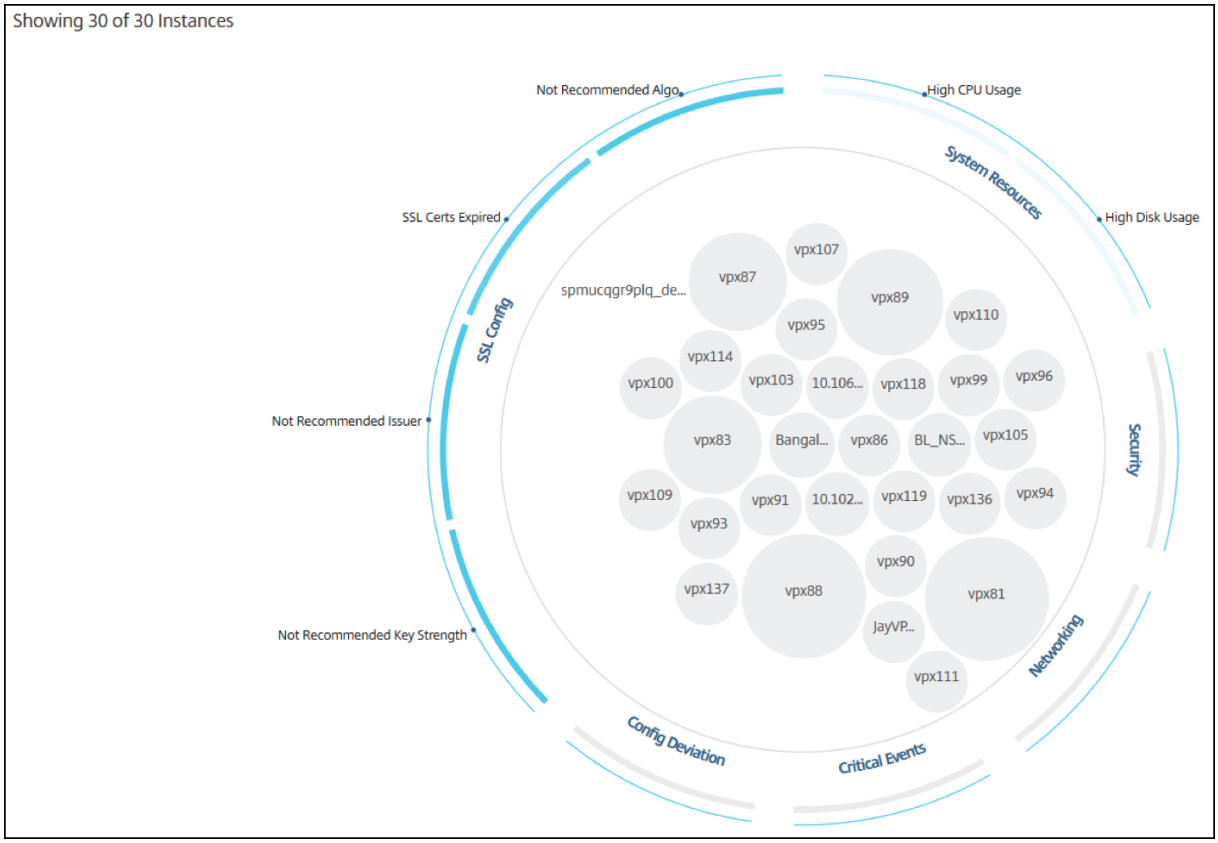
インフラストラクチャ分析は、サークルパック 形式または 表 形式で表示できます。2 つの形式を切り替えることができます。



- [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す。

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。



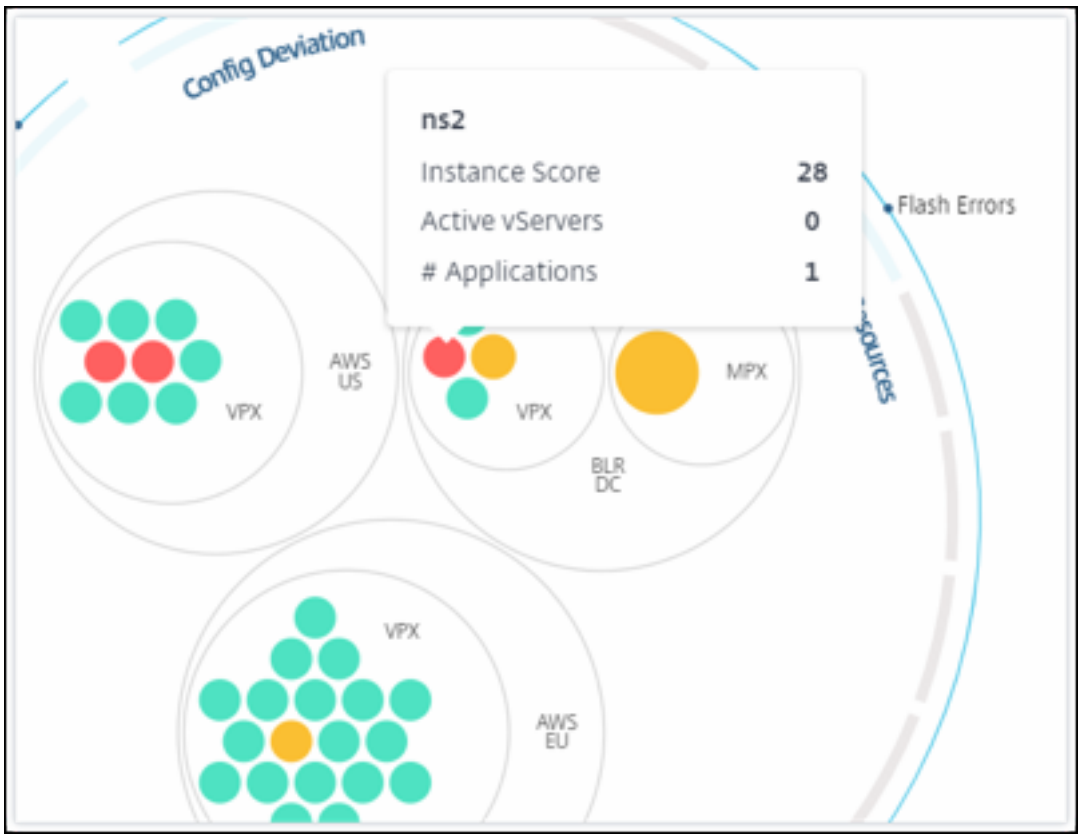
インスタンス円

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。

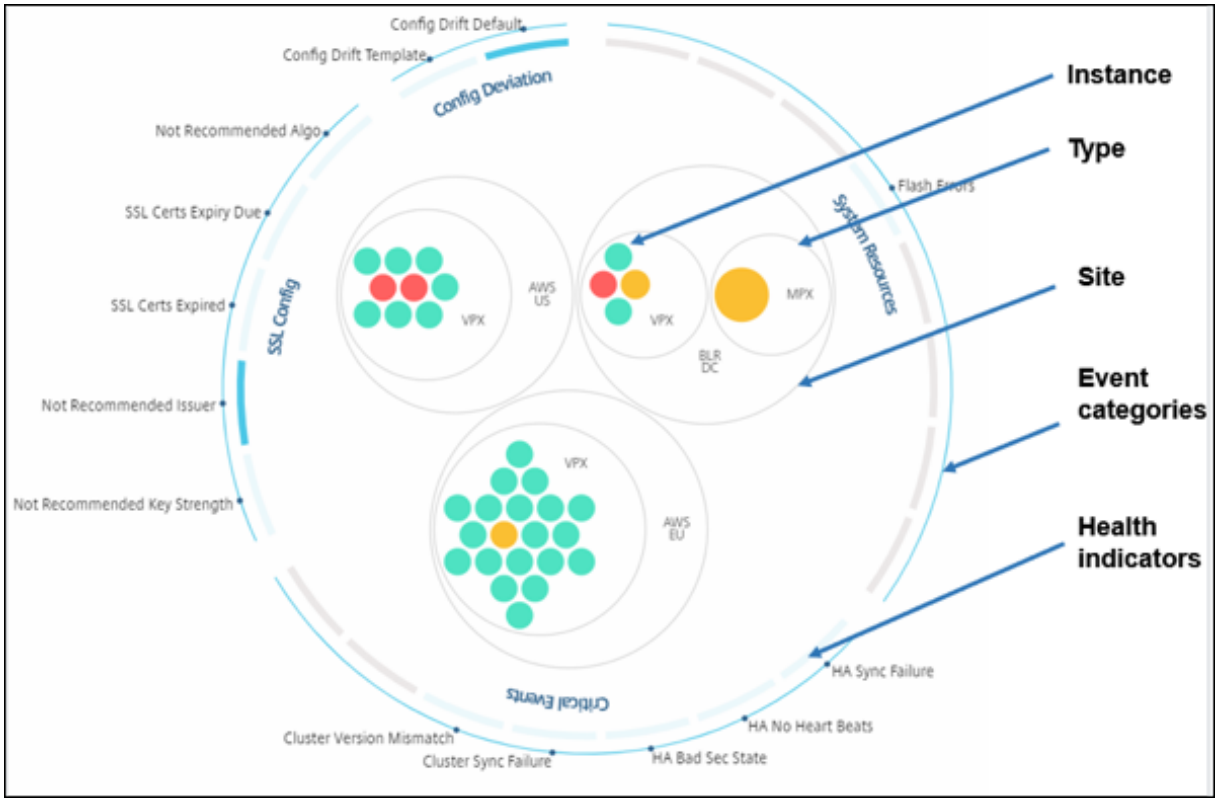


グループ化されたインスタンス円

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。

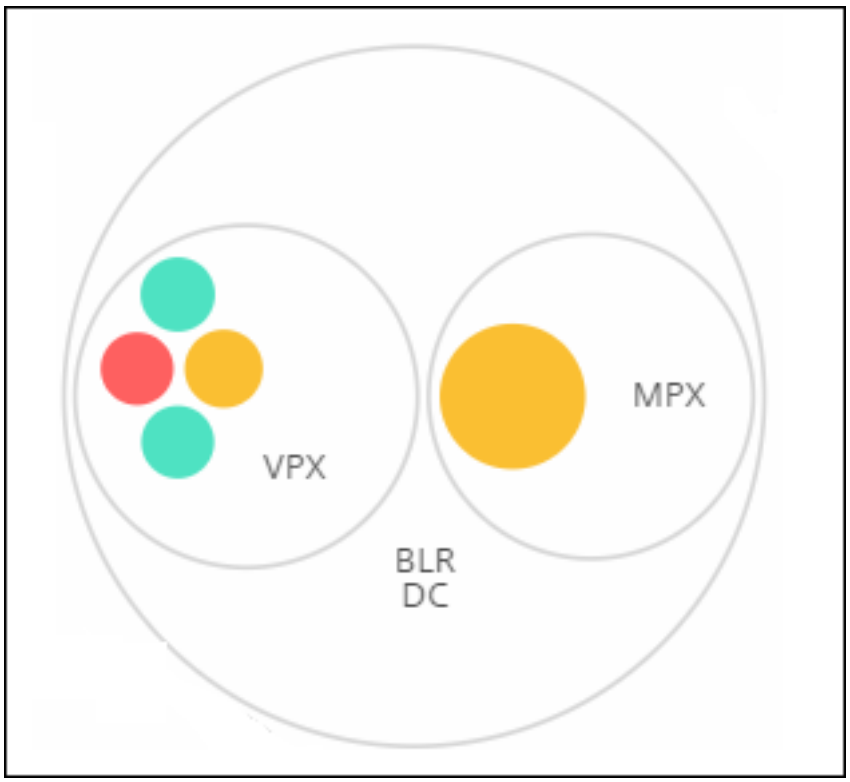


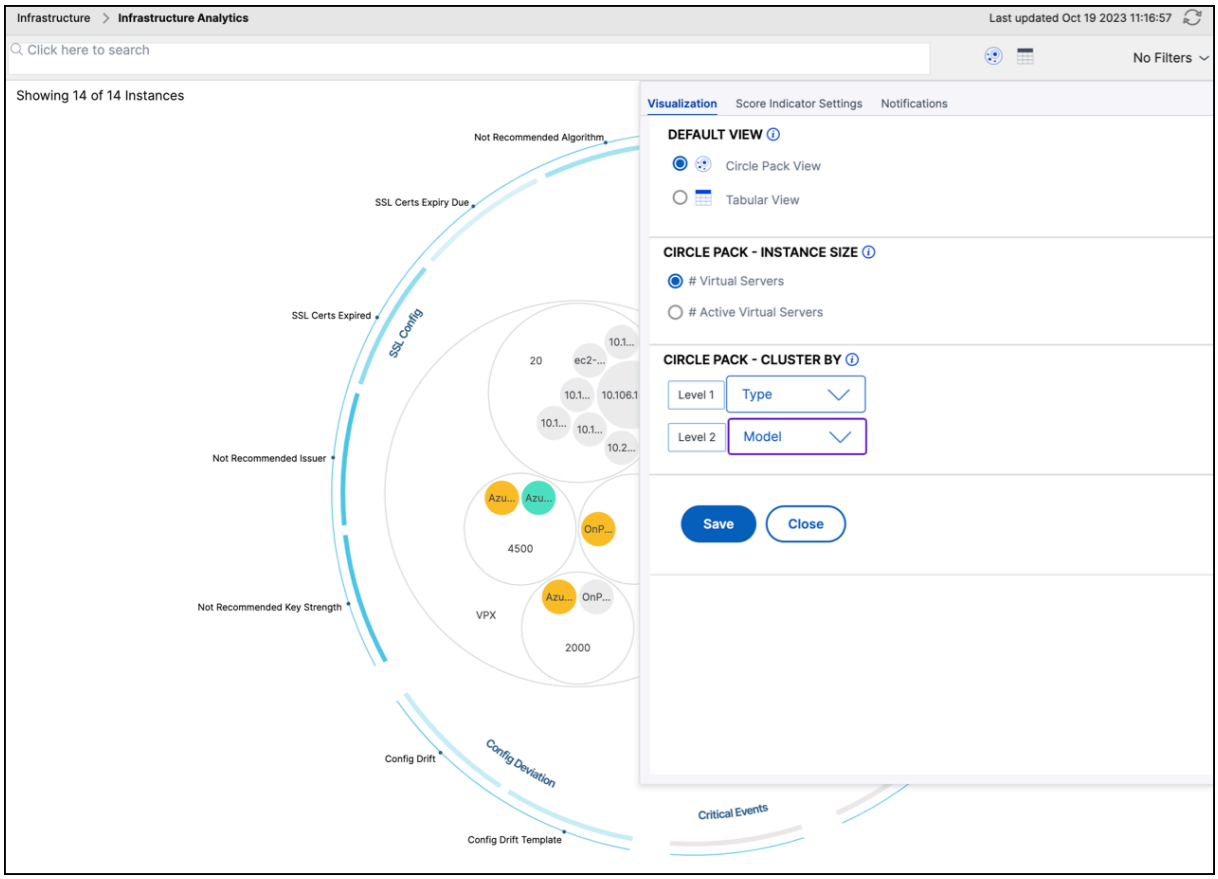
これらのネストされた円はすべて、最も外側の 2 つの円で囲まれています。外側の 2 つの円は、NetScaler ADM によって監視されるイベントの 4 つのカテゴリ（システムリソース、重要なイベント、SSL 構成、および構成の逸脱）とそれに寄与する正常性指標を表しています。

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の数を簡単に特定できるようになりました。

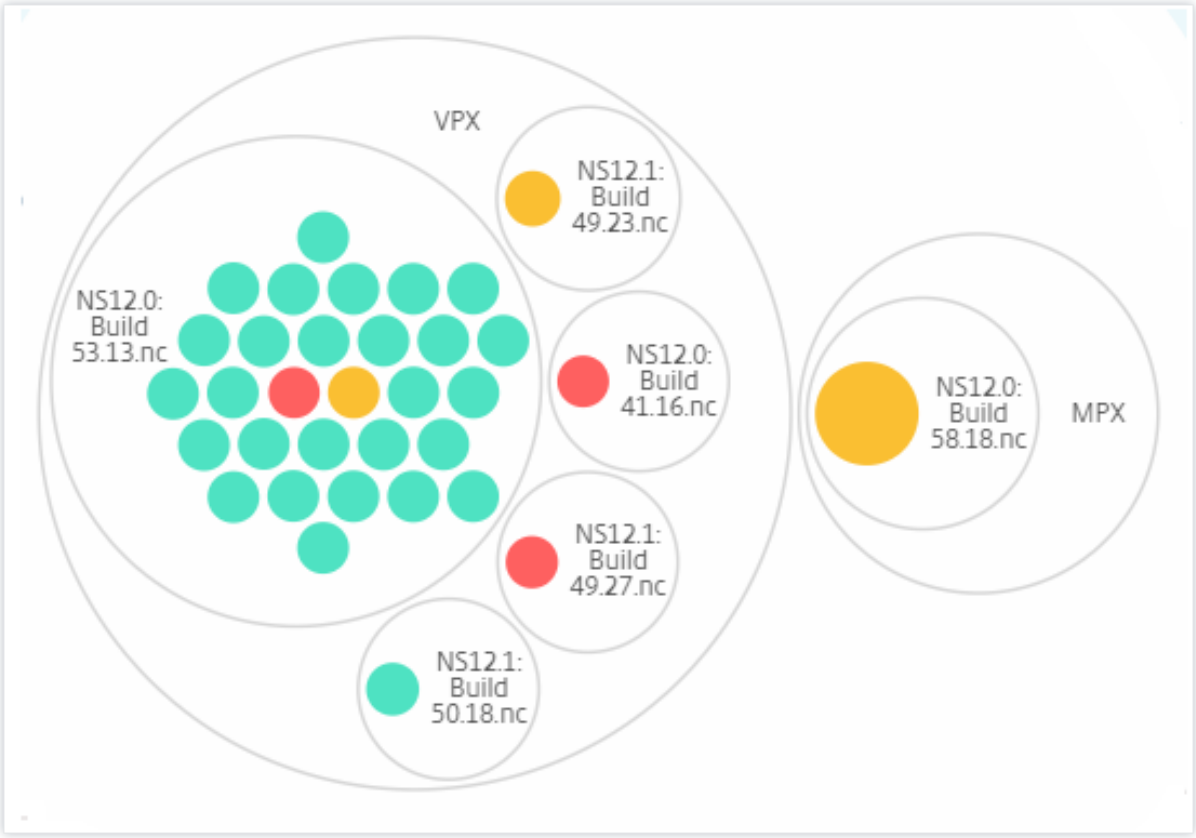




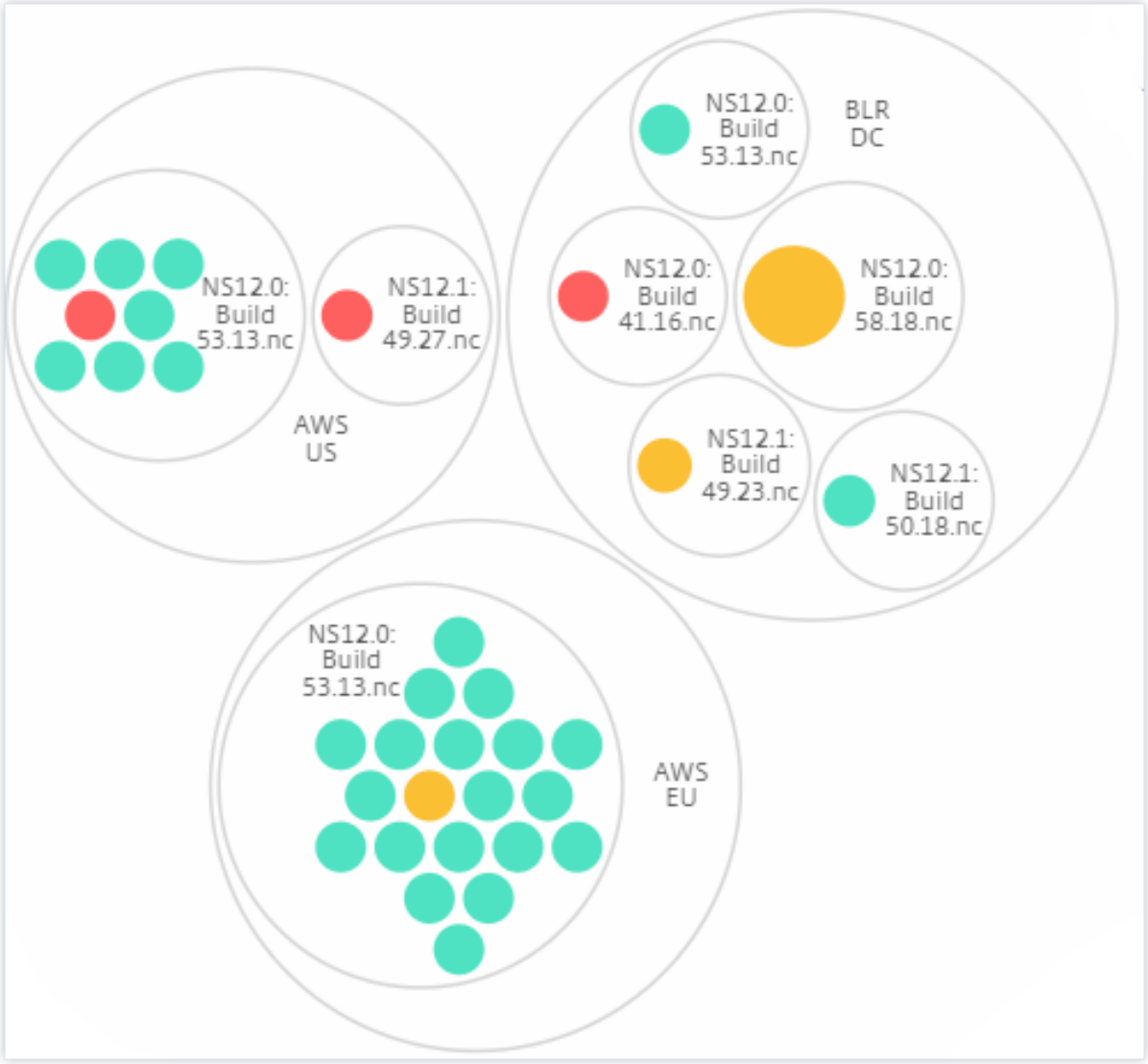
2 レベルクラスタリングのさらにいくつかの例を次に示します。

サイトとモデル**:**

タイプとバージョン**:**

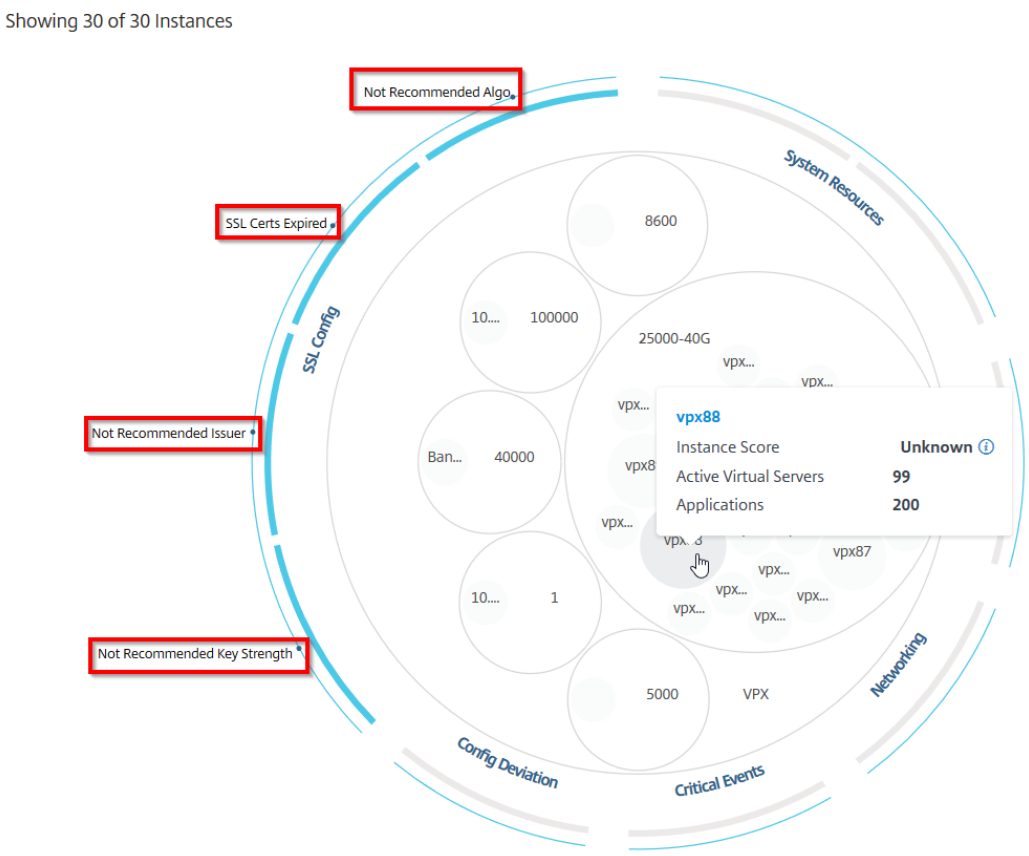


サイトとバージョン**:**



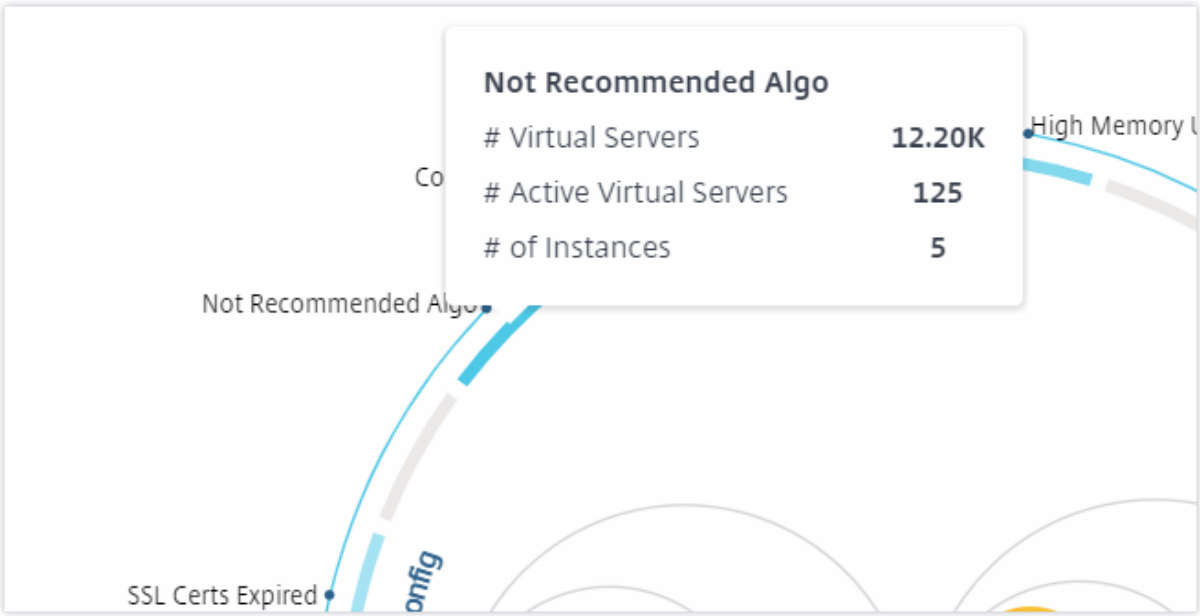
サークルパックの使用方法

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。



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。

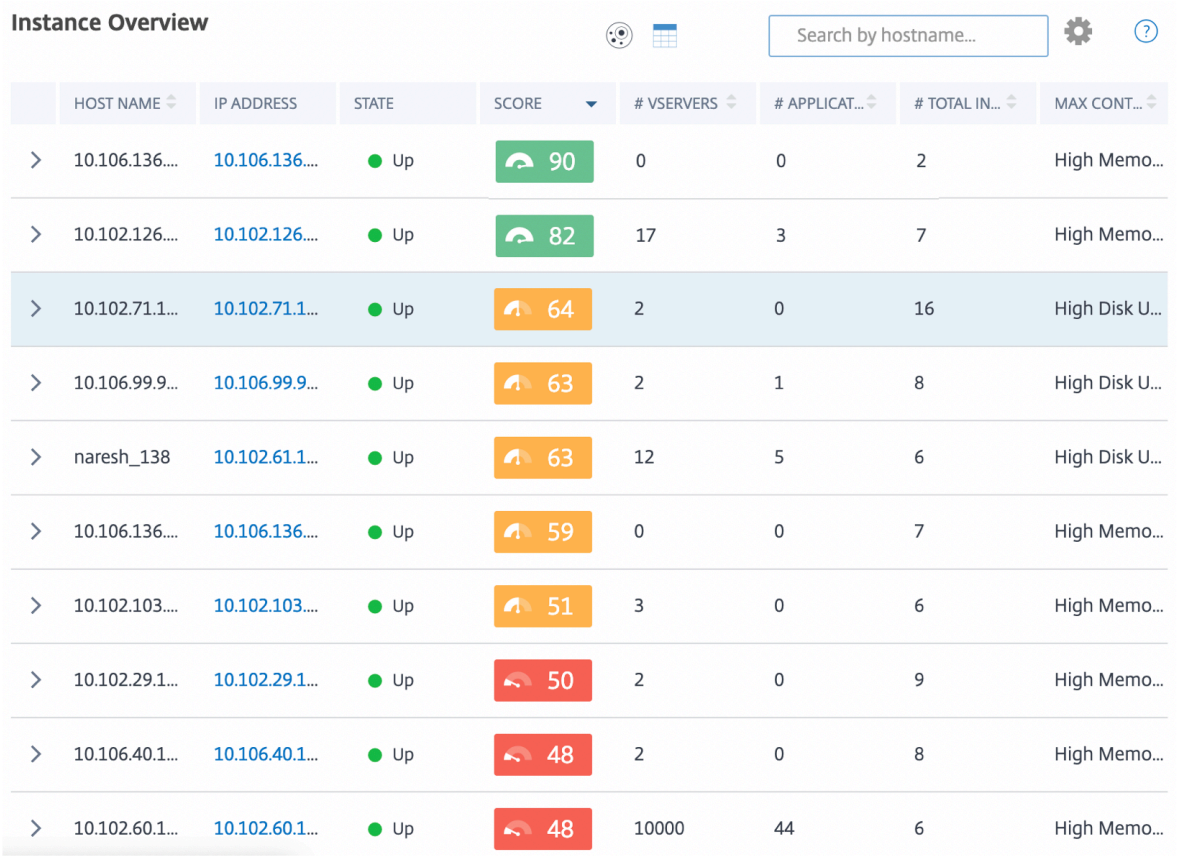


表形式ビュー

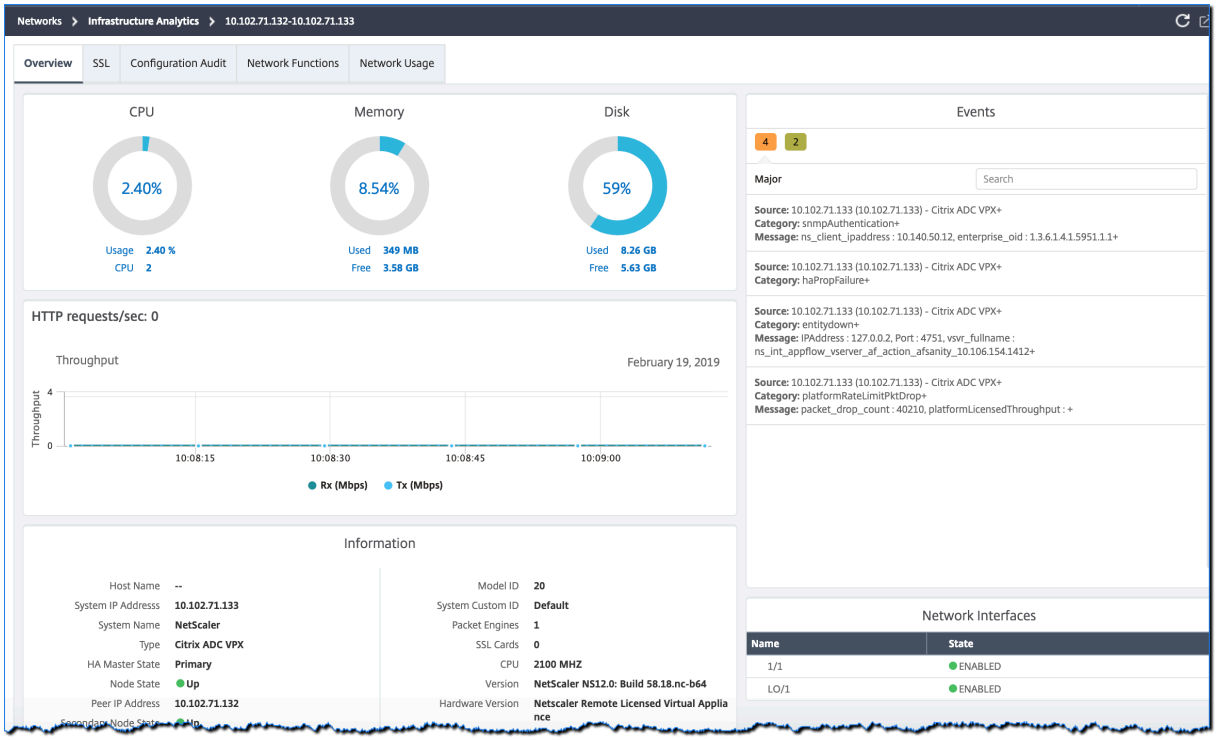
表形式ビューには、インスタンスとインスタンスの詳細が表形式で表示されます。表示される詳細は次のとおりです。

- 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

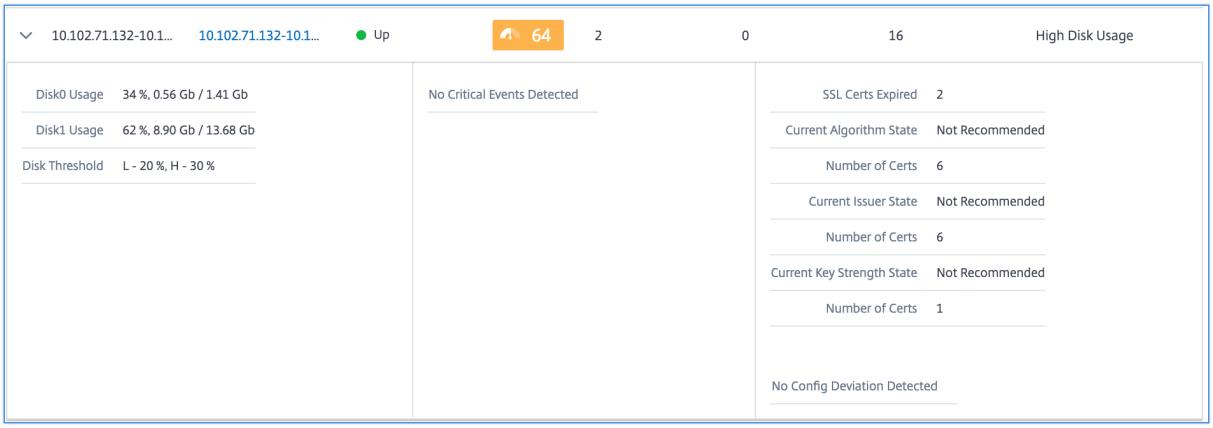
重要な状態のインスタンスが表の一番上にあり、その後にレビューが必要なインスタンス、そしてより正常なインスタンスが続きます。



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。

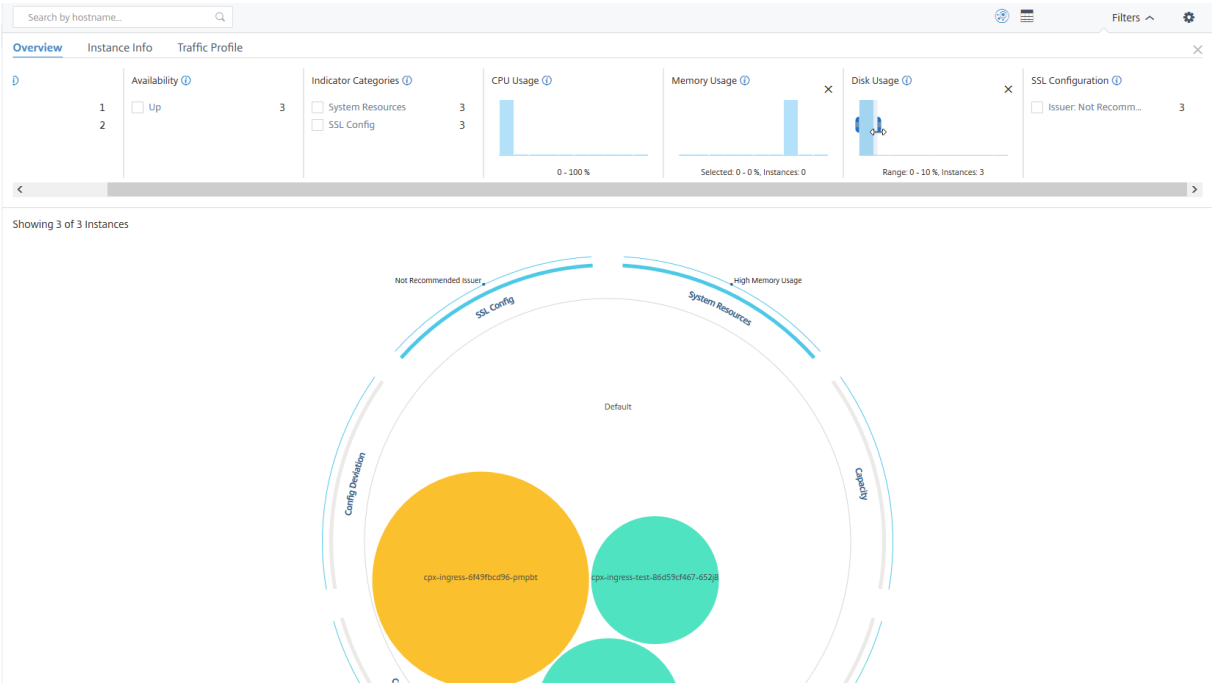
例 **2:** 割り当てられたメモリの **10%** から **20%** を消費しているインスタンスを表示する**:**

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。

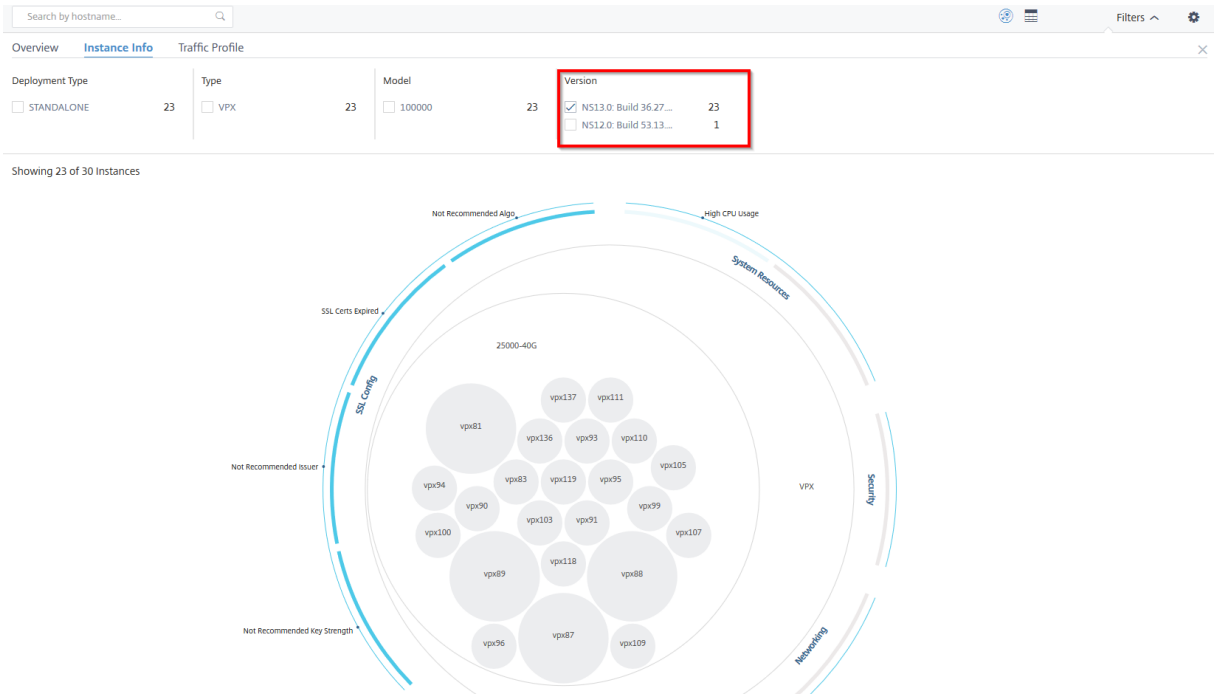
2 - **SSL** 証明書の有効期限セクションで、[期限切れ] チェックボックスを選択してインスタンスを表示します。

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 **NetScaler 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。

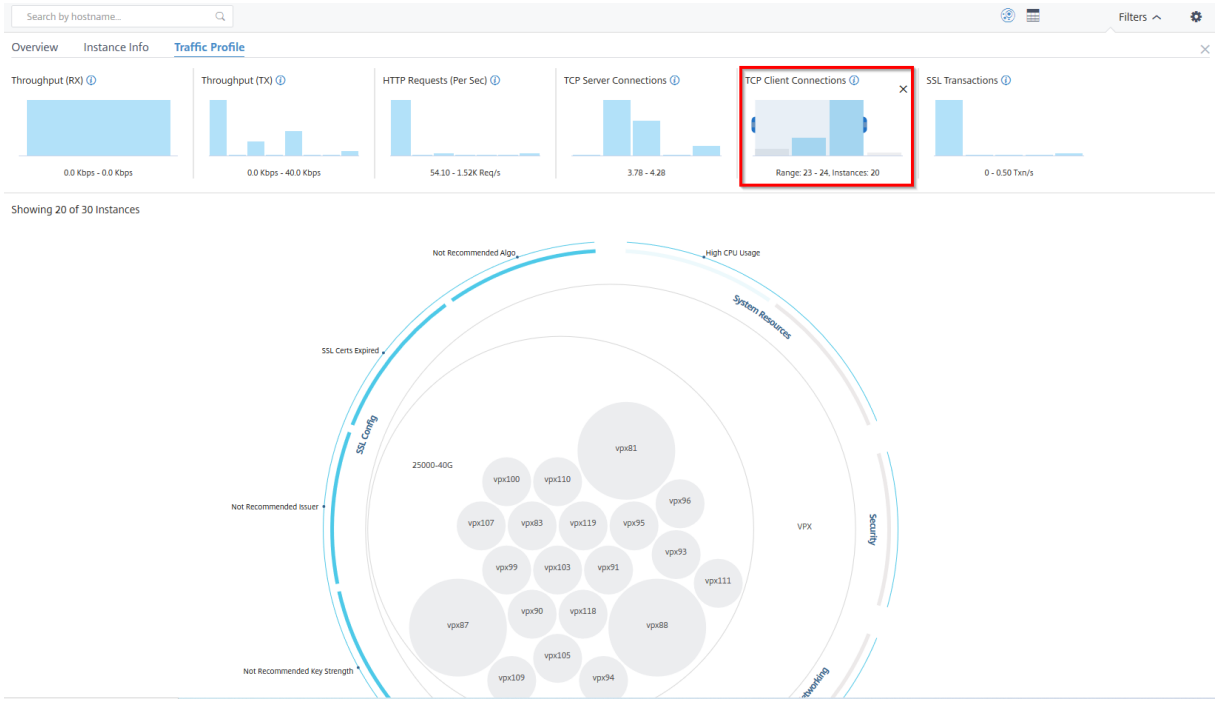


トラフィックプロファイル

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。

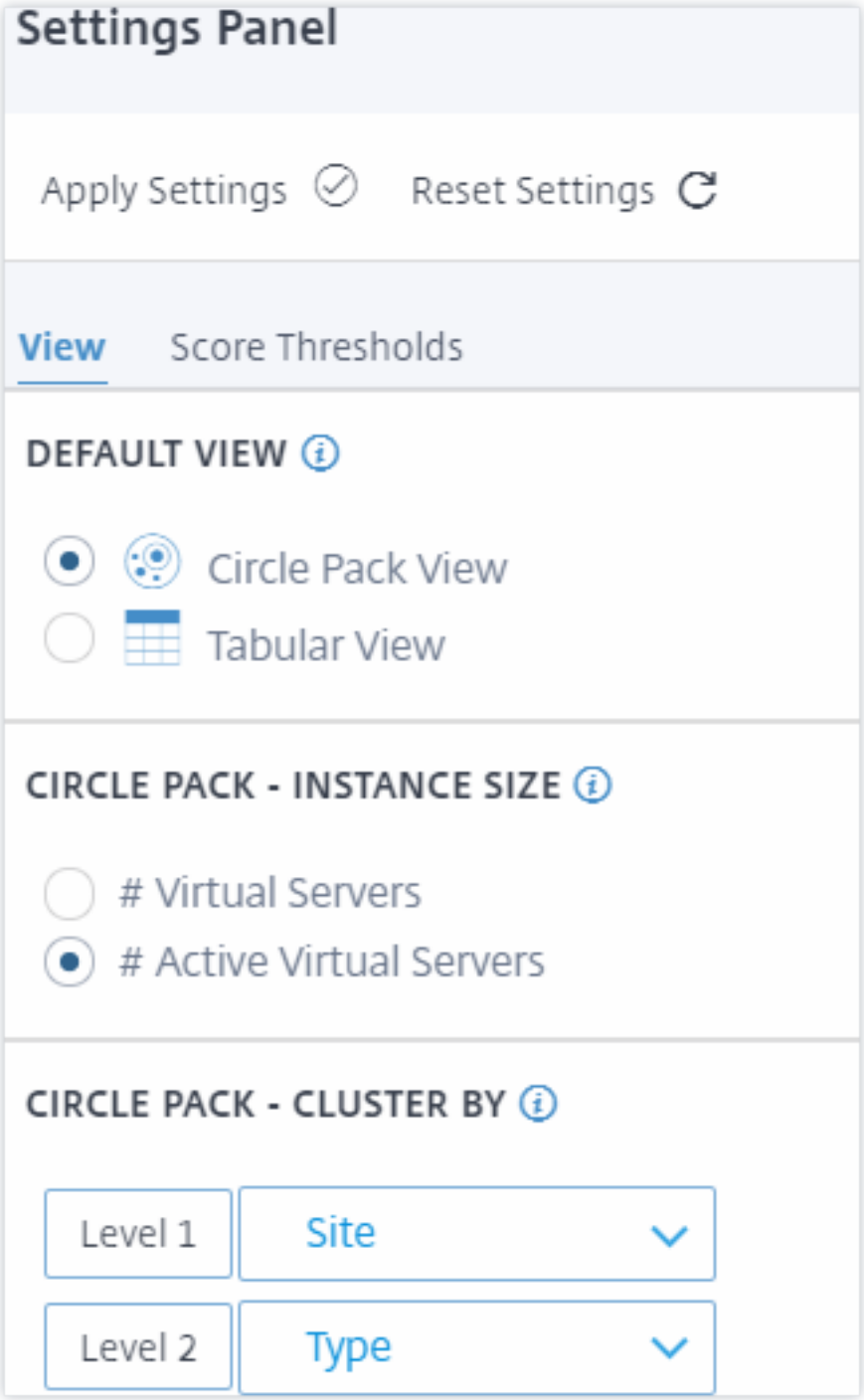


設定パネルの使い方

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、しきい値の下限値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。

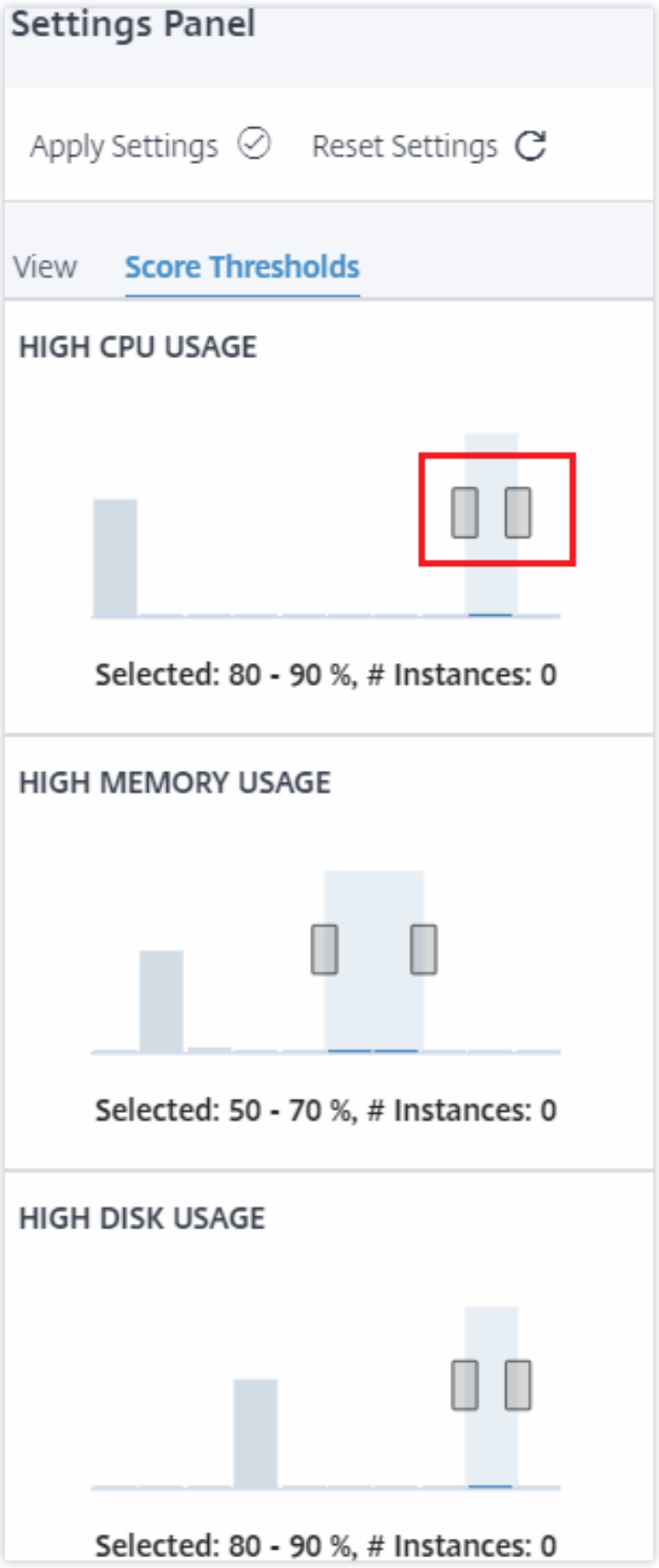
表示

- 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。



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。



> 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数の NetScaler 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付きました。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、データを手動で相関させ、どのインスタンスが最適な状態になく、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付きます。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。

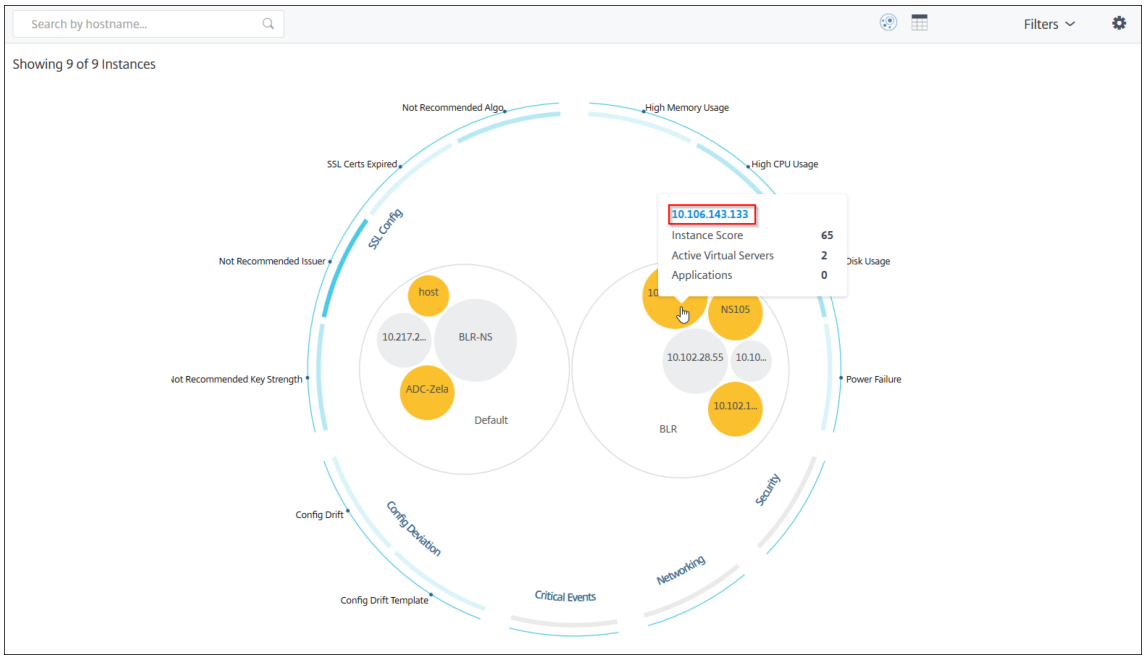
例 **2-**構成の変更を監視するには**:**

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付きます。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付きますが、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付きました。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。

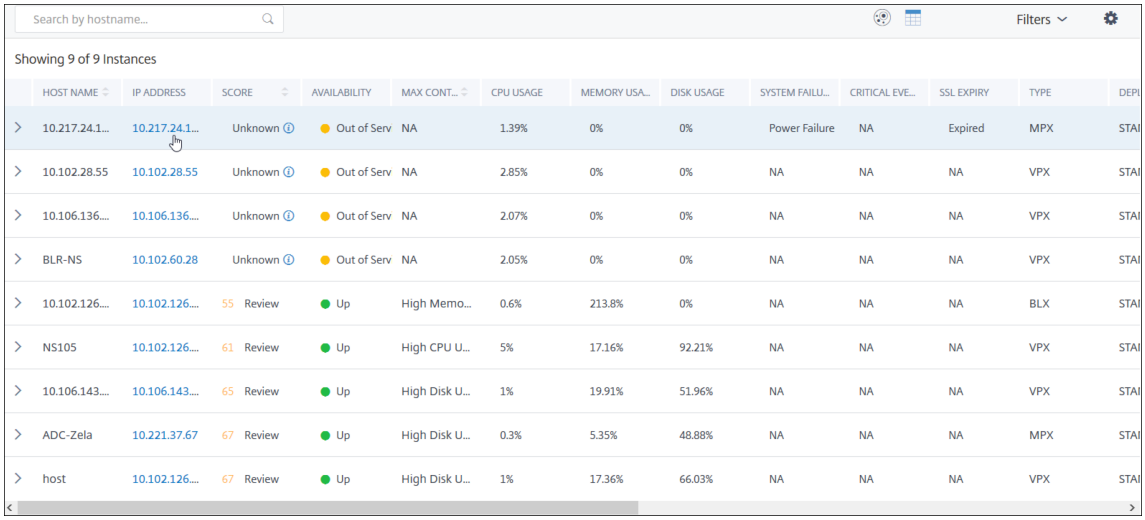
インフラストラクチャ分析でのインスタンスの詳細の表示

February 6, 2024

1. インフラストラクチャ **>** インフラストラクチャ分析に移動します。
2. サークルパックビューをクリックし、IP アドレスを選択します。



テーブルビューから IP アドレスをクリックすることもできます。



- ホスト名—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

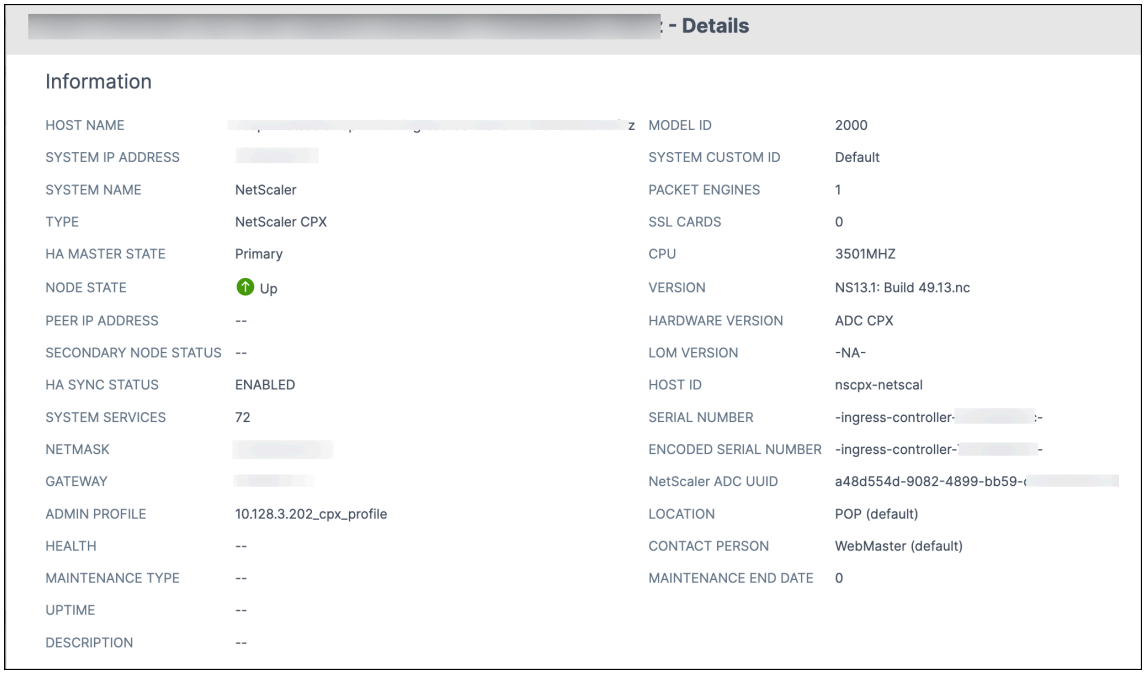
- メモリ使用量—インスタンスが現在使用しているメモリ (%) を示します
- **Disk usage** —インスタンスが現在使用しているディスク (%) を示します
- システム障害—インスタンス・システムのエラーの総数を示します
- 「クリティカルイベント」—NetScaler インスタンスに最大イベントがあるイベントカテゴリを示します。
- **SSL** 有効期限—ADC インスタンスにインストールされている SSL 証明書のステータスを示します
- タイプ: VPX、SDX、MPX、CPX などの ADC インスタンスタイプを示します。
- デプロイ—ADC インスタンスがスタン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。

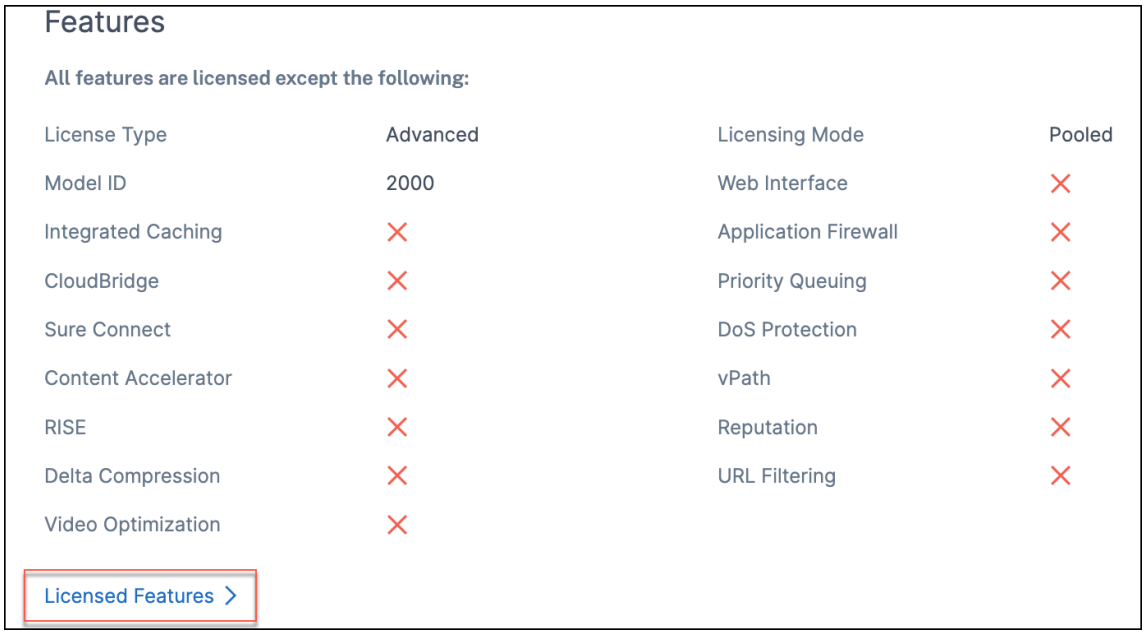
[インスタンスの詳細] をクリックして詳細を表示します。

次の詳細が表示されます。

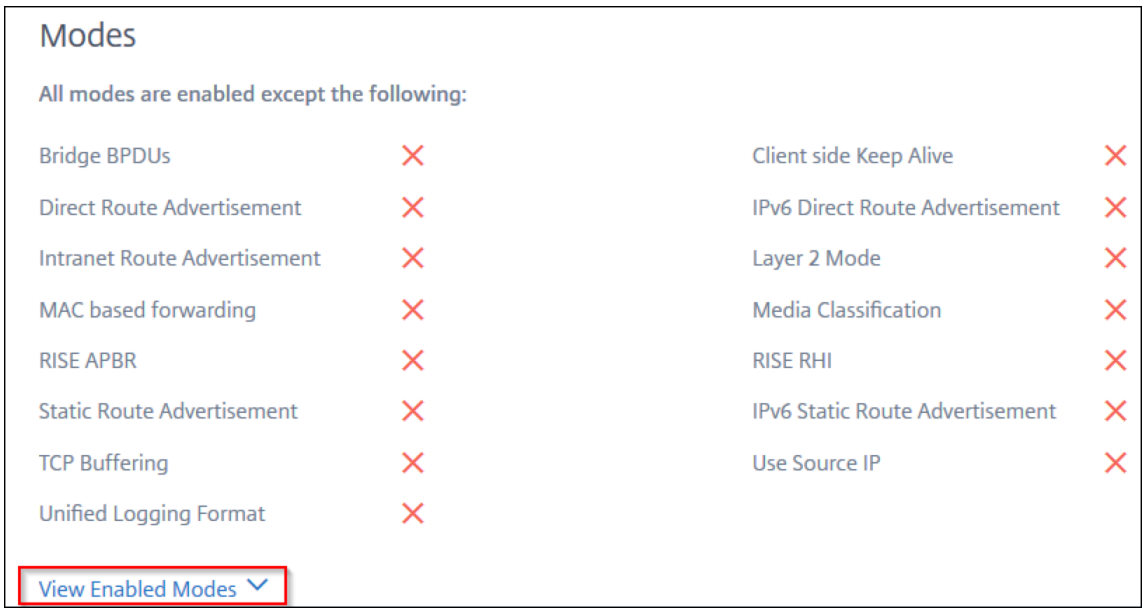
- 情報 -インスタンスタイプ、デプロイタイプ、バージョン、モデルなどのインスタンスの詳細。



- 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。

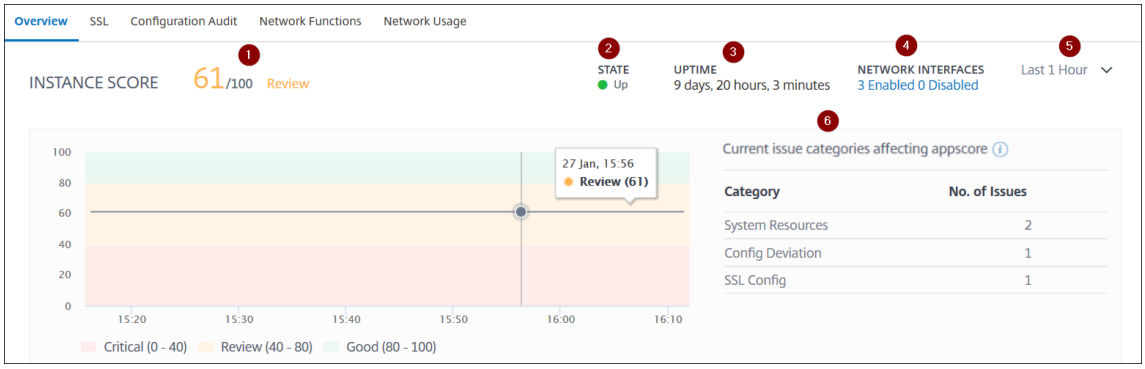


- モード—デフォルトでは、インスタンスで無効になっているすべてのモードが表示されます。「有効化されたモードを表示」をクリックすると、インスタンスで有効になっているモードが表示されます。



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 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 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。

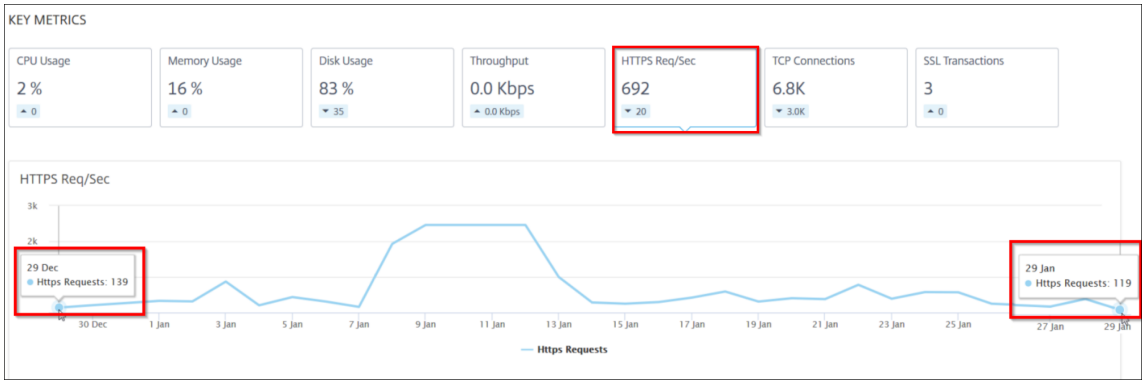
5 —インスタンスの詳細を表示する期間をリストから選択します。

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。

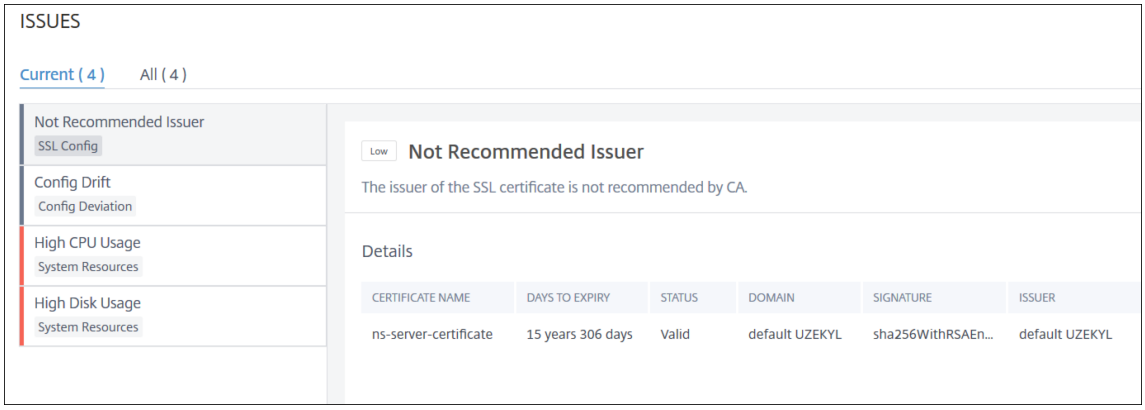
- 問題点

  NetScaler 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、NetScaler システムリソースに関連するすべての問題を表示します。	– 高い CPU 使用率 – 高いメモリ使用量 – 高いディスク使用量 – SSL カード障害 – 停電 – ディスクエラー – フラッシュエラー

問題カテゴリ	説明	問題
		– NIC 廃棄
SSL 設定	NetScaler 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。	-SSL 証明書の有効期限切れ – 推奨されない発行者 – 推奨されないアルゴリズム – 推奨キーストレングスではありません
設定偏差	NetScaler インスタンスに適用された構成ジョブに関連するすべての問題を表示します。	-構成ドリフト – 実行とテンプレート
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。	– クラスタプロップ障害 – クラスタ同期失敗 – クラスタバージョンの不一致 – HA セカンダリステートが不良です – HA ノーヒートビート – HA 同期失敗 – HA バージョンの不一致
ネットワーク	インスタンスで発生する運用上の問題を表示します。	詳細については、「新しい指標によるインフラストラクチャ分析の強化」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. [インフラストラクチャー**] > [**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:

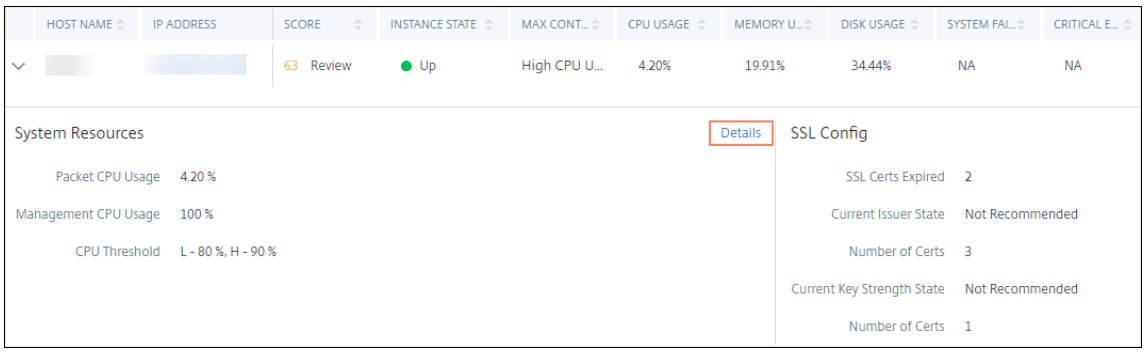
問題は次の容量パラメータに分類されます。

- 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。

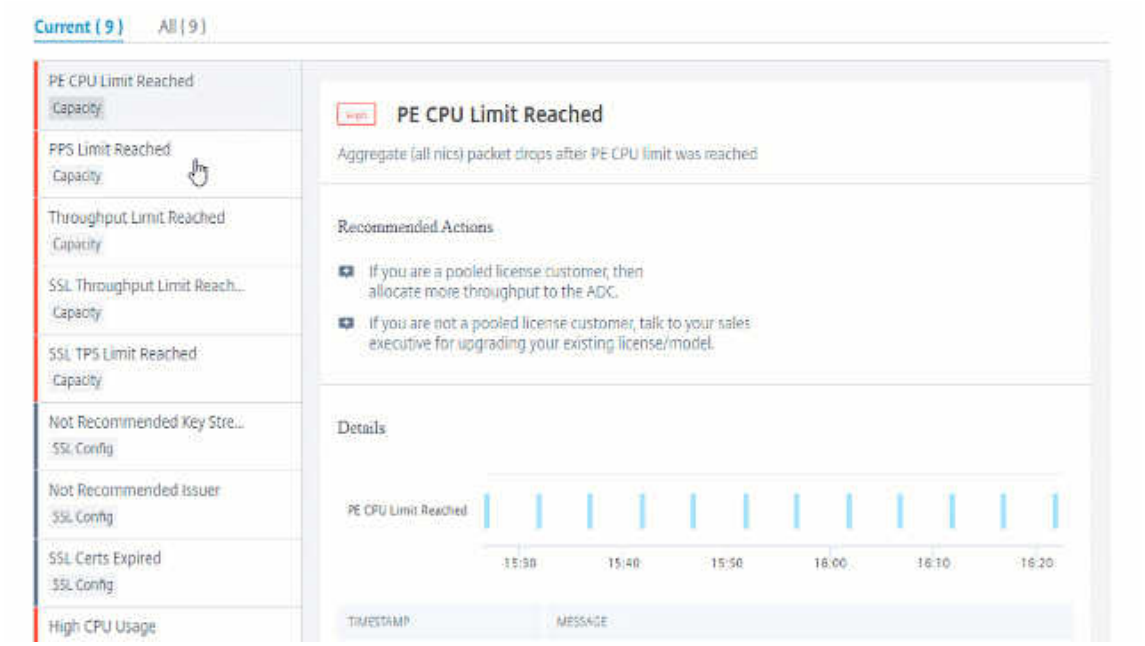
キャパシティの問題を解決するための推奨アクションを表示

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. [インフラストラクチャ**] > [**インフラストラクチャ分析] で、表形式ビューを選択します。
2. 容量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。



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。



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ー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 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。

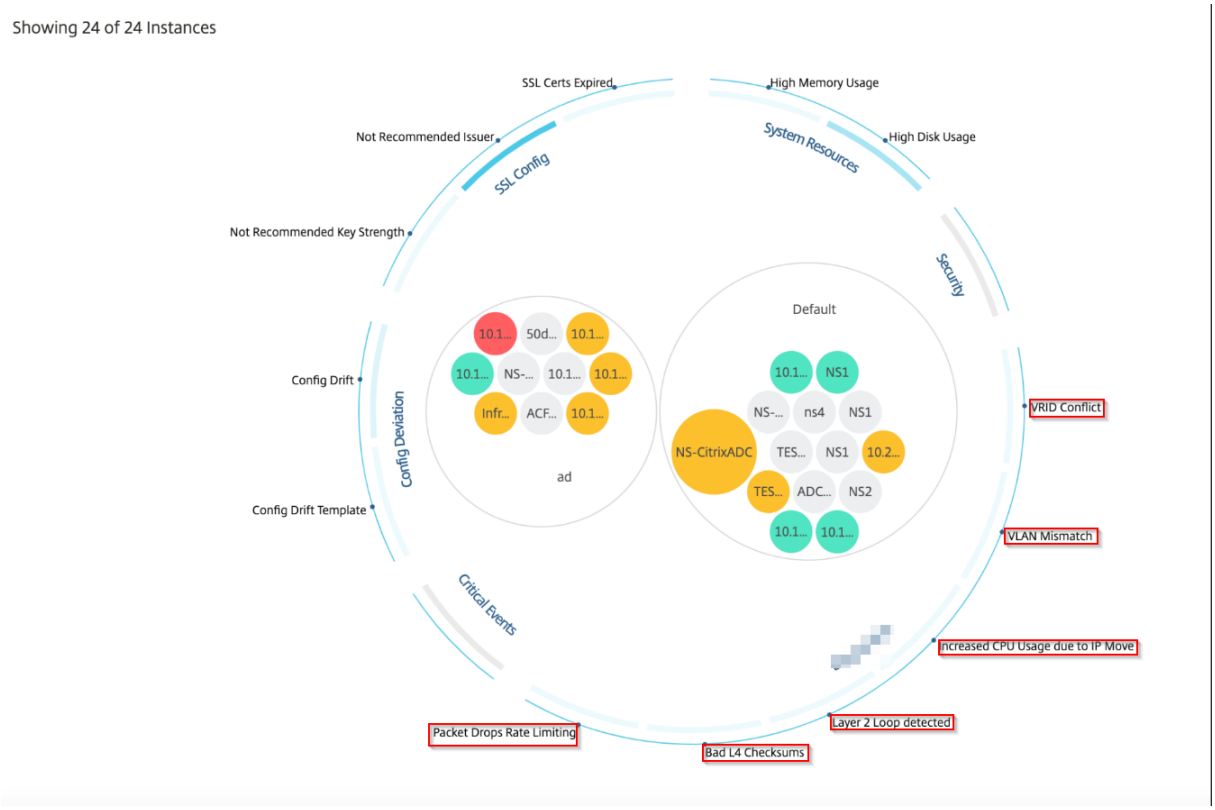
管理者は、問題の根本原因分析をすばやく特定できます。

> 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 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、［インフラストラクチャ］**>**［インフラストラクチャ分析］に移動して、以下のインジケーターを表示します。

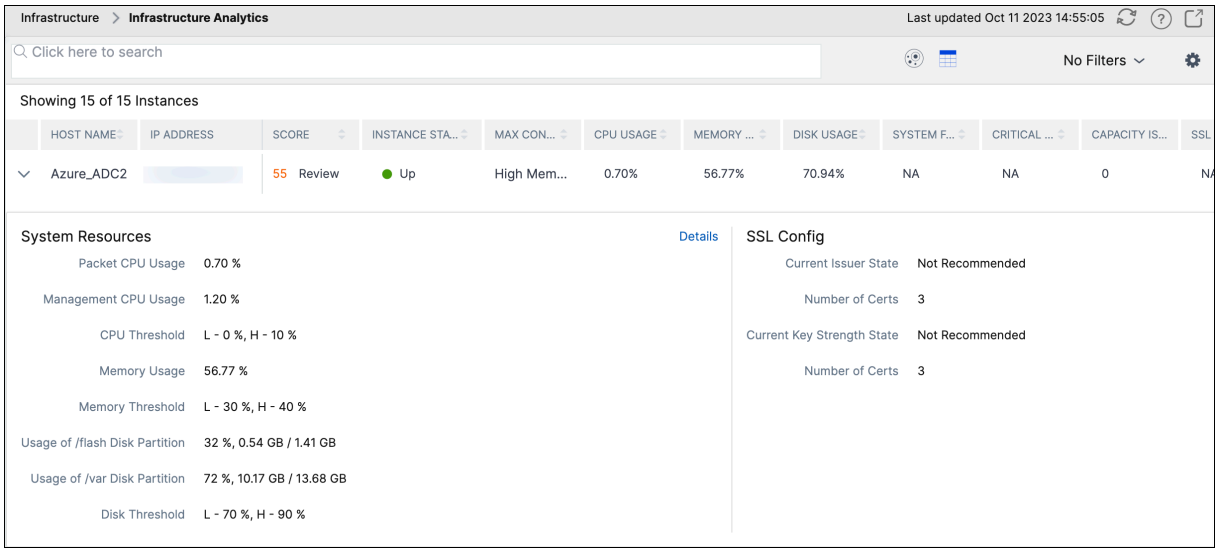
インフラストラクチャ分析のインジケータ名	説明
ポート割り当ての失敗	NetScaler ADC が SNIP を使用して新しいサーバー接続と通信し、その SNIP で使用可能なポートの合計が使い果たされたことを検出します。推奨されるアクションは、同じサブネットに別の SNIP を追加することです。
デフォルトのルート設定なし	ルートが使用できないためにトラフィックがドロップされたことを検出します。
IP の競合	ネットワーク内の複数のインスタンスに同じ IP アドレスが設定または適用されているかどうかを検出します。
VRID の競合	指定した VRID で断続的なアクセスの問題が発生したことを検出します。
VLAN 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。
TCP スモールウィンドウ攻撃	進行中のスモールウィンドウ攻撃の可能性を検出します。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 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
GSLB サイト名の不一致	サイト名の不一致が原因で GSLB 構成の同期エラーが発生したことを検出します。
不正な **IP** 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 **L4** チェックサム	TCP パケットのチェックサム検証が失敗したことを検出します。
IP 移動による **CPU** 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 **2** 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 **VLAN** の不一致	タグ付き VLAN パケットがタグなしインターフェイスで受信されたことを検出します。



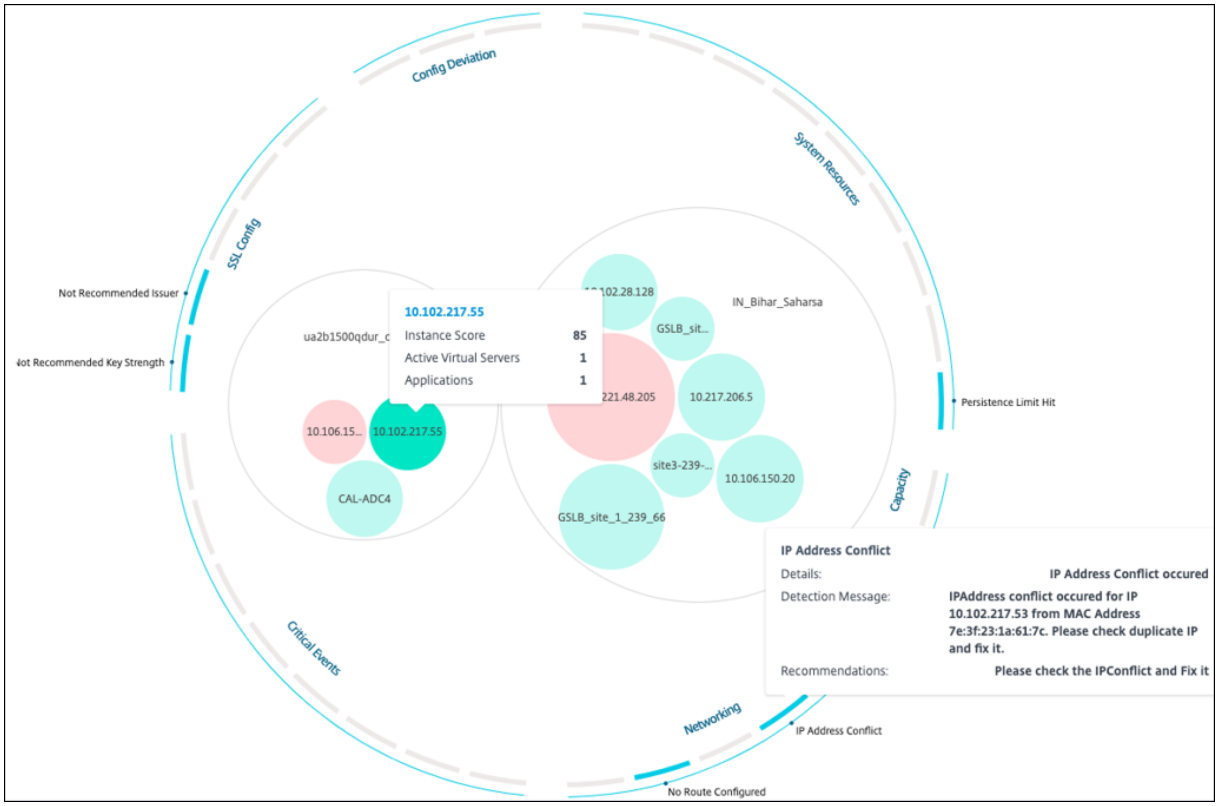
表形式ビュー

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。[インフラストラクチャ**] > [**インフラストラクチャ分析] に移動し、[ ] 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。



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。

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、およびトラブルシューティングできる Citrix アプリケーション 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、NetScaler ADM のセットアップ時または後で追加できます。NetScaler ADM にインスタンスを追加すると、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、[インフラストラクチャ**] > [**インスタンス**]** に移動して **[**すべてのインスタンス**]** をクリックすることで、その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。

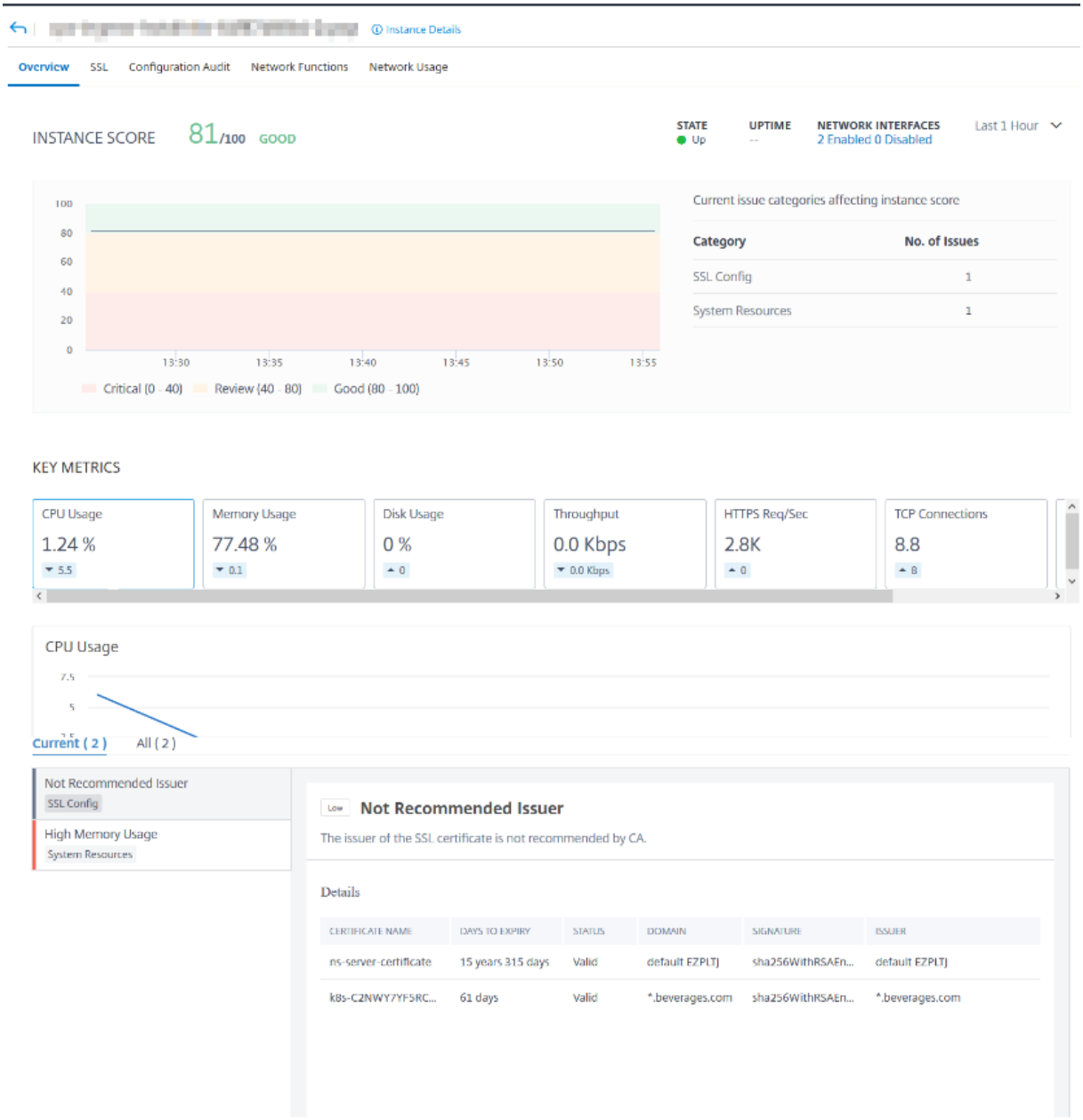
インスタンスダッシュボードの使用方法

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、[インフラストラクチャ**] > [**インスタンス] に移動します。概要からインスタンスタイプを選択し、表示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。

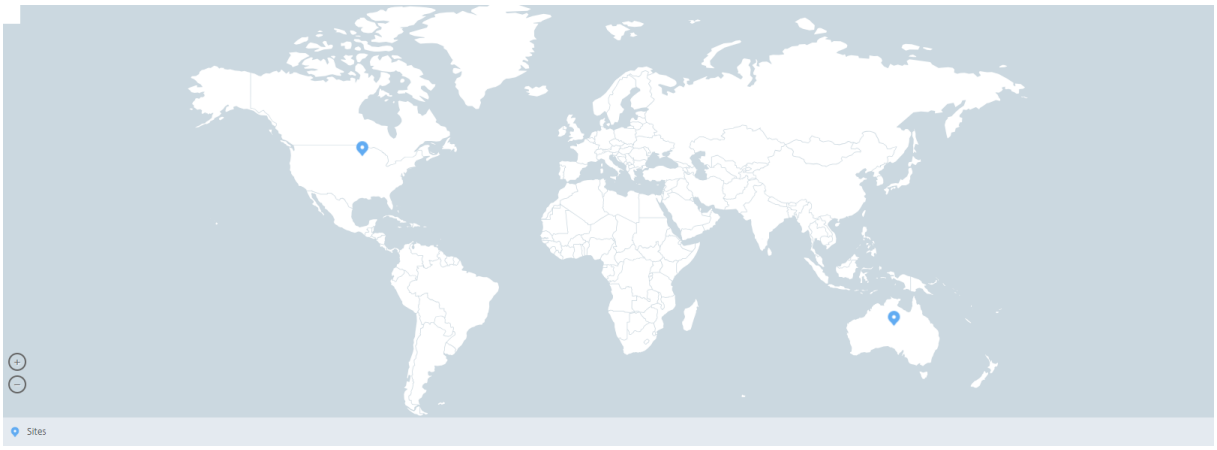
次のセクションでは、NetScaler ADM でデータセンターを監視する方法について説明します。

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 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。

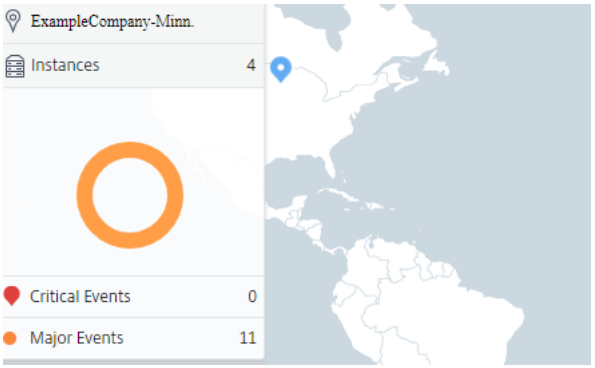
NetScaler ADM のジオマップでは、サイトをグラフィカルに表示できます。ジオマップでは、ネットワークモニタリング体験を地域ごとに分類することもできます。ジオマップを使用すると、場所ごとにネットワークインスタンスの分布を視覚化し、すべてのネットワーク問題を監視できます。[インフラストラクチャ**] > [**インスタンス] ページに移動すると、ワールドマップ上に作成されたサイトを視覚的に表示できます。

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。

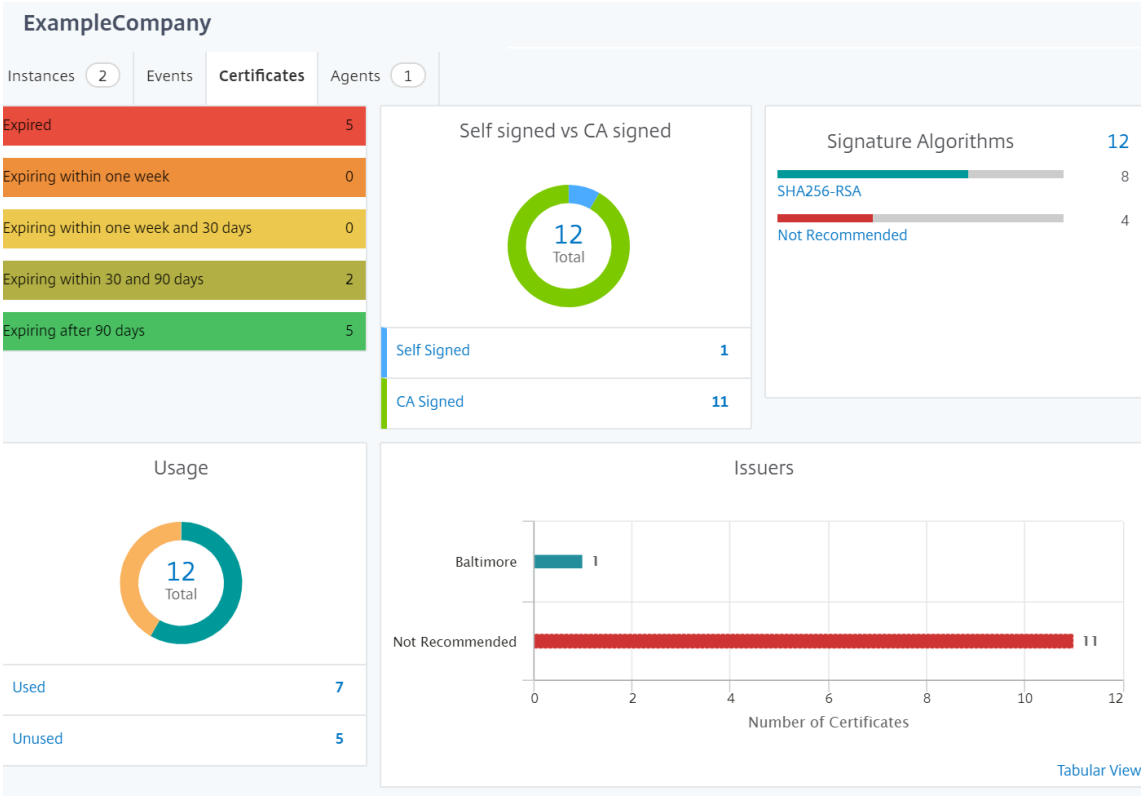


タブをクリックして、詳細情報を表示します。

- 「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 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 インスタンスとエージェントが属するサイトを認識します。

NetScaler インスタンスの追加について詳しくは、「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。

[インフラストラクチャ] > [インスタンス] > [サイト] に移動し、[追加] をクリックします。

1. **[** サイトの作成] ページで、次の情報を指定します。

   a) サイトタイプ: 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。

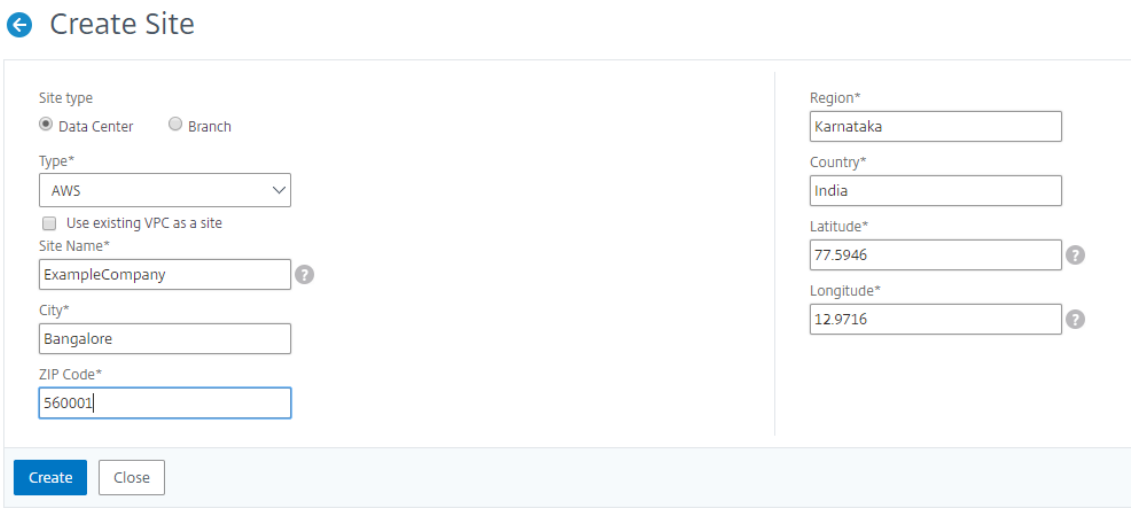
   f) 地域: 地域を入力します。

   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。

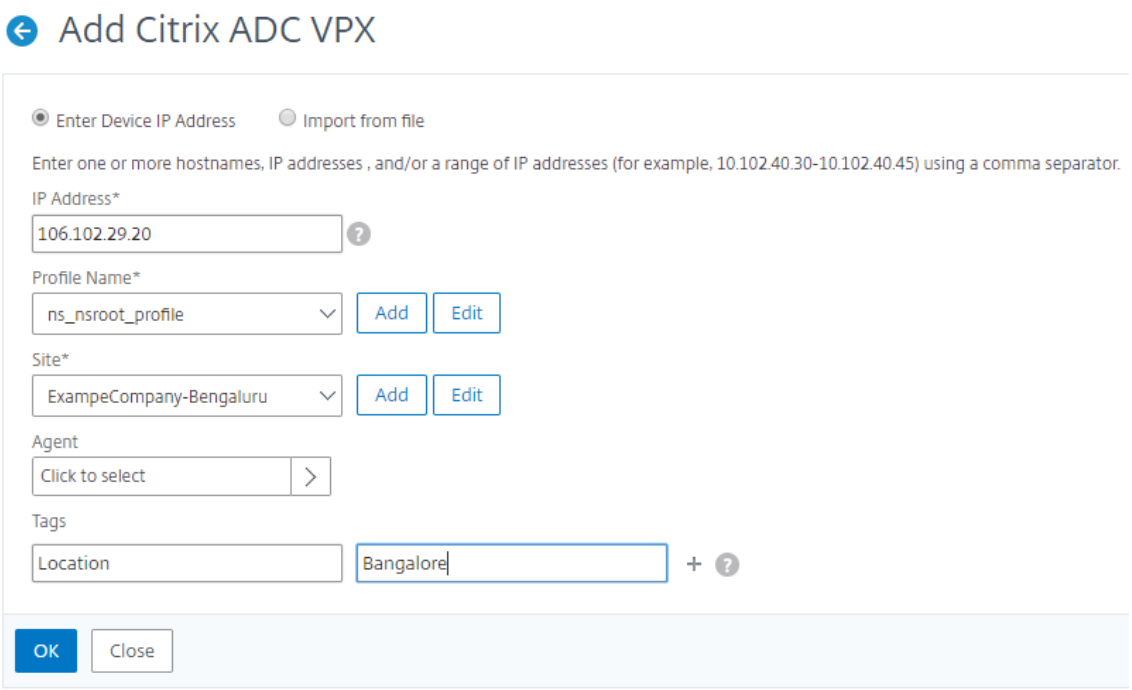


インスタンスを追加してサイトを選択するには**:**

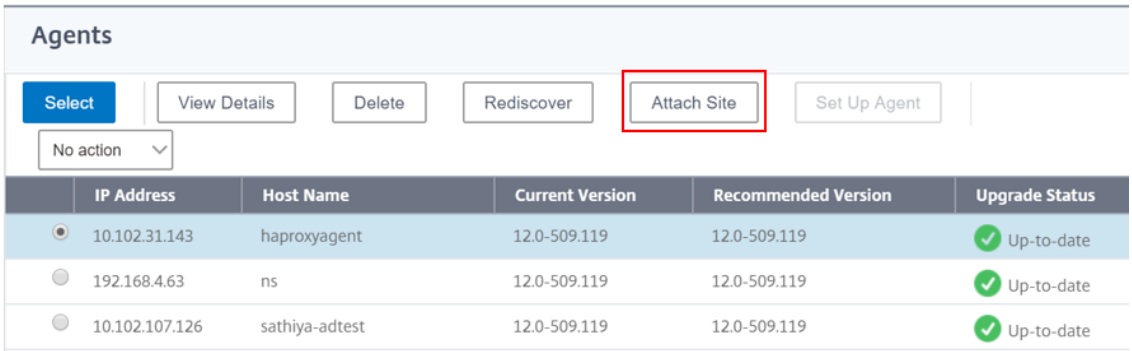
サイトを作成したら、NetScaler ADM にインスタンスを追加する必要があります。以前に作成したサイトを選択するか、サイトを作成してインスタンスを関連付けることもできます。

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、[インフラストラクチャ**] > [**インスタンス**]** に移動します。
2. 作成するインスタンスのタイプを選択し、[**Add**] をクリックします。
3. [**NetScaler VPX** の追加] ページで、IP アドレスを入力し、リストからプロファイルを選択します。
4. リストからサイトを選択します。サイトフィールドの横にある **+** 記号をクリックしてサイトを作成するか、編集アイコンをクリックしてデフォルトサイトの詳細を変更できます。
5. 右矢印をクリックし、表示されるリストからエージェントを選択します。



6. エージェントを選択したら、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。



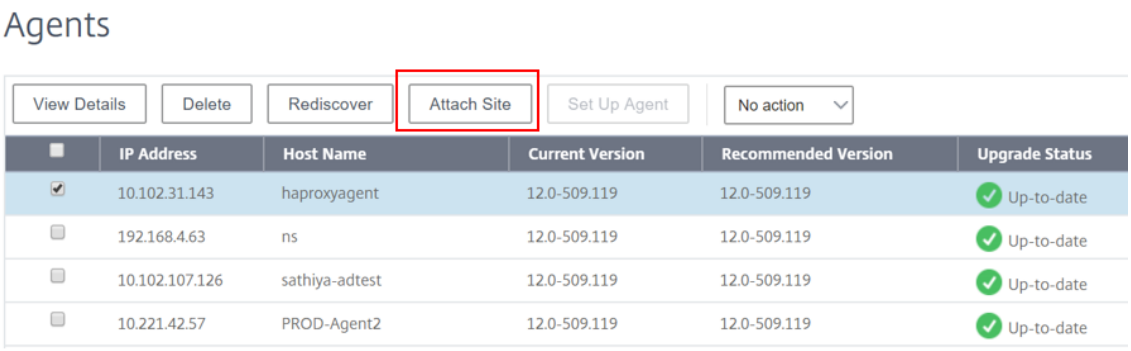
1. リストからサイトを選択し、[保存] をクリックします。

1. [**OK**] をクリックします。

[インフラストラクチャ] > [インスタンス] > [エージェント] の順に移動して、エージェントをサイトにアタッチすることもできます。

NetScaler ADM エージェントをサイトに関連付けるには:

1. NetScaler ADM で、インフラストラクチャ > インスタンス > エージェントの順に移動します。
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。



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

NetScaler 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。

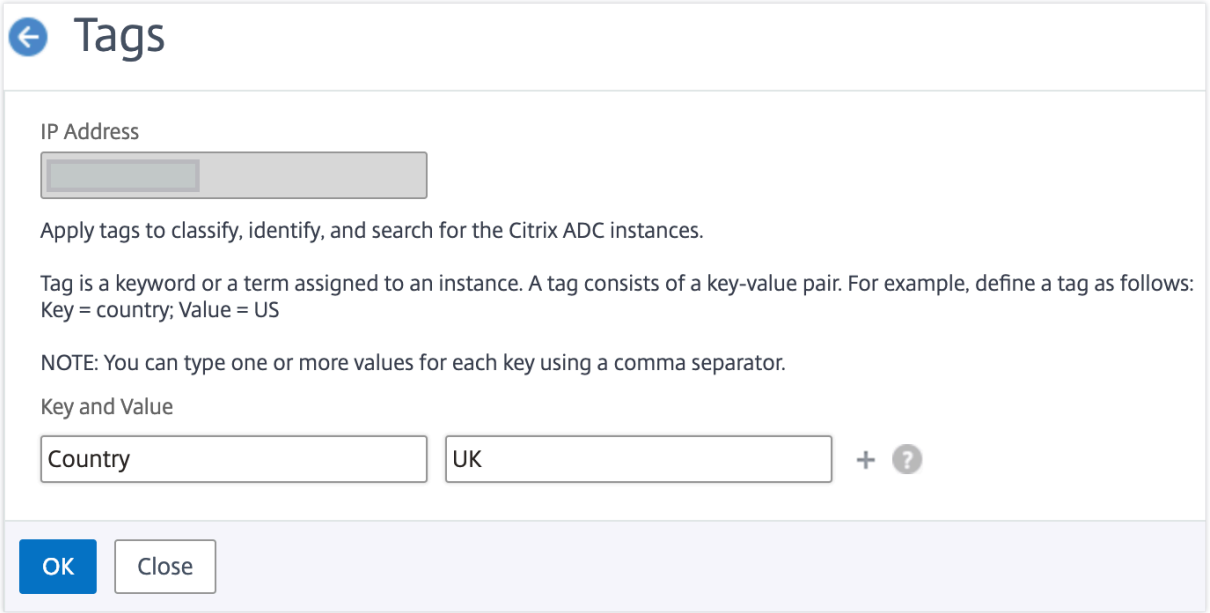
- ユースケース **2**: ステージング環境にあるインスタンスを検索する場合。ここでは、キーを「目的」、値を「staging_NS」としてタグを作成できます。このタグは、ステージング環境で使用されているすべてのインスタンスを、クライアント要求が実行されているインスタンスから分離するのに役立ちます。
- ユースケース **3**: 英国の「Swindon」エリアにあり、David T（David T）が所有している NetScaler ADC インスタンスのリストを調べる状況を考えてみましょう。これらすべての要件に対応するタグを作成し、これらの条件を満たすすべてのインスタンスに割り当てることができます。

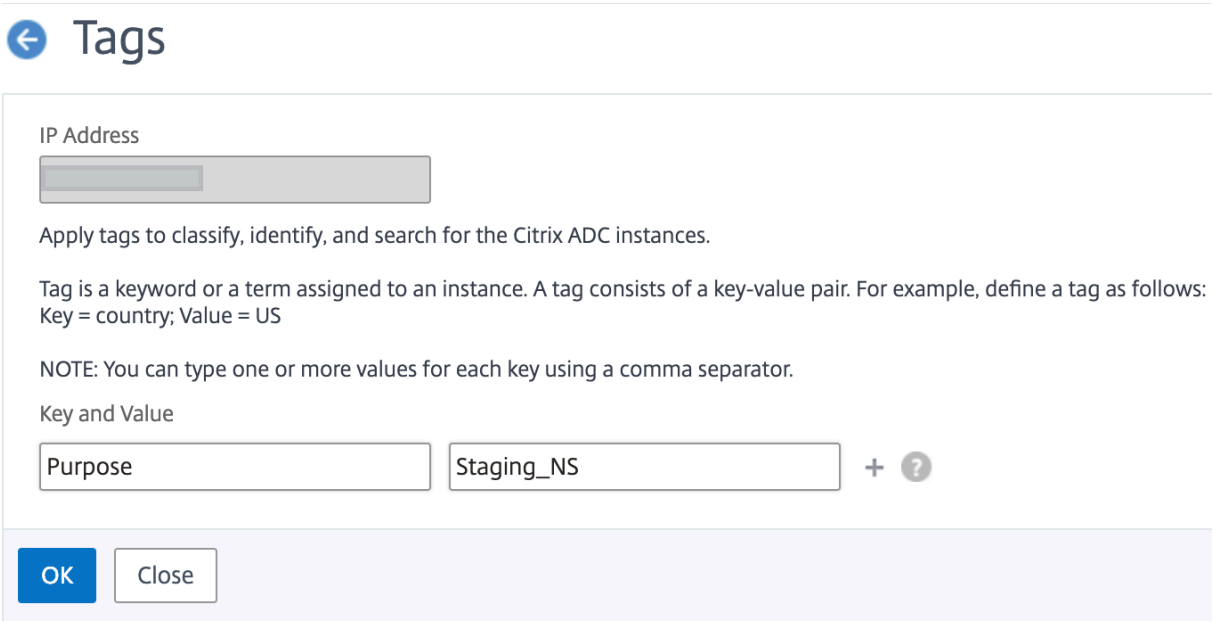
NetScaler VPX インスタンスにタグを割り当てるには:

1. NetScaler ADM で、インフラストラクチャ **>** インスタンス **> NetScaler** に移動します。
2. [**NetScaler VPX**] タブを選択します。
3. 必要な NetScaler VPX を選択します。
4. [タグ] をクリックします。
5. タグを作成して「**OK**」をクリックします。

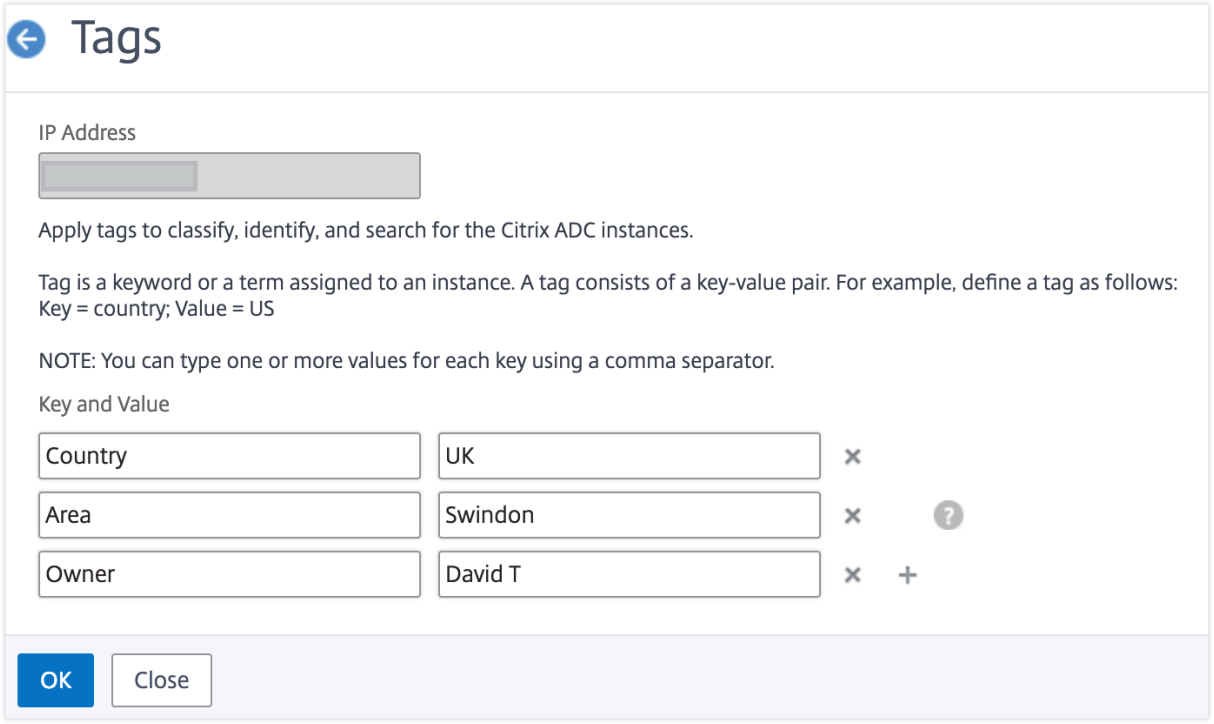
表示される [タグ] ウィンドウでは、作成したすべてのキーワードに値を割り当てることによって、独自の「キーと値」のペアを作成できます。

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。



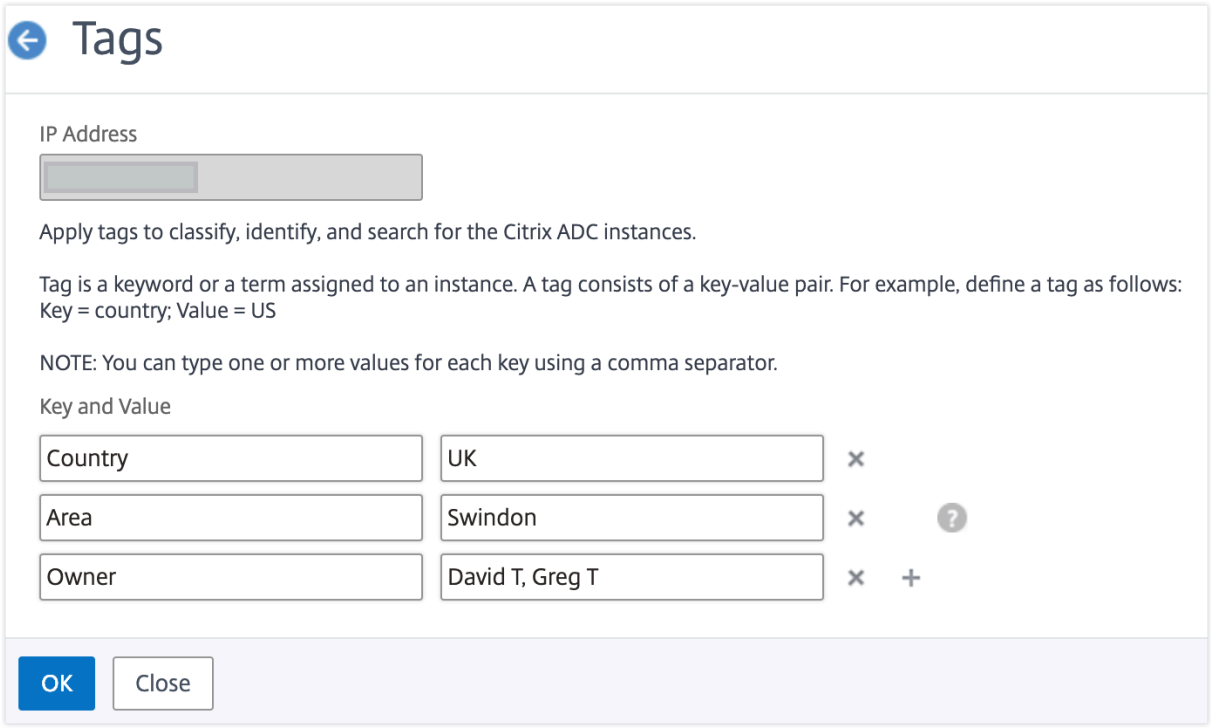


「+」をクリックして複数のタグを追加することもできます。複数の意味のあるタグを追加すると、インスタンスを効率的に検索できます。



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で検索できます。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。



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 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 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。

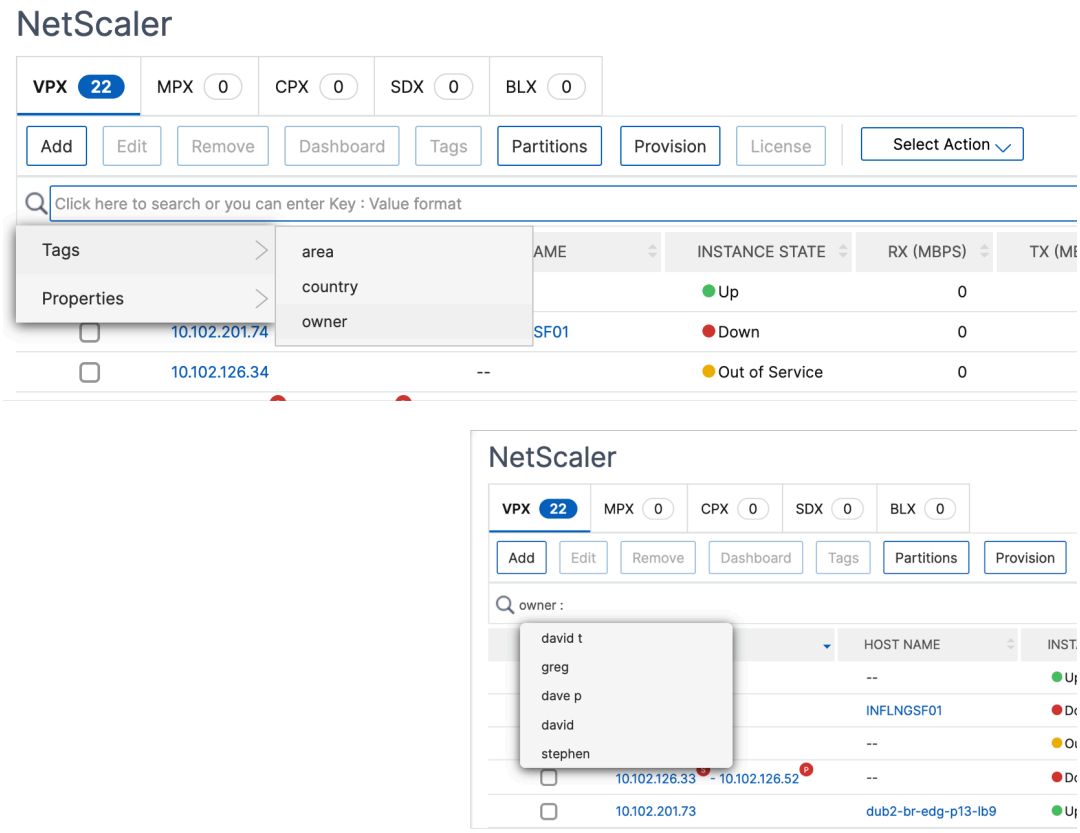
タグとプロパティの組み合わせを使用して、独自の検索条件を作成できます。

NetScaler VPX インスタンスを検索するには

1. NetScaler ADM で、インフラストラクチャ **>** 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。

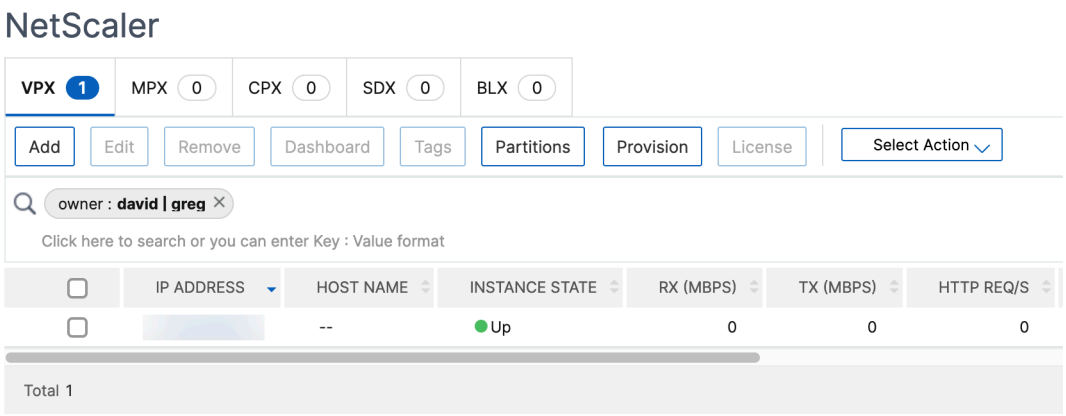
   次の例は、検索式を効率的に使用してインスタンスを検索する方法を示しています。

   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。

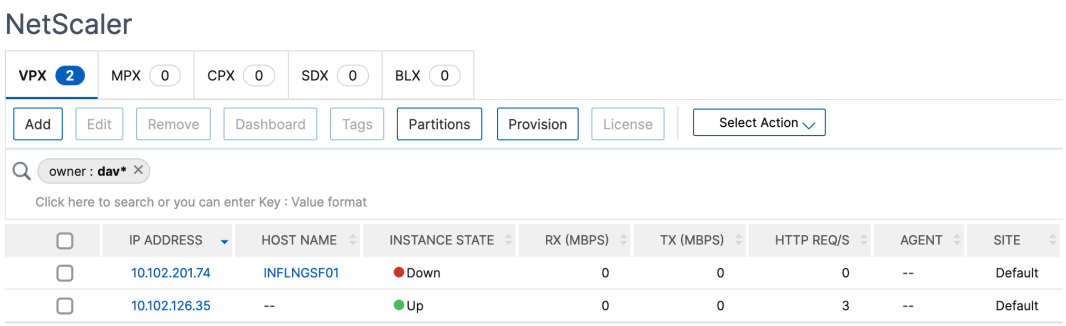


NetScaler ADM では、検索式で正規表現とワイルドカード文字がサポートされています。

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。



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。



> 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詳しくは、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

組織内のさまざまなグループに同じ NetScaler インスタンス上の異なるパーティションが割り当てられるように、Citrix Application Delivery Controller（ADC）インスタンスの管理パーティションを構成できます。ネットワーク管理者を割り当てて、複数の NetScaler インスタンス上の複数のパーティションを管理できます。

NetScaler Application Delivery Management（ADM）は、管理者が所有するすべてのパーティションを単一のコンソールからシームレスに管理する方法を提供します。これらのパーティションは、他のパーティション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 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 NetScaler VPX インスタンスがあり、1 つのインスタンスには 3 つ、もう 1 つのインスタンスには 2 つのパーティションが構成されているとします。たとえば、NetScaler インスタンス 10.102.216.49 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、[インフラストラクチャ**] > [**インスタンス**] > [NetScaler] > [VPX**] に移動し、[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。

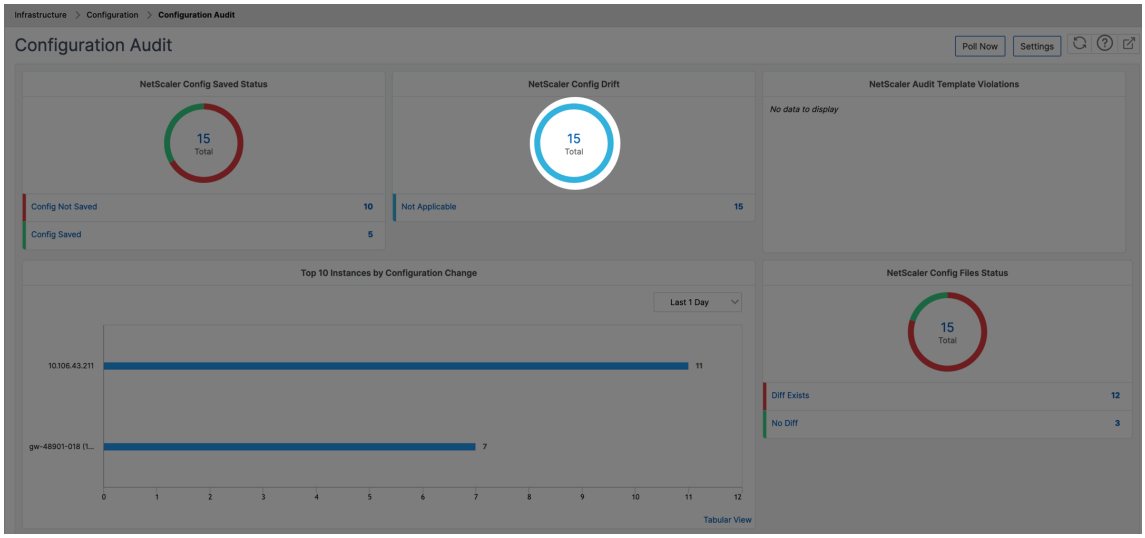
まず、適切な権限 (管理者権限など) を持つ 2 つのグループを作成し、各グループに必要な管理パーティションインスタンスを含める必要があります。たとえば、partition1-admin というシステムグループを作成し、NetScaler 管理パーティションの 10.102.29.120-p1 と 10.102.216.49-Partition_1 をそのグループに追加します。また、partition2-admin というシステムグループを作成し、NetScaler 管理パーティションの 10.102.29.120-p2、10.102.216.49-Partition_2、10.102.216.49-Partition_3 をそ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。

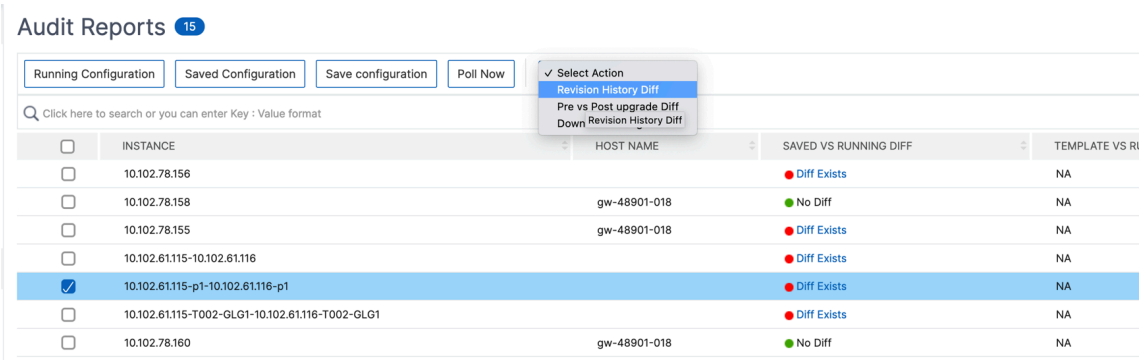
管理パーティションのリビジョン履歴の違いにより、パーティション化された NetScaler インスタンスの最新の 5 つの構成ファイルの違いを確認できます。構成ファイルを相互に比較したり（たとえば、構成リビジョン-1 と構成リビジョン -2)、構成リビジョンを使用して現在実行/保存されている構成と比較したりできます。構成の違いとともに、修正構成も示されています。すべての修正コマンドをローカルフォルダにエクスポートし、設定を修正できます。

改訂履歴の差異を表示する手順は、次のとおりです。

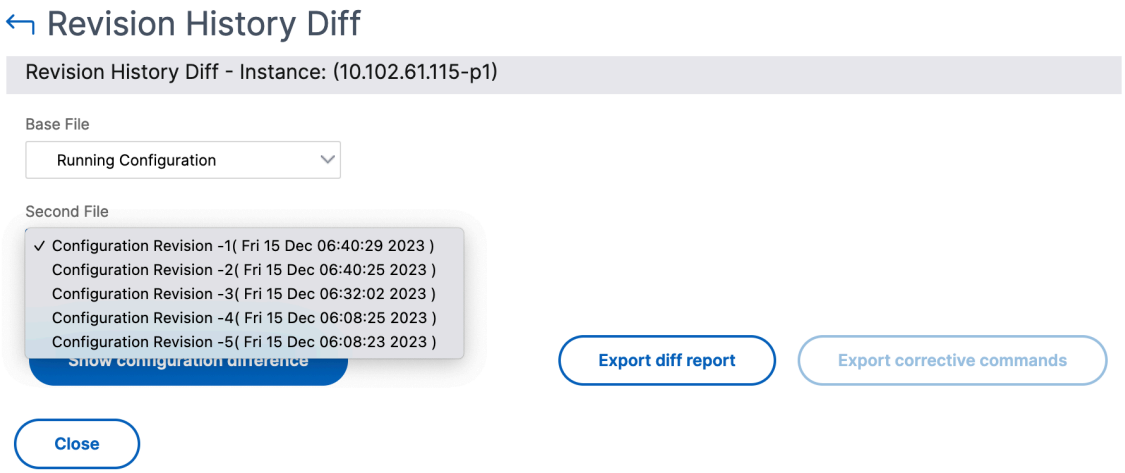
1. [インフラストラクチャ**] > [**構成監査**]** に移動します。インスタンスの構成ステータスを表すドーナツグラフ内をクリックします。表示される［監査レポート］ページで、パーティション分割された NetScaler ADC インスタンスをクリックします。



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。



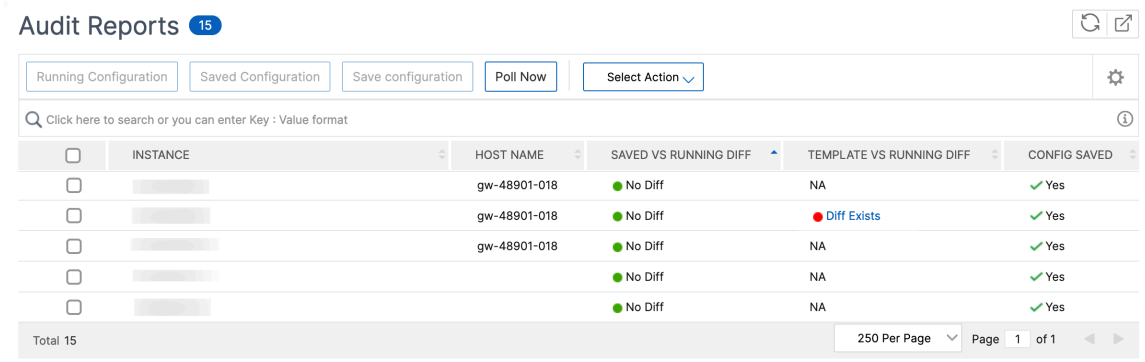
4. 次に示すように、選択したパーティション分割された NetScaler ADC インスタンスの最新の 5 つの構成ファ

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。

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。



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。

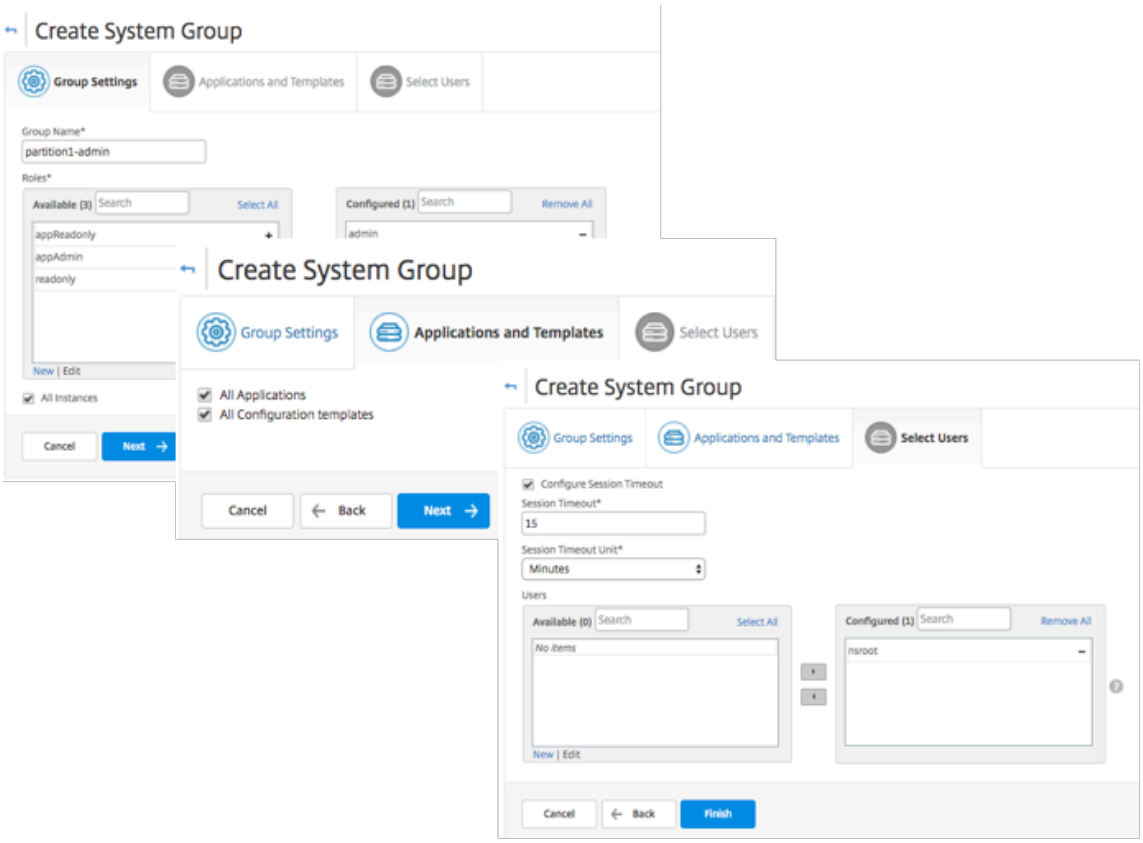
グループを作成するには、次の手順に従います。

1. [設定] **> [**ユーザー管理] **> [**グループ] に移動し、[追加] をクリックします。
2. **[** システムユーザーの作成] ページで、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. [設定] **>** [ユーザー管理] **>** [ユーザー] に移動し、[追加] をクリックします。
2. **[** システムユーザーの作成] ページで、ユーザー名とパスワードを指定します。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

February 6, 2024

NetScaler の高可用性（HA）ペアは、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運用を行うことができます。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 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. [インフラストラクチャ**] > [**インスタンス**] > [NetScaler**] 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。

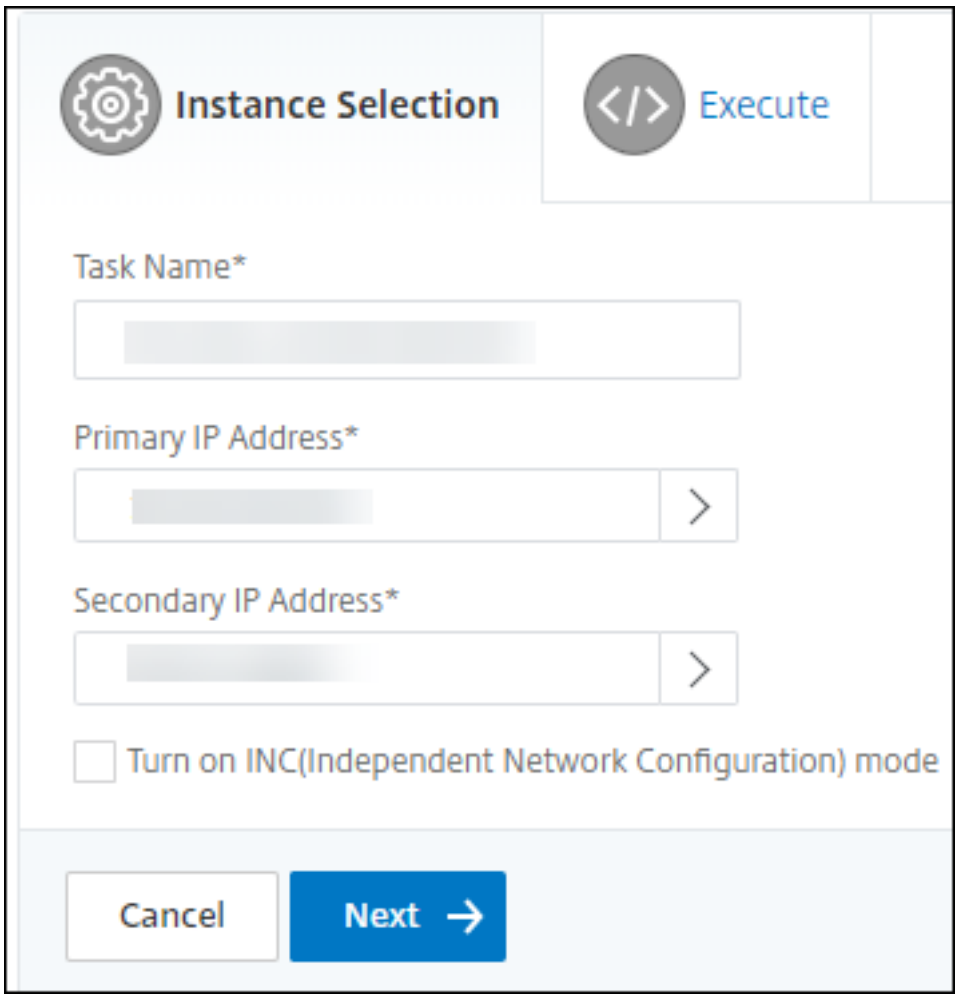
   選択したインスタンスが HA ペアのプライマリインスタンスになります。
3. アクションの選択 **> HA** ペアの作成をクリックします。
4.「インスタンスの選択」で、次の手順を実行します。

   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。



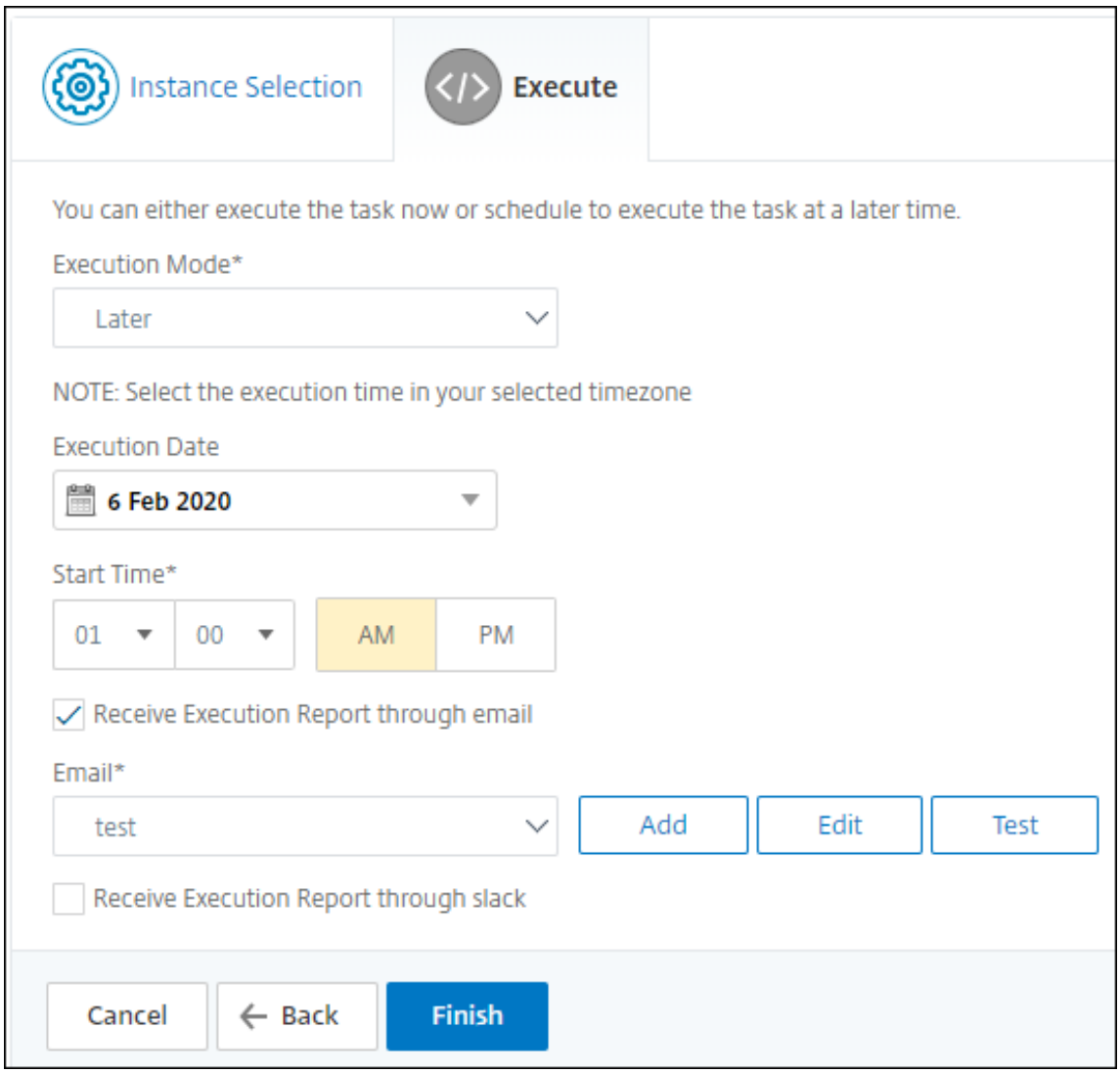
5. **Execute** では、HA ペアを今すぐ作成するか、後で作成するかを決定できます。

   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]**: 特定の日時に HA ペアを作成するには、このオプションを選択します。

   b)「実行モード」リストで「後で」を選択した場合は、このタスクを実行するときに「実行日」と「開始時刻」を選択します。

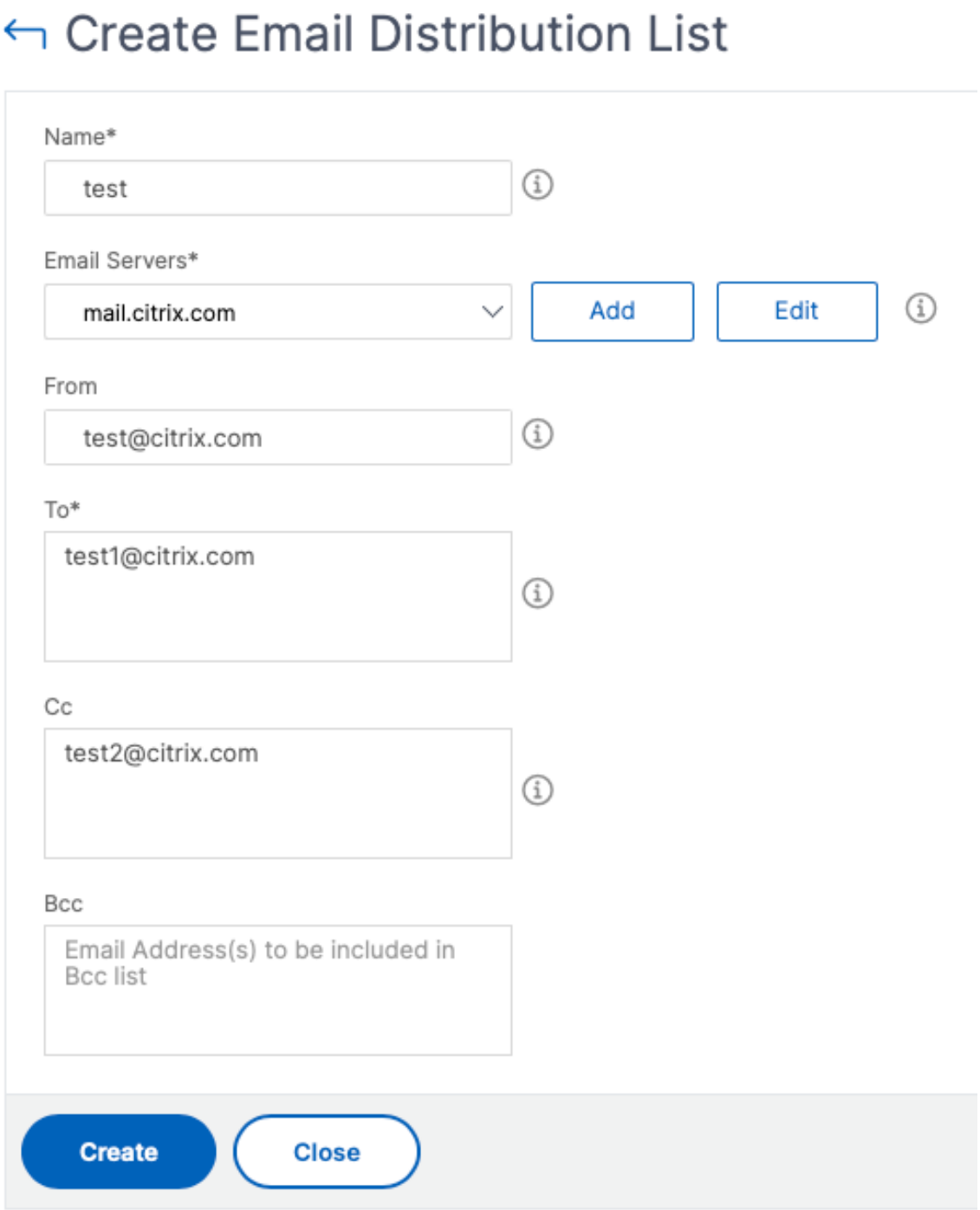
   > 注:
   >
   > 実行時間は、NetScaler ADM で設定されたタイムゾーンで表示されます。



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。

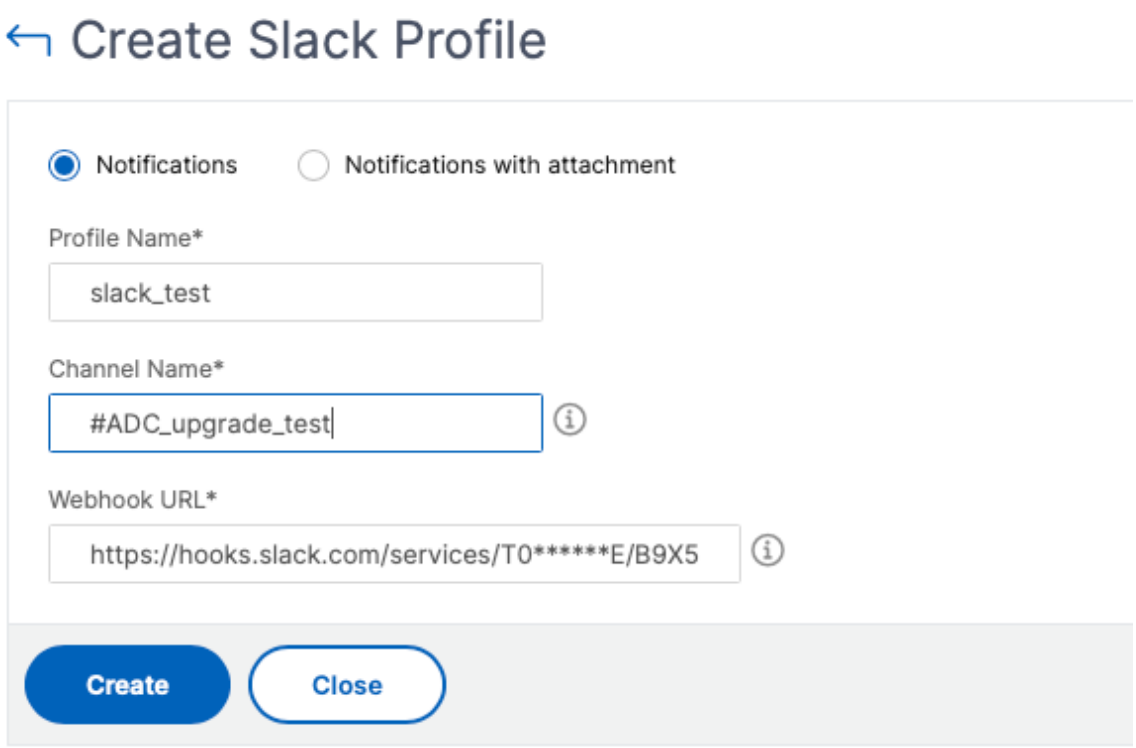
- 電子メール -リストから電子メールの配布を選択します。

  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。



- **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。プロファイル名、チャンネル名 **、** トークンを指定し、「作成」をクリックします。



NetScaler インスタンスのバックアップと復元

February 6, 2024

NetScaler インスタンスの現在の状態をバックアップし、後でバックアップ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 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、NetScaler 構成を手動でバックアップおよび復元できます。NetScaler ADM を使用して、自動バックアップと手動復元を実行することもできます。

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 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 インスタンスタイプを復元します。

- NetScaler SDX
- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

> 注:
>
> - NetScaler ADM プロファイルに、ADC インスタンスをバックアップおよび復元するための管理者アクセス権があることを確認してください。
> - NetScaler ADM では、NetScaler クラスター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。

```
/var/mps/tenants/root/device_backup/
<!--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 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、単一の NetScaler インスタンスまたは複数のインスタンスを選択し、これらのインスタンスで構成ファイルのバックアップを作成できます。必要に応じて、これらのバックアップファイルを使用して NetScaler インスタンスを復元することもできます。

インスタンスのバックアップ設定の構成

[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 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. NetScaler ADM で、[設定] > **[**管理] に移動します。
2. 「バックアップ」で、「システムとインスタンスのバックアップを設定」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 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ーでファイルを開くことはできません。暗号化されたバックアップファイルを復元する場合は、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。

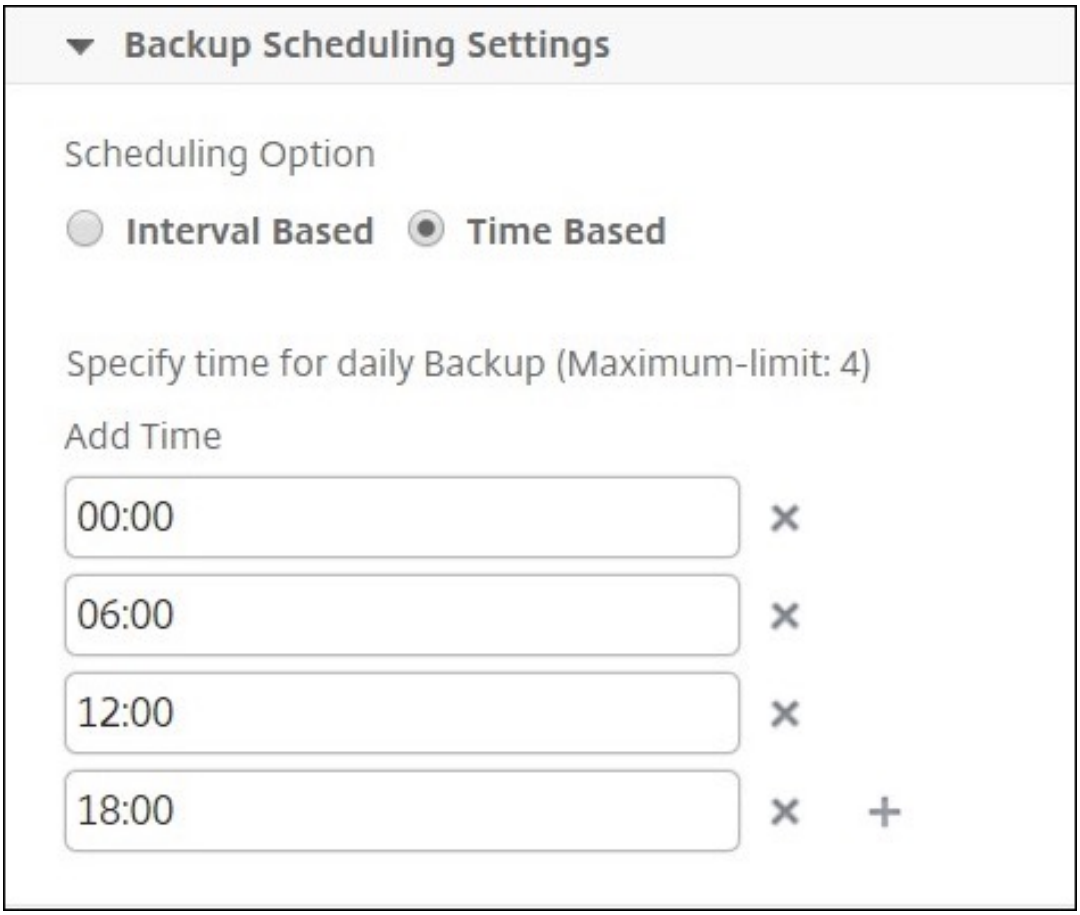
- 保持するバックアップファイルの数：NetScaler ADM で保持するバックアップファイルの数を指定します。ADC インスタンスごとに最大 50 個のバックアップファイルを保持できます。デフォルトでは、バックアップファイルは 3 つです。

  > 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、最適な数の NetScaler ADM バックアップファイルを NetScaler ADM に保存することをお勧めします。

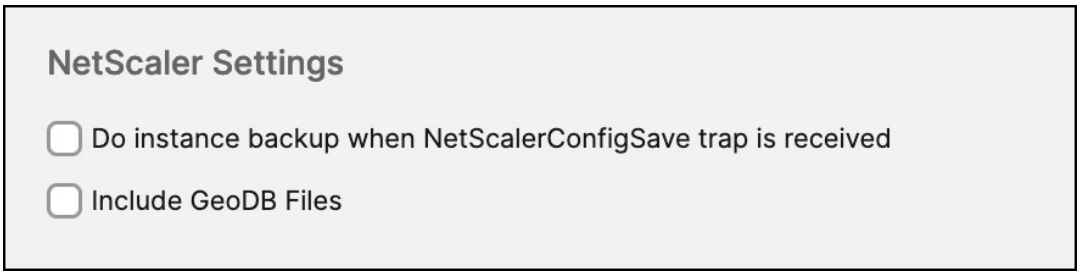
- バックアップのスケジュール設定: (オプション) バックアップファイルの作成には 2 つのオプションがありますが、一度に使用できるオプションは 1 つだけです。

  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、NetScaler ADM にバックアップファイルが作成されます。デフォルトのバックアップ間隔は 12 時間です。

  b) スケジュール・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。



- **NetScaler** 設定：（オプション）デフォルトでは、NetScaler ADM は「NetScalerConfigSave」トラップを受信したときにバックアップファイルを作成しません。ただし、NetScaler インスタンスが「NetScalerConfigSave」トラップを NetScaler ADM に送信するたびにバックアップファイルを作成するオプションを有効にすることはできます。NetScaler インスタンスは、インスタンスの構成が保存されるときには常に「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、NetScaler 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。



- 外部転送：（オプション）NetScaler ADM では、NetScaler インスタンスのバックアップファイルを外部の場所に転送できます。

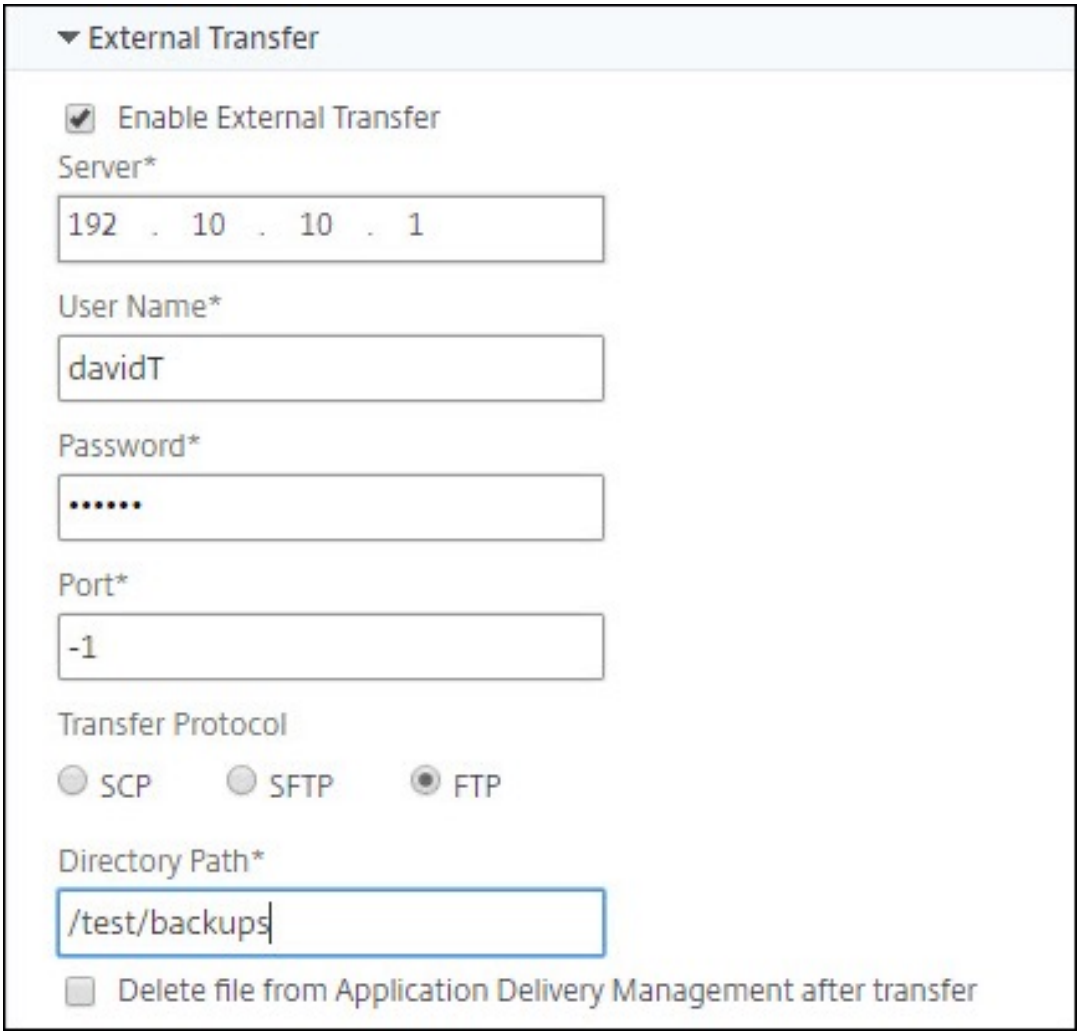
  a) ロケーションの IP アドレスを指定します。

  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に NetScaler ADM から削除することもできます。



> 注:
>
> NetScaler ADM は、選択した NetScaler 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 通知を自身に送信します。

Citrix ADNetScaler ADM を使用して、選択した **NetScaler** インスタンスのバックアップを作成する

選択した NetScaler インスタンスまたは複数のインスタンスをバックアップする場合は、次のタスクを実行します。

1. NetScaler ADM で、[インフラストラクチャ] > [インスタンス] に 移動します。[インスタンス] で、画面に表示するインスタンスのタイプ (NetScaler 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。

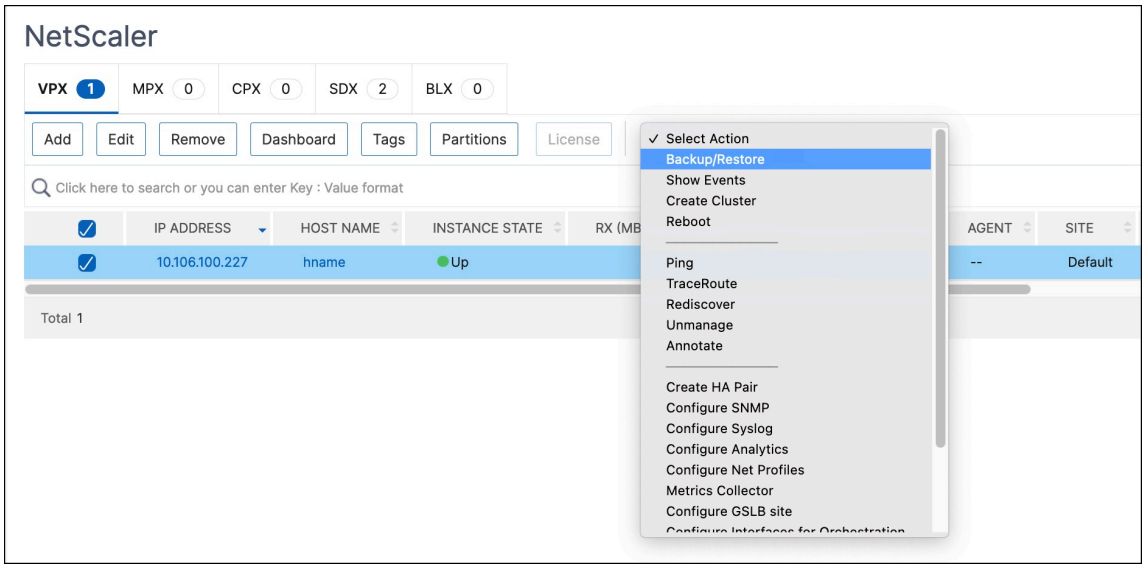
3. [ファイルのバックアップ] ページで、[バックアップ] をクリックします。
4. セキュリティを強化するために、バックアップファイルを暗号化するかどうかを指定できます。パスワードを入力するか、[インスタンスバックアップ設定] ページで以前に指定したグローバルパスワードを使用できます。
5. [続行] をクリックします。

NetScaler ADM を使用して NetScaler インスタンスを復元する

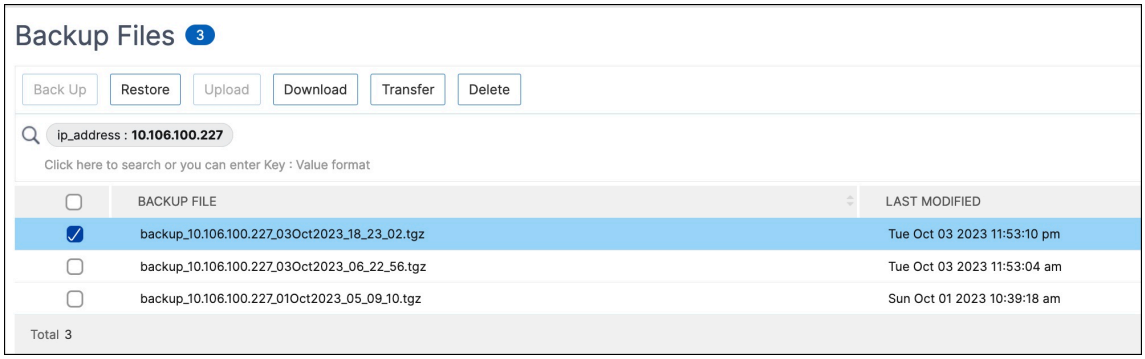
> 注:
>
> 高可用性ペアに NetScaler インスタンスがある場合は、次の点に注意する必要があります。
>
> - バックアップファイルの作成元と同じインスタンスを復元します。たとえば、HA ペアのプライマリインスタンスからバックアップが作成されたシナリオを考えてみましょう。復元プロセス中は、プライマリインスタンスではなくなった場合でも、必ず同じインスタンスを復元してください。
> - プライマリ ADC インスタンスで復元プロセスを開始すると、プライマリインスタンスにアクセスできなくなり、セカンダリインスタンスが **STAYSECONDARY** に変更されます。プライマリインス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。

次のタスクを実行して、以前に作成したバックアップファイルを使用して NetScaler インスタンスを復元します:

1. [インフラストラクチャ**] > [**インスタンス] に移動し、復元するインスタンスを選択して、[アクションの選択**] > [**バックアップ/復元] をクリック します。



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 SDX** アプライアンスを復元する

NetScaler ADM では、NetScaler SDX アプライアンスのバックアップには次のものが含まれます。

- アプライアンスでホストされている NetScaler インスタンス
- SVM SSL 証明書とキー
- 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 構成ファイル
- NetScaler ビルドイメージ
- NetScaler XVA イメージ。これらのイメージは次の場所に保存されます。
  `/var/mps/sdx_images/`
- SDX 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）

NetScaler SDX アプライアンスをバックアップファイルで使用可能な構成に復元します。アプライアンスの復元中に、現在の構成全体は削除されます。

別の NetScaler SDX アプライアンスのバックアップを使用して NetScaler SDX アプライアンスを復元する場合は、復元プロセスを開始する前に、必ずライセンスを追加し、新しいアプライアンスの Management Service ネットワーク設定をバックアップファイルの設定と一致するように構成してください。つまり、新しいアプライアンスはライセンスを取得し、バックアップファイルの最小ライセンス要件を満たしている必要があります。たとえば、バックアップに合計 5 GB の VPX インスタンスが 5 つある場合、新しいアプライアンスもこれらの要件をサポートできる必要があります。または、バックアップアプライアンスにプラチナライセンスがある場合、新しいアプライアンスには同じかそれ以上のライセンスが必要です。IP アドレス、ネットマスク、ゲートウェイ、XenServer IP アドレス、DNS サーバーなどのネットワーク設定は、新しいアプライアンスで正しく構成する必要があります。

SDX アプライアンスを復元する前に、バックアップした SDX アプライアンスプラットフォームバリアントがアプライアンスと同じであることを確認してください。異なるプラットフォームのバリアント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、バックアップされたバージョンが RMA バージョンと同じかそれ以上であることを確認してください。

バックアップしたファイルから SDX アプライアンスを復元するには:

1. NetScaler ADM GUI で、[インフラストラクチャ**] > [**インスタンス**] > [NetScaler] > [SDX**] に移動します。インスタンスを選択します。
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ールオーバーを強制できます。プライマリインスタンスでフェールオーバーを強制した場合、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。強制フェー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ときのみです。

強制フェールオーバーは継承されたり、同期されたりしません。強制フェー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、強制フェー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ールオーバーを強制する。
- セカンダリインスタンスが無効または非アクティブである。セカンダリインスタンスが非アクティブの場合、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。

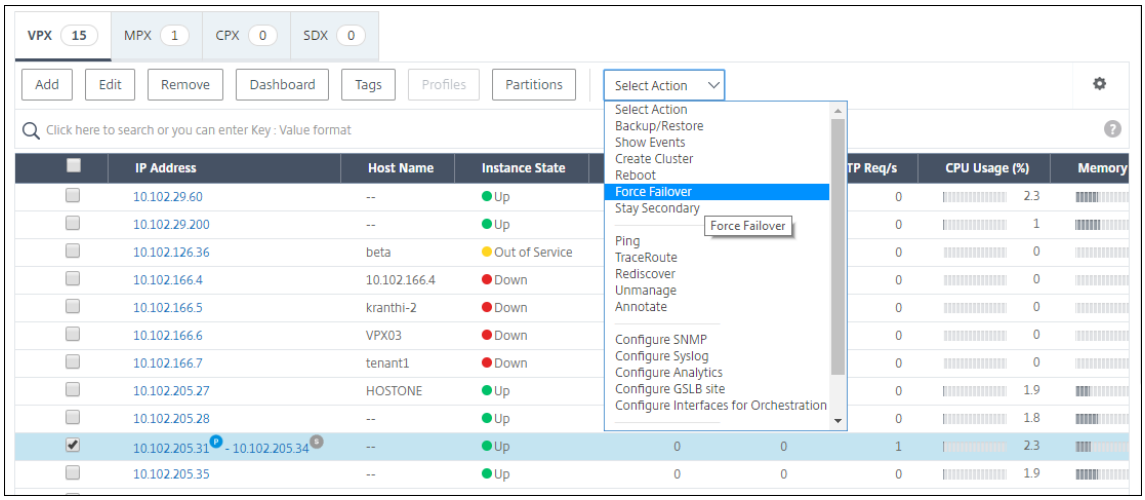
- セカンダリを維持するようにセカンダリインスタンスが構成されている。

NetScaler 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イルオーバーを強制するには:

1. NetScaler Application Delivery Management（ADM）で、［インフラストラクチャ］**>**［インスタンス］**>**［**NetScaler**］**>**［**VPX** ］タブに移動し、インスタンスを選択します。
2. 選択したインスタンス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、「強制フェイルオーバー」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。

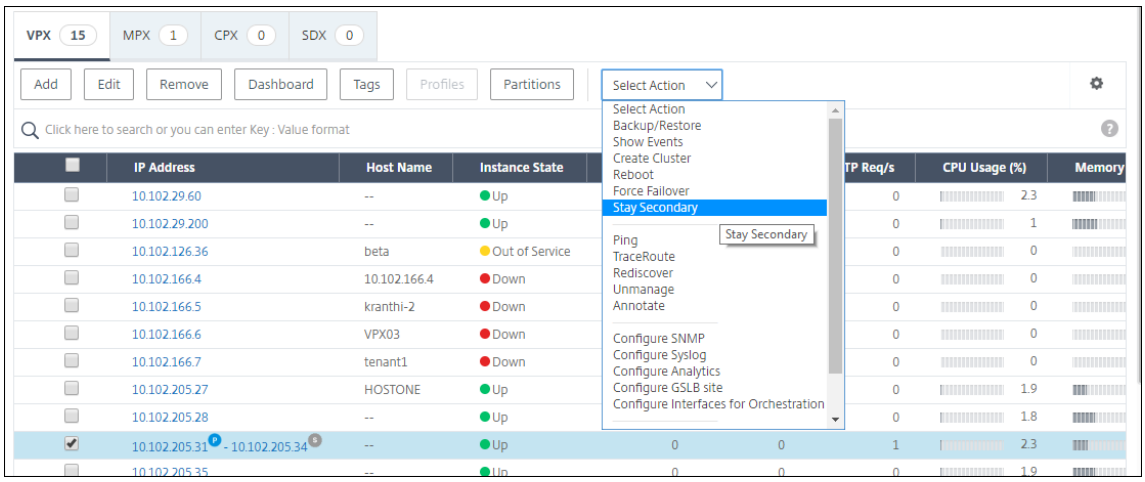
たとえば、プライマリノードをアップグレードする必要があり、アップグレード処理に数秒かかるとします。アップグレード中、プライマリノードが数秒間停止することがありますが、セカンダリノードを引き継ぎたくないようにします。プライマリノードで障害が検出された場合でも、セカンダリノードのままにします。

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. NetScaler Application Delivery Management（ADM）で、［インフラストラクチャ］**>**［インスタンス］>［**NetScaler** ］>［**VPX** ］タブに移動し、インスタンスを選択します。
2. 選択したインスタンス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

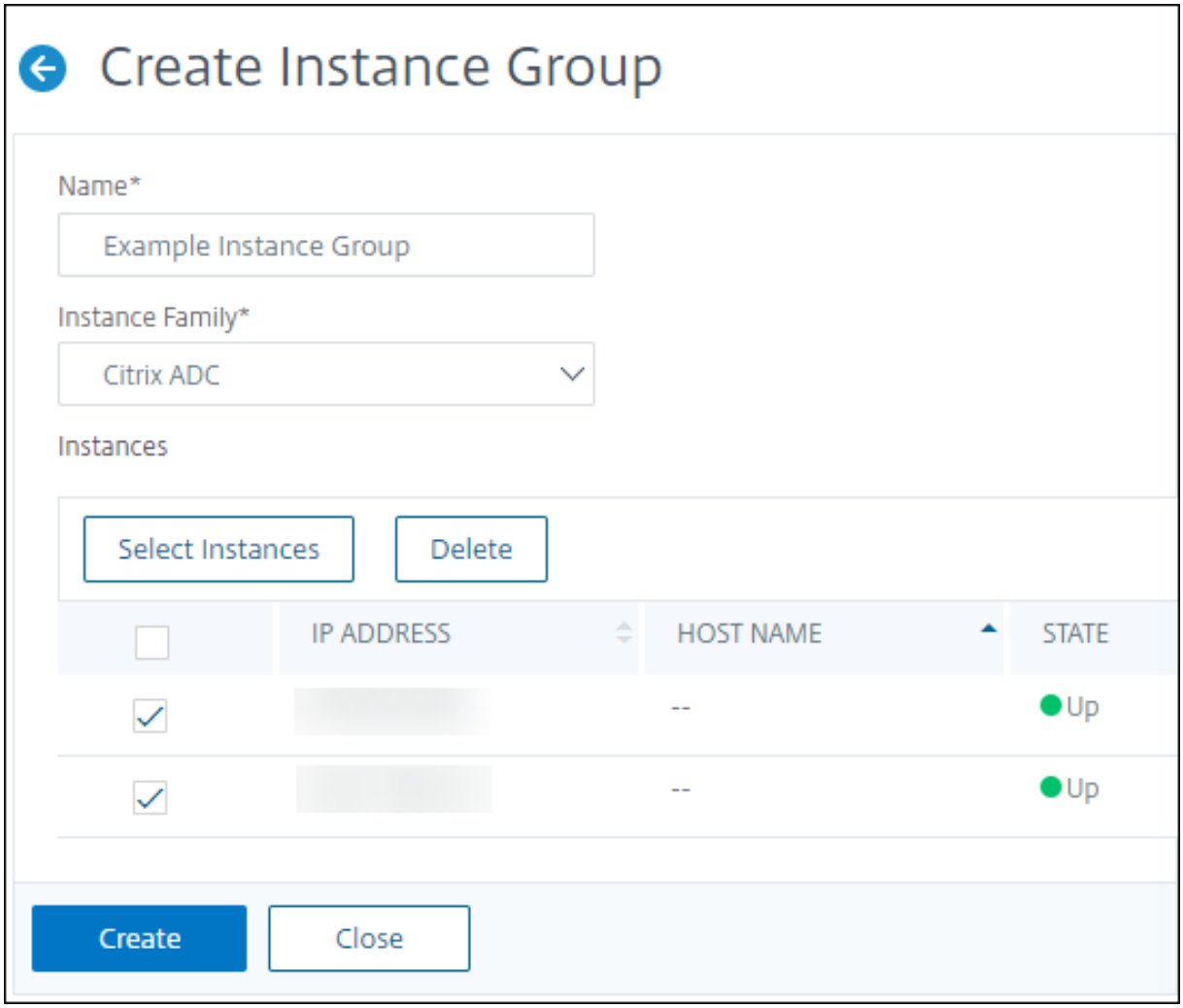
February 6, 2024

インスタンスグループを作成するには、まずすべての NetScaler 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、[インフラストラクチャ**] > [**インスタンスグループ] に移動し、[追加] をクリックします。
2. インスタンスグループの名前を指定し、［インスタンスファミリー］リストから ［**NetScaler**］を選択します。
3. [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。



ADM を使用して SDX 上で NetScaler VPX インスタンスをプロビジョニングします

February 6, 2024

NetScaler ADM を使用して、SDX アプライアンスに 1 つ以上の NetScaler VPX インスタンスをプロビジョニングできます。デプロイできるインスタンスの数は、購入したライセンスによって異なります。追加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 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. [インフラストラクチャ**] > [**インスタンス**] > [NetScaler**] に移動します。
2.「**SDX** 」タブで、VPX インスタンスをプロビジョニングする SDX インスタンスを選択します。
3.「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。

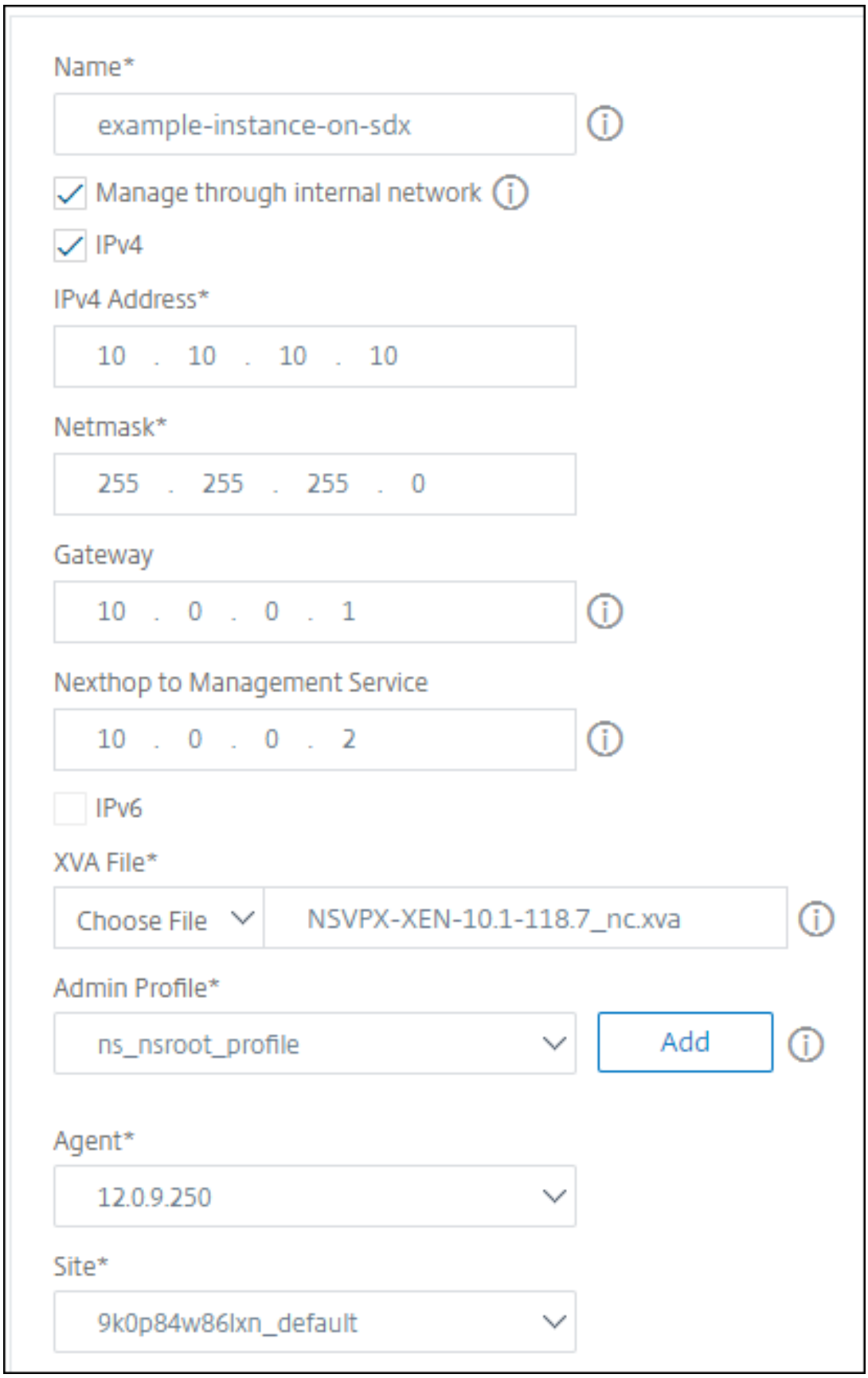
ステップ **1-VPX** インスタンスを追加する

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 - ****IPv4** アドレスまたは **IPv6** アドレス ** 、あるいはその両方を選択して、NetScaler VPX インスタンスを管理できます。VPX インスタンスは、1 つの管理 IP（NetScaler IP とも呼ばれます）のみを持つことができます。NetScaler IP アドレスを削除することはできません。

    選択したオプションで、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。



ステップ **2-**ライセンスの割り当て

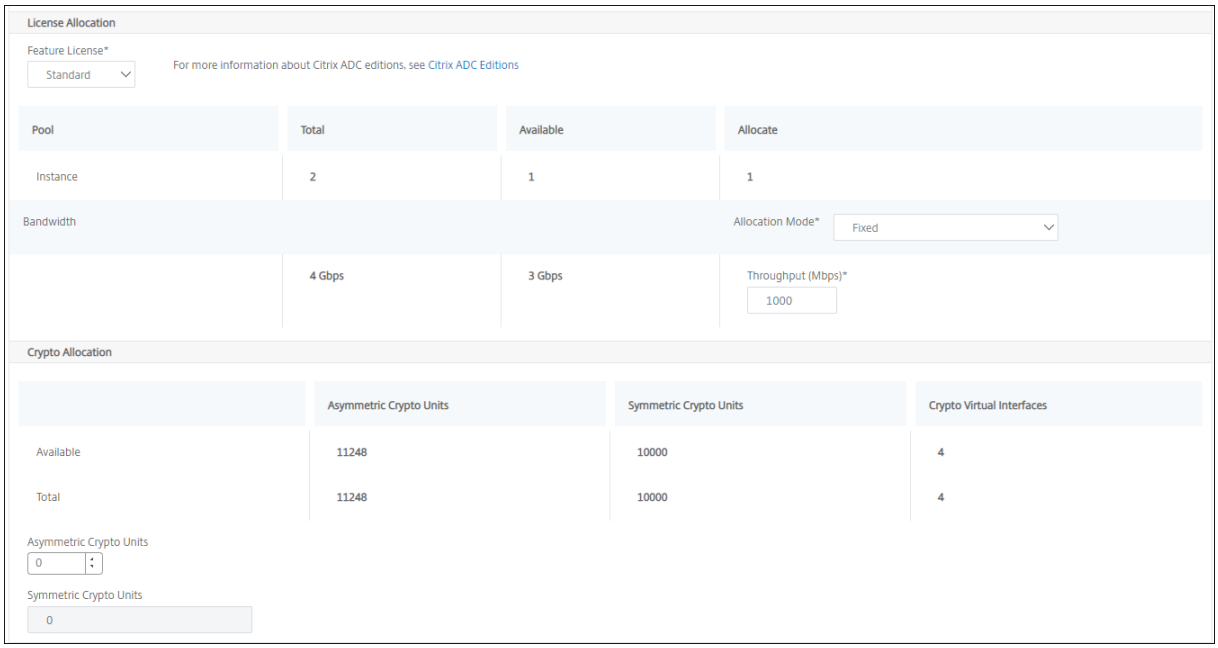
［ライセンスの割り当て］セクションで、VPX ライセンスを指定します。スタンダード、アドバンスト、プレミアムライセンスを使用できます。

- 割り当てモード：帯域幅プールに対して [固定] または [バースト可能] モードを選択できます。

  バースト可能モードを選択した場合、固定帯域幅に達したときに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。



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。

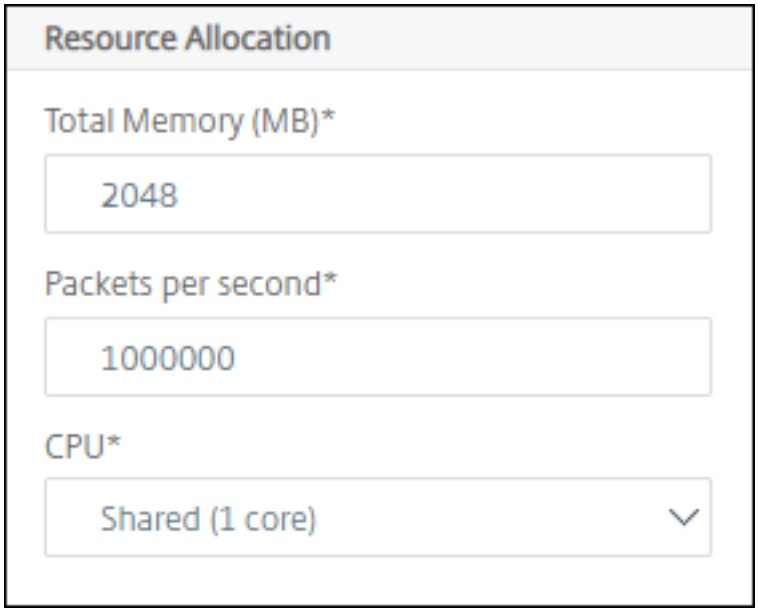
- [パケット/秒]-1 秒あたりに送信するパケット数を指定します。
- **CPU** -インスタンスに対する CPU コアの数を指定します。共有 CPU コアまたは専用の CPU コアを使用できます。

  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 25000xx 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。



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 11515、SDX 11520、SDX 11530、SDX 11540、SDX 11540、SDX 11542	12	10	5
SDX 17500、SDX 19500、SDX 21500	12	10	5
SDX 17550、SDX 19550、SDX 20550、SDX 21550	12	10	5
SDX 14020、SDX 14030、SDX 14040、SDX 14060、SDX 14080、SDX 14100	12	10	5
SDX 22040、SDX 22060、SDX 22080、SDX 22100、SDX 22120	16	14	7
SDX 24100 と SDX 24150	16	14	7
SDX 14020 40G、SDX 14030 40G、SDX 14040 40G、SDX 14060 40G、SDX 14060 40G、SDX 14080 40G、SDX 14100 40G	12	10	10
SDX 14020 FIPS、SDX 14030 FIPS、SDX 14040 FIPS、SDX 14060 FIPS、SDX 14080 FIPS、SDX 14100。FIPS	12	10	5
SDX 14040 40S、SDX 14060 40S、SDX 14080 40S、SDX 14100 40S	12	10	5
SDX 25100A、25160A、25200A	20	18	9
SDX 25100-40G、25160-40G、25200-40G	20	18	16 (バージョンが 11.1-51.x 以上の場合); 9 (バージョンが 11.1-50.x 以下の場合、11.0 および 10.5 のすべてのバージョン)

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
SDX 16000	64	30	16
SDX 9100	20	9	9

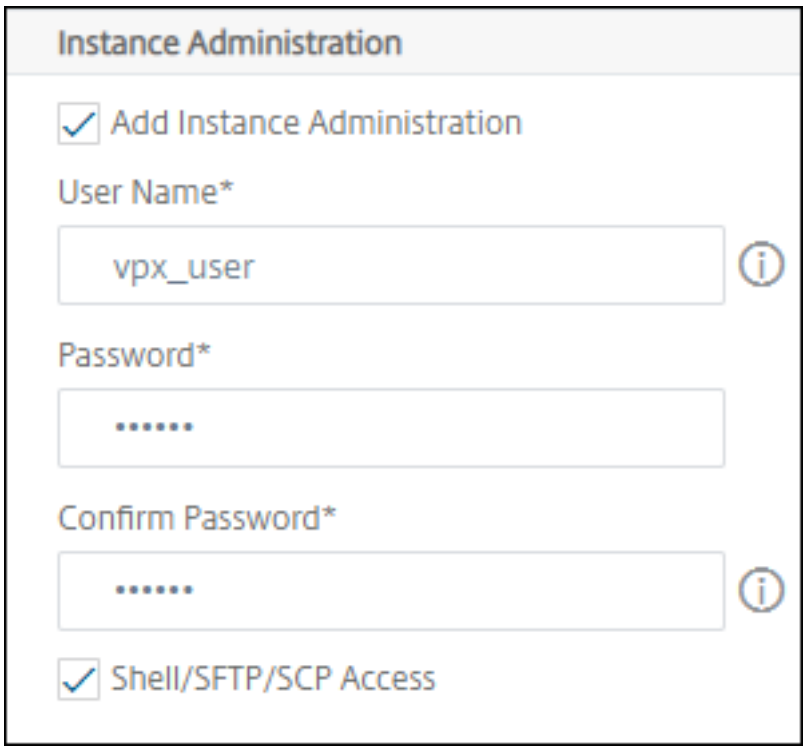
> 注:
>
> SDX 26xxx プラットフォームでは、VPX インスタンスに最大 26 個の CPU コアを割り当てることができます。暗号化ユニットがインスタンスに割り当てられている場合、コアの最大数は、暗号ユニットとデータインターフェイスの数によって異なります。
>
> たとえば、24000 暗号ユニットをインスタンスに割り当てると、24 の CPU コアと最大 2 つのデータインターフェイスをインスタンスに割り当てることができます。SDX アプライアンスは、データインターフェイスと暗号ユニットを PCI デバイスと見なします。26000 暗号ユニットでは、データインターフェイスを追加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:NetScaler 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**:NetScaler** インスタンス管理者に許可されているアクセス権。このオプションはデフォルトで選択されています。



手順 **5-**ネットワーク設定を指定する

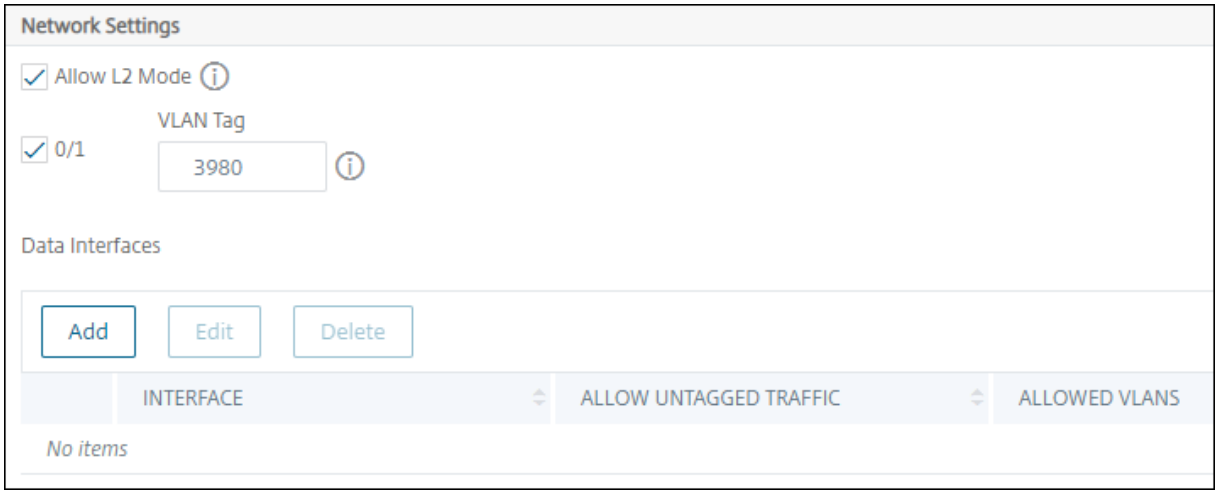
インスタンスに必要なネットワーク設定を選択します。

- ネットワーク設定で **L2** モードを許可する -NetScaler 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 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 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。

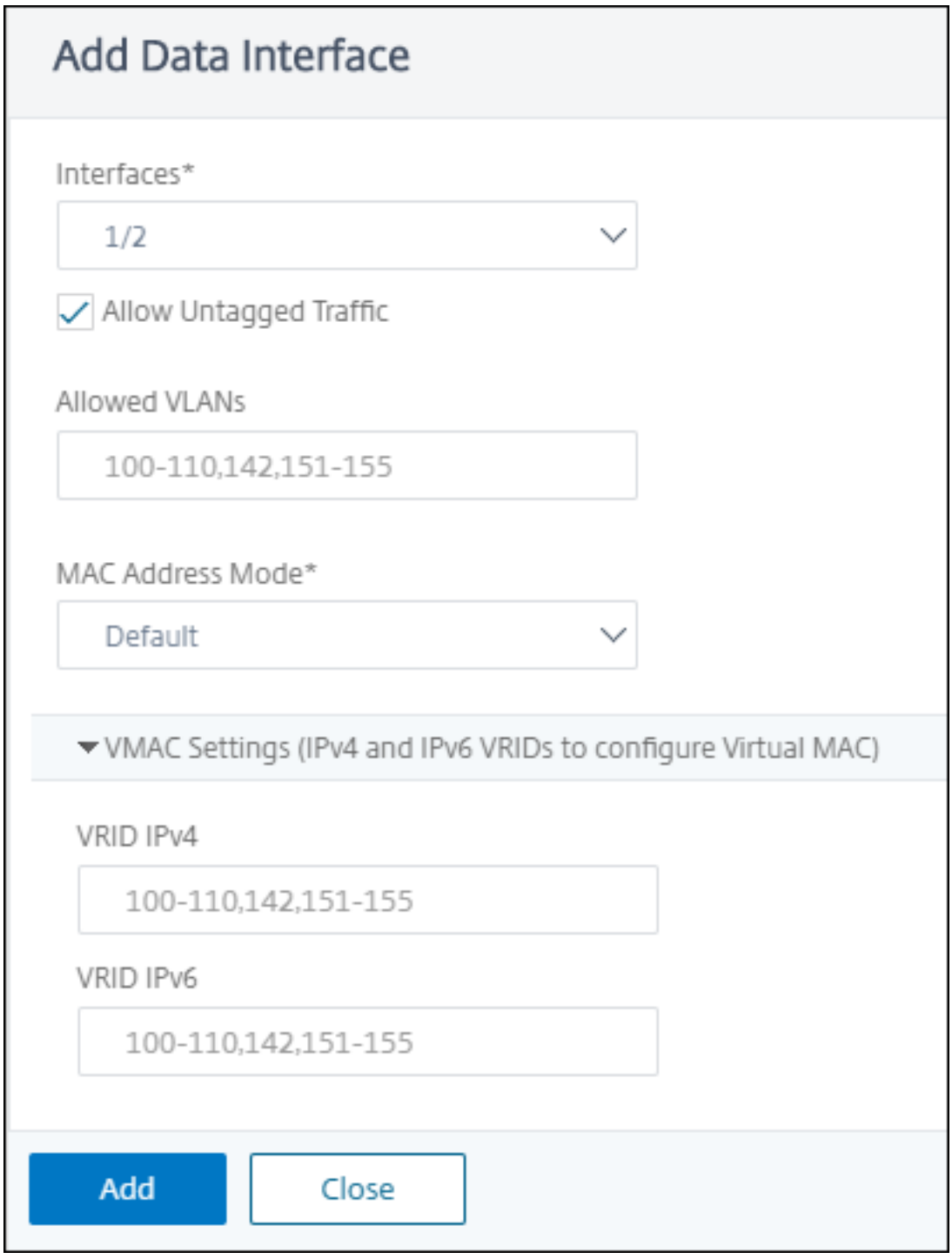


「データ・インタフェース」で、「追加」をクリックしてデータ・インタフェースを追加し、次を指定します。

- [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 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。



［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

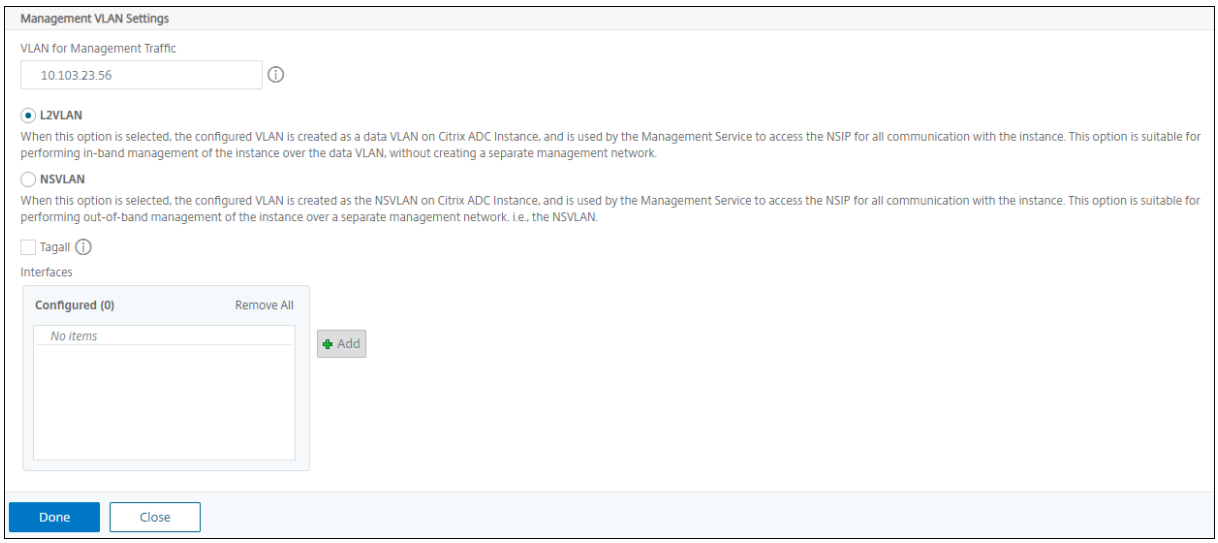
VPX インスタンスの管理サービスと管理アドレス（NSIP）は同じサブネットワークにあり、通信は管理インタフェースを介して実行されます。

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。

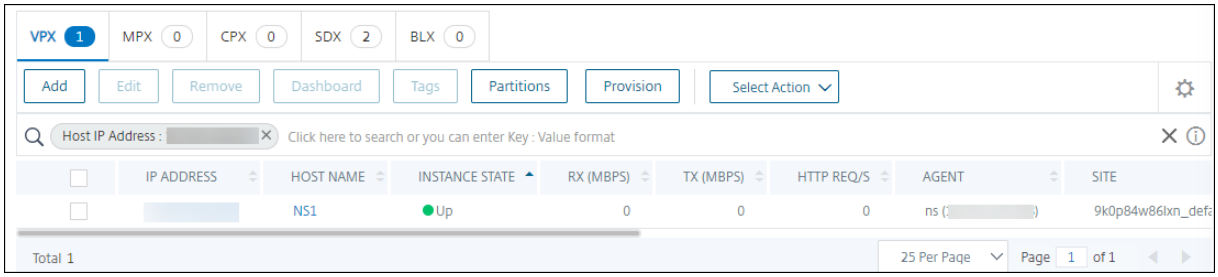


「完了」をクリックして、VPX インスタンスをプロビジョニングします。

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. [インフラストラクチャ**] > [**インスタンス**] > [NetScaler**] に移動します。
2. [**VPX**] タブで、[ホスト **IP** アドレス] プロパティでインスタンスを検索し、そのインスタンスに SDX インスタンスの IP を指定します。



複数の **NetScaler ADC VPX** インスタンスの再検出

February 6, 2024

NetScaler Application Delivery Management（ADM）設定で複数の NetScaler VPX インスタンスを再検出できます。また、複数の NetScaler VPX インスタンスを再検出して、それらのインスタンスの最新の状態と構成を確認することもできます。NetScaler ADM サーバーはすべての NetScaler VPX インスタンスを再検出し、Citrix アプリケーション Delivery Controller（ADC）インスタンスにアクセスできるかどうかを確認します。

複数の **NetScaler ADC VPX** インスタンスを再検出するには:

1. Web ブラウザーで、NetScaler 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. [インフラストラクチャ**] > [**インスタンス**] > [NetScaler**] > [**VPX**] タブに移動し、再検出するインスタンスを選択します。
4. **[** アクションの選択**]** メニューで、[再検出] をクリックします。
5. 再検出ユーティリティを実行するための確認メッセージが表示されたら、[はい] をクリックします。

   各 NetScaler ADC 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

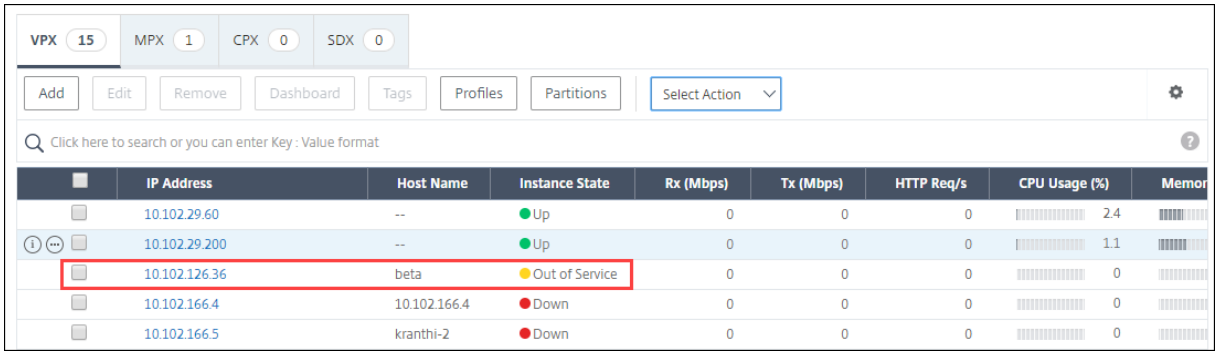
February 6, 2024

NetScaler Application Delivery Management（ADM）とネットワーク内のインスタンス間の情報交換を停止したい場合は、インスタンス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。

インフラストラクチャ **>** インスタンス **> NetScaler** > **VPX** タブに移動します。インスタンスのリストで、インスタンスを右クリックして [**UnManage**] を選択するか、インスタンスを選択し、[Select **Action]** リストから [**UnManage**] を選択します。

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。



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

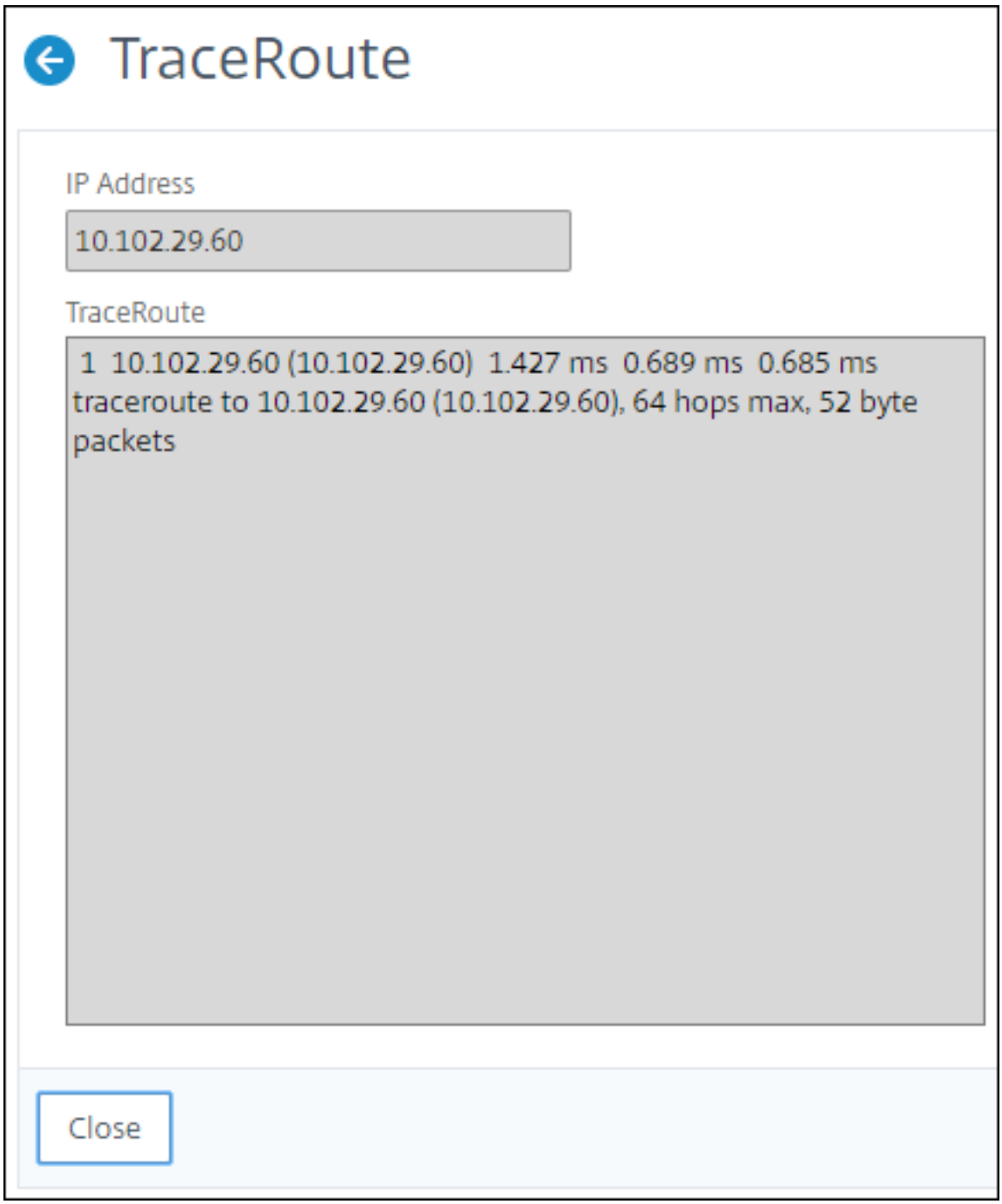
NetScaler Application Delivery Management（ADM）からインスタンスへのパケットのルートを追跡することで、インスタンスに到達するために必要なホップ数などの情報を確認できます。Traceroute では、ソースから宛先までのパケットのパスがトレースされます。これには、ルート内の各エンティティのホスト名と IP アドレスと共に、ネットワークホップの一覧が表示されます。

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. NetScaler ADM で、インフラストラクチャ **>** 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。



ある **NetScaler** インスタンスから別の **NetScaler** インスタンスに構成を複製

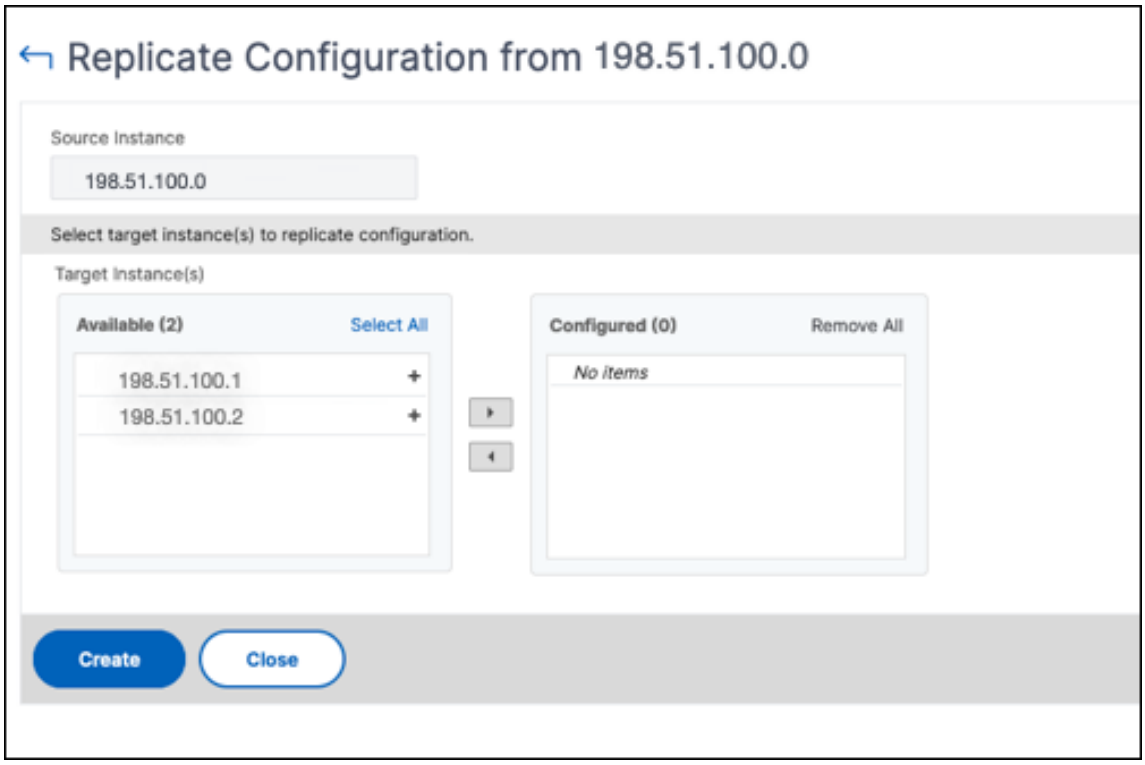
February 6, 2024

NetScaler ADM の構成の複製機能を使用して、NetScaler インスタンスから構成をコピーし、それを単一インスタ

ンスまたは多数のインスタンスに複製できます。

あるインスタンスから他の **NetScaler** インスタンスに構成を複製するには

1. [インフラストラクチャ**] > [**インスタンス**] > [NetScaler**] に移動します。構成を他のインスタンスに複製するソースインスタンスを選択し、「アクションの選択」リストから「構成の複製」をクリックします。
2. 「構成の複製」で、ソース・インスタンスから構成を適用するターゲット・インスタンスを選択します。1 つのソースインスタンスから 1 つのインスタンスまたは複数のターゲットインスタンスに構成を複製できます。



3. ［作成］をクリックします。

複製された構成は、NetScaler インスタンスのリストに追加されます。複製されたインスタンスのステータスを表示するには、更新アイコンをクリックします。

> 注:
>
> レプリケーション中、ソースインスタンスのすべてのネットワーク IP がターゲットインスタンスにレプリケートされます。ターゲットインスタンスがソースインスタンスとは異なるネットワークにある場合、ターゲットインスタンスの IP にアクセスできない可能性があります。IP にアクセスできない場合、ターゲットインスタンス内のエンティティのステータスは Down と表示されます。
>
> 管理対象の NetScaler インスタンスで構成されたエンティティのステータスを表示するには、[インフラストラクチャ**] > [**ネットワーク機能] に移動します。

SSL 証明書の管理

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。

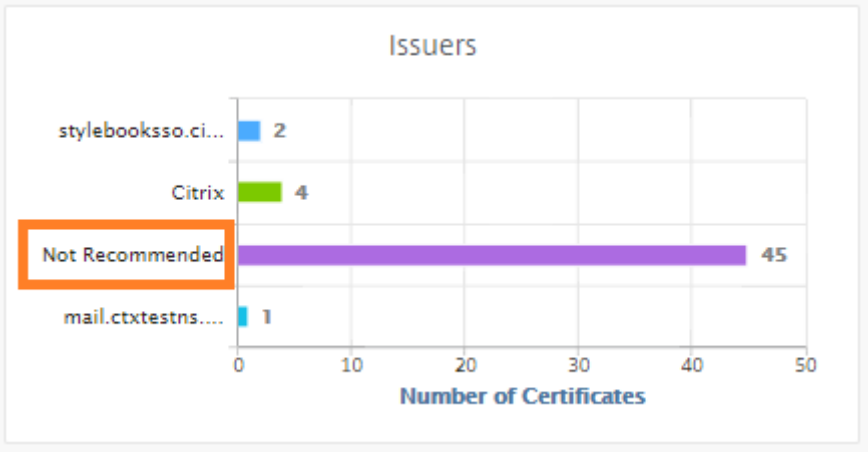
- Verisign などの承認された認証局 (CA) から
- NetScaler アプライアンス上で新しい SSL 証明書とキーを生成する

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。

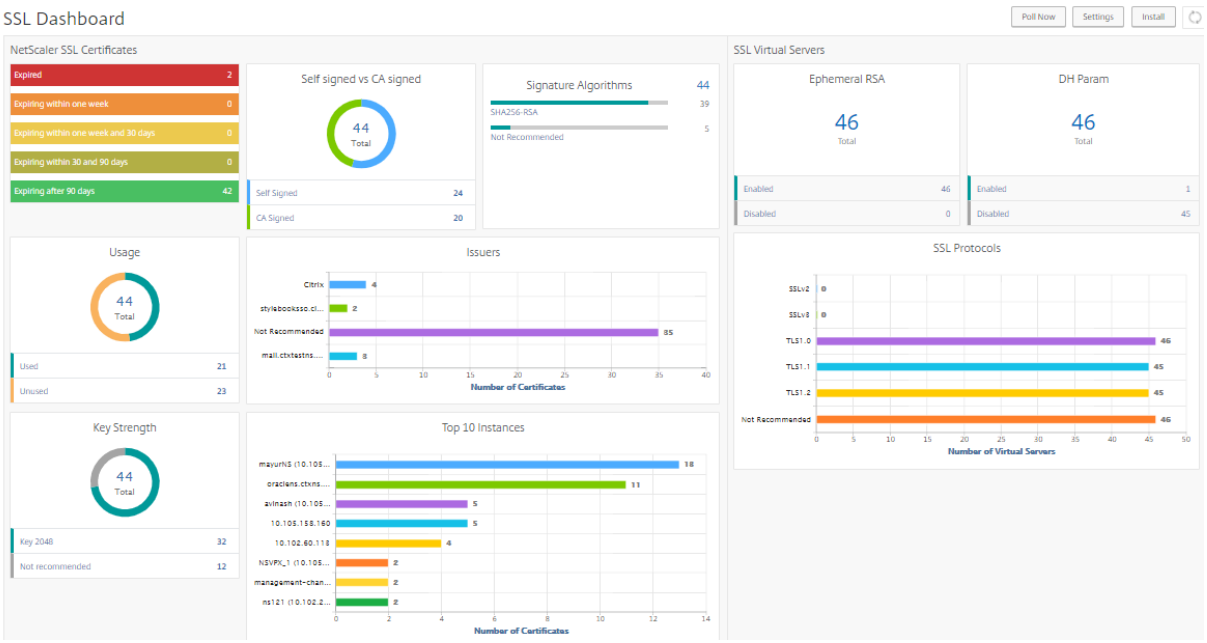


> 注
>
> 「推奨しない」証明書は、さまざまなパラメータに基づいて分類され、関連するコンポーネントで表示できます。

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、[インフラストラクチャ**] > [SSL** ダッシュボード] の順に移動します。

証明書の有効期限の通知設定

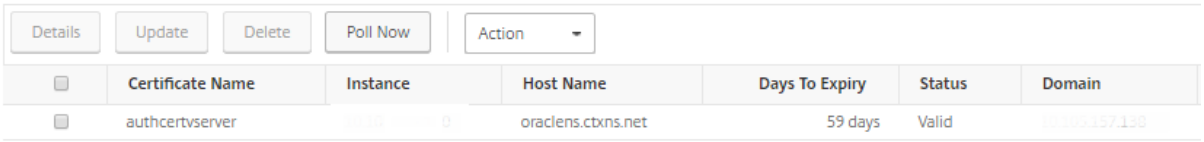
このユースケースでは、複数の NetScaler ADC インスタンスに複数の証明書が存在する可能性があり、各証明書の有効期限を追跡するオーバーヘッドになります。各証明書を手動で追跡し、有効期限が切れる前に更新するのは面倒な作業です。このようなシナリオを回避するには、構成済みの電子メール、ポケットベル、Slack、または

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。



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。

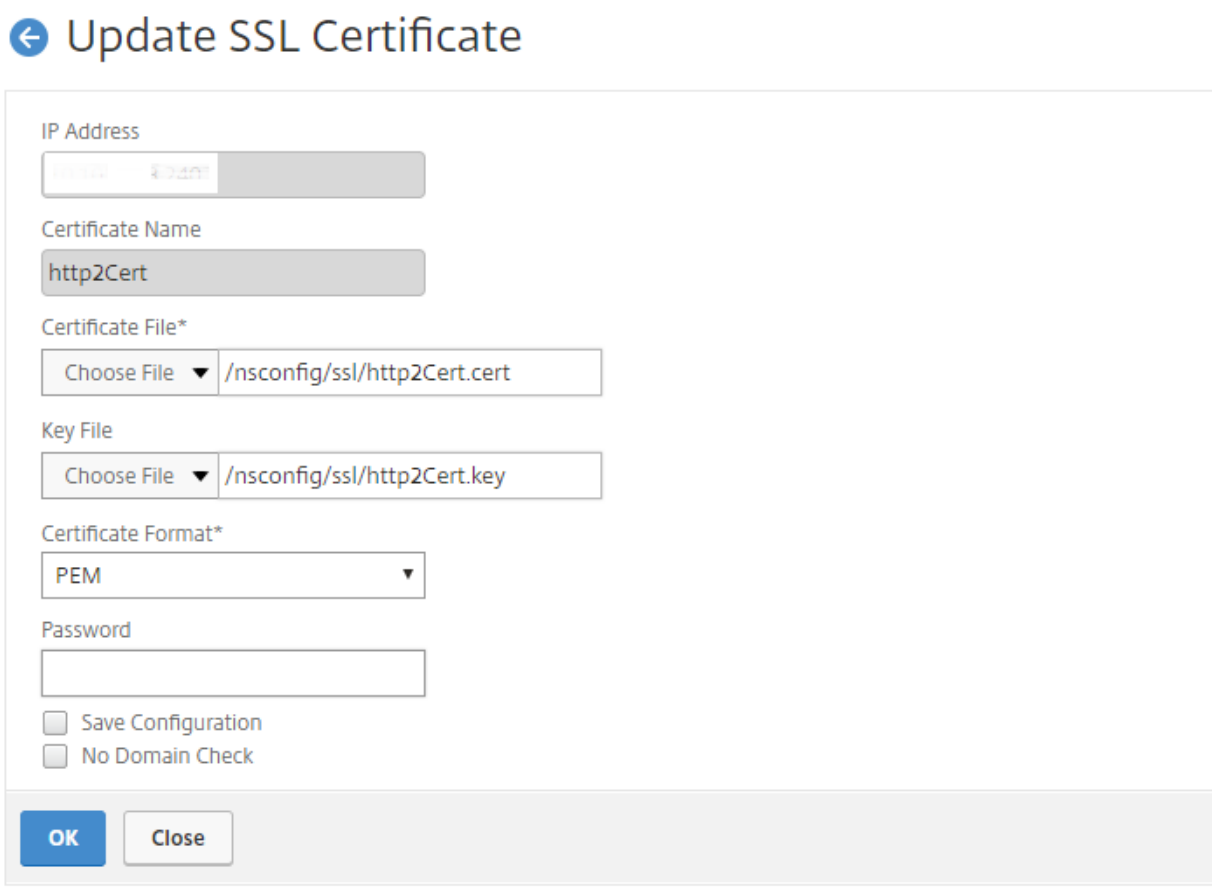
既存の証明書を更新する　このユースケースでは、認証局 (CA) から更新された証明書を受け取ったら、既存の証明書を更新する必要があります。NetScaler ADC インスタンスにログインすることなく、NetScaler ADM から既存の証明書を更新できるようになりました。

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、[インフラストラクチャ**] > [SSL** ダッシュボード] に移動します。

更新する証明書を選択し、[更新] をクリックします。

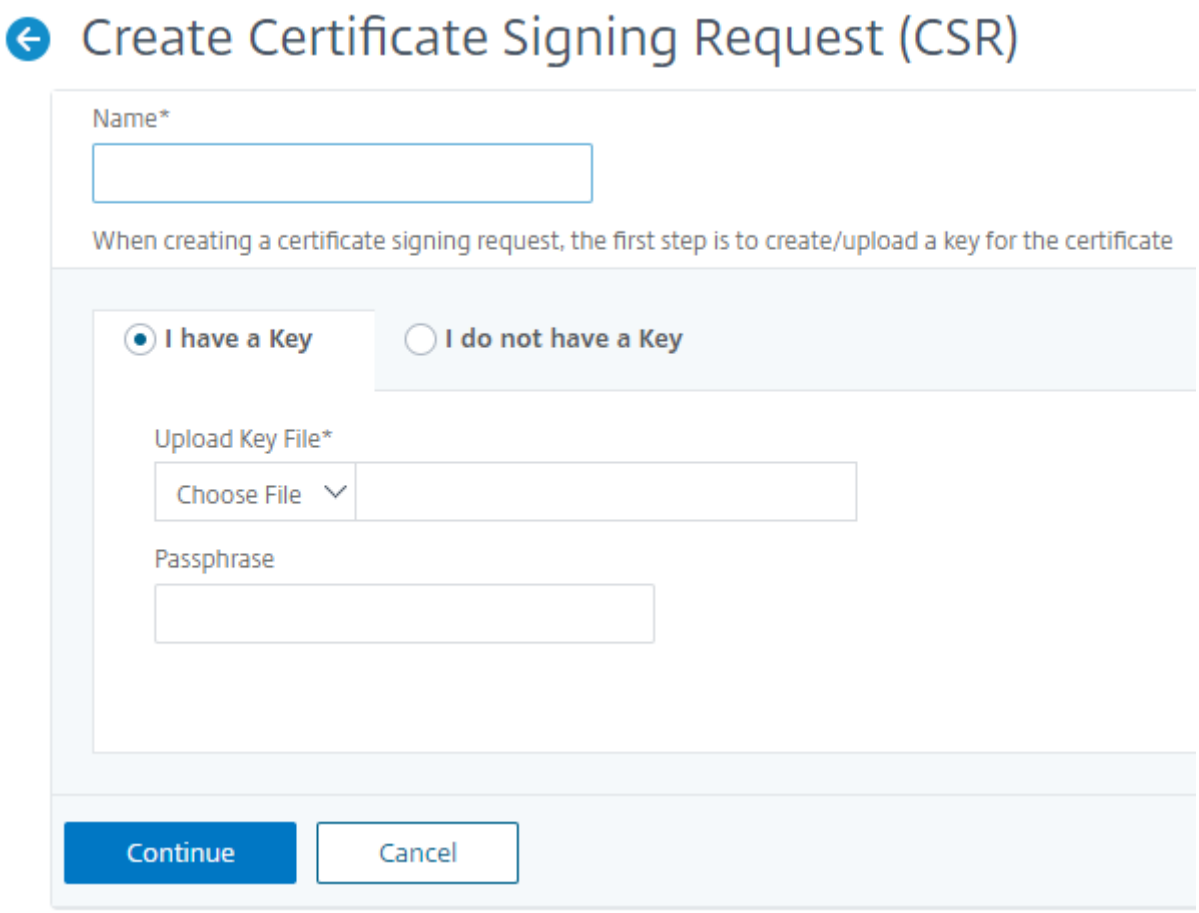
NetScaler ADM から選択した証明書の関連フィールドを更新するオプションがあります。



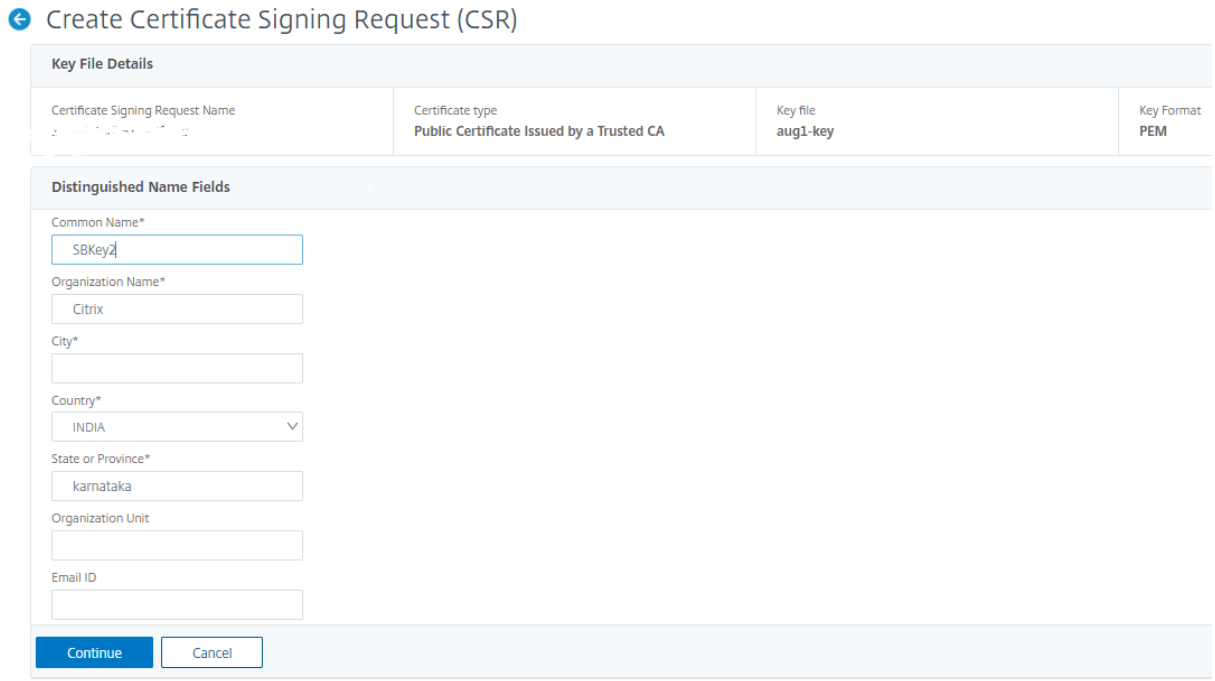
証明書署名要求の作成　SSL 証明書の 1 つが組織のポリシーに準拠していないユースケースを想像してください。証明機関から新しい証明書を取得したい。NetScaler ADM から証明書署名要求（CSR）を生成できるようになりました。CSR と公開鍵を CA に送信して SSL 証明書を取得できます。

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。

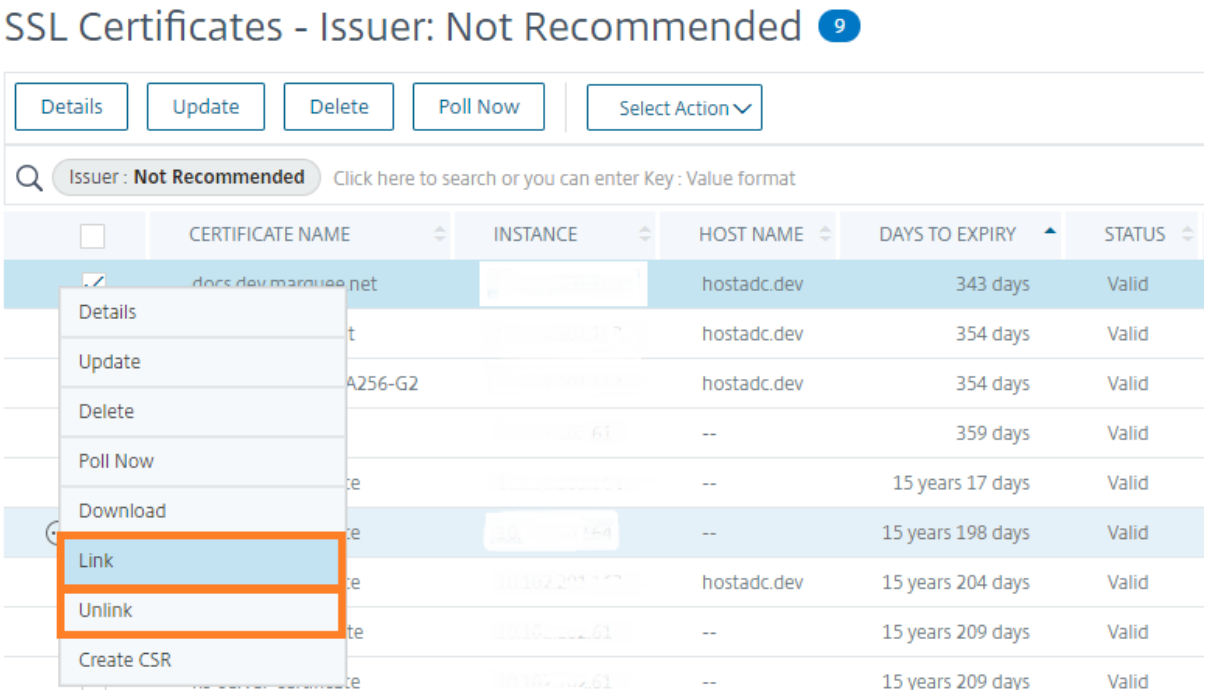


CSR を作成するには、共通名、組織名、都市、国、州、組織単位、電子メール ID など、選択したキーの詳細を指定します。



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。

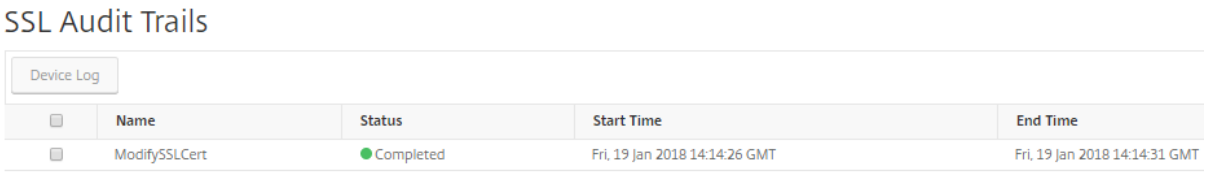


監査ログ

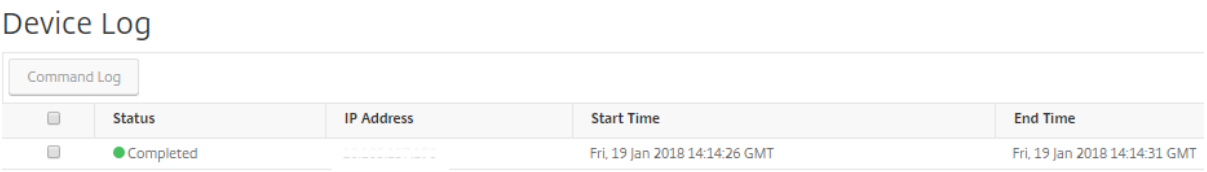
監査ログは、NetScaler ADM によって生成されるテキストログファイルのコレクションです。NetScaler ADM を使用して特定の NetScaler ADC アプライアンスに追加、変更、および変更された SSL 証明書の履歴が表示されます。監査ログには、NetScaler ADC アプライアンスの IP アドレス、ステータス、開始時刻、および特定の操作の終了時刻も表示されます。

この例では、特定の証明書に対して一定の期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。

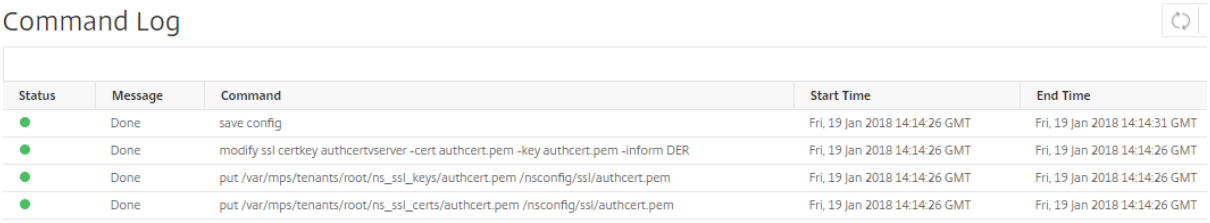
SSL 証明書の情報を調べるには、**SSL** ダッシュボードで、「監査ログ」をクリックします。アプリケーションの概要には、[開始時刻] と [終了時刻] の SSL 証明書ステータスが含まれます。



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。



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。



SSL ダッシュボードの使用

February 6, 2024

NetScaler Application Delivery Management（ADM）の SSL 証明書ダッシュボードを使用すると、証明書発行者、主な強み、署名アルゴリズムの追跡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

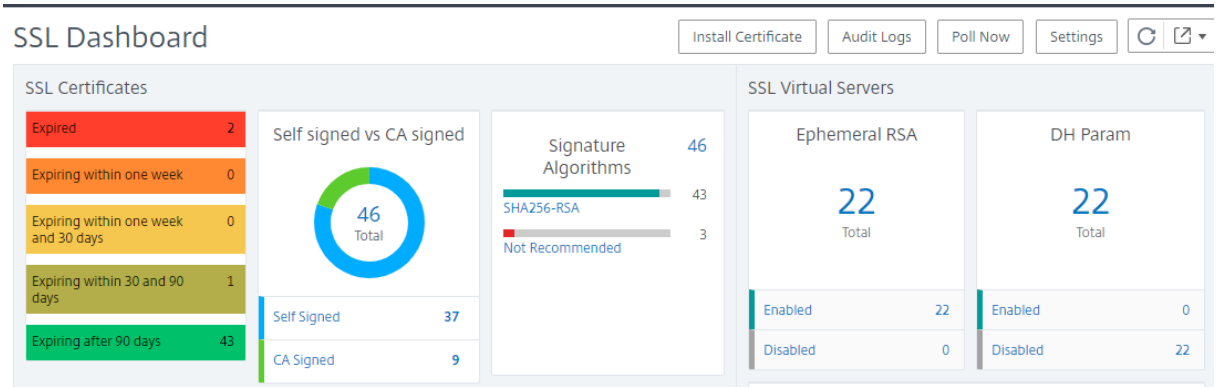
- 使用されている証明書および未使用の証明書の数
- 自己署名および CA 署名の証明書の数
- 発行者数
- 署名アルゴリズム
- SSL プロトコル
- 使用中の証明書件数上位 10 インスタンス

SSL 証明書を監視するには

会社の SSL ポリシーで特定の SSL 証明書要件を定義している場合、NetScaler ADM の SSL ダッシュボードを使用して証明書を監視できます。たとえば、すべての証明書には最低 2048 ビットのキー強度が必要で、信頼できる CA 機関による承認が必要です。

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、インフラストラクチャ **> SSL** ダッシュボードに移動します。



NetScaler ADM では、SSL 証明書をポーリングし、インスタンスのすべての SSL 証明書を直ちに NetScaler ADM に追加できます。そのためには、

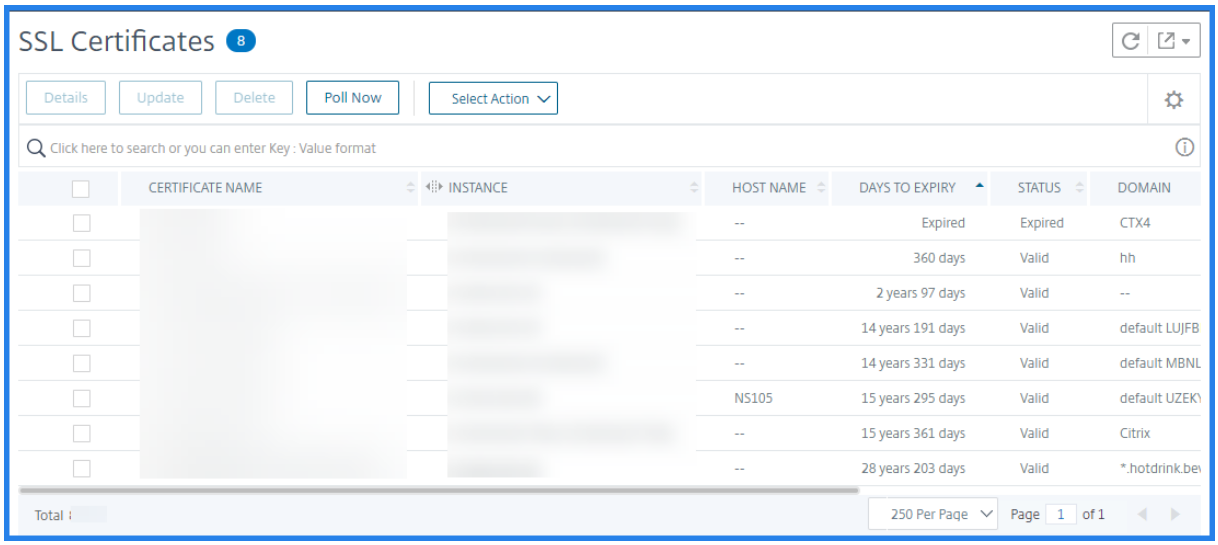
1. [インフラストラクチャ**] > [SSL** ダッシュボード**]** に移動します。
2. [今すぐ投票] をクリックします。

   「**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。



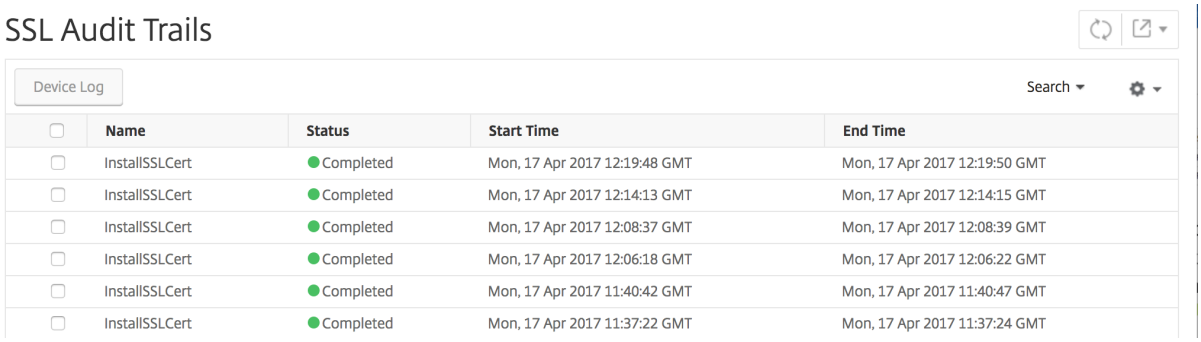
NetScaler ADM SSL ダッシュボードには、仮想サーバーで実行されている SSL プロトコルの分布も表示されます。管理者は、SSL ポリシーを通じて監視するプロトコルを指定できます。詳細については、「SSL ポリシーの設定」を参照してください。サポートされるプロトコルは、SSLv2、SSLv3、TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3 です。仮想サーバー上で使用されている SSL プロトコルは、棒グラフ形式で表示されます。特定のプロトコルをクリックすると、そのプロトコルを使用している仮想サーバーのリストが表示されます。

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。

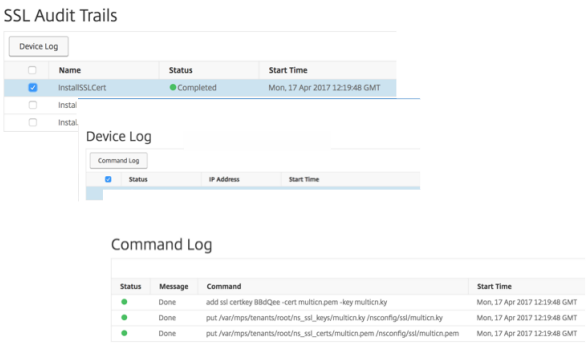
SSL 証明書の監査記録を表示するには

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、[インフラストラクチャ] **> [SSL** ダッシュボード] に移動し、[監査ログ] をクリックします。



SSL 証明書を使用して実行された特定の操作については、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。

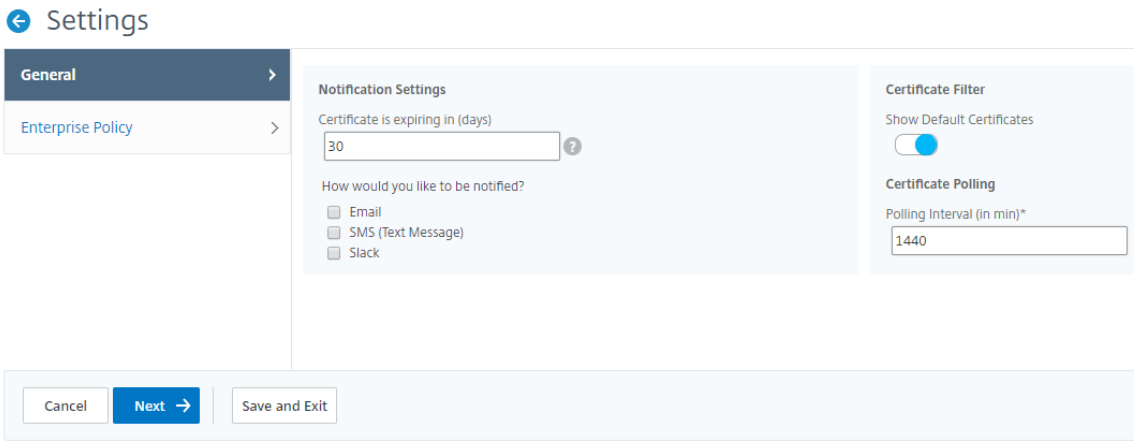


SSL ダッシュボードでデフォルトの **NetScaler ADC** 証明書を除外するには

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［インフラストラクチャ］**>**［**SSL** ダッシュボード］に移動します。
2. [**SSL** ダッシュボード] ページで、[設定] をクリックします。
3. **[** 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. 「証明書フィルター 」セクションで、「デフォルト証明書を表示」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

NetScaler ADM で SSL ファイルを表示するには、NetScaler ADM で［インフラストラクチャ］**>**［**SSL** ダッシュボード］**>**［**SSL** ファイル］に移動します。

NetScaler ADM では、次のファイルを表示、アップロード、ダウンロードできます。

- SSL 証明書
- SSL キー
- SSL CSR

NetScaler インスタンスで SSL ファイルを表示およびダウンロードするには、NetScaler で [インフラストラクチャ] **> [SSL** ダッシュボード] **> [SSL** ファイル] に移動します。

SSL ファイルには、NetScaler インスタンスが手動で、またはスケジュールされたバックアッププロセスを通じてバックアップされた後にのみアクセスできます。

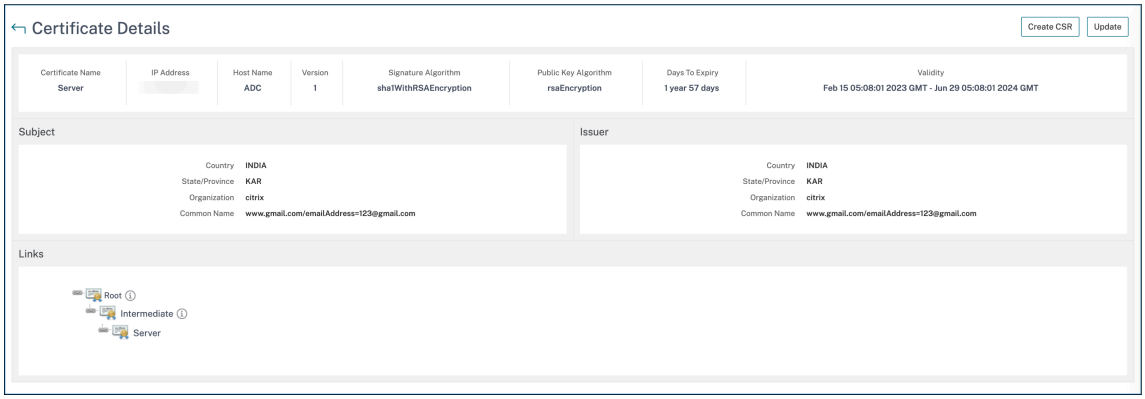
> 重要:
>
> ADC インスタンスからの SSL ファイルのダウンロードを有効にするには、インスタンス **SSL** 証明書 機能を有効にします。詳しくは、「ADM 機能の有効化または無効化」を参照してください。

SSL 証明書チェーンを表示する

中間証明書からルート CA 証明書までの完全な証明書チェーンを表示できます。

証明書チェーンを表示するには:

1. [インフラストラクチャ] **> [SSL** ダッシュボード] に移動し、任意のタイルの SSL 証明書をクリックします。
2. **SSL** 証明書ページで、証明書を選択し、「詳細」をクリックします。証明書チェーンはリンクの下に表示されます。



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。

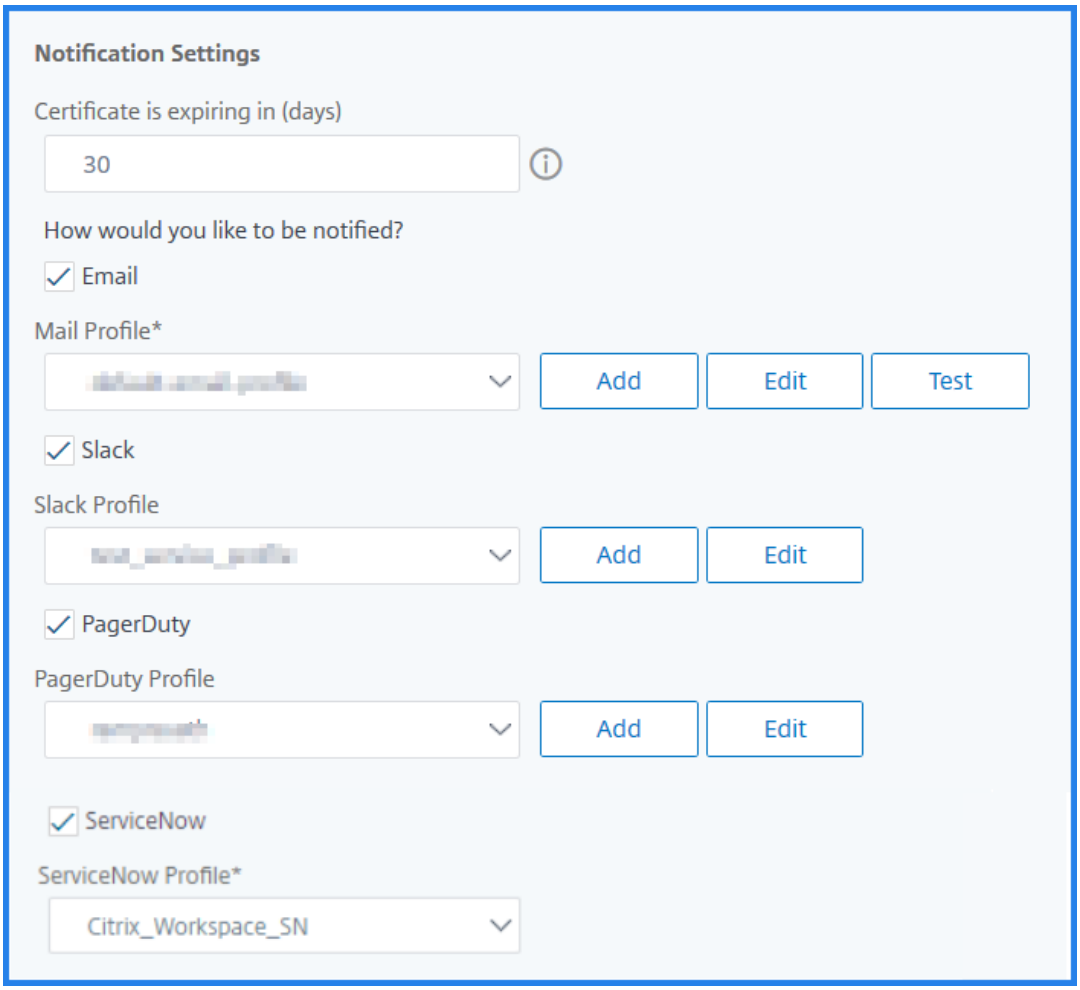
NetScaler ADM からの通知を設定するには：

1. NetScaler Application Delivery Management（ADM）で、［インフラストラクチャ］**>**［**SSL** ダッシュボード］に移動します。
2. [**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。



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。NetScaler 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。

トラップ送信先を設定するには、**[設定] > [SNMP] > [**トラップ送信先] の順に移動します。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。

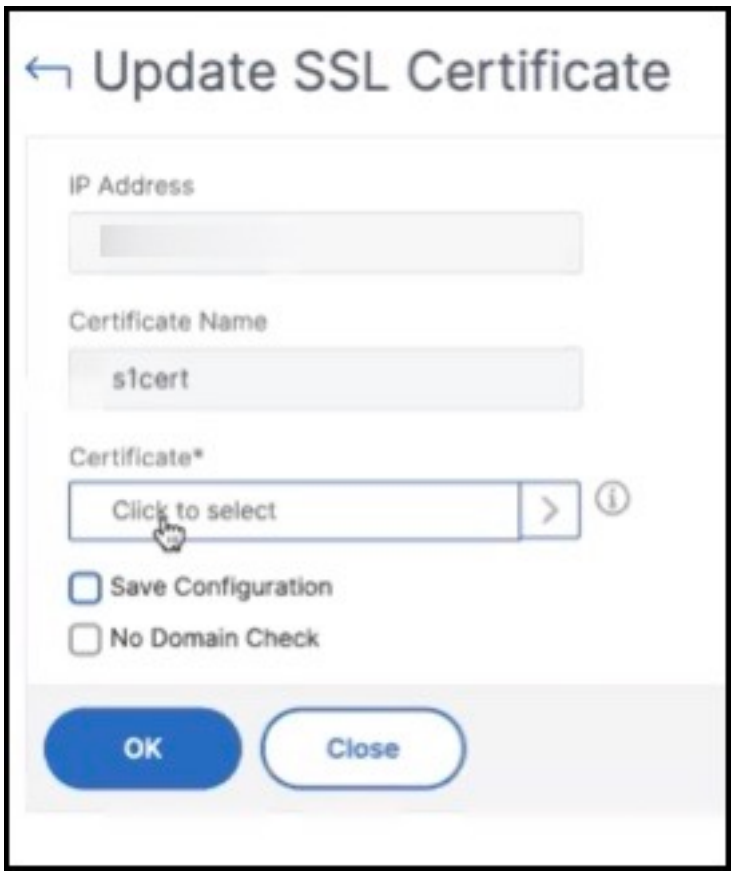
インストールされた証明書を更新する

February 6, 2024

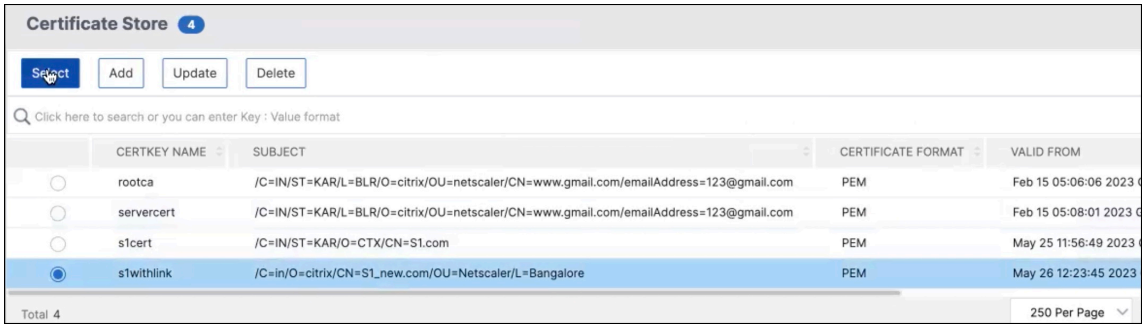
認証局（CA）から更新された証明書を受け取ったら、証明書を更新するために個々の NetScaler インスタンスにログオンする必要はありません。NetScaler ADM の既存の証明書は、証明書ストアの証明書で更新できます。

NetScaler ADM から SSL 証明書を更新するには：

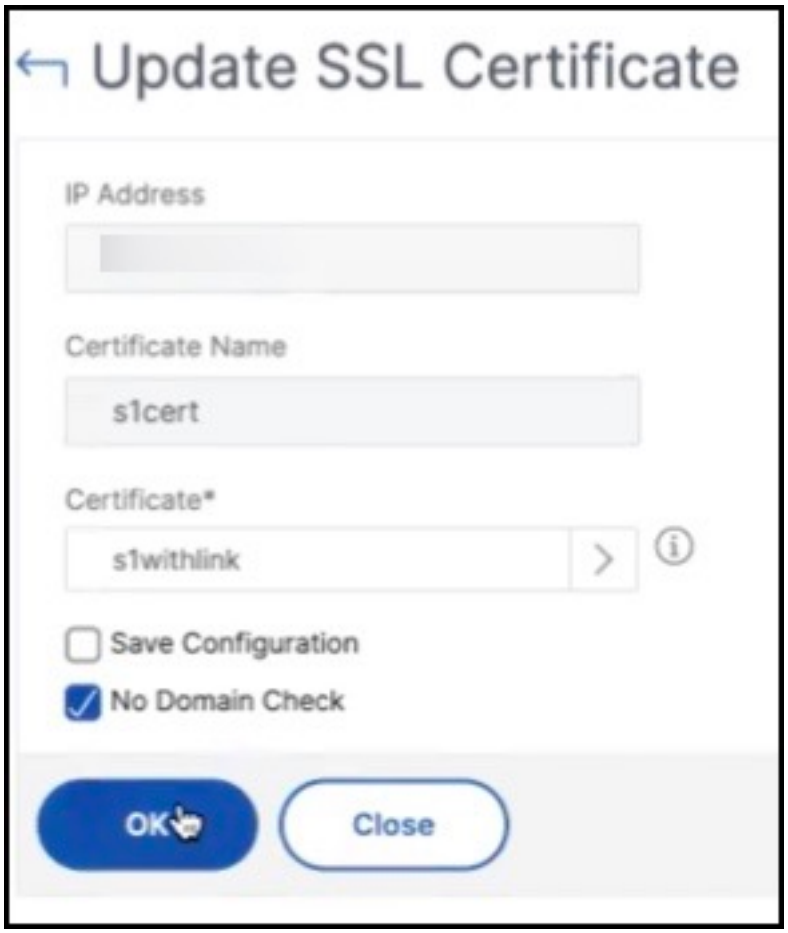
1. NetScaler ADM で、インフラストラクチャ **> SSL** ダッシュボードに移動します。
2. いずれかのグラフをクリックして、SSL 証明書の一覧を表示します。
3.「**SSL** 証明書」ページで、証明書を選択し、「更新」をクリックします。または、SSL 証明書をクリックして詳細を表示し、[**SSL** 証明書] ページの右上隅にある [更新] をクリックします。
4.「**SSL** 証明書の更新」ページで、「証明書」を選択し、「証明書ストア」ページを表示します。



5. 証明書ストアページで、追加する証明書ファイルを選択します。［**Select**］をクリックします。



6. 新しい証明書のドメイン名が古い証明書と一致しない場合、サーバーに新しいドメインをホストさせたい場合は、「ドメインチェックなし」を選択します。



［**OK**］をクリックします。この証明書がバインドされているすべての SSL 仮想サーバーは自動的に更新されます。

> 注:
>
> 証明書ストアの証明書チェーンを使用して既存の SSL 証明書を更新すると、既存の証明書はリンクされた証明書で更新されます。証明書を選択し、「詳細」をクリックして証明書チェーンを表示します。

NetScaler インスタンスへの **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. インフラストラクチャ **> SSL** ダッシュボードに移動します。
2. SSL ダッシュボードの右上隅にある [インストール] をクリックします。
3. **NetScaler** インスタンス への **SSL** 証明書のインストールページで、次のパラメータを指定します。

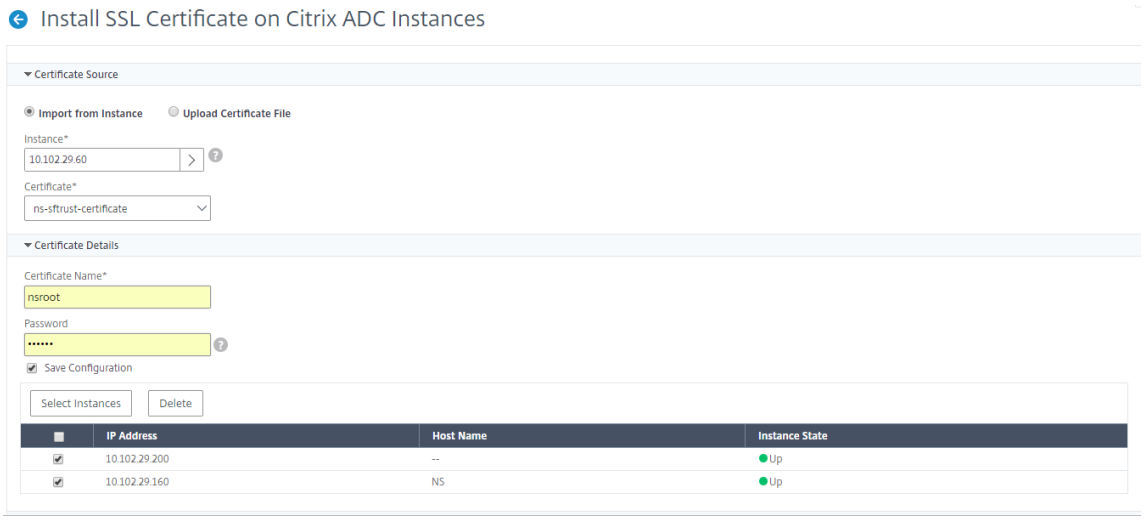
   a) [証明書のソース
   ] [インスタンスからインポート] オプションを選択します。

   - 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

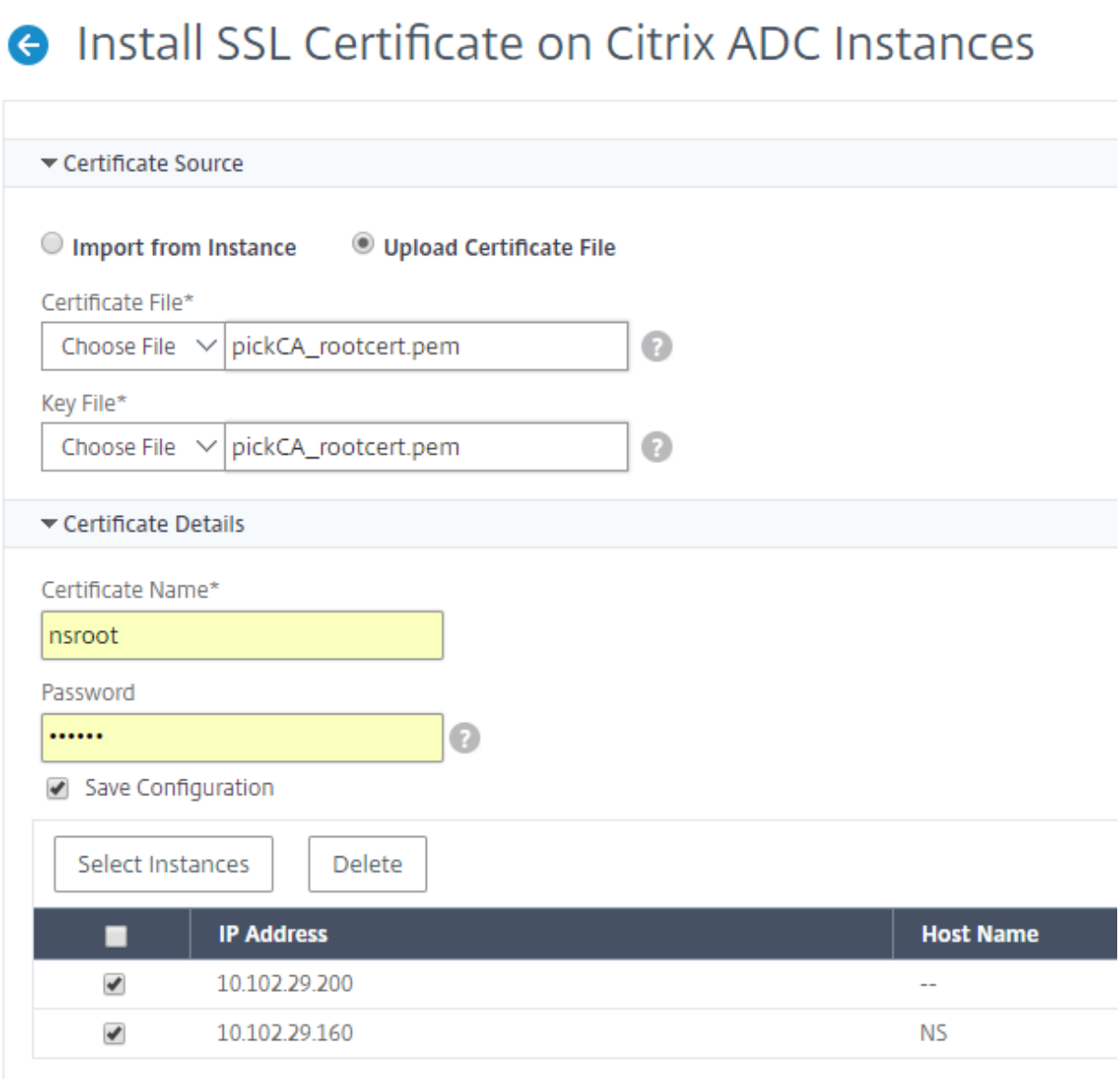
   - 証明書名。証明書キーの名前を指定します。
   - パスワード。プライベートキーを暗号化するためのパスワード。このオプションを使用して、暗号化された秘密キーをアップロードできます。

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 インスタンスを選択します。
5. [**OK**] をクリックします。



NetScaler ADM から **SSL** 証明書をインストールするには:

1. NetScaler ADM で、インフラストラクチャ **> SSL** ダッシュボードに移動します。
2. 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** 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 NetScaler 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。



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、［インフラストラクチャ］**>**［**SSL** ダッシュボード］に移動します。

2. いずれかのグラフをクリックして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 [**3**] または [**F4**] 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。
PEM 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（**DES** または **DES3**）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。
PEM 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。
PEM パスフレーズの確認	PEM パスフレーズを確認します。

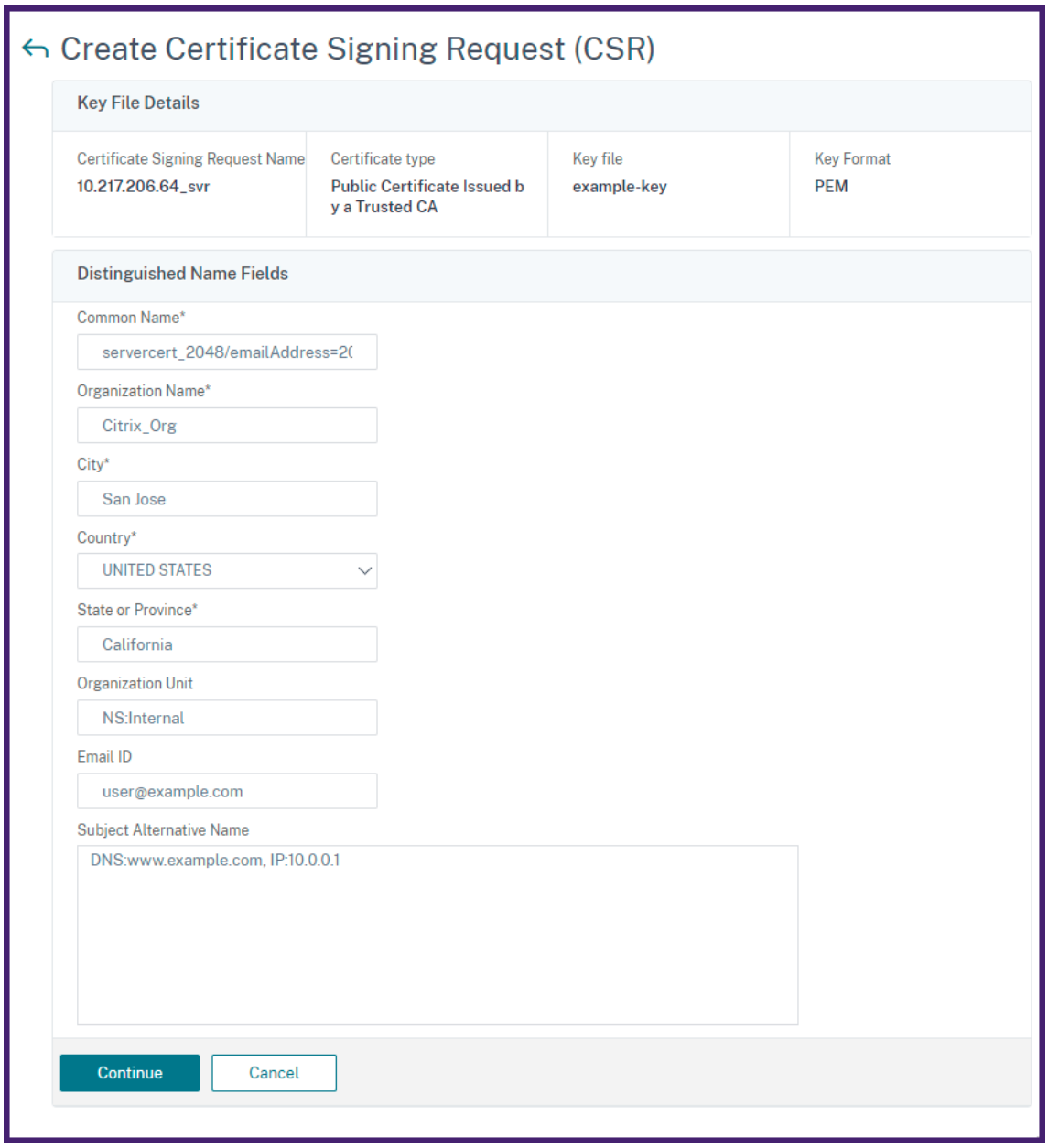
5. [続行] をクリックします。
6. 次のページで、詳細を入力します。

   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。

```
DNS:<Domain name>, IP:<IP address>
<!--NeedCopy-->
```

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、［インフラストラクチャ］**>**［**SSL** ダッシュボード］に移動します。
2. いずれかのグラフをクリックして、SSL 証明書の一覧を表示します。
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、インフラストラクチャ **> SSL** ダッシュボードに移動します。
2. いずれかのグラフをクリックして、SSL 証明書の一覧を表示します。
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. **NetScaler 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。

> 注
>
> SSL ダッシュボードには、［設定］オプションで選択した署名アルゴリズムのみが表示され、その他は「非推奨」として表示されます。

NetScaler ADC インスタンスからの **SSL** 証明書のポーリング

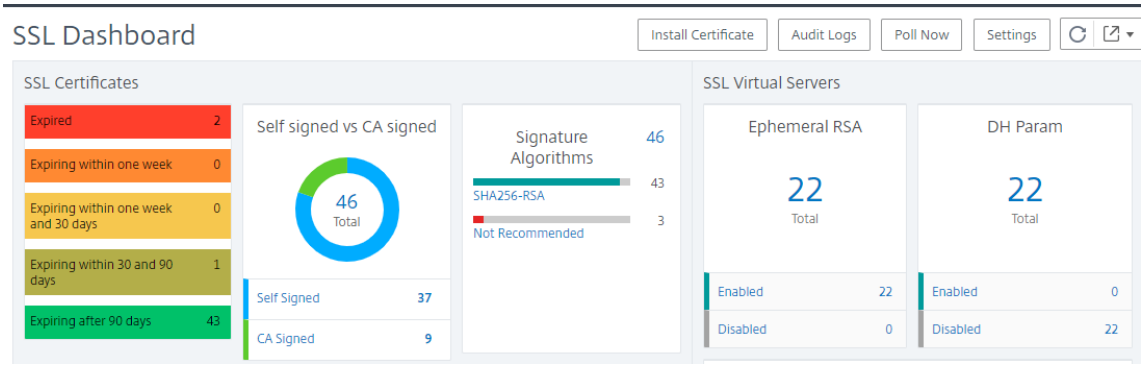
February 6, 2024

NetScaler Application Delivery Management（ADM）は、NITRO 呼び出しとセキュアコピー（SCP）プロトコルを使用して、24 時間ごとに 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。

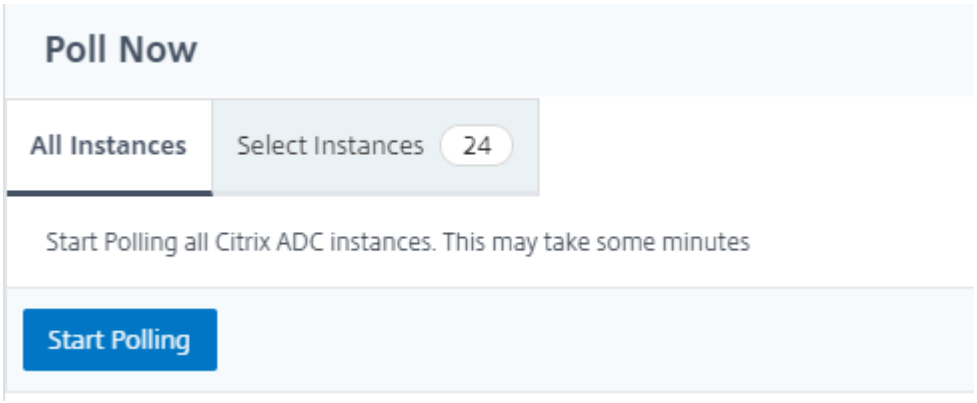
NetScaler インスタンスで **SSL** 証明書をポーリングするには：

1. NetScaler ADM で、インフラストラクチャ **> SSL** ダッシュボードに移動します。
2. [**SSL** ダッシュボード] ページの右上隅にある [今すぐポーリングする] をクリックします。

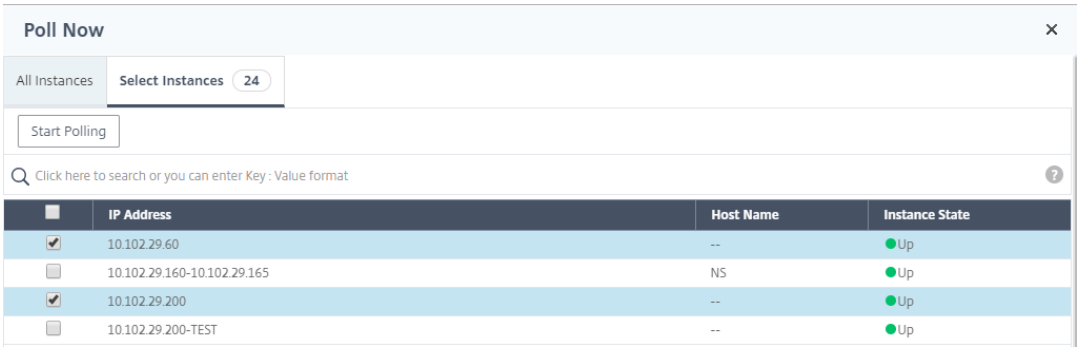


3. [**Poll Now**] ページが開き、ネットワーク内のすべての NetScaler インスタンスをポーリングするか、選択したインスタンスをポーリングするかを選択できます。

   a) すべての NetScaler インスタンスの SSL 証明書をポーリングするには、［すべてのインスタンス］タブを選択し、［ポーリング開始］をクリックします。



   b) 特定のインスタンスをポーリングするには、**[Select**Instances**]** タブを選択し、リストからインスタンスを選択し、**[**Poll Now**] をクリックします。**



NetScaler ADM 証明書ストアを使用して SSL 証明書を管理します

February 6, 2024

NetScaler ADM 証明書ストアを使用すると、SSL 証明書を 1 か所に保存して管理できます。保存した証明書を使用して、後で NetScaler 設定を構成できます。

証明書ストアでは、SSL 証明書を追加、更新、削除できます。証明書ストアを使用して、NetScaler インスタンスから証明書をインポートし、それを他のターゲット NetScaler インスタンスに適用することもできます。

SSL 証明書を証明書ストアに追加する

1. [インフラストラクチャ**] > [SSL** ダッシュボード**] > [**証明書ストア] に移動します。[追加] をクリックします。
2. 「証明書を追加」ページで、次の詳細を入力します。
    - 証明書キー名 -証明書の名前を入力します。名前には ASCII 英数字、アンダースコア、ハイフンのみを使用し、30 文字未満にする必要があります。証明書の作成後に名前を変更することはできません。
    - 証明書ファイル -ローカルドライブを参照し、証明書ファイルをアップロードします。
    - キーファイル -ローカルコンピューターからキーファイルをアップロードします。
    - パスワード -PEM 形式の暗号化された秘密鍵がある場合は、秘密鍵の暗号化に使用されたパスフレーズを入力します。
    - 証明書チェーンを追加 -このオプションを選択すると、証明書チェーンに証明書が追加されます。
    - 証明書チェーン -ローカルドライブを参照し、証明書ファイルをアップロードします。
    - [作成] をクリックします。

証明書ストアの **SSL** 証明書の更新

1. [インフラストラクチャ**] > [SSL** ダッシュボード**] > [**証明書ストア] に移動します。更新する証明書を選択し、[更新] をクリックします。
2. 「証明書の更新」ページで、次の詳細を入力します。
    - 証明書キー名 -更新対象として選択した証明書の名前が表示されます。
    - 証明書ファイル -証明書ファイルを更新するには、証明書ファイルをアップロードします。
    - キーファイル -キーファイルを更新するには、ローカルコンピューターからキーファイルをアップロードします。
    - パスワード -PEM 形式の暗号化された秘密鍵がある場合は、秘密鍵の暗号化に使用されたパスフレーズを入力します。
    - 証明書チェーンを追加 -このオプションを選択すると、証明書チェーンに証明書が追加されます。
    - 証明書チェーン -ローカルドライブを参照し、証明書ファイルをアップロードします。
    - [**OK**] をクリックします。

証明書ストアから **SSL** 証明書を削除する

1. [インフラストラクチャ**] > [SSL** ダッシュボード**] > [**証明書ストア] に移動します。[追加] をクリックします。
2. プロンプトが表示されたら、[はい] をクリックして証明書を削除します。

NetScaler インスタンスへの **SSL** 証明書のインストール

1. [インフラストラクチャ**] > [SSL** ダッシュボード**] > [**証明書ストア] に移動します。NetScaler インスタンスにインストールする証明書を選択します。
2.「**NetScaler** インスタンスへの **SSL** 証明書のインストール」ページで、次の詳細を入力します。

   a. 証明書ソース

   - 証明書 -選択した証明書の名前が表示されます。

   b。証明書の詳細

   - 証明書名 -証明書の名前が表示されます。
   - 構成の保存 -NetScaler 構成を保存するには、このオプションを選択します。NetScaler 構成は、証明書のインストール後に保存されます。

3.「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 インスタンスを選択します。

[**OK**] をクリックします。

NetScaler インスタンスから証明書をインポートする

1. [インフラストラクチャ**] > [SSL** ダッシュボード**] > [**証明書ストア] に移動します。[**ADC** 証明書のインポート] をクリックします。
2. **ADC** 証明書のインポートページでは、次のタブのいずれかを選択できます。

   - **ADC** 証明書のインポート -[ポーリングの開始] をクリックして、すべての NetScaler インスタンスのすべての SSL 証明書をポーリングします。
   - インスタンスの選択 -NetScaler インスタンスを選択し、「**ADC** 証明書のインポート」をクリックして、選択した NetScaler インスタンスの SSL 証明書のみをポーリングします。

   ポーリング後、SSL 証明書とキーファイルがダウンロードされ、証明書ストアに追加されます。

   > 注:
   >
   > ストアに同じ証明書名が存在する場合、証明書のインポート操作は失敗します。ただし、インポート操

> 作では残りの証明書のポーリングが継続され、NetScaler 証明書（使用可能な場合）がストアに追加されます。

可用性の高い導入環境におけるデータベースのカスタム証明書と暗号の管理

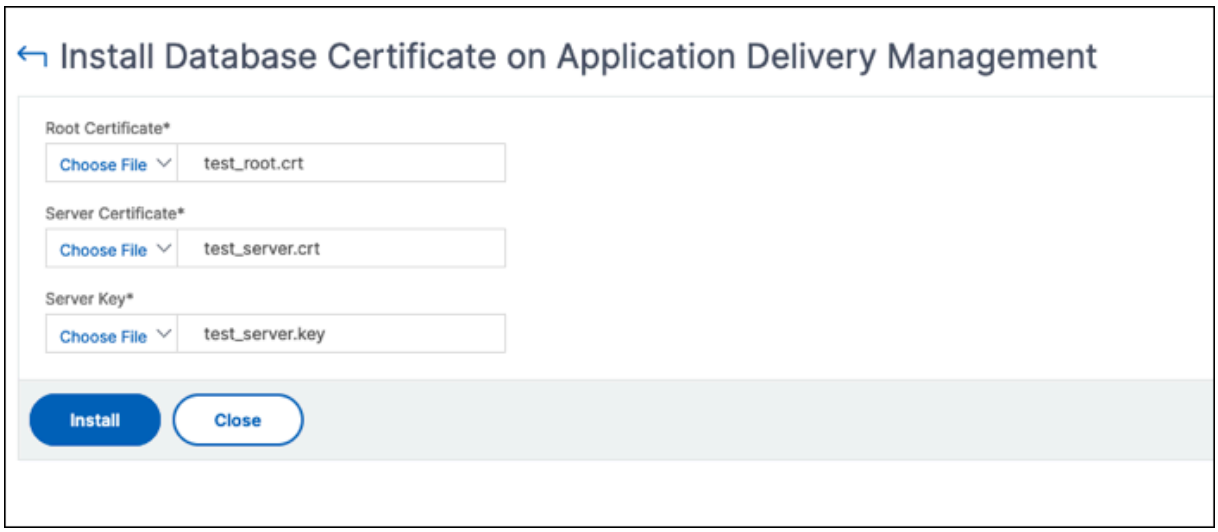
February 6, 2024

NetScaler ADM では、デフォルトの組み込みデータベース証明書を、信頼できる認証局からの独自の証明書に置き換えることができます。NetScaler ADM データベースで独自の暗号スイートを構成することもできます。この機能により、証明書管理のニーズに対する柔軟性とセキュリティが向上し、信頼できる SSL 証明書を使用して HA ノード間のすべての通信を保護できます。

NetScaler ADM にデータベース証明書をインストールします

HA セットアップで証明書をインストールするには:

1. [設定] **> [HA** 展開] に移動し、[データベース証明書] をクリックします。
2. [インストールされた証明書] タブをクリックし、[新しい証明書のインストール] をクリックします。
3. 「アプリケーション配信管理へのデータベース証明書のインストール」ページで、ルート証明書、サーバー証明書、およびサーバーキーをアップロードします。次のいずれかの操作を実行できます:
   - 「ファイル」**>**「ローカル」を選択し、ローカルマシンから証明書またはキーファイルをアップロードします。
   - **NetScaler ADM** にある証明書またはキーファイルをアップロードするには、**[**ファイル**] > [**アプライアンス**]** を選択します。
4. [**Install**] をクリックします。

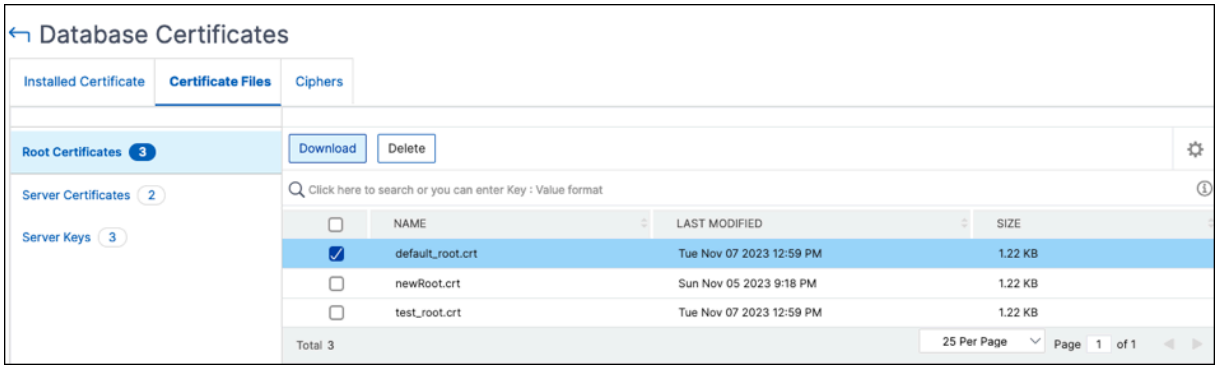


> 注:
>
> チェーン証明書が複数ある場合は、それらを 1 つのファイルにまとめる必要があります。連結の順序が正しく、最初に中間証明書、次にルート証明書が続くことを確認してください。この順序は、証明書チェーンが正しく認識されるために不可欠です。
>
> たとえば、次のコマンドは、各証明書ファイル (中間証明書 1.crt、中間証明書 2.crt、および root_certificate.crt) の内容を combined_certs.crt という名前のファイルに追加します。
>
> ```
> cat intermediate_certificate1.crt >> combined_certs.crt
> cat intermediate_certificate2.crt >> combined_certs.crt
> cat root_certificate.crt >> combined_certs.crt
> ```

インストールしたデータベース証明書を管理する

インストールされている証明書を表示、ダウンロード、削除するには:

1. [設定] **> [HA** 展開] に移動し、[データベース証明書] をクリックします。
2. [証明書ファイル] タブをクリックし、[ルート証明書]、[サーバー証明書]、または [サーバーキー] を選択すると、対応するファイルが表示されます。
3. ローカルマシンにファイルをダウンロードするには、「ダウンロード」をクリックします。
4. 証明書ファイルを削除するには、ファイルを選択して [削除] をクリックします。表示される確認ダイアログボックスで、「**OK**」をクリックします。

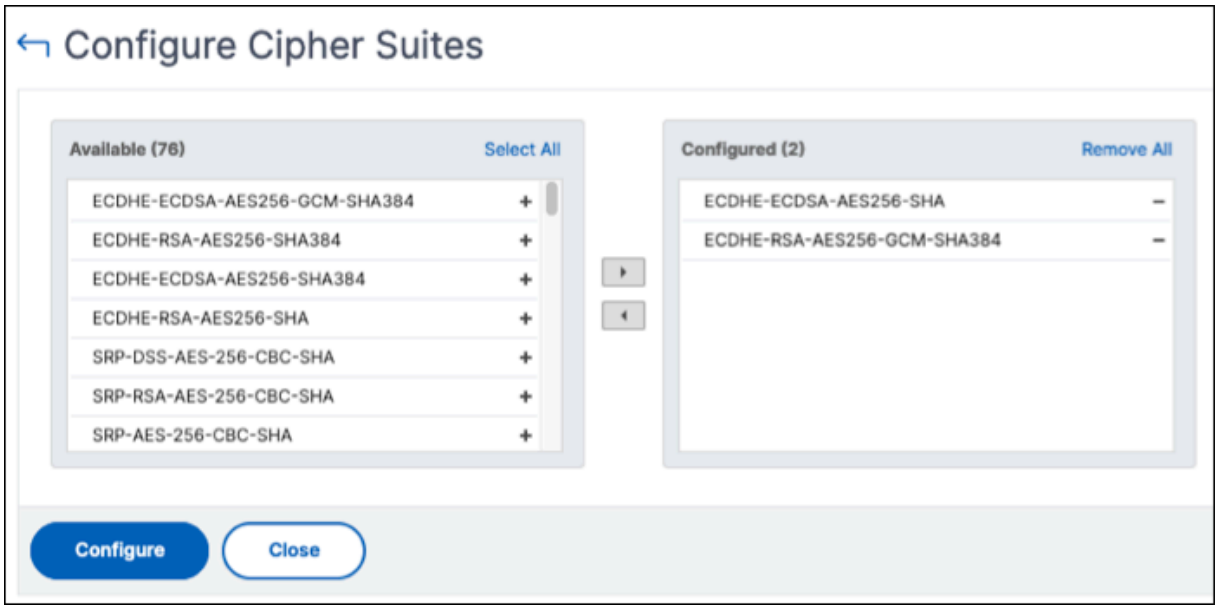


データベース暗号スイートの設定

HA デプロイメントの暗号スイートを構成するには:

1. [設定] **> [HA** 展開] に移動し、[データベース証明書] をクリックします。
2. [暗号] タブをクリックし、[****** 暗号の設定 ******] をクリックします。
3. 「暗号スイートの設定」ページで、使用可能な暗号のリストから 1 つ以上の暗号を選択します。

4. ［構成］をクリックします。表示される確認ダイアログボックスで、「はい」をクリックして暗号設定を変更します。



> 注:
>
> 暗号設定を変更すると、NetScaler ADM のセカンダリノードと障害復旧ノードが再起動します。

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、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（[インフラストラクチャ] > [イベント]）に表示され、すべてのアクティブなイベントは [イベントメッセージ] ページ（[インフラストラクチャ] > [イベント] > [イベントメッセージ]）に表示されます。

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 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

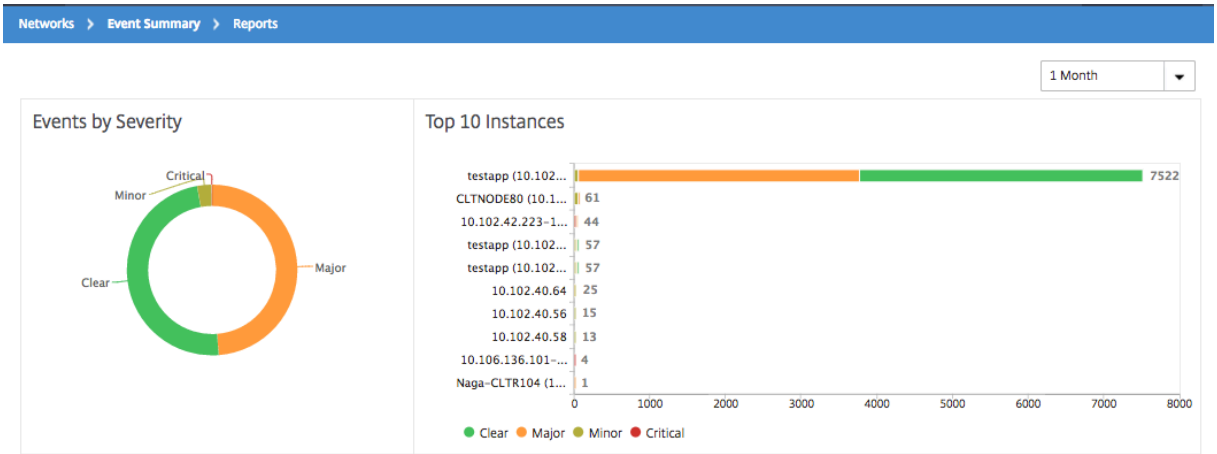
February 6, 2024

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。

インフラストラクチャ **>** イベント **>** レポートに移動します。

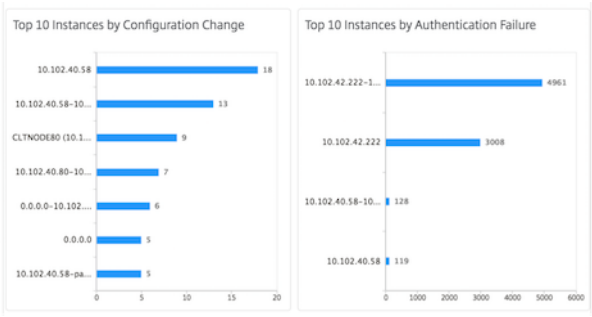
ダッシュボードの［Top 10 Devices］グラフには、各インスタンスで生成されたイベントの数に基づき、上位 10 個のインスタンスが表示されます。グラフのインスタンスをクリックすると、イベントの重大度の詳細を表示できます。



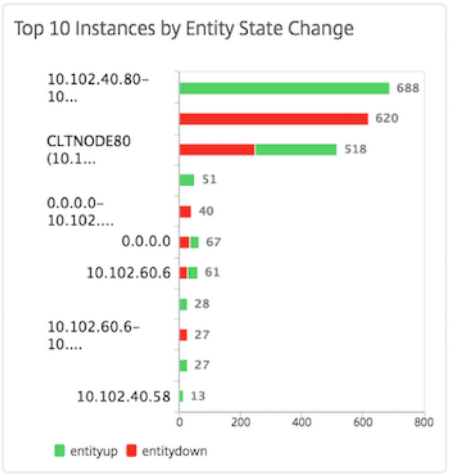
NetScaler インスタンスタイプ（[インフラストラクチャ] **>** [イベント] **>** [レポート] ** [****NetScaler/NetScaler SDX**]）に移動すると、次の情報が表示されます。

- ハードウェアエラー件数上位 10 デバイス

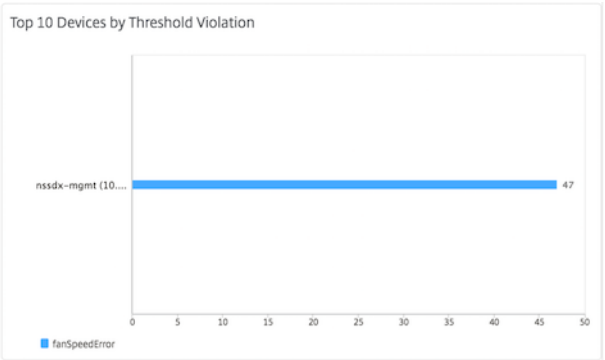
- 構成変更件数上位 10 デバイス
- 認証エラー件数上位 10 デバイス



- 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

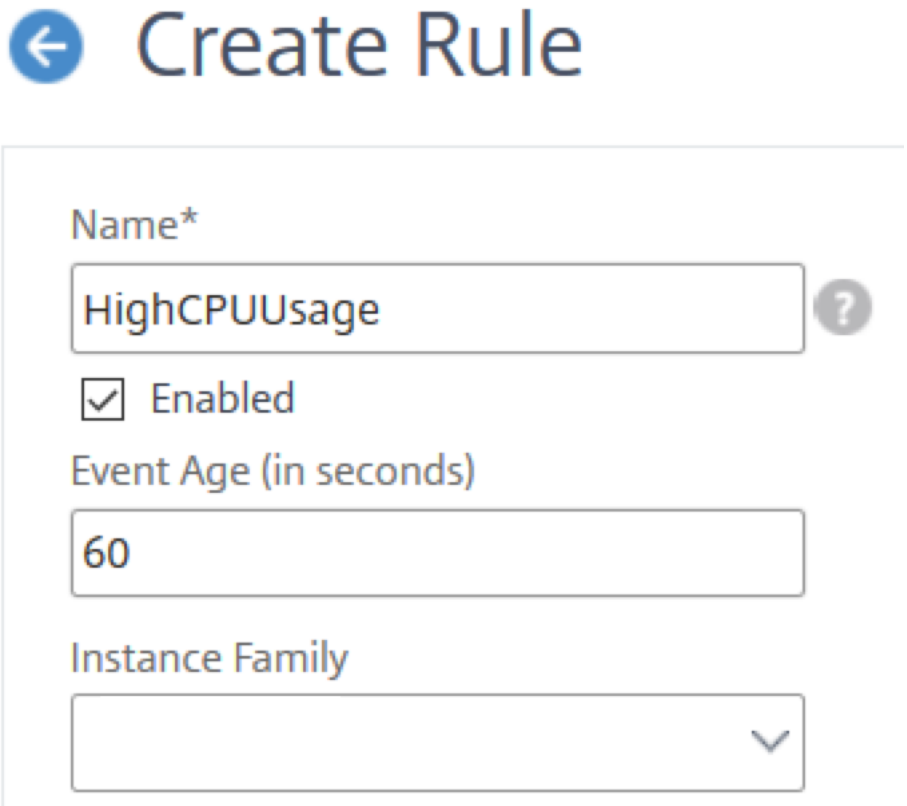
イベントの経過時間オプションを設定して、時間間隔 (秒単位) を指定できます。NetScaler ADM は、設定された期間までアプライアンスを監視し、イベントの経過時間が設定された期間を超えた場合にのみイベントを生成します。

> 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. NetScaler ADM で、インフラストラクチャ **>** イベント **>** ルールに移動し、追加をクリックします。
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。



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

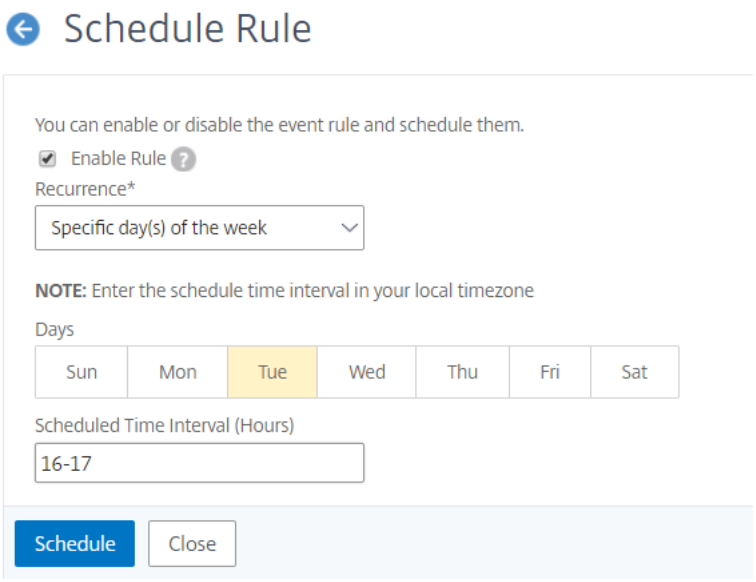
ルールのフィルターを作成した後、生成されたイベントがフィルター条件を満たすたびに NetScaler Application Delivery Management（ADM）サーバーから通知を送信したくない場合は、毎日、毎週、毎月などの特定の時間間隔でのみトリガーされるようにフィルターをスケジュールできます。

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メール通知を有効にしている場合、NetScaler ADM がこれらのトラップを受信すると、サーバーから大量のメール通知が送信されます。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. NetScaler ADM で、［インフラストラクチャ］**>**［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。



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

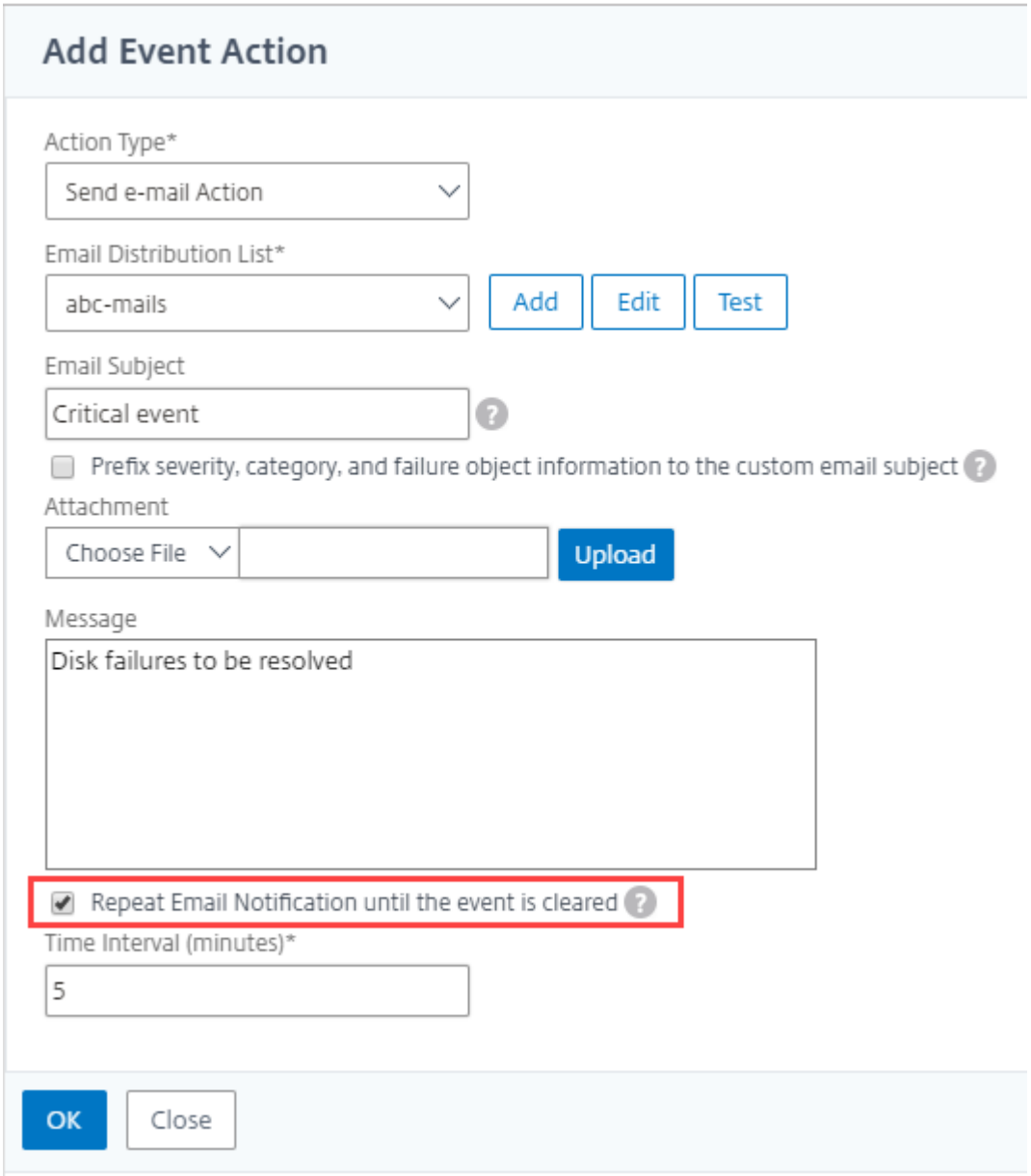
すべての重大なイベントに対応し、重要なメール通知を見落とさないために、指定した条件を満たすイベント規則に関して、連続してメール通知を送信するように指定できます。たとえば、ディスクエラーを伴うインスタンスに対するイベント規則を作成し、問題が解決するまで通知するようにする場合、それらのイベントに関して連続メール送信を指定できます。

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。
>
> - [インフラストラクチャ] > [イベント] > [イベントの概要] に移動し、カテゴリを選択してカテゴリ内のイベントを選択し、[クリア] をクリックします。
> - または、インフラストラクチャ > イベント > イベントメッセージに移動します。インスタンスタイプを選択し、下のグリッドからイベントを選択し、[**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. NetScaler Application Delivery Management（ADM）で、［インフラストラクチャ］**>**［イベント］**>**［ルール］に移動し、［追加］をクリックしてルールを作成します。
2. ［**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。



イベントを抑制する

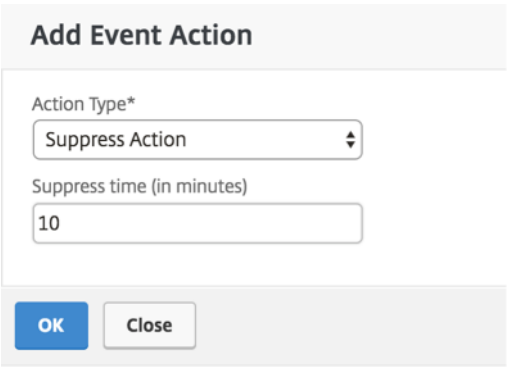
February 6, 2024

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. NetScaler Application Delivery Management（ADM）で、[インフラストラクチャ] **>** [イベント] **>** [ルール] に移動します。[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。



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。ルールを使用すると、インフラストラクチャ全体で生成された多数のイベントを容易に監視できます。

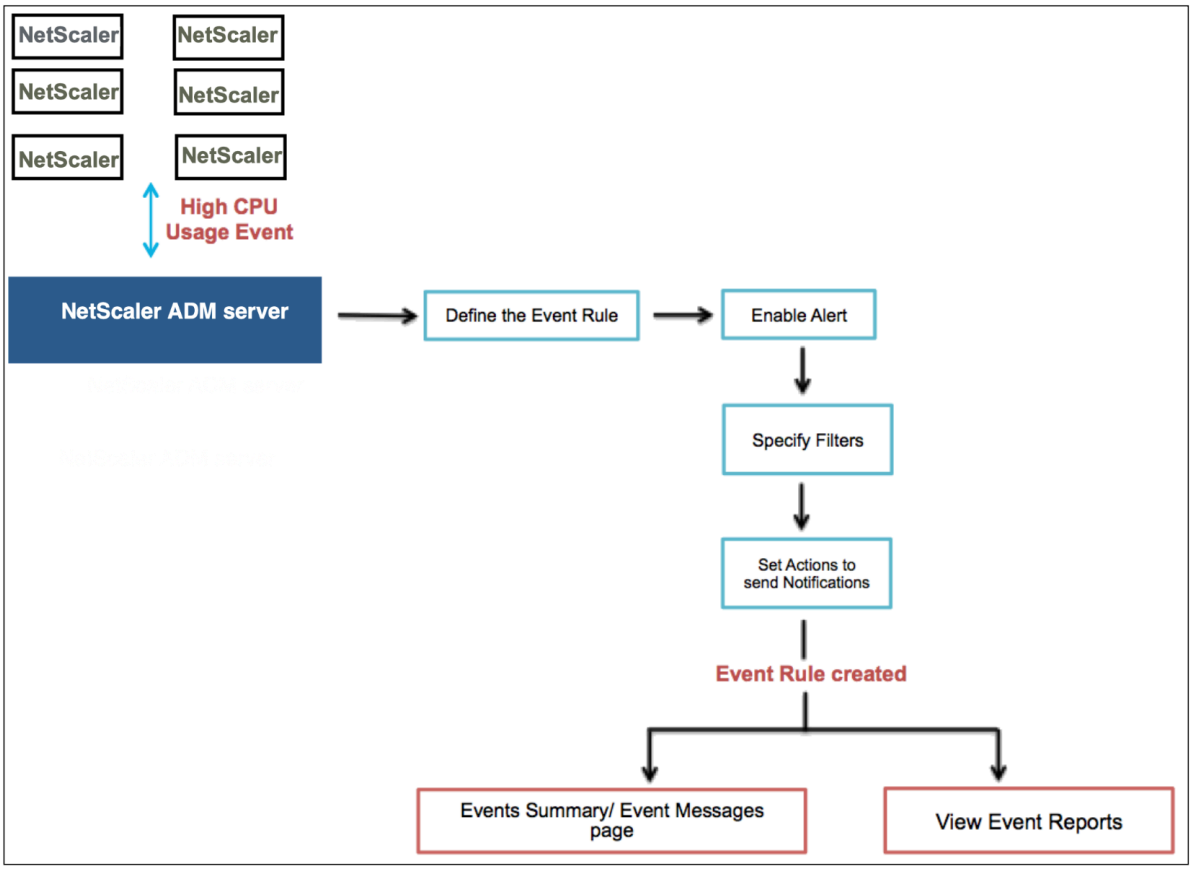
特定の条件で規則を構成し、規則にアクションを割り当てることで、一連のイベントにフィルターを適用できます。生成されたイベントがルール内のフィルタ条件を満たすと、そのルールに関連付けられたアクションが実行されます。フィルターを作成できる条件は、重大度、Citrix Application Delivery Controller（NetScaler）インスタンス、カテゴリ、障害オブジェクト、構成コマンド、メッセージです。

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 インスタンスの「高い CPU 使用率」イベントを監視すると、NetScaler 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 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

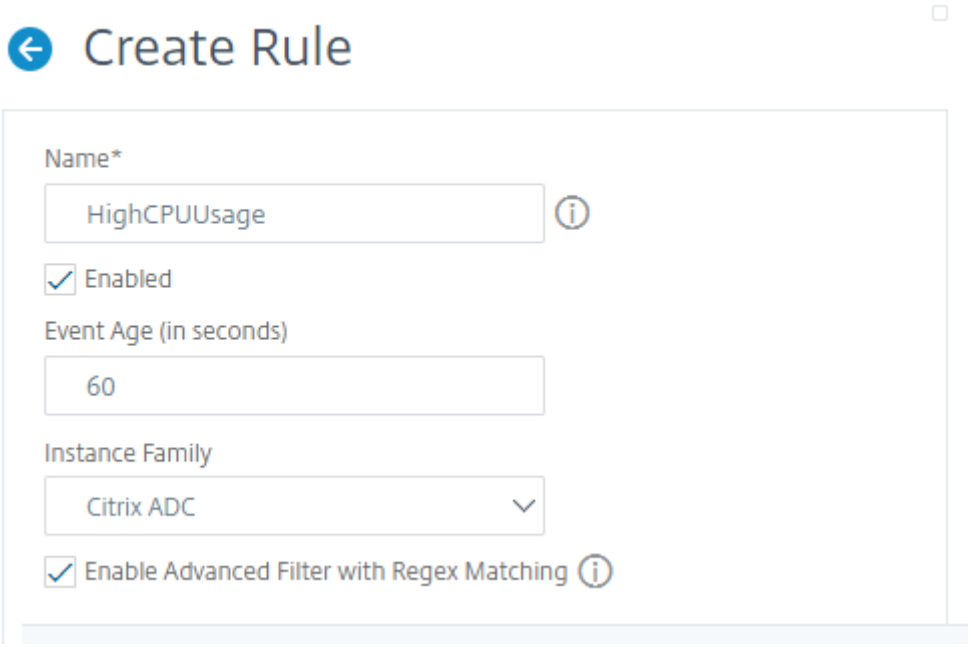
ステップ **1-**イベントルールを定義する

[インフラストラクチャ**] > [**イベント**] > [**ルール] に移動し、[追加] をクリックします。ルールを有効にする場合は、[ルールを有効にする] チェックボックスをオンにします。

イベント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 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 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。



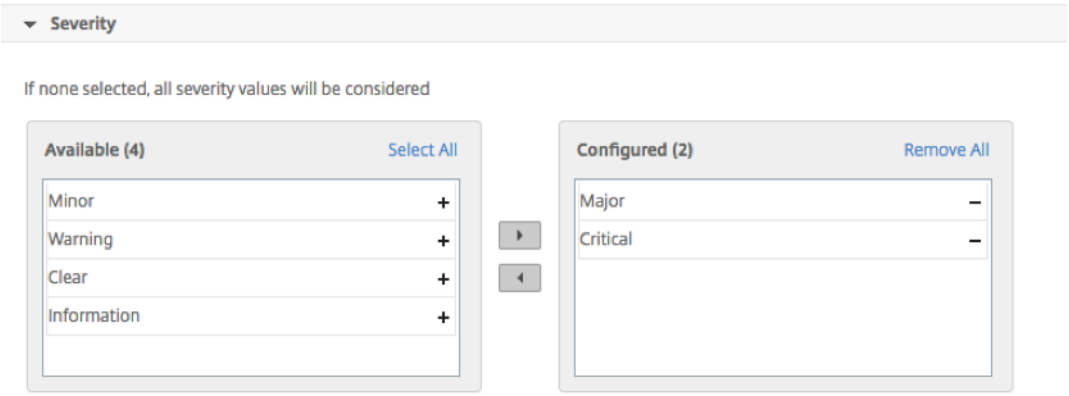
また、イベントルールをインスタンスファミリーでフィルタリングして、NetScaler ADM がイベントを受信する NetScaler インスタンスを追跡することもできます。

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。

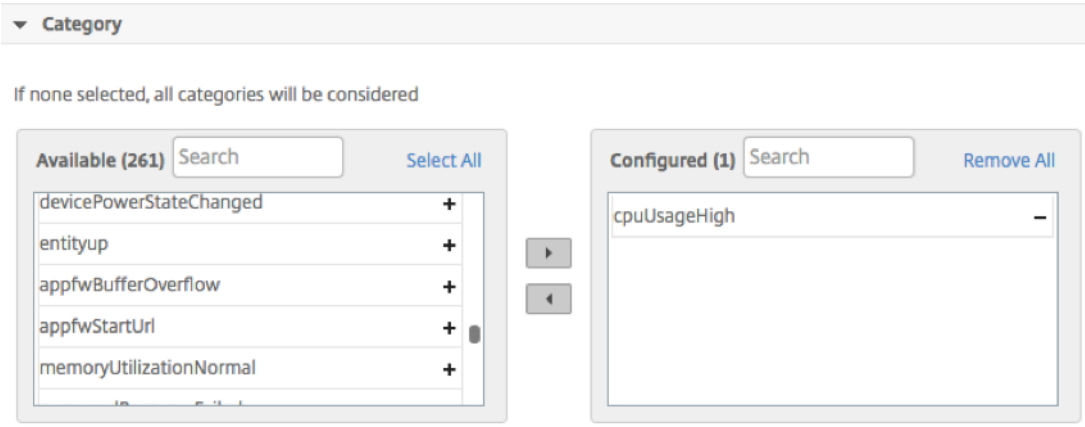


> 注
>
> 汎用イベントとアドバンス固有のイベントの両方について、重大度を設定できます。NetScaler ADM で管理されている NetScaler インスタンスのイベントの重要度を変更するには、[インフラストラクチャ] **>** [イベント] **>** [イベント設定] に移動します。イベントの重大度を設定するカテゴリ を選択し、[Configure Sever **ity**] をクリックします。新しい重大度レベルを割り当てて、[**OK**] をクリックします。

ステップ **3-**イベントカテゴリの指定

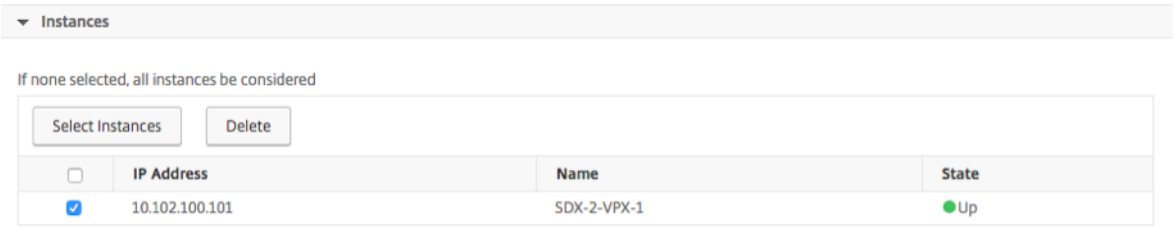
NetScaler インスタンスによって生成されるイベントのカテゴリを指定できます。すべてのカテゴリは、NetScaler インスタンスに作成されます。これらのカテゴリは、イベントルールの定義に使用できる NetScaler ADM にマッピングされます。考慮するカテゴリを選択し、「使用可能」(Available) テーブルから「構成済み」(構成済み) テーブルに移動します。

上の例では、表示されたテーブルからイベントカテゴリとして「cpuUsageHigh」を選択する必要があります。



ステップ **4-NetScaler** インスタンスの指定

イベントルールを定義する NetScaler インスタンスの IP アドレスを選択します。「インスタンス」セクションで、「インスタンスを選択」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。



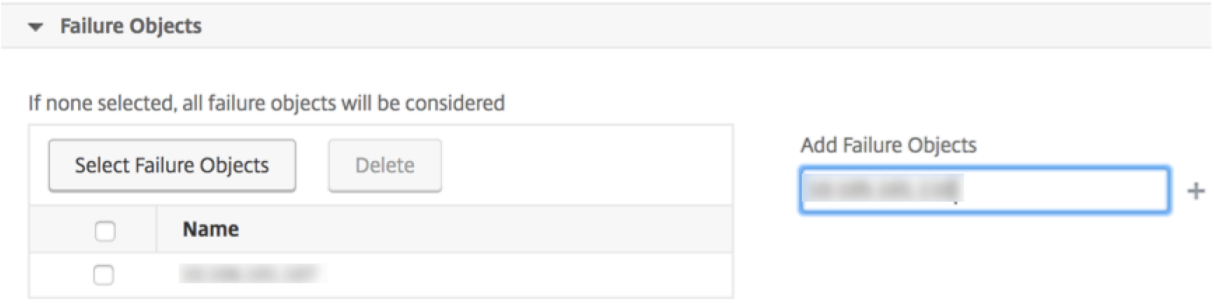
ステップ **5-**障害オブジェクトの選択

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問題が反映されるようにします。このフィルターを使用すると、障害オブジェクト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。

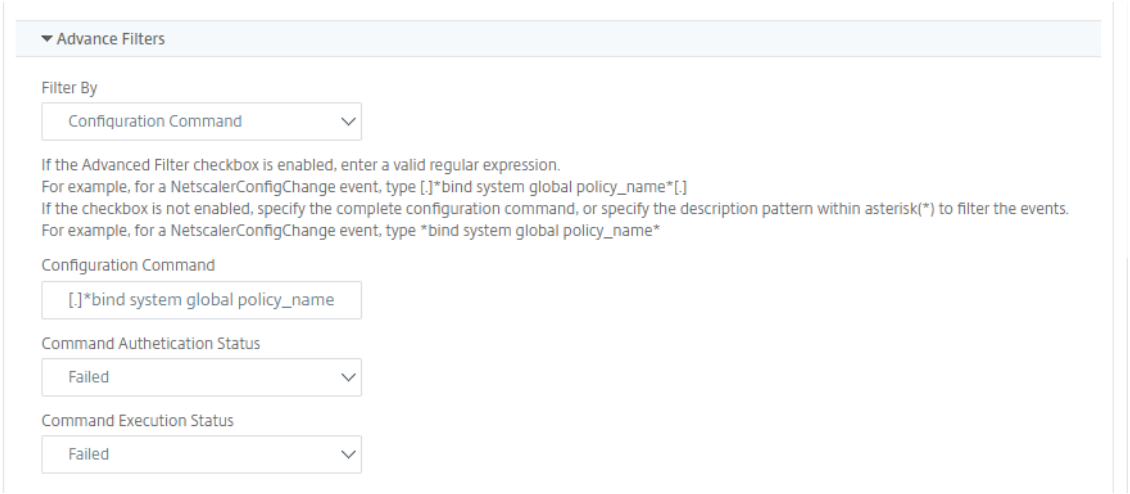


ステップ **6-**高度なフィルタを指定する

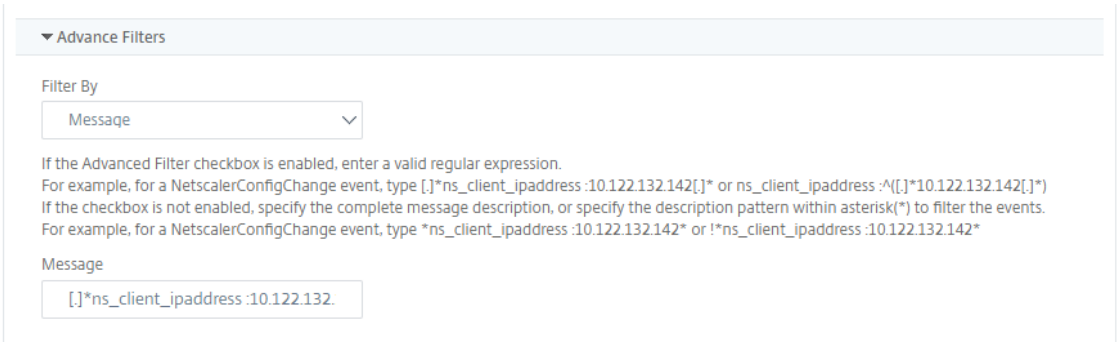
イベント規則は以下の基準によりフィルタリングできます。

- 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。



- 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。



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

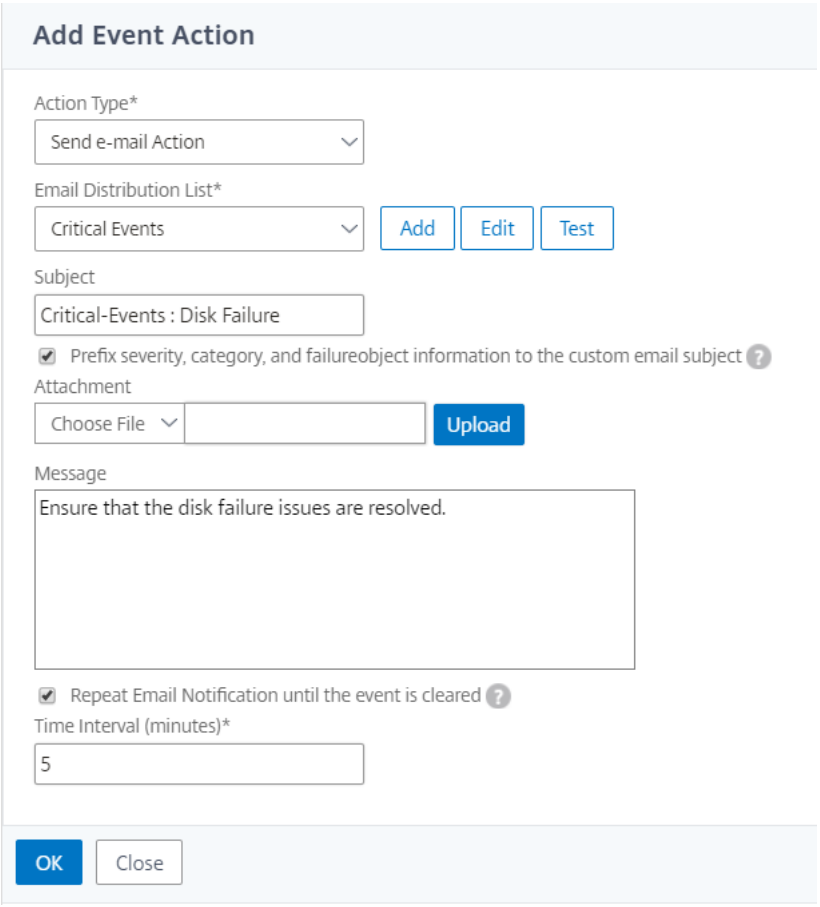
Send email Action イベントアクションタイプを選択すると、イベントが定義されたフィルター条件を満たすと E メールがトリガーされます。メールサーバーまたはメールプロファイルの詳細を指定してメール配布リストを作成するか、以前に作成したメール配布リストを選択する必要があります。

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、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。



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	障害オブジェクトはイベントの処理方法に影響を与え、障害オブジェクトに通知されたとおりの問題を反映するようにします。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。

```
#!/bin/sh
source=$1
failureobj=$2
payload='{
"params":{
"warning":"YES" }
,"lbvserver":{
"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","
   port":"80","td":"","m":"IP","state":"ENABLED","rhistate":"
   PASSIVE","appflowlog":"ENABLED","
bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":"" }
 }
'
url="http://$source/nitro/v1/config/lbvserver"
curl --insecure -basic -u nsroot:nsroot -H "Content-type:
   application/json" -X POST -d $payload $url

```



```
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。

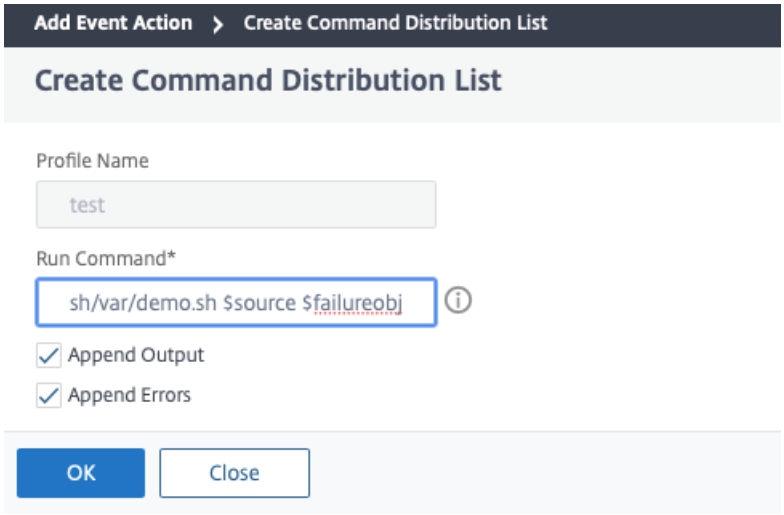
   b) ［コマンドの実行］で、スクリプトを実行する NetScaler ADM エージェントの場所を指定します。例：/sh/var/demo.sh $source $failureobj。

   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。

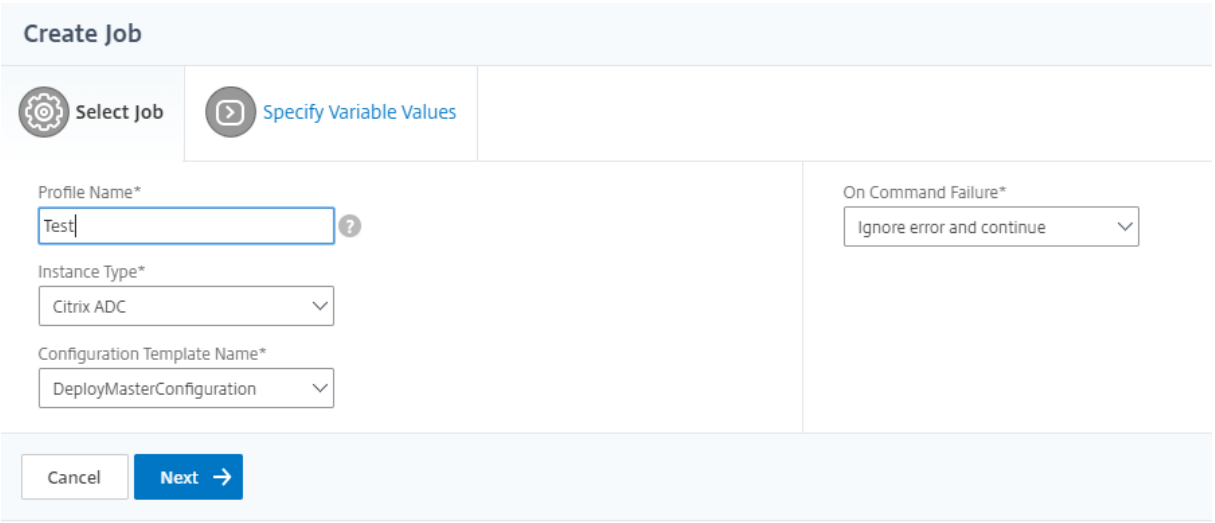


> 注
>
> コマンドスクリプトの実行時に生成された 出力 と エラー（存在する場合）を **NetScaler ADM** サーバーのログファイルに保存する場合は、[**Append** Output] オプションと [Append Errors] オプションを有効にできます。これらのオプションを有効にしないと、NetScaler ADM はコマンドスクリプトの実行中に生成されたすべての出力とエラーを破棄します。

Execute ジョブアクションを設定するには

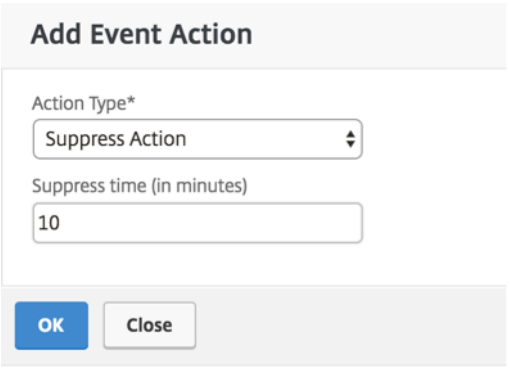
構成ジョブを含むプロファイルを作成すると、指定したフィルター条件に一致するイベントやアラームに対して、NetScaler および NetScaler SDX インスタンスの組み込みジョブまたはカスタムジョブとしてジョブが実行されます。

1. [イベントルールアクション] 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ー条件を満たしたときに実行するジョブを含むプロファイルを作成します。
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。



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。



NetScaler ADM から **Slack** 通知を設定するには

NetScaler ADM GUI でプロファイル名と Webhook URL を指定して、必要な Slack チャネルを構成します。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. NetScaler ADM で、［インフラストラクチャ］**>**［イベント］**>**［ルール］に移動し、［追加］をクリックしてルールを作成します。
2. 「ルールの作成」ページで、重要度やカテゴリなどのルールパラメータを設定します。監視する必要のある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/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK
6. [**Create**] をクリックし、[**Add Event Action**] ウィンドウで [**OK**] をクリックします。

> 注**:**
>
> [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 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 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 にログオンします。
2. 設定 **>** 通知 **> PagerDuty** プロファイルに移動します。

3. [追加] をクリックして、新しいプロファイルを作成します。
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 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 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、NetScaler ADM の 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

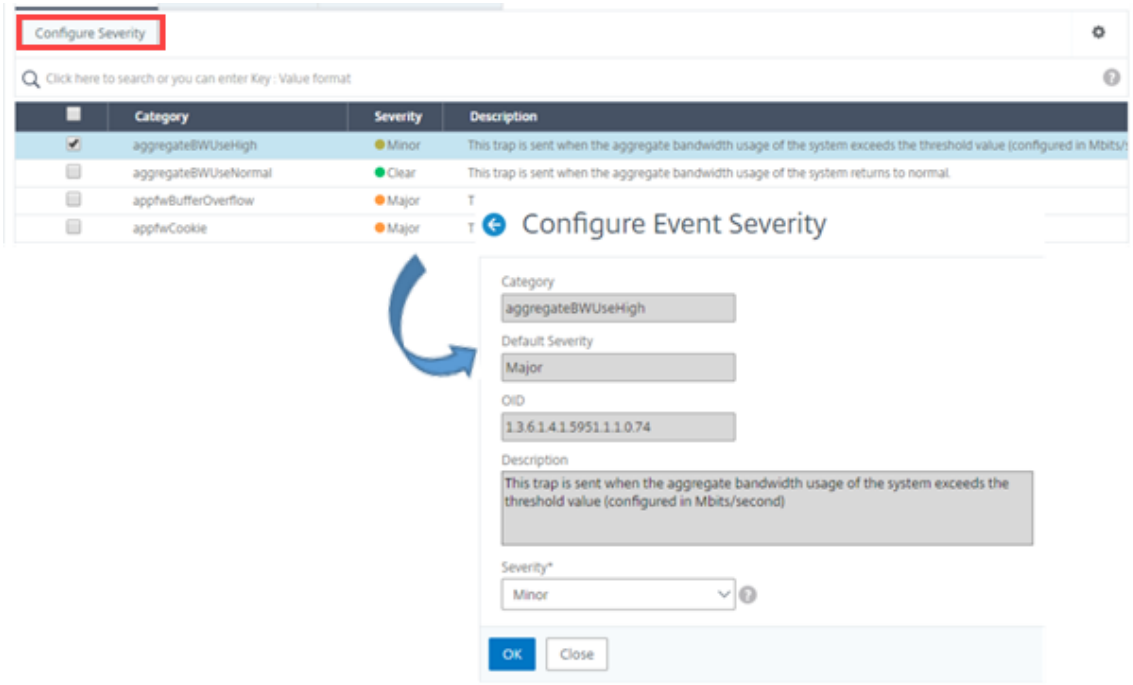
February 6, 2024

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. [インフラストラクチャ**] > [**イベント**] > [**イベント設定**]** に移動します。
2. 変更する 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。

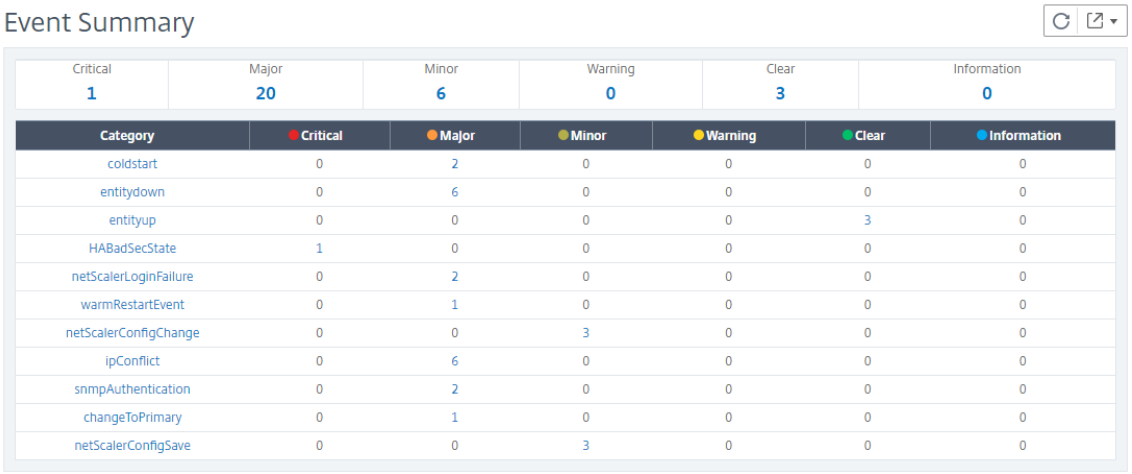


イベントの概要の表示

February 6, 2024

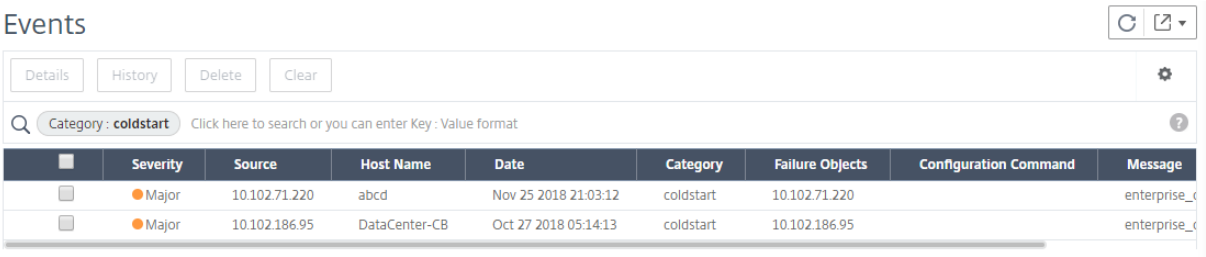
［イベントの概要］ページを表示して、NetScaler Application Delivery Management（ADM）サーバーで受信したイベントとトラップを監視できるようになりました。インフラストラクチャ **>** イベントに移動します。［Events Summary］ページには、以下の情報が表形式で表示されます。

- **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。



- 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に選択されます。このページには、NetScaler インスタンスの IP アドレスとホスト名、トラップを受信した日付、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。



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

NetScaler Application Delivery Management （ADM）でイベントとその設定を作成すると、イベント概要ページでそのイベントをすぐに表示できます。同様に、NetScaler ADM サーバーに追加されたすべての Citrix Application Delivery Controller（ADC）インスタンスのヘルス、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 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

ク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。

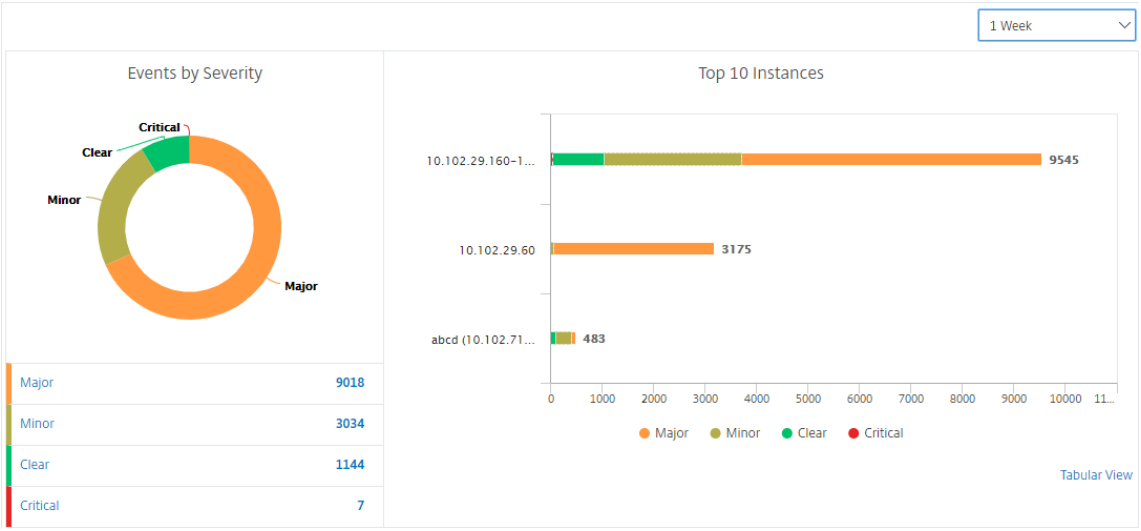
同様に、このダッシュボードでは、NetScaler VPX インスタンスの正常性を表示できます。インスタンスが稼働していた時間をマスクし、インスタンスが稼働停止していた時間のみを表示できます。グラフをクリックすると、そのインスタンスのページが表示され、サービス外 フィルタが既に適用され、ホスト名、1 秒あたりに受信した HTTP リクエストの数、CPU 使用率などの詳細が表示されます。インスタンスを選択し、特定の Citrix インスタンスのダッシュボードで詳細を確認することもできます。

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. インフラストラクチャ **>** ダッシュボードに移動します。

   または

   インフラストラクチャ **>** イベント **>** レポートに移動します。
3. ページの右上隅のメニューから、重大度別にイベントを表示する期間を選択します。

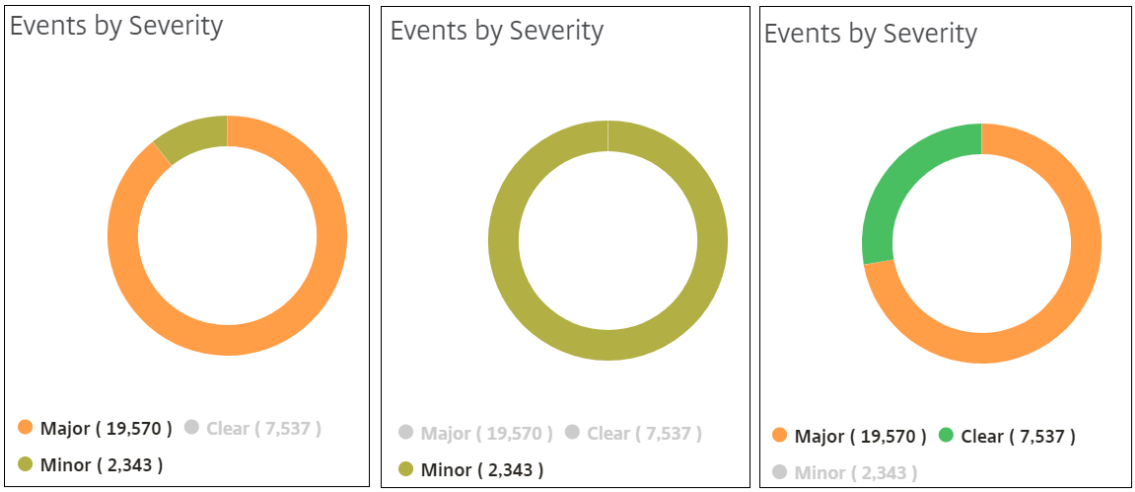


4. [**Events by Sev**erity] ドーナツグラフには、すべてのイベントが重要度別に視覚的に表示されます。異なる種類のイベントは異なる色が付いたセクションとして表され、各セクションの長さは、その種類の重要度の合計イベント数に対応しています。
5. ドーナツグラフの各セクションをクリックすると、対応する「重大度ベースのイベント」ページが表示されます。このページには、選択した期間における選択した重要度に関する次の詳細が表示されます。

   - インスタンスのソース
   - イベントの日付

- NetScaler 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。[インフラストラクチャ**] > [**イベント**] > [**イベント設定**]** に移動します。インスタンスから受信した特定のトラップについては、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 Syslog メッセージの表示とエクスポート

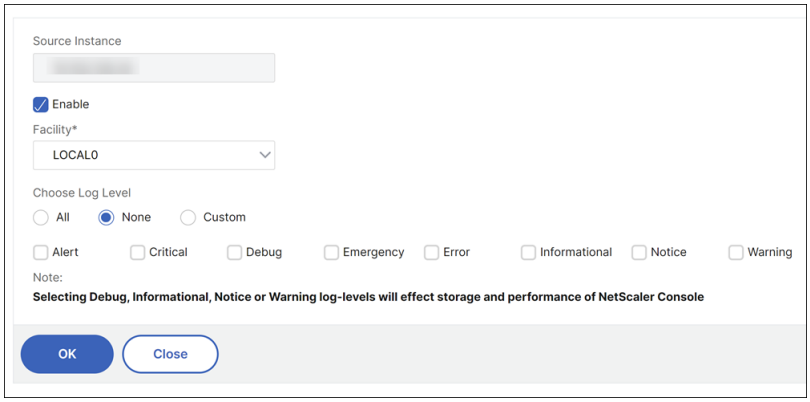
February 6, 2024

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 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、[インフラストラクチャ**] > [**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 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。

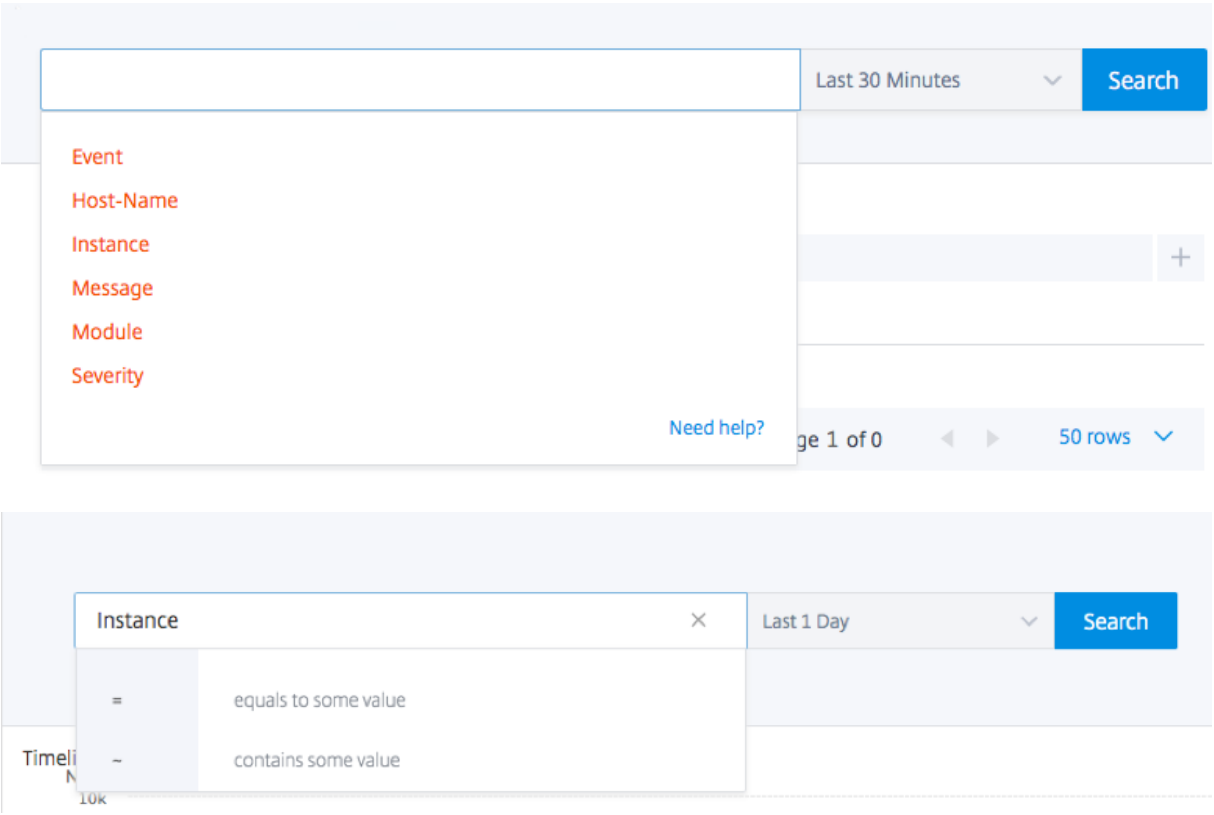


以下の手順では、NetScaler インスタンス内のすべての syslog コマンドを構成し、NetScaler ADM が syslog メッセージの受信を開始します。

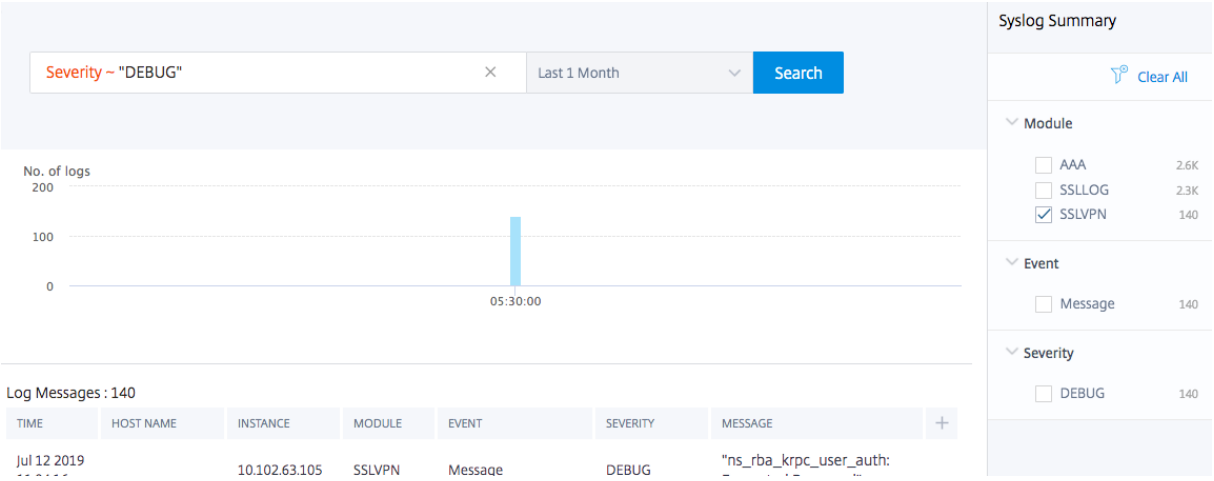
syslog メッセージの表示と検索

管理対象 NetScaler インスタンスで生成されたすべての syslog メッセージを表示できます。syslog メッセージはデータベースに一元的に保存され、[インフラストラクチャ**] > [**イベント**] > [Syslog** メッセージ] で監査目的で使用できます。このログ情報を組み合わせて、収集されたデータから分析用のレポートを生成できます。

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。

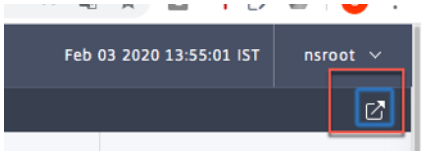


syslog メッセージのエクスポートとスケジュール設定

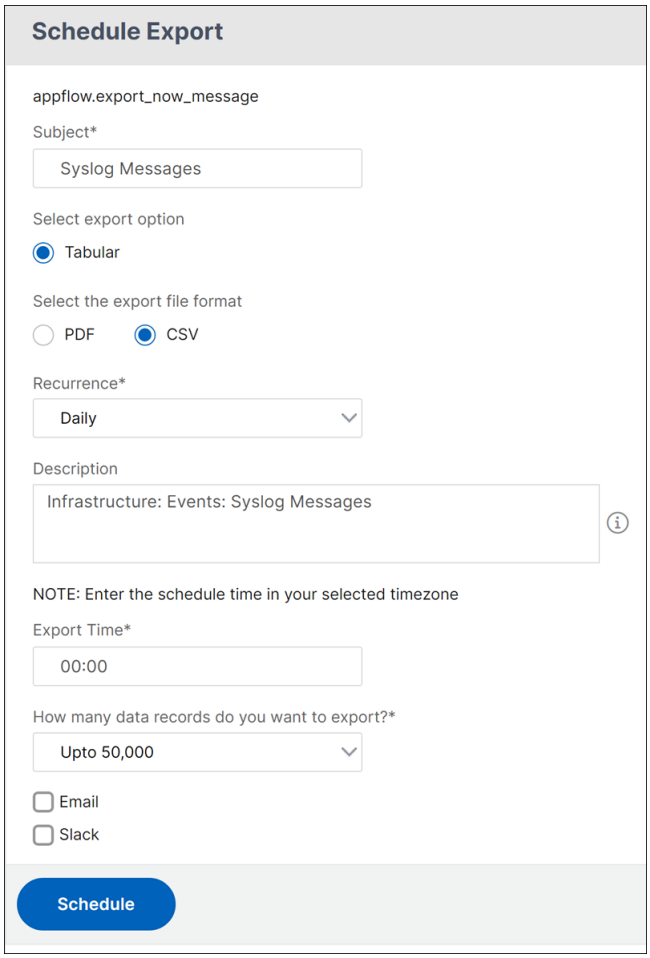
サーバで受信したすべての syslog メッセージのエクスポートをスケジューリングすることで、ADM にログインせずに syslog メッセージを表示できます。ADC インスタンスで生成された syslog メッセージを PDF、CSV、PNG、お

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。



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、NetScaler Application 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。NetScaler 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。NetScaler 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

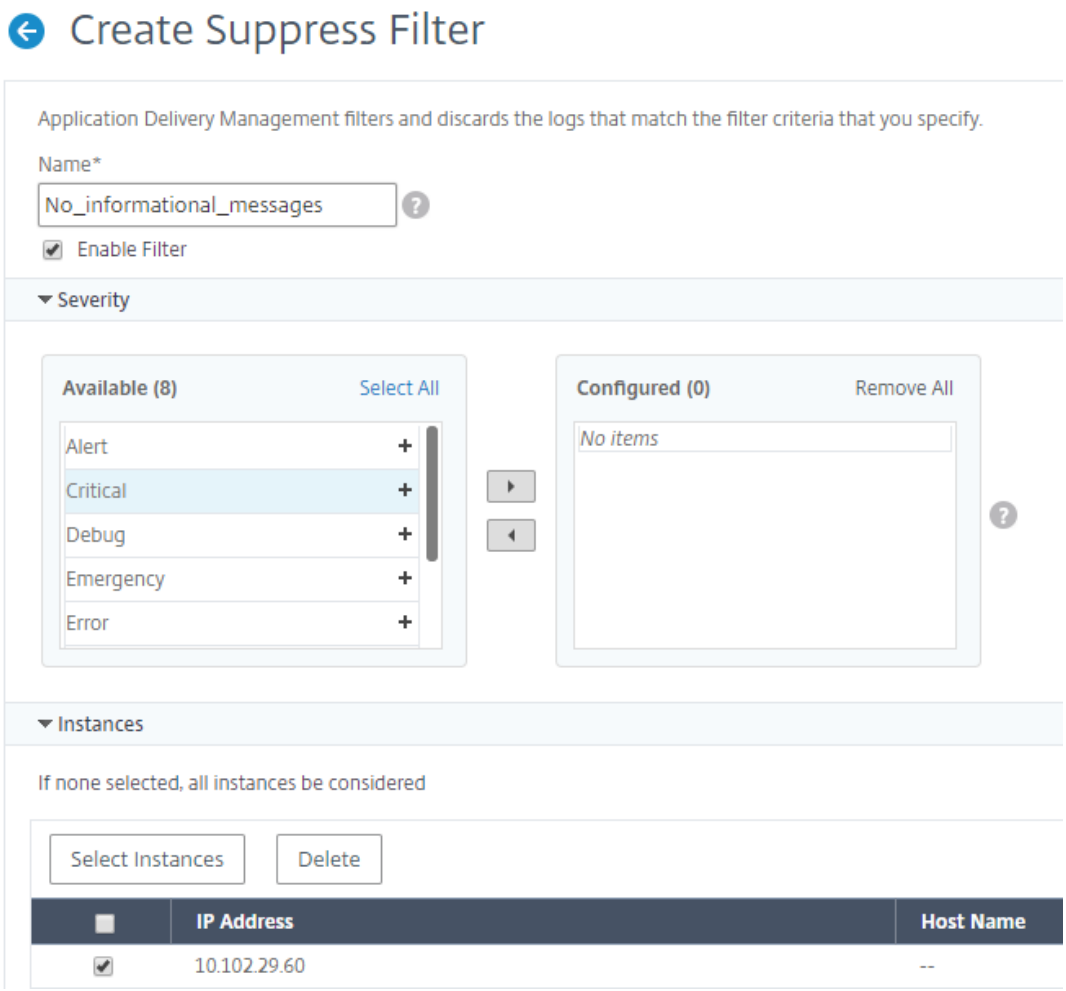
1. NetScaler ADM で、インフラストラクチャ **>** イベント **> Syslog** メッセージ > フィルターの抑制に移動します。
2. 「抑制フィルタの作成」ページで、次の情報を更新します。

    a) 名前 -フィルター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。

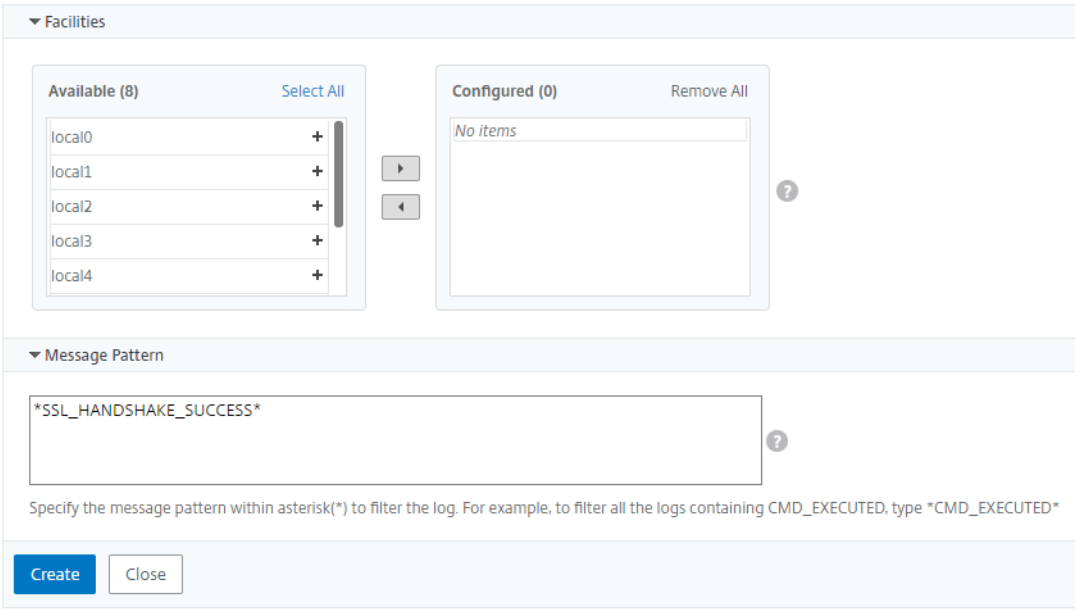
b) 重要度 -メッセージを非表示にする必要があるログレベルを選択して追加します。たとえば、受信した情報メッセージを表示する必要がない場合は、［Informational］を選択してそれらのメッセージを非表示にします。

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。



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. [インフラストラクチャ**] > [**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

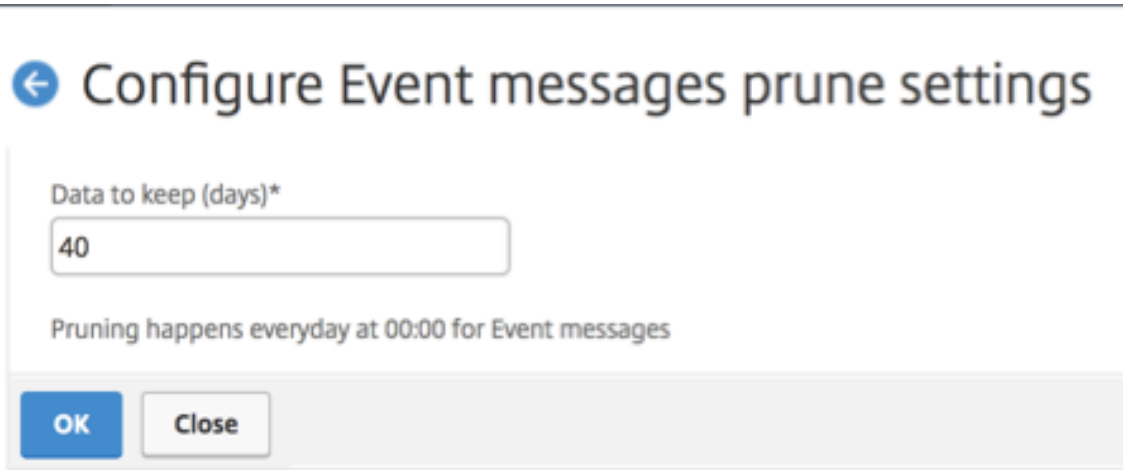
NetScaler Application Delivery Management （ADM）サーバーによって管理される Citrix アプリケーション Delivery Controller（ADC）インスタンスは、イベントメッセージデータを継続的に送信し、NetScaler ADM に保存します。NetScaler ADM でネットワークレポートデータ、イベント、監査ログ、タスクログを保持する間隔を指定できます。デフォルトでは、これらのデータは 24 時間ごとに（00:00 の時刻に）削除されます。

> 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. 「プルーニング設定」で、「インスタンスイベント」**>**「プルーニング設定」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。



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

NetScaler Application Delivery Management （ADM）では、あらゆるレベルの 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 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 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。

NetScaler IP Address	NetScaler HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:
[redacted]	[redacted]		Load Balancing	ADM-Test-LB3#10.1.1.3:80			
[redacted]	[redacted]		Load Balancing	334-lb#1.33.2.2:80			
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b1a9-26ca3			33f97d16-0413-4e6e-9f3d-84
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8404-b5b6			33f97d16-0413-4e6e-9f3d-84
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-99e1-6703			33f97d16-0413-4e6e-9f3d-84
[redacted]	[redacted]		Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		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：NetScaler インスタンスの IP アドレスがレポートに表示されます
- **NetScaler** ホスト名：ホスト名がレポートに表示されます。
- パーティション: 管理パーティションの IP アドレスが表示されます。
- 仮想サーバー:<name_of_the_virtual_server>#virtual_IP_address: port_number
- サービス:<name_of_the_service>#service-IP_Address: Port_Number
- サービスグループ:<name_of_service_group>#Server_Member1_IP_Address: Port、server_Member2_IP_Addre
  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 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のレポートをダウンロードできます。

NetScaler ADM では、レポートを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、[インフラストラクチャ**] > [**ネットワーク機能**] > [**負荷分散**]** に移動します。
2. [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。

> 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. NetScaler ADM で、[インフラストラクチャ**] > [**ネットワーク機能**] > [**負荷分散**] > [**サービス**]** に移動します。
2. [サービス] ページで、右上隅にある [エクスポート] ボタンをクリックします。
   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に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

NetScaler Application Delivery Management（ADM）では、負荷分散、コンテンツスイッチング、キャッシュリダイレクト、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 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 仮想サーバー

> 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. [インフラストラクチャー**] > [**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。

   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 IP Address	NetScaler HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:
[redacted]	[redacted]		Load Balancing	ADM-Test-LB3#10.1.1.3:80			
[redacted]	[redacted]		Load Balancing	334-lb#1.33.2.2:80			
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b1a9-26ca3			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8404-b5b6			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-99e1-6703			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing				

   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。

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）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。

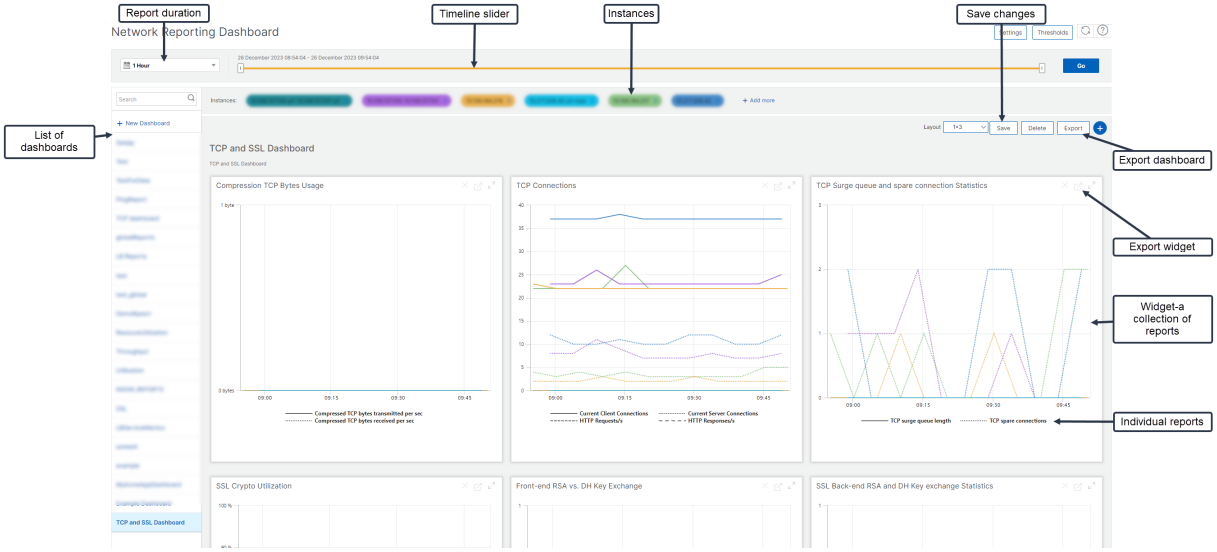
NetScaler ADM では、グローバルレベルのインスタンスだけでなく、仮想サーバーやネットワークインターフェイスなどのエンティティのレポートを生成できるようになりました。インスタンスファミリーは NetScaler インスタンスで構成されます。レポートを生成できる仮想サーバーは次のとおりです。

- 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ー
- 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、仮想サーバー、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。

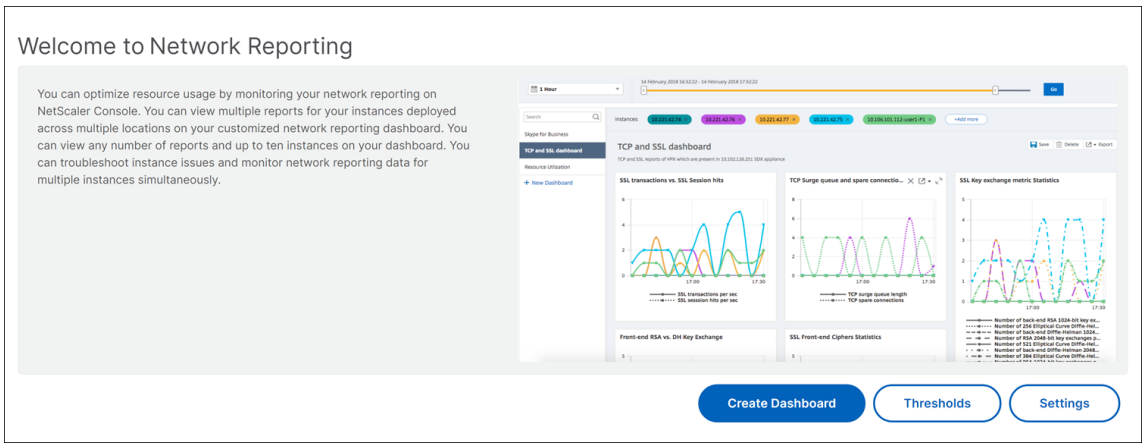
をクリックしてインスタンスを削除するか、レポートにインスタンスを追加できます。しかし、現在、NetScaler ADM では、10 インスタンスのレポートを表示できます。

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。

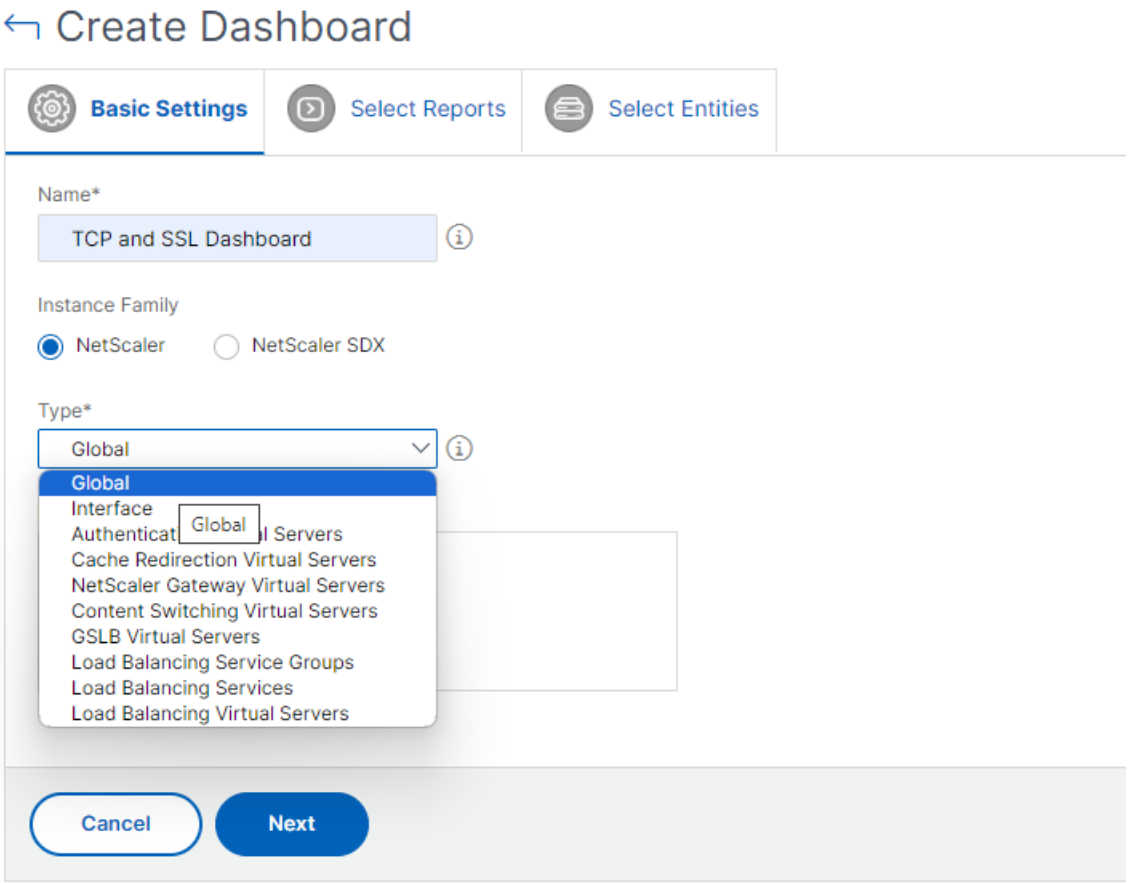
次のセクションでは、ダッシュボードの作成、レポートの生成、およびレポートのエクスポートのタスクについて詳しく説明します。

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、［インフラストラクチャ］**>**［ネットワークレポート］に移動します。



2. 既存のダッシュボードを表示するには、[ダッシュボードの表示] をクリックします。[ネットワークレポートダッシュボード] 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。



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。

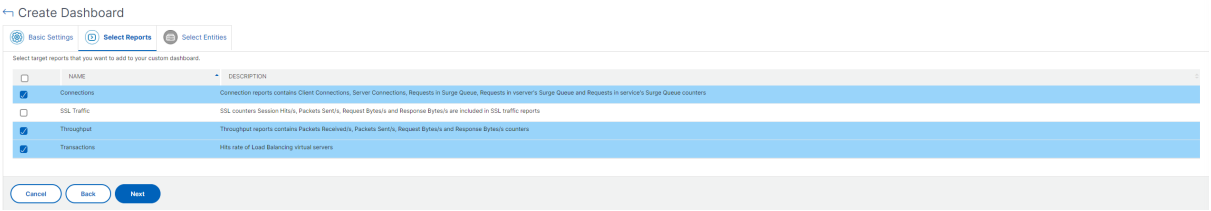
b) インスタンスファミリー。インスタンスのタイプ（NetScaler または NetScaler SDX）を選択します。

c) タイプ。レポートを生成するエンティティタイプを選択します。この例では、負荷分散仮想サーバーを選択します。

d) **[**説明]。ダッシュボードの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。

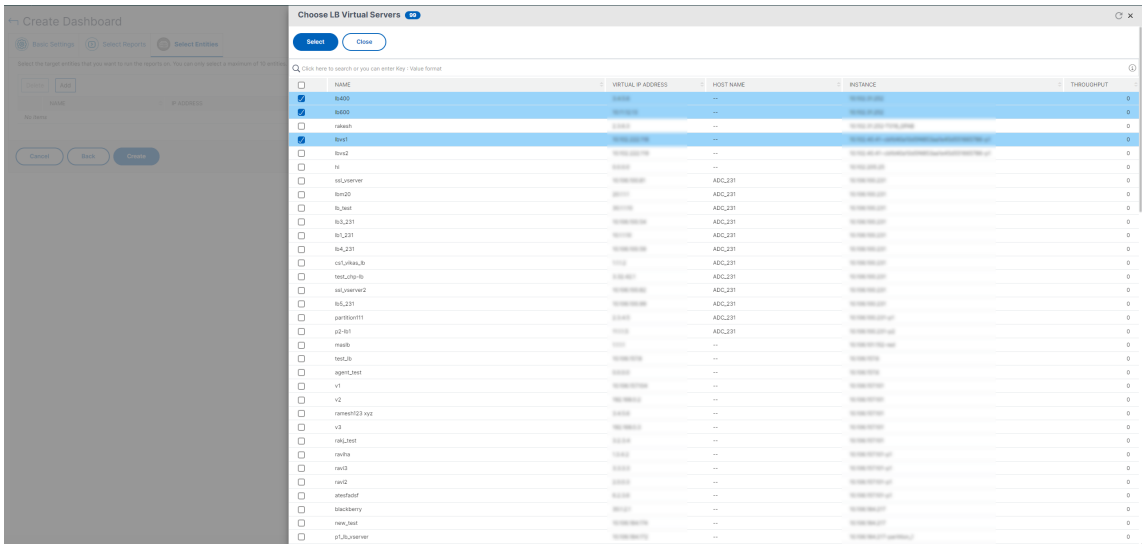
6. **[** レポートの選択] タブで、必要なレポートを選択します。この例では、トランザクション、接続、スループットを選択できます。［次へ］をクリックします。



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。



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. インフラストラクチャ **>** ネットワークレポートに移動します。
2. [ダッシュボードの表示] をクリックして、作成したすべてのダッシュボードを表示します。
3. 左側のペインで、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。

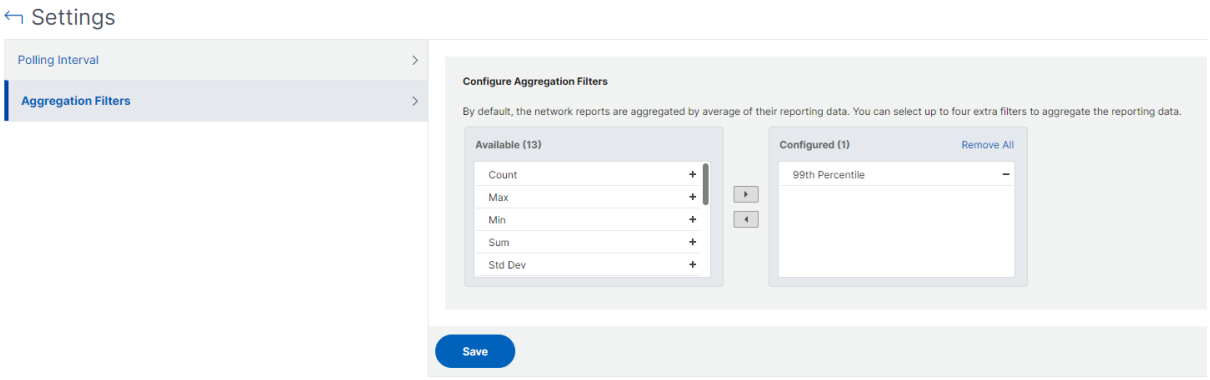
たとえば、特定の仮想サーバからのネットワークレポートの場合、サブジェクトに「認証レポート-10.106.118.120」と入力します。ここで、10.106.118.120 は監視対象の仮想サーバの IP アドレスです。

> 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。

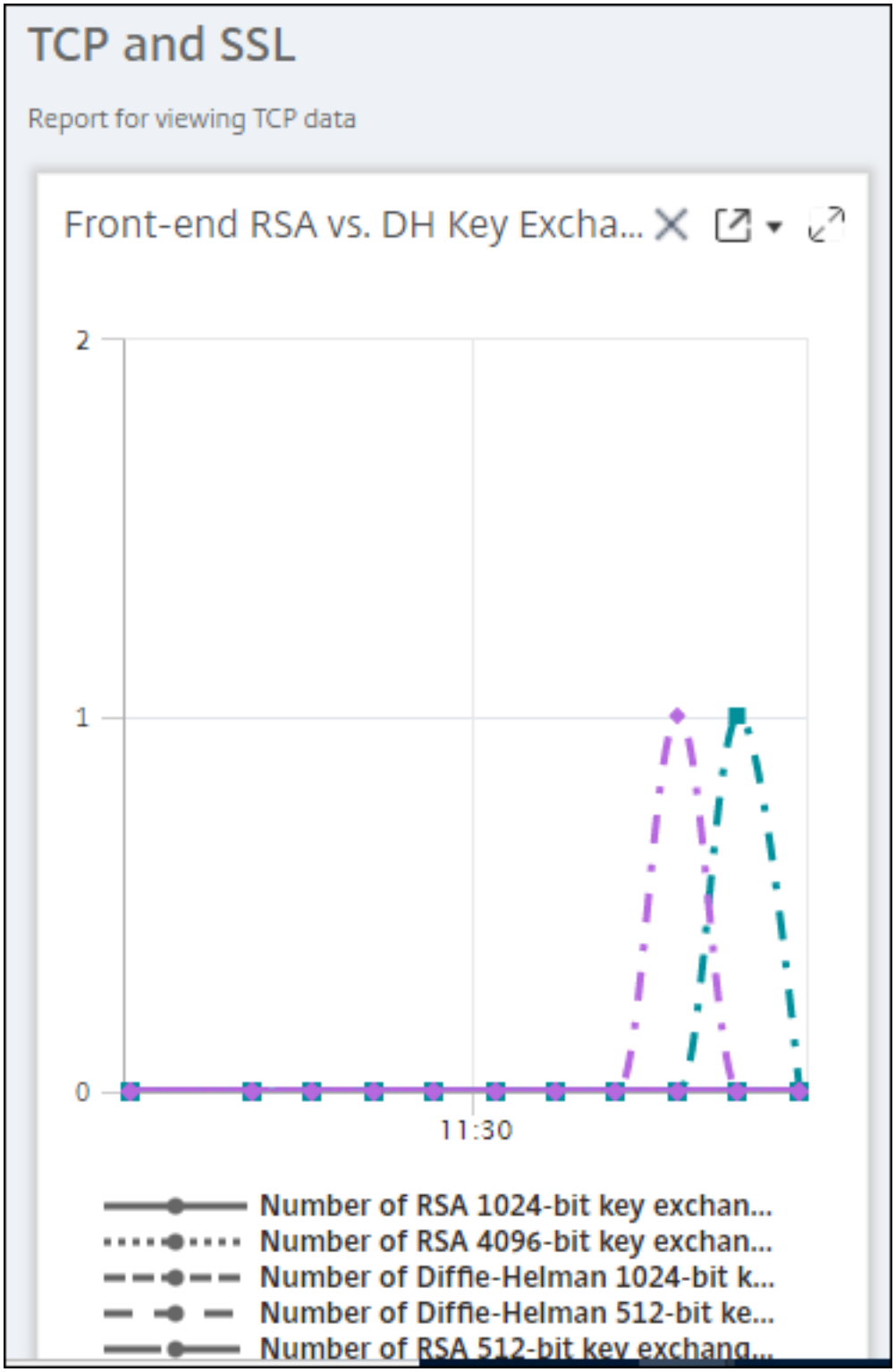
- Count
- 最大
- 最小
- SUM
- 標準開発
- 差異
- Mode
- 中央値
- 第 25 パーセンタイル
- 第 75 パーセンタイル
- 第 95 パーセンタイル

- 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. [インフラストラクチャー**] > [**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 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。これらのイベントを表示するには、[インフラストラクチャ**] > [**イベント**] > [**レポート**]** の順に移動します。「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. NetScaler ADM で、インフラストラクチャ **>** ネットワークレポート **>** しきい値に移動します。[**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 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。

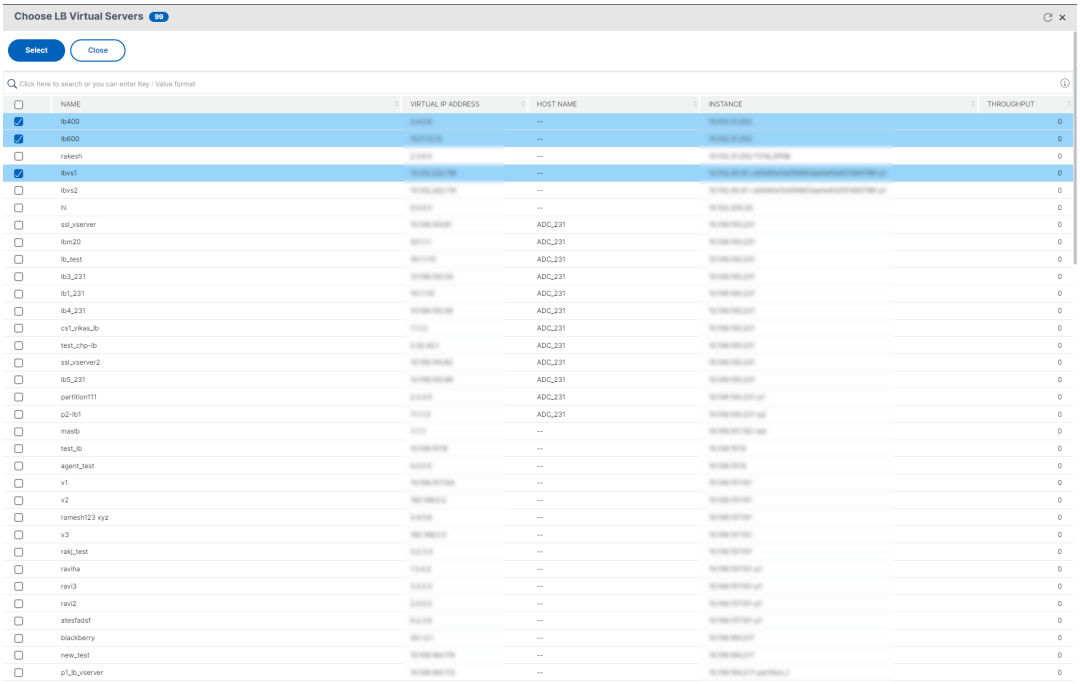
    - メトリック。しきい値を設定する指標を選択します。
    - コンパレータ。比較器を選択して、監視対象値が閾値以上か、それ以下かをチェックします。
    - しきい値。イベントの重要度を計算する基準となる値を入力します。たとえば、現在のクライアント接続の監視対象の値が 80%に達すると、重大なイベント重大度を持つイベントを生成することができます。この場合、しきい値として 80 を入力します。「重大度」イベントを表示するには、[インフラストラクチャ**] > [**イベント**] > [**レポート**]** の順に移動します。「レポート」ページで、「重要度別のイベント」ドーナツをクリックすると、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とエンティティを選択できます。「インスタンス」セクションで、次のいずれかのオプションを選択します。

- すべてのインスタンス。しきい値はすべてのインスタンスに設定されます。
- 特定のインスタンス。しきい値は特定のインスタンスに設定されます。右矢印を使用して、インスタンスを「使用可能」リストから「構成済み」リストに移動します。しきい値は、「構成済み」リスト内のインスタンスに設定されます。
- 特定のエンティティ。しきい値は特定のエンティティに設定されます。

  [追加] をクリックしてエンティティを選択します。

  「レポート名」フィールドで選択したレポートタイプに応じて、エンティティリストがウィンドウに表示されます。この例では、[**LB** 仮想サーバーの選択] ウィンドウが表示されます。



  しきい値を設定するエンティティを選択します。[**Select**] をクリックします。選択したエンティティが「インスタンス」セクションに表示されます。

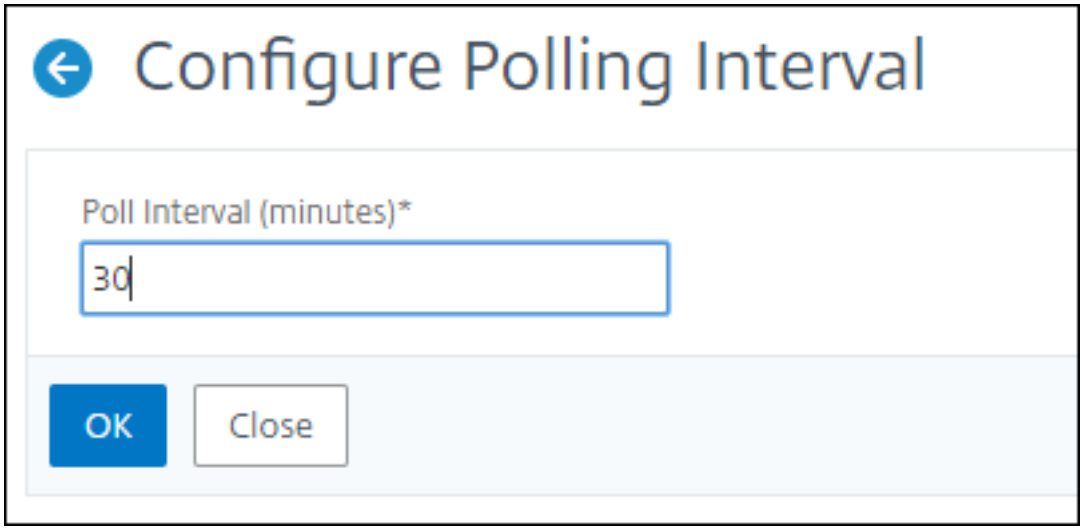
> 注:
>
> 「特定のエンティティ」オプションは、「レポート名」で「仮想サーバーベースのレポート」を選択した場合にのみ表示されます。たとえば、**LB** サービス統計を選択した場合

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、[インフラストラクチャ**] > [**ネットワークレポート] に移動し、[ポーリング間隔の構成] をクリックします。ポーリング間隔は 5 分未満または 60 分を超えることはできません。



ネットワークレポート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 30 日以内、または 1 日未満にすることはできません。

構成ジョブ

February 6, 2024

NetScaler Application Delivery Management （NetScaler ADM）の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）インスタンスにわたって、構成変更、システムアップグレード、およびその他のメンテナンスアクティビティ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

NetScaler 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。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。NetScaler 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-replicate-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. [インフラストラクチャー**] > [**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。構成ジョブの編集中に、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。「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 Instanc** es] 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。

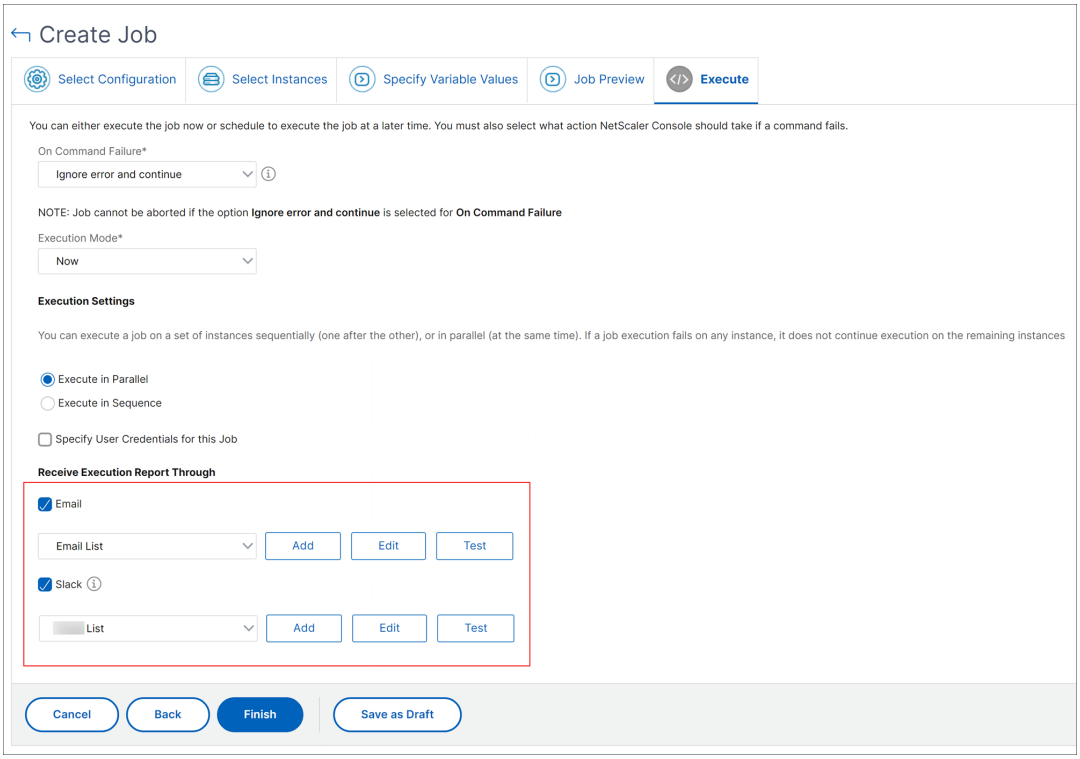
1. インフラストラクチャ **>** 構成ジョブに移動します。
2. メールと Slack 通知を有効にするジョブを選択し、[編集] をクリックします。
3. 「実行」タブの「実行レポートの受信」ペインに移動します。

   - 「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. インフラストラクチャ **>** 構成ジョブに移動します。
2. メールと Slack 通知を有効に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。

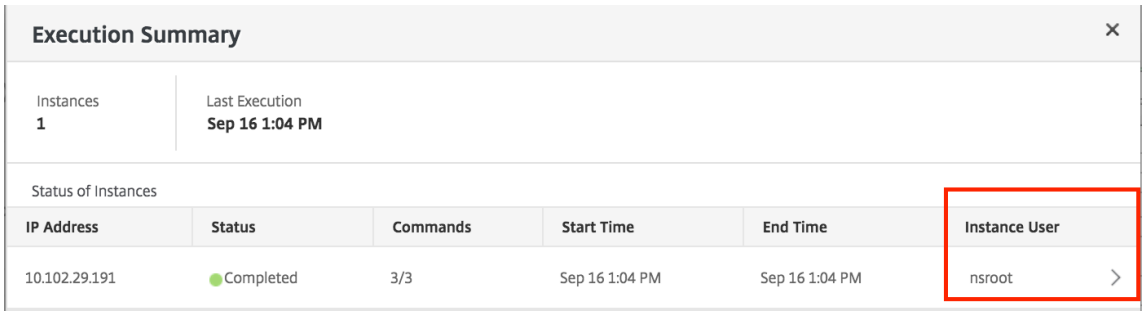
     Slack プロファイルを追加する場合は、[追加] をクリックし、必要な Slack チャンネルのプロファイル名 ******、チャンネル名、****** トークン を指定します。
4. [完了] をクリックします。

実行要約の詳細を表示する手順は、次のとおりです。

1. インフラストラクチャ **>** 構成ジョブに移動します。
2. 実行サマリーを表示するジョブを選択し、「詳細」をクリックします。

3.「実行サマリー」をクリックすると、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



監査レポートを表示する

February 6, 2024

(NetScaler 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、以下をエクスポートできます。

- インスタンスごとの全インスタンスにわたる概要レポート
- 各インスタンスとテンプレートのペアの詳細な差分 (差分) レポート

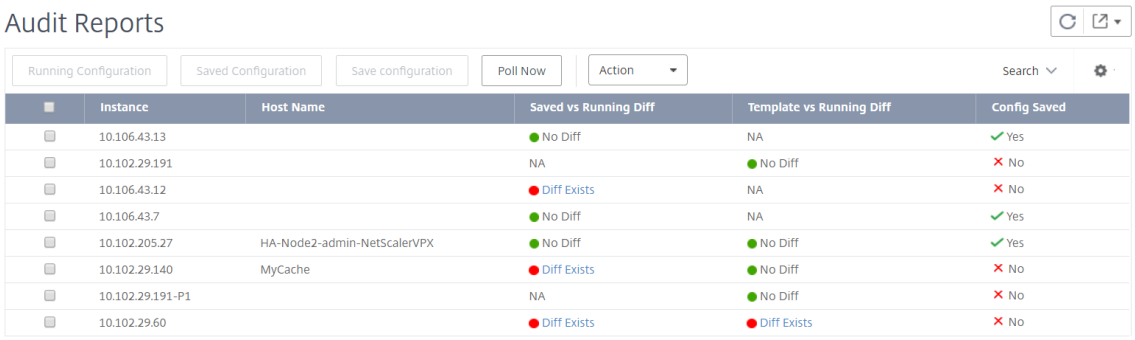
監査テンプレートの監査テンプレートは 、指定されたインスタンスの構成に対してスケジュールされた時間に実行されます。［構成監査］ダッシュボードの ［**NetScaler Config Drift** ］グラフには、保存されていない構成に対して保存された構成の変更に関する詳細な情報が表示されます。**NetScaler** 構成ドリフトチャートを クリックすると、続いて表示される監査レポートページに、「相違あり」と「差分なし」の両方を示すインスタンスのリストが表示されます。NetScaler ADM によって表示される差分レポートをダウンロードできます。

NetScaler ADM には、差分レポートをメールの添付ファイルとして自動エクスポートするようにスケジュールするオプションもあります。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、［インフラストラクチャ］**>**［構成］**>**［構成監査］に移動します
2.［構成監査］ページで、**NetScaler 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。

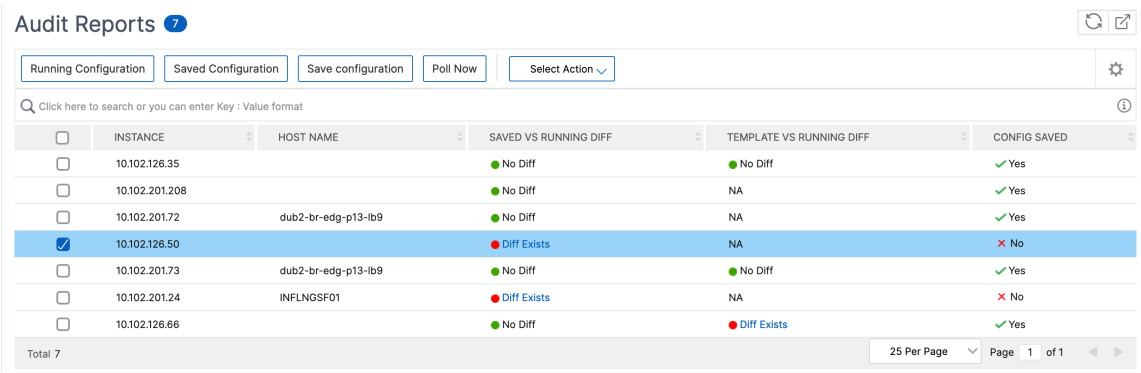


画像では、一部のインスタンスでは差分が 保存済みと実行差分 にのみ存在し、一部のインスタンスでは差分が テンプレートと実行差分にのみ存在することがわかります。場合によっては、保存された差分と実行中の差分とテンプレートと実行中の差分の両方に違いがあります。

保存された差分と実行中の差分比較

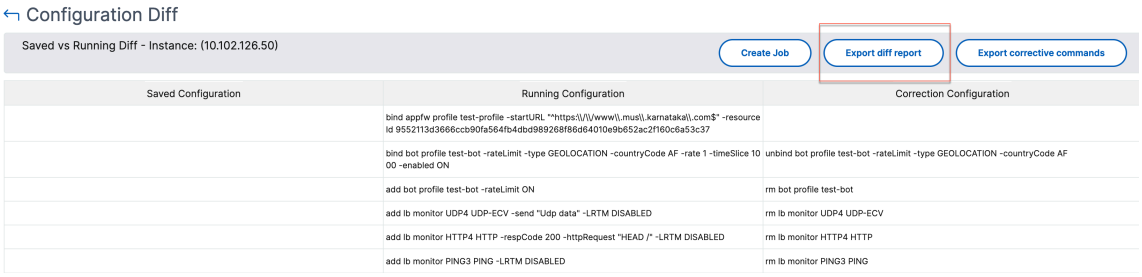
インスタンスに保存されている設定と、インスタンスで現在実行されている設定との差分のレポートを表示できます。

1. [保存された差分] と [実行中の差分] の下にあるインスタンスの [差分が存在 する] をクリックします。



保存された設定のレポートを、そのインスタンスの実行コンフィギュレーション差分と照合して表示できます。

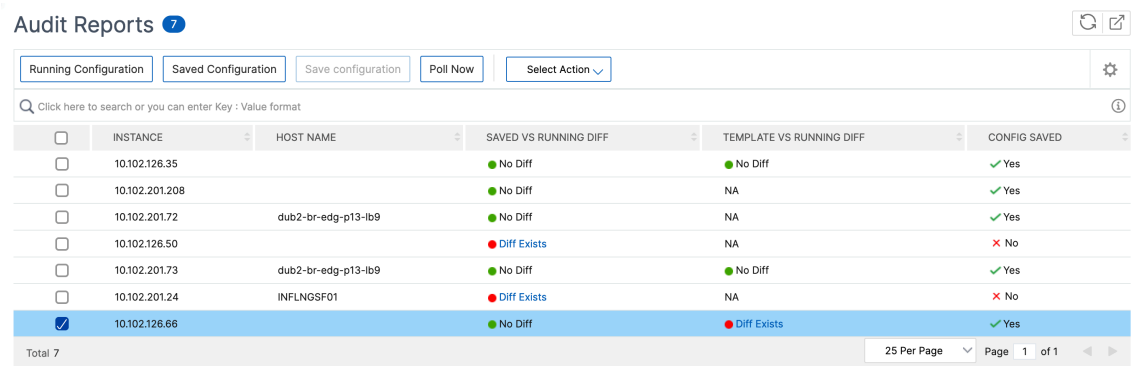
2. [差分レポートのエクスポート] をクリックして、差分レポートの.csv ファイルをダウンロードします。[修正コマンドのエクスポート] をクリックして、コマンドを.txt ファイルにエクスポートすることもできます。その後、関連する NetScaler ADM インスタンスで「構成ジョブ」からコマンドを実行して、そのインスタンスの構成を修正できます。



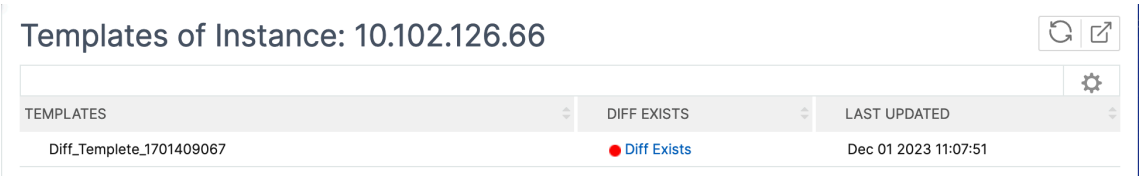
テンプレートと実行中の差分

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コンフィギュレーションの違いを確認できます。

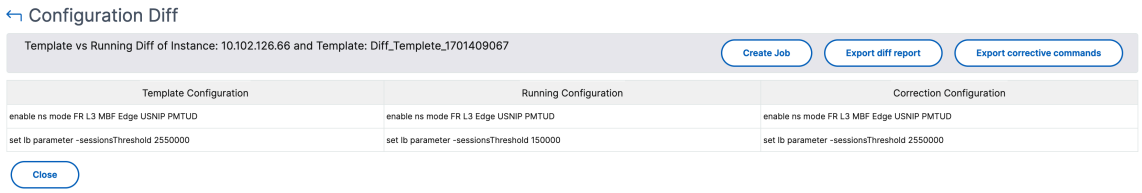
1. [テンプレートと実行中の差分] の下にあるいずれかのインスタンスで **[差分が存在する]** をクリックします。



2. NetScaler ADM インスタンスがテンプレートで指定された構成から外れると、テンプレートによって違いが明らかになります。



3. もう一度「相違が存在する」をクリックします。次の画像は、テンプレートが探している構成、実行中の構成、修正構成、または構成を修正するために実行するコマンドを示しています。実行設定が空白の場合は、コマンドが設定されていないか、削除されたことを意味します。



4. [差分レポートのエクスポート] をクリックして、差分レポートの.csv ファイルをダウンロードします。[修正コマンドのエクスポート] をクリックして、コマンドを.txt ファイルにエクスポートすることもできます。その後、CLI でコマンドを実行してインスタンスの設定を修正できます。

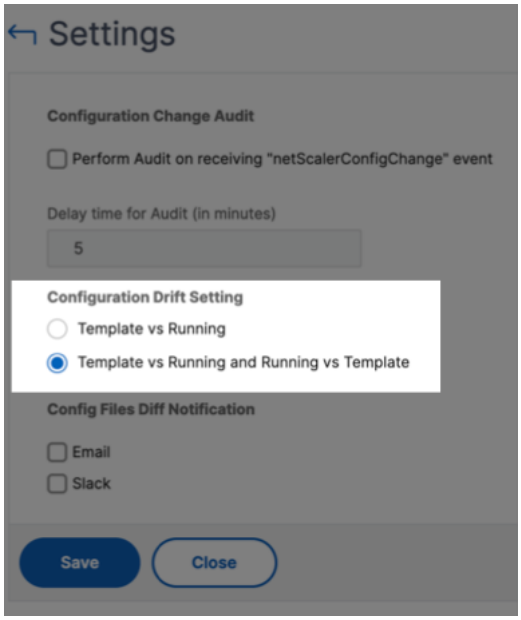
Template_vs_Running_Diff_of_Instance _10.102.126.66_and_Template _Diff_Templete_1701409067

Template Configuration	Running Configuration	Correction Configuration	
enable ns mode FR L3 MBF Edge USNIP PMTUD	enable ns mode FR L3 Edge USNIP PMTUD	enable ns mode FR L3 MBF Edge USNIP PMTUD	
set lb parameter -sessionsThreshold 2550000	set lb parameter -sessionsThreshold 150000	set lb parameter -sessionsThreshold 2550000	

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、テンプレートと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、構成監査ページの「設定」を選択します。



ファイルステータス監査レポートの表示

NetScaler File Status グラフを使用して、フォルダーにファイルが追加、変更、または削除されたかどうかをnsconfig監視します。たとえば、NetScaler インスタンスでライセンスファイルが更新された場合、このファイルの最終更新日を確認して、必要なアクションを実行できます。

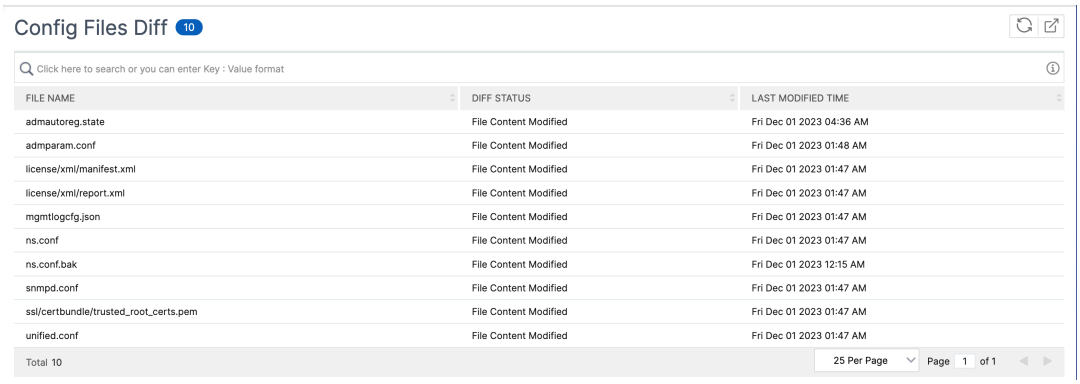
1. インフラストラクチャ **>** 構成 **>** 構成監査に移動します。

2. 「構成監査」ページで、「**NetScaler** 構成ファイルステータス」グラフをクリックします。

   監査レポートページには、Diff ステータスのインスタンスが一覧表示されます。

   Diff 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。

   - 差分あり-このステータスは、前回のポーリング時刻以降、インスタンスのnsconfigフォルダ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。



   - 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が適用されないことを示します。このステータスは、NetScaler ADM がインスタンスをポーリングしない場合に表示されます。たとえば、インスタンスが新しく追加された場合や、インスタンスの状態が非アクティブの場合、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 NetScaler 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のシャットダウン後に保存されていない構成の回復も必要になります。

特定の設定で監査テンプレートを作成して、特定のインスタンスを監査できます。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、構成に不一致があるかどうかを報告します。構成差分レポートにより、望ましくない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は、次の方法で自動化できます。

- テンプレートを実行する必要がある時間をスケジュールします。

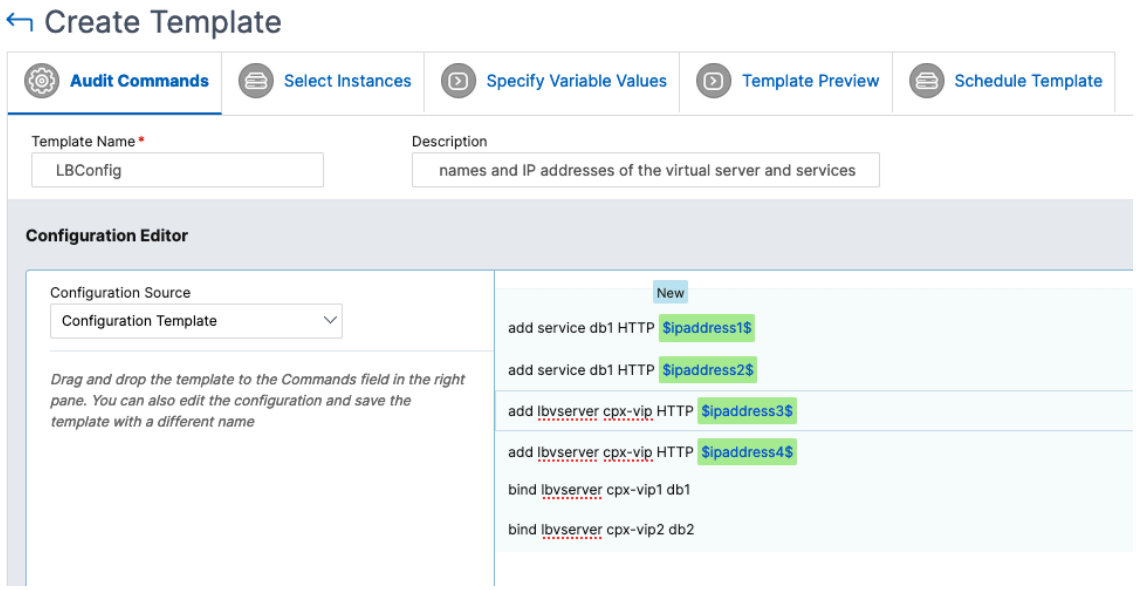
- NetScaler ADM がテンプレートを実行する必要がある頻度の設定。テンプレートは、毎日、週の特定の日、または月の特定の日に実行できます。

NetScaler ADM によって生成された差分レポートを、構成可能な指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の添付ファイルまたは Slack 通知として受け取ることができます。レポートを手動でエクスポートするために NetScaler ADM にログオンする必要はありません。

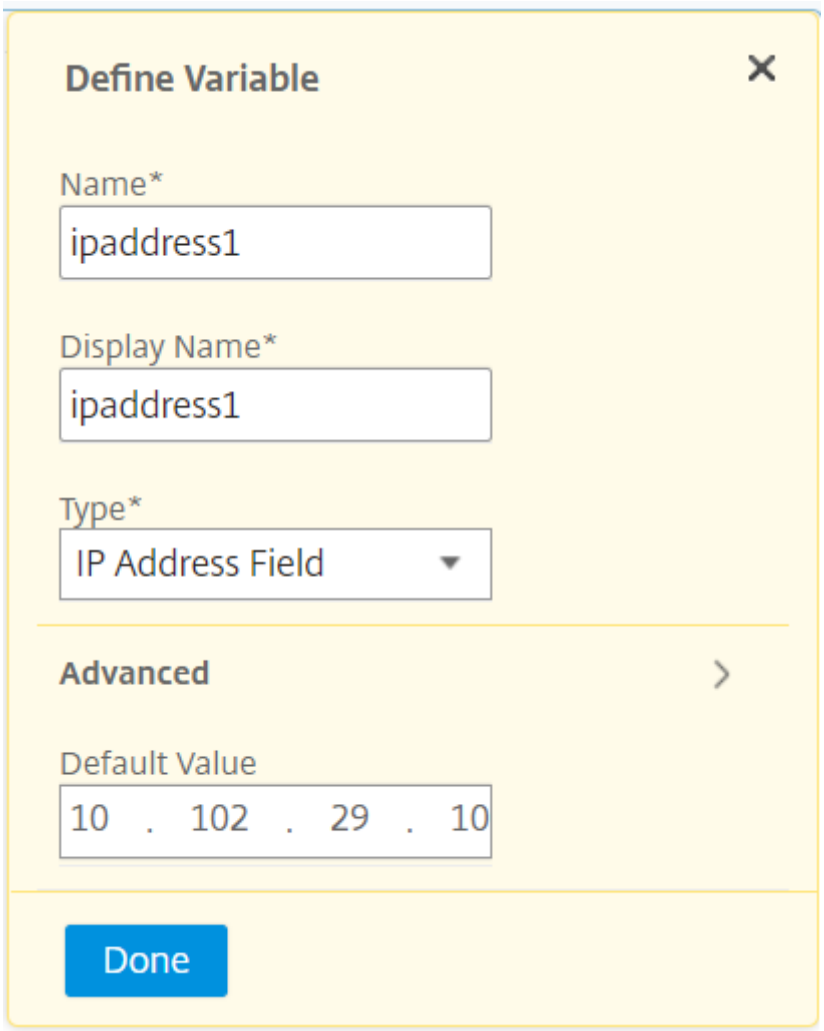
> 注:
>
> デフォルトの設定テンプレートでは、名前変更オプションは無効になっています。ただし、カスタム設定テンプレートの名前は変更できます。

監査テンプレートを作成するには、次の手順に従います。

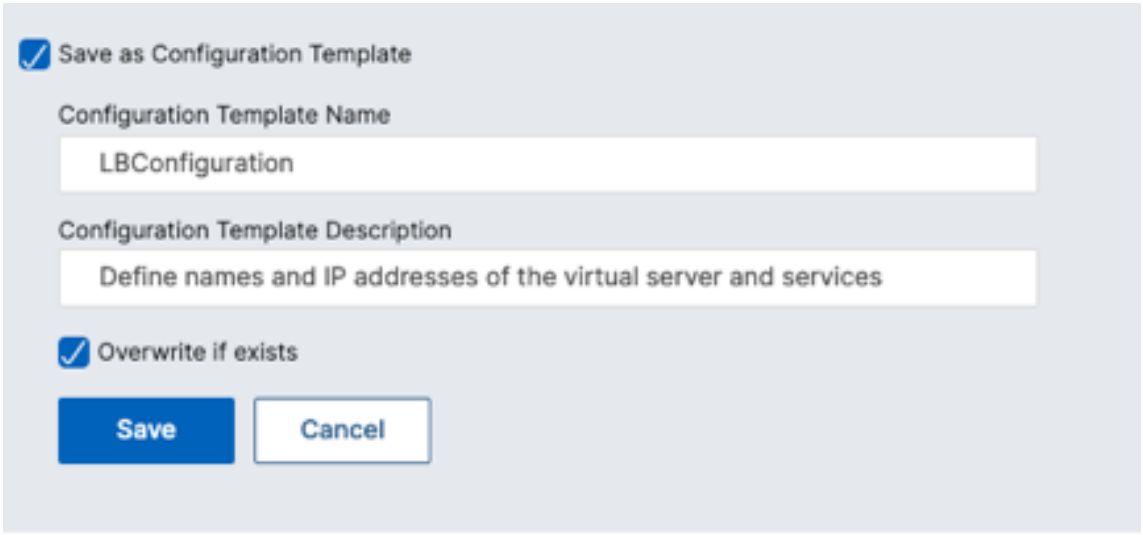
1. [インフラストラクチャ] > [構成] > [構成監査] > [監査テンプレート] に移動し 、[追加] をクリック します。
2. 「テンプレート の 作成」ページと「監査コマンド 」タブで 、テンプレート名とその説明を指定します。
3. [構成エディタ] ページで、コマンドを入力し、コマンドを構成テンプレートとして保存します。既存のテンプレートを左ペインからエディタにドラッグすることもできます。
4. 変数に変換する値を選択し、[変数に変換] をクリックします。たとえば、負荷分散サーバーの IP アドレス「ipaddress1」を選択し、「変数に変換」をクリックします。これで、変数は「$」で囲まれます。



「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。

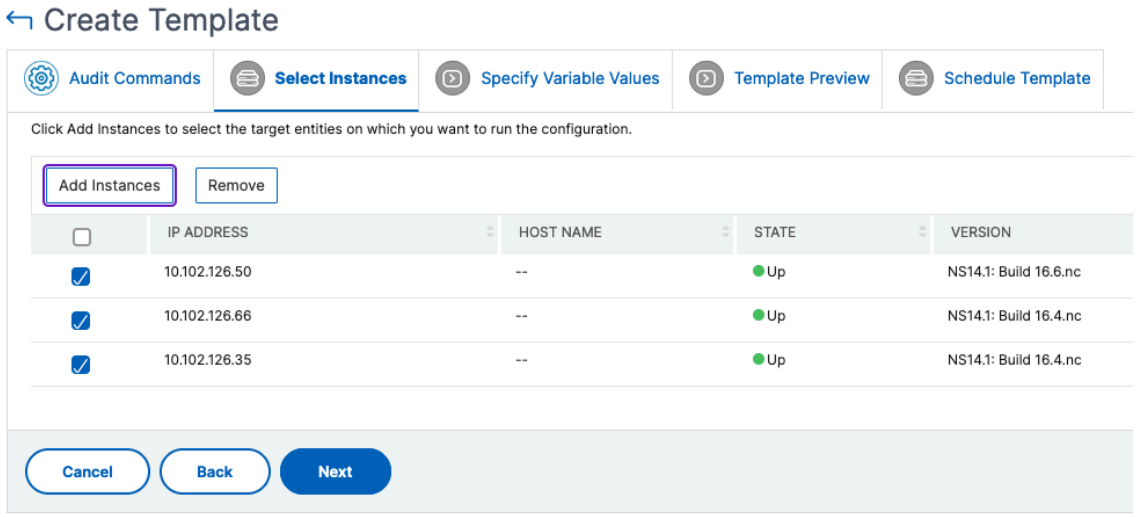


コマンドを構成テンプレートとして保存することもできます。



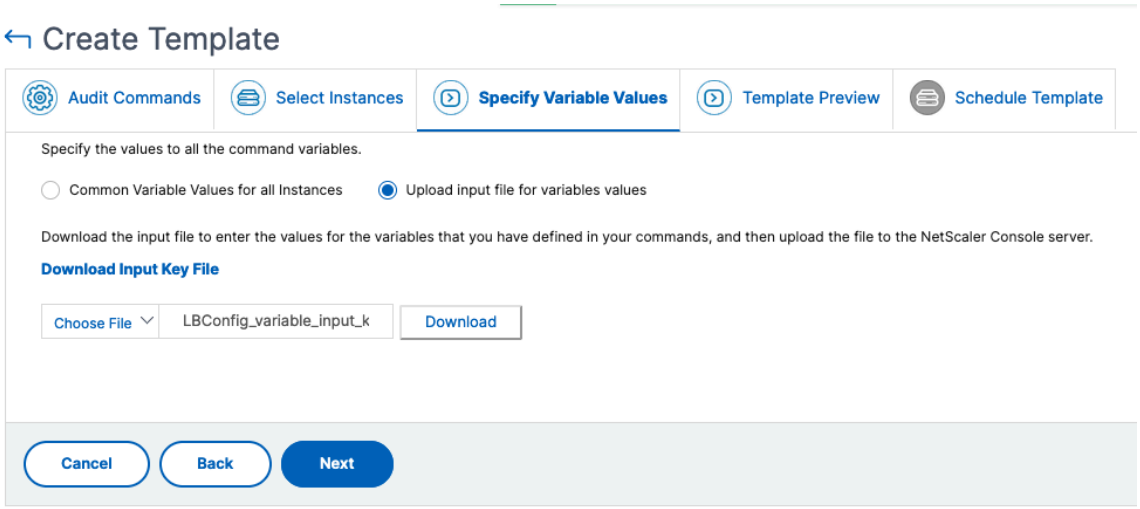
5. [保存] をクリックし、[次へ] をクリックします。

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。

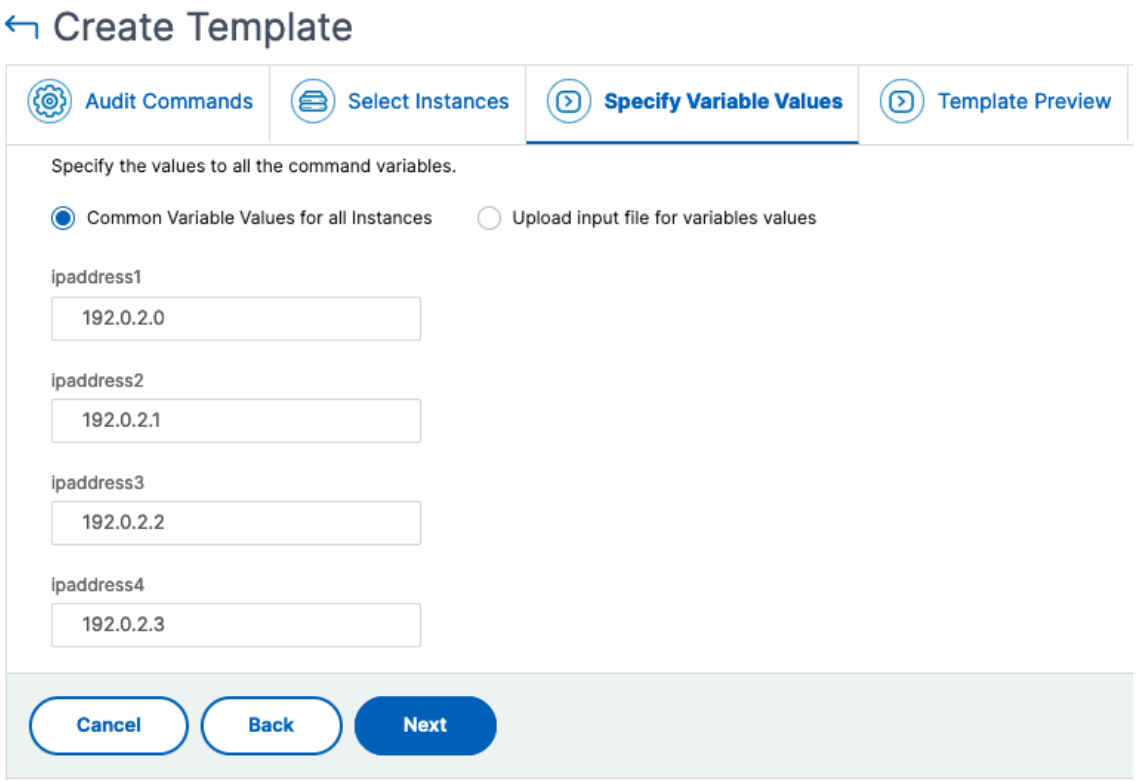


7. [変数値の指定] タブには、次の 2 つのオプションがあります。

   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ます。変数を入力したら、ファイルを NetScaler ADM サーバーにアップロードします。

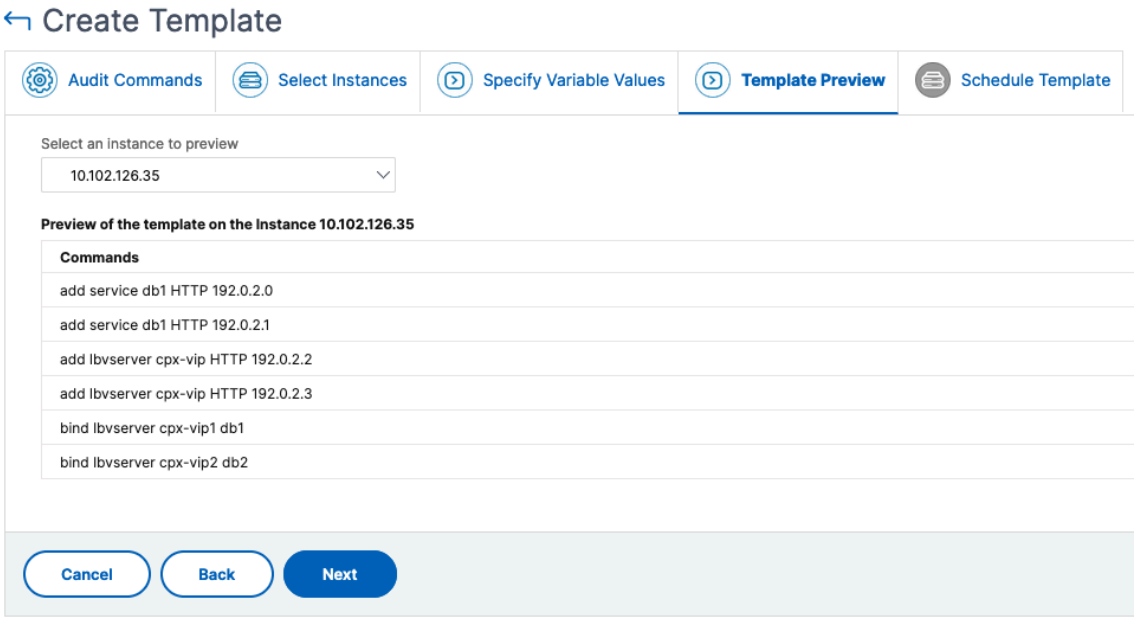


   a) すべてのインスタンスに定義した変数に共通の値を入力します。



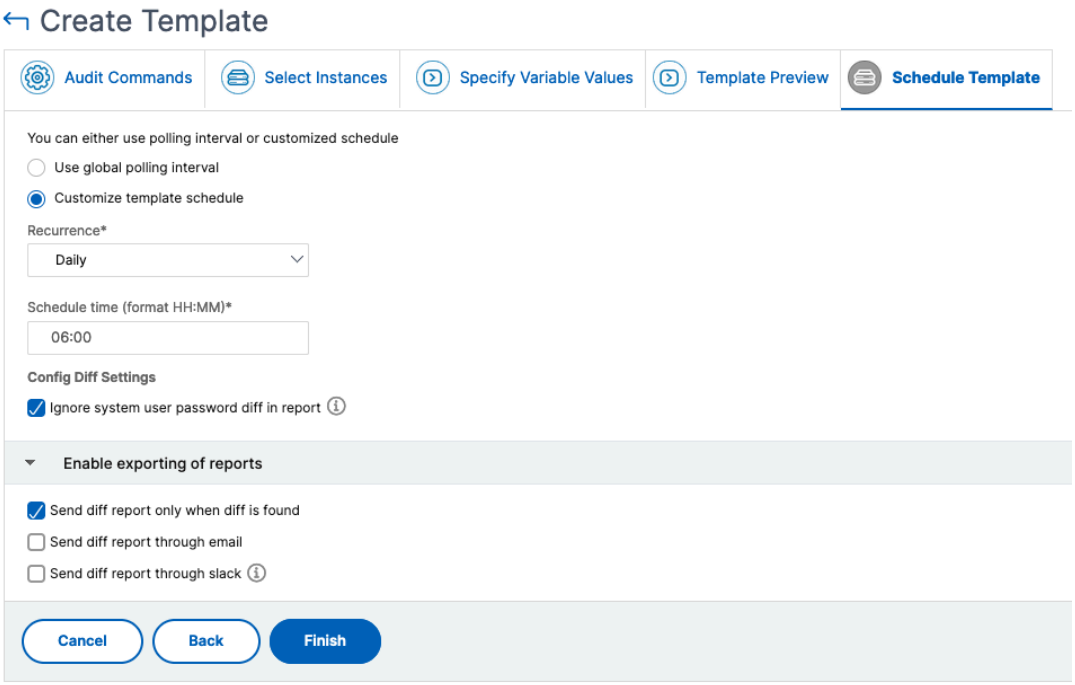
> 注:
>
> 各インスタンスを異なる値で監査する場合は、各インスタンスの入力ファイルに個別の変数を作成する必要があります。

8. [次へ] をクリックします。
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. [**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。
    - 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時間と頻度を設定します。
        - 監査テンプレートを実行する頻度とタイミングを指定します。
    - レポートのエクスポートを有効にします。このオプションを使用して次のことを行います。
        - 差分レポートを送信 **(**差分のみが見つかりました**)**
        - 差分レポートをメールで送信します。差分レポートをメール添付ファイルとして送信する必要があるメールプロファイルを設定します。
        - 差分レポートを **Slack** 経由で送信します。差分レポートを通知として送信する必要がある Slack チャンネルを設定します。



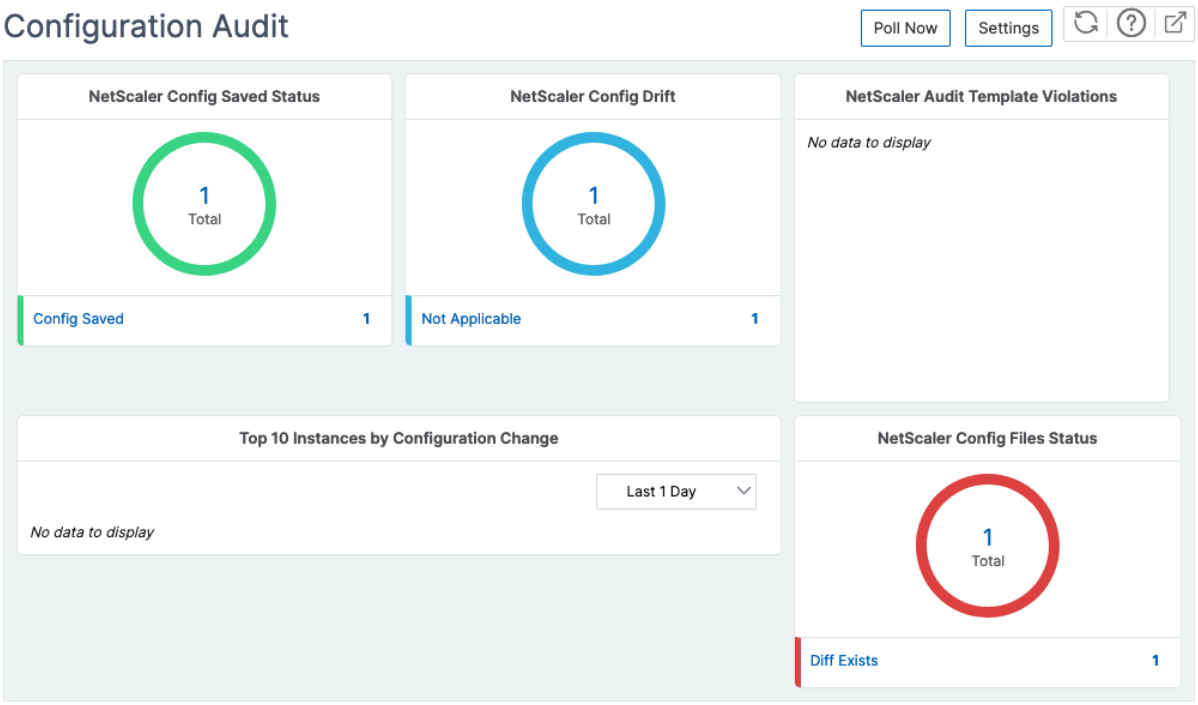
11. ［完了］をクリックします。

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。

構成の変更の表示

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大まか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 個のインスタンス
- 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

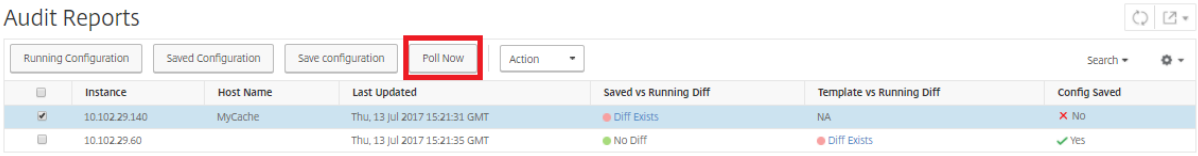


また、NetScaler ADM では、構成監査を手動でポーリングし、インスタンスのすべての構成監査を直ちに NetScaler ADM に追加します。そのためには、[インフラストラクチャ] **>** [構成] **>** [構成監査] に移動し 、[今すぐ投票] をクリックします。ポップアップページの [**Poll Now**] に、ネットワーク内のすべての NetScaler ADC インスタンスをポーリングするか、選択したインスタンスをポーリングするかを選択できます。

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** 構成保存ステータス
- **NetScaler** 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。



NetScaler 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. インフラストラクチャ **>** 構成 **>** 構成監査に移動します。

2. 「構成監査」ページで、「設定」をクリックします。
3. 通知設定ページで、編集アイコンをクリックして通知設定を有効にします。
4. 「有効」チェックボックスを選択します。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

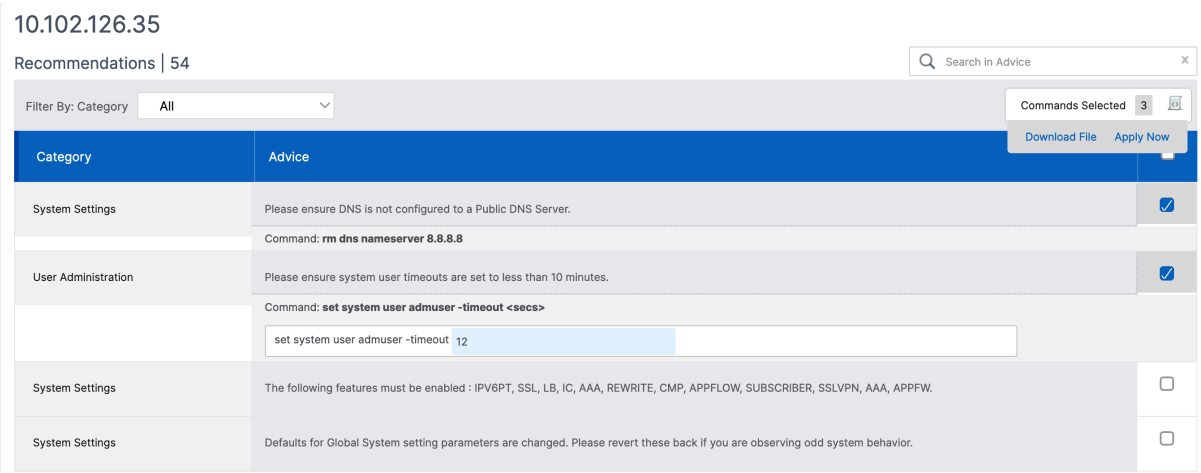
アプリケーションのパフォーマンスを最適化できるように、NetScaler ADC インスタンスを最適な構成でセットアップします。ただし、一部の構成は標準構成ではない場合があり、アプリケーションのパフォーマンスに影響を与える可能性があります。

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 ADM は NetScaler ADC インスタンスの構成を分析し、推奨事項を提示します。NetScaler ADM から推奨される構成を適用できます。

NetScaler インスタンスを分析するには:

1. インフラストラクチャ **>** 構成 **>** 構成監査 **>** 構成アドバイスに移動します。
2. 次のいずれかを行います:
   - [**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。

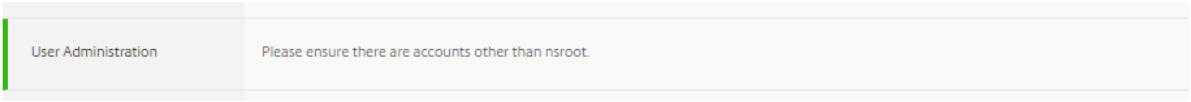
NetScaler ADM は、インスタンスの構成を分析し、次の図に示すように、推奨される構成のリストを提供します。構成アドバイスの横にあるチェックボックスをクリックすると、修正コマンドが表示されます。



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、「**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すぎません。読み取り権限と書き込み権限を持つユーザーは、この機能を使用して任意のコマンドを編集できます。コマンドを編集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。

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、アドバイスの横にあるチェックボックスが消えます。



ネットワークインスタンスで実行されたコマンドの詳細を表示するには、[インフラストラクチャ] **><Instance _Type\>** [インスタンス] に移動し、インスタンスの IP アドレスを選択して、[アクション] ドロップダウンリストから [イベントを表示] をクリックします。

「イベント」ページで、構成変更の詳細を表示します。

NetScaler インスタンスの構成監査をポーリングする

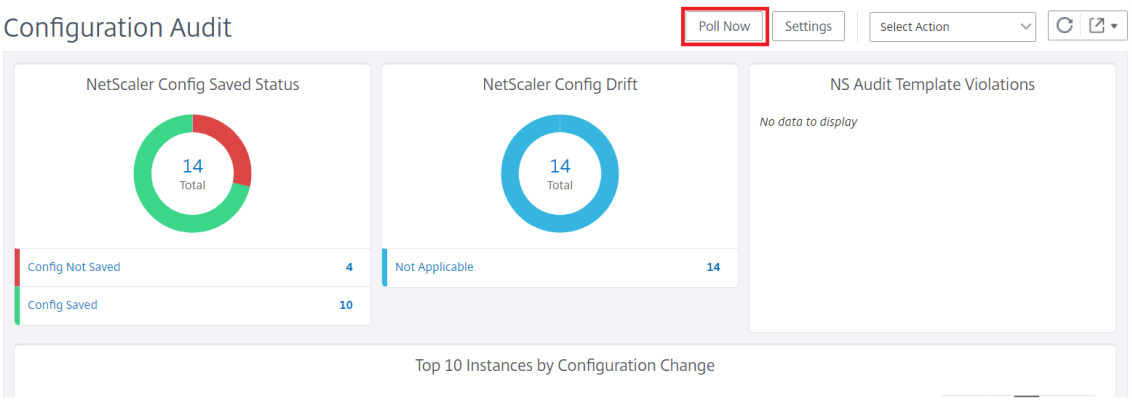
February 6, 2024

NetScaler ADM は、10 時間ごとに構成監査を自動的にポーリングして、NetScaler インスタンスで発生した構成の変更を探します。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 インスタンス構成監査全体をポーリングする代わりに、選択した 1 つまたは複数のインスタンスの構成監査のみを手動でポーリングできます。

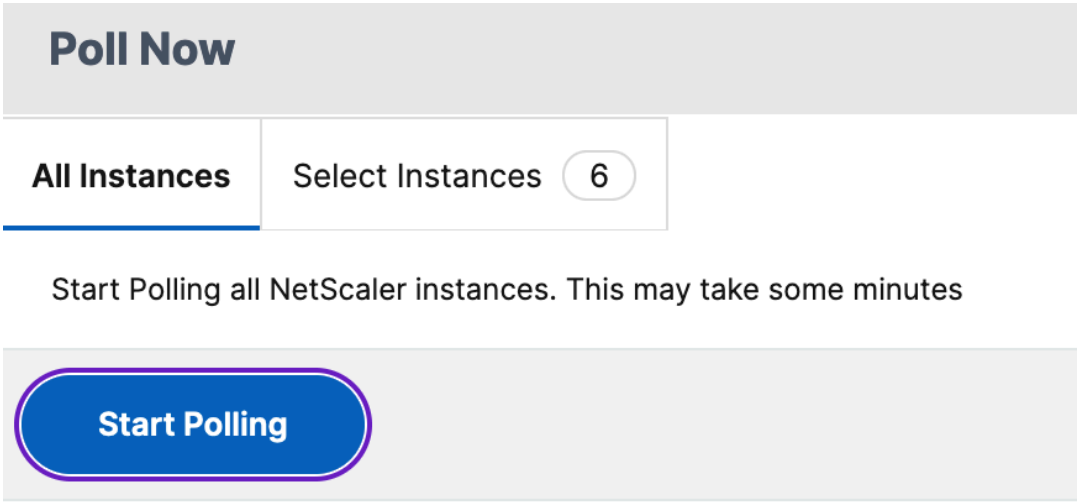
NetScaler インスタンスの構成監査をポーリングするには:

1. NetScaler ADM で、［インフラストラクチャ］**>**［構成］**>**［構成監査］に移動します
2. 「構成監査」で、「今すぐ投票」をクリックします。

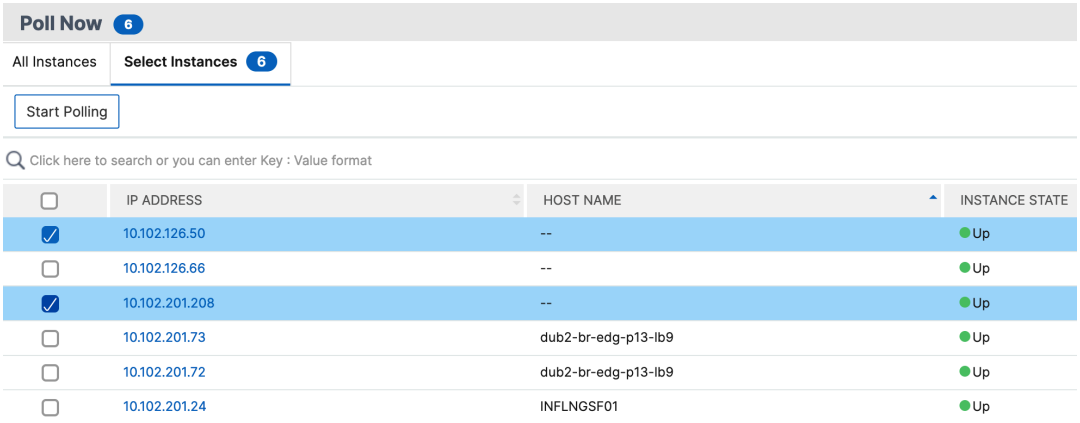


3. [**Poll Now**] ページが表示され、ネットワーク内のすべての NetScaler ADC インスタンスをポーリングするか、選択したインスタンスをポーリングするかを選択できます。

   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、**[Select**Instances] 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。



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 NetScaler ADC インスタンスの構成が変更されると、構成ファイルが更新されます。インスタンスは ConfigChange SNMP トラップを NetScaler ADM に送信します。NetScaler ADM を有効にして、インスタ

ンスが ConfigChange SNMP トラップを送信したときに、そのインスタンスの構成監査を実行することができます。

監査テンプレート設定と実行設定に違いがある場合、「監査レポート」ページに「Diff Exists」ステータスメッセージが表示されます。「**Diff Exists** 」リンクをクリックすると、修正コマンドを表示できる「設定の相違点」ページに移動します。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 の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、［インフラストラクチャ］ **>** ［構成］ **>** ［構成監査］に移動します
2. 「構成監査」ページの「設定」をクリック します。
3. 「NetScaler 構成変更」イベントの受信時に監査を実行を選択します。

> 注:
>
> NetScaler ADM は、今後 NetScalerConfigChange SNMP トラップを受信するすべてのインスタンスに対して構成監査を実行します。

1. 「監査テンプレートを実行するための遅延時間 (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 インスタンス上で構成監査テンプレートを実行します。

構成監査

February 6, 2024

このドキュメントには、次の方法に関するトピックが含まれています。

- 監査レポートを表示する
- インスタンス間の設定変更の監査
- ネットワーク構成に関する設定アドバイスを取得
- NetScaler インスタンスの構成監査をポーリングする
- 構成変更 SNMP トラップの構成監査差分を生成

ジョブのアップグレード

February 6, 2024

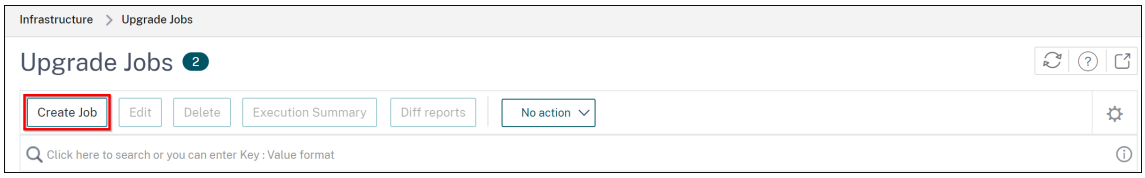
NetScaler ADM を使用して、次のメンテナンスタスクを作成できます。その後、特定の日時にメンテナンスタスクをスケジュールできます。

- NetScaler インスタンスのアップグレード
- NetScaler SDX インスタンスのアップグレード
- NetScaler BLX インスタンスをアップグレードする
- Autoscale グループの NetScaler ADC インスタンスをアップグレードする
- NetScaler インスタンスの HA ペアを構成する
- HA インスタンスのペアをクラスターに変換する

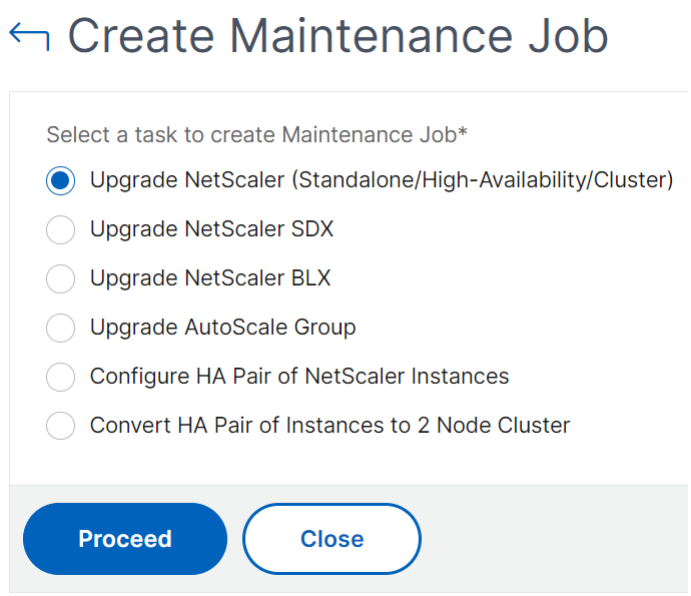
> 注:
>
> アップグレードジョブが失敗した場合、NetScaler ADM はビルドファイルやその他の抽出ファイルを削除して、NetScaler インスタンスに次のアップグレードを試行するための十分なディスク容量を確保します。

NetScaler インスタンスのアップグレードをスケジュールする

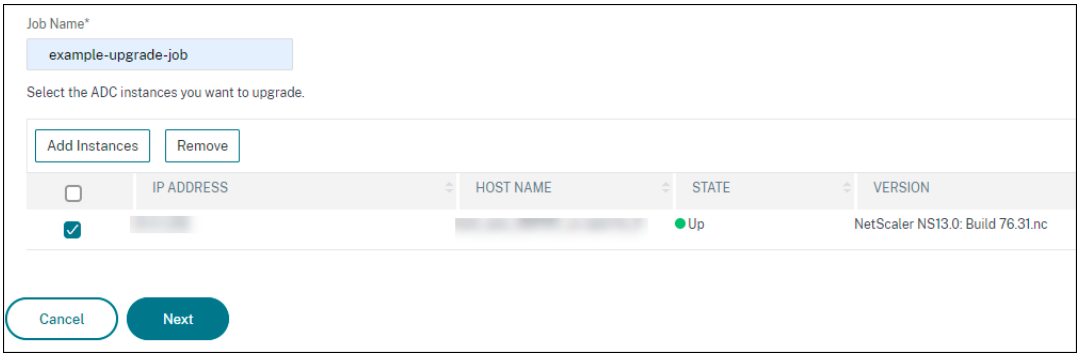
1. インフラストラクチャ **>** ジョブをアップグレードするに移動します。[ジョブの作成] をクリックします。



2. ［メンテナンスジョブの作成］で、［**NetScaler**（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。



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. [次へ] をクリックしてイメージを選択します。[ソフトウェアイメージ] リストから次の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 -NetScaler ADM ファイルブラウザからインスタンスアップグレードファイルを選択します。NetScaler ADM GUI には、`/var/mps/mps_images`にあるインスタンスファイルが表示されます。
     - 選択したイメージがすでに使用可能な場合は、**ADC** へのイメージのアップロードをスキップする -イメージが NetScaler ADC インスタンスにすでに存在する場合は、このオプションを選択します。

- アップグレードの成功時に **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。

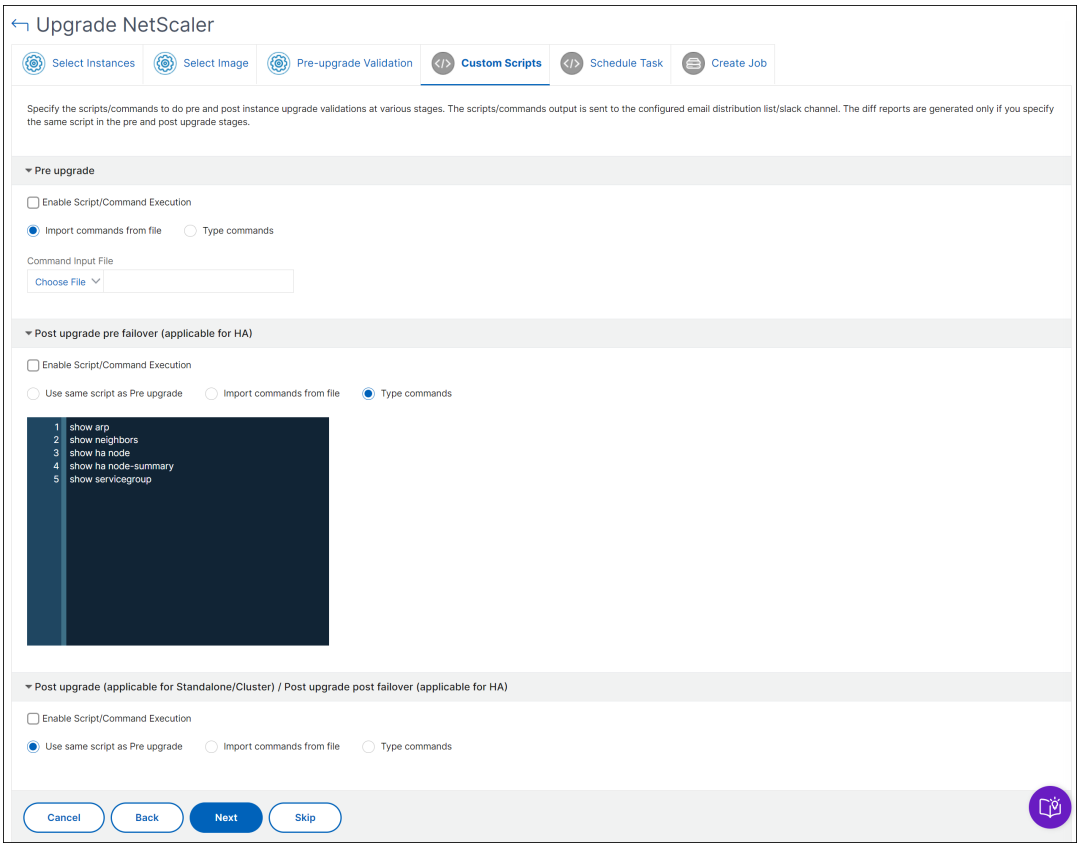
6. [**Next**] をクリックして、選択したインスタンスでアップグレード前の検証を開始します。

   アップグレード前の検証] 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、NetScaler 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。

7. 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。



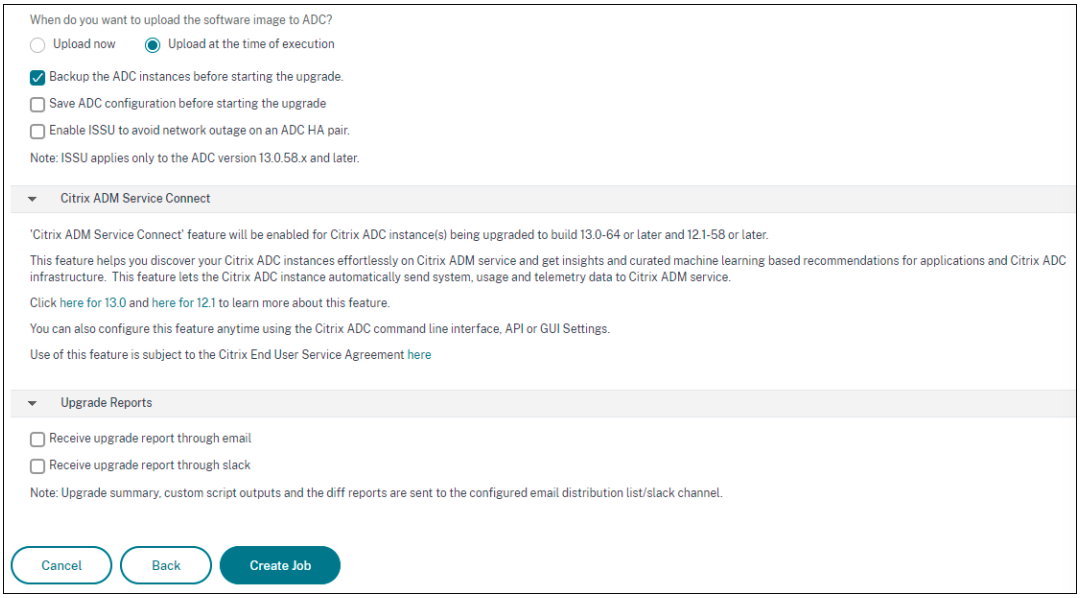
   カスタムスクリプトを使用して、インスタンスのアップグレードの前後に変更を確認できます。次に例を示します:

   - 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。

8. ［次へ］をクリックします。「タスクのスケジュール」で、次のいずれかのオプションを選択します。
   - 今すぐアップグレード -アップグレードジョブはすぐに実行されます。
   - 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。
9. ［次へ］をクリックします。「ジョブの作成」で、次の詳細を指定します。
   a) イメージをインスタンスにアップロードするタイミングを指定します。
      - 今すぐアップロード -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。
      - アップグレードを開始する前に **ADC** 設定を保存**-**アップグレード前にインスタンスに設定されている設定ジョブを保存します。
      - **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。
   - **NetScaler ADM** サービスコネクト - **** ビルド **13.0-64** 以降および **12.1-58** 以降にアップグレードする場合 **、NetScaler ADM サービスコネクトは自動的に有効になります。詳しくは、「NetScaler ADM サービス接続を使用した NetScaler インスタンスのロータッチオンボーディング」を参照してください。
   - 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。



10. [ジョブの作成] をクリックします。

NetScaler SDX インスタンスのアップグレードをスケジュールする

1. インフラストラクチャ **>** ジョブをアップグレードするに移動します。[ジョブの作成] をクリックします。
2. [**NetScaler SDX** のアップグレード］を選択し、［続行］をクリックします。
3. [**NetScaler SDX** のアップグレード］ページの［インスタンスの選択］タブで、次の操作を行います。

   a) タスク名を追加します。

   b) ［ソフトウェアイメージ］リストから、［ローカル］（ローカルマシン）または［アプライアンス］（ビルドファイルは NetScaler ADM 仮想アプライアンスに存在する必要があります）を選択します。

   アップロードプロセスが開始されます。

   c) アップグレードプロセスを実行する NetScaler ADC SDX インスタンスを追加します。

   d) ［次へ］をクリックします。

4. 「スケジュールタスク」タブで、「実行モード」リストから「Now」を選択して **NetScaler SDX** インスタンスを今すぐアップグレードし、「完了」をクリックします。
5. NetScaler SDX インスタンスを後でアップグレードするには、［実行モード］リストから［後で］を選択します。次に、NetScaler ADC インスタンスをアップグレードするための［実行日］と［開始時刻］を選択し、［完了］をクリックします。
6. また、アップグレード中の NetScaler ADC SDX インスタンスの実行レポートを受信するために、電子メールおよび Slack 通知を有効にすることもできます。通知を有効にするには、「実行レポートを電子メールで受信」チェックボックスと「**Slack** から実行レポートを受信」チェックボックスをクリックします。

電子メール配布リストと Slack チャネルを構成する方法の詳細については、「NetScaler ADC インスタンスのアップグレードのスケジュール」の手順 **8** を参照してください。

NetScaler BLX インスタンスのアップグレードをスケジュールする

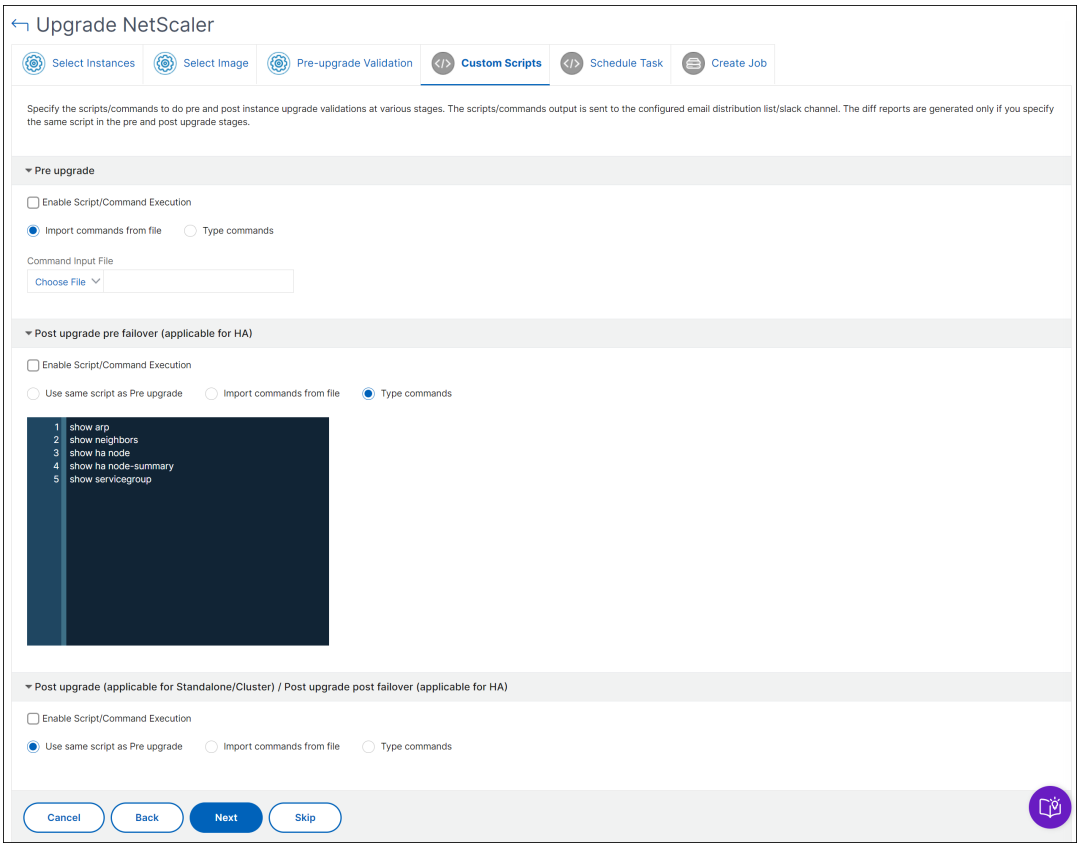
1. インフラストラクチャ **>** ジョブをアップグレードするに移動します。[ジョブの作成] をクリックします。
2. ［メンテナンスジョブの作成］で、［**NetScaler BLX** のアップグレード］を選択し、［続行
3. **[**インスタンスの選択**]** で、[ジョブ名**]** に任意の名前を入力します。
4. [**Add Instances**] をクリックして、アップグレードする BLX インスタンスを追加します。
   - HA ペアをアップグレードするには、プライマリノードまたはセカンダリノードの IP アドレスを指定します。ただし、プライマリインスタンスを使用して 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. [次へ] をクリックしてイメージを選択します。[ソフトウェアイメージ] リストから次のいずれかのオプションを選択します:
   - ローカル-ローカルマシンからインスタンスアップグレードファイルを選択します。
   - アプライアンス -NetScaler ADM ファイルブラウザからインスタンスアップグレードファイルを選択します。NetScaler ADM GUI には、`/var/mps/mps_images`にあるインスタンスファイルが表示されます。
     - 選択したイメージがすでに使用可能な場合は、**ADC** へのイメージのアップロードをスキップする -イメージが NetScaler ADC インスタンスにすでに存在する場合は、このオプションを選択します。
     - アップグレードの成功時に **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。
6. [**Next**] をクリックして、選択したインスタンスでアップグレード前の検証を開始します。

   アップグレード前の検証] 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、NetScaler 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。

7. 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。



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。

8. [次へ] をクリックします。「タスクのスケジュール」で、次のいずれかのオプションを選択します。

   - 今すぐアップグレード -アップグレードジョブはすぐに実行されます。
   - HA ペアを 2 段階でアップグレードする場合は、[HA のノードに **2** 段階アップグレードを実行する] を選択します。

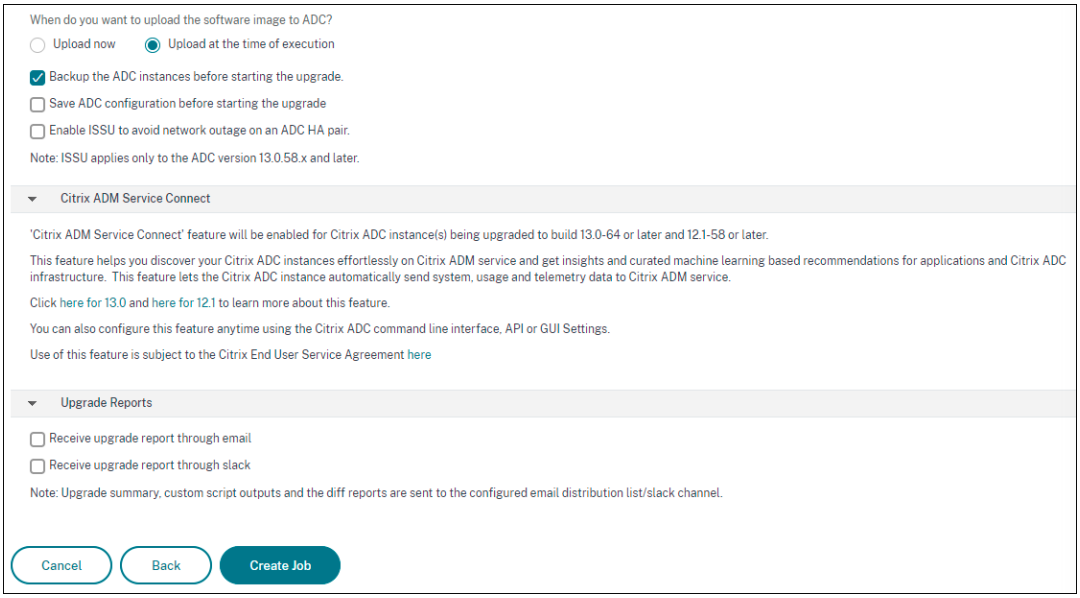
     HA ペアの別のインスタンスをアップグレードする場合は、[**Execution Date**] と [**Start Time**] を指定します。

9. [次へ] をクリックします。「ジョブの作成」で、次の詳細を指定します。

a) イメージをインスタンスにアップロードするタイミングを指定します。

- 今すぐアップロード -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。
- アップグレードを開始する前に **ADC** インスタンスをバックアップする -選択した ADC インスタンスのバックアップを作成します。
- アップグレードを開始する前に **ADC** 設定を保存**-**アップグレード前にインスタンスに設定されている設定ジョブを保存します。
- **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。

- **NetScaler ADM** サービスコネクト - **** ビルド **13.0-64** 以降および **12.1-58** 以降にアップグレードする場合 **、NetScaler ADM サービスコネクトは自動的に有効になります。詳しくは、「NetScaler ADM サービス接続を使用した NetScaler インスタンスのロータッチオンボーディング」を参照してください。
- 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。



10. [ジョブの作成] をクリックします。

Autoscale グループのアップグレードのスケジュール

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. インフラストラクチャ **>** ジョブをアップグレードするに移動します。[ジョブの作成] をクリックします。
2. [**AutoScale** グループをアップグレード] を選択し、[続行] をクリックします。
3. [アップグレード設定] タブで、次の操作を行います。
   a) アップグレードする **Autoscale** グループを選択します。
   b) [イメージ] で、NetScaler のバージョンを選択します。このイメージは、Autoscale グループの 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。
      - 今すぐ**:**NetScaler インスタンスをすぐに開始するには、アップグレードしてください。
      - 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。

   電子メール通知と Slack 通知を有効にして、アップグレードする Autoscale グループ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、「実行レポートを電子メールで受信」チェックボックスと「**Slack** から実行レポートを受信」チェックボックスをクリックします。
5.［完了］をクリックします。

NetScaler ADC インスタンスの **HA** ペアの構成をスケジュールする

1. インフラストラクチャ **>** ジョブをアップグレードするに移動します。[ジョブの作成] をクリックします。
2.［**NetScaler ADC** インスタンスの **HA** ペアの構成］を選択し、［続行］をクリックします。
3.［**NetScaler HA** ペア］ページの［インスタンスの選択］タブで、次の操作を行います。
   a) タスク名を追加します。
   b) プライマリ IP アドレスを選択します。［**OK**］をクリックします。

c) プライマリ RPC ノードパスワードを入力します。

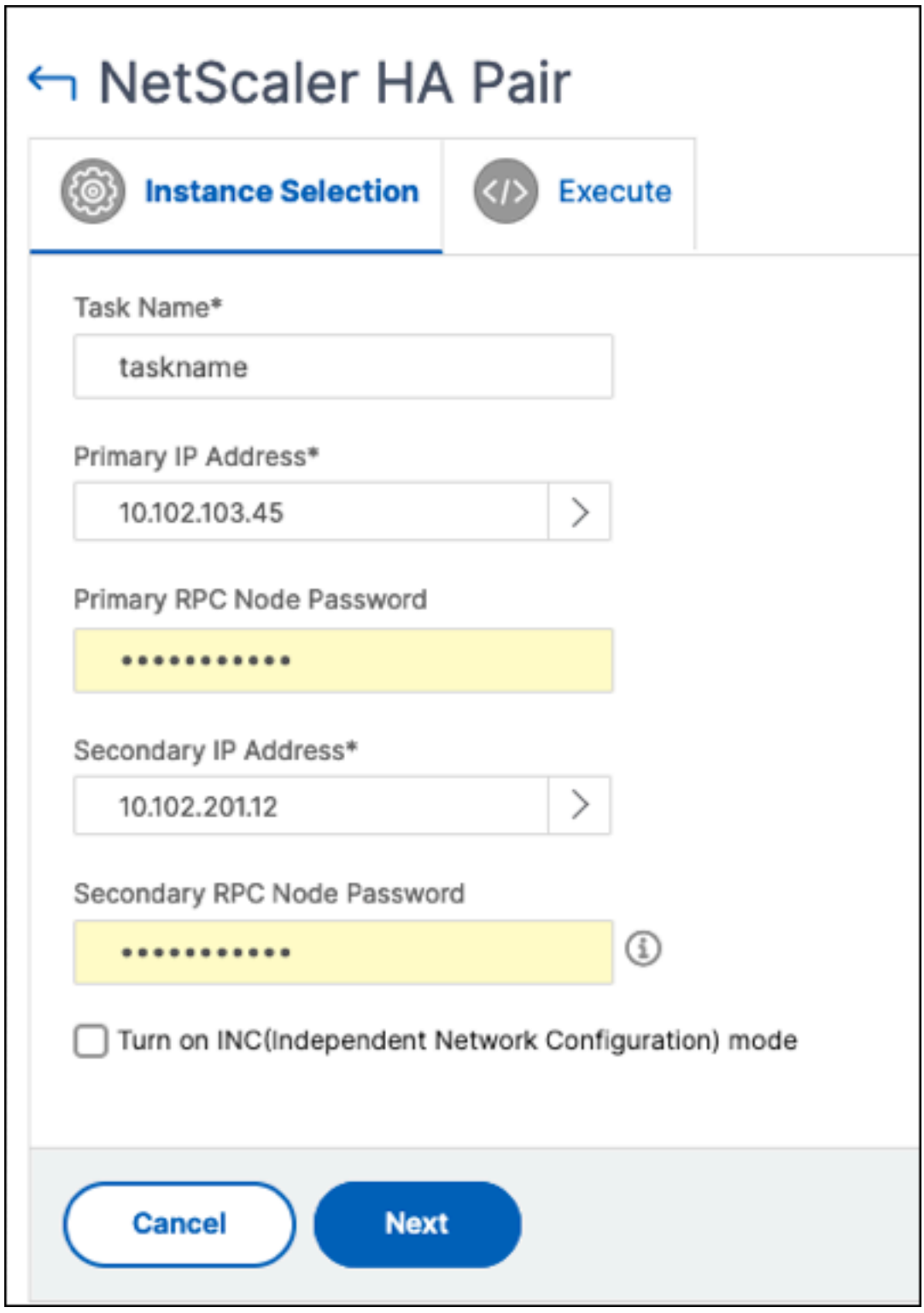
d) セカンダリ IP アドレスを選択します。[**OK**] をクリックします。

> 注:
>
> RPC ノードのパスワードフィールドは、NetScaler リリース 14.1 以降で使用できます。

e) セカンダリ RPC ノードのパスワードを入力します。

f) 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] をクリックして有効にします。

g) [次へ] をクリックします。



4. ［タスクのスケジュール］タブで、［実行モード］リストから［今すぐ **Citrix** ADC］インスタンスをアップグレードし、［完了］をクリックします。
5. NetScaler HA ペアを後でアップグレードするには、［実行モード］リストから［後で］を選択します。次に、

NetScaler ADC インスタンスをアップグレードするための［実行日］と［開始時刻］を選択し、［完了］をクリックします。

6. また、メール通知と Slack 通知を有効にして、ADC HA ペア作成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、「実行レポートを電子メールで受信」チェックボックスと「**Slack** から実行レポートを受信」チェックボックスをクリックします。

   電子メール配布リストと Slack チャネルを構成する方法の詳細については、「NetScaler ADC インスタンスのアップグレードのスケジュール」の手順 **8** を参照してください。

インスタンスの **HA** ペアをクラスターに変換するスケジュールを設定する

1. インフラストラクチャ **>** ジョブをアップグレードするに移動します。[ジョブの作成] をクリックします。
2. [**HA** インスタンスのペアを **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。
3. ［**NetScaler HA** をクラスタに移行する］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 IP アドレス、プライマリノード ID、セカンダリノード ID、クラスタ IP アドレス、クラスタ ID、バックプレーンを指定し、[次へ] をクリックします。
4. ［タスクのスケジュール］タブで、［実行モード］リストから［今すぐ **Citrix** ADC］インスタンスをアップグレードし、［完了］をクリックします。
5. 後でアップグレードするには、[実行モード] リストから [後でアップグレード] を選択します。次に、NetScaler HA ペアインスタンスをアップグレードするための［実行日］と［開始時刻］を選択し、［完了］をクリックします。
6. 電子メール通知と余裕期間の通知を有効にして、NetScaler SDX インスタンスのアップグレードの実行レポートを受信することもできます。通知を有効にするには、「実行レポートを電子メールで受信」チェックボックスと「**Slack** から実行レポートを受信」チェックボックスをクリックします。

   メール配布リストとスラックチャネルの設定について詳しくは、「NetScaler インスタンスのアップグレードをスケジュールする」のステップ **8** を参照してください。

ジョブを使用して **NetScaler** インスタンスをアップグレードする

February 6, 2024

NetScaler Application Delivery Management（ADM）を使用して、1 つ以上の NetScaler インスタンスをアップグレードできます。インスタンスをアップグレードする前に、ライセンスフレームワークとライセンスの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 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 フォルダーの容量が 6 GB 未満で、/flash フォルダーの容量が 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。

NetScaler 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。

NetScaler 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。

NetScaler 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。

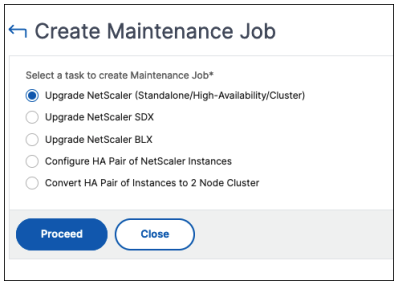
NetScaler インスタンスをアップグレードするためのアップグレードメンテナンスジョブを作成する

> 注
>
> NetScaler の上位バージョンから下位バージョンへのアップグレードはサポートされていません。たとえば、

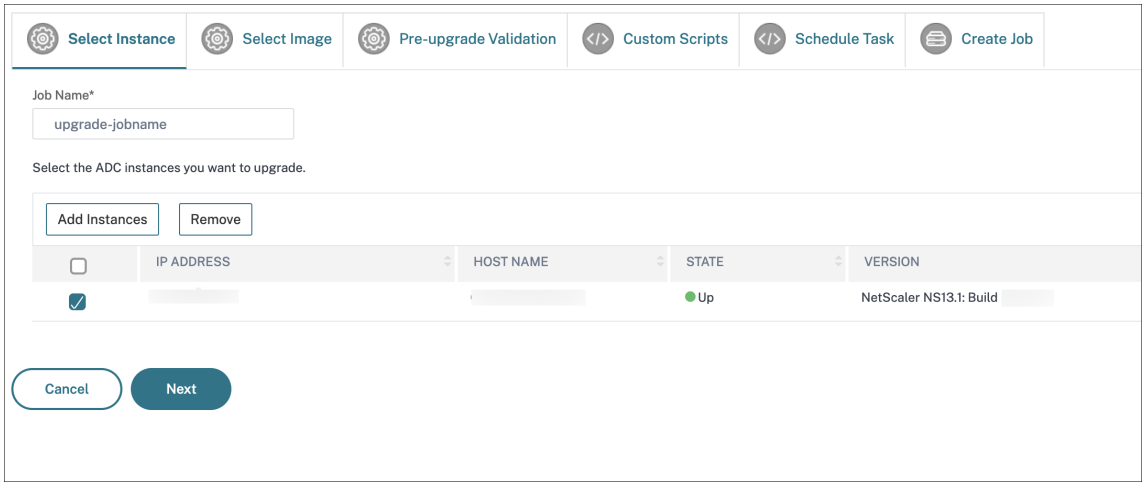
> NetScaler インスタンスが 13.0 82.x の場合、NetScaler インスタンスを 13.0 79.x またはその他の以前のバージョンにダウングレードすることはできません。

1. NetScaler ADM で、［インフラストラクチャ］**>**［アップグレードジョブ］に移動します。[ジョブの作成] 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**（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。

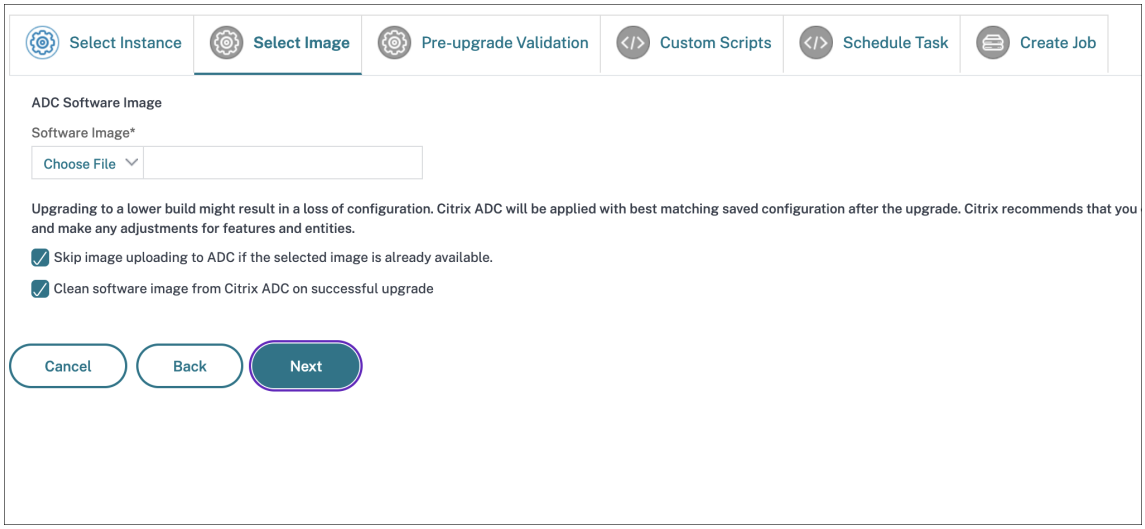


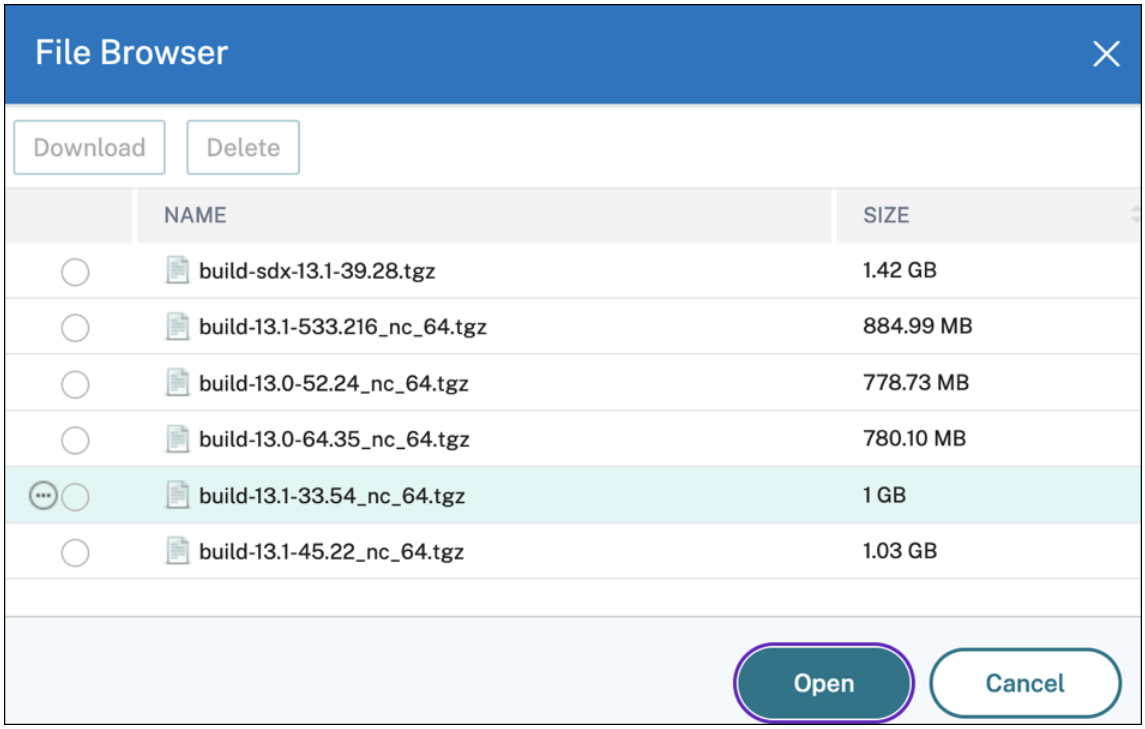
3. **[**インスタンスの選択**]** で、[ジョブ名**]** に任意の名前を入力します。
4. 「インスタンスを追加」をクリックして、アップグレードする NetScaler インスタンスを追加します。
    - NetScaler の高可用性ペアをアップグレードするには、高可用性ペアの IP アドレス（「S」と「P」の上付き文字で表示）を選択します。
    - クラスターをアップグレードするには、クラスターの IP アドレス (「C」の上付き文字で示される) を選択します。



5.「イメージの選択」タブで、ローカルドライブまたはビルドイメージから NetScaler イメージを選択します。

- ローカル-ローカルマシンからインスタンスアップグレードファイルを選択します。
- アプライアンス -NetScaler ADM ファイルブラウザーからインスタンスアップグレードファイルを選択します。NetScaler ADM GUI には、/var/mps/ns_imagesにあるインスタンスファイルが表示されます。





- 選択したイメージがすでに使用可能な場合は、**NetScaler** へのイメージのアップロードをスキップする -このオプションは、選択したイメージが NetScaler で使用できるかどうかをチェックします。アップグレードジョブでは、新しいイメージのアップロードがスキップされ、NetScaler で使用可能なイメージが使用されます。
- アップグレードが成功したら **NetScaler** からソフトウェアイメージを消去する**-**このオプションは、インスタンスのアップグレード後に **NetScaler** インスタンスにアップロードされたイメージを消去します。

[**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。

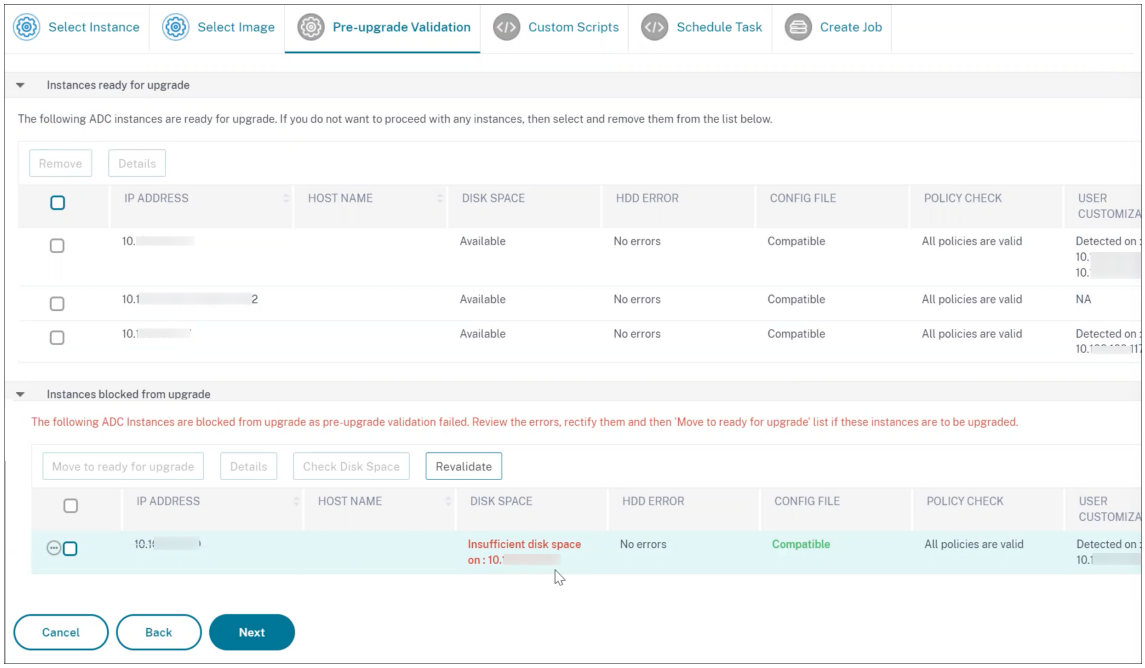
> 注:
>
> - ダウンロードされた NetScaler イメージは NetScaler ADM エージェントに保存され、`/var/mps/adcimages`にあります。これらのキャッシュされたイメージは複数の NetScaler アップグレードに使用できるため、アップグレードのたびにイメージをダウンロードする必要がなくなります。
> - NetScaler ADM は、キャッシュされた NetScaler イメージを、イメージの最終変更時刻に基づいて 3 日ごとに消去します。NetScaler ADM エージェントに一度にキャッシュされるのは、最新の 2 つのイメージファイルのみです。

6.「アップグレード前の検証」タブには、次のセクションが表示されます。

- インスタンスはアップグレードの準備ができています。これらのインスタンスのアップグレードを続行できます。

- インスタンスのアップグレードがブロックされました。これらの NetScaler インスタンスは、アップグレード前の検証エラーのためにアップグレードがブロックされています。

  エラーを確認して修正し、[アップグレードの準備完了] をクリックしてエラーをアップグレードできます。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。NetScaler のディスク容量のクリーンアップを参照してください。



- ポリシーチェック：NetScaler ADM がサポートされていないクラシックポリシーを見つけた場合は、そのようなポリシーを削除してアップグレードジョブを作成できます。

> 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。

7. 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、NetScaler インスタンスのアップグレードの前後に変更を確認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。

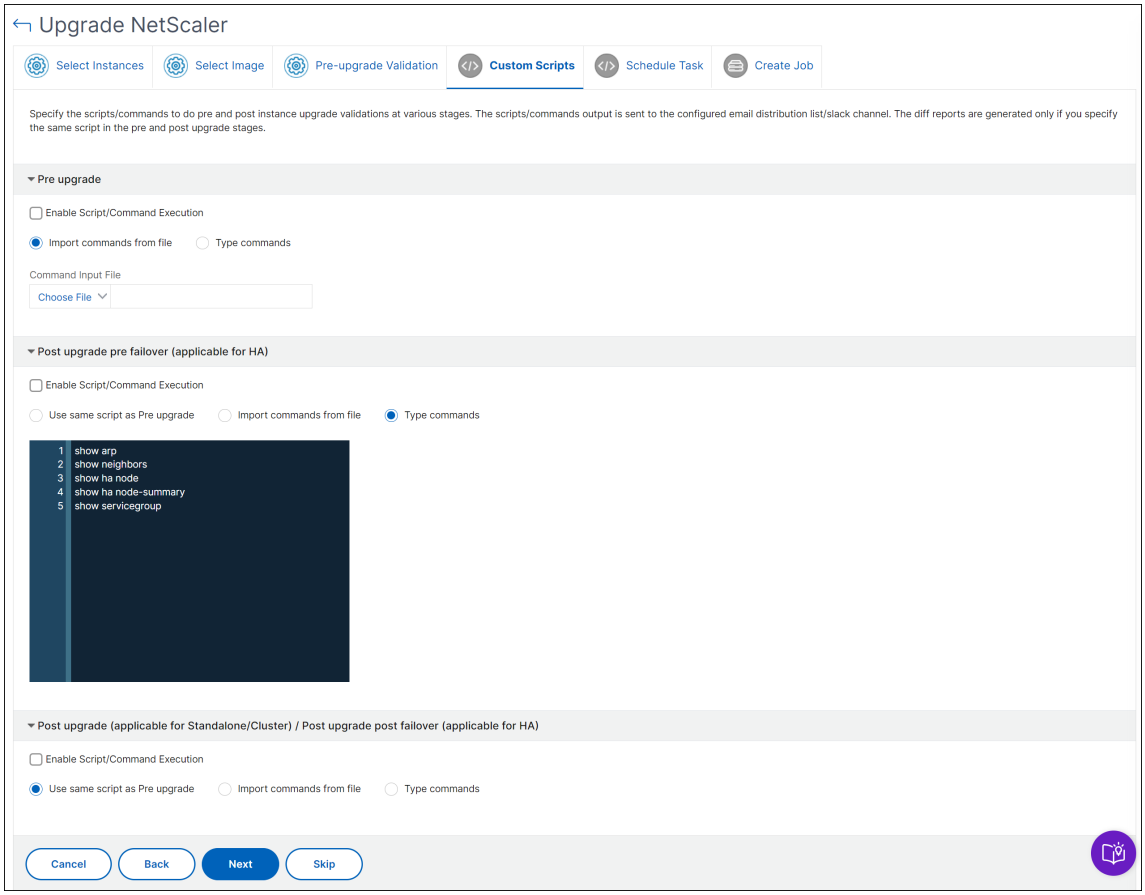
- アップグレード前: インスタンスをアップグレードする前に、指定されたスクリプトが実行されます。
- アップグレード前のフェールオーバー後（**HA** に適用可能）: このステージは、高可用性配置にのみ適用されます。指定されたスクリプトは、ノードのアップグレード後、フェールオーバーの前に実行されます。
- アップグレード後（スタンドアロンに適用）/フェールオーバー後のアップグレード後（**HA** に適用可能）: 指定されたスクリプトは、スタンドアロンデプロイでインスタンスをアップグレードした後に実行されます。高可用性展開では、スクリプトはノードとフェイルオーバーをアップグレードした後に実行されます。

> 注:
>
> 必要な段階でスクリプトの実行を有効にしてください。そうしないと、指定されたスクリプトは実行されません。

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 に直接コマンドを入力します。

アップグレード後のステージでは、アップグレード前のステージで指定したスクリプトと同じスクリプトを使用できます。



8. 「タスクのスケジュール」で、次のいずれかのオプションを選択します。

   - 今すぐアップグレード -アップグレードジョブはすぐに実行されます。
   - NetScaler HA ペアを 2 段階でアップグレードする場合は、［**HA** 内のノードに対して **2** 段階アップグレードを実行する］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。

9. 「ジョブの作成」で、次の詳細を指定します。

   a) [ソフトウェアイメージ] リストから次の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。

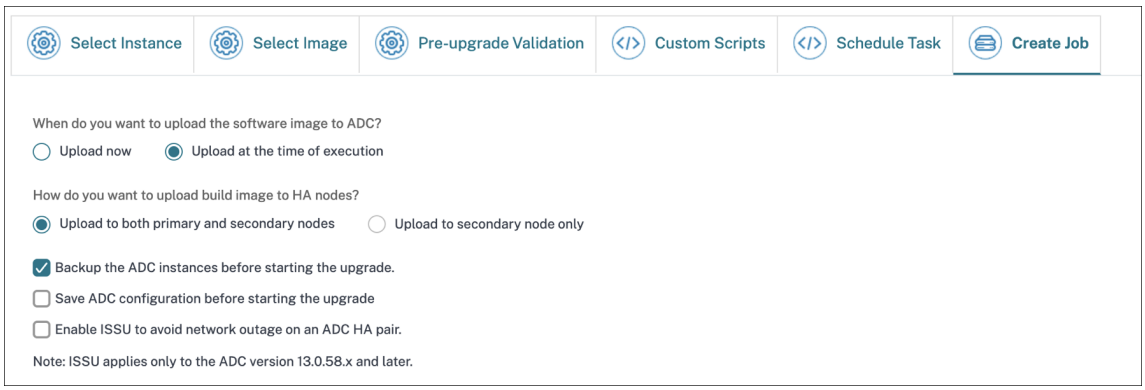
   b) イメージをインスタンスにアップロードするタイミングを指定します。

      - 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。

高可用性ペアの場合は、イメージをアップロードするノードを指定できます。

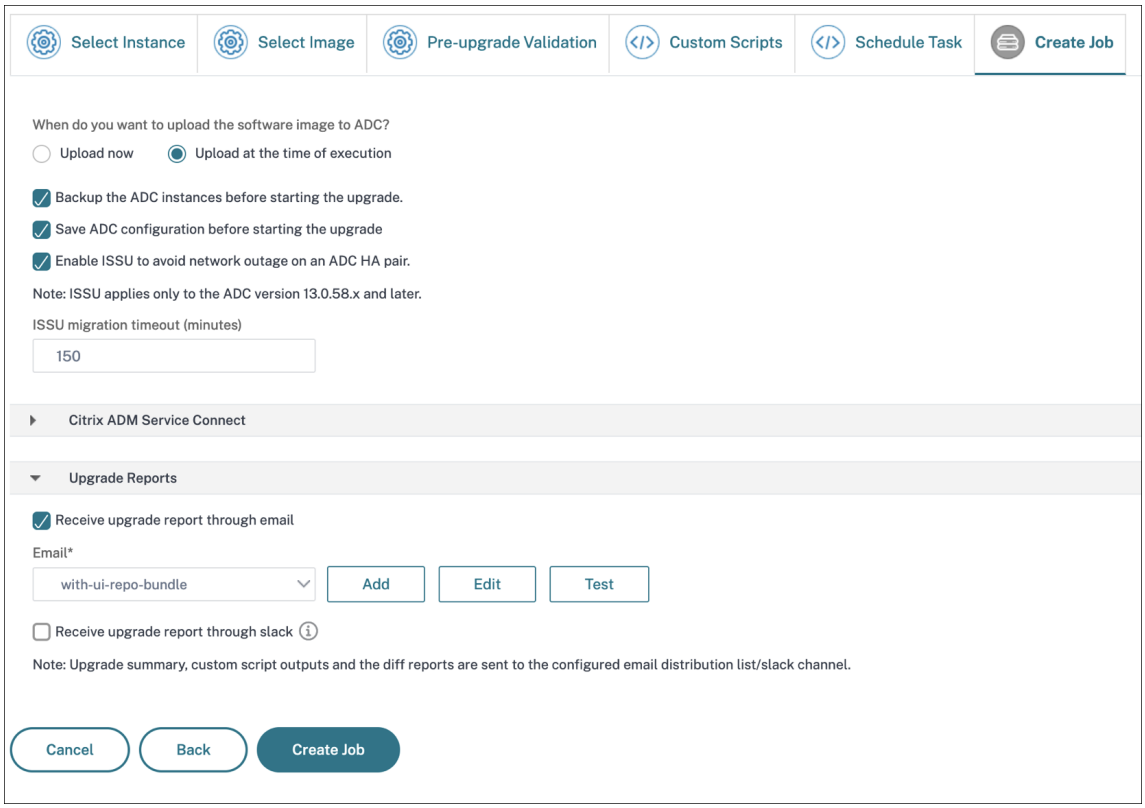
- プライマリノードとセカンダリノードの両方にアップロード: ビルドイメージファイルをプライマリノードとセカンダリノードの両方にアップロードします。
- セカンダリノードのみにアップロード: ビルドイメージファイルをセカンダリノードのみにアップロードします。セカンダリノードがアップグレードされると、フェイルオーバーが発生し、ビルドイメージファイルが、以前はプライマリノードであった新しいセカンダリノードにアップロードされます。



高可用性ペアで利用できるスケジューリングシナリオの詳細については、「高可用性ペアのアップグレードジョブのスケジュール」を参照してください。

- アップグレードが成功したら **NetScaler** からソフトウェアイメージを消去する**-**このオプションを選択すると、インスタンスのアップグレード後に **NetScaler** インスタンスにアップロードされたイメージが消去されます。
- アップグレードを開始する前に、**NetScaler** インスタンスをバックアップしてください。-選択した NetScaler インスタンスのバックアップを作成します。
- アップグレード後に **HA** ノードのプライマリステータスとセカンダリステータスを維持する**:** 各ノードのアップグレード後にアップグレードジョブがフェイルオーバーを開始するようにするには、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。
- アップグレードを開始する前に **NetScaler** 構成を保存する**-NetScaler** インスタンスをアップグレードする前に、実行中の NetScaler 構成を保存します。
- **ISSU** を有効にすると、**NetScaler HA** ペアのネットワーク停止を回避できます。**ISSU** を使用すると、**NetScaler** の高可用性ペアをダウンタイムなしでアップグレードできます。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。そのため、NetScaler HA ペアをダウンタイムなしで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。

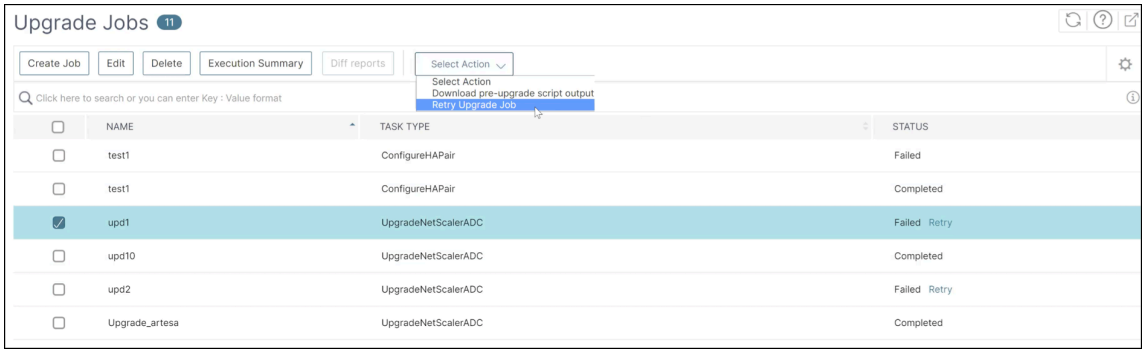


10. [ジョブの作成] をクリックします。

アップグレードジョブは [インフラストラクチャ] **>** [アップグレードジョブ] に表示されます。既存のジョブを編集するときに、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。

失敗したアップグレードジョブを再試行

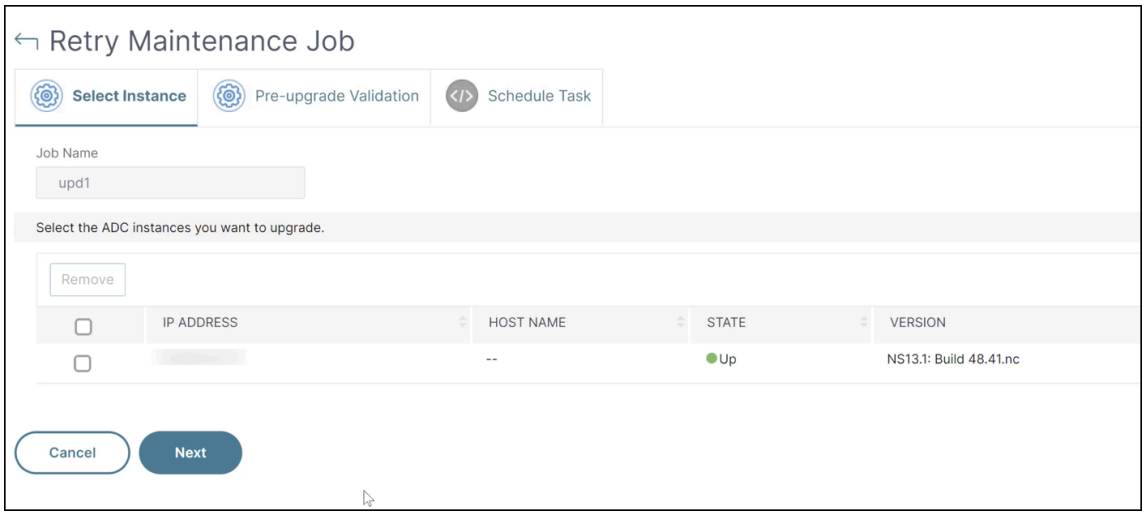
1. [インフラストラクチャ] **>** [アップグレードジョブ] で、失敗したアップグレードジョブを選択し、[再試行] をクリックします。または、[アクションの選択] **>** [アップグレードジョブの再試行] に移動して、失敗したジョブを再試行することもできます。



2. 「インスタンスの選択」で、次の詳細を指定します。

   - ジョブ名 -アップグレードの名前を入力します。
   - アップグレードする NetScaler インスタンスをリストから選択します。インスタンスを削除するには、[削除] をクリックします。

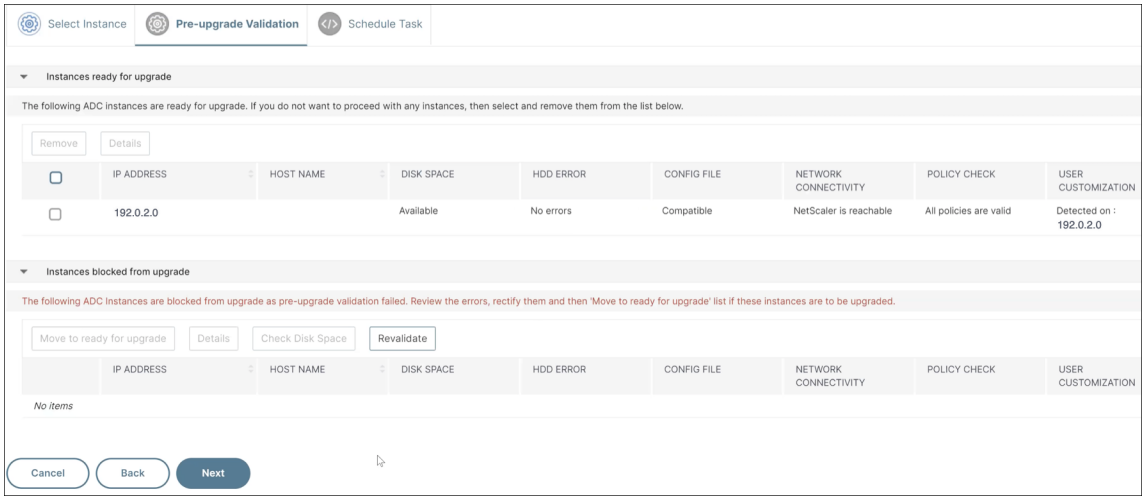
   [次へ] をクリックして検証プロセスを開始します。



3. 「アップグレード前の検証」タブには、次のセクションが表示されます。

   - インスタンスはアップグレードの準備ができています。これらのインスタンスのアップグレードを続行できます。
   - インスタンスのアップグレードがブロックされました。これらの NetScaler インスタンスは、アップグレード前の検証エラーのためにアップグレードがブロックされています。

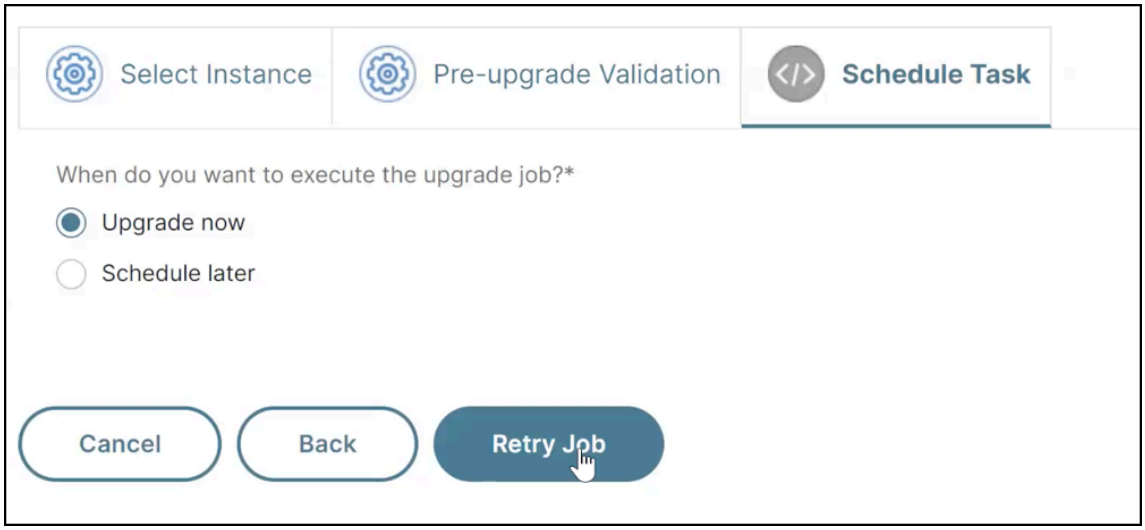
     エラーを確認して修正し、[アップグレードの準備完了] をクリックしてエラーをアップグレードできます。インスタンスのディスク領域が不足している場合は、ディスク領域を確認してクリーンアップできます。「NetScaler ディスク容量のクリーンアップ」を参照してください。
   - ポリシーチェック: NetScaler ADM がサポートされていないクラシックポリシーを見つけた場合は、そのようなポリシーを削除してアップグレードジョブを作成できます。



［次へ］をクリックします。

4. 「タスクのスケジュール」で、次のいずれかのオプションを選択します。

   - 今すぐアップグレード: アップグレードジョブはすぐに実行されます。
   -



［再試行］をクリックします。

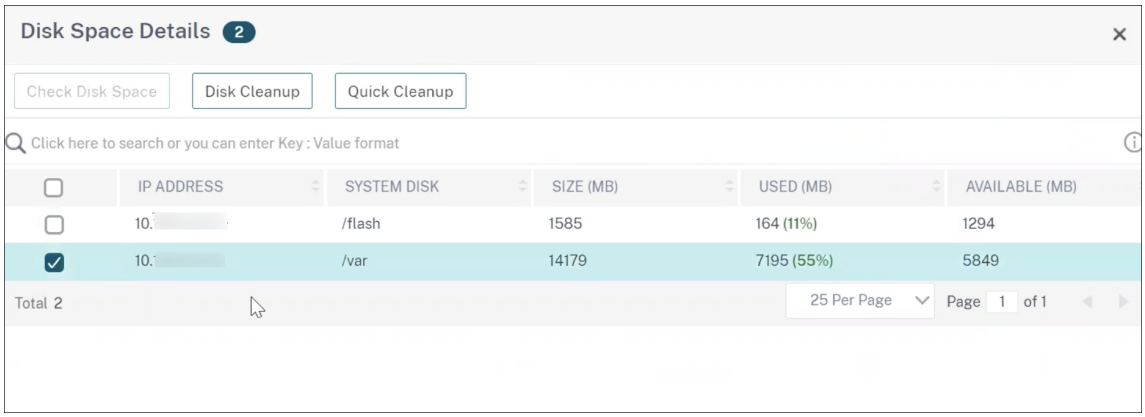
NetScaler のディスク容量をクリーンアップします

NetScaler インスタンスのアップグレード中にディスク容量不足の問題が発生した場合は、NetScaler ADM GUI 自体からディスク容量をクリーンアップしてください。

1. 「アップグレード前の検証」タブの「アップグレードがブロックされたインスタンス」セクションには、ディスク容量が不足しているためにアップグレードに失敗したインスタンスが表示されます。ディスク容量に問題があるインスタンスを選択します。

2. [ディスク容量の確認] をクリックします。

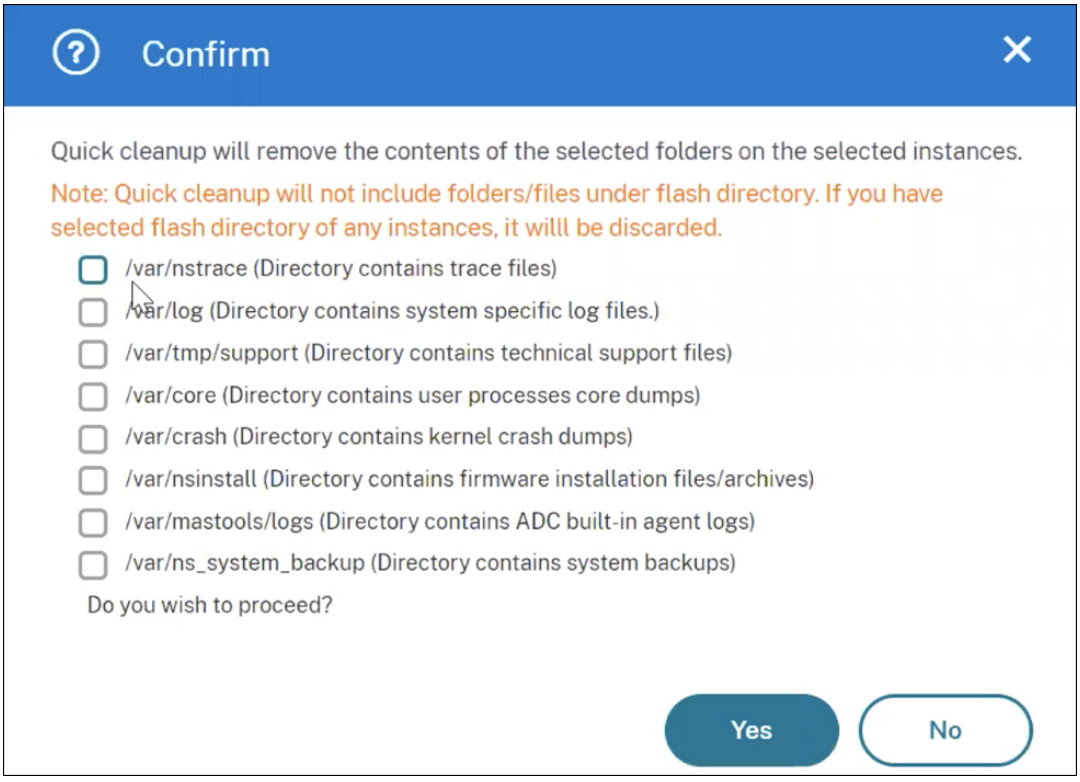
   [ディスク容量の詳細] ウィンドウが表示されます。このペインには、インスタンス、使用済みメモリ、および使用可能なメモリが表示されます。



3. ディスク容量の詳細ペインで、クリーンアップが必要なインスタンスを選択し、次のいずれかを実行します。

   a) ディスククリーンアップ -必要なフォルダまたはディレクトリに移動して削除し、ディスクの空き容量を増やします。

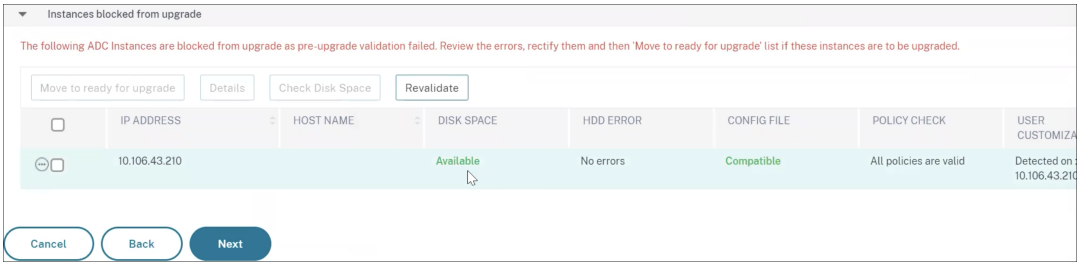
   b) クイッククリーンアップ -複数のフォルダーを削除して、ディスク容量をすばやく空けます。表示される [確認] ペインで、削除するフォルダを選択し、[はい] をクリックします。



   c) ディスク容量を空けたら、インスタンスをアップグレードするのに十分なディスク容量があるかどうかを確認できます。「アップグレードがブロックされたインスタンス」セクションで、「再検証」をクリッ

クします。

次の例では、ディスク容量が使用可能です。これで、[アップグレードの準備完了] をクリックしてインスタンスをアップグレードするか、[次へ] をクリックして次のステップに進むことができます。



NetScaler 高可用性ペアのアップグレードジョブのスケジュール設定

次の表は、「**Schedule Task** 」ページのさまざまなスケジューリングシナリオと、「**Create Job** 」ページで使用できる対応するアップグレードオプションを示しています。

アップグレードジョブをいつ実行しますか**?**	ソフトウェアイメージを **NetScaler** にいつアップロードしますか**?**	ビルドイメージを **HA** ノードにどのようにアップロードしますか**?**
今すぐアップグレード	該当なし	プライマリノードとセカンダリノードの両方にアップロード (デフォルトオプション)
後でスケジュールする	実行時にアップロード (デフォルトオプション)	プライマリノードとセカンダリノードの両方にアップロード (デフォルトオプション)
後でスケジュールする ([**HA** 内のノードの **2** 段階アップグレードを実行する] を選択した場合)	実行時にアップロード (デフォルトオプション)	今すぐアップロード セカンダリノードのみにアップロード (デフォルトかつ唯一のオプション) 今すぐアップロード

NetScaler アップグレードジョブの複合差分レポートをダウンロードする

カスタムスクリプトが指定されている場合は、NetScaler アップグレードジョブの差分レポートをダウンロードできます。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 NetScaler インスタンスにどのような変更が加えられたかを確認できます。

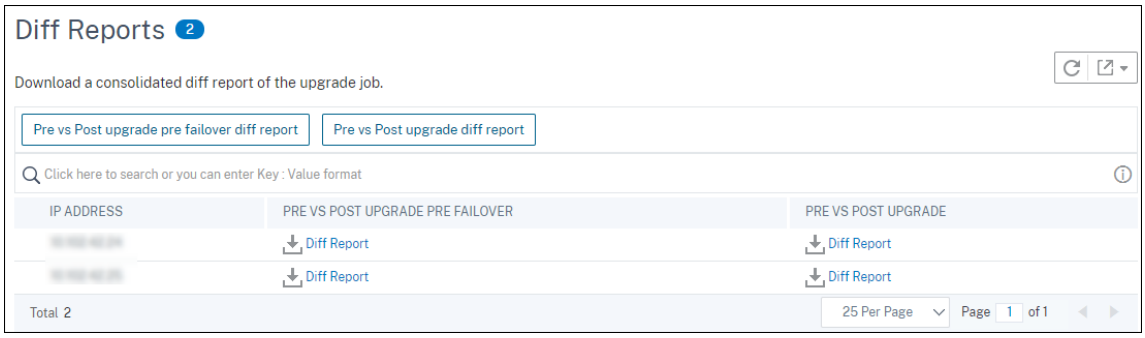
> 注:
>
> 相違レポートが生成されるのは、アップグレード前およびアップグレード後の段階で同じスクリプトを指定した場合のみです。

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. インフラストラクチャ **>** 構成ジョブ **>** メンテナンスジョブに移動します。
2. 差分レポートをダウンロードするアップグレードジョブを選択します。
3. 「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



セキュリティアドバイザリ

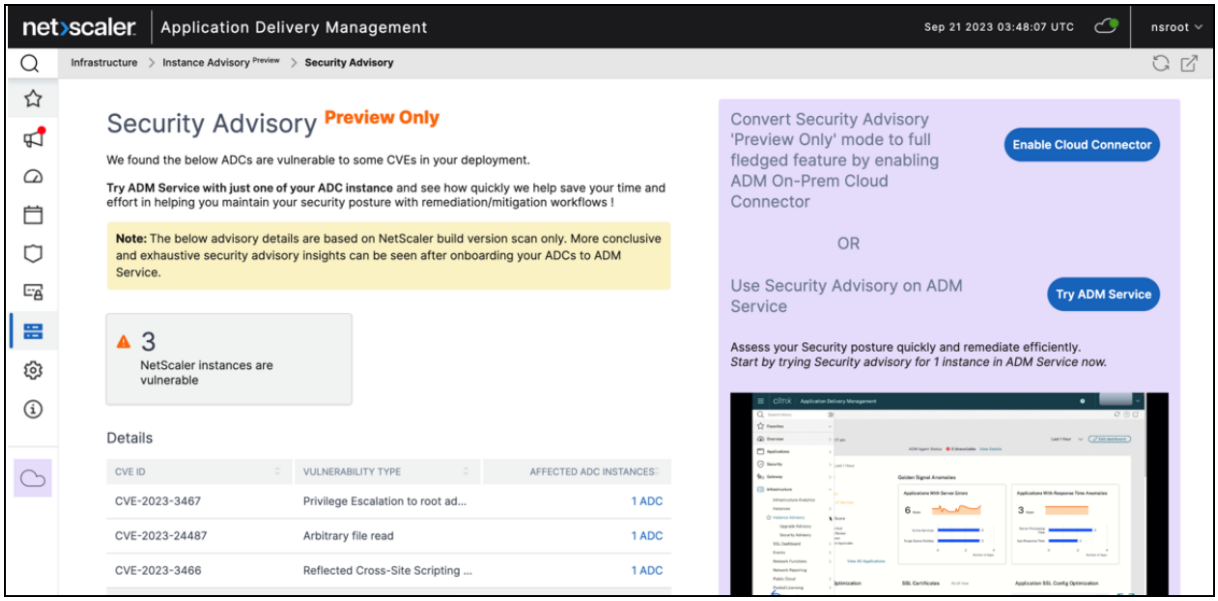
February 6, 2024

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修正方法を理解し、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リ機能を使用すると、NetScaler インスタンスを危険にさらしている CVE を特定し、修復方法を推奨できます。

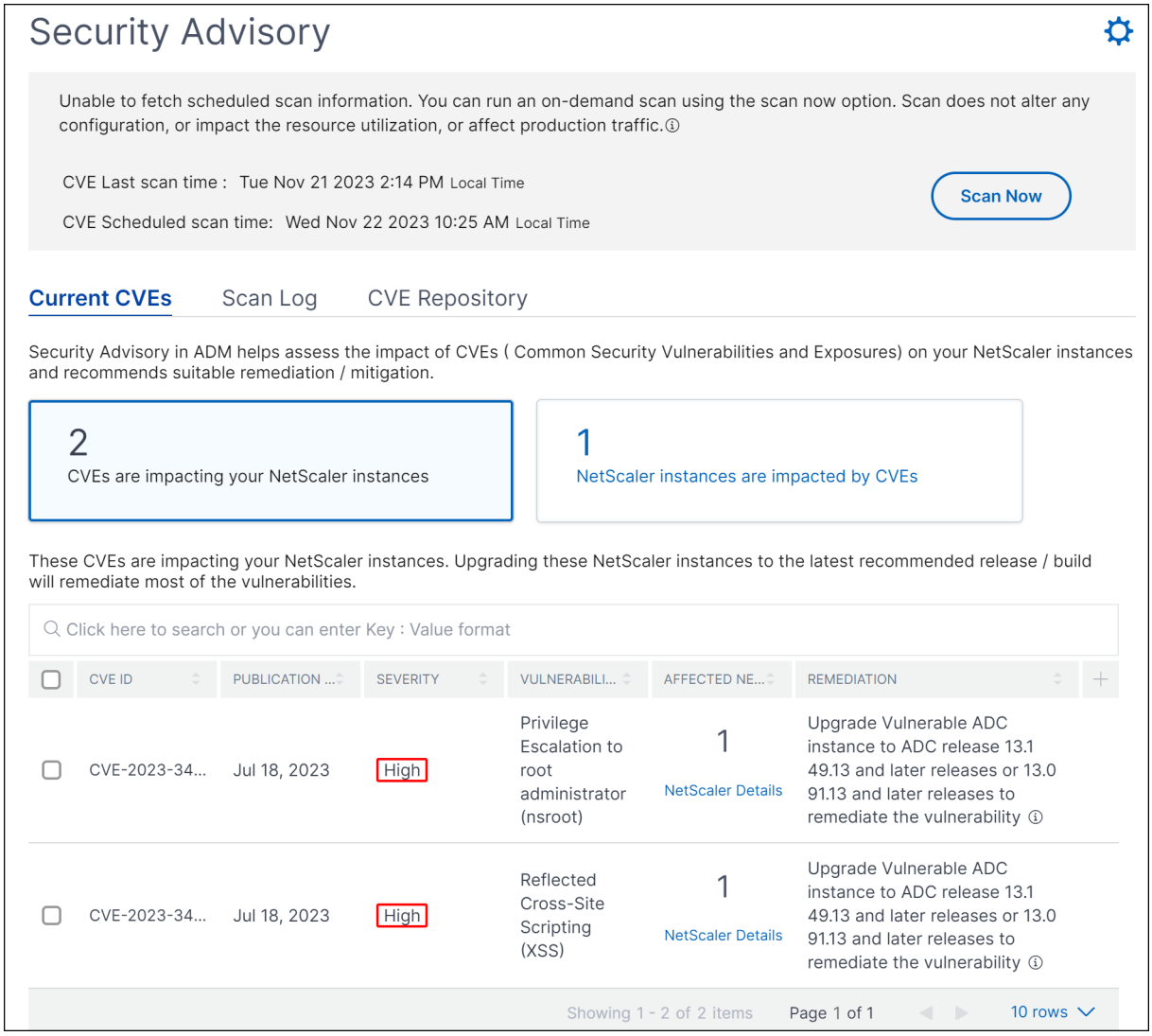
14.1 8.x ビルド以降では、ADM On-Prem Cloud Connector を設定してセキュリティアドバイザリを有効にすることで、セキュリティアドバイザリのフルバージョンを使用できます。

ADM On-Prem Cloud Connector を設定していない場合は、セキュリティアドバイザリのプレビュー専用バージョンを表示できます。「**Cloud Connector** を有効にする」をクリックして設定を完了すると、セキュリティアドバ

イザリのフルバージョンを使用できます。詳細については、「ADM オンプレミ CloudConnector」を参照してください。



ADM On-Prem Cloud Connector を設定し、セキュリティアドバイザリを有効にすると、更新されたセキュリティアドバイザリページを表示できます。



管理者は、新しい一般的な脆弱性と暴露 (CVE) を追跡し、CVE の影響を評価し、修復方法を理解し、脆弱性を解決する必要があります。

セキュリティアドバイザリの機能

以下のセキュリティアドバイザリ機能は、インフラストラクチャの保護に役立ちます。

機能	説明
システムスキャン	デフォルトでは、すべてのマネージドインスタンスを週に 1 回スキャンします。NetScaler ADM がシステムスキャンの日付と時刻を決定し、ユーザーが変更することはできません。

機能	説明
オンデマンドスキャン	必要に応じてインスタンスを手動でスキャンできます。最後のシステムスキャンからの経過時間が長い場合は、オンデマンドスキャンを実行して現在のセキュリティ状況を評価できます。または、修正を適用した後にスキャンして、修正後の状態を評価します。
CVE インパクト分析	インフラストラクチャに影響を及ぼすすべての CVE と影響を受けたすべての NetScaler インスタンスの結果を表示し、修正を提案します。この情報を使用して、セキュリティリスクを修正するための修正を適用します。
ログをスキャン	直近の 5 回のスキャンのコピーを保存します。これらのレポートは CSV および PDF 形式でダウンロードして分析できます。
CVE リポジトリ	Citrix が 2019 年 12 月以降に発表した、NetScaler インフラストラクチャに影響を与える可能性のある、すべての NetScaler 関連の CVE を詳細に表示します。このビューを使用すると、セキュリティアドバイザリスコープの CVE を理解し、CVE について詳しく知ることができます。サポートされていない CVE については、セキュリティアドバイザリの「サポートされていない CVE」を参照してください。

注意事項

- セキュリティアドバイザリは、製造終了（EOL）に達した NetScaler ビルドをサポートしていません。NetScaler がサポートするビルドまたはバージョンにアップグレードすることをお勧めします。
- CVE 検出がサポートされているインスタンス：すべての NetScaler（SDX、MPX、VPX）とゲートウェイ。
- サポートされている CVE: 2019 年 12 月以降のすべての CVE。

  > 注:
  >
  > Windows 用 NetScaler Gateway プラグインに影響する脆弱性の検出と修復は、NetScaler ADM セキュリティアドバイザリではサポートされていません。サポートされていない CVE については、セキュリティアドバイザリの「サポートされていない CVE」を参照してください。

- NetScaler ADM セキュリティアドバイザリは、脆弱性を特定する際に、機能の構成ミスを一切考慮していません。
- NetScaler ADM セキュリティアドバイザリは、CVE の識別と修復のみをサポートします。セキュリティに関する記事で取り上げられているセキュリティ上の問題の特定と修正はサポートしていません。

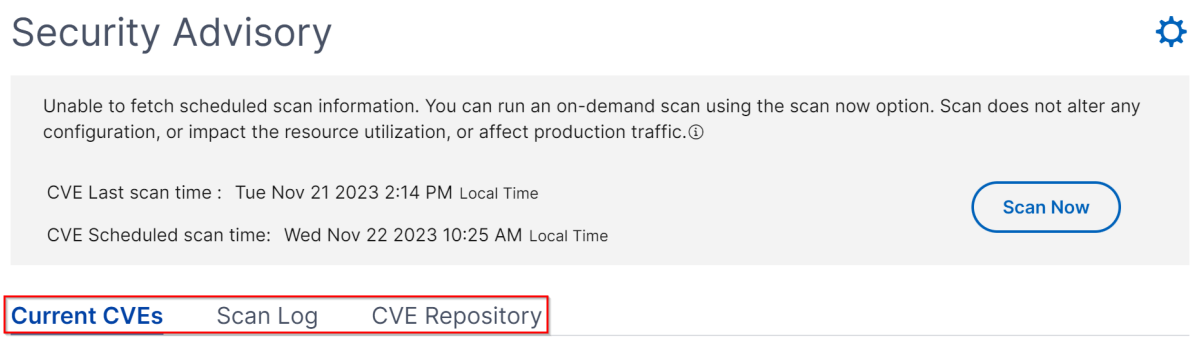
- NetScaler、Gateway リリースの範囲：この機能はメインビルドに限定されています。セキュリティアドバイザリには、その範囲に特別なビルドは含まれていません。
  - セキュリティアドバイザリは Admin パーティションではサポートされていません。
- CVE では次の種類のスキャンが可能です。
  - バージョンスキャン: このスキャンでは、NetScaler ADM が NetScaler インスタンスのバージョンと、修正が適用されるバージョンおよびビルドを比較する必要があります。このバージョン比較は、NetScaler ADM セキュリティアドバイザリが NetScaler が CVE に対して脆弱であるかどうかを特定するのに役立ちます。たとえば、NetScaler リリースとビルド xx.yy で CVE が修正された場合、セキュリティアドバイザリでは、xx.yy より前のビルドのすべての NetScaler インスタンスが脆弱であると見なされます。バージョンスキャンは現在、セキュリティアドバイザリでサポートされています。
  - 構成スキャン：このスキャンでは、NetScaler ADM が CVE スキャン固有のパターンを NetScaler 構成ファイル（nsconf）と一致させる必要があります。NetScaler ns.conf ファイルに特定の構成パターンが存在する場合、そのインスタンスはその CVE に対して脆弱であると見なされます。このスキャンは通常、バージョンスキャンと共に使用されます。
    設定スキャンは現在、セキュリティアドバイザリでサポートされています。
  - カスタムスキャン：このスキャンでは、NetScaler ADM が管理対象の NetScaler インスタンスに接続し、スクリプトをプッシュしてスクリプトを実行する必要があります。スクリプト出力は、NetScaler ADM が NetScaler が CVE に対して脆弱であるかどうかを識別するのに役立ちます。例としては、特定のシェルコマンド出力、特定の CLI コマンド出力、特定のログ、特定のディレクトリまたはファイルの存在または内容が含まれます。セキュリティアドバイザリでは、設定スキャンで同じ結果が得られない場合は、複数の設定パターンに一致するカスタムスキャンも使用します。カスタムスキャンを必要とする CVE の場合、スクリプトはスケジュールスキャンまたはオンデマンドスキャンが実行されるたびに実行されます。収集されたデータと特定のカスタムスキャンのオプションの詳細については、該当の CVE のセキュリティアドバイザリドキュメントをご覧ください。
- スキャンによって NetScaler の本番トラフィックに影響が及ぶことはなく、NetScaler 上の NetScaler 構成が変更されることもありません。
- NetScaler ADM セキュリティアドバイザリは CVE 緩和をサポートしていません。NetScaler インスタンスに緩和策（一時的な回避策）を適用した場合でも、修正が完了するまで、ADM は NetScaler を脆弱な NetScaler として識別します。
- FIPS インスタンスでは、CVE スキャンはサポートされていません。

セキュリティアドバイザリダッシュボードの使用方法

セキュリティアドバイザリダッシュボードにアクセスするには、NetScaler ADM GUI から［インフラストラクチャ］**>**［インスタンスアドバイザリ］**>**［セキュリティアドバイザリ］に移動します。

ダッシュボードには、次の 3 つのタブがあります。

- 現在の CVE
- ログをスキャン
- CVE リポジトリ



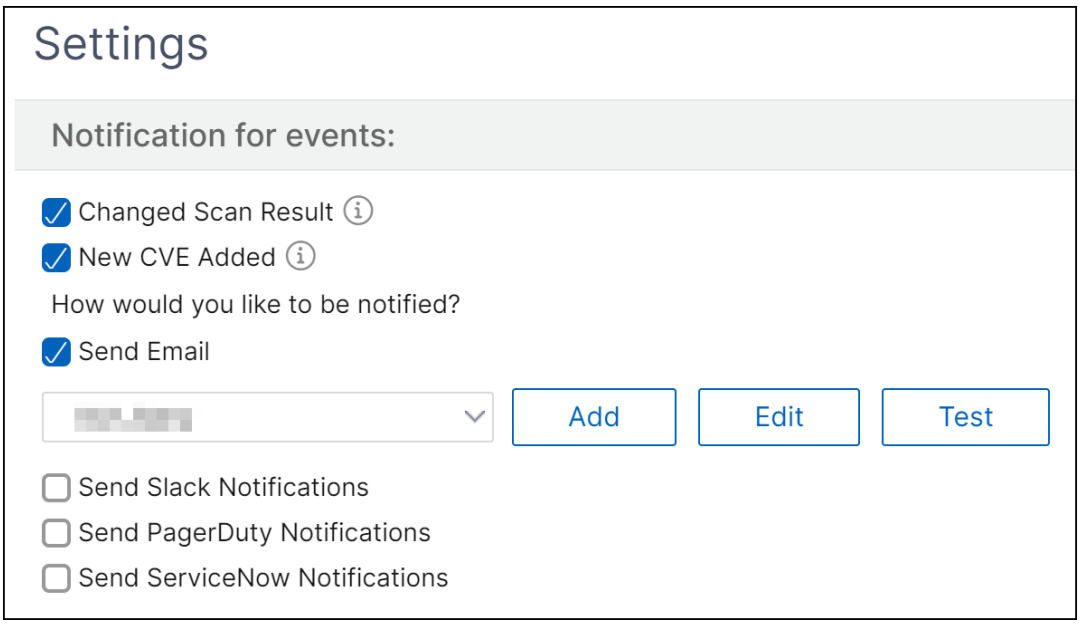
> 重要:
>
> セキュリティアドバイザリ GUI またはレポートでは、すべての CVE が表示されず、CVE が 1 つだけ表示される場合があります。回避策として、[今すぐスキャン] をクリックしてオンデマンドスキャンを実行します。スキャンが完了すると、スコープ内のすべての CVE（約 15）が UI またはレポートに表示されます。

ダッシュボードの右上隅には設定アイコンがあり、次のことができます。

- 通知を有効または無効にする。

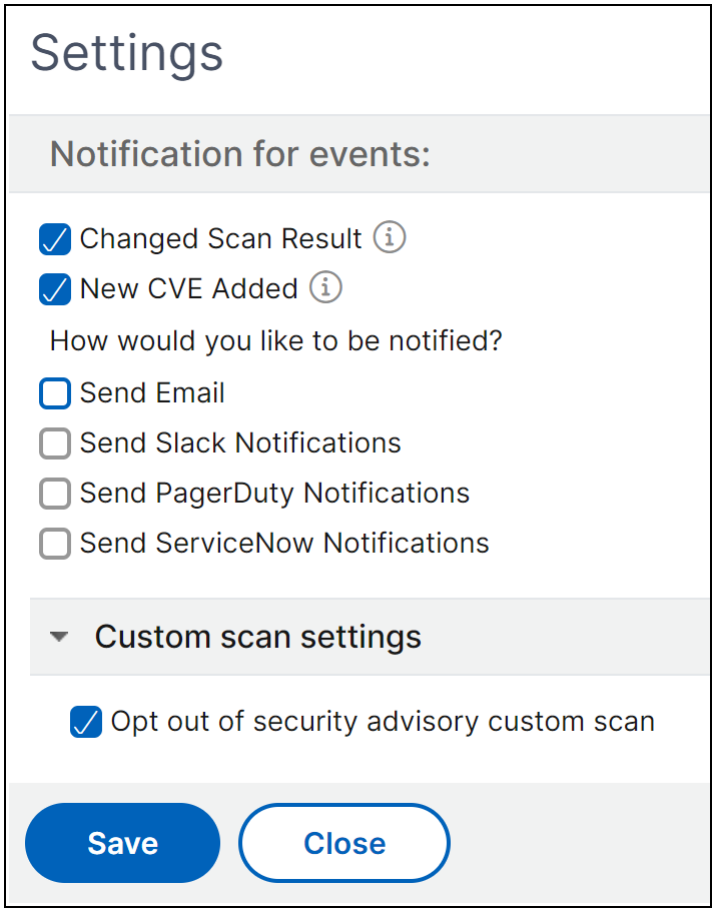
  CVE の影響に関する次の通知を受け取ることができます。

  - CVE スキャン結果の変更や CVE リポジトリに追加された新しい CVE に関する電子メール、Slack、PagerDuty、ServiceNow の通知。
  - CVE 影響スキャン結果の変更に関するクラウド通知。



- カスタムスキャンの設定

  「カスタムスキャン設定」リストをクリックすると、追加設定のチェックボックスが表示されます。チェックボックスを選択して、これらの CVE カスタムスキャンをオプトアウトすることもできます。カスタムスキャンが必要な CVE の影響は、セキュリティアドバイザリでは NetScaler インスタンスでは評価されません。



現在の **CVE**

このタブには、インスタンスに影響を与える CVE の数と、CVE の影響を受けるインスタンスが表示されます。タブはシーケンシャルではなく、管理者として、ユースケースに応じてこれらのタブを切り替えることができます。

NetScaler インスタンスに影響を与える CVE の数を示す表には、以下の詳細があります。

CVE ID: インスタンスに影響する CVE の ID。

発行日: その CVE のセキュリティ情報が公開された日付。

重要度スコア: 重要度タイプ (高/中/重大) とスコア。スコアを確認するには、重要度タイプにカーソルを合わせます。

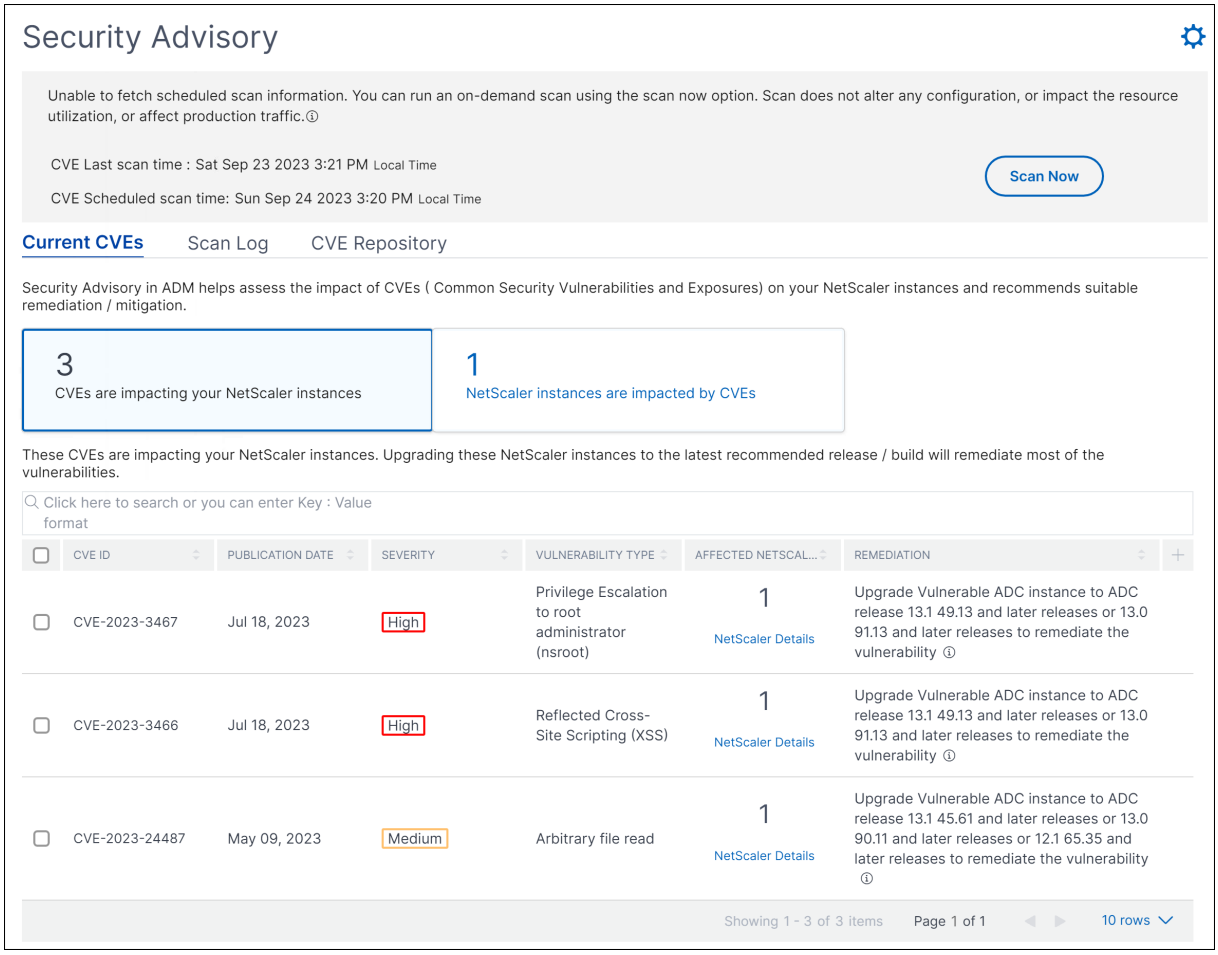
脆弱性タイプ: この CVE の脆弱性のタイプ。

影響を受ける **NetScaler** インスタンス: CVE ID が影響しているインスタンス数。カーソルを合わせると、NetScaler インスタンスのリストが表示されます。

修復: 利用可能な是正。インスタンスのアップグレード (通常は) または構成パックの適用です。

同じインスタンスは、複数の CVE によって影響を受ける可能性があります。この表では、1 つの特定の CVE または複数の選択した CVE が影響しているインスタンスの数を確認できます。影響を受けるインスタンスの **IP** アドレスを確認するには、「影響を受ける **NetScaler** インスタンス」の「**NetScaler** 詳細」にカーソルを合わせます。影響を受けるインスタンスの詳細を確認するには、テーブルの下部にある [影響を受けるインスタンスの表示] をクリックします。
プラス記号をクリックして、テーブルの列を追加または削除することもできます。

この画面では、インスタンスに影響を与える CVE の数は 3 つの CVE で、これらの CVE の影響を受けるインスタンスは 1 つです。

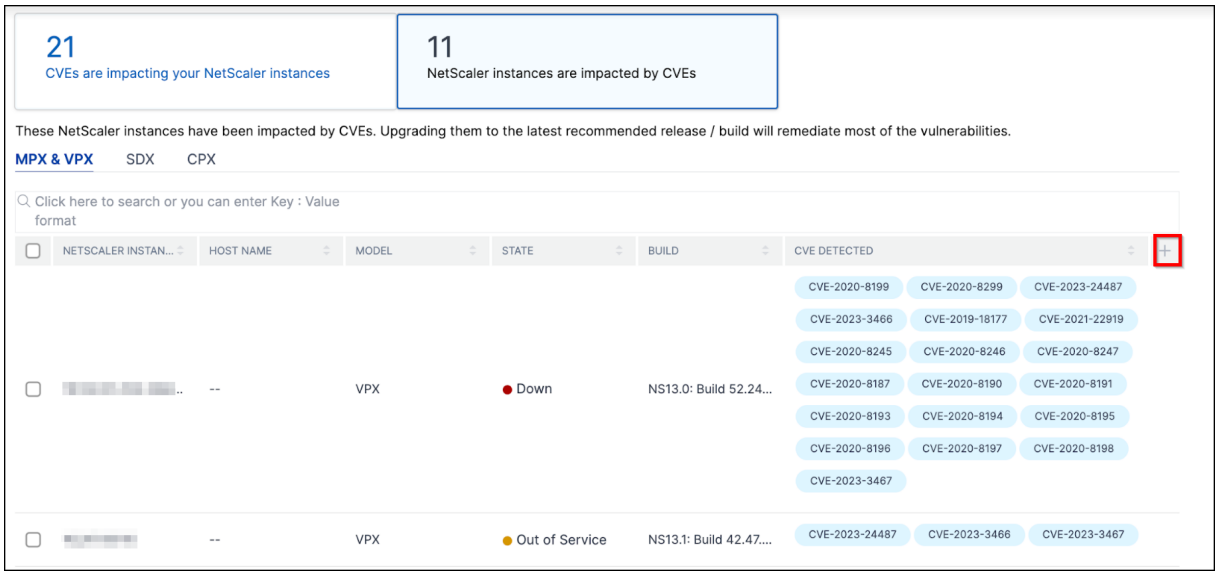


<number of> NetScaler インスタンスは **CVE** の影響を受けます。タブには、影響を受けるすべての **NetScaler** ADM NetScaler インスタンスが表示されます。表には次の詳細が表示されます。

- NetScaler IP アドレス
- ホスト名
- NetScaler モデル番号

- NetScaler 状態
- ソフトウェアバージョンとビルド
- NetScaler に影響を及ぼす脆弱性データの一覧です。

+ 記号をクリックすると、必要に応じてこれらの列を追加または削除できます。



脆弱性の問題を解決するには、NetScaler インスタンスを選択し、推奨される修正を適用します。ほとんどの CVE は修復としてアップグレードが必要ですが、他の CVE は修復としてアップグレードと追加の手順が必要です。

- CVE-2020-8300 の修復については、CVE-2020-8300 の脆弱性の修復を参照してください。
- CVE-2021-22927 と CVE-2021-22920 については、CVE-2021-22927 と CVE-2021-22920 の脆弱性の修復を参照してください。
- CVE CVE-2021-22956 については、「CVE-2021-22956 の脆弱性の特定と修正」を参照してください
- CVE CVE-2022-27509 については、CVE-2022-27509 の脆弱性の修復を参照してください

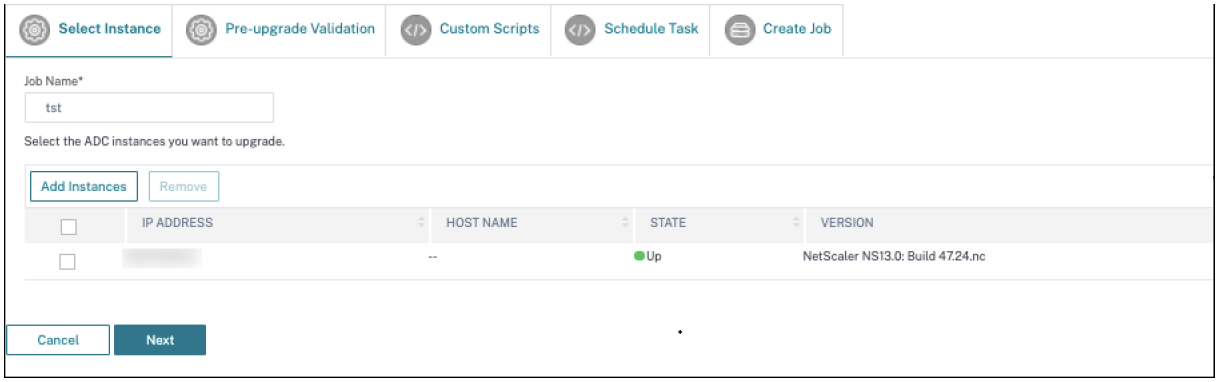
> 注
>
> NetScaler インスタンスにカスタマイズがある場合は、NetScaler のアップグレードを計画する前に、「カスタマイズされた NetScaler 構成のアップグレードに関する考慮事項」を参照してください。

アップグレード：脆弱な NetScaler インスタンスを、修正されたリリースとビルドにアップグレードできます。この詳細は、「是正」列に表示されます。アップグレードするには、インスタンスを選択し、[**Proceed to Upgrade]** ワークフローをクリックします。アップグレードワークフローでは、脆弱な NetScaler がターゲットの NetScaler として自動的に入力されます。

> 注
>
> 12.0、11,0、10.5 以降のリリースは、すでにサポート終了 (EOL) です。NetScaler インスタンスがこれらのリリースのいずれかで実行されている場合は、サポートされているリリースにアップグレードしてください。

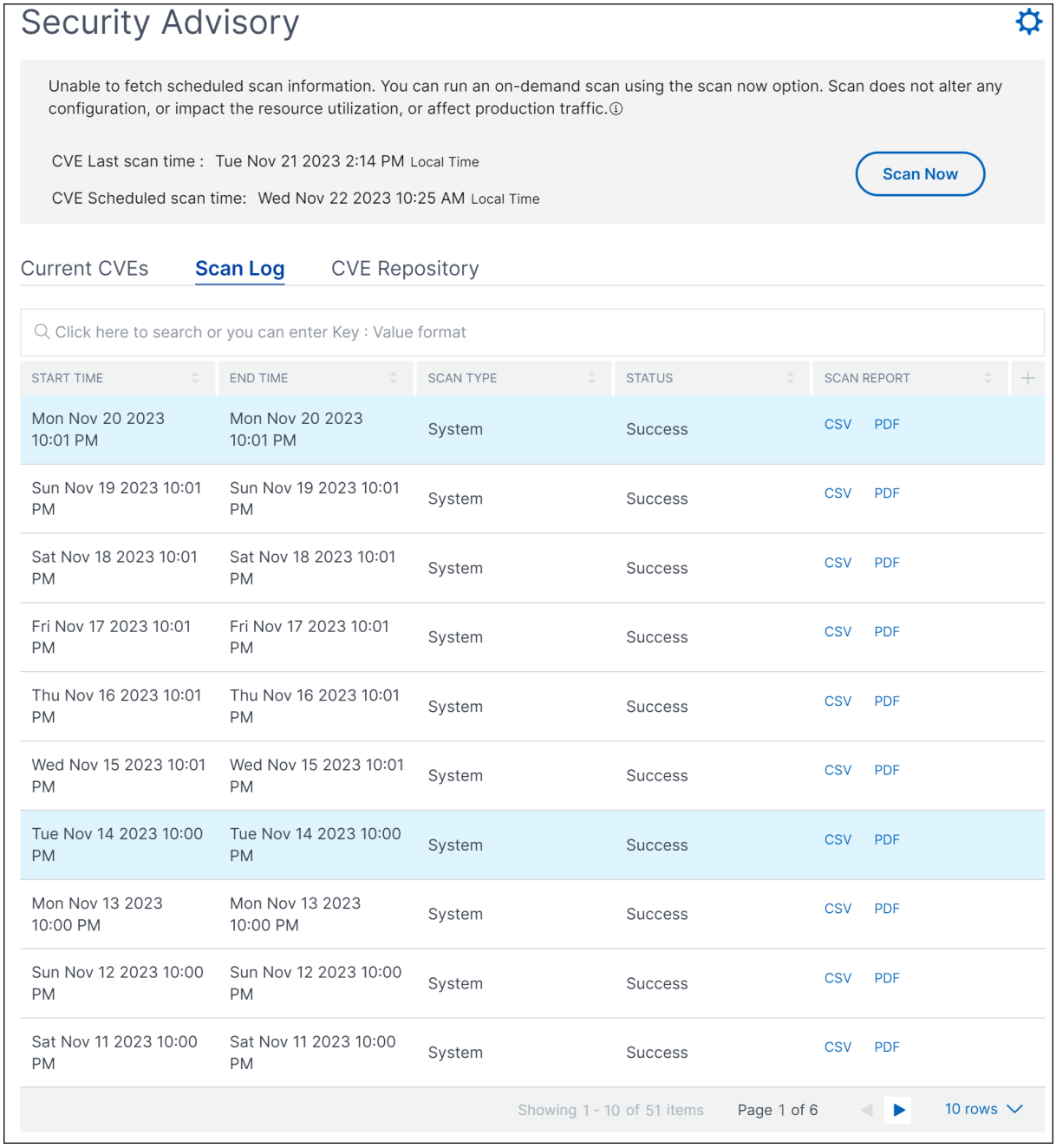
アップグレードワークフローが開始されます。NetScaler ADM を使用して NetScaler インスタンスをアップグレードする方法について詳しくは、「ジョブを使用して NetScaler インスタンスをアップグレードする」を参照してください。

> 注
>
> アップグレード先のリリースとビルドは、ユーザーの判断によります。どのリリースとビルドにセキュリティ修正が適用されているかを確認するには、修復列の下のアドバイスを参照してください。それに応じて、サポート対象のリリースとビルドを選択しますが、まだサポートが終了していません。



ログをスキャン

このタブには、デフォルトのシステムスキャンとオンデマンドのユーザー開始スキャンの両方を含む、過去 5 回の CVE スキャンのレポートが表示されます。各スキャンのレポートは CSV および PDF 形式でダウンロードできます。オンデマンドスキャンが進行中の場合は、完了状況も確認できます。

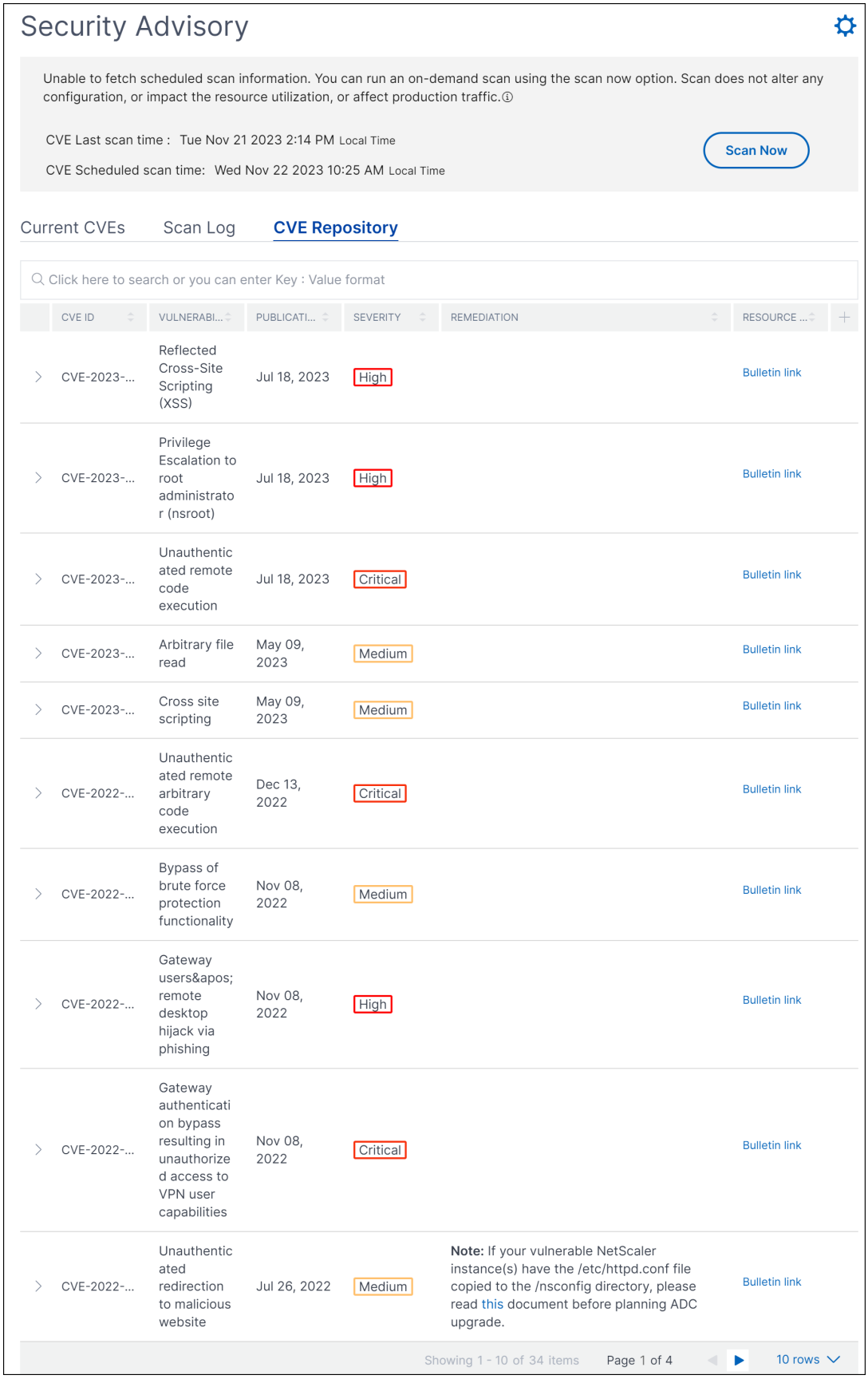


CVE リポジトリ

このタブには、2019 年 12 月のすべての CVE の最新情報と、以下の詳細が含まれています。

- CVE ID
- 脆弱性タイプ
- 発行日

- 重大度レベル
- 修復
- セキュリティ情報へのリンク



Security Advisory

Unable to fetch scheduled scan information. You can run an on-demand scan using the scan now option. Scan does not alter any configuration, or impact the resource utilization, or affect production traffic.

CVE Last scan time : Tue Nov 21 2023 2:14 PM Local Time

CVE Scheduled scan time: Wed Nov 22 2023 10:25 AM Local Time

Scan Now

Current CVEs | Scan Log | CVE Repository

Click here to search or you can enter Key : Value format

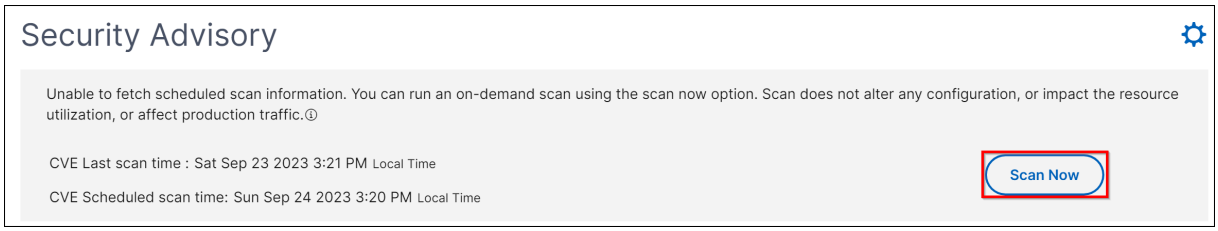
CVE ID	VULNERABI...	PUBLICATI...	SEVERITY	REMEDIATION	RESOURCE ...
CVE-2023-...	Reflected Cross-Site Scripting (XSS)	Jul 18, 2023	High		Bulletin link
CVE-2023-...	Privilege Escalation to root administrator (nsroot)	Jul 18, 2023	High		Bulletin link
CVE-2023-...	Unauthenticated remote code execution	Jul 18, 2023	Critical		Bulletin link
CVE-2023-...	Arbitrary file read	May 09, 2023	Medium		Bulletin link
CVE-2023-...	Cross site scripting	May 09, 2023	Medium		Bulletin link
CVE-2022-...	Unauthenticated remote arbitrary code execution	Dec 13, 2022	Critical		Bulletin link
CVE-2022-...	Bypass of brute force protection functionality	Nov 08, 2022	Medium		Bulletin link
CVE-2022-...	Gateway users' remote desktop hijack via phishing	Nov 08, 2022	High		Bulletin link
CVE-2022-...	Gateway authentication bypass resulting in unauthorized access to VPN user capabilities	Nov 08, 2022	Critical		Bulletin link
CVE-2022-...	Unauthenticated redirection to malicious website	Jul 26, 2022	Medium	**Note:** If your vulnerable NetScaler instance(s) have the /etc/httpd.conf file copied to the /nsconfig directory, please read this document before planning ADC upgrade.	Bulletin link

Showing 1 - 10 of 34 items Page 1 of 4 10 rows

今すぐスキャン

必要に応じて、いつでもインスタンスをスキャンできます。

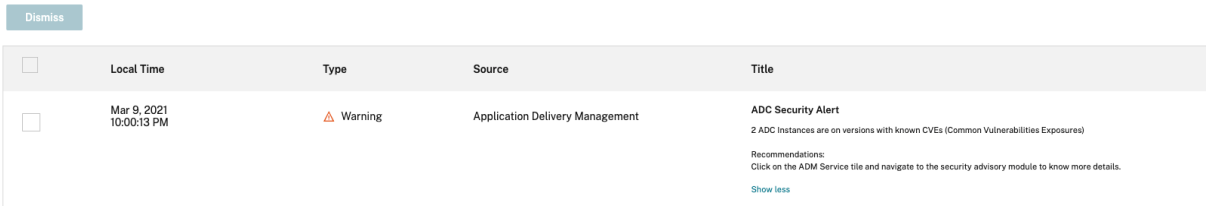
「今すぐスキャン」をクリックして、NetScaler インスタンスに影響を与えている CVE をスキャンします。スキャンが完了すると、改訂されたセキュリティの詳細がセキュリティアドバイザリ GUI に表示されます。



NetScaler ADM はスキャンを完了するまでに数分かかります。

通知

管理者には、CVE によって脆弱な NetScaler インスタンスがいくつあるかを示す Citrix Cloud 通知が届きます。通知を確認するには、NetScaler ADM GUI の右上隅にあるベルのアイコンをクリックします。



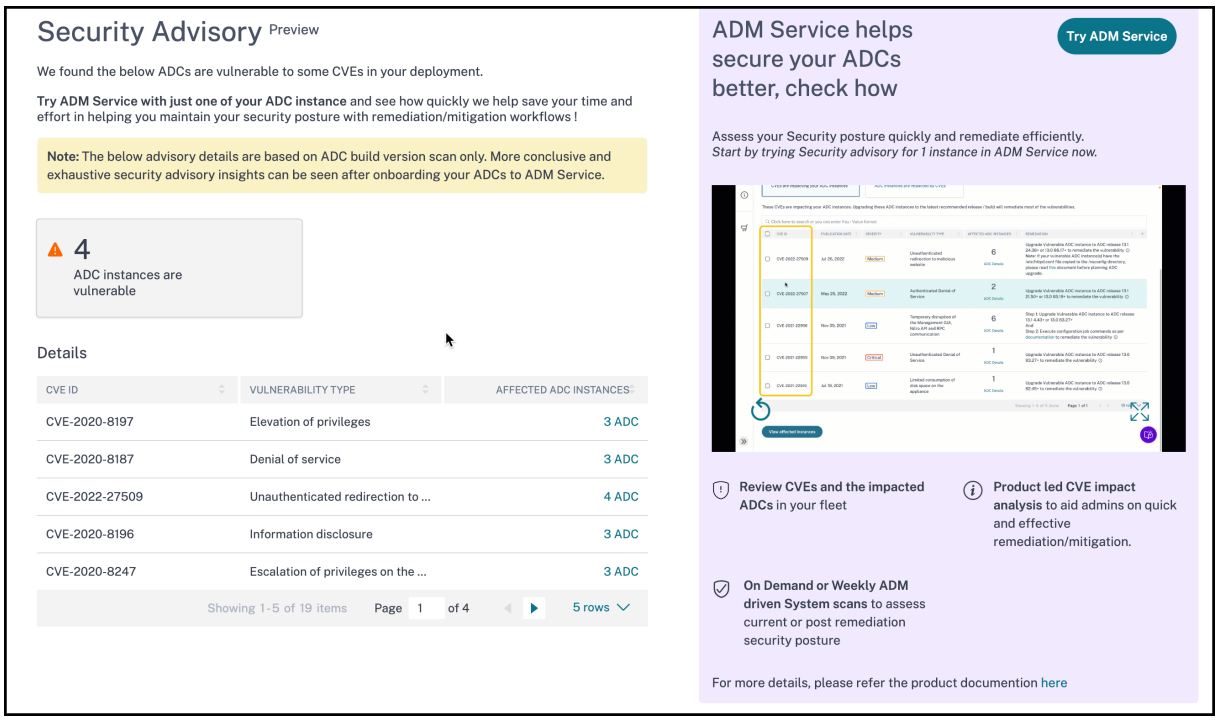
14.1 4.x 以前のビルドのセキュリティアドバイザリ

以前のビルドを使用している場合は、セキュリティアドバイザリ機能のプレビューバージョンしか使用できません。プレビューバージョンでは、リスクのある NetScaler CVE と ADM サービスにオンボーディングされた ADC インスタンスのみが強調表示されます。セキュリティアドバイザリ機能のフルバージョンを使用する場合は、ADM On-Prem Cloud Connector を有効にする必要があります。

> 重要
>
> CVE の影響に関する詳細な分析、カスタムスキャン/システムスキャンに関する決定的な情報、修復および軽減ワークフローについては、**NetScaler ADM Service** をお試しください。

セキュリティ勧告を見る

セキュリティアドバイザリにアクセスするには、インフラストラクチャ > インスタンスアドバイザリ > セキュリティアドバイザリに移動します。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。



NetScaler ADM オンプレミスセキュリティアドバイザリは ADC バージョンスキャンのみを実行して CVE をチェックし、次の情報が表示されます。

- **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。

NetScaler ADM オンプレミスセキュリティアドバイザリでは、ADC インスタンスのいずれかを選択して ADC インスタンスを ADM サービスにオンボーディングすることもできます。「**ADM** サービスを試す」をクリックし、ADC インスタンスを ADM サービスにオンボーディングします。ADM サービスセキュリティアドバイザリを使用すると、特定の CVE の脆弱性タイプを確認し、脆弱性を解決するための緩和策と修復に関する情報を取得できます。

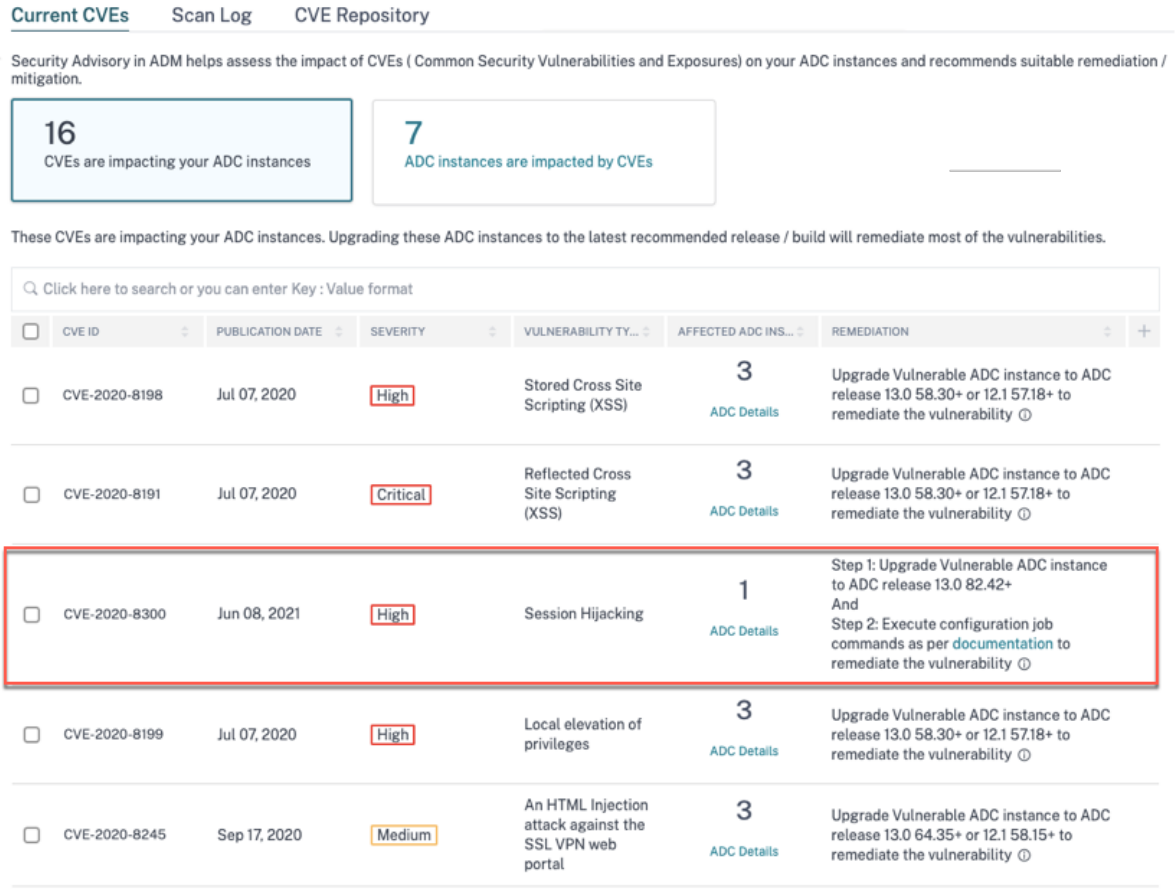
ADM サービスセキュリティアドバイザリの詳細については、セキュリティアドバイザリページの GIF アニメーションをご覧ください。

CVE-2020-8300 の脆弱性の修正

February 6, 2024

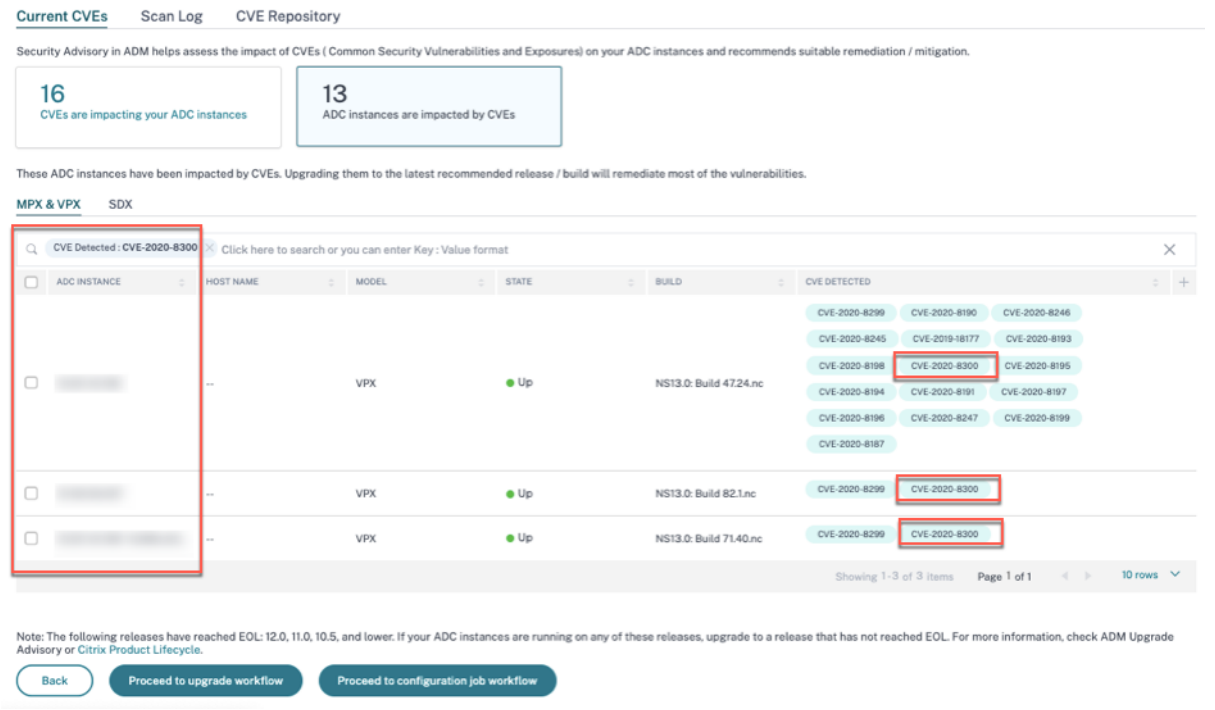
NetScaler ADM セキュリティアドバイザリダッシュボードの「現在の **CVE**」>「**<number of> ADC** インスタンスは **CVE** の影響を受ける」で、この特定の **CVE** によって脆弱なすべてのインスタンスを確認できます。

CVE-2020-8300 の影響を受けるインスタンスの詳細を確認するには、**CVE-2020-8300** を選択し、「影響を受けるインスタンスを表示」をクリックします。



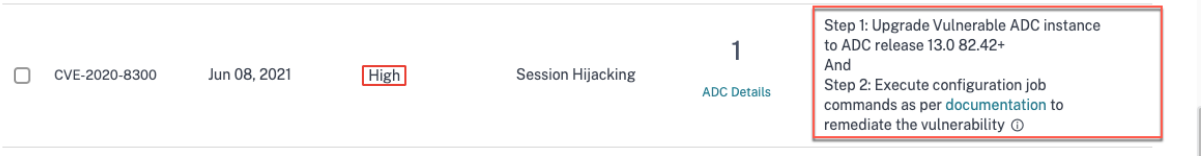
> 注
>
> セキュリティアドバイザリダッシュボードの詳細については、「セキュリティアドバイザリ」を参照してください。

<number of> CVE の影響を受ける **ADC** インスタンスのウィンドウが表示されます。ここでは、CVE-2020-8300 の影響を受けた ADC インスタンスの数と詳細を確認できます。



CVE-2020-8300 を修復してください

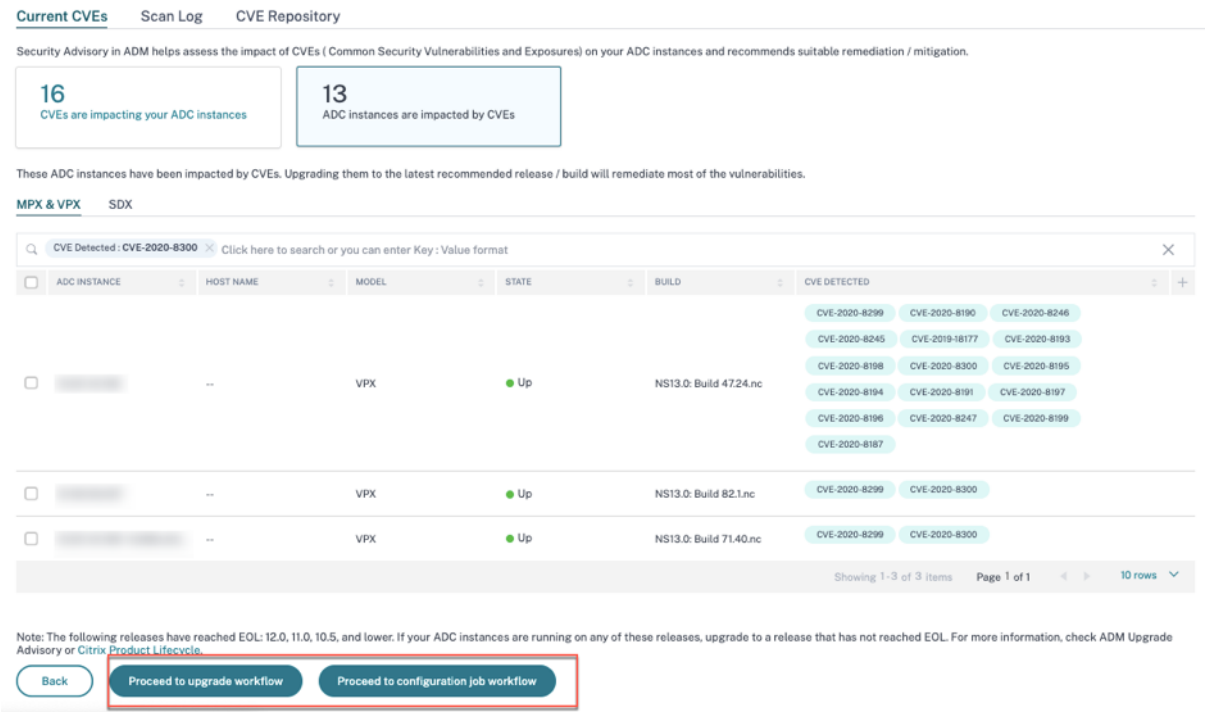
CVE-2020-8300 の影響を受ける ADC インスタンスの場合、修正は 2 段階のプロセスです。GUI の「現在の **CVE**」**>**「**ADC** インスタンスは **CVE** の影響を受ける」で、手順 1 と 2 を確認できます。



次の 2 つのステップがあります。

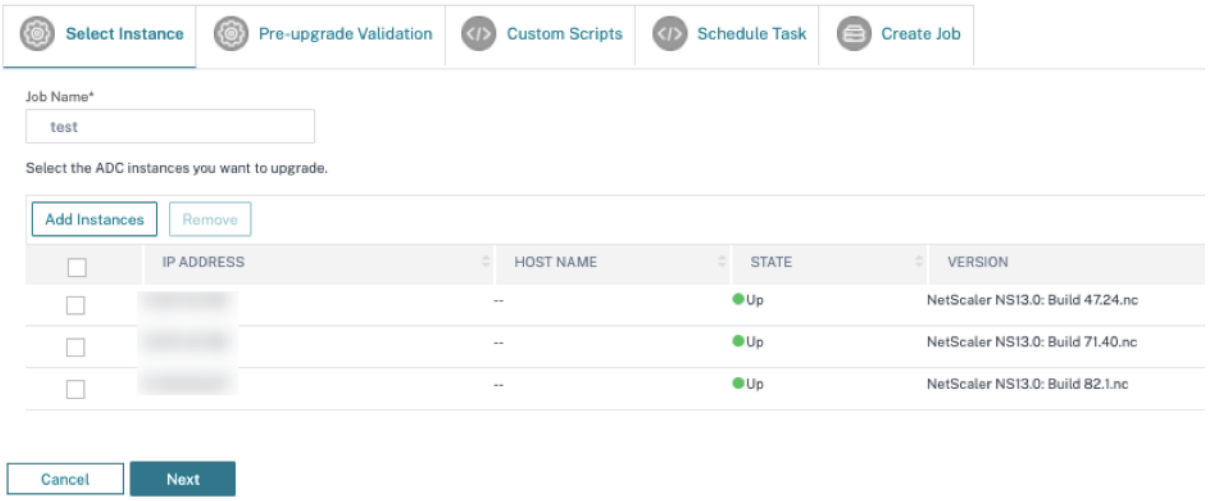
1. 脆弱な ADC インスタンスを、修正されたリリースとビルドにアップグレードします。
2. カスタマイズ可能な組み込み構成テンプレートを使用して、必要な構成コマンドを構成ジョブに適用します。脆弱な ADC ごとにこの手順を 1 つずつ実行し、その ADC のすべての SAML アクションと SAML プロファイルを含めてください。

「**Current CVES > CVE** の影響を受ける **ADC** インスタンス」に、この 2 段階の修正プロセスについて、「アップグレードワークフローに進む」と「設定ジョブワークフローに進む」の **2** つのワークフローが表示されます。



ステップ **1:** 脆弱な **ADC** インスタンスをアップグレードする

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、[ワークフローのアップグレードに進む] をクリックします。アップグレードワークフローは、脆弱な ADC インスタンスが既に入力されている状態で始まります。



NetScaler ADM を使用して ADC インスタンスをアップグレードする方法について詳しくは、「ADC アップグレードジョブの作成」を参照してください。

> 注
>
> このステップは、脆弱なすべての ADC インスタンスに対して一度に行うことができます。

ステップ **2:** 設定コマンドを適用する

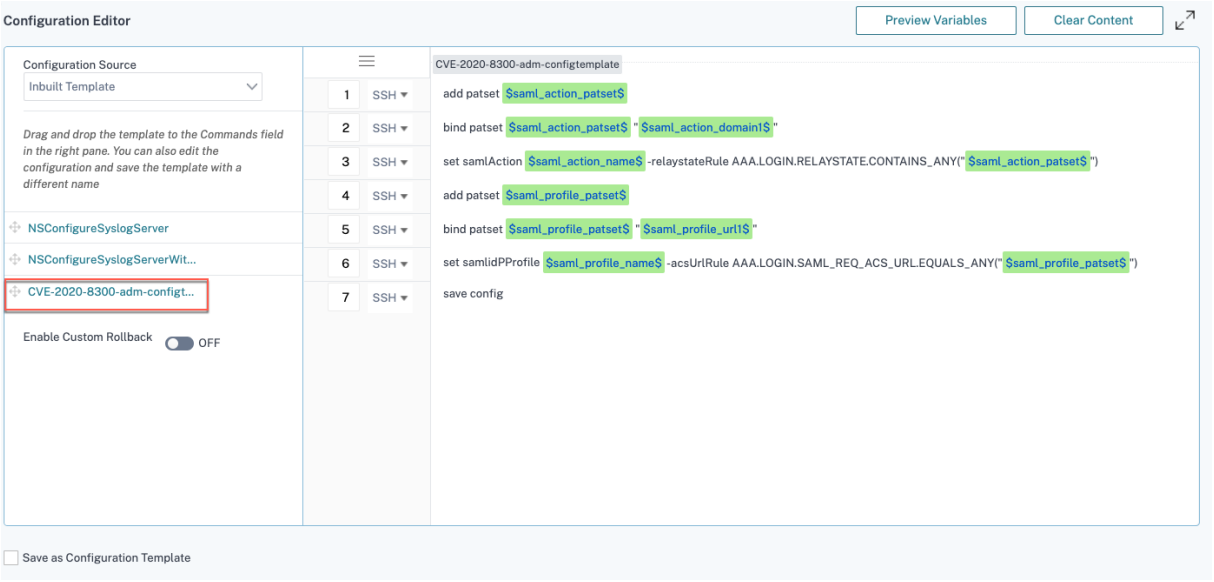
影響を受けるインスタンスをアップグレードしたら、**<number of> CVE** の影響を受ける **ADC** インスタンスウィンドウで、**CVE-2020-8300** の影響を受けるインスタンスを **1** つ選択し、「設定ジョブのワークフローに進む」をクリックします。ワークフローには次のステップが含まれます。

1. 構成をカスタマイズします。
2. 自動入力された影響を受けるインスタンスを確認する。
3. ジョブの変数への入力を指定する。
4. 変数入力を入力して最終構成を確認します。
5. ジョブを実行しています。

インスタンスを選択して [設定ジョブのワークフローに進む] をクリックする前に、次の点に注意してください。

- 複数の CVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920、CVE-2021-22956 など）の影響を受ける ADC インスタンスの場合：インスタンスを選択して **[**設定ジョブのワークフローに進む] をクリックしても、組み込みの設定テンプレートは [設定の選択] に自動入力されません。セキュリティアドバイザリテンプレートの下にある適切な設定ジョブテンプレートを右側の設定ジョブペインに手動でドラッグアンドドロップします。
- CVE-2021-22956 の影響を受ける複数の ADC インスタンスのみ: すべてのインスタンスで一度に構成ジョブを実行できます。たとえば、ADC 1、ADC 2、ADC 3 があって、それらすべてが CVE-2021-22956 の影響を受けるだけだとします。これらのインスタンスをすべて選択して **[**設定ジョブのワークフローに進む] をクリックすると、組み込みの設定テンプレートが **[**設定の選択**]** に自動入力されます。
- CVE-2021-22956 およびその他の 1 つ以上の CVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920 など）の影響を受ける複数の ADC インスタンスで、各 ADC に修正を一度に適用する必要がある場合：これらのインスタンスを選択して **[**設定ジョブのワークフローに進む] をクリックすると、エラーが表示されます各 ADC で一度に構成ジョブを実行するように指示するメッセージが表示されます。

ステップ **1:** 構成を選択する　設定ジョブのワークフローでは、組み込みの構成テンプレートが **[**構成の選択**]** に自動入力されます。



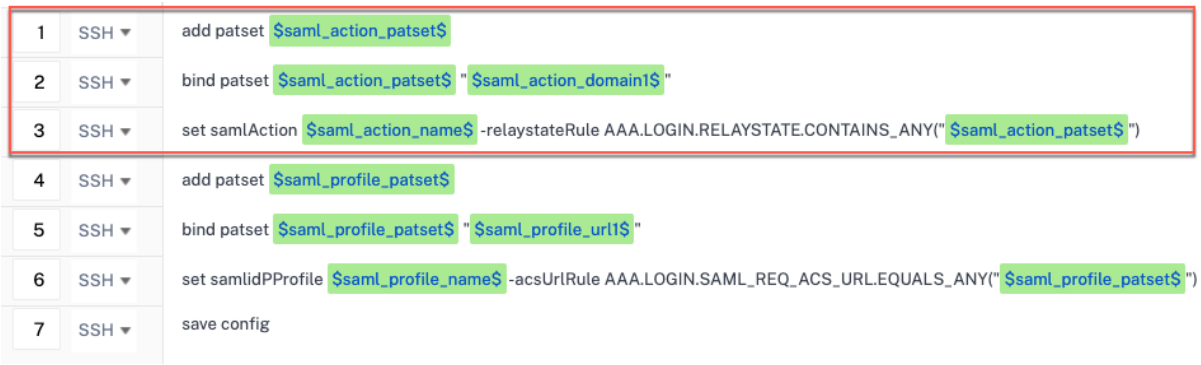
影響を受ける ADC インスタンスごとに個別の構成ジョブを 1 つずつ実行し、その ADC のすべての SAML アクションと SAML プロファイルを含めます。たとえば、脆弱な ADC インスタンスが 2 つあり、それぞれに 2 つの SAML アクションと 2 つの SAML プロファイルがある場合、この設定ジョブを 2 回実行する必要があります。ADC ごとに 1 回、すべての SAML アクションと SAML プロファイルをカバーします。

ADC 1	ADC2
ジョブ 1:2 つの SAML アクション +2 つの SAML プロファイル	ジョブ 2:2 つの SAML アクション +2 つの SAML プロファイル

ジョブに名前を付け、次の仕様に合わせてテンプレートをカスタマイズします。組み込みの構成テンプレートは、単なるアウトラインまたは基本テンプレートです。次の要件に合わせて、デプロイメントに基づいてテンプレートをカスタマイズします。

a.**SAML** アクションとそれに関連するドメイン

導入環境内の SAML アクションの数に応じて、1 ～3 行目を複製し、各 SAML アクションのドメインをカスタマイズする必要があります。



たとえば、2 つの SAML アクションがある場合、1 〜3 行目を 2 回繰り返し、それに応じて各 SAML アクションの変数定義をカスタマイズします。

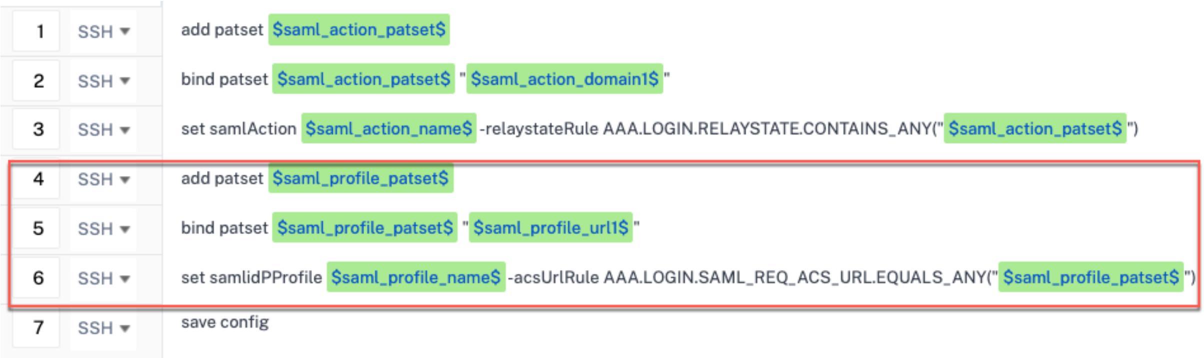
また、SAML アクションに N 個のドメインがある場合は、行`bind patset $saml_action_patset$ “$saml_action_domain1$”` を複数回手動で入力して、その SAML アクションに対して行が N 回表示されるようにする必要があります。そして、次の変数定義名を変更してください。

- `saml_action_patset`: は設定テンプレート変数で、SAML アクションのパターンセット (patset) の名前の値を表します。実際の値は、設定ジョブワークフローのステップ 3 で指定できます。このドキュメントの「ステップ 3: 変数値を指定する」セクションを参照してください。
- `saml_action_domain1`: は設定テンプレート変数で、その特定の SAML アクションのドメイン名を表します。実際の値は、設定ジョブワークフローのステップ 3 で指定できます。このドキュメントの「ステップ 3: 変数値を指定する」セクションを参照してください。

デバイスのすべての SAML アクションを検索するには、コマンド`show samlaction`を実行します。

b. **SAML** プロファイルとそれに関連する **URL**

導入環境内の SAML プロファイルの数に応じて、4 〜6 行目を繰り返します。各 SAML プロファイルの URL をカスタマイズします。



たとえば、SAML プロファイルが 2 つある場合は、4 行目から 6 行目を 2 回手動で入力し、それに応じて SAML アクションごとに変数定義をカスタマイズします。

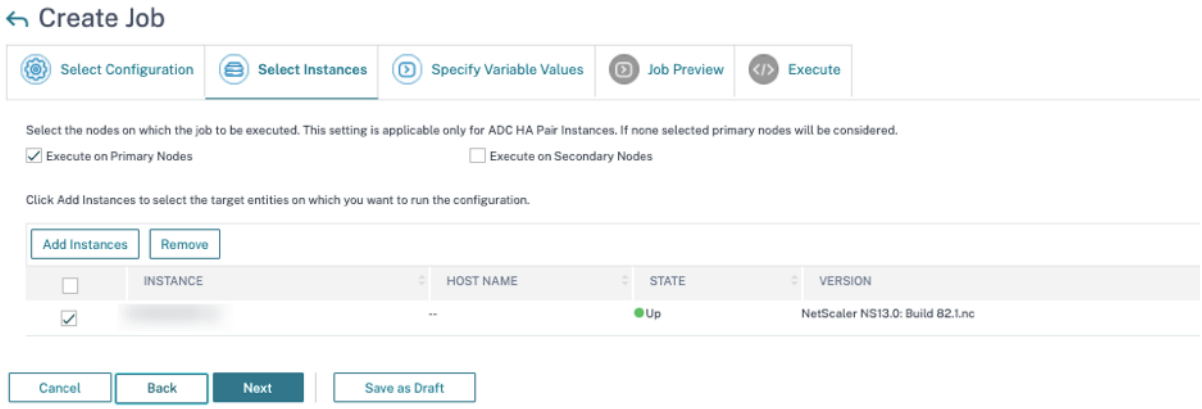
また、SAML アクションに N 個のドメインがある場合は、行`bind patset $saml_profile_patset$ “$saml_profile_url1$”` を手動で複数回入力して、その SAML プロファイルでその行が N 回表示されるようにする必要があります。そして、次の変数定義名を変更してください。

- saml_profile_patset: は設定テンプレート変数で、SAML プロファイルのパターンセット (patset) の名前の値を表します。実際の値は、設定ジョブワークフローのステップ 3 で指定できます。このドキュメントの「ステップ 3: 変数値を指定する」のセクションを参照してください。
- saml_profile_url1: は設定テンプレート変数で、その特定の SAML プロファイルのドメイン名を表します。実際の値は、設定ジョブワークフローのステップ 3 で指定できます。このドキュメントの「ステップ 3: 変数値を指定する」のセクションを参照してください。

デバイスのすべての SAM プロファイルを検索するには、コマンドshow samlidpProfileを実行します。

ステップ **2:** インスタンスを選択する

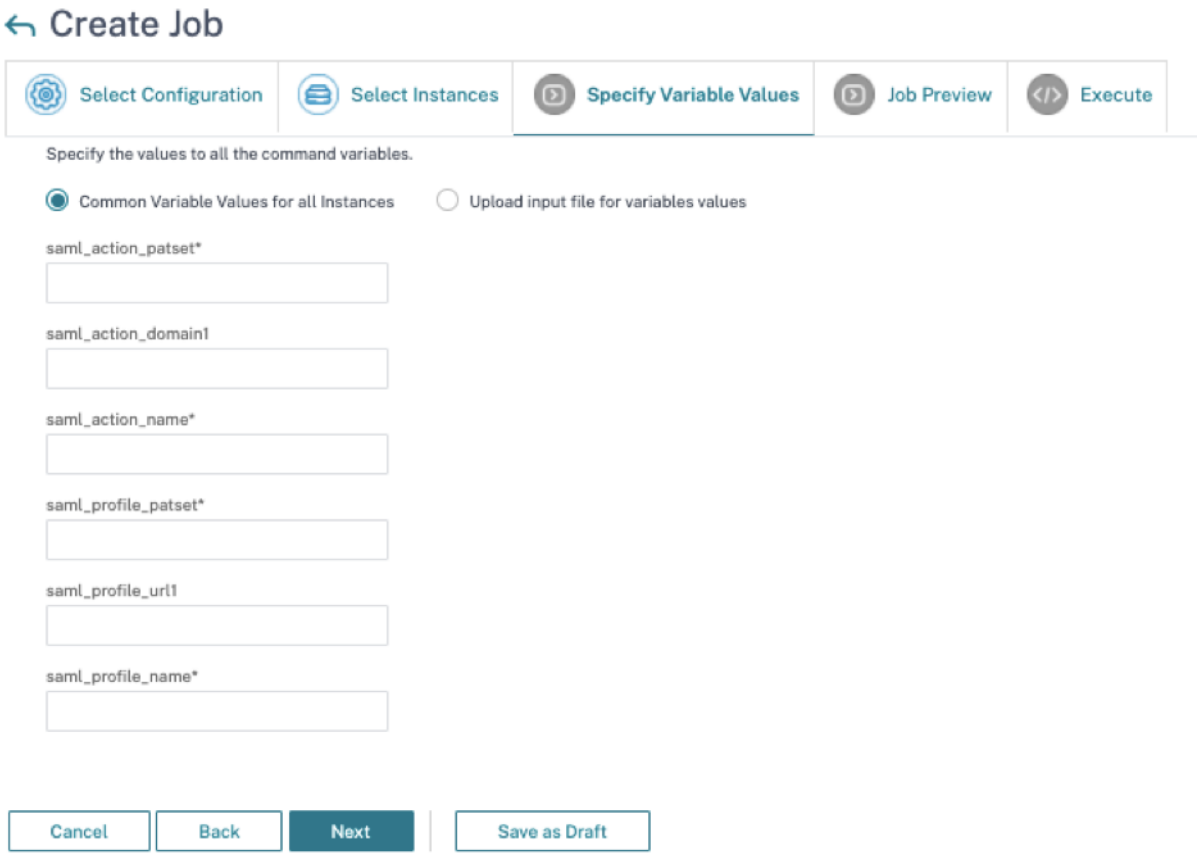
影響を受けるインスタンスは **[**インスタンスの選択**]** に自動的に入力されます。インスタンスを選択して [次へ] をクリックします。



ステップ **3:** 変数値を指定する　変数値を入力します。

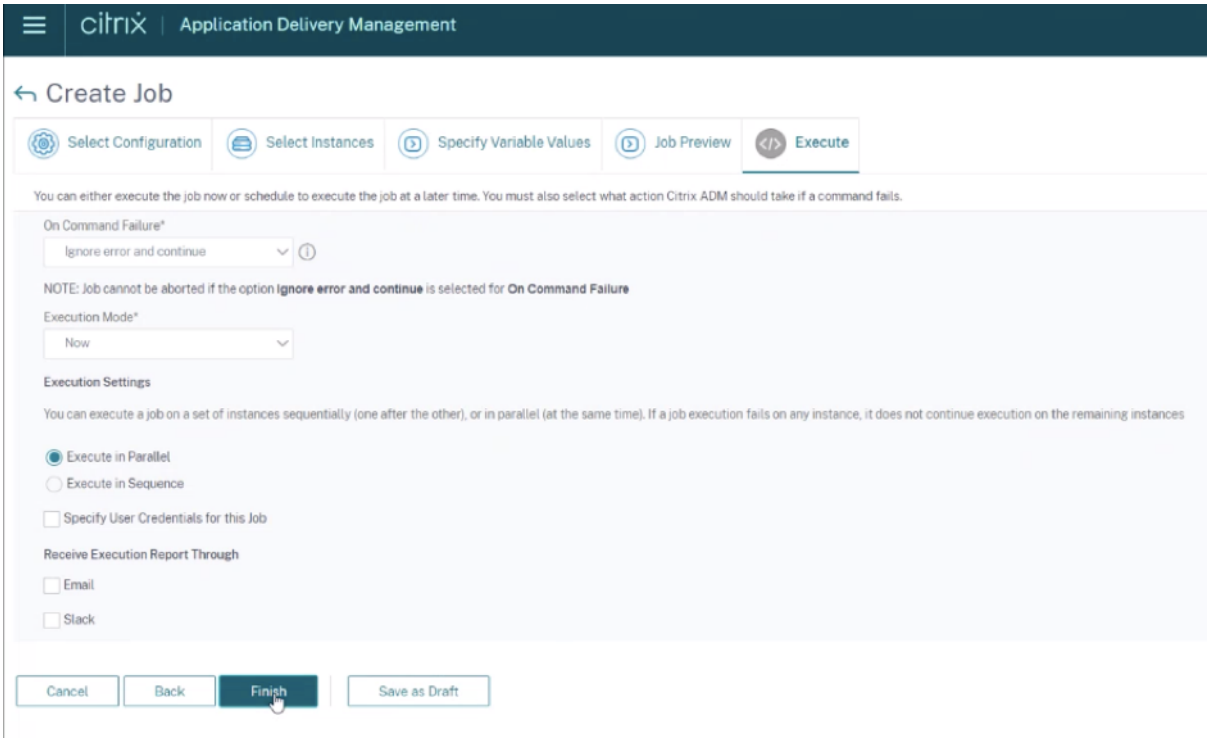
- saml_action_patset: SAML アクションの名前を追加
- saml_action_domain1: ドメインを次の形式で入力しますhttps://<example1.com>/
- saml_action_name: ジョブを設定している SAML アクションと同じものを入力します
- saml_profile_patset: SAML プロファイルの名前を追加します
- saml_profile_url1: URL を入力してくださいこの形式ですかhttps://<example2.com>/cgi/samlauth
- saml_profile_name: ジョブを設定している SAML プロファイルと同じものを入力します

> 注
>
> URL の場合、拡張子は必ずしも`cgi/samlauth`とは限りません。それはあなたが持っている第三者の認証によって異なりますので、それに応じて拡張機能を追加する必要があります。



ステップ **4:** 構成をプレビューする　設定に挿入された変数値をプレビューし、[次へ] をクリックします。

ステップ **5:** ジョブを実行する　「完了」をクリックして構成ジョブを実行します。



ジョブが実行されると、[インフラストラクチャ] **>** **[**構成**]** **>** **[**構成ジョブ**]** に表示されます。

すべての脆弱な ADC に対して 2 つの修復手順を完了したら、オンデマンドスキャンを実行して修正されたセキュリティ体制を確認できます。

NetScaler ADM Express アカウントに関する注意点

NetScaler ADM Express アカウントには、2 つの構成ジョブのみの制限など、限られた機能しかありません。

CVE-2020-8300 の修復では、脆弱な ADC インスタンスの数と同じ数の設定ジョブを実行する必要があります。そのため、Express アカウントをお持ちで、3 つ以上の構成ジョブを実行する必要がある場合は、次の回避策に従ってください。

回避策: 脆弱な 2 つの ADC インスタンスに対して 2 つの構成ジョブを実行し、次に両方のジョブを削除して、次の 2 つの脆弱な ADC インスタンスに対して次の 2 つのジョブを引き続き実行します。脆弱なインスタンスをすべてカバーするまで、これを続けてください。ジョブを削除する前に、後で参照できるようにレポートをダウンロードできます。レポートをダウンロードするには、[ネットワーク] **>** **[**ジョブ**]** でジョブを選択し、[アクション] の [ダウンロード] をクリックします。

例: 脆弱な ADC インスタンスが 6 つある場合は、2 つの脆弱なインスタンスでそれぞれ 2 つの設定ジョブを実行し、両方の設定ジョブを削除します。この手順をもう 2 回繰り返します。最後に、6 つの ADC インスタンスに対して 6 つの設定ジョブをそれぞれ実行することになります。NetScaler ADM UI の［インフラストラクチャ］**>**［ジョブ］には、最後の 2 つの構成ジョブのみが表示されます。

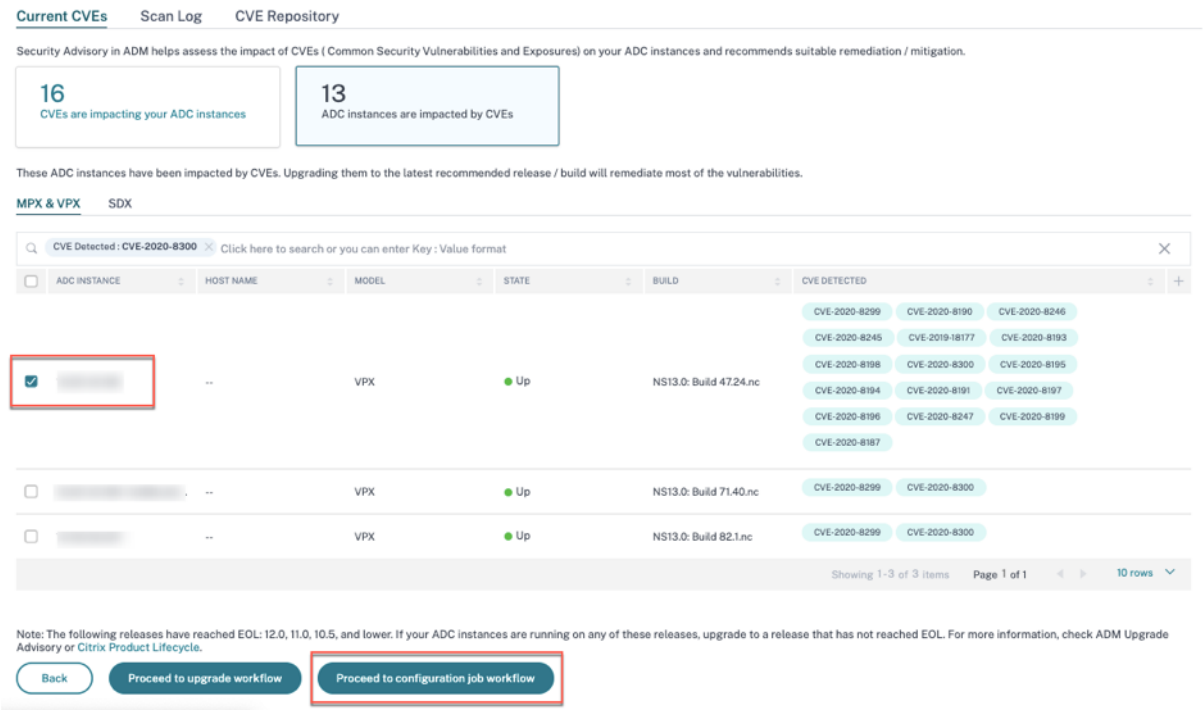
シナリオ

このシナリオでは、3 つの ADC インスタンスが CVE-2020-8300 に対して脆弱であるため、すべてのインスタンスを修正する必要があります。次の手順を実行します:

1. このドキュメントの「インスタンスのアップグレード」セクションに記載されている手順に従って、3 つの ADC インスタンスをすべてアップグレードします。
2. コンフィグレーション・ジョブのワークフローを使用して、コンフィグレーション・パッチを ADC に 1 つずつ適用します。このドキュメントの「設定コマンドの適用」セクションに記載されている手順を参照してください。

脆弱性のある ADC 1 の構成は次のとおりです。

2 つの SAML アクション	2 つの SAML プロファイル
SAML アクション 1 には 1 つのドメインがあり、SAML アクション 2 には 2 つのドメインがあります	SAML プロファイル 1 には 1 つの URL があり、SAML プロファイル 2 には 2 つの URL があります



ADC 1 を選択し、「設定ジョブのワークフローに進む」をクリックします。組み込みテンプレートは自動入力されます。次に、ジョブ名を指定し、指定された構成に従ってテンプレートをカスタマイズします。

次の表は、カスタマイズされたパラメータの変数定義を示しています。

表 1. SAML アクションの変数定義

ADC 構成	patset の変数定義	SAML アクション名の変数定義	ドメインの変数定義
SAML アクション 1 には 1 つのドメインがあります	saml_action_patset1	saml_action_name1	saml_action_domain1
SAML アクション 2 には 2 つのドメインがあります	saml_action_patset2	saml_action_name2	saml_action_domain2、saml_action_domain3

表 2. SAML プロファイルの変数定義

ADC 構成	patset の変数定義	SAML プロファイル名の変数定義	URL の変数定義
SAML プロファイル 1 には 1 つの URL があります	saml_profile_patset1	saml_profile_name1	saml_profile_url1
SAML プロファイル 2 には 2 つの URL があります	saml_profile_patset2	saml_profile_name2	saml_profile_url2、saml_profile_url3

[インスタンスを選択**]** で [ADC 1] を選択し、[次へ] をクリックします。**[**変数値の指定] ウィンドウが表示されます。このステップでは、前のステップで定義したすべての変数の値を指定する必要があります。

次に、変数を確認します。

[次へ] をクリックし、[完了] をクリックしてジョブを実行します。

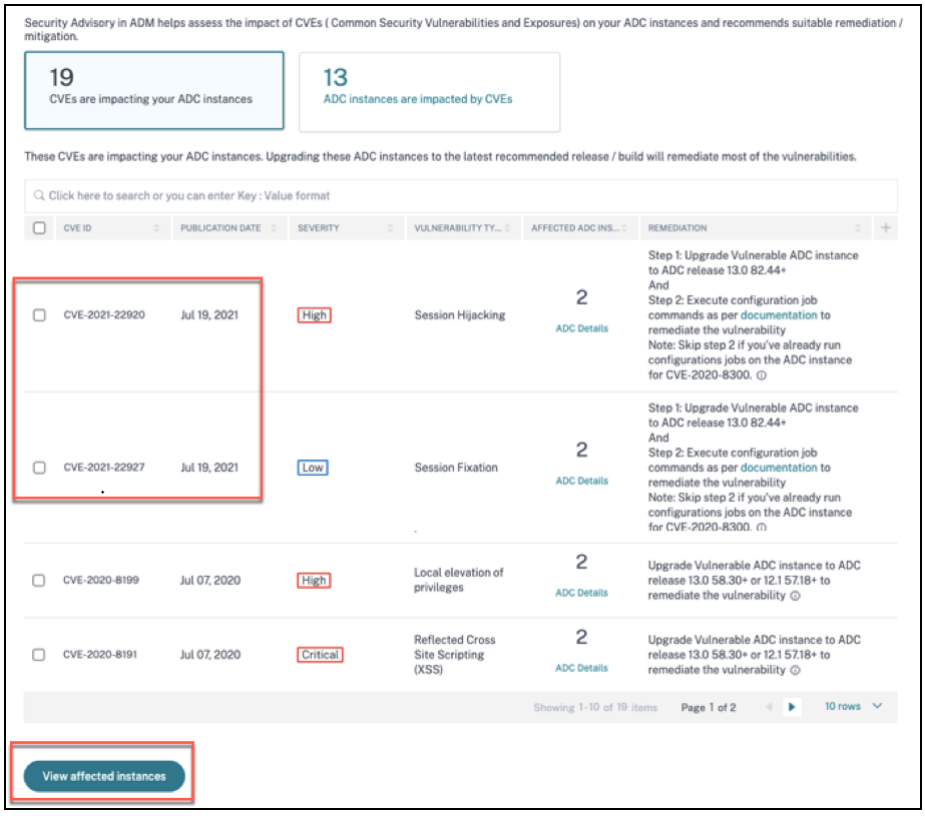
ジョブが実行されると、[インフラストラクチャ] > [構成] > [構成ジョブ] に表示されます。

ADC1 の 2 つの修復手順を完了したら、同じ手順に従って ADC 2 と ADC 3 を修正します。修正が完了したら、オンデマンドスキャンを実行して、修正されたセキュリティ体制を確認できます。

CVE-2021-22927 と CVE-2021-22920 の脆弱性の修正

February 6, 2024

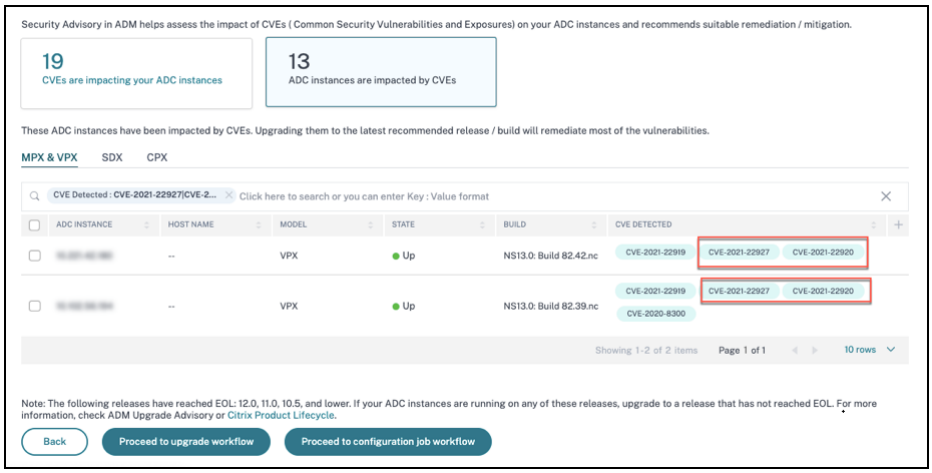
NetScaler ADM セキュリティアドバイザリダッシュボードの [現在の **CVE] > [<number of> ADC** インスタンスは **CVE** の影響を受ける] で、**CVE-2021-22927** および **CVE-2021-22920** によって脆弱なすべてのインスタンスを確認できます。これら 2 つの CVE の影響を受けるインスタンスの詳細を確認するには、1 つ以上の CVE を選択し、「影響を受けるインスタンスを表示」をクリックします。



> 注
>
> セキュリティアドバイザリシステムのスキャンが終了し、CVE-2021-22927 と CVE-2021-22920 の影響をセキュリティアドバイザリモジュールに反映させるには、数時間かかる場合があります。影響をより早く確認す

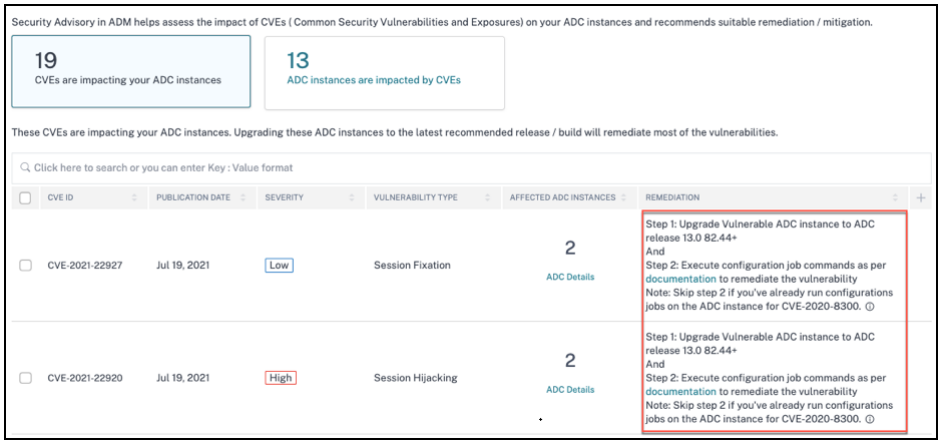
> るには、[**Scan-Now**] をクリックしてオンデマンドスキャンを開始します。
>
> セキュリティアドバイザリダッシュボードの詳細については、「セキュリティアドバイザリ」を参照してください。

<number of> CVE の影響を受ける **ADC** インスタンスのウィンドウが表示されます。次の画面キャプチャでは、CVE-2021-22927 と CVE-2021-22920 の影響を受ける ADC インスタンスの数と詳細を確認できます。



CVE-2021-22927 と **CVE-2021-22920** を修復してください

CVE-2021-22927 および CVE-2021-22920 の影響を受ける ADC インスタンスの場合、修正は 2 段階のプロセスです。GUI の「現在の **CVE**」**>**「**ADC** インスタンスは **CVE** の影響を受ける」で、手順 1 と 2 を確認できます。

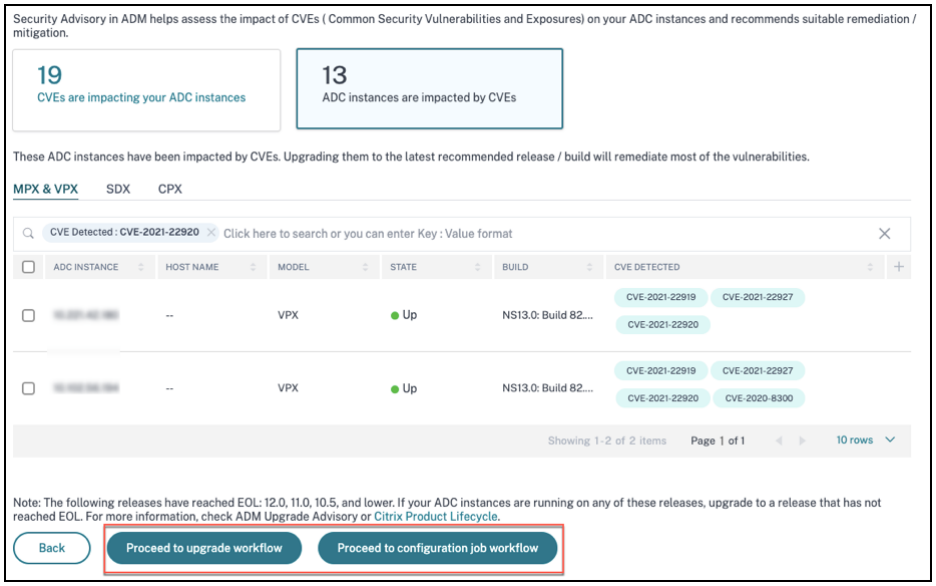


次の 2 つのステップがあります。

1. 脆弱な ADC インスタンスを、修正されたリリースとビルドにアップグレードします。
2. カスタマイズ可能な組み込み構成テンプレートを使用して、必要な構成コマンドを構成ジョブに適用します。脆弱な ADC ごとにこの手順を 1 つずつ実行し、その ADC のすべての SAML アクションを含めてください。

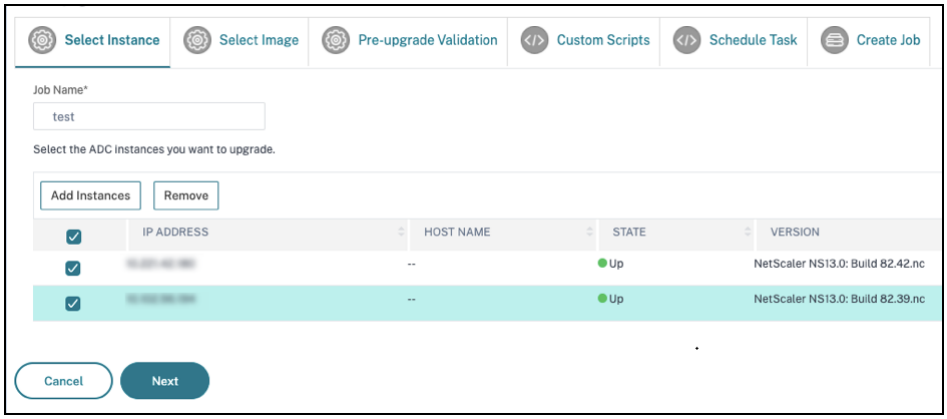
> 注
>
> CVE-2020-8300の ADC インスタンスで設定ジョブをすでに実行している場合は、ステップ 2 をスキップしてください。

「**Current CVES > CVE** の影響を受ける **ADC** インスタンス」に、この 2 段階の修正プロセスについて、「アップグレードワークフローに進む」と「設定ジョブワークフローに進む」の **2** つのワークフローが表示されます。



ステップ **1:** 脆弱な **ADC** インスタンスをアップグレードする

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、[ワークフローのアップグレードに進む] をクリックします。アップグレードワークフローは、脆弱な ADC インスタンスが既に入力されている状態で始まります。



NetScaler ADM を使用して ADC インスタンスをアップグレードする方法について詳しくは、「ADC アップグレードジョブの作成」を参照してください。

> 注
>
> このステップは、脆弱なすべての ADC インスタンスに対して一度に行うことができます。
> 注
>
> CVE-2021-22920 および CVE-2021-22927 に対して脆弱なすべての ADC インスタンスについてステップ 1 を完了したら、オンデマンドスキャンを実行します。**Current CVE** の最新のセキュリティ体制は、ADC インスタンスがこれらの CVE に対して依然として脆弱であるかどうかを理解するのに役立ちます。新しい姿勢から、構成ジョブを実行する必要があるかどうかも確認できます。
> CVE-2020-8300 の ADC インスタンスに適切な設定ジョブを既に適用していて、ADC インスタンスをアップグレードした場合、オンデマンドスキャンを実行した後、インスタンスが CVE-2020-8300、CVE-2021-22920、および CVE-2021-22927 に対して脆弱であるとは表示されなくなります。

ステップ **2:** 設定コマンドを適用する

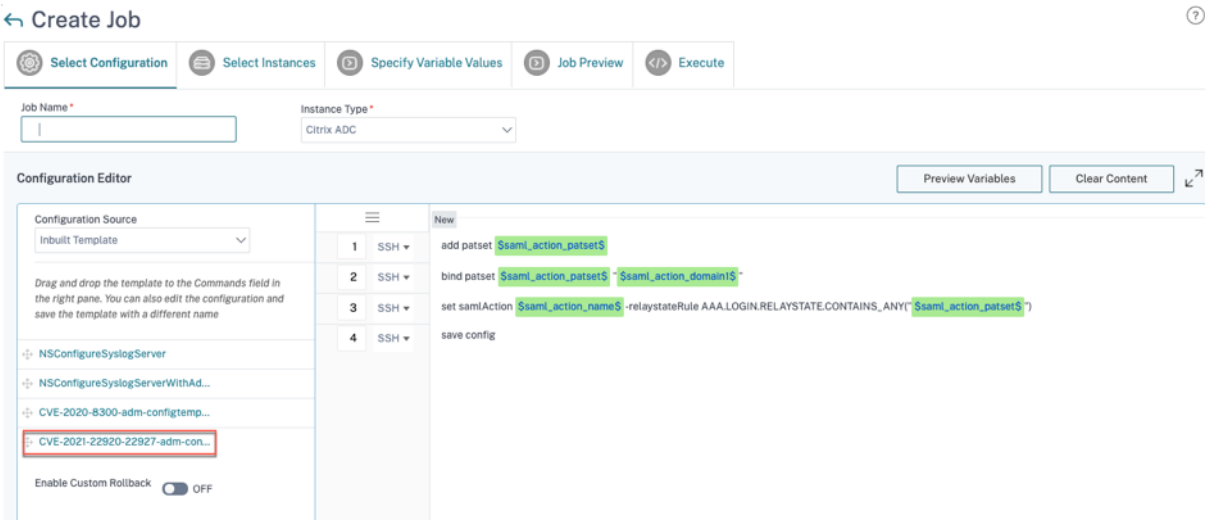
影響を受けるインスタンスをアップグレードしたら、**<number of> CVE** の影響を受ける **ADC** インスタンスウィンドウで、**CVE-2021-22927** と **CVE-2021-22920** の影響を受けるインスタンスを **1** つ選択し、「設定ジョブのワークフローに進む」をクリックします。ワークフローには次のステップが含まれます。

1. 構成をカスタマイズします。
2. 自動入力された影響を受けるインスタンスを確認する。
3. ジョブの変数への入力を指定する。
4. 変数入力を入力して最終構成を確認します。
5. ジョブを実行しています。

インスタンスを選択して [設定ジョブのワークフローに進む] をクリックする前に、次の点に注意してください。

- 複数の CVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920、CVE-2021-22956 など）の影響を受ける ADC インスタンスの場合：インスタンスを選択して **[**設定ジョブのワークフローに進む] をクリックしても、組み込みの設定テンプレートは [設定の選択] に自動入力されません。セキュリティアドバイザリテンプレートの下にある適切な設定ジョブテンプレートを右側の設定ジョブペインに手動でドラッグアンドドロップします。
- CVE-2021-22956 の影響を受ける複数の ADC インスタンスのみ: すべてのインスタンスで一度に構成ジョブを実行できます。たとえば、ADC 1、ADC 2、ADC 3 があって、それらすべてが CVE-2021-22956 の影響を受けるだけだとします。これらのインスタンスをすべて選択して **[**設定ジョブのワークフローに進む] をクリックすると、組み込みの設定テンプレートが **[**設定の選択**]** に自動入力されます。
- CVE-2021-22956 およびその他の 1 つ以上の CVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920 など）の影響を受ける複数の ADC インスタンスで、各 ADC に修正を一度に適用する必要がある場合：これらのインスタンスを選択して **[**設定ジョブのワークフローに進む] をクリックすると、エラーが表示されます各 ADC で一度に構成ジョブを実行するように指示するメッセージが表示されます。

ステップ **1:** 構成を選択する　設定ジョブのワークフローでは、組み込みの構成ベーステンプレートが **[**構成の選択**]** に自動的に入力されます。



> 注
>
> ステップ 2 で設定コマンドを適用するために選択した ADC インスタンスが CVE-2021-22927、CVE-2021-22920、および CVE-2020-8300 に対して脆弱である場合、CVE-2020-8300 の基本テンプレートは自動的に入力されます。CVE-2020-8300 テンプレートは、3 つの CVE すべてに必要な設定コマンドのスーパーセットです。ADC インスタンスのデプロイと要件に応じて、この基本テンプレートをカスタマイズします。

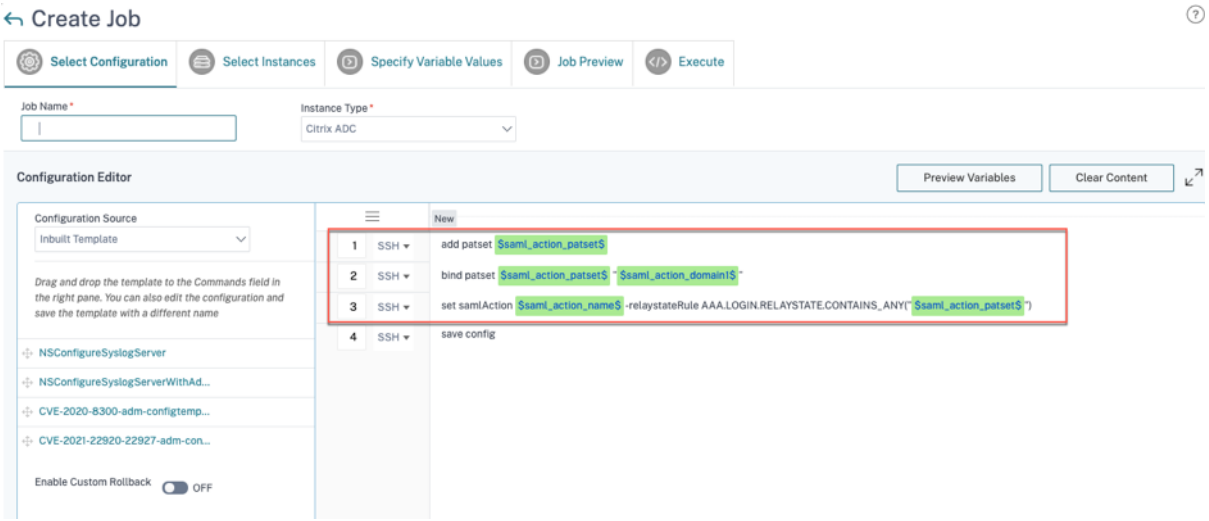
影響を受ける ADC インスタンスごとに個別の構成ジョブを 1 つずつ実行し、その ADC のすべての SAML アクションを含める必要があります。たとえば、脆弱な ADC インスタンスが 2 つあり、それぞれに 2 つの SAML アクションがある場合、この設定ジョブを 2 回実行する必要があります。ADC ごとに 1 回、すべての SAML アクションをカバーします。

ADC 1	ADC2
ジョブ 1:2 つの SAML アクション	ジョブ 2:2 つの SAML アクション

ジョブに名前を付け、次の仕様に合わせてテンプレートをカスタマイズします。組み込みの構成テンプレートは、単なるアウトラインまたは基本テンプレートです。次の要件に合わせて、デプロイメントに基づいてテンプレートをカスタマイズします。

a.**SAML** アクションとそれに関連するドメイン

導入環境内の SAML アクションの数に応じて、1 ～3 行目を複製し、各 SAML アクションのドメインをカスタマイズする必要があります。



たとえば、2 つの SAML アクションがある場合、1 ～3 行目を 2 回繰り返し、それに応じて各 SAML アクションの変数定義をカスタマイズします。

また、SAML アクションに N 個のドメインがある場合は、行`bind patset $saml_action_patset$ “$saml_action_domain1$”` を複数回手動で入力して、その SAML アクションに対して行が N 回表示されるようにする必要があります。そして、次の変数定義名を変更してください。

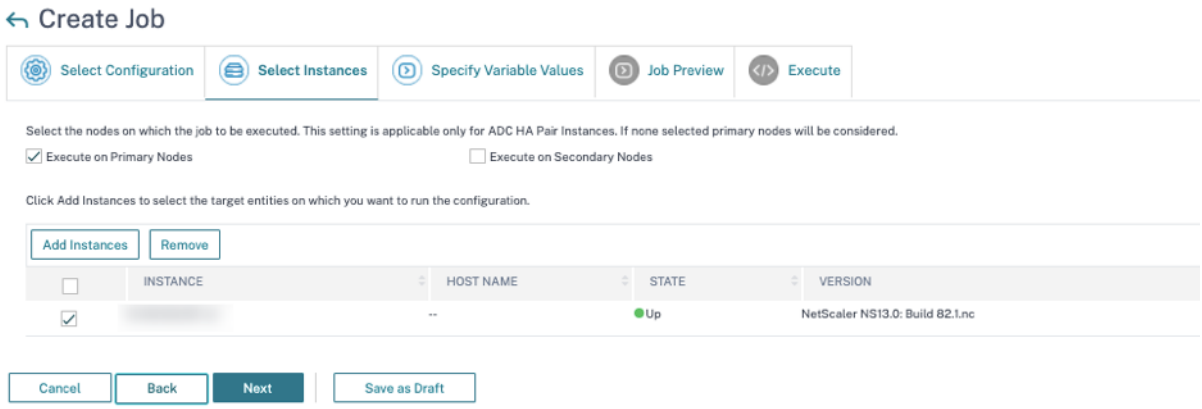
- `saml_action_patset`: は設定テンプレート変数で、SAML アクションのパターンセット (patset) の名前の値を表します。実際の値は、設定ジョブワークフローのステップ 3 で指定できます。このドキュメントの「ステップ 3: 変数値を指定する」セクションを参照してください。
- `saml_action_domain1`: は設定テンプレート変数で、その特定の SAML アクションのドメイン名を表します。実際の値は、設定ジョブワークフローのステップ 3 で指定できます。このドキュメントの「ステップ 3: 変数値を指定する」セクションを参照してください。

デバイスのすべての SAML アクションを検索するには、コマンド`show samlaction`を実行します。

```
> show samlaction -summary
------------------------------------------------------------------------------------------------------------------------------------------------
      Name            Username field  Decryption key       Encryption key       Url to be redirected to
                    Reject unsigned assertions Issuer name          Two factor Smart Group
------------------------------------------------------------------------------------------------------------------------------------------------

1     SamlSPAct1                      idp_private_public   sp_private_public    https://<IP3>/saml/login
                  ON          http://<IP1>          OFF
2     SamlSPAct2                      idp_private_public   sp_private_public    https://          /saml/login
                  ON          http://               OFF
Done
```

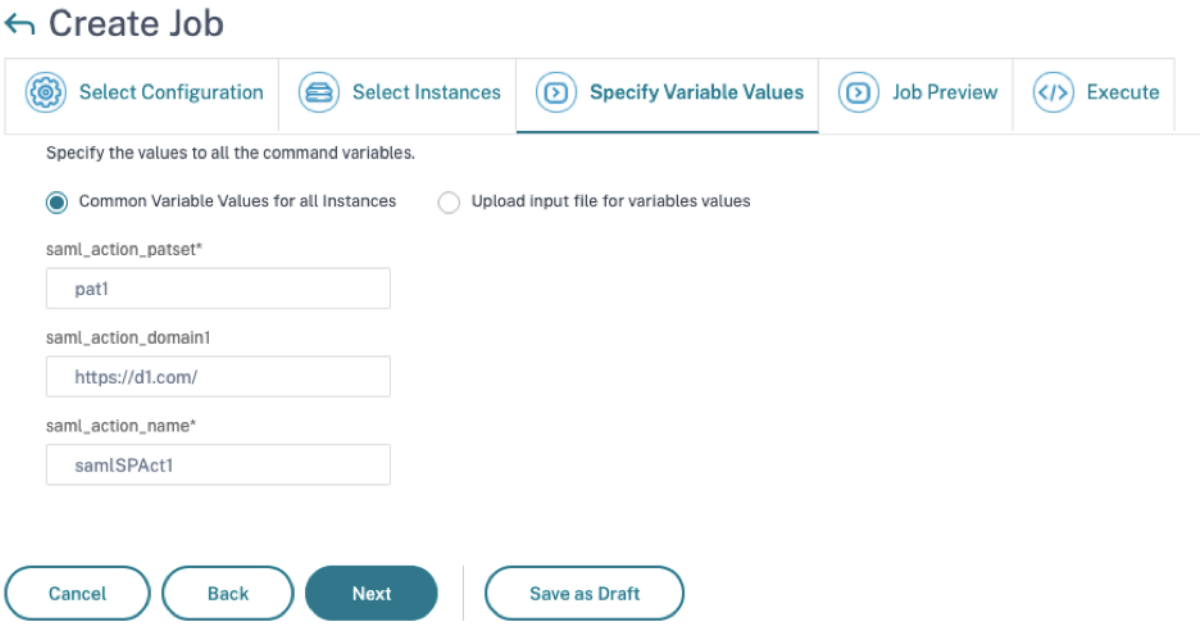
ステップ **2:** インスタンスを選択する

影響を受けるインスタンスは **[**インスタンスの選択**]** に自動的に入力されます。インスタンスを選択して [次へ] をクリックします。

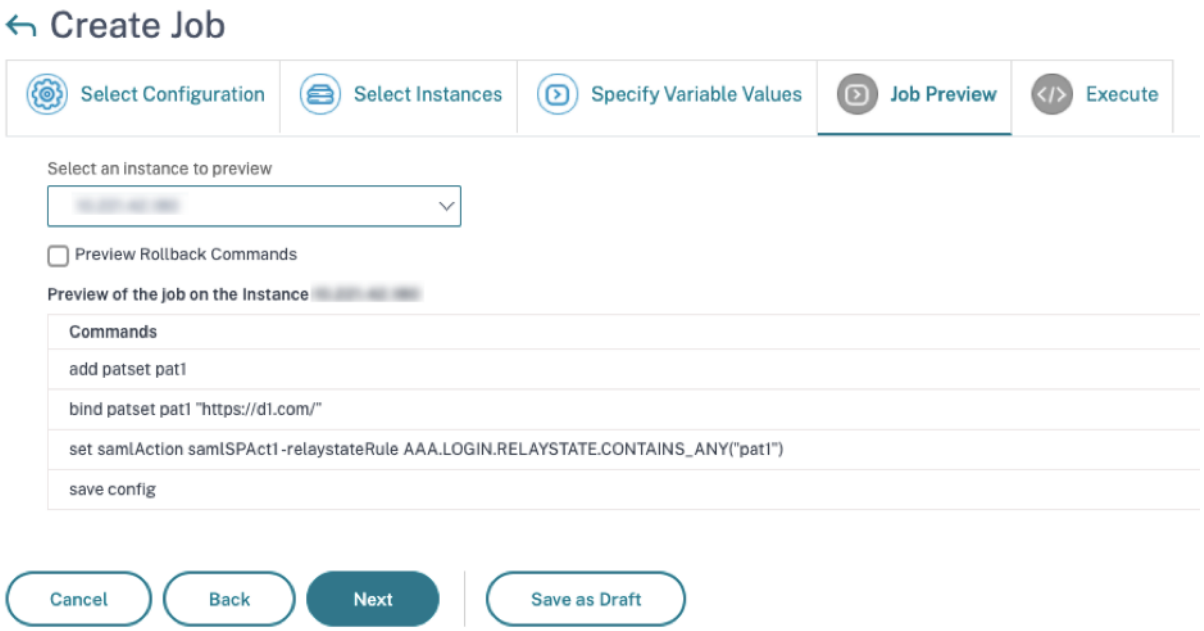


ステップ **3:** 変数値を指定する　変数値を入力します。

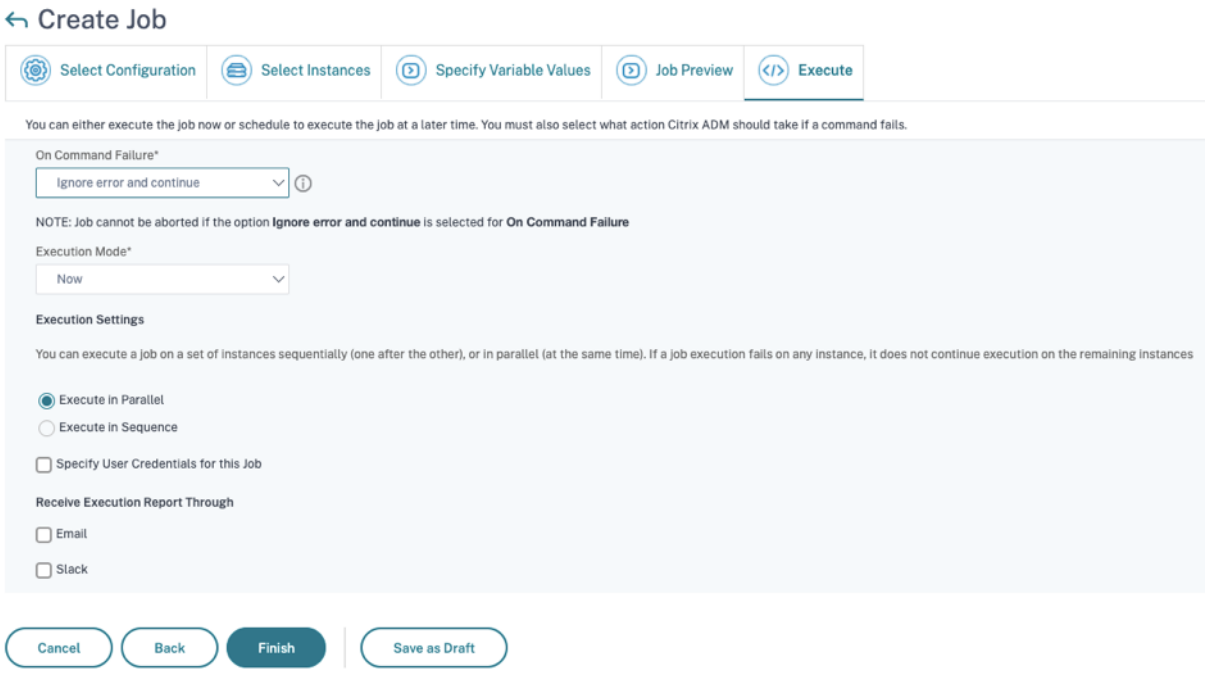
- `saml_action_patset`: SAML アクションの名前を追加
- `saml_action_domain1`: ドメインを次の形式で入力します `https://<example1.com>/`
- `saml_action_name`: ジョブを設定している SAML アクションと同じものを入力します



ステップ **4:** 構成をプレビューする　設定に挿入された変数値をプレビューし、[次へ] をクリックします。



ステップ **5:** ジョブを実行する　「完了」をクリックして構成ジョブを実行します。



ジョブが実行されると、[インフラストラクチャ**] > [**構成**] > [**構成ジョブ**]** に表示されます。

すべての脆弱な ADC に対して 2 つの修復手順を完了したら、オンデマンドスキャンを実行して修正されたセキュリティ体制を確認できます。

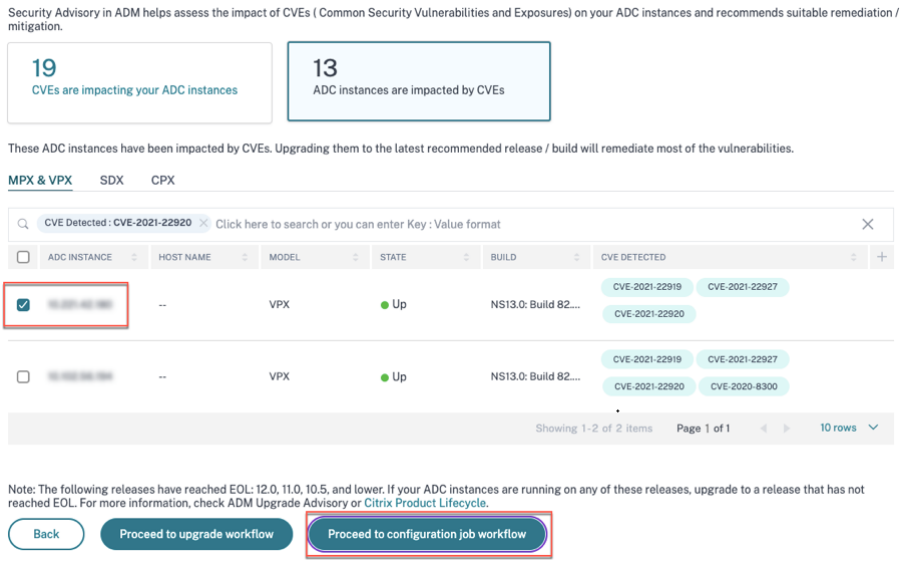
シナリオ

このシナリオでは、2 つの ADC インスタンスが CVE-2021-22920 に対して脆弱であるため、すべてのインスタンスを修正する必要があります。次の手順を実行します:

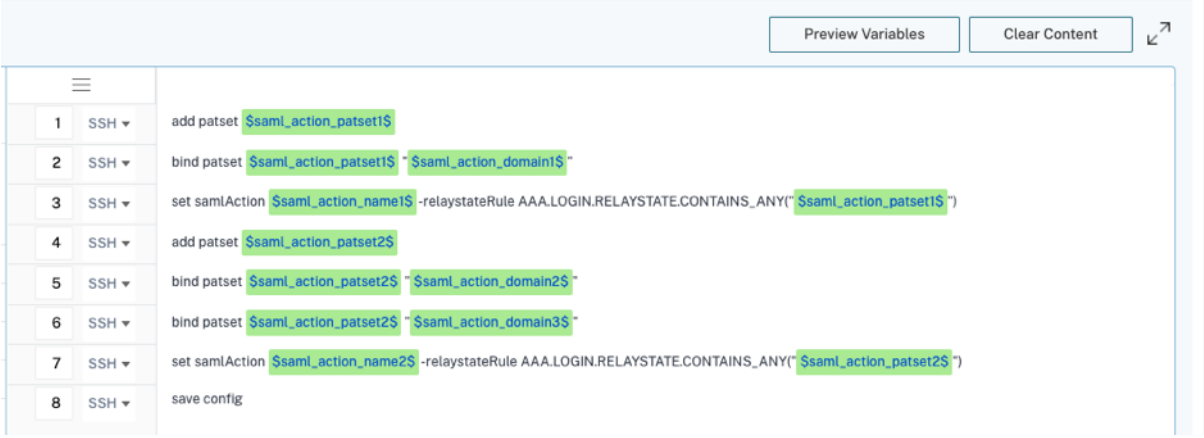
1. このドキュメントの「インスタンスのアップグレード」セクションに記載されている手順に従って、3 つの ADC インスタンスをすべてアップグレードします。
2. コンフィグレーション・ジョブのワークフローを使用して、コンフィグレーション・パッチを ADC に 1 つずつ適用します。このドキュメントの「設定コマンドの適用」セクションに記載されている手順を参照してください。

脆弱な ADC 1 には 2 つの SAML アクションがあります。

- SAML アクション 1 には 1 つのドメインがあります
- SAML アクション 2 には 2 つのドメインがあります



ADC 1 を選択し、「設定ジョブのワークフローに進む」をクリックします。ビルトインの基本テンプレートは自動的に入力されます。次に、ジョブ名を指定し、指定された構成に従ってテンプレートをカスタマイズします。

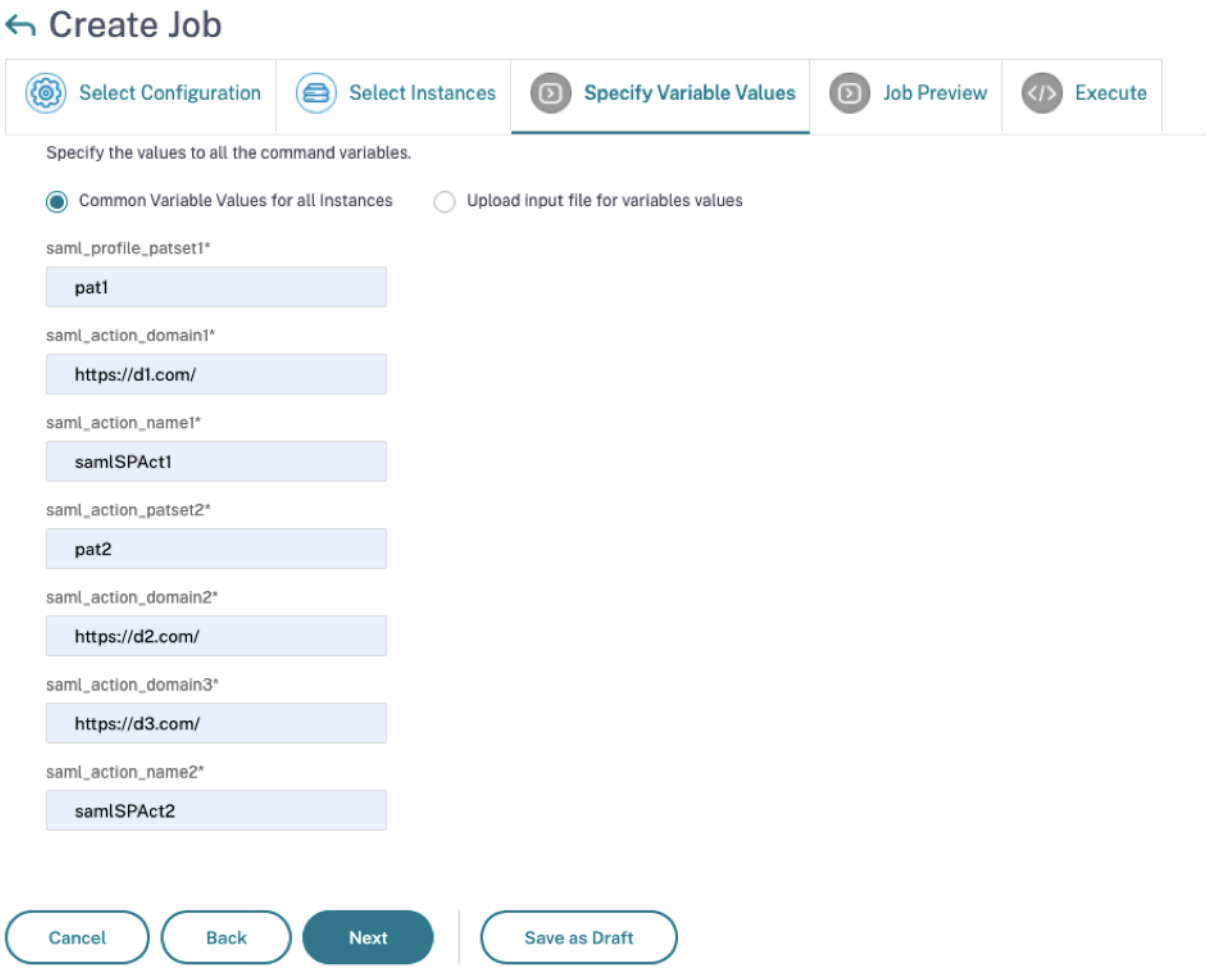


次の表は、カスタマイズされたパラメータの変数定義を示しています。

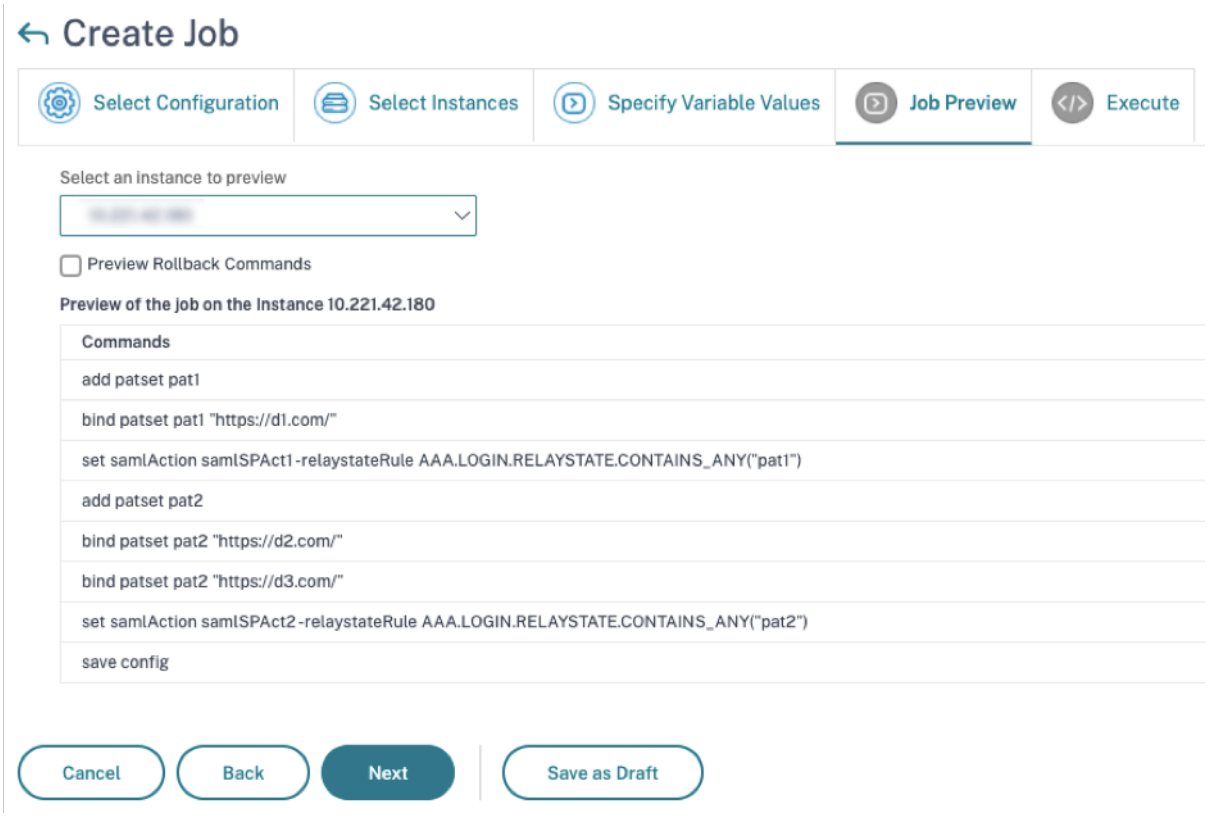
テーブル。SAML アクションの変数定義

ADC 構成	patset の変数定義	SAML アクション名の変数定義	ドメインの変数定義
SAML アクション 1 には 1 つのドメインがあります	saml_action_patset1	saml_action_name1	saml_action_domain1
SAML アクション 2 には 2 つのドメインがあります	saml_action_patset2	saml_action_name2	saml_action_domain2、saml_action_domain3

[インスタンスを選択**]** で [ADC 1] を選択し、[次へ] をクリックします。**[**変数値の指定] ウィンドウが表示されます。このステップでは、前のステップで定義したすべての変数の値を指定する必要があります。



次に、変数を確認します。



[次へ] をクリックし、[完了] をクリックしてジョブを実行します。

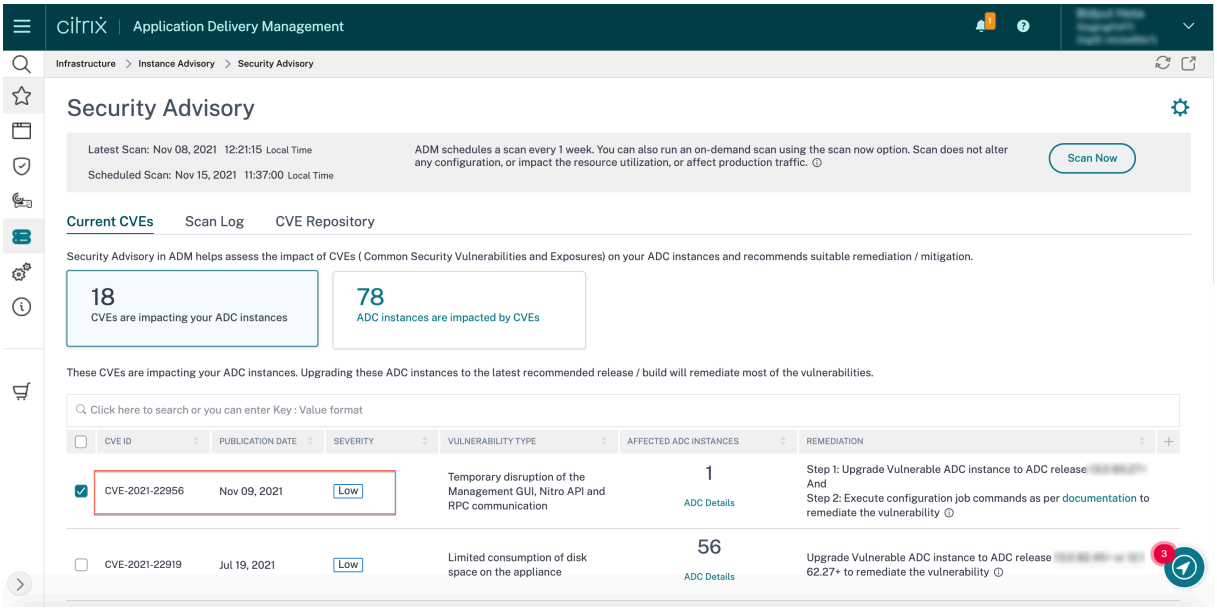
ジョブが実行されると、[インフラストラクチャ] **>** [構成] **>** [構成ジョブ] に表示されます。

ADC1 の 2 つの修復手順を完了したら、同じ手順に従って ADC 2 と ADC 3 を修正します。修正が完了したら、オンデマンドスキャンを実行して、修正されたセキュリティ体制を確認できます。

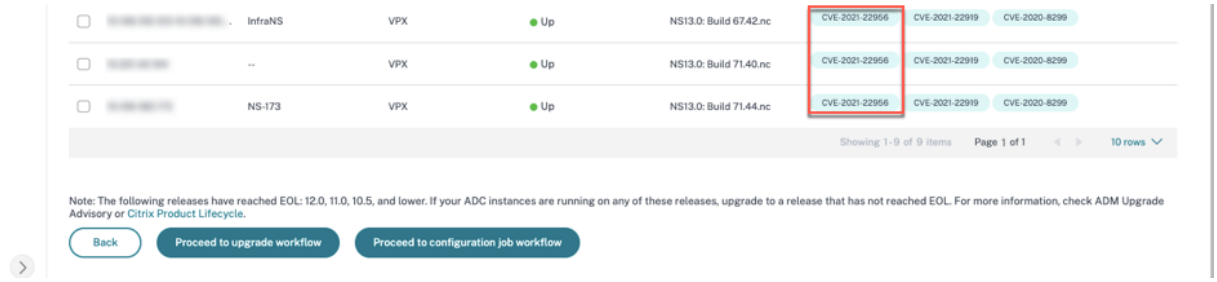
CVE-2021-22956 の脆弱性の特定と修正

February 6, 2024

NetScaler ADM セキュリティアドバイザリダッシュボードの「現在の **CVE**」**>**「**<number of>**ADC インスタンスは一般的な脆弱性と露出（CVE）の影響を受ける（CVE)」で、この特定の CVE によって脆弱なすべてのインスタンスを確認できます。CVE-2021-22956 の影響を受けるインスタンスの詳細を確認するには、CVE-2021-22956 を選択し、「影響を受けるインスタンスを表示」をクリックします。



<number of>CVE の影響を受ける ADC インスタンスウィンドウが表示されます。ここでは、CVE-2021-22956 の影響を受ける ADC インスタンスの数と詳細を確認できます。



セキュリティアドバイザリダッシュボードの詳細については、「セキュリティアドバイザリ」を参照してください。

> 注
>
> セキュリティアドバイザリシステムスキャンが終了し、CVE-2021-22956 の影響をセキュリティアドバイザリモジュールに反映するまでには、しばらく時間がかかる場合があります。影響をすぐに確認するには、「今すぐスキャン」をクリックしてオンデマンドスキャンを開始します。

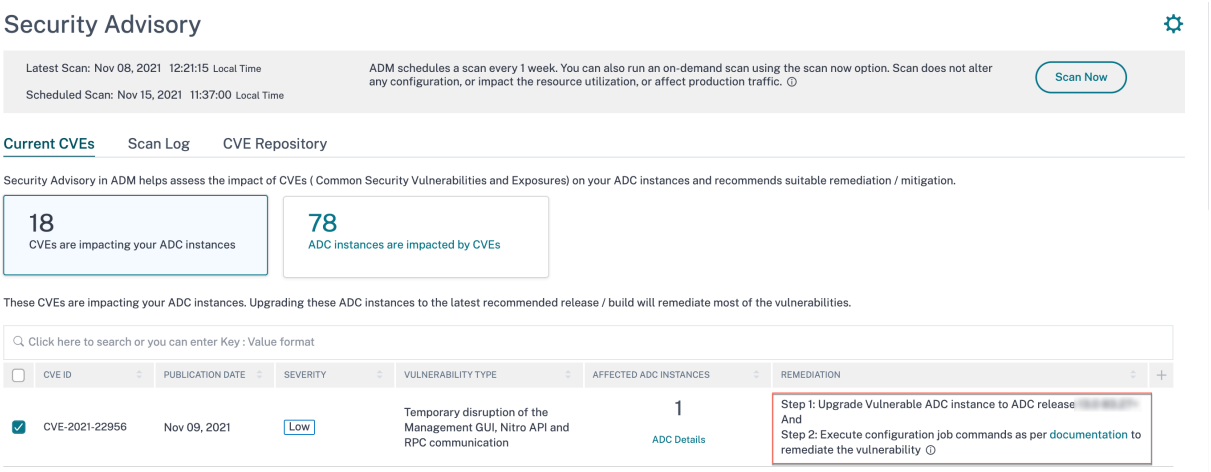
CVE-2021-22956 の影響を受けるインスタンスを特定してください

CVE-2021-22956 では、ADM サービスがマネージド ADC インスタンスに接続し、スクリプトをインスタンスにプッシュするカスタムスキャンが必要です。このスクリプトは ADC インスタンスで実行され、Apache 設定ファイル (`httpd.conf file`) と最大クライアント接続数 (`maxclient`) パラメータをチェックして、インスタンスに脆弱性があるかどうかを判断します。スクリプトが ADM サービスと共有する情報は、ブール値の脆弱性ステータス (true または false) です。また、このスクリプトは、ローカルホスト、NSIP、管理アクセス権のある SNIP など、さまざまなネットワークインタフェースの max_clients の数の一覧を ADM サービスに返します。

このスクリプトは、スケジュールされたオンデマンドスキャンが実行されるたびに実行されます。スキャンが完了すると、スクリプトは ADC インスタンスから削除されます。

CVE-2021-22956 を修復してください

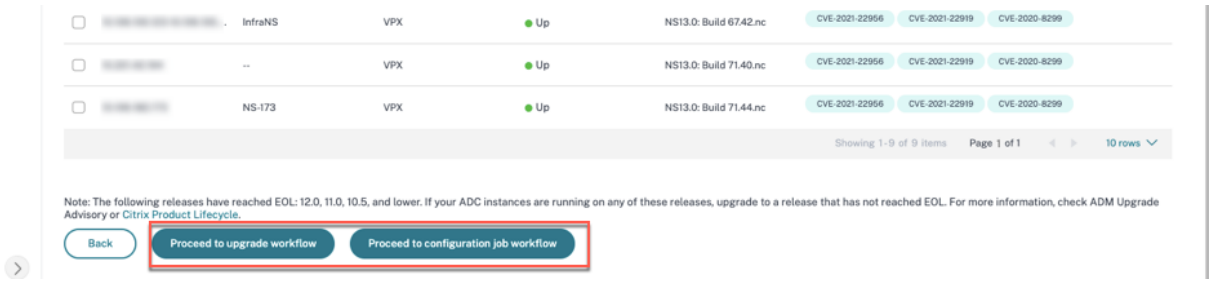
CVE-2021-22956 の影響を受ける ADC インスタンスの場合、修正は 2 段階のプロセスです。GUI の「現在の **CVE**」**>**「**ADC** インスタンスは **CVE** の影響を受ける」で、手順 1 と 2 を確認できます。



次の 2 つのステップがあります。

1. 脆弱な ADC インスタンスを、修正されたリリースとビルドにアップグレードします。
2. カスタマイズ可能な組み込み構成テンプレートを使用して、必要な構成コマンドを構成ジョブに適用します。

「Current CVES > CVE の影響を受ける ADC インスタンス」に、この 2 段階の修正プロセスについて、「アップグレードワークフローに進む」と「設定ジョブワークフローに進む」の 2 つのワークフローが表示されます。



ステップ **1:** 脆弱な **ADC** インスタンスをアップグレードする

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、[ワークフローのアップグレードに進む] をクリックします。アップグレードワークフローは、脆弱な ADC インスタンスが既に入力されている状態で始まります。

NetScaler ADM を使用して ADC インスタンスをアップグレードする方法について詳しくは、「ADC アップグレードジョブの作成」を参照してください。

> 注
>
> このステップは、脆弱なすべての ADC インスタンスに対して一度に行うことができます。

ステップ **2:** 設定コマンドを適用する

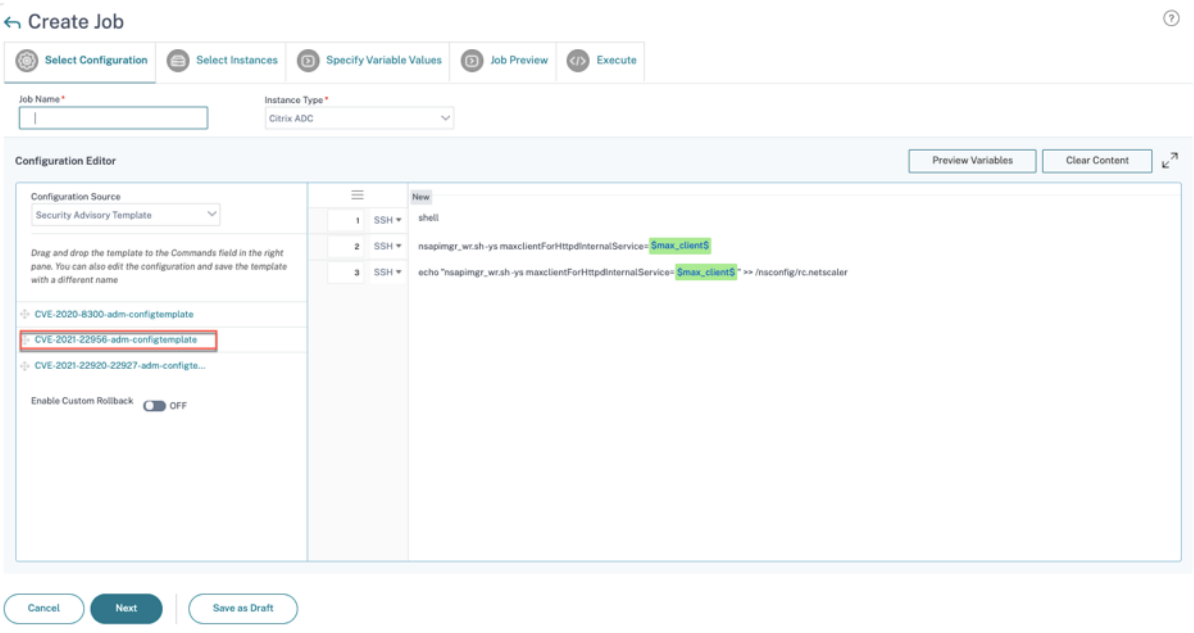
影響を受けるインスタンスをアップグレードしたら、**<number of> CVE** の影響を受ける **ADC** インスタンスウィンドウで、**CVE-2021-2295** の影響を受けるインスタンスを選択し、「設定ジョブのワークフローに進む」をクリックします。ワークフローには次のステップが含まれます。

1. 構成をカスタマイズします。
2. 自動入力された影響を受けるインスタンスを確認する。
3. ジョブの変数への入力を指定する。
4. 変数入力を入力して最終構成を確認します。
5. ジョブを実行しています。

インスタンスを選択して [設定ジョブのワークフローに進む] をクリックする前に、次の点に注意してください。

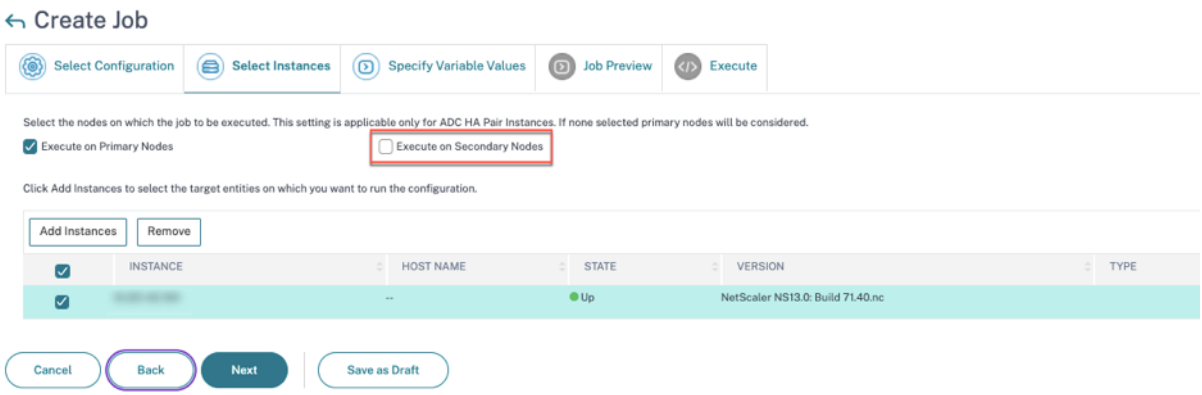
- 複数の CVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920、CVE-2021-22956 など）の影響を受ける ADC インスタンスの場合：インスタンスを選択して [設定ジョブのワークフローに進む] をクリックしても、組み込みの設定テンプレートは [設定の選択] に自動入力されません。セキュリティアドバイザリテンプレートの下にある適切な設定ジョブテンプレートを右側の設定ジョブペインに手動でドラッグアンドドロップします。
- CVE-2021-22956 の影響を受ける複数の ADC インスタンスのみ: すべてのインスタンスで一度に構成ジョブを実行できます。たとえば、ADC 1、ADC 2、ADC 3 があって、それらすべてが CVE-2021-22956 の影響を受けるだけだとします。これらのインスタンスをすべて選択して [設定ジョブのワークフローに進む] をクリックすると、組み込みの設定テンプレートが [設定の選択] に自動入力されます。リリースノートの既知の問題である NSADM-80913 を参照してください。
- CVE-2021-22956 およびその他の 1 つ以上の CVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920 など）の影響を受ける複数の ADC インスタンスで、各 ADC に修正を一度に適用する必要がある場合：これらのインスタンスを選択して [設定ジョブのワークフローに進む] をクリックすると、エラーが表示されます各 ADC で一度に構成ジョブを実行するように指示するメッセージが表示されます。

ステップ **1:** 構成を選択する　設定ジョブのワークフローでは、組み込みの構成ベーステンプレートが [構成の選択] に自動的に入力されます。



ステップ **2:** インスタンスを選択する

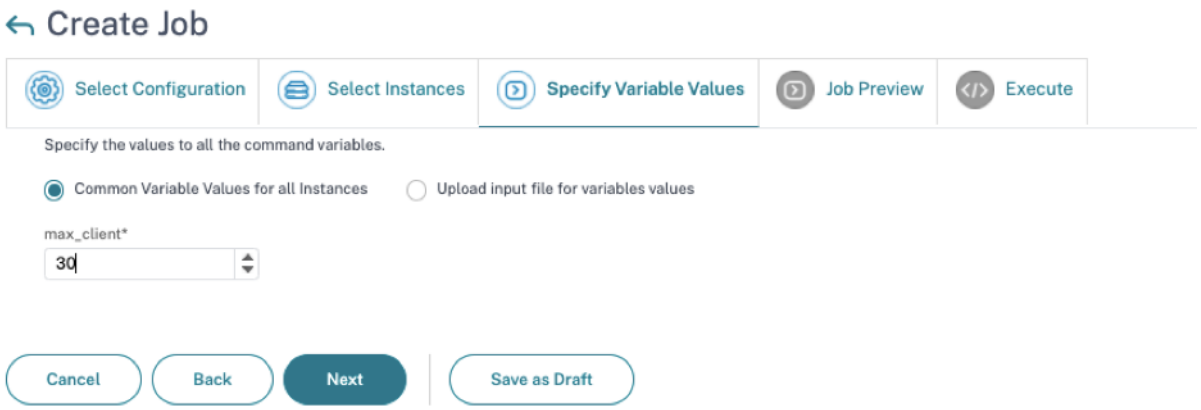
影響を受けるインスタンスは **[**インスタンスの選択**]** に自動的に入力されます。インスタンスを選択します。このインスタンスが HA ペアの一部である場合は、[セカンダリノードで実行する] を選択します。[次へ] をクリックします。



> 注
>
> クラスターモードの ADC インスタンスの場合、ADM セキュリティアドバイザリを使用すると、ADM はクラスター構成コーディネーター (CCO) ノードでのみ構成ジョブの実行をサポートします。CCO 以外のノードで個別にコマンドを実行します。

`rc.netscaler`はすべての HA ノードとクラスタノードで同期されるため、再起動のたびに修正が持続します。

ステップ **3:** 変数値を指定する　変数値を入力します。



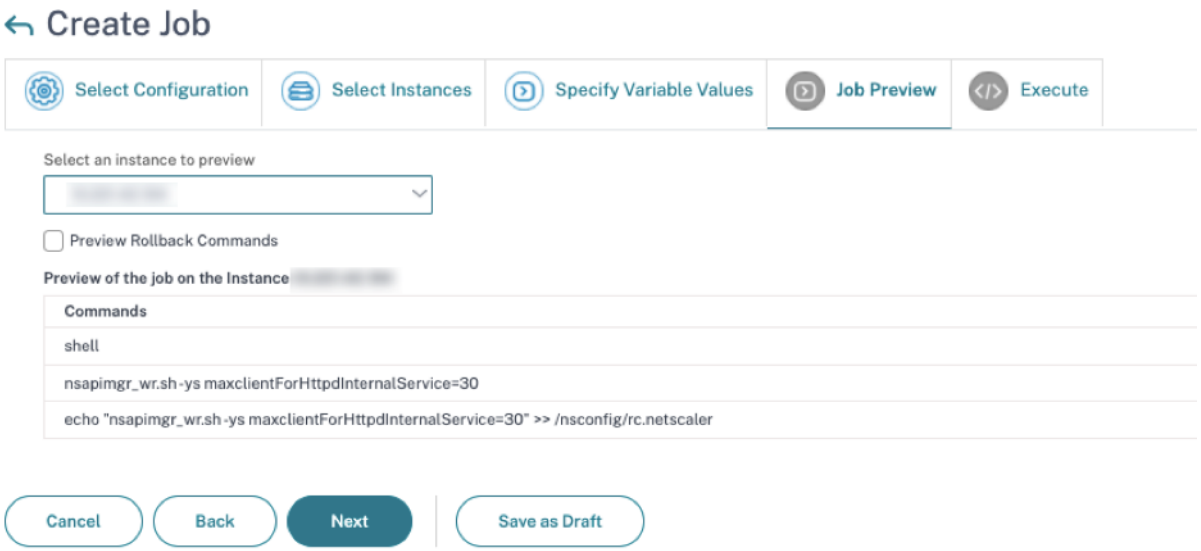
次のオプションのいずれかを選択して、インスタンスの変数を指定します。

すべてのインスタンスに共通の変数値: 変数max_clientに共通の値を入力します。

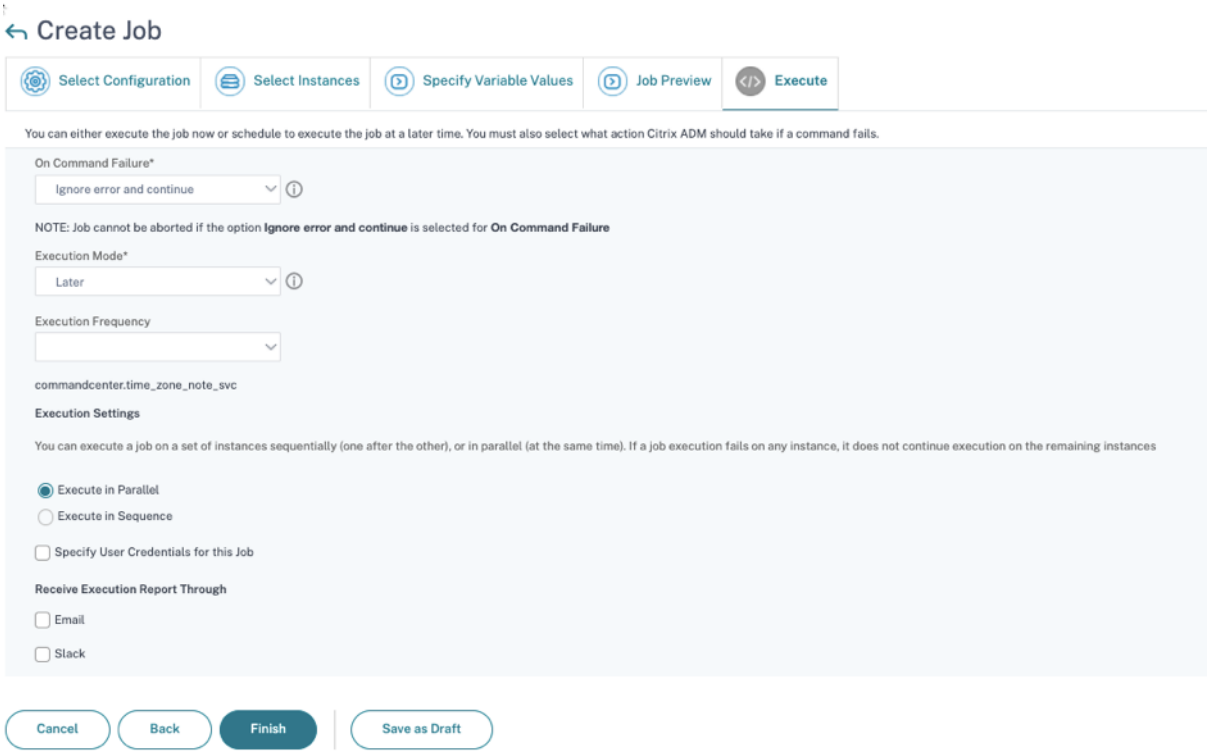
変数値の入力ファイルをアップロード:「入力キーファイルをダウンロード」をクリックして入力ファイルをダウンロードします。入力ファイルで、変数max_clientの値を入力し、ファイルを ADM サーバーにアップロードします。このオプションの問題については、リリースノートの既知の問題である NSADM-80913 を参照してください 。

> 注
>
> 上記のどちらのオプションでも、推奨max_client値は 30 です。現在の価値に応じて値を設定できます。ただし、ゼロであってはならず、/etc/httpd.conf ファイルに設定されている max_client 以下でなければなりません。Apache HTTP サーバー設定ファイル/etc/httpd.confに設定されている現在の値は、ADC インスタンスで文字列MaxClientsを検索することで確認できます。

ステップ **4:** 構成をプレビューする　設定に挿入された変数値をプレビューし、[次へ] をクリックします。



ステップ **5:** ジョブを実行する　「完了」をクリックして構成ジョブを実行します。



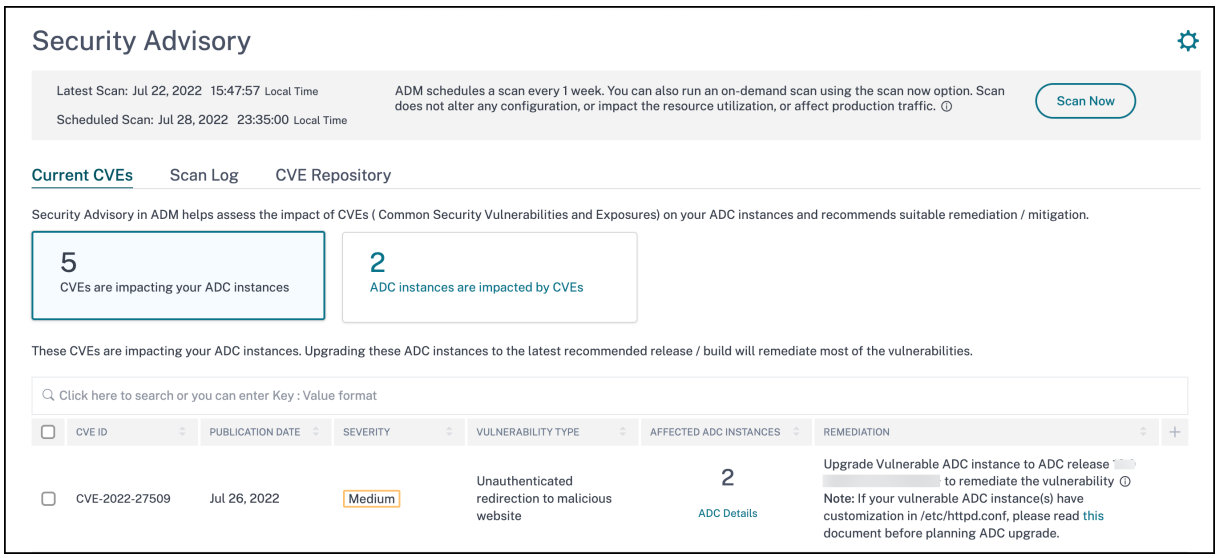
ジョブが実行されると、[インフラストラクチャ] **>** [構成] **>** [構成ジョブ] に表示されます。

すべての脆弱な ADC に対して 2 つの修復手順を完了したら、オンデマンドスキャンを実行して修正されたセキュリティ体制を確認できます。

CVE-2022-27509 の脆弱性の特定と修正

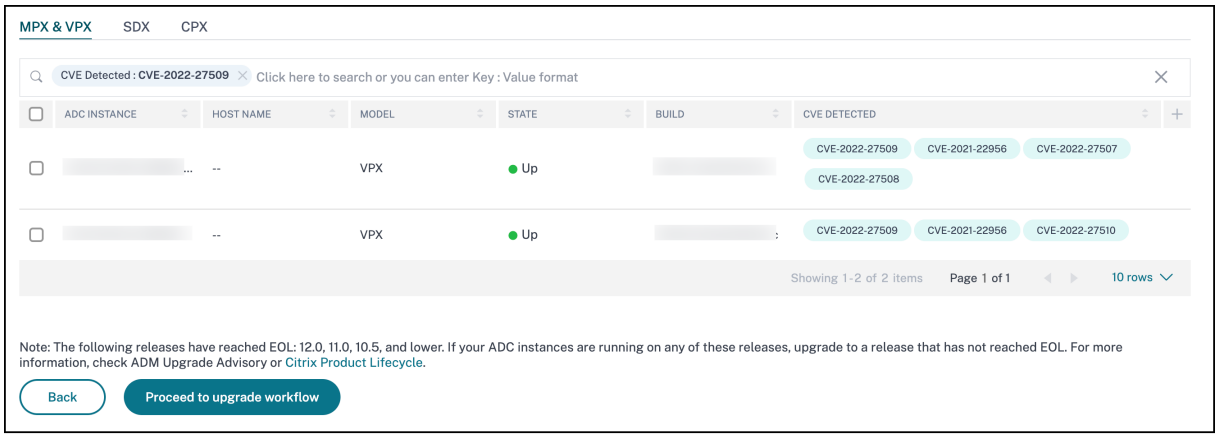
February 6, 2024

NetScaler ADM セキュリティアドバイザリダッシュボードの「現在の **CVE <number of> ADC** インスタンスは **CVE** の影響を受ける」で、**CVE-2022-27509** によって脆弱なすべてのインスタンスを確認できます。CVE の影響を受けるインスタンスの詳細を確認するには、CVE-2022-27509 を選択し、「影響を受けるインスタンスを表示」をクリックします。



> 注
>
> ADC 脆弱性の原因を理解するには、セキュリティアドバイザリの [スキャンログ] タブにある CSV レポートをダウンロードしてください。

<number of> CVE の影響を受ける **ADC** インスタンスのウィンドウが表示されます。次の画面キャプチャでは、CVE-2022-27509 の影響を受ける ADC インスタンスの数と詳細を確認できます。



セキュリティアドバイザリダッシュボードの詳細については、「セキュリティアドバイザリ」を参照してください。

> 注
>
> セキュリティアドバイザリシステムのスキャンが終了し、CVE-2022-27509 の影響がセキュリティアドバイザリモジュールに反映されるまでには、数時間かかる場合があります。影響をより早く確認するには、[**Scan-Now**] をクリックしてオンデマンドスキャンを開始します。

CVE-2022-27509 の影響を受けるインスタンスを特定してください

CVE-2022-27509 では、カスタムスキャンとバージョンスキャンの組み合わせが必要です。カスタムスキャンの一部として、ADM サービスはマネージド ADC インスタンスに接続し、スクリプトをインスタンスにプッシュします。スクリプトは ADC インスタンスで実行され、インスタンスに脆弱性があるかどうかを判断します。このスクリプトは、定期スキャンまたはオンデマンドスキャンが実行されるたびに実行されます。

スキャンが完了すると、スクリプトは ADC インスタンスから削除されます。

これらのセキュリティアドバイザリカスタムスキャンをオプトアウトすることもできます。カスタムスキャン設定とカスタムスキャンのオプトアウトの詳細については、**** セキュリティアドバイザリページの「カスタムスキャン設定の設定 ** 」セクションを参照してください。

CVE-2022-27509 を修復してください

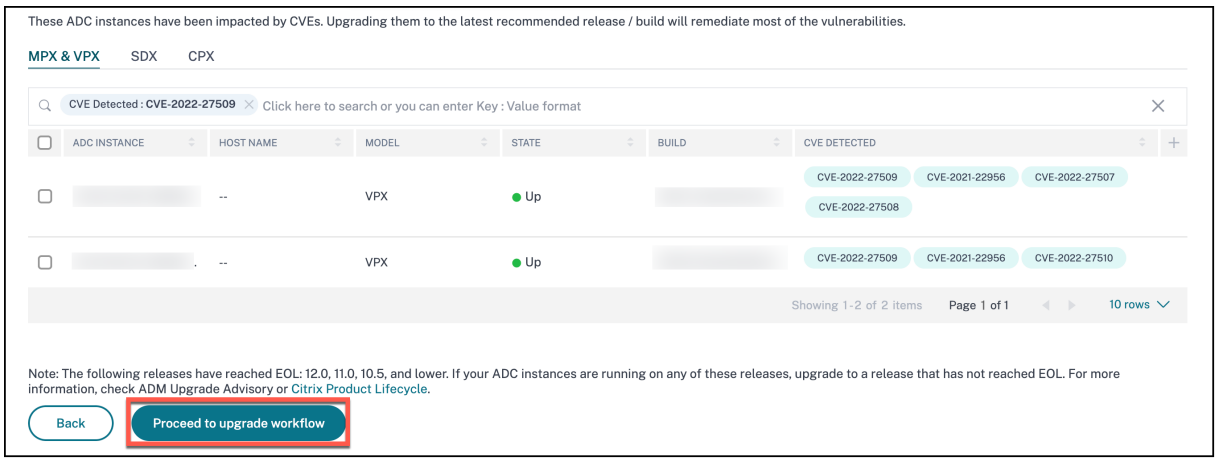
CVE-2022-27509 の影響を受ける ADC インスタンスの場合、修正は単一ステップのプロセスであり、脆弱な ADC インスタンスを修正を含むリリースとビルドにアップグレードする必要があります。GUI の [**Current CVE] > [ADC** インスタンスは **CVE** の影響を受ける] に、修正する手順が表示されます。

Current CVEs> CVE の影響を受ける **ADC** インスタンスの下に、この単一ステップの修正プロセスに関する次のワークフロー、つまり「アップグレードワークフローに進む」が表示されます。

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、[ワークフローのアップグレードに進む] をクリックします。アップグレードワークフローは、脆弱な ADC インスタンスが既に入力されている状態で始まります。

> 重要
>
> 脆弱な ADC インスタンスの /etc/httpd.conf ファイルが /nsconfig ディレクトリにコピーされている場合は、ADC のアップグレードを計画する前に、「カスタマイズされた ADC 構成のアップグレードに関する考慮事項 」を参照してください。

NetScaler ADM を使用して ADC インスタンスをアップグレードする方法について詳しくは、「ADC アップグレードジョブの作成」を参照してください。



セキュリティアドバイザリでサポートされていない **CVE**

February 6, 2024

NetScaler ADM セキュリティアドバイザリは、すべての新しい共通脆弱性と暴露（CVE）を追跡し、CVE がインフラストラクチャに与える影響を評価します。推奨事項を確認して適切なアクションを取ることができます。ただし、サポートされていない CVE がいくつかあり、脆弱性の検出と修復は NetScaler ADM セキュリティアドバイザリの範囲外です。

- **CVE-2022-21827:**

  CVE-2022-21827 は、21.9.1.2 より前の Windows サポートバージョンの NetScaler Gateway プラグインに影響します。

  Windows 用 NetScaler Gateway プラグインに影響する脆弱性の検出と修復は、NetScaler ADM ではサポートされていません。また、NetScaler Gateway プラグインの脆弱性は、ADC 側でチェックを実行したり、ADC のバージョンを確認したり、ADC 構成を確認したりしても評価できません。この CVE の検出と修復は、クライアントに導入されている Windows 用 NetScaler Gateway プラグインのバージョンに基づいてのみ評価できます。

  そのため、この脆弱性の検出と修復は NetScaler ADM セキュリティアドバイザリの対象外となります。

アップグレードアドバイザリ (プレビュー)

February 6, 2024

ネットワーク管理者は、NetScaler ADM のさまざまな ADC ビルド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。NetScaler 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（EOM）に近づいている、または達している 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。

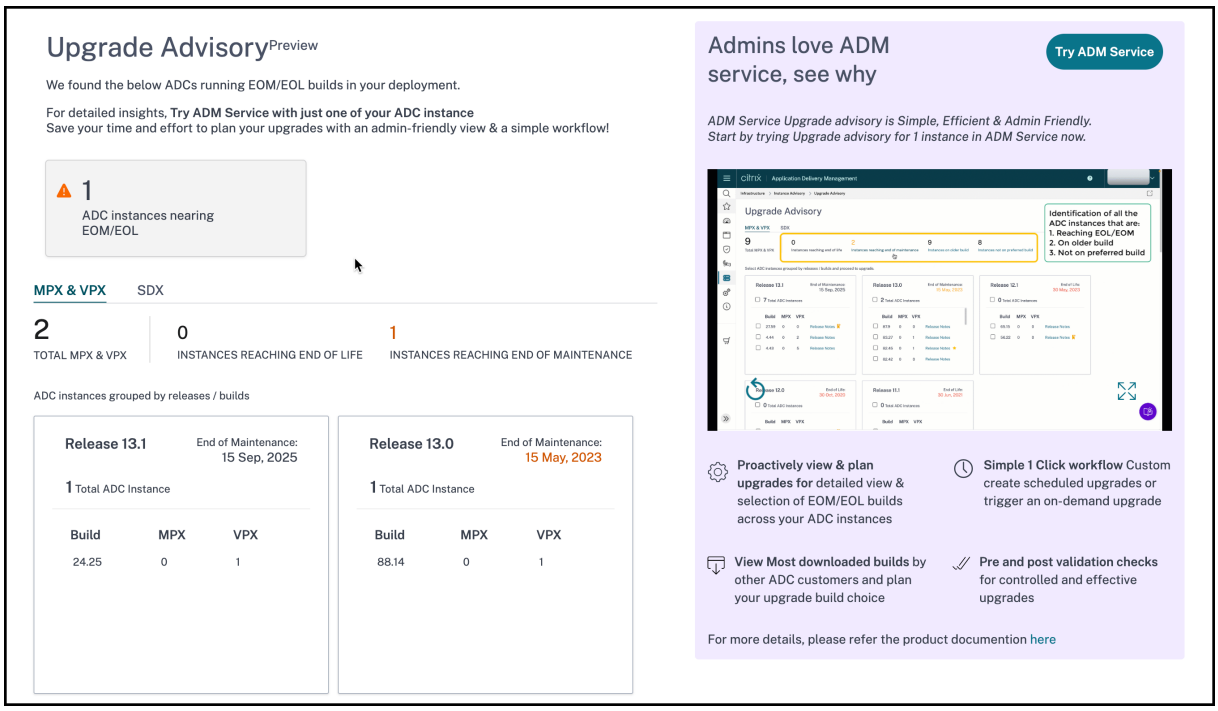
NetScaler ADM オンプレミスアップグレードアドバイザリは、ADC のバージョンスキャンを実行し、ADC インスタンス全体の EOM/EOL ビルドを表示します。

> 重要
>
> ADC インスタンスをアップグレードするための詳細な情報とワークフローについては、**NetScaler ADM Service** をお試しください。

アップグレードアドバイザリを表示

[インフラストラクチャ**] > [**インスタンスアドバイザリ**] > [**アップグレードアドバイザリ] に移動し、次の情報を表示します。

- 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。



「アップグレードアドバイザ」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。

NetScaler ADM オンプレミスアップグレードアドバイザリでは、ADC インスタンスのいずれかを選択して ADC インスタンスを ADM Service にオンボーディングすることもできます。「**ADM** サービスを試す」をクリックし、ADC インスタンスを ADM サービスにオンボーディングします。ADM サービスアップグレードアドバイザリは、選択した ADC インスタンスごとにアップグレードするワークフローを提供します。

ADM サービスアップグレードアドバイザリの詳細については、アップグレードアドバイザリページの **GIF** アニメーションをご覧ください。

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

NetScaler Application Delivery Management （ADM）は、さまざまなベンダーの SDN コントローラーと統合することにより、企業ネットワークの SDN をサポートします。NetScaler ADM は、VMware NSX Manager と Cisco 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）の両方をサポートしています。

VMware NSX Manager

NetScaler ADM は VMware ネットワーク仮想化プラットフォームと統合して、NetScaler サービスの導入、構成、管理を自動化します。この統合により、物理ネットワークトポロジにつきものである従来の複雑さが取り除かれ、vSphere および vCenter 管理者はプログラミングによって短時間で NetScaler サービスを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キング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キングを可能にします。また、外部ネットワーキングやセキュリティサービスをサポートします。

NetScaler ADM のクラウドオーケストレーション機能により、NetScaler 製品と 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 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 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の自動化を実行し、L4-L7 構成は APIC のデバイスマネージャーとして機能する NetScaler ADM に委任できます。

NetScaler ハイブリッドモードソリューションは、ハイブリッドモードのデバイスパッケージと NetScaler ADM によってサポートされています。APIC 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 オートメーション」を参照してください。

OpenStack: NetScaler 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。以後、OpenStack ユーザーは、OpenStack のロードバランサー構成を NetScaler インスタンスに展開できます。

以下のセクションでは、NetScaler 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 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 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 はこのドライバーを使用して NetScaler ADM を定期的に呼び出し、NetScaler から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）のステータスを取得します。OpenStack プラットフォーム用の NetScaler ドライバーソフトウェアは、NetScaler ADM にバンドルされています。ドライバをダウンロードしてインストールするには、まず NetScaler ADM をインストールしてアプリケーションを起動する必要があります。

NetScaler ADM と **OpenStack** 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 コントローラーの IP アドレスとクラウド管理者ユーザー資格情報、さらに OpenStack の NetScaler ドライバーのユーザー資格情報を設定します。後で Neutron 構成ファイル（neutron.conf）の NetScaler_Driver セクションで同じログイン資格情報を指定して、OpenStack の NetScaler ドライバーが LB 構成中に NetScaler ADM に接続できるようにすることができます。

OpenStack と NetScaler ADM が相互に登録されると、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 の既存の資格情報を使用して NetScaler ADM ユーザーインターフェイスにログオンし、LB 構成が NetScalers 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

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 NetScaler インスタンスを、配置ポリシーを通じて柔軟に決定できます。また、NetScaler ADM には、OpenStack テナントに基づいて NetScaler インスタンスを割り当

てるオプションも用意されています。

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
- NetScaler ADM と OpenStack ワークフローの統合
- Prerequisites
- NetScaler ADM と OpenStack での事前構成タスク

- Horizon を使用した LBaaS V1 の構成手順
- コマンドラインを使用した LBaaS V2 の構成手順
- OpenStack への NetScaler VPX インスタンスの手動プロビジョニング
- NetScaler ADM と OpenStack Heat サービスの統合
- 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 NetScaler ADM に登録し、OpenStack のネットワークコンポーネントである Neutron で NetScaler LBaaS ドライバーを構成する必要があります。登録が完了すると、NetScaler ADM は OpenStack のすべてのテナントの詳細を表示します。スティーブは、NetScaler LBaaS 機能を必要とするユーザーを一覧から Example-SportsOnline を選択し、NetScaler ADM のロードバランサー構成に専用の NetScaler を割り当てるようにトムを構成できます。

このため、スティーブは NetScaler ADM ユーザーインターフェイスを使用して OpenStack のコンピューティングレイヤー（Nova）に NetScaler VPX インスタンスをプロビジョニングすることも、トムが OpenStack で LB 構成を行うときに MAS が NetScaler VPX インスタンスをオンデマンドで自動プロビジョニングできるようにすることもできます。いずれの場合も、NetScaler ADM は VPX インスタンスを管理します。これを実現するために、Steve は NetScaler ADM でサービスパッケージを作成し、Tom との SLA で合意した条件をサービスパッケージに定義します。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、さまざまな NetScaler VPX インスタンスをサービスパッケージに割り当て、そのサービスパッケージの専用 NetScaler を必要とする他のテナントと共に、Example-SportsOnline を割り当てます。その結果、トムが

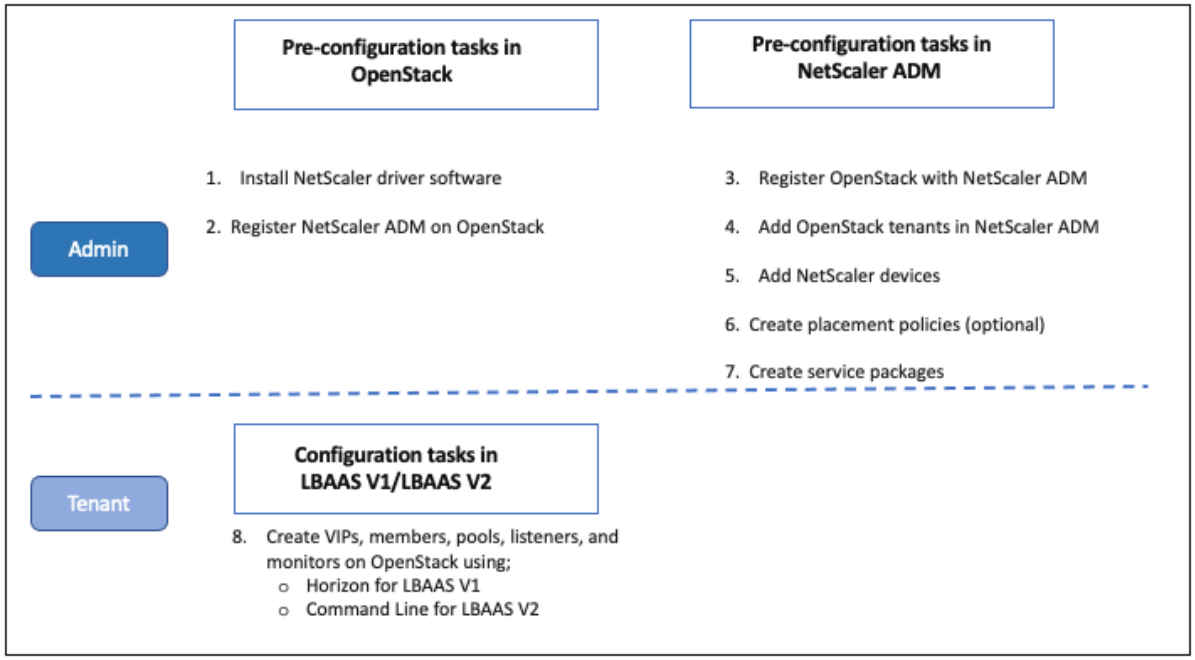
初めてロードバランサー構成を実行すると、NetScaler ADM はサービスパッケージ内の NetScaler VPX インスタンスの 1 つを Example-SportsOnline に割り当てて、その構成もその NetScaler に展開します。

これでトムは、OpenStack の LBaaS および UI によるプール、VIP（Virtual IP：仮想 IP アドレス）、ヘルスモ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、NetScaler インスタンスのサービスグループおよび仮想サーバーとして配置されます。また、トムはヘルスモニターを作成して、サーバーを監視したり、常に UP の状態で NetScaler から到達可能なサーバーだけにアプリケーショントラフィックを送信したりできます。

こうして OpenStack で作成された負荷分散構成は NetScaler インスタンスに実装されます。完全に構成されると、NetScaler VPX インスタンスが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。

NetScaler ADM と OpenStack ワークフローの統合

次のフローチャートは、LBaaS V1 および LBaaS V2 構成時に従う必要のあるワークフローです。



NSX Manager：NetScaler インスタンスの手動 Provisioning

February 6, 2024

NetScaler Application Delivery Management （ADM）は、VMware ネットワーク仮想化プラットフォームと統合して、NetScaler サービスの導入、構成、管理を自動化します。この統合により、物理ネットワークトポロジ

につきものである従来の複雑さが取り除かれ、vSphere および vCenter 管理者はプログラミングによって短時間で NetScaler サービスを展開できるようになります。

この記事では、VMware NSX Manager と NetScaler ADM の両方で実行する必要があるタスクのリストを紹介します。

> 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 ビルド 13.1 をインストールするタスクについては、「NetScaler ADM の展開」を参照してください。

VMware ESXi のハードウェア要件

次の表は、NetScaler ADM 仮想アプライアンスをインストールするために VMware ESXi サーバー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、NetScaler ADM を VMware ESXi サーバーに展開するためのものです。ただし、ホスト上で実行されている仮想マシンは他にありません。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。

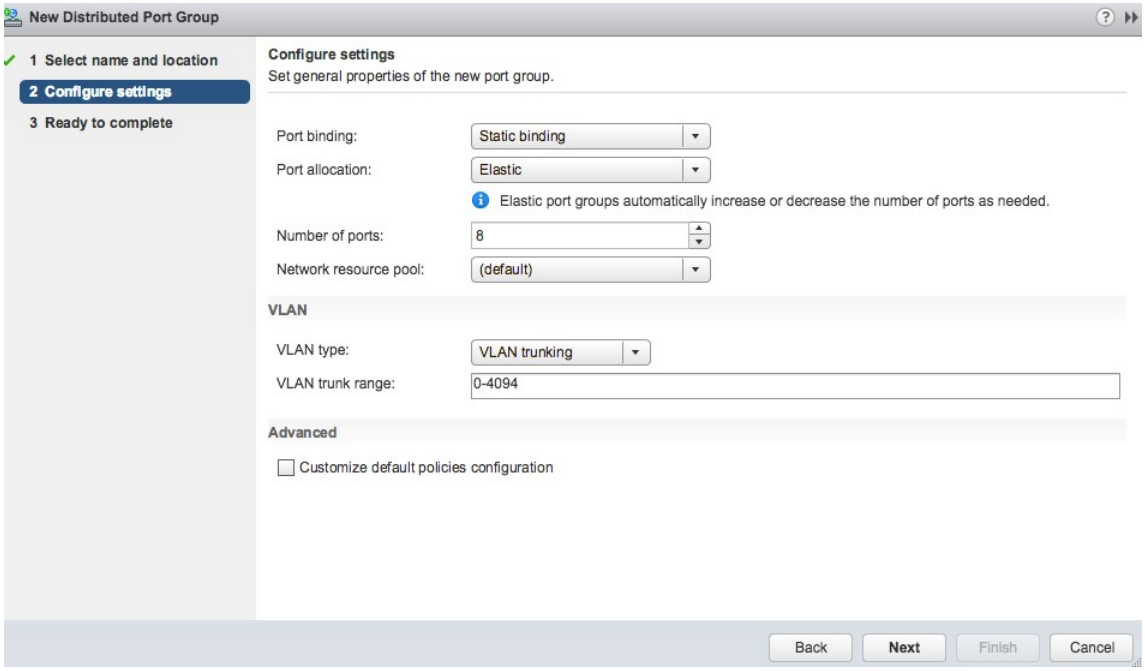
VMware NSX の構成

- さまざまな容量の NetScaler VPX インスタンスによるプールを作成します。これらは、異なるサービスパッケージに追加されます。

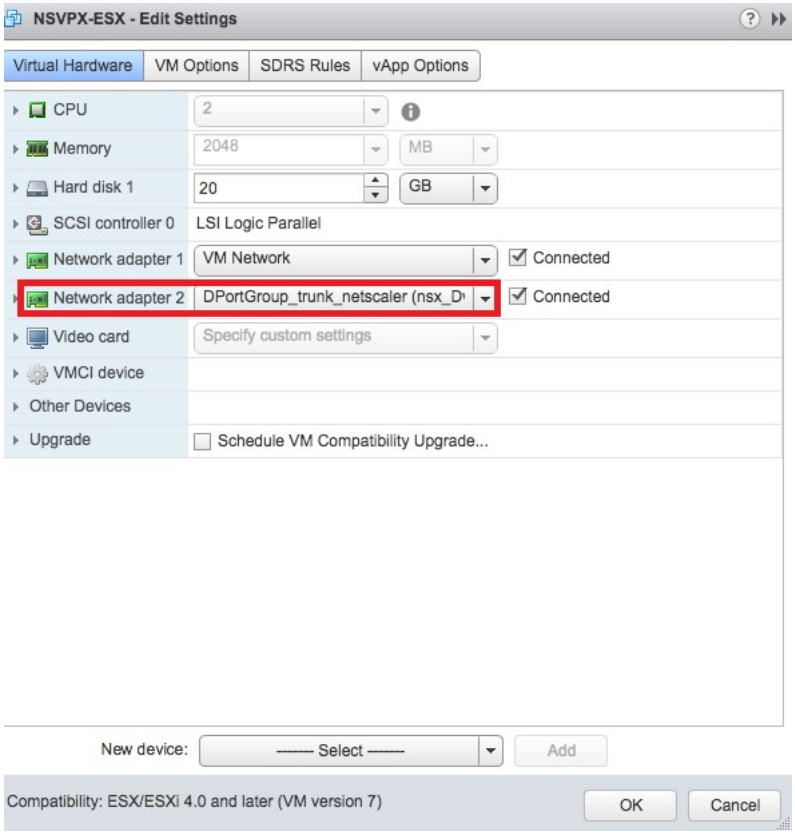
次に例を示します:

- VPX1000（1Gbps）の NetScaler VPX インスタンスを 5 つ作成します。これらのインスタンスは Gold サービスパッケージに追加されます。
- VPX10（10Mbps）の NetScaler VPX インスタンスを 5 つ作成します。これらのインスタンスは Bronze サービスパッケージに追加されます。

1. vSphere Client で［**Networking**］に移動し、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）。

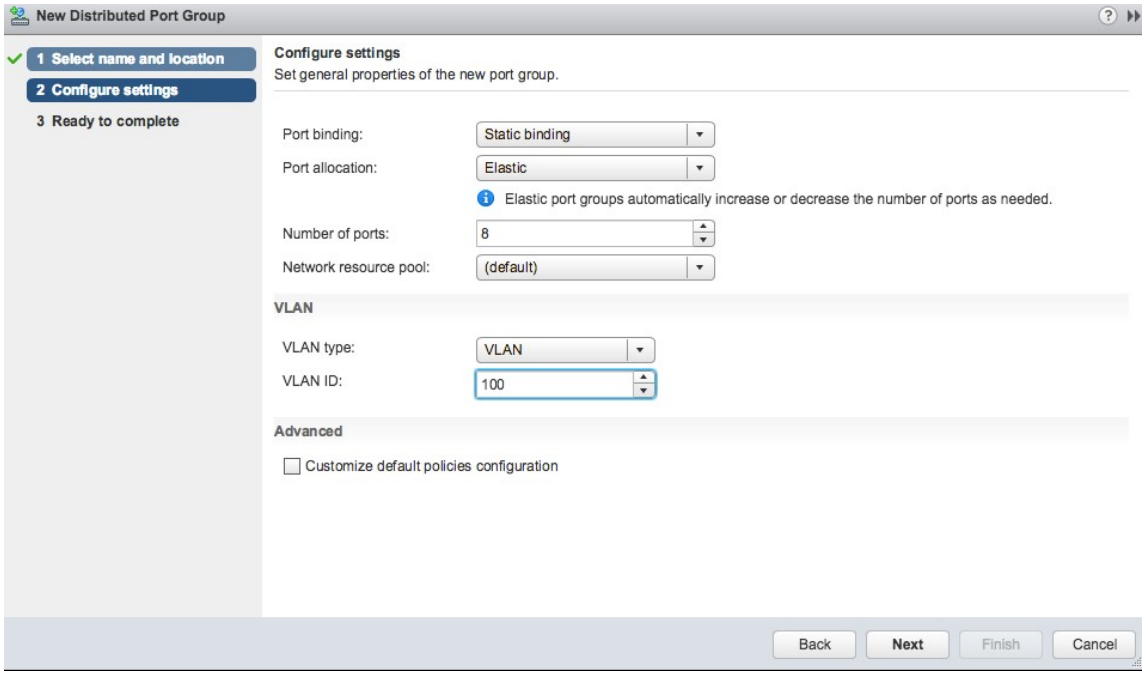


2. NetScaler VPX インスタンスごとに新しいインターフェイスを作成し、上で作成した VLAN 範囲トランクポートグループに接続します。



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。

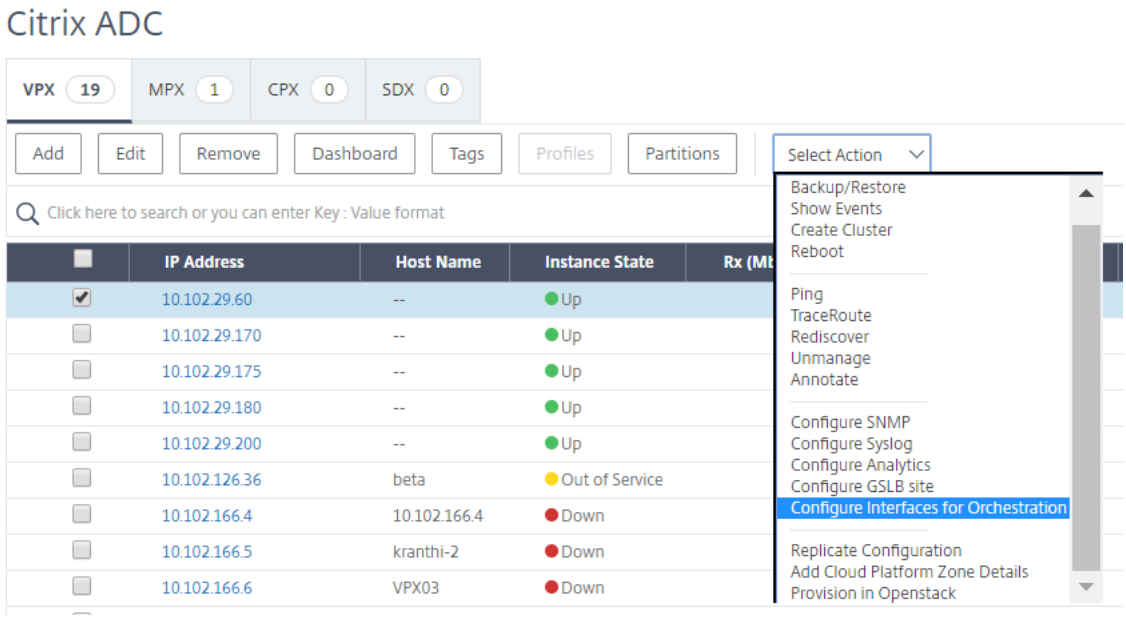
   たとえば、最初のトランク接続のポートグループを 101 から 105 の範囲で作成した場合、VLAN ごとに 1 つずつ、合計 5 つの VLAN ポートグループを作成します。VLAN 101 のポートグループ、VLAN102 のポートグループというように、VLAN 105 まで作成します。



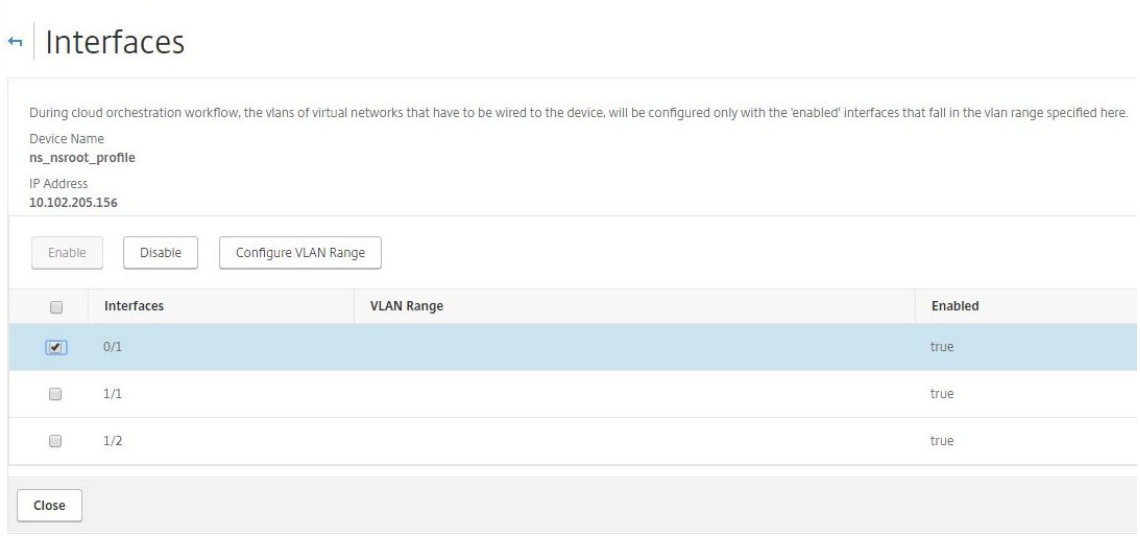
NetScaler ADM での **NetScaler ADC VPX** インスタンスの追加

NetScaler ADM に NetScaler VPX インスタンスを追加し、デバイスごとにトランクグループの VLAN 範囲を指定します。

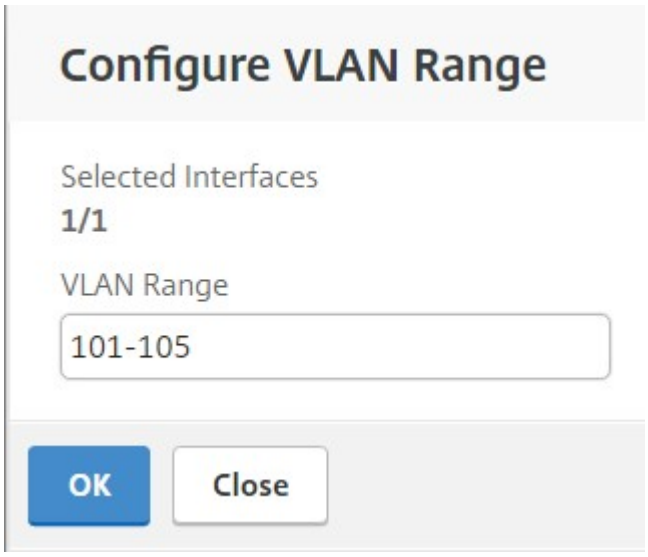
1. **NetScaler ADM** で、**[**** インフラストラクチャ] > [インスタンス] > [**NetScaler VPX**] に移動し、[追加] をクリックします。******
2. **NetScaler VPX** 追加ページで、インスタンスのホスト名、各インスタンスの **IP** アドレス、または **IP** アドレスの範囲を指定し、「プロファイル名」リストからインスタンスプロファイルを選択します。[+] をクリックして新しいインスタンスプロファイルを作成することもできます。
3. [**OK**] をクリックします。
4. **NetScaler**VPX ページのリストから新しく追加された NetScaler 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。



5. [**Inter** faces] 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 NetScaler ADM に登録して、それらの間の通信チャネルを作成します。

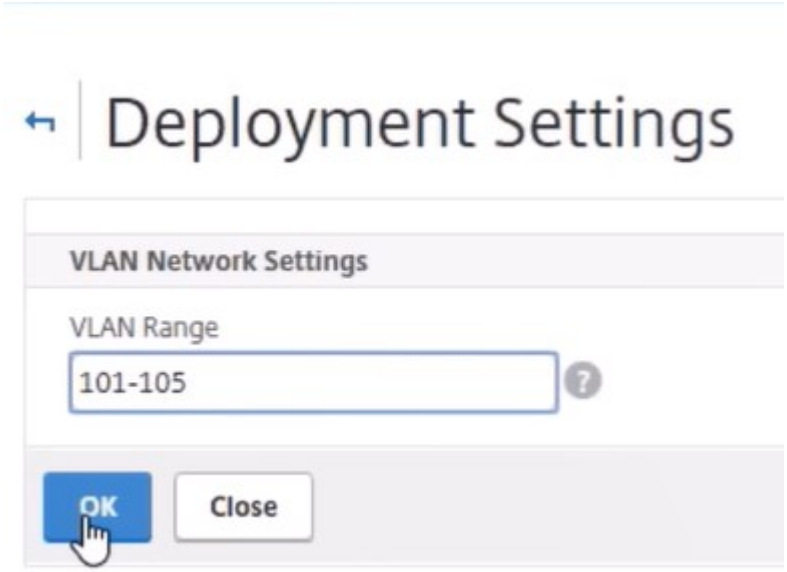
1. **NetScaler ADM** で、ドロップダウンリストから **[**オーケストレーション**] > [SDN** オーケストレーション**] > [**VMware NSX Manager] に移動し、[NSX Manager** 設定の構成] をクリックします。**
2. **NSX Manager** の設定ページで、次のパラメータを設定します。

    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。

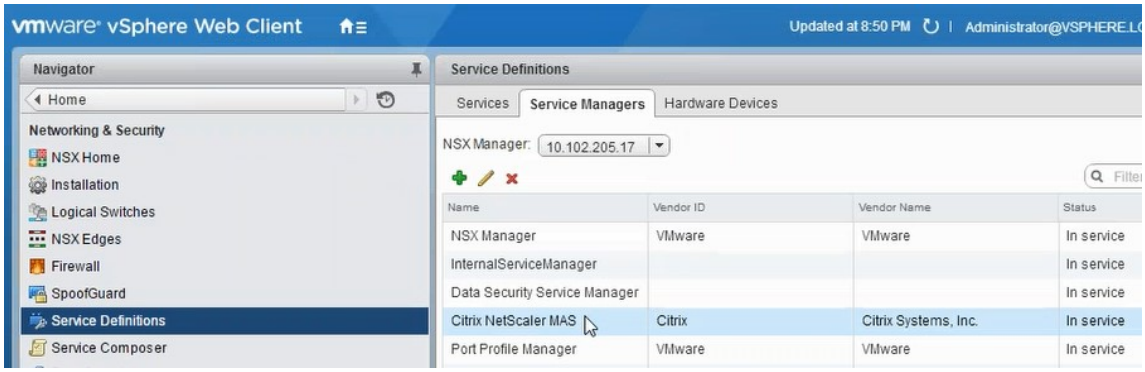
c) Password - NSX Manager の管理者ユーザーのパスワード

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 NetScaler ADM をサービスマネージャーの 1 つとして表示できます。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。

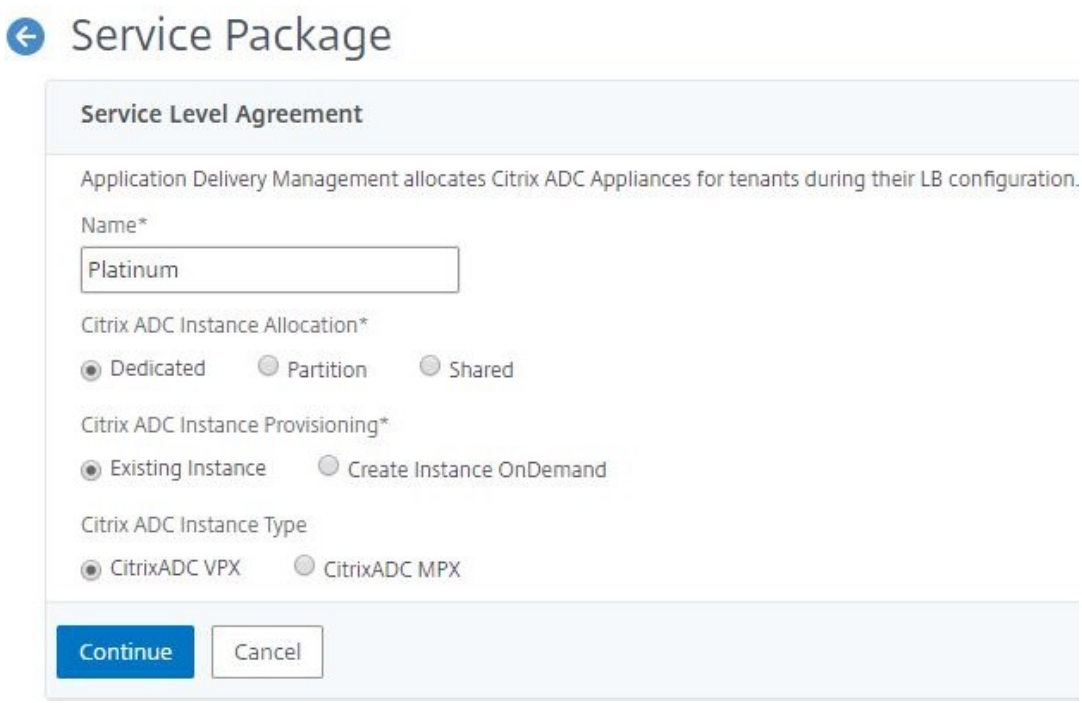


NetScaler ADM でのサービスパッケージの作成

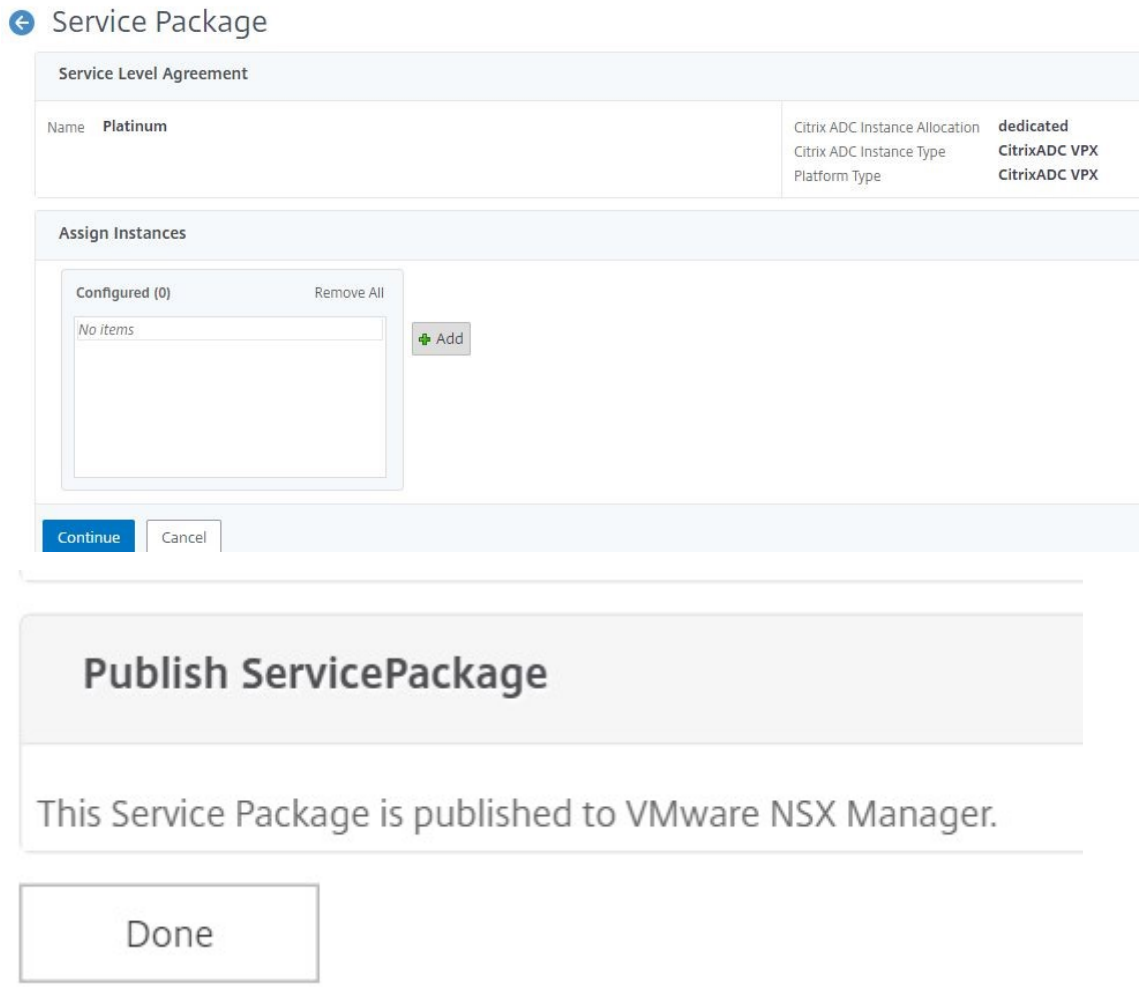
1. **NetScaler ADM** で、**[**オーケストレーション**] > [SDN** オーケストレーション**] > [**VMware NSX Manager**] > [**サービスパッケージ**]** に移動し、**[**追加**]** をクリックして新しいサービスパッケージを追加します。
2. 「サービスパッケージ」ページの「基本設定」セクションで、次のパラメータを設定します。
   a) Name - サービスパッケージの名前を入力します。
   b) Isolation Policy - デフォルトでは、分離ポリシーは［Dedicated］に設定されています。
   c) Device Type - デフォルトでは、デバイスの種類は［NetScaler VPX］に設定されています。

   > 注:
   >
   > これらの値は、このバージョンではデフォルトで設定されており、変更することはできません。

   d)［続行］をクリックします。



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。



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 NetScaler VPX インスタンスを NetScaler ADM にオフロードできます。

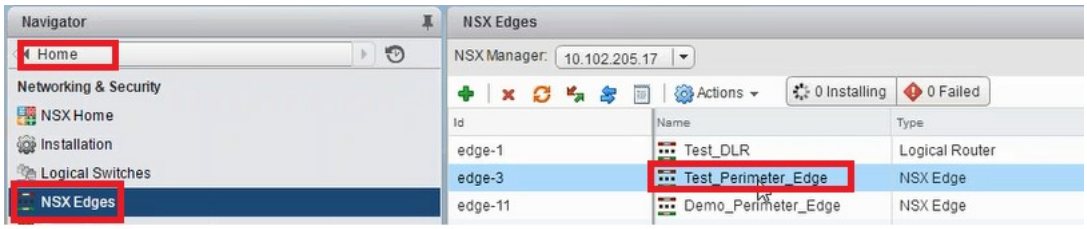
5. **vSphere Web Client** で **NSX Manager** にログインし、**[**** サービス定義**] > [**サービス] に移動します。**

   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。

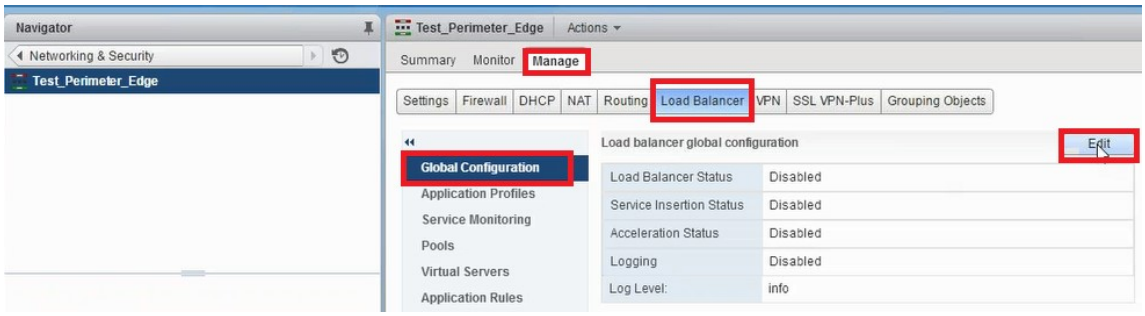
Edge 向けのロードバランサーサービスの挿入の実行

これまでに作成した NSX Edge ゲートウェイでロードバランサーサービスの挿入を実行します（NSX LB から NetScaler への負荷分散機能のオフロード）。

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。

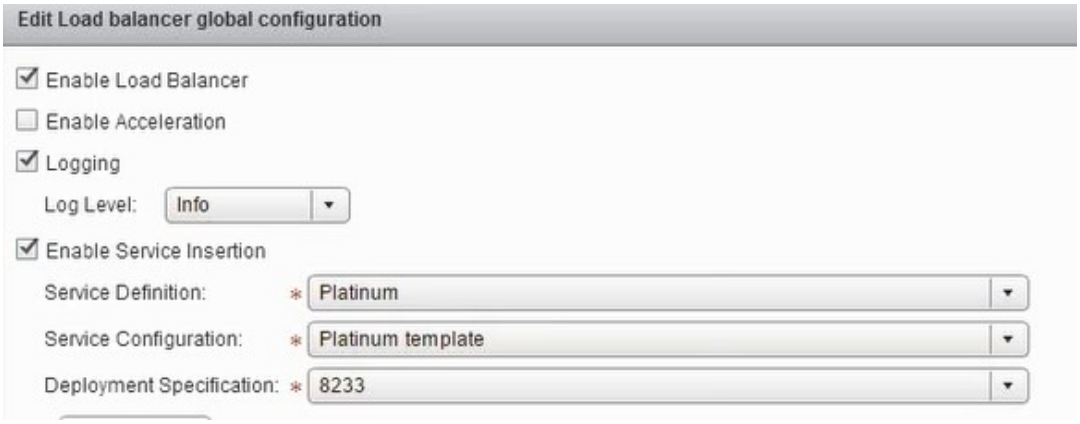


2. [管理] をクリックし、[ロードバランサ] タブで [グローバル構成] を選択し、[編集] をクリックします。

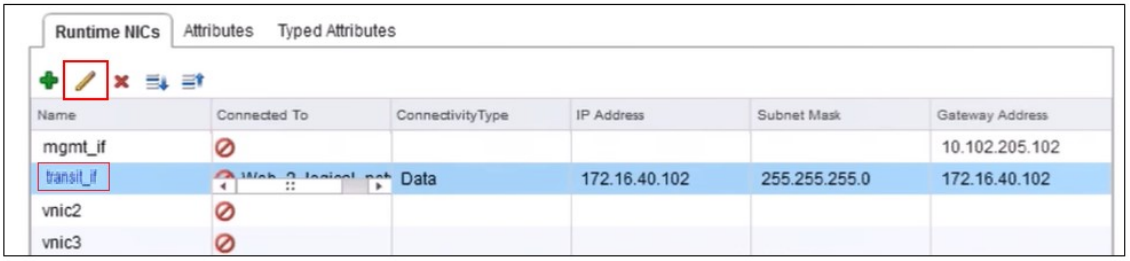


3. [ロードバランサを有効にする]、[ログ]、[サービス挿入を有効にする] の順に選択して有効にします。

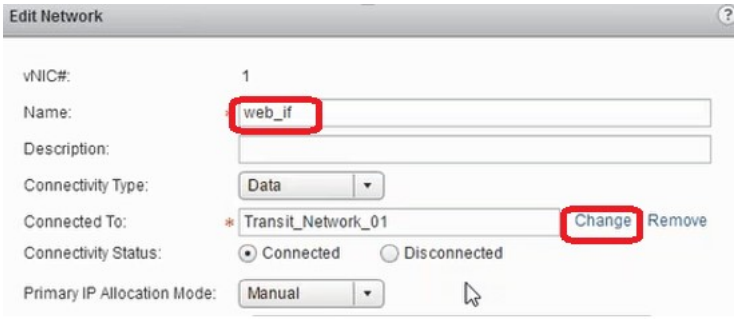
   a) [サービス定義**]** で、 NetScaler ADM で作成され、NSX Manager に公開されたサービスパッケージを選択します。



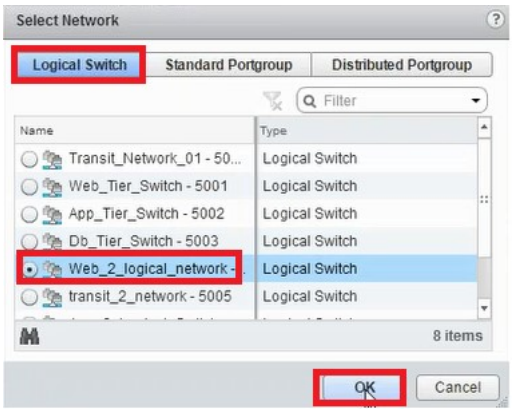
4. 既存のランタイム NIC を選択し、［編集］アイコンをクリックして、NetScaler VPX が割り当てられているときに接続する必要があるランタイム NIC を編集します。



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。

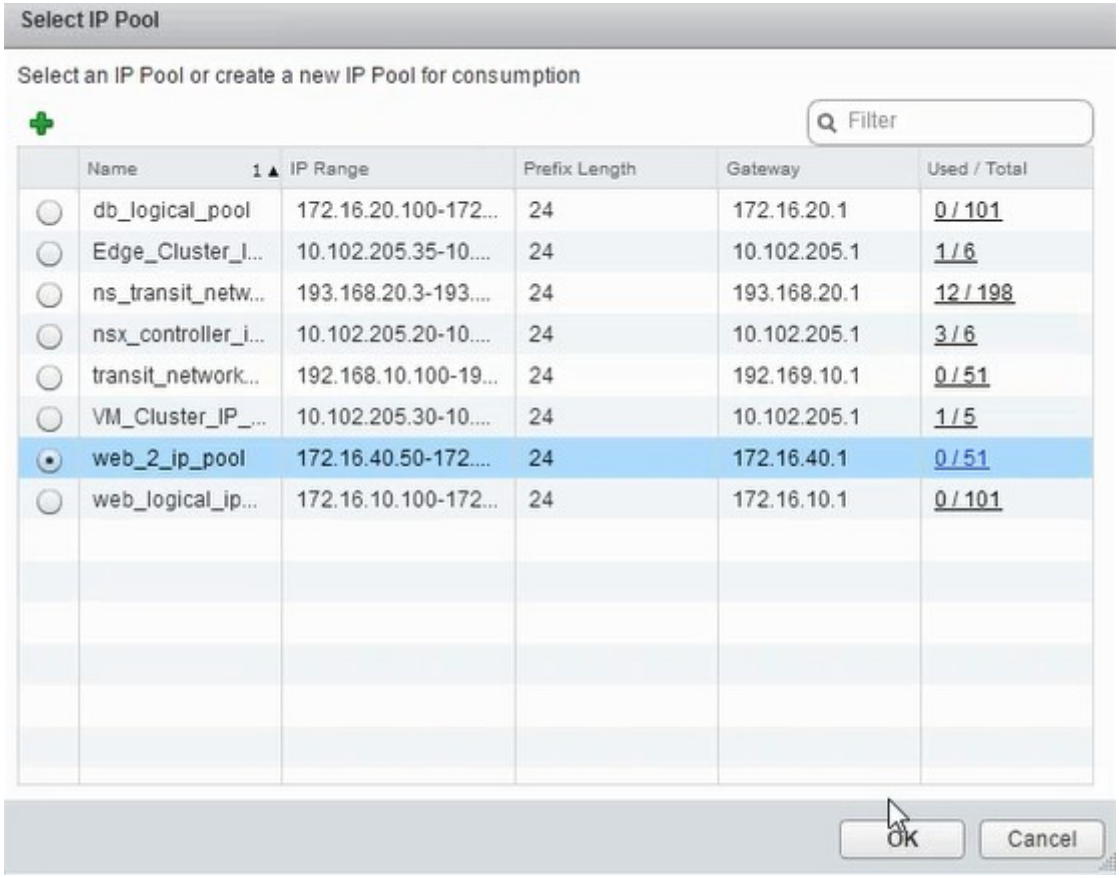


6. 適切な Web 論理スイッチを選択します。



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。

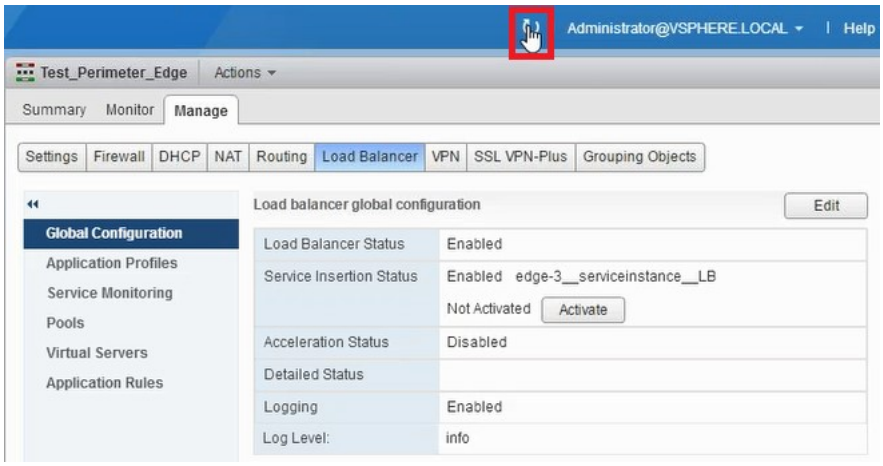
8. **[IP** プールの選択**]** ウィンドウで、適切な IP プールを選択し、[**OK**] をクリックします。

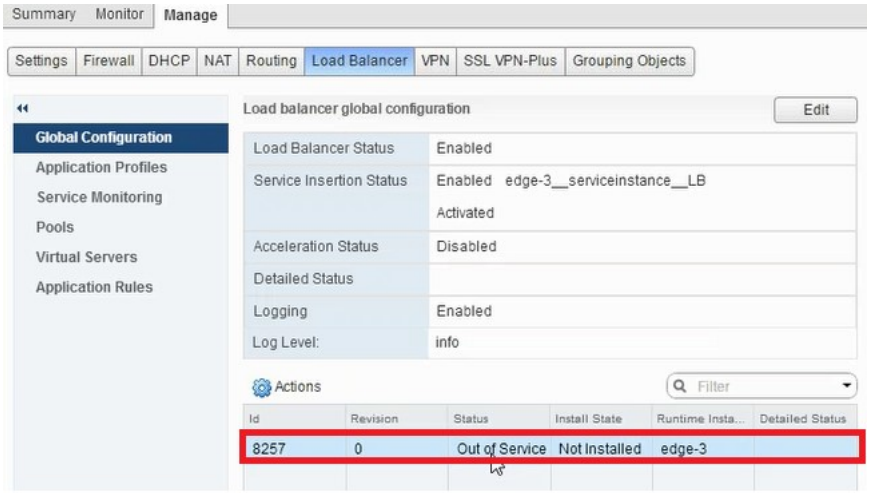


IP アドレスが取得され、NetScaler VPX アプライアンスのソースネット IP アドレスとして設定されます。VXLAN を VLAN にマッピングするために、NSX Manager で L2 ゲートウェイが作成されます。

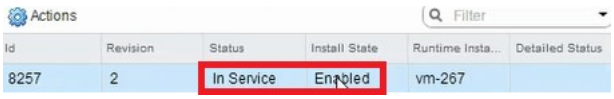
> 注:
>
> すべてのデータインターフェイスは実行時 NIC として接続され、分散論理ルーター用のインタフェースの一部です。

9. ビューを更新して、実行時の作成を確認します。





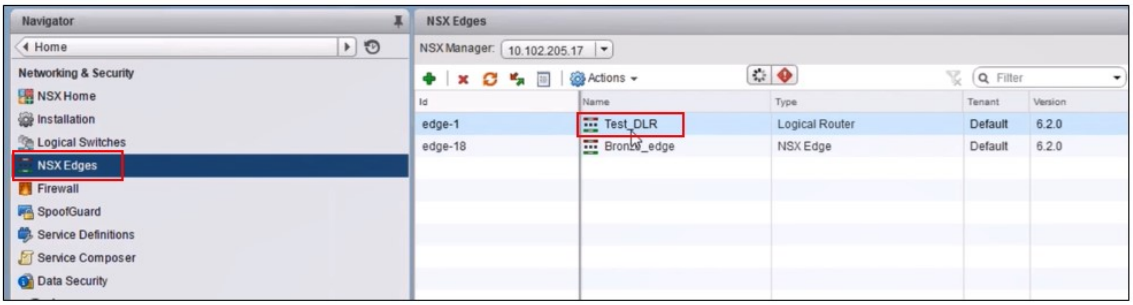
10. 仮想マシンの起動後、[状態] の値が [サービス 中] に変わり、[インストール状態] の値が [有効] に変わります。



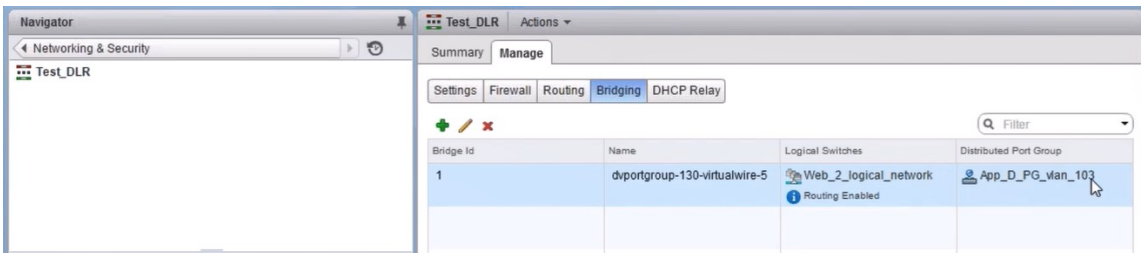
> 注:
>
> NetScaler ADM で、［オーケストレーション］>［リクエスト］に移動して、LB サービス挿入の完了の進行状況の詳細を確認します。

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。

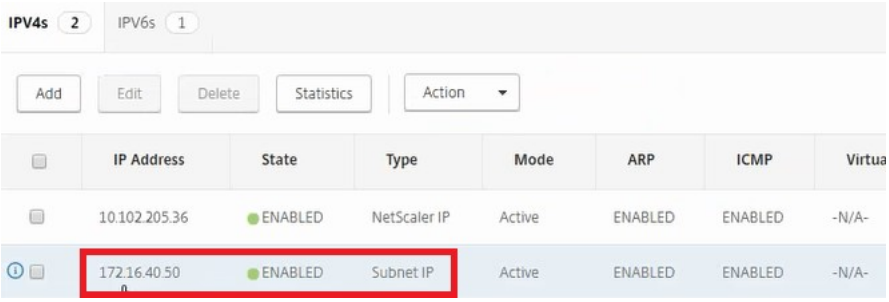


> 注:
>
> L2 Gateway は、データインターフェイスごとに作成されます。

割り当てられた **NetScaler** の表示

1. NetScaler ADM に表示されている IP アドレスを使用して NetScaler VPX インスタンスにログオンします。次に、[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。



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

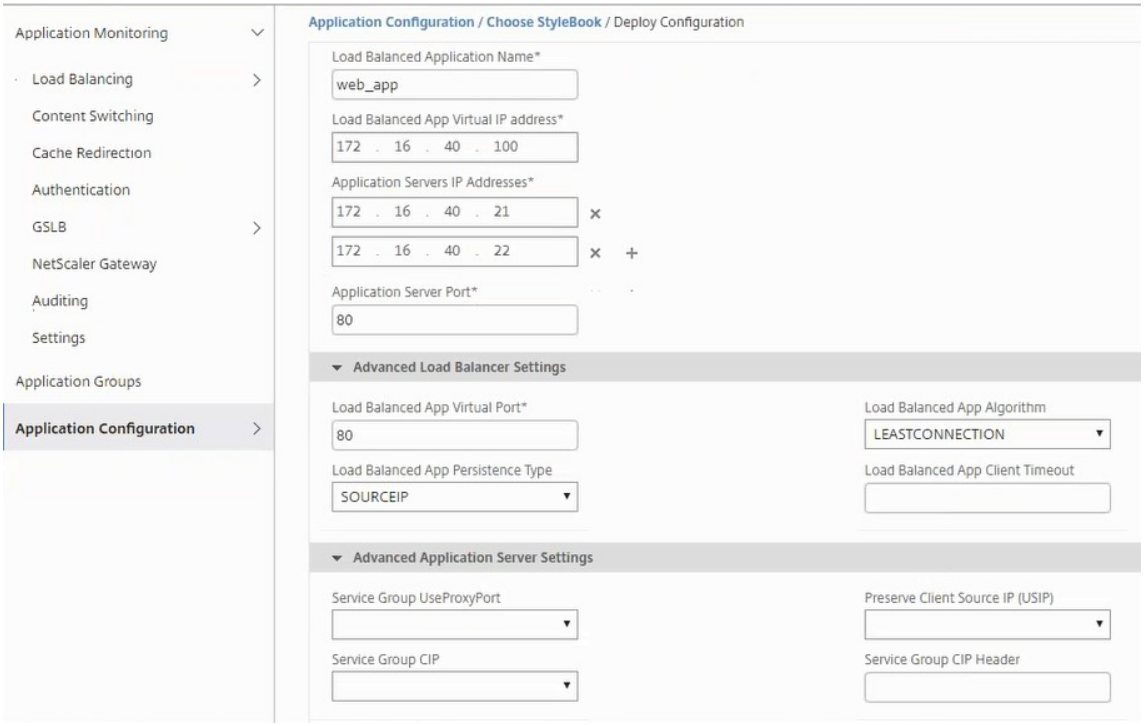
1. NetScaler ADM で、［オーケストレーション］>［**SDN** オーケストレーション］>［**NSX Manager** の構成］>［エッジゲートウェイ］に移動します。

   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。

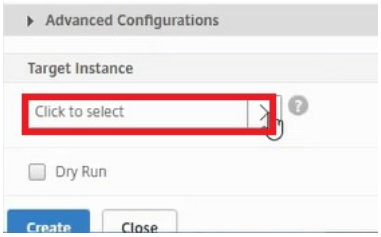
2. 新しい StyleBook を作成します。「アプリケーション」>「設定」の順に選択し、StyleBook をインポートして、リストから StyleBook を選択します。

   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。

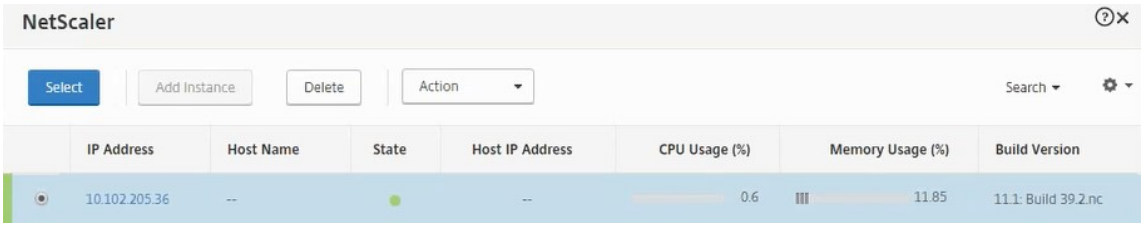
3. すべての必須パラメーターに対して値を指定します。



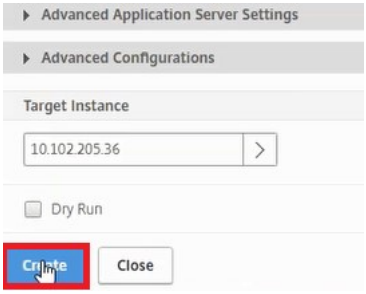
4. これらの構成設定を実行する NetScaler ADC VPX インスタンスを指定します。



5. 前述の IP インスタンスを選択し、[**Select**] をクリックします。

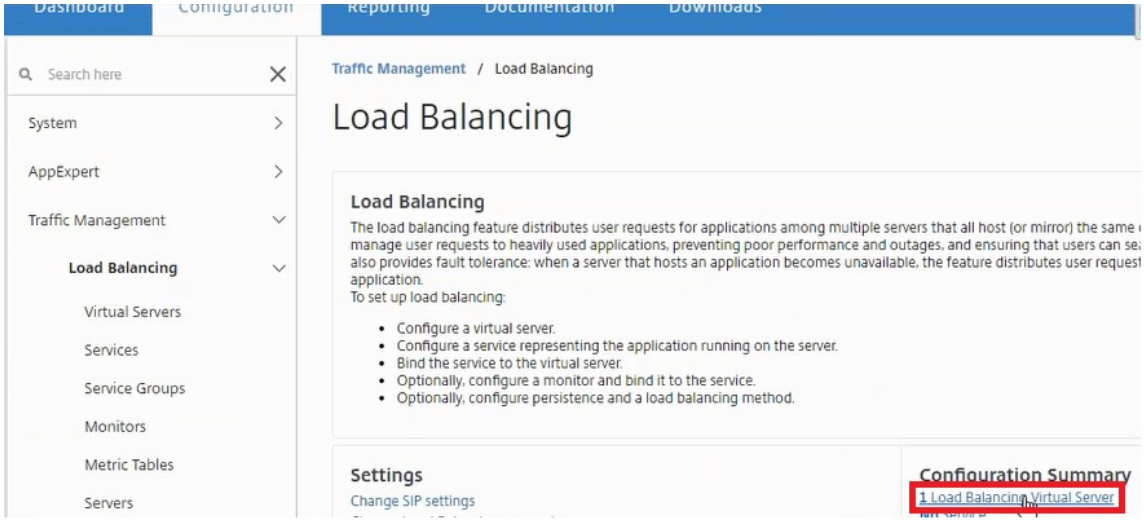


6. [**Create**] をクリックして、選択したデバイスに設定を適用します。

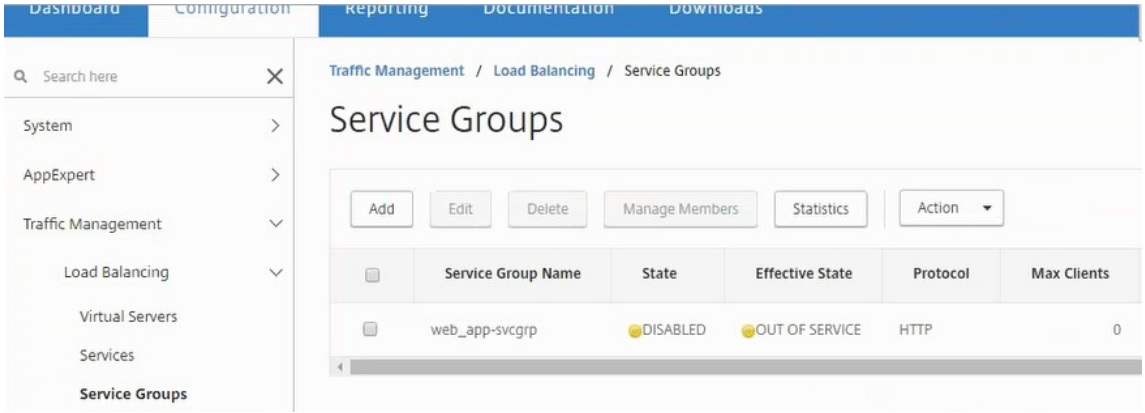


ロードバランサー構成の表示

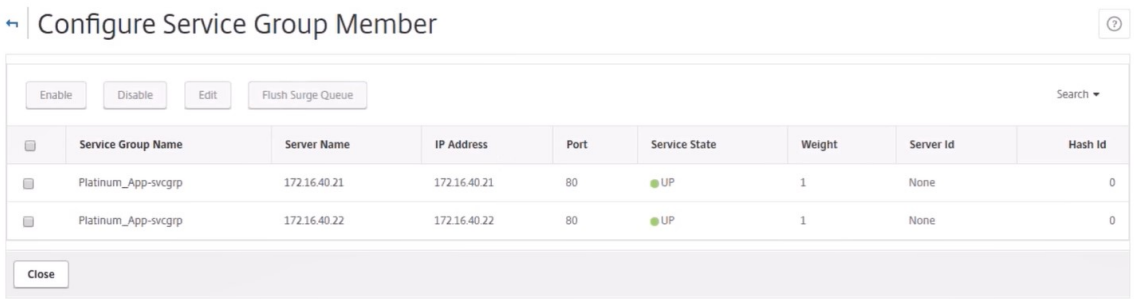
1. NetScaler VPX インスタンスにログオンし、［構成］>［トラフィック管理］>［負荷分散］の順に選択し、作成された負荷分散仮想サーバーを表示します。



作成したサービスグループも表示できます。



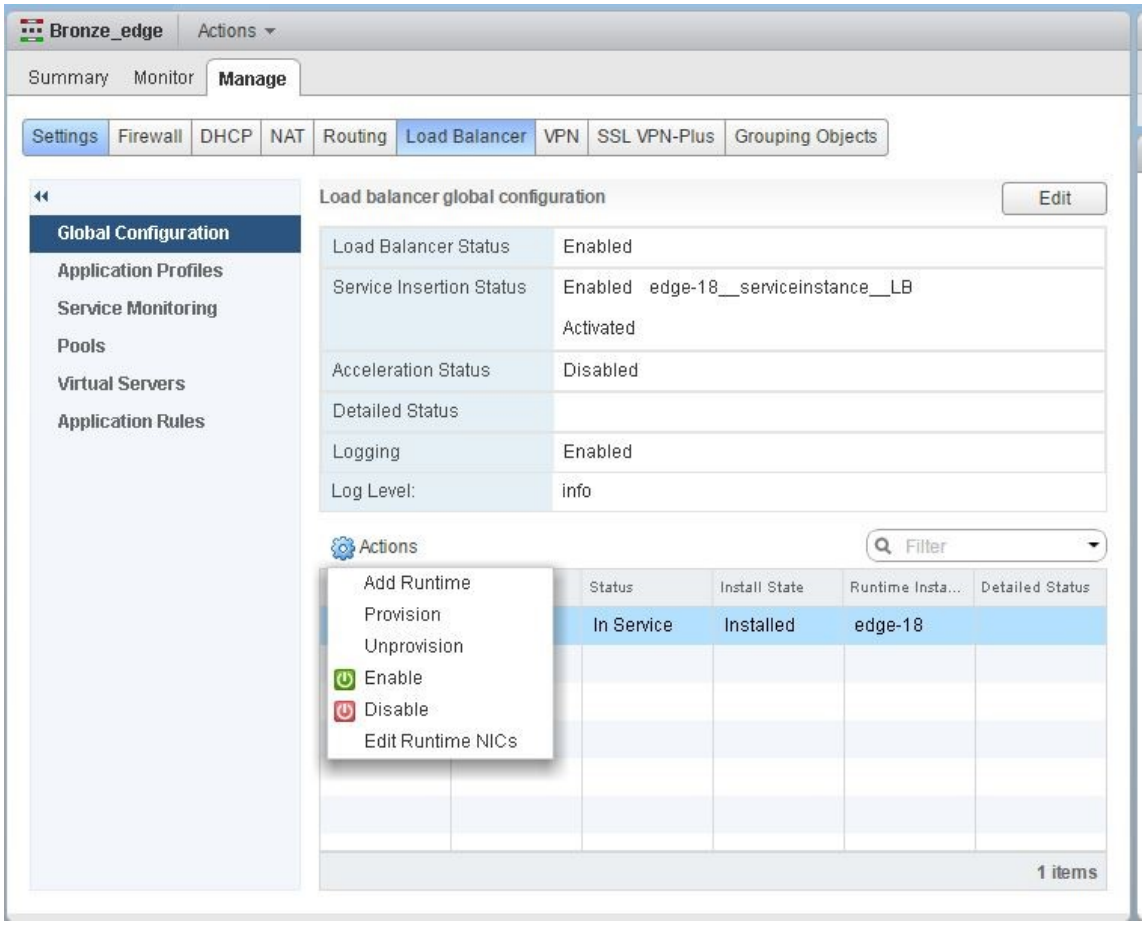
2. サービスグループを選択し、[メンバーの管理] をクリックします。サービスグループに割り当てられたメンバーが［**Configure Service Group Member**］ページに表示されます。



ロードバランサーサービスの削除

1. NetScaler 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、NetScaler VPX インスタンスが接続されているエッジゲートウェイに移動します。
3. [管理] > [ロードバランサー] > [グローバル設定] 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 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 インスタンスの自動 Provisioning

February 6, 2024

概要

NetScaler Application Delivery Management （ADM）は、VMware ネットワーク仮想化プラットフォームと統合して、NetScaler サービスの導入、構成、管理を自動化します。この統合により、物理ネットワークトポロジにつきものである従来の複雑さが取り除かれ、vSphere および vCenter 管理者はプログラミングによって短時間で NetScaler サービスを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、NetScaler ADM は NetScaler インスタンスを動的にプロビジョニングおよび破棄します。この動的プロビジョニングでは、NetScaler VPX ライセンスの割り当てを NetScaler ADM で自動化する必要があります。NetScaler ライセンスが NetScaler ADM にアップロードされると、NetScaler ADM はライセンスサーバーの役割を果たします。

前提条件

> 注
>
> この統合は、**vSphere 6.1** 以前の **VMware NSX** でのみサポートされます。

- NetScaler ADM バージョン 13.0 が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。
- NetScaler VPX、バージョン 13.0
- NetScaler VPX Version 13.0 のインスタンス用の NetScaler VPX ライセンス
- 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。

NetScaler ADM および NetScaler インスタンスの高可用性導入

NetScaler ADM HA セットアップをプロビジョニングするには、NetScaler サイトからダウンロードした NetScaler ADM イメージファイルをインストールします。NetScaler ADM HA セットアップ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。

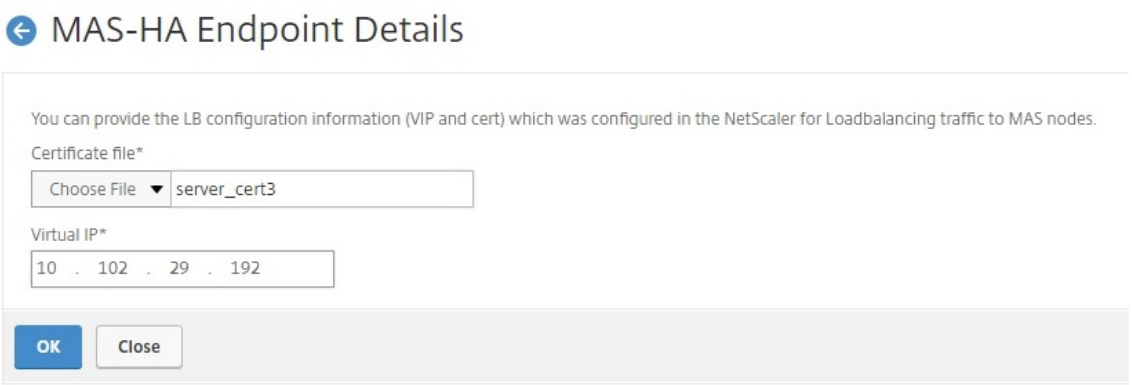
NetScaler ADM HA エンドポイントの詳細の設定

VMware NSX Manager を HA モードでデプロイされた NetScaler ADM と統合するには、まず負荷分散 NetScaler インスタンスの仮想 IP アドレスを入力する必要があります。また、NetScaler 負荷分散仮想サーバーにある証明書ファイルを NetScaler ADM ファイルシステムにアップロードする必要があります。

NetScaler ADM で負荷分散構成情報を提供するには:

1. **NetScaler 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 Detail** s 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。



VMware NSX マネージャーを **NetScaler ADM** に登録する

2 台の NetScaler 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 NetScaler ADM サーバーノードにログオンして、VMware NSX Manager を HA の NetScaler ADM に登録し、それらの間の通信チャネルを作成します。

VMware NSX マネージャーを **NetScaler ADM** に高可用性で登録するには:

1. プライマリ **NetScaler ADM** サーバーノードで、**[**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 NetScaler ADM アカウントセクションで、NSX Manager の NetScaler ドライバーパスワードを設定します。
5. [**OK**] をクリックします。

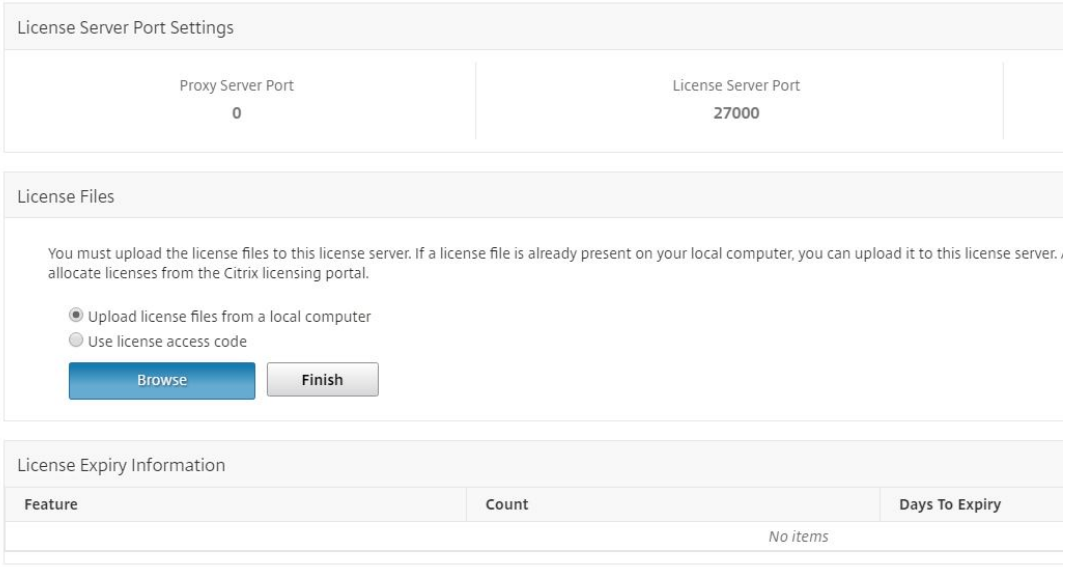
NetScaler ADM でのライセンスのアップロード

NetScaler VPX ライセンスを NetScaler ADM にアップロードすると、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. NetScaler ADM で、[インフラストラクチャ] **>** [プールライセンス] に移動します。
2. [ライセンスファイル] セクションで、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。



NetScaler ADM での **NetScaler ADC VPX** イメージのアップロード

NetScaler 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。

NetScaler VPX イメージを **NetScaler 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。

NetScaler 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 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。

NetScaler ADM でサービスパッケージを作成するには:

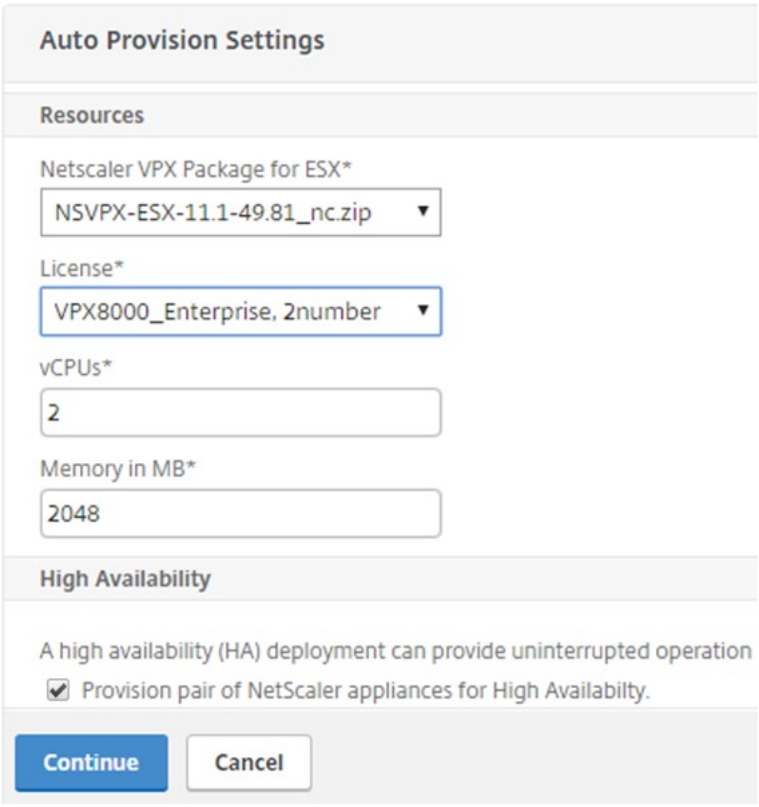
1. **NetScaler ADM** で、**[**オーケストレーション**] > [SDN** オーケストレーション**] > [**VMware NSX Manager**] > [**サービスパッケージ**]** に移動し、**[**追加**]** をクリックして新しいサービスパッケージを追加します。
2. 「サービスパッケージ」ページの「基本設定」セクションで、次のパラメータを設定します。
   a) Name - サービスパッケージの名前。
   b) 隔離ポリシー-「専用」を選択
   c) **NetScaler** インスタンス **Provisioning-**「オンデマ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- **CitrixNetScaler SDX** を選択

e)［**Continue**］をクリックします

3.「自動プロビジョニング設定」セクションで、**NSX** プラットフォームに展開する最近アップロードした **NetScaler VPX zip** パッケージを選択し、対応するライセンスを選択して、「続行」をクリックします。

> 注:
>
> ［高可用性］セクションで、NetScaler 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。



> 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。
> - アドバンスド-NetScaler には、スタンダード、アドバンス、プレミアムの 3 種類のライセンスがあります
> - 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。NetScaler ADM をサービスマネージャーの 1 つとして表示できます。これは、登録が成功し、NSX Manager と NetScaler ADM 間で双方向通信が確立されたことを示しています。

> 注:
>
> 高可用性環境の NetScaler ADM では、ライセンスは NetScaler ADM ライセンスサーバーノードにのみアップロードされます。NetScaler ADM ノードはアクティブ/パッシブモードです。

Edge 向け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 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。NetScaler 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:
>
> HA 展開では 2 つの NetScaler VPX インスタンスを展開するため、NSX Manager では 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. NetScaler 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捗状況の詳細を確認します。NetScaler ADM にランタイムの作成と更新のリクエストが届いていることがわかります。ランタイムが更新されたら、リクエストを選択して [タスク] ボタンをクリックすると、NetScaler ADM が NSX Manager に追加されたことを確認できます。

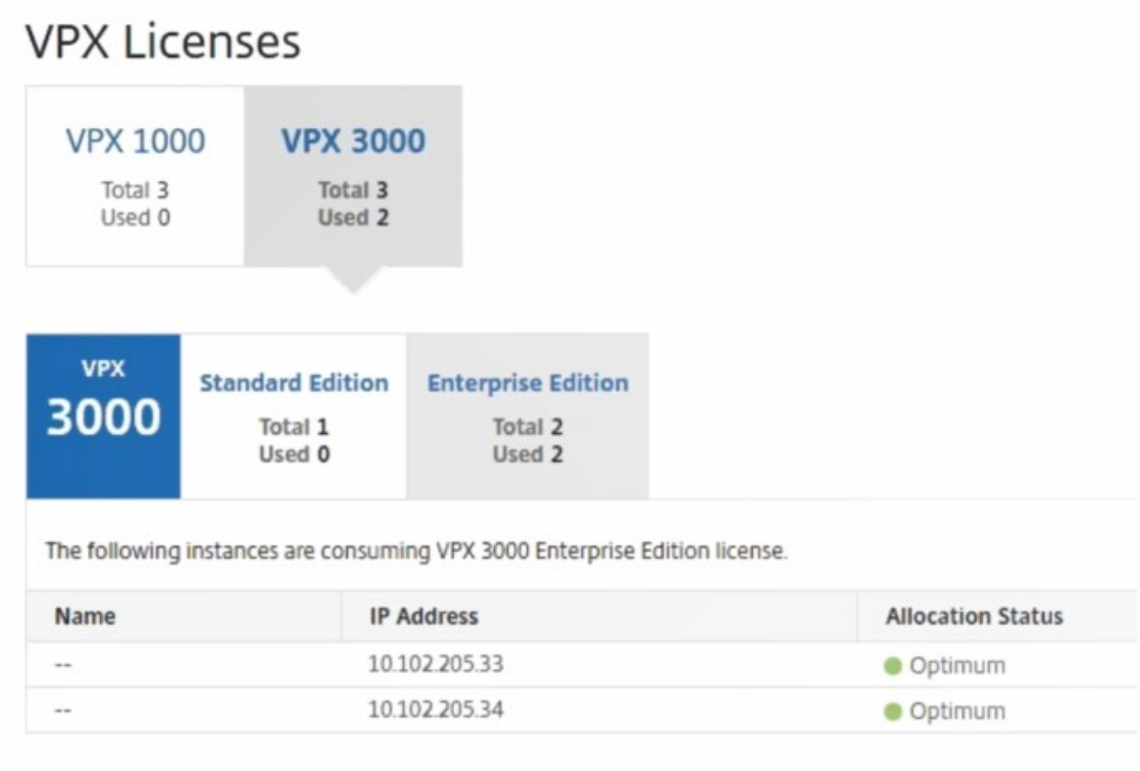
   HA の場合、NetScaler ADM で 2 つのランタイムを作成および更新するリクエストが 2 回送信されます。両方のランタイムが更新されたら、両方のリクエストを選択して［タスク］ボタンをクリックすると、NSX Manager に 2 つの NetScaler ADM HA ノードが追加されたことを確認できます。

10. **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 Manager] > [エッジゲートウェイ] に移動します。** 右側のパネルで、NetScaler VPX が NSX Edge ゲートウェイに追加されたことを確認します。

    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. NetScaler ADM で、［インフラストラクチャ］**>**［プールライセンス］**>**［**VPX** ライセンス］に移動します。NetScaler VPX ライセンスとインストールしたエディションを選択します。

    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 の GUI で NetScaler VPX の負荷分散サービスを構成する
- NetScaler ADM GUI での NetScaler ADC VPX での負荷分散サービスの構成

VMware NSX Manager の **GUI** で **NetScaler VPX** の負荷分散サービスを構成する

組み込みの StyleBook を使用して NSX Edge ゲートウェイデバイス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。

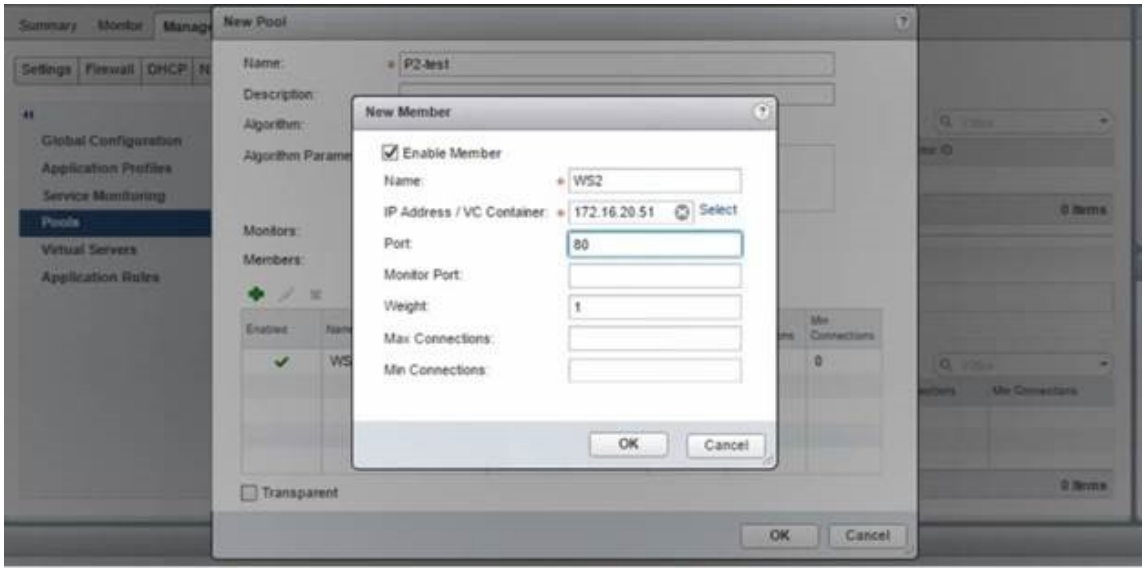
d) Members - ［+］をクリックしてプールにメンバーを追加し、［New Member］ウィンドウで必須パラメーターを入力します。

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。

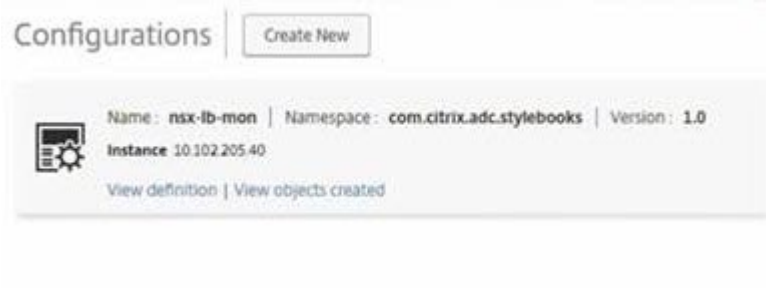
a) アプリケーションプロファイル-デフォルトでは、NetScaler ADM で作成したサービスプロファイルが表示されます。

b) 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 ADMStyleBook 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。高可用性展開であるため、ロードバランサー構成は高可用性モードである両方の NetScaler インスタンスに展開されます。

StyleBooks を使用してコンフィグパックを作成するには**:**

1. NetScaler ADM で、[アプリケーション] > [構成] > [新規作成] に移動し、一覧から [**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 NetScaler VPX インスタンスを選択し、[作成] をクリックして選択したデバイスに構成を適用します。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。

NetScaler VPX インスタンスでの仮想サーバーおよびサーバーグループの作成を確認する

NetScaler 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 VPX インスタンスにログオンします。高可用性展開であるため、高可用性モードである両方の NetScaler インスタンスへ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. NetScaler 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、NetScaler VPX インスタンスが接続されている Edge ゲートウェイにアクセスします。**[**** 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動状態になります。
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

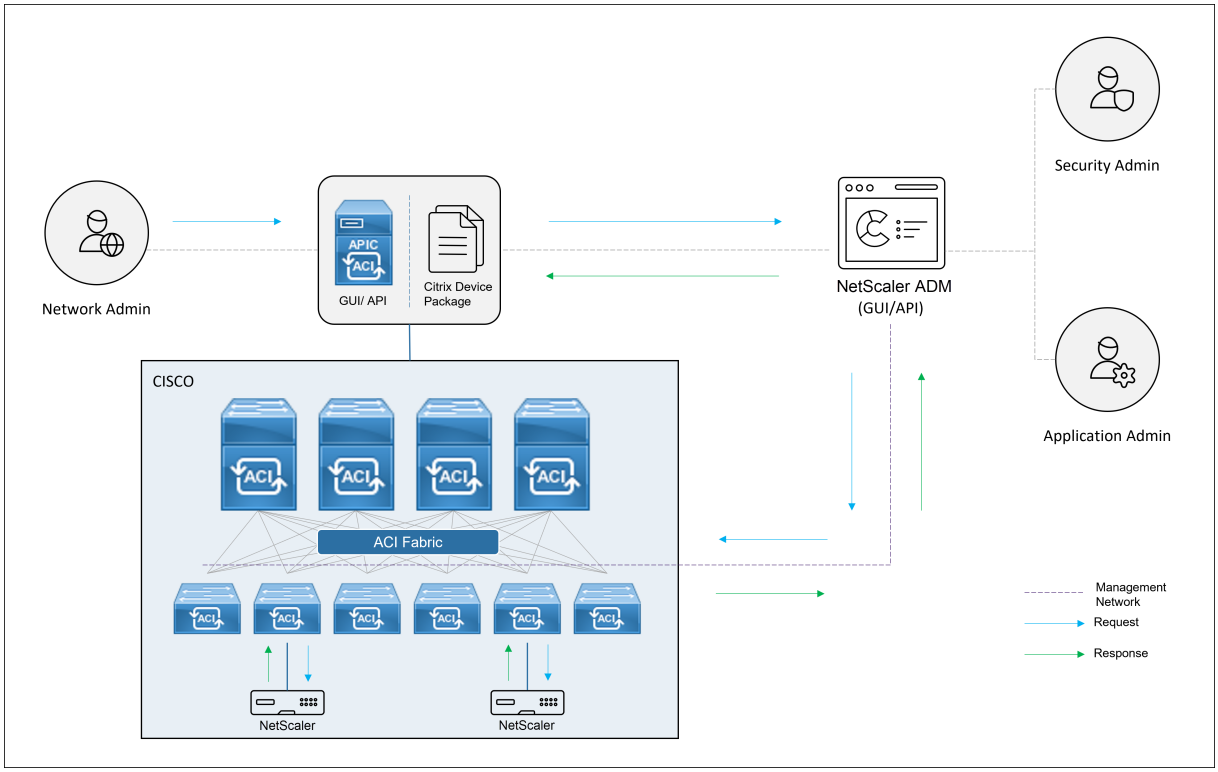
February 6, 2024

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）を介してネットワークの自動化を実行し、L4-L7 構成は APIC のデバイスマネージャーとして機能する NetScaler Application Delivery Management（ADM）に委任できます。

NetScaler ハイブリッドモードソリューションは、ハイブリッドモードのデバイスパッケージと NetScaler ADM によってサポートされています。APIC 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。このパッケージには、NetScaler からの L2〜L3 ネットワーク構成可能エンティティがすべて含まれていま

す。アプリケーションパリティは StyleBook によって NetScaler 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 から NetScaler 用にネットワークエンティティを構成しているときに、StyleBook 名を指定する必要があります。

次の図は、ハイブリッドモードソリューションにおける NetScaler ADC 概要を示しています。

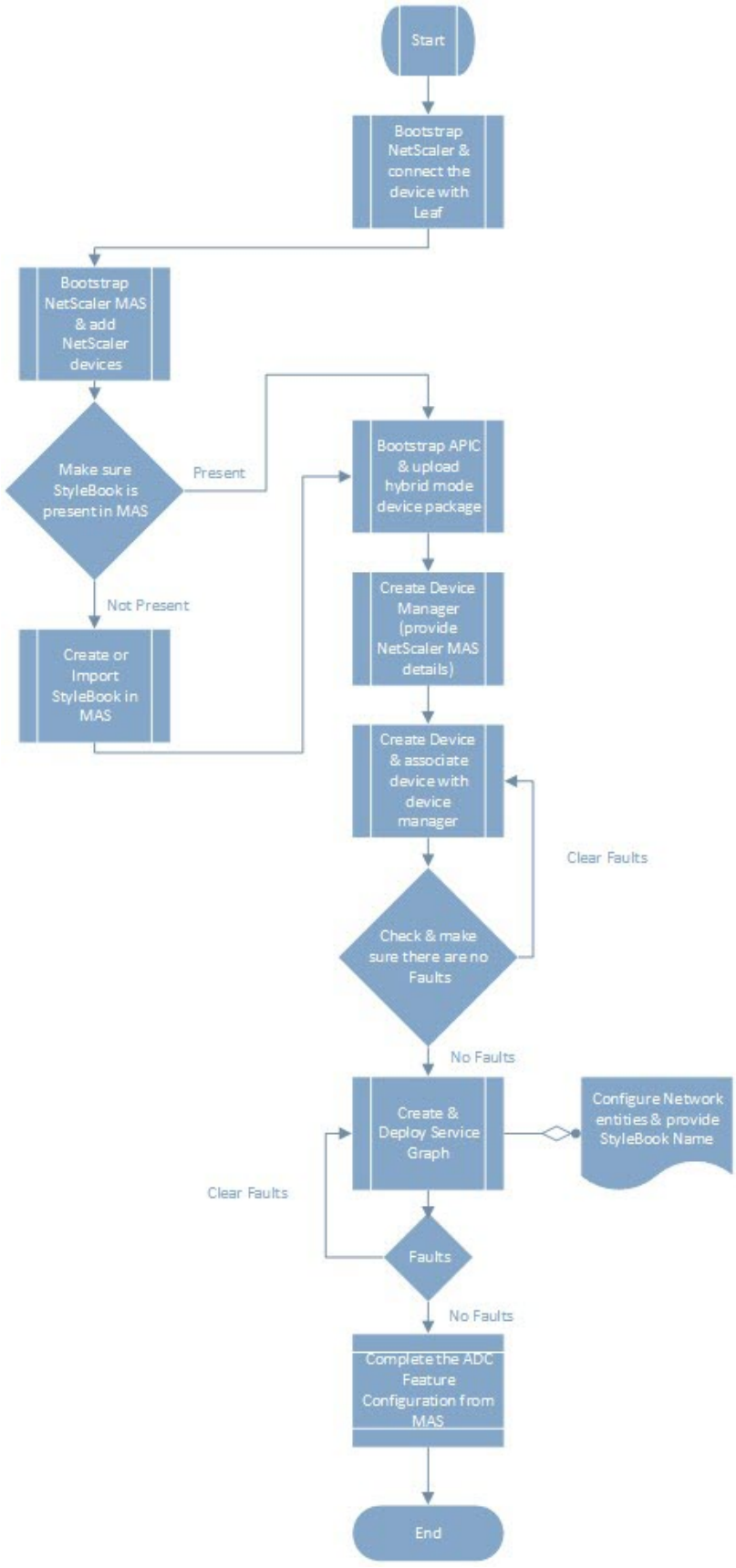


ハイブリッドモードでは、NetScaler 構成は次の 2 つのフェーズで実行されます。

1. Cisco APIC からネットワーク切り替えを実行する。
2. 構成は NetScaler ADM から行われます

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。次に、これらの構成の詳細がデバイスパッケージを通じて NetScaler ADM にプッシュされ、NetScaler ADM が内部でそれらを処理して NetScaler を構成します。アプリケーション管理者は NetScaler ADM の StyleBook を使用してアプリケーションの ADC 関連の構成を作成し、これらの構成は NetScaler ADM から NetScaler にプッシュされます。Cisco APIC と NetScaler ADM は、管理ネットワークを介して ADC と通信します。

次の図は、ハイブリッドソリューションにおける NetScaler ADC ワークフローを示しています。



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

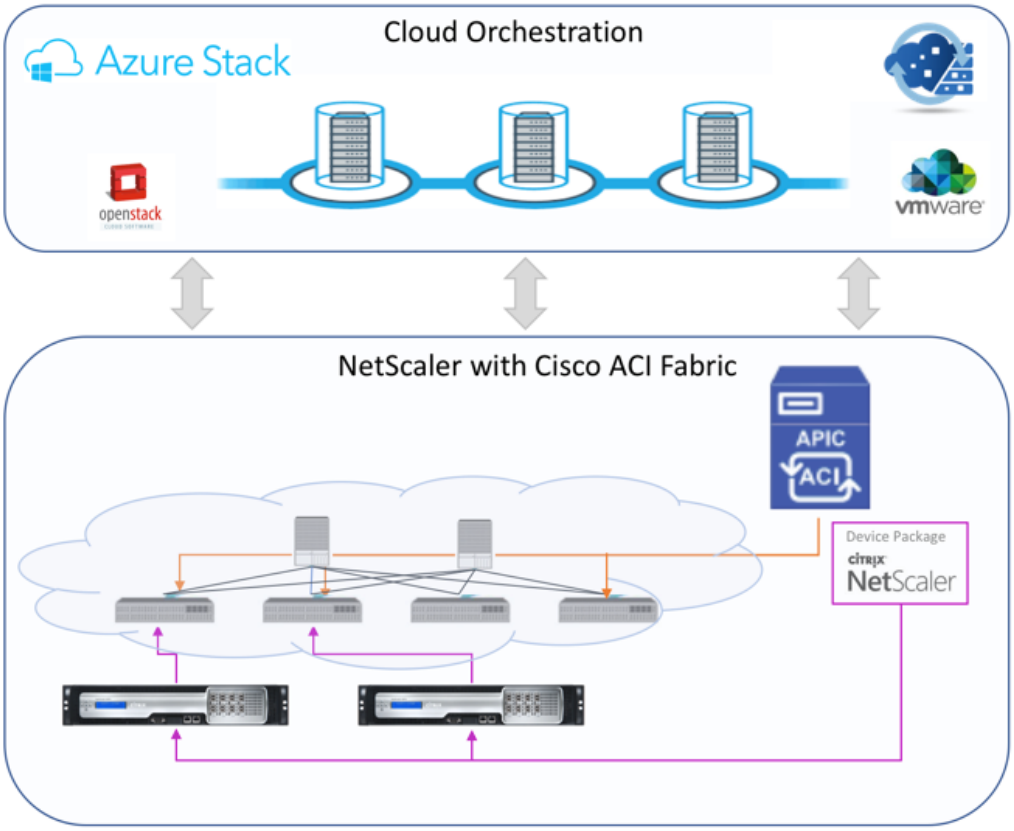
アプリケーションポリシーインフラストラクチャコントローラ（APIC）バージョン 3.1 により、Citrix ADC と Cisco ACI は共同統合ポートフォリオを拡大し、お客様のニーズに対応する新しいソリューションを提供します。新しい統合モードである ACI Cloud Orchestrator Mode* は、標準化されたパラメーターによって構成の複雑さを抽象化することで、L4-L7 の統合を簡素化します。このソリューションはシームレスに動作し、L4-L7 サービスを自動化し、アジャイルなアプリケーション展開、運用の柔軟性、シンプルさという目標を達成します。

NetScaler 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。

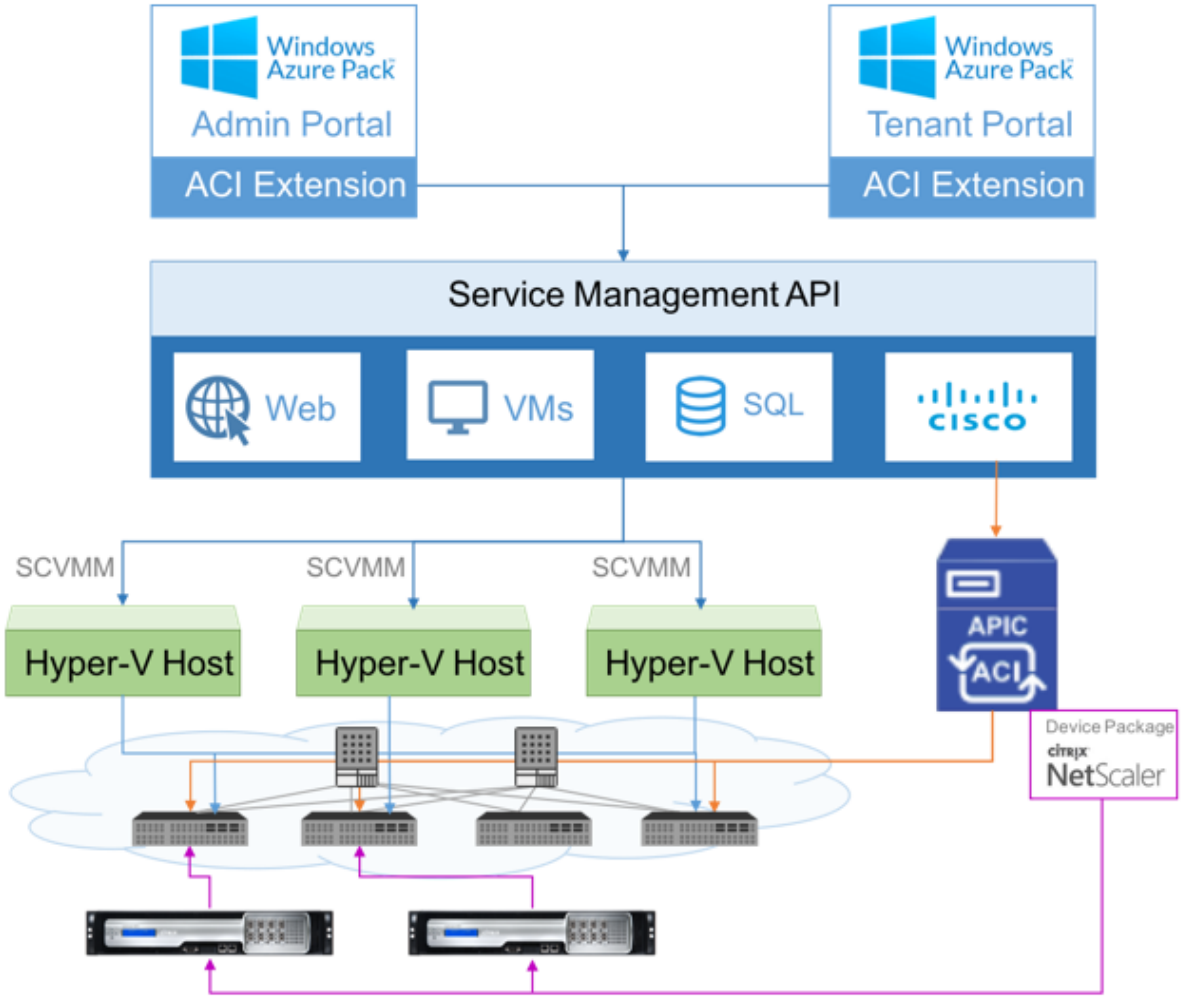


Microsoft Azure パックを使用するクラウドオーケストレーターモードソリューションには、Azure Pack から Cisco APIC、Cisco APIC からシステムセントラルのバーチャルマシンマネージャー (SCVMM)、Cisco APIC から NetScaler への統合など、多くのポイントが含まれます。プライベートクラウドのテナントとして、NAT の有効化、ネットワークサービスのプロビジョニング、ロードバランサーの追加を行うことができます。

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 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 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 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 MPX アプライアンスおよび NetScaler ADC VPX アプライアンス（NetScaler 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 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 のワンアームおよびツー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ーとして機能し、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ーモード（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 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 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
>
> - NetScaler ADM は、Kubernetes バージョン 1.14 ～1.21 のクラスターでイングレス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、同じクラスタまたは異なるクラスタ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、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 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、クラスタで必要な 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。

   ```
   kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole
      =cluster-admin --serviceaccount=default:citrixadm-sa
   <!--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。

   ```
   kubectl describe sa citrixadm-sa
   <!--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。

   ```
   kubectl describe secret <token-name>
   <!--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 クラスターを NetScaler ADM に登録する必要があります。

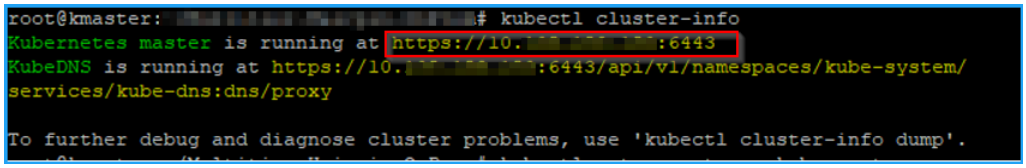
Kubernetes クラスターを登録するには、次の手順を実行します。

1. 管理者の資格情報を使用して NetScaler ADM にログオンします。
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。

      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 クラスターを管理するように 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 クラスターと 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。

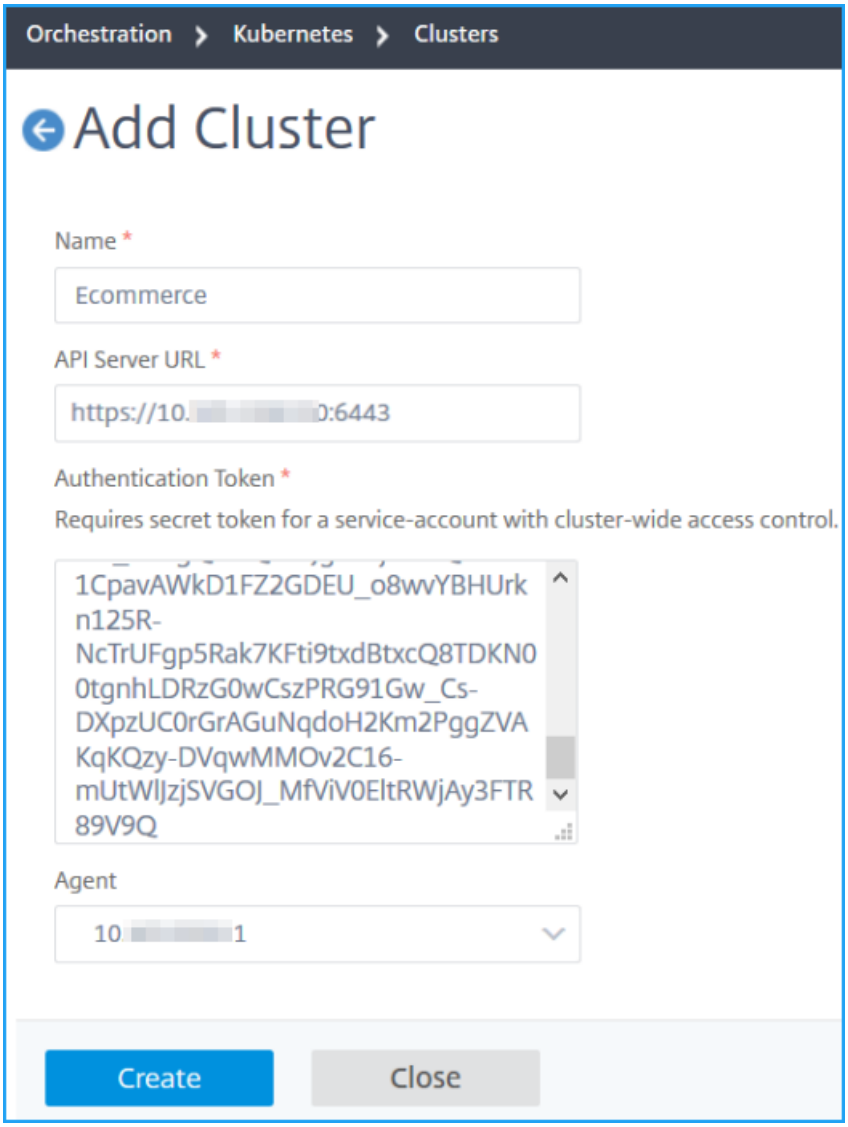
      ```
      kubectl describe secret <token-name>
      <!--NeedCopy-->
      ```

      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。



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 Net**work] 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、[インフラストラクチャー**] > [IP** アドレス管理] 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。

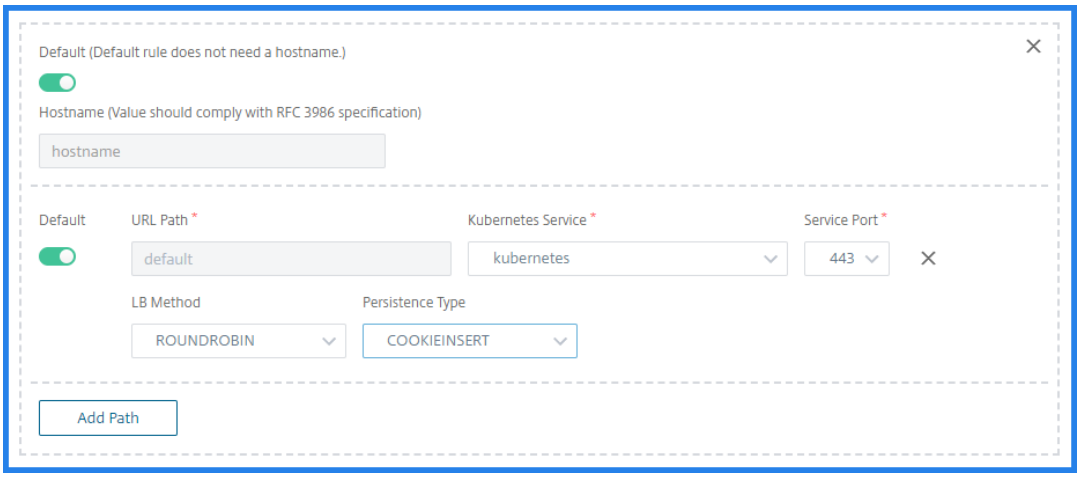
```
"lbmethod":"ROUNDROBIN"
<!--NeedCopy-->
```

- 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。

```
"persistenceType":"COOKIEINSERT"
<!--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。



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. **[設定] > [ライセンスと分析の設定]** に移動します。
> 2. [仮想サーバーライセンスの概要] で、**[仮想サーバーの自動選択]** を有効にします。

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。
- サブスクライバ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 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 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 アプライアンスを NetScaler Application Delivery Management（ADM）と統合すると、NetScaler アプライアンスを流れるビデオデータから重要な情報が収集されます。この情報を使用することで、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 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 プレミアムライセンスを持つ NetScaler インスタンスでサポートされます。NetScaler Premium ライセンスは、NetScaler Telco プラットフォーム（VPX T1000 および VPX-T）でサポートされています。

NetScaler インスタンスで Video Insight を構成するには、まず AppFlow 機能を有効にして AppFlow のコレクター、アクション、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。コレクターを構成するときは、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。

NetScaler 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

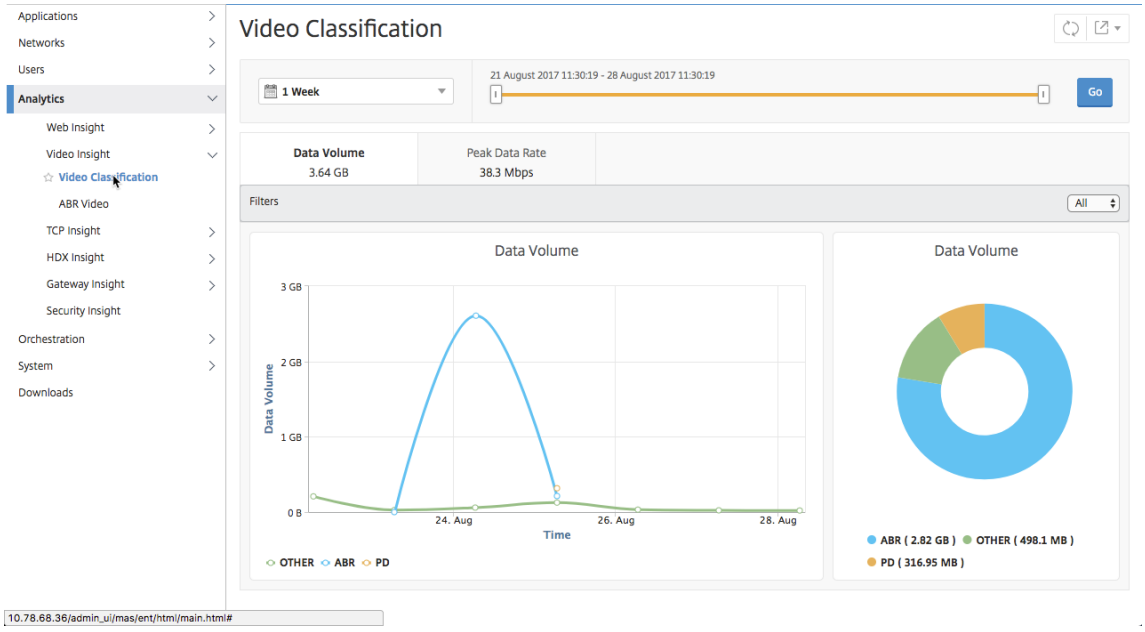
```
add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -
    Transport logstream
set appflow param -videoInsight ENABLED
add appflow action act1 -collectors col1 -videoAnalytics ENABLED
add appflow policy appol true act1
bind appflow global appol 1
enable ns mode ulfd
enable feature appflow
<!--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。

NetScaler ADM でビデオインサイトのメトリックを表示するには:

1. Web ブラウザで、NetScaler ADM 仮想アプライアンスの IP アドレス（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

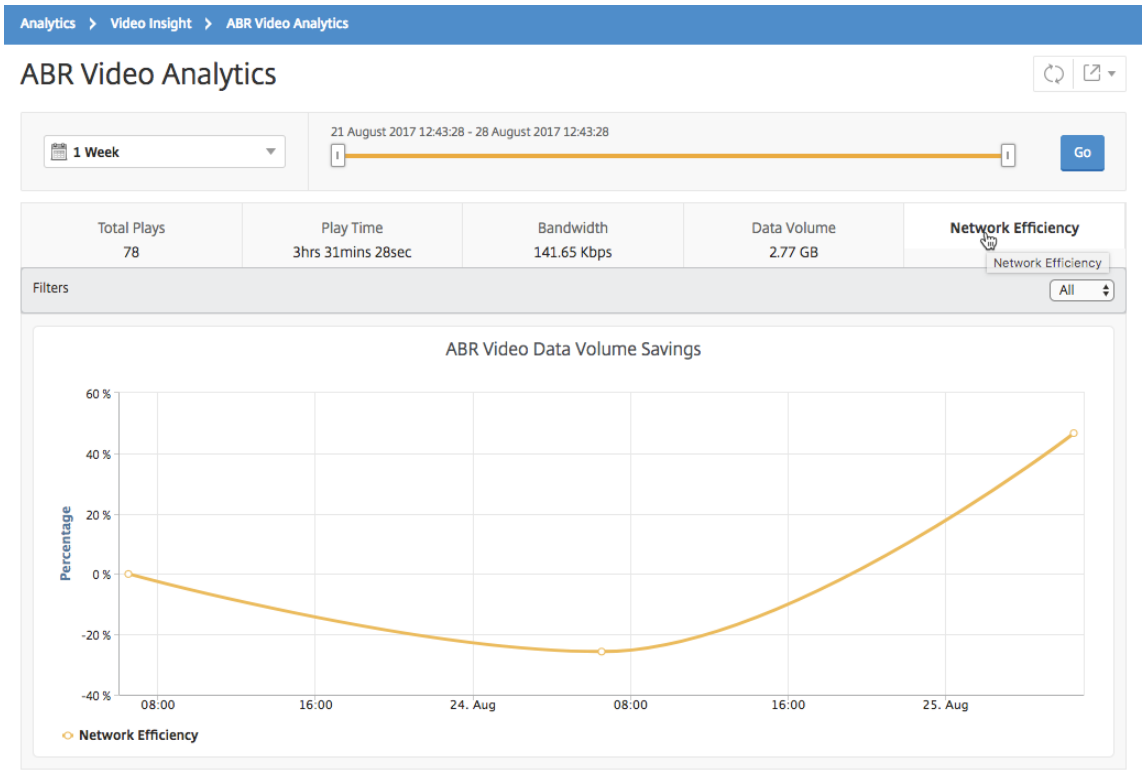
February 6, 2024

NetScaler Application Delivery Management（ADM）は、特定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

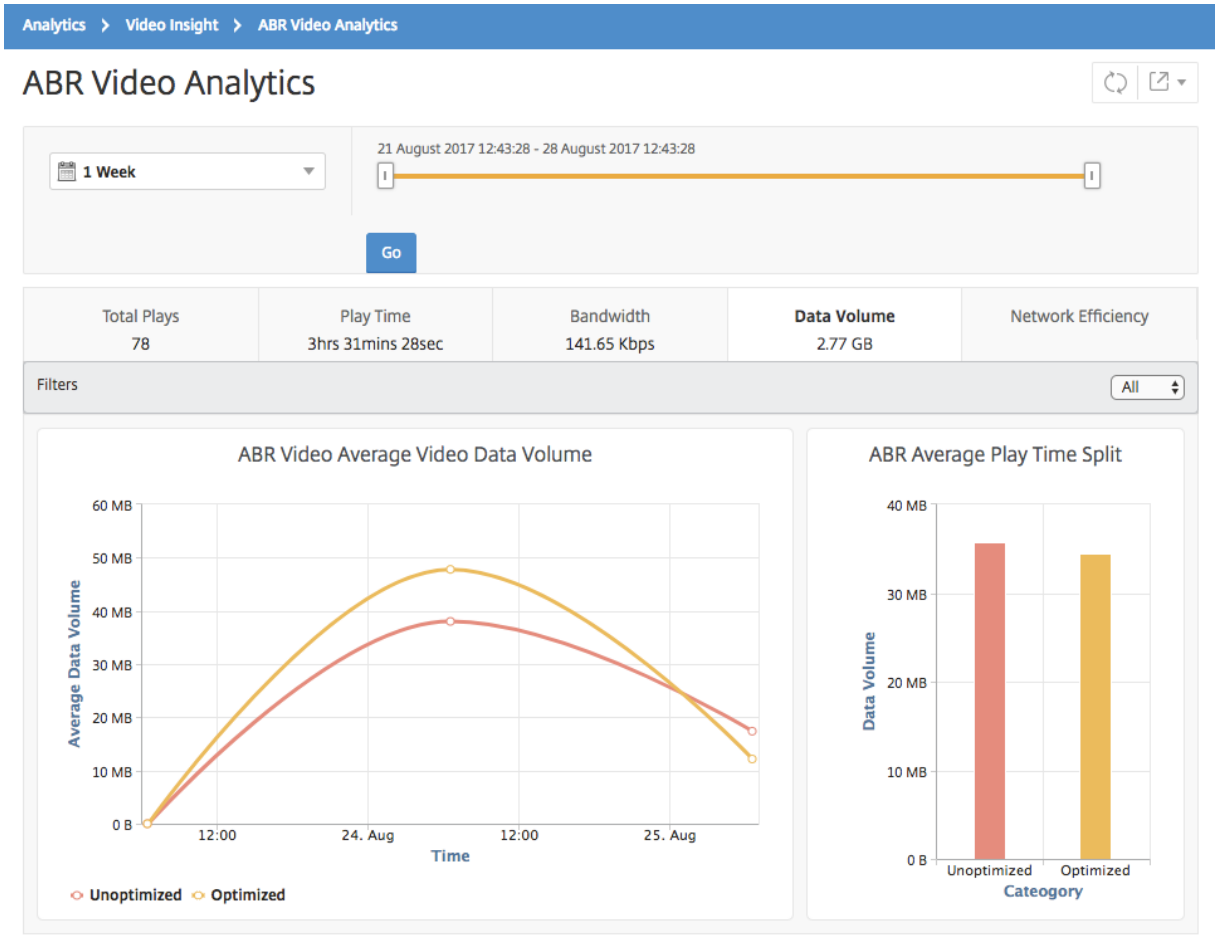
February 6, 2024

NetScaler Application Delivery Management（ADM）は、特定の時間枠で最適化された ABR ビデオと最適化されていない ABR ビデオで使用されたデータ量を表示するので、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:

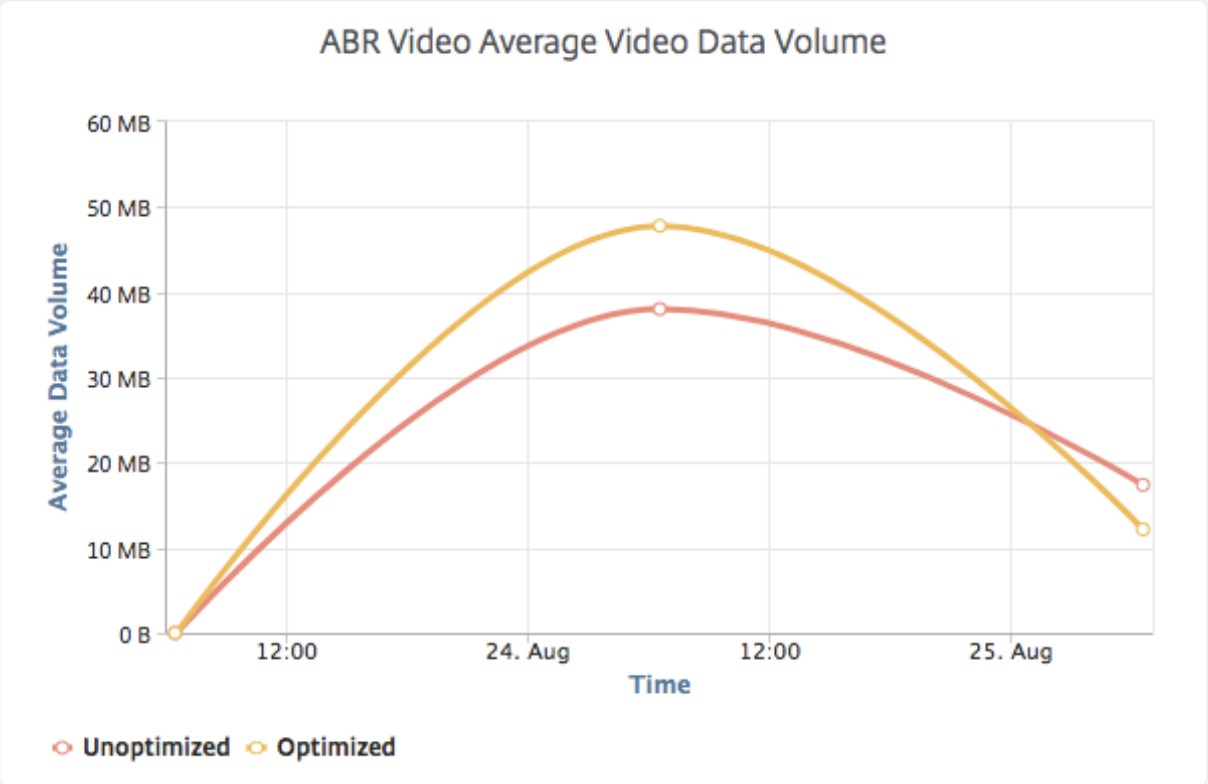
1. [分析] **>** [ビデオインサイト] に移動し、[**ABR** ビデオ] をクリックします。
2. 右側のペインで、リストから時間枠を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。
3. 「実行」をクリックし、「データボリューム」タブを選択します。

[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 ― 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

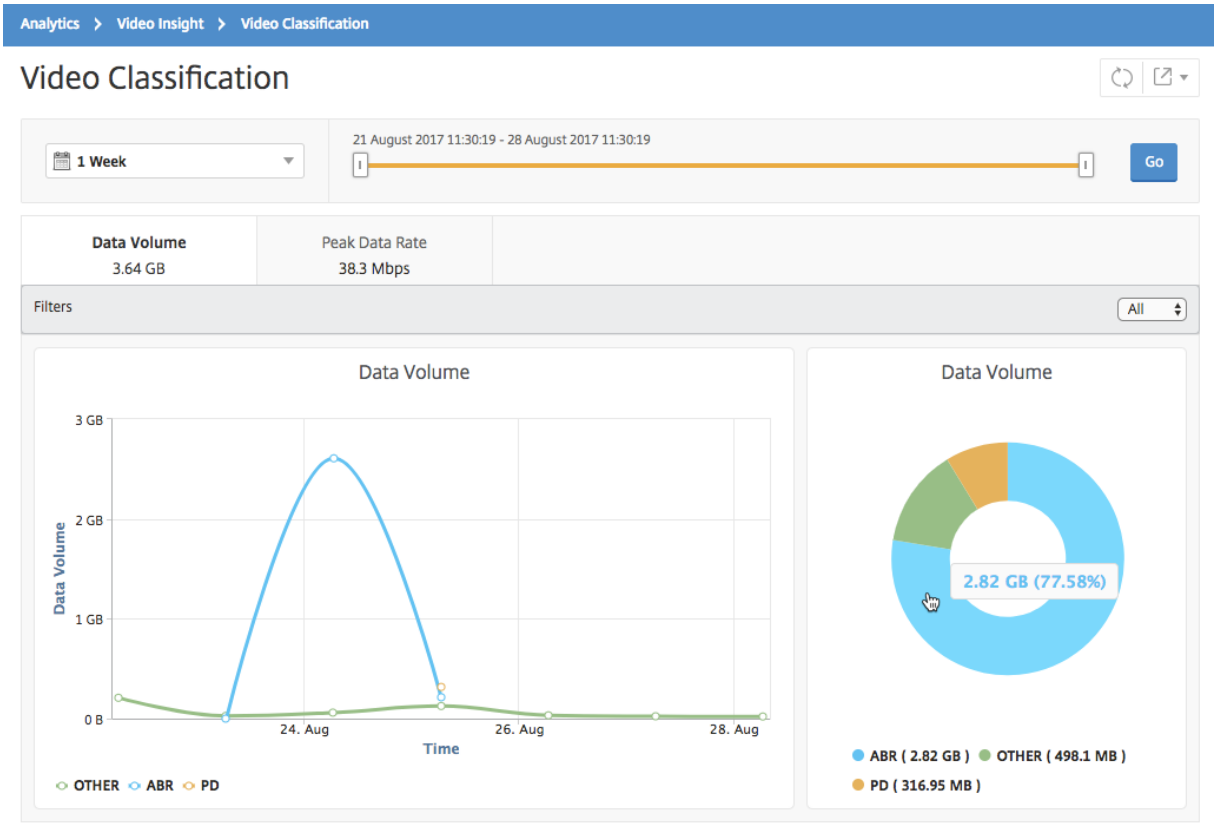
February 6, 2024

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。

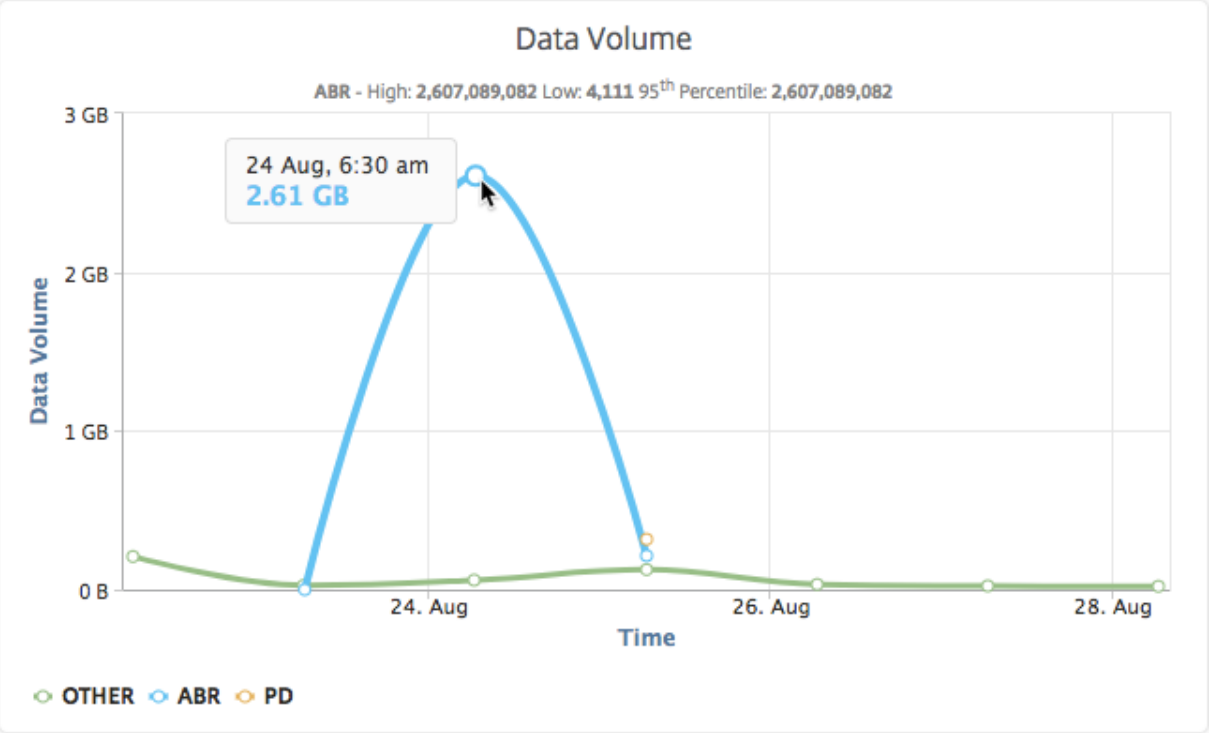
動画の種類と消費データ量を確認するには:

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。

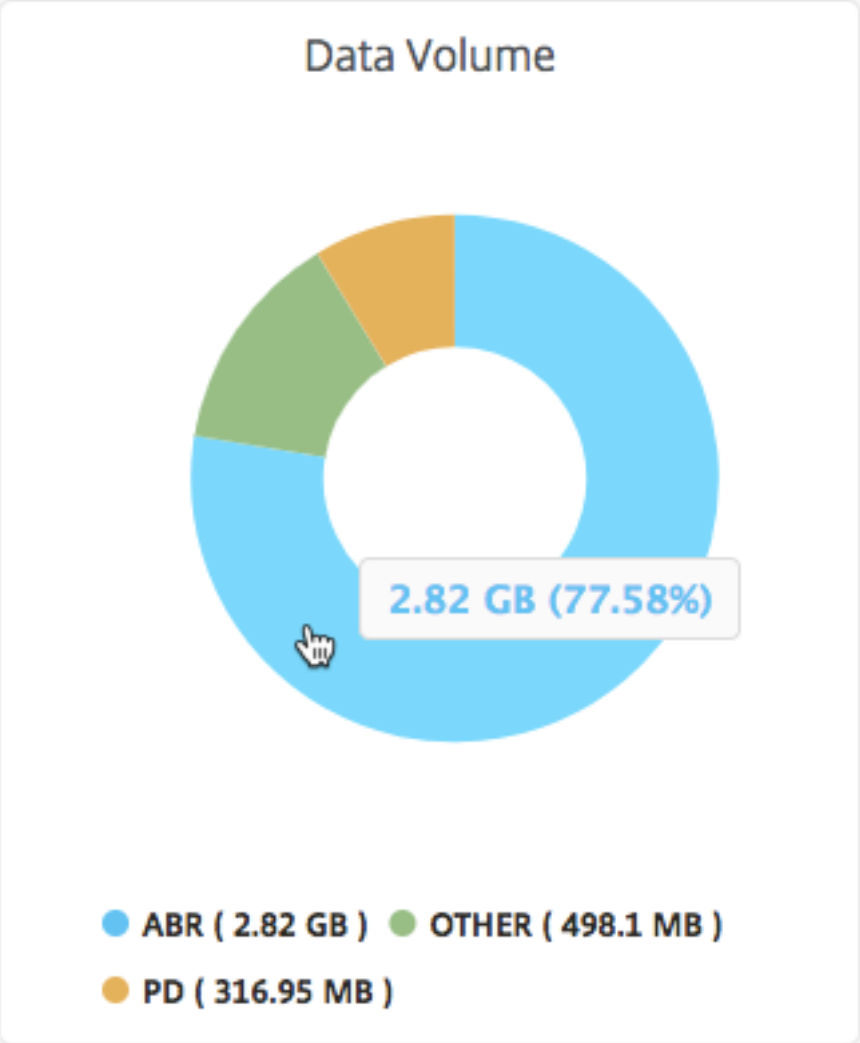
[フィルタ] リストを使用して、HTTP、HTTPS、または QUIC トラフィックを選択できます。



[**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 — 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

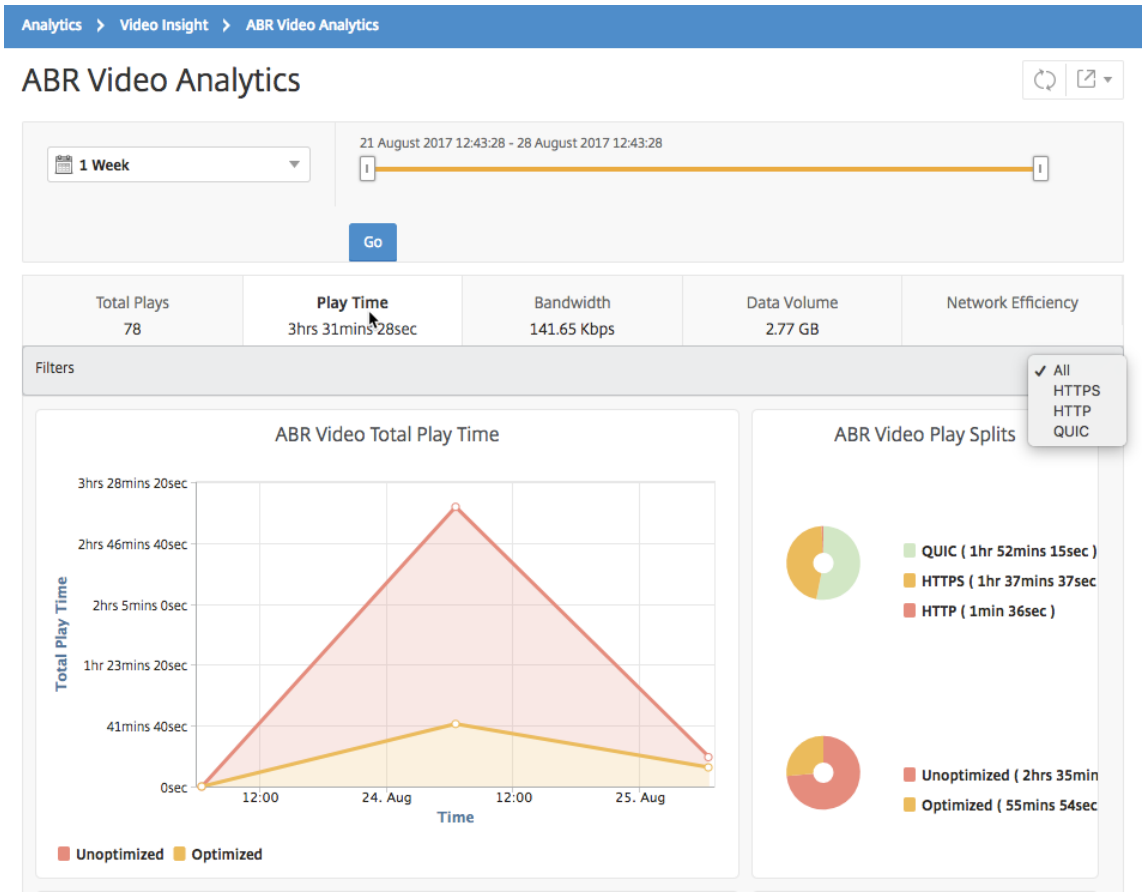
NetScaler Application Delivery Management （ADM）は、特定の時間枠で ABR ビデオの再生時間を表示し、ネットワーク内の最適化された ABR ビデオと最適化されていない ABR ビデオの再生時間を比較することもできます。

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。

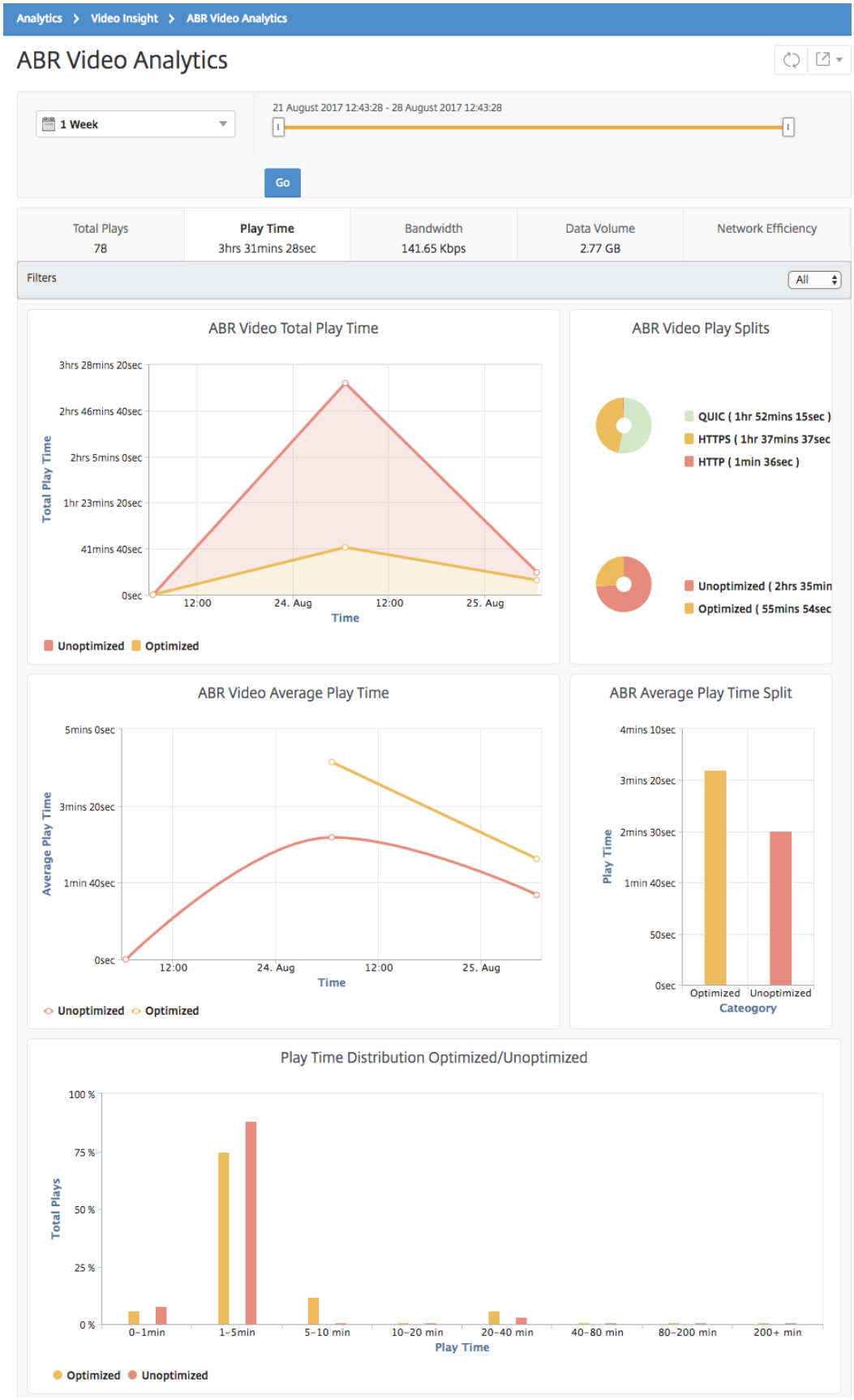
3. [移動] をクリックし、[再生時間] タブを選択します。

   [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

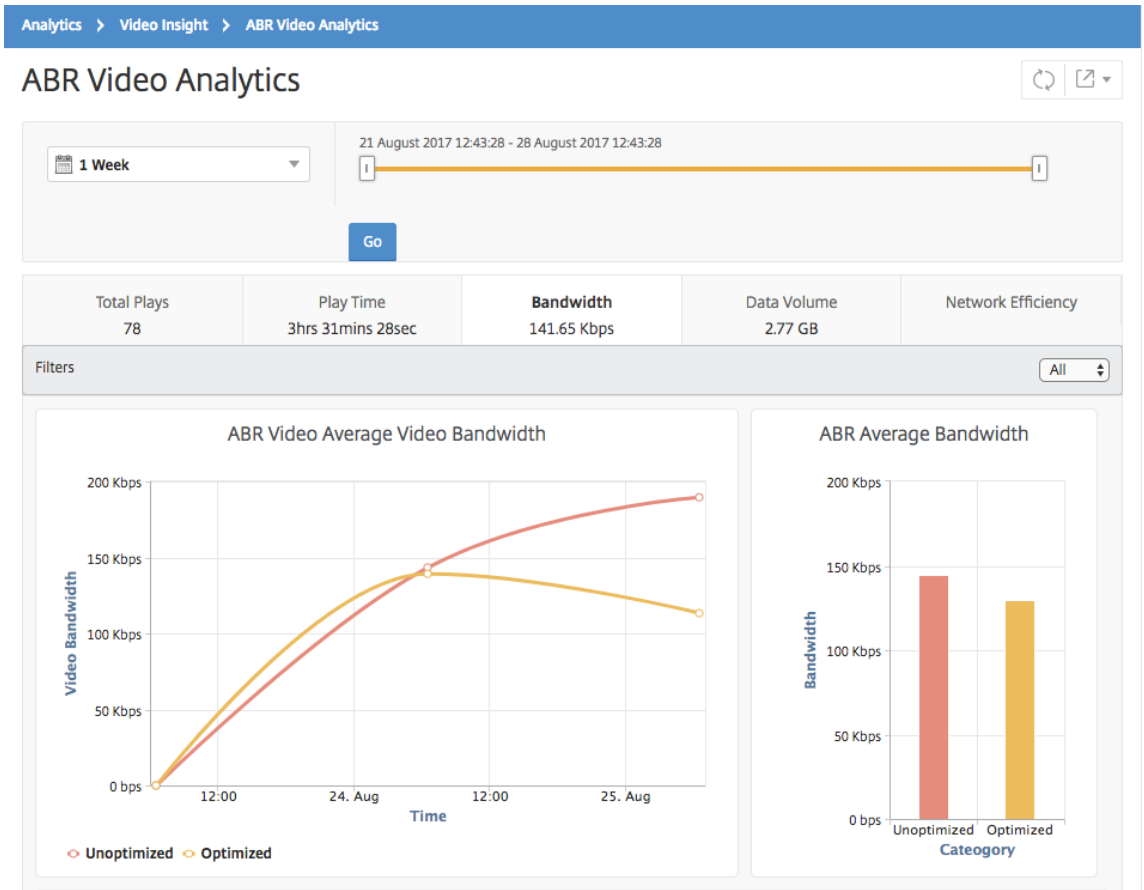
NetScaler Application Delivery Management（ADM）は、特定の時間枠において、ABR ビデオの最適化および非最適化によって消費される帯域幅を提供します。また、ネットワーク内で最適化された ABR ビデオと最適化されていない ABR ビデオによって消費される帯域幅を、以下に基づいて比較することもできます。

- 再生時間
- データ量

帯域幅の消費量を確認するには:

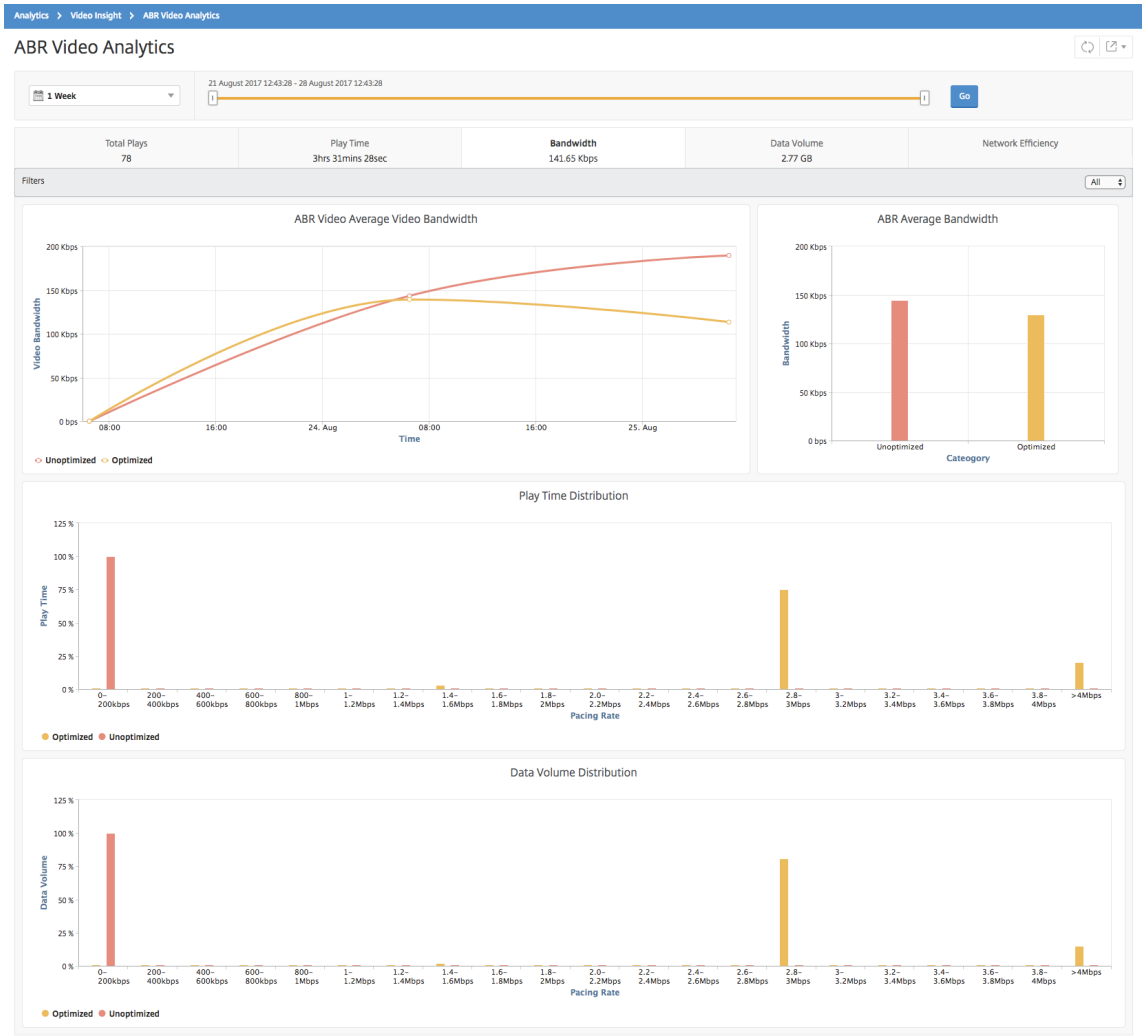
1. [分析] **>** [ビデオインサイト] に移動し、[**ABR** ビデオ分析] をクリックします。
2. 右側のペインで、リストから時間枠を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。
3. [移動] をクリックし、[帯域幅] タブを選択します。

   [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

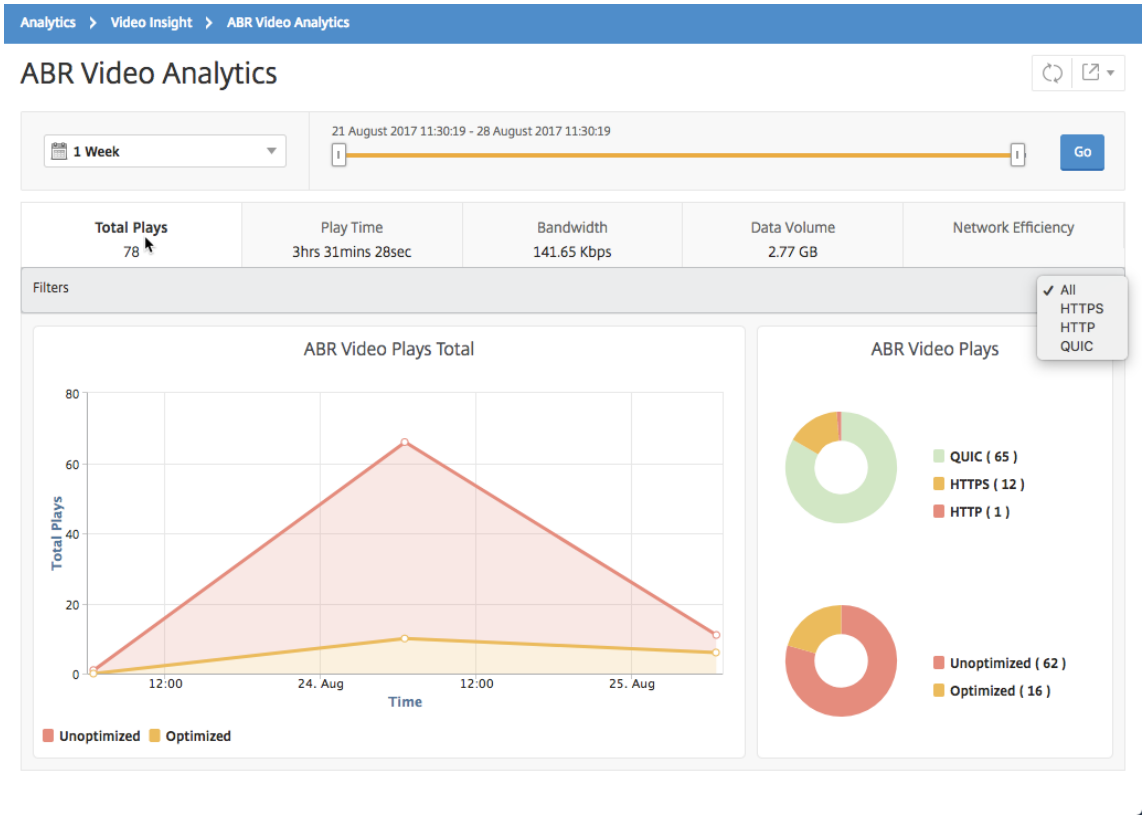
February 6, 2024

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。

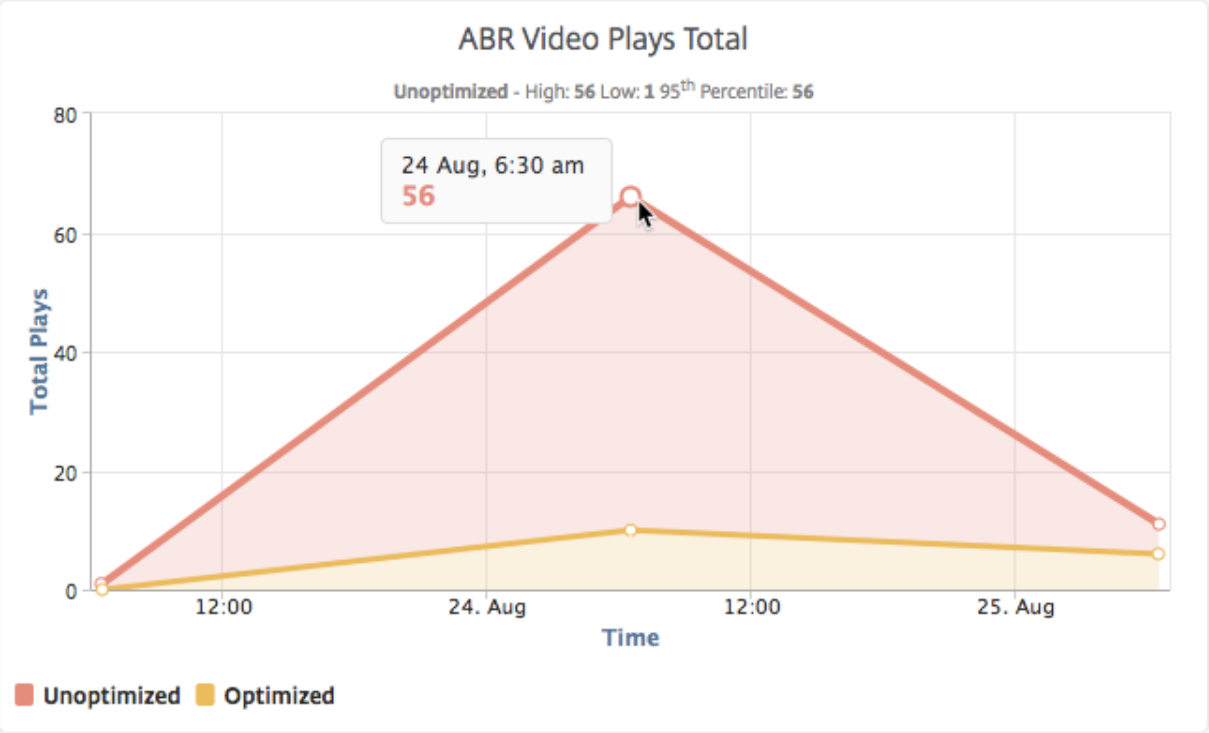
プレイ回数を確認するには:

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。

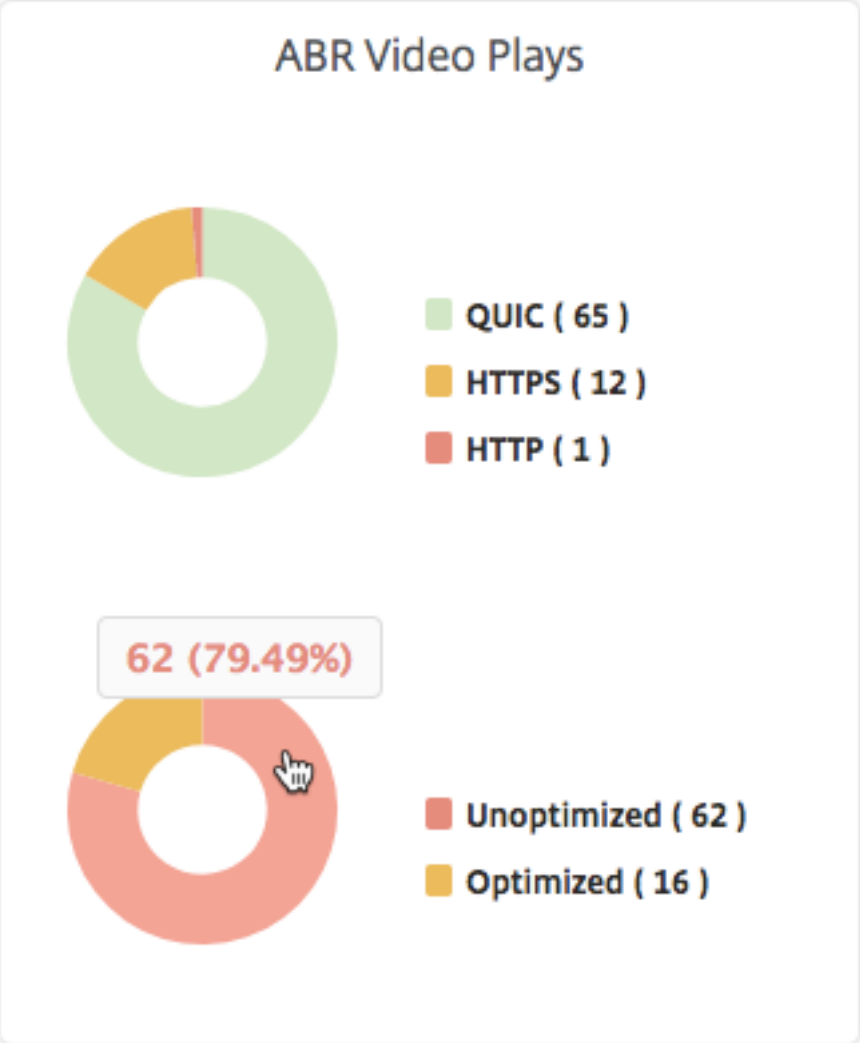
   [フィルタ] リストを使用して、HTTP、HTTPS、または QUIC ABR ビデオを選択できます。



[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 — 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、暗号化および暗号化解除された 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

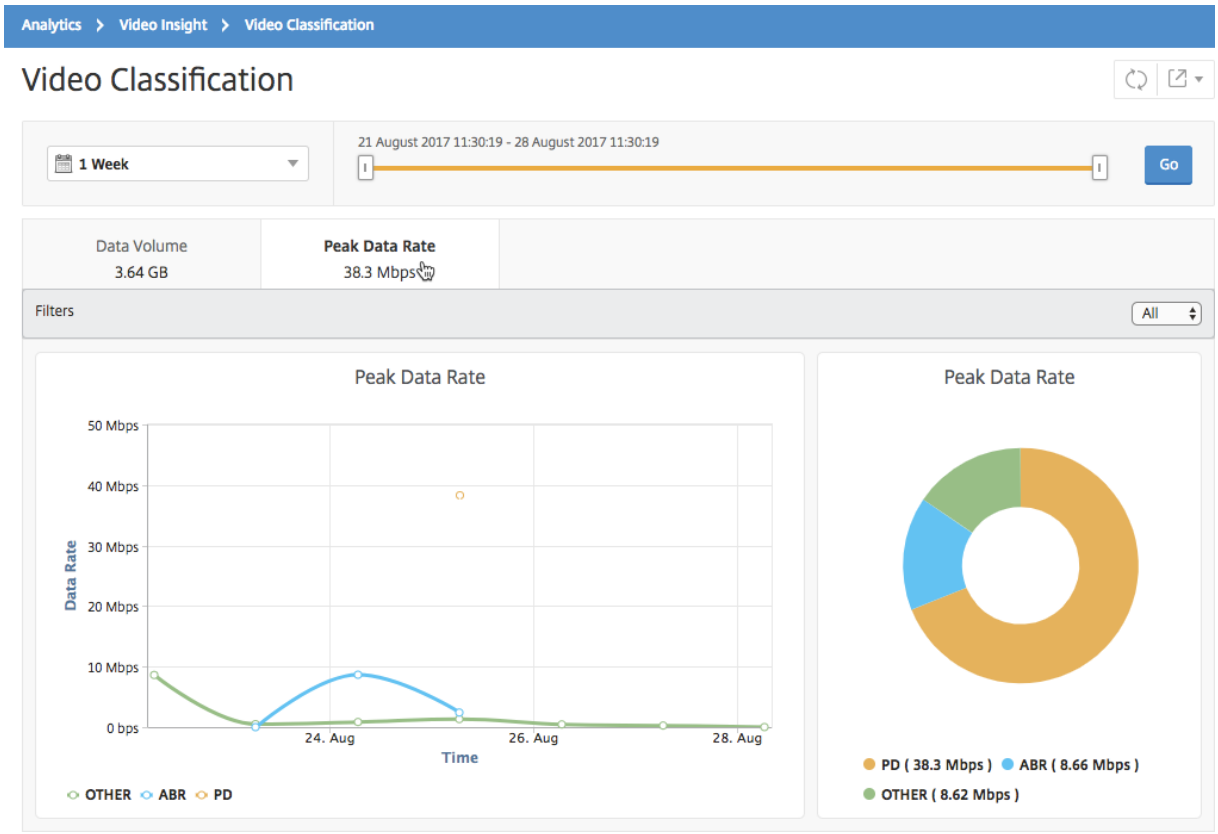
February 6, 2024

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プットまたはデータレートが表示されます。

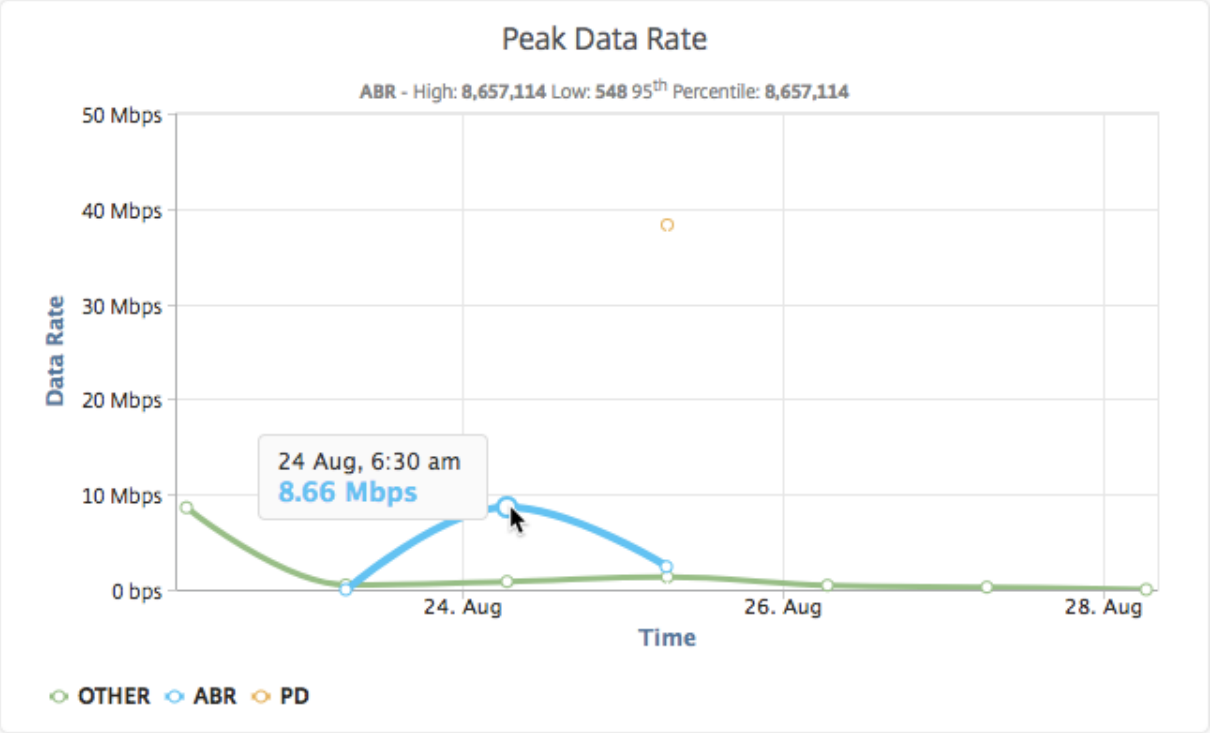
ビデオトラフィックのピークデータレートを確認するには:

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。

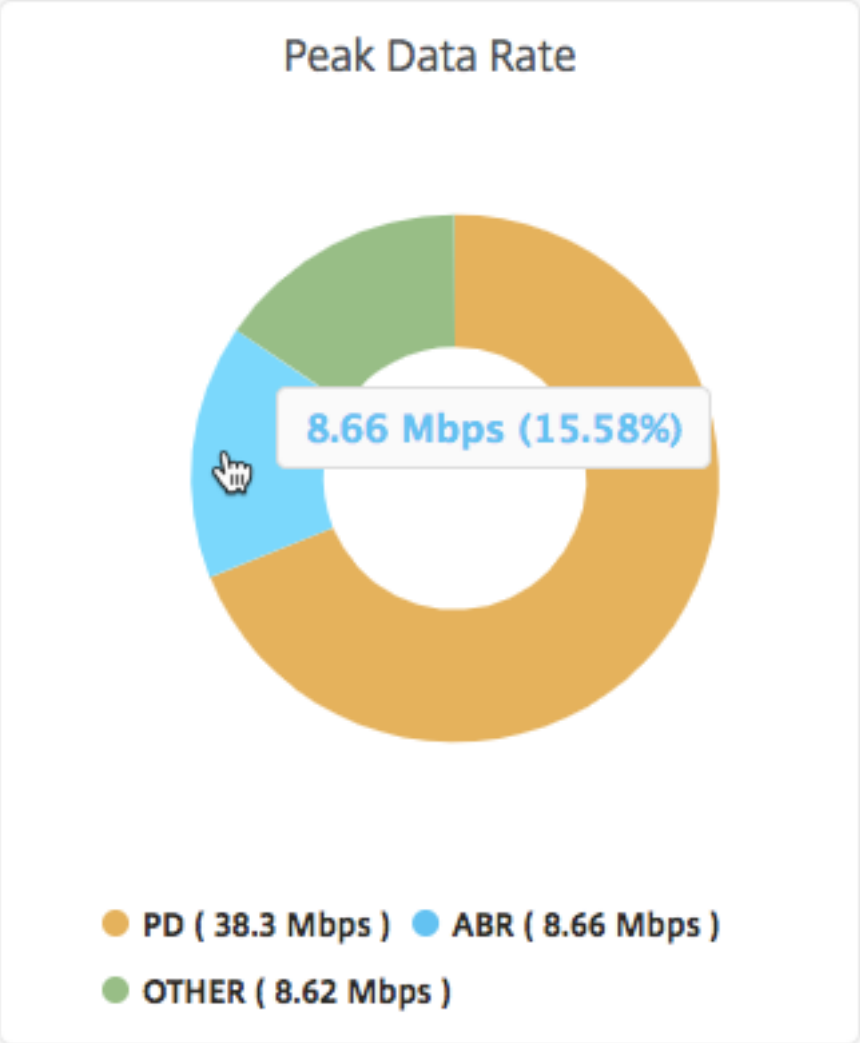
[フィルタ] リストを使用して、HTTP、HTTPS、または QUIC トラフィックを選択できます。



[**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 — 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。



IP アドレス管理 (IPAM) の構成

February 6, 2024

NetScaler ADM IPAM を使用すると、NetScaler ADM が管理する構成内の IP アドレスを自動的に割り当てたり解放したりできます。次の IP プロバイダーを使用して定義されたネットワークまたは IP 範囲から IP を割り当てることができます。

- NetScaler 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。

NetScaler ADM IPAM は次の場所で使用できます。

- **StyleBooks**: 構成を作成するときに仮想サーバーに IP を自動割り当てします。

- **API** ゲートウェイ: API プロキシに IP アドレスを自動割り当てます。

各ネットワークの IP アドレスまたは NetScaler ADM が管理する IP 範囲を追跡することもできます。

外部 **IP** アドレスプロバイダーの追加

NetScaler ADM には、IP アドレスと IP アドレス範囲を管理する IP アドレス管理プロバイダが組み込まれています。NetScaler ADM には外部 IP アドレスプロバイダーを使用することもできます。

> 重要**:**
>
> 開始する前に、外部 IP アドレスプロバイダーで次の権限が有効になっていることを確認してください。
>
> - プロバイダーに存在するネットワークを照会する機能。
> - ネットワーク内の IP アドレスを予約します。
> - ネットワークから IP アドレスを解放します。
> - ネットワークから使用された IP アドレスを取得します。
> - ネットワークから利用可能な IP アドレスを取得します。

次の手順を実行して、NetScaler ADM に外部 IPAM プロバイダーソリューションを追加します。

1. [設定**] > [IP** アドレス管理**]** 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 アドレス管理プロバイダを追加するには、次の詳細を指定します。
   - 名前 -NetScaler ADM で使用する IP プロバイダー名を指定します。
   -
   - **URL** -NetScaler 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。URL を次の形式で指定してください。

     ```
     https://<host name>
     <!--NeedCopy-->
     ```

     例: `https://myinfoblox.example.com`
   -
   - パスワード -IPAM ソリューションにログインするためのパスワードを指定します。
4. [追加] をクリックします。

外部プロバイダーとしての **Infoblox DDI**

現在、NetScaler ADM は外部プロバイダーとして Infoblox DDI をサポートしています。

NetScaler ADM IPAM を Infoblox プロバイダーと組み合わせて使用すると、次のアクションを実行できます。

- IPAM ネットワークを一覧表示する
- IP アドレス管理ネットワークの作成、更新、削除
- IP アドレス管理ネットワークからの IP アドレスの予約と解除

IPAM ネットワークを作成する　Infoblox プロバイダーを使用して NetScaler ADM IPAM ネットワークを作成するには、同じ CIDR IP 範囲のネットワークが Infoblox 上に存在する必要があります。

NetScaler ADM 内で IPAM ネットワークを作成する場合、登録するのは Infoblox ネットワークの使用を NetScaler ADM 内に登録することだけです。次に、ADM は Infoblox と連携して、ネットワークから割り当てられた IP アドレスを管理します。InfoBlox ネットワークは、NetScaler ADM の外部でも引き続き使用できます。

同様に、NetScaler ADM IPAM ネットワークを削除すると、NetScaler ADM は Infoblox ネットワークの登録を解除します。つまり、NetScaler ADM は Infoblox と通信してそのネットワーク内の IP アドレス管理を行う必要がなくなります。

Infoblox DDI API　NetScaler ADM IPAM は、以下の Infoblox API を使用してそれぞれのアクションを実行します。

- (/network)-利用可能なすべての Infoblox ネットワークを一覧表示します
- (/ネットワーク?network= {id})-特定の Infoblox ネットワークの詳細を取得します
- (/ipv4 アドレス)-Infoblox ネットワーク上のすべての IP を一覧表示します
- (/record: ホスト)-特定の IP アドレスの詳細を取得します
- (/{IP})-Infoblox ネットワーク上の IP を予約して解放します

Infoblox API の詳細については、Infoblox DDI で入手できる Infoblox REST API リファレンスガイドを参照してください。

ネットワークの追加

NetScaler ADM 管理構成で IPAM を使用するネットワークを追加します。

1. [設定] **> [IP** アドレス管理**]** 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 -NetScaler 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、NetScaler 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:
>
> NetScaler 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。

```
<first-IP-address>-<last-IP-address>
<!--NeedCopy-->
```

例:

```
10.0.0.20-10.0.0.100
<!--NeedCopy-->
```

CIDR では、次の形式でネットワーク値を指定します。

```
<IP-address>/<subnet-mask>
<!--NeedCopy-->
```

例:

```
10.70.124.0/24
<!--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. [設定] **> [IP** アドレス管理**]** に移動します。
2. 「ネットワーク」タブで、「割り当てられたすべての **IP** を表示」をクリックします。

   このペインには、IP アドレス、プロバイダー名、プロバイダーのベンダー、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 アドレスを予約した NetScaler ADM モジュールが表示されます。たとえば、StyleBooks が IP アドレスを予約した場合、この列には StyleBooks がモジュールとして表示されます。
   - 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。したがって、この列の下に [構成] が表示されます。
   - リソース **ID**: 正確なリソース ID をリンク付きで表示します。このリンクをクリックして、IP アドレスを使用しているリソースにアクセスします。設定リソースタイプでは、コンフィグパック ID がリソース ID として表示されます。

> 注**:**
>
> IP アドレスを解放する場合は、解放する IP アドレスを選択し、「割り当てられた **IP** を解放する」をクリックします。

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

NetScaler 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

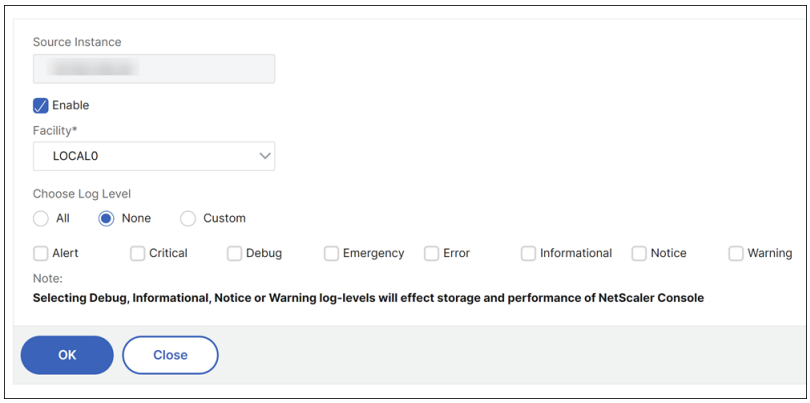
ADM からの ADC インスタンス関連の syslog メッセージを表示する前に、NetScaler ADM サービスを NetScaler インスタンスの syslog サーバーとして構成してください。設定が完了すると、すべての syslog メッセージがインスタンスから ADM にリダイレクトされます。

ADM サービスを **Syslog** サーバーとして設定する

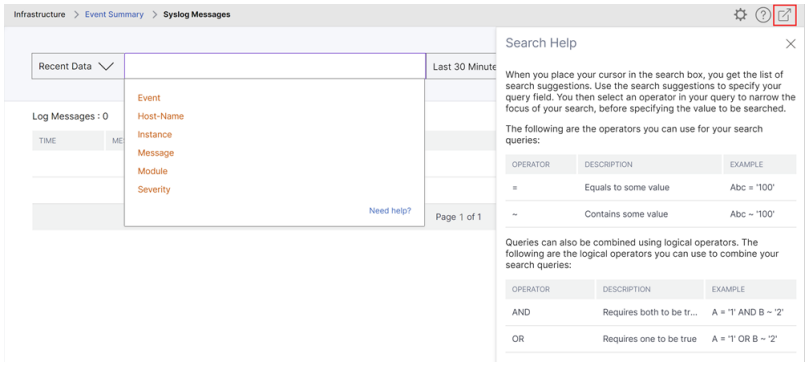
ADM を syslog サーバとして設定するには、次の手順を実行します。

1. ADM GUI から、[インフラストラクチャ**] > [**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 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 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、[インフラストラクチャ**] > [**イベント**] > [Syslog** メッセージ**]** の順に移動します。[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。



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、[設定**] > [ADM** 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、[インフラストラクチャ**] > [**ネットワーク機能**] > [**監査] の順に移動します。
- ADM 内の特定のアプリケーションの監査ログメッセージを表示するには、[アプリケーション**] > [**ダッシュボード] に移動し、仮想サーバーをクリックして [監査ログ] を選択します。

フレキシブルライセンスとプールライセンスの **NetScaler** ライセンス管理

February 6, 2024

> 注:
>
> NetScaler ライセンスの種類について詳しくは、「ライセンスの概要」を参照してください。

ポート設定、ライセンスファイル、有効期限情報、通知設定など、ライセンスに関連するすべての詳細がこのページに表示されます。ライセンスを適用したり、ライセンスの有効期限チェックを設定したり、ライセンスの使用状況や有効期限までの日数に関する通知を設定したりできます。

ライセンスサーバーのポート設定

ポートは、NetScaler インスタンスがライセンスサーバーと通信するために使用されます。「編集」アイコンをクリックし、次のパラメータの値を指定します。

- ライセンスサーバーポート**:NetScaler** インスタンスが Citrix ライセンスポータルにアクセスしてライセンスを割り当てるために使用するプロキシサーバーポート。デフォルト値：27000。
- ベンダーデーモンポート:NetScaler インスタンスがライセンスサーバーと通信するために使用するライセンスサーバーポート。デフォルト値は 7279 です。
- プロキシサーバーポート**:NetScaler ADM** を **NetScaler** インスタンスのフォワード HTTP プロキシとして使用すると、MyCitrix Portal にアクセスしてライセンスを自動的に取得できます。この機能を有効にするには、プロキシがリッスンする TCP ポートを指定します。

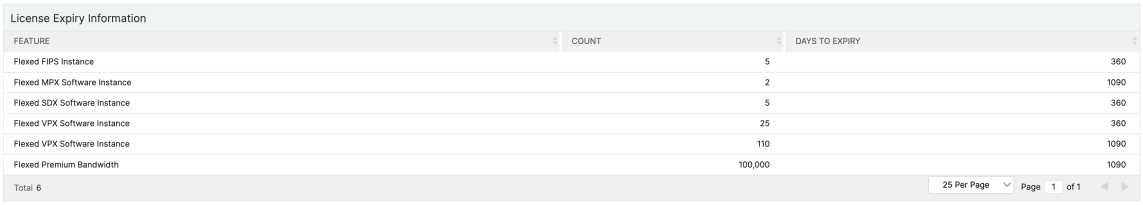
ライセンスファイル

このセクションには、NetScaler にあるライセンスファイルが一覧表示されます。ライセンスを追加、削除、ダウンロードできます。使用する前にライセンスを適用する必要があります。

ライセンスファイルを適用する

1. 「**NetScaler** ライセンス」**>**「ライセンス管理」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を追加」をクリックし、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ーからのライセンスファイルのアップロード: ライセンスファイルがローカルコンピューターに既に存在する場合は、NetScaler ADM にアップロードできます。
   - ライセンスアクセスコードを使用する: Citrix から購入したライセンスのライセンスアクセスコードを指定します。[ライセンスを取得] をクリックし、[完了] をクリックします。
3. [完了] をクリックします。
   ライセンスファイルが NetScaler ADM に追加されます。
   ライセンス有効期限情報セクションには、NetScaler ADM に存在するライセンス、数、および有効期限までの残り日数が表示されます。

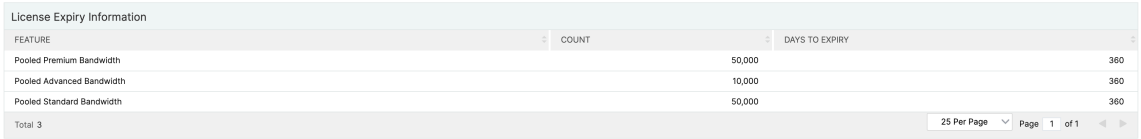
   次のスクリーンショットは、Flexed NetScaler VPX、NetScaler MPX、NetScaler SDX、NetScaler VPX FIPS ソフトウェアインスタンスのライセンス数、現在のフレックスプレミアム帯域幅容量、および有効期限までの日数を示しています。

   
   License Expiry Information

FEATURE	COUNT	DAYS TO EXPIRY
Flexed FIPS Instance	5	360
Flexed MPX Software Instance	2	1090
Flexed SDX Software Instance	5	360
Flexed VPX Software Instance	25	360
Flexed VPX Software Instance	110	1090
Flexed Premium Bandwidth	100,000	1090

   Total 6 — 25 Per Page — Page 1 of 1

   次のスクリーンショットは、利用可能なスタンダード、アドバンス、プレミアムのプール帯域幅と、有効期限までの日数を示しています。

   
   License Expiry Information

FEATURE	COUNT	DAYS TO EXPIRY
Pooled Premium Bandwidth	50,000	360
Pooled Advanced Bandwidth	10,000	360
Pooled Standard Bandwidth	50,000	360

   Total 3 — 25 Per Page — Page 1 of 1
4. ライセンスファイルを選択し、[ライセンスを適用] をクリックします。

ライセンスファイルを削除する

ライセンスファイルを削除するには、1 つまたは複数のファイルを選択して [削除] をクリックします。ライセンスを削除する場合、最初にライセンスを追加する必要があります。そうしないと適用できません。

ライセンスファイルのダウンロード

ライセンスファイルをダウンロードするには、ファイルを選択して [ダウンロード] をクリックします。ライセンスファイルはバックアップとしてオフラインで保存できます。

ライセンス有効期限情報

フレックスキャパシティライセンスまたはプールキャパシティライセンスの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と、NetScaler 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 の［インフラストラクチャ］**>**［イベント］から表示できます。

ライセンスの有効期限を表示

1. 「**NetScaler** ライセンス」**>**「ライセンス管理」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が切れるまでの日数。

> 注:
>
> プールに新しいライセンスを追加すると、NetScaler インスタンスは既存のライセンスの有効期限が切れると新しいライセンスを使用します。

通知設定

ライセンスの使用状況と有効期限に関する通知の送信基準となる設定を指定します。

1. 「通知設定」セクションで、「編集」アイコンをクリックし、「ライセンスの使用状況を通知する」を選択します。アラートしきい値を設定します。これは、通知の送信に使用されるフレックスライセンスまたはプールライセンスのキャパシティのパーセンテージです。
2. 適切なチェックボックスを選択して、ライセンスがしきい値に達したとき、または有効期限が切れるときに送信する通知の種類を選択します。通知タイプは次のとおりです。通知タイプを選択し、[追加] をクリックして詳細を追加します。設定を保存する前に、各通知が配信されるかどうかをテストすることもできます。

    - 電子メール: 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。詳細については、「メール配布リストの作成」を参照してください。
    - **SMS**: 通知を送信するための SMS プロファイルまたは配布リスト。
    - **Slack**: 通知を送信するための Slack プロファイルの詳細。
    - ページデューティ: 通知を送信するためのページャーデューティプロファイル。

- **ServiceNow：Citrix ServiceNow プロファイルはデフォルトで指定されており、現在利用できる唯一のオプションです。
  これらのプロファイルの作成について詳しくは、「通知の設定」を参照してください

3. Days to Expiiry（有効期限までの日数）を指定します。これは、ライセンスの有効期限が切れることを通知するまでの日数です。
4. ［保存］をクリックします。

メール配布リストを作成する

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. [電子メール] を選択し、[追加] をクリックします。
2.「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には、「追加」をクリックします。サーバー名/IP アドレスとポートを指定します。メールサーバーにアクセスするための認証を義務付けるには、[認証] を選択します。メールサーバーが SSL 認証をサポートしている場合は、「セキュア」を選択します。［作成］をクリックします。
   - 差出人-NetScaler 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-NetScaler 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**-NetScaler ADM がメッセージをコピーする電子メールアドレスを指定します。
   - **Bcc**-NetScaler ADM がメッセージをブラインドカーボンコピーする（電子メールアドレスは表示しない）電子メールアドレスを指定します。

3. ［作成］をクリックします。

SMS 配布リストを作成する

SMS 通知設定を構成するには、次の手順を実行します。

1. **SMS** で、[追加] をクリックします。
2.「**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。SMS サーバーを追加するには、「追加」をクリックします。サーバーの詳細を指定し、「作成」をクリックします。
   - 宛先-NetScaler ADM がメッセージを送信する電話番号を指定します。

3. ［作成］をクリックします。

Slack プロファイルの作成

Slack プロファイルを作成するには、次の手順に従います。

1. **Slack** で [追加] をクリックします。
2.「**Slack** プロファイルの作成」で、次の詳細を指定します。

    - プロファイル名 -プロファイル名を指定します。この名前は Slack のプロフィールリストに表示されます。
    - チャンネル名-NetScaler ADM が通知を送信する SSlack 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。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.

PagerDuty プロファイルを作成する

PagerDuty では、登録された番号への電子メール、SMS、プッシュ通知、および電話による通知を設定できます。NetScaler アプリケーションの配信と管理に PagerDuty プロファイルを追加する前に、PagerDuty で必要な構成を完了していることを確認してください。PagerDuty を使い始めるには、PagerDuty のドキュメントを参照してください。

PagerDuty プロファイルを作成するには、次の手順を実行します。

1. [**PagerDuty**] で、[追加] をクリックします。
2.「**PagerDuty** プロファイルの作成」で、次の詳細を指定します。

    - プロファイル名-プロファイル名を指定します。この名前は、イベントルールや SSL 通知など、さまざまなモジュールで PagerDuty アラートを送信するために使用されます。
    - 統合キー -統合キーを指定します。このキーは PagerDuty ポータルから入手できます。

3. [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。

ServiceNow のプロフィールを表示する

NetScaler イベントと NetScaler ADM イベントの ServiceNow 通知を有効にするには、ITSM コネクタを使用して NetScaler アプリケーションの配信と管理を 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. **ServiceNow** では、**Citrix_Workspace_SN** プロファイルがデフォルトで選択されています。
2. 「テスト」をクリックして ServiceNow チケットを自動生成し、構成を確認します。

フレックスキャパシティライセンス

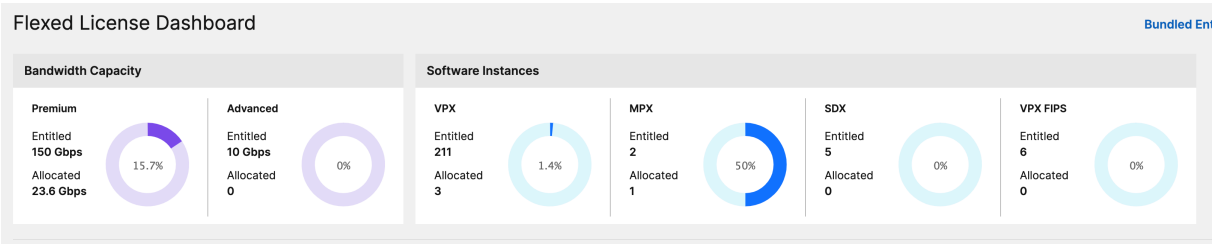
February 6, 2024

NetScaler Flexed ライセンスは、ライセンス管理プロセスを簡素化することを目的とした新しいライセンスフレームワークです。フレックスライセンスには、ソフトウェアインスタンスライセンス（VPX/CPX/BLX、SDX、MPX、VPX FIPS）と帯域幅容量ライセンスが含まれます。フレックスライセンスは、NetScaler コンソールサービスまたはオンプレミスの NetScaler ADM に適用する必要があります。また、MPX Z-Cap ライセンスと SDX Z-Cap ライセンスをそれぞれ NetScaler MPX および NetScaler SDX ハードウェアに適用する必要があります。その後、クラウドまたはオンプレミスに展開されているすべての NetScaler フォームファクターにそれらを割り当てることができます。

Flexed ライセンスでは、無制限の仮想サーバーの分析も提供されます。

Pooled ライセンスをお持ちで、Flexed ライセンスを購入した場合は、Flexed ライセンスダッシュボードでライセンスの詳細を確認できます。帯域幅とインスタンスの組み合わせが Flexed ライセンスダッシュボードに表示されます。

帯域幅ライセンスには通常、プレミアムエディションのみが含まれます。ただし、以前にプールスタンダードまたはアドバンスドライセンスを持っていた場合は、スタンダード、アドバンス、プレミアムエディションがフレックスライセンスダッシュボードに表示されます。



詳細については、「Flexed ライセンスダッシュボード」を参照してください。

Flexed ライセンスを使用すると、インスタンスに必要な帯域幅を必要以上に割り当てないようにすることで、帯域幅の使用率を最大化できます。トラフィックに影響を与えずに、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。

Flexed ライセンスでのテレメトリ収集

現在のフレックスライセンス要件に準拠するには、ADM オンプレミ Cloud Connector を有効にしてください。この機能は、オンプレミスの ADM を ADM サービス（現在は NetScaler Console サービスにリブランディング）に接

続してテレメトリ収集を行います。Flexed ライセンスを使用している場合は、テレメトリ収集を有効にすることをお勧めします。ADM オンプレミ Cloud Connector を有効にするには、「Cloud Connector」を参照してください。

ADM オンプレミスの Cloud Connector により、Citrix Cloud はライセンスコンプライアンスのためにライセンス、構成、および使用状況データを収集し、サービスを管理、測定、および改善できるようになります。当社が収集するデータの詳細をご覧ください。

> 注:
>
> この自動データ収集モードに加えて、テレメトリデータを有効にして共有する手動モードも今後のリリースで利用可能になる予定です。テレメトリデータは、自動モードまたは手動モードで共有できます。これらのモードが両方利用可能になったら、テレメトリデータを共有することが必須であり、共有しないと、90 日後にサポートとメンテナンスが停止されます。

ゼロキャパシティハードウェア

NetScaler Flexed ライセンスで管理する場合、MPX および SDX インスタンスは、帯域幅プールからリソースをチェックアウトするまで機能しないため、「ゼロキャパシティハードウェア」と呼ばれます。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。

ゼロキャパシティのハードウェアでは、共通プールから帯域幅をチェックアウトするための Z-Cap ライセンスが必要です。

> 注:
>
> - ゼロキャパシティライセンスのインストールは、他の NetScaler ローカルライセンスと同じように機能します。ゼロキャパシティライセンスを取得してインストールする方法について詳しくは、NetScaler のライセンスガイドを参照してください。

Z-Cap ライセンスの管理とインストール

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、Z-Cap ライセンスを手動でインストールする必要があります。Z-Cap ライセンスをインストールすると、ハードウェアにロックされ、必要に応じて NetScaler ハードウェアインスタンス間で共有することはできません。ただし、Z-Cap ライセンスを別の NetScaler ハードウェアインスタンスに手動で移動することはできます。

NetScaler ソフトウェアリリース 11.1 ビルド 54.14 以降を実行する NetScaler MPX インスタンスと、11.1 ビルド 58.13 以降を実行する NetScaler SDX インスタンスは、NetScaler Flexed ライセンスをサポートしています。詳細については、表 **1** を参照してください。**MPX** および **SDX** インスタンスの Flexed ライセンスをサポートしました。

スタンドアロン **NetScaler VPX** インスタンス

以下のハイパーバイザーで NetScaler ソフトウェアリリース 11.1 ビルド 54.14 以降を実行する NetScaler VPX インスタンスは、フレキシブルライセンスをサポートします。

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

以下のハイパーバイザーおよびクラウドプラットフォーム上で NetScaler ソフトウェアリリース 12.0 Build 51.24 以降を実行する NetScaler VPX インスタンスは、Flexed ライセンスをサポートします。

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

以下のハイパーバイザーおよびクラウドプラットフォーム上で NetScaler ソフトウェアリリース 13.0 および 13.1（すべてのバージョン）を実行する NetScaler VPX インスタンスは、Flexed ライセンスをサポートします。

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- 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。 詳しくは、「クラウドにデプロイされた NetScaler VPX インスタンスを NetScaler ADM に追加する」を参照してください。容量ゼロのハードウェアとは異なり、NetScaler VPX には容量ゼロの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 CPX** インスタンス

Docker ホストにデプロイされた NetScaler CPX インスタンスは、フレキシブルライセンスをサポートします。容量ゼロのハードウェアとは異なり、NetScaler CPX には Z-Cap 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 1 つの NetScaler CPX インスタンスは、1 つのインスタンスのみをチェックアウトし、ライセンスプールから帯域幅はチェックアウトしません。たとえば、20 Gbps の帯域幅プールを備えた NetScaler CPX インスタンスが 20 個あるとします。NetScaler CPX インスタンスの 1 つが 500 Mbps のスループットを消費する場合、残りの 19 個の NetScaler CPX インスタンスの帯域幅プールは 20Gbps のままになります。

同じ NetScaler CPX インスタンスが 1500 Mbps のスループットを消費し始めた場合、残りの 19 個の NetScaler CPX インスタンスの帯域幅プールは 19.5 Gbps になります。

フレックスライセンスの場合、帯域幅を追加できるのは 10 Mbps の倍数だけです。

スタンドアロンの **NetScaler BLX** インスタンス

NetScaler BLX インスタンスはフレキシブルライセンスをサポートしています。NetScaler BLX インスタンスには Z-Cap ライセンスは必要ありません。トラフィックを処理するには、NetScaler BLX インスタンス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 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、Premium ソフトウェアエディションのプールで構成されます。プールライセンスからフレックスライセンスに移行すると、スタンダード、アドバンス、プレミアムのソフトウェアエディションが混在することがあります。特定の NetScaler MPX/VPX/CPX/BLX 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

ソフトウェアインスタンスプールには次の 3 つのタイプがあります。

- VPX/CPX/BLX ソフトウェアインスタンス
- MPX ソフトウェアインスタンス (MPX FIPS にも同じプールが適用されます)
- SDX ソフトウェアインスタンス (SDX FIPS にも同じプールが適用されます)
- VPX FIPS ソフトウェアインスタンス

ライセンスをプールからチェックアウトすると、CPU/PE、SSL コア、1 秒あたりのパケット数、帯域幅などのソフトウェアインスタンスのリソースのロックが解除されます。

NetScaler ADM ライセンスサーバー

NetScaler Flexed ライセンスでは、ライセンスサーバーとして構成された NetScaler ADM を使用して、Flexed ライセンス（帯域幅プールライセンスとインスタンスプールライセンス）を管理します。

帯域幅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 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 インスタンスが機能する前にチェックアウトする必要のある最小帯域幅とインスタンス数。
- NetScaler がチェックアウトできる最大帯域幅とインスタンス数。
- 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 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 最小帯域幅単位が 1 Gbps の場合、1000 Mbps はチェックアウトできますが、200 Mbps または 150.5 Gbps 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 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にのみ動作します。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 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 インスタンスのさまざまなフォームファクターのライセンス要件をまとめたものです。次の表はシステム要件を示しています。

> 注:
>
> NetScaler CPX/BLX/VPX の最小帯域幅チェックアウト単位は 10Mbps です。NetScaler MPX/SDX の最小帯域幅チェックアウト単位は 1Gbps です。

テーブル **1A. MPX** でサポートされるフレックスキャパシティ

製品ライン	最小帯域幅 (Gbps)	最大帯域幅（Gbps）	最小帯域幅単位
MPX 5900Z	1	10	1Gbps
MPX 8900Z	5	30	1Gbps
MPX 8900Z FIPS	5	20	1Gbps
MPX 9100Z	10	95	1Gbps
MPX 9100Z FIPS	10	95	1Gbps
MPX 14000Z	20	100	1Gbps
MPX 14000Z-40G	20	100	1Gbps
MPX 14000Z-40S	40	100	1Gbps
MPX 14000Z FIPS	30	80	1Gbps
MPX 15000Z	20	120	1Gbps
MPX 15000Z-50G	20	120	1Gbps
MPX 15000Z FIPS	30	120	1Gbps

製品ライン	最小帯域幅 (Gbps)	最大帯域幅（Gbps）	最小帯域幅単位
MPX 16000Z	30	250	1Gbps
MX 22000Z	40	120	1Gbps
MPX 24000Z	100	150	1Gbps
MPX 25000Z	100	160	1Gbps
MPX 25000Z-40G	100	200	1Gbps
MX 26000Z	100	200	1Gbps
MPX 26000Z-50S	100	200	1Gbps
MPX 26000Z-100G	100	200	1Gbps

テーブル **1A.** ビルド **13.0-47.x** より前の **NetScaler SDX** バージョンでサポートされていたフレックスキャパシティ

製品ライン	最小帯域幅 (Gbps)	最大帯域幅 (Gbps)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
SDX 8900Z	10	30	2	7	1Gbps
14000Z	20	100	5	25	1Gbps
SX 14000Z-40G	40	100	20	25	1Gbps
SDX 15000Z	20	120	5	55	1Gbps
SDX 15000Z-50G	20	120	5	55	1Gbps
SDX 22000Z	40	120	80	80	1Gbps
SDX 24000Z	100	150	80	80	1Gbps
SDX 25000Z	100	200	20	115	1Gbps
SX 25000Z-40G	100	200	20	115	1Gbps
SDX 26000Z	100	200	20	115	1Gbps
SX 26000Z-50S	100	200	20	115	1Gbps

製品ライン	最小帯域幅 (Gbps)	最大帯域幅 (Gbps)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
SDX 26000Z-100G	100	200	20	115	1Gbps

テーブル **1B. NetScaler SDX** バージョン **13**（ビルド **13.0-47.x** 以降）、バージョン **13.1**（**51.x** より前のビルド）、およびバージョン **14.1**（以前の **12.x** のビルド）でサポートされるフレックスキャパシティ

製品ライン	最小帯域幅 (Gbps)	最大帯域幅 (Gbps)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
SDX 8900Z	5	30	1	7	1Gbps
SDX 9100Z	10	95	2	7	1Gbps
14000Z	10	100	2	25	1Gbps
SX 14000Z-40G	20	100	10	25	1Gbps
SDX 15000Z	10	120	2	55	1Gbps
SDX 15000Z-50G	10	120	2	55	1Gbps
SDX 16000Z	15	250	10	55	1Gbps
SDX 22000Z	20	120	40	80	1Gbps
SDX 24000Z	50	150	40	80	1Gbps
SDX 25000Z	50	200	10	115	1Gbps
SX 25000Z-40G	50	200	10	115	1Gbps
SDX 26000Z	50	200	10	115	1Gbps
SX 26000Z-50S	50	200	10	115	1Gbps
SDX 26000Z-100G	50	200	10	115	1Gbps

テーブル **1C. NetScaler SDX** バージョン **13.1**（ビルド **51.x** 以降）およびバージョン **14.1**（ビルド **12.x** 以降）でサポートされるフレックスキャパシティ

製品ライン	最小帯域幅 (Gbps)	最大帯域幅 (Gbps)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
SDX 8900Z	5	30	1	7	1Gbps
SDX 9100Z	10	95	1	7	1Gbps
14000Z	10	100	1	25	1Gbps
SX 14000Z-40G	20	100	1	25	1Gbps
SDX 15000Z	10	120	1	55	1Gbps
SDX 15000Z-50G	10	120	1	55	1Gbps
SDX 16000Z	15	250	1	55	1Gbps
SDX 22000Z	20	120	1	80	1Gbps
SDX 24000Z	50	150	1	80	1Gbps
SDX 25000Z	50	200	1	115	1Gbps
SX 25000Z-40G	50	200	1	115	1Gbps
SDX 26000Z	50	200	1	115	1Gbps
SX 26000Z-50S	50	200	1	115	1Gbps
SDX 26000Z-100G	50	200	1	115	1Gbps

> 注:
>
> - 最小購入数量は、最小システム要件とは異なる場合があります。
> - ビルド 14.1-12.x 以降を実行する NetScaler SDX で、Flexed ライセンスを使用すると、最小インスタンスライセンスをチェックアウトする制限がなくなりました。つまり、少なくとも 1 つのインスタンスライセンスをチェックアウトできます。

表 **2. NetScaler CPX** インスタンスでサポートされる最小/最大帯域幅と最小/最大インスタンス

製品ライン	最大帯域幅 (Gbps)	最小帯域幅 (Mbps)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
CPX	10	10	1	1	10Mbps

表 **3.** ハイパーバイザーとクラウドサービス上の **NetScaler VPX** インスタンスでサポートされる最小/最大帯域幅と最小/最大インスタンス

ハイパーバイザ/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
Citrix Hypervisor	40 Gbps	10Mbps	1	1	10Mbps
VMware ESXi	100 Gbps	10Mbps	1	1	10Mbps
Linux KVM	100 Gbps	10Mbps	1	1	10Mbps
Microsoft Hyper-V	3Gbps	10Mbps	1	1	10Mbps
AWS	30 Gbps	10Mbps	1	1	10Mbps
Azure	10 Gbps	10Mbps	1	1	10Mbps
Google Cloud	10 Gbps	10Mbps	1	1	10Mbps

> 注
>
> 最小購買数量は、最小システム要件とは異なります。

表 **4. NetScaler BLX** インスタンスでサポートされる最小/最大帯域幅と最小/最大インスタンス

製品ライン	最大帯域幅 (Gbps)	最小帯域幅 (Mbps)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
BLX	100	10	1	1	10Mbps

表 **5.** さまざまなフォームファクターに対応するゼロキャパシティライセンス要件

製品ライン	ゼロキャパシティハードウェア
MPX	ライセンスが必要です
SDX	ライセンスが必要です
VPX	-
CPX	-
BLX	-

フレックスライセンスの設定

February 6, 2024

> 注**:**
>
> プールライセンスを所有していて、Flexed ライセンスを購入して適用した場合、Flexed ライセンスダッシュボードに結合されたライセンスが表示されます。

NetScaler Flexed ライセンスでは、さまざまな NetScaler フォームファクター間で帯域幅またはインスタンスライセンスを共有できます。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は、この Flexed 容量を使用してください。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 NetScaler インスタンスで再利用します。

Flexed ライセンスを使用すると、インスタンスに必要な帯域幅を必要以上に割り当てないようにすることで、帯域幅の使用率を最大化できます。トラフィックに影響を与えずに、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。

NetScaler ADM では次のタスクを実行できます。

1. Flexed ライセンスファイル (帯域幅プールまたはソフトウェアインスタンスプール) をライセンスサーバーにアップロードします。

   > 注:
   >
   > ライセンスサーバーは NetScaler ADM オンプレミスサーバーです。

2. SDX または MPX ゼロキャパシティライセンスを SDX または MPX ハードウェアにアップロードし、必要に応じてライセンスプールから NetScaler インスタンスにライセンスを割り当てます。

   - インスタンスの最小容量と最大容量に基づいて、NetScaler インスタンスのライセンスを確認してください。

帯域幅、インスタンス、Z-cap ライセンスを含む Flexed ライセンスは、citrix.com からダウンロードできます。詳しくは、「NetScaler ライセンスガイド」を参照してください。

NetScaler フレックスライセンスの状態

Flexed ライセンスの状態は、NetScaler インスタンスのライセンス要件を示しています。Flexed ライセンスで構成された NetScaler インスタンスには、次のいずれかの状態が表示されます。

- 割り当て済み: インスタンスは適切なライセンス容量で実行されています。
- **Grace**: インスタンスは猶予ライセンスで実行されています。
- 接続が失われました:NetScaler ADM からインスタンスへの通信が機能していません。

はじめに

Flexed ライセンスを設定する前に、次の前提条件が満たされていることを確認してください。

- NetScaler から27000NetScaler 7279ADM におよびポートにアクセスして、ライセンスをチェックアウトできます。「システム要件」を参照してください。

ステップ 1-NetScaler ADM でライセンスを適用する

1. 「**NetScaler** ライセンス」**>**「ライセンス管理」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。ライセンスファイルがローカルコンピューターにすでに存在する場合は、NetScaler 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 **NetScaler 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 NetScaler ADM に追加されます。ライセンス有効期限情報セクションには、NetScaler ADM に存在するライセンスと有効期限までの残り日数が表示されます。

4. [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、NetScaler インスタンスは選択したライセンスを Flexed ライセンスとして使用できます。

ステップ **2-NetScaler ADM** をライセンスサーバーとして登録し、ライセンスを割り当てる

NetScaler ADM をライセンスサーバーとして NetScaler インスタンスに登録できます。

GUI を使用して **NetScaler ADM** サーバーを登録する

NetScaler ADM GUI で、NetScaler インスタンスに関連付けられている NetScaler ADM サーバーを登録します。

1. NetScaler GUI にログインします。
2. [システム**] > [**ライセンス**] > [**ライセンスの管理] に移動します。
3. [新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」フィールドに、NetScaler ADM に登録されている関連する NetScaler 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. NetScaler ADM サーバーの資格情報を入力してインスタンスを NetScaler ADM に登録し、[続行] をクリックします。NetScaler ADM では、サーバーの 1 つがライセンスサーバーです。
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 でライセンスを割り当てます。ライセンス割り当ては、後で NetScaler ADM GUI から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 **NetScaler ADM** サーバーを追加します

NetScaler インスタンスに GUI がない場合は、次の CLI コマンドを使用して、インスタンスに関連付けられた NetScaler ADM サーバーを追加します。

1. NetScaler ADC コンソールにログインします。
2. NetScaler ADM に登録されている関連する NetScaler ADM サーバーの IP アドレスを追加します。デフォルトのライセンスポートは 27000 です。


```
> add ns licenseserver <adm-server-IP-address> -port <adm-server-
    license-port-number>
<!--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。

```
> sh ns licenseserverpool
<!--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。

```
> set ns capacity -unit gbps -bandwidth <specify-license-bandwidth
    > edition <specify-license-edition>
<!--NeedCopy-->
```

> 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-NetScaler** インスタンスのフレキシブル帯域幅を編集する

1. 「**NetScaler** ライセンス」**>**「フレックスライセンス」「ダッシュボード」に移動します。
2. 「ライセンスされた **NetScalers** 」セクションでインスタンスを選択し、「帯域幅の編集」をクリックします。
3. [帯域幅の編集] ページで、[割り当て] 列に数値を入力します。
4. [**Submit**] をクリックします。

NetScaler MPX-Z

MPX-Z は、フレックスキャパシティ対応の NetScaler MPX アプライアンスです。MPX-Z は、Premium エディションライセンスのみの帯域幅プールをサポートします。

MPX-Z は、ライセンスサーバーに接続する前にライセンスが必要です。MPX-Z ライセンスは、次のいずれかの方法でインストールできます。

- ローカルコンピュータからライセンスファイルをアップロードする。
- インスタンスのハードウェアシリアル番号を使用する。
- インスタンスの GUI の [システム] > [ライセンス] セクションにあるライセンスアクセスコード。

MPX-Z ライセンスを削除すると、MPX はライセンスなしになります。ライセンスはライセンスサーバーにリリースされます。

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、設定された容量に必要な Flexed ライセンスが自動的にチェックアウトされます。

NetScaler SDX-Z

SDX-Z は、フレックスキャパシティ対応の NetScaler SDX アプライアンスです。SDX-Z は、Premium エディションライセンスの帯域幅とインスタンスプールをサポートします。

SDX-Z は、ライセンスサーバーに接続する前にライセンスが必要です。SDX-Z ライセンスは、次のいずれかの方法でインストールできます。

- ローカルコンピュータ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。

SDX-Z ライセンスを削除すると、SDX はライセンスなしになります。ライセンスはライセンスサーバーにリリースされます。

SDX-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。

> 注:
>
> インスタンスを再起動すると、設定された容量に必要な Flexed ライセンスが自動的にチェックアウトされます。

NetScaler の高可用性ペア

開始する前に、NetScaler ADM サーバーがライセンスサーバーとして構成されていることを確認します。詳しくは、「ライセンスサーバーとしての NetScaler ADM の構成」を参照してください。

NetScaler HA ペアに帯域幅を割り当てると、NetScaler ADM は割り当てられた帯域幅をプライマリインスタンスにチェックアウトします。セカンダリインスタンスに対してこのプロセスを繰り返す必要があります。

プールライセンスを NetScaler HA ペアに割り当てるには、「NetScaler インスタンスへのフレックスライセンスの割り当て」を参照してください。

Flexed Capacity ページには、インスタンスとそれらに割り当てられた容量が個別に表示されます。

フレックスライセンスダッシュボード

February 6, 2024

Flexed ライセンスダッシュボードでは、購入した帯域幅容量とインスタンスを包括的に確認できます。

このページには、エディション間の帯域幅容量と、MPX、VPX、SDX などのさまざまなフォームファクターのインスタンスの詳細が表示されます。NetScaler MPX と NetScaler MPX FIPS には同じライセンスファイルがあります。同様に、NetScaler SDX と NetScaler SDX FIPS には同じライセンスファイルがあります。ただし、NetScaler VPX FIPS には NetScaler VPX とは異なるファイルがあり、個別に表示されます。また、NetScaler BLX と NetScaler CPX には NetScaler VPX ライセンスが必要であり、VPX のエンタイトルメントと割り当ての一部です。Flexed ライセンスはプレミアムエディションのみをサポートします。ただし、Flexed ライセンスを購入していて、以前にプールスタンダードまたはアドバンスト帯域幅キャパシティを使用していた場合は、帯域幅容量（スタンダードまたはアドバンス）に関する詳細も Flexed ライセンスダッシュボードに表示されます。

ライセンスされた NetScaler インスタンスの詳細は、「ライセンスされた **NetScalers** 」セクションで確認できます。インスタンスを選択して帯域幅を編集するか、そのインスタンスのライセンスを解放できます。

次のパラメータに基づいて結果をフィルタリングできます。

- 帯域幅で絞り込む
  - Premium
  - 詳細設定
  - Standard
- フォームファクター
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
- ライセンスステータス
  - 接続が失われました
  - グレイス
  - 割り当て済み

NetScaler インスタンスに割り当てられた帯域幅を編集する

1. 「**NetScaler** ライセンス」**>**「フレックスライセンス」「ダッシュボード」に移動します。
2. 「ライセンスされた **NetScalers** 」セクションでインスタンスを選択し、「帯域幅の編集」をクリックします。
3. [帯域幅の編集] ページで、[割り当て] 列に数値を入力します。
4. [**Submit**] をクリックします。

NetScaler インスタンスのライセンスをリリースする

ライセンスを別のインスタンスに移すには、現在のインスタンスのライセンスを解放してから、新しいインスタンスにライセンスを適用する必要があります。リリースライセンスを選択すると、次のことが行われます。

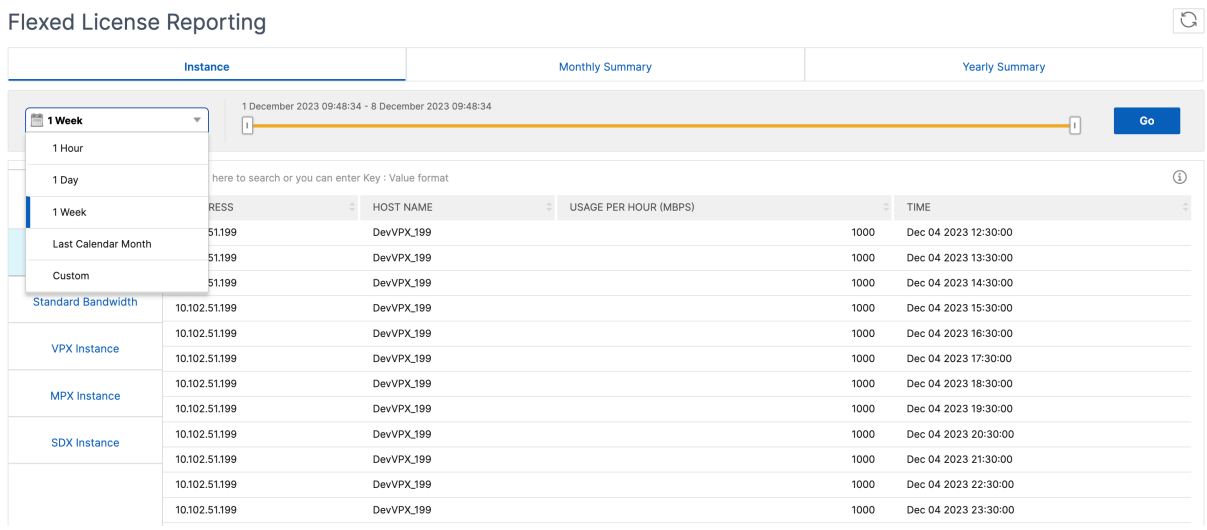
- そのインスタンスでチェックアウトされているすべてのライセンスをライセンスサーバーにリリースします。
- そのインスタンスのライセンスサーバー設定を削除します。

［はい］を選択すると、NetScaler インスタンスはライセンスなしになり、トラフィックを処理できなくなります。

フレックスライセンスレポート

February 6, 2024

ソフトウェアインスタンスと帯域幅ライセンスの割り当てとエンタイトルメントの詳細を表示して、エンタイトルメントからどれだけ割り当てられているかを確認できます。どのインスタンスが帯域幅を消費しているか（1 時間あたりの使用量）、消費時間など、インスタンスの詳細を表示できます。1 時間からカスタム期間までの期間を指定できます。



「月次サマリー」タブと「年間サマリー」タブにはグラフィカルビューがあります。次のグラフは、ソフトウェアインスタンスのエンタイトルメントと割り当ての例です。

NetScaler プール容量

February 6, 2024

NetScaler プール容量により、さまざまな NetScaler フォームファクター間で帯域幅またはインスタンスライセンスを共有できます。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。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は、このプール容量を使用してください。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 NetScaler インスタンスに再利用します。

プールライセンスを使用すると、インスタンスに必要な帯域幅を必要以上に割り当てないようにすることで、帯域幅の使用率を最大化できます。トラフィックに影響を与えずに、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。プールキャパシティライセンスを使用すると、インスタンスのプロビジョニングを自動化できます。

NetScaler プールキャパシティライセンスの仕組み

NetScaler プール容量には次のコンポーネントがあります。

- NetScaler インスタンス。次のものに分類できます。
  - ゼロキャパシティハードウェア
  - スタンドアロンの NetScaler VPX インスタンスまたは NetScaler CPX インスタンスまたは NetScaler BLX インスタンス
- 帯域幅プール
- インスタンスプール
- 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 Pooled Capacity 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。さまざまな 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。
> - ゼロキャパシティライセンスのインストールは、他の NetScaler ローカルライセンスと同じように機能します。ゼロキャパシティライセンスを取得してインストールする方法について詳しくは、NetScaler のライセンスガイドを参照してください。

プラットフォームライセンスの管理とインストール

プラットフォームライセンスは、ハードウェア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 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 ハードウェアインスタンスに手動で移動することはできます。

NetScaler ソフトウェアリリース 11.1 ビルド 54.14 以降を実行する NetScaler MPX インスタンスと、11.1 ビルド 58.13 以降を実行する NetScaler SDX インスタンスは、NetScaler プール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。

スタンドアロン **NetScaler VPX** インスタンス

以下のハイパーバイザーで NetScaler ソフトウェアリリース 11.1 ビルド 54.14 以降を実行する NetScaler 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

以下のハイパーバイザーおよびクラウドプラットフォーム上で NetScaler ソフトウェアリリース 12.0 Build 51.24 以降を実行する NetScaler VPX インスタンスは、プールキャパシティをサポートします。

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

以下のハイパーバイザーおよびクラウドプラットフォーム上で NetScaler ソフトウェアリリース 13.0 および 13.1（すべてのバージョン）を実行する NetScaler VPX インスタンスは、プールキャパシティをサポートします。

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

- 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 VPX インスタンスを NetScaler ADM に追加する」を参照してください。
> 容量ゼロのハードウェアとは異なり、NetScaler VPX にはプラットフォームライセンスは必要ありません。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 CPX** インスタンス

Docker ホストにデプロイされた NetScaler CPX インスタンスは、プールキャパシティをサポートします。容量ゼロのハードウェアとは異なり、NetScaler CPX にはプラットフォームライセンスは必要ありません。最大 1 Gbps のスループットを消費する 1 つの NetScaler CPX インスタンスは、1 つのインスタンスのみをチェックアウトし、ライセンスプールから帯域幅はチェックアウトしません。たとえば、20 Gbps の帯域幅プールを備えた NetScaler CPX インスタンスが 20 個あるとします。NetScaler CPX インスタンスの 1 つが 500 Mbps のスループットを消費する場合、残りの 19 個の NetScaler CPX インスタンスの帯域幅プールは 20Gbps のままになります。

同じ NetScaler CPX インスタンスが 1500 Mbps のスループットを消費し始めた場合、残りの 19 個の NetScaler CPX インスタンスの帯域幅プールは 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 BLX** インスタンス

NetScaler BLX インスタンスはプールキャパシティライセンスをサポートしています。NetScaler BLX インスタンスには、プラットフォームライセンスは必要ありません。トラフィックを処理するには、NetScaler BLX インスタンス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 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 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 VPX インスタンスまたは NetScaler CPX インスタンスまたは NetScaler BLX インスタンスの数、または NetScaler BLX インスタンスの数、または NetScaler BLX インスタンスの数、または SDX-Z インスタンス内の NetScaler VPX インスタンスの数を定義します。

プールからチェックアウトすると、ライセンスによって MPX-Z、SDX-Z、VPX、NetScaler CPX、および NetScaler BLX インスタンスのリソース（CPU/PE、SSL コア、1 秒あたりのパケット数、帯域幅など）のロックが解除されます。

> 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 プールキャパシティは、ライセンスサーバーとして構成された NetScaler ADM を使用して、プールキャパシティライセンス（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、NetScaler ADM ライセンスがなくてもプール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 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 インスタンスが機能する前にチェックアウトする必要のある最小帯域幅とインスタンス数。
- NetScaler がチェックアウトできる最大帯域幅とインスタンス数。
- 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 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 最小帯域幅単位が 1 Gbps の場合、1000 Mbps はチェックアウトできますが、200 Mbps または 150.5 Gbps 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 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にのみ動作します。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 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 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
MPX 5900Z	10	1	-	-	1Gbps

製品ライン	最大帯域幅 (Gbps)	最小帯域幅 (Gbps)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
MPX 8900Z	30	5	-	-	1Gbps
MPX 9100Z	30	10	-	-	1Gbps
MPX 8900Z FIPS	33	5	-	-	1Gbps
MPX 14000Z シリーズ	100	20	-	-	1Gbps
MPX 14000Z 40G シリーズ	100	20	-	-	1Gbps
MPX 14000Z FIPS シリーズ	100	20	-	-	1Gbps
MPX 14000Z 40S シリーズ	100	20	-	-	1Gbps
MPX 15000Z シリーズ	120	20	-	-	1Gbps
MPX 15000Z FIPS シリーズ	120	20	-	-	1Gbps
MPX 15000Z 50G シリーズ	120	20	-	-	1Gbps
MPX 16000Z シリーズ	200	30	-	-	1Gbps
MPX 22000Z シリーズ	120	40	-	-	1Gbps
MPX 24000Z シリーズ	150	100	-	-	1Gbps
MPX 25000Z 40G	200	100	-	-	1Gbps
MPX 25000ZA	200	100	-	-	1Gbps
MPX 26000Z シリーズ	200	100	-	-	1Gbps
MPX 26000Z 100G シリーズ	200	100	-	-	1Gbps

製品ライン	最大帯域幅 (Gbps)	最小帯域幅 (Gbps)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
MPX 26000Z 50S シリーズ	200	100	-	-	1Gbps
SDX 8900Z	30	10	1	7	1Gbps
SDX 9100Z	95	20	1	7	1Gbps
SDX 14000Z シリーズ	100	10	1	25	1Gbps
SDX 14000Z 40G シリーズ	100	1	2	25	1Gbps
SDX 14000Z 40S シリーズ	100	20	1	25	1Gbps
SDX 14000Z FIPS シリーズ	100	10	1	25	1Gbps
SDX 15000Z 50G	120	10	1	55	1Gbps
SDX 15000Z	120	10	1	55	1Gbps
SDX 16000Z シリーズ	200	15	1	55	1Gbps
SDX 22000Z シリーズ	120	20	1	80	1Gbps
SDX 25000Z 40G	200	50	1	115	1Gbps
SDX 25000ZA	200	50	1	115	1Gbps
SDX 26000Z 100G	200	50	1	115	1Gbps
SDX 26000Z	200	50	1	115	1Gbps
SDX 26000Z 50S	200	50	1	115	1Gbps
SDX 24000Z シリーズ	150	50	1	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. NetScaler CPX** インスタンスでサポートされるプールキャパシティ

製品ライン	最大帯域幅 (Gbps)	最小帯域幅 (Mbps)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
CPX	10	10	1	1	10Mbps

表 **3.** ハイパーバイザーとクラウドサービス上の **NetScaler VPX** インスタンスでサポートされるプール容量

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
Citrix Hypervisor	40 Gbps	10Mbps	1	1	10Mbps
VMware ESXi	100 Gbps	10Mbps	1	1	10Mbps
Linux KVM	100 Gbps	10Mbps	1	1	10Mbps
Microsoft Hyper-V	3Gbps	10Mbps	1	1	10Mbps
AWS	30 Gbps	10Mbps	1	1	10Mbps
Azure	10 Gbps	10Mbps	1	1	10Mbps
Google Cloud	10 Gbps	10Mbps	1	1	10Mbps

> 注
>
> 最小購買数量は、最小システム要件とは異なります。

表 **4. NetScaler BLX** インスタンスでサポートされるプールキャパシティ

製品ライン	最大帯域幅 (Gbps)	最小帯域幅 (Mbps)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
BLX	100	10	1	1	10Mbps

表 **5.** さまざまなフォームファクタのライセンス要件

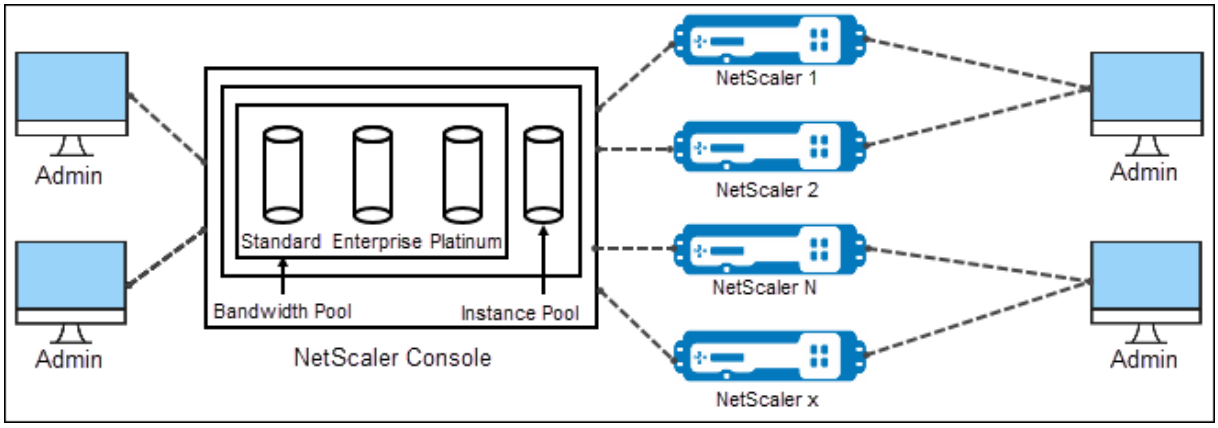
製品ライン	ゼロキャパシティハードウェアの購入	帯域幅とエディションサブスクリプション	インスタンスのサブスクリプション
MPX	ライセンスが必要です	ライセンスが必要です	-
SDX	ライセンスが必要です	ライセンスが必要です	ライセンスが必要です
VPX	-	ライセンスが必要です	ライセンスが必要です
CPX	-	-	ライセンスが必要です
BLX	-	ライセンスが必要です	ライセンスが必要です

NetScaler プールキャパシティの構成

February 6, 2024

NetScaler プールキャパシティを使用するには、NetScaler ADM を必要な NetScaler インスタンスのライセンスサーバーとして構成します。NetScaler インスタンスは、NetScaler 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。NetScaler アプリケーション配信および管理 GUI では、次のタスクを実行できます。

- プールキャパシティライセンスファイル (帯域幅とインスタンスプール) をライセンスサーバーにアップロードします。
- 必要に応じて、ライセンスプールから NetScaler インスタンスにライセンスを割り当てます。
- インスタンスの最小容量と最大容量に基づいて、NetScaler インスタンス（MPX-Z /SDX-Z/VPX/CPX/BLX）からライセンスを確認します。
- 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、NetScaler FIPS インスタンスのプール容量を構成します。



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 プール容量」を参照してください。

NetScaler プールキャパシティの状態

プール容量の状態は、NetScaler インスタンスのライセンス要件を示します。プールキャパシティで構成された NetScaler インスタンスには、次のいずれかの状態が表示されます。

- **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。
- 使用不可: インスタンスが管理用に NetScaler ADM に登録されていないか、NetScaler 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-NetScaler ADM でライセンスを適用する

1. NetScaler ADM で、「NetScaler ライセンス」>「プールライセンス」に移動します。
2. [ライセンスファイル] セクションで、[ライセンスファイルの追加] を選択し、次のいずれかのオプションを選択します。
    - ローカルコンピュータからライセンスファイルをアップロードします。ライセンスファイルがローカルコンピューターに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:
>
> NetScaler ADM には、［ライセンス設定］からいつでもライセンスを追加できます。

3. ［完了］をクリックします。

   ライセンスファイルが NetScaler ADM に追加されます。［ライセンス有効期限情報］タブには、NetScaler ADM に存在するライセンスと有効期限までの残り日数が表示されます。

4. [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、NetScaler 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。

プールライセンスを NetScaler アプリケーションの配信と管理に適用する方法について詳しくは、以下の関連ビデオを参照してください。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

手順 **2-NetScaler ADM** をライセンスサーバーとして登録する

NetScaler ADM をライセンスサーバーとして NetScaler 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 **NetScaler ADM** をライセンスサーバーとして登録する

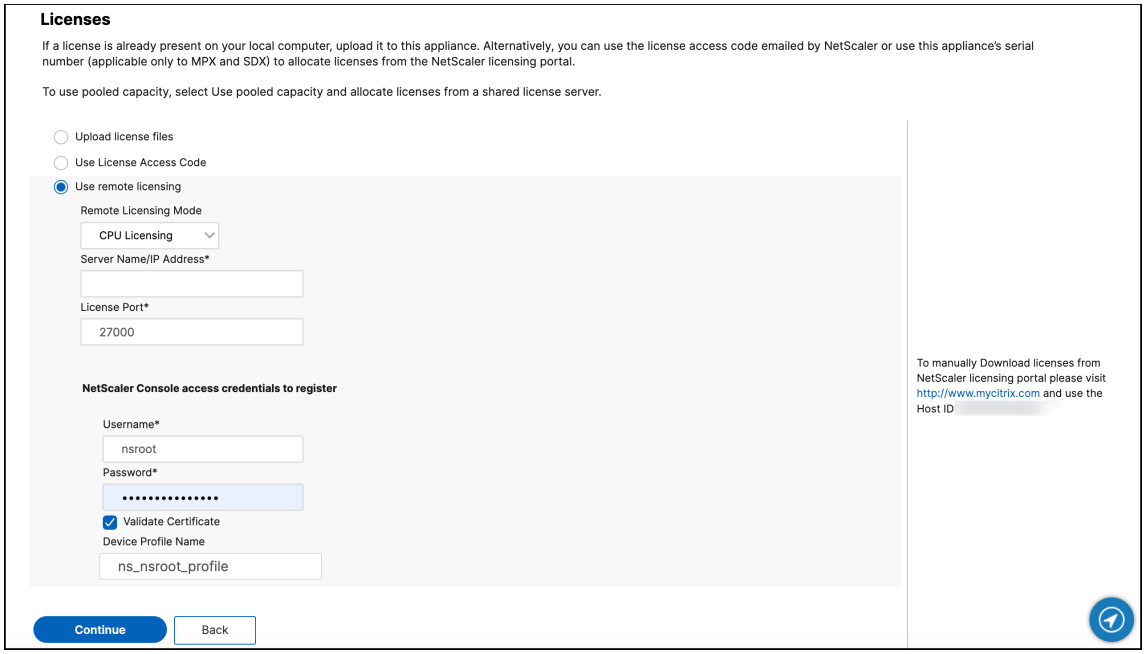
NetScaler GUI で、NetScaler ADM サーバーをライセンスサーバーとして登録します。

1. NetScaler GUI にログインします。
2. [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」フィールドに、NetScaler ADM サーバーの IP アドレスを指定します。

> 高可用性環境では、フローティング IP を使用してください。設定の詳細については、「高可用性デプロイの設定」を参照してください。
>
> スタンドアロンの NetScaler ADM またはエージェントを使用する展開については、「ライセンスの概

> 要」を参照してください。

6. [**NetScaler ADM** に登録] を選択します。
7. NetScaler ADM の認証情報を入力してインスタンスを NetScaler ADM に登録し、[続行] をクリックします。



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 でライセンスを割り当てます。ライセンス割り当ては、後で NetScaler ADM GUI から変更または解放できます。

   a) [**Get Licenses**] をクリックします。

> 重要:
>
> ライセンスエディションを変更した場合は、インスタンスをウォームリスタートします。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 **NetScaler ADM** をライセンスサーバーとして追加します

NetScaler インスタンスに GUI がない場合は、次の CLI コマンドを使用して NetScaler ADM サーバーをライセンスサーバーとして追加します。

1. NetScaler ADC コンソールにログインします。
2. NetScaler ADM サーバーの IP アドレスを追加します。

```
1 > add ns licenseserver <adm-server-IP-address> -port <adm-server-
     port-number> -licensemode <license-mode>
2 <!--NeedCopy-->
```


詳細については、「ライセンスの概要」を参照してください。

3. ライセンスサーバーで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-->
```

このコマンドは、ライセンスサーバーを追加するときに、指定したライセンスモードに基づいてライセンスを一覧表示します。

例 **1**:

指定したライセンスモードがCICOの場合、出力には CICO ライセンスのみが含まれます。

```
> add licenseserver [redacted] -licensemode CICO
 Done
> sh licenseserverpool
        VPX8000P Total                  : 1
        VPX8000P Available              : 1
```

例 **2**:

指定されたライセンスモードがPooledの場合、出力にはプールキャパシティライセンスのみが含まれます。

```
> add licenseserver [redacted] -licensemode Pooled
 Done
> sh licenseserverpool
        Instance Total                  : 40
        Instance Available              : 38
        Standard Bandwidth Total        : 210.00 Gbps
        Standard Bandwidth Available    : 210.00 Gbps
        Enterprise Bandwidth Total      : 50.00 Gbps
        Enterprise Bandwidth Available  : 50.00 Gbps
        Platinum Bandwidth Total        : 210.00 Gbps
        Platinum Bandwidth Available    : 205.00 Gbps
```

例 **3**:

指定したライセンスモードがvCPUの場合、出力には仮想 CPU ライセンスのみが含まれます。

```
> add licenseserver [redacted] -licensemode vCPU
 Done
> sh licenseserverpool
        Standard CPU Total              : 100
        Standard CPU Available          : 100
        Enterprise CPU Total            : 100
        Enterprise CPU Available        : 100
        Platinum CPU Total              : 25
        Platinum CPU Available          : 20
```

すべてのライセンスをまとめて表示するには、次のコマンドを実行します。

```
1 > sh ns licenseserverpool -getallLicenses
2 <!--NeedCopy-->
```

出力例:


```
> sh licenseserverpool -getallLicenses
        Instance Total                      : 40
        Instance Available                  : 33
        Standard Bandwidth Total            : 210.00 Gbps
        Standard Bandwidth Available        : 210.00 Gbps
        Enterprise Bandwidth Total          : 50.00 Gbps
        Enterprise Bandwidth Available      : 50.00 Gbps
        Platinum Bandwidth Total            : 210.00 Gbps
        Platinum Bandwidth Available        : 205.00 Gbps
        VPX8000P Total                      : 1
        VPX8000P Available                  : 1
        Standard CPU Total                  : 100
        Standard CPU Available              : 100
        Enterprise CPU Total                : 100
        Enterprise CPU Available            : 100
        Platinum CPU Total                  : 25
        Platinum CPU Available              : 20
```

4. 必要なライセンスエディションからライセンス帯域幅を割り当てます。

```
> set ns capacity -unit <specify-mbps-or-gbps> -bandwidth <specify
    -amount-license-bandwidth> -edition <specify-license-edition>
<!--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-**プールされたライセンスを **NetScaler** インスタンスに割り当てる

NetScaler 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:

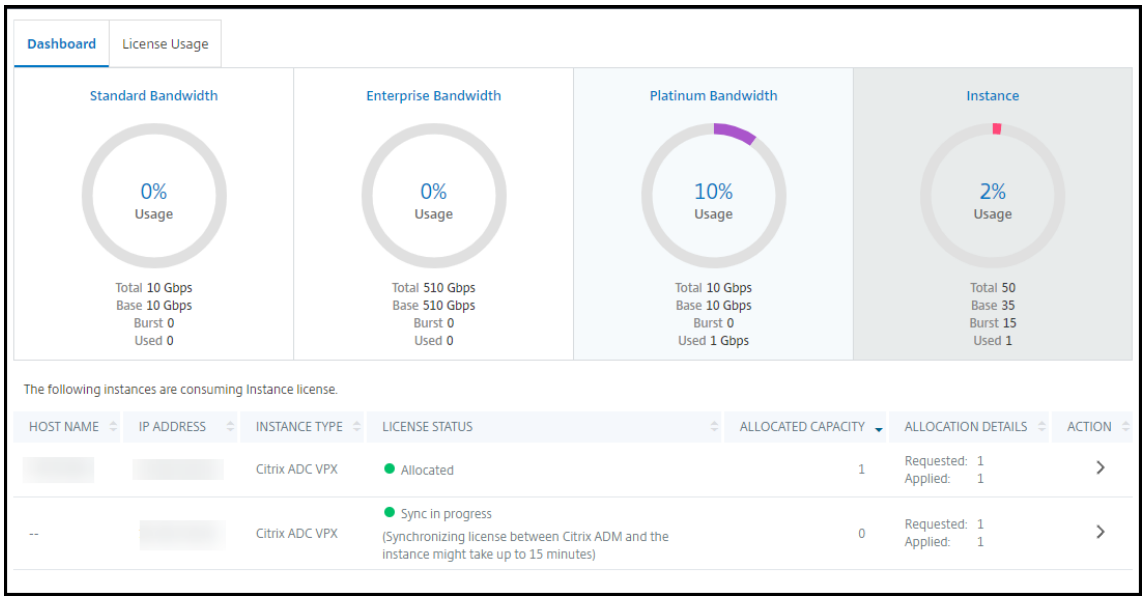
1. NetScaler ADM にログインします。
2. インフラストラクチャ **>** ライセンス **>** 帯域幅ライセンス **>** プールキャパシティに移動します。

   FIPS インスタンスの容量は、FIPS インスタンスのライセンスを NetScaler ADM にアップロードした場合にのみ表示されます。
3. 管理するライセンスプールをクリックします。

> (注)
>
> [割り当て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、NetScaler 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。

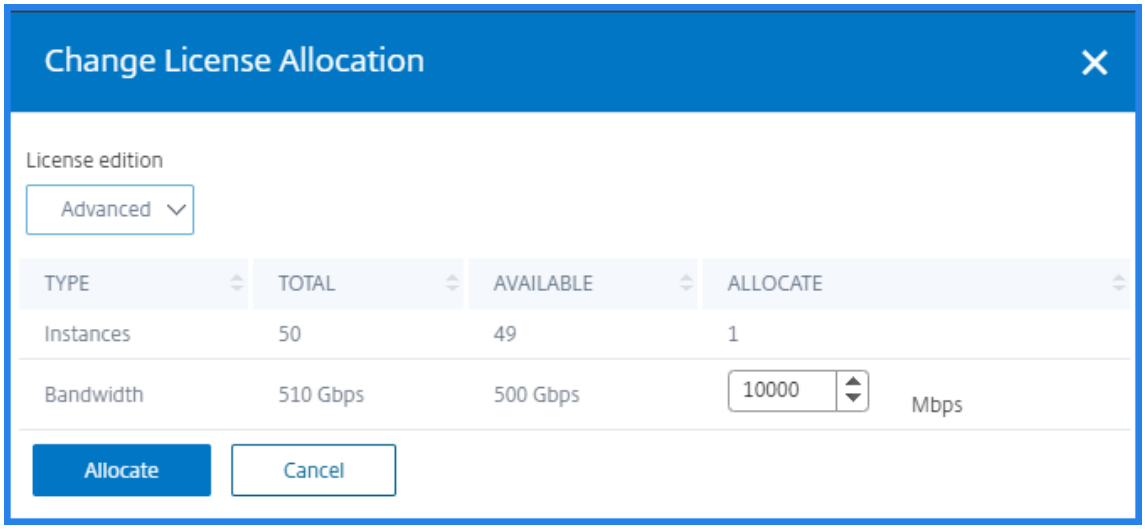
4. ボタンをクリックして、使用可能なインスタンスのリストから **NetScaler** インスタンスを選択します。



LICENSE STATUS 列には、対応するライセンス割り当てステータスメッセージが表示されます。

> 注:
>
> 「管理対象外のインスタンス」タブには、NetScaler ADM で検出されたが管理されていないインスタンスが表示されます。
>
> 
>

5. [割り当ての変更] または [割り当ての解除] 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** list 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割り当てを選択できます。選択後、[割り当て] をクリックします。
8. 「ライセンス割り当ての変更」ウィンドウのリストオプションから、割り当てられたライセンスエディションを変更することもできます。



> 注
>
> ライセンスエディションを変更した場合は、インスタンスをウォームリスタートしてください。

帯域幅割り当てを変更する方法の詳細については、関連ビデオを参照してください。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

NetScaler インスタンスのプール容量を構成する

プールキャパシティライセンスは、次の NetScaler インスタンスで構成できます。

- NetScaler インスタンス
- NetScaler VPX インスタンス
- NetScaler の高可用性ペア

NetScaler MPX インスタンス

MPX-Z は、プールキャパシティ対応の NetScaler 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、設定された容量に必要なプールライセンスが自動的にチェックアウトされます。

NetScaler VPX インスタンス

プールキャパシティ対応の NetScaler 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。NetScaler GUI を使用して、ライセンスサーバーからライセンスをチェックアウトできます。

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、構成されたプールキャパシティライセンスが NetScaler ADM サーバーから自動的にチェックアウトされます。

NetScaler の高可用性ペア

開始する前に、NetScaler ADM サーバーがライセンスサーバーとして構成されていることを確認します。詳しくは、「NetScaler 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 NetScaler インスタンスの場合、高可用性ペアの各ノードでプール容量を構成する必要があります。プライマリノードとセカンダリノードの両方に、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 NetScaler 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。まず、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。

NetScaler VPX の永続ライセンスを **NetScaler** プールキャパシティにアップグレードする

February 6, 2024

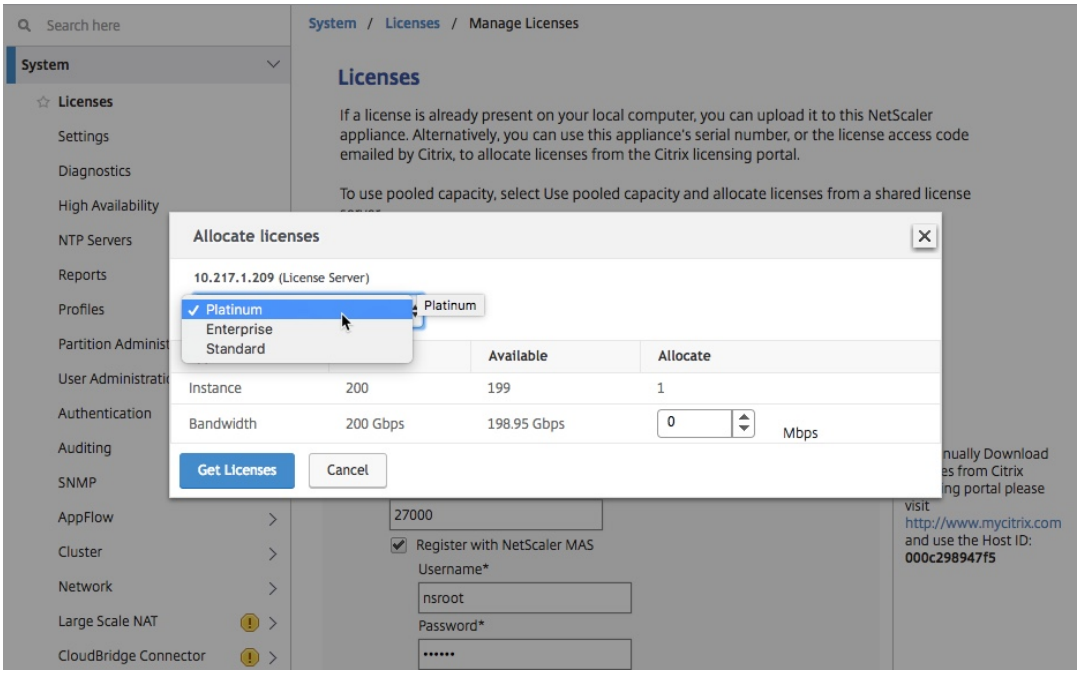
永久ライセンスの NetScaler VPX インスタンスは、ADC プールキャパシティライセンスにアップグレードできます。プールキャパシティライセンスにアップグレードすると、ライセンスプールから VPX インスタンスにライセンス

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 ADC インスタンスにプールキャパシティライセンスを設定することもできます。VPX インスタンスのプールキャパシティライセンスを高可用性モードで構成するには、「NetScaler VPX 高可用性ペアの永続ライセンスの NetScaler プールキャパシティへのアップグレード」を参照してください。

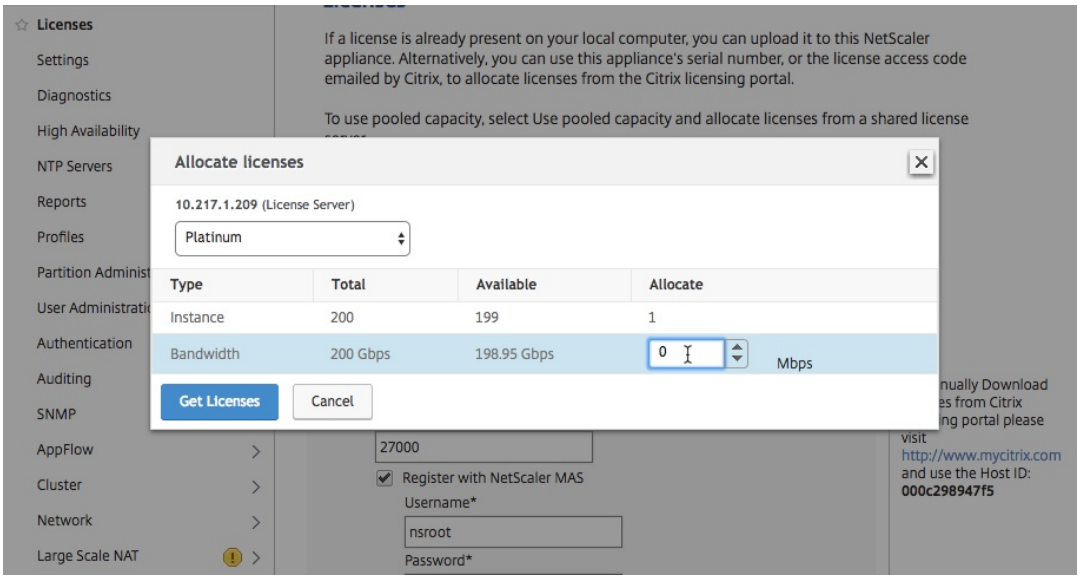
前提条件

NetScaler プールキャパシティにアップグレードするには:

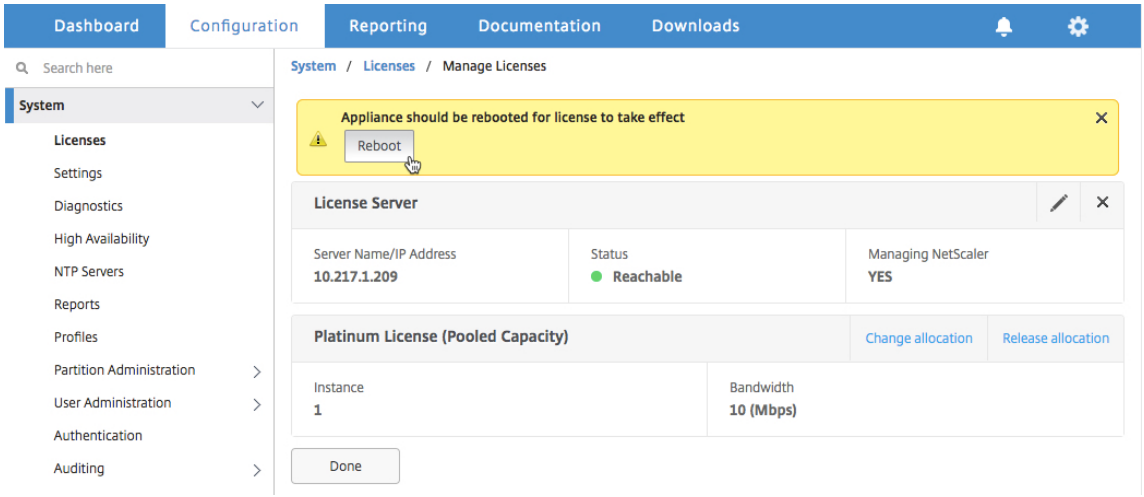
1. Web ブラウザで、VPX インスタンスの IP アドレス (http://192.168.100.1など) を入力します。
2. ［**User Name**］ボックスと ［**Password**］ボックスに管理者資格情報を入力します。
3. [ようこそ] ページで、[続行] をクリックします。
4. [構成] タブで、[システム**] > [**ライセンス**]** に移動し、**[** ライセンスの管理] をクリックします。
5. [ライセンス] ページで、[新しい ****** ライセンスの 追加 ******] をクリックします。
6. [ライセンス] ページで、[リモートライセンスを使用する] 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 に登録する」チェックボックスが選択されていることを確認し、NetScaler ADM 認証情報を入力します。
   d) ［続行］をクリックします。
7. 「ライセンスの割り当て」で、次の操作を行います。
   a) ドロップダウンリストからライセンスエディションを選択します。



b) ［割り当て］メニューから NetScaler アプライアンスに帯域幅 を割り当て 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 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 VPX 高可用性ペアの永続ライセンスを **NetScaler** プールキャパシティにアップグレードします

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容量を設定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 VPX HA** セットアップを **NetScaler** プール容量にアップグレードするには:

1. セカンダリ VPX (ノード 2) インスタンスにログオンします。Web ブラウザーで、NetScaler アプライアンスの IP アドレス（`http://192.168.100.1`など）を入力します。
2. ［**User Name**］ボックスと ［**Password**］ボックスに管理者資格情報を入力します。
3. [ようこそ] ページで、[続行] をクリックします。
4. [構成] タブで、[システム**] > [**ライセンス] に移動し、[ライセンスの管理] をクリックします。
5. [ライセンス] ページで、[新しい **** ライセンスの 追加 **] をクリックします。

6. [リモートライセンスを使用] を選択し、次の操作を行います。

   a) [リモートライセンスモード] ドロップダウンリストで、[プールライセンス] を選択します。

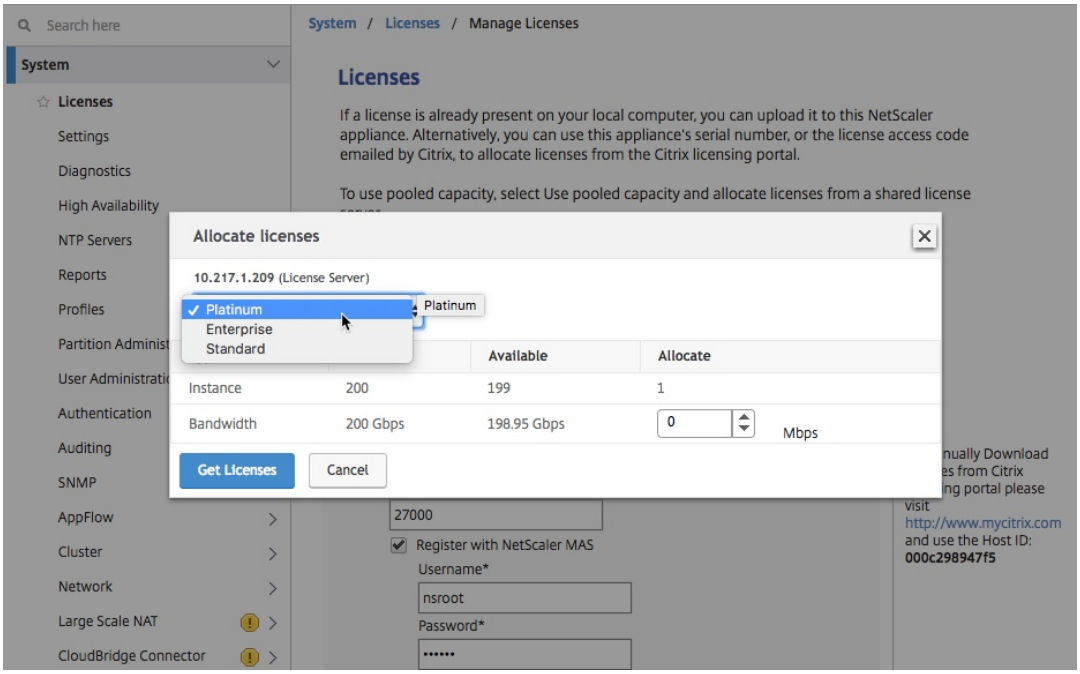
   b) [サーバ名/**IP** アドレス] フィールドに、ライセンスサーバの詳細を入力します。

   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 に登録する」チェックボックスが選択されていることを確認し、NetScaler ADM 認証情報を入力します。

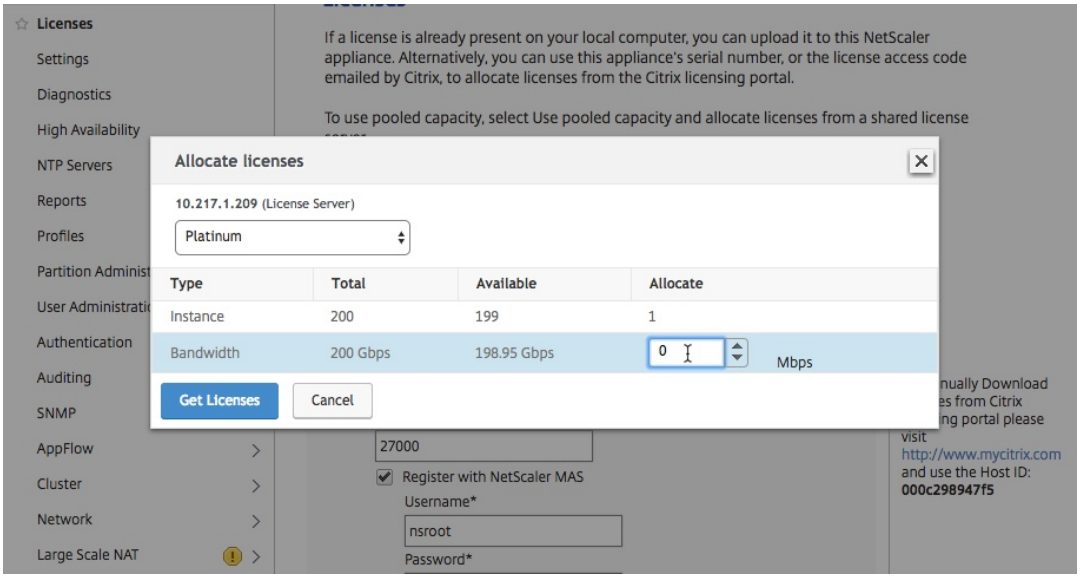
   d) [続行] をクリックします。

7. 「ライセンスの割り当て」で、次の操作を行います。

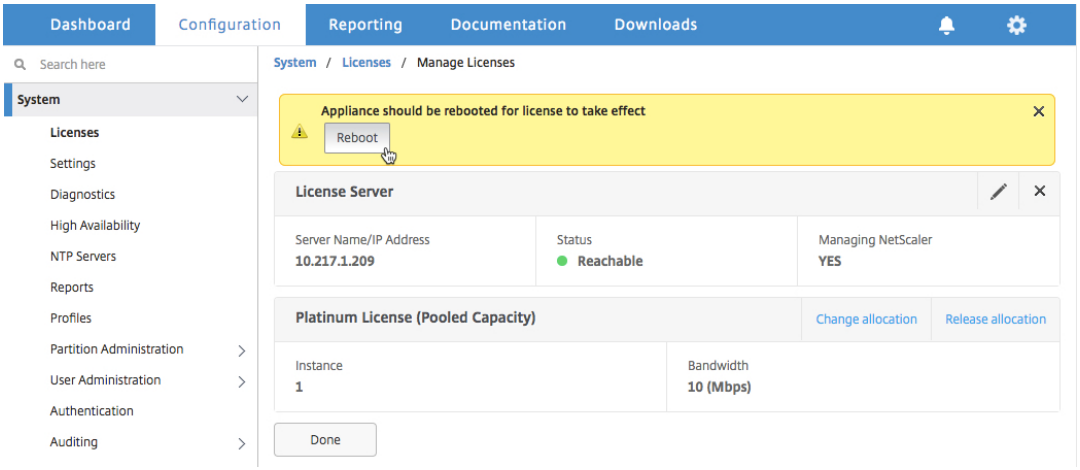
   a) ドロップダウンリストからライセンスエディションを選択します。



   b) [割り当て] メニューから NetScaler アプライアンスに帯域幅 を割り当て 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` このフェールオーバーにより、HA ペアの正常な状態が保証されます。

9. フェイルオーバー後、新しいセカンダリ VPX インスタンス（ノード 1）にログオンし、同じプロセスを繰り返して新しいセカンダリをプールに追加します。

   HA ペアのプライマリインスタンスとセカンダリインスタンスを元の HA ペア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-->
```


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、次の手順を実行します。

    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 MPX 永続ライセンスから **NetScaler** プールキャパシティへのアップグレード

February 6, 2024

永久ライセンスの NetScaler MPX は、NetScaler プールキャパシティライセンスにアップグレードできます。NetScaler プール容量ライセンスにアップグレードすると、ライセンスプールから NetScaler アプライアンスに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 インスタンスに NetScaler 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。NetScaler MPX インスタンスの NetScaler プールキャパシティライセンスを高可用性モードで構成するには、「NetScaler MPX 高可用性ペアの永続ライセンスの NetScaler プールキャパシティへのアップグレード」を参照してください。

> 注
>
> 永久ライセンスからプールキャパシティライセンスへの切り替えは、ライセンスを取得するための一方的なプロセスです。プールキャパシティライセンスを永続ライセンスに戻すことはできません。
> 重要
>
> NetScaler MPX を NetScaler 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。

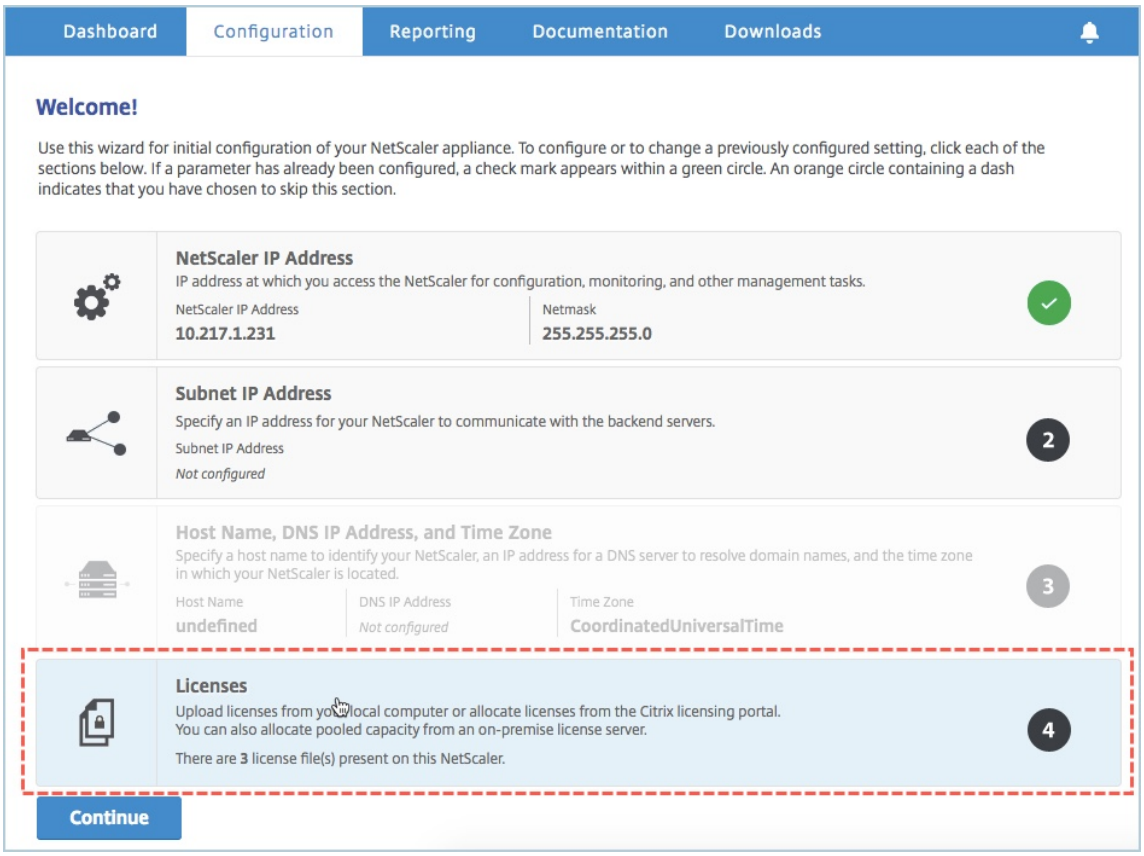
NetScaler プールキャパシティにアップグレードするには:

1. Web ブラウザーで、NetScaler の IP アドレス（など）を入力しますhttp://192.168.100.1。
2. ［**User Name**］ボックスと ［**Password**］ボックスに管理者資格情報を入力します。
3. [ようこそ] ページで、[続行] をクリックします。
4. ゼロキャパシティライセンス (MPX-Z ライセンス) をアップロードします。[構成] タブで、[システム] > [ライセンス] に移動します。
5. 詳細ペインで、[ライセンスの管理**]** をクリックし、**[**** 新しいライセンス ** の追加] をクリックします。
6. ライセンスページで、[ライセンスファイルのアップロード] を選択し、[参照] をクリックしてローカルマシンからゼロキャパシティライセンスを選択します。

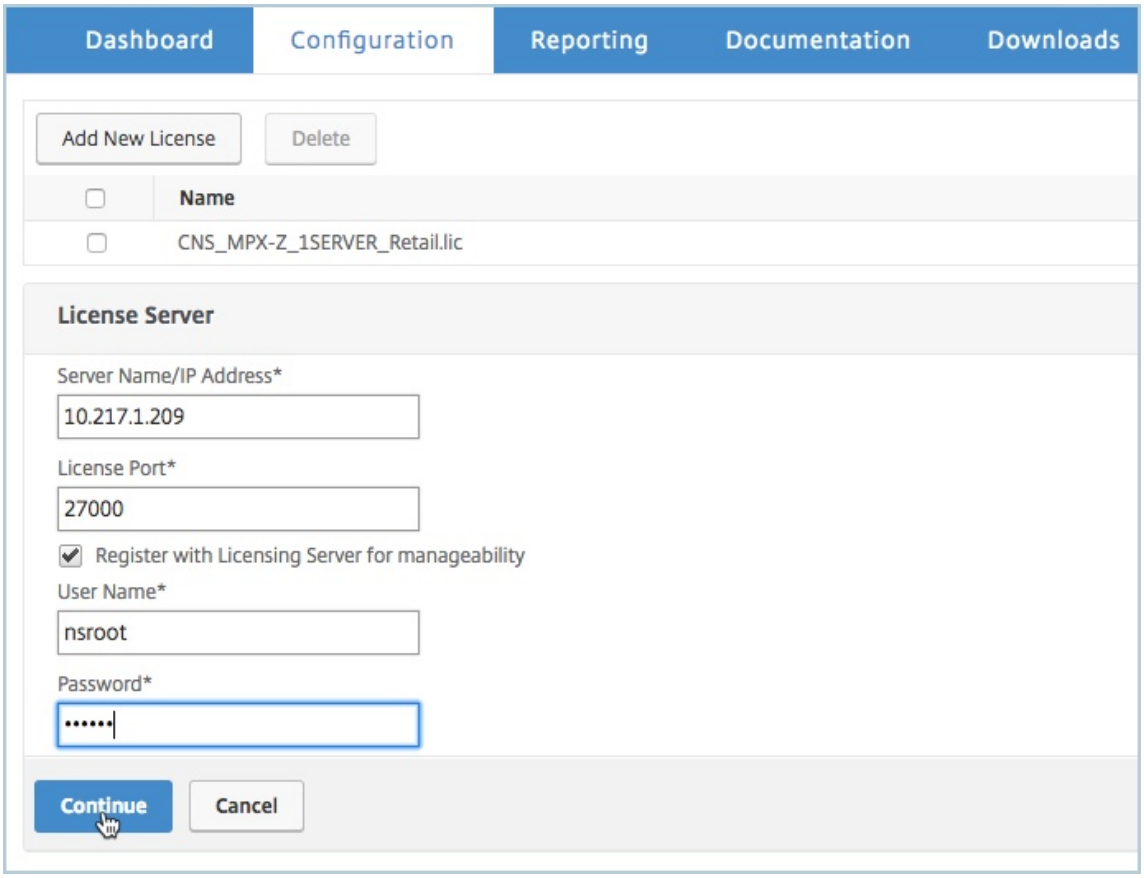
7. ライセンスがアップロードされたら、[**Reboot**] をクリックしてアプライアンスを再起動します。

> 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と、NetScaler ADM GUI から HTTPS を使用して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。



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。

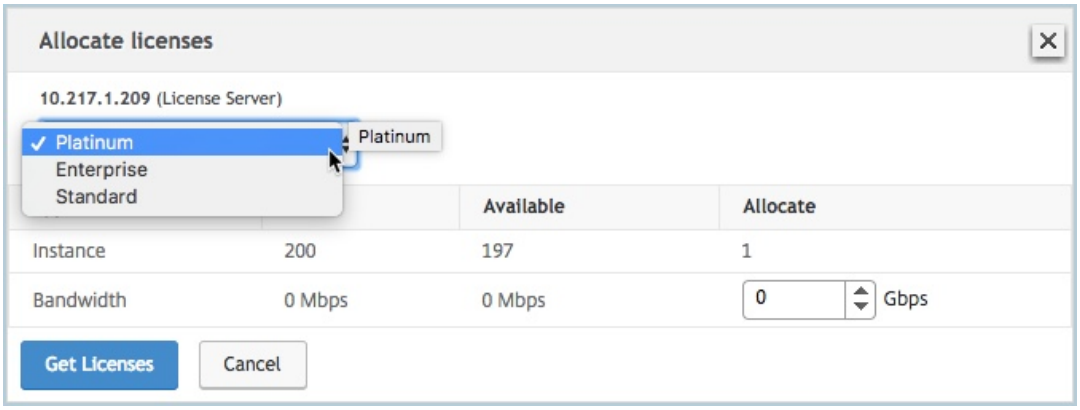
b) [**License Port**] フィールドに、ライセンスサーバのポートを入力します。デフォルト値：27000。

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、NetScaler ADM 認証情報を入力します。

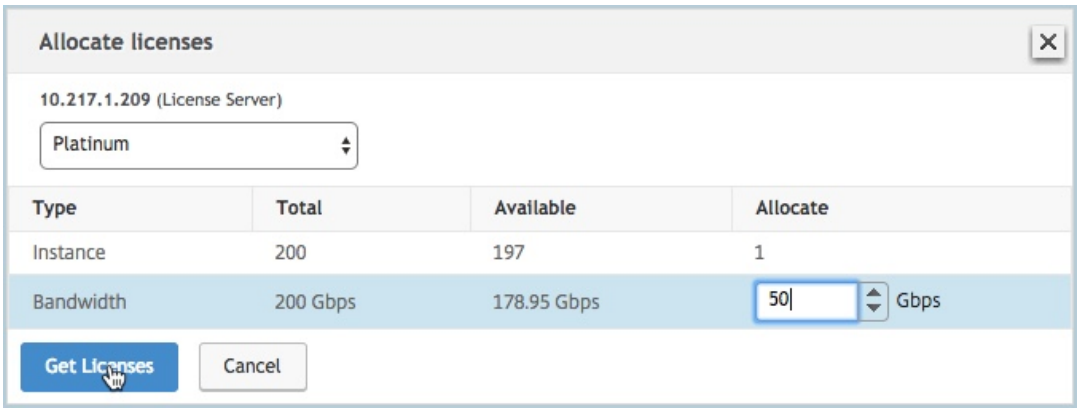
d) ［続行］をクリックします。

12.「ライセンスの割り当て」で、次の操作を行います。

a) ドロップダウンリストからライセンスエディションを選択します。



b) ［割り当て］メニューから NetScaler に帯域幅を割り当て、［ライセンスの取得］をクリックします。



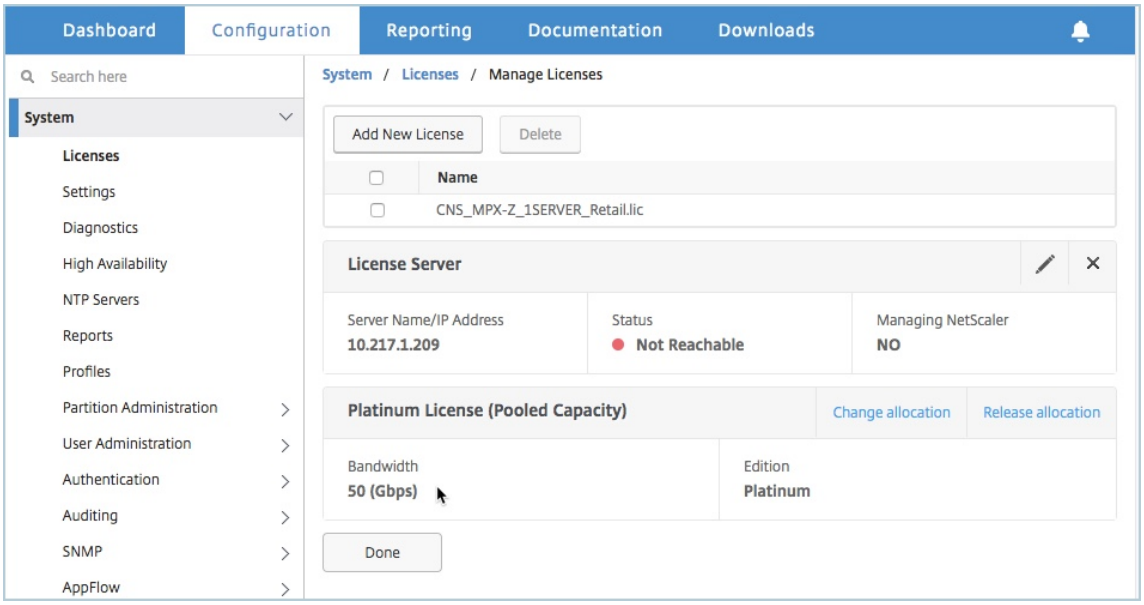
c) プロンプトが表示されたら、[**Reboot**] をクリックしてアプライアンスを再起動します。

13. NetScaler MPX が再起動したら、NetScaler MPX にログオンします。[ようこそ] ページで、[続行] をクリックします。

    [ライセンス] ページには、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 MPX 高可用性ペアの永久ライセンスから **NetScaler** プールキャパシティへのアップグレード

高可用性モードで構成された MPX アプライアンスの場合、HA ペアのプライマリ NetScaler インスタンスとセカンダリ NetScaler インスタンスの両方でプール容量を構成する必要があります。HA ペアのプライマリ NetScaler イ

ンスタンスとセカンダリ NetScaler インスタンスの両方に同じ容量のライセンスを割り当てます。たとえば、HA ペアの各インスタンスから 1 Gbps の容量が必要な場合は、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 インスタンスにそれぞれ 1 Gbps を割り当てることができます。

> 重要
>
> NetScaler MPX をアップグレードして NetScaler 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。

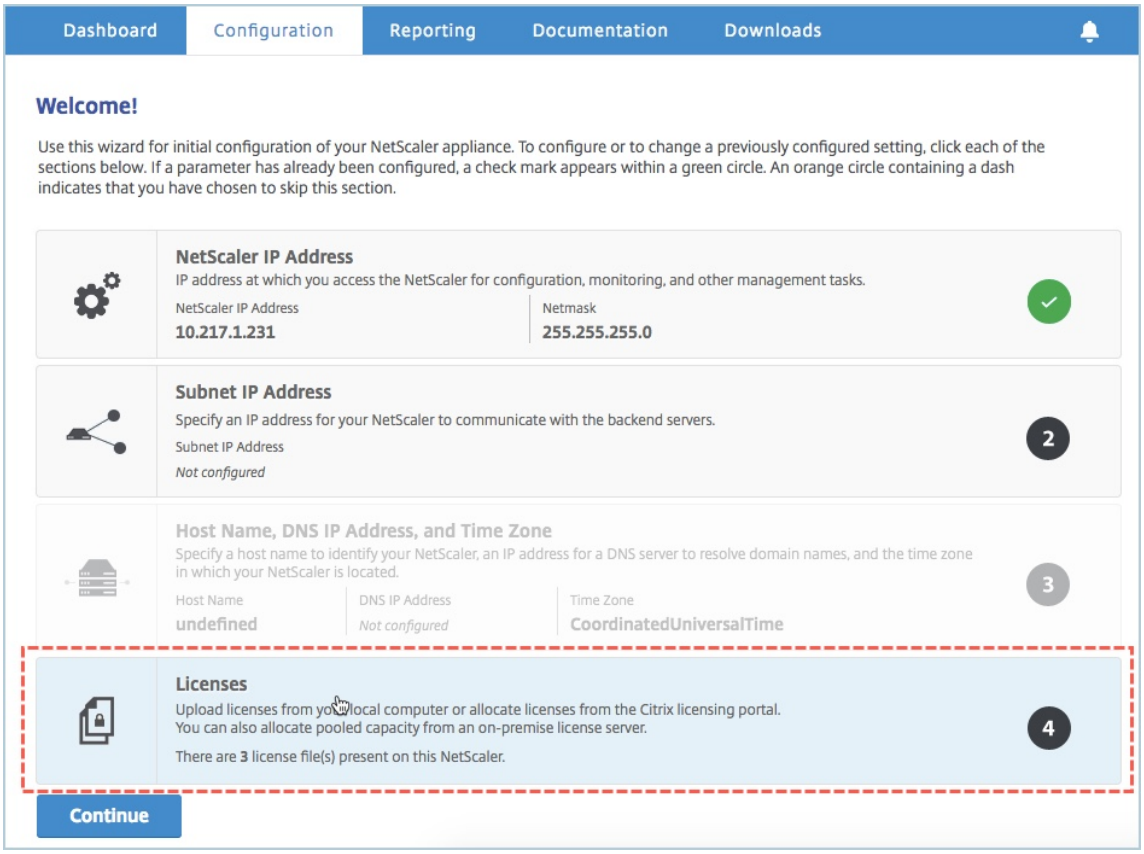
MPX-Z ライセンスを **HA** ペアの **NetScaler MPX** インスタンスにアップロードするには:

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. [**User Name**] ボックスと [**Password**] ボックスに管理者資格情報を入力します。
3. [ようこそ] ページで、[続行] をクリックします。
4. ゼロキャパシティライセンス (MPX-Z ライセンス) をアップロードします。[**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。

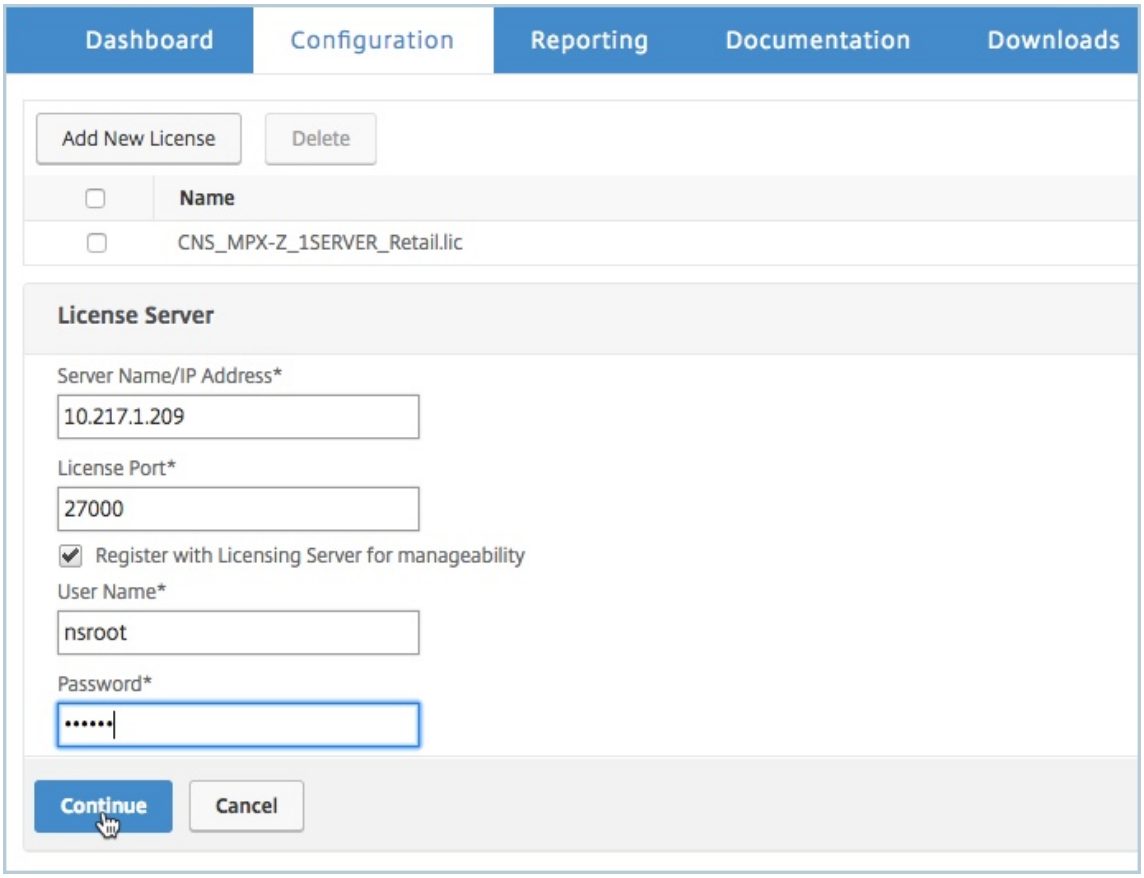
   ライセンスがアップロードされると、アプライアンスを再起動するように求められます。
7. [**Reboot**] をクリックして、アプライアンスを再起動します。
8. 「確認」ページで、「はい」をクリックします。

既存の高可用性セットアップを **NetScaler** プール容量にアップグレードするには:

1. セカンダリ NetScaler MPX インスタンスにログオンします。Web ブラウザーで、NetScaler の IP アドレス（など）を入力しますhttp://192.168.100.1。
2. [**User Name**] ボックスと [**Password**] ボックスに管理者資格情報を入力します。
3. 「ようこそ」ページで、「ライセンス」セクションをクリックします。



4. [ライセンスサーバー] セクションで、次の操作を行います。



a) [サーバ名**/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。

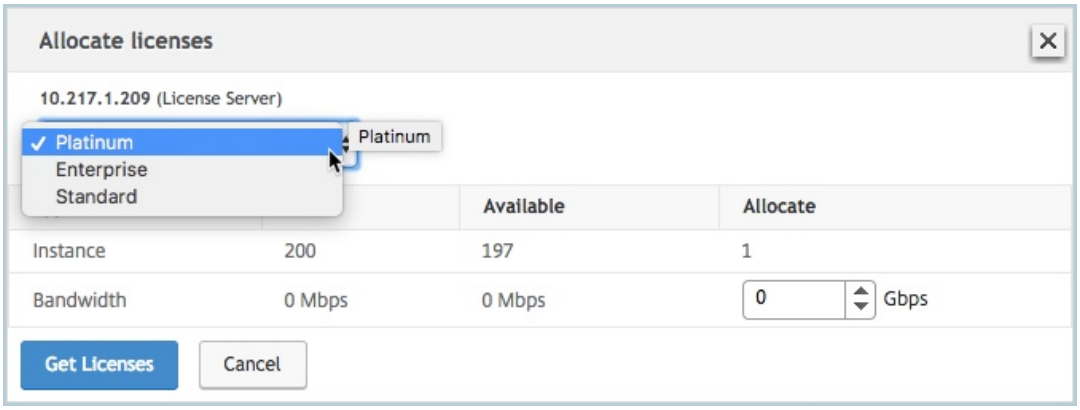
b) [**License Port**] フィールドに、ライセンスサーバのポートを入力します。デフォルト値：27000。

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、NetScaler ADM 認証情報を入力します。

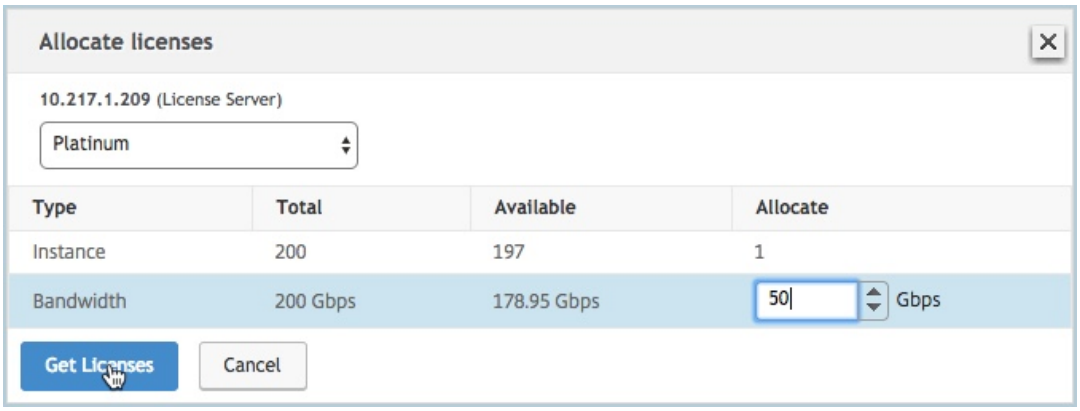
d) ［続行］をクリックします。

5.「ライセンスの割り当て」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 に帯域幅を割り当て、［ライセンスの取得］をクリックします。



c) プロンプトが表示されたら、[**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` このフェールオーバーにより、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 MPX 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：

a) Web ブラウザーで、NetScaler の IP アドレス（など）を入力しますhttp://192.168.100.1。

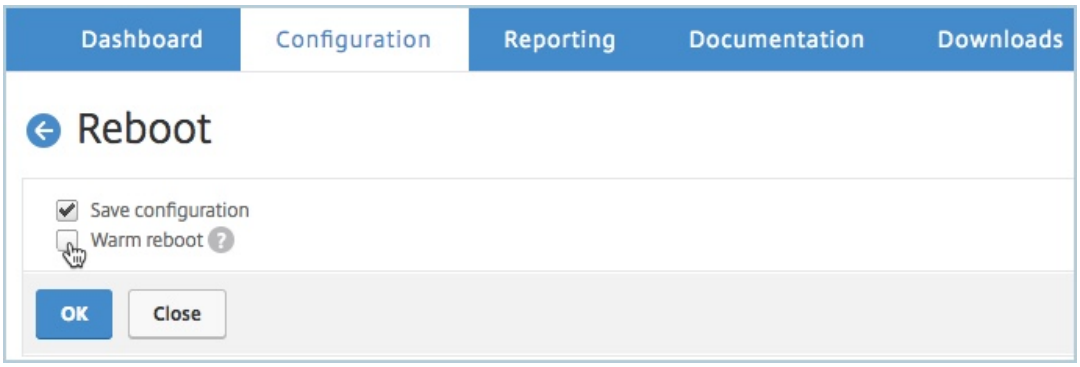
b) ［**User Name**］ボックスと ［**Password**］ボックスに管理者資格情報を入力します。

c) [ようこそ] ページで、[続行] をクリックします。

d) [構成] タブで [システム] をクリックします。

e) [システム] ページで、[再起動] をクリックします。

f) [再起動] ページで、[ウォーム再起動] を選択し、[**OK**] をクリックします。



プライマリの NetScaler MPX は再起動後、HA ペアのセカンダリ NetScaler MPX になります。HA ペアのプライマリ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 SDX の永続ライセンスを NetScaler プールキャパシティにアップグレードする

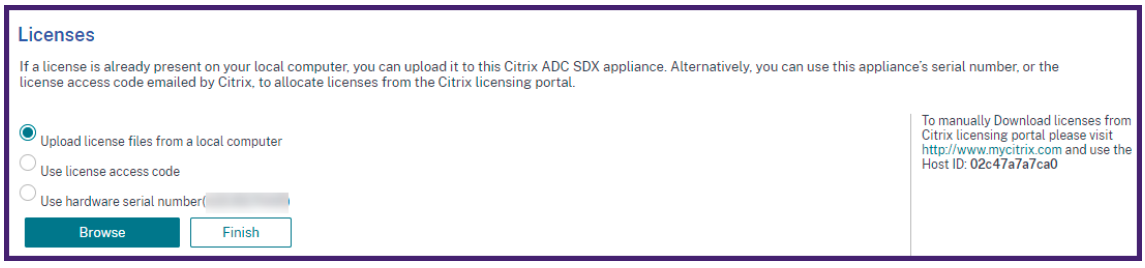
February 6, 2024

永久ライセンスの NetScaler SDX は、NetScaler プールキャパシティライセンスにアップグレードできます。NetScaler 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 NetScaler 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 インスタンスに NetScaler 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。

> 重要
>
> 永久ライセンスからプールキャパシティライセンスへの切り替えは、一方向のライセンス権限付与プロセスです。プールキャパシティライセンスを永久に戻すことはできません。
>
> - NetScaler SDX を NetScaler 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、SDX-Z ライセンスをアプライアンスにアップロードする必要があります。
> - NetScaler ADM にネットスケーラーインスタンスを追加する権限があることを確認してください。
> - 現在のライセンスに影響がないようにするには、お客様は永久ライセンスの一部として使用できるのと同じ数のインスタンスと帯域幅を割り当てる必要があります。

NetScaler プールキャパシティにアップグレードするには:

1. Web ブラウザーで、NetScaler SDX の IP アドレス（など）を入力しますhttp://192.168.100.1。
2. [**User Name**] ボックスと [**Password**] ボックスに管理者資格情報を入力します。
3. [ようこそ] ページで、[続行] をクリックします。
4. ゼロキャパシティライセンスをアップロードします。[構成] タブで、[システム] > [ライセンス] に移動します。
5. [ライセンスの管理] ページで、[ライセンスファイルの追加] をクリックします。
6. 「ライセンス」ページで、「ローカルコンピューターからライセンスファイルをアップロード」を選択し、「参照」をクリックしてローカルマシンから容量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。



ゼロキャパシティライセンスが正常に適用されると、ライセンスページに「プールライセンス」セクションが表示されます。

> 注
>
> 古いライセンスファイルを削除する場合、NetScaler SDX を再起動する必要がないため、ダウンタイムは発生しません。詳細については、NetScaler サポートにお問い合わせください。

7. ［プールライセンス］セクションで、次の操作を行います。

   a) [ライセンスサーバ名] 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。

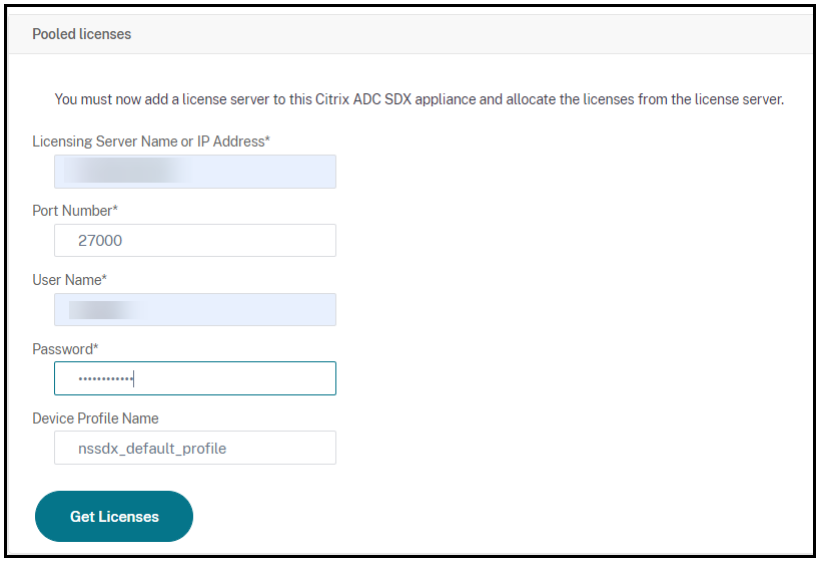
   - NetScaler ADM サーバーをライセンスサーバーとして構成する場合は、NetScaler ADM サーバーの IP アドレスを指定します。
   - エージェントを使用して NetScaler ADM サーバーと通信する場合は、NetScaler ADM エージェントの IP アドレスを指定します。

   b)「ポート番号」フィールドに、ライセンスサーバーのポートを入力します。デフォルト値：27000。

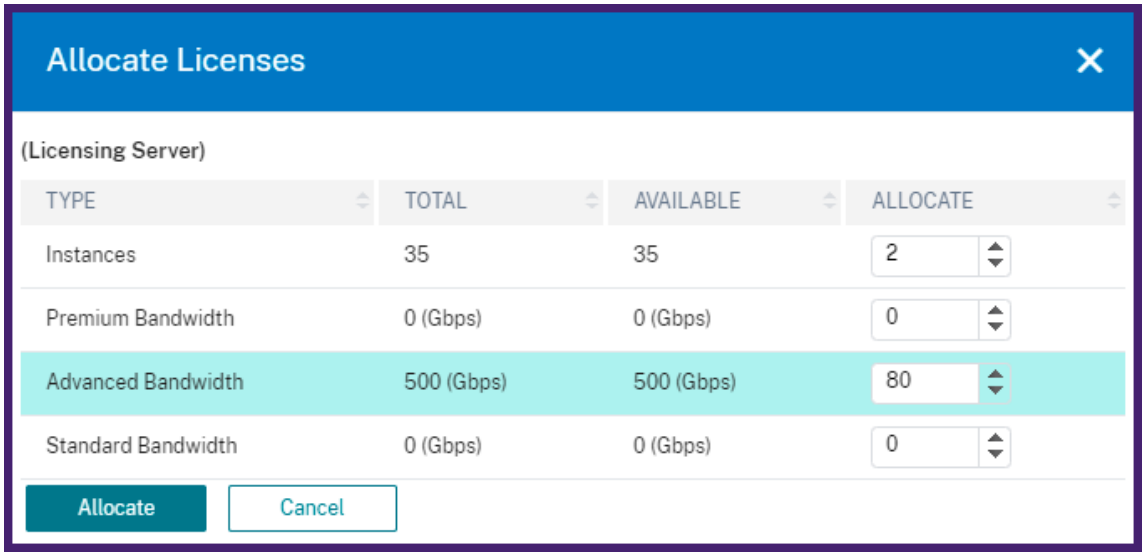
   c) ライセンスサーバーのユーザー名とパスワードを指定します。

   - NetScaler ADM サーバーの場合は、管理者の資格情報を入力します。
   - NetScaler ADM エージェントの場合は、エージェントの資格情報を入力します。

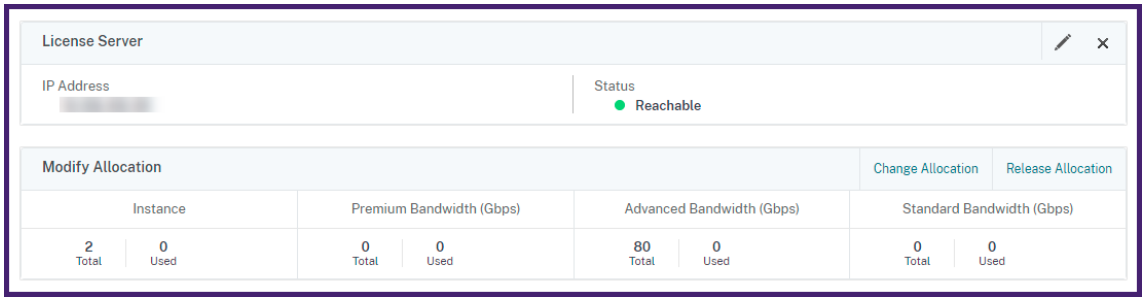
   d) ［**Get Licenses**］をクリックします。



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。



[**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。



> 注
>
> 永久ライセンスをプールキャパシティ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** インスタンス上の **NetScaler** プールキャパシティ

February 6, 2024

クラスターとして構成された NetScaler インスタンスで NetScaler プール容量を構成できます。NetScaler インスタンスのプール容量をクラスターモードで構成するための前提条件は次のとおりです。

- インスタンスは個別にプールキャパシティライセンスモードで実行され、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 アプリケーションの配信と管理からプール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と同じでない限り、新しいインスタンスを既存の NetScaler クラスターに追加することはできません。

NetScaler クラスターから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 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。

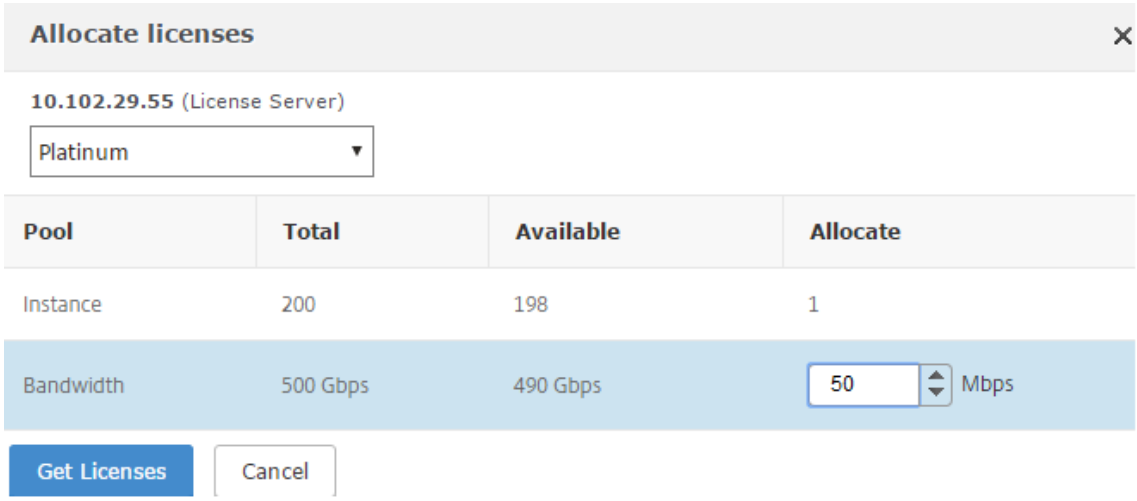
> 注
>
> クラスター内の 1 つ以上のインスタンスが応答しなくなった場合、クラスターは残りのインスタンスの容量でトラフィックを処理し続けます。

ADC プール容量を ADC クラスタに割り当てる

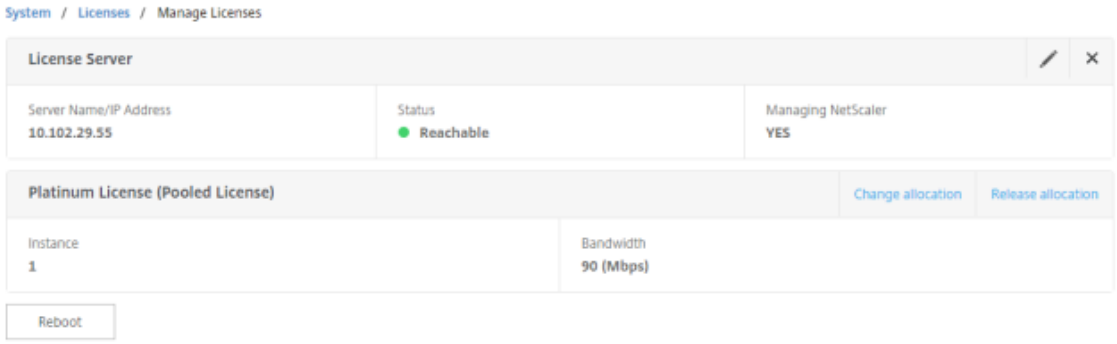
各クラスタノードに個別にライセンスを割り当てます。これは、クラスタノード間でライセンスを伝達および同期するコマンドが無効になっているためです。

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、NetScaler 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. [構成] タブで、[システム] **>** [ライセンス] **>** [ライセンスの管理] に移動します。「新規ライセンスを追加」をクリックし、「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. 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 **NetScaler ADM** に登録する] チェックボックスを選択し、NetScaler ADM の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 Lic**enses] をクリックします。

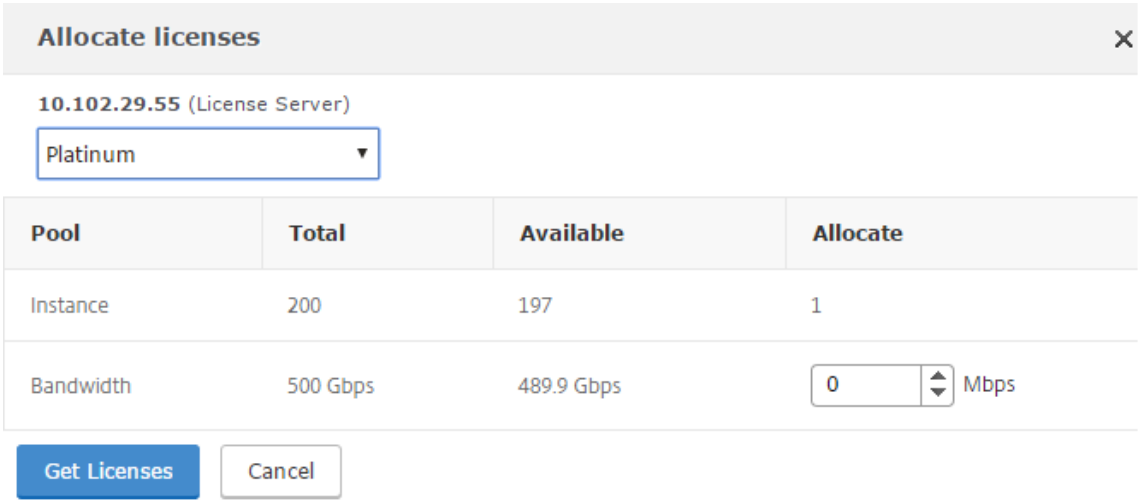


7. [割り当ての変更] または [割り当ての解除] を選択すると、**** ライセンスの割り当てを変更または解除できます **。



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。



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、NetScaler 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。

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    port number >]
<!--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。

```
sh licenseserverpool
<!--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 VPX アプライアンスにライセンスを割り当てるには、次のコマンドを入力します。

```
set capacity  - platform V[S/E/P][Bandwidth]
<!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```


問題が発生したときに予想される動作

February 6, 2024

ライセンスサーバーおよび NetScaler インスタンスで下記の問題が発生した場合の想定動作を以下に示します。

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 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。

NetScaler プールされたインスタンスが応答を停止する

NetScaler Pooled 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 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** プール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 Pooled 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、NetScaler Pooled インスタンスは再起動の完了後に自動的にライセンスをチェックアウトします。

NetScaler プールインスタンスは正常にシャットダウンします

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。NetScaler Pooled インスタンス内のライセンスが、再起動後にライセンスされていないことを確認した場合。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、プールに使用可能な容量がないためにチェックアウトに失敗した場合、NetScaler は NetScaler アプリケーションデリバリーおよび管理プールライセンスのインベントリを確認し、使用可能な容量をチェックします。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。帯域幅プールに使用可能な容量がない場合、プールインスタンスはライセンスなしになります。

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 Pooled インスタンスが正常な状態にあるのに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。

猶予期間

NetScaler Pooled インスタンスが正常な状態で、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。

フレックスライセンスまたはプールライセンスの有効期限が切れて接続の問題が発生するシナリオ

February 6, 2024

このドキュメントでは、NetScaler MPX、NetScaler SDX、および NetScaler VPX/NetScaler BLX/NetScaler CPX におけるライセンスの有効期限切れと接続の問題の動作に関するさまざまなシナリオについて説明します。

フレックスライセンスの種類

- ソフトウェアインスタンス (VPX/BLX/CPX、SDX、MPX、VPX FIPS)
- 帯域幅容量

MPX FIPS は、MPX ソフトウェアプールのライセンスを使用します。SDX FIPS は、SDX ソフトウェアプールのライセンスを使用します。VPX FIPS は、VPX FIPS ソフトウェアプールのライセンスを使用します。

シナリオ**:MPX** フォームファクター

Flexed/Pooled ライセンスを使用していますが、ライセンスはまもなく期限切れになります。次のシナリオでは、有効期限が切れる前後に NetScaler Application Delivery and Management に新しいライセンスをアップロードした場合、またはライセンスファイルが存在しない場合の動作について説明します。

期限が切れる前

期限が切れる前に新しいライセンスをアップロードしても、古いライセンスがまだ有効な場合は、2 つの異なる容量プール (古いものと新しいもの) を使用できます。

- NetScaler が稼働している場合、古いライセンスの有効期限が切れると、新しいフレックス/プールライセンスにシームレスに切り替わります。
- 再起動は不要です。
- NetScaler では、手動で容量を再構成する必要はありません。

期間満了後

この場合、既存のキャパシティプールの有効期限が切れています。

- NetScaler は、再起動するまでライセンス供与され続けます。
- NetScaler が再起動しても有効なライセンスファイルがない場合は、ライセンスなしになります。
- NetScaler が新しいライセンスを引き続き取得する場合は、手動で再構成（容量の再割り当て）する必要があります。

シナリオ**:SDX** フォームファクター

Flexed/Pooled ライセンスを使用していますが、ライセンスはまもなく期限切れになります。次のシナリオでは、有効期限が切れる前後に NetScaler Application Delivery and Management に新しいライセンスをアップロードした場合、またはライセンスファイルが存在しない場合の動作について説明します。

期限が切れる前

期限が切れる前に新しいライセンスをアップロードしても、古いライセンスがまだ有効な場合は、2 つの異なる容量プール (古いものと新しいもの) を使用できます。

- NetScaler が稼働している場合、古いライセンスの有効期限が切れると、新しいフレックス/プールライセンスにシームレスに切り替わります。
- 再起動は不要です。
- NetScaler では、手動で容量を再構成する必要はありません。

期間満了後

この場合、既存のキャパシティプールの有効期限が切れています。

- NetScaler は、再起動するまでライセンス供与され続けます。
- Management Service が再起動しても有効なライセンスファイルがない場合、すべての VPX のスループットは 1 Mbps に低下します。
- Management Service が新しいライセンスを取得できない場合は、手動で再構成（容量の再割り当て）する必要があります。

シナリオ**:VPX/BLX/CPX** フォームファクター

Flexed/Pooled ライセンスを使用していますが、ライセンスはまもなく期限切れになります。次のシナリオでは、有効期限が切れる前後に NetScaler Application Delivery and Management に新しいライセンスをアップロードした場合、またはライセンスファイルが存在しない場合の動作について説明します。

期限が切れる前

期限が切れる前に新しいライセンスをアップロードしても、古いライセンスがまだ有効な場合は、2 つの異なる容量プール (古いものと新しいもの) を使用できます。

- NetScaler が稼働している場合、古いライセンスの有効期限が切れると、新しいフレックス/プールライセンスにシームレスに切り替わります。
- 再起動は不要です。
- NetScaler では、手動で容量を再構成する必要はありません。

期間満了後

この場合、既存のキャパシティプールの有効期限が切れています。

- NetScaler は、再起動するまでライセンス供与され続けます。
- NetScaler が再起動しても有効なライセンスファイルがない場合、VPX と BLX はライセンスなしになり、CPX は CPX Express になります。
- NetScaler が新しいライセンスを引き続き取得する場合は、手動で再構成（容量の再割り当て）する必要があります。

まとめ

次の表は、NetScaler アプリケーションの配信と管理に新しいライセンスが適用されない場合のすべての NetScaler フォームファクターの動作をまとめたものです。

フォームファクター	ライセンスの有効期限が切れた後	NetScaler 再起動後
ボックス/ボックス	再起動するまで実行し続ける	VPX/BLX のライセンスが不要になります
CPX	再起動するまで実行し続ける	CPX が CPX エクスプレスになる
MPX	再起動するまで実行し続ける	MPX がライセンス不要になる
SDX	再起動するまで実行し続ける	すべての VPX のスループットが 1 Mbps に低下します（使用できなくなります）

接続の問題と動作のシナリオ

NetScaler と NetScaler アプリケーションデリバリーおよび管理オンプレミスサーバー間の接続が切断された場合の動作は次のとおりです。

- NetScaler が 30 日間猶予されます。
- この猶予期間中、ライセンス機能は 30 日目まで引き続き機能します。
- 三十一日目に、
  - NetScaler VPX/NetScaler CPX/NetScaler BLX と NetScaler MPX は強制的に再起動され、ライセンスが不要になります。
  - NetScaler SDX 上のすべての VPX のスループットは、1 Mbps に低下します。

NetScaler アプリケーション配信および管理サーバーをフレキシブルライセンスサーバーまたはプールライセンスサーバーとして構成

February 6, 2024

管理者は、NetScaler アプリケーション配信および管理サーバーを Flexed ライセンスサーバーまたは Pooled ライセンスサーバーとしてのみ構成できます。この構成では、NetScaler ADM サーバーは NetScaler インスタンスからライセンスデータのみを受信します。

場合によっては、NetScaler インスタンスのデータが規制区域外に出ないように制限することが規制当局によって義務付けられている場合があります。このような状況では、規制区域に ADM オンプレミス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、分析機能を使用できます。同じ方法でフレキシブルライセンス機能またはプールライセンス機能を使用する場合、フレックスライセンスまたはプールライセンスをさまざまな NetScaler ADM ラ

イセンスサーバーに分割する必要があります。この方法では、グローバルに展開されている NetScaler インスタンス全体に Flexed ライセンスまたは Pooled ライセンスを柔軟に割り当てることができません。

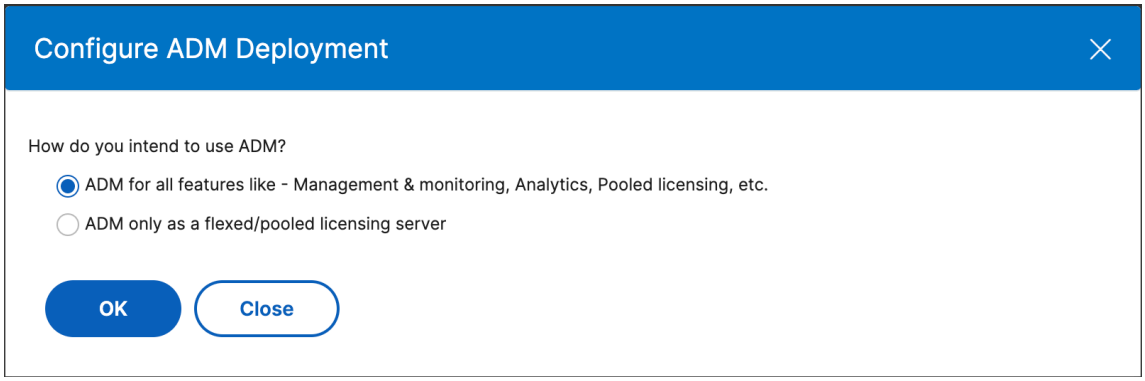
そのため、NetScaler ADM サーバーはフレックスライセンスサーバーまたはプールライセンスサーバーとしてのみ構成してください。NetScaler ADM サーバーは、すべての NetScaler インスタンスからライセンスデータのみを受け取ります。そのため、規制上の義務に従い、グローバルに展開されている NetScaler インスタンス全体にフレキシブルキャパシティライセンスまたはプールキャパシティライセンスを動的に割り当てることができます。

NetScaler ADM サーバーをフレックスライセンスサーバーまたはプールライセンスサーバーとしてのみ構成する方法

開始する前に、NetScaler ADM サーバーに NetScaler インスタンスが追加されていないことを確認してください。NetScaler インスタンスは、手順 4 を完了した後にのみ追加してください。

NetScaler ADM サーバーをフレックスライセンスサーバーまたはプールライセンスサーバー専用に構成するには、次の操作を行います。

1. [設定] **>** [管理] に移動します。
2. [システム構成] セクションで、[システムの展開] を選択します。
3. **ADM Deployment** で、フレックス/プールライセンスサーバーとして **ADM** のみを選択します。



4. [**OK**] をクリックします。

   この操作では、Flexed ライセンス機能または Pooled ライセンス機能のみが保持され、次の NetScaler ADM 機能が無効になります。

   - NetScaler 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:
>
> デフォルトでは、NetScaler 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。

NetScaler ADM GUI には、フレックスライセンス機能またはプールライセンス機能のみが表示されるようになりました。また、残りのフィーチャは表示されません。

5. ライセンス機能のみを対象に NetScaler ADM を構成したら、[インフラストラクチャ] > [インスタンス] ページで NetScaler インスタンスを追加します。

> 注
>
> - 1 つまたは複数の NetScaler ADM サーバーに NetScaler インスタンスを追加できます。このような NetScaler インスタンスのパスワードを変更する場合は、インスタンスが検出されたすべての NetScaler ADM サーバーでパスワードを更新してください。
> - ユーザーは、NetScaler ADM GUI で無効になっている機能の一部の操作を引き続き実行できます。たとえば、イベントポーリングや NetScaler 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したい場合は、適切なアクセスポリシーを使用して他の管理者のユーザーアクセスを無効にしてください。詳しくは、「NetScaler ADM でのアクセスポリシーの構成」を参照してください。

ネットスケーラー **VPX** および **NetScaler BLX** ライセンスのチェックインとチェックアウト

February 6, 2024

NetScaler VPX および NetScaler BLX のライセンスは、「NetScaler アプリケーションの配信と管理」から必要に応じて NetScaler インスタンスに割り当てることができます。NetScaler ADM ソフトウェアはライセンスを保存および管理します。ライセンスフレームワークには、スケーラブルで自動化されたライセンスプロビジョニングを提供するライセンスフレームワークがあります。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 を実行する NetScaler VPX イメージを使用していること。
  例：NSVPX-ESX-12.0-xx.xx_nc.zip

- バージョン 12.0 を実行する NetScaler ADM がインストールされました。
  例:MAS-ESX-12.0-xx.xx.zip

> 注
>
> 既存の NetScaler VPX ライセンスを NetScaler ADM で管理するには、ライセンスを NetScaler ADM に再ホストする必要があります。

NetScaler ADM へのライセンスのインストール

> 注:
>
> ソフトウェアエディションまたは帯域幅を変更した場合は、ライセンスをインストールする前に、NetScaler ADM 仮想アプライアンスを再起動してください。

NetScaler ADM にライセンスファイルをインストールするには:

1. Web ブラウザーで、NetScaler ADM 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. [インフラストラクチャー**] > [**プールライセンス] に移動します。
4. 「ライセンスファイル」セクションで、次の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。

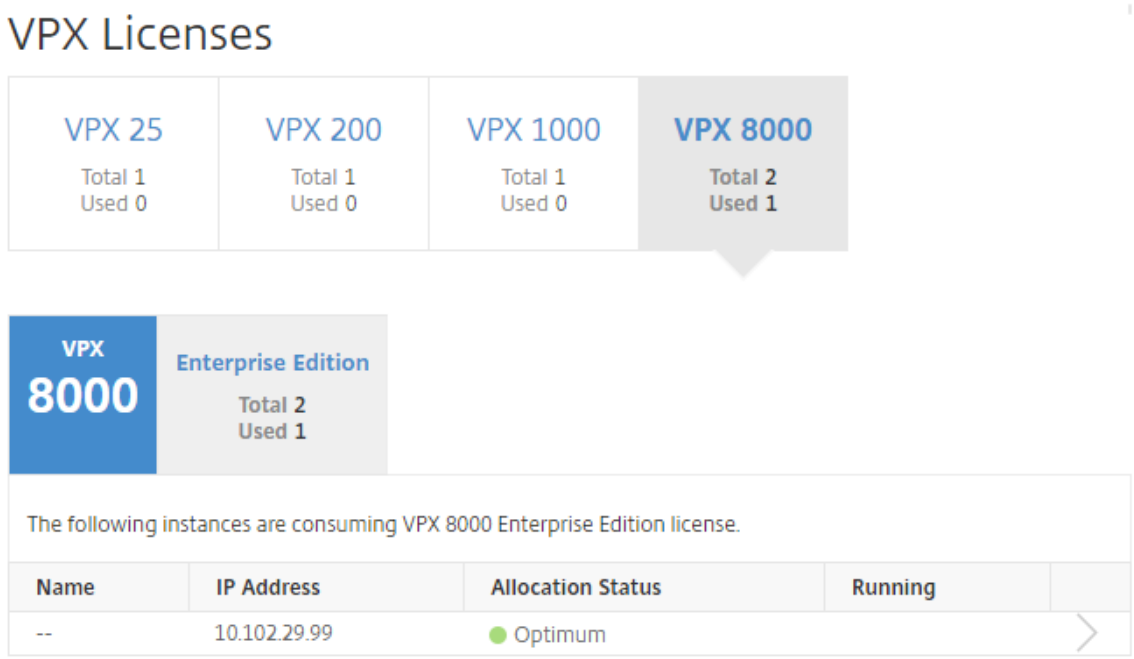
   ライセンス設定ページからいつでも **NetScaler ADM** にライセンスを追加できます。

確認

NetScaler ADM GUI で、使用可能なライセンスと割り当てられているライセンスを表示できます。

ライセンスを表示するには**:**

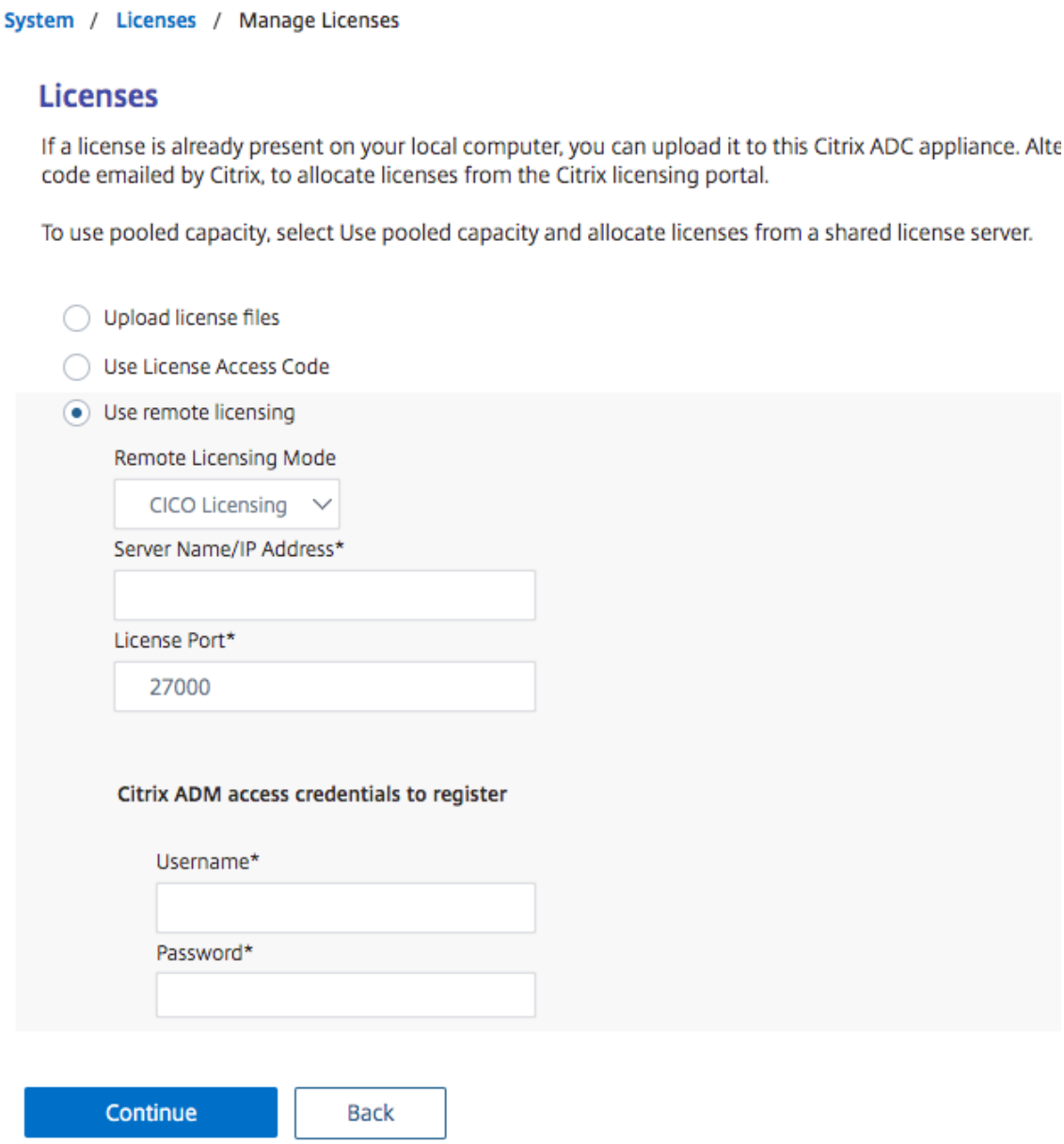
1. Web ブラウザで、NetScaler ADM IP アドレス（例：http://192.168.100.1）を入力します。
2. ［**User Name**］と ［**Password**］に管理者の資格情報を入力します。
3. [構成] タブで、[インフラストラクチャ**] > [**プールライセンス**] > [VPX** ライセンス] に移動します。



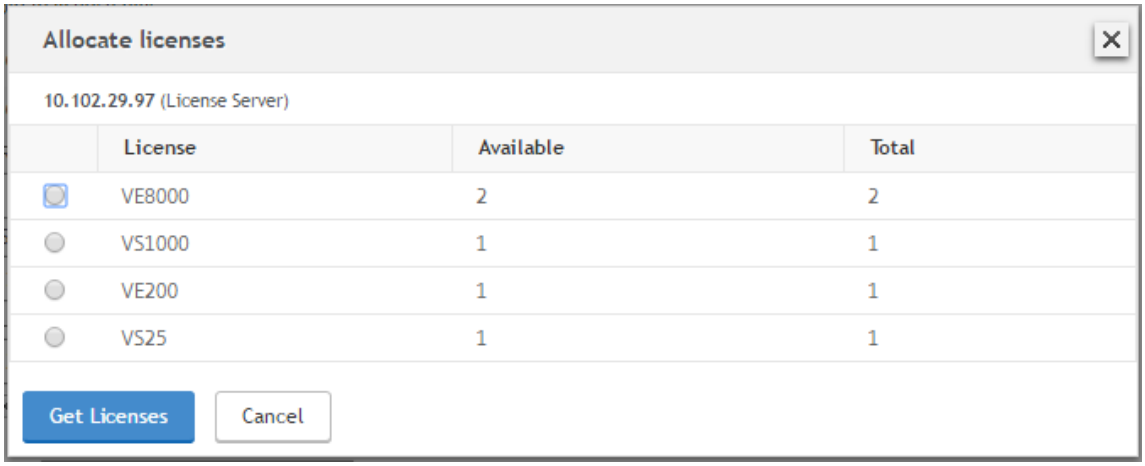
4. 割り当て済みのライセンスは、利用可能なライセンスのセクションの下の表で表示できます。

NetScaler GUI を使用して **NetScaler VPX** および **NetScaler BLX** ライセンスを **NetScaler** インスタンスに割り当てます

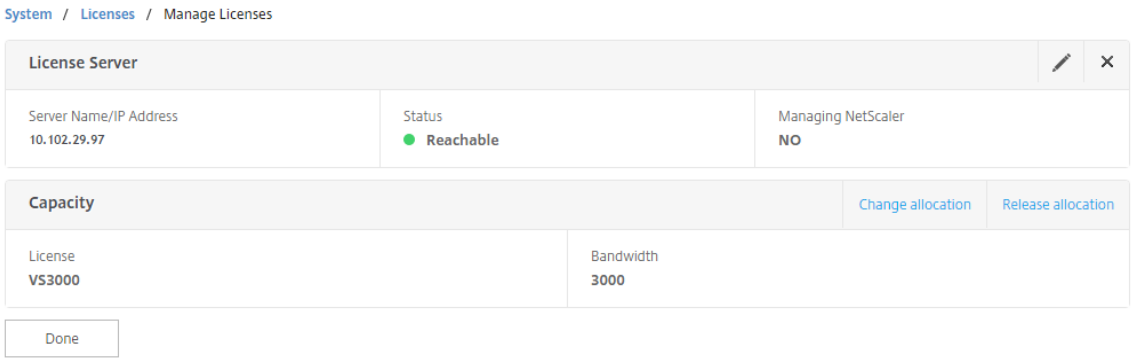
1. Web ブラウザで、NetScaler インスタンスの IP アドレス（例：http://192.168.100.1）を入力します。
2. ［**User Name**］と ［**Password**］の各フィールドに管理者の資格情報を入力します。
3. [構成] タブで、[設定**] > [**ライセンス**] > [**ライセンスの管理] に移動し、[新しいライセンスの追加] をクリックし、[リモートライセンスの使用**] > [CICO** ライセンス] を選択します。
4. 「サーバー名**/IP** アドレス」フィールドにライセンスサーバーの詳細を入力します。
5. [ユーザー名 **] **** と **[**** パスワード] に NetScaler ADM 資格情報を入力し、[続行] をクリックします。



6. 必要な帯域幅のライセンスエディションを選択し、[**Get Lic**enses] をクリックします。



7. [再起動] をクリックすると、NetScaler インスタンスが再起動します。
8. 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。



9. [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 CLI を使用して、**NetScaler VPX** および **NetScaler BLX** ライセンスを **NetScaler** インスタンスに割り当てます

1. SSH クライアントで、NetScaler インスタンスの IP アドレスを入力し、管理者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。

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    port number >]
<!--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。

```
sh licenseserverpool
<!--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 アプライアンスにライセンスを割り当てるには、次のコマンドを入力します。

```
set capacity  -platform V[S/E/P][Bandwidth]
<!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

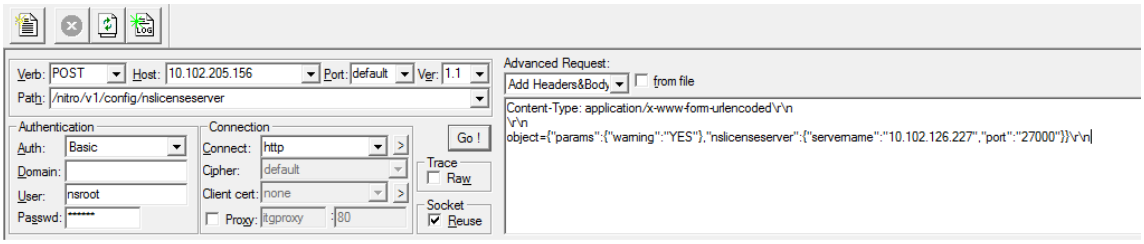
API を使用して **NetScaler VPX** ライセンスと **NetScaler BLX** ライセンスを **NetScaler** インスタンスに割り当てる

Web ブラウザーまたは API クライアントで、管理者の資格情報を使用して NetScaler 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。

```
content-type: application/x-www-form-urlencoded\r\n
\r\n
object= {
  “params” ;{
 warning” :” yes”  }
 ,” nslicensing server” ;{
 servername” :” <NetScaler ADM IP>” ,  “port” :” 27000”  }
  }
 \r\n
<!--NeedCopy-->
```

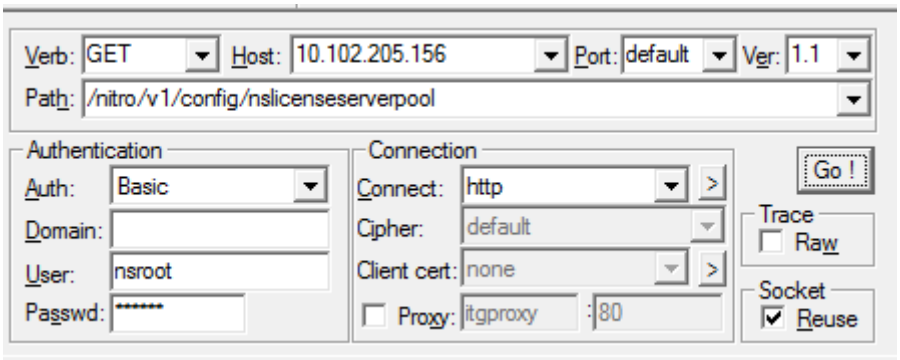


NetScaler ADM は要求に応答します。次のサンプル応答は、成功を示しています。

```
RESPONSE: **************\n
HTTP/1.1 201 Created\r\n
Date: Fri, 06 Jan 2017 19:03:21 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: 57\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "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。



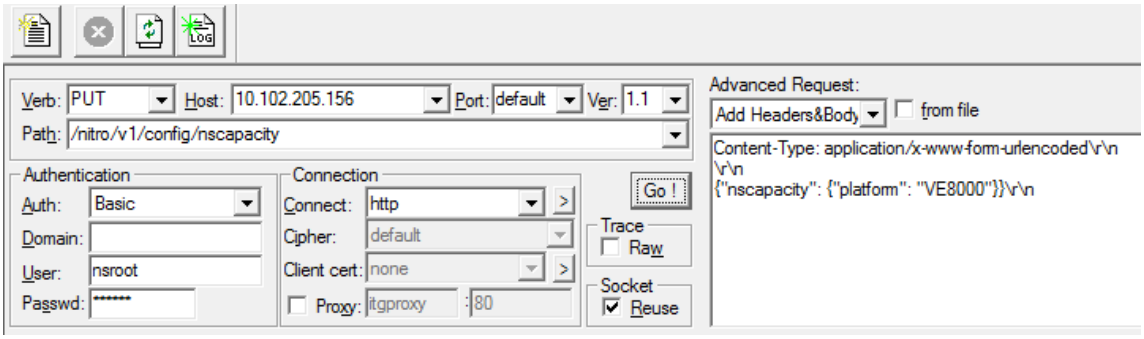
NetScaler ADM は要求に応答します。次のサンプル応答は成功と、ライセンスサーバーで利用可能なライセンスの一覧を示しています。

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
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE", "nslicenseserverpool": { "instancetotal": 0, "instanceavailable": 0, "standardbandwidthtotal":
0, "standardbandwidthavailable": 0, "enterprisebandwidthtotal": 0, "enterprisebandwidthavailable": 0, "platinumbandwidthtotal": 0, "platinumbandwidthav
ailable": 0, "cpxinstancetotal": 0, "cpxinstanceavailable": 0, "vpx1stotal": 0, "vpx1savailable": 0, "vpx1ptotal": 0, "vpx1pavailable": 0, "vpx5stotal"
: 0, "vpx5savailable": 0, "vpx5ptotal": 0, "vpx5pavailable": 0, "vpx10stotal": 0, "vpx10savailable": 0, "vpx10etotal": 0, "vpx10eavailable": 0, "vpx10p
total": 0, "vpx10pavailable": 0, "vpx25stotal": 0, "vpx25savailable": 0, "vpx25etotal": 0, "vpx25eavailable": 0, "vpx25ptotal": 0, "vpx25pavailable": 0
, "vpx50stotal": 0, "vpx50savailable": 0, "vpx50etotal": 0, "vpx50eavailable": 0, "vpx50ptotal": 0, "vpx50pavailable": 0, "vpx100stotal": 0, "vpx100sav
ailable": 0, "vpx100etotal": 0, "vpx100eavailable": 0, "vpx100ptotal": 0, "vpx100pavailable": 0, "vpx200stotal": 0, "vpx200savailable": 0, "vpx200etota
l": 0, "vpx200eavailable": 0, "vpx200ptotal": 0, "vpx200pavailable": 0, "vpx500stotal": 0, "vpx500savailable": 0, "vpx500eto
tal": 0, "vpx500eavailable": 0, "vpx500ptotal": 0, "vpx500pavailable": 0, "vpx1000stotal": 0, "vpx1000savailable": 0, "vpx1000etotal": 0, "vpx1000eavail
able": 0, "vpx1000ptotal": 0, "vpx1000pavailable": 0, "vpx2000ptotal": 0, "vpx2000pavailable": 0, "vpx3000stotal": 0, "vpx3000savailable": 0, "vpx3000e
total": 0, "vpx3000eavailable": 0, "vpx3000ptotal": 0, "vpx3000pavailable": 0, "vpx4000ptotal": 0, "vpx4000pavailable": 0, "vpx5000stotal": 0, "vpx5000
savailable": 0, "vpx5000etotal": 0, "vpx5000eavailable": 0, "vpx5000ptotal": 0, "vpx5000pavailable": 0, "vpx8000stotal": 1, "vpx8000savailable": 1, "vp
x8000etotal": 2, "vpx8000eavailable": 1, "vpx8000ptotal": 1, "vpx8000pavailable": 1 } }
finished.

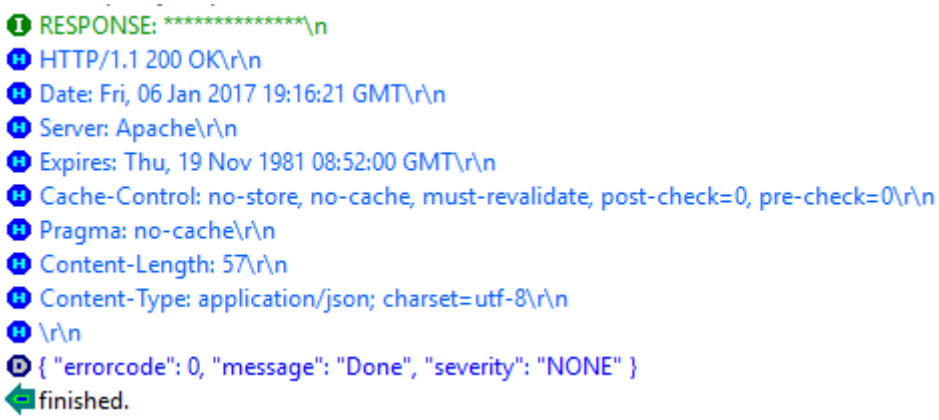
NetScaler アプライアンスにライセンスを割り当てるには:

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。

```
content-type: application/x-www-form-urlencoded\r\n
\r\n
{
  “nscapacity:{
  “platform” :” VE8000”  }
  }
 \r\n
<!--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。



ライセンスサーバーの **IP** アドレスを更新する

NetScaler VPX および NetScaler 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、データを失っ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ている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。詳しくは、「NetScaler GUI を使用して NetScaler VPX および NetScaler BLX ライセンスを NetScaler インスタンスに割り当てる」を参照してください。

NetScaler VPX および **NetScaler BLX** の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の設定

NetScaler VPX および NetScaler 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 で表示できます。

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. [インフラストラクチャー**] > [**プールライセンス] 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。管理者に通知するために使用するプールライセンス容量の割合を設定できます。
4. 適切なチェックボックスを選択して、送信する通知の種類を選択します。通知の種類を次に示します。
    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、通知を送信するタイミングを、ライセンスの有効期限までの日数で指定します。
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 VPX ライセンスは、インスタンスによる帯域幅消費に基づいて割り当てられていました。NetScaler VPX は、バインドされているライセンスエディションに基づいて、特定の帯域幅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。シナリオによっては、帯域幅要件が少なくても、SSL TPS や圧縮スループットなど、他の L7 パフォーマンスの要件が高くなる場合があります。このような場合、NetScaler VPX ライセンスのアップグレードは適切ではない可能性があります。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 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 VPX は、システムで実行されている CPU の数に応じてライセンスをチェックアウトします。NetScaler VPX は、ライセンス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。

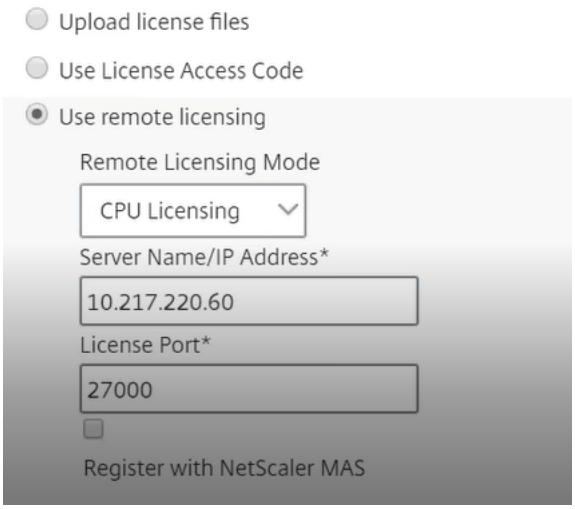
プールライセンス容量や CICO ライセンス機能と同様に、NetScaler ADM ライセンスサーバーは個別の仮想 CPU ライセンスセットを管理します。また、仮想 CPU ライセンスで管理されているエディションは、スタンダード、アドバンス、プレミアムの 3 つです。これらのエディションは、帯域幅ライセンスのエディションでロック解除された機能と同じ機能のセットをロック解除します。

仮想 CPU の数が変更されたり、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 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:

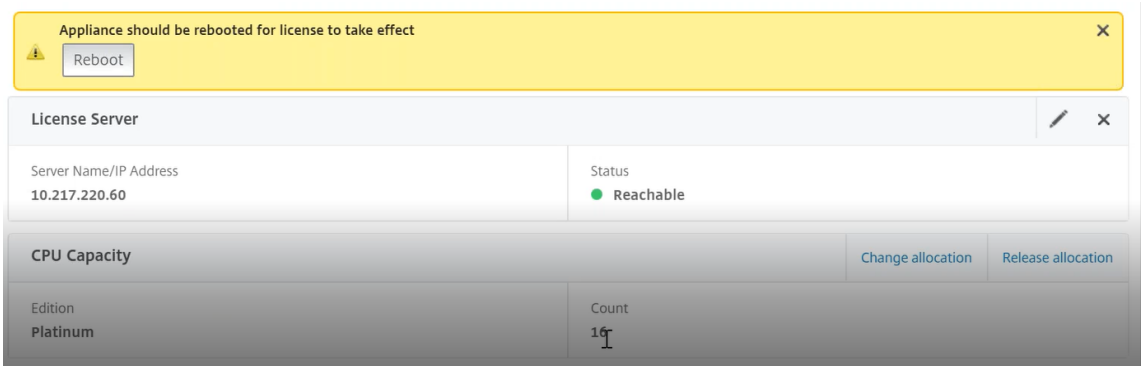
1. NetScaler VPX で、[システム**] > [**ライセンス**]** に移動し、**[**ライセンスの管理] をクリックします。
2. ライセンスページで、「新規ライセンスを追加」をクリックします。
3. ライセンスページで、「リモートライセンスを使用する **」オプションを選択します。
4. **** リモートライセンスモードリストから CPU**** ライセンスを選択します。
5. ライセンスサーバーの IP アドレスとポート番号を入力します。

6. [続行] をクリックします。



> 注
>
> :NetScaler VPX インスタンスは常に NetScaler ADM に登録する必要があります。まだ行っていない場合は、「NetScaler **ADM** への登録」を有効にして、**NetScaler ADM** のログイン認証情報を入力します。

7. [ライセンスの割り当て] ウィンドウで、ライセンスの種類を選択します。このウィンドウには、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。
8. 次のページで [再起動] をクリックしてライセンスを申請します。



> 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、インスタンスですでに Standard エディションのライセンスを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 を使用して **NetScaler VPX** ライセンスでライセンスサーバーを構成する

NetScaler VPX コンソールで、次のコマンドを入力して次の 2 つのタスクを実行します。

1. ライセンスサーバーを NetScaler ADC VPX に追加するには:

```
add licenseserver <IP address of the license server>
<!--NeedCopy-->
```

2. ライセンスを申請するには:

```
set capacity -vcpu - edition premium
<!--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。

```
reboot -w
<!--NeedCopy-->
```

ライセンスサーバーの **IP** アドレスを更新する

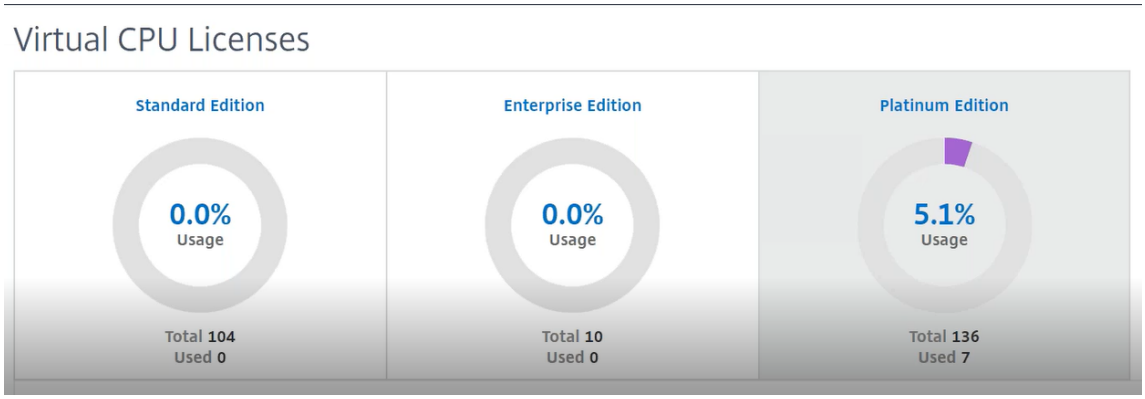
NetScaler VPX インスタンスのライセンスサーバーの IP アドレスは、インスタンスに割り当てられたライセンス帯域幅に影響を与えたり、データを失ったりすることなく更新できます。ライセンスサーバーの IP アドレスを更新するには、NetScaler VPX インスタンスで次のコマンドを入力します。

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

このコマンドは、新しいサーバーに接続し、以前のライセンスサーバーに関連付けられている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. NetScaler ADM で、[インフラストラクチャ**] > [**プールされたライセンス**] > [**プールされた **VCPU**] に移動します。
2. このページには、各ライセンスエディション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。



NetScaler CPX 用の仮想 **CPU** ライセンス

NetScaler CPX インスタンスをプロビジョニングするときに、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 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 CPX は、起動時にライセンスサーバーからライセンスをチェックアウトします。NetScaler CPX がシャットダウンすると、ライセンスはライセンスサーバーにチェックインされます。

NetScaler CPX イメージは、「docker pull」コマンドを使用して Quay コンテナレジストリからダウンロードし 、環境にデプロイできます。

NetScaler CPX のライセンスには、次の 3 つのライセンスタイプがあります。

1. NetScaler CPX および VPX でサポートされる仮想 CPU サブスクリプションライセンス
2. プールキャパシティライセンス
3. 単一から複数の仮想 CPU をサポートする CP1000 ライセンスは、NetScaler CPX のみを対象としています

NetScaler 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 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。NetScaler CPX は 1 コアから 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。

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
   -e EULA=yes -e CPX_CORES=2
<!--NeedCopy-->
```

NetScaler 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。

```
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
<!--NeedCopy-->
```

各項目の意味は次のとおりです。

- *<LS_IP_ADDRESS>* は NetScaler ライセンスサーバーの IP アドレスです。
- *<LS_PORT>* は 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 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。NetScaler CPX インスタンスは、インスタンスが「n」個の CPU で実行されている場合、「n」

> 個のライセンスをチェックアウトします。

NetScaler CPX インスタンスのプロビジョニング中に **NetScaler** プールキャパシティまたは **CP1000** ライセンスを構成するには:

プールライセンス（帯域幅ベース）または NetScaler CPX プライベートプール（CP1000 またはプライベートプールベース）を使用して NetScaler CPX インスタンスのライセンスをチェックアウトする場合は、それに応じて環境変数を指定する必要があります。

例:

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
    LS_PORT> -e PLATFORM=CP1000 cpx:11.1
<!--NeedCopy-->
```

CP1000. このコマンドは、CP1000 プール（NetScaler CPX プライベートプール）からのチェックアウトをトリガーします。次に、NetScaler CPX インスタンスは、CPX_CORES に指定された「n」個のコアに対して「n」個のインスタンスを取得します。最も一般的な使用例は、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。マルチコアの NetScaler CPX ユースケースでは、「n」個の vCPU（「n」は 1 から 7 まで）を確認してください。

```
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
<!--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、NetScaler CPX は最大 2000 Mbps で実行できます。プールライセンスでは、最初の 1000 Mbps は課金されません。

> 注
>
> : 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

システム設定の管理

February 6, 2024

次の表に、**[設定] > [管理]** で使用できるオプションの一覧を示します。

ネットワーク構成

ネットワーク構成	オプション	説明
IP アドレス、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
	2 つ目の NIC	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、「NetScaler ADM にアクセスするためのデュアル NIC の構成」を参照してください。
	ホスト名	NetScaler ADM にホスト名を割り当てることができます。詳しくは、「NetScaler ADM サーバーにホスト名を割り当てる」を参照してください。
	プロキシサーバー	ADM をプロキシサーバとして設定できます。詳しくは、「API プロキシサーバーとしての NetScaler ADM」を参照してください。
静的ルート		静的ルートを構成して、NetScaler ADM と NetScaler VPX インスタンス間の接続を確立できます
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、「NTP サーバーの構成」を参照してください。

ネットワーク構成	オプション	説明
ADM ポート情報		ADM インスタンスと ADC インスタンス間の通信用にどのポートを開いておく必要があるかを理解できます。詳細については、「サポートされるポート」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	`nsrecover` ログインの有効化、セッションタイムアウトの有効化など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。
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、「データガバナンス」を参照してください。

システム構成	オプション	説明
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、「アップグレード」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、「ディザスタリカバリを構成する」を参照してください。

データプルーニング

データプルーニング	オプション	説明
システムとインスタンスのデータプルーニング	システム	NetScaler ADM サーバーデータベースに保存されるレポートデータの量を制限できます。詳細については、「システム削除設定の構成」を参照してください。
	インスタンスイベント	NetScaler 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、「インスタンスの Syslog プルーニング設定の構成」を参照してください。

データプルーニング	オプション	説明
	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、「システムバックアップ設定」を参照してください。
	インスタンス	NetScaler ADM 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、「インスタンスバックアップ設定の構成」を参照してください。

イベント通知

イベント通知	オプション	説明
イベント通知とダイジェストの設定	イベント通知	複数のシステム関連機能について、選択したユーザーグループに通知を送信できます。これらのシステムの機能は SystemReboot、StatusPoll、SystemState といったイベントのカテゴリ別に整理されています。NetScaler Application Delivery Management（ADM）は、電子メール、SMS、または Slack のいずれかを介して通知を送信するように構成できます。これにより、データストレージの容量超過やバックアップ障害など、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。
	イベントダイジェスト	重要なシステムイベントと機能イベントの統合レポートを取得できます

SSL 設定

SSL 設定	説明
SSL 証明書のインストール	SSL 証明書と SSL キーファイルをインストールできます
SSL 証明書を表示	SSL 証明書の詳細を表示できます
SSL 設定の構成	詳細については、「SSL 設定の構成」を参照してください。
SSL 証明書	SSL 証明書または SSL キーファイルをアップロード、ダウンロード、または削除できます
暗号グループ	詳細については、「暗号グループの構成」を参照してください。

機能の構成

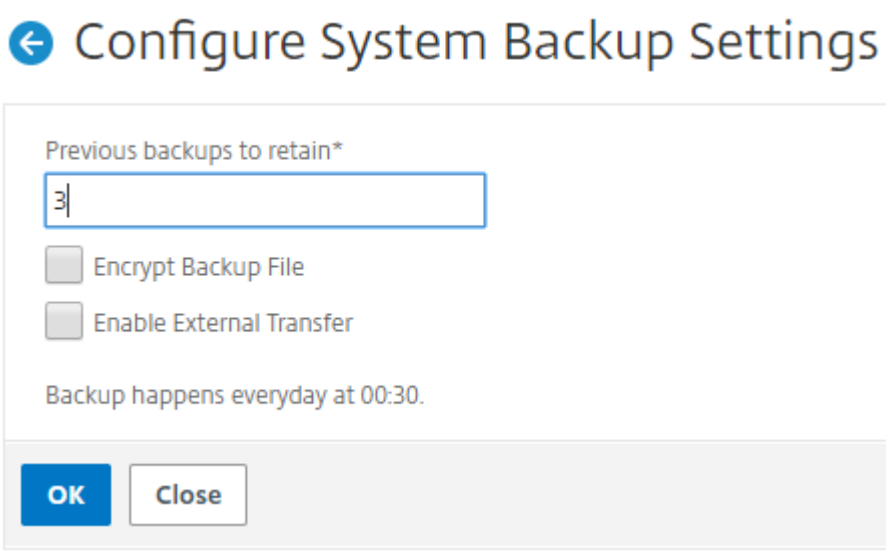
機能の構成	説明
機能の無効化または有効化	NetScaler ADM の機能を有効または無効にすることができます。詳しくは、「ADM 機能の有効化または無効化」を参照してください。

システムバックアップの設定を構成する

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. [設定**] >** [管理] に 移動します。[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。
2. [バックアップ**] > [**システム] ページで、以下を指定します。
   - 以前のバックアップは保持しておいてください。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を暗号化するには、「バックアップファイルを暗号化」を選択します。
   - バックアップファイルのコピーを別のシステムに転送するには、**[**外部転送を有効にする] を選択します。構成を復元する場合は、まずファイルを NetScaler 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。



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。

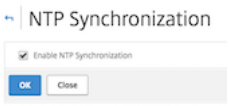
NetScaler ADM で **NTP** サーバーを構成するには:

1. [設定**] > [NTP** サーバ] に移動し、[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（2^6 で表すことができる）にするには、6 を入力します。
   - **Minimum 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. [設定] **> [NTP** サーバ**]** に移動します。
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。



> 注: NTP ログメッセージは、`/var/log/ntpd.log` ファイルファイル内の /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。

NetScaler ADM をアップグレードするには:

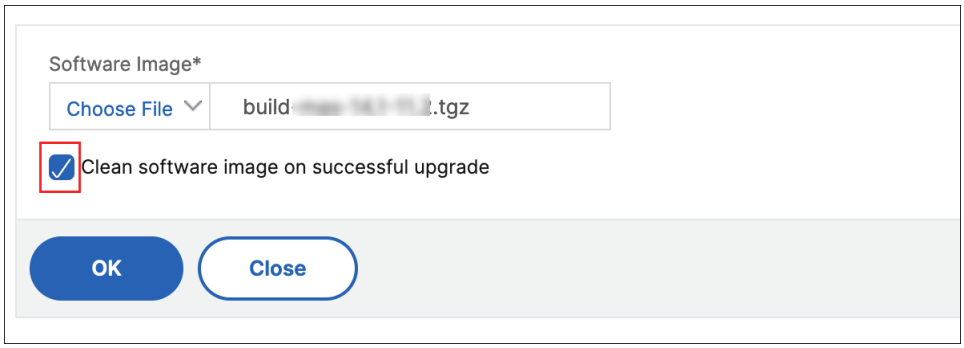
1. [設定] **>** [管理] に移動します。[システムメンテナンス] で、[**NetScaler ADM** のアップグレード] をクリックします。

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。



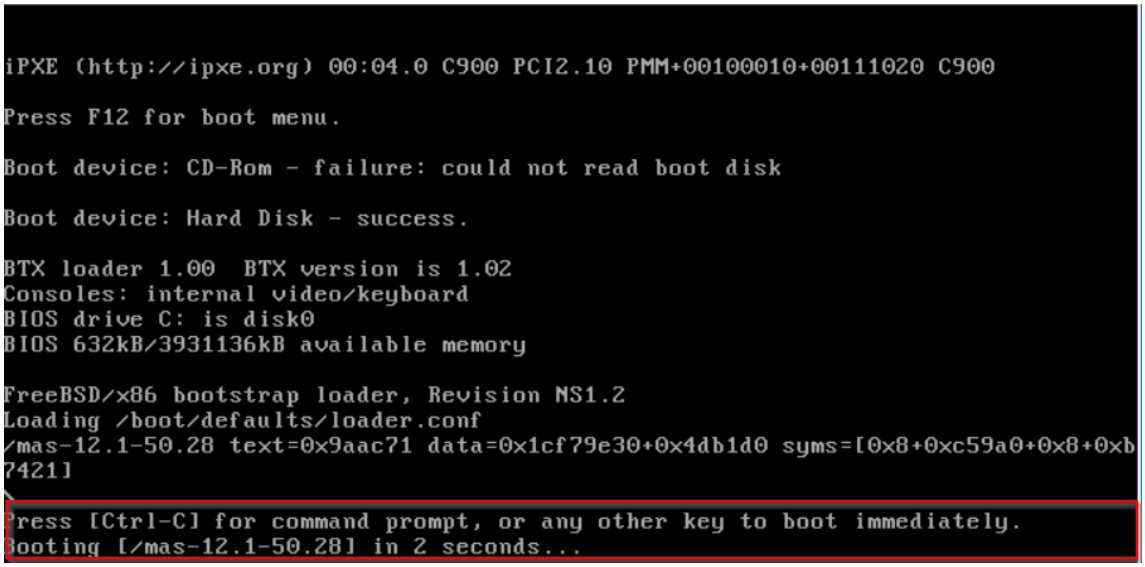
NetScaler ADM パスワードをリセットする方法

February 6, 2024

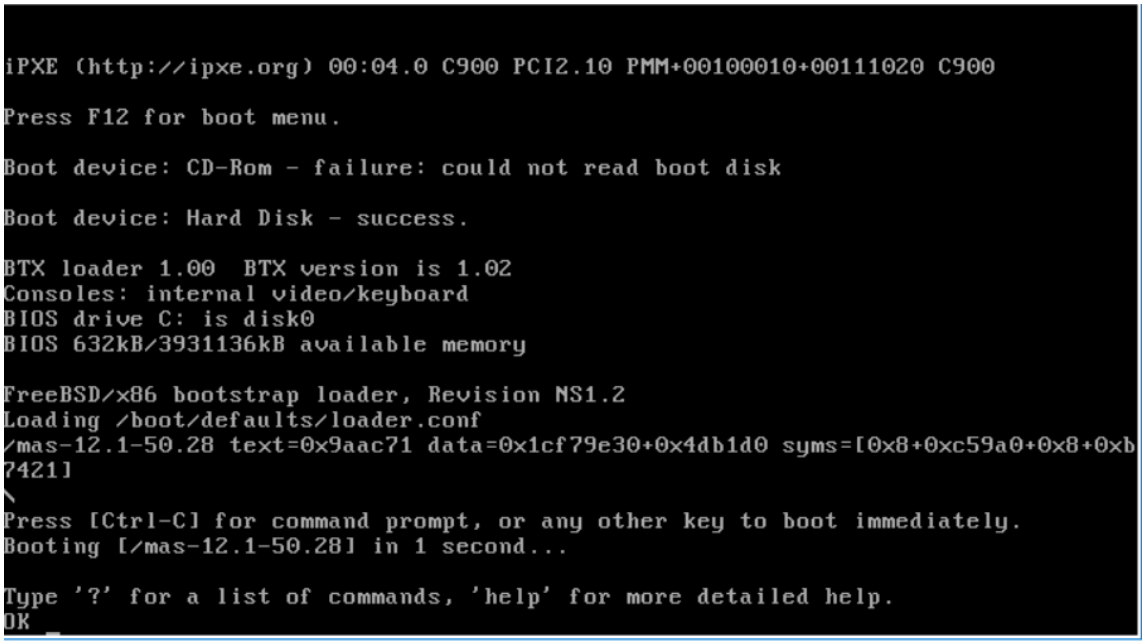
NetScaler ADM のパスワードをリセットする手順は、ホストされているハイパーバイザーによって異なる場合があります。デフォルトのパスワードを変更し、デフォルトのパスワードにリセットしたい場合は、NetScaler ADM ノードを再起動してパスワードをリセットできます。

XenCenter を使用する **Citrix Hypervisor**:

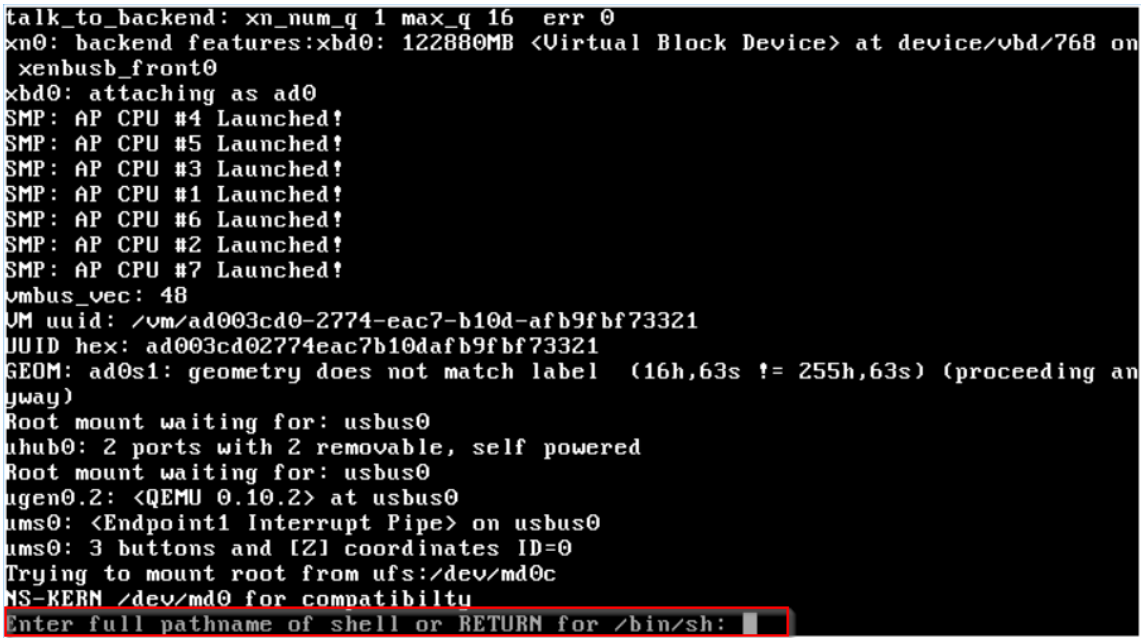
1. XenCenter を使用して Citrix Hypervisor にログオンします。
2. NetScaler ADM ノードを選択して右クリックし、「再起動」を選択します。
3. ** コンソールタブで **CTL+C** を押してブートシーケンスを中断します ** 。



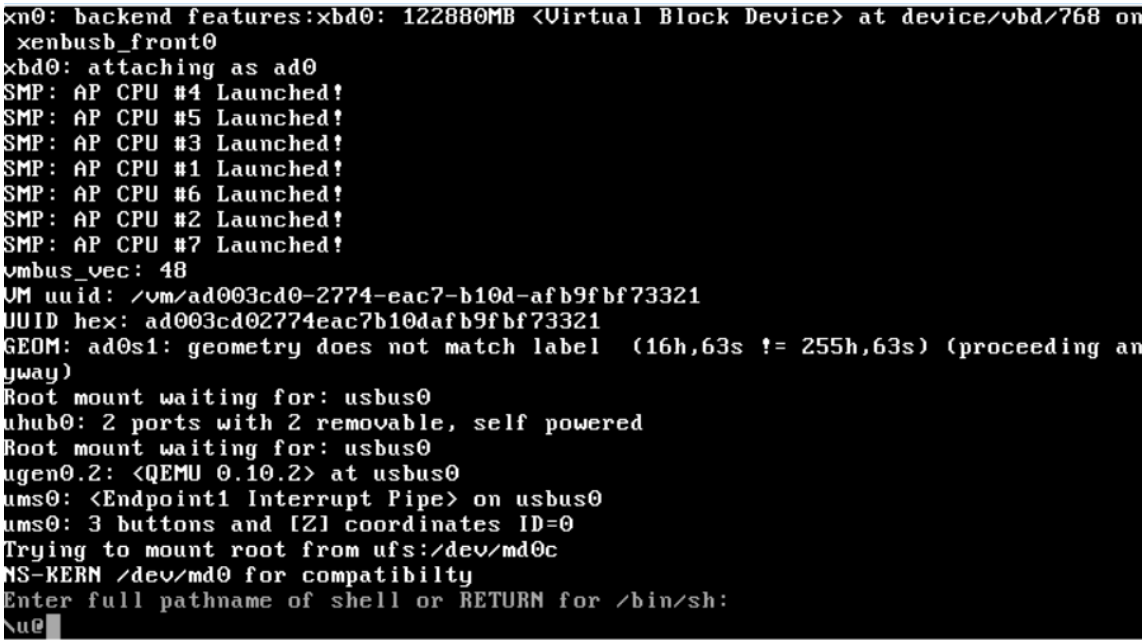
4. OK プロンプトで **boot-s** コマンドを実行します。



NetScaler ADM が再起動し、次のメッセージが表示されます。

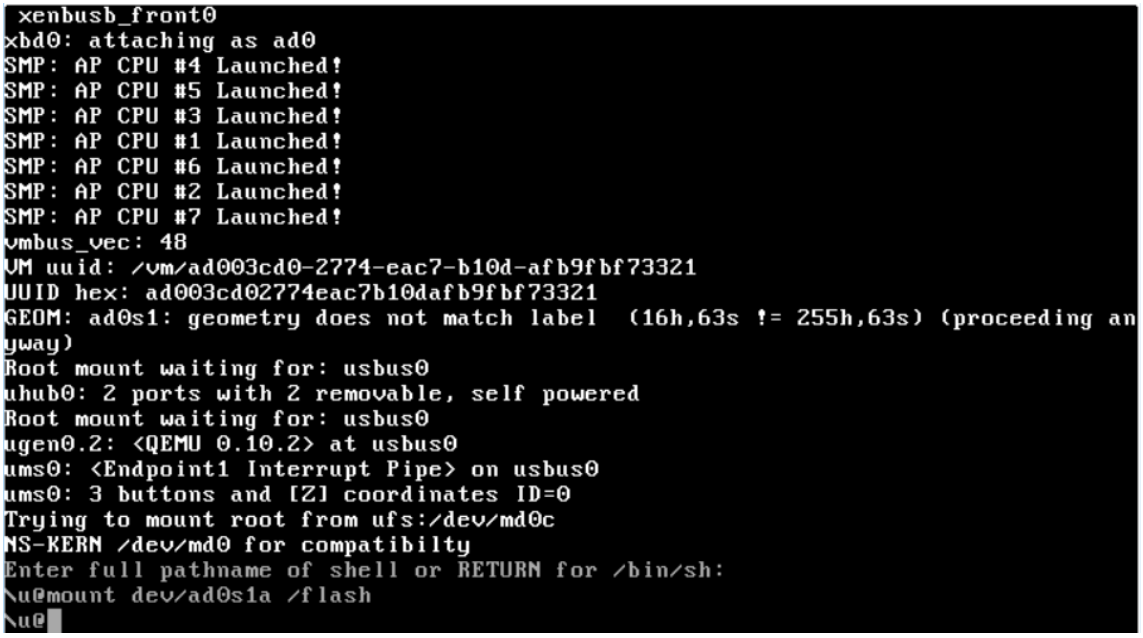


5. **Enter** キーを押して /u @ プロンプトを表示します。



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
```

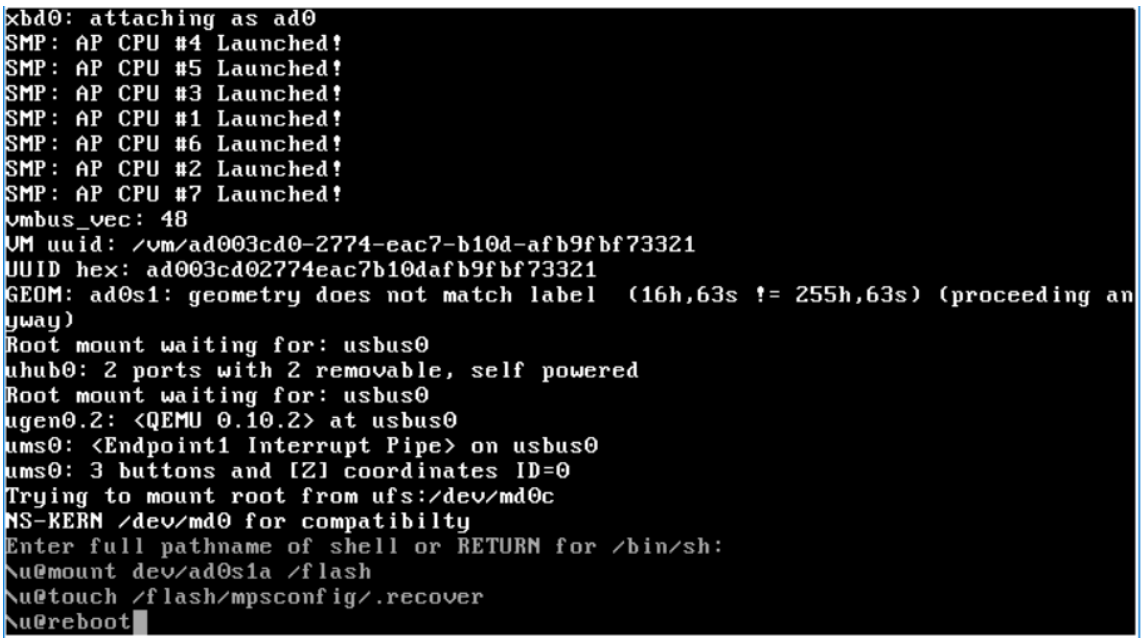



7. 次のコマンドを使用してファイルを作成します。

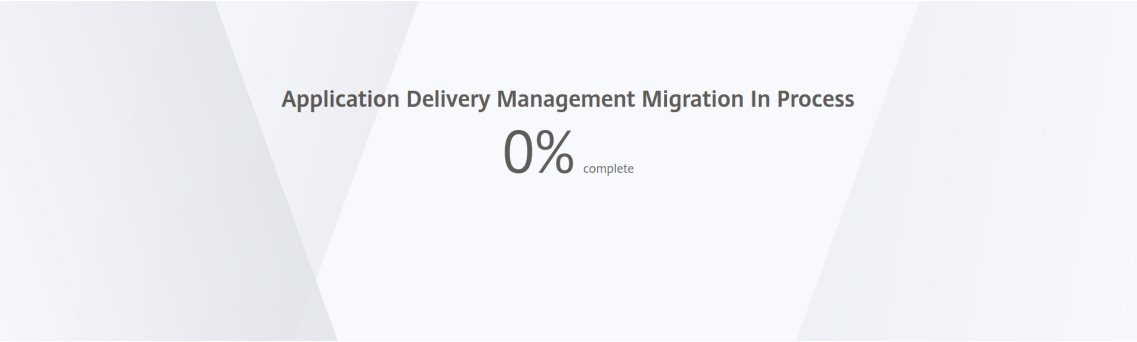
   ```
   touch /flash/mpsconfig/.recover
   ```

   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。

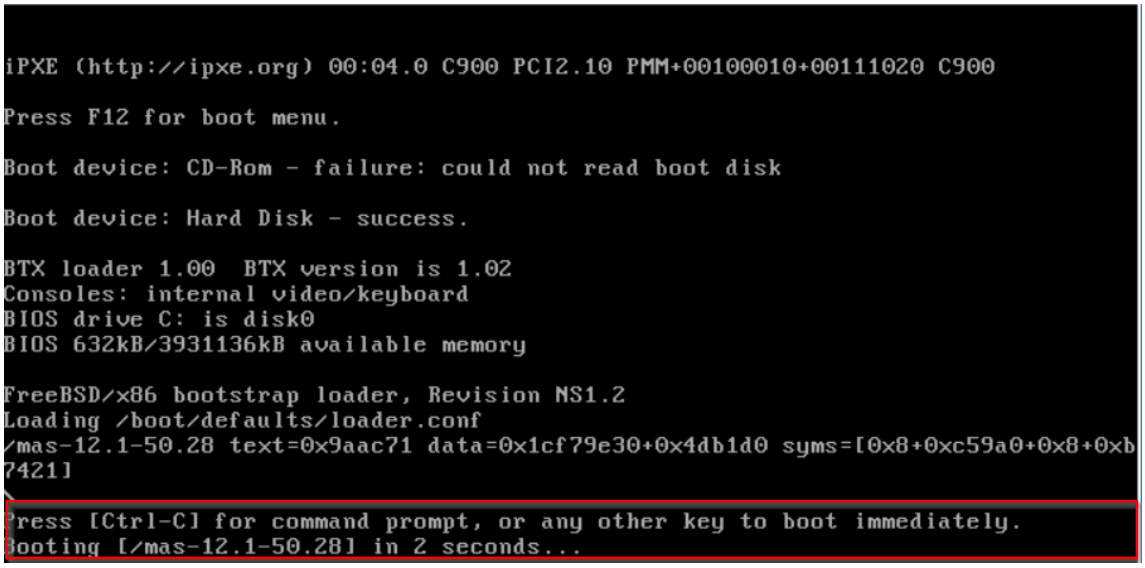


nsro *ot/nsroot* 認証情報を使用して GUI からログオンし、*nsrecover/nsroot* を使用して Hypervisor からログオンできるようになりました。

> 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 ** 。



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。

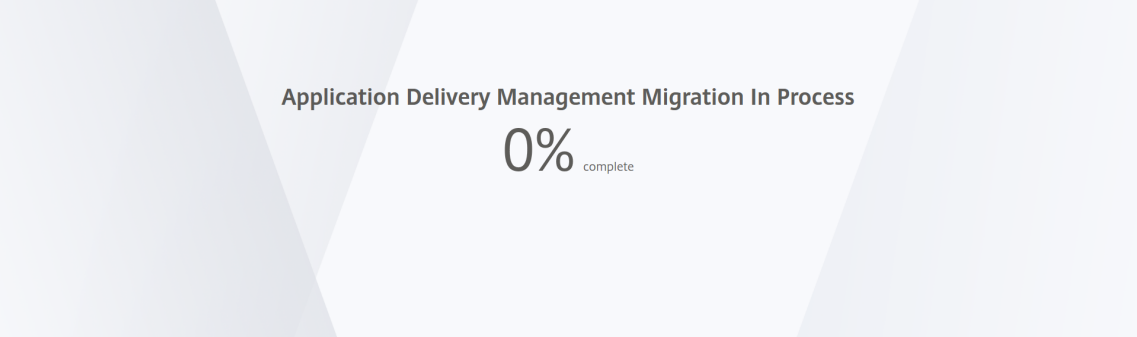
5. **Enter** キーを押して /u @ プロンプトを表示します。
6. 次のコマンドを使用して、フラッシュパーティションをマウントします。

   ```
   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。

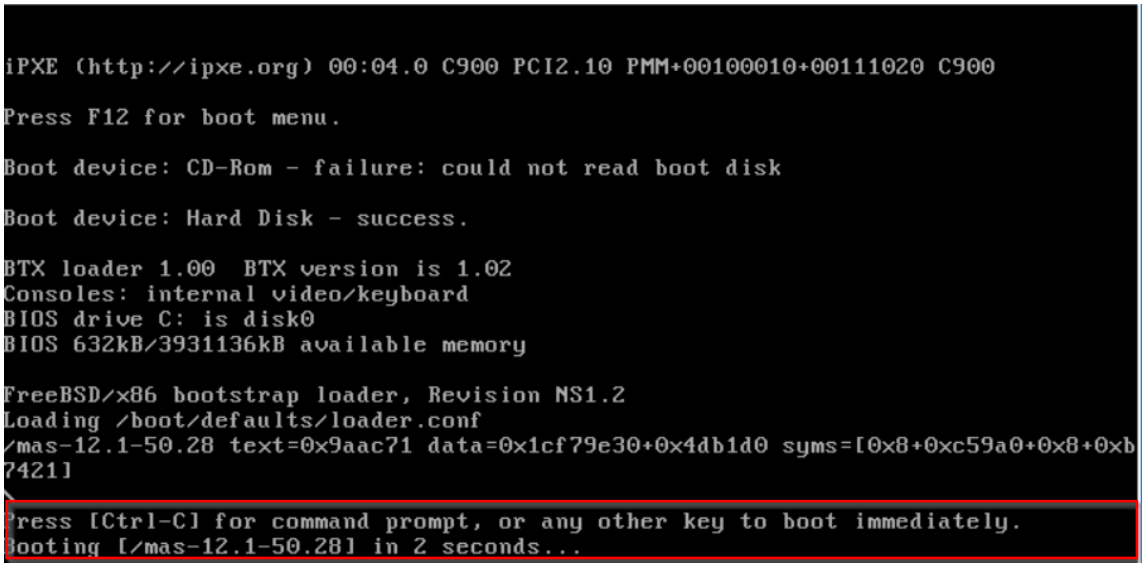


   nsro *ot/nsroot* 認証情報を使用して GUI からログオンし、*nsrecover/nsroot* を使用して ESX サーバからログオンできるようになりました。

   > 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 **** 。



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。

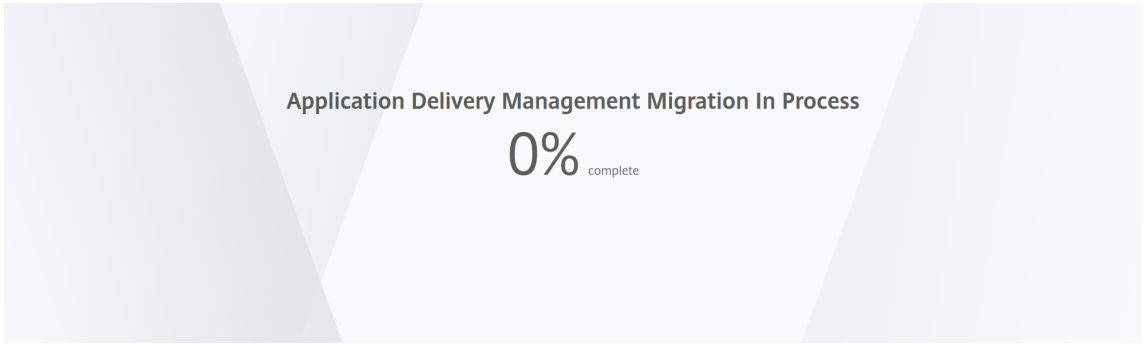
   ```
   mount dev/ad0s1a /flash
   ```

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。



   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 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'
   ```

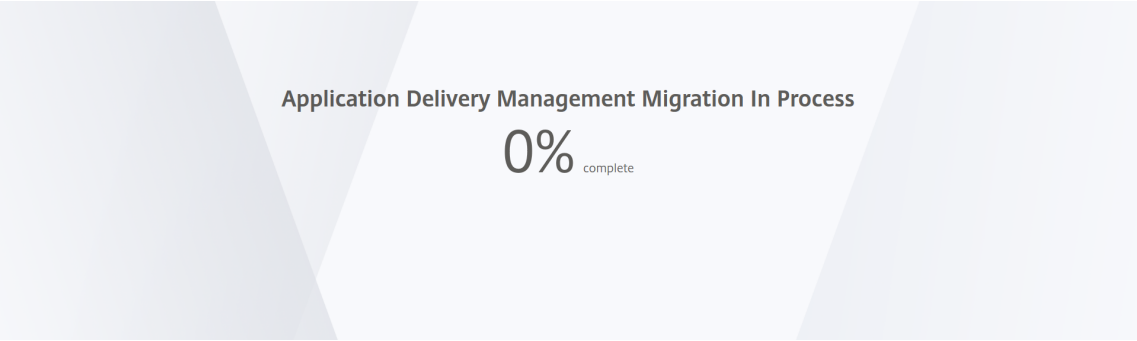
5. **boot-s** コマンドを実行して、NetScaler ADM を再起動します。
6. 「シェルのフルパスを入力してください」または「**/bin/sh:** 」というメッセージが表示されたら、**Enter** キーを押して /u @ プロンプトを表示します。
7. 次のコマンドを使用して、フラッシュパーティションをマウントします。

   ```
   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 にアクセスするようにセカンダリ NIC を構成する

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。

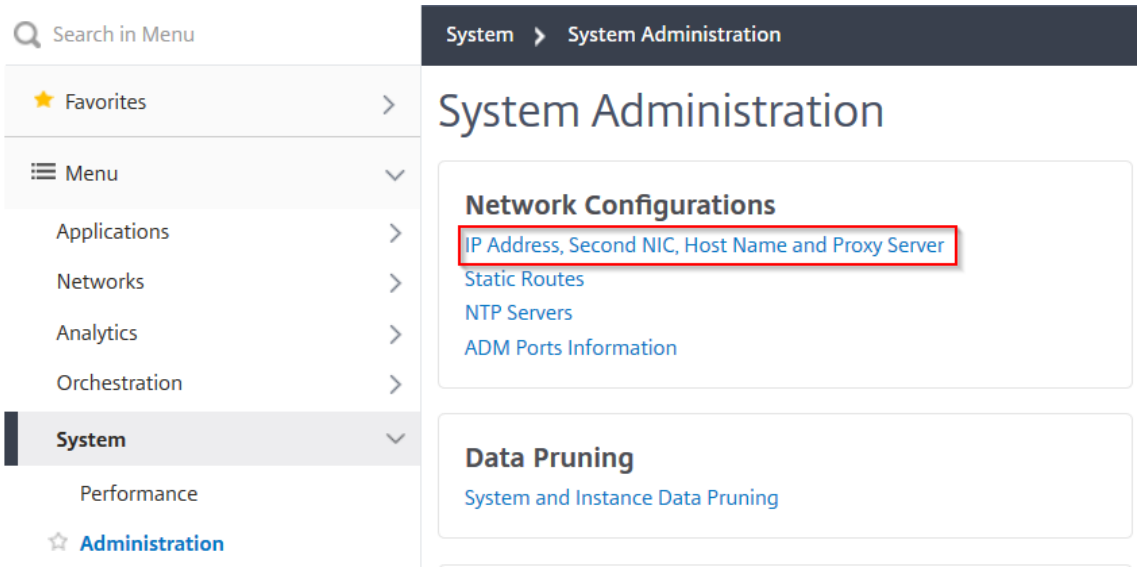
前提条件

- 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。

Citrix Hypervisor 上の NIC に IP アドレスを割り当ててセカンダリインターフェイスを作成するには、「NIC への IP アドレスの割り当て」を参照してください。

NetScaler ADM で 2 つ目の NIC を設定します

1. ADM GUI にログオンします。
2. [設定] > [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。

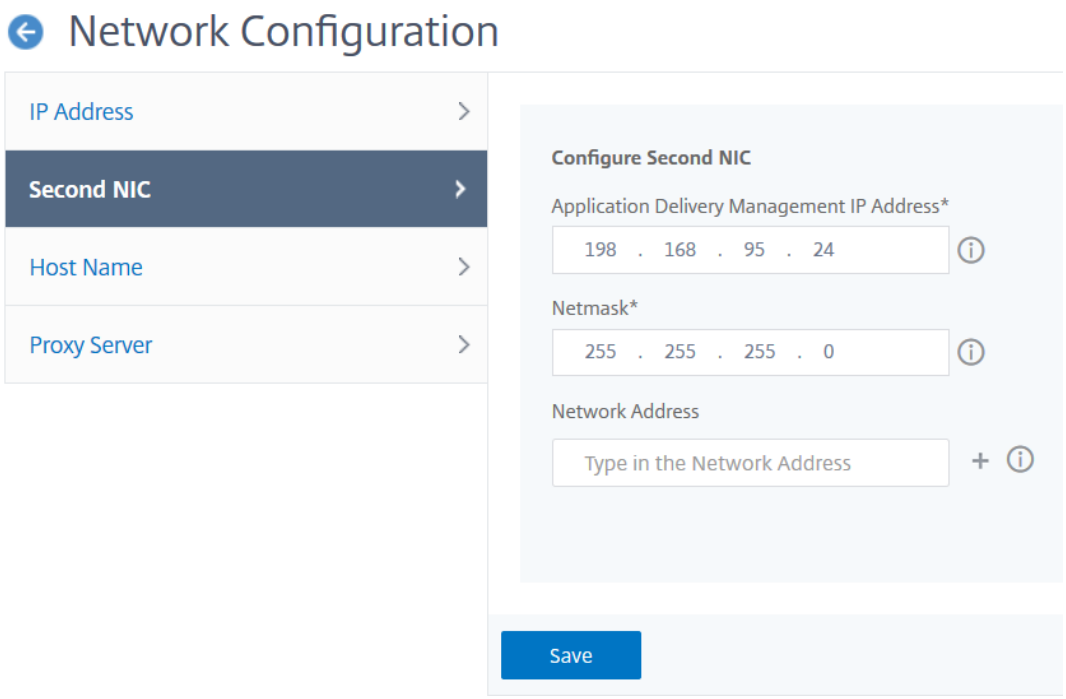
4. Second NIC タブをクリックし、次のパラメータを設定します。

   a) **Application Delivery Management 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。



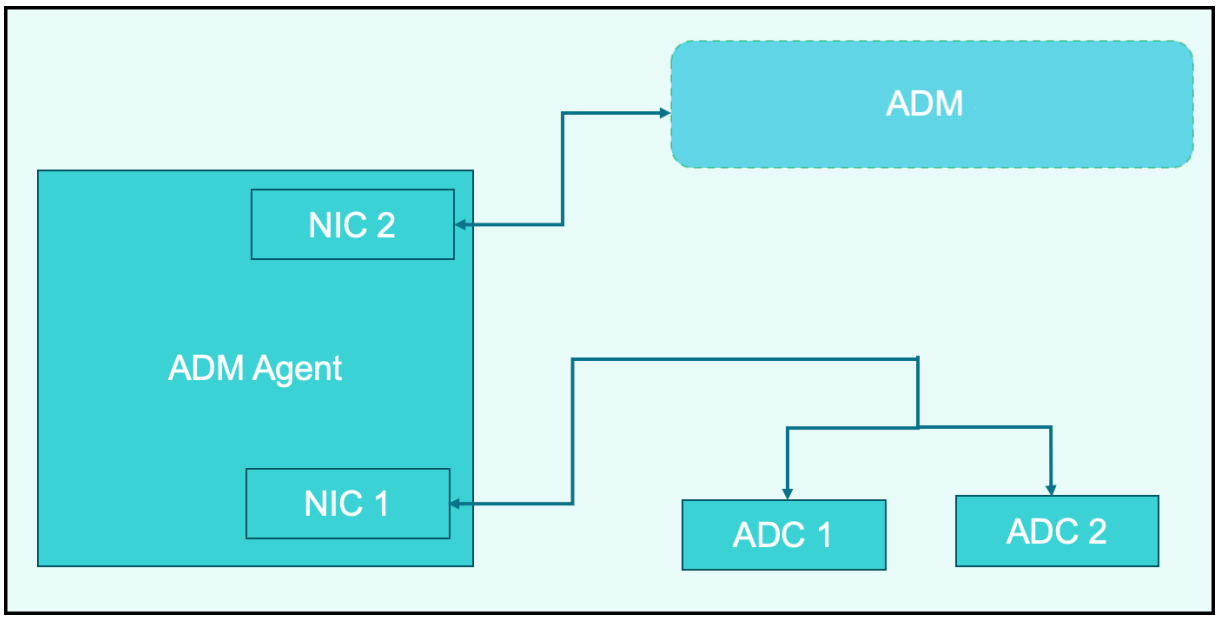
ADM エージェントにアクセスするためのセカンダリ NIC の設定

February 6, 2024

ADM エージェントには 2 つの NIC を設定できます。デュアル NIC アーキテクチャを使用すると、ADM エージェントは次のことが可能になります。

- ADM エージェントと ADC インスタンス間の通信を確立する-最初の NIC を使用して、NetScaler ADM を介して送受信されるトラフィックを分離したり、別のネットワーク上の NetScaler ADM とその管理対象 NetScaler ADC インスタンス間の通信を行うことができます。
- ADM エージェントと NetScaler ADM 間の通信の確立-2 つ目の NIC を使用して、ネットワーク上の NetScaler ADM を管理し、管理タスクを実行できます

> 注
>
> 両方の NIC の機能と構成を入れ替えることはできません。



このシナリオでは、管理者は次のことができます。

- NetScaler ADM と、その管理対象の NetScaler インスタンス間のトラフィックの 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 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
>
> ADM エージェントにはデュアル NIC の設定は必須ではありません。これはオプションであり、ADM エージェント、NetScaler ADM、および ADC 間のトラフィックを分離する必要がある場合にのみ必要です。

CLI を使用して **IPV4 NIC** ネットワークアドレスを変更する

1. PuTTY などの SSH クライアントを使用して、NetScaler ADM エージェントコンソールへの SSHConnection を開きます。
2. **nsrecover/nsroot** 認証情報を使用してログインし、シェルプロンプトに切り替えます。
3. **ifconfig** コマンドを実行します。設定した 2 つの NIC の詳細が表示されます-
    - NIC 1 —ADM エージェントと ADC 間の通信用
    - NIC 2 —ADM エージェントと NetScaler ADM 間の通信用


```
bash-3.2# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPV6,TXCSUM_IPV6>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: lo
pflog0: flags=0<> metric 0 mtu 33152
        groups: pflog
1/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether a2:56:cd:d2:f8:8c
        hwaddr a2:56:cd:d2:f8:8c
        inet6 fe80::a056:cdff:fed2:f88c%1/1 prefixlen 64 scopeid 0x3
        inet 10.102.103.247 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
1/2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 32:89:fe:8c:8f:45
        hwaddr 32:89:fe:8c:8f:45
        inet6 fe80::3089:feff:fe8c:8f45%1/2 prefixlen 64 scopeid 0x4
        inet 10.102.103.250 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
```

4. **networkconfig** コマンドを実行します。IPV4 ネットワークアドレスを設定または変更できるメニューが表示されます。

```
bash-3.2# /mps/networkconfig

------------------------------------------------------------------------------
Citrix ADM Agent 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 Agent Host Name [ns]:
      2. Citrix ADM Agent IPv4 address [10.102.103.247]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.103.1]:
      5. DNS IPv4 Address [10.102.166.70]:
      6. Second NIC IPv4 address [10.102.103.250]:
      7. Second NIC Netmask [255.255.255.0]:
      8. Second NIC Network address [10.102.103.251,10.102.103.252,10.102.103.252]:
      9. Second NIC Gateway IPv4 address [10.102.103.2]:
     10. Cancel and quit.
     11. Save and quit.
```

> 注
>
> 2 番目の NIC ネットワークアドレスは複数の IP 値をとることができます。

5. 変更するメニュー項目を選択します。設定を保存して終了します。

syslog パージ間隔の設定

February 6, 2024

Syslog は、ログ記録用の標準プロトコルです。2 つのコンポーネントで構成されています。1 つは Citrix アプリケーション Delivery Controller（ADC）インスタンスで実行される Syslog 監査モジュールで、もう 1 つは NetScaler インスタンスの基盤となる FreeBSD オペレーティングシステム（OS）またはリモートシステムで実行できる Syslog サーバーです。Syslog は、データ転送に 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。

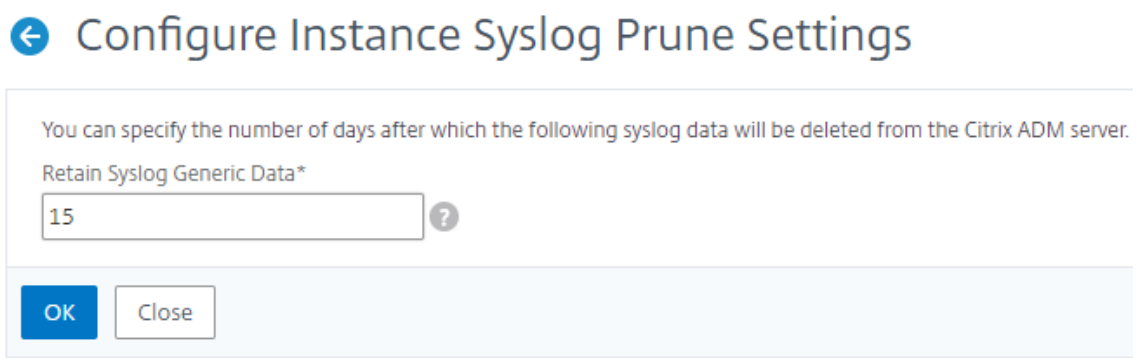
データベースに保存される syslog データの量を制限するには、syslog データを削除する間隔を指定できます。次の syslog データが NetScaler Application Delivery Management（ADM）から削除されるまでの日数を指定できます。

- 汎用 Syslog データ
- AppFirewall データ
- NetScaler Gateway データ

NetScaler Gateway のプルーニング間隔を syslog タイプ別に設定することもできます。このプルーニング間隔は、NetScaler Gateway データを保持するように構成されたルーン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. [設定**] >** [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。



システムプルーニングとイベントプルーンの設定

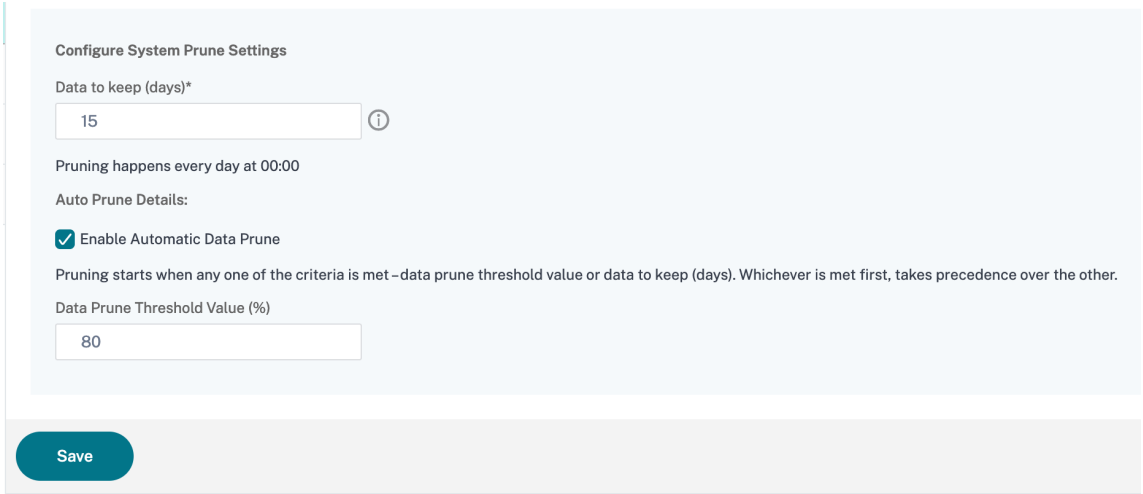
February 6, 2024

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
>
> 30 日を超える値や 15 日未満の値を指定することはできません。

パフォーマンス・レポートのシステム・プルーニング設定を構成するには:

1. [設定] > **[**管理] に 移動します。[データプルーニング] 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. 「システムプルーン設定の構成」ページで、次の項目を指定します。
   - データを保存する日数
   - ディスク容量のパーセンテージ (プルーニングしきい値)
3. [**OK**] をクリックします。



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選択します。ディスク使用量が設定されたデータプルーン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。

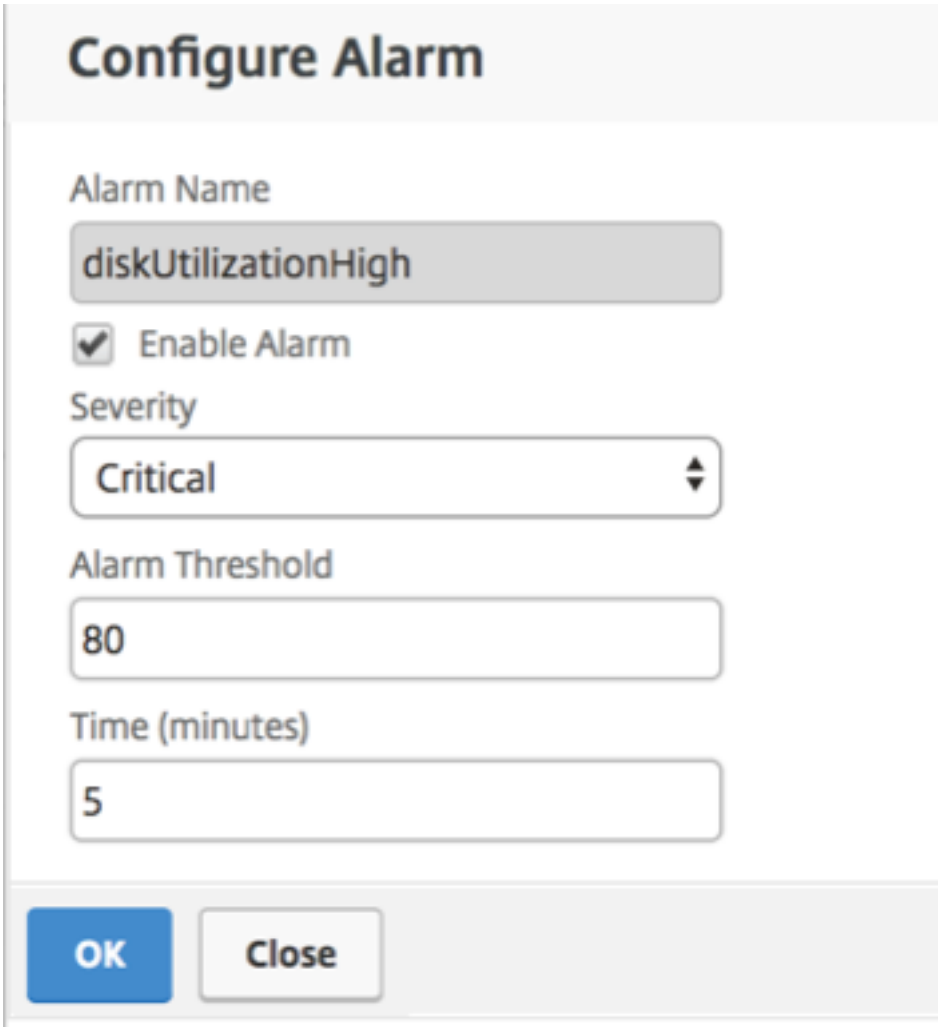
> 注

> プルーニングは、データプルーニングの閾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。

アラーム設定を構成して有効にするには：

1. [設定] > [**SNMP**] に移動します。右上隅の [アラーム] をクリックします。
2. 設定するアラーム (DiskUtilizationHigh など) を選択し、[編集] をクリックします。
3.「アラームの設定」ページで、以下を指定します。

- 重要度—重大度レベルを選択します。
- **Alarm Threshold**：イベントの重大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）を入力します。



NetScaler ADM を使用してイベントプルーンの設定を構成する

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。

1. [設定**] > [**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。
2. NetScaler ADM サーバーにデータを保存する時間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

NetScaler 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。

NetScaler ADM でデフォルト以外のユーザーのシェルアクセスを有効にするには：

1. NetScaler ADM で、[設定**] >** [管理] に移動します。
2.「システム構成」で、「システム」、「タイムゾーン」、「許可する **URL**」、「エージェント設定」をクリックします。
3.「システム構成」ページで、次のパラメータを設定します。

    - **Communication with instances** - 通信プロトコルを選択します。
    - 安全なアクセス -NetScaler ADM へ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 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**-NetScaler** 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。
    - インスタンスのログイン時にユーザー認証情報を要求する -ユーザーが NetScaler ADM からインスタンスにログオンしているときに、ユーザー資格情報を入力できるようにします。
        - **Stylebook** 操作用のプロンプト認証情報**-NetScaler** インスタンスで **StyleBook** および構成パックの操作を使用する際に、ユーザーがユーザー資格情報を入力できるようにします。

> 注:
> 「インスタンスログインの認証情報を入力する」が選択され、「**Stylebook** 操作用の認証情報を入力する」がオフになっている場合、NetScaler インスタンスでの StyleBook 操作と構成パック操作の資格情報の入力を求めるメッセージは表示されません。

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

NetScaler 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ためのデータベース保守ツールが提供されるようになりました。これで、NetScaler 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した。NetScaler 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。

NetScaler ADM スタンドアロン展開で **NetScaler ADM** データベース回復スクリプトを使用する方法

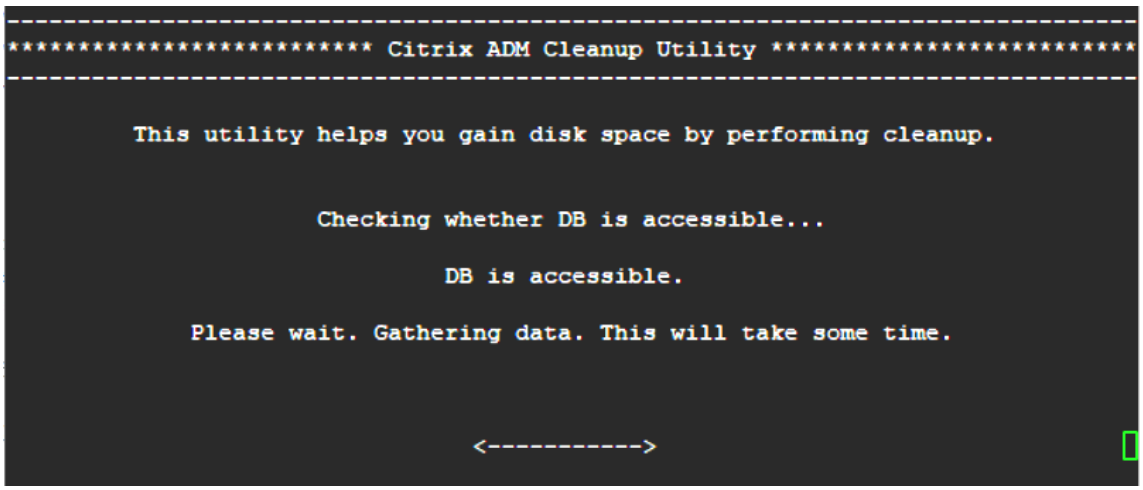
単一サーバーの NetScaler ADM 展開環境で次の手順を使用して、ファイルシステムに接続し、いくつかのコンポーネントを削除し、データベースにアクセスできるようにしてから、リカバリ操作を実行します。

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。

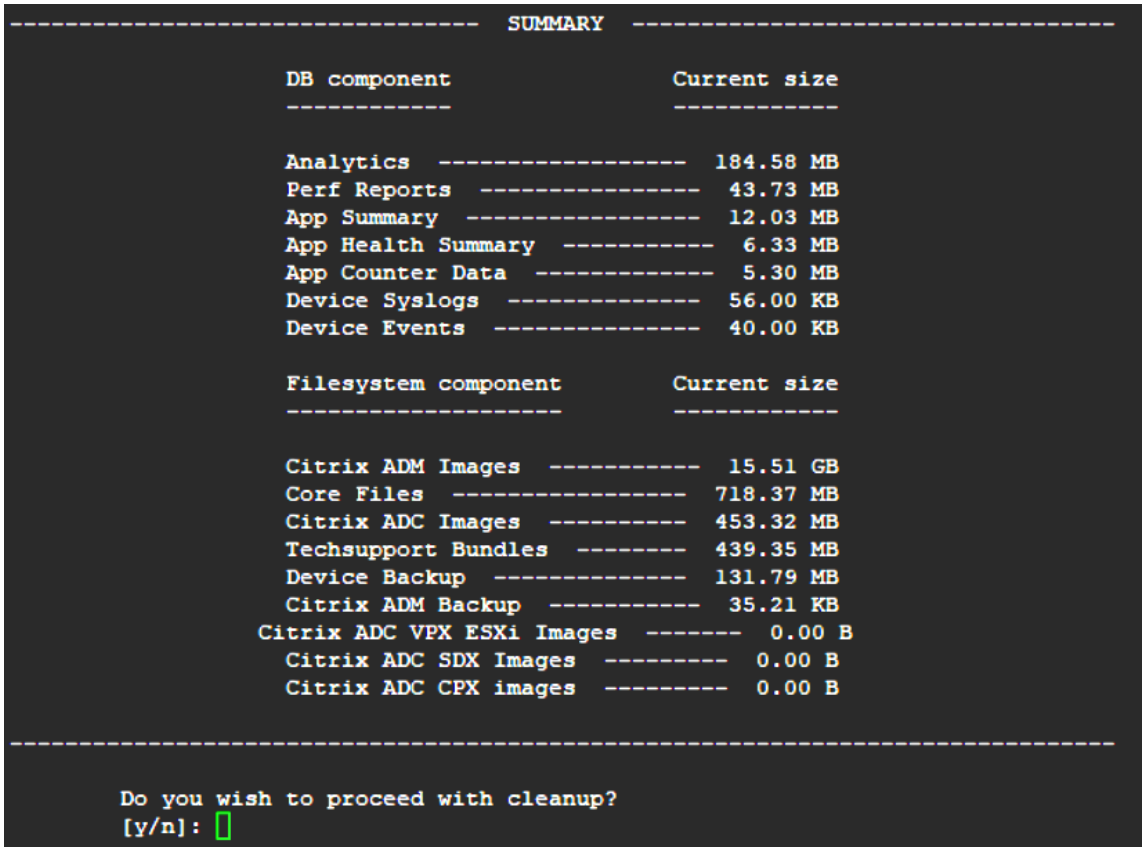
```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

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。



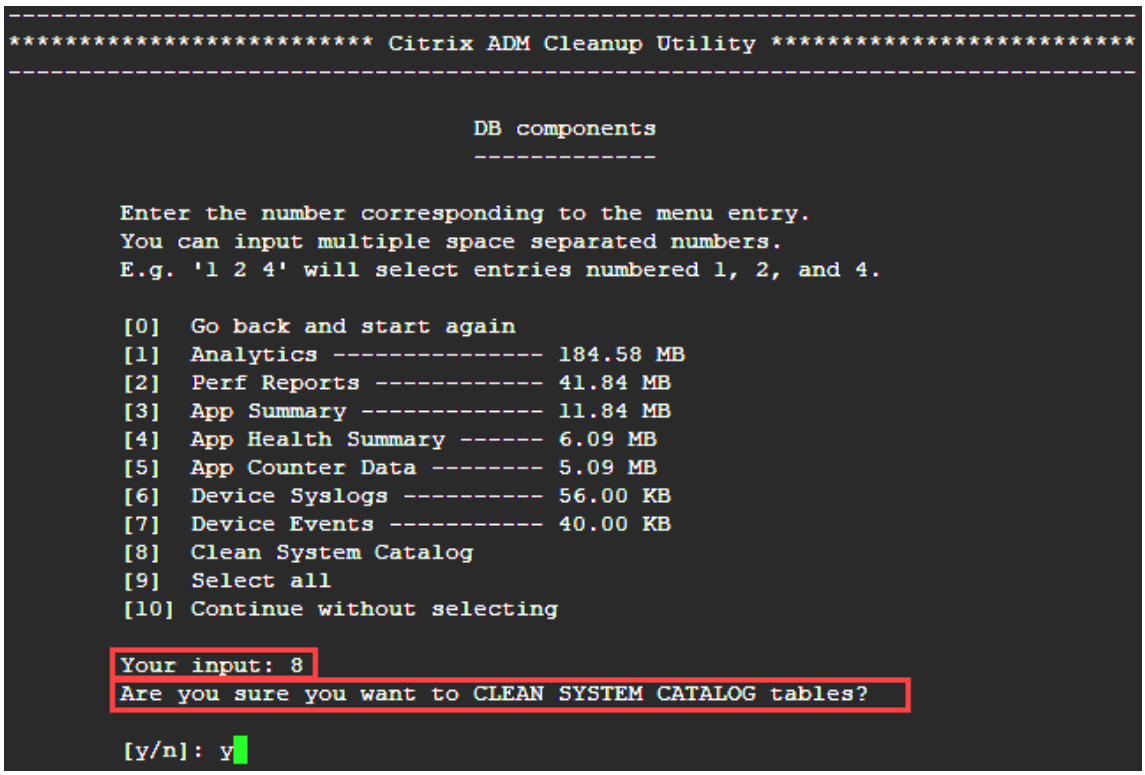
3. 画面に、データベース内のファイルのリストが表示されます。「y」と入力し、Enter キーを押してクリーンアッププロセスを開始します。



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。

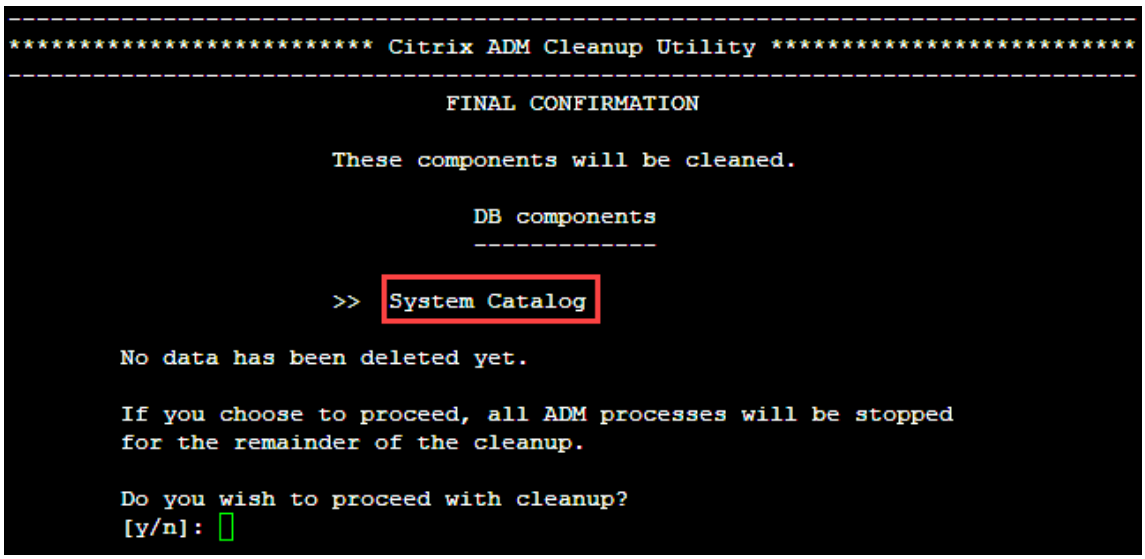
> 注:
>
> NetScaler ADM には、システムカタログと呼ばれるユーザーテーブルが含まれています。システムカタログは、リレーショナルデータベース管理システムがテーブルや列、内部レコードに関する情報などのスキーマメタデータを格納する NetScaler ADM データベース内の場所です。システムカタログのテーブルは通常のテーブルに似ており、時間が経つにつれて膨張した行や使用されなくなった行が蓄積されることがあるため、最適なパフォーマンスを得るには定期的なクリーンアップが必要です。これらのテーブルは定期的に管理することをお勧めします。このアクティビティにより、ディスク容量が解放されるだけでなく、データベース、ひいては NetScaler ADM の全体的なパフォーマンスも向上します。



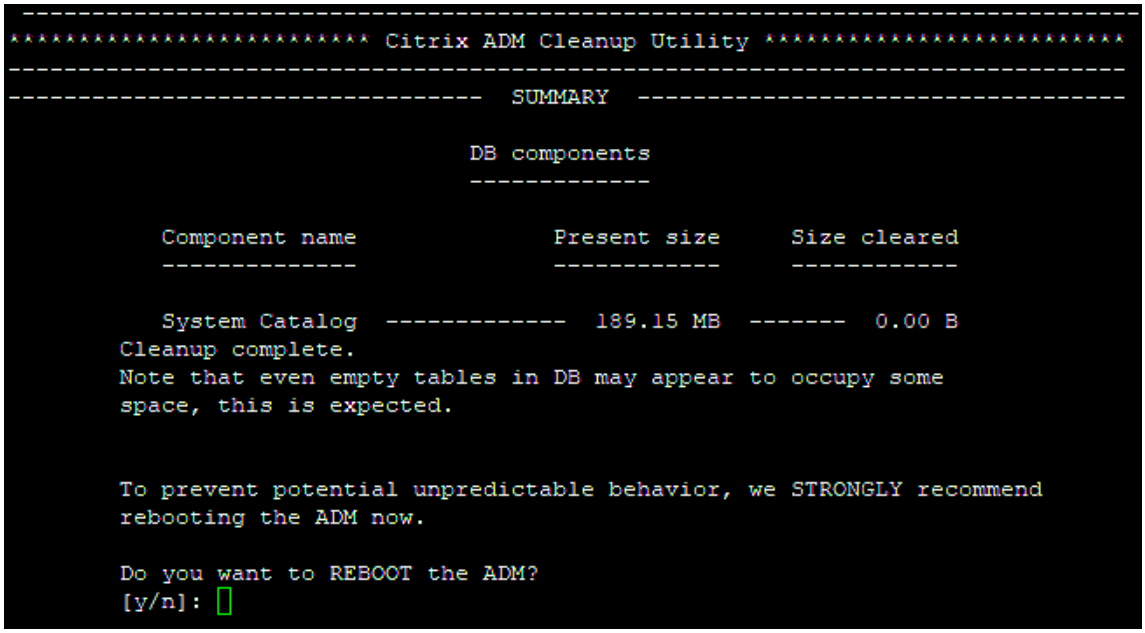
クリーンアップユーティリティには、データベースコンポーネントとファイルコンポーネントをクリーンアップするオプションがあります。「1」から「9」までの数字を入力して任意のファイルコンポーネントを選択するか、「11」と入力して Enter キーを押してデータベースコンポーネントをクリーンアップできます。

> 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。

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。



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。



6. 「y」と入力して **Enter** キーを押し、NetScaler ADM を再起動します。

   システムをクリーンアップした後は、必ず NetScaler ADM を再起動してください。NetScaler ADM が再起動した後、内部データベース操作が完了するまで約 30 分間待ちます。これで、NetScaler ADM データベースに接続できるはずです。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。NetScaler ADM が稼働していれば、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。

NetScaler ADM データベースリカバリスクリプトを NetScaler ADM 高可用性環境で使用する方法

高可用性環境の NetScaler 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 NetScaler 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。

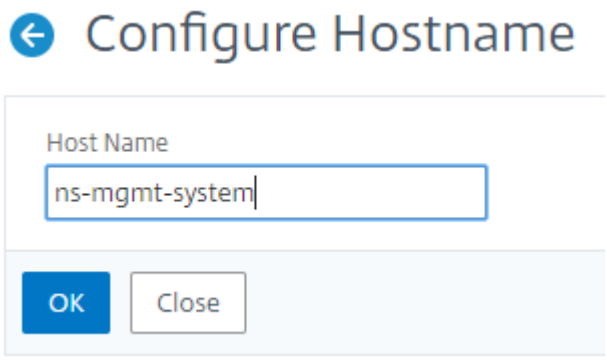
NetScaler ADM サーバーへのホスト名の割り当て

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。



> 注
>
> ハイパーバイザーで`networkconfig`コマンドを使用して、ホスト名を変更することもできます。

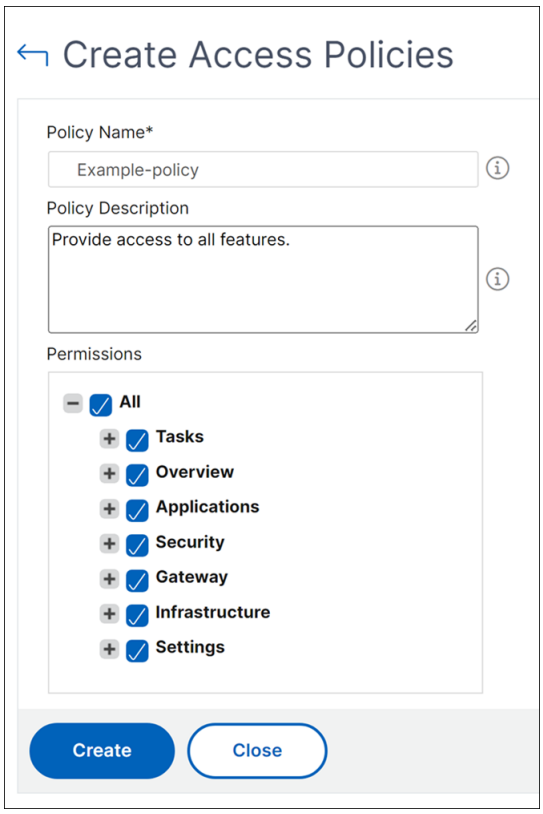
NetScaler ADM サーバーのバックアップと復元

February 6, 2024

NetScaler ADM サーバーのバックアップを定期的に作成できます。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。[設定**] > [**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にのみ表示されます。ユーザーは、アクセスポリシーにすべての権限がある場合にのみ、このページにアクセスできます。通常、スーパーユーザー

はすべての ADM 機能にアクセスできます。



、「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。

- NetScaler ADM 構成ファイル:
  - SNMP
  - Syslog サーバー構成ファイル
  - NTP ファイル
  - SSL 証明書
  - Control Center ファイル
- NetScaler ADM サーバーが管理する NetScaler インスタンスのバックアップ。
- 構成監査テンプレート
- データベースに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
  - 外部認証サーバーの構成（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:
  - 追加された管理対象 NetScaler インスタンスのデータ
  - 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す。

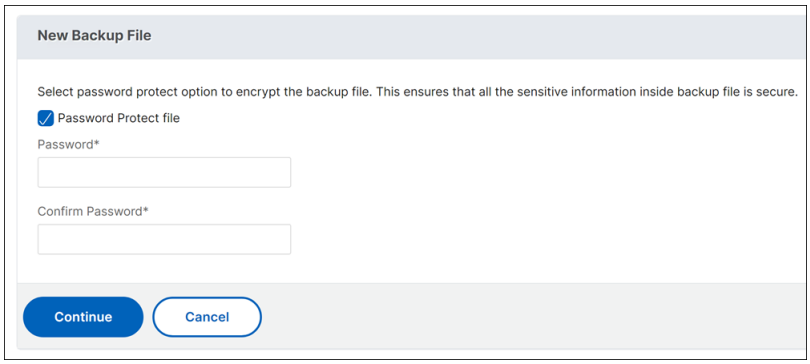
NetScaler ADM 構成のバックアップ

デフォルトでは、NetScaler ADM サーバーは 24 時間ごと（00.30 時間）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. [設定] **>** [バックアップファイル] に移動し、[バックアップ] をクリックします。
2. バックアップファイルを暗号化するには、[ファイルを パスワードで保護 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。

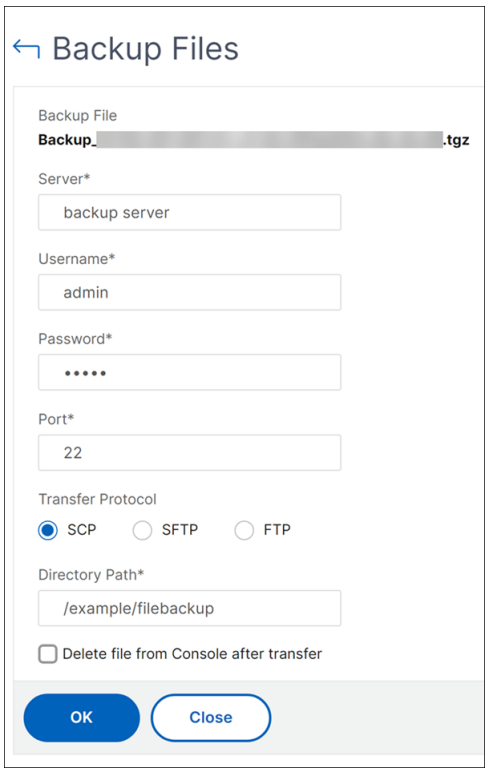


NetScaler ADM バックアップファイルを外部システムに転送する

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。

NetScaler ADM バックアップファイルを転送するには:

1. [設定] **>** [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 **Application Delivery Management** 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。



> 注
>
> バックアップファイルのコピーをローカルシステムに保存するには、[設定] **>** **[**バックアップファイル] に移動し、コピーするファイルを選択して [ダウンロード] をクリックします。

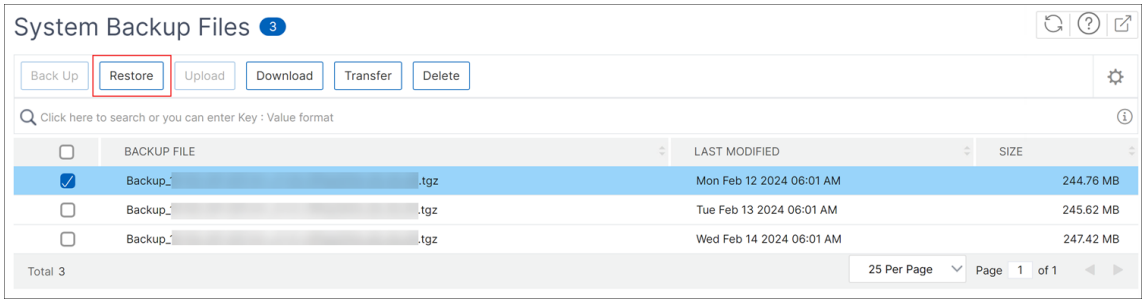
バックアップファイルから **NetScaler ADM** 構成を復元する

以前にバックアップしたファイルから NetScaler 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. [設定] **>** **[**バックアップファイル] に移動します。
2. 復元するバックアップ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、[設定] **>** **[**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。

高可用性展開における **NetScaler ADM** の仮想マシンスナップショット

February 6, 2024

アップグレードを開始する前に、HA 展開内の NetScaler ADM サーバーのスナップショットを作成できます。スナップショットは、作成時の仮想マシンの状態全体をキャプチャします。

NetScaler ADM サーバーのスナップショットを撮る

次の順序を使用して、NetScaler ADM サーバーのスナップショットを取得します。

1. NetScaler ADM セカンダリサーバー
2. NetScaler ADM プライマリサーバー

NetScaler ADM サーバーのスナップショットを撮るには:

1. ハイパーバイザーで、仮想マシンのリストから NetScaler ADM セカンダリサーバーを選択します。
2. VM のスナップショットを取得します。

   > 注:
   >
   > スナップショットの作成中は、[**VM memory**] を選択することをお勧めします。

3. スナップショットにわかりやすい名前を付け、必要に応じて説明を入力します。

   スナップショットはデフォルトの VM ディレクトリに保存されます。

4. プライマリサーバーでも同じ手順を繰り返します。

> 注:
>
> スナップショットを撮るときに VM の電源を切る必要はありません。

NetScaler ADM サーバーのスナップショットを復元する

スナップショットを復元すると、仮想マシンのメモリ、設定、および仮想マシンディスクの状態が、スナップショットを作成した時点の状態に戻ります。

NetScaler ADM サーバーのスナップショットを復元するには、次の順序に従います。

1. NetScaler ADM プライマリサーバー
2. NetScaler ADM セカンダリサーバー

NetScaler ADM サーバーのスナップショットを復元するには:

1. ハイパーバイザーで、仮想マシンのリストから NetScaler ADM プライマリサーバーを選択します。
2. VM を右クリックして、スナップショットを元に戻します。

   仮想マシンは最新のスナップショットに戻されます。

3. NetScaler ADM セカンダリサーバーについても同じ手順を繰り返します。

監査情報の表示

February 6, 2024

Syslog は、ログ記録用の標準プロトコルです。2 つのコンポーネントで構成されています。1 つは Citrix アプリケーション Delivery Controller（ADC）インスタンスで実行される Syslog 監査モジュールで、もう 1 つは NetScaler インスタンスの基盤となる FreeBSD オペレーティングシステム（OS）またはリモートシステムで実行できる Syslog サーバーです。Syslog は、データ転送に 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。

NetScaler デバイスが生成する Syslog メッセージを NetScaler 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、NetScaler デバイスが生成する syslog メッセージを監視できます。NetScaler 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。

NetScaler 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。

NetScaler ADM で **Syslog** の日付と時刻の形式を構成するには：

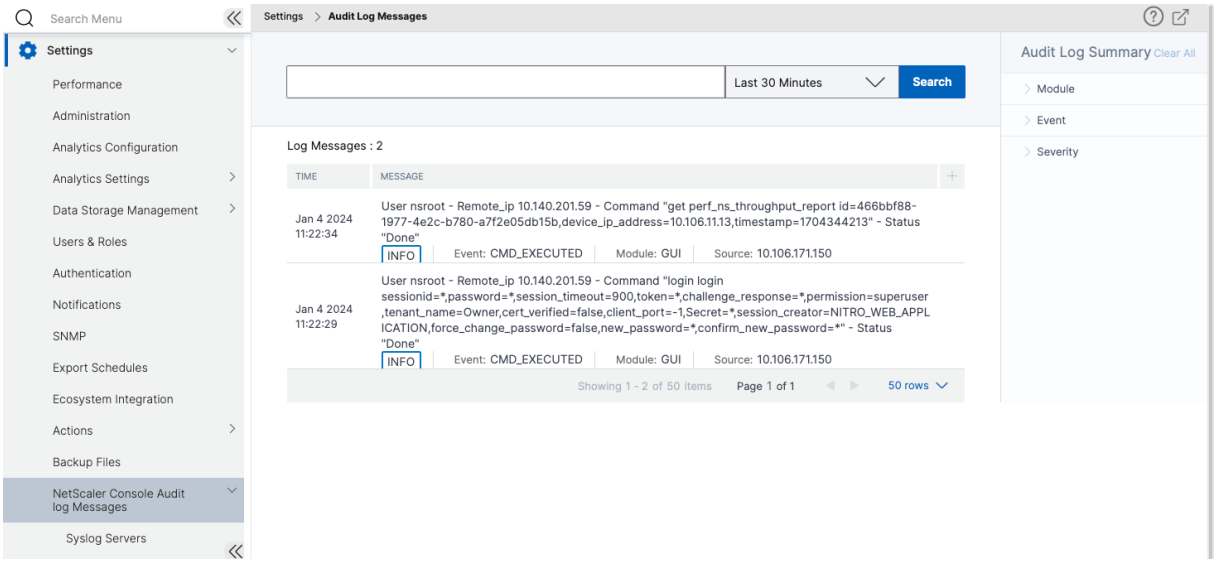
1. [システム] > [監査] に移動します。「構成の概要」で、「**Syslog** サーバー」を選択します。
2. 「**Syslog** サーバー」ページで、Syslog サーバーを選択し、「**Syslog** パラメータ」をクリックします。
3. [**Configure Syslog Parameters**］ページで日時形式を指定します。
4. [**OK]** をクリックします。

NetScaler 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 NetScaler 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、管理対象の NetScaler インスタンスで生成されたすべての syslog メッセージを表示できるようになりました。Syslog メッセージは NetScaler 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。



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。NetScaler Application Delivery Management （ADM）で SSL 設定を構成し、システムに接続するクライアントのタイプを指定できます。

NetScaler 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。

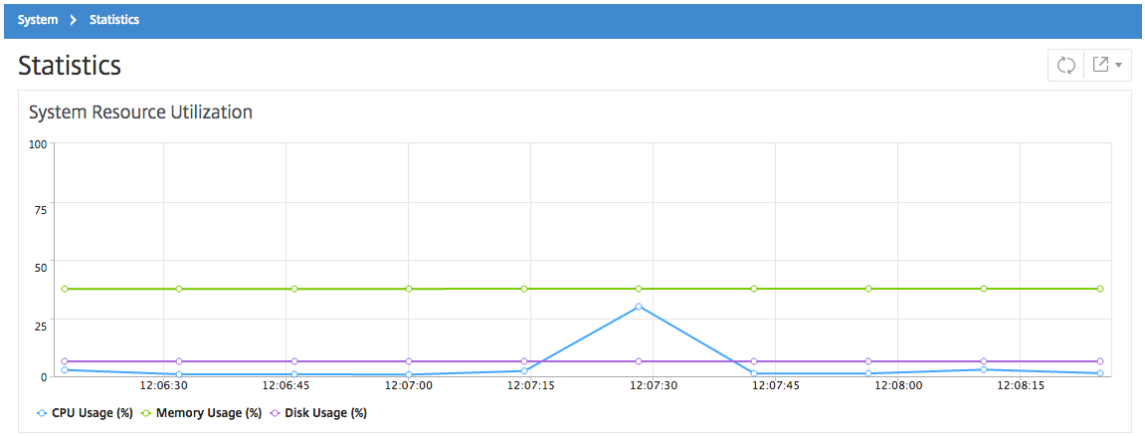
CPU、メモリ、ディスク使用率の監視

February 6, 2024

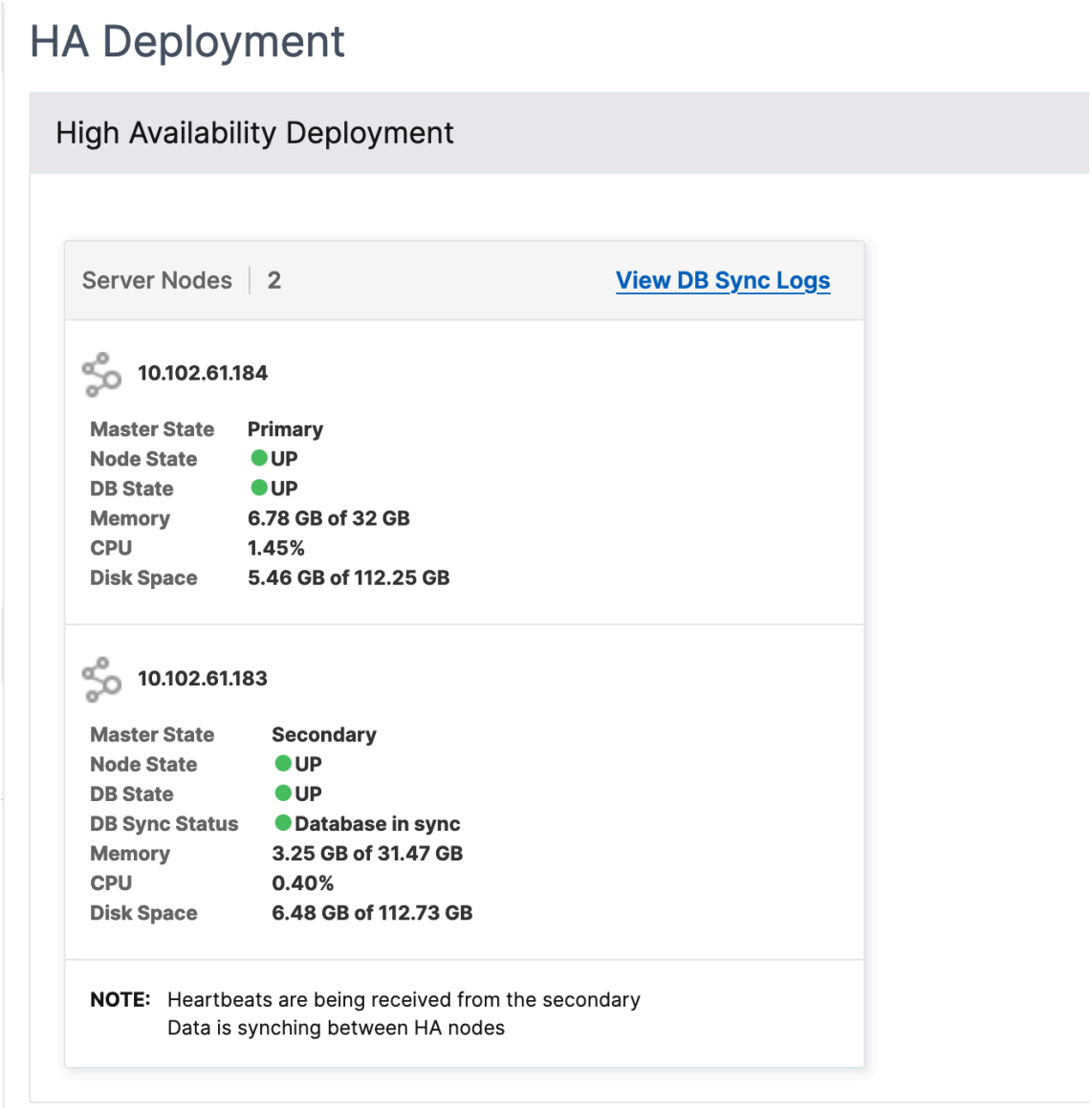
ログと統計に保持されている情報を使用できます。この情報は、NetScaler Application Delivery Management（ADM）の構成と保守に役立つレポートにも表示されます。

CPU、メモリ、ディスクの使用状況を監視するには、

- スタンドアロンデプロイメント。[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。設定 **>** デプロイメントに移動します。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

February 6, 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 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 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

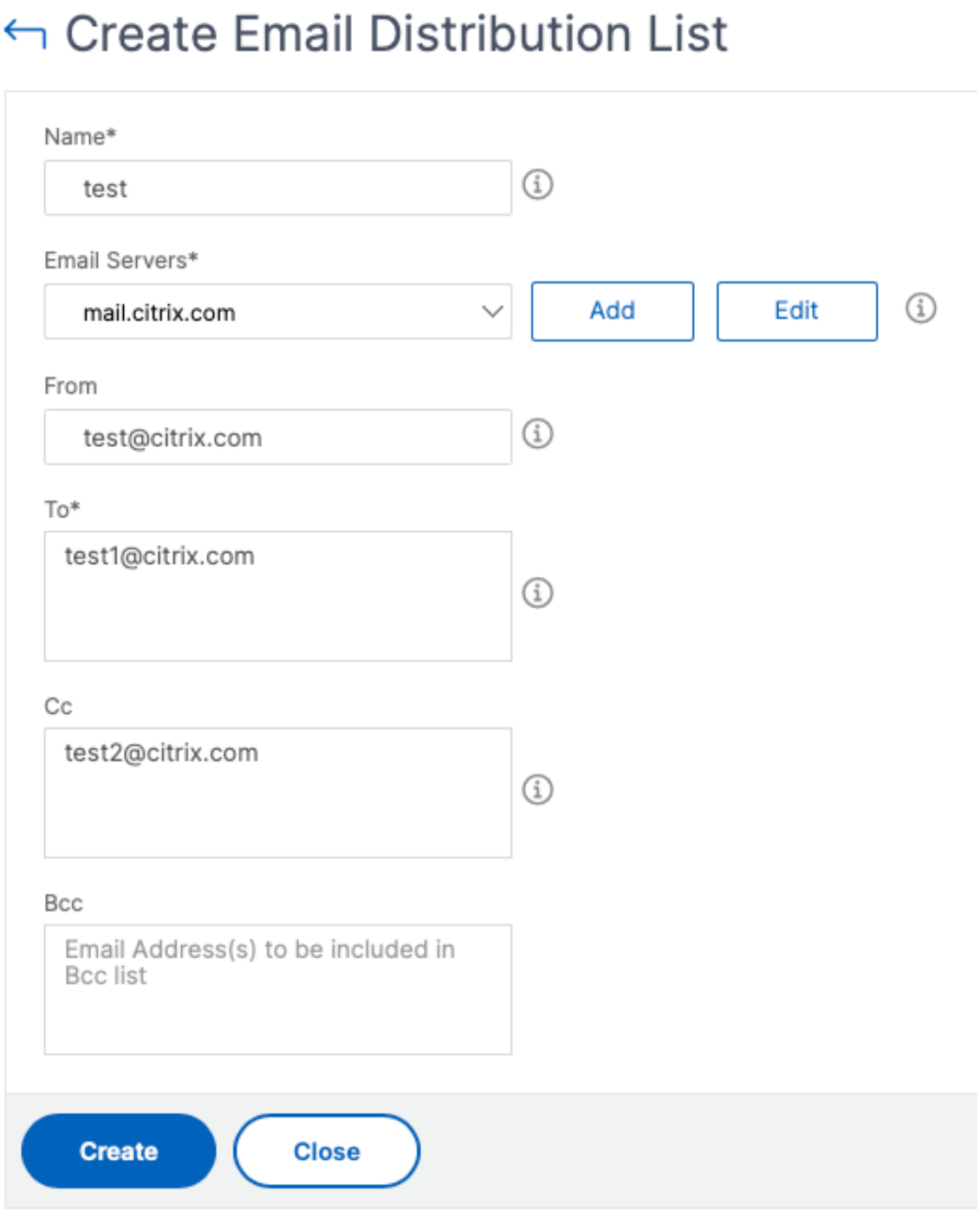
ADM GUI には、通知タイプごとに、設定された配布リストまたはプロファイルが表示されます。ADM は、選択した配布リストまたはプロファイルに通知を送信します。

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. [設定] **>** [通知] に移動します。
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。



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. [設定**] > [**通知**]** に移動します。
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。

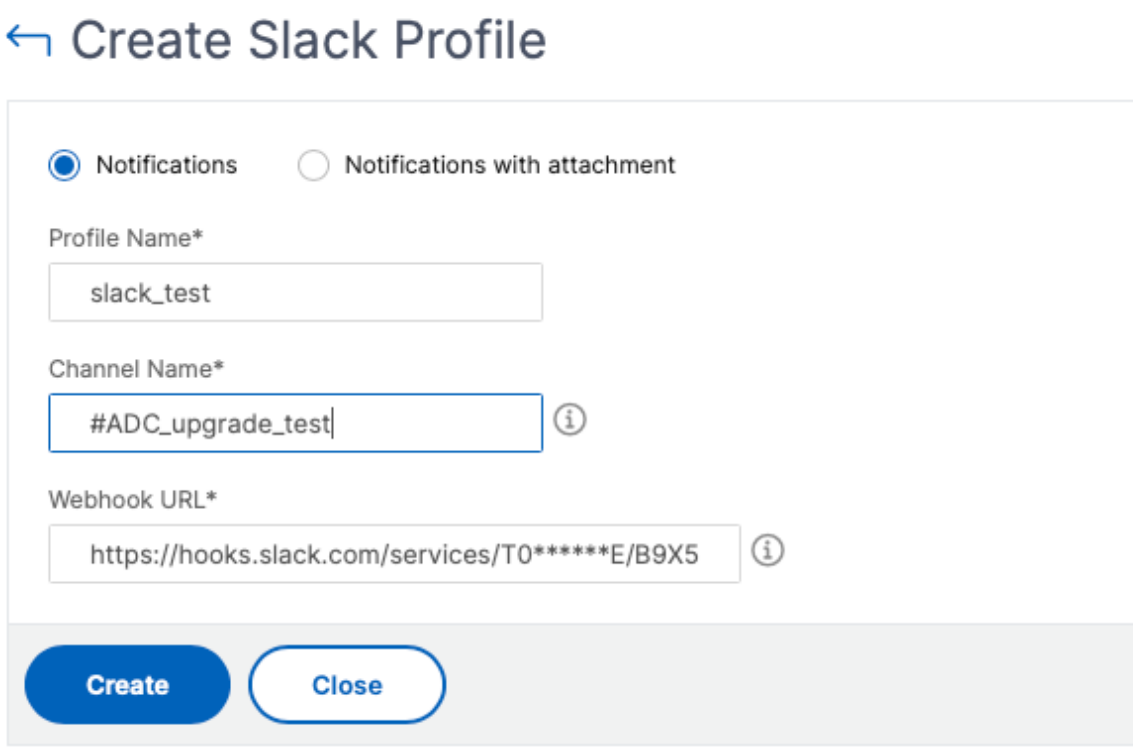
この手順を繰り返して、複数の SMS 配布リストを作成します。**SMS** タブには、ADM にあるすべての SMS 配布リストが表示されます。

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. [設定**] > [**通知**]** に移動します。
2. **Slack** で [追加] をクリックします。
3.「**Slack** プロファイルの作成」で、次の詳細を指定します。
    - プロファイル名 -プロファイル名を指定します。この名前は Slack 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



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. [設定**] > [**通知**]** に移動します。
2. [**PagerDuty**] で、[追加] をクリックします。
3.「**PagerDuty** プロファイルの作成」で、次の詳細を指定します。
   - プロファイル名 -任意のプロファイル名を指定します。
   - 統合キー -統合キーを指定します。このキーは PagerDuty ポータルから入手できます。
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. [設定] **>** [通知] に移動します。
2. [**ServiceNow**] で、リストから **Citrix_Workspace_sn** プロファイルを選択します。
3. 「テスト」をクリックして ServiceNow チケットを自動生成し、構成を確認します。

   NetScaler ADM GUI で ServiceNow チケットを表示する場合は、[**ServiceNow** 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 NetScaler 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。

```
The archive file is created as a TAR file.

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 Citrix Insight Services（CIS）にアップロードできます。

   b) ADM コンソールでスクリプトを実行して、テクニカルサポートファイルを CIS Web サイトにアップロードすることもできます。

      i. SSH を使用して、ADM コンソールにログオンします。

      ii. シェルプロンプトに切り替えて、次のように入力します。

      /mps/collector_upload.pl

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。

```
/mps/collector_upload.pl [-proxy [<proxy_user>:<proxy_password>@]<
   proxy_host>:<proxy_port>] [-user <user>] [-password <password>] [-sr
    <sr>] [-description <description>] [-debug] <file>
<!--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することもできます。

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。)
引き続き、ADM シェルから CIS にファイルを直接アップロードできます。

> 注:
>
> ADM がコンソールから CIS にファイルをアップロードできない場合でも、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。

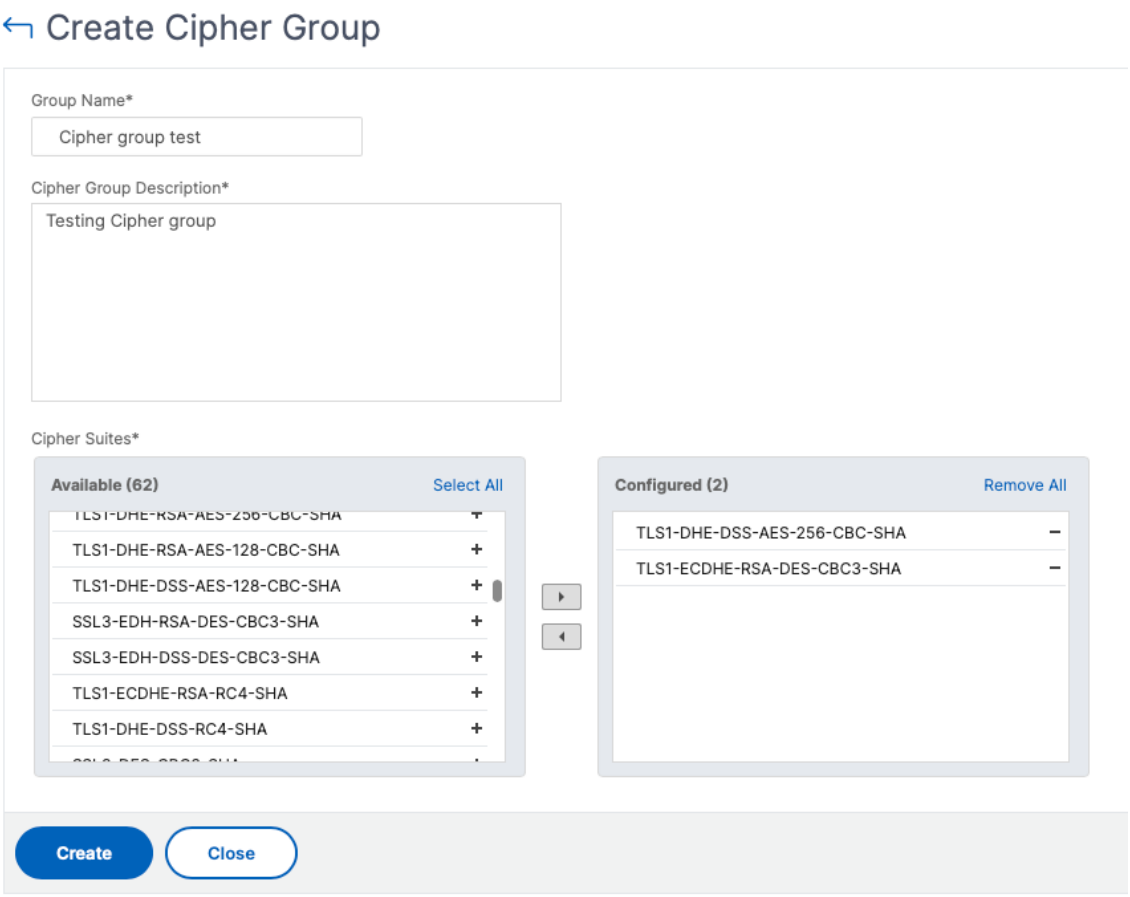
暗号グループの構成

February 6, 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. [設定**] > [**管理**]** に移動します
2. [**SSL** 設定] で [暗号グループ] をクリックします。
3. ［追加］をクリックします
4. ［**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。



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

NetScaler 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、NetScaler ADM がトラップの宛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。

NetScaler ADM で **SNMP** トラップデスティネーションを作成するには：

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。NetScaler ADM でメッセージを表示したり、メールまたは SMS で通知を受け取ることができます。

アラームを設定するには、BackupFailed アラームを選択し、重大度レベルを Major として指定する必要があります。このアラームはデフォルトで有効化されています。

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. [設定] **> [SNMP**] に移動します。右上隅の [アラーム] をクリックします。

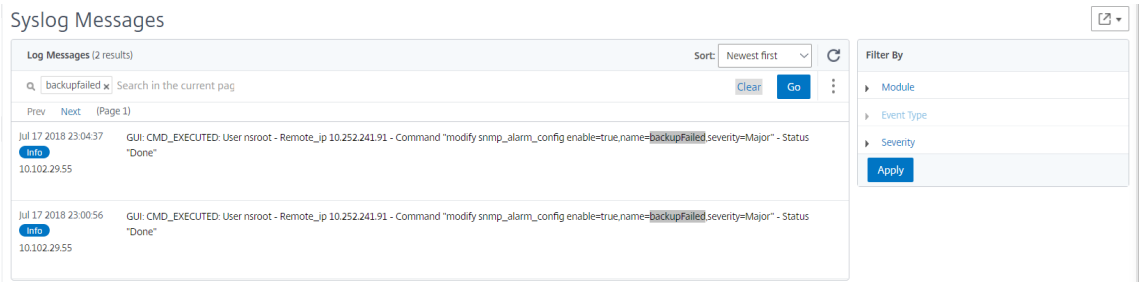
2. 設定するアラーム（BackupFailed など）を選択し、[**Edit**] をクリックして設定を変更します。
3. このアラームはデフォルトで有効化されています。重要度レベル (例: メジャー) を割り当て、「**OK**」をクリックします。

> 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。

NetScaler ADM を使用して **BackupFailed** アラームによって生成されたイベントを表示するには：

1. [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。



   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。

NetScaler ADM エージェント用の SNMP マネージャーとユーザーの作成

February 6, 2024

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。

SNMP マネージャーを追加して NetScaler ADM エージェントにクエリを実行できます。マネージャーは SNMP V2 および V3 に準拠しています。1 つ以上の SNMP マネージャーを指定した場合、NetScaler ADM エージェントは、指定された SNMP マネージャー以外のホストからの SNMP クエリを受け入れません。

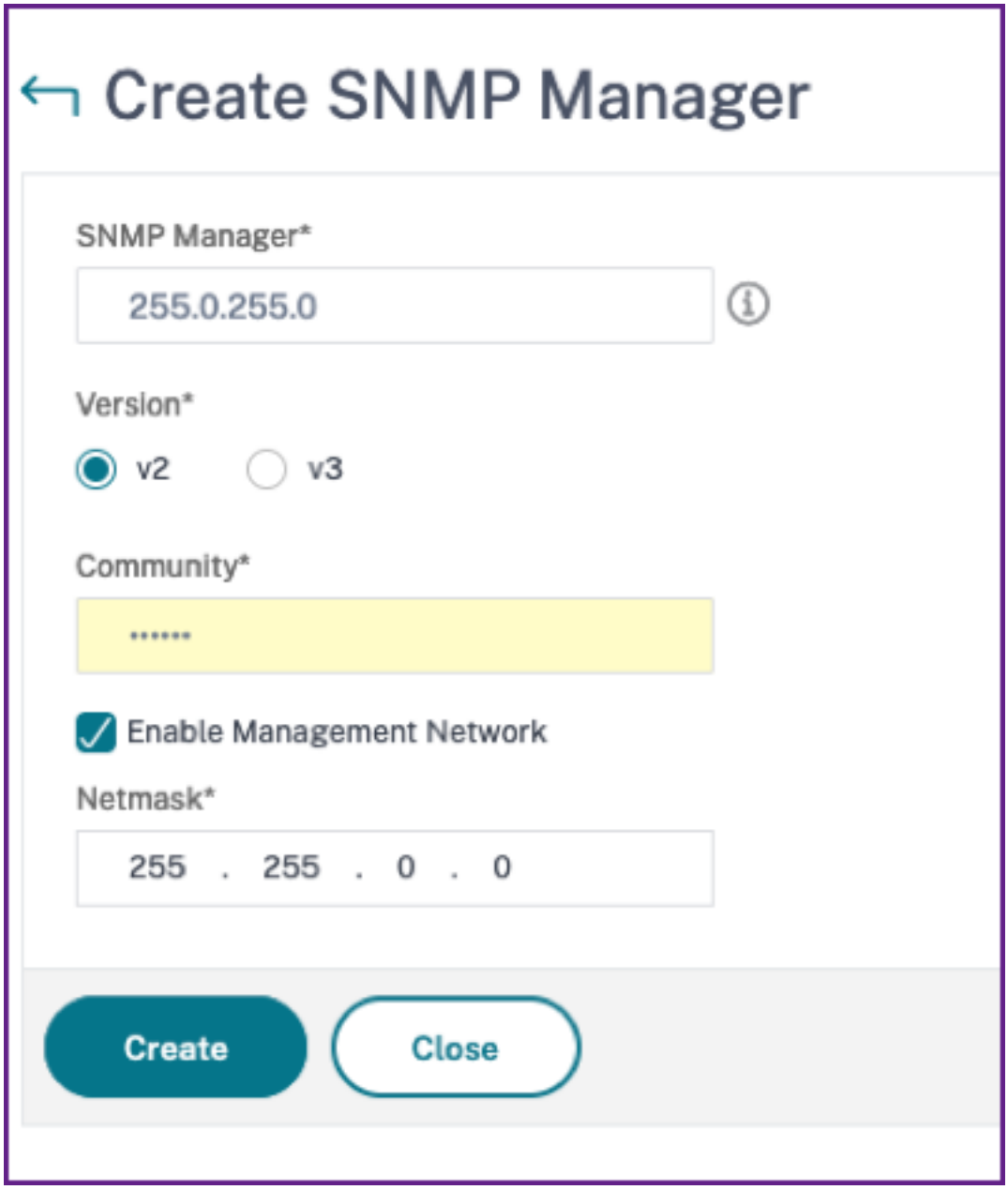
SNMP v2 マネージャーの追加

NetScaler ADM エージェントに SNMP v2 マネージャーを追加するには：

1. [インフラストラクチャ**] > [**エージェント] に移動し、NetScaler ADM エージェントを選択して、[アクションの選択] > [SNMP の管理] をクリックします。
2. 「SNMP」 > 「SNMP マネージャ」タブで、「追加」をクリックします。
3. **SNMP** マネージャーの作成ページで、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。
   - バージョン。v2 を選択します。
   - コミュニティ。コミュニティ名を入力します。SNMP コミュニティ設定は、SNMP マネージャーからの SNMP クエリを認証します。

- 管理ネットワークを有効にする: この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ネットマスクを指定します。
- ネットマスク:IP アドレスに関連付けられたサブネットマスクを入力します。

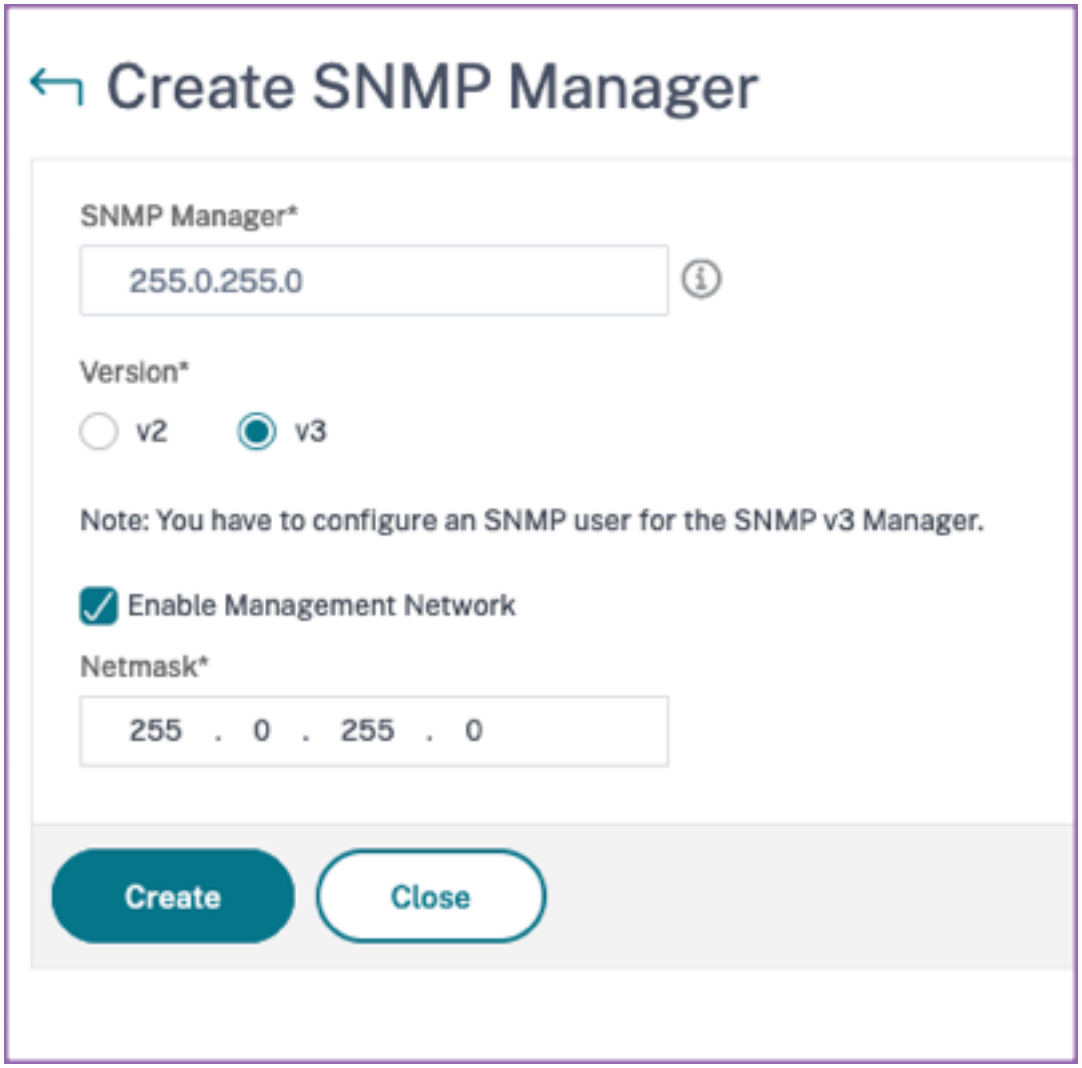
4. ［作成］をクリックします。



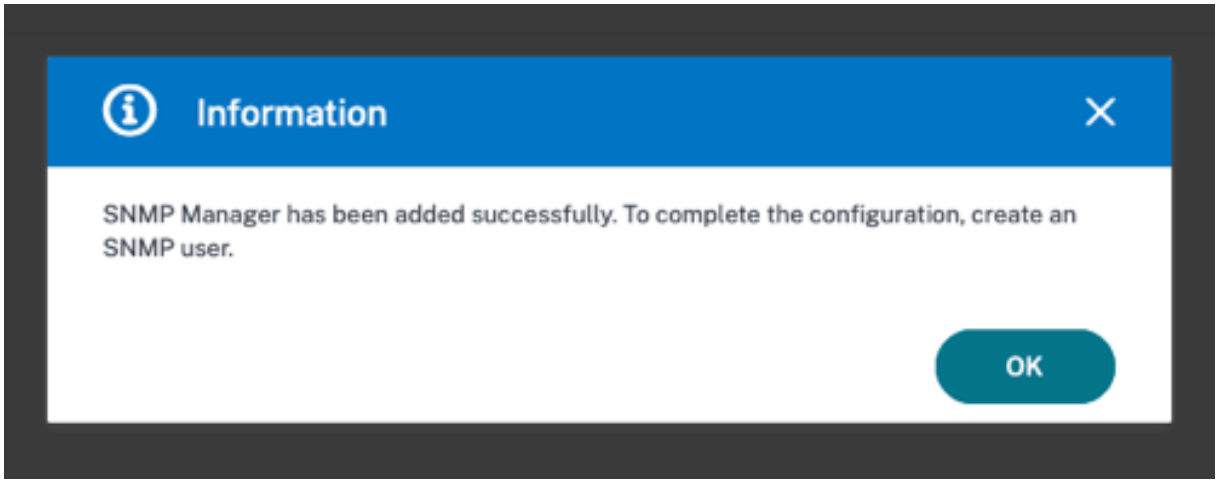
SNMP v3 マネージャーの追加

NetScaler ADM エージェントに SNMP v3 マネージャーを追加するには:

1. [インフラストラクチャ**] > [**エージェント] に移動し、NetScaler ADM エージェントを選択して、[アクションの選択] > [SNMP の管理] をクリックします。
2. 「SNMP」 > 「SNMP マネージャ」 タブで、「追加」 をクリックします。
3. **SNMP** マネージャーの作成ページで、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。
   - バージョン。v3 を選択します。
   - 管理ネットワークを有効にする: この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ネットマスクを指定します。
   - ネットマスク:IP アドレスに関連付けられたサブネットマスクを入力します。
4. ［作成］ をクリックします。



SNMP マネージャーが作成されたことを確認し、SNMP ユーザーを設定するように求めるダイアログボックスが表示されます。



> 注
>
> SNMP v3 マネージャーには SNMP ユーザーを設定する必要があります。SNMP ユーザーを設定するには、「SNMP」**>**「**SNMP** ユーザー」に移動します。

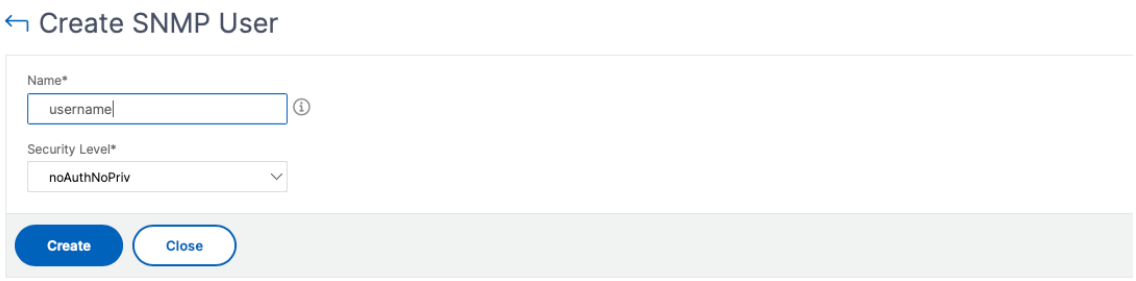
SNMP ユーザーを追加する

SNMP マネージャーからの SNMP v3 クエリに応答する SNMP ユーザーを追加します。

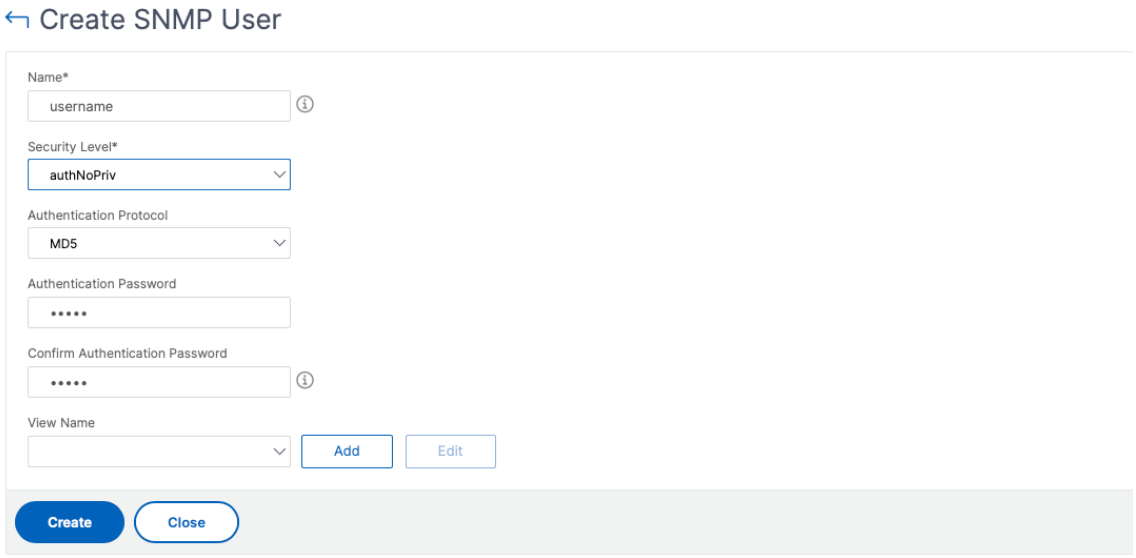
NetScaler ADM エージェントに SNMP ユーザーを追加するには:

1. [インフラストラクチャ**] > [**エージェント] に移動し、NetScaler ADM エージェントを選択して、[アクションの選択] > [SNMP の管理] をクリックします。
2. **[SNMP]**> [SNMP ユーザ] タブで、[追加 **] をクリックします。**
3.「**SNMP** ユーザーの作成」ページで、次の詳細を追加します。
   - 名前。ユーザー名を入力します。
   - セキュリティレベル。NetScaler ADM エージェントと SNMP マネージャー間の通信に必要なセキュリティレベル。

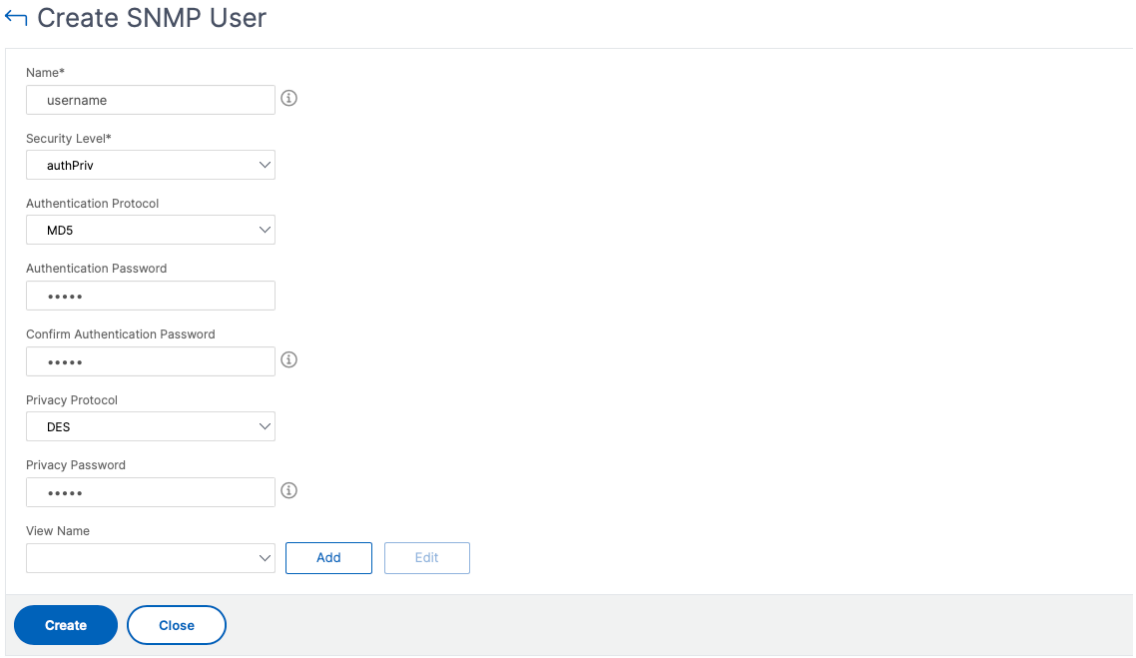
     次のセキュリティレベルのいずれかを選択します。
   - **noAuthNoPriv**. 認証も暗号化も必要ありません。



- **authNoPriv**. 認証は必須ですが、暗号化は必須ではありません。



- **authPriv**. 認証と暗号化が必要です。



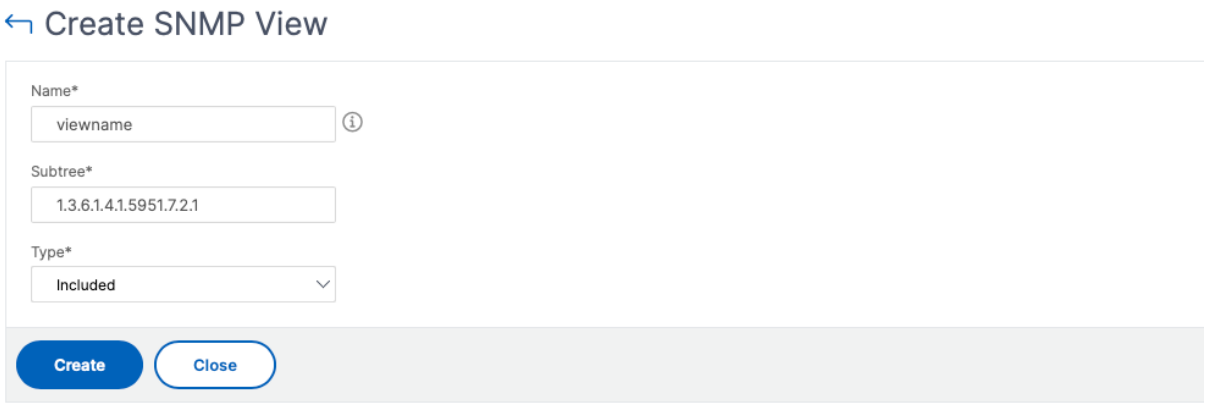
ユーザーに割り当てたセキュリティレベルに基づいて、認証プロトコル、プライバシーパスワードなどの追加の認証プロトコルを指定し、SNMP ビューの割り当てを行います。

SNMP ビューの管理

SNMP ビューは、SNMP ユーザーのアクセス制御を実装するために使用されます。SNMP ビューでは、ユーザアクセスが MIB の特定の部分に制限されます。

NetScaler ADM エージェントの SNMP OID を許可または制限するには:

1. **[**** インフラストラクチャ**] > [**エージェント**] > [SNMP** の管理] に移動し、[**SNMP** ビュー] タブで [追加] をクリックします。******
2. 「**SNMP** の作成」ビューで、次の詳細を入力します。
   - ビュー名:SNMP ビューの名前。インスタンスには、サブツリーのパラメータ設定によって区別される同じ名前の SNMP ビューを多数含めることができます。
   - サブツリー: この SNMP ビューに関連付けたい MIB ツリーの特定のブランチ (サブツリー)。サブツリーは SNMP OID として指定する必要があります。
3. [作成] をクリックします。



エージェント設定を行う

February 6, 2024

NetScaler ADM エージェントのキープアライブ間隔とパスワード変更の要件を変更できます。

エージェントのキープアライブ間隔を設定する

NetScaler ADM サーバーとエージェントは、指定されたキープアライブ間隔の間同じ TCP 接続を維持します。エージェントはこの接続を使用して、管理対象インスタンスのデータを NetScaler ADM サーバーに送信します。

1. [設定**] >** [管理] に移動します。
2. [****** システム構成**]** で **[**システム]、[タイムゾーン]、[許可された URL]、[エージェント設定]****** を選択します。
3. **[**基本設定**] > [**エージェント設定**]** で、キープアライブ間隔を 30 ～120 秒の範囲で指定します。
4. [保存] をクリックします。

現在のパスワードなしでエージェントのパスワードを変更

現在のパスワードがなくてもエージェントパスワードを変更できるようにすることができます。

1. [設定**] >** [管理] に移動します。
2. [****** システム構成**]** で **[**システム]、[タイムゾーン]、[許可された URL]、[エージェント設定]** を選択します。
3. **[**基本設定**] > [**エージェント設定**] > [**エージェントパスワード変更の現在のパスワード前提条件を削除する] チェックボックスでは、次の操作を行うことができます。
   - チェックボックスを選択すると、「****** エージェントパスワードの変更」ページの「現在のパスワード ** 」フィールドが削除されます。
   - チェックボックスをオフにすると、[エージェントパスワードの変更**]** ページの **[**** 現在のパスワード **] フィールドがそのままになります。
4. ［保存］をクリックします。

> 注
>
> エージェントパスワードの変更ページを表示するには、[インフラストラクチャ**] > [**インスタンス**] > [**エージェント] に移動し、エージェントを選択し、[アクションの選択**] > [**パスワードの変更] をクリックします。

データストレージ管理ダッシュボードを使用する

February 6, 2024

NetScaler ADM で使用されている機能と、これらの各機能のデータ使用量を把握することが重要です。データストレージ管理ダッシュボードはこの目的を果たし、視覚化ツールとして機能し、さまざまな機能にわたって NetScaler ADM データベースに格納されているデータの合計を把握できるようにします。ダッシュボードには、消費されたストレージが指定された制限内にあるのか、それとも資格のあるストレージを超えているのかも表示されます。

管理者は、データストレージ管理ダッシュボードで次のタスクを実行できます。

- 過去 30 日間のデータストレージ使用量を表示する-データストレージの傾向は、過去 30 日間の NetScaler ADM データベースに保存されます。これらの傾向は、グラフ形式または表形式で確認できます。これらの傾向は、NetScaler ADM でスケジュールされたプルーニングサイクルの後に受信されたデータ量と保存されたデータ量を示しています。
- データ取り込みステータスの表示-データ取り込みアクティビティは、使用済みストレージが資格のあるストレージの制限内である限り実行されます。使用中のストレージが資格のあるストレージを超えると、データアクティビティは一時停止されます。

- 通知を送信-使用済みストレージが資格のあるストレージの 75% または 100% に達したときに通知を送信するように設定できます。これにより、ユーザーは自分のストレージを管理できます。
- データストレージスペースを柔軟に管理-削除または削減に適していると思われるデータを削除することで、保存されたデータ内のスペースを増やすことができます。

[設定] **>** [データストレージ管理] に移動して、データストレージダッシュボードを表示します。

以下のセクションでは、データストレージ管理ダッシュボードを使用して効果的なデータストレージ管理を行う方法の概要を説明します。

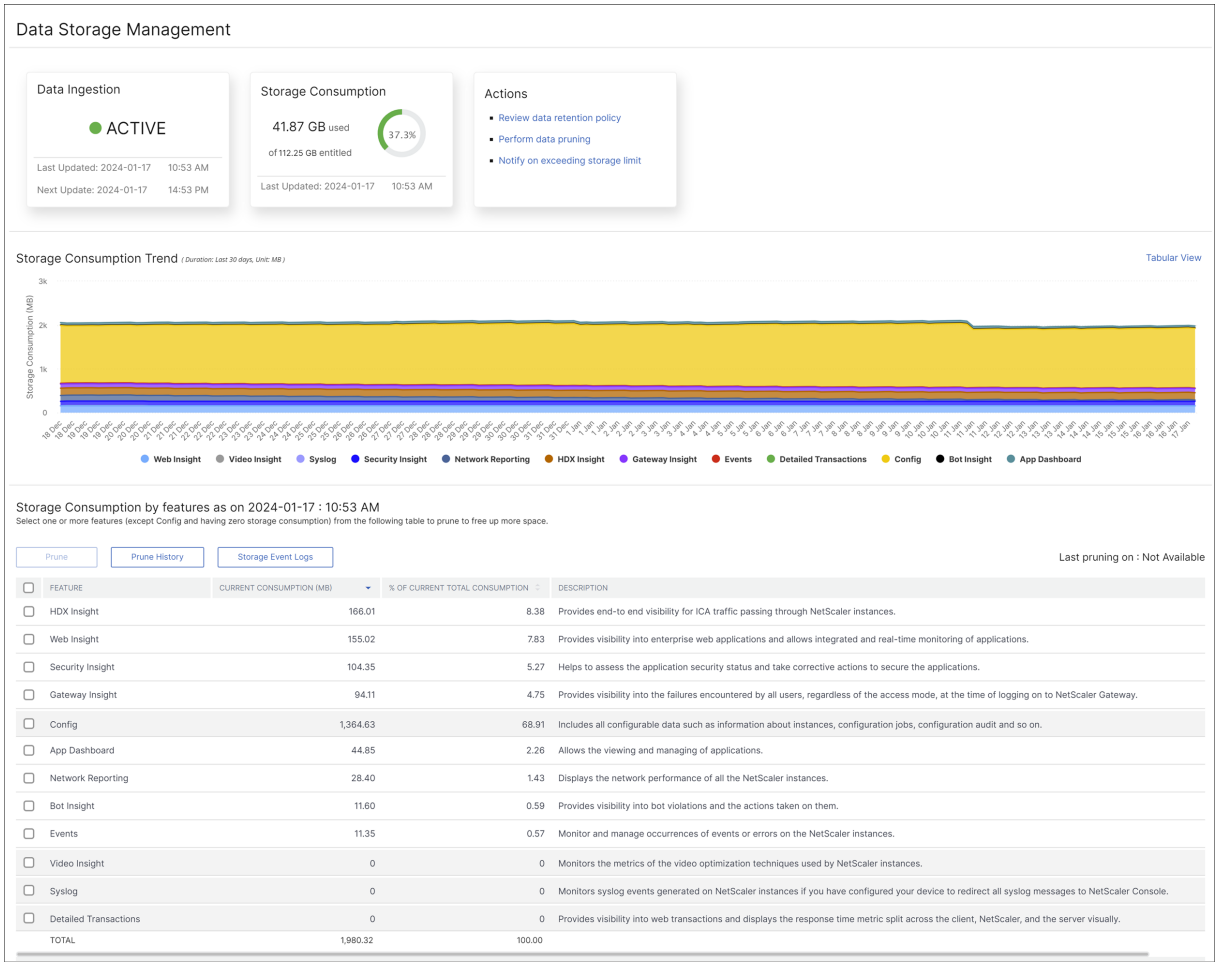
- データストレージについて理解する -このセクションは、ダッシュボードを使用してデータストレージに関する情報を表示する方法を理解するのに役立ちます。
- データストレージの管理 -このセクションでは、データストレージを管理するためにダッシュボードで実行できるアクションについて説明します。

データストレージを理解する

February 6, 2024

NetScaler **ADM** のデータストレージ管理ダッシュボードを使用して、データストレージの使用状況を追跡するのに役立つデータとグラフを表示できます。

データストレージの消費量を監視するには、[設定] **>** [データストレージ管理] に移動します。



データストレージ管理ダッシュボードには、次の情報が表示されます。

- データ取り込みアクティビティの状態
- 総ストレージ消費量
- ストレージ消費トレンド
- 機能別のストレージ消費量

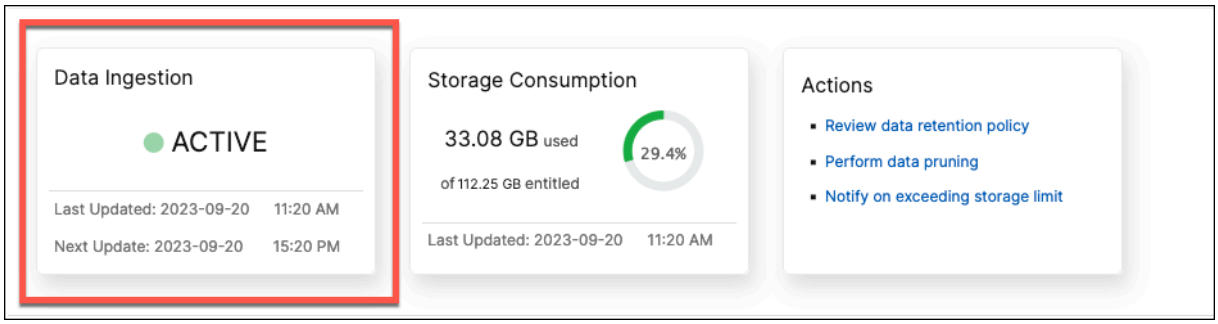
データ取り込みアクティビティの状態

データ取り込みとは、イベント、Syslog、ネットワークレポートなどのさまざまな機能を使用して、管理対象のすべての NetScaler インスタンスから、NetScaler ADM ストレージに大規模で多様なデータをインポートするプロセスを指します。

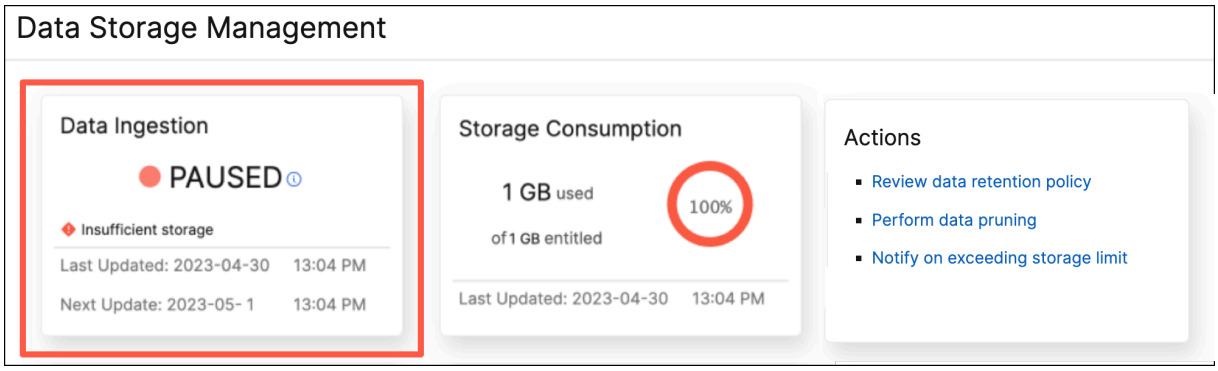
データ取り込みステータスには、NetScaler ADM が NetScaler インスタンスから統計を収集しているかどうかが示されます。データ取り込みアクティビティは、使用したストレージが資格のあるストレージ内にある限り継続されます。使用量が資格のあるストレージを超えると、データの取り込みは一時停止されます。

データ取り込みタイルを表示して、現在のデータ取り込みの状態を把握できます。このタイルには、次の 2 つの状態のいずれかが表示されます。

- アクティブ -データ取り込みアクティビティが進行中です。



- 一時停止-使用済みストレージが資格のあるストレージを超えているため、データ取り込みアクティビティは一時停止されます。

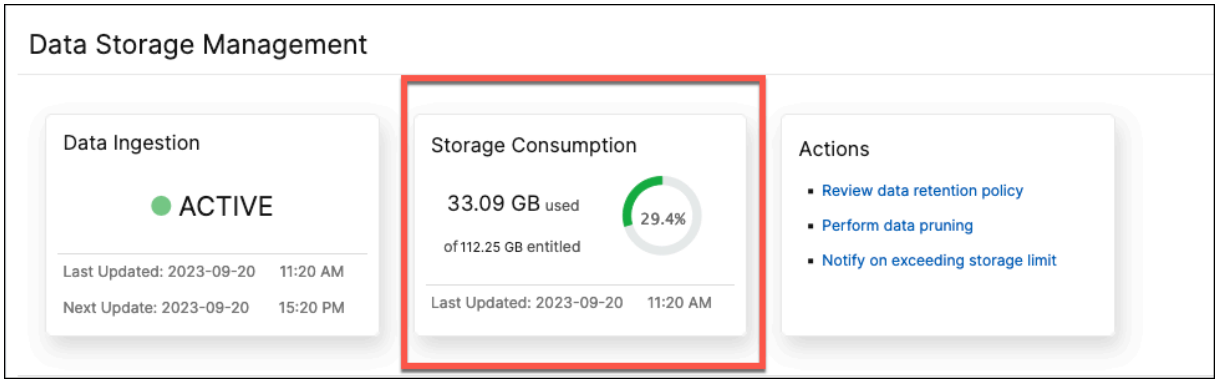


一時停止したデータ取り込みを再開する方法

データ取り込みアクティビティを再開するには、データプルーニングを実行します。詳細については、「データプルーニングの実行」を参照してください。

総ストレージ消費量

データストレージの概要については、「ストレージ消費量」タイルをご覧ください。



ストレージ消費量タイルには、デプロイ内のすべての機能が使用しているストレージの合計が表示されます。

ドーナツチャートにカーソルを合わせると、以下が表示されます。

資格のあるストレージ

使用資格のあるストレージとは、ライセンスに従って使用できるストレージの合計です。Express ライセンスをお持ちの場合は、500 MB のストレージをご利用いただけます。Advanced ライセンスをお持ちの場合は、購入した VIP ごとに 500 MB のストレージと、VIP を購入せずに直接購入した追加ストレージの合計が 500 MB になります。

以下のシナリオを考えてみましょう。

- VIP を 20 個購入しました。VIP ごとに 500 MB の無料ストレージを利用できます。使用資格のあるストレージは 20*500 = 10 GB です。
- 20 台の VIP と 5 GB のアドオンストレージを購入しました。VIP ごとに 500 MB の無料ストレージを利用できます。利用資格のあるストレージは 20*500 + 5 = 15 GB です。

消費済みストレージ

消費ストレージは、展開内のすべての機能が使用するストレージの合計です。次の色分け基準は、機能が使用するストレージの量を指定します。

- 緑 -使用済みストレージは、使用済みストレージの 75% 未満です。
- オレンジ -使用済みストレージは、使用権限のあるストレージの 75% ～99% です。
- 赤 -使用済みストレージの上限が、現在使用資格のあるストレージに達しているか、それを上回っています。

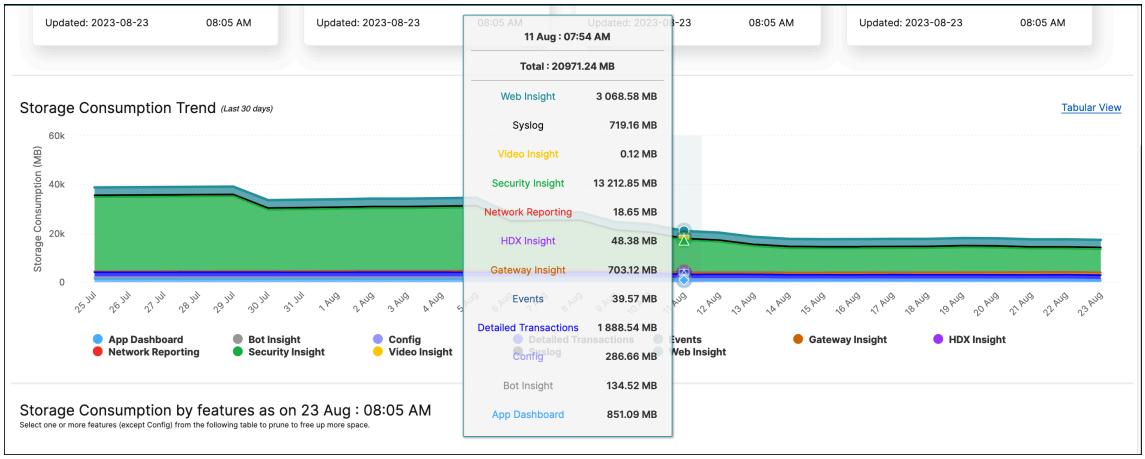
ストレージ消費トレンド

過去 30 日間のデータ消費状況を確認するには、「ストレージ消費トレンド」セクションをご覧ください。

Storage Consumption Trend は、ある期間にどの機能がストレージを最も多く使用したか、または最も少なく使用したかを把握し、データストレージ消費量を効果的に管理するのに役立ちます。

ストレージデータの傾向は、次のいずれかの形式で表示できます。

- グラフィカルビュー—データストレージがさまざまな NetScaler ADM 機能にどのように分散されているかを表示します。タイムラインの上にマウスを置くと、その月の任意の日のデータストレージ情報が表示されます。



> 注:
>
> グラフィカルビューがデフォルトビューです。

- 表形式ビュー—表形式ビューをクリックすると、データストレージ情報が表形式で表示されます。

> 注:
>
> 表形式ビューでは、検索フィールドを使用してデータをフィルタリングできます。

次の表では、「ストレージ消費トレンド」セクションに表示されるフィールドについて説明します。

機能	説明
構成	インスタンス、構成ジョブ、構成監査などに関する情報など、設定可能なすべてのデータが含まれます。

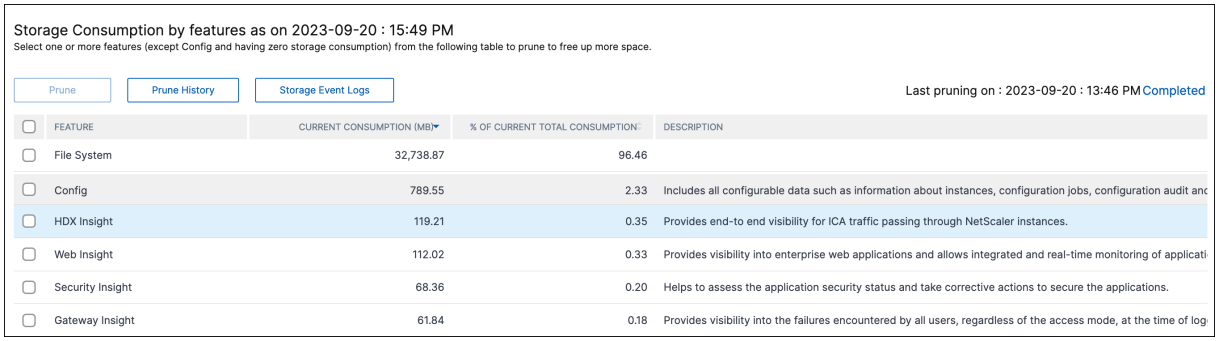
機能	説明
HDX Insight	NetScaler ADC を通過する ICA トラフィックのエンドツーエンドの可視性を提供します。
ネットワークレポート作成	すべての NetScaler ADC インスタンスのネットワークパフォーマンスを表示します。
Web Insight	エンタープライズウェブアプリケーションを可視化し、アプリケーションの統合的かつリアルタイムな監視を可能にします。
Security Insight	アプリケーションのセキュリティステータスを評価し、アプリケーションを保護するための是正措置を講じるのに役立ちます。
Gateway Insight	NetScaler Gateway へのログオン時に、アクセスモードに関係なく、すべてのユーザーが遭遇した障害を可視化します。
イベント	NetScaler インスタンスでのイベントやエラーの発生を監視および管理します。
アプリダッシュボード	アプリケーションの表示と管理を可能にします。
ボットのインサイト	ボットの違反とそれに対して実行されたアクションを可視化します。
Syslog	すべての syslog メッセージを NetScaler ADM にリダイレクトするようにデバイスを構成している場合、NetScaler インスタンスで生成された syslog イベントを監視します。
Video Insight	NetScaler インスタ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ます。
詳細な取引	Web トランザクションを可視化し、クライアント、NetScaler、およびサーバーに分割された応答時間メトリックを視覚的に表示します。

機能別のストレージ消費量

データストレージがさまざまな機能にどのように分散されているかについて詳しくは、「*dd mmm*」セクションの「機能別のストレージ消費量」を参照してください。

***dd**mmm** に記載されている機能別のストレージ消費量は、以下の内容を理解するのに役立ちます。

- NetScaler ADM のさまざまな機能によって使用されるストレージ容量
- 特定の日に機能が消費するスペースの割合



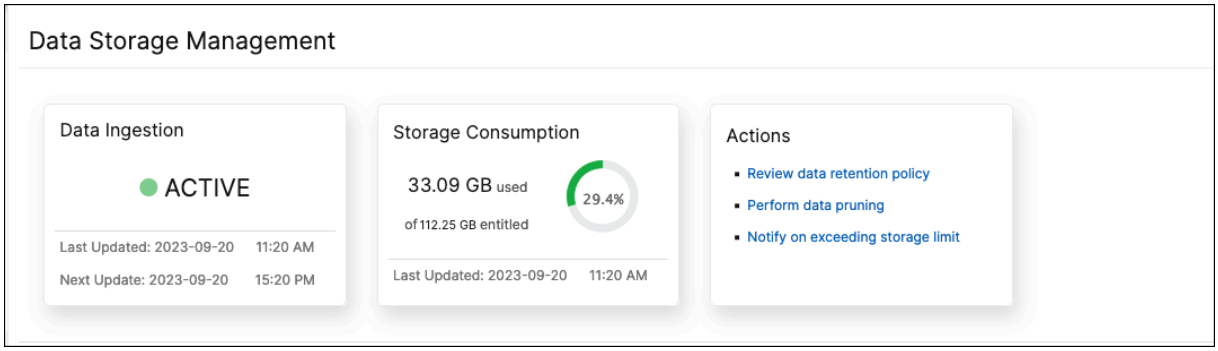
テーブルエントリ、つまりテーブルのヘッダーをソートしたい場合。NetScaler ADM は、選択した列のデータに基づいて、テーブルを上から下にアルファベット順に並べ替えます。テーブルを逆の順序でソートするには、列見出しをもう一度クリックします。

データ、プルーニング履歴、ストレージイベントログの削除について詳しくは、「データストレージの管理」を参照してください。

ストレージスペースを管理

February 6, 2024

データストレージ管理ダッシュボードを使用して、データストレージの使用状況を監視し、データストレージがライセンス制限を超えたときにスペースを空けるか、ストレージを増やすために必要なアクションを実行できます。



アクションタイルには、ストレージ容量を管理するために実行できる推奨手順のリストが表示されます。

- データ保持ポリシーを確認
- データプルーニングを実行
- ストレージ制限を超えたときに通知する

データプルーニングを実行

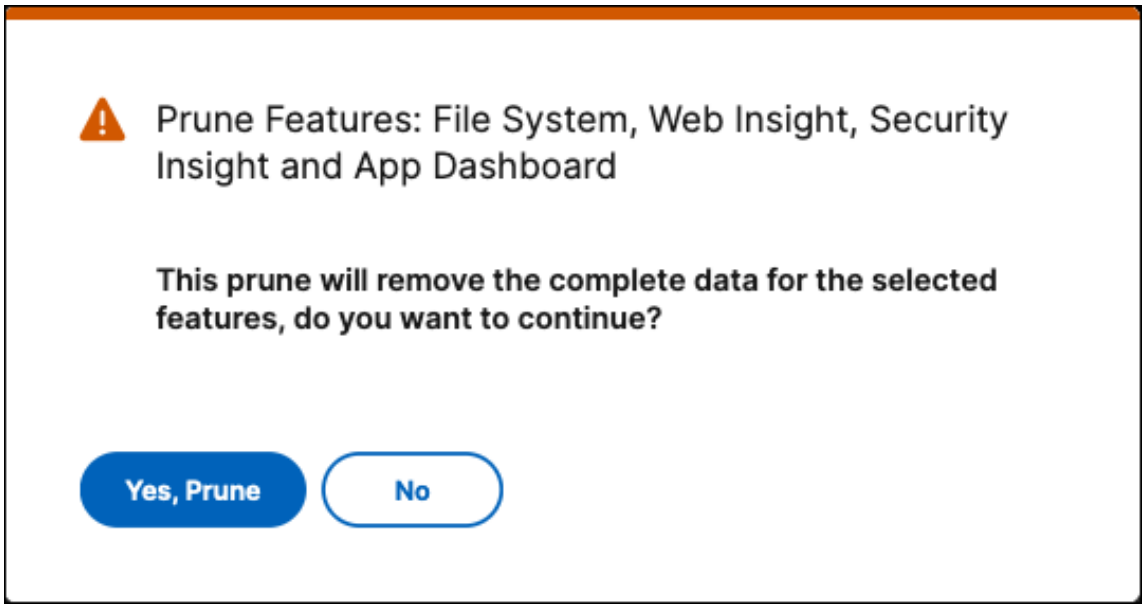
データを整理してストレージリソースを最適化し、ストレージ容量を増やします。データプルーニングは、スペースを解放するだけでなく、データ品質を高め、処理時間を短縮します。不要なデータを定期的に確認して削除すること

をお勧めします。このプロセスにより、リソースが慎重に使用され、NetScaler ADM の俊敏性と応答性が確保されます。

データを削除するには:

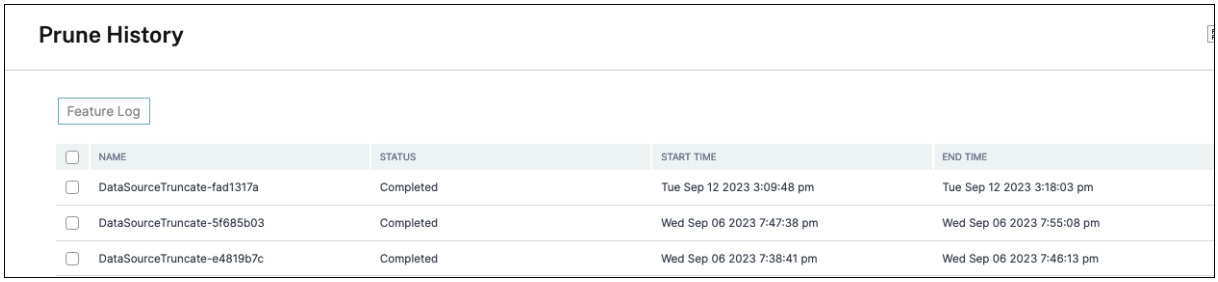
1. 「データストレージ管理」ページで、「***yyyy-mm-dd***」セクションの「機能別のストレージ消費量」までスクロールします。
2. 1 つまたは複数の機能を選択し、[プルーン] をクリックします。Config にはすべてのシステム構成が含まれているため、「**Config** 」を選択することはできません。

   ポップアップウィンドウが開き、選択したフィーチャのデータをすべて削除するかどうかの確認を求められます。[はい、プルーニング] をクリックします。



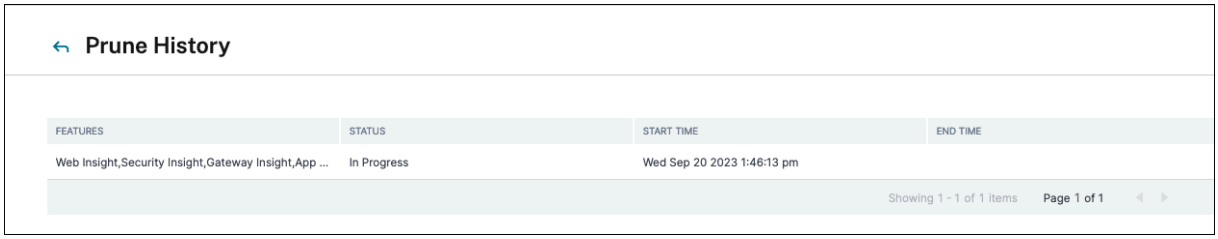
プルーンの履歴を表示

「プルーニング履歴の表示」をクリックすると、NetScaler ADM で行ったすべてのプルーニングアクティビティの詳細が表示されます。



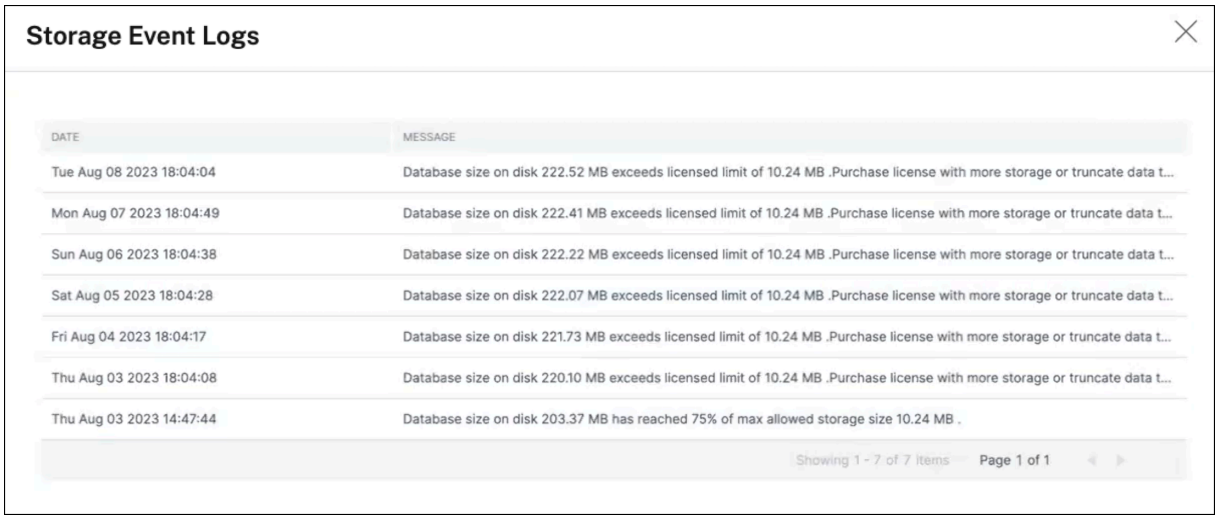
プルーニングログ**:** タスクログページには、それぞれのステータス、開始時間、終了時間を含むすべてのプルーニングタスクのリストが表示されます。

各プルーニング操作でどの機能が削除されたかを確認するには、タスクを選択して [機能ログ] をクリックします。



ストレージイベントログを表示する

「ストレージイベントログ」をクリックすると、データがライセンス制限の 75% を超えたり、に達した回数をすべて把握できます。



データ保持ポリシーを確認

データ保存ポリシーとは、NetScaler ADM が長期にわたって履歴データを管理および維持する方法を決定する一連のルールと構成を指します。このポリシーは、データが自動的に削除されるまでのデータの保存期間を概説しています。

さまざまな機能によって使用されるストレージ容量を削減したい場合は、NetScaler ADM にデータを保持する期間を変更できます。

データ保持ポリシーページを使用して、以下のデータストレージ設定を編集します。

- イベントメッセージ
- Syslog メッセージ
- ネットワークレポートデータ

データストレージ設定の詳細については、「データ保持ポリシー」を参照してください。

ストレージ制限を超えると通知する

データストレージ容量が指定された制限を超えたときにアラートを送信するように NetScaler ADM の通知を設定できます。

システム通知を表示して設定するには:

1. 「アクション」タイルで、「ストレージ制限を超えると通知する」をクリックします。
2. 「システム通知の設定」ページの「システムイベント」カテゴリで、通知を受信する「**DataStorageExceeded**」カテゴリが選択されていることを確認します。

自分や他のユーザーに通知を送信する方法とタイミングに関するさまざまなパラメータを指定できます。希望する通信方法 (メール、Slack、PagerDuty、ServiceNow 通知など) を選択し、通知の受信者を定義します。

プロファイルを設定して通知を送信する方法の詳細については、「通知の設定」を参照してください。

データ保持ポリシー

February 6, 2024

NetScaler ADM サーバーのデータベースに保存されるレポートデータの量を制限するには、NetScaler ADM がネットワークレポートデータ、イベント、監査ログ、およびタスクログを保持する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. [設定**] > [**データストレージ管理**] > [**データ保持ポリシー] に移動します。
2. 「データプルーニング」ページで、「システム」をクリックします。
3. 「システム」ページで、次の詳細を入力します。

    - 保存するデータ **(**日数**)** -データを保持する必要がある日数を入力します。1 から 30 までの値を指定する必要があります。
    - データプルーニングしきい値 **(%)** -データプルーニングまたはデータクリーンアッププロセスの条件として設定するしきい値制限 (パーセンテージ) を入力します。データベース内のデータが、指定されたストレージ容量の割合に達すると、データプルーニング手順がトリガーされ、データが削除され、スペースが解放されます。
    - 自動プルーニングの詳細 - 次のいずれかの基準が満たされた場合にデータプルーニングを開始する場合は、「自動データプルーニングを有効にする」を選択します。
        - データプルーニングしきい値 **(%)** で指定されたデータしきい値に達しました。
        - [保存するデータ **(**日数**)]** の値で指定した日数に達した。

- データ取り込み設定 -データ取り込みの条件として設定する閾値制限 (パーセンテージ) を入力します。データベース内のデータがこの指定された割合に達すると、データ取り込みアクティビティは一時停止されます。50% から 80% の範囲で制限を指定する必要があります。

4. [保存] をクリックして設定を保存します。

インスタンスの **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. [設定**] > [**データストレージ管理**] > [**データ保持ポリシー] に移動します。
2. 「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。
3. 「**Syslog** 汎用データを保存」フィールドに、1 から 180 までの日数を指定します。
4. ［保存］をクリックします。

インスタンスイベントプルーニング設定の構成

NetScaler ADM サーバーのデータベースに保存されるイベントメッセージデータの量を制限するために、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. [設定**] > [**データストレージ管理**] > [**データ保持ポリシー] に移動します。
2. 「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。
3. 「保持するデータ（日数）」フィールドに、**NetScaler ADM** サーバー上のデータを保持する期間を日単位で入力し、「保存」をクリックします。

ネットワークレポートのプルーニング設定の設定

NetScaler ADM に保存されるネットワークレポートデータを制限するには、ネットワークレポートの履歴データを保持する間隔を指定できます。

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. [設定**] > [**データストレージ管理**] > [**データ保持ポリシー] に移動します。
2. [データプルーニング] ページで、[ネットワークレポート] をクリックします。

3.「保存するデータ **(**日数**)** 」フィールドに、1 から 30 までの日数を指定します。

4.［保存］をクリックします。

API プロキシサーバーとしての **NetScaler ADM**

February 6, 2024

NetScaler Application Delivery Management （NetScaler 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、管理対象インスタンスの REST API プロキシサーバーとしても機能できます。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 NetScaler ADM に送信できます。NetScaler ADM は、応答する必要がある API リクエストと、変更せ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。

NetScaler ADM は API プロキシサーバーとして次のようなメリットがあります。

- **API** 要求の検証：NetScaler 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）ポリシーに照らして検証します。NetScaler ADM はテナント認識機能も備えているため、API アクティビティがテナントの境界を越えないようにします。
- 集中監査：NetScaler ADM は、管理対象インスタンスに関連するすべての API アクティビティの監査ログを保持します。
- セッション管理：NetScaler ADM は、API クライアント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。

NetScaler 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。

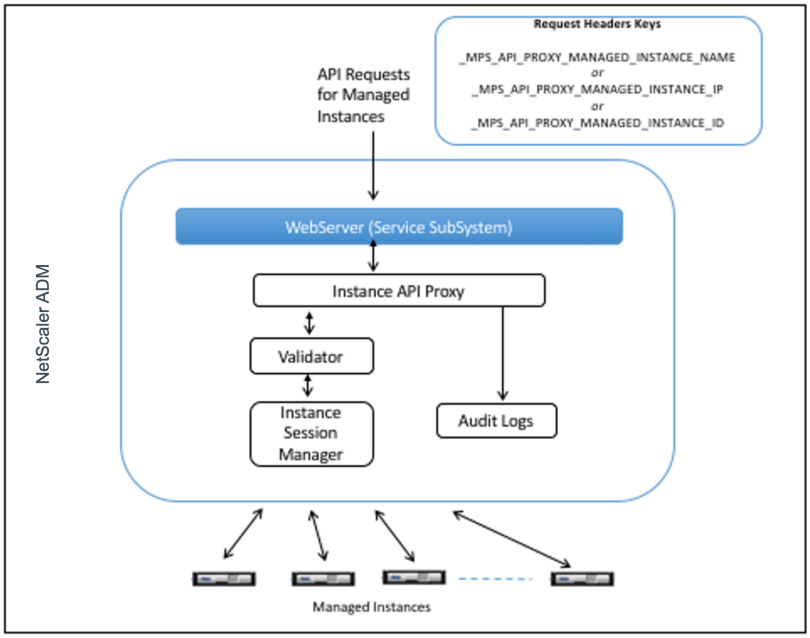
ヘッダー値	説明
_MPS_API_PROXY_MANAGED_INSTANCE_NAME	管理対象インスタンスの名前。
_MPS_API_PROXY_MANAGED_INSTANCE_IP	管理対象インスタンスの IP アドレス。
_MPS_API_PROXY_MANAGED_INSTANCE_ID	管理対象インスタンスの ID。
MPS_API_PROXY_TIMEOUT	NITRO API 要求のタイムアウト値。タイムアウト値を秒単位で設定します。プロキシタイムアウトを設定すると、ADM は要求がタイムアウトするまで指定された期間待機します。

ヘッダー値	説明
_MPS_API_PROXY_MANAGED_INSTANCE_USERNAME	管理対象 ADC インスタンスにアクセスするためのユーザー名。
MPS_API_PROXY_MANAGED_INSTANCE_PASSWORD	管理対象の ADC インスタンスにアクセスするためのパスワード。
MPS_API_PROXY_MANAGED_INSTANCE_SESSID	管理対象インスタンスにアクセスするためのセッション ID。

> 注:
>
> [設定] > [管理] > [システム構成] > [基本設定] で、[インスタンスログインの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、NetScaler ADM がリクエストの転送先とな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. リクエストを変更せずに、NetScaler ADM はリクエストをインスタンス API プロキシエンジンに転送します。

2. インスタンス API プロキシエンジンは API 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. [設定] **>** [管理] に移動します。
> 2. [システム構成] で、[システム]、[タイムゾーン]、[許可された **URL**]、[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 NetScaler ADM サーバーに送信する REST API リクエストを示しています。NetScaler ADM は、IP アドレス 192.0.2.10 の管理対象インスタンスにリクエストを変更せずに転送する必要があります。すべての例で _MPS_API_PROXY_MANAGED_INSTANCE_IP ヘッダーを使用します。

NetScaler ADM に API リクエストを送信する前に、API クライアントは次のことを行う必要があります。

- NetScaler ADM にログインします
- 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。

```
    POST /nitro/v1/config/login
    Content-Type: application/json

    {

        "login": {

            "username":"nsroot",
            "password":"nsroot"
          }

     }

<!--NeedCopy-->
```


NetScaler ADM は、セッション ID を含む応答でログオン要求に応答します。次のサンプル応答本文は、セッション ID を示しています。


```
{


  "errorcode": 0,

  "message": "Done",

  "operation": "add",

  "resourceType": "login",

  "username": "**********",

  "tenant_name": "Owner",

  "resourceName": "nsroot",

  "login": [

    {


      "tenant_name": "Owner",

      "permission": "superuser",

      "session_timeout": "36000",

      "challenge_token": "",

      "username": "",

      "login_type": "",

      "challenge": "",

      "client_ip": "",

      "client_port": "-1",

      "cert_verified": "false",

      "sessionid": "##
    D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",

      "token": "b2f3f935e93db6a"
     }


  ]
```



```
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: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5 <!--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/lbvserver/sample_lbvserver
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          "lbvserver":{
10
11             "name":"sample_lbvserver",
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。


```
    PUT /nitro/v1/config/lbvserver
    Content-type: application/json
    Accept-type: application/json
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    SESSID: ##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D

    {

       "lbvserver":{

            "name":"sample_lbvserver",
            "appflowlog":"DISABLED"
        }

     }

<!--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。

```
    DELETE /nitro/v1/config/lbvserver/sample_lbvserver
    Accept-type: application/json
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    SESSID: ##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D

<!--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。

```
    GET /nitro/v1/config/nsrunningconfig
    Accept-type: application/json
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    SESSID: ##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D

<!--NeedCopy-->
```


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] > [**NetScaler**] に移動し、分析を有効にする NetScaler インスタンスを選択します。
2. **[** アクションの選択] リストから、[**Analytics** の設定] を選択します。
3. [**Analytics** の構成] ページで、分析を有効にするすべての仮想サーバーを選択し、[**AppFlow** を有効にする] をクリックします。詳しくは、「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 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

いや。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実行されます。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、あなたが 120GB の NetScaler ADM 仮想マシンディスク容量を 200GB に増やすと想定しましょう。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 インスタンスでコレクタが構成されていないとはどういう意味ですか**?**

コレクターは、NetScaler アプライアンスによって生成された AppFlow レコードを受信します。

AppFlow 機能が有効になっている場合、NetScaler ADM は NetScaler 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 インスタンスが NetScaler ADM に追加されます。コレクタが 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。詳細については、「フォールバックローカル認証」を参照してください。

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。

NetScaler ADM で、［設定］**>**［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 インスタンス、NetScaler SDX インスタンス、仮想サーバーなどを管理する権限で、そのグループのユーザーがこれらのインスタンスまたは仮想サーバーのみを管理できるようにします。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。

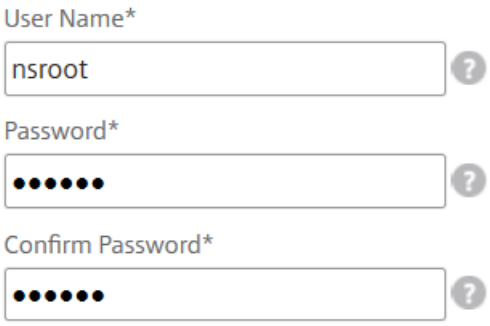
1. NetScaler ADM で、［設定］**>**［ユーザー管理］**>**［ユーザー］に移動します。

   [ユーザ**]** 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。

   [システムユーザの設定] ページが表示されます。

3. [パスワードの変更] を選択し、任意のパスワードを作成します。



4. ［**OK**］をクリックします。

   これで、新しいパスワードを使用して GUI、ハイパーバイザー、または SSH コンソールからログオンできるようになりました。

   > 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。設定 **>** デプロイメントに移動します。

   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。設定 **>** デプロイメントに移動します。

   「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. 設定 **>** デプロイメントに移動します。

   「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** プロセッサーをサポートしていますか

AMD プロセッサーは以下でサポートされています。

- **NetScaler ADM 13.1** ビルド **4.43** 以降。
- **NetScaler ADM** エージェント **13.1** ビルド **17.42** 以降。

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ーには適用されないため、ブレーク **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** 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、NetScaler ADM インフラストラクチャ全体で生成される多くのイベントを簡単に監視できます。

特定の条件で規則を構成し、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 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。また、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。NetScaler ADM サーバーを使用して、管理対象インスタンスからの syslog、アプリケー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について詳しくは、「NetScaler 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 **NetScaler ADC** アプライアンスにはどのようなものがありますか

インスタンスとは、NetScaler ADM から検出、管理、監視したい NetScaler ADC アプライアンスまたは仮想アプライアンスのことです。これらのインスタンスは NetScaler ADM サーバーに追加する必要があります。次の NetScaler ADC アプライアンスと仮想アプライアンスを NetScaler ADM に追加できます。

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway

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となる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 で複数の **NetScaler VPX** インスタンスを再検出することはできますか**?**

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。

[インフラストラクチャ**] > [**インスタンス**] > [NetScaler] > [VPX**] に移動し、再検出するインスタンスを選択し、[アクション] 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 **NetScaler SDX** にインストールできますか**?**

いいえ

パブリック **IP** アドレスを使用して、**ADM** ソフトウェアに **NetScaler 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。

```
./mps/change_freebsd_password.sh <username> <password>
<!--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手順に従います。

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、[システム] > [システム管理] > [システム設定] に移動し、[ホスト名の変更] 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] に移動し、[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ティティを監視できます。

カウンターの値がしきい値を超えると、NetScaler ADM はパフォーマンス関連の問題を示す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設定して送信するには、[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。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 のパージとは何ですか

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 データをパージする間隔を指定できます。すべての汎用 Syslog データ、AppFirewall データ、NetScaler Gateway データが NetScaler ADM から削除されるまでの日数を指定できます。

NetScaler ADM で **NTP** サーバーを構成できますか**?**

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 サーバを設定するには、[システム] > [**NTP** サーバ] 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\ 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。NetScaler ADM バックアップファイルをダウンロードし、別の NetScaler 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。

高可用性ペアでインスタンスを復元する前に、バックアップファイルに保存されている IP アドレスと状態 (プライマリまたはセカンダリ) が元の HA 設定の 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。

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

はい。NetScaler ADCitrix 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** 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 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

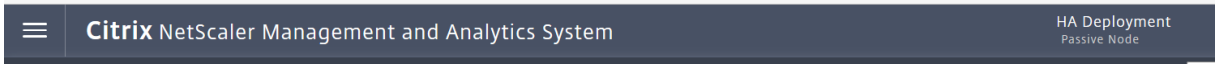
すべての NetScaler ADC インスタンスは、プライマリ NetScaler ADM ノードによって管理されます。

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。代替方法については、NetScaler サポートにお問い合わせください。

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

いいえ。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「Passive」というタグが付いており、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** 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/