NetScaler Application Delivery Management 12.1

Machine translated content

Disclaimer

Contents

リリースノート

February 6, 2024

NetScaler Application Delivery Management（ADM）12.1 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。12.1 リリースのリリースノートのセクションには、次のセクションがあります。

- 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。

詳細なリリースノートドキュメントを表示するには、次のリンクをクリックしてください。

リリースノート	公開日	バージョン
NetScaler ADM 12.1 リリースのビルド 62.21 のリリースロート	公開日：2021 年 5 月 13 日	リリースノートのバージョン:1.0
NetScaler ADM 12.1 リリースのビルド 61.18 のリリースロート	公開日：2021 年 2 月 4 日	リリースノートのバージョン:1.0
NetScaler ADM 12.1 リリースのビルド 60.16 のリリースノート	公開日：2020 年 11 月 6 日	リリースノートのバージョン:1.0
NetScaler ADM 12.1 リリースのビルド 59.16 のリリースノート	公開日：2020 年 9 月 28 日	リリースノートのバージョン:1.0
NetScaler ADM 12.1 リリースのビルド 58.14 のリリースノート	公開日：2020 年 8 月 20 日	リリースノートのバージョン:1.0
NetScaler ADM 12.1 リリースのビルド 57.18 のリリースノート	公開日：2020 年 6 月 11 日	リリースノートのバージョン:1.0
NetScaler ADM 12.1 リリースのビルド 56.22 のリリースノート	公開日：2020 年 3 月 30 日	リリースノートのバージョン:1.0
NetScaler ADM 12.1 リリースのビルド 55.13 のリリースノート	公開日：2019 年 11 月 7 日	リリースノートのバージョン:1.0
NetScaler ADM 12.1 リリースのビルド 54.13 のリリースノート	公開日：2019 年 9 月 20 日、9 月 26 日更新	リリースノートバージョン:2.0
NetScaler ADM 12.1 リリースのビルド 53.12 のリリースノート	公開日：2019 年 8 月 28 日	リリースノートバージョン:3.0

リリースノート	公開日	バージョン
NetScaler ADM 12.1 リリースのビルド 52.15 のリリースノート	公開日：2019 年 6 月 10 日	リリースノートのバージョン:1.0
NetScaler ADM 12.1 リリースのビルド 50.43 のリリースノート	公開日：2019 年 5 月 17 日	リリースノートバージョン:2.0
NetScaler ADM 12.1 リリースのビルド 50.39 のリリースノート	公開日：2019 年 5 月 17 日	リリースノートバージョン:2.0
NetScaler ADM 12.1 リリースのビルド 50.33 のリリースノート	公開日：2019 年 4 月 16 日	リリースノートのバージョン:1.0
NetScaler ADM 12.1 リリースのビルド 50.30 のリリースノート	公開日：2019 年 1 月 14 日	リリースノートのバージョン:1.0
NetScaler ADM 12.1 リリースのビルド 50.28 のリリースノート	公開日：2018 年 12 月 1 日	リリースノートのバージョン:1.0
NetScaler ADM 12.1 リリースのビルド 49.23 のリリースノート	公開日：2018 年 8 月 29 日	リリースノートのバージョン:1.0
NetScaler ADM 12.1 リリースのビルド 48.18 のリリースノート	公開日：2018 年 6 月 18 日	リリースノートバージョン:2.0

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

はじめに

February 6, 2024

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

NetScaler ADM の既存ユーザーの場合は、サーバーを最新リリースの Citrix [ADM にアップグレードする前に](/ja-jp/netscaler-application-delivery-management-software/12-1/upgrade.html)、リリースノート、システム要件 、およびライセンスの詳細を確認することをお勧めします 。

手順 **1-**システム要件を確認する

NetScaler ADM をデータセンターに導入する前に、ソフトウェア要件、ブラウザ要件、ポート情報、ライセンス情報、および制限を確認してください。

- ライセンス情報。ライセンスがないインスタンスとエンティティを数に限りなく管理し、監視することができます。ただし、ライセンスを適用しない場合、検出されたアプリケーションは 30 まで管理でき、仮想サーバーの分析情報の表示は 30 台までになります。31 以上のアプリケーションを管理し、または 31 台以上の仮想サーバーの分析情報を表示するには、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 ADC または SD-WAN インスタンス、または NetScaler ADC インスタンスと SD-WAN インスタンスの両方と通信するために必要なポートが開いていることを確認します。詳細情報。
- **NetScaler ADC** インスタンスの要件。さまざまな NetScaler ADM 機能が、さまざまな NetScaler ADC ソフトウェアバージョンでサポートされています。この情報を確認して、NetScaler ADC インスタンスを正しいバージョンにアップグレードしていることを確認します。詳細情報。
- **Citrix SD-WAN** インスタンスの要件。この情報を確認して、Citrix SD-WAN インスタンスを正しいバージョンにアップグレードし、正しいプラットフォームエディションがあることを確認します。詳細情報。

手順 **2-NetScaler ADM** を展開する

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

- 単一サーバーの導入。NetScaler ADM 単一サーバー展開では、データベースがサーバーと統合され、単一のサーバーがすべてのトラフィックを処理します。NetScaler ADM Citrix Hypervisor、VMware ESXi、Microsoft Hyper-V、Linux KVM とともに展開できる。参照:
  - Citrix Hypervisor を使用した NetScaler ADM
  - Microsoft Hyper-V を搭載した NetScaler ADM
  - VMware ESXi を使用した NetScaler ADM
  - Linux KVM サーバーを使用した NetScaler ADM

- 高可用性導入。2 台の NetScaler ADM サーバーの高可用性展開（HA）により、中断のない操作が可能になります。高可用性設定では、両方の NetScaler ADM ノードを同じソフトウェアバージョンとビルドを使用して同じサブネット上にアクティブ/パッシブモードで展開し、同じ構成にする必要があります。高可用性展開では、NetScaler ADM プライマリノードでフローティング IP アドレスを構成できるため、NetScaler ADC ロードバランサを別途用意する必要がなくなります。詳細については、「高可用性展開での構成」をご参照ください。

ステップ **3-NetScaler ADM** にインスタンスを追加する

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

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

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

詳しい情報

ステップ **4-**仮想サーバーでの分析を有効にする

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

詳しい情報

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

NetScaler ADM でネットワークタイムプロトコル（NTP）サーバーを構成して、そのクロックを NTP サーバーと同期させます。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。
- システム通知を設定します。さまざまなシステム関連機能について、ユーザーのグループを選択するために通知を送信できます。NetScaler ADM で通知サーバーを設定し、電子メールおよびショートメッセージサービス（SMS）Gateway サーバーを構成して、ユーザーに電子メールおよびテキスト通知を送信できます。これによりユーザーログインやシステムの再起動などの、システムレベルのアクティビティが管理者に通知されます。
- システム削除設定を構成します。NetScaler ADM サーバーのデータベースに保存されるレポートデータの量を制限するために、NetScaler ADM がネットワークレポートデータ、イベント、監査ログ、およびタスクログを保持する間隔を指定できます。デフォルトでは、これらのデータは 24 時間ごとに（00:00 の時刻に）削除されます。
- システムバックアップの設定を構成します。NetScaler ADM は、毎日 00:30 にシステムを自動的にバックアップします。デフォルトでは、3 つのバックアップファイルが保存されます。それ以上の数のシステムのバックアップを保持する必要があるかもしれません。
- インスタンスのバックアップ設定を構成します。NetScaler ADC インスタンスの現在の状態をバックアップする場合、インスタンスが不安定になった場合に備えて、バックアップファイルを使用して安定性を回復できます。アップグレードを実行する前にこれを行うことは特に重要です。デフォルトでは、12 時間ごとにバックアップされて、3 つのバックアップファイルがシステムに保持されます。
- インスタンスイベント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 Syslog 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 ADC インスタンスとアプリケーションの管理。NetScaler ADM のすべての機能は、NetScaler ADC インスタンスでサポートされています。いずれの機能も使用を開始できます。

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

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

すべての方法記事

February 6, 2024

NetScaler Application Delivery Management（NetScaler ADM）「ハウツー記事」は、NetScaler ADM の機能に関するシンプルで関連性が高く、実装が簡単な記事です。これらの記事には、インスタンス管理、アプリケーション管理、StyleBook、証明書管理、分析など、NetScaler ADM の一般的な機能に関する情報が含まれています。

次の表の機能名をクリックすると、各機能のハウツー記事の一覧が表示されます。

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

インスタンス管理

グローバルに分散したサイトを監視する方法

NetScaler ADC インスタンスの管理パーティションを管理する方法

NetScaler ADM にインスタンスを追加する方法

NetScaler ADM でインスタンスグループを作成する方法

NetScaler ADM でジオマップ用のサイトを構成する方法

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

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

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

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

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

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

HAProxy インスタンスに設定されているサーバーの詳細を表示する方法

NetScaler ADM から HAProxy インスタンスを再起動する方法

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

NetScaler ADM を使用して HAProxy 構成ファイルを編集する方法

複数の NetScaler ADC VPX インスタンスを再検出する方法

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

NetScaler ADM でインスタンスを管理解除する方法

NetScaler ADM からインスタンスへのルートをトレースする方法

構成管理

NetScaler ADM で構成ジョブを作成する方法

設定ジョブで SCP (put) コマンドを使用する方法

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

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

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

実行した設定ジョブを再利用する方法

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

NetScaler ADM の構成ジョブで変数を使用する方法

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

NetScaler ADM の修正コマンドから構成ジョブを作成する方法

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

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

レコードアンドプレイを使用して構成ジョブを作成する方法

構成ジョブを使用して、1 つのインスタンスから複数のインスタンスに構成をレプリケートする方法

NetScaler ADM でマスター構成テンプレートを使用する方法

NetScaler ADC インスタンスの構成監査をポーリングする方法

設定ジョブで構成監査テンプレートを再利用する方法

設定テンプレートをインポートおよびエクスポートする方法

ConfigChange SNMP トラップの設定監査差分を生成する方法

証明書管理機能

NetScaler ADM でエンタープライズポリシーを構成する方法

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

インストールした証明書を NetScaler ADM から更新する方法

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

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

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

NetScaler ADM で SSL ダッシュボードを使用する方法

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

アプリケーション管理

Citrix ADM でアプリケーション定義を作成する方法

StyleBook

StyleBook のさまざまなグループを表示する方法

Citrix ADM に同梱されている StyleBook の使用方法

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

ABR 動画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する方法

ABR 動画の最適化された再生時間と最適化されていない再生時間を比較する方法

最適化された ABR 動画と最適化されていない ABR 動画の帯域幅消費量を比較する方法

最適化された ABR 動画と最適化されていない ABR 動画で使用されるデータ量を比較する方法

ネットワークの効率を表示する方法

イベントの管理

NetScaler ADM でイベントのイベント経過時間を設定する方法

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

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

NetScaler ADM を使用してイベントを抑制する方法

イベントダッシュボードを使用してイベントを監視する方法

NetScaler ADM でイベントルールを作成する方法

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

NetScaler ADM でイベントの概要を表示する方法

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

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

NetScaler ADM でシステムログメッセージを非表示にする方法

インスタンスイベントのプルーニング設定を構成する方法

認証

外部認証サーバをカスケードする方法

RADIUS 認証サーバーを追加する方法

LDAP 認証サーバーを追加する方法

TACACS 認証サーバを追加する方法

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

Citrix ADC インスタンスを診断およびトラブルシューティングする方法

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

Citrix Application Delivery Management（ADM）は、管理者に企業全体の可視性を提供し、複数のインスタンスにわたって実行する必要のある管理ジョブを自動化することで運用を簡素化する一元管理ソリューションです。NetScaler ADC MPX、NetScaler ADC VPX、NetScaler ADC SDX、NetScaler ADC CPX、NetScaler Gateway、Citrix SD-WAN などのアプリケーションネットワーク製品を管理および監視できます。ADM を使用すると、単一の統合コンソールから、グローバルなアプリケーション配信インフラストラクチャ全体を管理、監視、トラブルシューティングできます。

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

- ユーザー・セッション・レベルの情報

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

ADM により、IT 管理者はわずか数分で顧客の問題をトラブルシューティングし、プロアクティブに監視することができます。

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。応答性の観点からアプリケーションが適切に機能しているか、脅威に対して脆弱でないか、すべてのシステムが稼働しているかどうかが表示されます。

アプリケーション・セキュリティ分析

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

ネットワーク

インスタンス

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

インスタンスグループ

次のようにインスタンスをグループ化できます。

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

イベントの管理

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

イベントは、マネージド 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い始めるには、SSL 証明書とは何か、また ADM を使用して SSL 証明書を追跡する方法を理解する必要があります。

構成管理

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

構成監査

インスタンスの構成を監視して、異常を特定できます。

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

ネットワークレポート作成

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

分析

Web Insight

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

HDX Insight

NetScaler ADC を通過する ICA トラフィックをエンドツーエンドで可視化します。管理者は、HDX Insight を通じて、リアルタイムのクライアントとネットワークの遅延測定基準、履歴レポート、エンドツーエンドのパフォーマンスデータを確認し、パフォーマンスの問題をトラブルシューティングできます。

Gateway Insight

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

Security Insight

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

SSL Insight

SSL Insight は、セキュアな Web トランザクション（HTTPS）を可視化し、IT 管理者は、セキュアな Web トランザクションのリアルタイムおよび履歴の統合監視を提供することで、NetScaler ADC によって提供されるすべてのセキュアな Web アプリケーションを監視できます。

TCP Insight

TCP Insight は、ADC インスタンスで使用される最適化手法と輻輳制御戦略（またはアルゴリズム）のメトリックを監視して、データ送信時のネットワークの輻輳を回避するための、簡単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 ADC インスタンスが使用するビデオ最適化手法の指標を監視するための簡単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 の分析機能を使用すると、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間を流れるアクセラレーションが有効および無効の WAN トラフィックを容易に監視できます。また WAN Insight では、ネットワーク上のクライアント、アプリケーション、支社の状態を把握できるので、ネットワーク問題を効果的にトラブルシューティングできます。

オーケストレーション

クラウドオーケストレーション

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

オーケストレーション

Citrix ADM は、さまざまなベンダーの SDN コントローラーと統合することにより、企業ネットワーク内の SDN をサポートします。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。

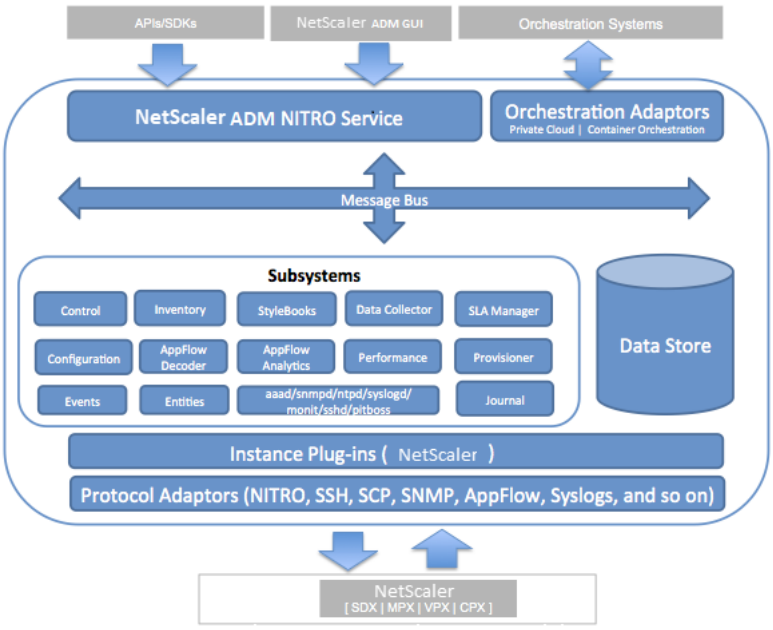
アーキテクチャ

February 6, 2024

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

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

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



ADM のサービスサブシステムは、ポート 80 と 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は、インベントリ、StyleBook、データコレクター、構成、AppFlow デコーダー、AppFlow 分析、パフォーマンス、イベント、エンティティ、SLA マネージャー、プロビジョナー、およびジャーナルで、それぞれが特定の役割を果たします。

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

NetScaler ADM によるインスタンスの検出方法

February 6, 2024

インスタンスとは、NetScaler Application Delivery Management（ADM）から検出、管理、監視したい Citrix アプライアンスまたは仮想アプライアンスです。これらのインスタンスを管理および監視するには、NetScaler ADM サーバーに追加する必要があります。次の Citrix アプライアンスと仮想アプライアンスを ADM に追加できます。

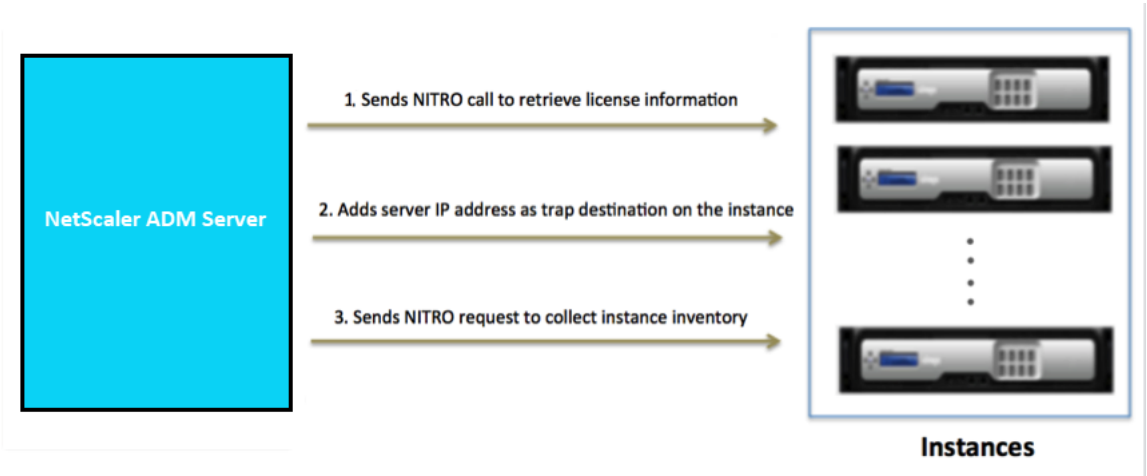
- Citrix ADC インスタンス
  - Citrix MPX
  - Citrix VPX
  - Citrix SDX
  - Citrix CPX
- NetScaler Gateway インスタンス
- Citrix SD-WAN インスタンス

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

> 注
>
> NetScaler ADM は、通信に NetScaler ADC インスタンスの NetScaler IP（NSIP）アドレスを使用します。ADM では、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。
>
> Citrix SD-WAN WO の場合、ADM はインスタンスの管理 IP アドレスを使用して通信します。
>
> ADM に Citrix SD-WAN SE/PE インスタンスを追加することはできません。Citrix SD-WAN SE/PE アプライアンスで、ADM を AppFlow ow コレクタとして構成できます。

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

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



図に示すように、次のステップは Citrx 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 呼び出しを使用して、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（Citrix ADC MPX、ADC VPX、ADC SDX、または Citrix Gateway など）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。

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

   この手順は、インスタンスプロファイルに正しい資格情報が含まれていない場合は失敗することがあります。ADC MPX、ADC VPX、ADC SDX、Citrix 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、この手順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。

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

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

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

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

ポーリングの概要

February 6, 2024

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

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

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

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

NetScaler ADM は、デフォルトで定期的にポーリングを自動的に行います。NetScaler ADM では、いくつかのポーリングタイプのポーリング間隔を構成したり、必要に応じて手動でポーリングしたりすることもできます。

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

ポーリングタイプ	ポーリング間隔	ポーリングされた情報	使用プロトコル	ポーリング間隔の設定
インスタンスのポーリング	5 分ごと (デフォルト)	状態、1 秒あたりの HTTP リクエスト数、CPU 使用率、メモリ使用量、スループットなどの統計情報。	NITRO コール。	いいえ
インベントリのポーリング	30 分ごと (デフォルト)	ビルドバージョン、システム情報、ライセンスされた機能、モードなどのインベントリの詳細。	NITRO コールと SSH	いいえ
パフォーマンスデータ収集	5 分ごと (デフォルト)	ネットワークレポート情報	NITRO コール	いいえ
インスタンスバックアップポーリング	12 時間ごと (デフォルト)	管理されている ADC インスタンスの現在の状態のバックアップファイル	NITRO 呼び出し、SSH、および SCP。	はい。[ネットワーク] > [インスタンス] > **[**Citrix ADC]** に移動します。インスタンスを選択し、**[**Select Action**] リストから [バックアップ/復元] をクリックします。
構成監査ポーリング	10 時間ごと (デフォルト)	ADC インスタンスで発生する構成変更 (実行中の構成と保存されている構成など)	SSH、SCP、および NITRO コール	はい。[ネットワーク] > [構成監査] に移動します。[構成監査] ページで、[設定] をクリックし、[構成監査ポーリング] のポーリング間隔を構成します。

ポーリングタイプ	ポーリング間隔	ポーリングされた情報	使用プロトコル	ポーリング間隔の設定
				構成監査を手動でポーリングし、インスタンスのすべての構成監査を直ちに NetScaler ADM に追加できます。これを行うには、[ネットワーク] > [構成の監査] に移動し、[今すぐポーリング] をクリックします。[**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 ADC インスタンスにインストールされている SSL 証明書。	NITRO コールと SCP	はい。[ネットワーク] > [**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、[ネットワーク] > [**SSL** ダッシュボード] に移動し、[今すぐポーリング] をクリックします。[**Poll Now**] ページでは、ネットワーク内のすべてのインスタンスまたは選択したインスタンスをポーリングできます。
エンティティのポーリング	30 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。	NITRO 呼び出し	はい。ただし、10 分未満に設定することはできません。設定するには、[ネットワーク] > [ネットワーク機能] に移動します。[ネットワーク機能] ページで、[設定] をクリックしてポーリング間隔を構成します。

ポーリングタイプ	ポーリング間隔	ポーリングされた情報	使用プロトコル	ポーリング間隔の設定
				エンティティを手動でポーリングし、インスタンスのすべてのエンティティを直ちに NetScaler ADM に追加できます。これを行うには、[ネットワーク] > [ネットワーク機能] に移動し、[今すぐポーリングする] をクリックします。[**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、**[**** ネットワーク] > [ネットワーク機能] > [設定] に移動して、要件に応じて間隔を設定できます。**

インスタンスの手動ポーリング

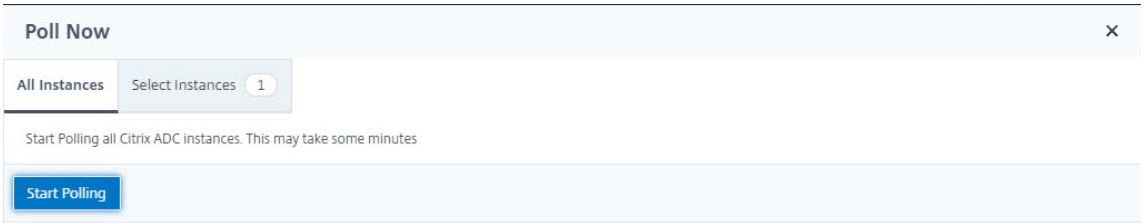
NetScaler ADM が多数のエンティティを管理している場合、ポーリングサイクルでレポートの生成に時間がかかり、画面が空白になったり、システムが以前のデータを表示したりする可能性があります。

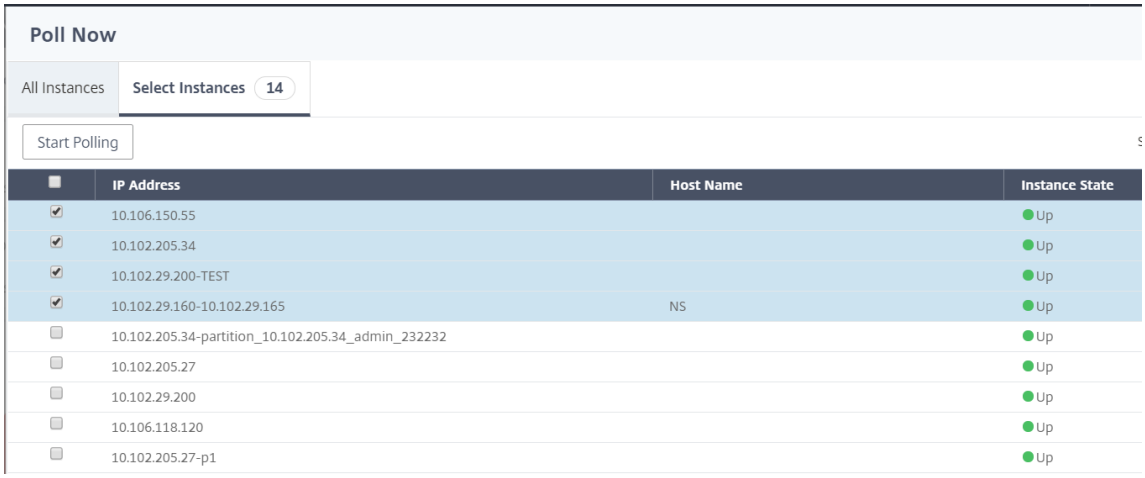
NetScaler ADM には、自動ポーリングが行われない最小ポーリング間隔があります。新しい NetScaler ADC インスタンスを追加した場合、またはエンティティが更新された場合、NetScaler ADM は次のポーリングが行われるまで、新しいインスタンスまたはエンティティに加えられた更新を認識しません。また、さらに操作を行うために仮想 IP アドレスの一覧をすぐに取得する方法はありません。最短のポーリング間隔期間が経過するまで待つ必要があります。手動でポーリングを実行して新しく追加されたインスタンスを検出することもできますが、これによって NetScaler ADC ネットワーク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、［ネットワーク］>［ネットワーク機能］に移動します。
2. [ネットワーク機能] ページの右上隅にある [今すぐポーリングする] をクリックします。
3. ポップアップページの「**Poll Now** 」には、ネットワーク内のすべての NetScaler ADC インスタンスをポーリングするか、選択したインスタンスをポーリングするかを選択できます。
   a) **All Instances** タブ- **Start Polling** をクリックしてすべてのインスタンスをポーリングします。
   b) **[** インスタンスを選択] タブ-リストからインスタンスを選択します。
4. [ポーリングの開始] をクリックします。





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

エンティティの手動ポーリング

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

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

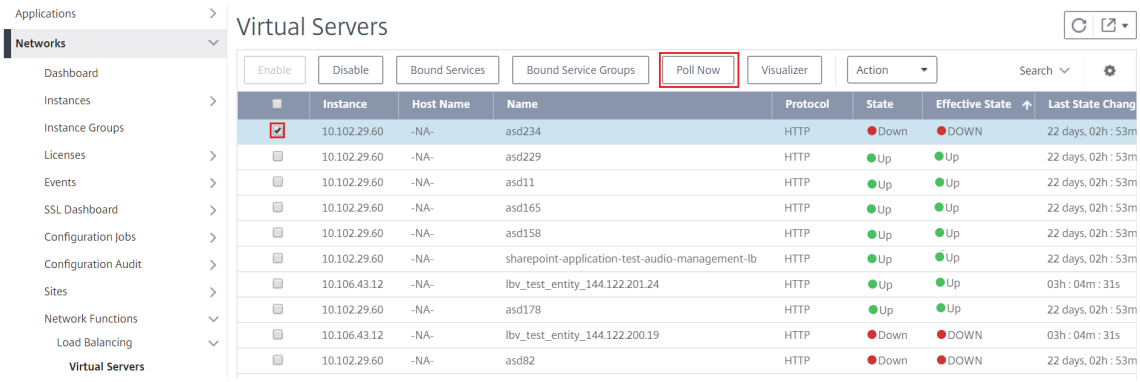
サービス、サービスグループ、負荷分散仮想サーバー、キャッシュ削減仮想サーバー、コンテンツスイッチング仮想サーバー、認証仮想サーバー、VPN 仮想サーバー、GSLB 仮想サーバー、およびアプリケーションサーバーをポーリングして、ステータスの更新を確認できるようになりました。

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

NetScaler ADM で特定のエンティティをポーリングするには:

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

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



データガバナンス

February 6, 2024

顧客認証は、認証された顧客またはユーザーのみにネットワークへのアクセスを許可することで組織のネットワークリソースを保護できるため、組織にとって非常に重要です。管理者は、ユーザーを Citrix ネットワーク内のリソースに接続させる前にユーザーを特定することが重要です。

12.1 リリース 50.x ビルド以降では、CitrixApplication Delivery Management（ADM）では、情報へのアクセスを開始する前に、ADM GUI で自分自身を認証する必要があります。ADM で認証する前に、Citrix クラウドサービスに自分自身を登録する必要があります。ADM GUI で Citrix クラウドユーザーの認証情報を指定する必要があります。詳しくは、「Citrix Cloud へのサインアップ」を参照してください。

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

新規ユーザーの場合のワークフロー

1. 選択した Hypervisor への NetScaler ADM のインストールを完了します。
2. 必要な IP アドレスをさまざまに設定します。
3. Web ブラウザで、NetScaler ADM の IP アドレスを入力します。
4. 「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。
5. [顧客 ID の設定] ページが開きます。ここで、Citrix Cloud の認証情報を使用して本人確認を行う必要があります。

   Citrix クラウドでアカウントを作成していない場合は、「Citrix Cloud」をクリックして登録してください。
6. 「認証」をクリックし、Citrix Cloud への登録に使用したメールアドレスを入力します。

7. [テレメトリ用にデータを共有することに同意します] の横にあるチェックボックスをオンにし、[送信] をクリックします。

既存ユーザーが **12.1** リリースの最新バージョンにアップグレードする場合のワークフロー

1. Citrix ADM を 12.1 リリースの最新バージョンにアップグレードした後、Web ブラウザで Citrix ADM 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. [顧客 ID の設定] ページが開きます。ここで、Citrix Cloud の認証情報を使用して本人確認を行う必要があります。

   Citrix クラウドでアカウントを作成していない場合は、「Citrix Cloud」をクリックして登録してください。
4.「認証」をクリックし、Citrix Cloud への登録に使用したメールアドレスを入力します。
5. [テレメトリ用にデータを共有することに同意します] の横にあるチェックボックスをオンにし、[送信] をクリックします。

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

- [システム] > [システム管理] に移動し、[認証] をクリックします。
- ADM GUI の右上にある雲のアイコンをクリックします。認証が成功すると、「X」は緑色のチェックマークに変わります。

> 注:
>
> 次のドメインがホワイトリストに登録されていることを確認してください。
>
> - *.citrixnetworkapi.net
> - *.blob.core.windows.net

Citrix ADM にデータをアップロードし、Citrix ADM の機能を使用することにより、Citrix がお客様の Citrix 製品およびサービスに関する技術情報、ユーザー情報、または関連情報を収集、保存、送信、維持、処理、および使用することに同意したものとみなされます。

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

ライセンス

February 6, 2024

Citrix ADC インスタンスが https プロトコルで検出された場合、Citrix ADC インスタンスを管理および監視するには、Citrix Application Delivery Management （ADM）の検証済み Citrix ADC ライセンスが必要です。

ライセンスがないインスタンスとエンティティを数に限りなく管理し、監視することができます。ただし、ライセンスを適用しない場合、アプリダッシュボードで管理できる検出済みアプリケーションは 30 個まで、分析データを確認できる仮想サーバーは 30 台までになります。31 個以上の検出済みアプリケーションを管理するか、または 31 台以上の仮想サーバーについて分析情報を確認するには、ライセンスを購入して適用する必要があります。

	NetScaler ADM 機能	[無料] 仮想サーバーの数に関係なく、Citrix ADM ライセンスは必要ありません	30 台以上の仮想サーバーには NetScaler ADM ライセンスが必要	NetScaler ADC ライセンス要件
分析	Web Insight	いいえ	はい	該当なし
	HDX Insight*	いいえ	はい	エンタープライズ (1 時間未満のレポート) プレミアム (レポート = 無制限)
	Security Insight	いいえ	はい	プレミアム (または) エンタープライズ with App Firewall ライセンス
	SSL Insight	いいえ	はい	該当なし
	Gateway Insight	いいえ	はい	エンタープライズ (1 時間未満のレポート) プレミアム (レポート = 無制限)
	TCP Insight	いいえ	はい	該当なし
	Video Insight	いいえ	はい	プレミアム (Citrix T 1000 シリーズ、VPX-T)
	WAN Insight	いいえ	該当なし	Citrix SD-WAN インスタンスは最適化エディション (WANOP) である必要があります
アプリケーション				

	NetScaler ADM 機能	[無料] 仮想サーバーの数に関係なく、Citrix ADM ライセンスは必要ありません	30 台以上の仮想サーバーには NetScaler ADM ライセンスが必要	NetScaler ADC ライセンス要件
	アプリケーション統計情報（アプリダッシュボード、アプリセキュリティダッシュボード）	いいえ	はい	アプリダッシュボードとアプリセキュリティダッシュボードの Citrix ADC Web App Firewall 関連情報には、プレミアム（または）エンタープライズ版アプリファイアウォールライセンスが必要です。
	「StyleBook」を参照してください	はい	いいえ	該当なし
ネットワーク				
	ライセンスサーバー	はい	いいえ	該当なし
	インベントリ管理—インフラストラクチャダッシュボード、インスタンスグループ、インスタンスダッシュボード、サイト	はい	いいえ	該当なし
	イベント管理および syslog	はい	いいえ	該当なし
	構成ジョブ、構成監査、構成アドバイス	はい	いいえ	該当なし
	ネットワークレポート（インスタンスレベル）	はい	いいえ	該当なし
	ネットワークレポート（仮想サーバーレベル）	はい	いいえ	該当なし

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

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

*Citrix Director を Citrix ADM サポートと統合するには、Citrix Director には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。

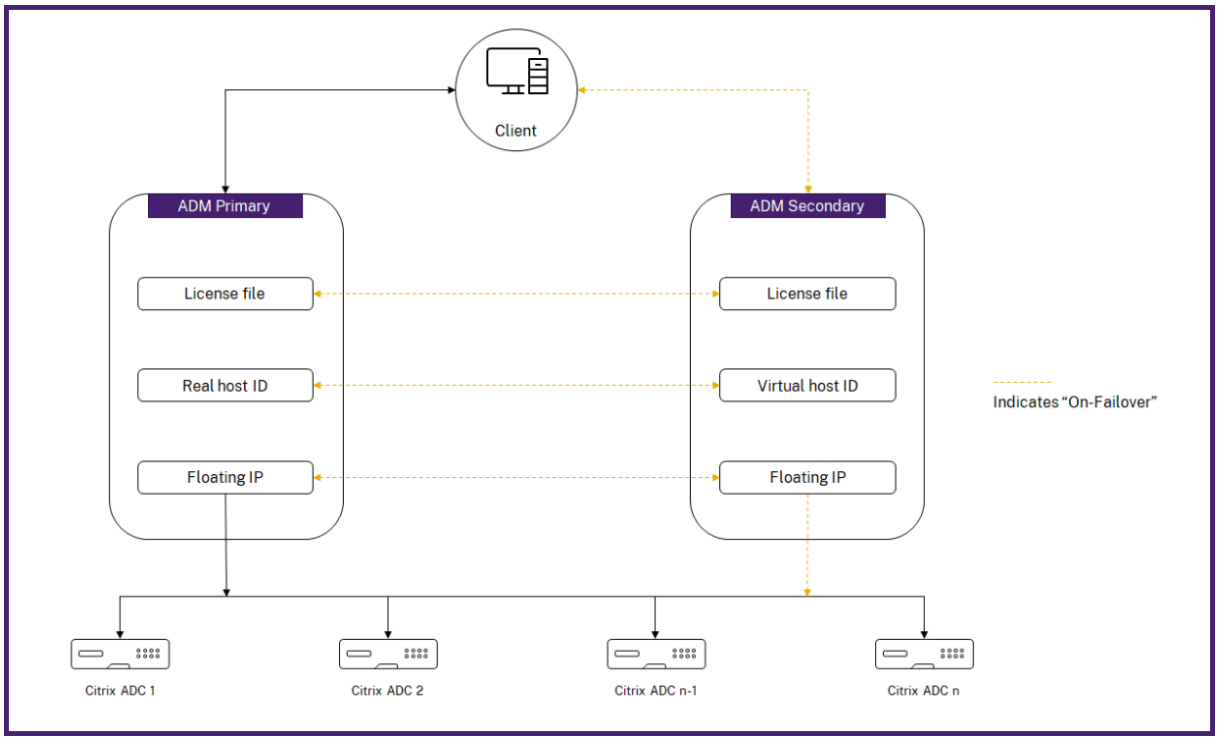
> 注
>
> - NetScaler ADM 12.1.49.x 以前のリリースをインストールしている場合、セカンダリノードでライセンスを維持するために 30 日間の猶予期間があります。猶予期間の後、Citrix に連絡して元のライセンスを再ホストする必要があります。
> - 12.1.50.x 以降のリリースでは、NetScaler ADM ライセンスは自動的にセカンダリノードに同期されま

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

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

オーケストレーション

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

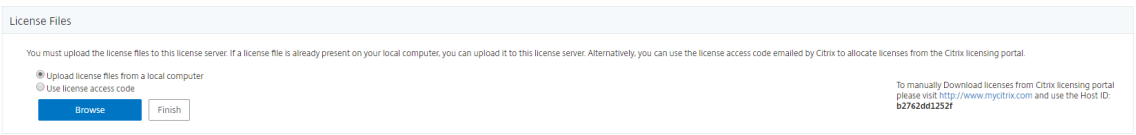
仮想サーバーライセンスをアップグレードする

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

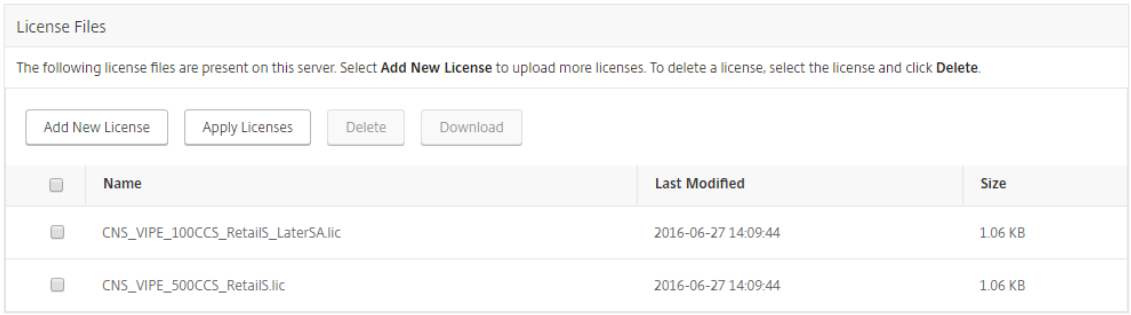
アプライアンスライセンスをアップグレードするには**:**

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

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

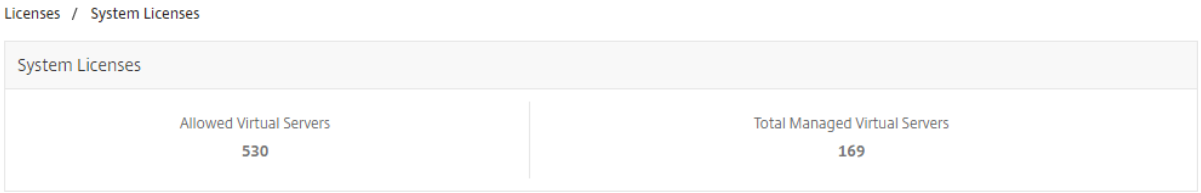


4. [ライセンス設定] ページからいつでもライセンスを追加できます。



確認

Citrix ADM にインストールされているライセンスは、**[**ネットワーク **] > [ライセンス] > [システムライセンス] に移動して確認できます。**



仮想サーバーのライセンス取得

Citrix ADM を使用して管理および監視する仮想サーバーを選択できます。検出された Citrix ADC インスタンスによってホストされる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、Citrix ADM はすべての仮想サーバーのライセンスを取得します。

Citrix ADM を使用して管理および監視する仮想サーバーを選択できます。

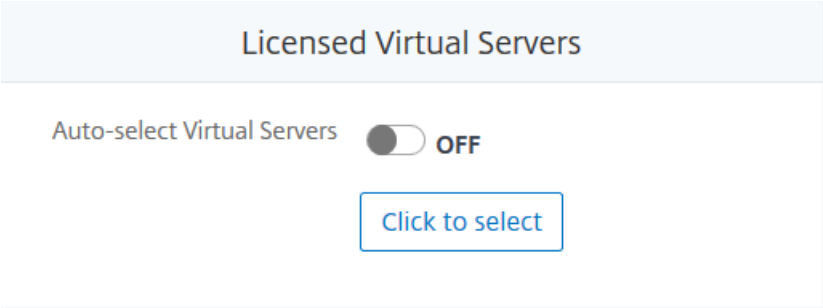
注意事項:

- 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。
- Citrix ADM は、アドレス指定できない仮想サーバーのライセンスを取得しません。管理するには、手動でライセンスを取得する必要があります。

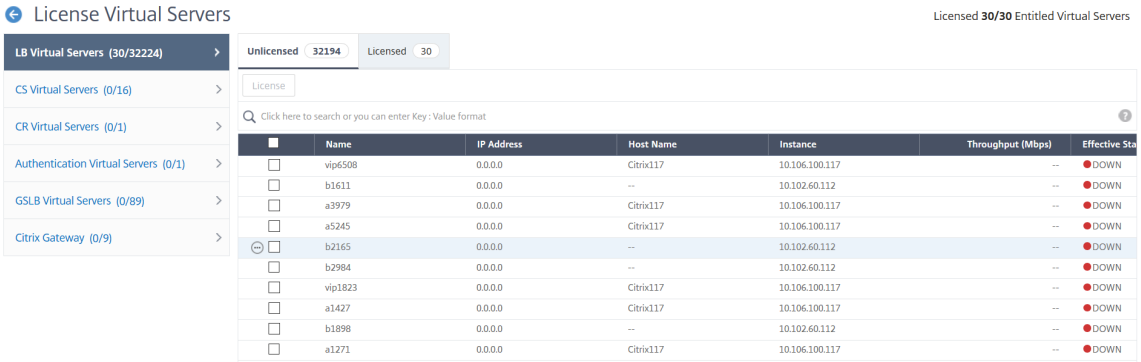
ライセンスされた仮想サーバーを管理するには:

1. 管理者の資格情報を使用して NetScaler ADM にログオンします。
2. [ネットワーク] > [ライセンス] > [システムライセンス] に移動します。

   システムライセンスダッシュボードが表示されます。
3. [ライセンス仮想サーバー] で [仮想サーバーの自動選択] を無効にし、[クリックして選択] オプションをクリックします。



4.「ライセンス仮想サーバー」画面で、関連するタブをクリックして仮想サーバーのタイプを選択します。



5.「ライセンスなし」タブから、ライセンスを取得する仮想サーバーを選択し、「ライセンス」をクリックします。「ライセンス済み」タブから、ライセンスを解除する仮想サーバーを選択し、「ライセンス解除」をクリックします。
6. [次へ] をクリックして他の仮想サーバーのタブに移動するか、[保存して終了] をクリックして選択した仮想サーバーのライセンスを取得します。

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。

Citrix ADM では、[ネットワーク] > [ライセンス] > [** システムライセンス] に新しいオプションが追加されました。つまり、** アドレス指定できない仮想サーバーを自動選択する新しいオプションです。このオプションを有効に

すると、アドレス指定できない仮想サーバもライセンスに含める必要があることを明示的に指定できるようになりました。

> 注
>
> - Citrix ADM は、デフォルトではまだアドレス指定できない仮想サーバーをライセンス用に自動選択しません。
> - 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。

仮想サーバライセンスの有効期限チェック

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

ライセンスのステータスを表示するには、次の手順に従います。

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

ライセンスの通知設定を構成するには:

1. [ネットワーク] > [ライセンス**] > [**設定**]** に移動します。
2. [通知設定] セクションで、鉛筆アイコンをクリックし、パラメータを編集します。
    - 電子メールプロファイル**:** ライセンスがしきい値に達したとき、または期限切れになったときに通知を送信するための電子メールプロファイルまたは配布リスト。
    - **SMS** プロファイル**:** ライセンスがしきい値に達したときや期限切れになりそうな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。
    - **Alert Threshold**：メールまたは SMS で管理者に通知する、プールされたライセンスのパーセントを設定します。
    - **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。
    - **Days to expiry**：有効期限までに残されている日数。

システム要件

February 6, 2024

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

NetScaler ADM の要件

コンポーネント	条件
RAM	32 GB
仮想 CPU	8 基の CPU 注：Citrix ADM の展開にはソリッドステートドライブ（SSD）テクノロジーを使用することをお勧めします。
記憶域	デフォルト値は 120GB です。実際のストレージ要件は、NetScaler ADM のサイズ設定の見積もりによって異なります。Citrix ADM HA 導入ガイドの「最大制限」セクション（7 ページ）に記載されているサイジング計算ツールを使用してください。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 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

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

NetScaler ADM オンプレミスエージェントの要件

コンポーネント	条件
RAM	8 GB 注: デフォルト値は 8 GB です。パフォーマンスを向上させるには、デフォルト値を 32 GB に増やすことをお勧めします。
仮想 CPU	2 つの CPU 注: デフォルトは 2 CPU です。パフォーマンスを向上させるには、デフォルト値を 8 CPU に増やすことをお勧めします。
記憶域	30 GB
仮想ネットワークインターフェイス	1
スループット	1Gbps

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

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

> 重要
>
> NetScaler ADM のバージョンとビルドは、NetScaler ADC のバージョンおよびビルドと同じかそれ以上である必要があります。たとえば、NetScaler ADM 12.1 ビルド 50.39 をインストールしている場合は、NetScaler ADC 12.1 ビルド 50.28/50.31 以前がインストールされていることを確認します。

NetScaler ADM 機能	NetScaler ADC ソフトウェアのバージョン
StyleBook	10.5 以降
OpenStack/CloudStack のサポート	11.0 以降 (パーティションが必要な場合) 11.1 以降 (共有仮想 LAN 上のパーティションが必要な場合)
NSX のサポート	11.1 Build 47.14 以降（VPX）
Mesos/Marathon のサポート	10.5 以降

NetScaler ADM 機能	NetScaler ADC ソフトウェアのバージョン
バックアップ/復元	NetScaler ADC、10.1 以降の場合 Citrix SDX の場合、11.0 以降
ジョブを使用した監視/レポート作成および構成	10.1 以降
分析機能	
Web Insight	10.5 以降
HDX Insight	10.1 以降
Security Insight	11.0.65.31 以降
Gateway Insight	11.0.65.31 以降
Cache Insight	10.5 以降 *
SSL Insight	12.0 以降

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

Citrix SD-WAN インスタンス管理の要件

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

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

Citrix SD-WAN インスタンスでサポートされるシンクライアント

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

- Dell Wyse WTOS モデル R10L Rx0L シンクライアント
- NComputing N400
- Dell Wyse WTOS Model CX0 C00X Xenith
- Dell Wyse WTOS Model TXO T00X Xenith2
- Dell Wyse WTOS Model CX0 C10LE
- Dell Wyse WTOS モデル R00LX Rx0L HDX シンクライアント
- Dell Wyse 拡張 SUSE Linux エンタープライズ、モデル Dx0D、D50D
- Dell Wyse ZX0 Z90D7（WES7）シンクライアント

NetScaler ADM 分析の要件

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

NetScaler ADM 機能	Citrix Virtual Apps and Desktops バージョン
HDX Insight	Citrix Virtual Apps and Desktops 7.0 以降

> 注
>
> NetScaler Gateway 機能（バージョン 9.3 および 10.x では Access Gateway Enterprise としてブランド化されています）は、NetScaler ADC インスタンスで使用できる必要があります。NetScaler ADM では、スタンドアロンの Access Gateway Standard アプライアンスはサポートされません。

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

HDX Insight でサポートされているシンクライアント

- 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 Platinum および Enterprise アプライアンスに対してのみ表示されます。

NetScaler ADC ライセンス/期間	5 分	1 時間	1 日	1 週間	1 か月超
Standard	いいえ	いいえ	いいえ	いいえ	いいえ
Enterprise	はい	はい	いいえ	いいえ	いいえ
Platinum	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
Microsoft Hyper-V	2012 R2 および 2016
汎用 KVM	RHEL 7.4 and Ubuntu 16.04

サポートされているオペレーティングシステムとレシーバのバージョン

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

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

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

サポートされているブラウザー

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
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

サポートされるポート

NetScaler ADM は、NetScaler ADC IP（NSIP と呼ばれる）アドレスを使用して NetScaler ADC と通信します。NetScaler ADC インスタンスと NetScaler ADM、または Citrix SD-WAN インスタンスと NetScaler ADM の間の通信では、NetScaler ADM で次のポートを開く必要があります。

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

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

ADC へ、NetScaler ADC から NetScaler ADM へ |
TCP	22	NetScaler ADM から NetScaler ADC または Citrix SD-WAN インスタンスへの SSH 通信用です。高可用性モードで展開された NetScaler ADM サーバー間の同期用。また、このポートは、ADM エージェントと NetScaler ADC 間の SSH 通信に必要です。	NetScaler ADM から NetScaler ADC に、NetScaler ADM エージェントは NetScaler ADC に
UDP	4739	NetScaler ADC または Citrix SD-WAN インスタンスから NetScaler ADM への AppFlow ow 通信の場合。	NetScaler ADC または Citrix SD-WAN から NetScaler ADM へ
ICMP	予約されているポートなし	高可用性モードで展開された NetScaler ADM と NetScaler ADC インスタンス、SD WAN インスタンス、またはセカンダリ NetScaler ADM サーバー間のネットワーク到達可能性を検出するため。
UDP	161, 162	NetScaler ADC インスタンスから NetScaler ADM に SNMP イベントを受信する。	** ポート 161**-Citrix ADM-Citrix ADC
			** ポート 162** -NetScaler ADC から NetScaler ADM へ
UDP	514	NetScaler ADC または Citrix SD-WAN インスタンスから NetScaler ADM への syslog メッセージを受信する。	NetScaler ADC または Citrix SD-WAN から NetScaler ADM へ
TCP	25	NetScaler ADM からユーザーに SMTP 通知を送信する場合。
TCP	389/636	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
UDP	123	のデフォルト NTP サーバポート。複数のタイムソースと同期しています。
RADIUS	1812	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
TACACS	49	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
TCP	5563	NetScaler ADC インスタンスから NetScaler ADC NetScaler ADM への 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。	NetScaler ADC から NetScaler ADM へ
TCP	5557/5558	Citrix ADC から Citrix ADM へのログ ** ストリーム ** 通信（セキュリティインサイト、Web インサイト、および HDX Insight 用）用。	NetScaler ADC から NetScaler ADM へ
TCP	5454	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
TCP	27000	NetScaler ADM ライセンスサーバーと CPX インスタンス間の通信に使用するライセンスポート。	NetScaler ADC から NetScaler ADM へ
TCP	7279	Citrix ベンダーデーモンポート。	NetScaler ADC から NetScaler ADM へ
TCP	443/8443/7443	NetScaler ADM エージェントと NetScaler ADM 間の通信用のポート。ADM エージェントが NetScaler ADM との通信を開始します。	NetScaler ADM エージェントから Citrix ADM へ

制限事項

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

次の機能は IPv6 をサポートしていません。

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

展開

February 6, 2024

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、まずハイパーバイザーのいずれかに 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。

- 単一サーバー展開。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。Citrix ADM は、Citrix Hypervisor、VMware ESXi、Microsoft Hyper-V、および Linux KVM でデプロイできます。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 **(HA)** 導入。2 台の Citrix ADM サーバーの高可用性導入により、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/パッシブモードで展開し、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展開し、同じ構成にする必要があります。HA 展開では、Citrix 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 ロードバランサーを別途用意する必要がなくなります。「高可用性展開での構成」を参照してください。
- **NetScaler Insight Center** から **Citrix ADM** に移行します。既存の構成、設定、またはデータを失うことなく、NetScaler Insight Center デプロイメントを Citrix ADM に移行できます。Citrix ADM を使用すると、NetScaler および NetScaler SD-WAN インスタンスによって生成されたさまざまな分析を表示できるだけでなく、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。
- **Citrix ADM** を **Director** と統合します。Director は Citrix 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。NetScaler ADM と Director の統合を参照してください。

NetScaler ADM をインストールするための前提条件

February 6, 2024

Microsoft HyperV、VMware ESXi、Linux KVM、および Citrix Hypervisor プラットフォーム用の Citrix 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 Citrix ADM をインストールする詳細な手順については、以下のトピックを参照してください。

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

Citrix ADM リリース **12.1** 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	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。 必要なデフォルトのストレージ容量は 120 GB です。実際のストレージ要件は、NetScaler ADM のサイズ設定の見積もりによって異なります。Citrix ADM HA 導入ガイドの「最大制限」セクション（7 ページ）に記載されているサイジング計算ツールを使用してください。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 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。 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。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 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。

Citrix Hypervisor を使用した NetScaler ADM

February 6, 2024

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

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

前提条件

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

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

XenCenter のシステム要件

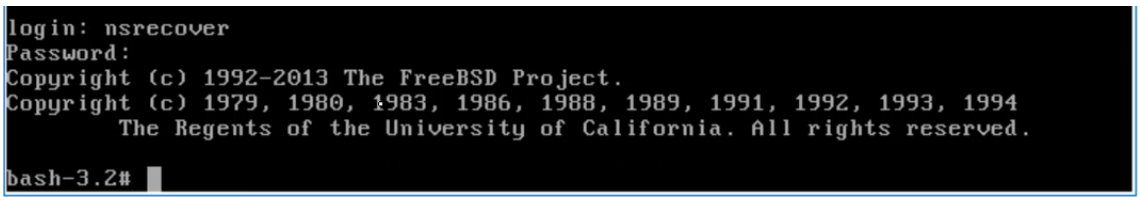
XenCenter は、Windows のクライアントアプリケーションです。Citrix Hypervisor ホストと同じマシン上で実行することはできません。次の表は、最小システム要件を示しています。

コンポーネント	条件
オペレーティングシステム	Windows 7、Windows Server 2003、または Windows 10
.NET Framework	バージョン 2.0 以降
CPU	750MHz。推奨：1GHz 以上
RAM	1GB。推奨：2GB
ネットワークインターフェイスカード	100Mbps 以上の NIC

Citrix Application Delivery Management のインストール

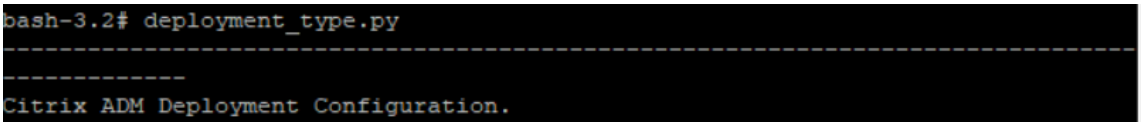
1. XVA イメージファイルを Citrix Hypervisor にインポートし、［コンソール］タブで初期ネットワーク構成オプションを構成します。

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`を入力して構成を更新し、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、デプロイ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、Citrix ADM サーバーの IP アドレスを Web ブラウザーに入力することで、グラフィカルユーザーインターフェイス（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 を搭載した NetScaler ADM

February 6, 2024

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

前提条件

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

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

Microsoft Hyper-V のシステム要件

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

コンポーネント	条件
オペレーティングシステム	Windows Server 2012 R2

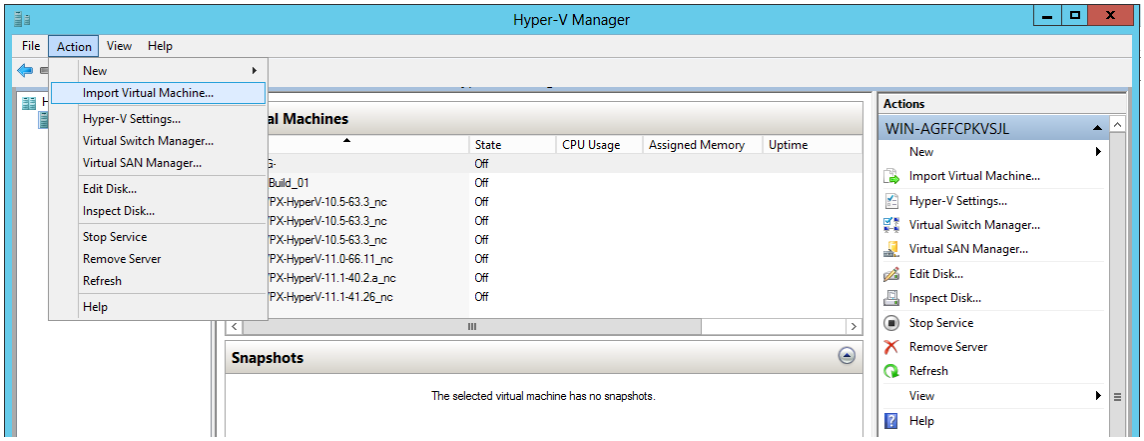
コンポーネント	条件
.NET Framework	バージョン 2.0 以降
CPU	750MHz。推奨：1GHz 以上
RAM	1GB。推奨：2GB
ネットワークインターフェイスカード	100Mbps 以上の NIC

NetScaler Application Delivery Management インストール

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

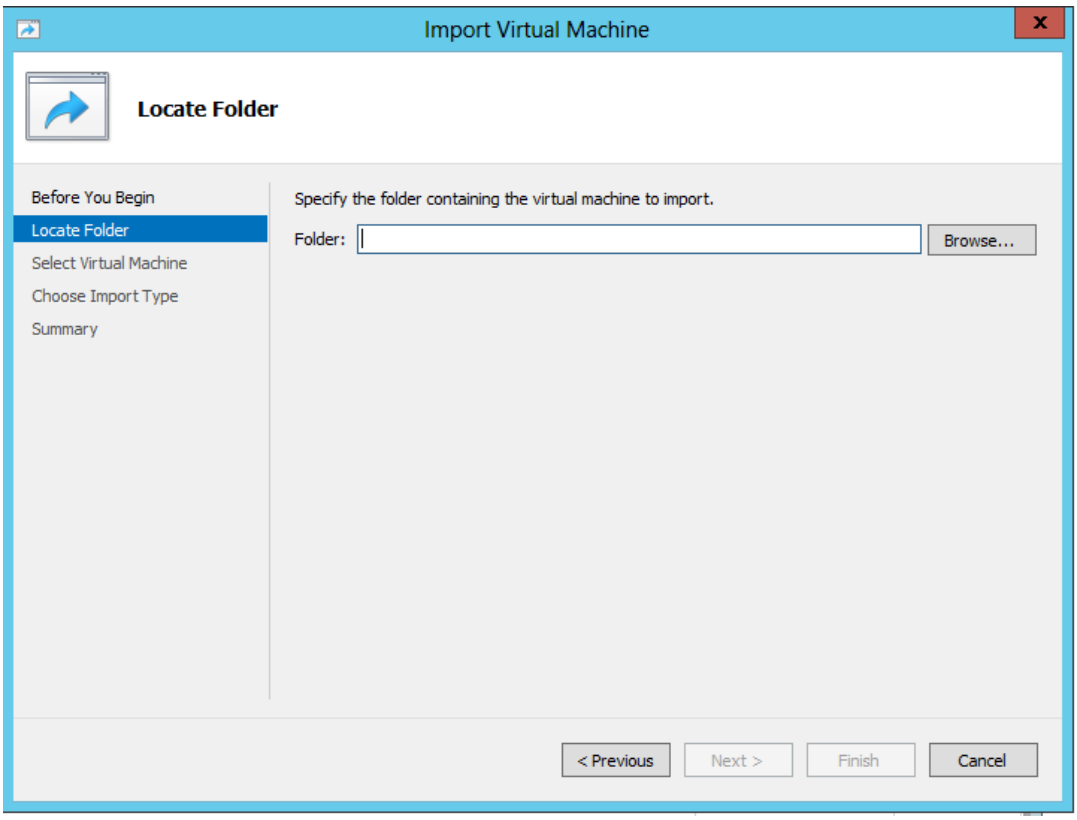
NetScaler ADM をインストールするには:

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



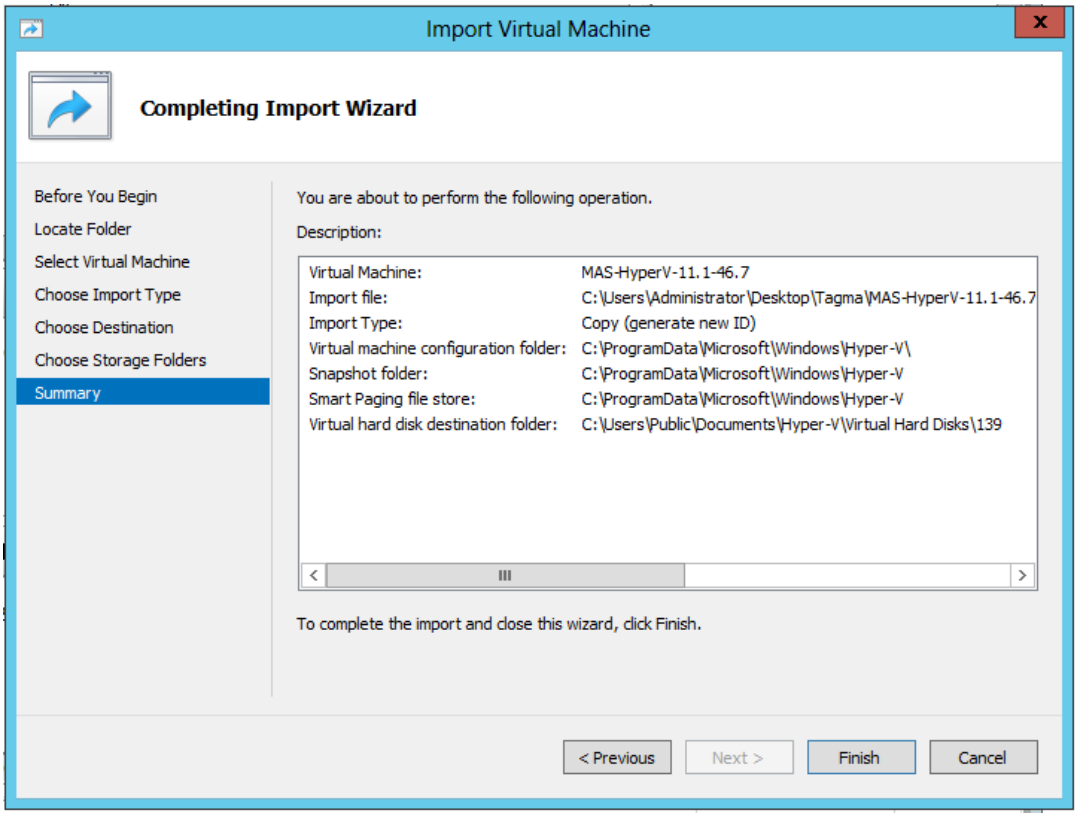
3. Hyper-V イメージをインポートし、次の操作を行います。
   a) ［仮想マシンのインポート］ダイアログボックスの［フォルダーの検索］セクションで、Citrix ADM Hyper-V イメージを保存したフォルダーを参照し、フォルダーを選択して［次へ］をクリックします。
   b) ［Select virtual machine］セクションで、該当する仮想マシン名を選択します。
   c) ［**Choose Import Type**］セクションで、［Copy the virtual machine (create a new unique ID)］オプションを選択し、［Next］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

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



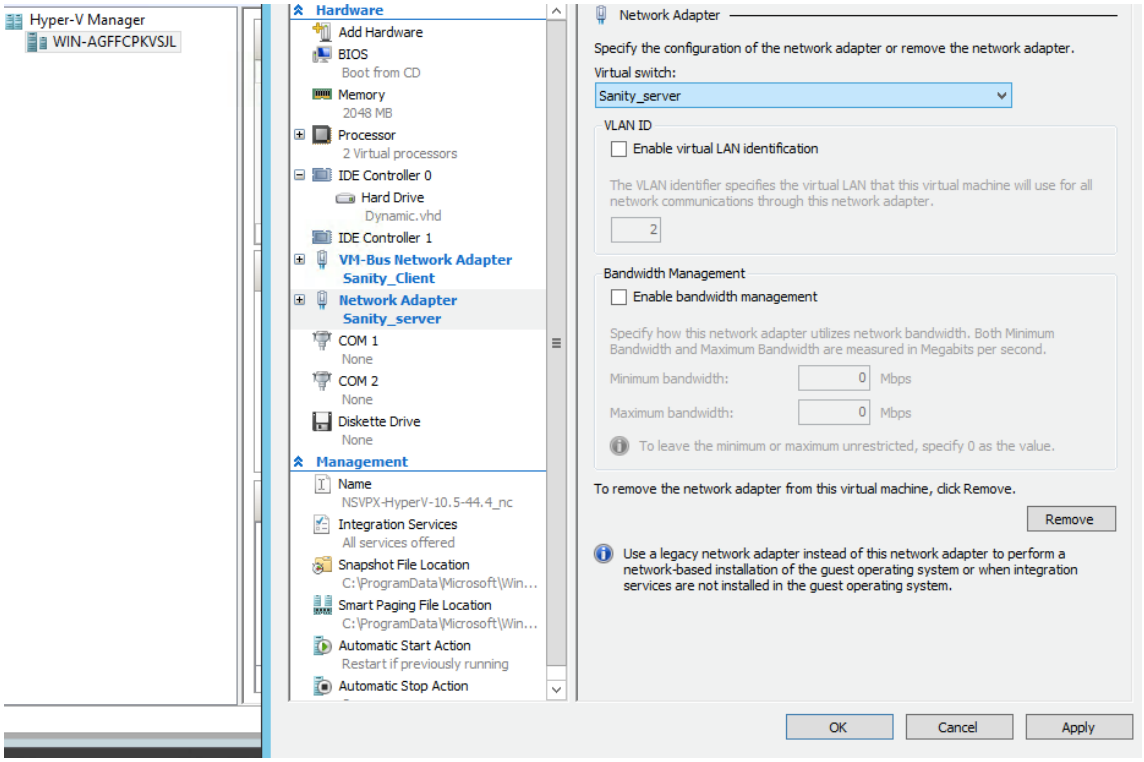
e) [**Choose Storage Folders**] セクションで、仮想ハードディスクを保存する場所を選択し、[**Next**] をクリックします。

f) 概要を示すペインで仮想マシンの情報を確認したら、[**Finish**] をクリックします。



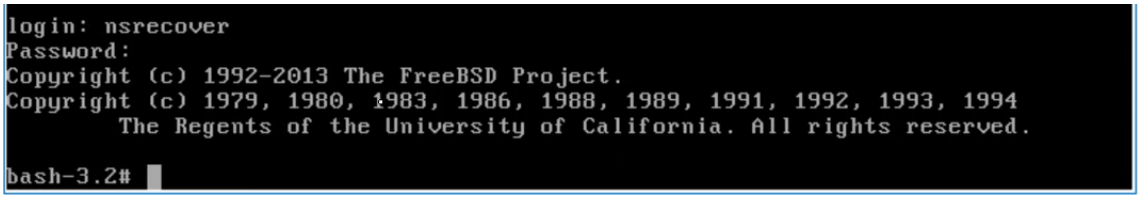
Citrix ADM Hyper-V イメージが右側のペインに表示されます。

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



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

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。



> 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を入力して構成を更新し、構成を保存します。

12. シェルプロンプトで以下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. Citrix ADM を スタンドアロン環境として展開するには、「はい」と入力します。
15. 「はい」と入力して、NetScaler ADM サーバーを再起動します。

> 注
>
> Citrix 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、ブラウザのアドレスバーに Citrix ADM サーバーの IP アドレスを入力して、グラフィカルユーザーインターフェイス（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 を使用した NetScaler ADM

February 6, 2024

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

前提条件

仮想アプライアンスのインストールを開始する前に、次の必要条件を確認します。

- サポートされている VMware ESXi バージョン（6.0、6.5、および 6.7）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 Citrix ADM ではサポートされていません。

NetScaler ADM をインストールするには

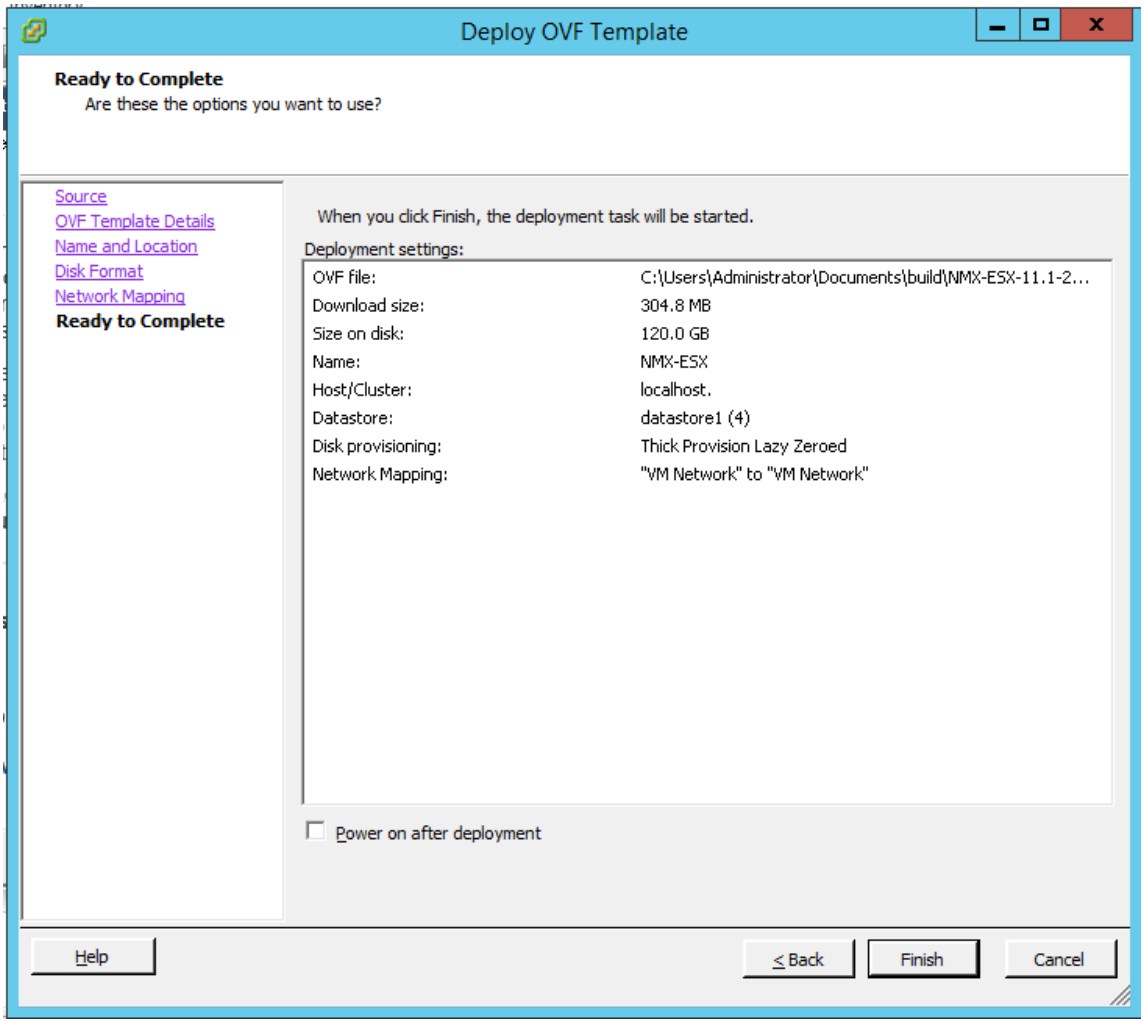
1. ワークステーション上で VMware vSphere Client を起動します。
2. [**IP** アドレス/名前] テキストボックスに、接続する VMware ESXi サーバの IP アドレスを入力します。
3. ［**User Name**］と［**Password**］の各テキストボックスに管理者資格情報を入力してから、［**Login**］をクリックします。
4. ［**File**］メニューの［**Deploy OVF Template**］を選択します。
5. [**OVF** テンプレートのデプロイ] ダイアログボックスの [ファイルまたは **URL** からのデ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

   > 注
   >
   「The operating system identifier is not supported on the selected host.」という文章の警告メッセージが表示された場合、VMware サーバーが FreeBSD オペレーティングシステムをサポートしているかどうかを確認してください。［はい］をクリックします。

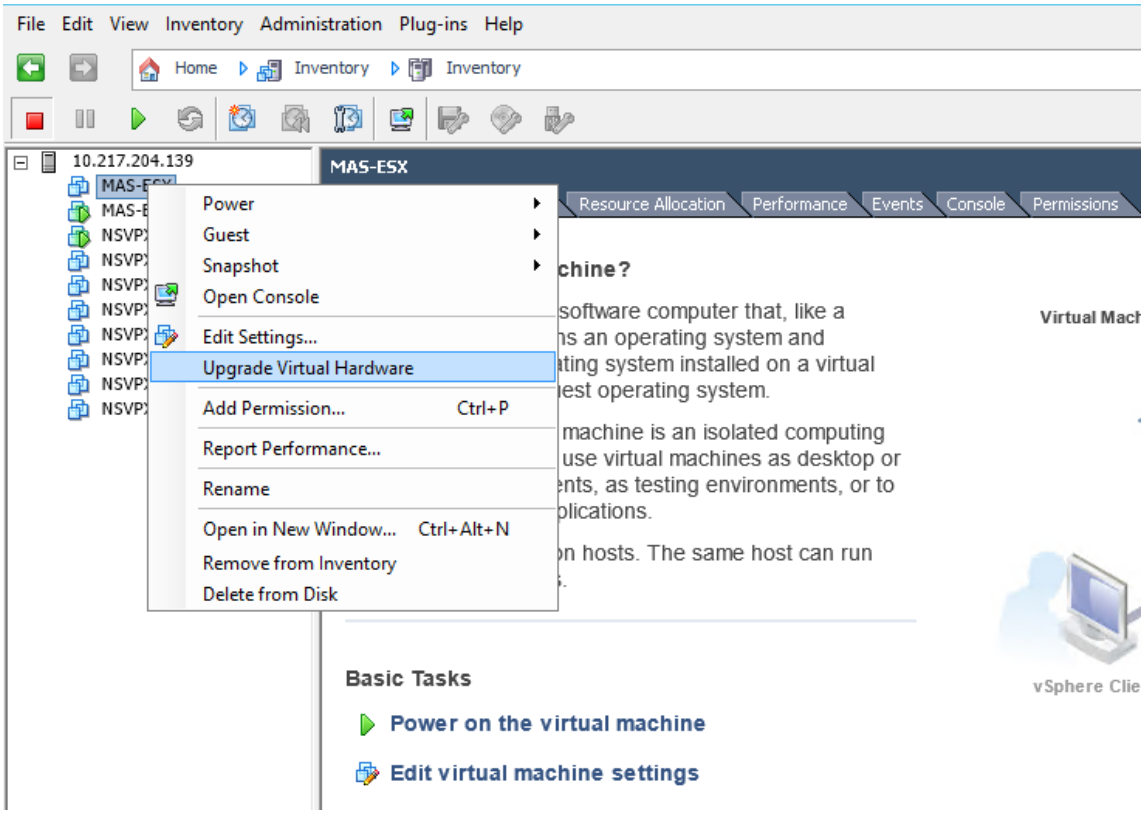
6. [**OVF** テンプレートの詳細] ページで、[次へ] をクリックします。
7. NetScaler ADM 仮想アプライアンスの名前を入力し、[次へ] をクリックします。
8. ［Disk Format］で［Thin provisioned format］または［Thick provisioned format］を選択し、ディスク形式を指定します。

> 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。

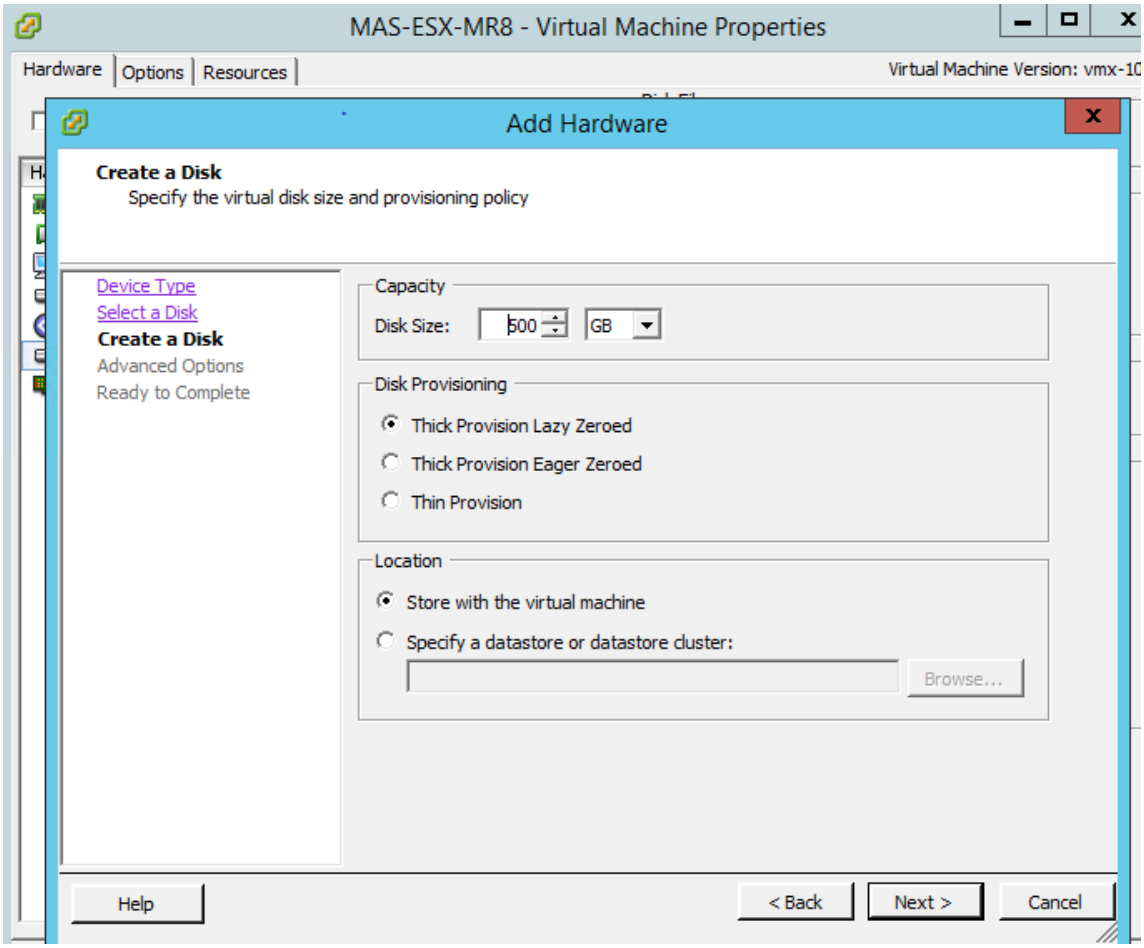
9. [完了] をクリックして、インストールプロセスを開始します。



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。

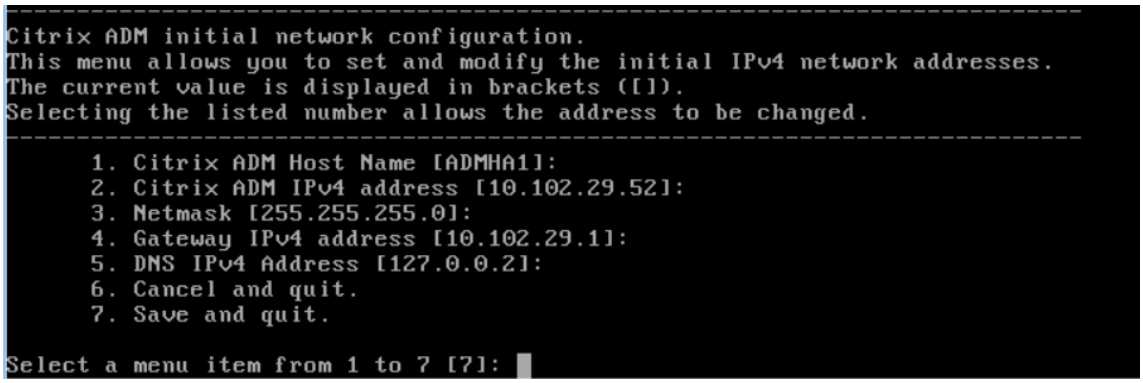


12. [インベントリ] メニューで、[仮想マシン] をクリックし、[設定の編集] をクリックします。
13. [仮想マシンのプロパティ] ダイアログボックスの [ハードウェア] タブで [メモリ] をクリックし、右側のペインで [メモリサイズ] に 32 GB を指定します。
14. [**CPU**] をクリックし、右側のペインで CPU を 8 と指定します。[**OK**] をクリックします。
15. 要件に応じて別のディスクを追加します。



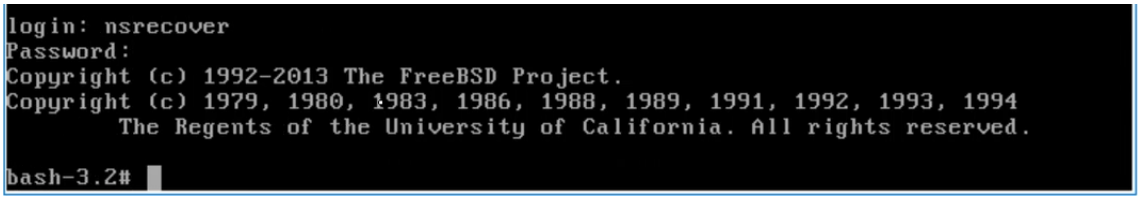
16. ナビゲーションペインで、インストールした仮想アプライアンスを選択します。[インベントリ] メニューから、[仮想マシン]、[パワー]、[パワーオン] の順にクリックします。

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。

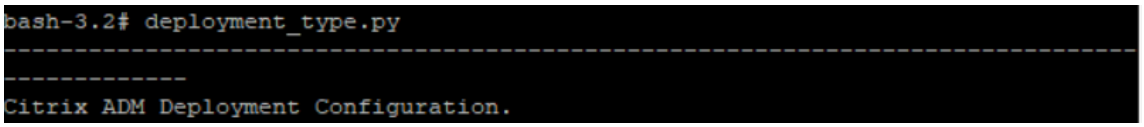
19. プロンプトが表示されたら、nsrecover/nsroot 認証情報を使用してログオンします。



> 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を入力して構成を更新し、構成を保存します。

20. シェルプロンプトで以下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
>
> VMware ESXi にデプロイした場合、Citrix ADM が起動するまでに最大 30 分以上かかる場合があります。

Linux KVM サーバーを使用した 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。また、*virsh*（仮想マシンを管理するためのコマンドラインツール）がハイパーバイザーで使用可能であることも確認します。

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

前提条件

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

ハードウェア要件

コンポーネント	条件
CPU	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、速度が高いほど、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 Citrix ADM 仮想マシンには 120 GB のディスク容量が必要です。

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

ソフトウェア要件

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

ネットワークの要件　NetScaler ADM は、VirtIO 準仮想化ネットワークインターフェイスを 1 つだけサポートします。Citrix 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する必要があります。

NetScaler ADM セットアップファイルのダウンロード

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

1. Web ブラウザーを開き、アドレスバーに「www.citrix.com」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」ドロップダウンリストから、「**Citrix Application Delivery Management**」を選択します。
5. ［**NetScaler Application Delivery Management** ］ページで、リリースを選択します。たとえば、リリース **12.1** 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、**Citrix ADM** リリース（機能フェーズ）**12.1** ビルド **49.23/49.37** を選択します。

   選択したビルドページが表示されます。
7. 「ダウンロードに移動」ドロップダウンリストで、**KVM** 用の **Citrix ADM** イメージ、**12.1 Build xx.xx** を選択します。
8. ［**Download File**］をクリックし、エンドユーザー向け使用許諾契約に同意したら、ローカルマシンの任意のフォルダーに圧縮イメージファイルをダウンロードします。

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

1. SSH を使用して、KVM ホストにログオンします。
2. CLI プロンプトで、いずれかのファイル転送プログラムを使用して、イメージをサーバーのフォルダーにコピーします。
3. ダウンロードしたイメージを保存したディレクトリに移動します。
4. コマンドラインで次の手順を実行します。

   a) ディレクトリ内のファイルの一覧を表示して、イメージファイルが存在することを確認します。

   b) tar コマンドを使用して、Citrix Application Delivery Management イメージファイルを解凍します。解凍したパッケージには、次のコンポーネントが含まれています。

      i. Citrix ADM 属性を指定するドメイン XML ファイル

      ii. ドメインディスクイメージのチェックサムが記述されたテキストファイル

      iii. ドメインディスクイメージ

```
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. 名前-名前を指定します。

B. mac-MAC アドレスを指定します。

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

> 注
>
> ドメイン名と MAC アドレスは一意である必要があります。

D. モード-モードを指定します。

E. モデルタイプ-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. *<FileName\ > 以下のコマンドを使用して MAS1-KVM.xml ファイル内の VM 属性を定義します。virsh define\.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#
```

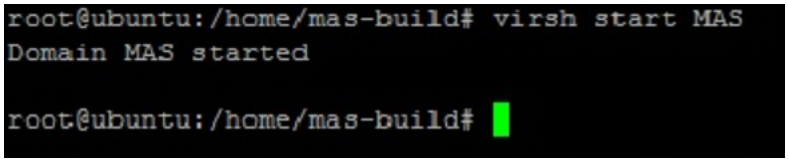
次のコマンドを入力して Citrix ADM を起動します。 \ <DomainUUID\ >]*

*virsh start\ [\ <DomainName\ >

---

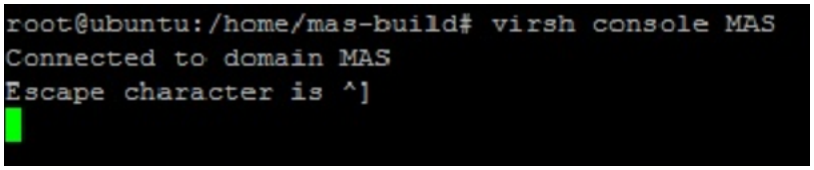
vii.

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



viii. Citrix ADM 仮想マシンに接続するには、次のコマンドを使用します。*virsh console\<DomainName\ >*

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



CitrixApplication Delivery Management の構成

> 注
>
> Linux KVM ホストによっては、複数の CPU が使用されていると、FreeBSD ゲストが正常に再起動しない場合があります。Citrix ADM 仮想アプライアンスを再起動すると、Citrix ADM CLI と GUI が応答しなくなります。詳細については、https://bugs.launchpad.net/qemu/+bug/1329956
> を参照してください。
> NetScaler ADM 仮想アプライアンスの再起動時に NetScaler ADM CLI と GUI が応答しなくなるのを避けるには、KVM ホスト上のすべての仮想マシンをシャットダウンし、KVM ホストで次の操作を実行します。
>
> 1. 次のコマンドを使用して kvm_intel モジュールを削除します。
>   *rmmod kvm_intel*
> 2. 次のコマンドを使用して APICv を無効にし、kvm_intel モジュールをリロードします。
>   *modprobe kvm_intel enable_apicv=n*
> 3. KVM ホスト上で仮想マシンを起動します。

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

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

- ユーザー名:nsroot
- パスワード: nsroot

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

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

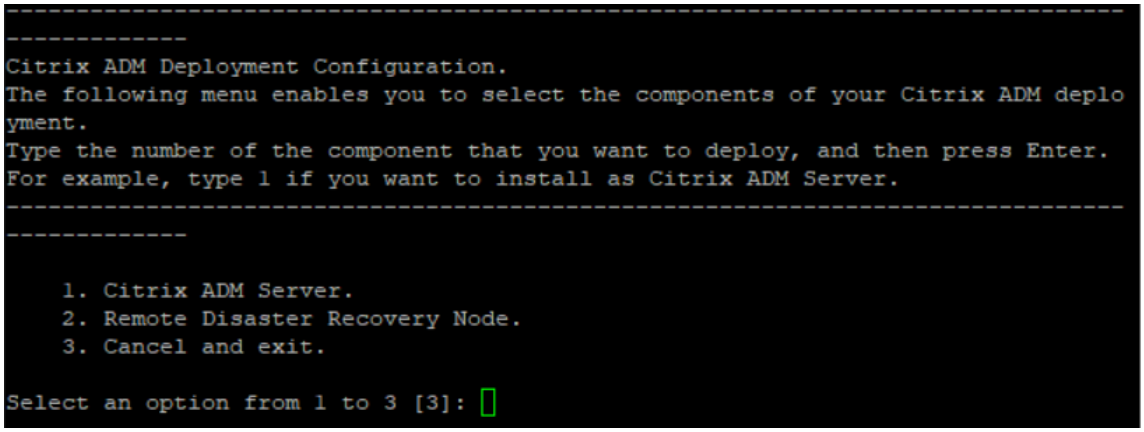
   a) **2** を入力して Citrix ADM IPv4 アドレスを更新します-Citrix ADM にアクセスする管理 IP アドレス

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

   c) ゲートウェイ **IPv4** アドレス（Citrix ADM の管理 IP アドレスのサブネットのデフォルトゲートウェイ IP アドレス）を更新するには、4 を入力します

   d) 保存して終了するには **7** を入力します。設定の変更を保存し、システムを終了します。

5. シェルプロンプトで *deployment_type.py* というコマンドを入力してデプロイスクリプトを実行します。
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、「**Yes** 」と入力します。
8. 「はい」と入力して Citrix ADM サーバーを再起動します。
9. Citrix ADM サーバーを再起動したら、コマンドラインまたは GUI を使用してデフォルトの管理者資格情報を nsroot/nsroot として使用して Citrix ADM にログオンします。

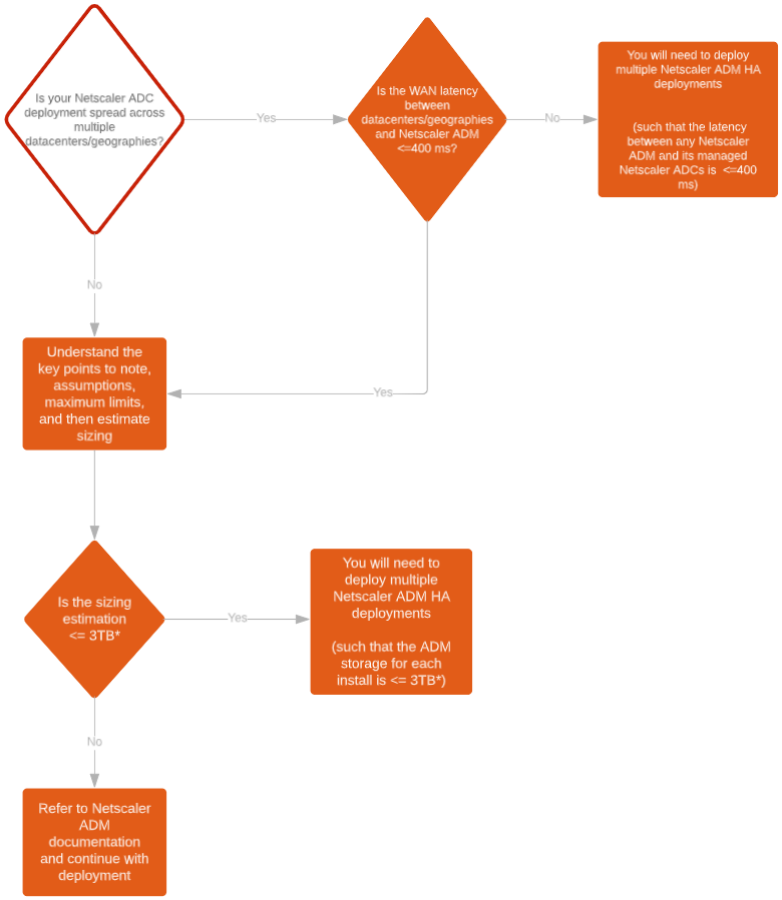
   ブラウザのアドレスバーに Citrix ADM サーバーの IP アドレスを入力することで、後で Citrix ADM にアクセスできます。サーバにログオンするためのデフォルトの管理者認証情報は *nsroot/nsroot* です。

高可用性展開の構成

February 6, 2024

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

導入シナリオ



> 注
>
> 単一の NetScaler ADM HA 展開での検証済みの最大ストレージ制限は 3TB です。詳細については、『導入ガイド』を参照してください。
>
> 重要
>
> **HTTPS** を使用して **Citrix ADM 12.1** ビルド **48.18** 以降のバージョンにアクセスするには:
>
> Citrix ADM を高可用性モードで負荷分散するように Citrix ADC インスタンスを構成している場合は、まず Citrix ADC インスタンスを削除します。次に、高可用性モードで Citrix ADM にアクセスするためのフローティング IP アドレスを構成します。

Citrix ADM での高可用性展開の利点は次のとおりです:

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

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

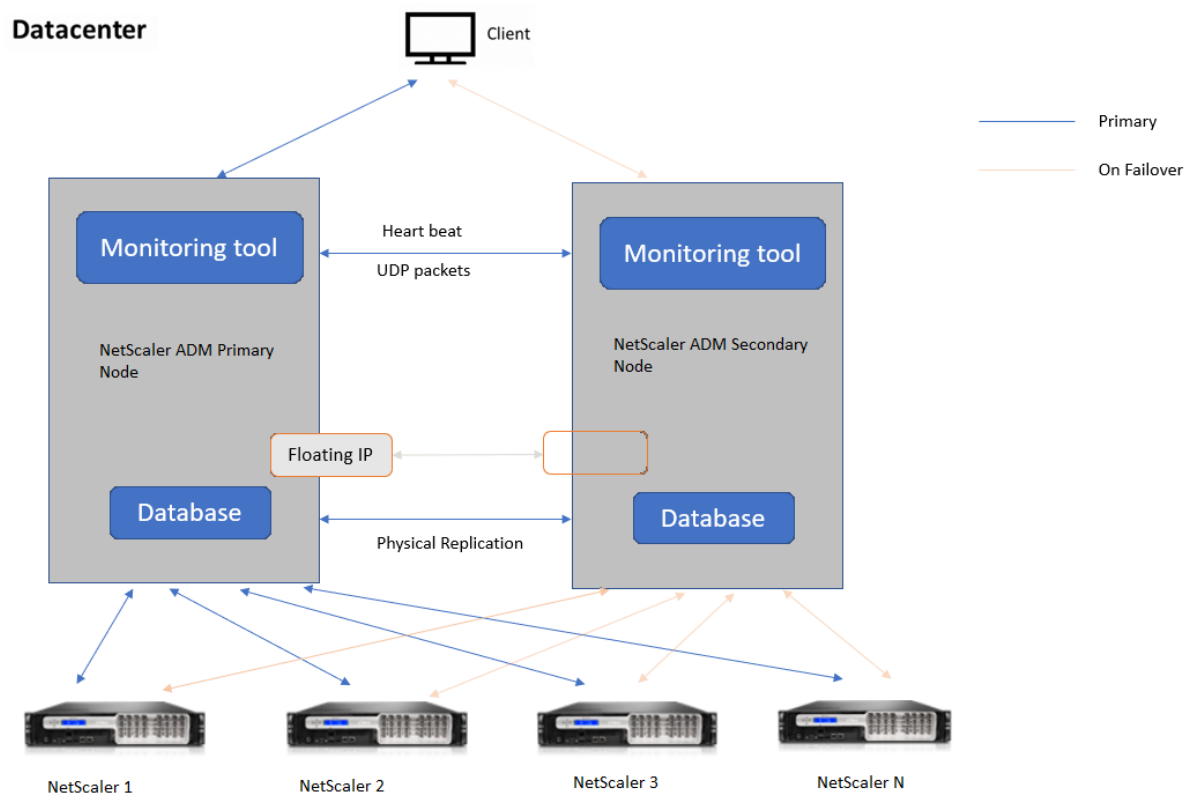
次の表は、高可用性導入で使用される用語をまとめたものです。

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

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

高可用性アーキテクチャのコンポーネント

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



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

監視ツール

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

プライマリノード

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

2 次ノード

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

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

物理ストリーミングレプリケーション

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

ハートビートメッセージ

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

フローティング **IP** アドレス

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

注意すべき重要なポイント

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

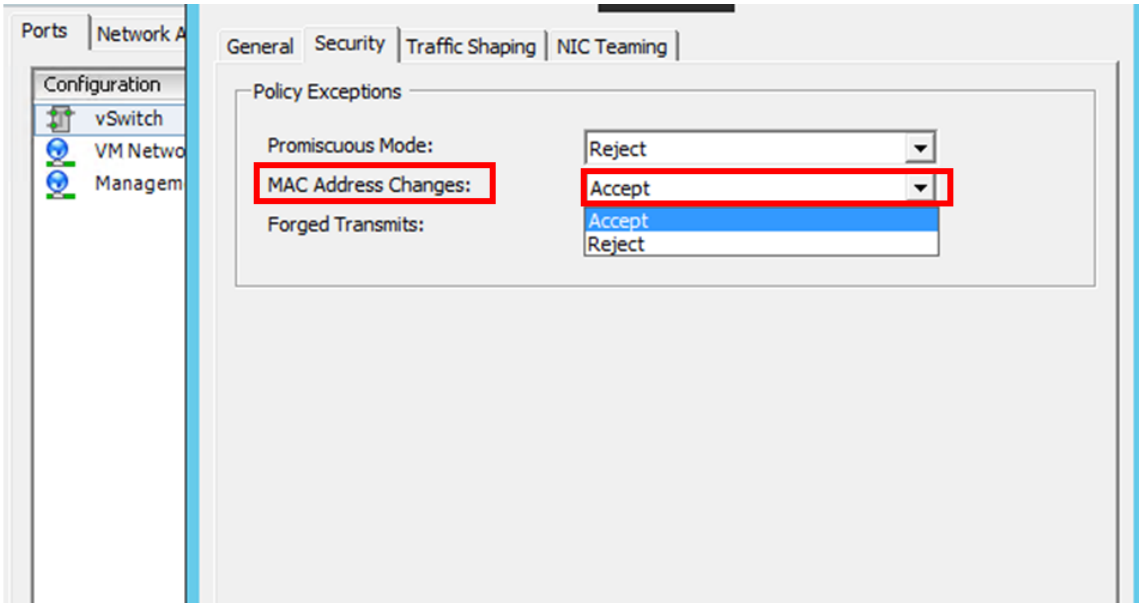
    > 注
    >
    > Citrix では、ユーザーインターフェイスへのアクセスにはフローティング IP アドレスを使用する

> ことをお勧めします。

- データベース:
  - 高可用性セットアップでは、すべての構成ファイルが 1 分間隔でプライマリノードからセカンダリノードに自動的に同期されます。
  - データベースの同期は、データベースを物理的に複製することによって即座に行われます。
  - セカンダリノードのデータベースはリードレプリカモードです。
- NetScaler ADM アップグレード:
  - 内部プロセスは、Citrix ADM を以前のバージョンから暗黙的にアップグレードします。

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

- UDP のデフォルトポート 5005 は、ハートビートを送信するノードとメッセージを受信するノードの両方で使用できます。
- MAC
  アドレスハイパーバイザーの「MAC アドレス変更」オプションの設定は、仮想マシンが受信するトラフィックに影響します。仮想スイッチで MAC アドレスの変更を有効にして、フェールオーバー後にフローティング IP アドレスが新しいプライマリノードにシームレスに移動できるようにします。
  たとえば、Citrix ADM を Vmware ESXi の高可用性環境にデプロイする場合は、MAC アドレスの変更を受け入れるようにしてください。ESXi では、アクティブ MAC アドレスを初期 MAC アドレス以外に変更する要求が許可されるようになりました。



前提条件

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

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

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

次の表は、仮想コンピューティングリソースの最小要件を示しています。

コンポーネント	条件
RAM	**32 GB**
仮想 CPU	**8** 基の **CPU**
記憶域	Citrix ADM 展開では、ソリッドステートドライブ（SSD）テクノロジを使用することをお勧めします。デフォルト値は 120GB です。実際のストレージ要件は、NetScaler ADM のサイズ設定の見積もりによって異なります。Citrix ADM ストレージ要件が 120 GB を超える場合は、追加のディスクを接続する必要があります。**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、「Citrix ADM に追加ディスクを接続する方法」を参照してください。
仮想ネットワークインターフェイス	1
スループット	1Gbps または 100Mbps
ハイパーバイザー	バージョン
Citrix Hypervisor	6.2 と 6.5
VMware ESXi	5.5 と 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu と Fedora

Citrix ADM を高可用性モードでセットアップするには

1. 最初のサーバー (プライマリノード) を登録してデプロイします。

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

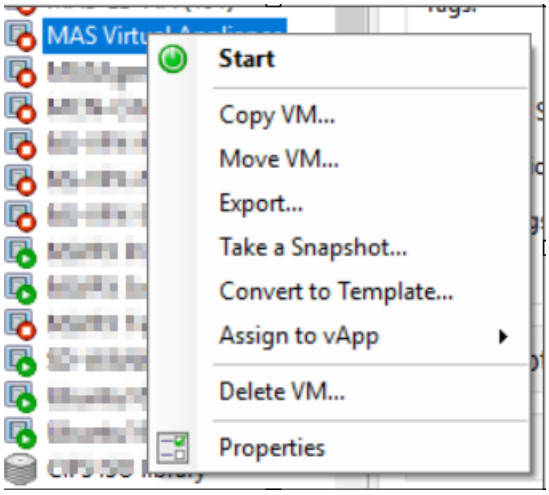
最初のサーバー (プライマリノード) を登録してデプロイする

最初のノードを登録するには:

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

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

2. インポートが成功したら、右クリックして [開始] をクリックします。

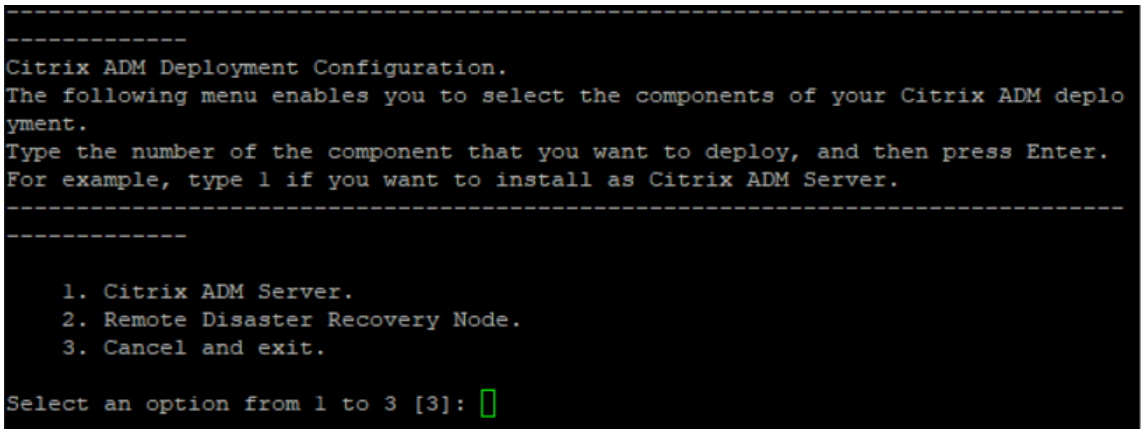
3. [コンソール] タブから、初期ネットワーク構成で Citrix ADM を構成します。

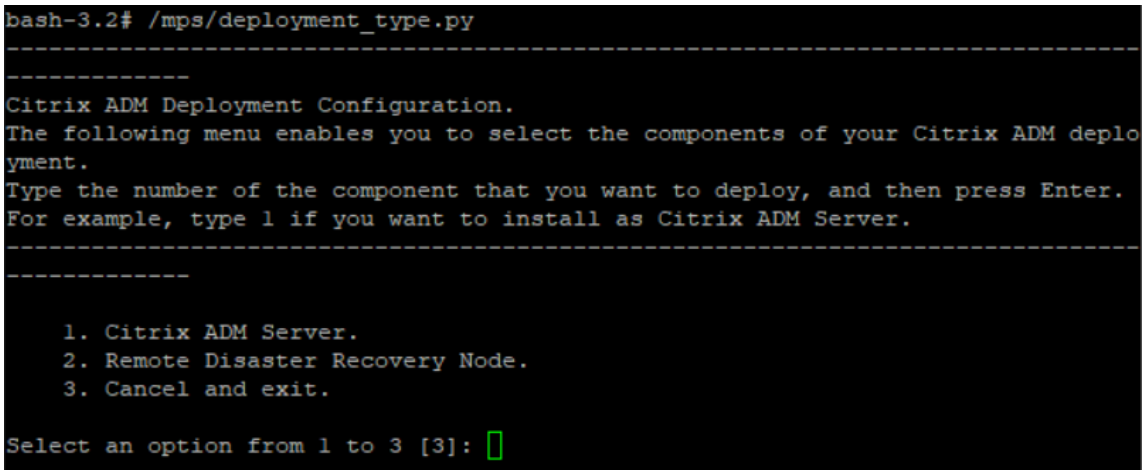
4. 初期ネットワーク設定が完了すると、ログインのプロンプトが表示されます。次の認証情報(*nsrecover/nsroot*)を使用してログオンします。

> 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を入力して構成を更新し、構成を保存します。

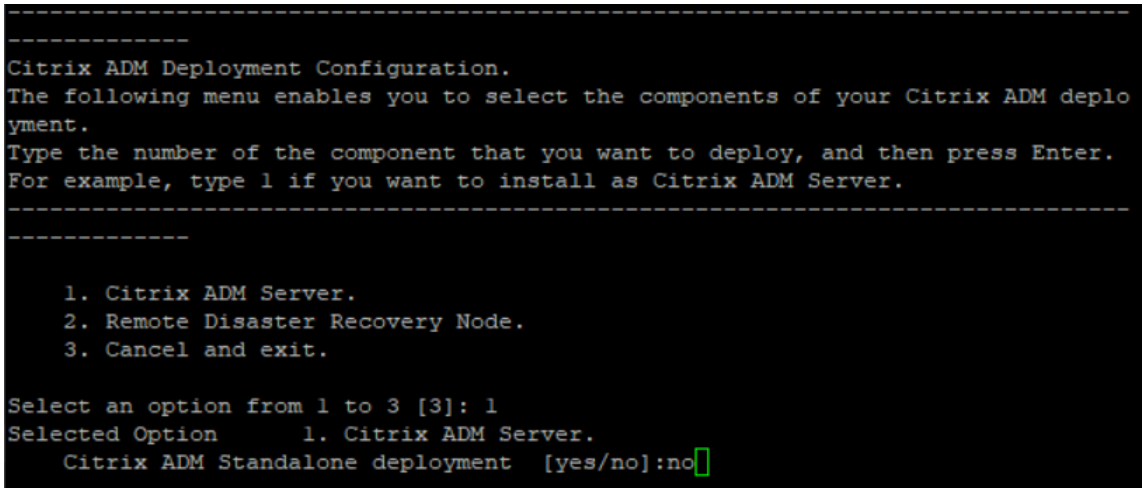
5. プライマリノードをデプロイするには、**/mps/deployment_type.py** と入力します。Citrix ADM デプロイメント構成メニューが表示されます。



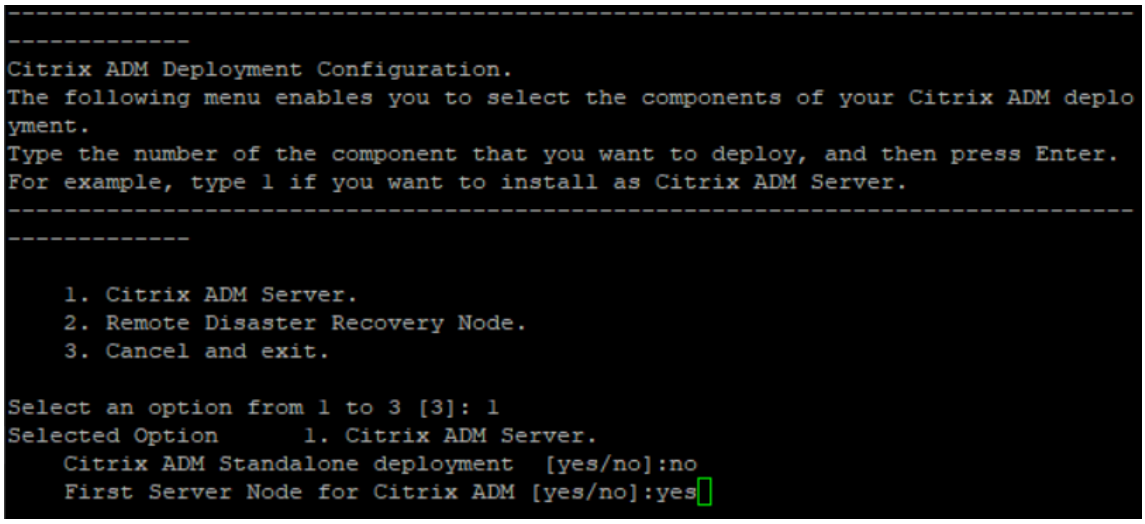
6. **1** を選択して、NetScaler ADM サーバーをプライマリノードとして登録します。



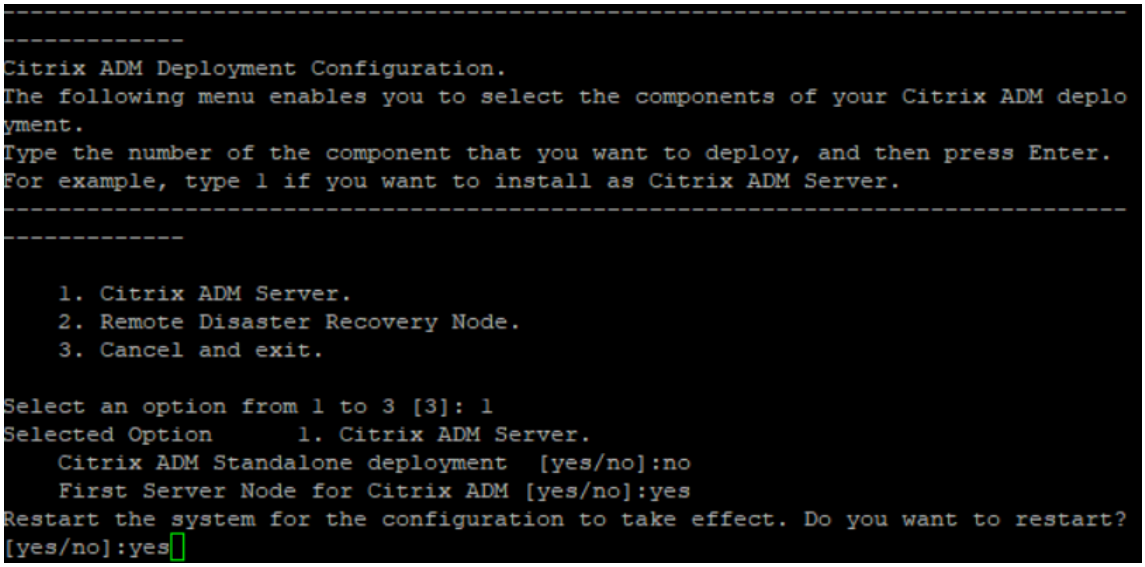
7. コンソールで、NetScaler ADM スタンドアロン展開を選択するように求められます。**No** と入力して、展開を高可用性として確認します。



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。



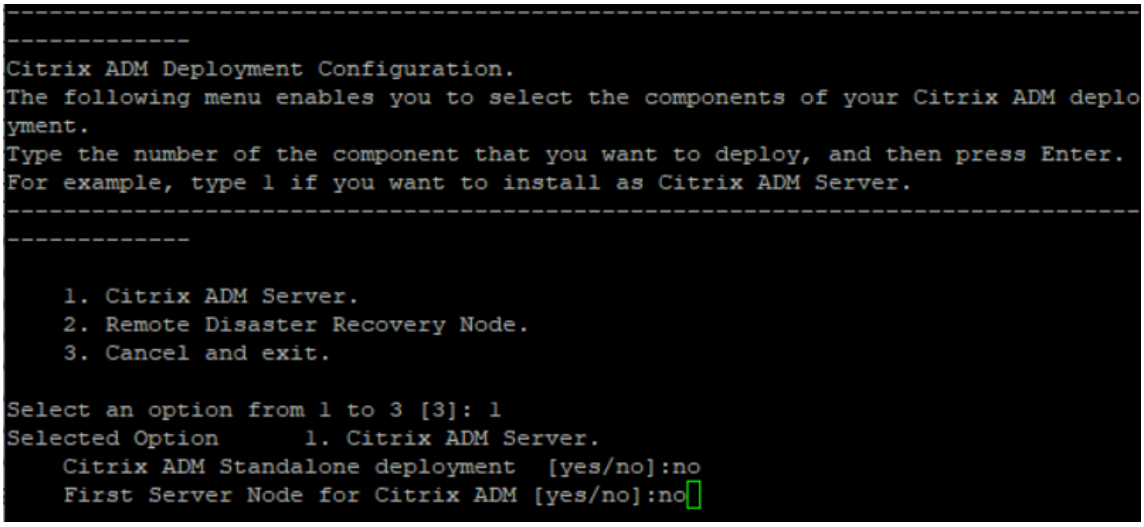
システムが再起動し、NetScaler ADM ユーザーインターフェイスにプライマリノードとして表示されます。

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

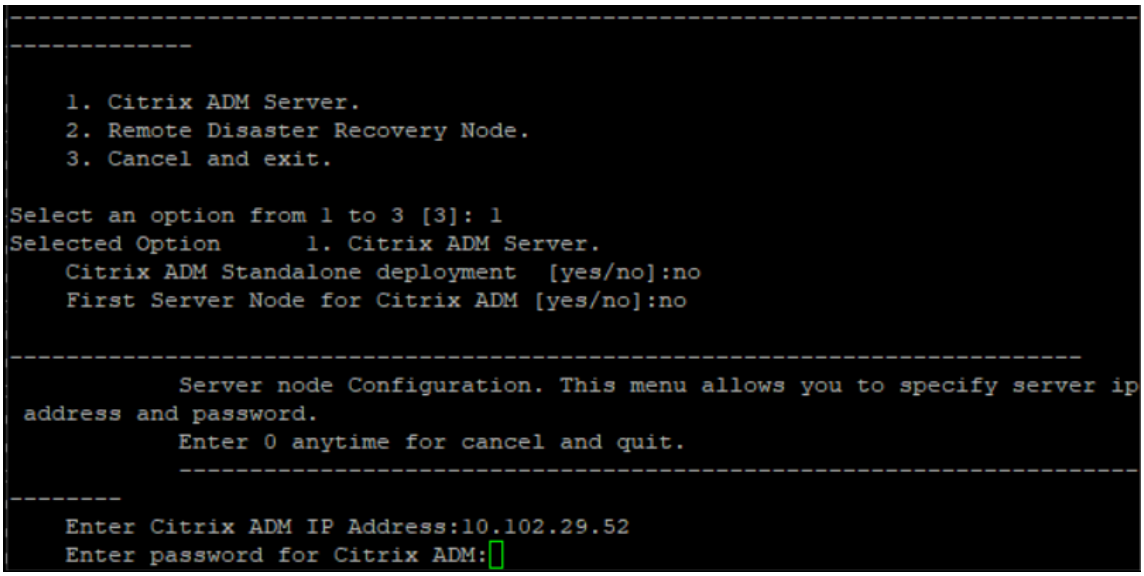
1. **Citrix** のダウンロードサイトからダウンロードした**.xva** イメージファイルを使用して、ハイパーバイザーにインポートします。
2. ［コンソール］タブから、次の図に示す初期ネットワーク構成で Citrix ADM を構成します。
3. 初期ネットワーク設定が完了すると、システムはログインを要求します。次の認証情報（*nsrecover/nsroot*）を使用してログオンします。

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

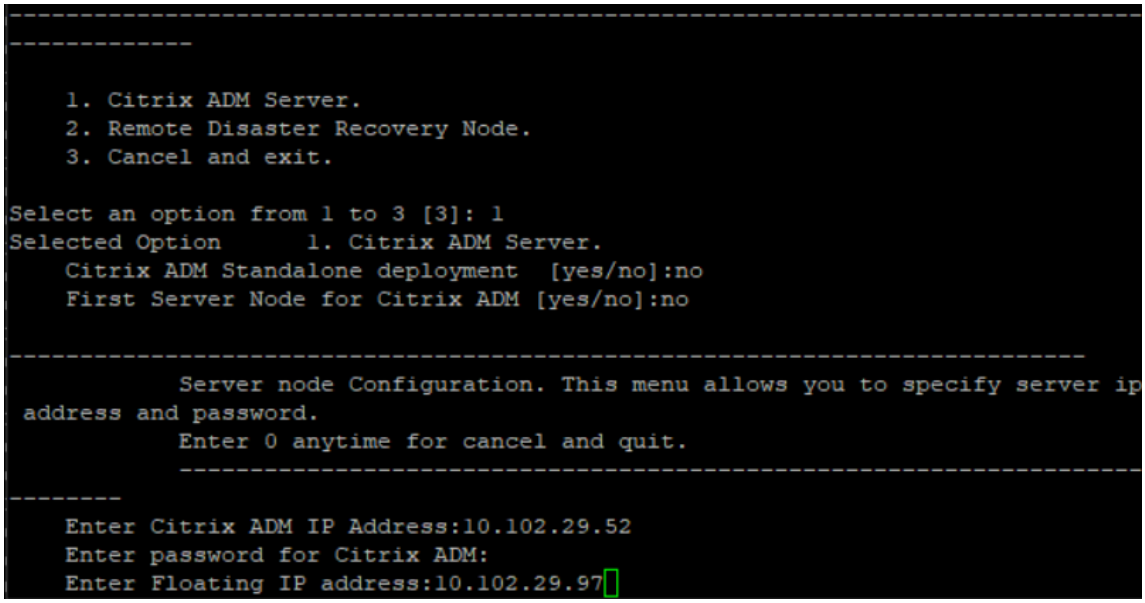
4. セカンダリノードをデプロイするには、**/mps/deployment_type.py** と入力します。Citrix ADM 展開構成メニューが表示されます。
5. **1** を選択して Citrix ADM サーバーをセカンダリノードとして登録します。
6. コンソールでは、Citrix ADM をスタンドアロン展開として選択するよう求められます。**No** と入力して、展開を高可用性として確認します。
7. コンソールでは、最初のサーバーノードを選択するように求められます。**No** を入力して、ノードを 2 番目のサーバとして確認します。



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

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

ノードを高可用性ペアとしてデプロイするには**:**

1. Web ブラウザーを開き、最初の Citrix ADM サーバーノードの IP アドレスを入力します。
2. 「ユーザー名」フィールドと「パスワード」フィールドに、管理者の資格情報を入力します。
3. ホームページの「はじめに」をクリックします。
4. 展開の種類として、[高可用性モードで展開された **2** つのサーバー] を選択し、[次へ] をクリックします。

5. [配置] ページで、[配置] をクリックします。
6. 確認メッセージが表示されます。［はい］をクリックします。

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

   > 注:
   >
   > これで、Floating IP アドレスの使用を開始できます。

7. 管理者資格情報を使用して Citrix ADM にログオンし、ホームページで「はじめに」をクリックし、オプションで次の操作を行います:

   a) NetScaler ADC インスタンスの追加

   b) カスタマー ID の設定

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

8. [システム] > [配置] に移動して、配置を検証します。

   詳細については、「よく寄せられる質問」を参照してください。

高可用性の無効化

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

> 注
>
> プライマリノードからの高可用性を無効にします。

高可用性を無効にするには**:**

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

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

高可用性を再デプロイ

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

高可用性フェイルオーバーのシナリオ

フェ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。

スプリットブレインシナリオ

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

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

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

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

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

高可用性を実現するためのディザスタリカバリの構成

February 6, 2024

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

Citrix ADM 12.1 のディザスタリカバリ（DR）機能は、高可用性モードで展開された Citrix ADM に完全なシステムバックアップおよびリカバリ機能を提供します。リカバリ時には、証明書、構成ファイル、およびデータベースの完全なバックアップがリカバリサイトで使用できます。

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

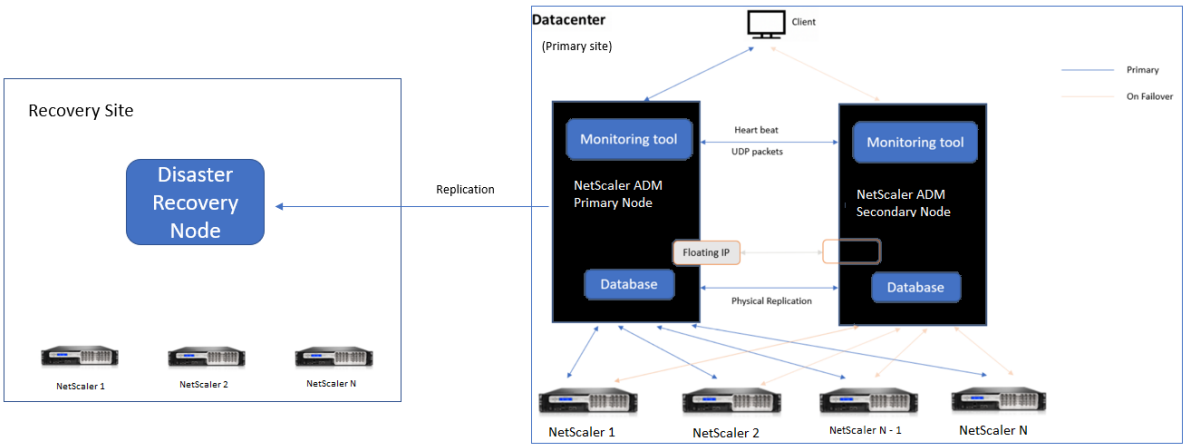
利用規約	説明
プライマリサイト (データセンター A)	プライマリサイトには、高可用性モードで展開された NetScaler ADM ノードがあります。
リカバリサイト (データセンター B)	リカバリ・サイトには、スタンドアロン・モードで展開された災害復旧ノードがあります。このノードは読み取り専用モードで、プライマリサイトがダウンするまで動作しません。
災害復旧ノード	リカバリ・ノードは、リカバリ・サイトにデプロイされたスタンドアロン・ノードです。このノードは、プライマリ・サイトに災害が発生して機能しなくなった場合に備えて、（新しいプライマリに対して）稼働状態になります。

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

ディザスタリカバリのワークフロー

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

災害発生前の初期設定



この図は、ディザスタ前のディザスタリカバリ設定を示しています。

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

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

前提条件

障害回復ノードをセットアップする前に、次の前提条件に注意してください:

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

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

次の表は、ディザスタリカバリノードを設定するための最小要件を示しています。

コンポーネント	条件
RAM	32 GB
仮想 CPU	8 基の CPU
記憶域	NetScaler ADM 展開では、ソリッドステートドライブ（SSD）テクノロジを使用することをお勧めします。デフォルト値は 120GB です。実際のストレージ要件は、NetScaler ADM のサイズ設定の見積もりによって異なります。Citrix ADM ストレージ要件が 120 GB を超える場合は、追加のディスクを接続する必要があります。**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

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

初めてのディザスタリカバリのセットアップ

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

高可用性モードで **NetScaler ADM** を展開する

障害復旧設定を設定するには、Citrix ADM が高可用性モードで展開されていることを確認してください。NetScaler ADM を高可用性で展開する方法については、「高可用性展開」を参照してください。

> 注
>
> - 高可用性モードでデプロイされた Citrix ADM は、Citrix ADM リリースバージョン 12.1 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。

NetScaler ADM 障害回復ノードを展開して登録する

NetScaler ADM 災害復旧ノードを登録するには:

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

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


```
--------------------------------------------------------------------------------
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
--------------------------------------------------------------------------------
      1. Citrix ADM Host Name [DR]:
      2. Citrix ADM IPv4 address [10.102.29.53]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.29.1]:
      5. DNS IPv4 Address [127.0.0.2]:
      6. Cancel and quit.
      7. Save and quit.

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

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 (*nsrecover/nsroot*) を使用してログオンします。
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。Citrix ADM 展開構成メニューが表示されます。

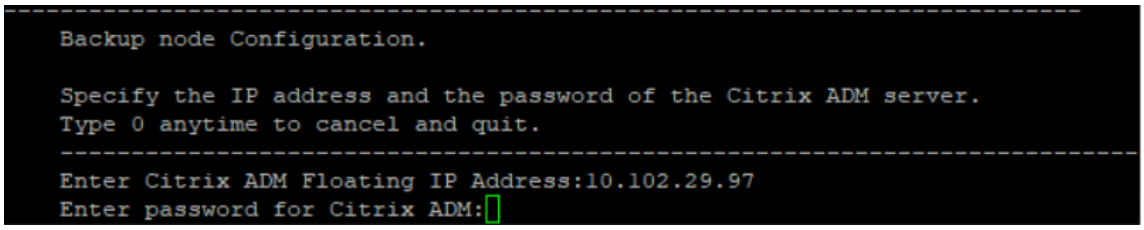
```
bash-3.2# /mps/deployment_type.py
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want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

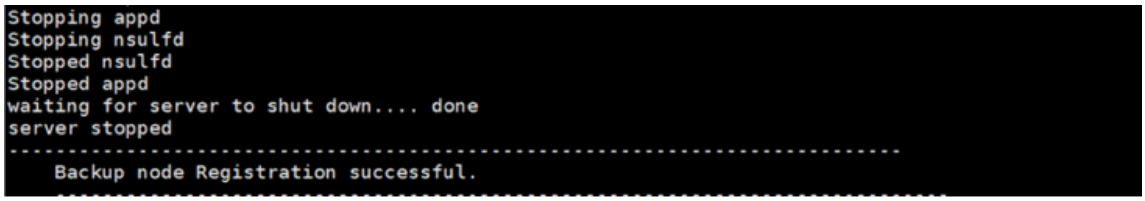
```
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------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

    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。



これで、災害復旧ノードが正常に登録されました。

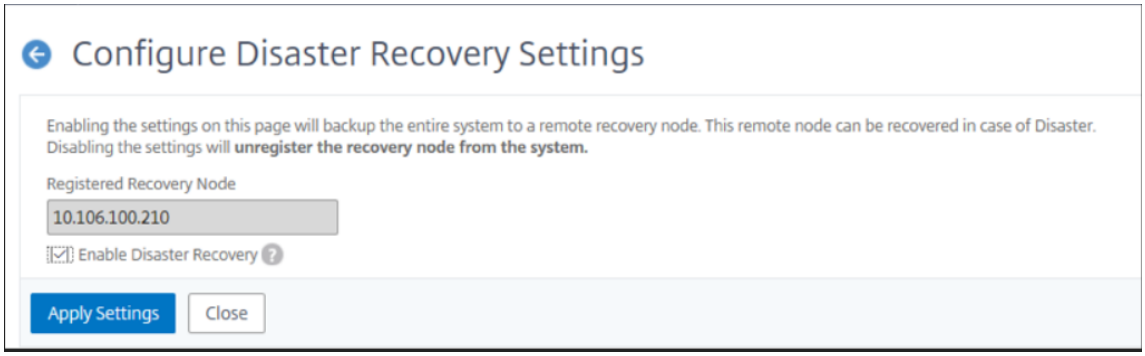


> 注:
>
> 災害復旧ノードには GUI がありません。

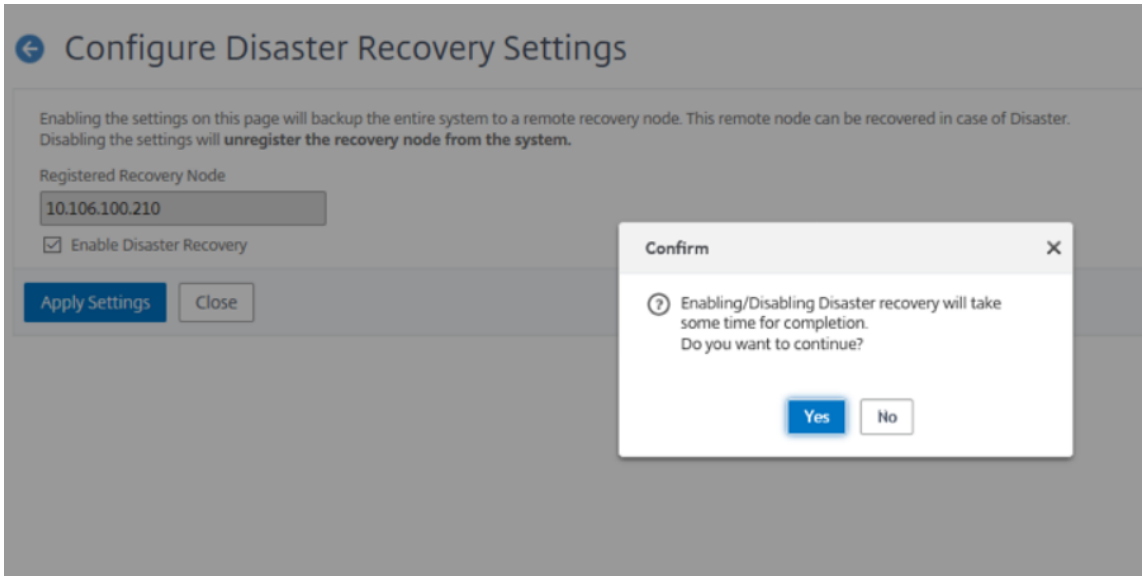
Citrix ADM GUI からディザスタリカバリ設定を有効にする

ディザスタリカバリノードが正常に登録されたら、Citrix ADM プライマリサイトの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にできます。

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. 「ディザスタリカバリ設定の構成」ページで、「ディザスタリカバリを有効にする」チェックボックスを選択し、「設定を適用」をクリックします。



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 (ワイドエリアネットワーク) のリンク速度によって異なります。

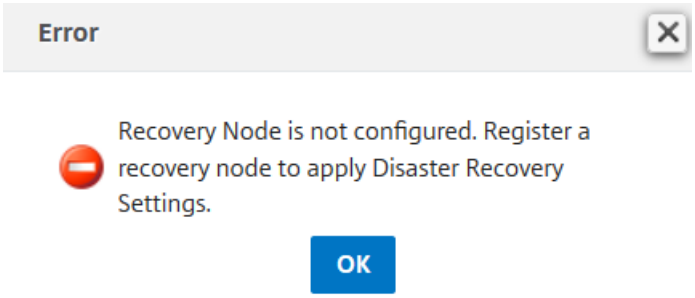
ディザスタリカバリ設定を無効にするには、「ディザスタリカバリを有効に する」チェックボックスをオフにし、「設定を適用」をクリック します。

確認ダイアログが表示されます。[はい] をクリックして続行します。

> 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。
> - ディザスタリカバリのワークフローは自動化されていないため、プライマリサイトの障害後に管理者が手動で開始する必要があります。
> - 管理者は、リカバリ・サイトの災害復旧ノードでリカバリ・スクリプトを実行して、プロセスを手動で開始する必要があります。
> - プライマリサイトの 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を手動でアップグレードする必要があります。

［ディザスタリカバリを有効にする］オプションを無効にして［設定の適用］をクリックすると、Citrix ADM では［ディザスタリカバリを有効にする］オプションを再度選択できなくなります。

ディザスタリカバリ設定をクリックすると、次のエラーメッセージが表示されます。



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:

a) 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。

b)「Citrix ADM ディザスタリカバリノードの展開と登録」に記載されている手順に従って、DR ノードを構成します。

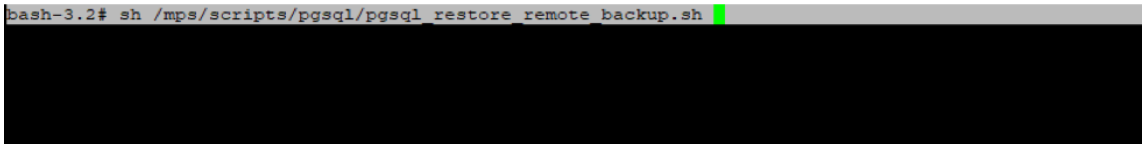
c) ディザスタリカバリオプションを有効にします。

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。

災害後のワークフロー

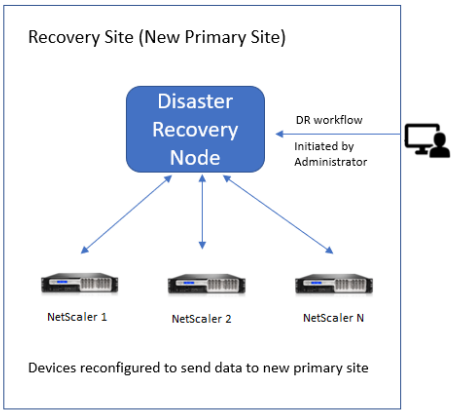
障害発生後にプライマリサイトがダウンした場合は、災害復旧ワークフローを次のように開始する必要があります。

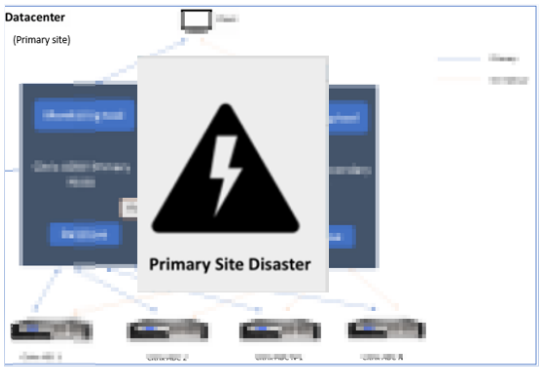
1. 管理者は、プライマリ・サイトが障害に見舞われ、そのサイトが稼働していないことを確認しました。
2. 管理者がリカバリプロセスを開始します。
3. 管理者は、ディザスタリカバリノード (リカバリサイト) で次のリカバリスクリプトを手動で実行する必要があります。**/mps/scripts/pgsql/pgsql_restore_remote_backup.sh**



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

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





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

災害復旧後

障害が発生し、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。

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

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 Citrix ADM では、リモートデータセンターにデプロイされた Citrix ADC インスタンスは、プライマリデータセンターで実行されている Citrix ADM から管理および監視できました。NetScaler ADC インスタンスは、データをプライマリ NetScaler ADM に直接送信し、WAN（ワイドエリアネットワーク）帯域幅を消費しました。さらに、分析データの処理には、プライマリ Citrix ADM の CPU とメモリリソースが使用されます。

お客様は、世界各地にデータセンターを設置しています。エージェントは、顧客が選択できる次のシナリオで重要な役割を果たします。

- WAN 帯域幅の消費を減らすために、リモートデータセンターにエージェントをインストールすること。
- データ処理のためにプライマリ Citrix ADM にトラフィックを直接送信するインスタンスの数を制限します。

> 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 Citrix ADC インスタンスをプライマリ Citrix ADM に直接追加できます。
> - リモートデータセンター用のエージェントをインストールしている場合、エージェントとプライマリサイト間の通信はフローティング IP アドレス経由で行われます。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、プールされたライセンスをリモートデータセンターのインスタンスに適用できます。このシナリオでは、プライマリサイトとリモートデータセンター間の通信は Floating IP アドレスを介して行われます。

Citrix ADM 12.1 では、別のデータセンターにあるプライマリ Citrix ADM と通信するようにエージェントを使用してインスタンスを構成できます。

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

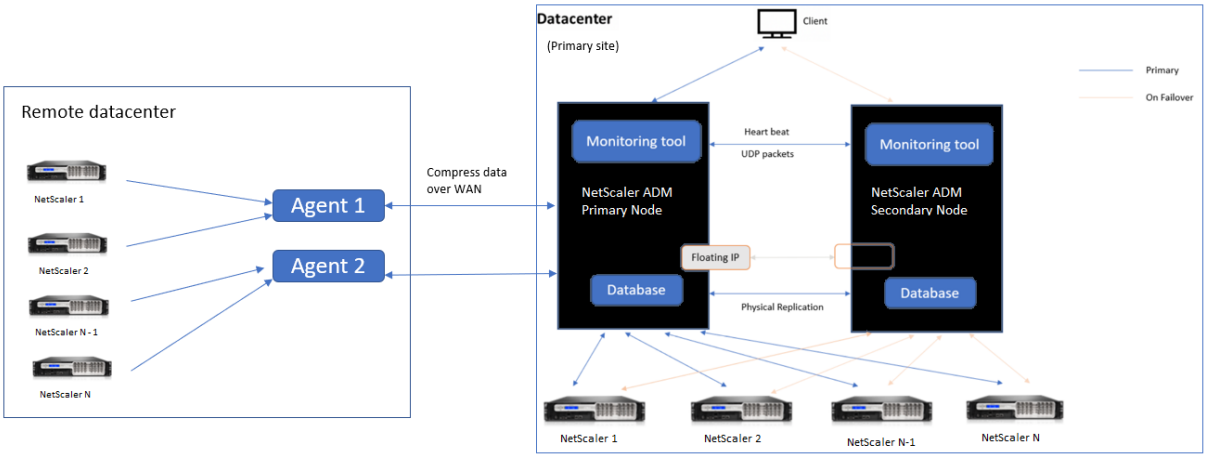
エージェントは、プライマリ NetScaler ADM と、異なるデータセンターで検出されたインスタンスの間の仲介者として動作します。エージェントをインストールする利点は次のとおりです。

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

  > 注
  >
  > サイトごとにインストールされるエージェントの数は、処理されるトラフィックによって異なります。現在、Citrix は、エージェントフェイルオーバーシナリオについて、サイトごとに 2 つのエージェントを検証しています。Citrix では、エージェントのフェイルオーバー時にトラフィックが別のエージェントに流れるように、サイトごとに少なくとも 2 つのエージェントをインストールすることをお勧めします。

アーキテクチャ

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



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

セカンダリサイトでは、エージェントがプライマリサイトの NetScaler ADM サーバーに展開され、登録されます。これらのエージェントはクラスタ内で動作し、エージェントのフェイルオーバーが発生した場合にトラフィックの継続的なフローを処理します。セカンダリサイトの NetScaler ADC インスタンスは、そのサイト内のエージェントを介してプライマリ NetScaler ADM サーバーに登録されます。インスタンスは、プライマリ NetScaler ADM ではなく、エージェントにデータを直接送信します。エージェントは、インスタンスから受信したデータを処理し、圧縮形式でプライマリ NetScaler ADM に送信します。エージェントは安全なチャネルを介して 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
  - エージェントを追加
- NetScaler ADC インスタンスの追加
  - 新しいインスタンスを追加する
  - 既存のインスタンスを更新する

エージェントをデータセンターにインストールする

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

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

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

> 注
>
> マルチサイト展開用のオンプレミスエージェントは、Citrix 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	8 GB 注：Citrix では 、パフォーマンスを向上させるためにデフォルト値を 32 GB に増やすことを推奨しています。
仮想 CPU	2 つの CPU 注：Citrix では 、パフォーマンスを向上させるためにデフォルト値を 8CPU に増やすことを推奨しています。
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。

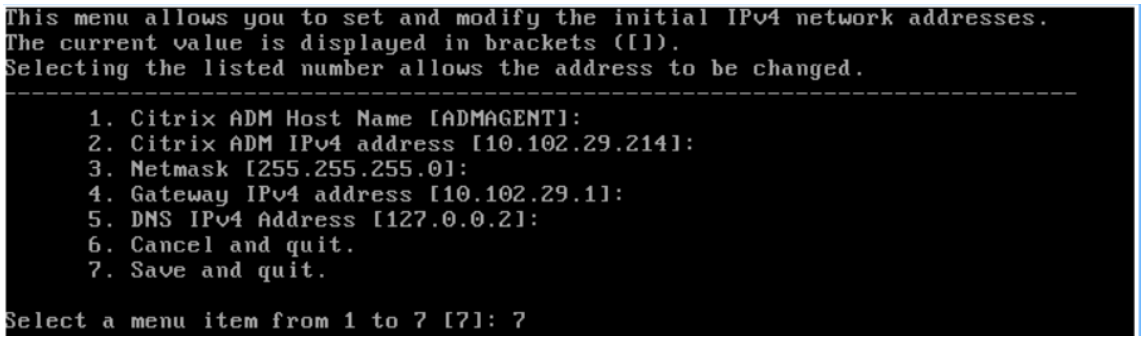
種類	ポート	詳細
TCP	8443, 7443, 443	エージェントと NetScaler ADM オンプレミスサーバー間の送信および受信通信用。

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

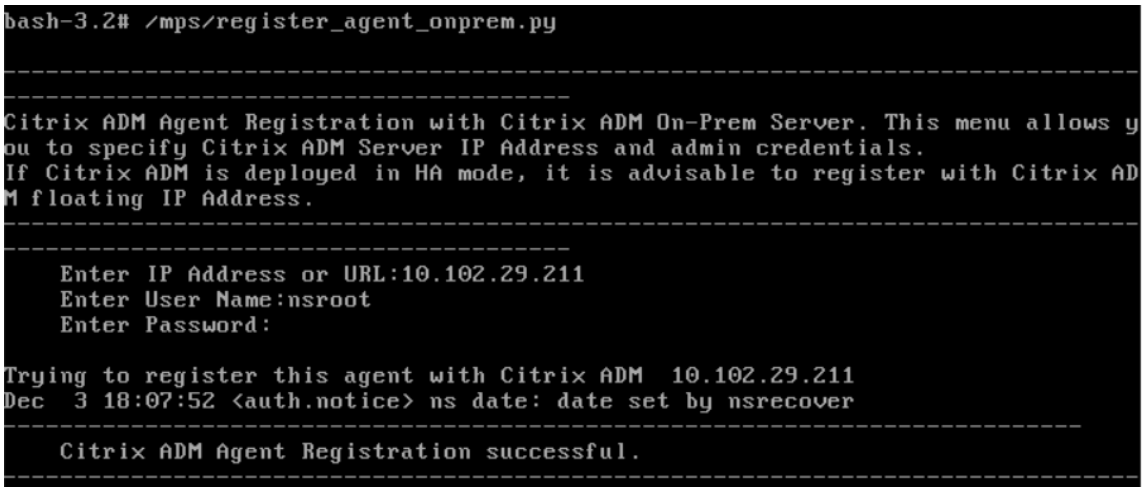
種類	ポート	詳細
TCP	80	エージェントと NetScaler ADC または Citrix SD-WAN インスタンス間の NITRO 通信用。
TCP	22	エージェントと NetScaler ADC または Citrix SD-WAN インスタンス間の SSH 通信用。高可用性モードで展開された NetScaler ADM サーバー間の同期用。
UDP	4739	エージェントと NetScaler ADC または Citrix SD-WAN インスタンス間の AppFlow ow 通信用。
ICMP	予約されているポートなし	高可用性モードで展開された NetScaler ADM と NetScaler ADC インスタンス、SD WAN インスタンス、またはセカンダリ NetScaler ADM サーバー間のネットワーク到達可能性を検出するため。
SNMP	161, 162	NetScaler ADC インスタンスからエージェントに SNMP イベントを受信する。
Syslog	514	NetScaler ADC または Citrix SD-WAN インスタンスからエージェントへの syslog メッセージを受信します。
TCP	5557	エージェントと Citrix ADC インスタンス間のログストリーム通信用。

エージェントを登録する

1. Citrix ダウンロードサイトからダウンロードしたエージェントイメージファイルを使用して、ハイパーバイザーにインポートします。<Version.no\ > エージェントイメージファイルの命名パターンは、**MASAGENT-\-**<HYPERVISOR\ > です。例：**MASAGENT-XEN-12.1-xy.xva**
2. ［コンソール］タブから、初期ネットワーク構成で Citrix ADM を構成します。
3. NetScaler ADM ホスト名、IPv4 アドレス、およびゲートウェイの IPv4 アドレスを入力します。オプション 7 を選択して、設定を保存して終了します。



4. 登録が成功すると、コンソールはログオンを要求します。資格情報として *nsrecover/nsroot* を使用します。
5. エージェントを登録するには、**/ mps/register_agent_onprem.py** と入力します。Citrix ADM エージェント登録資格情報は、次の図のように表示されます。
6. NetScaler ADM フローティング IP アドレスとユーザー資格情報を入力します。



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、Citrix ADM GUI にアクセスし、メインメニューから [ネットワーク**] > [**エージェント**]** ページに移動して、エージェントの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** 状態になります。

> 注
>
> NetScaler ADM はエージェントのバージョンを表示し、エージェントが最新バージョンであるかどうかも確認します。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追加

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 接続] ページで、リストからサイトを選択するか、プラス (+) ボタンを使用して新しいサイトを作成します。
3. 「保存」をクリックします。

> 注
>
> - デフォルトでは、新しく登録されたすべてのエージェントがデフォルトのデータセンターに追加されます。
> - エージェントを正しいサイトに関連付けることが重要です。エージェントに障害が発生した場合、エージェントに割り当てられた NetScaler ADC インスタンスは、同じサイト内の他の機能しているエージェントに自動的に切り替わります。

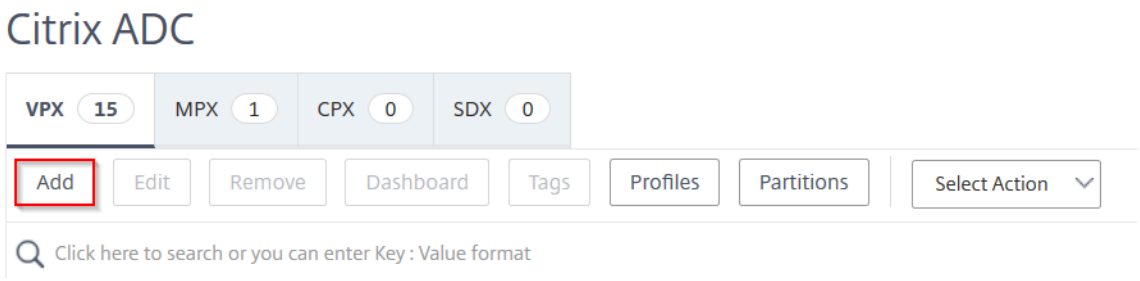
NetScaler ADC インスタンスの追加

インスタンスは、エージェントを介して NetScaler ADM から検出、管理、監視する Citrix アプライアンスまたは仮想アプライアンスです。次の Citrix アプライアンスおよび仮想アプライアンスを NetScaler ADM またはエージェントに追加できます。

- NetScaler ADC MPX
- NetScaler ADC VPX
- NetScaler ADC SDX
- NetScaler ADC CPX
- NetScaler Gateway
- Citrix Secure Web Gateway
- Citrix SD-WAN WO

新しいインスタンスを追加

1. [ネットワーク**] > [**インスタンス] に移動し、インスタンスタイプを選択します。たとえば、NetScaler ADC などです。
2. [追加] をクリックして新しいインスタンスを追加します。

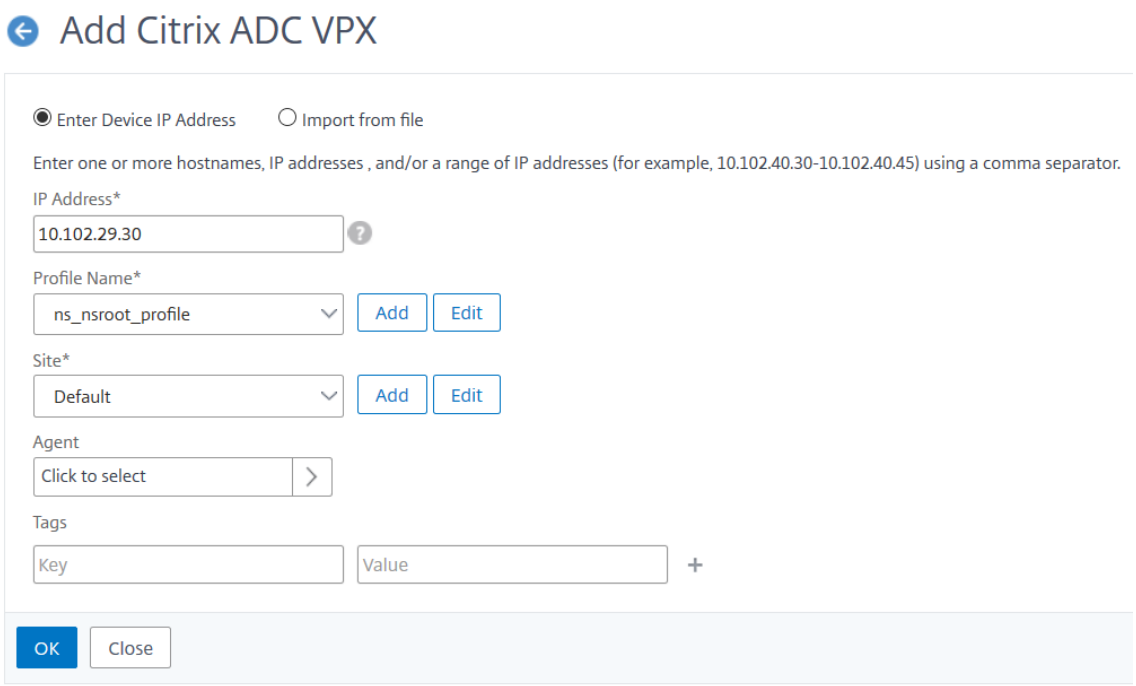


3. **[**デバイスの **IP** アドレスを入力] にチェックを入れ、IP アドレスを入力します。
4. 「プロファイル 名」から 適切なインスタンスプロファイルを選択するか、「**+**」アイコンをクリックして新しいプロファイルを 作成します。

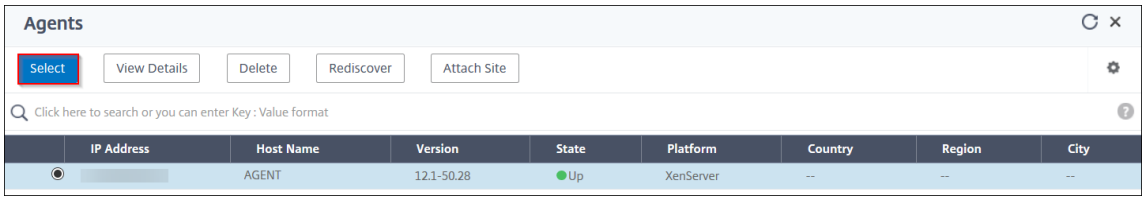
   > 注:
   >
   > インスタンスタイプごとに、デフォルトのプロファイルが用意されています。たとえば、ns-root-profile は、NetScaler ADC インスタンスのデフォルトプロファイルです。

5. インスタンスを関連付けるサイトを選択します。

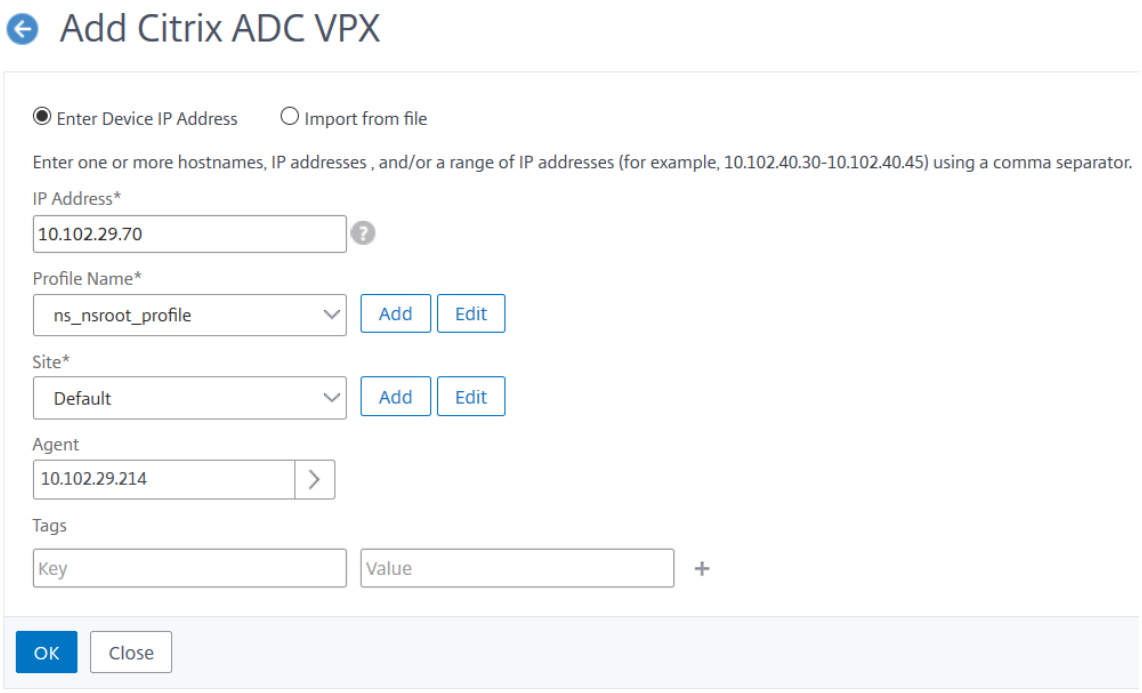
   > 注
   >
   > 選択したサイトに基づいて、そのサイトに関連付けられているエージェントのリストが表示されます。インスタンスを関連付けるサイトを必ず選択してください。



6. エージェントをクリックして選択します。エージェントページから 、インスタンスを関連付けるエージェントを選択し、[選択] をクリック します。



7. 「**Citrix VPX** の追加」ページで、「**OK**」をクリックします。



既存のインスタンスを更新してエージェントにアタッチする

インスタンスがすでにプライマリ Citrix ADM に追加されている場合は、インスタンスの追加ワークフローを編集してエージェントを選択することで、そのインスタンスをエージェントにアタッチできます。

1. [ネットワーク**] > [**インスタンス] に移動し、インスタンスタイプを選択します。たとえば、NetScaler ADC などです。
2. 既存のインスタンスを編集するには、[編集] ボタンをクリックします。
3. エージェントをクリックして選択します。
4. [**Agent**] ページで、インスタンスを関連付けるエージェントを選択し、[**OK**] をクリックします。

> 注:
>
> インスタンスを関連付けるサイトを必ず選択してください。

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、トラップ先が設定されているかどうかを確認します。

NetScaler ADM で、[ネットワーク**] > [**インスタンス**]** に移動します。[インスタンス] で、アクセスするインスタンスのタイプ（NetScaler ADC VPX など）を選択し、特定のインスタンスの IP アドレスをクリックします。

選択したインスタンスの GUI がポップアップウィンドウに表示されます。

デフォルトでは、エージェントはインスタンスのトラップ送信先として設定されます。確認するには、インスタンスの GUI にログオンし、トラップの送信先を確認します。

> 重要
>
> リモートデータセンターに Citrix ADC インスタンス用のエージェントを追加することをお勧めしますが、必須ではありません。
>
> インスタンスをプライマリ MAS に直接追加する場合は、インスタンスの追加中にエージェント を選択しないでください。

エージェントをクラスタ化する

エージェントクラスタという用語は、サイトに接続されているエージェントを論理的にグループ化するメカニズムを指します。これにより、エージェントの 1 つに障害が発生した場合、そのエージェントにトラフィックを送信する Citrix ADC インスタンスは、そのグループまたはサイト内の他の正常なエージェントへのトラフィックの送信を開始するように自動的に再構成されます。

エージェントをリモートサイトにクラスター化することの利点は、1 つのエージェントに障害が発生した場合、Citrix ADM によって検出され、すべてのインスタンスがそのクラスター内の他の使用可能なエージェントに暗黙的に再配布されることです。

たとえば、次に示すように、バンガロールのサイトには 10.106.1xx.2x と 10.106.1xx.7x の 2 つのエージェントが接続され、稼働しています。

1 つのエージェントがダウンすると、Citrix ADM はそれを検出し、ダウン状態を表示します 。

そのエージェントにアタッチされたインスタンスは、同じクラスターの他のエージェントをトラップ先や syslog サーバーなどに使用するように自動的に再構成されます。

> 注**:**
>
> インスタンスの再構成には多少の遅延があります。

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

Citrix ADM 単一サーバーを、2 台の Citrix ADM サーバーからなる高可用性展開にアップグレードできます。Citrix ADM サーバーの高可用性ペアはアクティブ/パッシブモードで、両方のサーバーの構成は同じです。このタイプのアクティブ/パッシブ展開では、一方の Citrix ADM サーバーがプライマリノードとして構成され、もう一方がセカンダリノードとして構成されます。何らかの理由でプライマリノードがダウンした場合、セカンダリノードが引き継ぎます。

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

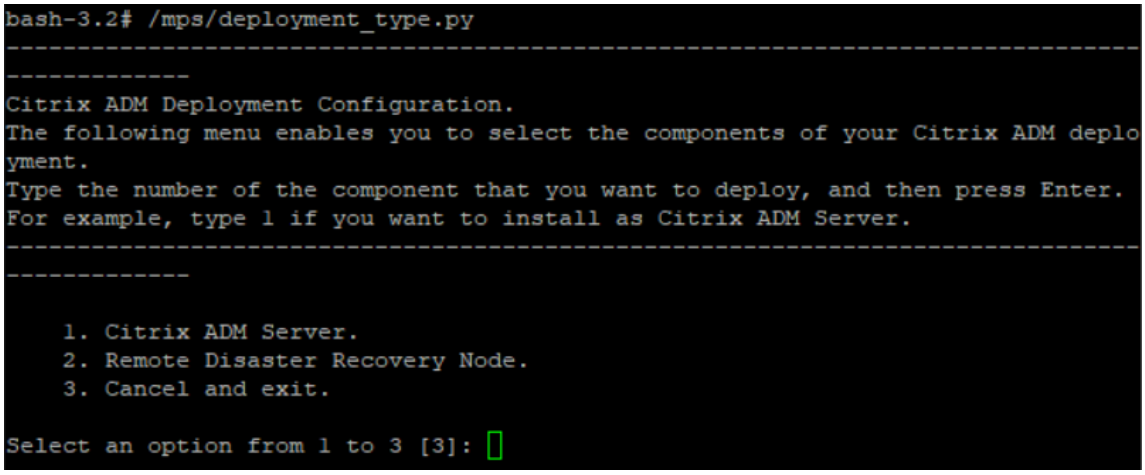
Citrix ADM 単一サーバーを高可用性モードに移行するには、次の手順が必要です:

1. 既存のサーバーノードを変更します
2. 2 台目のサーバーノードをプロビジョニングします
3. HA モードで 2 つのノードを展開します
4. 高可用性ペアの設定

既存の **Citrix ADM** サーバーノードを変更します

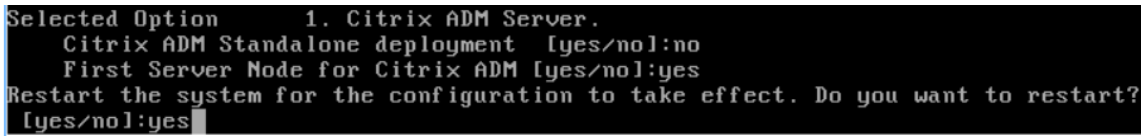
Citrix ADM を単一サーバーから高可用性モードに移行するには、サーバーノードの初期展開タイプを高可用性モードに変更する必要があります。

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



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。

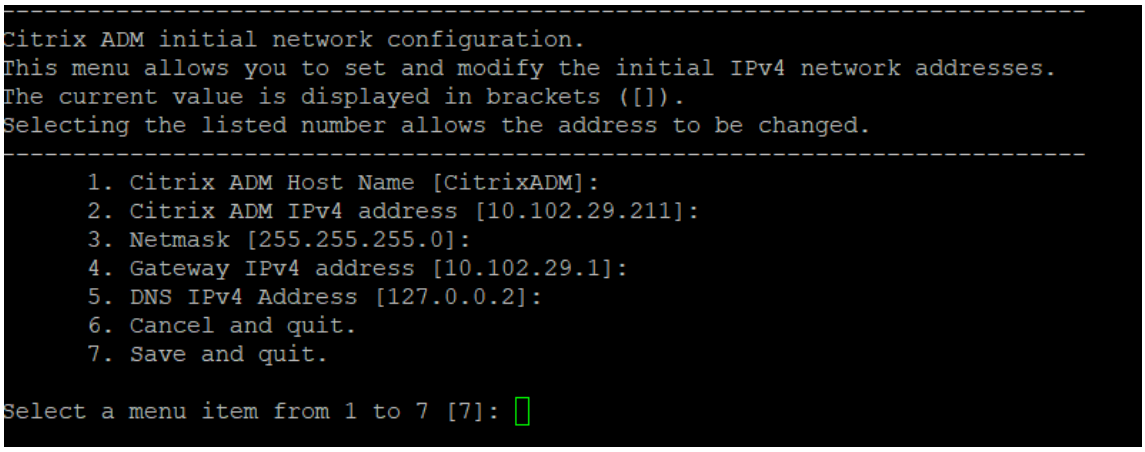
7. サーバーを再起動するかどうかを尋ねるメッセージがコンソールに表示されます。
8. 「**Yes**」と入力して再起動します。



2 番目のサーバ・ノードのプロビジョニング

ハイパーバイザー上に 2 台目のサーバーをプロビジョニングする必要があります。1 台目のサーバーのインストールに使用したものと同じイメージファイルを使用するか、同じバージョンのイメージファイルを Citrix のダウンロードサイトから取得します。

1. イメージファイルを Hypervisor にインポートし、[Console] タブから、次の画面の説明に従って初期ネットワーク構成オプションを設定します:



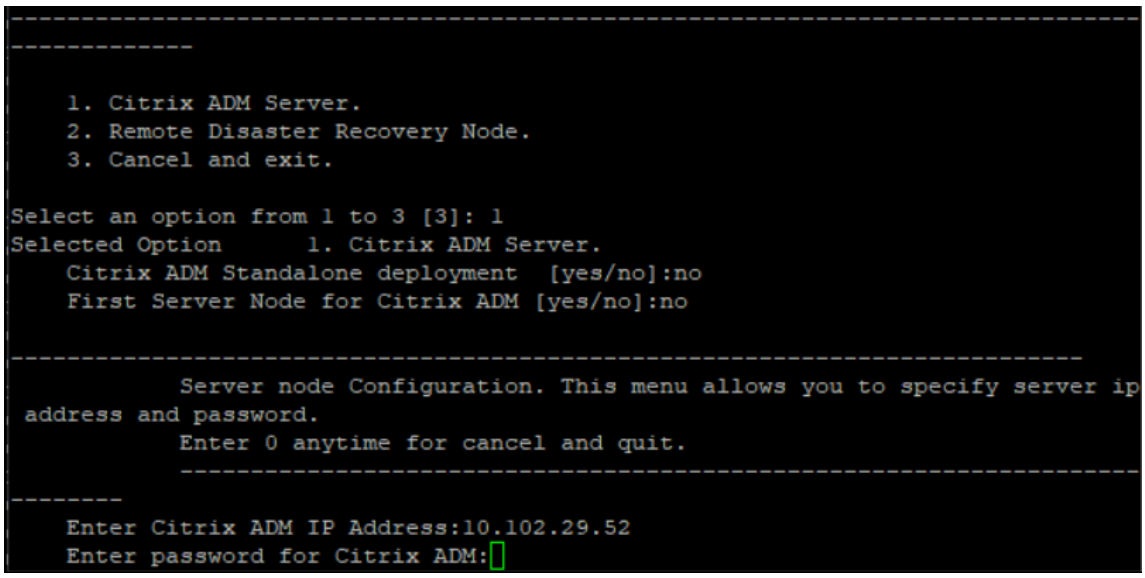
2. 必要な IP アドレスを指定した後、シェルプロンプトで /mps/deployment_type.py と入力し、Enter キーを押します。
3. 展開タイプを **Citrix ADM** サーバーとして選択します。
4. デプロイメントコンソールで、サーバーデプロイメントを選択するよう求められます（スタンドアロンとして）。「**No** 」と入力して、展開を高可用性ペアとして確認します。


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

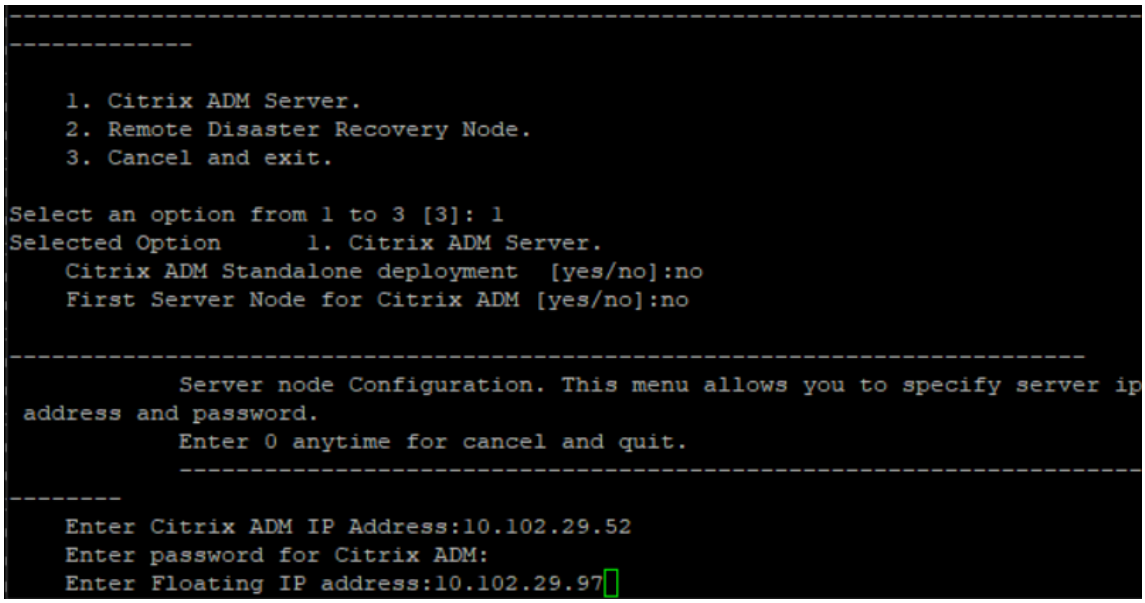
5. （最初のサーバーノード）を選択するかどうかを尋ねるメッセージがコンソールに表示されます。「**No** 」と入力して、ノードを 2 番目のサーバ・ノードとして確認します。

```
------------------------------------------------------------------------------
-------------
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
    First Server Node for Citrix ADM [yes/no]:no
```

6. 最初のサーバーの IP アドレスとパスワードを入力します。



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 Citrix ADM サーバーノードの GUI からこれらのノードを展開する必要があります。2 台のサーバー間の内部通信は、2 つのサーバーノードを展開した時点で開始されます。

1. Web ブラウザで、既存の NetScaler ADM サーバーノードの IP アドレスを入力します。
2. ［**User Name**］と ［**Password**］の各フィールドに管理者の資格情報を入力します。

3. [システム] タブで、[配置] に移動し、[****** 配置 ******] をクリックします。
4. 確認のメッセージが表示されます。［はい］をクリックします。

   > 注:
   >
   > Citrix ADM を高可用性で展開すると、フローティング IP を使用してプライマリノードにアクセスできます。12.1 リリース以降では、セカンダリノードにアクセスできません。

5. 2 番目のサーバノードの設定時に Floating IP を入力しましたが、システムページで FIP を更新することもできます。[**HA** 設定] > [高可用性モード用のフローティング **IP** アドレスの設定] をクリックします。前に設定したフローティング IP アドレスを表示できます。新しい IP アドレスを入力して [**OK**] をクリックします。

NetScaler Insight Center から **Citrix ADM** への移行

February 6, 2024

既存の構成、設定、またはデータを失うことなく、NetScaler Insight Center 展開を NetScaler ADM に移行できるようになりました。Citrix ADM を使用すると、アプリケーションに関連する 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することもできます。

> 注
>
> 現在のところ、移行は、NetScaler Insight Center スタンドアロンインスタンスでのみサポートされています。

前提条件

NetScaler Insight Center 仮想アプライアンスを Citrix ADM に移行する前に、次の要件が満たされていることを確認してください。

- NetScaler Insight Center 11.1 Build 47.14 以降がインストールされている。
- NetScaler ADM 12.0 ビルド 57.24.tgz イメージファイルをダウンロードしました。

  > 注
  >
  > :Citrix ADM 12.0 ビルド 57.24 をインストールしてから、最新の Citrix ADM 12.1 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 12.1 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 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。
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
ヴイエムウェア 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 のシェルプロンプトにログオンします。
2. NetScaler ADM 12.0 ビルド 57.24 を */var/mps/mps_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. Citrix 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 Citrix ADM 12.1 ビルドにアップグレードする必要があります。

移行後、NetScaler Insight Center インベントリで検出されたすべての NetScaler インスタンスが、Citrix ADM の［ネットワーク］**>**［インスタンス］セクションに表示されます。ただし、最初は、検出されたアプライアンスでホストされている仮想サーバーを手動でポーリングする必要があります。

> 注
>
> Citrix ADM では、デフォルトでは、検出された NetScaler インスタンス内に作成された 30 台の仮想サーバーを管理および監視するためのライセンスコストはかかりません。30 台を超える数の仮想サーバーを監視および管理するには、必要な MAS ライセンスをインストールしてください。詳しくは、「NetScaler ADM ライセンス」を参照してください。

Command Center 構成を **NetScaler ADM** に移行する

February 6, 2024

Command Center 環境と NetScaler ADM 展開の既存の構成、設定、またはデータを失うことなく、Command Center 構成を NetScaler Application Delivery Management（ADM）に移行できるようになりました。移行プロセスが完了すると、移行された Command Center 構成を NetScaler ADM で表示できます。

注意事項

- Command Center 構成の NetScaler ADM への移行は、次の展開でサポートされています。
  - Command Center スタンドアロンから NetScaler ADM スタンドアロン展開または NetScaler ADM 高可用性展開へ。
  - NetScaler ADM スタンドアロン展開または NetScaler ADM 高可用性展開への Command Center の高可用性。

  > 注:
  >
  > Command Center スタンドアロンまたは高可用性展開を NetScaler ADM スタンドアロンまたは高可用性展開に移行する場合は、Command Center および NetScaler ADM の高可用性展開のプライマリノード IP アドレスのみを使用する必要があります。

- Command Center ツールは、同じまたは異なる NetScaler ADM 展開で複数回実行できます。
  - 同じ Citrix ADM で初めて Command Center ツールを実行すると、すでに移行されて Citrix ADM に存在する構成のログが失敗として表示されます。

  - 同じ NetScaler ADM に対してツールを実行した時点から今までの間に Command Center に新しい構成が追加されている場合は、新しいカスタムタスクを除くすべての構成が NetScaler ADM に移行されます。

- Command Center 構成の Citrix ADM への移行は、Citrix ADC、Citrix ADC SDX、および Citrix SD-WAN WO デバイスでサポートされています。
- Command Center と NetScaler ADM 間の通信はすべて HTTPS 接続で行われます。
- Command Center 構成を移行する前に、NetScaler ADM の既存のデータをバックアップすることを強くお勧めします。
- Command Center 移行が完了すると、NetScaler ADC の管理パーティションが NetScaler ADM で自動検出されます。

制限事項

以下の Command Center 構成は、Command Center アプライアンスから NetScaler ADM に移行されません。

- デバイスバックアップ構成ファイル
- SD-WAN WO デバイスプロファイルのタイムアウトの詳細
- イベントトリガーおよびアラームトリガーの以下の詳細は移行されません。
  - コマンド実行アクションの中止の詳細
  - タスク実行の詳細
  - パラメーター（重要度/カテゴリ/インスタンス/エラーオブジェクト）がすべて空のトリガーは移行されません
  - インスタンスの状態が HA クラスター、プライマリ、セカンダリであるトリガーは、インスタンスで 3 つの状態すべてが選択されている場合移行されません
- 説明の設定されていないカスタムタスクは移行されません
- イベントの重要度設定
- イベント規則のスケジュールの詳細
- syslog の非表示フィルター
- 構成タスクの詳細
- 監査テンプレート
- デバイスが設定されていない監査ポリシー
- 監査ポリシーのスケジュールの詳細

- RBAC グループの承認済みスコープ設定
- データベースのモニターおよび管理の設定
- カスタムパフォーマンスレポート
- パフォーマンスしきい値
- エラー/syslog/レポート/エンティティ監視のカスタムビュー
- AppFirewall および NS ゲートウェイのレポートおよびスケジュールの詳細
- SD-WAN WO 自動構成の詳細
- 高可用性設定
- スケジュール済みのシステムバックアップ設定
- データベースの再試行設定
- syslog パージのスケジュール
- すべてのモジュールの全統計データ（syslog、イベント、監査ログなど）

前提条件

Command Center 構成を NetScaler ADM に移行する前に、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。

- Command Center Version 5.2 のビルド 48.2 以降を実行している。
- NetScaler ADM バージョン 12.0 ビルド 51.24 以降をインストールして構成しました。
- 管理者ユーザーのみが Command Center 構成の移行を実施する。
- カスタムタスクを正常に移行するためには、Command Center の［description］ボックスへの入力が必須になる。
- Command Center と NetScaler ADM 間の通信は NITRO ベースです。NITRO 通信には、Command Center と NetScaler ADM で必要な SSL（セキュアソケットレイヤー）および TLS（トランスポートレイヤーセキュリティ）プロトコル設定を構成して開く必要があります。

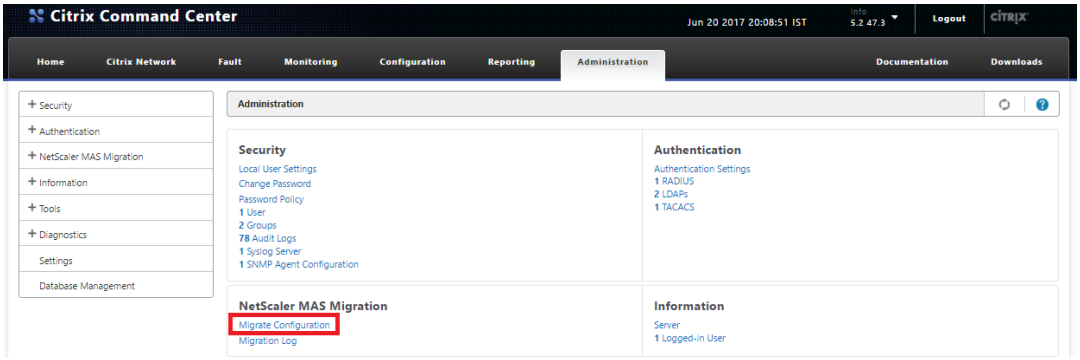
> 注
>
> 5.2 build 48.2 より前の Command Center バージョンを使用している場合は、Command Center バージョンを 5.2 build 48.2 にアップグレードしてから、Command Center 構成を NetScaler ADM に移行する必要があります。Command Center アプライアンスのアップグレードの詳細については、Command Center のアップグレードを参照してください。

構成の移行

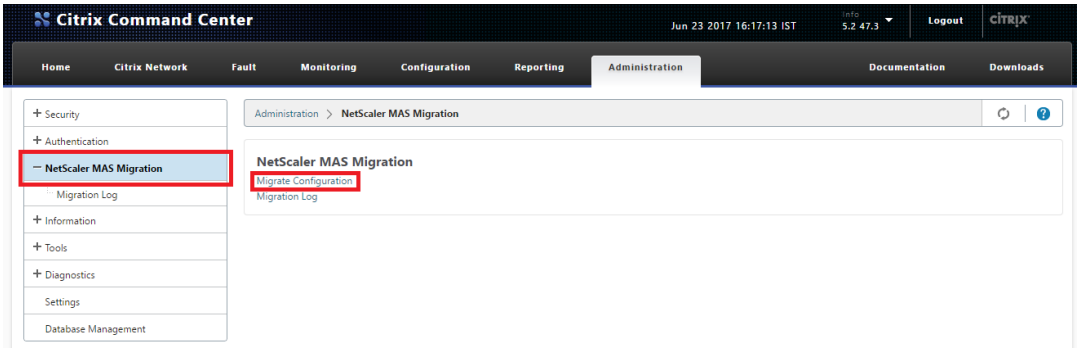
Command Center 構成を NetScaler ADM に移行するには、Command Center アプライアンスの IP アドレスと管理者の資格情報が必要です。

Command Center 構成を **NetScaler ADM** に移行するには:

1. Web ブラウザーに Command Center アプライアンスの IP アドレスを入力します。
2. [ユーザー名] と [パスワード] フィールドに、管理者の資格情報を入力してログインします。
3. ログインに成功したら、表示される画面で［管理］タブを選択し、次のいずれかの操作を行います。
   - 右側のペインの［**Citrix ADM** 移行］で、次の図に示すように［構成の移行］を選択します。

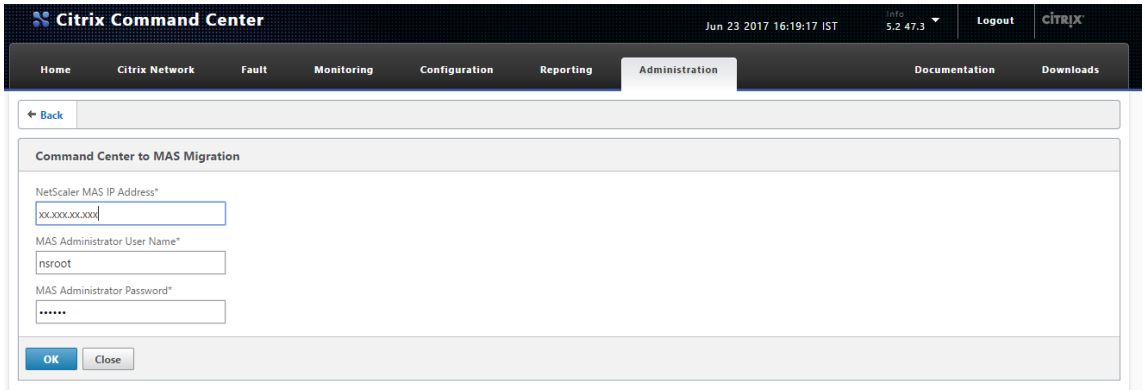


   - 次の図に示すように、左側のペインで［**Citrix ADM** 移行］を選択し、［構成の移行］をクリックします。

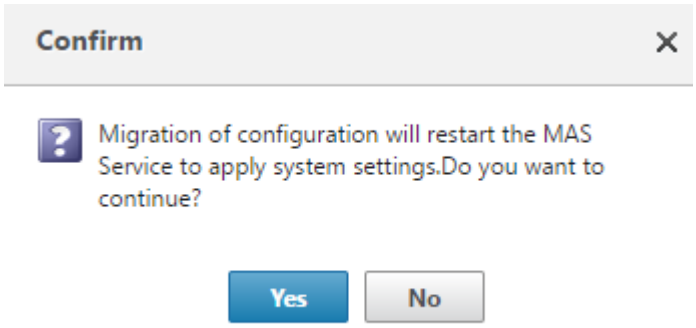


4. 「**Command Center** から **MAS** への移行」ダイアログボックスで、Citrix ADM サーバーの IP アドレスと管理者の資格情報を入力し、「**OK**」をクリックします。

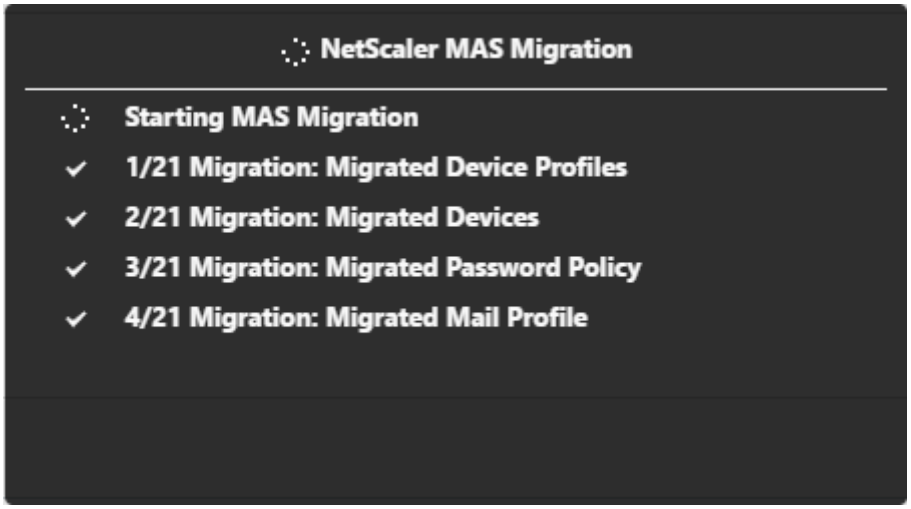
> 注:
>
> NetScaler ADM の高可用性展開の場合は、プライマリノードの IP アドレスを入力します。



5. 確認のプロンプトで、[はい] をクリックします。



画面に移行タスクの進捗状況が表示されます。



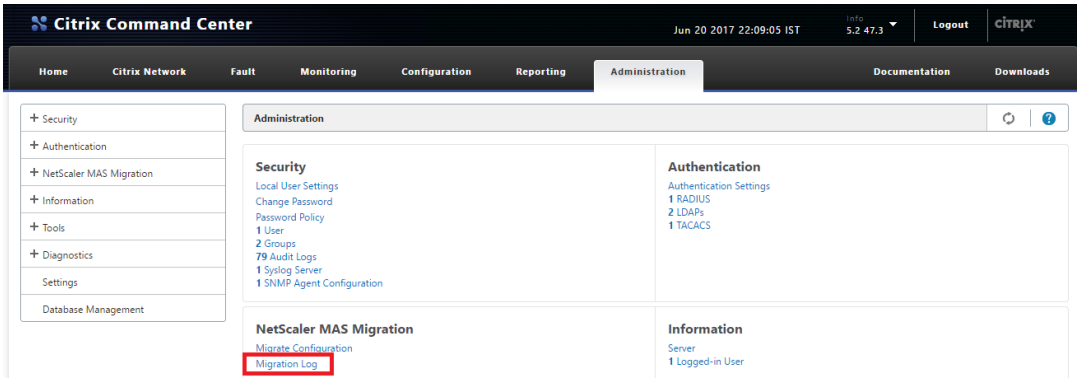
構成の移行 操作では、NetScaler ADM 展開の詳細と管理者の資格情報を入力として受け取ります。次に、構成の移行操作により、Command Center 展開の構成が NetScaler ADM 展開に移行されます。

タスクが完了すると、移行されたコマンドセンターの構成を Command Center 移行ログと NetScaler ADM データから確認できます。

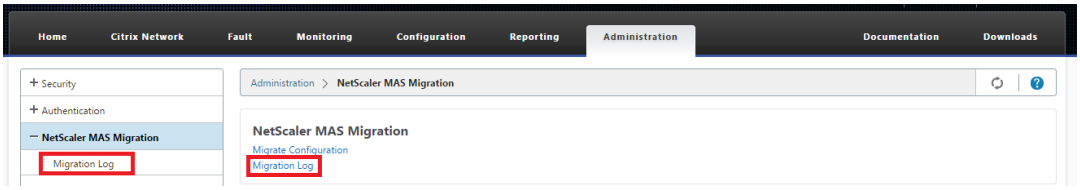
Command Center 移行ログを使用して移行を検証するには

1. Command Center GUI の [管理] タブで、次のいずれかの操作を行います。

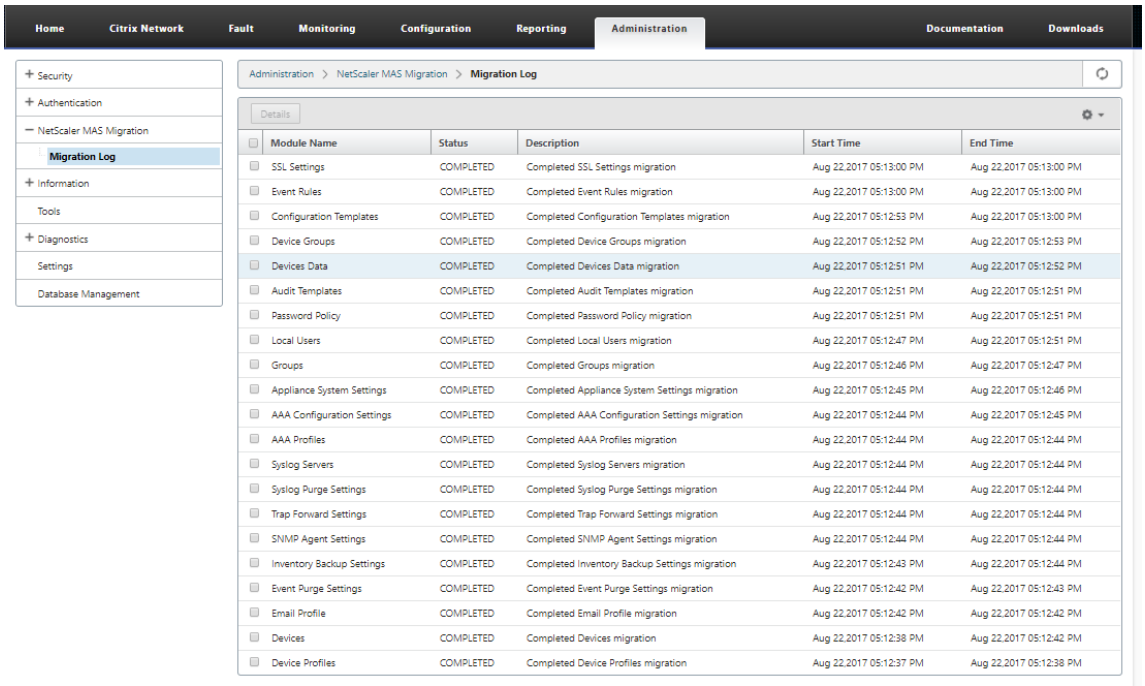
   - 右側のペインの［**Citrix ADM** 移行］で、［移行ログ］をクリックします。



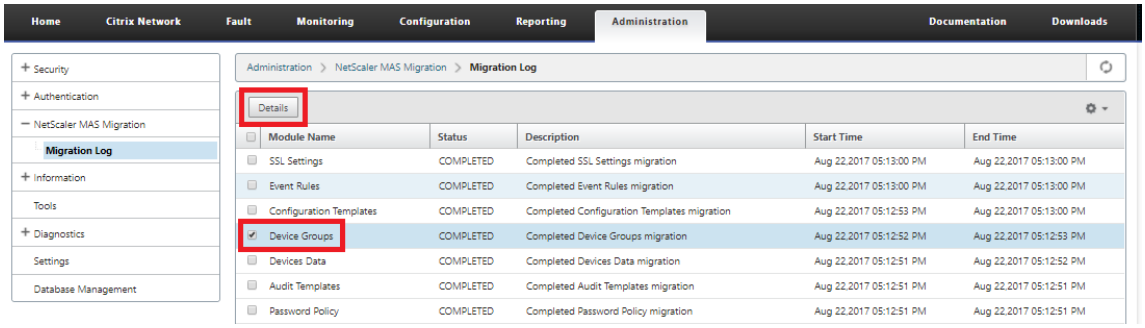
   - 左側のペインで［**Citrix ADM** 移行］を選択し、［移行ログ］をクリック します。



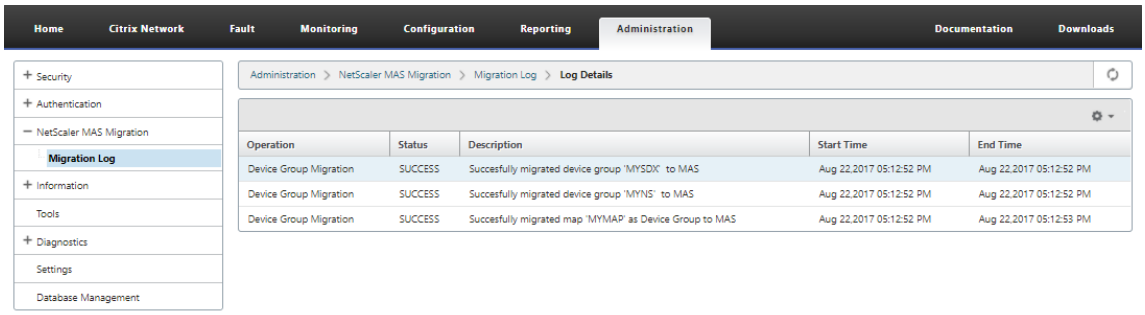
2. 移行ログの一覧を確認します。



3. 詳細を表示するには、「モジュール名」を選択するか、特定のモジュールの詳細を表示するには、そのモジュールを選択して「詳細」をクリックします。



4. 以下の例に、選択したモジュールのログの詳細を示します。



NetScaler ADM を使用して移行を確認するには、次の手順に従います

移行プロセス中に、Command Center 構成は NetScaler ADM に移行され、NetScaler ADM GUI に NetScaler ADM 構成として表示されます。

移行プロセスが完了すると、NetScaler ADM サーバーが再起動し、一時的にダウンタイムが発生する可能性があります。NetScaler ADM サーバーが起動したら、ブラウザのアドレスバーに NetScaler ADM サーバーの IP アドレスを入力して NetScaler ADM GUI にアクセスします。

次の表は、移行された構成の NetScaler ADM 用語が Command Center で使用されている用語とどのように対応しているかを示しています。

Command Center 用語	NetScaler ADM 用語
デバイスプロファイル	インスタンスプロファイル
デバイスとその状態（管理対象/管理対象外など）	インスタンスとその状態（管理対象/管理対象外など）
デバイスコメント	インスタンスコメント
デバイスグループ	インスタンスグループ
マップ	インスタンスグループ
イベントトリガーとアラームトリガー	イベント規則
組み込み/カスタムのタスクコマンド	ジョブ作成エディターの構成テンプレート

Command Center 用語	NetScaler ADM 用語
定期監査ポリシー	監査テンプレート
パスワードポリシー	パスワードポリシー
ユーザー（ローカルユーザーのみ）	システムユーザー
グループ *	システムグループ
認証プロファイルおよび認証設定	認証プロファイルおよび認証構成
メール設定	メールサーバー/メール配布リスト
Syslog サーバー	Syslog サーバー
SSL 設定	SSL 設定
SNMP エージェント構成	SNMP マネージャー
トラップ転送設定	トラップ転送
イベントパージ設定	イベント削除設定
インベントリ設定	インスタンスバックアップ設定
syslog パージ設定	syslog 削除設定
アプライアンスネットワーク設定（DNS、NTP、タイムゾーンなど）	DNS、NTP、タイムゾーンなどの NetScaler ADM ネットワーク設定

*Command Center のすべての権限を持つグループは、NetScaler ADM の「管理者」ロールを持つグループとして移行されます。他のすべての Command Center グループは、NetScaler ADM で「読み取り専用」の役割を持つグループとして移行されます。

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 **Citrix ADM** への移行のハードウェア要件

コンポーネント	条件
RAM	32 GB
仮想 CPU	8
記憶域	500GB。NetScaler ADM 展開では、ソリッドステートドライブ（SSD）テクノロジを使用することをお勧めします。
仮想ネットワーク インターフェイス	1
スループット	1Gbps または 100Mbps

ソフトウェア要件

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

- Director Version 1811 がインストールされている。
- NetScaler HDX Insight Version 10.1 以降がインストールされている。
- HDX Insight と Citrix ADM は Citrix VDA バージョン 7.0 以降をサポートしています
- Citrix Workspace は、Citrix Virtual Apps and Desktops バージョン 7.0 以降でサポートされています
- MAC Citrix Receiver for Mac Version 11.8 以降および Windows Citrix Receiver for Windows 14.0 以降が有効であり、正確な ICA RTT の測定基準を表示できる。
- NetScaler ADM バージョン 11.0 以降がインストールされます。NetScaler ADM のインストール方法の詳細については、「NetScaler ADM の展開」を参照してください。

制限事項

- この機能は、組織のライセンスおよび管理者権限によっては使用できない場合があります。

- ICA セッション RTT（Round Trip Time：往復時間）のデータは、Citrix Receiver for Windows 3.4 以降および Citrix Receiver for Mac 11.8 以降の場合、正確に表示されます。これらのバージョンよりも前のバージョンの Receiver については、正確なデータが表示されません。
- ［Trends］ビューでは、7 よりも前のバージョンの VDA に対しては HDX 接続のログオンデータが収集されません。以前のバージョンの VDA については、グラフのデータが 0 として表示されます。
- 500GB 未満の記憶域の外部ハードディスクが既に存在する展開に対して、追加ハードディスクは設定できません。

> 注
>
> - Director の詳細と、NetScaler ADM を Director と統合する手順については、http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director.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。

NetScaler ADM に追加ディスクを接続する

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。データの保存に 120 GB を超える容量が必要な場合は、追加のディスクを接続できます。

> 注
>
> - Citrix ADM の初期展開時に、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。
> - Citrix ADM 高可用性展開では、各ノードに追加のディスクを接続する必要があります。両方のディスクのサイズは同じである必要があります。
> - 以前より容量の低い外部ディスクを接続していた場合は、新しいディスクを接続する前にディスクを取り外す必要があります。
> - 2 TB を超える容量の追加ディスクを接続できます。必要に応じて、ディスクのサイズも 2 テラバイト未満にすることができます。
> - NetScaler ADM 展開では、ソリッドステートドライブ（SSD）テクノロジを使用することをお勧めします。

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

1. 新しい追加ディスクを接続
2. ディスクパーティション化ツールの起動
3. 新しい追加ディスクにパーティションを作成する
4. 既存の追加ディスクのサイズを変更
5. 追加ディスク上のパーティションを削除する

スタンドアロン **Citrix ADM** に追加のディスクを接続する

仮想マシンにディスクをアタッチするには、次の手順を実行します。

1. NetScaler ADM 仮想マシンをシャットダウンします。
2. ハイパーバイザーで、必要なディスクサイズの追加ディスクを Citrix ADM 仮想マシンに接続します。

   新しく接続された大きなディスクには、データベースデータと NetScaler ADM ログファイルが格納されます。コアファイル、オペレーティングシステムログファイルなどの保存には、既存の 120 ギガバイトのデフォルトディスクが使用されます。
3. NetScaler ADM 仮想マシンを起動します。

NetScaler ADM ディスクパーティションツール

NetScaler ADM では、新しいコマンドラインツールである **NetScaler ADM** ディスクパーティションツールが提供されるようになりました。このツールの機能については、次のように詳しく説明します。

1. このツールを使用すると、新しく追加されたディスクにパーティションを作成できます。
2. このツールを使用して、既存の追加ディスクのサイズを変更することもできます。ただし、既存の外部ディスクは 2 TB を超えないようにしてください。

   > 注
   >
   > - データを失わずに 2 テラバイトを超える既存のディスクのサイズを変更することはできません。これは、プラットフォームの既知の制限によるものです。
   > - 2 テラバイトを超えるストレージ容量を作成するには、既存のパーティションを削除し、この新しいツールを使用してパーティションを作成する必要があります。
3. この新しいツールを使用すると、ディスク上で任意のパーティションアクションを明示的に実行できます。このツールを使用すると、ディスクと関連データを明確に可視化して制御できます。

> 注:
>
> このツールは、NetScaler ADM サーバーに接続した追加ディスクでのみ使用できます。このツールを使用してプライマリ (デフォルト) の 120 ギガバイトディスクにパーティションを作成することはできません。

ディスクパーティションツールを起動する

1. PuTTY などの SSH クライアントを使用して、NetScaler ADM への SSH 接続を開きます。
2. 管理者の資格情報を使用して Citrix ADM にログオンします。
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。

コマンドを実行すると、GUID パーティションテーブル (GPT) パーティションスキームが作成されます。また、残りの領域を使用するために 32 GB の swap パーティションとデータパーティションが作成されます。その後、プライマリパーティションに新しいファイルシステムが作成されます。

> 注:
>
> このプロセスには数秒かかることがあり、プロセスを中断しないでください。

```
(dpt): create

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

```
Creating GPT partition scheme...
da1 created

Creating partition 1 using (456287933) blocks. Leaving aside 32G for swap...
da1p1 added

Creating partition 2 for swap using remaining 32G...
da1p2 added

Formatting the new partition. This may take some time (~20 seconds). Please be patient and don't interrup the process...
```

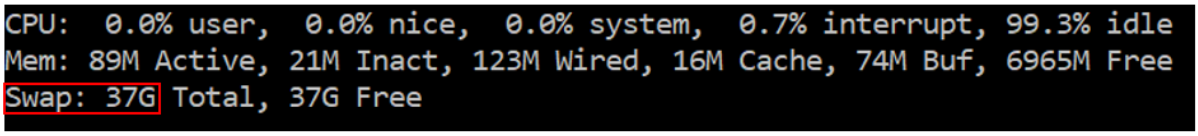
create コマンドが完了すると、仮想マシンが自動的に再起動され、新しいパーティションがマウントされます。

```
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。

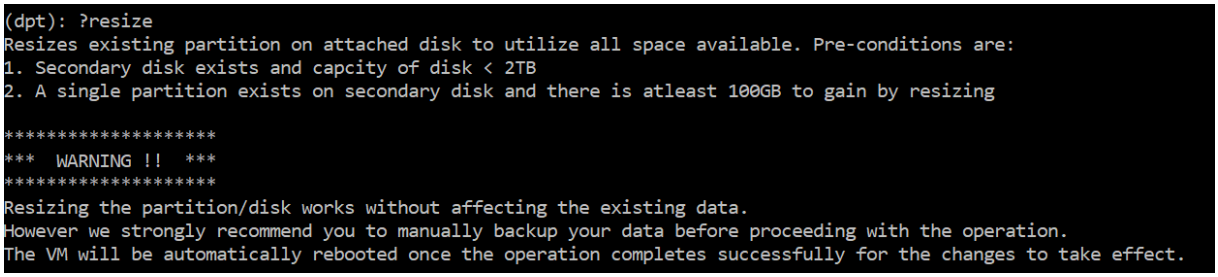


> 注
>
> パーティションを作成すると、このツールによって仮想マシンが再起動されます。

既存の追加ディスク内のパーティションのサイズを変更する

resize コマンドを使用して、アタッチされている (セカンダリ) ディスクのサイズを変更できます。マスターブートレコード (MBR) または GPT スキームの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、最大 2 TB のサイズにする必要があります。

> 注
>
> - 「resize」コマンドは、既存のデータを失うことなく機能するように設計されています。ただし、サイズ変更を試みる前に、このディスク内の重要なデータを外部ストレージにバックアップすることを Citrix ではお勧めします。データバックアップは、サイズ変更操作中にディスクデータが破損する可能性がある場合に役立ちます。
> - パーティションのサイズ変更中は、ディスク領域を 100 GB ずつ増やしてください。このような増分増加により、より頻繁にサイズを変更する必要がなくなります。



「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続行します。これにより、NetScaler ADM サブシステム、PostgreSQL DB プロセス、および NetScaler ADM モニタープロセスなど、ディスクにアクセスするプロセスが停止されます。プロセスが停止すると、ディスクはアンマウントされ、サイズ変更の準備をします。サイズ変更は、使用可能な領域全体を占有するようにパーティションを拡張し、ファイルシステムを拡張することによって行われます。スワップパーティションがディスク上に存在する場合、サイズ変更後に削除され、ディスクの最後に再作成されます。スワップパーティションについては、このドキュメントの「**Create** command」セクションで説明しています。

> (注
>
>)「ファイルシステムの拡大」プロセスでは、完了までに多少時間がかかる場合があり、プロセスの進行中にプロセスを中断しないように注意してください。パーティションのサイズを変更した後、ツールによって仮想マ

> シンが再起動されます。

```
(dpt): resize

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to resize (Y/N): y
```

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to resize existing partition.
Disabling swap on partition: /dev/da1p2
Deleting swap partition: da1p2
Resizing partition da1p1...
da1p1 resized

Adding a swap partition da1p2...
da1p2 added

Formatting the newly added portions of the partition. This may take some time (~10 seconds). Please be patient and don't
 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観察することができます。サイズを大きくした後の前後の詳細は次のとおりです。

```
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。これは、パーティションの既知の制限によるものです。2 テラバイトを超えるディスクが必要な場合は、新しいディスクを接続し、ディスクパーティションツールを使用してパーティションを作成します。remove コマンドを使用して既存のパーティションを削除し、パーティションを作成することもできます。

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

```
(dpt): ?remove
Removes existing partition from attached disk.

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

「remove」コマンドを実行すると、確認が要求され、確認されると、セカンダリディスクを使用するすべてのプロセス（ADM サブシステム、PostgreSQL プロセス、ADM モニターなど）が停止します。swap パーティションが存在し、そのパーティションで swap が有効になっている場合、swap は無効になります。

```
(dpt): remove

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

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

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to remove existing partitions.
Disabling swap on partition: /dev/da1p2
Removing all partitions from: da1
Remove Done.
Rebooting VM now...
```

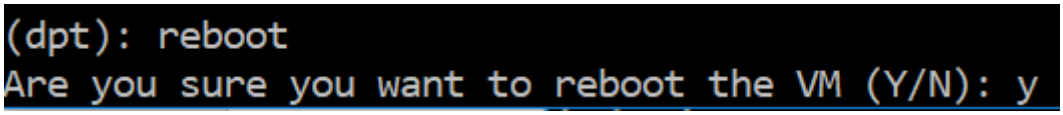
> 注
>
> パーティションを削除すると、仮想マシンが再起動されます。

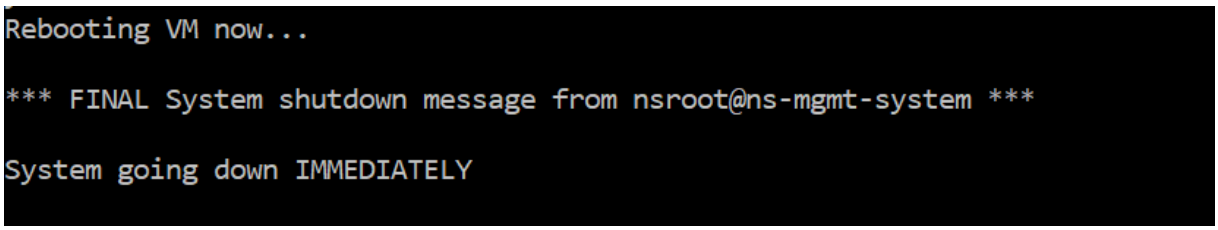
仮想マシンの再起動

パーティションの作成、サイズ変更、またはスワップファイルの作成時に、仮想マシンを再起動します。変更は再起動後にのみ有効になります。この目的のために、ツールに 再起動 コマンドが用意されています。

```
(dpt): ?reboot
Reboot the VM. Note: VM has to be rebooted after new partition is created, existing one is resized or swap file is creat
ed.
The VM is rebooted automatically after these operations. If the automatic reboot does not happen, then this command can
be used to reboot the VM.
```


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





ディスクデータのバックアップファイルを作成する

パーティションのサイズ変更または削除を行う前に、NetScaler ADM データをバックアップする手順を次に示します。

> 注:
>
> バックアップファイルを作成するにはディスク容量が必要です。Citrix では、バックアップコマンドを実行する前に、十分な空きディスク容量（50% 以上）があることを確認することをお勧めします。

1. ADM を停止します。

```
/mps/masd stop
<!--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. スターボールを作成します。

```
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応じて、操作に時間がかかります。

5. チェックサムを生成します。


```
md5 mps_backup.tgz > mps_backup_checksum
<!--NeedCopy-->
```

6. tarball とチェックサムをリモートコピーします。

```
scp
<!--NeedCopy-->
```

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。

```
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。各コマンドのヘルプを表示するには、**[help]** または **[?]** を押します。**** に続けてコマンド名を入力し ** 、Enter キーを押します。

```
(dpt): help

DPT Commands
------------
create  create_swapfile  exit  help  info  reboot  remove  resize

(dpt):
```

情報コマンド**:**

info コマンドは、接続されているセカンダリディスクが存在する場合、そのディスクに関する情報を提供します。このコマンドは、デバイス名、パーティション構成、人間が読める形式のサイズ、およびディスクブロック数を提供します。スキームは MBR または GPT です。MBR スキームとは、以前のバージョンの NetScaler ADM バージョンを使用してディスクがパーティション分割されたことを意味します。MBR/GPT ベースのパーティションはサイズ変更できますが、2 テラバイトを超えることはできません。GPT パーティションスキームとは、NetScaler ADM 12.1 以降を使用してディスクがパーティション分割されたことを意味します。

> 注:
>
> GPT パーティションは、作成時に 2 テラバイトを超える場合があります。ただし、小さいサイズのディスクを作成した後は、ディスクのサイズを 2 テラバイトを超えるサイズに変更することはできません。これは、プラットフォームの既知の制限です。

```
(dpt): ?info
Provides information about attached disk (if found).
(dpt): info
--------------
Disk: da1
Scheme: MBR
Size: (150G)
Blocks: 314572737
--------------
(dpt):
```

スワップファイル作成コマンド:

NetScaler ADM のプライマリディスクのデフォルトのスワップパーティションは 4 GB であるため、デフォルトのスワップ領域は 4 GB です。NetScaler ADM のデフォルトのメモリ構成（2 GB）では、このスワップ領域で十分です。ただし、より高いメモリ構成で NetScaler ADM を実行する場合は、ディスクにより多くのスワップ領域を割り当てる必要があります。

> 注:
>
> スワップパーティションは通常、オペレーティングシステムのインストール中にハードディスクドライブ (HDD) 上に作成される専用パーティションです。このようなパーティションは、スワップスペースとも呼ばれます。スワップパーティションは、追加のメインメモリをシミュレートする仮想メモリに使用されます。

以前のバージョンの NetScaler ADM で追加されたセカンダリディスクには、デフォルトでスワップパーティションが作成されません。「create_swapfile」コマンドは、スワップパーティションのない古い Citrix ADM バージョンを使用して作成されたセカンダリディスクを対象としています。このコマンドでは、次の項目がチェックされます。

- セカンダリディスクの存在
- マウント中のディスク
- ディスクのサイズ (500 GB 以上)
- スワップファイルの存在

「create_swapfile」コマンドは、メモリが 16 GB 以上の場合にのみ有効で、メモリが不足しているときには使用できません。したがって、このコマンドはスワップファイルの作成を続行する前にメモリをチェックします。


```
(dpt): ?create_swapfile
Creates a 32GB swap file on the secondary disk. Pre-conditions are:
1. Secondary disk exists
2. Secondary disk is partitioned and mounted
3. Capacity of disk >= 500GB
4. Swap file is not already found
5. RAM size >= 16GB

Creating swapfile is a time consuming operation and can take ~5 minutes to complete. Once started the operation should 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

ここでは、セカンダリディスクなしで高可用性セットアップで NetScaler ADM サーバーのペアを構成したシナリオを考えてみましょう。また、Citrix ADC インスタンスを 2 つ以上追加し、すべてのプロセスが実行されていることを確認したとします。この設定では、セカンダリディスクを仮想マシンに追加できます。高可用性セットアップでは、次のタスクで説明するように、両方のノードにディスクを追加する必要があります。

1. NetScaler ADM ノード名は「adm_primary」および「adm_secondary」であると仮定します。
2. まず、ADM_Secondary でパーティションツールを実行してから、セカンダリディスクを追加します。ディスクが追加されると、仮想マシンが再起動します。
3. 再起動後、ADM_SECONDARY をシャットダウンします。

4. 次に、ADM_Primary でパーティションツールを実行し、セカンダリディスクを追加します。ディスクが追加されると、仮想マシンが再起動します。

   両方のノードに、同じ容量のディスクを追加してください。たとえば、500 GB の容量のディスクをプライマリノードに追加する場合、500 GB の容量のディスクをセカンダリノードにも追加します。

5. ADM_Primary が再起動したら、そのノードがプライマリノードであることを確認します。
6. ここで、adm_secondary ノードを起動します。セカンダリノードとして起動し、データベースが同期されていることを確認します。
7. すべてのデータがまだ存在することを確認します。

次の手順を実行して、両方のノードの **RAM** の容量を増やします。

1. ADM_Secondary をシャットダウンし、必要に応じて RAM サイズを増やします。ノードを再起動しないでください。
2. ADM_Primary をシャットダウンし、必要に応じて RAM サイズを増やします。

   両方のノードで RAM サイズを均等に増やしてください。たとえば、プライマリノードの RAM サイズを 16 GB に増やす場合は、セカンダリノードでも同じようにします。

3. ADM_Primary を再起動します。
4. ADM_Primary が再起動したら、そのノードがプライマリノードであることを確認します。
5. ここで、adm_secondary ノードを起動します。再起動後、セカンダリとして起動し、DB 同期が機能していることを確認します。
6. ここで、すべてのデータがまだ存在していることを確認します。

> （注）
>
> セカンダリディスクを追加すると、プライマリノードが起動するまでに多少時間がかかります。また、セカンダリディスクを両方のノードに追加して RAM 容量を増やすプロセス全体で、しばらくの間、両方のノードがダウンする必要があります。このメンテナンス作業を計画する際には、このダウンタイムを考慮してください。

構成

February 6, 2024

NetScaler ADM サーバーにアクセスするには、グラフィカルユーザーインターフェイス（GUI）を使用します。GUI にアクセスして、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と監視、分析の表示、Citrix ADM サーバーの設定を行う必要があります。

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。

Web ブラウザー	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:

1. Web ブラウザで、Citrix ADM IP アドレス（例: http://192.168.100.1）を入力します。これは、サーバーをインストールするときに指定した IP アドレスと同じです。
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。デフォルトの管理者資格情報は、nsroot/nsroot です。

   NetScaler ADM にログオンした後、次の手順を実行して作業を開始する必要があります。

   - NetScaler ADM にインスタンスを追加します。これらのインスタンスを管理および監視する場合は、Citrix ADM サーバーにインスタンスを追加する必要があります。
   - 仮想サーバーで分析を有効にします。アプリケーショントラフィックフローの分析データを表示するには、特定のアプリケーションのトラフィックを受け取る仮想サーバーの分析機能を有効化する必要があります。
   - NetScaler ADM で NTP サーバーを構成します。Citrix ADM でネットワークタイムプロトコル（NTP）サーバーを構成して、その時計を NTP サーバーと同期する必要があります。
   - NetScaler ADM のパフォーマンスを最適化するためのシステム設定を構成します。Citrix ADM を使用してインスタンスとアプリケーションの管理と監視を開始する前に、Citrix ADM サーバーのパフォーマンスを最適化するためのいくつかのシステム設定を構成することをお勧めします。

Citrix ADM へのインスタンスの追加

February 6, 2024

インスタンスは、NetScaler ADM から検出、管理、監視する Citrix アプライアンスまたは仮想アプライアンスです。これらのインスタンスを管理および監視するには、NetScaler ADM サーバーにインスタンスを追加する必要があります。以下の Citrix アプライアンスと仮想アプライアンスを NetScaler ADM に追加できます。

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

インスタンスは、NetScaler ADM サーバーの初回セットアップ時に追加することも、後で追加することもできます。次に、NetScaler ADM がインスタンスにアクセスするために使用できるインスタンスプロファイルを指定する必要があります。

> 注
>
> - NetScaler ADM は、通信に NetScaler ADC インスタンスの NetScaler IP（NSIP）アドレスを使用します。NetScaler ADC インスタンスと NetScaler ADM の間で開く必要のあるポートについては、「ポート」を参照してください。
> - Citrix SD-WAN WO および Citrix SD-WAN EE インスタンスの場合、NetScaler ADM はインスタンスの管理 IP アドレスを使用して通信します。
> - NetScaler ADM がインスタンスを検出する方法については、「インスタンスの検出」を参照してください。

Citrix ADC プロファイルを作成する方法

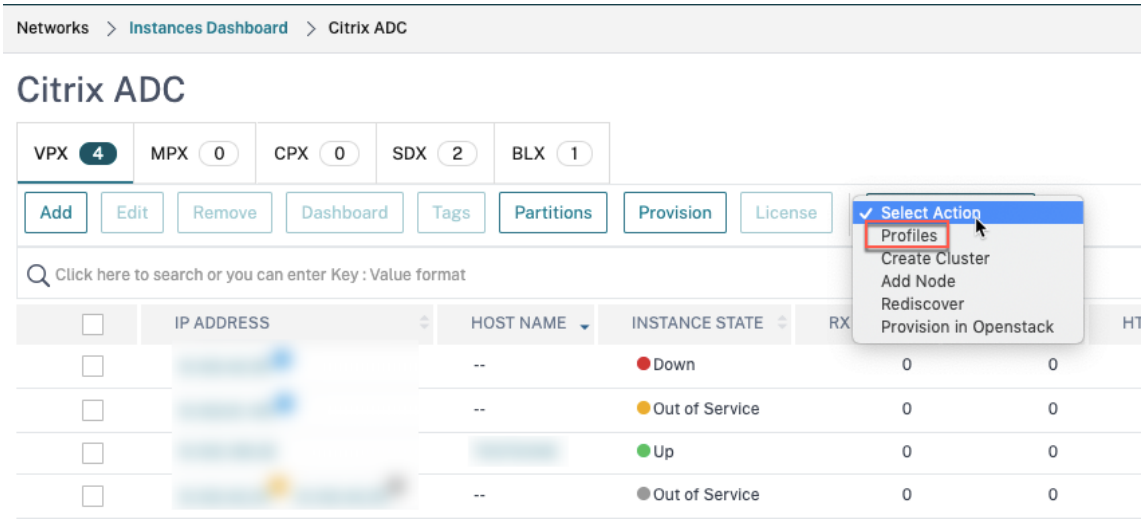
NetScaler ADC プロファイルには、NetScaler ADM に追加するインスタンスのユーザー名、パスワード、通信ポート、認証タイプが含まれます。インスタンスの種類ごとにデフォルトのプロファイルが用意されています。たとえば、nsroot は Citrix ADC インスタンスのデフォルトプロファイルです。デフォルトのプロファイルは、デフォルトの NetScaler ADC 管理者の資格情報を使用して定義されます。インスタンスのデフォルトの管理者資格情報を変更した場合は、それらのインスタンスのカスタムのインスタンスプロファイルを定義できます。インスタンスが検出された後にインスタンスの資格情報を変更した場合は、インスタンスプロファイルを編集、またはプロファイルを作成してからインスタンスを再検出する必要があります。

NetScaler ADC プロファイルは、［インスタンス］ページから、またはインスタンスの追加または変更時に作成できます。

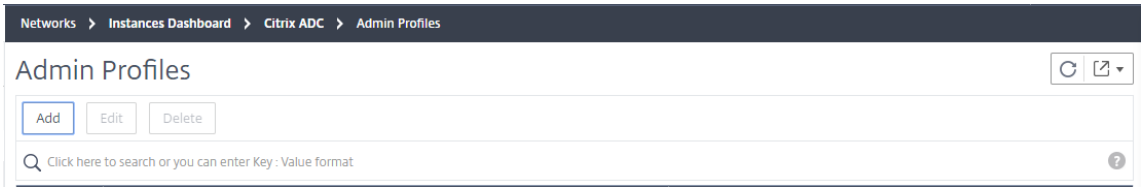
［インスタンス］ページから **NetScaler ADC** プロファイルを作成するには：

1. ［ネットワーク**] > [**インスタンス**]** に移動します。
2. インスタンスを選択します。たとえば、NetScaler ADC などです。

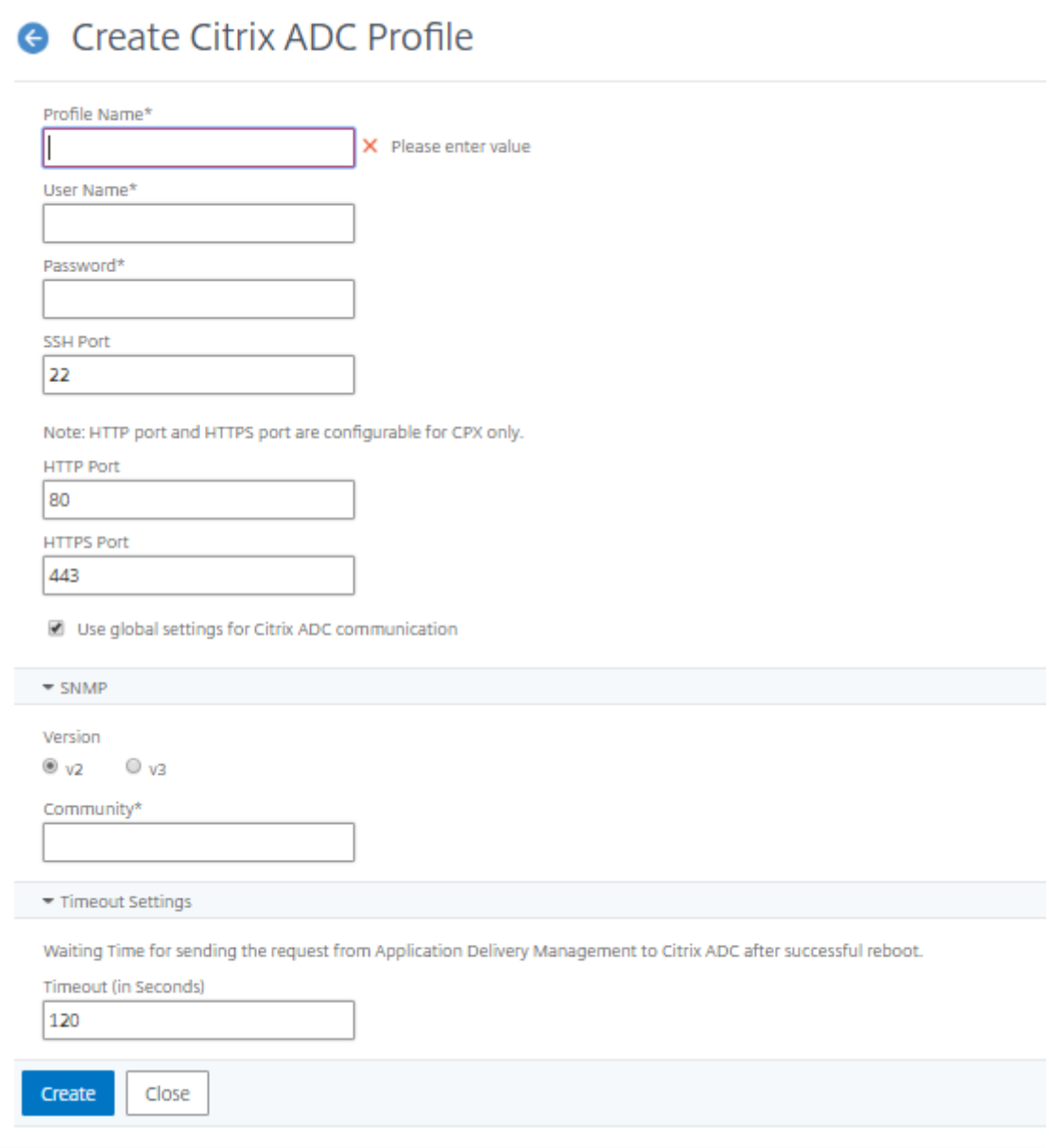
3. NetScaler ADC ページで、［プロファイル］を選択します。



4. [管理プロファイル] ページで、[追加] を選択します。



5. **NetScaler ADC** プロファイルの作成ページで、次の操作を行います。



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

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

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

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

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

> 注:
>
> デフォルトの HTTP ポートは 80 です。NetScaler ADC CPX インスタンスで構成したデフォルト以外またはカスタマイズされた HTTP ポートを指定することもできます。カスタマイズされた HTTP ポートは、NetScaler ADM と NetScaler ADC CPX 間の通信にのみ使用できます。

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

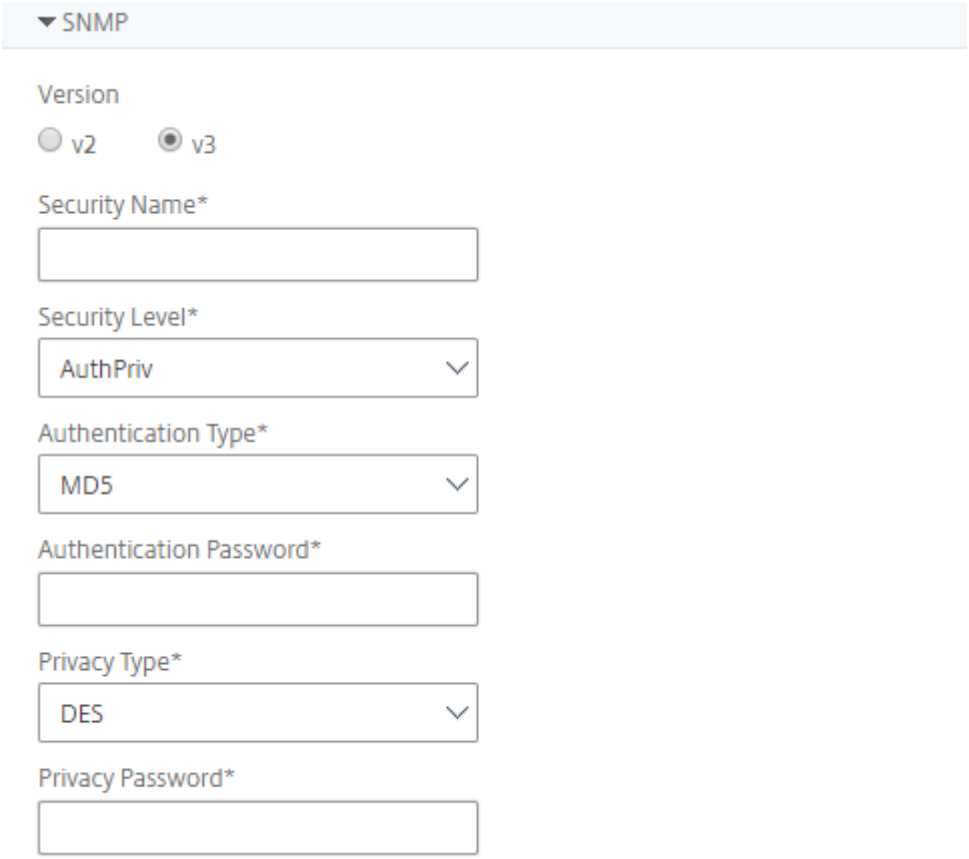
> 注:
>
> デフォルトの HTTPS ポートは 443 です。NetScaler ADC CPX インスタンスで構成したデフォルト以外またはカスタマイズされた HTTPS ポートを指定することもできます。カスタマイズされた HTTPS ポートは、NetScaler ADM と NetScaler ADC CPX の間の通信にのみ使用できます。

g) **Citrix ADC** 通信にグローバル設定を使用する:**Citrix ADM** と **Citrix 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、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 ADC SDX では、**SNMPv2** のみがサポートされています。

i) タイムアウト設定：再起動後、NetScaler ADM が NetScaler ADC インスタンスに接続要求を送信する前に待機する必要がある時間を指定します。

j)［作成］を選択します。

ADC インスタンスを **NetScaler ADM** に追加する

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

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

SD-WAN インスタンスの場合、各インスタンスの IP アドレス、または IP アドレスの範囲を指定する必要があります。NetScaler ADM は、Citrix SD-WAN WO エディションと Citrix SD-WAN PE エディションのみをサポートすることに注意してください。

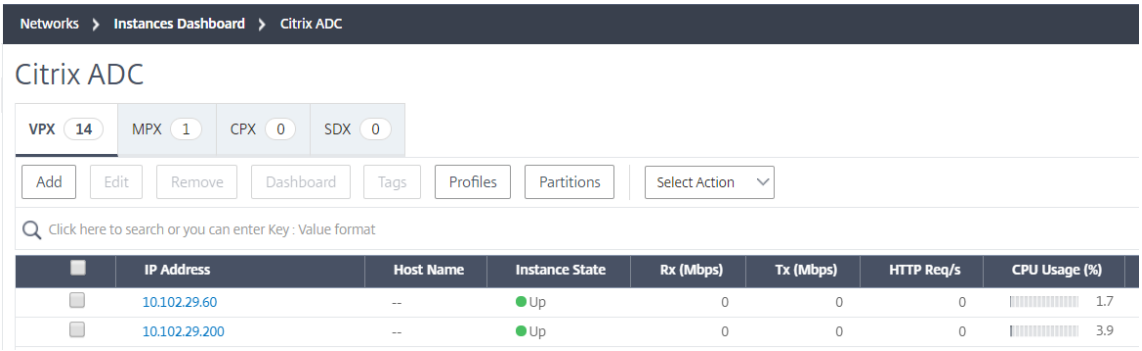
> 注
>
> - クラスターで構成された NetScaler ADC インスタンスを追加するには、クラスターの IP アドレスまたはクラスター設定の個々のノードのいずれかを指定する必要があります。ただし、NetScaler ADM では、クラスターはクラスター IP アドレスだけで表されます。
> - 高可用性ペアとして設定された NetScaler ADC インスタンスの場合、一方のインスタンスを追加すると、そのペアのもう一方のインスタンスが自動的に追加されます。

2 つの Citrix ADM サーバーが高可用性モードでセットアップされている場合、インスタンスが追加されると、トラフィックソースは ADM フローティング IP アドレスを経由します。

オンプレミスエージェントを使用して設定されたリモートデータからインスタンスを追加すると、トラフィックソースは ADM エージェントを経由します。

NetScaler ADM にインスタンスを追加するには:

1. 管理者の資格情報を使用して NetScaler ADM にログオンします。
2. [ネットワーク] > [インスタンス] > [**NetScaler ADC**] に移動します。追加するインスタンスのタイプ（NetScaler ADC VPX など）を選択し、［追加］をクリックします。



3. 次のいずれかのオプションを選択します:
   - デバイス **IP** アドレスの入力-NetScaler ADC インスタンスの場合は、各インスタンスのホスト名または IP アドレス、または IP アドレスの範囲を指定します。SD-WAN インスタンスの場合、各インスタンスの IP アドレス、または IP アドレスの範囲を指定する必要があります。
   - **Import from file** - ローカルシステムから、追加するすべてのインスタンスの IP アドレスを含むテキストファイルをアップロードします。
4. 「プロファイル名」から、適切なインスタンスプロファイルを選択するか、「+」アイコンをクリックして新しいプロファイルを作成します。
5. サイトから、インスタンスを追加する場所を選択するか、**+** アイコンをクリックして新しい場所を作成します。
6. 「**OK**」をクリックして、NetScaler ADM にインスタンスを追加するプロセスを開始します。

> 注
>
> インスタンスを再検出する場合は、[ネットワーク] > [インスタンス] > [**NetScaler ADC**] に移動します。再検出するインスタンスを選択し、「アクションの選択」リストから「再検出」をクリックします。

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

NetScaler ADM は、CPX 機能の改善をサポートするように拡張されました。NetScaler ADC CPX インスタンスは、CPX の IP アドレスをデバイスプロファイルとともに提供することにより、NetScaler ADM に追加されるようになりました。CPX インスタンスの追加プロセスは、ADM で VPX や MPX などの他の ADC タイプを追加する方法と似ています。また、ADM における CPX の登録が強化されました。CPX が起動すると、NetScaler ADM は自動的に CPX インスタンスを検出して登録します。CPX インスタンスは、Docker ホストを介して検出されなくなりました。

1. [ネットワーク] > [インスタンス] > [**NetScaler ADC**] に移動し、[**CPX**] タブをクリックします。
2. ［追加］をクリックします。
3. ［**NetScaler ADC CPX** の追加］ページが開きます。次のパラメーターの値を入力します：

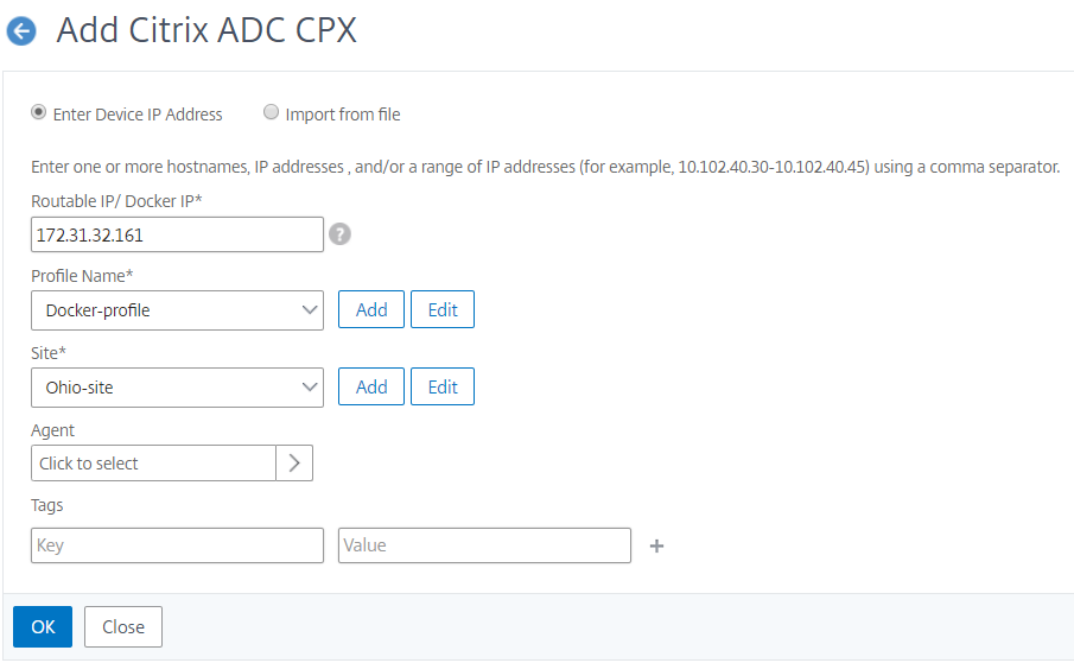
    a) CPX インスタンスの到達可能な IP アドレス、または CPX インスタンスがホストされている Docker コンテナの IP アドレスのいずれかを指定することにより、CPX インスタンスを追加できます。

    b) CPX インスタンスのプロファイルを選択します。

    c) インスタンスを展開するサイトを選択します。

    d) エージェントを選択します。

    e) オプションとして、キーと値のペアをインスタンスに入力できます。キーと値のペアを追加すると、後でインスタンスを簡単に検索できます。



> 注
>
> NetScaler ADC CPX インスタンスの場合、CPX インスタンスプロファイルを作成するときに、ホストの **HTTP**、**HTTPS**、**SSH**、および **SNMP** ポートの詳細を指定する必要があります。ホストが公開したポートの範囲を [開始ポート] と [** ポート数 **] フィールドで指定することもできます。

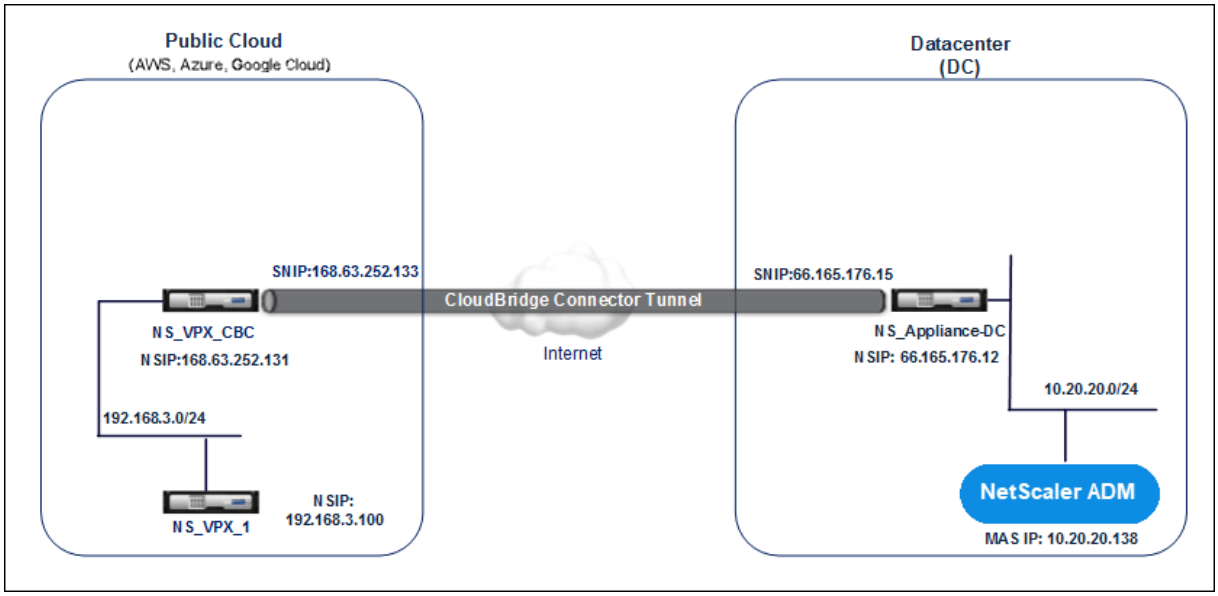
4. [**OK**] をクリックします。

クラウドにデプロイされた **NetScaler ADC VPX** インスタンスを **NetScaler ADM** に追加する

February 6, 2024

Citrix ADM を使用して、Amazon Web Services（AWS）や Microsoft Azure などのパブリッククラウドにデプロイされた Citrix ADC VPX インスタンスを管理および監視できます。パブリッククラウドに展開されている NetScaler ADM と NetScaler ADC VPX インスタンスの間にレイヤー 3 接続を確立する必要があります。レイヤー 3 接続を確立するには、NetScaler CloudBridge Connector、Citrix SD-WAN、AWS へのダイレクトコネクト、Azure の VPN などのソリューション、または Equinix などのサードパーティコネクタを使用できます。

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

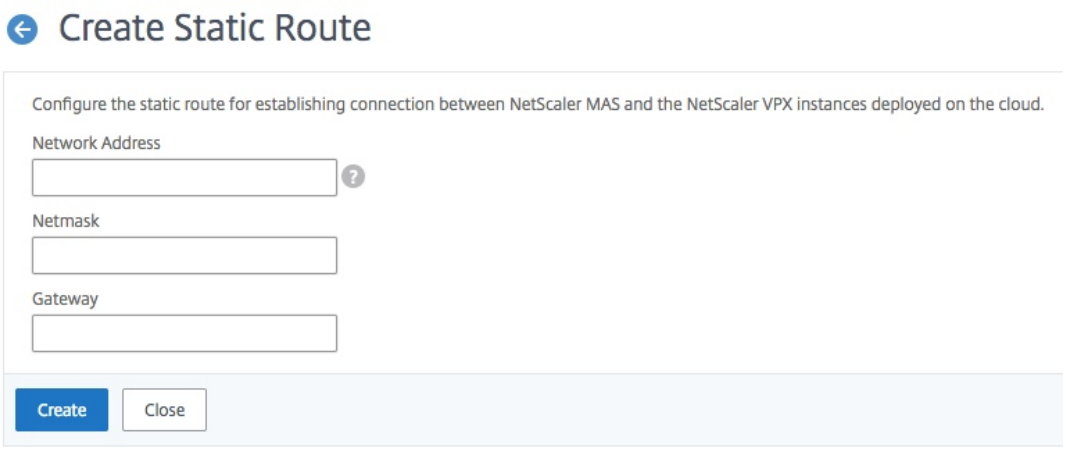


CloudBridge Connector トンネルは、データセンター DC の Citrix ADC アプライアンス NS_Appliance-DC とパブリッククラウドの Citrix ADC 仮想アプライアンス（VPX）NS_VPX_CBC との間にセットアップされます。NS_Appliance-DC および NS_VPX_CBC を使用すると、NetScaler ADM とパブリッククラウドにデプロイされた NetScaler ADC VPX インスタンス NS_VPX_1 との間の通信が可能になります。通信が確立されると、NetScaler ADM で NS_VPX_1 を検出できるようになります。

このトポロジを設定するには:

1. パブリッククラウドで NetScaler ADC VPX インスタンスをインストール、構成、および起動します。
   - 手順については 、「AWS への Citrix ADC VPX のインストール」を参照してください。
   - 手順については、「Microsoft Azure への Citrix ADC VPX のインストール」を参照してください。
2. NetScaler ADC 物理アプライアンスを展開して構成するか、データセンターの仮想化プラットフォームで 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 への Citrix ADC 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、「VMwareESXi 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、「MicrosoftHyper-V への Citrix ADC 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。
3. データセンターとパブリッククラウド間で CloudBridge Connector を構成します。手順については、「CloudBridge Connector の設定」を参照してください。
4. Citrix ADM とクラウドにデプロイされた Citrix 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、Citrix ADM からコネクタを介して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 ADC VPX クラウドインスタンスを Citrix ADNetScaler ADM に追加します。詳細な手順については、「NetScaler ADM にインスタンスを追加する」を参照してください。

仮想サーバーでの分析の有効化

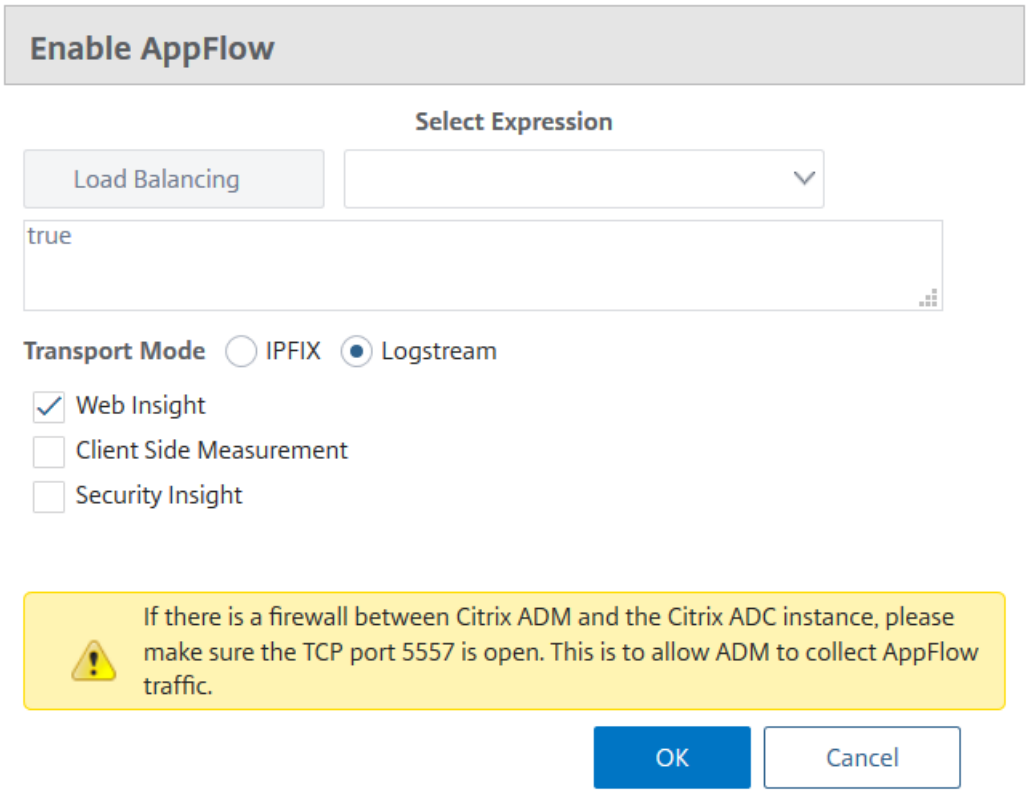
February 6, 2024

選択したインスタンス上の特定の仮想サーバー（アプリケーションサーバー）に対して分析を有効化し、このアプリケーションサーバーのトラフィックを監視できます。分析では、仮想サーバーに関する統計情報が提供されます。

> 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。Citrix ADC インスタンスで AppFlow パラメータを設定してください。AppFlow パラメータの設定が完了すると、Citrix ADM は Web インサイトトラフィックとともにセキュリティインサイトトラフィックの受信を開始します。NetScaler ADC インスタンスで AppFlow パラメーターを設定する方法について詳しくは、「構成ユーティリティを使用して AppFlow パラメーターを設定するには」を参照してください。

Citrix ADM の各インスタンスでアナリティクスを有効にするには:

1. [ネットワーク] > **[**インスタンス] に移動し、分析を有効にする Citrix ADC インスタンスを選択します。たとえば、NetScaler ADC などです。
2. インスタンスのリストから、インスタンスを選択します。
3. 「アクション の選択」リストから、「アナリティクスの設定」を選択 します。
4. 「アプリケーションリスト」で、仮想サーバーを選択し、「**AppFlow** を有効にする」をクリック します。
5. 「**AppFlow** を有効に する」フィールドに「 **true**」と入力し、有効にする分析に基づいて、「セキュリティインサイト」または「**Web** インサイト」、あるいはその両方を選択 します。

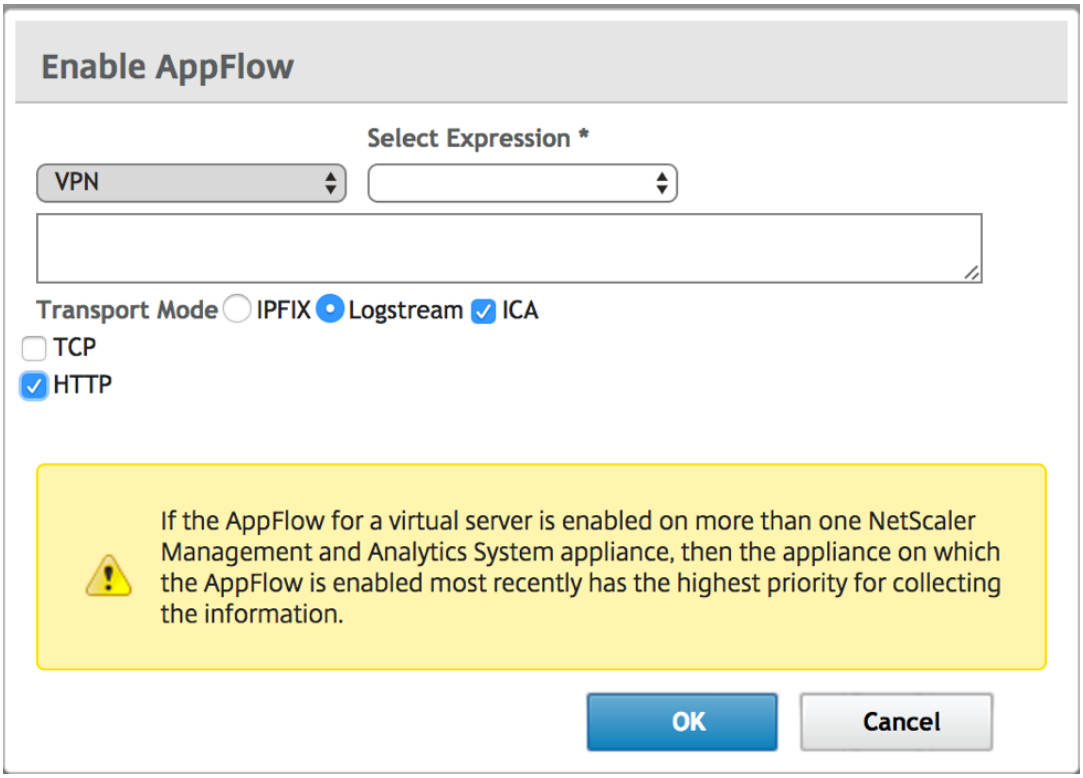


> 注
>
> Citrix ADM では、ログストリームに Citrix ADC SNIP を使用し、IPFIX には NSIP を使用します。NetScaler ADM と NetScaler ADC インスタンスの間でファイアウォールが有効になっている場合は、次のポートを開いて NetScaler ADM が AppFlow トラフィックを収集できるようにします。

転送モード	接続元 IP	種類	ポート
IPFIX	NSIP	UDP	4739
Logstream	SNIP	TCP	5557

- **HDX Insight** と Gateway**Insight** では、「**AppFlow** を有効にする」をクリックしながら、Citrix ADC インスタンスで構成されている **VPN** 仮想サーバーを選択し、それに応じて **ICA** または **HTTP** の

チェックボックスを選択する必要があります。



- **TCP Insight** の場合は、[システム] > [分析設定] > [機能の設定] に移動し、[**TCP Insight** を有効にする] を選択します。
- ビデオインサイトでは、Citrix ADC アプライアンスで構成を変更する必要があります。ビデオインサイトの分析を有効にする方法について詳しくは、Video Insightを参照してください。
- **WAN** インサイトについては、

  a) [インフラストラクチャ] > [インスタンス] > [**NetScaler SD-WAN WO**] に移動し、データセンター WAN 最適化アプライアンスを選択します。

  b) [アクション] ドロップダウンから、[インサイトを有効にする] を選択します。

  c) 必要に応じて以下のパラメーターを選択します。

  - HDX Insight の地情報データ収集: クライアントの IP アドレスを Google Geo API と共有します。
  - AppFlow: WAN 最適化インスタンスからのデータの収集を開始します。
    * TCP と WANOpt: TCP と WanOpt のインサイトレポートを提供します。
    * HDX: HDX Insight レポートを提供します。
    * HDX 用の TCP のみ:HDXInsight レポートにのみ TCP を提供します。

Citrix ADM で検出された Citrix ADC インスタンスで **AppFlow** を有効にしているときに、**AppFlow** トランスポートモードを IPFIX またはログストリームに選択できます。IPFIX とログストリームの詳細については、「ログストリームの概要」を参照してください。

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

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

Citrix ADM の「Web Insight を有効にする」オプションを使用して、Web Insight トラフィックの処理を有効または無効にすることもできます。Web Insight トラフィックを監視しない場合は、このオプションを無効にすることができます。詳しくは、「Citrix ADM による Web Insight トラフィックの処理」を参照してください。

NTP サーバーの構成

February 6, 2024

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

Citrix ADM で NTP サーバーを構成するには:

1. ［**System**］>［**NTP Servers**］の順に選択して、［**Add**］をクリックします。
2. ［**Create NTP Server**］ページで、次の詳細情報を入力します。

- **Server Name/IP Address** –NTP サーバーのドメイン名と IP アドレスを入力します。ここで入力したドメイン名と IP アドレスは、NTP サーバーを追加した後は変更できません。
- **Minimum Poll Interval** –NTP メッセージの送信間隔の最小値を秒数（2 のべき乗）で指定します。たとえば、最小ポーリング間隔を 64 秒にする場合、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 Synchronization**］をクリックして［**Enable NTP Synchronization**］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。

システムアラームの設定

システムのアラームを構成して、システム上の重大な問題や重要な問題を確実に把握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）のしきい値を超えるか、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。

システムアラームを設定するには、次の手順を実行します。

1. [システム**] > [**アラーム] に移動し、設定するアラームを選択して [編集] をクリックします。
2. [**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。
3. しきい値を超えたアラーム、またはイベントが発生したアラームを表示するには、[システム**] > [**監査] に移動し、[**Syslog** メッセージ] をクリックします。

システム通知の設定

多くのシステム関連機能に関して、選択したグループのユーザー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。

システム通知を構成するには、次の手順に従います。

1. ［**System**］**>** ［**Notifications**］の順に選択します。[設定] で、[通知設定の変更] 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

Citrix 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、Citrix ADM がネットワークレポートデータ、イベント、監査ログ、およびタスクログを保持する間隔を指定できます。デフォルトでは、これらのデータは 24 時間ごとに（00:00 の時刻に）削除されます。

システムプルーニング設定を構成するには:

1. ［**System**］**>** ［**System Administration**］の順に選択します。「プルーニング設定」で、「システムプルーニング設定」をクリックします。
2. [システム削除設定の構成**]** ページで、データを保持する日数を指定し、[**OK**] をクリックします。

システムバックアップの設定を構成する

Citrix 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. [**System**] > [**System Administration**] の順に選択します。
2. [バックアップ設定] で、[システムバックアップ設定] をクリックします。
3. [システムバックアップ設定の構成] ページで、必要な値を指定します。

インスタンスのバックアップ設定の構成

Citrix ADC インスタンスの現在の状態をバックアップすると、インスタンスが不安定になった場合にバックアップファイルを使用して安定性を回復できます。アップグレードを実行する前にこれを行うことは特に重要です。デフォルトでは、12 時間ごとにバックアップされて、3 つのバックアップファイルがシステムに保持されます。

インスタンスのバックアップ設定を構成するには:

1. [**System**] > [**System Administration**] の順に選択します。
2. 「バックアップ設定」で、「インスタンスバックアップ設定」を選択し、必要な値を指定します。

インスタンスイベントプルーニング設定の構成

Citrix ADM サーバーのデータベースに保存されるイベントメッセージデータの量を制限するには、Citrix 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. [**System**] > [**System Administration**] の順に選択します。
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. Citrix ADM サーバーにデータを保持する時間間隔を日単位で入力し、「**OK**」をクリックします。

インスタンスの **Syslog** 消去設定を設定する

データベースに保存される Syslog データの量を制限するために、Syslog データをパージする間隔を指定できます。汎用 syslog データが Citrix ADM から削除されるまでの日数を指定できます。

インスタンスの **Syslog** 消去設定を構成するには:

1. [**System**] > [**System Administrations**] の順に選択します。「プルーニング設定」で、「インスタンスの **Syslog** 消去設定」をクリックします。

2. インスタンス Syslog 消去設定の構成ページの「Syslog 汎用データの保持」フィールドに、1〜180 日までの日数を指定します。
3. [**OK**] 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しておくことも重要です。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 12.1 ビルドにアップグレードします。アップグレード操作が開始されると、NetScaler ADM が再起動し、アップグレードが正常に完了すると、既存の接続が終了して再接続されます。既存の構成は保持されますが、アップグレードが正常に完了するまで NetScaler ADM はデータを処理しません。

> 重要
>
> NetScaler ADM のバージョンとビルドは、NetScaler ADC のバージョンおよびビルドと同じかそれ以上である必要があります。たとえば、NetScaler ADM 12.1 ビルド 50.39 をインストールしている場合は、NetScaler ADC 12.1 ビルド 50.28/50.31 以前がインストールされていることを確認します。

12.1 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 56.x より前のバージョン 12.0 ビルドから NetScaler ADM 12.1 ビルド 48.18 バージョンにアップグレードする場合は、次の手順を実行してください。
  - 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。
  - 次に、バージョン 12.1 の最新ビルドにアップグレードします。

    12.1 リリースに正常にアップグレードするには特定のクリーンアップ手順が必要なため、この 2 段階のプロセスに従う必要があります。これらのプロシージャは、12.0 ビルド 56.x 以降でのみ使用できます。

- 12.1 では、高可用性展開でプライマリノードにフローティング IP アドレスを構成できるため、NetScaler ADC ロードバランサーを別途用意する必要がなくなります。この改善により、高可用性展開は同じサブネット上に存在する必要があります。現在のデプロイが別のサブネット上にある場合は、この記事を確認してアップグレードプロセスについて学ぶ必要があります。
- 12.1 では、高度なバックアップのサポートが削除されました。NetScaler ADM 12.1 にアップグレードすると、高度なバックアップ機能は利用できなくなります。詳細については、この記事をご覧ください。

> 注
>
> NetScaler ADM を 12.1 ビルドから以前のリリースのビルドにダウングレードすることはできません。

推奨される注意事項:

- アップグレードする前に、NetScaler ADM サーバーをバックアップしてください。
- アップグレード後、NetScaler ADM サーバーと管理対象インスタンス間の接続の再確立が必要になる場合があります。「続行すると接続に失敗する可能性がある」という旨を警告する確認メッセージが表示されます。
- 高可用性セットアップの NetScaler ADM サーバーでは、アップグレード時にどちらのノードでも構成を変更しないでください。

  > 警告
  >
  > アップグレード処理が正常に完了するまでブラウザーを更新しないでください。アップグレード処理が完了するまでに数分かかることがあります。

- アップグレード後、アクティブノードは高可用性ペアで変更できます。

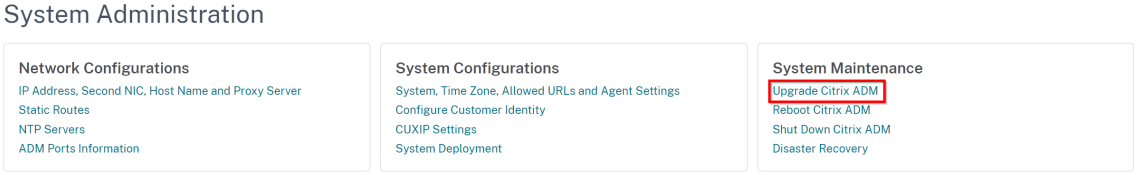
単一の **NetScaler ADM** サーバーのアップグレード

単一の **NetScaler ADM** サーバーをアップグレードするには:

1. ウェブブラウザに、NetScaler ADM サーバーの IP アドレスを入力します。

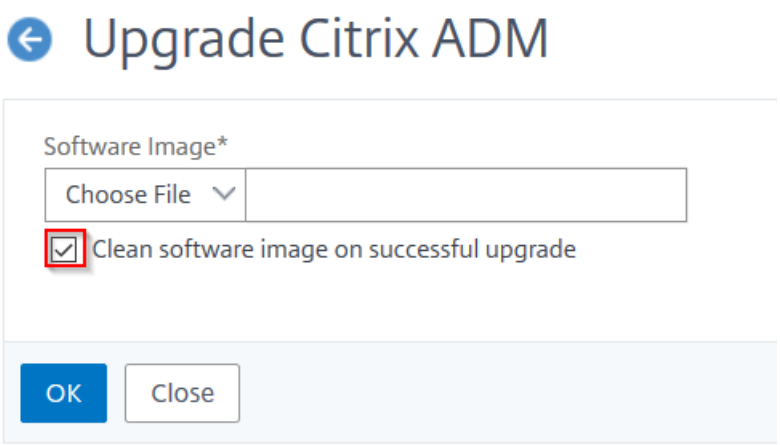
   > 注:
   >
   > 高可用性モードの NetScaler ADM サーバーの場合は、HA ペアの NetScaler ADM サーバーまたは負荷分散仮想サーバーのいずれかの IP アドレスを入力します。

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] > **[**システム **** 管理**]** に 移動します。システム管理の小見出しの下で、「NetScaler ADM のアップグレード **」をクリックします。

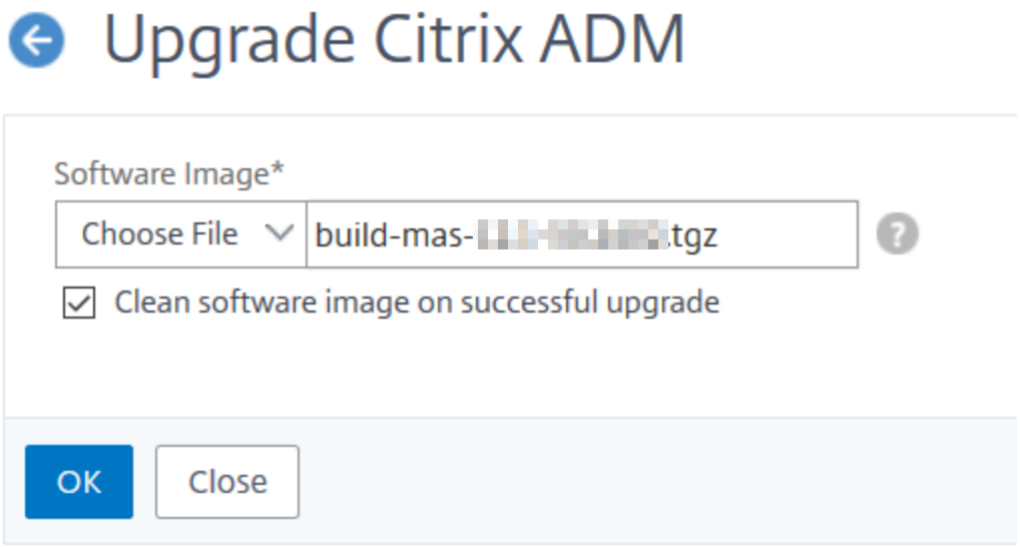


4. **NetScaler ADM** をアップグレードする］ページで、［アップグレードに成功したらソフトウェアイメージをクリーンアップ する］チェックボックスをオンにして、アップグレード後にイメージファイルを削除します。このオプションを選択すると、アップグレード時に NetScaler ADM イメージファイルが自動的に削除されます。

   > 注
   >
   > このオプションはデフォルトで選択されています。アップグレードプロセスを開始する前にこのチェックボックスをオンにしない場合は、イメージを手動で削除する必要があります。



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



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

6. ［**OK**］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。

高可用性ペアを以前のリリースから **12.1** にアップグレード

高可用性モードの NetScaler ADM サーバーでは、アクティブノードまたは負荷分散仮想サーバーの 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。

> 重要
>
> **NetScaler ADM** を高可用性モードでアップグレードする場合の注意点
>
> 高可用性モードの NetScaler ADM を以前のリリースから 12.1 にアップグレードすると、高可用性接続は、セカンダリノードで実行される「Join HA」スクリプトによって内部的に確立されます。アップグレードプロセスにかかる時間は、ネットワークインフラストラクチャ、データベースに存在するデータ、およびリンクの速度によって異なります。2 つのノード間の接続を再確立するには数時間かかる場合があります。この間、プライマリノードはセカンダリノードからハートビートを受信しません。アップグレードプロセスが完了するまで、プライマリ UI にハートビートがないことを示す通知が表示されます。アップグレードプロセスが終了すると、セカンダリノードが再起動し、高可用性デプロイが完了します。
>
> 注
>
> : アップグレードのステータスを確認するには、SSH を使用して各ノードにログオンし、次のコマンドを実行して出力を確認します。
>
> pgrep -lf installmas
>
> pgrep -lf maintenance
>
> pgrep -lf join_streaming_replication
>
> pgrep -lf pg_basebackup
>
> これらのコマンドのいずれかがノードで実行中のプロセスを示している場合、アップグレードは進行中であり、中断しないでください。この間、NetScaler ADM を再起動したり、セカンダリノードで強制フェイルオーバーを試みたりしないでください。
>
> アップグレードプロセスが完了すると、nsroot/nsroot またはユーザー認証情報でログオンできない場合があります。これは、NetScaler ADM サブシステムが完全に再起動していないか、移行がまだ進行中である可能性があるためです。NetScaler ADM を再起動したり、パスワードの回復を試みたりしないでください。これは望ましくない影響をもたらし、システムの動作が一貫していない可能性があります。必要に応じて、nsrecover/<your_password_for_the_nsroot_user> 認証情報を使用してログオンしてみることができます。
>
> アップグレード後、操作を開始する前に、プライマリノードとセカンダリノードの両方がアップグレードされ、再起動が完了していることを確認します。
>
> 注:
>
> CLI を使用して NetScaler ADM を高可用性モードでアップグレードすることはできません。

高可用性の **NetScaler ADM** サーバーでのプールライセンス:

NetScaler ADM サーバーを高可用性モードで展開すると、ライセンスファイルがプライマリノードに添付され、プライマリサーバーのホスト ID または MAC アドレスで構成（ノードロック）されます。プールライセンス機能は、12.1 ビルド以降の高可用性で NetScaler ADM でサポートされるようになりました。両方のノードでプールライセンス機能を設定するには、両方のノードに同一のライセンスファイルが必要です。セカンダリノードに同一のライセンスをインストールするには、セカンダリノードの HostID (MAC アドレス) にライセンスを再ホストする必要があります。

NetScaler ADM に高可用性モードの 2 つのサーバーノード S1 と S2 があるシナリオを考えてみましょう。元のライセンスファイル L1 は、サーバ S1 にインストールされます。これで、再ホストされたライセンスファイル L2 が S2 に割り当てられるはずです。

手順に従って、高可用性モードの NetScaler ADM を 12.0 から 12.1 にアップグレードし、プールライセンス機能を設定します。

1. 高可用性モードで NetScaler ADM サーバーのプライマリノードにログオンし、アップグレードプロセスを実行します。
2. 再ホストされたライセンスファイル L2 をセカンダリサーバノード S2 にインストールします。

   この時:

   - S2 がプライマリノードの場合、そのインスタンスの GUI にアクセスして L2 ライセンスをインストールできます。
   - S2 がセカンダリノードの場合は、S2 がプライマリノードになるように、手動でフェイルオーバーを実行する必要があります。GUI を使用して、ライセンス L2 を新しいプライマリノードにインストールします。
     これは、GUI からアクセスできるのは可用性の高いプライマリサーバだけだからです。
3. 新しいプライマリノードにフローティング IP アドレスを設定します。
4. NetScaler ADC インスタンスのライセンスサーバー IP アドレスを削除し、フローティング IP アドレスを使用するように再構成します。これをすべての NetScaler ADC インスタンスで実行します。

NetScaler ADC インスタンスにメンテナンスウィンドウを作成して、NetScaler ADM 高可用性プールライセンスのアップグレードを実行することをお勧めします。これは、ライセンスサーバーを削除してフローティング IP アドレスを追加すると、NetScaler ADC インスタンスが一時的に最小帯域幅サポートに戻るためです。

高可用性アップグレードシナリオ

NetScaler ADM サーバーを高可用性モードで展開するシナリオは 2 つあります。

- プライマリサーバーとセカンダリサーバーは同じサブネットにデプロイされます。
- プライマリサーバーとセカンダリサーバーは異なるサブネットに配置されます。

このアップグレードドキュメントは、これらの両方のシナリオで NetScaler ADM をアップグレードするのに役立ちます。

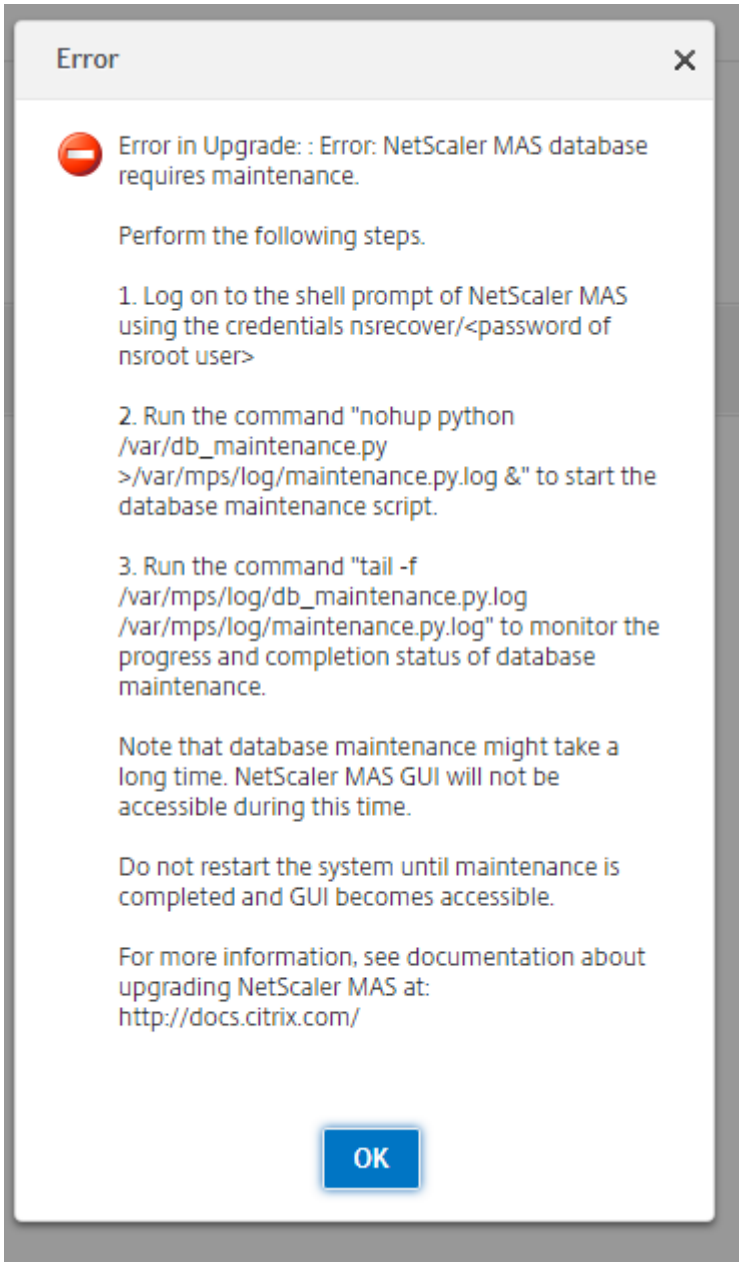
- 同じサブネットでの高可用性セットアップのアップグレード
- 異なるサブネットの高可用性セットアップのアップグレード

同じサブネットの高可用性セットアップをアップグレード

同じサブネット上に高可用性モードで展開された NetScaler ADM サーバーのアップグレードは、NetScaler ADM 12.1 によって自動的に処理されます。

同じサブネットで高可用性モードで展開されている **NetScaler ADM** をアップグレードするには:

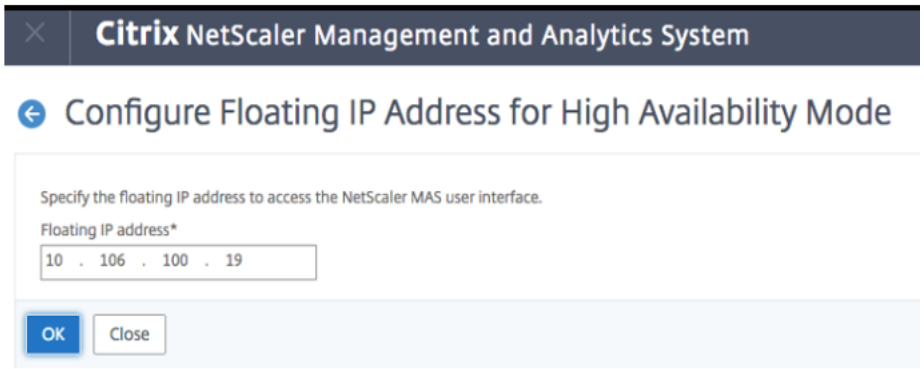
1. プライマリノードにログインし、[システム] > [システム管理**]** に移動します。
2. [システム管理] で、[**NetScaler ADM** のアップグレード] をクリックします。
3. アップグレード中にエラーが発生すると、次のエラーメッセージが表示されます。プライマリサーバ上のメッセージに記載されている指示に従います。



4. アップグレードプロセスの一環として、CLI を使用してクリーンアップ手順を実行する必要があります。クリーンアップ処理中、2 次ノードが主ノードになります。古いプライマリノードには GUI からアクセスできません。クリーンアッププロセスの進行中は、古いプライマリノードと新しいプライマリノードを再起動しないでください。クリーンアッププロセスが完了したら、新しいプライマリノードからアップグレード手順を続行します。
5. アップグレードプロセスが完了したら、2 つのノードはデータベースを同期する必要があります。同期が完了して新しいセカンダリノードが起動するまでにかかる時間は、データベースに存在するデータによって異なります。

> 注
>
> アップグレードが成功したら、NetScaler ADM ユーザーインターフェイスを使用してフローティング IP アドレスを構成する必要があります。

6. フローティング IP アドレスを設定するには、[システム] **>** [デプロイ] **>** [高可用性モードのフローティング **IP** アドレスの設定] に移動します。
7. 次の図に示すようにフローティング IP アドレスを指定し、「**OK**」をクリックします。



異なるサブネットの高可用性セットアップをアップグレード

異なるサブネットに高可用性モードで展開された NetScaler ADM サーバーのアップグレードは、管理者が処理する必要があります。

このシナリオでは、NetScaler ADM HA ノード 1（プライマリ）はサブネット 1 にあり、NetScaler ADM HA ノード 2（セカンダリ）はサブネット 2 にあります。

異なるサブネットで高可用性モードで展開された **NetScaler ADM** をアップグレードするには:

1. 高可用性設定を手動で解除します。詳細については、「高可用性の無効化」を参照してください。
2. NetScaler ADM スタンドアロンノード 1 をアップグレードします。NetScaler ADM のアップグレード方法の詳細については、「単一の NetScaler ADM サーバーのアップグレード」を参照してください。
3. サブネット 1 に新しい NetScaler ADM スタンドアロンノード 3 をセットアップして登録します。
4. ノード 1 とノード 3 を登録したら、これらのノードの両方を高可用性モードでデプロイします。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。

   > 注:
   >
   > フローティング IP アドレスの設定は必須です。

5. NetScaler ADM ノード 2 を削除します。

高可用性ペアを以前の **12.1** バージョンから最新バージョンにアップグレードする

高可用性で展開された NetScaler ADM サーバーは、以前の 12.1 ビルドから新しい 12.1 ビルドにアップグレードできます。

高可用性モードで展開された NetScaler ADM をアップグレードするには:

1. NetScaler ADM 12.1 ビルド 49.37 イメージファイルを Citrix.com のダウンロードページからダウンロードします。
2. プライマリノードにログインし、[システム] > [システム管理] に移動します。
3. [システム管理] で、[**NetScaler ADM** のアップグレード] をクリックします。
4. 画像が保存されているフォルダーに移動します。

   アップグレード中は、どちらのノードに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。アップグレード処理が完了するまでに数分かかることがあります。

   アップグレード後、アクティブノードは高可用性ペアで変更できます。

NetScaler ADM ディザスタリカバリ展開のアップグレード

NetScaler ADM ディザスタリカバリ展開のアップグレードは、次の 2 ステップのプロセスです。

まず、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する必要があります。後で災害復旧ノードをアップグレードする必要があります。

障害復旧ノードをアップグレードする前に、高可用性で展開されている NetScaler ADM サーバーをアップグレードしていることを確認してください。

- NetScaler ADM サーバーを高可用性モードで古いリリースから 12.1 にアップグレードする場合は、このドキュメントの「以前のリリースから 12.1 への高可用性ペアのアップグレード 」を参照してください。
- 高可用性ペアで以前の 12.1 ビルドから新しい 12.1 ビルドにアップグレードする場合は、このドキュメントの「高可用性ペアを以前の 12.1 バージョンから最新バージョンにアップグレードする 」を参照してください。

NetScaler ADM 障害回復ノードをアップグレードする

1. Citrix ダウンロードサイトから NetScaler ADM アップグレードイメージファイルをダウンロードします。
2. 「nsrecover」認証情報を使用して、このファイルを災害復旧ノードにアップロードします。

3.「nsrecover」認証情報を使用して災害復旧ノードにログオンします。

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Fri Aug 31 05:41:16 2018 from 10.252.241.37
bash-3.2# cd /var/mps/mps_images/
bash-3.2# tar zxvf build-mas-12.1-500.113.tgz
```

4. イメージファイルを配置したフォルダに移動し、ファイルを解凍します。
5. 次のスクリプトを実行します。

   ./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。

   - NetScaler ADM サーバーを高可用性モードで古いリリースから 12.1 にアップグレードする場合は、このドキュメントの「以前のリリースから 12.1 への高可用性ペアのアップグレード」を参照してください。
   - 高可用性ペアで以前の 12.1 ビルドから新しい 12.1 ビルドにアップグレードする場合は、「高可用性ペアを以前の 12.1 バージョンから最新バージョンにアップグレードする」を参照してください。

2. NetScaler ADM 障害回復ノードをアップグレードします。

   詳しくは、「NetScaler ADM ディザスタリカバリ展開のアップグレード」を参照してください。

オンプレミスエージェントのアップグレード

1. Citrix ダウンロードサイトから NetScaler ADM エージェントのアップグレードイメージファイルをダウンロードします。
2.「nsrecover」認証情報を使用して、このファイルをエージェントノードにアップロードします。
3. 正しいエージェントアップグレードイメージをダウンロードしてください。画像ファイル名の形式は次のとおりです。

   ビルドマスエージェント-12.1-48.18.tgz

4.「nsrecover」認証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。

   。/エージェントとしてインストール

```
bash-3.2# ./installmasagent
```

NetScaler ADM の高度なバックアップと復元機能のサポートを削除

高度なバックアップ機能を使用して NetScaler ADM サーバーの完全なバックアップを作成する代わりに、NetScaler ADM バージョン **12.1** で利用可能になった新しいディザスタリカバリ機能を使用して、NetScaler ADM 高可用性セットアップの完全なバックアップを作成し、ビジネス継続性のユースケースを支援できるようになりました。

> 重要
>
> 1. NetScaler ADM 12.1 にアップグレードすると、高度なバックアップ機能は利用できなくなります。高度なバックアップ機能を削除し、ディザスタリカバリ機能を使用してバックアップを続行するには、「NetScaler ADM 12.1 へのアップグレード後に NetScaler ADM をバックアップする」を参照してください。ディザスタリカバリは、NetScaler ADM HA でのみサポートされています。
> 2. 構成ファイル、インスタンスの詳細、システムデータなどを含む NetScaler ADM サーバーの部分的なバックアップを引き続き作成し、NetScaler ADM サーバーをスタンドアロン展開で復元するには（部分バックアップ）、「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」を参照してください。

プライマリサーバーで障害が発生した場合は、障害回復機能を使用して、データを失うことなく同じプライマリサーバー上で NetScaler ADM を起動および構成します。この機能は、NetScaler ADM バージョン 12.1 からの高可用性セットアップでデプロイされた NetScaler ADM サーバーでのみ使用できます。

NetScaler ADM 12.1 にアップグレードしたら、NetScaler ADM サーバーをバックアップしてください

NetScaler ADM サーバーを引き続きバックアップするには、Citrix では次のことを推奨します。

1. 次の手順を実行して、NetScaler ADM のリモートバックアップ設定を削除します。

a) [システム] > [システム管理] > [高度なシステムバックアップ設定] に移動します。

b)「バックアップの詳細設定」ページで、「いいえ」を選択してリモートバックアップを無効にします。

c) [設定の適用] をクリックします。NetScaler ADM サーバーが再起動し、変更した設定が適用されるまでお待ちください。

d) リモートバックアップノードを削除します。

2. 新しい NetScaler ADM サーバーを展開して構成し、上記の手順で再起動した既存の NetScaler ADM サーバーを使用して高可用性セットアップを作成します。

   - NetScaler ADM スタンドアロン展開の詳細については、「NetScaler ADM の展開」を参照してください。
   - NetScaler ADM HA の展開について詳しくは、「高可用性展開」を参照してください。

3. 引き続きデータのバックアップと復元を行うようにディザスタリカバリを設定します。ディザスタリカバリの詳細については、「高可用性を実現するためのディザスタリカバリの設定」を参照してください。

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 ギガバイト）を超える場合は、追加のディスクを接続できます。単一サーバー展開と高可用性展開の両方で、追加のディスクを接続できます。

NetScaler ADM をリリースバージョン 12.0 から 12.1 にアップグレードしても、以前のバージョンの追加ディスクに作成したパーティションは変わりません。パーティションは削除されず、サイズも変更されません。

追加ディスクを接続する手順は、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。ツールを使用して、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こともできます。追加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ツールを使用する方法について詳しくは、「NetScaler ADM に追加ディスクを接続する方法」を参照してください。

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

NetScaler ADM 12.1 ビルド 49.23 以降、OpenStack オーケストレーションワークフローのアーキテクチャが更新されました。ワークフローでは、NetScaler ADM StyleBook を使用して NetScaler ADC インスタンスを構成するようになりました。バージョン 12.0 またはバージョン 12.1 ビルド 48.18 のいずれかから NetScaler ADM 12.1 ビルド 49.23 にアップグレードする場合は、次の移行スクリプトを実行する必要があります。

```
/mps/scripts/migration_scripts/migrate_configurations.py
<!--NeedCopy-->
```

「os-cs-lb-mon」StyleBook とマイグレーションスクリプトの詳細については、「StyleBook を使用した OpenStack 上の NetScaler ADC VPX インスタンスの Provisioning」を参照してください

認証

February 6, 2024

2018 年 5 月 24 日

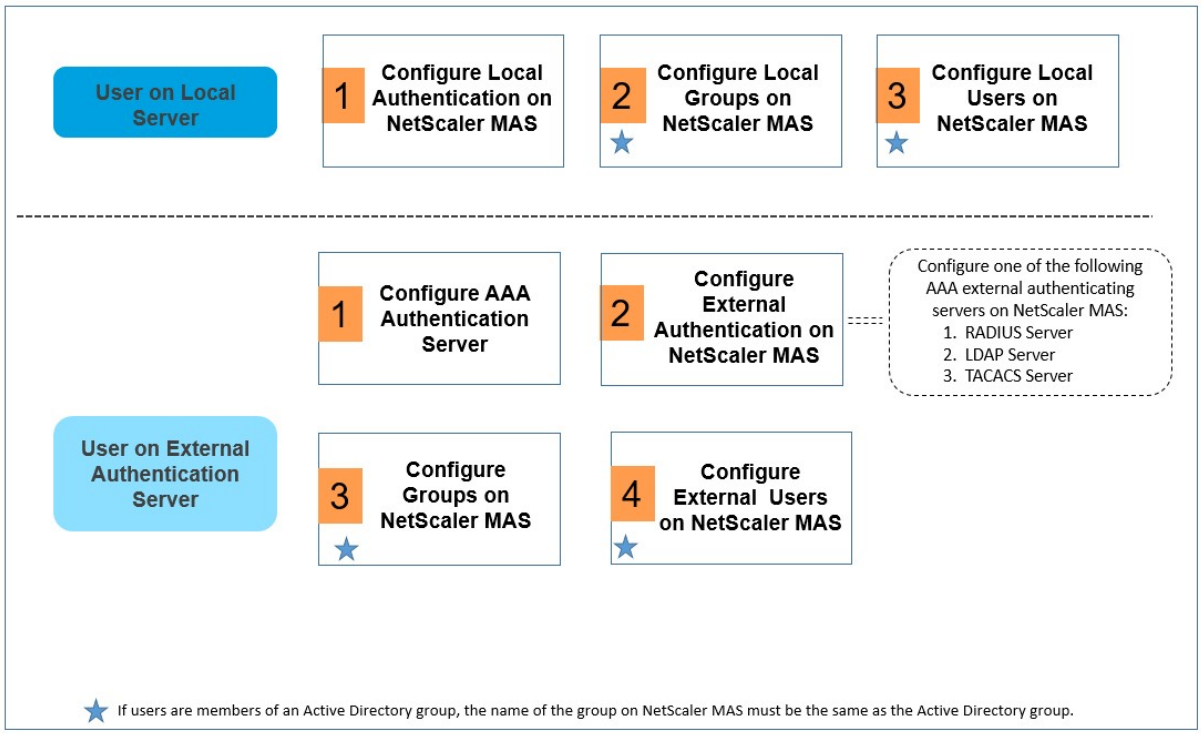
ユーザーは、Citrix Application Delivery Management（ADM）による内部認証、認証サーバーによる外部認証、またはその両方による認証が可能です。ローカル認証を使用する場合、ユーザーは NetScaler ADM セキュリティデータベースに存在する必要があります。ユーザーを外部認証する場合は、選択した認証プロトコルに応じて、そのユーザーの「外部名」が、認証サーバーに登録された外部ユーザー ID と一致する必要があります。

Citrix ADM は、RADIUS、LDAP、および TACACS プロトコルによる外部認証をサポートしています。この統合されたサポート機能により、システムにアクセスしているローカルと外部の AAA（Authentication, Authorization, and Accounting）サーバーユーザーすべてを共通のインターフェイスから認証、承認できます。NetScaler ADM では、システムとの通信に使用する実際のプロトコルに関係なく、ユーザーを認証できます。外部認証用に構成された Citrix ADM 実装にユーザーがアクセスしようとすると、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、対応するプロトコルを使用して Citrix ADM でユーザーが識別されます。

NetScaler ADM でユーザーを認証するには、次の 2 つの方法があります。

- Citrix ADM ローカルサーバーを使用して
- 外部認証サーバーの使用

次のフローチャートは、ローカルユーザーまたは外部ユーザーを認証する場合のワークフローを示しています。



外部認証サーバーの設定

Citrix ADM は、外部の認証、承認、アカウンティング（AAA）サービスを提供するためのさまざまなプロトコルをサポートしています。

Citrix ADM は、すべての認証、承認、アカウンティング（AAA）サービスリクエストをリモートの RADIUS、LDAP、または TACACS+ サーバーに送信します。リモート AAA サーバーは要求を受信し、要求を検証して、Citrix ADM に応答を送り返します。認証にリモートの RADIUS、TACACS+、または LDAP サーバーを使用するように構成すると、Citrix 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。ログインとログアウトのアカウント名、割り当てられた権限、およびタイムアカウンティング（time-accounting）の記録もユーザーごとに AAA サーバーに格納されます。

さらに、NetScaler ADM 内部データベースを使用して、ローカルでユーザーを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。特定の種類の認証用に、サーバーグループを作成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。グループ内に異なる種類のサーバーを構成できるほか、内部データベースを認証バックアップのフォールバックとして、AAA サーバーの構成一覧に含めることができます。

RADIUS 認証サーバーを設定します

Citrix ADM は、1 つまたは複数の RADIUS サーバーでユーザーアクセスを認証するように構成できます。構成には、ネットワークアクセスサーバーの IP（NAS IP）アドレス、またはネットワークアクセスサーバー識別子（NAS ID）の使用が必要な場合があります。RADIUS 認証サーバーを使用するように Citrix ADM を構成する場合は、次のガイドラインに従ってください。NAS IP アドレスの使用を有効にすると、アプライアンスは、RADIUS 接続の確立に使用された送信元 IP アドレスを送信するのではなく、構成した IP アドレスを RADIUS サーバーに送信します。

- NAS ID を構成すると、アプライアンスは RADIUS サーバーにこの識別子を送信します。NAS ID を構成しないと、アプライアンスは RADIUS サーバーにホスト名を送信します。
- NAS IP アドレスを有効にすると、アプライアンスは構成されるすべての NAS ID を無視して、RADIUS サーバーとの通信に NAS IP を使用します。

RADIUS 認証サーバーを構成するには：

1. Citrix ADM で、[システム] > [認証] > [**RADIUS**] に移動します。
2.「**RADIUS** 」ページで、「追加」をクリックします。
3.「**RADIUS** サーバーの作成」ページでパラメータを設定し、「作成」をクリックしてサーバーを RADIUS 認証サーバーのリストに追加します。次のパラメーターを必ず設定する必要があります。

   a) 名前。RADIUS サーバーの名前。

   b) サーバー名**/IP** アドレス。RADIUS サーバのサーバ名または IP アドレス。

c) ポート。デフォルトでは、RADIUS 認証には、ポート 1812 が使用されます。必要に応じて、別のポート番号を指定できます。

d) タイムアウト **(**秒**)**。Citrix ADM システムが RADIUS サーバーからの応答を待つ時間（秒単位）。

e) シークレットキー。任意の英数字の式。これは、通信を可能にするために Citrix ADM と RADIUS サーバー間で共有されるキーです。

4. [詳細] をクリックしてセクションを展開し、追加のパラメーターを設定して、[作成**]** をクリックします。

RADIUS サーバーを追加する方法の詳細については、「RADIUS 認証サーバーを追加する方法」を参照してください。

LDAP 認証サーバーを設定する

Citrix ADM は、1 つまたは複数の LDAP サーバーでユーザーアクセスを認証するように構成できます。LDAP 認証では、Active Directory、LDAP サーバー、および Citrix ADM で同じグループ名を使用する必要があります。グループ名は、大文字小文字の使い分けを含め、一字一句正確に一致させる必要があります。

LDAP 認証サーバーを設定するには:

1. Citrix ADM で、[システム] > [認証] > **[****LDAP**] に移動します。
2. [**LDAP**] ページで、[追加] をクリックします。
3. 「**LDAP** サーバーの作成」ページでパラメーターを設定し、「作成」をクリックしてサーバーを LDAP 認証サーバーのリストに追加します。次のパラメーターを必ず設定する必要があります。

   a) 名前。LDAP サーバーの名前。

   b) サーバー名**/IP** アドレス。LDAP サーバーのサーバー名または IP アドレス。

   c) セキュリティタイプ。システムと LDAP サーバー間で必要な通信の種類です。ドロップダウンの一覧から選択します。平文通信が適切でない場合は、Transport Layer Security（TLS）または SSL を選択することで暗号化通信を選択できます。

   d) ポート。デフォルトでは、LDAP 認証にはポート 389 が使用されます。必要に応じて、別のポート番号を指定できます。

   e) サーバータイプ。LDAP サーバのタイプとして、**Active**Directory (AD**)** または **Novell** ディレクトリサービス **(NDS)** を選択します。

   f) タイムアウト **(**秒**)**。Citrix ADM システムが LDAP サーバーからの応答を待つ時間（秒単位）。

追加の詳細情報を入力できます。LDAP 証明書を検証するには、「LDAP 証明書を検証」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することもできます。追加パラメーターとして、ディレクトリサービスに対するクエリのドメインネームサーバー（DN）の詳細、デフォルトの認証グループ、グループの属性、その他の属性などがあります。

通常は、バインド識別名からユーザー名を除き、ユーザーが属するグループ名を指定したものが基本識別名になります。[Administrator Bind DN] テキストボックスに、LDAP ディレクトリのクエリで使用する管理者のバインド識別名を入力します。

基本識別名の構文の例を次に示します。

- ou=users,dc=ace,dc=com
- cn=Users,dc=ace,dc=com

バインド識別名の構文の例を次に示します。

- domain/user name
- ou=administrator,dc=ace,dc=com
- user@domain.name（Active Directory の場合）
- cn=Administrator,cn=Users,dc=ace,dc=com

Citrix ADM で定義するグループ名とユーザーの名前は、LDAP サーバーで構成されたものと同じである必要があります。

> 注
>
> RADIUS または LDAP サーバの設定時に、「詳細」セクションにデフォルト認証グループの名前を入力できます。ユーザーがグループに関連付けられているかどうかに関係なく認証が成功した場合には、ユーザーの承認にこのデフォルトのグループが選択されます。このグループに割り当てられているかどうかに基づいて、ユーザーはこのデフォルトのグループとその他のグループで構成された権限の組み合わせを受け取ります。

LDAP サーバーを追加する方法の詳細については、「LDAP 認証サーバーを追加する方法」を参照してください。

外部認証サーバーをカスケードする方法の詳細については、「外部認証サーバーをカスケードする方法」を参照してください。

TACACS 認証サーバーを設定します

TACACS は、RADIUS および LDAP と同様に、ネットワークアクセスのリモート認証サービスを処理します。

TACACS 認証サーバを設定します。

1. **Citrix ADM** で 、[システム] > [認証] > **[TACACS**] に 移動します。
2. [**TACACS**] ページで 、[追加] をクリック します。
3. 「**TACACS** サーバ の 作成」ページで、次の詳細を入力します。
    a) TACACS サーバーの名前
    b) TACACS サーバーの IP アドレス

c) ポートおよびタイムアウト（秒）

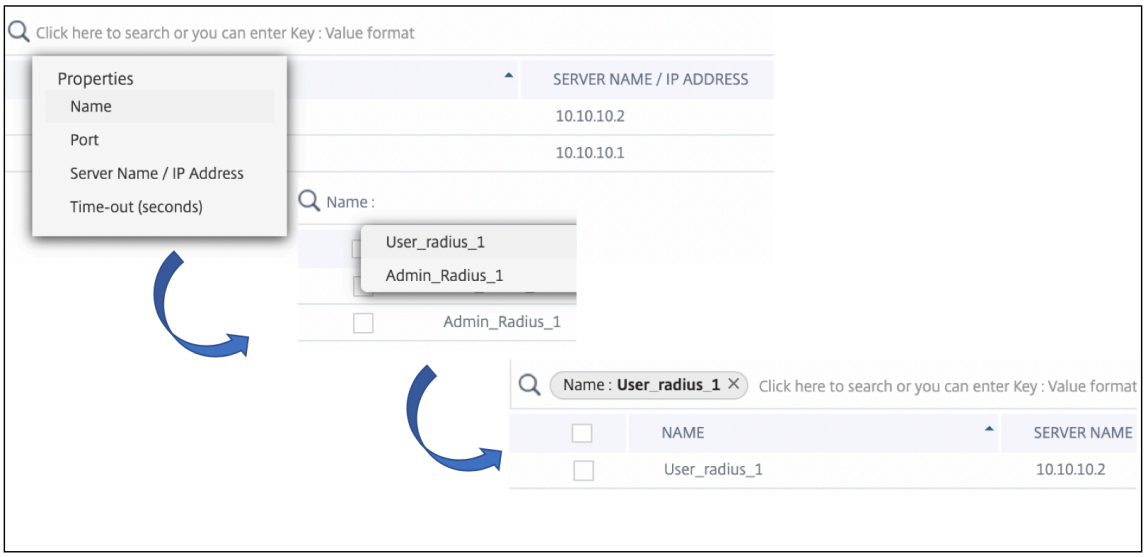
d) システムと TACACS サーバーが互いに通信するために共有するキー。

e) 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。

TACACS サーバーを追加する方法の詳細については、「TACACS 認証サーバーの追加方法」を参照してください。

> 注
>
> Citrix ADM に追加された認証サーバーを検索するには、検索バーをクリックして、必要な検索条件を選択します。



Citrix ADM でユーザーのローカル認証を構成する

ローカル認証を使用している場合は、ユーザーを作成し、Citrix ADM で作成したグループに追加します。ユーザーとグループを構成したら、承認およびセッションポリシーを適用し、ブックマークを作成し、アプリケーションを指定し、ユーザーがアクセスできるファイル共有とサーバーの IP アドレスを指定できます。

Citrix ADM でローカル認証を構成するには：

1. Citrix ADM で、［システム］>［認証］に移動し、［認証構成］をクリックします。
2. 「認証設定」ページで、「サーバータイプ」ドロップダウンボックスから「**LOCAL** 」を選択し、「**OK**」をクリックします。

Citrix ADM で外部認証を構成する

Citrix ADM で外部認証サーバーを構成すると、それらの外部サーバーで認証されたユーザーグループが Citrix ADM にインポートされます。Citrix ADM でユーザーを作成する必要はありません。ユーザーは、Citrix ADM の外部サーバーで管理されます。ただし、外部認証サーバーに対するユーザーグループの権限レベルが Citrix ADM で維持されていることを確認する必要があります。Citrix ADM は、特定の負荷分散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り、ユーザーの認証を実行します。認証サーバーが後でシステムから削除されると、グループとユーザーは自動的にシステムから削除されます。

Citrix ADM で外部認証を構成するには:

1. Citrix ADM で、［システム］>［認証］に移動し、［認証構成］をクリック します。
2.「認証設定」ページで、「サーバータイプ」ドロップダウンリストから「**EXTERNAL** 」を選択します。
3. [挿入] をクリックします。
4.「外部サーバー」ページで、認証サーバーを選択します。必要に応じて、カスケードする認証サーバーを複数選択できます。

   > 注
   >
   > カスケードできるのは外部サーバーだけです。

5. 外部認証が失敗した場合にローカル認証を引き継ぐ場合は、「フォールバックローカル認証を有効にする」を選択します。
6. [**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「認証サーバー」ページに表示されます。

   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。

Citrix ADM でグループを構成する

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。グループは「管理者」または「読み取り専用」のいずれかの権限を持ち、グループ内のすべてのユーザーが同じ権限を受け取ります。

Citrix ADM では、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。グループは 1 つまたは複数の役割を持つことができます。ユーザーは、割り当てられた権限に基づくアクセス権を持つエンティティとして定義されます。ユーザーは、1 つまたは複数のグループに所属できます。

NetScaler ADM でローカルグループを作成し、グループ内のユーザーに対してローカル認証を使用できます。認証に外部サーバーを使用している場合は、内部ネットワークの認証サーバーで構成されたグループと一致するように Citrix ADM 上のグループを構成します。ユーザーがログオンして認証されると、グループ名が認証サーバー上のグループと一致すると、ユーザーは NetScaler ADM でそのグループの設定を継承します。

グループを構成したら、承認およびセッションポリシーを適用し、ブックマークを作成し、アプリケーションを指定し、ユーザーがアクセスできるファイル共有とサーバーの IP アドレスを指定できます。

ローカル認証を使用している場合は、ユーザーを作成し、Citrix ADM で構成されている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。

> 注
>
> ユーザーが AcActive Directory グループのメンバーである場合、グループの名前と Citrix ADM 上のユーザーの名前は Active Directory グループの名前と同じである必要があります。

Citrix ADM でユーザーグループを構成するには:

1. NetScaler ADM で、［システム］>［ユーザー管理］>［グループ］に移動します。
2.「グループ」ページで、「追加」をクリックしてグループを作成します。デフォルトでは、Citrix ADM には 2 つのグループが作成され、権限は管理者と読み取り専用に設定されます。これらのグループにユーザーを追加できるほか、ユーザーのために別のグループを作成することもできます。
3.「システムグループの作成」ページの「グループ設定」タブで、グループの名前を入力し、ロールを管理者または読み取り専用に設定します。「ユーザーセッションタイムアウトの設定」を選択して、そのグループにログインしているユーザーセッションのタイムアウト制限を設定できます。

   > 注
   >
   > Citrix ADM で作成されたユーザーグループの名前が、外部認証サーバーの名前と同じであることを確認してください。ユーザーグループの名前が正確に一致していないと、グループが認識されないので、グループメンバーの抽出とシステムへの取り込みが行われません。

4.「認証設定」タブで、必要なグループを選択します。［**Create Group**］をクリックします。
5.「ユーザーの割り当て」タブで、グループに追加するユーザーを選択します。Citrix ADM の「ユーザーの構成」でユーザーを構成すると、このテーブルにユーザーが追加されます。
6.［完了］をクリックします。

システムでグループの作成が完了すると、外部認証サーバー内のすべてのユーザーが抽出され、システムに取り込まれます。グループ名が外部認証サーバーのグループ名と同じ場合、ユーザーは、システムにログオンしたときに、すべての権限定義を継承します。

Citrix ADM でユーザーを構成する

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。外部認証サーバー上に存在するユーザーをローカルで認証する場合は、認証サーバーと Citrix ADM の両方に同じユーザーが存在することを確認してください。

NetScaler ADM でユーザーを構成するには:

1. NetScaler ADM で、［システム］>［ユーザー管理］>［ユーザー］に移動します。
2. ［ユーザー］ページで、［追加］をクリックして Citrix ADM にユーザーを追加します。
3. 「システムユーザーの作成」ページで、次のパラメータを設定します。
    a) ユーザー名。ユーザーの名前
    b) パスワード。ユーザーが Citrix ADM へのログオンに使用するパスワード
    c) 外部認証を有効にします。これが有効になっていない場合、ユーザーはローカルユーザーとして認証されます。
    d) ユーザーセッションタイムアウトを設定します。ユーザーがアクティブな状態でいられる時間です。この期間は、分単位または時間単位で設定できます。
4. 「グループ」テーブルで、ユーザーを追加するグループを選択します。Citrix ADM のユーザーグループの構成でグループを構成すると、グループメンバーがこのテーブルに追加されます。
5. ［作成］をクリックします。

> 注
>
> ユーザーが Active Directory を使用している場合は、Citrix ADM のグループ名が外部サーバーの Active Directory グループのグループ名と同じであることを確認してください。

認証サーバグループの抽出方法

February 6, 2024

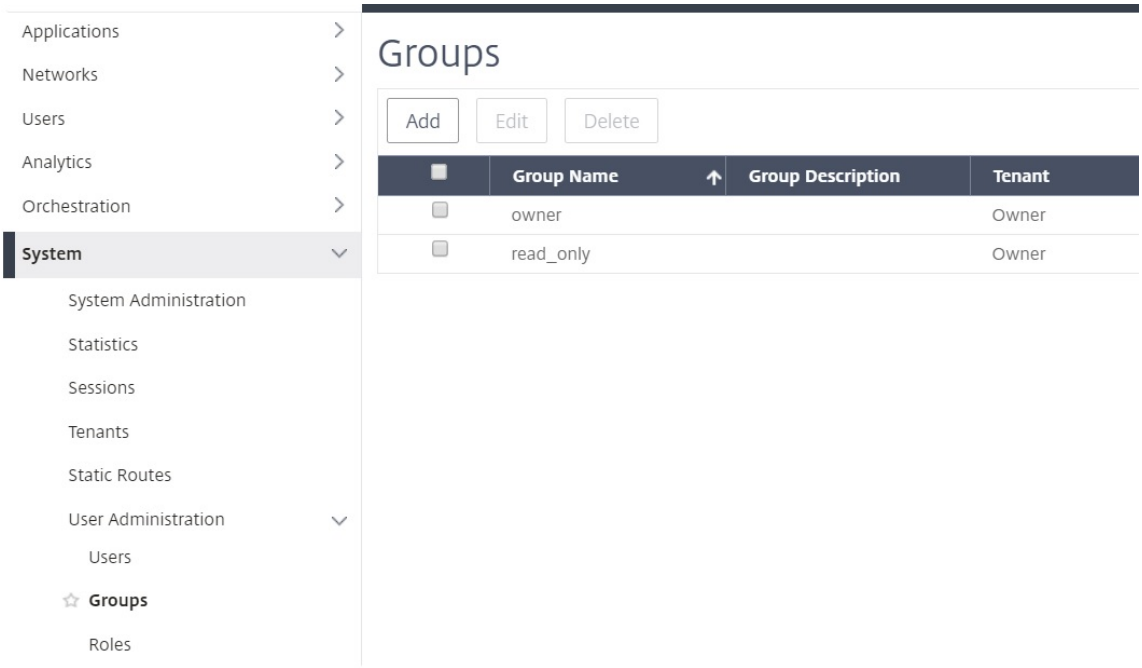
Citrix Application Delivery Management（ADM）を使用すると、外部認証サーバーに存在するユーザーのグループを抽出し、役割の要求に応じて、また Citrix ADC の定義に従って権限を割り当てることができます。これには次の 2 つの利点があります。

1. Citrix ADM でユーザーを作成する必要はありません。グループは Citrix ADM サーバーに抽出されますが、システムに追加されるのではなく、Citrix ADM から外部サーバーで管理されます。
2. 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。将来は、特定の認証サーバーがシステムから削除されると、グループとユーザーが自動的にシステムから削除される予定です。

グループの設定とグループ権限の割り当て

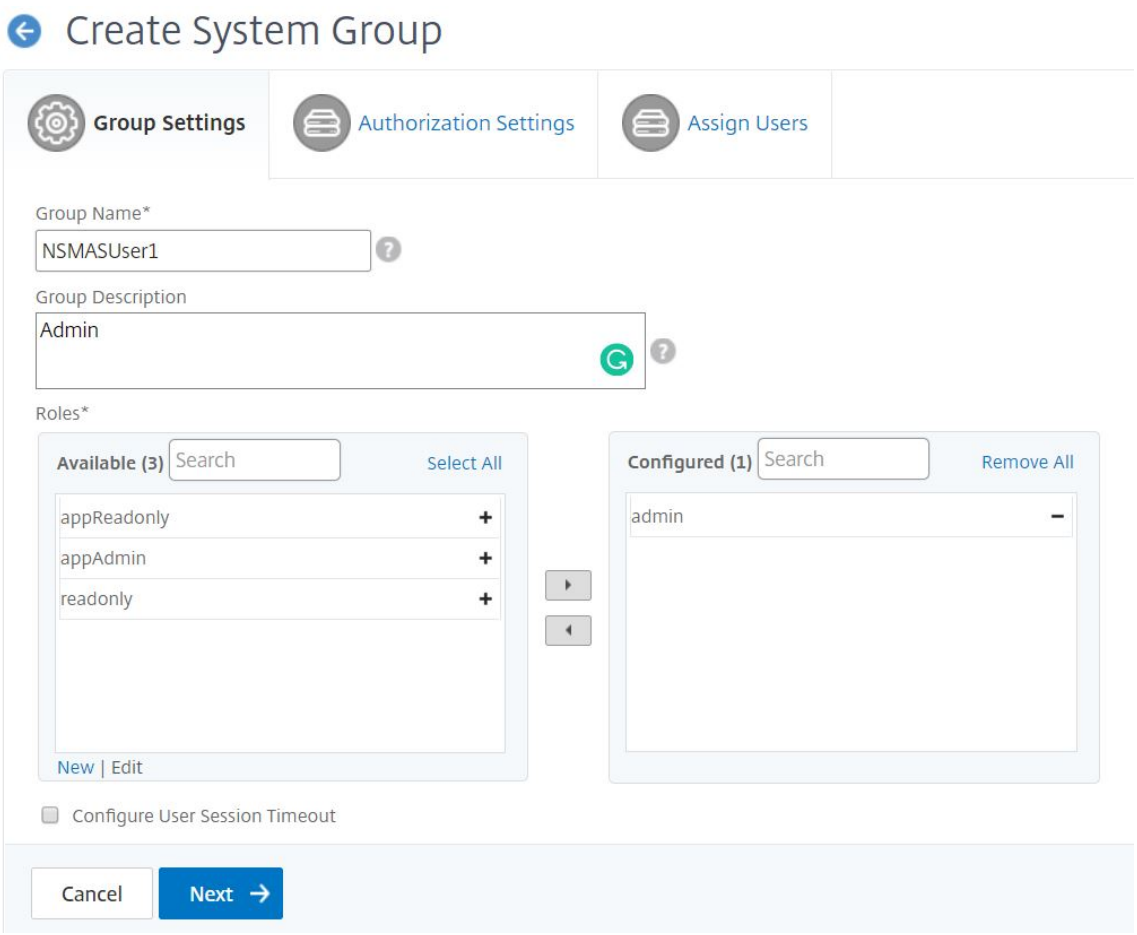
1. NetScaler ADM で、［システム］>［ユーザー管理］>［グループ］に移動します。

2. [追加] をクリックしてグループを作成します。



3.「グループ設定」タブで、グループの名前を入力し、権限を管理者、読み取り専用、AppReadOnly、または AppAdmin に設定します。ほかに構成できるオプションとして、セッションタイムアウトがあります。セッションタイムアウトでは、そのグループのユーザーがログインするセッションのタイムアウト制限を設定できます。また、グループメンバーがアクセスできる仮想マシンインスタンスを設定することもできます。

> 注
>
> Citrix ADM で作成されたユーザーグループの名前が、外部認証サーバーで作成されたユーザーグループの名前とまったく同じであることを確認してください。ユーザーグループの名前が正確に一致していないと、グループが認識されないので、グループメンバーの抽出とシステムへの取り込みが行われません。



4. 「認証設定」タブでは、次の 4 つのグループの承認設定を指定できます。

   - インスタンス
   - アプリケーション
   - 構成テンプレート
   - StyleBook

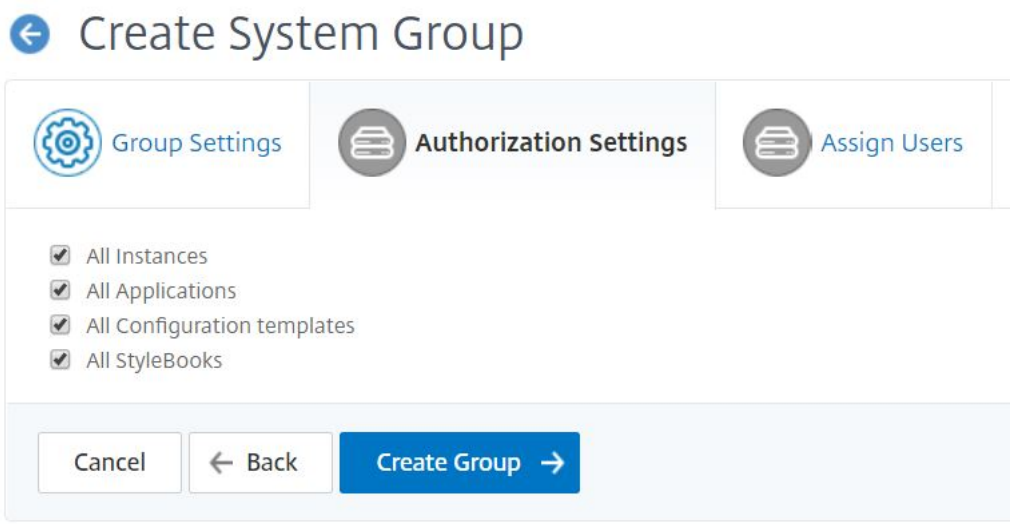
デフォルトでは、ユーザーは上記のすべてのグループにアクセスできます。チェックボックスをオフにして、これらの各グループに選択的にアクセスできるようにすることができます。

次に例を示します:

- [インスタンス] チェックボックスをオフにして、ユーザーにアクセス権を付与する必要なインスタンスのみを選択できます。
- [すべてのアプリケーション] チェックボックスをオフにし、必要なアプリケーションとテンプレートのみを選択します。Citrix ADM のグループにアプリケーションを追加すると、正規表現を使用して、グループの正規表現条件を満たすアプリケーションを検索して追加できます。これらのグループにバインドされているユーザーは、それらの特定のアプリケーションにのみアクセスできます。指定された正規表現式は、NetScaler

ADM に保持されます。つまり、Citrix ADM では、「正規表現の追加」テキストボックスに 入力された正規表現 をシステムに保存し、新しいアプリケーションがこの正規表現を満たすたびに認証範囲を動的に更新します。新しいアプリケーションがシステムに追加されると、Citrix ADM は新しいアプリケーションに検索条件を適用し、条件を満たすアプリケーションがグループに動的に追加されます。新しいアプリケーションを手動でグループに追加する必要はありません。アプリケーションはシステム内で動的に更新され、各グループのユーザーは、NetScaler ADM 適切なモジュールの下にあるアプリケーションを表示できます。

- 必要 なテンプレート のみにアクセスできるようにするには、「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ます。
- 「**** すべて の **StyleBooks**** 」チェックボックスをオフにし、ユーザーがアクセスできる必要な StyleBook を選択します。
- 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。その StyleBook の設定パックは、ユーザーがアクセスできるものにも含まれています。



システムでグループの作成が完了すると、外部認証サーバー内のすべてのユーザーが抽出され、システムに取り込まれます。これを確認するには、グループを選択して [編集] をクリックします。[Create System Group] の [Users] テーブルに、グループに関連付けられているユーザーの一覧が表示されます。「ユーザーの割り当て」タブでユーザーをグループに 割り当てることもできます。

グループ名が外部認証サーバーのグループ名と同じ場合、ユーザーは、システムにログオンしたときに、すべての権限定義を継承します。

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 認証サーバーと統合すると、Citrix ADM を使用して分散ディレクトリからユーザー資格情報を検索して認証できます。

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

   a) 名前—LDAP サーバー名を指定します。

   b) サーバー名**/IP** アドレス—LDAP IP アドレスまたはサーバー名を指定します。

   c) セキュリティタイプ—システムと LDAP サーバー間で必要な通信のタイプ。一覧から選択します。プレーンテキスト通信が不十分な場合は、トランスポート層セキュリティ (TLS) または SSL を選択して暗号化通信を選択できます。

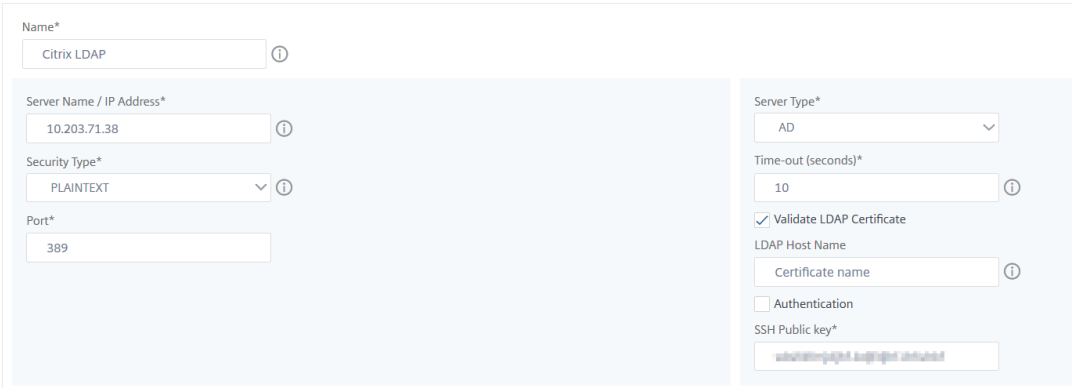
   d) ポート—デフォルトでは、ポート 389 が PLAINTEXT に使用されます。SSL/TSL にはポート 636 を指定することもできます。

   e) サーバーの種類—LDAP サーバーの種類として Active Directory (AD) または NDS (ノベルディレクトリサービス) を選択します。

   f) タイムアウト（秒）—Citrix ADM システムが LDAP サーバーからの応答を待つ時間（秒単位）

   g) **LDAP** ホスト名—「LDAP 証明書の検証」チェックボックスを選択し、証明書に入力するホスト名を指定します。

   [認証] オプションをオフにして、SSH 公開キーを指定します。鍵ベースの認証では、ユーザーオブジェクトに保存されている公開鍵のリストを取得できます。これらの公開鍵は SSH 経由で LDAP サーバーに保存されます。



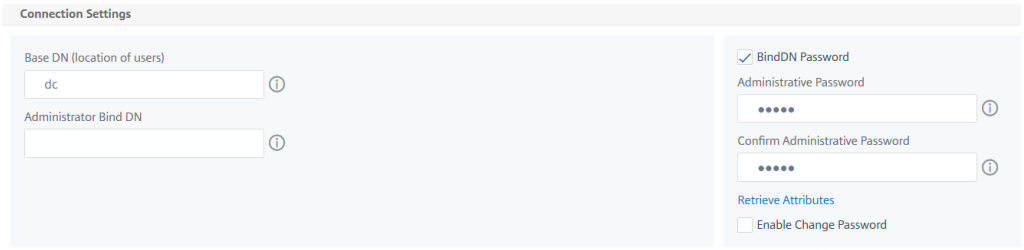
   [接続設定] で、次のパラメータを指定します。

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。

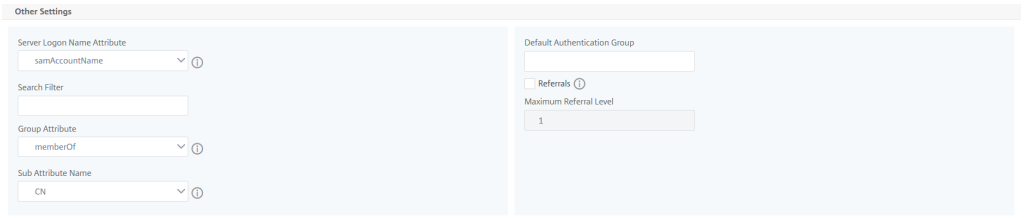
i. サーバーログオン名属性—システムが外部 LDAP サーバーまたは Active Directory にクエリを実行するために使用する名前属性。リストから **samAccountname** を選択します。

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、vpnallowed=true に ldaploginname samaccount を指定し、ユーザー指定のユーザー名 bob を指定すると、LDAP 検索文字列は: になります。&(vpnallowed=**true**)(samaccount=bob)

iii.「グループ属性」—リストから「MemberOf」を選択します。

iv. サブ属性名—LDAP サーバーからグループを抽出するためのサブ属性名。

v. デフォルト認証グループ—抽出されたグループに加えて、認証が成功したときに選択されるデフォルトグループ。



4. [作成] をクリックします。

LDAP サーバーが設定されました。

> 注
>
> ユーザーが Active Directory グループメンバーである場合、NetScaler ADM 上のグループとユーザーの名前は、同じ Active Directory グループメンバーの名前である必要があります。

フォールバックローカル認証を有効にする方法

February 6, 2024

ローカル認証のフォールバック機能を使用すると、外部認証に失敗したとき、ローカル認証によって処理を引き継ぐことができます。Citrix Application Delivery Management（ADM）と外部認証サーバーの両方で構成されたユーザーは、構成された外部認証サーバーがダウンしているかアクセスできない場合でも、Citrix ADM にログオンできます。ローカル認証のフォールバックが機能するためには、次の 3 点を確認する必要があります。

- 外部認証サーバーがダウンした後でも、Citrix ADM にアクセスできるはずです。
- Citrix ADM と外部認証サーバーの両方で構成する必要があります。
- 少なくとも 1 台の外部サーバーを追加している。

ローカル認証のフォールバックを有効にするには、次の手順を実行します。

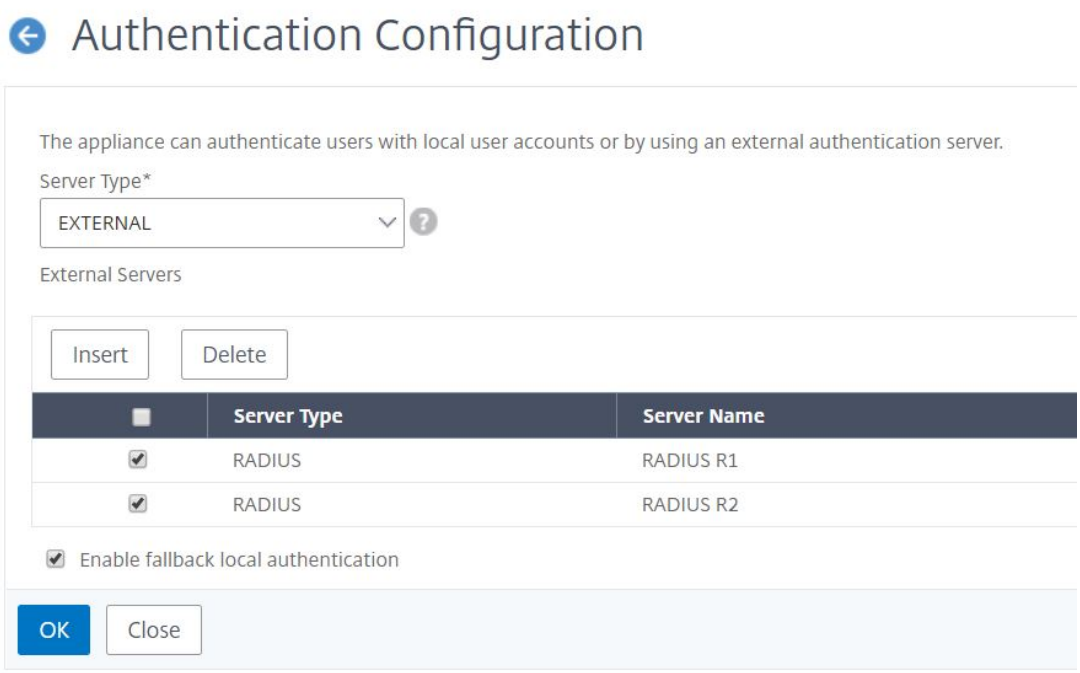
1. Citrix ADM で、［システム］>［認証］に移動し、［認証構成］をクリックします。
2. 「サーバータイプ」リストから「外部」を選択します。

   > 注: リストから **LOCAL** を選択すると、ユーザーの認証はデフォルトのローカル認証サーバーで行われます。

3. 「挿入」をクリックし、表示された外部サーバーのリストから外部サーバーを選択し、「**OK**」をクリックして外部サーバーを追加します。

   > 注: 外部サーバーをリストに表示するには、このステップの前に外部サーバーをすでに追加しておく必要があります。外部サーバーの追加方法について詳しくは、以下の記事を参照してください。
   >
   > - RADIUS 認証サーバーを追加する方法
   > - LDAP 認証サーバーを追加する方法
   > - TACACS 認証サーバーを追加する方法

4. 「フォールバックローカル認証 を有効に する」オプションを選択します。



RADIUS 認証サーバーを追加する方法

February 6, 2024

RADIUS 認証サーバーは、ユーザーデータグラムプロトコル（UDP）を使用して動作します。RADIUS サーバーは、ユーザーの接続要求を受信し、ユーザーを認証します。次に、サーバーは、ユーザーにサービスを提供するシステムに構成情報を返します。RADIUS サーバーは、ネットワークアクセスサーバー（NAS）に接続します。NAS がアクセス要求を送信すると、RADIUS サーバーは、そのデータベースを検索して、ユーザー名とその他の情報を探します。ユーザー名がデータベースに存在しない場合、RADIUS サーバーはすぐにアクセス拒否メッセージを送信するか、Citrix ADM にデフォルトプロファイルを読み込むことができます。RADIUS では、認証と承認が対になっています。ユーザー情報が認証されると、RADIUS サーバーは、アクセス承認応答を返します。また、その特定のセッションで使用されるパラメーターを記述した、属性と値のペアの一覧も送信します。

RADIUS 認証サーバーの設定

1. Citrix ADM で、[システム] > [認証] > [**RADIUS**] に移動します。

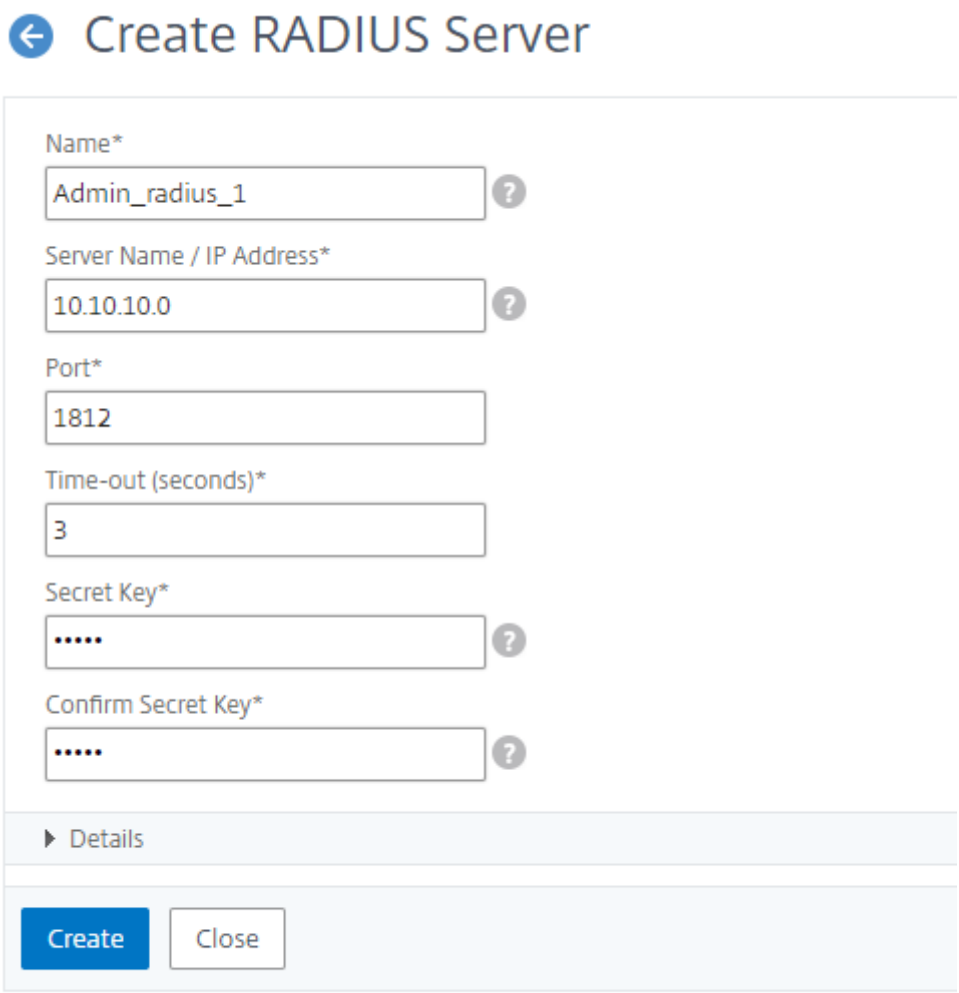
2.「**RADIUS** 」ページで、「追加」をクリックします。

3.「**RADIUS** サーバーの作成」ページでパラメータを設定し、「作成」をクリックしてサーバーを RADIUS 認証サーバーのリストに追加します。

4. RADIUS サーバを作成するには、次のパラメータが必須です。

   - 名前—RADIUS サーバーの名前を入力します
   - サーバー名**/IP** アドレス—RADIUS サーバーのサーバー名または IP アドレスを入力します
   - ポート：デフォルトでは、ポート 1812 が RADIUS 認証メッセージに使用されます。必要に応じて、別のポート番号を指定できます。
   - タイムアウト **(**秒**)**—秒数を入力します。Citrix ADM システムが RADIUS サーバーからの応答を待つ時間。
   - シークレットキー—任意の英数字表現を入力します。Citrix ADM と RADIUS サーバー間で通信用に共有されるキー。

5.「詳細」をクリックしてセクションを展開し、追加のパラメータを設定します。

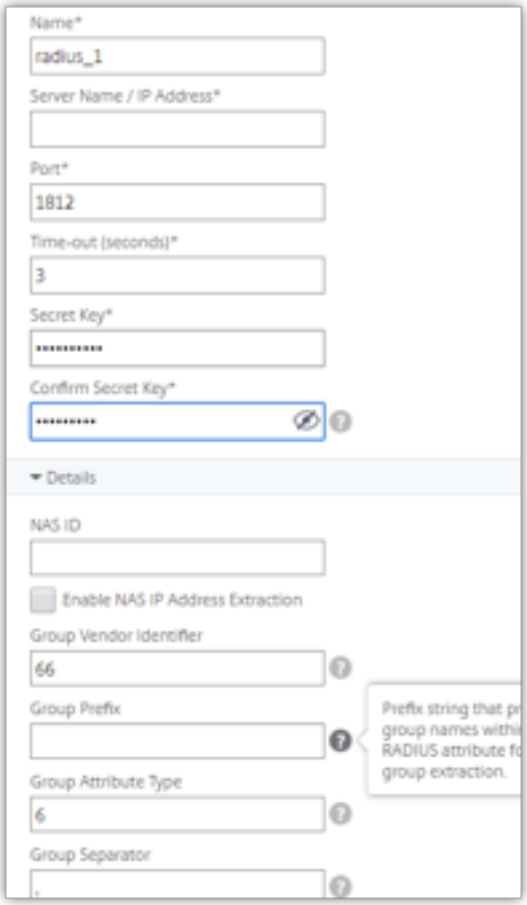


RADIUS サーバを追加する際に、さらに詳細な情報を指定できます。NAS の情報、ベンダーの情報、属性の情報、パスワード認証のタイプなどのパラメーターを追加で入力できます。

> 注
>
> : RADIUS 認証を機能させるには、Citrix ADM で構成されたグループと RADIUS ユーザーを介して抽出されたグループが同じであることを確認してください。ユーザーは、グループに割り当てられた権限に基づいて承認されます。
>
> たとえば、FreeRADIUS サーバーのシナリオを考えてみましょう。
>
> - クリアテキストパスワード =「1.citrix」
> - グループ名 =「radiusgroup1, group1”

この場合、ユーザーは半径グループ 1 とグループ 1 の 2 つのグループに属しています。この場合のグループ区切り文字は「」です。

グループ「radiusgroup1」に属する RADIUS ユーザー「RadiusUser1」として Citrix ADM にログオンする場合は、Citrix ADM でも同じグループ名「radiusgroup1」が設定されていることを確認してください。



次の図に示すように、グループ抽出を行うためのベンダー ID、属性タイプ、グループセパレーター (該当する場合) に関する詳細を指定します。

```
#
# Created for Citrix Use

# currently only using attribute 6 in this setup.

VENDOR Citrix 66


BEGIN-VENDOR Citrix
ATTRIBUTE Group-Names 6 string
END-VENDOR Citrix
```

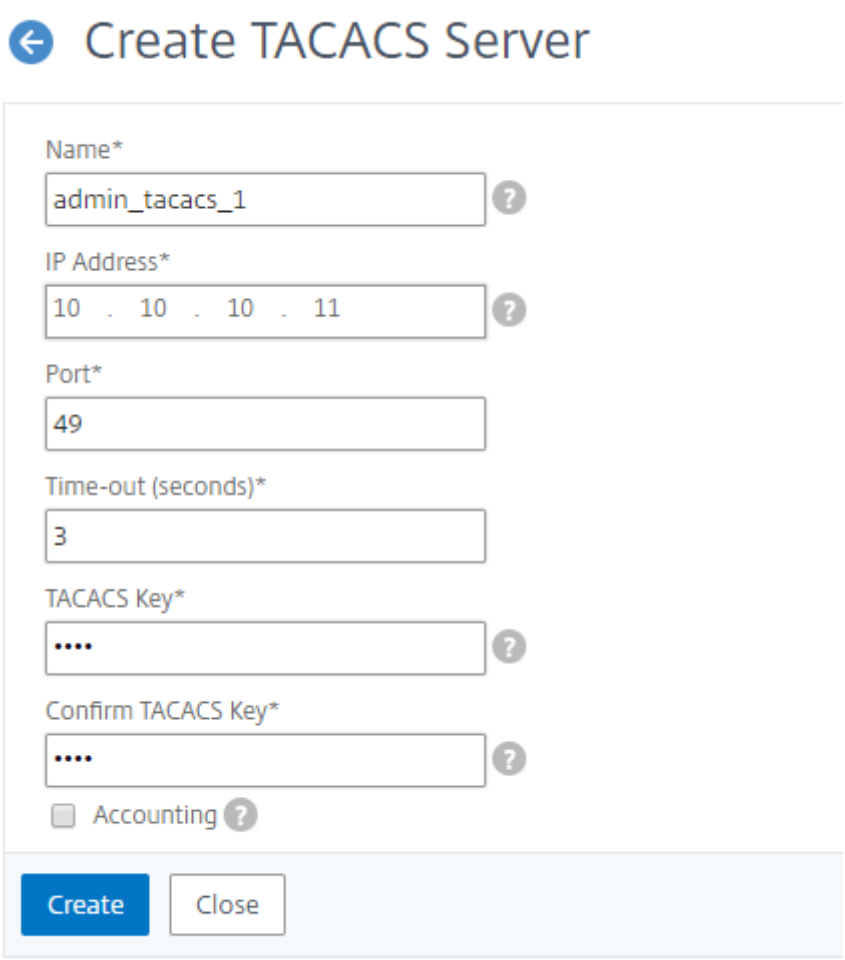

TACACS 認証サーバを追加する方法

February 6, 2024

TACACS は、RADIUS および LDAP とともに、ネットワークアクセスのリモート認証サービスを処理します。

TACACS 認証サーバーの構成

1. **Citrix ADM** で、[システム] > [認証] > **[****TACACS**] に移動します。
2. [**TACACS**] ページで、[追加] をクリックします。
3.「**TACACS** サーバの作成」ページで、次の詳細を入力します。
    a) TACACS サーバーの名前
    b) TACACS サーバーの IP アドレス
    c) ポートおよびタイムアウト（秒）
    d) システムと TACACS サーバーが互いに通信するために共有するキーを入力します。
4. 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。
5.［作成］をクリックします。



外部認証サーバをカスケードする方法

February 6, 2024

Citrix Application Delivery Management（ADM）は、ローカルユーザーとグループを認証するためのローカルサーバーをサポートするだけでなく、RADIUS、LDAP、TACACS などの認証、承認、アカウンティング（AAA）プロトコルの統合システムをサポートします。統合されたサポート機能により、システムにアクセスしているローカルと外部の AAA クライアントすべてを共通のインターフェイスから認証、承認できます。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、外部認証サーバーを Citrix ADM に追加す

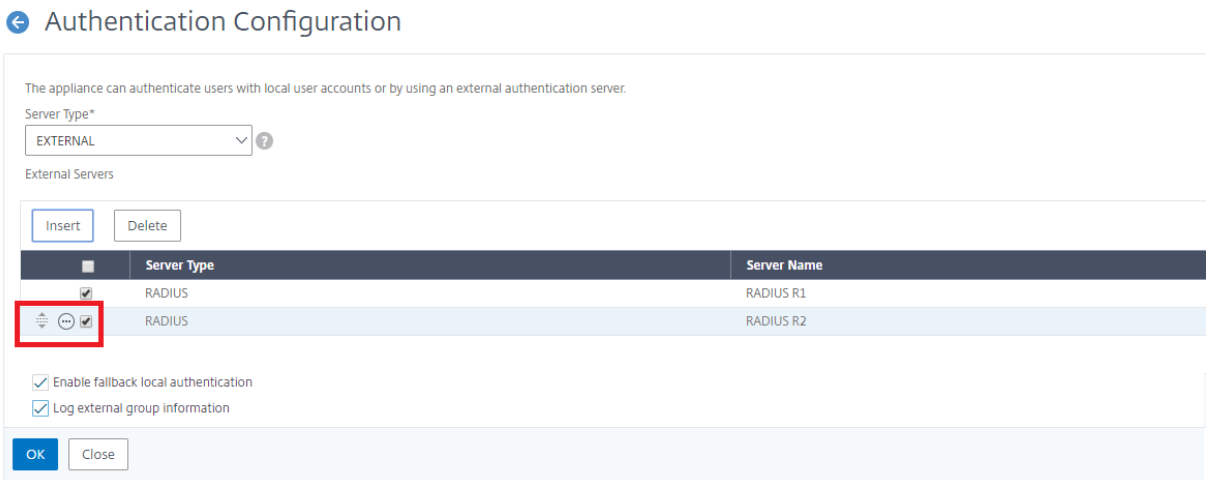
る必要があります。サポートされている外部認証サーバー（RADIUS、LDAP、TACACS）であれば、いずれの種類でも追加できます。たとえば、カスケード認証用に 4 台の外部認証サーバーを追加する場合、RADIUS サーバー 2 台、LDAP サーバー 1 台、TACACS サーバー 1 台にすることも、すべてを RADIUS サーバーで追加することもできます。NetScaler ADM では、最大 32 台の外部認証サーバーを構成できます。

カスケード外部認証サーバーの設定

1. Citrix ADM で、[システム] > [認証] に移動します。
2.「認証」ページで、 「認証設定」をクリックします。
3.「認証設定」ページで、「サーバータイプ」ドロップダウンリストから「**EXTERNAL**」を選択します (カスケード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 1 つまたは複数の認証サーバーを選択します。
5. 外部認証が失敗した場合にローカル認証を引き継ぐ場合は、「フォールバックローカル認証を有効にする」を選択します。
6. [**OK**] をクリックしてページを閉じます。

選択したサーバーは、次の図のように外部サーバーの下に表示されます。

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。認証を実行するには、認証メカニズムによる調査が可能なシステムにユーザーのアカウントが作成されているか、最初の認証プロセスの一部として、アカウントが作成されている必要があります。NetScaler Application Delivery Management（ADM）は、ローカルユーザーと外部ユーザーの両方を認証する方法を提供します。ローカルユーザーは内部で認証されますが、Citrix ADM は RADIUS、LDAP、および TACACS プロトコルによる外部認証をサポートします。外部認証用に構成された NetScaler ADM にユーザーがアクセスしようとすると、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 Citrix ADM 上のユーザーを識別します。

アクセス制御とは、特定のリソースに対して必要なセキュリティを適用するプロセスです。このセキュリティ技術は、コンピューターのシステム環境でリソースを表示または使用できるユーザーを制限するために使用できます。アクセス制御は、コンピューターシステムの正規ユーザーが実行できるアクションや操作を制限することを目的とします。アクセス制御は、ユーザーが直接実行できることのほか、ユーザーの代わりに実行されているプログラムに対して許可されることを制約します。アクセス制御はこのようにして、セキュリティ侵害につながる可能性があるアクティビティを防止することを目指しています。アクセス制御では、参照モニターを通じてアクセス制御が適用される前に、ユーザー認証が正常に検証されていることが前提になっています。Citrix ADM では、きめ細かな役割ベースのアクセス制御（RBAC）が可能であり、管理者は企業内の個々のユーザーの役割に基づいてユーザーにアクセス権限を与えることができます。Citrix ADM の RBAC は、アクセスポリシー、ロール、グループ、およびユーザーを作成することによって実現されます。

役割ベースのアクセス制御

February 6, 2024

Citrix Application Delivery Management（ADM）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）を提供します。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、あるユーザーにはすべてのネットワーク操作の実行を許可し、別のユーザーはアプリケーションのトラフィックフローを監視して構成テンプレートの作成を補助できるようにします。

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。役割は、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。Citrix ADM では、ロールとポリシーの作成は Citrix ADC の 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 証明書管理と監視機能への完全なアクセスが必要

ですが、システム管理操作については読み取り専用アクセスにする必要があります。アプリケーション管理者は担当する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。クリスはセキュリティ管理者、アプリケーション管理者、ネットワーク管理者という 3 つの管理者の役割を作成します。

セキュリティ管理者のデイビットは、SSL 証明書管理と監視への完全なアクセスが必要ですが、システム管理操作については読み取り専用アクセスにする必要があります。

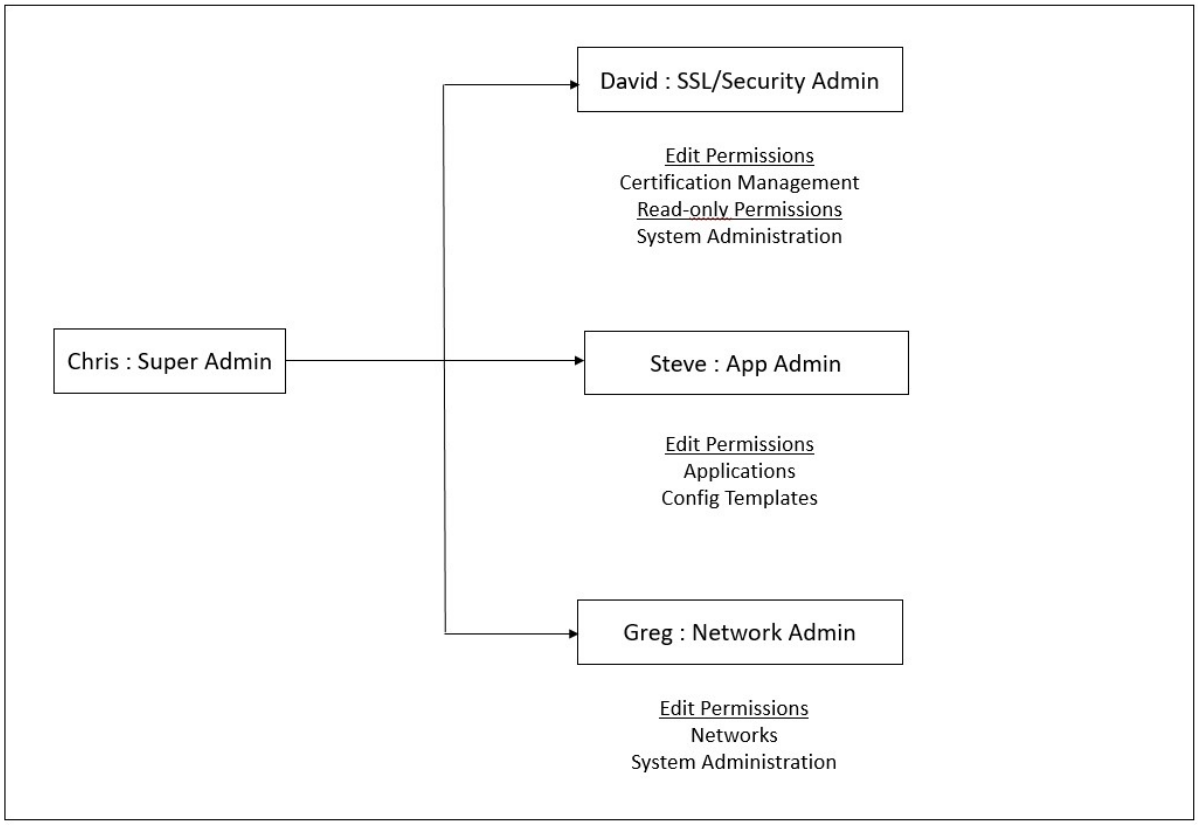
アプリケーション管理者のスティーブは、特定のアプリケーションと特定の構成テンプレートのみのアクセスが必要です。

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。

クリスは、ユーザーがローカルか、外部か、マルチテナントであるかに関わらずすべてのユーザーに RBAC を提供する必要があります。

NetScaler ADM ユーザーは、ローカルで認証されるか、外部サーバー（RADIUS/LDAP/TACACS）を介して認証されます。RBAC 設定は、採用される認証方法に関わらずすべてのユーザーに適用可能でなければなりません。

下図に、各種の管理者とほかのユーザーが持つ権限と社内での役割を示します。



制限事項

RBAC は、以下の Citrix ADM 機能については完全にはサポートされていません。

- **Analytics** -RBAC は、分析モジュールでは完全にサポートされていません。RBAC のサポートはインスタンスレベルに限定されており、Web Insight、SSL Insight、Gateway Insight、HDX Insight、および Security Insight の分析モジュールのアプリケーションレベルには適用できません。たとえば、以下のようなものです。

例 **1**: インスタンスベースの RBAC (サポート)

RBAC はインスタンスレベルでサポートされているため、いくつかのインスタンスを割り当てられた管理者は、**Web Insight >**Instance でそれらのインスタンスのみを表示でき ******、****Web Insight** > **Applications** で対応する仮想サーバーのみを見ることができます。

例 **2**: アプリケーションベースの RBAC (サポート対象外)

いくつかのアプリケーションを割り当てられている管理者は、[**Web Insight**] > [アプリケーション] ですべての仮想サーバーを表示できますが、**RBAC** はアプリケーションレベルではサポートされていないため、アクセスできません。

- **StyleBook** —RBAC は StyleBook では完全にはサポートされていません。
  - Citrix ADM では、StyleBook と構成パックは個別のリソースと見なされます。アクセス権限（表示、編集、またはその両方）は、Stylebook と構成パックに個別または同時に提供できます。構成パックの表示権限または編集権限によって、ユーザーに対して暗黙的に StyleBook の表示が許可されます。StyleBook の表示は構成パックの詳細取得や新しい構成パックの作成に不可欠です。
  - 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：インスタンスにすでに構成パックがある場合、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 Citrix ADC インスタンスの構成を変更できます。
- オーケストレーション -RBAC はオーケストレーションではサポートされていません。

アクセスポリシーの構成

February 6, 2024

アクセスポリシーでは、権限が定義されます。ポリシーは、1 人のユーザーや 1 つのグループ、または複数のユーザーやグループに適用できます。Citrix Application Delivery Management（ADM）には、4 つの定義済みアクセスポリシーがあります。

1. 管理ポリシー。Citrix ADM のすべての機能へのアクセスを許可します。ユーザーには表示権限と編集権限があり、すべての NetScaler ADM コンテンツを表示でき、すべての編集操作を実行できます。つまり、ユーザーはリソースに対して追加、変更、削除の操作を実行できます。

2. 読み取り専用ポリシー。読み取り専用権限を付与します。ユーザーは Citrix ADM のすべてのコンテンツを表示できますが、操作を実行する権限はありません。
3. アプリ管理ポリシー。NetScaler ADM アプリケーション機能にアクセスするための管理権限を付与します。このポリシーにバインドされているユーザーは、カスタムアプリケーションを追加、変更、削除できるほか、サービス、サービスグループ、および各種仮想サーバー（コンテンツスイッチ、キャッシュリダイレクト、および HAProxy 仮想サーバーなど）を有効または無効にできます。
4. アプリ読み取り専用ポリシー。アプリケーション機能に対する読み取り専用権限を付与します。このポリシーにバインドされているユーザーはアプリケーションを表示できますが、追加、変更、削除、有効化、および無効化の操作は実行できません。

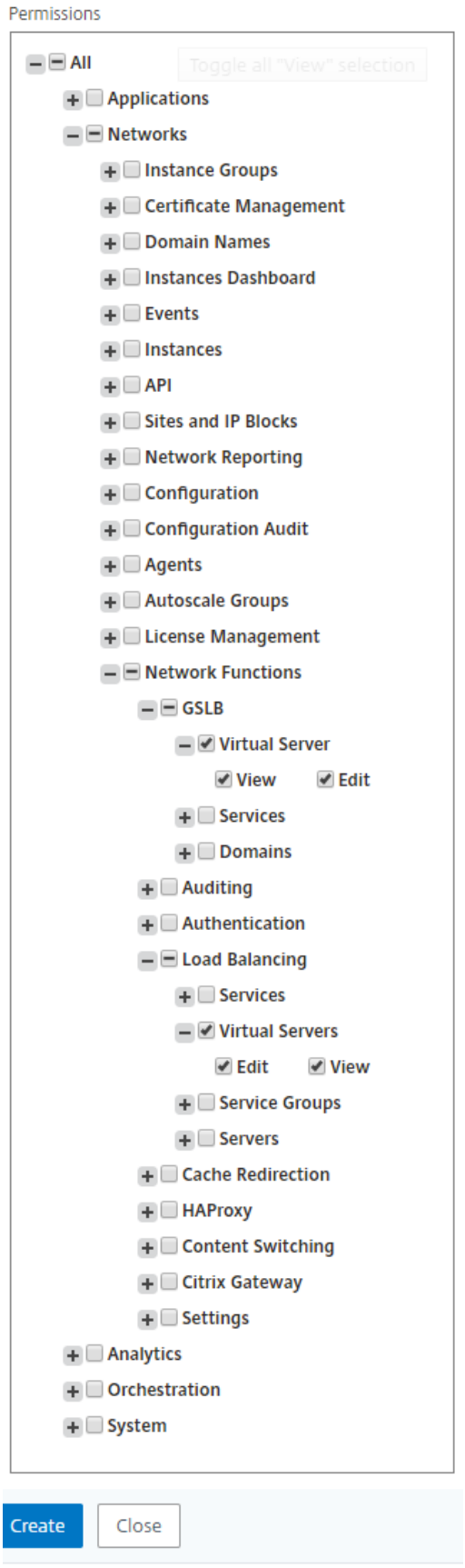
> 注**:** 定義済みのポリシーは編集できません。

また、ユーザーは独自の（ユーザー定義の）ポリシーを作成できます。

ユーザー定義のアクセスポリシーを作成するには、次の手順を実行します。

1. Citrix ADM で、［システム］>［ユーザー管理］>［アクセスポリシー］に移動します。
2. ［追加］をクリックします。
3. 「ポリシー名」フィールドにポリシーの名前を入力し、「ポリシーの説明」フィールドに説明を入力します。
4. 権限セクションには、Citrix ADM のすべての機能と、読み取り専用または編集アクセスを指定するオプションが一覧表示されます。［+］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。ユーザーに表示権限または編集権限を付与するには、機能名の横にあるチェックボックスを選択する必要があります。［Edit］オプションには表示権限も含まれます。読み取り専用の場合は [表示] を選択し、フルアクセスの場合は [編集] を選択します。

   > 注: 負荷分散と GSLB を展開すると、その他の設定オプションが表示されます。

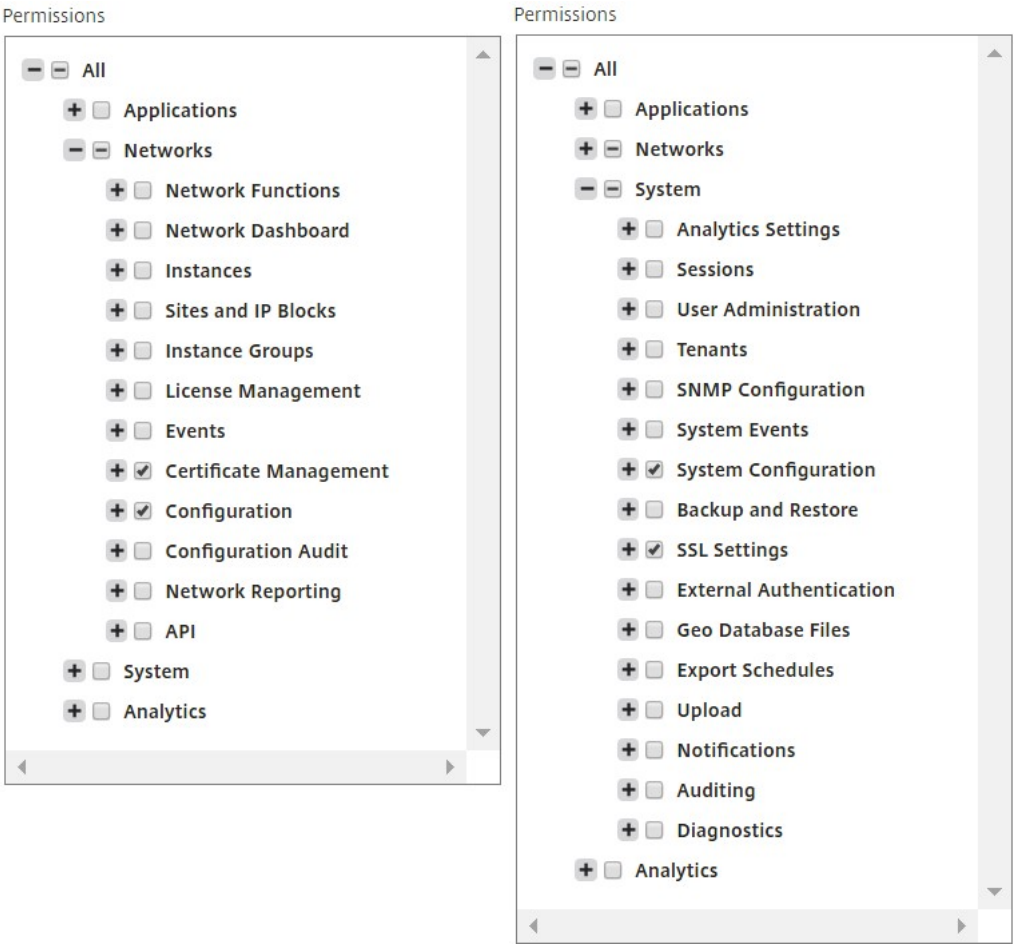


> 注: [編集] を選択すると、[権限] セクションで有効と表示されていない従属権限が内部的に割り当てられる場合があります。たとえば、障害管理の編集権限を有効にすると、NetScaler ADM は、メールプロファイルの構成または SMTP サーバー設定の作成のためのアクセス許可を内部的に提供します。これにより、ユーザーはレポートをメールとして送信できます。

例:

デビッドは、Citrix ADM の SSL 証明書管理/セキュリティの管理者です。David に割り当てられたポリシーでは、管理者は権限セクションの次のチェックボックスを選択します。

- **[**ネットワーク ****] > [**** 構成] > [編集]
- **[**ネットワーク ****] > [**** 証明書管理] > [編集]
- システム > **SSL** 設定 > 編集
- **[**システム ****] > [**** システム構成] > [編集]



5. ［作成］をクリックします。

グループの構成

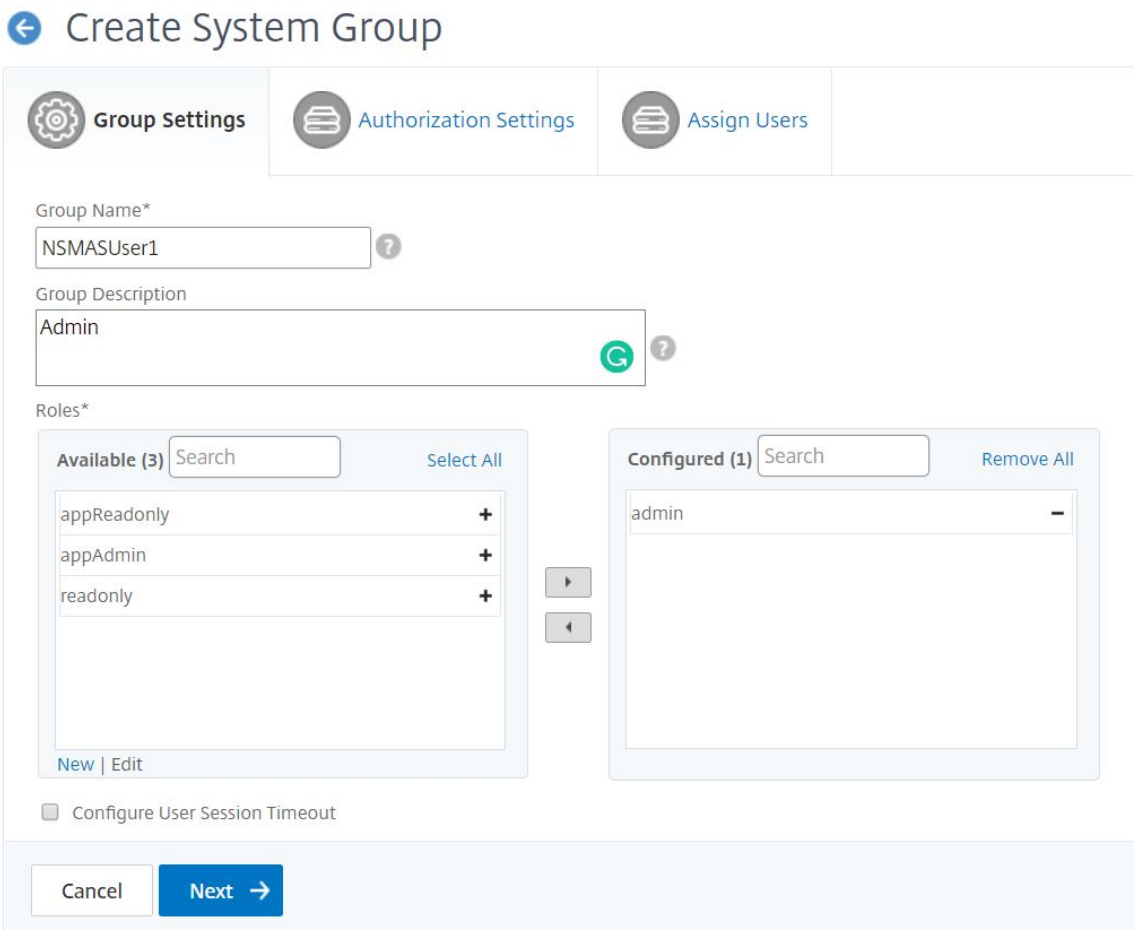
February 6, 2024

Citrix Application Delivery Management（ADM）では、グループは機能レベルとリソースレベルの両方のアクセス権を持つことができます。たとえば、あるユーザーグループは選択した Citrix ADC インスタンスにのみアクセスでき、別のグループは選択した少数のアプリケーションにのみアクセスできる、というような場合があります。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。

ユーザーグループを作成し、ユーザーグループにロールを割り当てるには:

1. NetScaler ADM で、［システム］>［ユーザー管理］>［グループ］に移動します。
2. ［追加］をクリックします。
3. [グループ名] フィールドに、グループの名前を入力します。
4. 「グループの 説明 」フィールドに、グループの説明を入力します。グループについてわかりやすい説明をしておくと、後でグループの役割と機能をよりよく理解するのに役立ちます。
5. [ロール] セクションで、1 つ以上のロールを [構成済み] リストに追加または移動します。

> 注**:** 「使用可能」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、**[**** システム] > [ユーザー管理**] > [**ユーザー] に移動し、ユーザーを作成または変更することもできます。**



> 注
>
> [新規] をクリック して新しいロールを作成するか、 [システム] > [ユーザー管理] > [ユーザー] に 移動 し て、この画面から新しいユーザーを作成できます。

6. [次へ] をクリックします。 「認証設定」タブでは、次の 4 つのグループの承認設定を指定できます。

   - インスタンス
   - アプリケーション
   - 構成テンプレート
   - StyleBook

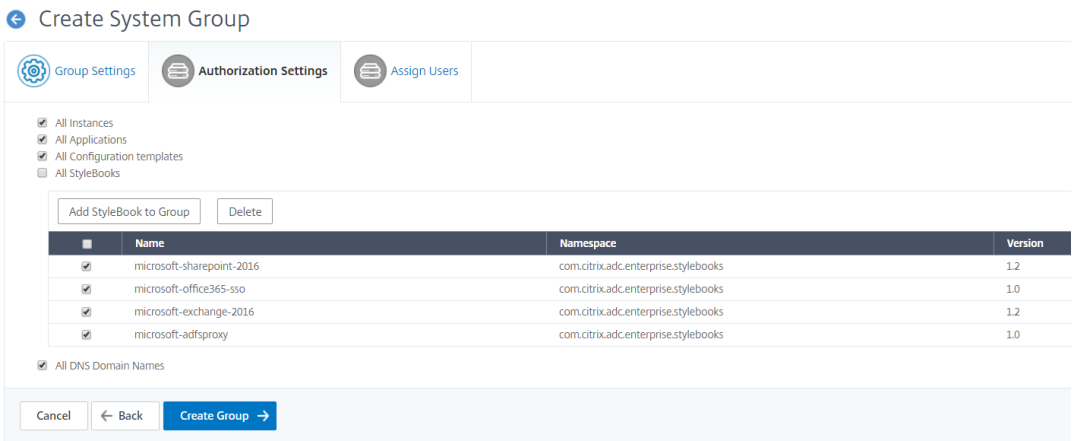
   デフォルトでは、ユーザーは上記のすべてのグループにアクセスできます。チェックボックスをオフにして、これらの各グループに選択的にアクセスできるようにすることができます。

   次に例を示します:

   - [インスタンス] チェックボックスをオフにして、ユーザーにアクセス権を付与する必要なインスタンスのみを選択できます。

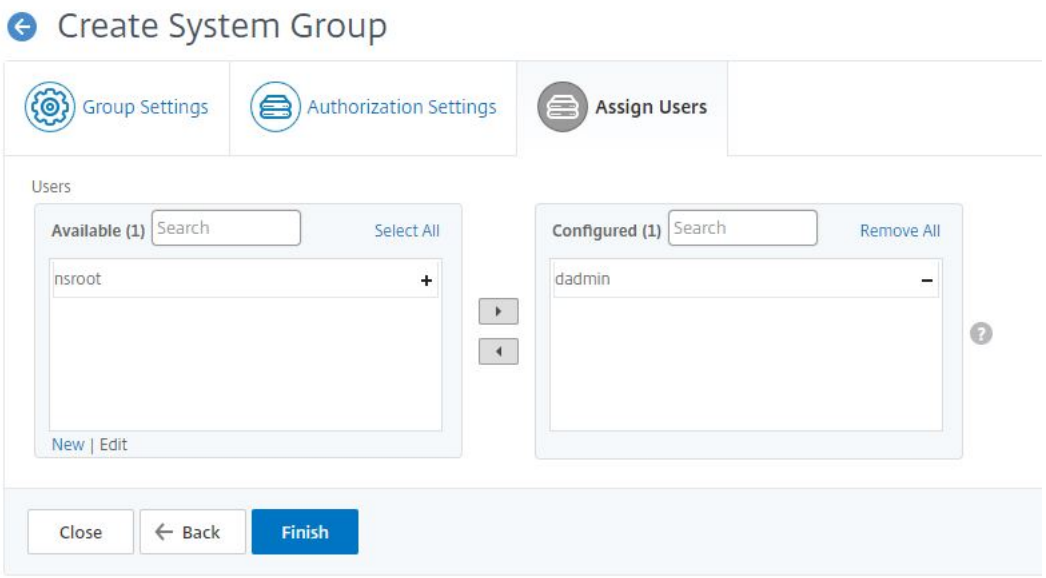
- [すべてのアプリケーション] チェックボックスをオフにし、必要なアプリケーションとテンプレートのみを選択します。Citrix ADM のグループにアプリケーションを追加すると、正規表現を使用して、グループの正規表現条件を満たすアプリケーションを検索して追加できます。これらのグループにバインドされているユーザーは、それらの特定のアプリケーションにのみアクセスできます。指定された正規表現式は、NetScaler ADM に保持されます。つまり、Citrix ADM では、「正規表現の追加」テキストボックスに 入力された正規表現 をシステムに保存し、新しいアプリケーションがこの正規表現を満たすたびに認証範囲を動的に更新します。新しいアプリケーションがシステムに追加されると、Citrix ADM は新しいアプリケーションに検索条件を適用し、条件を満たすアプリケーションがグループに動的に追加されます。新しいアプリケーションを手動でグループに追加する必要はありません。アプリケーションはシステム内で動的に更新され、各グループのユーザーは、NetScaler ADM 適切なモジュールの下にあるアプリケーションを表示できます。
- 必要 なテンプレート のみにアクセスできるようにするには、「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ます。
- すべての **StyleBooks** チェックボックスをオフにして、ユーザーがアクセスできる必要な StyleBook を選択します。

  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。その StyleBook の設定パックは、ユーザーがアクセスできるものにも含まれています。



- **All DNS Domain Names** チェックボックスをオフにして、ユーザーにアクセスさせたいドメイン名をリストから追加します。

7. [**Create Group**] をクリックします。
8. 「ユーザーの割り当て」タブで、「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。たとえば、「管理者」などです。



> 注**:** 「新規」をクリックして新しいユーザーを追加することもできます。

9. [完了] をクリックします。

> 注:
>
> Citrix ADM 管理者は、RBAC のアクセスポリシー設定に基づいて、個々の ADM モジュール UI の「表示専用」権限または「表示および編集」権限のいずれかをユーザーに提供できます。ユーザーが 2 つ以上のグループに割り当てられている場合、つまりユーザーが内部で複数の承認スコープと複数のアクセスポリシーにマップされている場合、ADM はそれらすべてのグループの権限を結合して、それに応じてユーザーを承認します。
>
> たとえば、User1 が P1 と P2 の 2 つのアクセスポリシーを持つグループに割り当てられているとします。各ポリシーには異なる種類の権限があります。P1 には「読み取り専用」権限があり、P2 には「表示と編集」権限があります。ユーザーに P1 ポリシーの一部として一連のアプリケーションを表示させ、P2 ポリシーの一部として別のアプリケーションセットを編集できるようにしたいと考えています。ただし、デフォルトの動作として、Citrix ADM は 2 つの権限タイプを組み合わせて、「表示と編集」権限をユーザーに割り当てます。これで、ユーザーはすべてのアプリケーションを表示および編集できるようになります。
>
> ADM は、同じユーザーに異なる種類の権限を割り当てることができるようなユースケースをサポートしていません。ユーザーには 1 種類の権限のみを割り当てることができます。ADM では、User1 にすべてのアプリまたは選択したアプリセットの表示を許可するか、User1 にすべてのアプリまたは選択したアプリセットの表示と編集を許可できます。

Citrix ADM を **12.0** から **12.1** にアップグレードする場合の **RBAC** のマッピング

Citrix ADM 12.0 から 12.1 にアップグレードすると、グループの作成時に「読み取り/書き込み」または「読み取り」権限を提供するオプションが表示されません。これらの権限は「役割」と「アクセスポリシー」に置き換えられており、より柔軟に役割ベースの権限をユーザーに提供できます。次の表は、リリース 12.0 の権限がリリース 12.1 にどのようにマッピングされるかを示しています。

12.0	アプリケーションのみ許可	12.1
admin read-write	False	admin
admin read-write	True	appAdmin
admin read-only	False	readonly
admin read-only	True	appReadonly

役割の設定

February 6, 2024

Citrix Application Delivery Management（ADM）では、各ロールは 1 つ以上のアクセスポリシーにバインドされます。ポリシーと役割には、1 対 1、1 対多、多対多の関係を定義できます。1 つの役割を複数のポリシーにバインドすることも、複数の役割を 1 つのポリシーにバインドすることもできます。

たとえば、ある機能のアクセス権を定義するポリシーと別の機能のアクセス権を定義する別のポリシーの 2 つのポリシーに、1 つの役割をバインドできます。一方のポリシーでは、Citrix ADM に Citrix ADC インスタンスを追加する権限を付与し、もう一方のポリシーでは StyleBook を作成して展開し、Citrix ADC インスタンスを構成する権限を付与する場合があります。

複数のポリシーで 1 つの機能に編集権限と読み取り専用権限を定義する場合、編集権限が優先されます。

Citrix ADM には、次の 4 つの定義済みロールがあります。

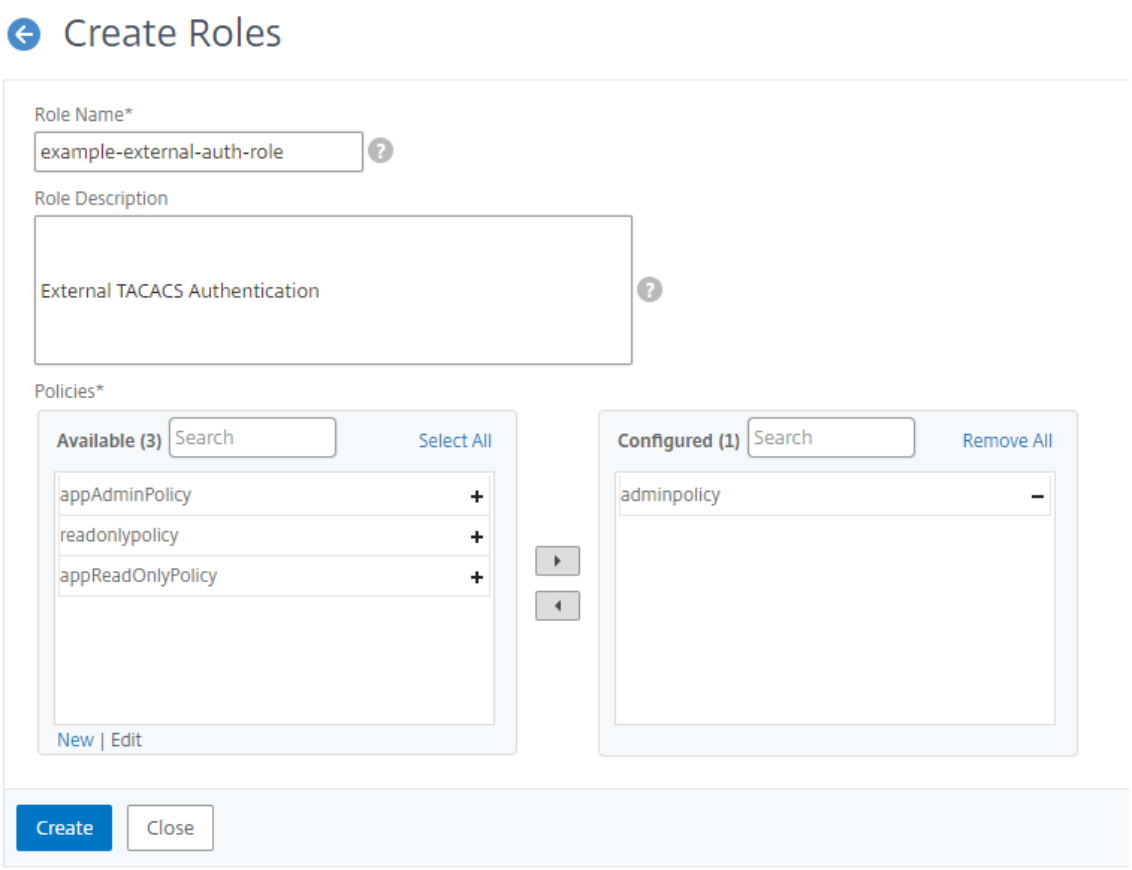
- 管理者。すべての NetScaler ADM 機能にアクセスできます。（この役割は adminpolicy にバインドされています）。
- 読み取り専用。読み取り専用アクセスが設定されています（この役割は readonlypolicy にバインドされています）。
- **appAdmin**。NetScaler ADM アプリケーション機能にのみ管理者権限が付与されます。（この役割は appAdminPolicy にバインドされています）。
- **appReadonly**。アプリケーション機能に対する読み取り専用アクセス権が設定されています（この役割は appReadOnlyPolicy にバインドされています）。

> 注: 定義済みのロールは編集できません。

また、独自の（ユーザー定義の）役割を作成することもできます。

ロールを作成してポリシーを割り当てるには、次の手順に従います。

1. Citrix ADM で、［システム］>［ユーザー管理］>［ロール］に移動します。
2. ［追加］をクリックします。
3. 「ロール名」フィールドにロールの名前を入力し、「ロールの説明」フィールドに説明を入力します (オプション)。
4. 「ポリシー」セクションで、**1** つ以上のポリシーを設定済みリストに追加または移動します。



5. ［作成］をクリックします。

ユーザーの構成

February 6, 2024

デフォルトでは、Citrix Application Delivery Management（ADM）には 1 人のユーザーがいます。

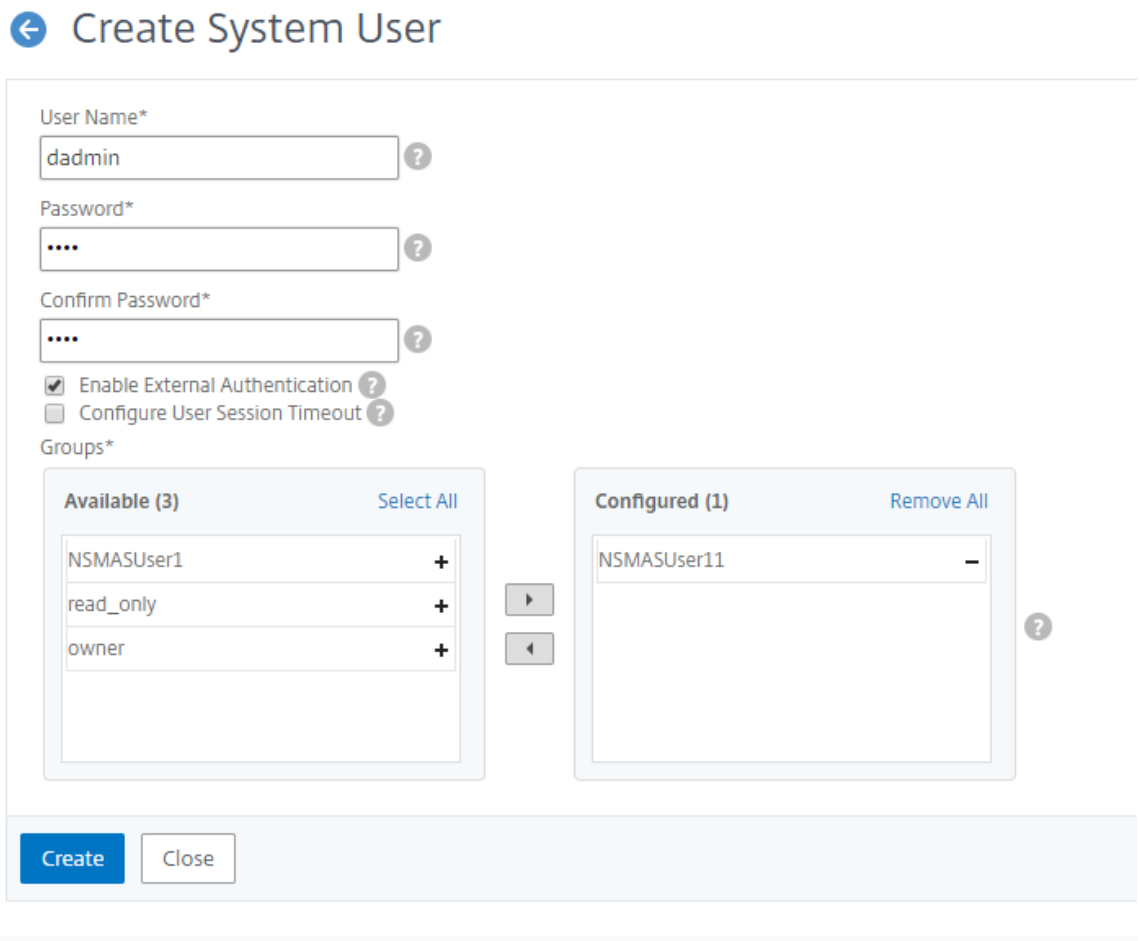
nsroot - ルートユーザー（nsroot）は、アプライアンスに対するすべての管理権限を持ちます。nsroot ユーザーは Citrix ADM のスーパー管理者です。

ユーザーは、アカウントを構成することで追加できます。Citrix ADM に新しいユーザーを追加するときは、適切なグループ、役割、およびポリシーを割り当てることによってそのユーザーの権限を定義できます。

ユーザーをグループに割り当てて、グループを複数の役割にバインドすることができます。ユーザー、グループ、役割、およびアクセスポリシーの間には、1 対 1、1 対多、多対多の関係を定義できます。複数のデスクトップを単一のユーザーに割り当てることができます。グループには複数の役割を設定することも、複数のグループに同一の役割を設定することもできます。

NetScaler ADM でユーザーを構成するには：

1. NetScaler ADM で、［システム］>［ユーザー管理］>［ユーザー］に移動します。
2. ［追加］をクリックします。
3. 次の詳細情報を入力します：
    a) ユーザー名。ユーザーの名前
    b) パスワード。ユーザーが Citrix ADM にログオンするときに使用するパスワード
4. 必要に応じて、「外部認証を有効にする」を選択して、外部認証サーバーを介してユーザーを認証できるようにします。
5. グループを作成していて、ユーザーをグループに割り当てたい場合は、「グループ」セクションで、**1** つ以上のグループを「使用可能」リストから「構成済み」リストに移動します。



6. ［作成］をクリックします。

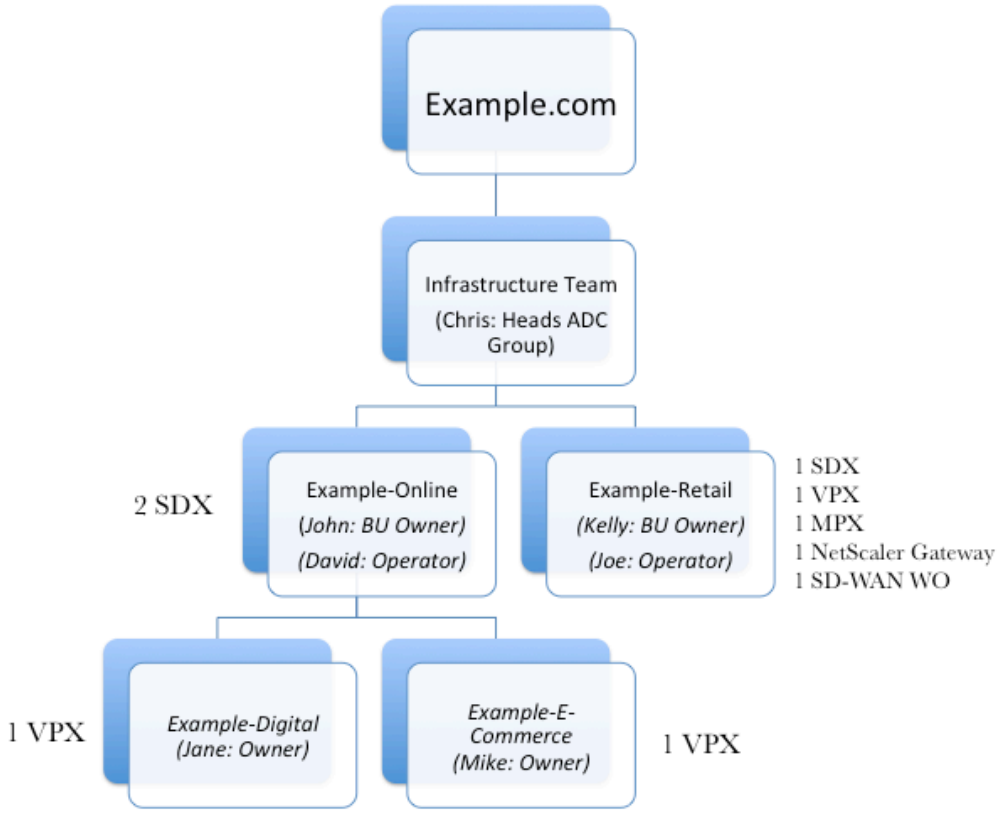
マルチテナンシー: テナント専用の管理環境を提供

February 6, 2024

CitrixApplication Delivery Management（ADM）は、複数のテナント向けにシステムを構成できるマルチテナント機能を提供します。各テナントは、ネットワーク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および監視、テナント固有のユーザーとグループの作成を実行できます。どのテナントも別のテナントのインスタンスとアプリケーションを見ることはできません。システム管理者のみ、すべてのテナントのすべてのインスタンス、アプリケーション、レポートを見ることができます。ただし、システム管理者でもテナントのユーザーを作成することはできません。すべてのシステムレベルのタスクはシステム管理者のみ実行できます。

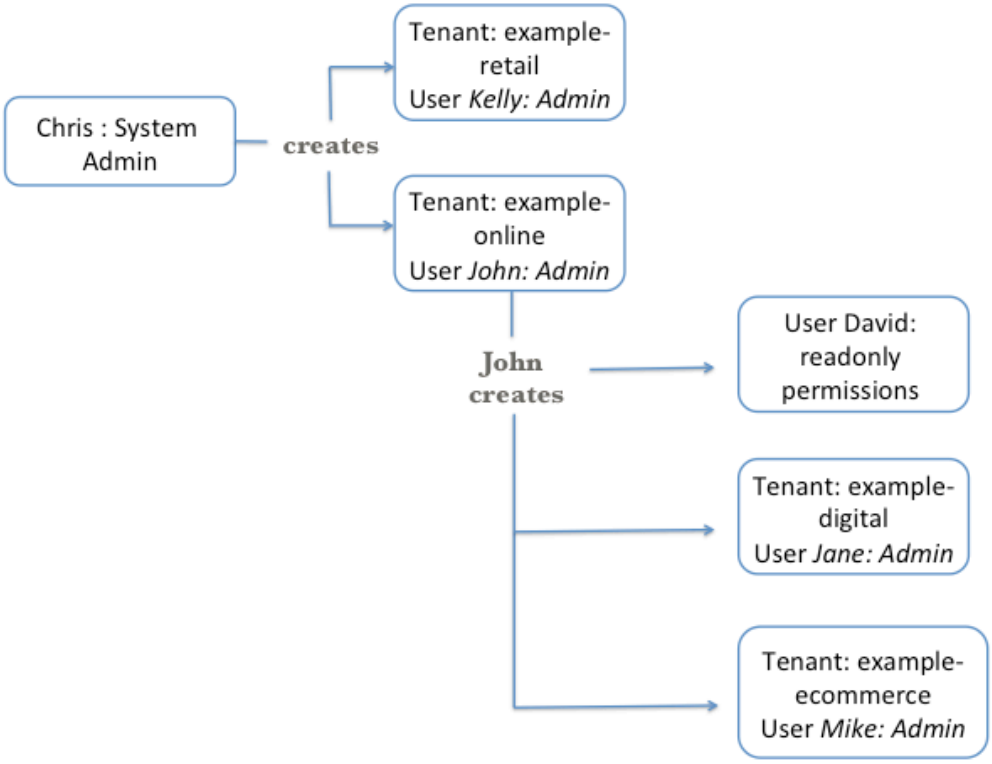
Example.com という組織に、1 つのインフラストラクチャグループと複数の事業単位が存在するケースを考えてみます。この組織では、ネットワーク内のすべてのインスタンスを一元管理する必要があります。ただし、事業単位ごとに排他的な環境を用意する必要があります。

下図に、example.com 組織のインフラストラクチャグループの構築方法を示します。4 つの各事業単位に排他的な管理環境を用意する必要があります。この図には、各事業単位の管理対象となるインスタンス数も表示されています。



ADC グループ長であるクリスは、NetScaler ADM システム管理者です。クリスは、2 つの事業単位用に、2 つのテナント、Example-online と Example-Retail を作成し、これらのテナントの管理者として 2 人のユーザーを割り当てます。各テナント管理者は、ユーザーの追加、管理対象インスタンスの追加、テナント環境内でのサブテナントの作成を実行できます。

次の図は、この例で NetScaler ADM で作成されたテナントとユーザーを示しています。

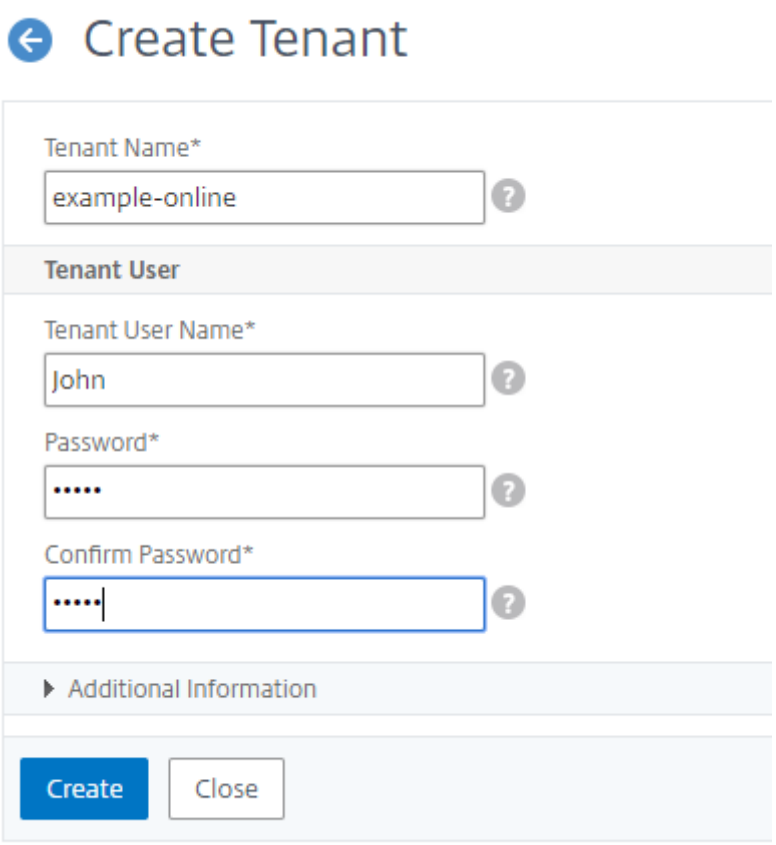


テナントの追加

この例では、システム管理者であるクリスが 2 つのテナント example-online と example-retail を作成します。テナントを作成するとき、クリスは各テナントのデフォルトの管理者ユーザーも作成します。

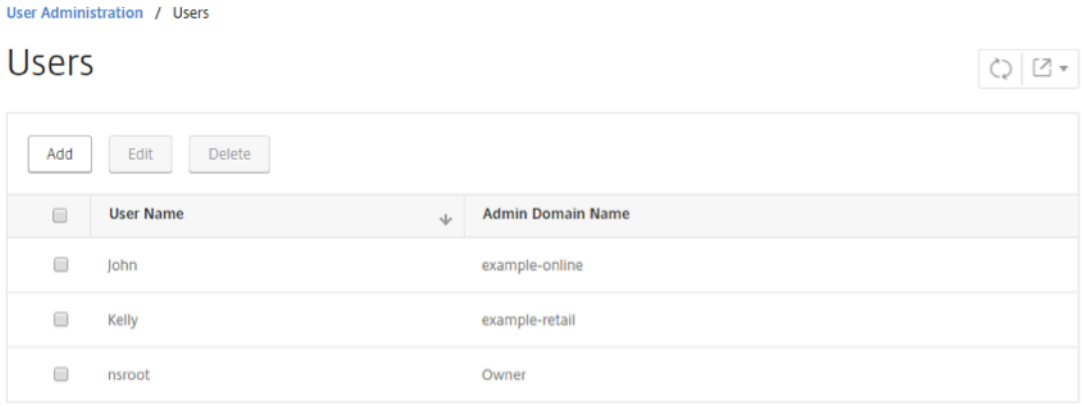
テナントを追加するには

1. [システム] > [テナント] に移動し、[追加] をクリックします。
2. テナントの作成ページで、このテナントの管理者として割り当てるテナント名とテナントユーザー名を指定します。パスワードも指定します。
3. ［作成］をクリックします。



[テナント] ページでは、作成されるテナントのリストを表示できます。

[** システム] > [ユーザー管理] > [ユーザー] ページで、各テナントの管理ユーザー の一覧を表示することもできます。****

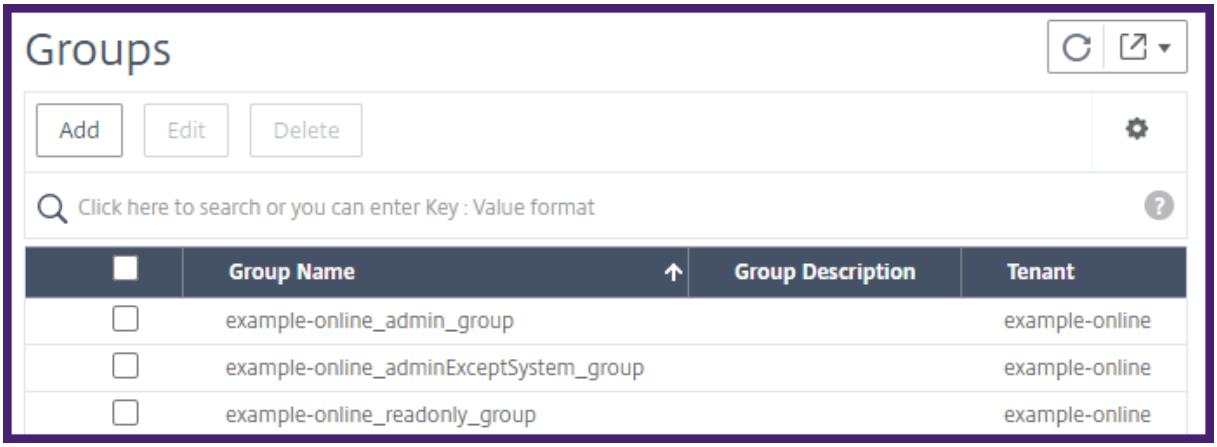


テナントを作成すると、管理者グループ、adminExceptSystem_Group、および読み取り専用グループの 3 つの既定のシステムグループが作成されます。

例:

example-online テナントには次のデフォルトグループがあります。

- `example-online_admin_group`
- `example-online_adminExceptSystem_group`
- `example-online_readonly_group`

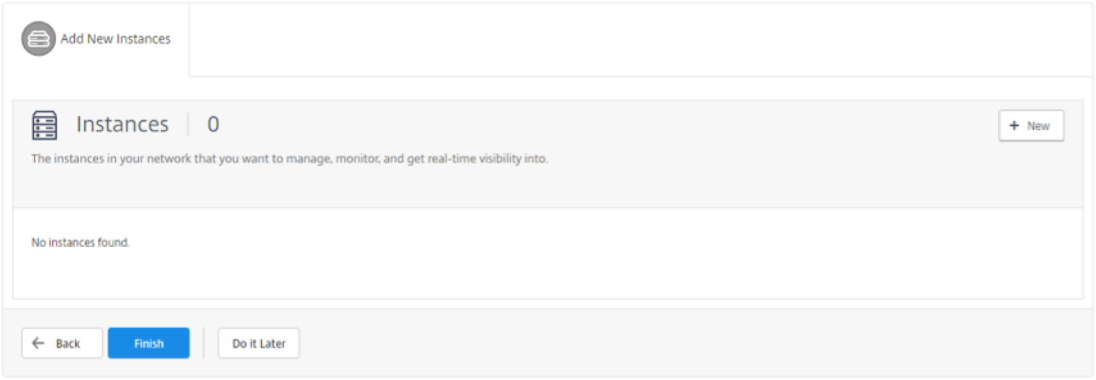


テナントユーザーとして **NetScaler ADM** にログオンする

テナントが作成されると、テナントユーザーはテナントユーザーの資格情報を使用して Citrix ADM にログオンできます。ログオンするには、テナントのドメイン名とユーザー名の両方を指定する必要があります（例: example-online\John）。

テナントユーザーとしてインスタンスを追加する

テナントがログオンすると、Citrix ADM はテナントにインスタンスの追加を促します。[**+ New**] をクリックして、管理対象のインスタンスを追加します。または、[Do it Later] をクリックして、インスタンスを後で [Infrastructure] タブから追加することもできます。詳しくは、「*NetScaler ADM* へのインスタンスの追加」を参照してください。



この例では、ジョンは 2 つの NetScaler ADC SDX インスタンスを追加します。

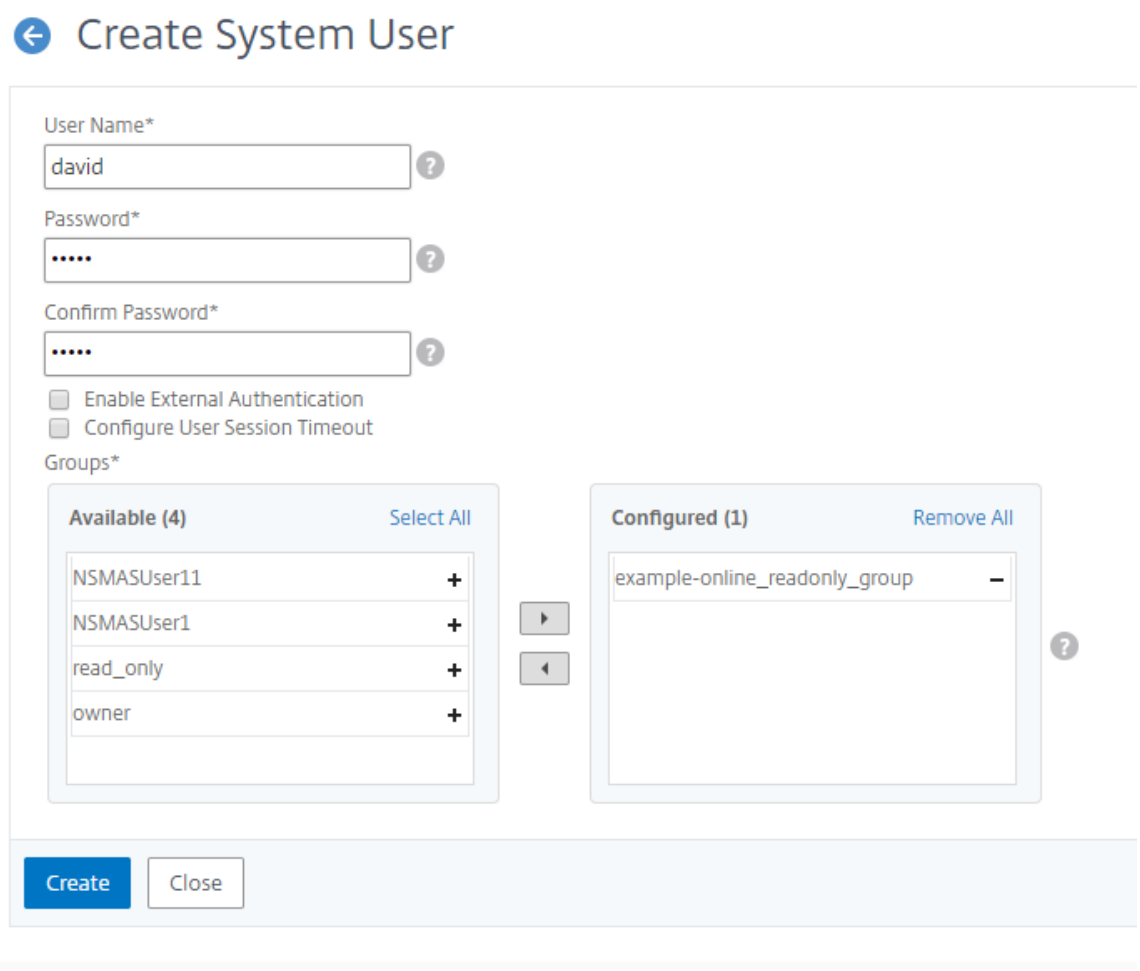
Citrix ADM がインスタンスにアクセスするために使用できるインスタンスタイプ、IP アドレス（カンマで区切る）、およびプロファイル名を指定し、「**OK**」をクリックします。

ユーザーの作成

テナント管理者のジョンは、ユーザーとしてデイビットを作成して、デイビッドがこのテナントのすべてのインスタンスとアプリケーションを監視できるようにしたいと考えています。ただし、クリスは、インスタンスに対するすべての構成タスクの実行またはテナントのシステム設定の変更をデイビッドに行わせたくありません。そこで、クリスは、読み取り専用アクセス許可を持つユーザーとしてデイビッドを作成します。

ユーザーを作成するには、次の手順に従います。

1. [システム] > [ユーザー管理] > [ユーザー] に移動し、[追加] をクリックします。
2. [システムユーザーの作成] ページで、作成するユーザーのユーザー名とパスワードを指定します。
3. [グループ] で、このユーザーに割り当てるグループを選択します。この例では、example-online_readonly_group をデイビッドに割り当てています。

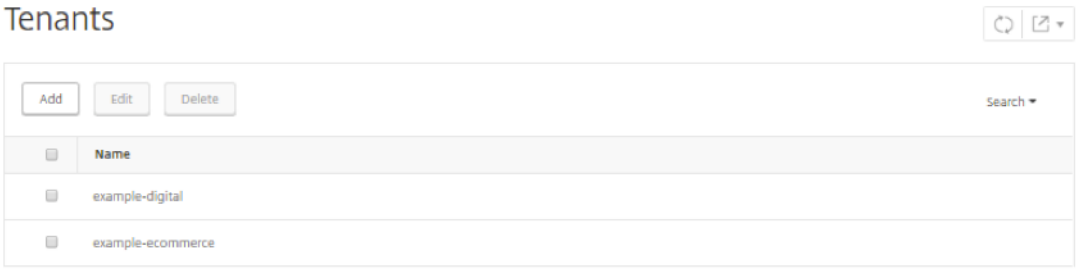


テナント内のテナントの作成

テナント管理者は、テナントをさらに分割したい場合にサブテナントを作成できます。ただし、作成できるサブテナントは 1 階層のみです。この例では、ジョンが、2 つのサブテナント、example-digital と example-ecommerce を作成しています。これら 2 つのサブテナントを作成するときに、クリスはジェーンとマイクを管理ユーザーとして、それぞれのサブテナントに割り当てています。

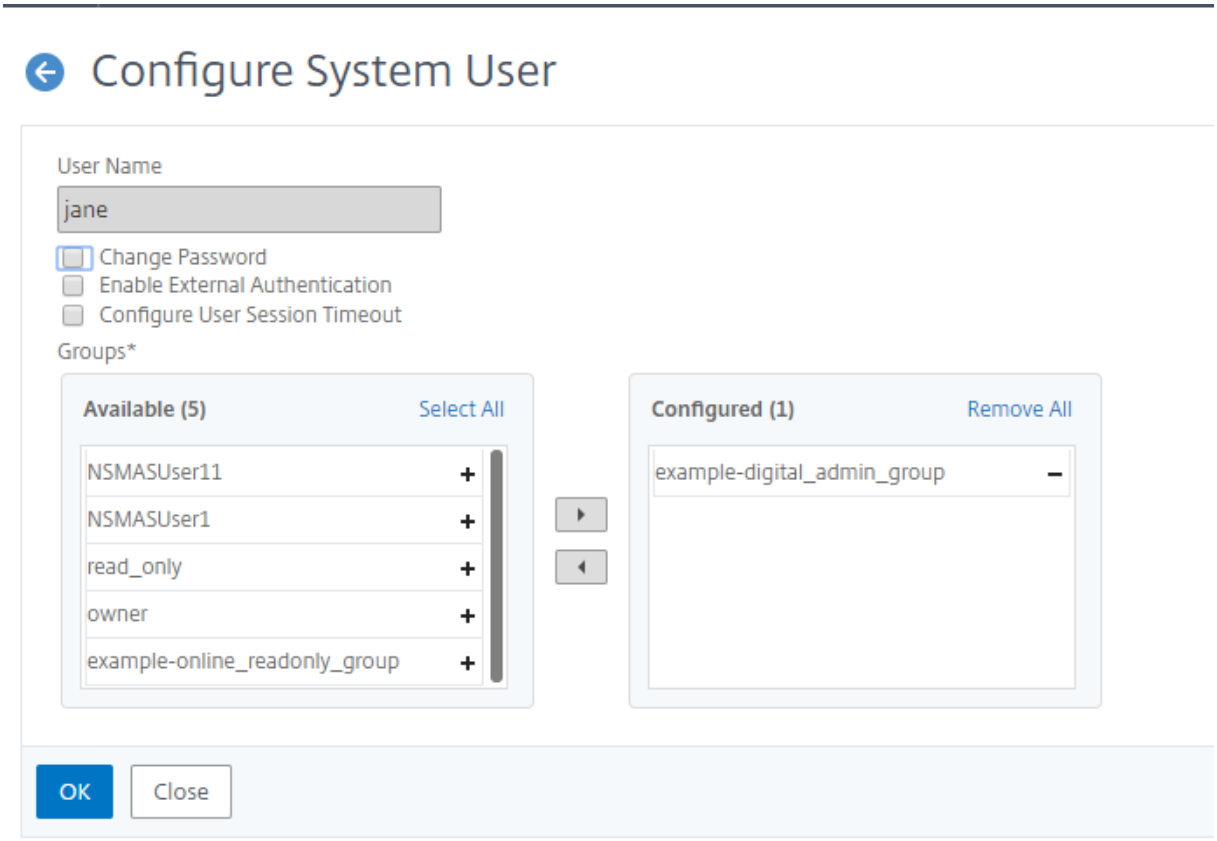
テナント内にテナントを作成するには、「テナントの追加」で説明されている手順に従います。

作成したテナントは、**[**テナント**]** ページで表示できます。



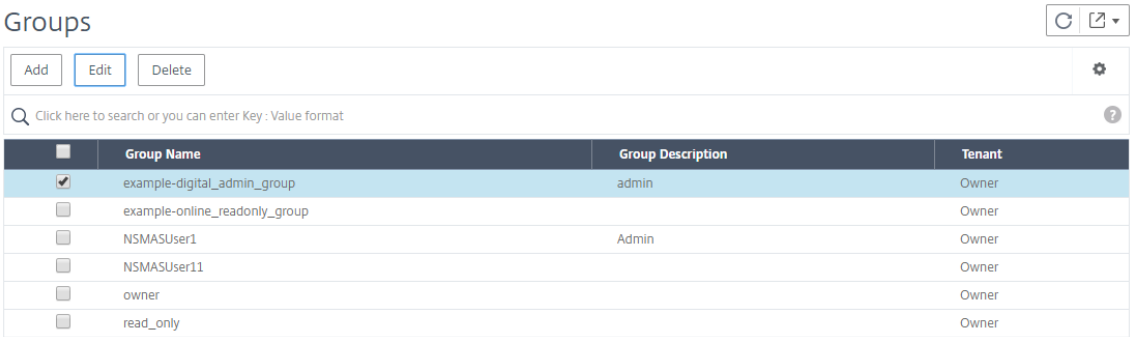
ユーザーに割り当てられたアクセス許可を確認することもできます。[システム] > [ユーザー管理] > [ユーザー] に移動し、ユーザーを選択して [編集] をクリックします。

「システムユーザーの設定」ページの「グループ」で、そのユーザーに割り当てられているグループを表示できます。この例では、example-digital_admin_group がジェーンに割り当てられていることがわかります。

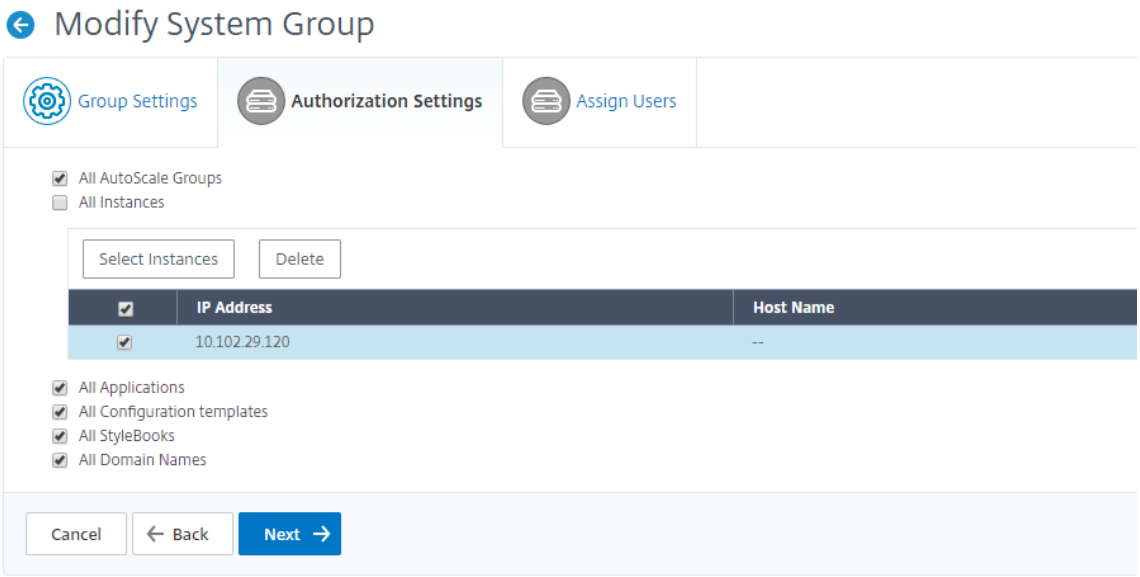


Citrix ADM にインスタンスをすでに追加している場合は、テナント管理者として、テナントまたはサブテナントのユーザーにインスタンスを割り当てて管理および監視することができます。たとえば、ジョンは、1 つの VPX インスタンスを管理用にジェーンに割り当てることができます。

1. [システム] > [ユーザー管理] > [グループ] に移動します。
2. ユーザーが割り当てられているグループを選択し、[**Edit**] をクリックします。



3. [システムグループの変更] ページの [承認設定] タブで、[すべてのインスタンス] チェックボックスをオフにします。



4. ユーザーが管理するインスタンスを選択し、[**Select Instances**] をクリックします。
5. [次へ]、[完了] の順にクリックします。

アプリケーション

February 6, 2024

NetScaler ADM のアプリケーション分析と管理機能は、アプリケーション中心のアプローチを強化し、さまざまなアプリケーション配信の課題に対処するのに役立ちます。この方法ではアプリケーションの正常性スコアが視覚的に表示されるため、セキュリティ上のリスクを判断し、アプリケーションのトラフィックフローにおける異常を検出して、適切な措置を講じることができます。

次の図は、アプリケーション管理と分析で実行できるさまざまなタスクの概要を示しています。

アプリケーションは、検出されたアプリケーション、HAProxy アプリケーション、またはカスタムアプリケーションのいずれかです。

検出されたアプリケーション

管理対象のすべての仮想サーバーに自動的に作成されるアプリケーション。検出済みのアプリケーションには常に 1 台の仮想サーバーがあり、これらのアプリケーションを直接編集したり削除することはできません。

カスタムアプリケーション

検出済みのアプリケーションからユーザーによって作成されたアプリケーション。Citrix ADM では、これらのアプリケーションを追加、編集、削除できます。カスタムアプリケーションは以下によって作成されます。

- 1 つ以上の仮想サーバー
- 1 つ以上の HAProxy フロントエンド。

カスタムアプリケーションを作成すると、カスタムアプリケーションに追加されたすべての検出されたアプリケーションがアプリケーションダッシュボードから削除されます。

注意事項

- 検出されたアプリケーションを複数のカスタムアプリケーションに追加することはできません。
- すべての検出済みのアプリケーションが既に他のカスタムアプリケーションに割り当てられている場合は、カスタムアプリケーションを作成できません。既存のカスタムアプリケーションを削除して検出済みのアプリケーションの割り当てを解除し、新しいカスタムアプリケーションの作成で使用できるようにする必要があります。
- 仮想サーバーと HAProxy フロントエンドを含むカスタムアプリケーションは作成できません。

HAProxy アプリケーション

HAProxy ディスクリートアプリケーションは、マネージド HAProxy フロントエンドごとに自動的に作成されます。これらのアプリケーションをグループ化して、NetScaler ADC アプリケーションと同様のカスタムアプリケーションを形成することもできます。詳しくは、「Citrix ADM による HAProxy インスタンスの管理と監視」を参照してください。

注意事項

以下のアプリダッシュボード機能またはメトリクスは HAProxy アプリケーションではサポートされていません。

- User Activity Investigator
- App Score
- 脅威指数
- ピーク使用量トレンド
- スループット
- サーバー接続
- トランザクション

カスタムアプリケーションの作成

アプリケーションの定義時に 1 つまたは複数の検出済みのアプリケーションを追加することで、カスタムアプリケーションを作成できます。

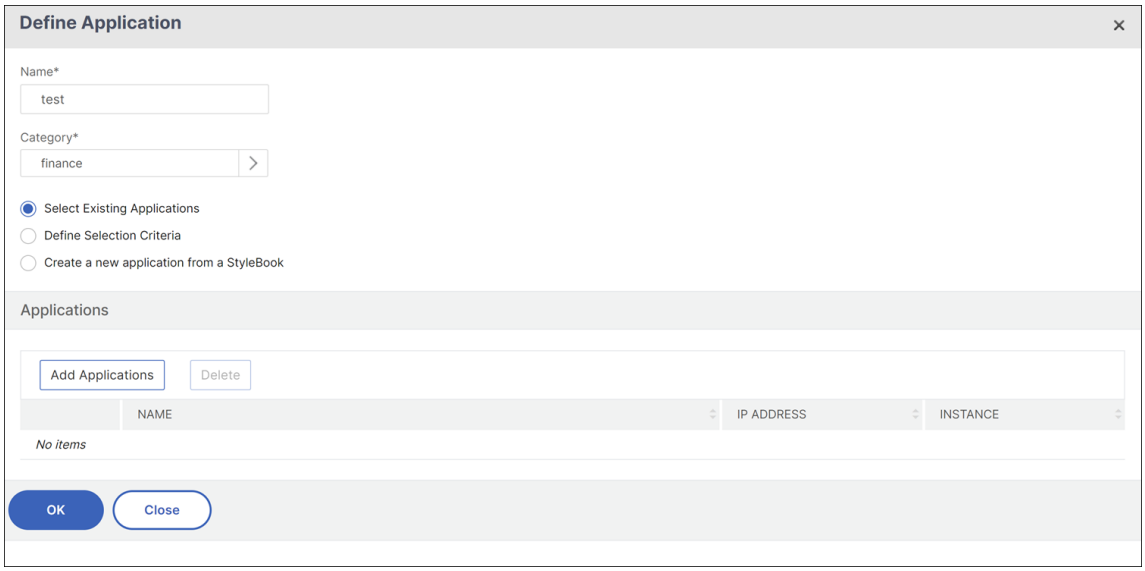
カスタムアプリケーションを作成するには**:**

1. [アプリケーション] > [ダッシュボード] に移動し、[カスタムアプリの定義] をクリックします。
2. アプリケーションの定義画面で、次のパラメーターを設定します。

フィールド	説明
名前	カスタムアプリケーションの名前
カテゴリ	このカテゴリに関連するすべてのアプリケーションが、アプリケーションダッシュボードでグループ化されるカテゴリの名前。
既存のアプリケーションの選択	定義基準が Citrix ADM によって監視されるライセンス仮想サーバーに基づいている場合は、仮想サーバーを追加するオプション。
選択条件の定義	仮想サーバーの範囲、または元のサーバー/サービスの IP アドレスの範囲でアプリケーションを定義するオプション。 • サーバー。アプリケーションが動作するサーバーかサービスの IP アドレス、サーバー名、またはバックエンドサーバーのポートを指定します。1 つの IP アドレスか IP アドレスの範囲、またはコンマ区切りでそれらを組み合わせて入力できます。たとえば、「10.102.29.20, 10.102.43.10-60, 10.216.43.45」と入力します。 • 仮想サーバー。アプリケーションが動作する仮想サーバー IP アドレス、仮想サーバー名、バックエンドサーバーのポートのいずれかを指定できます。1 つの IP アドレスか IP アドレスの範囲、またはコンマ区切りによるそれらの組み合わせで入力できます。たとえば、「10.102.29.20, 10.102.43.10-60, 10.216.43.45」と入力します。

3. [OK] をクリックします。

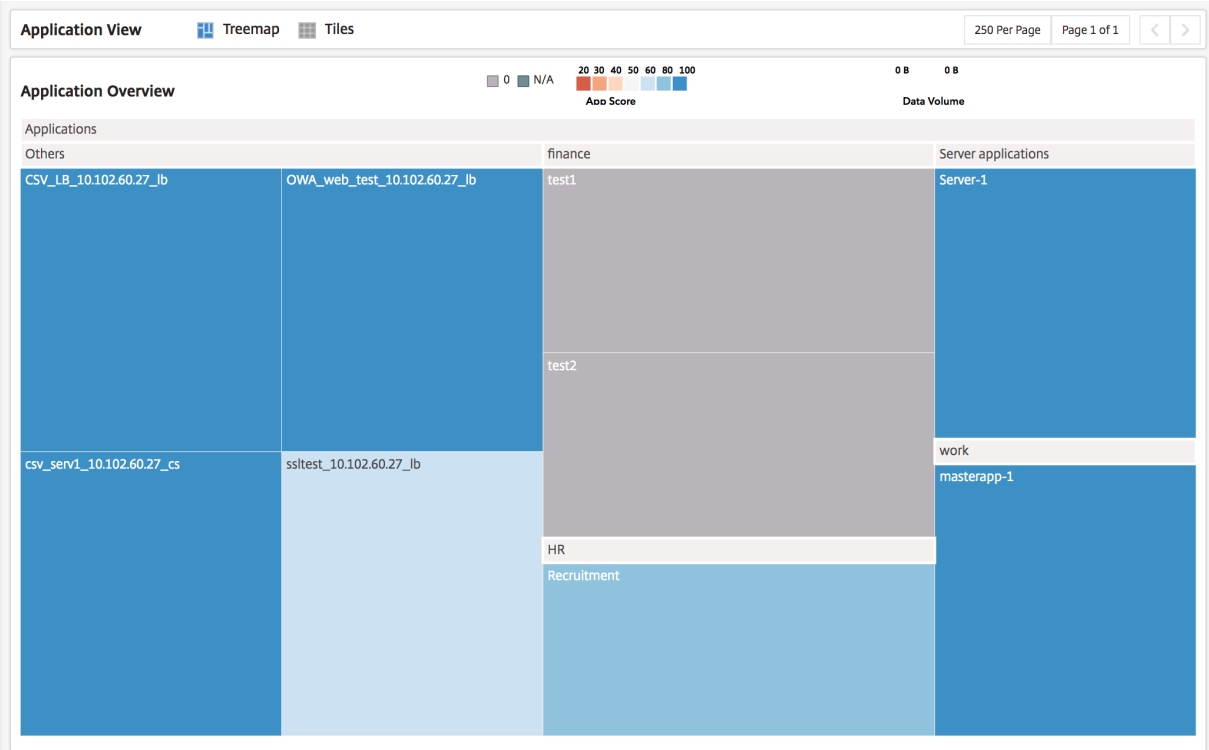
> 注
>
> 現在、Application Dashboard では、負荷分散とコンテンツスイッチング仮想サーバーのみがサポートされています。



アプリケーションをグループ化

アプリケーションをグループ化すると、アプリケーションの管理と監視を簡略化できます。アプリケーションを定義するときにカテゴリーを選択または作成して、アプリケーションをグループ化できます。カテゴリを作成または選択するには、アプリケーションを定義するときに、「カテゴリ」フィールドの 横 ** にある「」ボタンをクリックします。

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、「その他」カテゴリに表示されます。



アプリケーションダッシュボード

アプリケーションダッシュボードには、Citrix ADM によって監視されているすべてのアプリケーションの全体像が表示され、すべてのアプリケーションに関連する重要な情報が表示されます。たとえば、ダッシュボードには、パフォーマンスおよびセキュリティの測定基準、カウンター、アプリケーションのヘルス状態が表示されます。特定のアプリケーションに関する情報を表示するには、該当するアプリケーションを選択します。[Summary] パネルに、監視対象のすべてのアプリケーションのアプリスコアや脅威指数などの測定基準が棒グラフで表示されます。

アプリケーションの表示

アプリケーションダッシュボードでは、アプリケーションはツリーマップ上のノードとして表示され、そのサイズはアプリケーションのデータボリュームに応じて決まります。タイルの色はアプリケーションのアプリスコアを表し、赤色の場合は正常性が最も低く、青色の場合は正常性が良好であることを表します。

アプリケーションダッシュボード画面からオプションのいずれかを選択すると、アプリケーションダッシュボードビューをツリーマップまたはタイルに切り替えることができます。この画面では、アプリケーションの詳細がカード形式で表示されます。デフォルトでは、250 のアプリケーションがアプリケーションダッシュボードに表示されます。さらに多くのアプリケーションを表示するには、次のページのオプションをクリックします。

アプリケーションは、アプリケーションの定義時に選択したカテゴリ別にグループ化されます。アプリケーションを分類または表示するには、アプリケーションの [Summary] パネルでアプリケーションの測定基準を選択します。たとえば、アプリスコアの範囲が 20～40 のアプリケーションを表示するには、[App Summary Panel] の [App

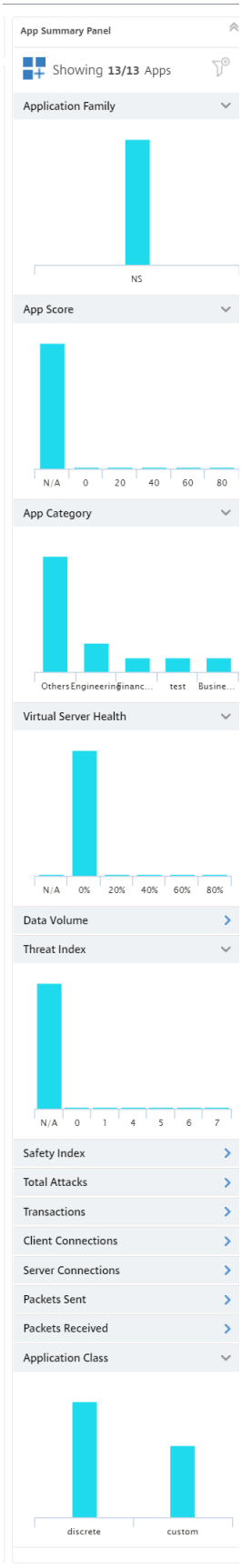
Score］セクションで適切な棒グラフを選択します。［App Summary Panel］では同様にその他の測定基準も選択できます。

アプリ概要パネル

［App Summary Panel］には、アプリケーションダッシュボードに表示されているアプリケーションのすべての測定基準が表示されます。このパネルでは、アプリケーションの測定基準を選択または選択解除することで、ダッシュボード上のアプリケーションを分類して表示することができます。［App Summary Panel］には次の測定基準が表示されます。

メトリックス	説明
アプリケーションファミリー	構成されている Citrix ADC インスタンスのタイプに応じてアプリケーションの数をグループ化する棒グラフ。
App Score	アプリケーションのパフォーマンスを定義するスコアリングシステム
アプリカテゴリ	Citrix ADM で定義されているすべてのカテゴリのヒストグラムを表示する棒グラフ。これで、すべての個別のアプリケーションが「その他」カテゴリに表示され、カスタムアプリケーションはそれぞれのカテゴリ名の下に表示されます。
仮想サーバーヘルス	各カテゴリのアプリケーション数を示す棒グラフ。アプリケーションは、ヘルススコアの値が 0%、20%、40%、60%、80%、100%に分類されます。
データ量	アプリケーションのデータ量に応じてアプリケーションの数をグループ化するスコアリングシステム。データ量は、アプリケーションが要求した合計バイト数と、アプリケーションからの応答として受信したバイト数によって計算されます。
脅威指数	アプリケーションが Citrix ADC アプライアンスによって保護されているかどうかに関係なく、アプリケーションに対する攻撃の重要度を示す 1 桁の評価システム。
安全性指数	外部からの脅威や脆弱性からアプリケーションを保護するために、NetScaler ADC インスタンスをどのように安全に構成したかを示す 1 桁の評価システム。
攻撃総数	アプリケーションに対する攻撃の総数
トランザクション	アプリケーションが実行したトランザクションの範囲。
クライアント接続	アプリケーションによって確立されたクライアント接続の数。

メトリックス	説明
サーバー接続	アプリケーションによって確立されたサーバー接続の数。
送信済みパケット	アプリケーションが送信したパケットの数。
受信済みパケット	アプリケーションが受信したパケットの数。
アプリケーションクラス	個別のアプリケーションかカスタムアプリケーションかに応じて、アプリケーションの数をグループ化する棒グラフ。

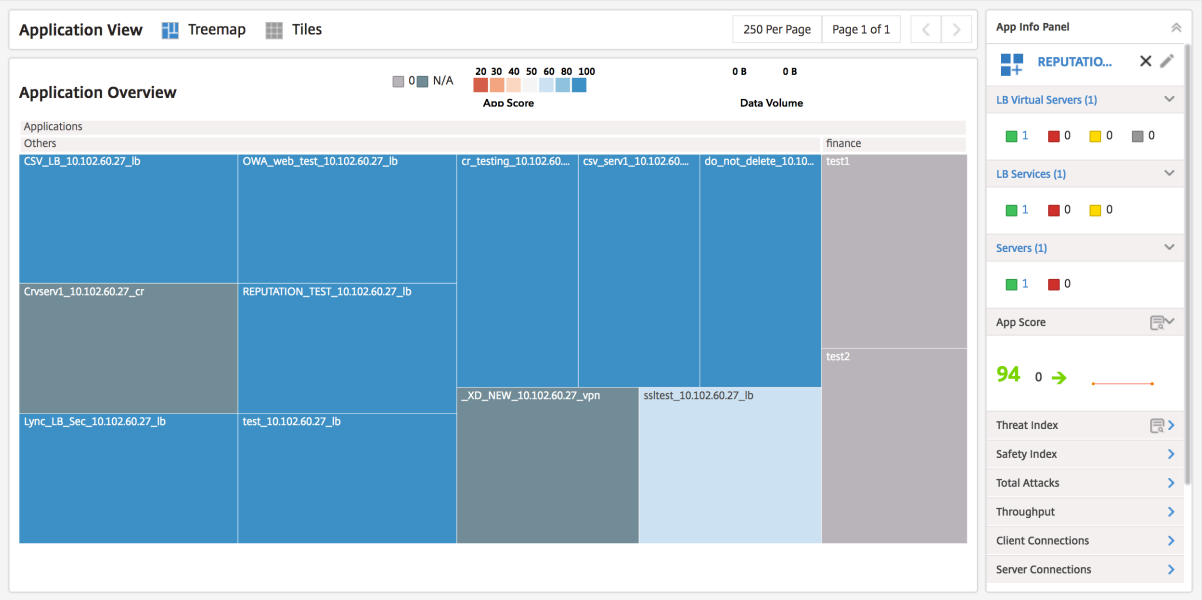


たとえば、アプリの概要パネルで下にスクロールすると、「仮想サーバーヘルス」の棒グラフが表示されます。仮想サーバーの正常性棒グラフでは、NetScaler ADM は仮想サーバーの正常性の割合に基づいてアプリケーションを分類します。棒グラフには、仮想サーバーのヘルス値が 0% ～100% の範囲にあるアプリケーションの数が表示されます。

仮想サーバーの状態は、個別のアプリケーションにグループ化された仮想サーバーの状態を表します。ただし、複数の仮想サーバで構成されるカスタムアプリケーションがある場合は、グループ間で仮想サーバのヘルスの最小数が考慮されます。

これで、フィルタを適用し、選択条件に一致するアプリケーションのみをアプリケーションダッシュボードに表示できます。0% と表示されているバーをクリックします。このバーには、仮想サーバーの正常性が 0% から 20% の間にあるアプリケーションの数が表示されます。仮想サーバーの状態が悪いアプリケーションを分離し、修復対策を講じることができるようになりました

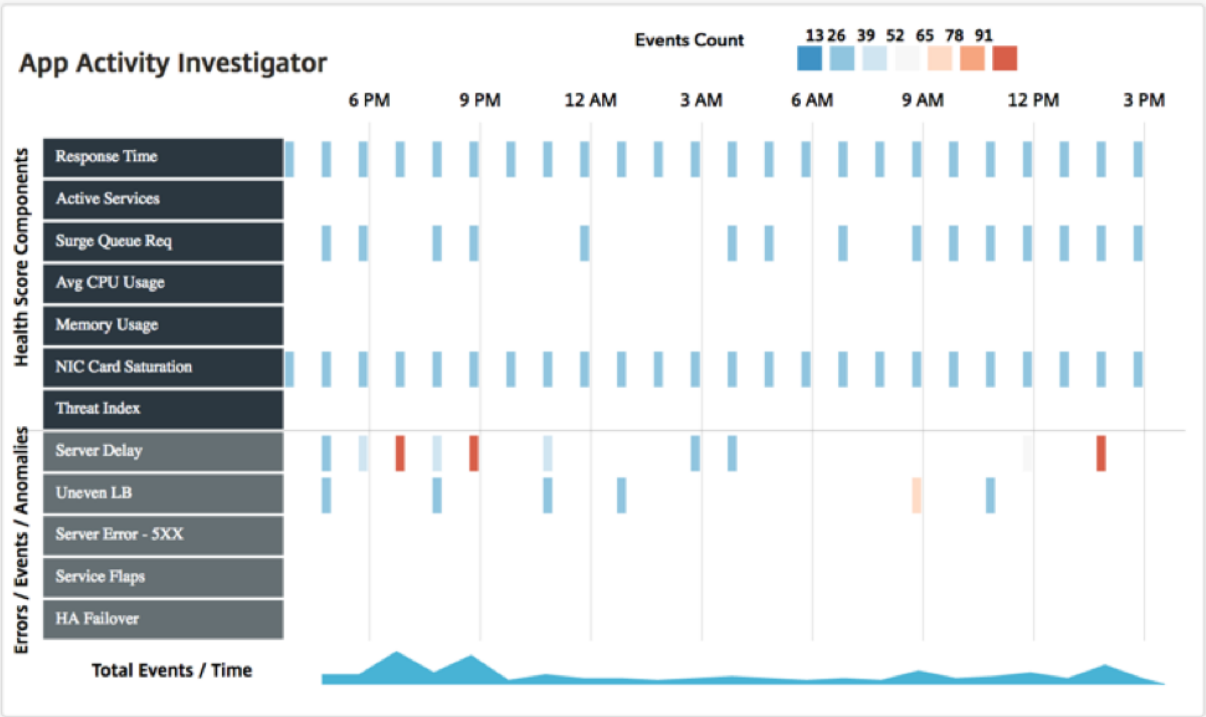
アプリ情報パネル　［App Info Panel］は、アプリケーションをドリルダウンすると最初のレベルにあります。アプリケーションの状態とともに、主要な測定基準とコンポーネントが表示されます。たとえば、［App Info Panel］には、選択したアプリケーションの仮想サーバーの合計数、サービスの合計数、アプリスコア、およびその他の情報が表示されます。［App Info Panel］を表示するには、アプリケーションダッシュボードで任意のアプリケーションタイルをクリックします。［App Summary Panel］が［App Info Panel］に置き換わります。



App activity investigator　App Activity Investigator は、アプリケーションからドリルダウンするときの 2 番目のレベルの 1 つです。App Activity Investigator に到達するには、［App Info Panel］で検索アイコンをクリックするか、アプリケーションダッシュボードでアプリケーションタイルをダブルクリックします。

App Activity Investigator には、App Score のコンポーネント、エラー、イベント、異常などの主要な情報が表示されます。

凡例はそれぞれ、選択した期間が 1 時間の場合は 1 分間隔、選択した期間が 1 日の場合は 1 時間間隔で集計されます。



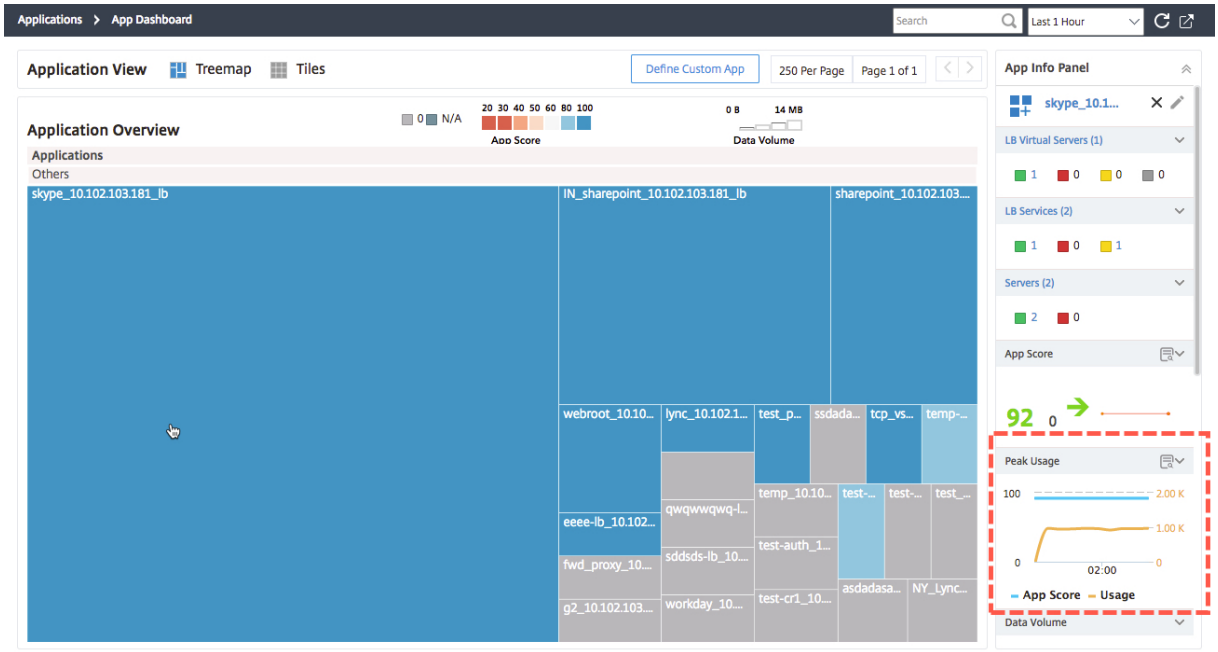
これらの偏差は、グラフ上に長方形の凡例として表示されます。集計された凡例は、イベントの発生回数に応じて色分けされます。青色はイベント数が最も少ないことを表し、赤色は最も多いことを表します。凡例にマウスポインターを重ねると、選択した凡例について集計されたエラーの種類、時間、イベント数などの詳細情報が表示されます。グラフの期間は、期間のボックスの一覧から時間を選択することでカスタマイズできます。

アプリの使用傾向　ほとんどの場合、ビジネスオーナーは、統計とデータに基づいてアプリケーションの有効性と使用傾向に関する決定を下します。アプリケーションの使用傾向を理解するには、バックエンドインフラストラクチャ、プロキシ、CDN ネットワークなど、デプロイメント内の複数のエンティティからの情報を照合する必要があります。次に、収集した情報を相互に関連付けて適切な分析を行います。これには多くの時間がかかります。

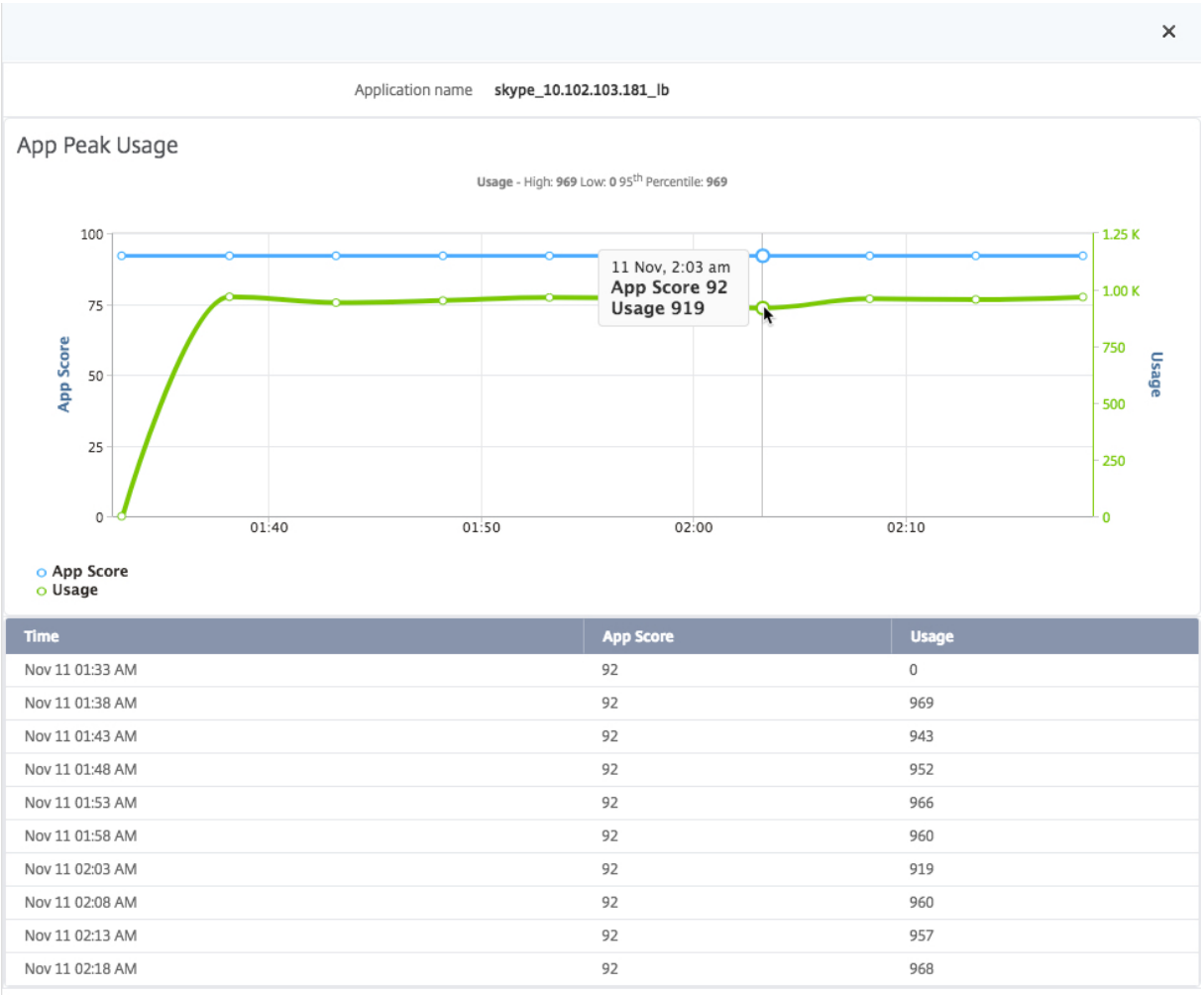
代わりに、展開環境で ADC として展開された Citrix ADC アプライアンスには、アプリケーションに関するすべての情報とアプリケーションの使用統計が含まれています。この情報は Citrix ADM に転送できます。Citrix ADM はこの情報を収集し、アプリケーションの使用状況とパフォーマンスに関する詳細な洞察を提供します。これらの洞察を活用して、アプリケーションの使用状況とパフォーマンスに基づいて効果的な意思決定を行うことができます。

アプリケーションダッシュボードのアプリ情報パネルには、アプリケーションのピーク使用傾向が表示されます。ピーク使用量の傾向を使用してアプリケーションのパフォーマンスを評価し、適切なアクションを実行して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。

アプリケーションのピーク使用傾向を確認するには、[アプリケーション] **>** [アプリケーションダッシュボード] に移動します。アプリケーションを選択すると、アプリケーション情報パネルの [ピーク使用量] セクションにアプリケーションのピーク使用量の傾向が表示されます。



さらに「ピーク使用量」セクションをクリックすると、アプリスコアとアプリケーションの使用状況が表示されます。この情報を使用して、アプリケーションのピーク使用量を特定し、それを対応するアプリスコアと関連付けて、ピーク使用期間におけるアプリケーションのパフォーマンスへの影響を評価できます。



Time	App Score	Usage
Nov 11 01:33 AM	92	0
Nov 11 01:38 AM	92	969
Nov 11 01:43 AM	92	943
Nov 11 01:48 AM	92	952
Nov 11 01:53 AM	92	966
Nov 11 01:58 AM	92	960
Nov 11 02:03 AM	92	919
Nov 11 02:08 AM	92	960
Nov 11 02:13 AM	92	957
Nov 11 02:18 AM	92	968

アプリダッシュボードとセキュリティダッシュボードのレポートのエクスポート

Citrix ADM では、現在のアプリケーションダッシュボードページとアプリケーションセキュリティダッシュボードページのスナップショットを取得し、レポートとしてエクスポートできます。頻繁な間隔で、アプリ管理者はこれらのレポートを使用して、アプリの使用状況やパフォーマンス上のペナルティについて更新する必要があります。

この機能により、管理者はこのデータを.png または.pdf レポートとして抽出できます。

> 注
>
> : Citrix ADM の他のレポートエクスポートオプションとは異なり、アプリダッシュボードレポートとセキュリティダッシュボードレポートは.pdf または.png ファイルとしてのみエクスポートできます。.jpg や.csv などの他のオプションは現在サポートされていません。

1. アプリケーションダッシュボードまたはアプリセキュリティダッシュボードページで、ページの右上にあるエクスポートアイコンをクリックします。
2. エクスポートオプションを.pdf または.png ファイルとして選択します。

3. [**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。アプリダッシュボードとアプリセキュリティダッシュボードページから、第 2 レベルのページに移動してレポートとしてエクスポートすることもできます。現在、一度に 1 つのアプリケーションのレポートしかダウンロードできません。

アプリケーション・パフォーマンス分析

February 6, 2024

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。アプリケーションの応答性が良好で、すべてのシステムが稼働しているかどうかがわかります。App Score は、アプリケーションレベルで表示されます。スコアの計算は、次の 3 つの主要なコンポーネントに基づいています。

- アプリパフォーマンススコア **(**アプリケーションの **APDEX** スコア**)**。アプリケーションのサーバー応答時間の変動から導出されます。
- **Citrix ADC** システムリソース。さらに 3 つのコンポーネントに基づいて派生しました。
  - CPU 使用率
  - メモリ使用率
  - NIC カードの飽和
- アプリケーションサーバーリソース。さらに 2 つのコンポーネントから派生しました。
  - アクティブなサービスの割合
  - サージキューの要求件数

アプリスコアは、NetScaler ADC システムリソーススコアとアプリサーバーリソーススコアがアプリパフォーマンススコアから差し引かれるこれらのスコアから計算されます。アプリケーションスコアは、検出された負荷分散およびコンテンツスイッチング仮想サーバーで定義されているすべてのアプリケーションと、アプリケーションダッシュボードで定義したカスタムアプリケーションで使用できます。

NetScaler ADM でアプリのスコアを構成するには:

1. Citrix ADM で、[アナリティクス] > [設定] に移動します。
2. [設定] ページで、[アプリスコアの構成] をクリックします。
3. [アプリスコアの構成] ページで、次のパラメータの値を入力します。
   a) サージキューしきい値の下限。仮想サーバーの送信保留中の接続の総数と確立された接続の比率の下限値。

b) サージキューのしきい値が高い。仮想サーバーおよび確立された接続の送信保留中の接続の合計数の比率の上限しきい値。

c) **CPU しきい値が低い (%) Citrix ADC インスタンスの合計 CPU 使用量の下限値。

d) **CPU** しきい値が高い **(%)**。Citrix ADC インスタンスの合計 CPU 使用率の上限値。

e) 低メモリしきい値 **(%)**。Citrix ADC インスタンスの合計メモリ使用量の下限値。

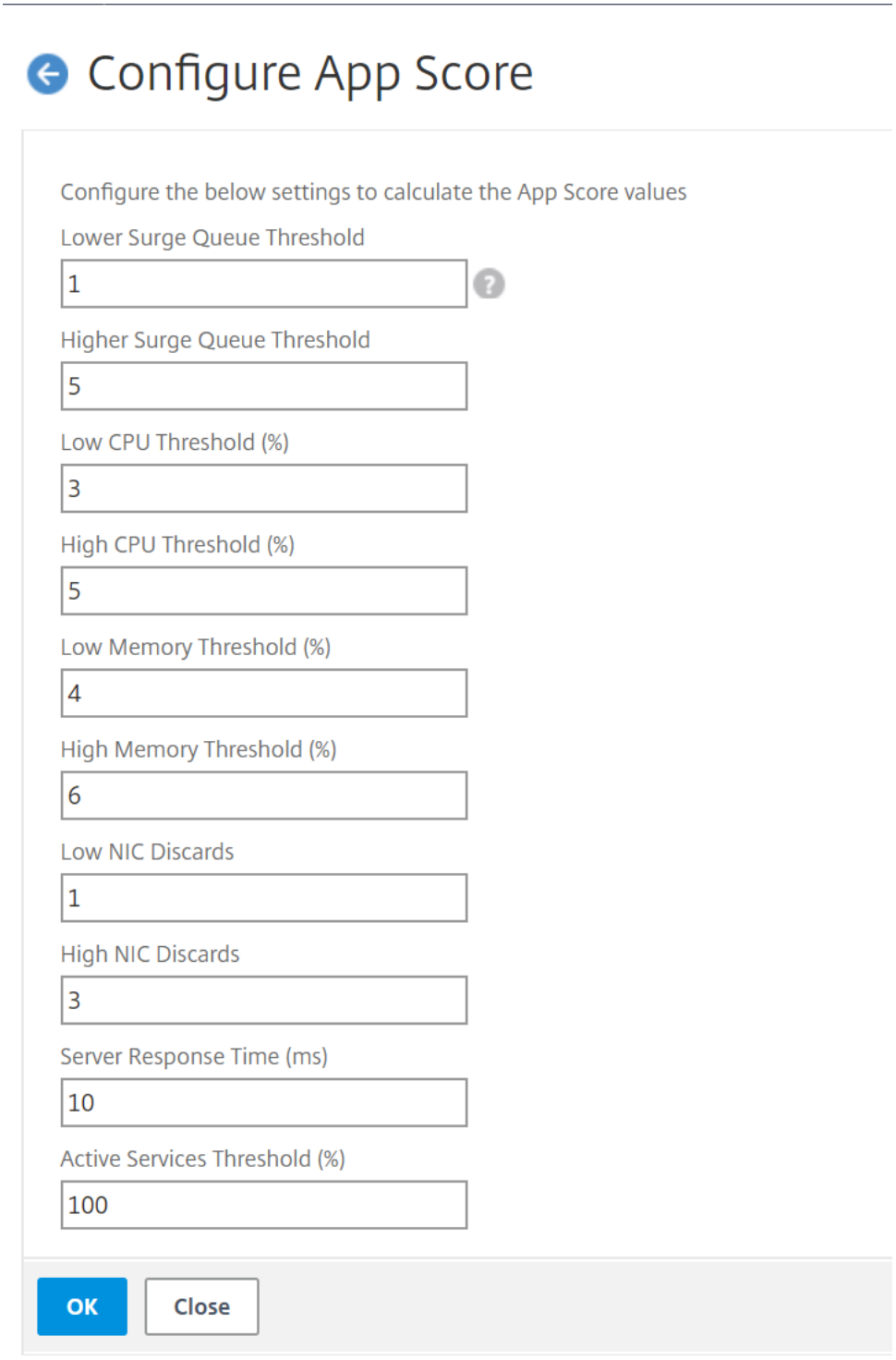
f) 高メモリしきい値 **(%)**。Citrix ADC インスタンスの合計メモリ使用量の上限値。

g) **NIC** の廃棄量が少なくなっています。インターフェイスによって廃棄されるパケットの下限しきい値。

h) **NIC** 廃棄率が高い。インターフェイスによって廃棄されるパケットのしきい値が高いほど。

i) 応答時間。要求パケットの送信から、仮想サーバ上で構成されたサービスからの最初の応答パケットを受信するまでの時間間隔。Citrix ADM で設定されているデフォルト値は 500 ミリ秒です。

j) アクティブサービスのしきい値。仮想サーバーにバインドされているアクティブでなければならないサービスのパーセンテージのしきい値。



4. [**OK**] をクリックします。

アプリケーション・セキュリティ分析

February 6, 2024

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 Citrix ADC インスタンスに対する同期攻撃、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。

> 注
>
> アプリセキュリティダッシュボードのメトリックを表示するには、監視対象の Citrix ADC インスタンスで AppFlow for Security Insight を有効にする必要があります。

Citrix ADC インスタンスのセキュリティメトリックをアプリセキュリティダッシュボードに表示するには:

1. Web ブラウザで、Citrix Application Delivery Management IP アドレス（例: http://192.168.100.1）を入力します。
2. [ユーザー名] と [パスワード] に、管理者の資格情報を入力します。
3. [アプリケーション] > **[**アプリケーションセキュリティダッシュボード**]** に移動し、[デバイス] ドロップダウンリストからインスタンスの IP アドレスを選択します。

グラフにプロットされた吹き出しをクリックして、App Security Investigator に報告された不一致をさらにドリルダウンできます。

アプリケーション定義の作成

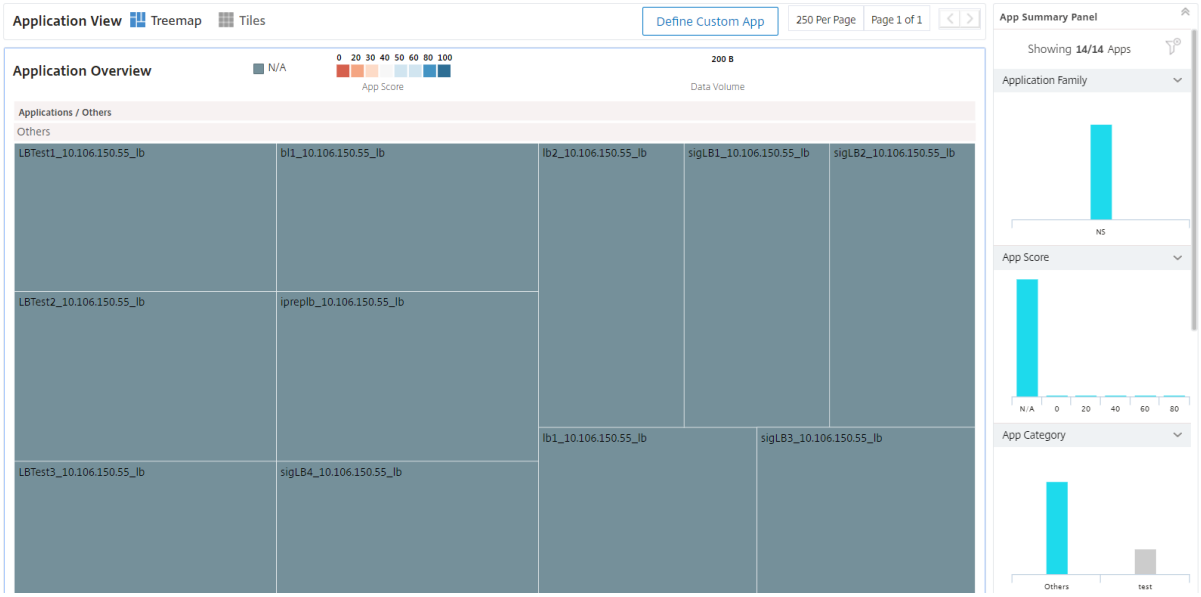
February 6, 2024

Citrix ADM で検出されたアプリケーションのコレクションに基づいてカスタムアプリケーションを定義できます。

Citrix ADM では、アプリケーションダッシュボードに移動すると、アプリケーション概要ページにデフォルトのアプリケーションが表示されます。これらのデフォルトアプリケーションまたは「個別のアプリケーション」は、デフォルトライセンスを持っている 30 のアプリケーションです。これらのアプリケーションは、ビジネス環境に Citrix ADM をインストールしたときにわかります。

「カスタムアプリケーション」を作成すると、個別のアプリケーションがカスタムアプリケーションに置き換わります。カスタムアプリケーションは、作成時に選択されたカテゴリに従って、ダッシュボードに配置されます。

検出された、およびカスタムの両方のアプリケーションはツリーマップと並べての 2 とおりの方法で表示できます。



静的または動的な構成によってカスタムアプリケーションを作成できます。

1. アプリケーションの静的定義 -静的定義では、アプリケーションを定義できます。この定義は、Citrix ADC インスタンスで新しい仮想サーバーを構成しても更新されません。さらに仮想サーバーを含めるには、このリストを手動で更新する必要があります。
2. アプリケーションの動的定義 -動的定義では、次の 3 つの基準のいずれかを使用してアプリケーションを定義できます。

   a) サーバー。サーバーまたはサービスの IP アドレス、サーバー名、またはアプリケーションが実行されているバックエンドサーバーのポートを指定します。1 つの IP アドレスか IP アドレスの範囲、またはコンマ区切りでそれらを組み合わせて入力できます。たとえば、「10.102.29.20, 10.102.43.10-60, 10.216.43.45」と入力します。

   b) 仮想サーバー。次のいずれかを指定できます。

      i. 仮想サーバーの IP アドレス

      ii. 仮想サーバ名、または

      iii. アプリケーションが実行されているバックエンドサーバーのポート。

   1 つの IP アドレスか IP アドレスの範囲、またはコンマ区切りによるそれらの組み合わせで入力できます。たとえば、「10.102.29.20, 10.102.43.10-60, 10.216.43.45」と入力します。

3. **StyleBook**。Citrix ADM にすでに存在するデフォルトまたはカスタムの StyleBook を使用してカスタムアプリケーションを作成できます。StyleBook は、アプリケーションの複雑な NetScaler ADC 構成の管理作業を簡素化します。Citrix ADM に存在する StyleBook を選択し、StyleBook パラメータ値を入力します。Citrix ADM は、選択した StyleBook に基づいてターゲットの Citrix ADC インスタンスに構成（コンフィグパック）を作成します。Citrix ADM は、構成パックで定義されているすべての仮想サーバーを含むカスタムアプリケーションも作成します。

> 注
>
> 十分な Citrix ADC ライセンスがある場合は、カスタムアプリケーションと構成パックが作成されます。

上記の 3 つの条件のいずれかで定義されたこれらの条件を満たすアプリケーションを作成すると、NetScaler ADM がエンティティをポーリングすると、アプリケーションダッシュボードでアプリケーションが自動的に更新されます。ポーリングを手動で開始するには、[**Applications**] タブの [**Poll Now**] をクリックしてください。

アプリケーションを作成するには

1. NetScaler ADM で、[アプリケーション] > [ダッシュボード] に移動し、[カスタムアプリの定義] をクリックしてカスタムアプリケーションを作成します。
2. 「アプリケーションを定義」ウィンドウの「名前」フィールドにアプリケーションの名前を入力します。
3. 「カテゴリ」セクションからアプリケーションカテゴリを選択します。NetScaler ADM では、ユーザー定義のアプリケーションをグループ化するカテゴリを定義できます。必要であれば、カテゴリを追加できます。
4. カスタムアプリケーションは、次の 3 つの方法のいずれかで作成できます。

    a) 「既存のアプリケーション」を選択します。既存のアプリケーションを選択するには、「既存のアプリケーションを選択」が有効になっていることを確認してください。[アプリケーション] セクションのリストから アプリケーション を選択します。[アプリケーションの追加] をクリックして、新しいアプリケーションをリストに追加します。

    b) 選択基準を定義します。Citrix ADM にアプリケーションを追加するための選択基準を定義することもできます。アプリは、次の 3 つの方法のいずれかで追加できます。

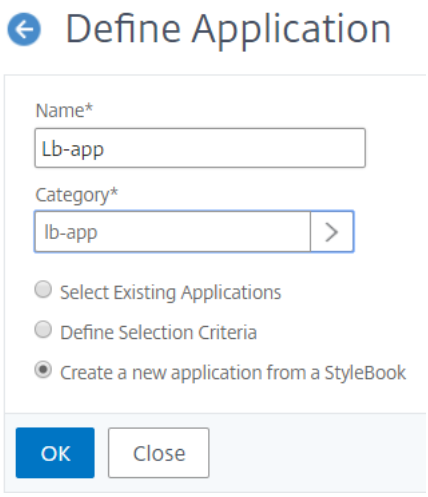
        i. 仮想サーバーの IP アドレスを指定します。1 つの IP アドレスか IP アドレスの範囲、またはコンマ区切りによるそれらの組み合わせで入力できます。

        ii. アプリケーションまたはサービスを実行中のサーバーの名前を指定します。

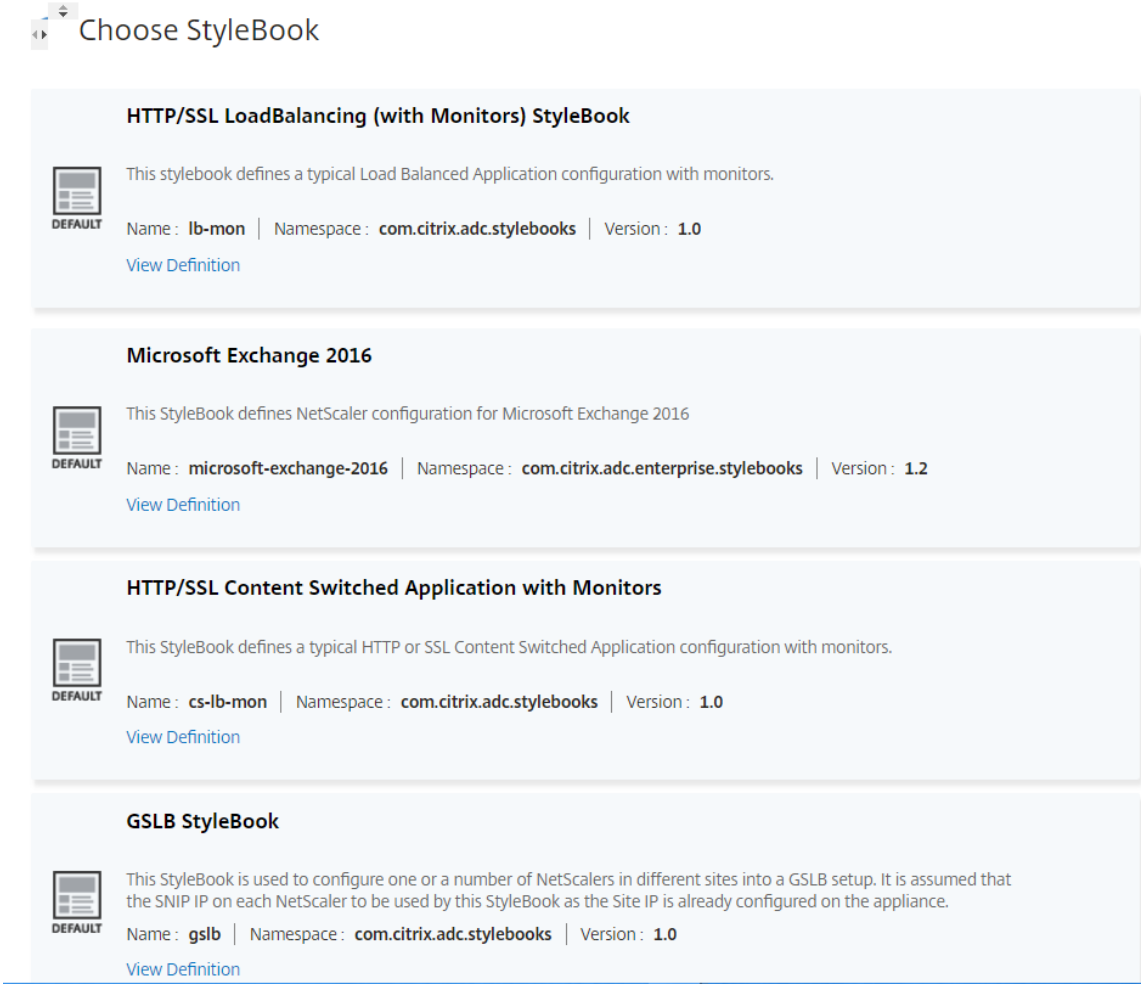
        > 注:
        >
        > ワイルドカード拡張子を使用してサーバー名を検索することもできます。たとえば、「ssl*」はすべての ssl 仮想サーバーをアプリケーションに追加します。

        iii. 選択されたサーバー上でアプリケーションが待ち受けているポート番号を指定します。

    c) **StyleBook** から新しいアプリケーションを作成します。Citrix ADM で必要な StyleBook を選択して、Citrix ADC インスタンスで構成パックを作成し、仮想サーバーをカスタムアプリケーションに関連付けます。



5. [**OK**] をクリックします。StyleBooks からアプリケーションを作成することを選択した場合は、「StyleBook の選択」ページが開きます。このページには、NetScaler ADM に存在するすべての StyleBook のリストが含まれています。

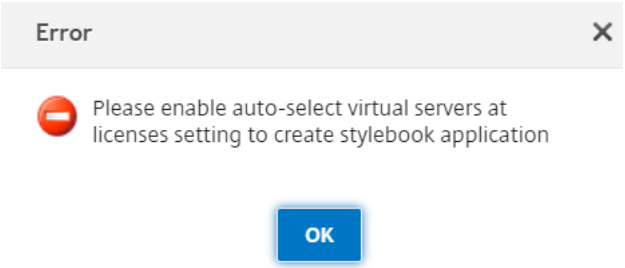


6. StyleBook を選択します。StyleBook がユーザーインターフェイスフォームとして開きます。StyleBook のすべてのパラメーターの値を入力します。StyleBook を使用する前に、[**View Definition**] をクリックして StyleBook の構成を表示することもできます。カスタム StyleBook またはデフォルトの StyleBook を使用する方法について詳しくは、デフォルトの StyleBook の使用を参照してください。
7. これで、StyleBook のターゲットセクションで選択した Citrix ADC インスタンスにカスタムアプリケーションと構成パックが作成されました。

> 注
>
> : 十分な Citrix ADM ライセンスがある場合は、カスタムアプリケーションと構成パックが作成されます。

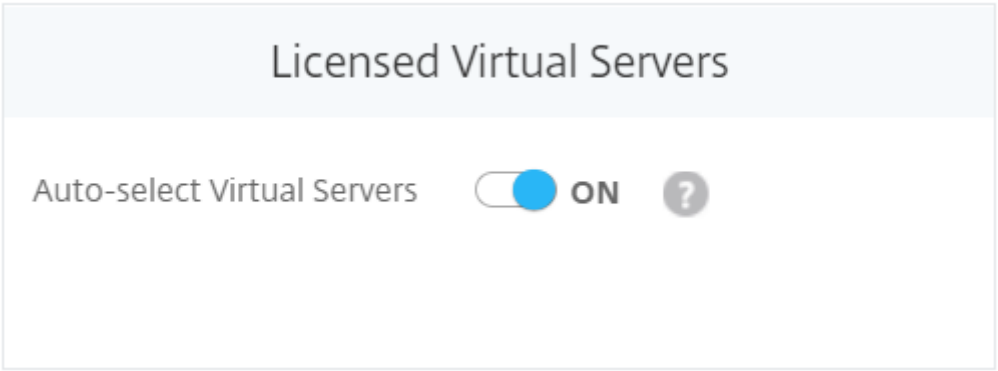
ライセンスを取得する仮想サーバーを自動的に選択するには

StyleBook オプションを使用して構成を作成する場合、NetScaler ADM でライセンス取得用の仮想サーバーが自動的に選択されるようにする必要があります。自動選択を有効にしていない場合、以下の画像のようなエラーメッセージが表示されることがあります。



仮想サーバーの自動選択を有効にするには:

1. Citrix ADM で、［ネットワーク］>［ライセンス］>［システムライセンス］に移動します。
2. [仮想サーバーの自動選択] をクリックして、[ライセンスされた仮想サーバー] セクションのオプションを有効にします。



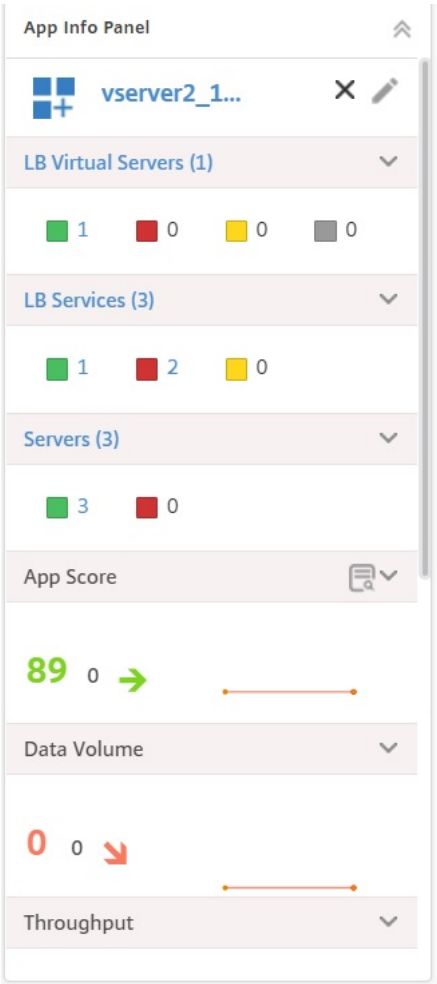
有効にすると、NetScaler ADM はライセンスを取得する仮想サーバーを自動的に選択します。また、有効になっていない場合は、仮想サーバーを明示的に選択する必要があります。

Citrix ADM でアプリケーションの詳細を表示するには

Citrix ADM は、アプリケーションのすべての詳細を、一番右側のアプリ情報パネルと呼ばれる別のペインに表示します。

アプリ情報パネルを表示するには**:**

1. Citrix ADM で、［アプリケーション］>［ダッシュボード］に移動します。
2. [アプリケーションの概要] セクションで、詳細を表示するアプリケーションをクリックします。



選択したアプリケーションにバインドされているエンティティは、[**App Info Panel]** ペインで垂直に配置されます。ウィンドウ内の縦に並べられたボックスには、以下が表示されます。

- 各エンティティの名前
- アクティブなエンティティの数
- 非アクティブなエンティティ
- サービス対象外のエンティティ

ここに表示されるエンティティは、仮想サーバー、サービス、サービスグループ、およびアプリケーションサーバーです。このペインは、App Score、データボリューム、スループット、サーバーとクライアント両方の接続、およびそれぞれのアプリケーションで起きたトランザクションといった他のデータも表示します。

それぞれのアプリケーションで異なる状態になっている仮想サーバー、サービス、サービスグループの数も表示されます。エンティティの名前、または表示される数をクリックして、エンティティを直接有効化または無効化することができます。また、仮想サーバー、サービス、およびサービスグループといった他のバインドされたエンティティを有効化または無効化することもできます。

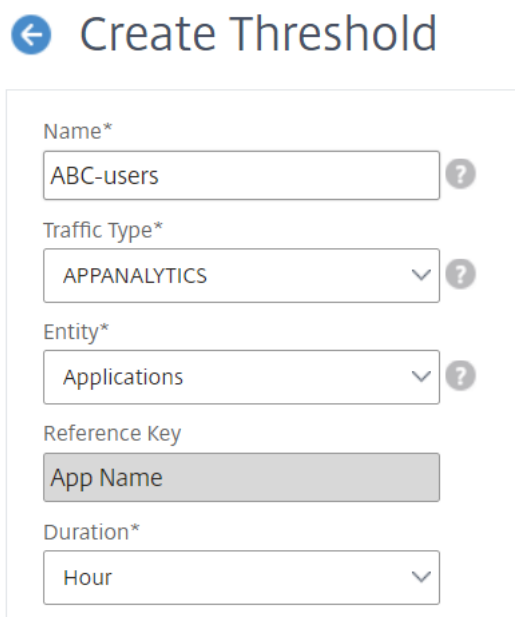
負荷分散サーバーの構成方法について詳しくは、「アプリケーションダッシュボードによる負荷分散サポートの作成」を参照してください。

アプリケーション分析のしきい値およびアラートの作成

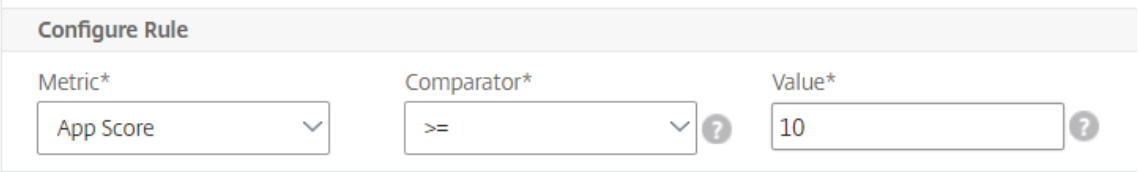
February 6, 2024

Citrix ADM のアプリケーション分析により、Citrix インスタンスを通過するさまざまなタイプのトラフィックを監視できます。Citrix ADM では、インサイトトラフィックの監視に使用されるさまざまなカウンター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。

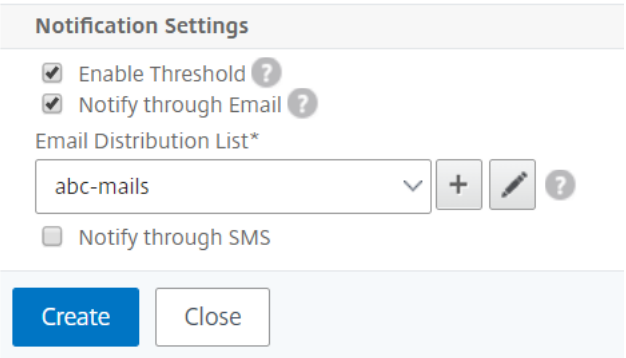
1. NetScaler ADM で、[**Analytics**] > [設定] > [しきい値] に移動します。「しきい値」ページで 、「追加」をクリックします。
2. 「しきい値 の作成」ページで、次の詳細を指定します。
    a) 名前。NetScaler ADM がアラートを生成するイベントを作成するための名前を入力します。
    b) **** **** トラフィックタイプ。リストボックスから「アプリ分析」を選択します。
    c) エンティティ。リスト・ボックスから、カテゴリまたはリソース・タイプを選択します。デフォルトでは、エンティティとして「アプリケーション」が選択されています。
    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. 「ルールを設定」セクションで、アプリスコア指標と必要なコンパレータを選択してルールを作成し、しきい値を指定します。



4. 「しきい値 を有効にする」をクリックして、Citrix ADM がエンティティの監視を開始できるようにします。
5. 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。［作成］をクリックします。



StyleBook

February 6, 2024

StyleBook は、アプリケーションの複雑な NetScaler ADC 構成の管理作業を簡素化します。StyleBook は、NetScaler ADC 構成の作成と管理に使用できるテンプレートです。NetScaler ADC の特定の機能を構成するための StyleBook を作成することも、Microsoft Exchange や Lync などのエンタープライズアプリケーション展開用の構成を作成するように StyleBook を設計することもできます。

StyleBook は DevOps チームによって実践されているコードとしてのインフラストラクチャの原則によく適しています。コードとしてのインフラストラクチャの構成は宣言的でバージョン管理されるものです。構成は繰り返され全体として展開されるものでもあります。StyleBooks には以下の利点があります。

- 宣言：**StyleBook** は、命令構文ではなく宣言構文で書かれています。Stylebook では、特定の NetScaler ADC インスタンスで実現する手順ではなく、構成の結果や「望ましい状態」の説明に集中できます。Citrix Application Delivery Management（ADM）は、Citrix ADC 上の既存の状態と指定した目的の状態との差分を計算し、インフラストラクチャに必要な編集を行います。StyleBook は YAML で記述された宣言構文を使用するため、StyleBook のコンポーネントは任意の順序で指定でき、NetScaler ADM は計算された依存関係に基づいて正しい順序を決定します。
- アトミック:StyleBooks を使用して構成をデプロイすると、フル構成レーションがデプロイされるか、何もデプロイされないので、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 ADC 構成を定義できます。アプリケーションの構成はパラメーターを使用することで抽象化できます。そのため、StyleBook から構成を作成するユーザーは、いくつかのパラメーターを入力するだけのシンプルなインターフェイスを使用して複雑な Citrix ADC 構成を作成できます。StyleBooks から作成された構成は、インフラストラクチャに関連付けられていません。したがって、1 つの構成を 1 つまたは複数の Citrix ADC に展開したり、インスタンス間で移動したりできます。
- 自動生成 **UI**：NetScaler ADM は、NetScaler ADM GUI を使用して構成を行うときに、StyleBook のパラメータを入力するために使用する UI フォームを自動生成します。StyleBook の作成者が新しい GUI 言語を学習したり、UI ページやフォームを個別に作成したりする必要はありません。
- **API** 主導：すべての構成操作は、NetScaler ADM GUI または REST API を使用してサポートされます。API は、同期モードまたは非同期モードで使用できます。StyleBook の API では、構成タスクに加えて、実行時に StyleBook のスキーマ（パラメーターの説明）を見つけることもできます。

1 つの StyleBook を使用して複数の構成を作成できます。各構成は構成パックとして保存されます。たとえば、通

常の HTTP 負荷分散アプリケーションの構成を定義する StyleBook があるとします。負荷分散エンティティの値を使用して構成を作成し、Citrix ADC インスタンスで実行できます。この構成は構成パックとして保存されます。同じ StyleBook を使用して異なる値を持つ別の構成を作成し、同じまたは別の Citrix ADC インスタンスで実行できます。この構成には、新しい構成パックが作成されます。構成パックは、Citrix ADM と、構成が実行される Citrix ADC インスタンスの両方に保存されます。

NetScaler ADM に同梱されているデフォルトの StyleBook を使用して展開用の構成を作成するか、独自の StyleBook を設計して NetScaler ADM にインポートすることができます。StyleBooks を使用して、NetScaler ADM GUI または API を使用して構成を作成できます。

このドキュメントでは、次の内容について説明します。

- StyleBook の閲覧方法
- デフォルトの StyleBook
- ビジネスアプリケーション向けに開発された StyleBook
- カスタム StyleBook
- StyleBook の API
- StyleBook の文法

StyleBook グループ

February 6, 2024

Citrix Application Delivery Management（ADM）の StyleBook は、2 つの方法でグループ化できます。これらは、デフォルトの StyleBook またはカスタム StyleBook としてグループ化できます。また、公開または非公開の StyleBook としてグループ化することもできます。Citrix ADM では、システムに存在するすべての StyleBook を表示できます。Citrix ADM では、StyleBook をソートして表示することもできます。また、StyleBook 同士がどのように接続されているかをグラフィカルに表示することもできます。

また、カスタム StyleBook をダウンロードして削除する方法についても説明します。カスタム StyleBook をダウンロードして、変更を加えたり、以前の StyleBook に基づいて新しい StyleBook を作成したりできます。カスタム StyleBook を削除することもできます。

デフォルトおよびカスタム StyleBook

- デフォルトの StyleBook は、Citrix ADM ファイルシステムに存在する StyleBook で、Citrix ADC インスタンスにデプロイできる構成を作成できます。
- カスタム StyleBook は、Citrix ADM に書き込んでインポートしたり、構成オブジェクトを作成したりできる独自の StyleBook です。

デフォルトの StyleBook とカスタム StyleBook はどちらもパブリックまたはプライベートにすることができます。

パブリックおよびプライベートの **StyleBook**

Citrix ADC インスタンスにデプロイする構成パックを作成できる StyleBook は、「パブリック」StyleBook として分類できます。つまり、これらはすべて直接使用して構成を作成できます。

しかし、一部の StyleBook は、他の StyleBook のビルディングブロックとして使用されます。これらのビルディングブロックは、デフォルトの StyleBook を構成する組み込みの StyleBook です。このような StyleBook は「プライベート」StyleBook と呼ばれます。インスタンスでの構成パックの作成には直接使用されませんが、これらの StyleBook を Citrix ADM に表示したい場合があります。StyleBook をプライベートとしてマークするには、プライベート属性を使用して StyleBook が Citrix ADM に表示されないようにすることができます。

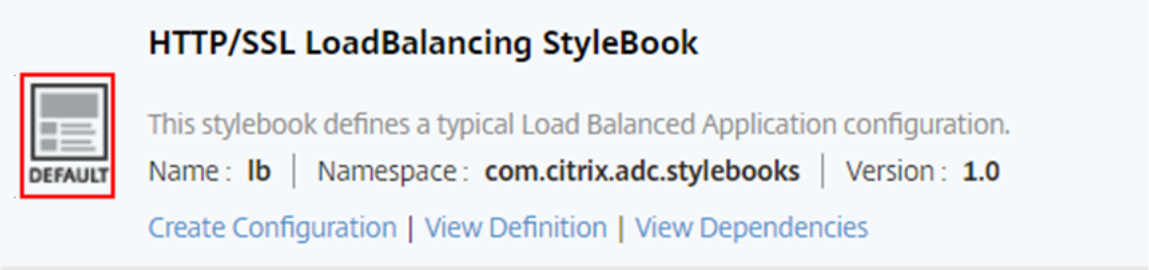
```
name: basic-lb-config
description: This StyleBook defines a simple load balancing
   configuration and is a building block to build other load balancing
   configurations.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
private: true
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

StyleBook の表示

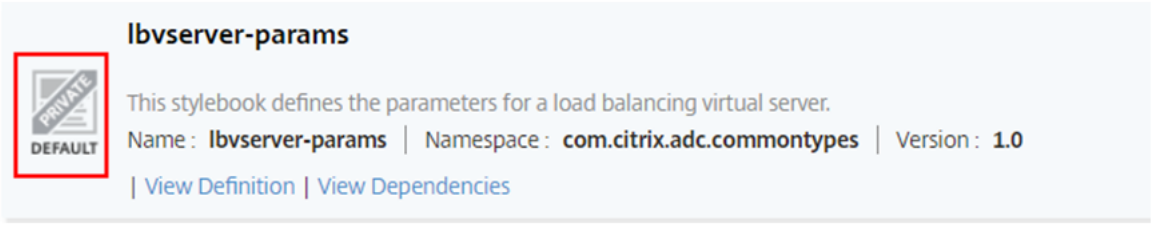
Citrix ADM では、デフォルトとプライベートの両方の StyleBook の数が増えています。アクセスしたい特定の StyleBook を検索したい場合があります。また、両方のタイプの StyleBook を別々に表示することもできます。

Citrix ADM では、［アプリケーション］> ［**StyleBook**］に 移動すると、システムに存在する StyleBook のリストを 表示できます。

デフォルトのパブリック StyleBook のパネルには、次のアイコンがあります。

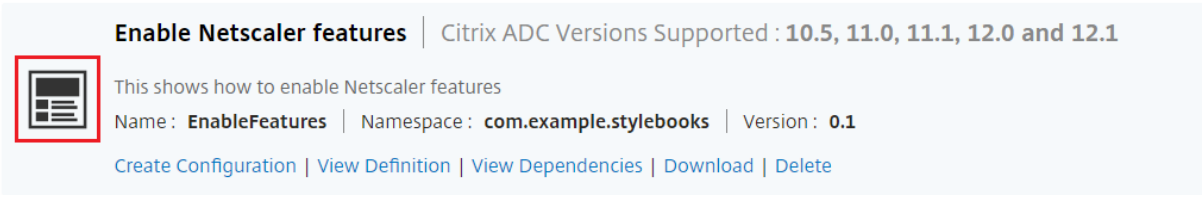


一方、デフォルトのプライベート StyleBook には、プライベート StyleBook であることを宣言するアイコンが付いています:

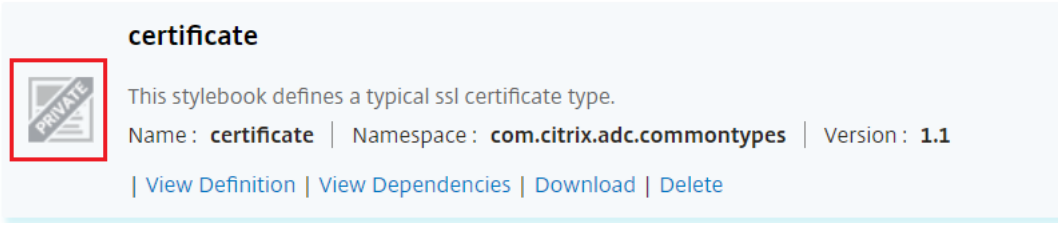


プライベート StyleBook の定義と依存関係は表示できますが、プライベート StyleBook から構成パックを作成することはできません。ご自分の StyleBook でプライベート StyleBook を引き続き使用できます。

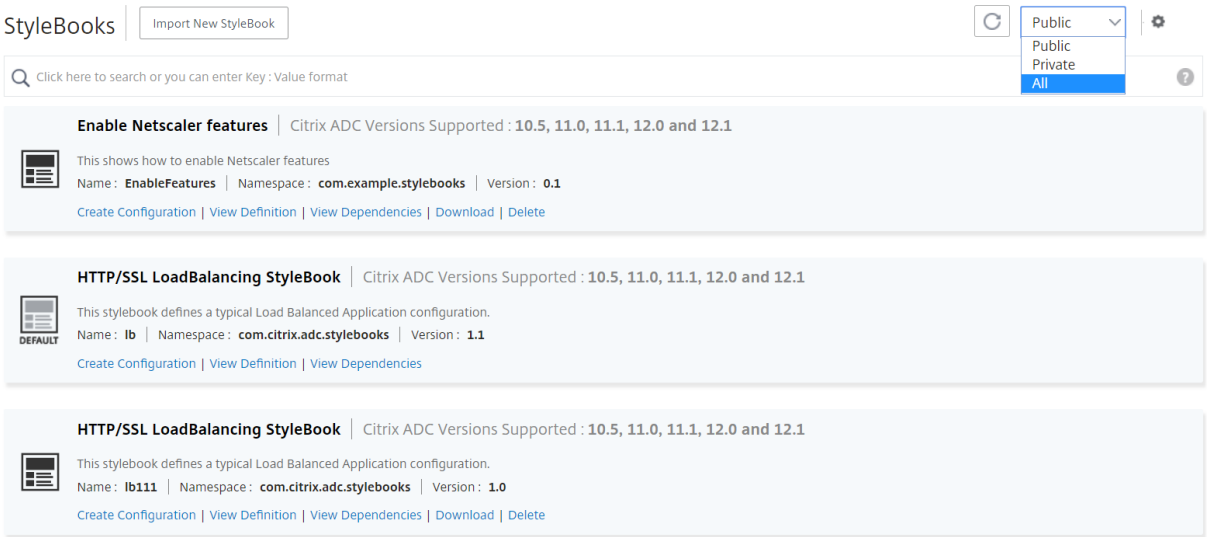
カスタムビルドのパブリック StyleBook は、次の図に示すように、異なるアイコンを持っています。



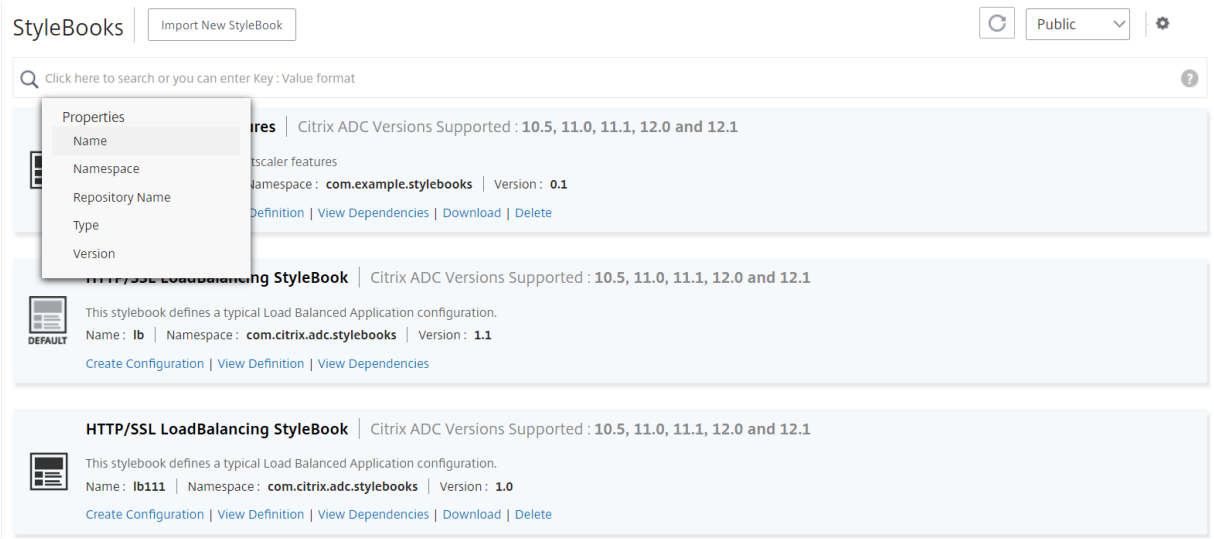
一方、カスタムビルドのプライベート StyleBook には、次のアイコンが表示されます。



ページの右上に、StyleBook を並べ替えるオプションが表示されます。StyleBook には、すべて、パブリック、またはプライベートの 3 つのオプションがあります。オプションの 1 つをクリックします。



検索アイコンをクリックして、特定の StyleBook を検索することもできます。使用可能な検索オプションは、名前、名前空間、バージョンの 3 つです。検索操作では、大文字と小文字は区別されません。



StyleBook の依存関係の表示

NetScaler ADM では、StyleBook の相互接続方法をグラフィカルに表示できます。

Citrix ADM では、デフォルトの StyleBook を使用して展開環境の設定を作成することもできます。独自の StyleBook をデザインして Citrix ADM にインポートすることもできます。

StyleBook の重要かつ便利な特徴の 1 つは、別の StyleBook の構築ブロックとして使用できる点です。StyleBook を別の StyleBook にインポートできます。インポートされた Stylebook はタイプとして宣言され、2 つ目の StyleBook のコンポーネントまたはパラメーターによって使用されます。

他の StyleBook で使用されている StyleBook は、システムから削除できません。ただし、StyleBook をグラフィカルに表示すると、どの StyleBook が StyleBook の削除を妨げているかを知ることができます。グラフを見ると、複数の StyleBook 間の関係を確認できます。

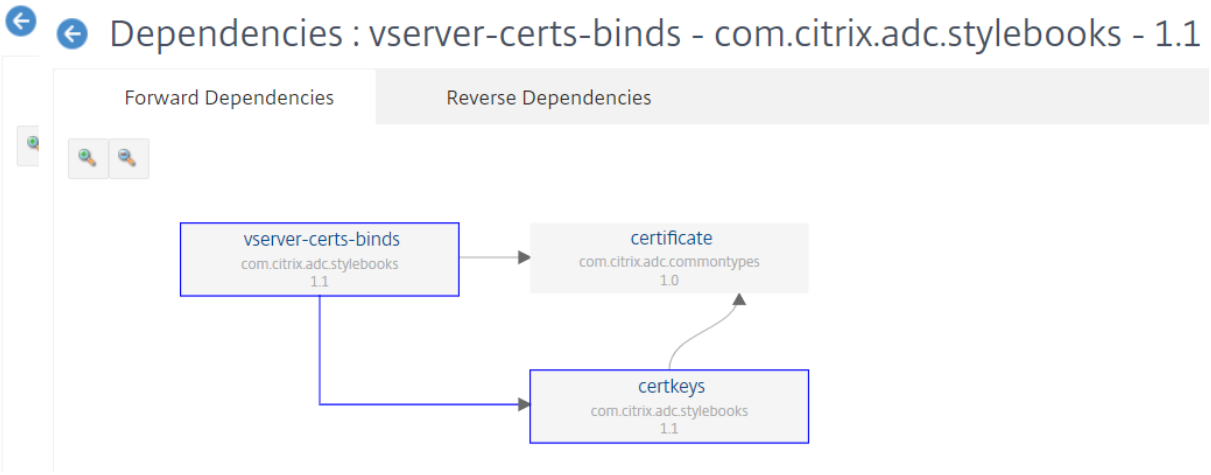
StyleBook の依存関係を表示するには

Citrix ADM で、「アプリケーション」> 「**StyleBook**」に 移動します。StyleBook ページには、Citrix ADM で使用できるすべての StyleBook が表示されます。下にスクロールして、ご使用の StyleBook を見つけてください。StyleBook パネルには、構成の作成、StyleBook 定義の表示、および StyleBook の依存関係の表示を行うためのリンクが表示されます。[依存関係の表示] をクリックします。

フォワード依存関係

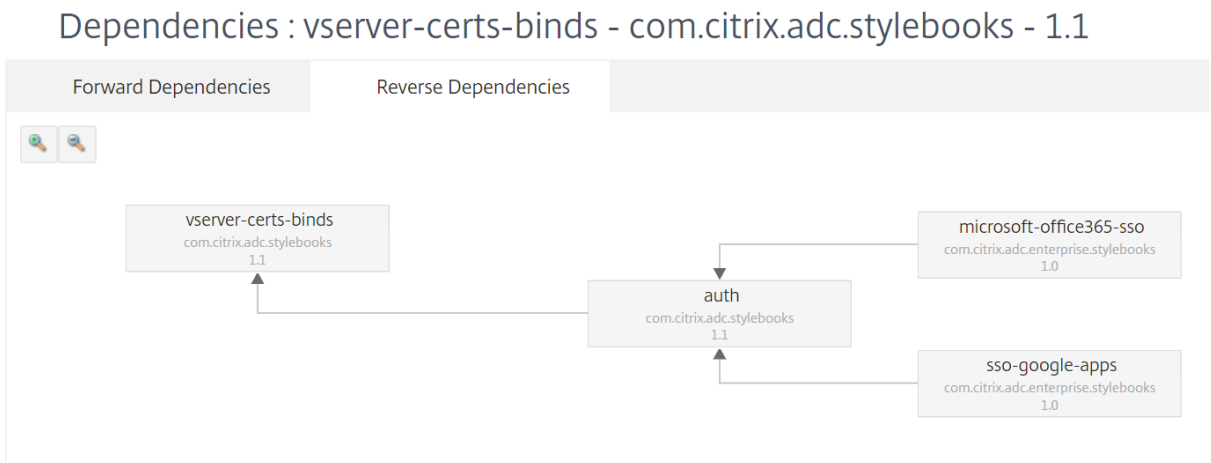
前方依存関係タブでは、StyleBook が使用しているさまざまなデフォルトの StyleBook を表示できます。矢印に従って、StyleBook が使用している StyleBook を見つけてください。矢印の 1 つにマウスを合わせると、矢印と相互

に接続されている StyleBook が強調表示されます。StyleBook の名前をクリックして、その StyleBook の定義を表示することもできます。



逆依存関係

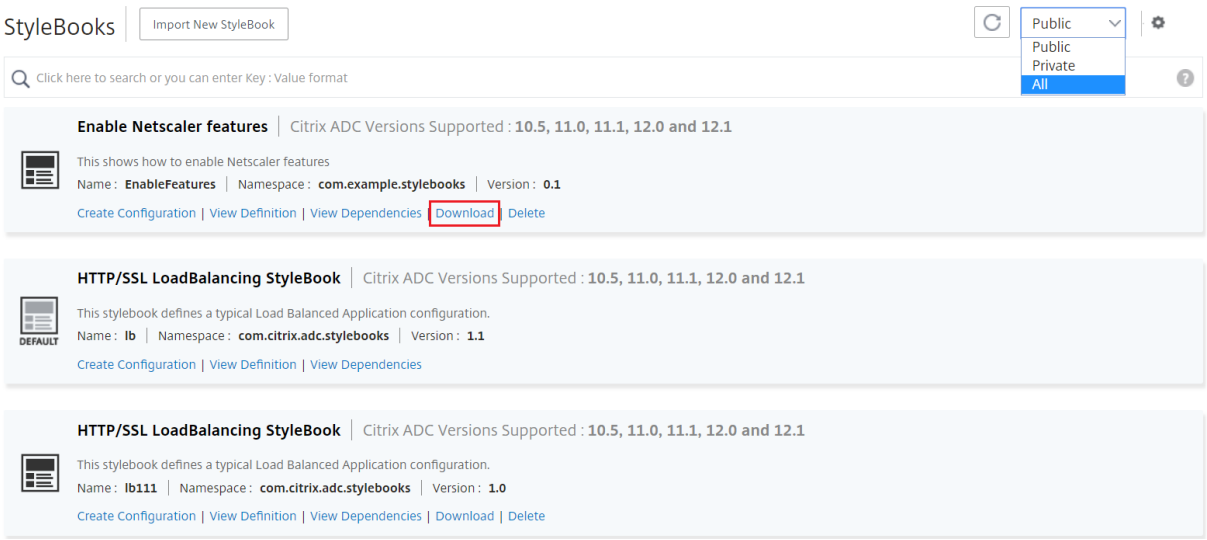
「逆依存関係」タブでは、StyleBook を使用している StyleBook をグラフィカルに表示できます。矢印をたどると、ディスプレイ内のすべての StyleBook が StyleBook の方を向いていることがわかります。StyleBook が直接使用している場合や、StyleBook が別の StyleBook を介して StyleBook を使用している場合があります。



カスタム **StyleBook** のダウンロード

Citrix ADM からカスタム StyleBook をダウンロードするには、[アプリケーション] > [**StyleBook**] > [構成] に移動します。右側のパネルに表示される StyleBook のリストには、カスタム定義 StyleBook をダウンロードするオプションがあります。[**Download**] をクリックします。StyleBook に依存するカスタム StyleBook がある場合は、それらの StyleBook もシステムにダウンロードされます。

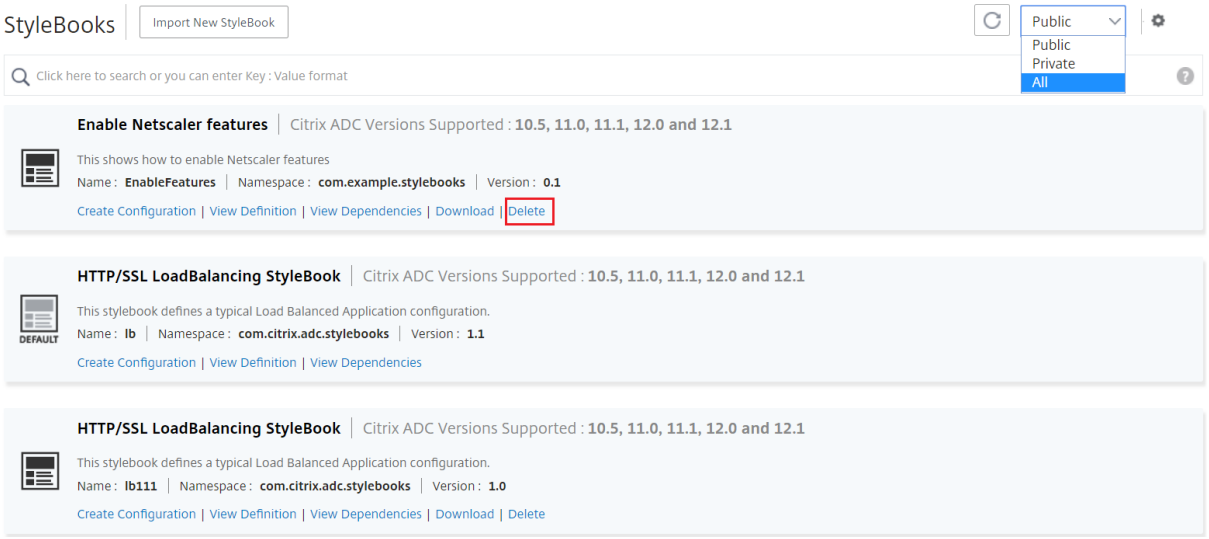
> 注:
>
> パブリックまたはプライベートとしてマークされているデフォルトの StyleBook またはカスタム StyleBook をダウンロードすることはできません。



> 注
>
> NetScaler ADM デフォルトの StyleBook をダウンロードすることはできません。ただし、StyleBook パネルの「定義を表示」および「依存関係を表示」リンクをクリックすると、その定義と依存関係を表示できます。

カスタム **StyleBook** の削除

StyleBook パネルの右側にある「X」アイコンをクリックして、カスタム StyleBook を削除することもできます。NetScaler ADM から StyleBook を削除するかどうかを確認するポップアップウィンドウが表示されます。StyleBook が他のカスタム StyleBook（他の StyleBook では使用されていない）を使用している場合は、チェックボックスを選択してそれらを削除することもできます。



> 注
>
> NetScaler ADM に他の StyleBook が依存しているカスタム StyleBook は削除できません。

GitHub リポジトリからの StyleBook のインポートと同期

February 6, 2024

開発に CI/CD プロセスを使用しているか、GitHub ですべてのデプロイオブジェクトを管理しているとしましょう。Citrix ADC 構成を展開するために複数の StyleBook を作成し、その StyleBook を GitHub リポジトリで管理している場合があります。これで、これらの StyleBook を Citrix アプリケーションおよびデリバリー管理（ADM）に直接インポートできます。それらを GitHub から手動でコピーして Citrix ADM にアップロードする必要はありません。

GitHub リポジトリの URL を指定することで、GitHub リポジトリを表すリポジトリを Citrix ADM で定義できるようになりました。GitHub で作成したユーザー名とパスワード (または API トークン) を入力する必要があります。つまり、GitHub に有効なアカウントを持つ権限のあるユーザーのみが StyleBook をインポートして同期できます。

リポジトリを作成したら、NetScaler ADM を GitHub リポジトリと同期できます。Citrix ADM は、そのリポジトリにある StyleBook をインポートして検証し、Citrix ADM の StyleBook のリストに追加します。検証に失敗した場合、StyleBook は NetScaler ADM に追加されません。エラーを修正し、更新したバージョンを GitHub リポジトリにコミットする必要があります。その後、それらをインポートするか、NetScaler ADM に再度同期してみてください。

> 注
>
> - 現在、インポートおよび同期できるのは、依存する StyleBook が関連付けられていない StyleBook の

> みです。つまり、StyleBook には、1 つのファイルに定義する必要があるすべての構成が含まれている必要があります。
> - GitHub リポジトリからの同期は、Citrix ADM GUI または API から手動で開始する必要があります。つまり、現在のところ、StyleBooks のインポートは GitHub のコミットアクティビティに基づいて自動的に行われません。
>
> 現在、StyleBooks ファイルはマスターブランチからのみインポートできます。

前提条件

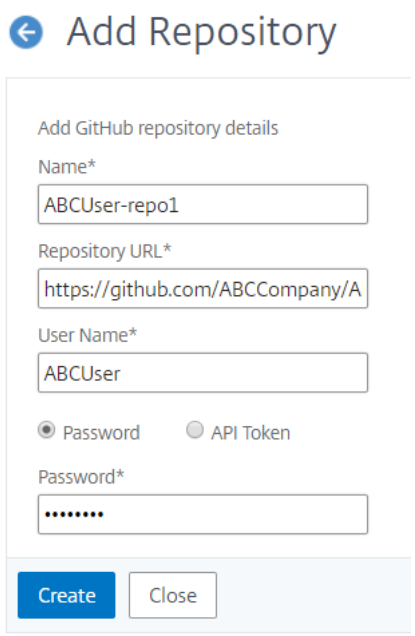
- GitHub の有効なアカウントが必要です。
- StyleBook ファイルは、GitHub リポジトリのマスターブランチのルートフォルダーに存在する必要があります。

リポジトリの追加と **GitHub** からの **StyleBook** のインポート

1. Citrix ADM で、［アプリケーション］>［構成］>［****** リポジトリ］に移動 ****** します。
2. ［追加］をクリックします。「リポジトリの追加」ウィンドウで、次のパラメータを入力します。
   - 名前。リポジトリの名前を入力します。この名前は、GitHub のリポジトリ名と同じでもかまいません。
   - リポジトリの **URL**。GitHub リポジトリの URL を入力します。
   - ユーザー名とパスワード。GitHub アカウントにアクセスするためのユーザー名とパスワードを入力します。

   > 注: パスワードの代わりに API トークンを指定することもできます。HTTPS 経由で GitHub のパスワードの代わりに API トークンを使用できます。また、これらを使用して基本認証で API を認証することもできます。

3. ［作成］をクリックします。



リポジトリは NetScaler ADM で作成されます。

4. **StyleBook** をインポートまたは同期するには、リポジトリページでリポジトリを選択し、「同期」をクリックします。

ここで使用できるその他のアクションは次のとおりです。

- 編集。リポジトリの URL、ユーザー名、パスワード (または API トークン) を編集できます。
- **[削除]**。リポジトリを、その GitHub リポジトリから以前にインポートされた Citrix ADM に存在するすべての StyleBook とともに削除できます。

  > 注:
  >
  > ConfigPack が関連付けられている StyleBook がある場合は、NetScaler ADM からリポジトリを削除できません。

- リセット。Citrix ADM からリポジトリエントリを実際に削除しなくても、そのリポジトリから同期された Citrix ADM 内のすべての StyleBook を削除できます。
- ファイルを一覧表示します。Citrix ADM に存在する GitHub リポジトリから取得されたすべての StyleBook のリストを表示できます。

デフォルトの **StyleBook** を使用する

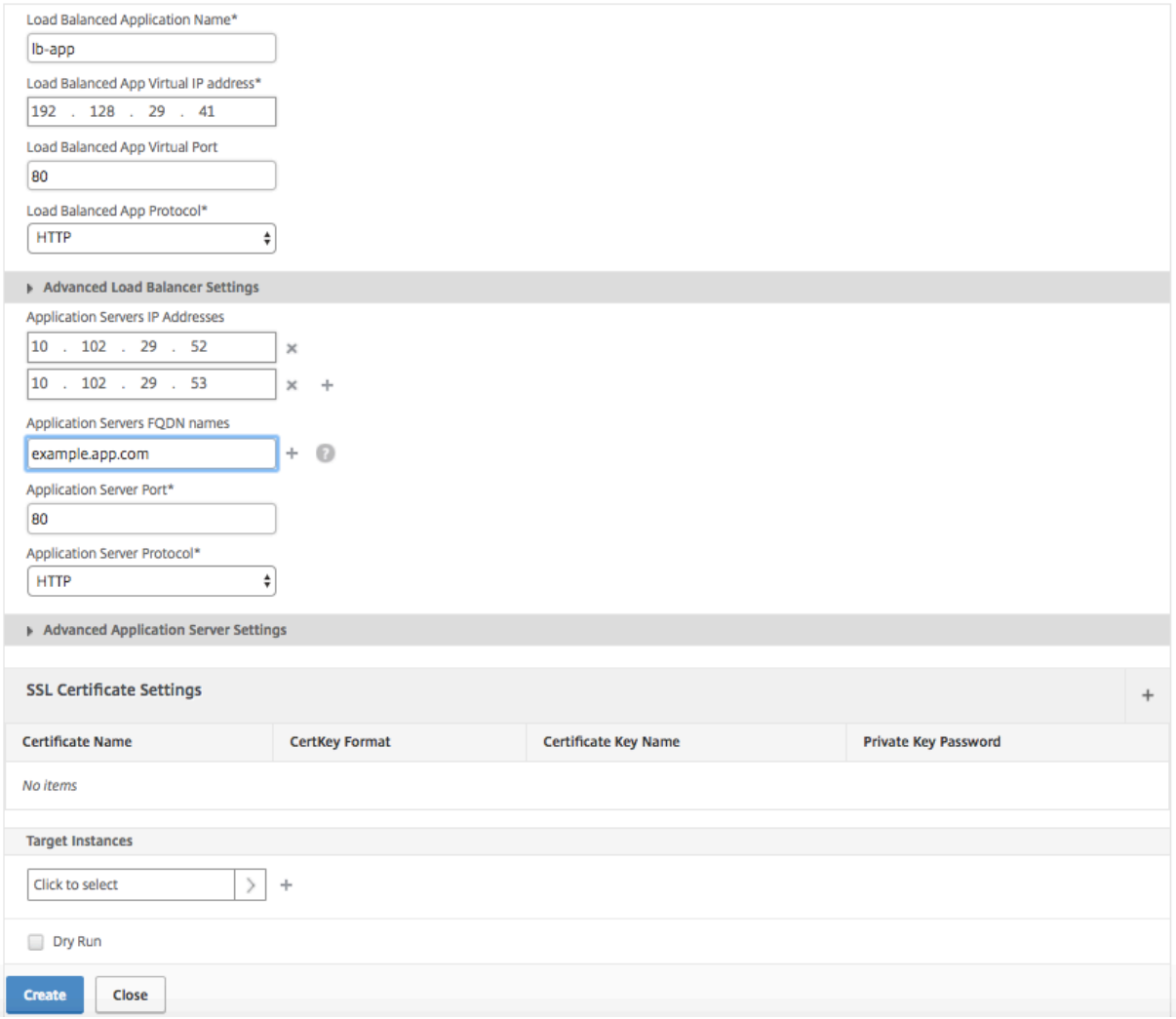
February 6, 2024

デフォルトの StyleBook のセットは、NetScaler Application Delivery Management (ADM) に付属しています。デフォルトの StyleBook を使用する場合は、StyleBook でパラメータの値を指定し、構成を実行する NetScaler ADC インスタンスの IP アドレスを選択する必要があります。構成を送信すると、NetScaler ADM は指定したパラメーター値を検証し、構成のグラフを作成し、NetScaler ADC インスタンスに接続して、インスタンスで構成を実行します。

デフォルトの **StyleBook** から設定を作成するには

1. アプリケーション > 構成 **> StyleBooks** に移動します。StyleBook ページには、NetScaler ADM のすべての StyleBook が表示されます。このリストには、デフォルトとカスタムの StyleBook の両方が含まれています。検索フィールドに StyleBook の名前 を入力し、Enter キーを押します。それ以外の場合は、リストを下にスクロールして StyleBook を見つけることができます。

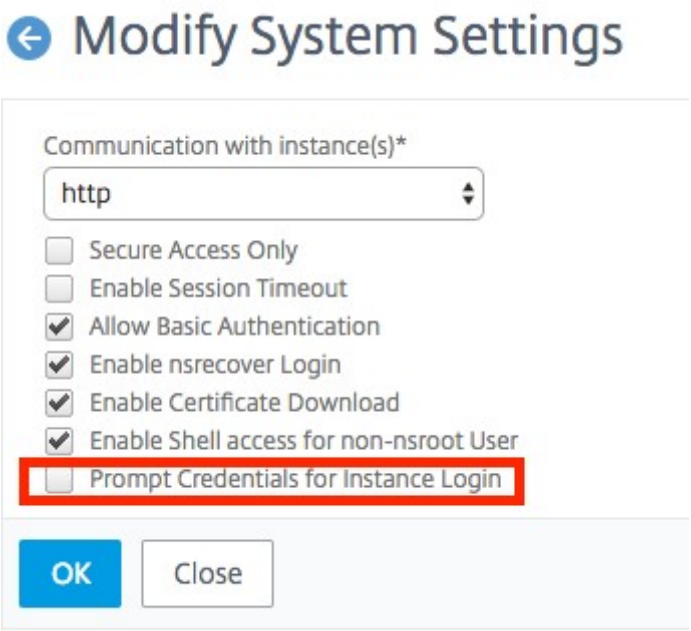
2.「構成を作成」をクリックします。パラメータに必要な値を指定します。



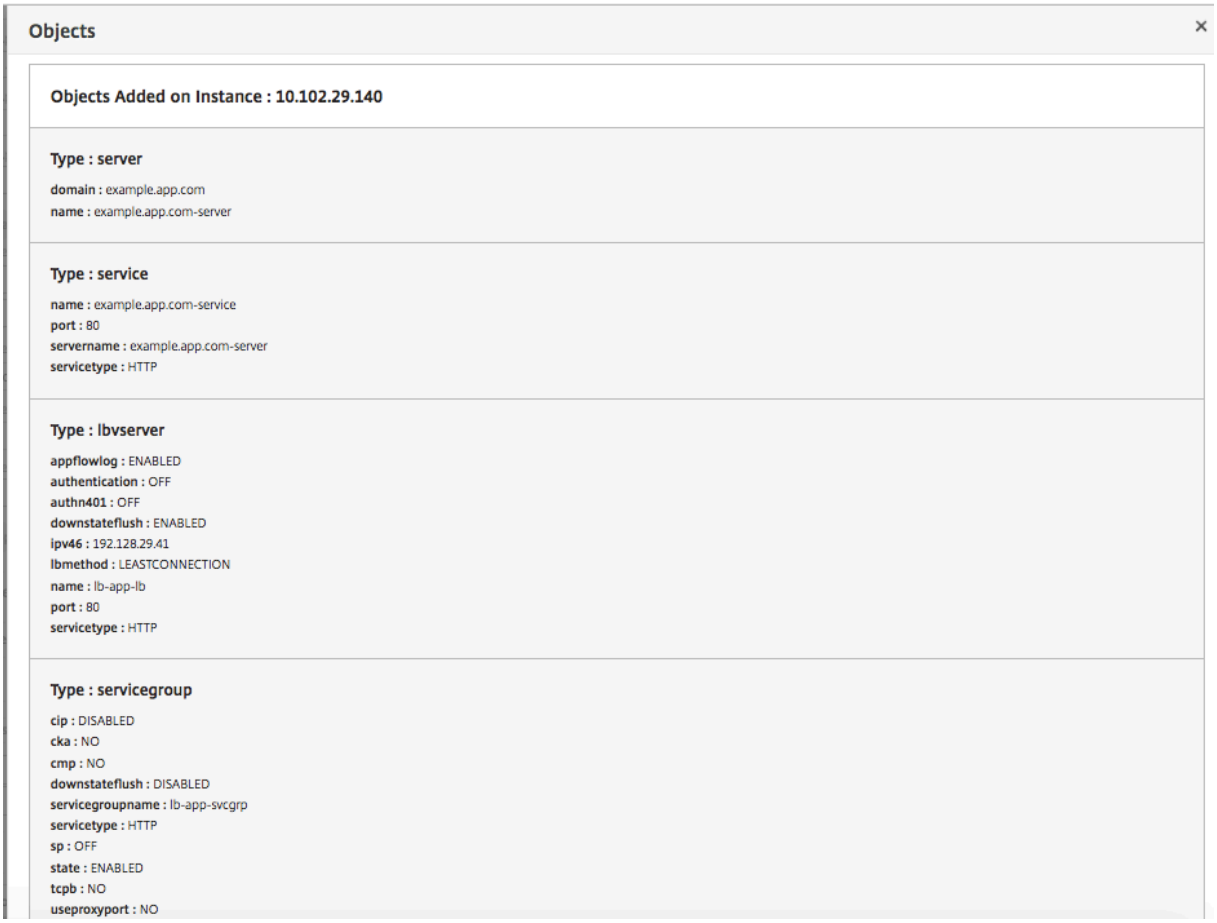
3. [ターゲットインスタンス] で、構成を実行する NetScaler ADC インスタンスの IP アドレスをクリックして選択

します。この設定を複数のインスタンスで実行する場合は、「+」をクリックしてさらにインスタンスを追加します。

Citrix ADM> [システム] > [システム設定の 変更] > [システム設定の 変更 **] で **[**インスタンスログイン ** の認証情報を確認する] オプションが有効になっている場合、選択した Citrix ADC インスタンスで構成を実行すると、Citrix ADC インスタンスの認証情報の入力を求められます。それ以外の場合、NetScaler ADM はインスタンスプロファイルに格納されているインスタンス認証情報を使用してインスタンスにログインします。



NetScaler ADC インスタンスで実行する前に構成をテストまたは検証する場合は、[ドライラン] を選択し、[作成] をクリックします。構成が有効の場合は、指定した値に基づいて作成されたオブジェクトが表示されます。



4.［ドライラン］チェックボックスをオフにし、［作成］をクリックして構成を作成し、NetScaler ADC インスタンスで構成を実行します。作成した StyleBook 構成は、以下に示すように構成のリストに表示されます。

> 注
>
> 更新アイコンをクリックして、NetScaler ADM で最近検出された NetScaler ADC インスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。

NetScaler ADM を使用して、この構成パックを調査、更新、または削除できるようになりました。

すべてのデフォルト **StyleBook** を非表示にする

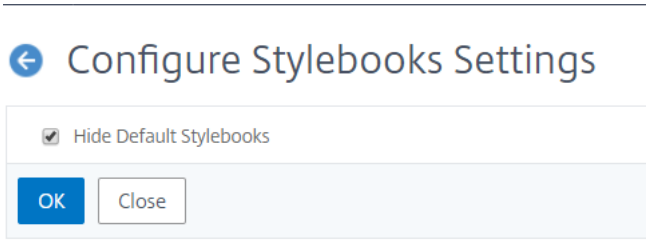
February 6, 2024

Citrix ADM は、Citrix ADM フォルダシステムに存在するすべての StyleBook を一覧表示します。StyleBook のリストには、プライベートとパブリックの両方に使用できるデフォルトの StyleBook とカスタム StyleBook が含まれています。管理者は、デフォルトの StyleBook をすべて非表示にしたい場合があります。ユーザーに、自分またはユーザーが作成したカスタム StyleBook のみの表示とアクセスを許可できます。

NetScaler ADM では、カスタム StyleBook を表示したり、NetScaler ADM に同梱されているデフォルトの StyleBook をすべて非表示にしたりできます。デフォルトの StyleBook をすべて非表示にできる新しい GUI オプションが提供されました。

すべてのデフォルトの **StyleBook** を非表示にするには:

1. NetScaler ADM で、［アプリケーション］>［構成］**>**［設定］に移動します。
2. 設定ページには、デフォルトの StyleBook がユーザーに表示されるかどうかに関する情報が表示されます。
3. デフォルトの StyleBook を非表示にするには、右上の編集アイコンをクリックします。
4.「**StyleBook** 設定の構成」ページで、「デフォルトの **StyleBook** を非表示にする」オプションを選択します。
5.［**OK**］をクリックします。



RBAC 機能を使用してページを非表示にすることを選択していない場合でも、**StyleBook** 設定の構成ページはユーザーに表示されます。ユーザーには、デフォルトの StyleBook を再表示するためのオプションが残っている場合があります。

StyleBook の設定ページを非表示にするには、ポリシーを作成し、そのポリシーをデフォルトの StyleBook が表示されないはずのユーザーに割り当てる必要があります。

RBAC ポリシーを作成するには、次の手順を実行します。

1. NetScaler ADM で、［アカウント］>［ユーザー管理］>［アクセスポリシー］に移動します。
2.［**Add**］をクリックしてポリシーを作成します。
3. ポリシー名を入力します。
4.「権限」セクションで、「すべて」>「アプリケーション」>「構成」>「設定」が選択されていないことを確認し、「**OK**」をクリックします。

ポリシーを作成したら、ロールを作成し、各ロールを 1 つ以上のポリシーにバインドし、ロールをユーザグループに割り当てる必要があります。ポリシーをユーザに関連付ける方法の詳細については、「ロールベースのアクセス制御の設定」を参照してください。

SSO Google Apps StyleBook

February 6, 2024

Google Apps は、Google が開発したクラウドコンピューティング、生産性向上およびコラボレーションツール、ソフトウェア、および製品のコレクションです。シングルサインオン (SSO) を使用すると、ユーザーは、エンタープライズ資格情報を使用してすべてのサービスに対して 1 回サインインすることで、管理コンソールへのサインインを含め、すべてのエンタープライズクラウドアプリケーションにアクセスできます。

NetScaler ADM SSO Google Apps StyleBook を使用すると、NetScaler ADC インスタンスを介して Google Apps SSO を有効にすることができます。StyleBook は、Google Apps にアクセスするユーザーを認証するための SAML ID プロバイダーとして NetScaler ADC インスタンスを構成します。

この StyleBook を使用して NetScaler ADC インスタンスで Google アプリの SSO を有効にすると、次の手順になります。

1. 認証仮想サーバーの構成
2. SAML IDP ポリシーとプロファイルの設定
3. 認証仮想サーバーへのポリシーとプロファイルのバインド
4. インスタンスの LDAP 認証サーバーとポリシーの設定
5. LDAP 認証サーバーとポリシーを、インスタンスに構成されている認証仮想サーバーにバインドする

構成の詳細:

次の表に、この統合が正常に機能するために必要な最低限のソフトウェアバージョンを示します。統合プロセスは、同じバージョンの上位バージョンでも機能するはずです。

Product	最低限必要なバージョン
Citrix ADC	リリース 11.0、エンタープライズ/プラチナライセンス

以下の手順では、認証要求を NetScaler ADC で監視される IP アドレスにルーティングするための適切な外部 DNS エントリーまたは内部 DNS エントリーがすでに作成されていることを前提としています。

SSO Google アプリの **StyleBook** 設定をデプロイする:

次のタスクは、Microsoft SSO Google Apps StyleBook をビジネスネットワークにデプロイする際に役立ちます。

SSO Google アプリの **StyleBook** をデプロイするには

1. Citrix ADM で、「アプリケーション」>「構成」>「**StyleBook** 」に移動します。[StyleBook] ページには、Citrix ADM で使用可能なすべての StyleBook が表示されます。下にスクロールして **SSO Google Apps StyleBook** を見つけてください。[構成を作成] をクリックします。

2. StyleBook がユーザーインターフェイスページとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。
3. 次のパラメーターの値を入力します:
   a) アプリケーション名。ネットワークにデプロイする SSO Google アプリ設定の名前。
   b) 認証仮想 **IP** アドレス。Google アプリの SAML IdP ポリシーがバインドされている AAA 仮想サーバが使用する仮想 IP アドレス。
   c) **SAML** ルール式。デフォルトでは、次の Citrix ADC ポリシー（PI）式が使用されます: HTTP.REQ.HEADER (「リファラー」) .CONTAINS (「google」)。要件が異なる場合は、このフィールドを別の式で更新します。このポリシー式は、これらの SAML SSO 設定が適用されるトラフィックと一致し、Referer ヘッダーが Google ドメインからのものであることを確認します。
4. SAML Idp 設定セクションでは、手順 3 で作成した AAA 仮想サーバーで使用される SAML IDP プロファイルとポリシーを作成することで、Citrix ADC インスタンスを SAML ID プロバイダーとして構成できます。
   a) **SAML** 発行者名。このフィールドには、認証仮想サーバーのパブリック FQDN を入力します。例: `https://<Citrix ADC Auth VIP>/saml/login`
   b) **SAML** サービスプロバイダー **(SP) ID**。（オプション）NetScaler ADC ID プロバイダーは、この ID と一致する発行者名からの SAML 認証要求を受け入れます。
   c) アサーションコンシューマサービス **URL**。ユーザー認証が成功した後、NetScaler ADC ID プロバイダーが SAML アサーションを送信する必要があるサービスプロバイダーの URL を入力します。アサーションコンシューマサービス URL は、ID プロバイダサーバサイトまたはサービスプロバイダサイトで開始できます。
   d) このセクションには、他にも入力できるオプションフィールドがあります。たとえば、次のオプションを設定できます。
      i. SAML バインディングプロファイル (デフォルトは「POST」プロファイル)。
      ii. SAML リクエスト/レスポンスを検証/署名する署名アルゴリズム (デフォルトは「RSA-SHA1」)。
      iii. SAML リクエスト/レスポンスのハッシュをダイジェストする方法 (デフォルトは「SHA-1」)。
      iv. 暗号化アルゴリズム (デフォルトは AES256)、およびその他の設定

      > 注
      >
      > これらの設定は Google Apps で動作することがテストされているため、Citrix ではデフォルト設定をそのまま使用することをお勧めします。

   e)「ユーザー属性」チェック・ボックスを有効にして、次のようなユーザー詳細を入力することもできます。
      i. ユーザー属性の名前
      ii. 属性の値を抽出するために評価される NetScaler ADC PI 式

iii. わかりやすい属性の名前

iv. ユーザー属性の形式を選択します。

これらの値は、発行された SAML アサーションに含まれています。この StyleBook を使用して NetScaler ADC が発行するアサーションには、最大 5 セットのユーザー属性を含めることができます。

5. LDAP 設定セクションで、Google Apps ユーザーを認証するための次の詳細を入力します。ドメインユーザーが会社の電子メールアドレスを使用して NetScaler ADC インスタンスにログオンできるようにするには、以下を構成する必要があります。

   a) **LDAP (Active Directory)** ベース。認証を許可する Active Directory（AD）内にユーザーアカウントが存在するドメインの基本ドメイン名を入力します。たとえば、dc=netscaler、dc=com

   b) **LDAP**（**Active Directory**）バインド **DN**。AD ツリーを参照する権限を持つドメインアカウント (構成を容易にするために電子メールアドレスを使用) を追加します。たとえば、CN= マネージャ、dc=netscaler、dc=com

   c) **LDAP (Active Directory)** バインド **DN** パスワード。認証用のドメインアカウントのパスワードを入力します。

   d) このセクションに入力する必要があるその他のフィールドは次のとおりです。

      i. NetScaler ADC がユーザーを認証するために接続する LDAP サーバーの IP アドレス

      ii. LDAP サーバーの FQDN 名

      > 注:
      >
      > 上記の 2 つのうち少なくとも 1 つ (LDAP サーバの IP アドレスまたは FQDN 名) を指定する必要があります。

      iii. NetScaler ADC がユーザーを認証するために接続する LDAP サーバーポート（デフォルトは 389 です）。

      iv. LDAP ホスト名。これは、検証がオンになっている場合（デフォルトではオフになっています）、LDAP 証明書を検証するために使用されます。

      v. LDAP ログイン名属性。ログイン名の抽出に使用されるデフォルトの属性は「SAMAccountName」です。

      vi. その他のオプションの LDAP 設定

6. SAML IdP SSL 証明書セクションでは、SSL 証明書の詳細を指定できます。

   a) 証明書名。SSL 証明書の名前を入力します。

   b) 証明書ファイル。ローカルシステムまたは NetScaler ADM 上のディレクトリから、SSL 証明書ファイルを検索します。

c) 証明書キー形式。ドロップダウンリストボックスから、証明書と秘密キーファイルの形式を選択します。サポートされている形式は、.pem と.der ファイル拡張子です。

d) 証明書キー名。証明書の秘密鍵の名前を入力します。

e) 証明書キーファイル。ローカルシステムまたは NetScaler ADM から、証明書の秘密鍵を含むファイルを選択します。

f) 秘密鍵のパスワード。秘密鍵ファイルがパスフレーズで保護されている場合は、このフィールドにそれを入力します。

g) 証明書の詳細設定チェックボックスを有効にして、証明書の有効期限通知期間などの詳細を入力したり、証明書有効期限モニターを有効または無効にしたりすることもできます。

7. 上記で入力した SAML IdP 証明書で NetScaler ADC に CA パブリック証明書をインストールする必要がある場合は、オプションで IdP SSL CA 証明書を選択できます。詳細設定で「Is a CA Certificate」を必ず選択してください。
8. オプションで、[SAML SP SSL 証明書] を選択して、Google Apps (SAML SP) からの認証リクエストの検証に使用する Google SSL 証明書 (公開鍵) を指定できます。
9. [ターゲットインスタンス] をクリックし、この Google Apps SSO 構成を展開する NetScaler ADC インスタンスを選択します。[作成] をクリックして構成を作成し、選択した NetScaler ADC インスタンスに構成を展開します。

> 注
>
> 更新アイコンをクリックして、NetScaler ADM で最近検出された NetScaler ADC インスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。

また

> ヒント
> » Citrix
> では、実際の構成を実行する前に、「ドライラン 」を選択 して、StyleBook によってターゲットの Citrix ADC インスタンス上に作成された構成オブジェクトを視覚的に確認することをお勧めします。

SSO Office 365 StyleBook

February 6, 2024

Microsoft™ Office 365 は、Microsoft がサブスクリプションベースで提供する、クラウドベースの生産性向上およびコラボレーションアプリケーションのスイートです。これには、Exchange、SharePoint、Office、Skype for Business iness など、Microsoft の一般的なサーバーベースのアプリケーションが含まれています。シングル・サインオン（SSO）により、ユーザーはすべてのエンタープライズ・クラウド・アプリケーションにアクセスできます。

- 管理者コンソールにサインインする管理者を含む
- エンタープライズ認証情報を使用して、すべての Microsoft Office 365 サービスにワンタイムサインオンします。

SSO Office 365 StyleBook を使用すると、NetScaler ADC インスタンスを介して Microsoft オフィス 365 の SSO を有効にすることができます。NetScaler ADC を SAML アイデンティティプロバイダー（IdP）として、Microsoft Office 365 を SAML サービスプロバイダーとして使用して、SAML 認証を構成できるようになりました。

この StyleBook を使用して NetScaler ADC インスタンスで Microsoft Office 365 の SSO を有効にするには、次の手順が必要です。

1. 認証仮想サーバーの構成
2. SAML IDP ポリシーとプロファイルの設定
3. 認証仮想サーバーへのポリシーとプロファイルのバインド
4. インスタンスの LDAP 認証サーバーとポリシーの設定
5. LDAP 認証サーバーとポリシーを、インスタンスに構成されている認証仮想サーバーにバインドします。

この統合が正常に機能するために最低限必要なソフトウェアバージョンを示します。統合プロセスは、同じバージョンの上位バージョンでも機能するはずです。

Product	最低限必要なバージョン
——	————————
Citrix ADC	11.0、エンタープライズ/プラチナライセンス

次の手順は、適切な外部および内部 DNS エントリが既に作成されていることを前提としています。これらのエントリは、認証要求を NetScaler ADC が監視する IP アドレスにルーティングするために不可欠です。

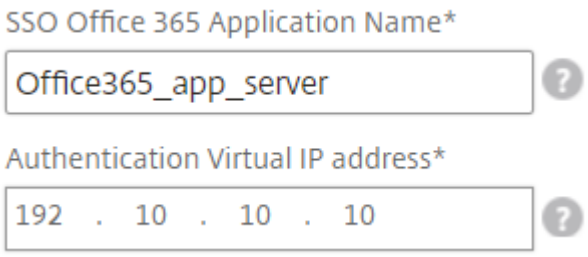
以下の手順は、SSO Office 365 StyleBook をビジネスネットワークに実装するのに役立ちます。

SSO Microsoft オフィス **365 StyleBook** を展開するには

1. Citrix Application Delivery Management（ADM）で、「アプリケーション」>「**StyleBook**」に移動します。**StyleBook** ページには、Citrix ADM で使用できるすべての StyleBook が表示されます。下にスクロールして **SSO Office 365 StyleBook** を見つけてください。[構成を作成] をクリックします。
2. StyleBook がユーザーインターフェイスページとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。
3. 次のパラメーターの値を入力します：

    a) アプリケーション名。ネットワークに展開する SSO Microsoft Office 365 構成の名前。

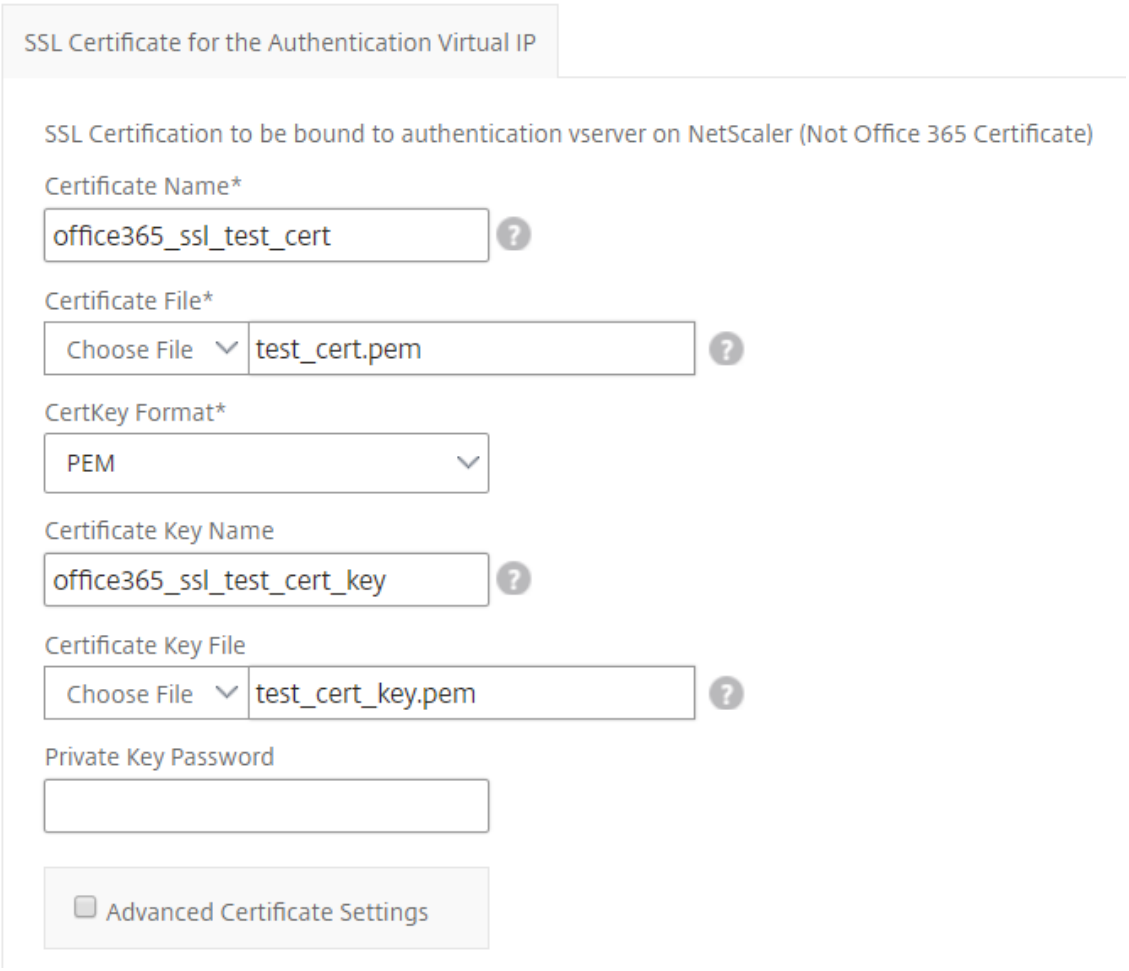
    b) 認証仮想 **IP** アドレス。Microsoft Office 365 SAML IdP ポリシーがバインドされている AAA 仮想サーバが使用する仮想 IP アドレス。



4. **SSL** 証明書の設定セクションで **、SSL 証明書の名前と証明書キーを入力します。

   > 注
   >
   > これは Office 365 サービスプロバイダー証明書ではありません。この SSL 証明書は、NetScaler ADC インスタンス上の仮想認証サーバーにバインドされます。

5. ローカルストレージフォルダからそれぞれのファイルを選択します。また、秘密鍵パスワードを入力して、暗号化された秘密鍵を PEM 形式でロードすることもできます。



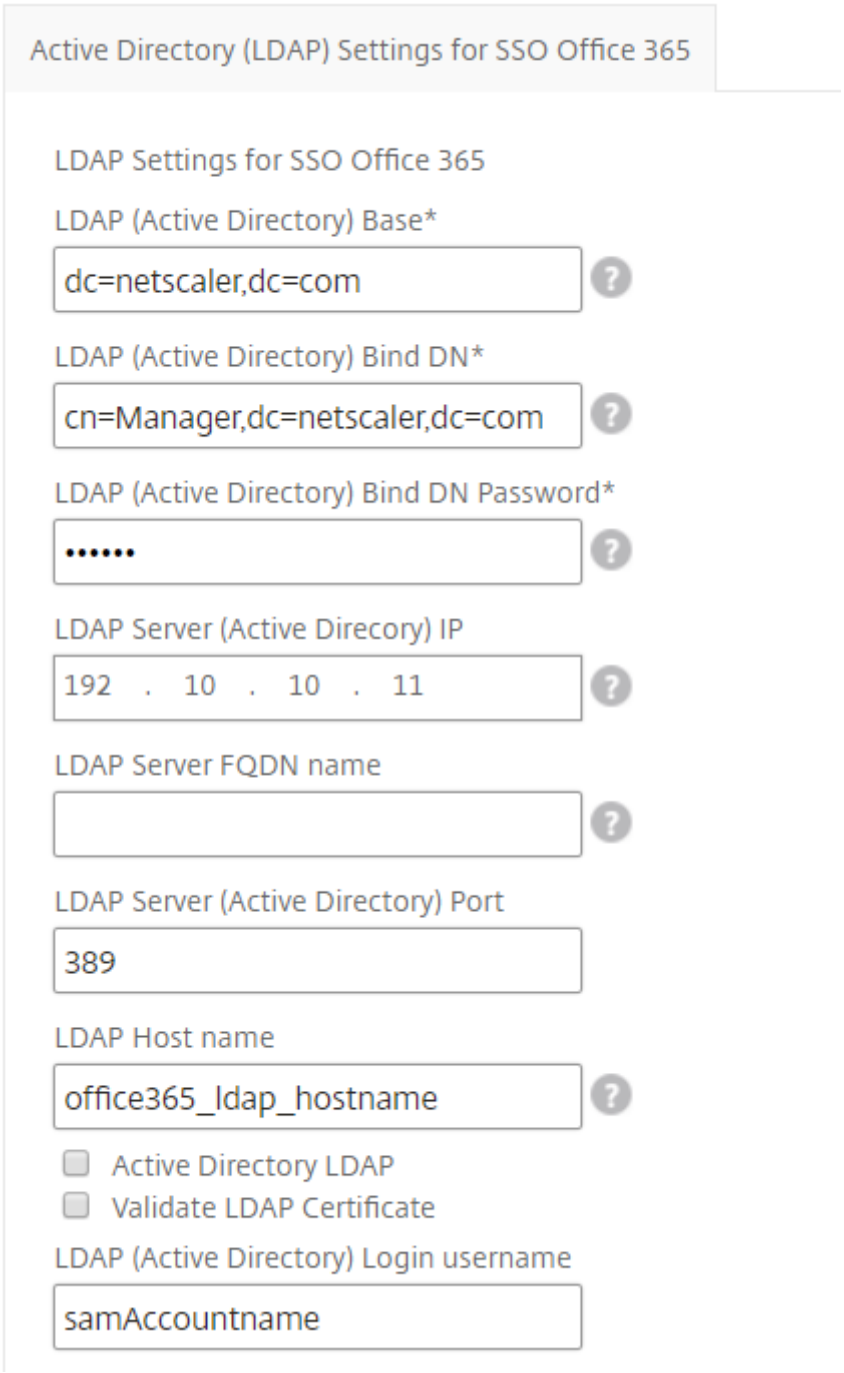
6. **[** 証明書の詳細設定] チェックボックスをオンにすることもできます。ここでは、証明書の有効期限通知期間などの詳細を入力したり、証明書の有効期限モニターを有効または無効にすることができます。

7. **SSL** 証明書で **NetScaler ADC** に **CA** パブリック証明書をインストールする必要がある場合は、オプションで認証仮想 **IP** チェックボックスに **SSL** CA 証明書を選択できます。上記の「証明書の詳細設定」セクションで「**Is a CA Certificate** 」を選択してください。
8. [**SSO Office 365** の **LDAP** 設定] セクションで、次の詳細を入力して Office 365 ユーザーを認証します。ドメインユーザーが会社の電子メールアドレスを使用して NetScaler ADC インスタンスにログオンできるようにするには、次のように構成します。

   - **LDAP (Active Directory)** ベース。認証を許可する Active Directory（AD）内にユーザーアカウントが存在するドメインの基本ドメイン名を入力します。たとえば、dc=netscaler、dc=com
   - **LDAP**（**Active Directory**）バインド **DN**。AD ツリーを参照する権限を持つドメインアカウント (構成を容易にするために電子メールアドレスを使用) を追加します。たとえば、CN= マネージャ、dc=netscaler、dc=com
   - **LDAP (Active Directory)** バインド **DN** パスワード。認証用のドメインアカウントのパスワードを入力します。
   - このセクションに入力する必要があるその他のフィールドは次のとおりです。
     - NetScaler ADC がユーザーを認証するために接続する LDAP サーバーの IP アドレス。
     - LDAP サーバーの FQDN 名。

       > 注:
       >
       > 上記の 2 つのうち少なくとも 1 つ (LDAP サーバの IP アドレスまたは FQDN 名) を指定する必要があります。

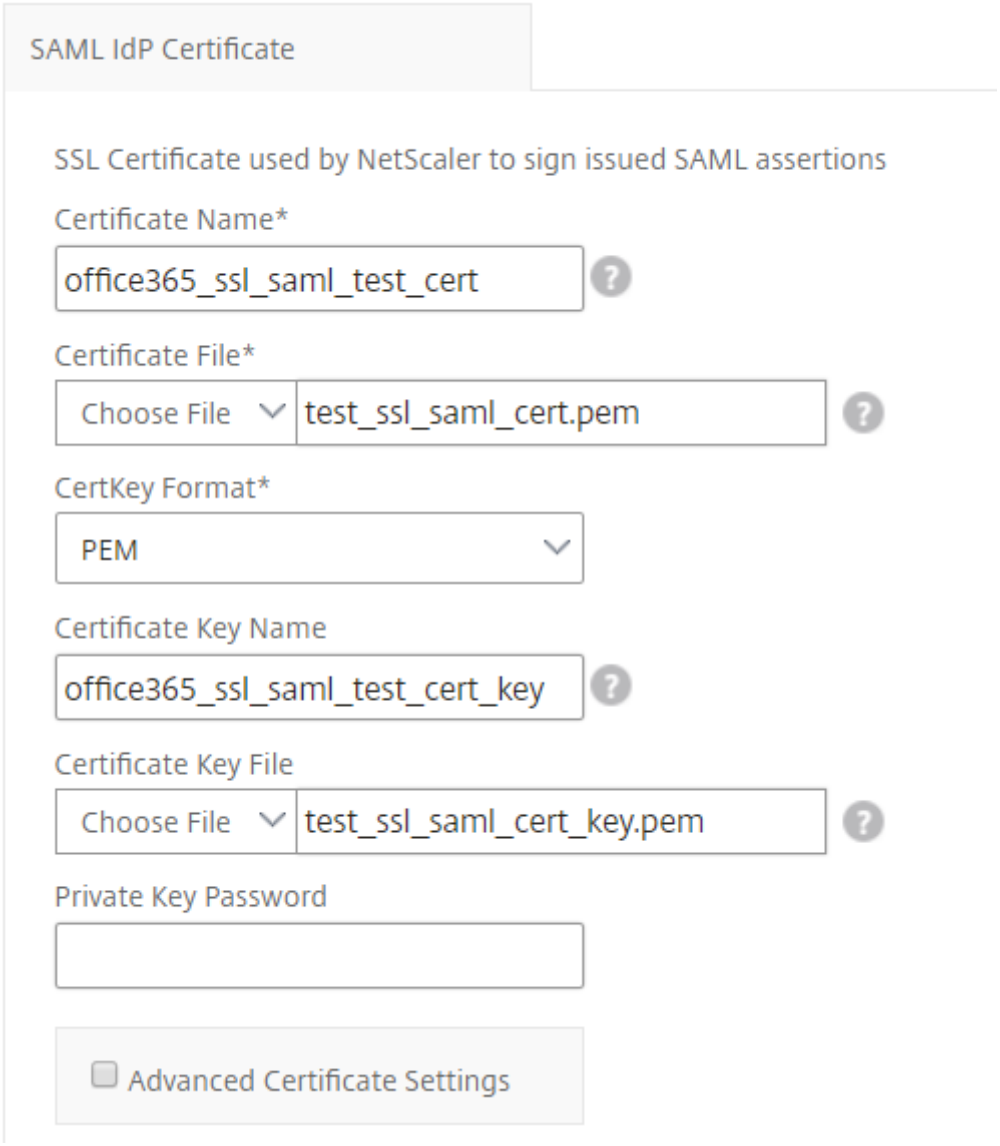
     - NetScaler ADC がユーザーを認証するために接続する LDAP サーバーポート（デフォルトは 389 です）。LDAPS は 636 を使用している。
     - LDAP ホスト名。検証がオン (デフォルトではオフ) の場合、ホスト名は LDAP 証明書の検証に使用されます。
     - LDAP ログイン名属性。ログイン名の抽出に使用されるデフォルトの属性は「SAMAccountName」です。
     - その他のオプションの LDAP 設定。



9. **SAML IdP** 証明書 セクションでは、SAML アサーションに使用される SSL 証明書の詳細を指定できます。
   - 証明書名。SSL 証明書の名前を入力します。
   - 証明書ファイル。ローカルシステム上のディレクトリから SSL 証明書ファイルを選択します。
   - 証明書キー形式。ドロップダウンリストボックスから、証明書と秘密キーファイルの形式を選択します。サポートされている形式は、.pem と.der ファイル拡張子です。
   - 証明書キー名。証明書の秘密鍵の名前を入力します。

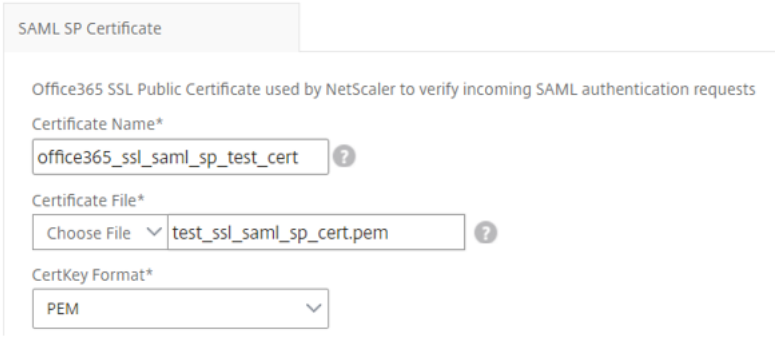
- 証明書キーファイル。ローカルシステムから証明書の秘密キーを含むファイルを選択します。
- 秘密鍵のパスワード。プライベートキーファイルを保護するパスフレーズを入力します。

[証明書の詳細設定] チェックボックスをオンにすることもできます。ここでは、証明書の有効期限通知期間などの詳細を入力したり、証明書の有効期限モニターを有効または無効にすることができます。



10. 上記の **SAML IdP** 証明書で **NetScaler ADC** に **CA** パブリック証明書をインストールする必要がある場合は、オプションで「SAML IdP CA 証明書」を選択できます。上記の [****** 証明書の詳細設定**]** セクションで **[CA** 証明書です ******] を選択してください。
11. [**SAML SP** 証明書] セクションで、Office 365 SSL パブリック証明書について次の詳細を入力します。この証明書は、NetScaler ADC インスタンスが受信した SAML 認証要求を検証するために使用されます。
    - 証明書名。SSL 証明書の名前を入力します。

- 証明書ファイル。ローカルシステム上のディレクトリから SSL 証明書ファイルを選択します。
- 証明書キー形式。ドロップダウンリストボックスから、証明書と秘密キーファイルの形式を選択します。サポートされている形式は、.pem と.der ファイル拡張子です。
- **[** 証明書の詳細設定] チェックボックスをオンにすることもできます。ここでは、証明書の有効期限通知期間などの詳細を入力したり、証明書の有効期限モニターを有効または無効にすることができます。



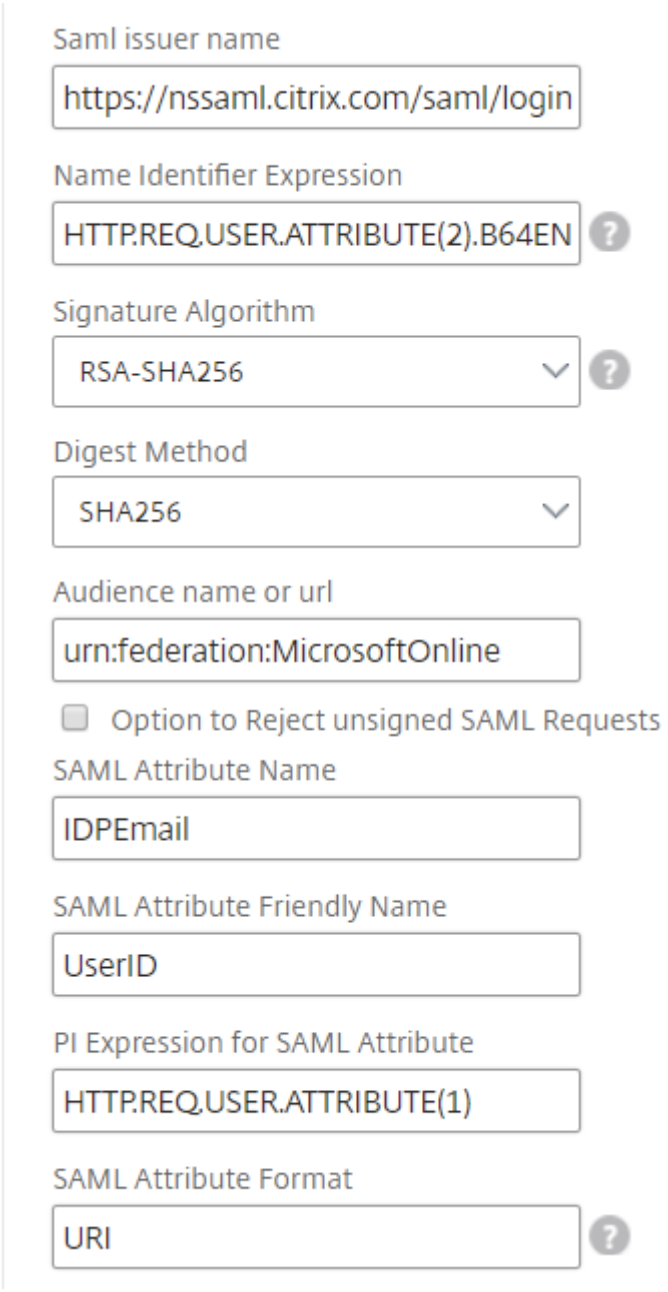
12. **SAML Idp** 設定セクションでは、手順 3 で作成した AAA 仮想サーバーで使用される SAML IDP プロファイルとポリシーを作成することで、Citrix ADC インスタンスを SAML ID プロバイダーとして構成できます。

    - **SAML** 発行者名。このフィールドには、認証仮想サーバーのパブリック FQDN を入力します。例: `https://<Citrix ADC Auth VIP>/saml/login`
    - 名前識別子の表現。評価される NetScaler ADC 式を入力して、SAML アサーションで送信された SAML NameIdentifier を抽出します。例: `"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`
    - 署名アルゴリズム:SAML リクエスト/レスポンスを検証/署名するアルゴリズムを選択します (デフォルトは「RSA-SHA256」)。
    - ダイジェスト方式。SAML リクエスト/レスポンスのハッシュをダイジェストする方法を選択します (デフォルトは「SHA256」)。
    - オーディエンスの名前。サービスプロバイダー (Microsoft Office 365) を表すエンティティ名または URL を入力します。
    - **SAML** サービスプロバイダー **(SP) ID**。(オプション) NetScaler ADC ID プロバイダーは、この ID と一致する発行者名からの SAML 認証要求を受け入れます。
    - アサーションコンシューマサービス **URL**。ユーザー認証が成功した後、NetScaler ADC ID プロバイダーが SAML アサーションを送信する必要があるサービスプロバイダーの URL を入力します。アサーションコンシューマサービス URL は、ID プロバイダサーバサイトまたはサービスプロバイダサイトで開始できます。
    - このセクションには、他にも入力できるオプションフィールドがあります。たとえば、次のオプションを設定できます。
        - **SAML** 属性名。SAML アサーションで送信されるユーザー属性の名前。

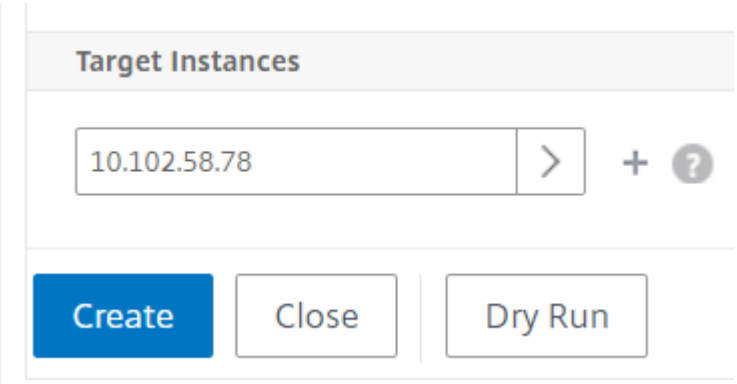
- **SAML** 属性のわかりやすい名前。SAML アサーションで送信されるユーザー属性のわかりやすい名前。
- **SAML** 属性の **PI** 式。デフォルトでは、次の NetScaler ADC ポリシー（PI）式が使用されます: HTTP.REQ.USER.ATTRIBUE（1）。このフィールドは、LDAP サーバー (メール) から送信される最初のユーザー属性を SAML 認証属性として指定します。
- ユーザー属性の形式を選択します。

これらの値は、発行された SAML アサーションに含まれています。

> ヒント
>
> Citrix では、これらの設定は Microsoft Office 365 アプリで動作することがテストされているため、デフォルト設定のままにしておくことをお勧めします。



13. ［ターゲットインスタンス］をクリックし、この Microsoft Office 365 SSO 構成を展開する NetScaler ADC インスタンスを選択します。［作成］をクリックして構成を作成し、選択した NetScaler ADC インスタンスに構成を展開します。



> ヒント
>
> 実際の構成を実行する前に、[**Dry Run**] を選択して、StyleBook によってターゲットの NetScaler ADC インスタンスに作成された構成オブジェクトを表示することをお勧めします。

StyleBook のための Microsoft Skype for Business

February 6, 2024

Skype for Business 2015 アプリケーションは、いくつかの外部構成要素に依存して機能します。Skype for Business ネットワークは、サーバーとそれらのオペレーティングシステム、データベース、認証システムと承認システム、ネットワーキングシステムとインフラストラクチャ、および電話の PBX（Private Branch Exchange：構内交換機）システムなど、さまざまなシステムで構成されています。Skype for Business Server 2015 は、標準版とエンタープライズ版の 2 つのバージョンで利用可能です。主な違いは、Enterprise Edition のみに高可用性機能のサポートが含まれている点です。高可用性を実装するには、複数のフロントエンドサーバーをプールに展開し、SQL サーバーをミラーリングする必要があります。

Enterprise Edition の展開では、異なる役割がある複数のサーバーを作成できます。

主要コンポーネント

Skype for Business 2015 アプリケーションの主な構成要素を次に示します。

- フロントエンドサーバー
- エッジサーバー
- Director サーバー
- データベース（SQL）サーバー

フロントエンドサーバー

Skype for Business アプリケーションでは、フロントエンドサーバーは、ネットワーク内の中核的なサーバーです。これは、ユーザー認証、登録、プレゼンス、アドレス帳、音声またはビデオ（Audio/Video：A/V）会議、アプリケーション共有、インスタントメッセージング、および Web 会議のためのリンクとサービスを提供します。Skype for Business 2015 Enterprise Edition を展開している場合、トポロジは、一般的には、1 つのフロントエンドプールに負荷分散される 2 台以上のフロントエンドサーバーと、Skype for Business データベースを保持する SQL Server インスタンスをホストする 1 つのデータベースサーバーで構成されています。

エッジサーバー

組織の内部ネットワークにログインしていない外部ユーザーが内部ユーザーと対話できるようにする必要がある場合は、Skype for Business 用のエッジサーバーを導入する必要があります。これらの外部ユーザーとしては、認証されている匿名のリモートユーザー、連携パートナー、またはその他のモバイルクライアントが考えられます。

Skype For Business エッジサーバーにおける役割には、次の 4 種類があります。

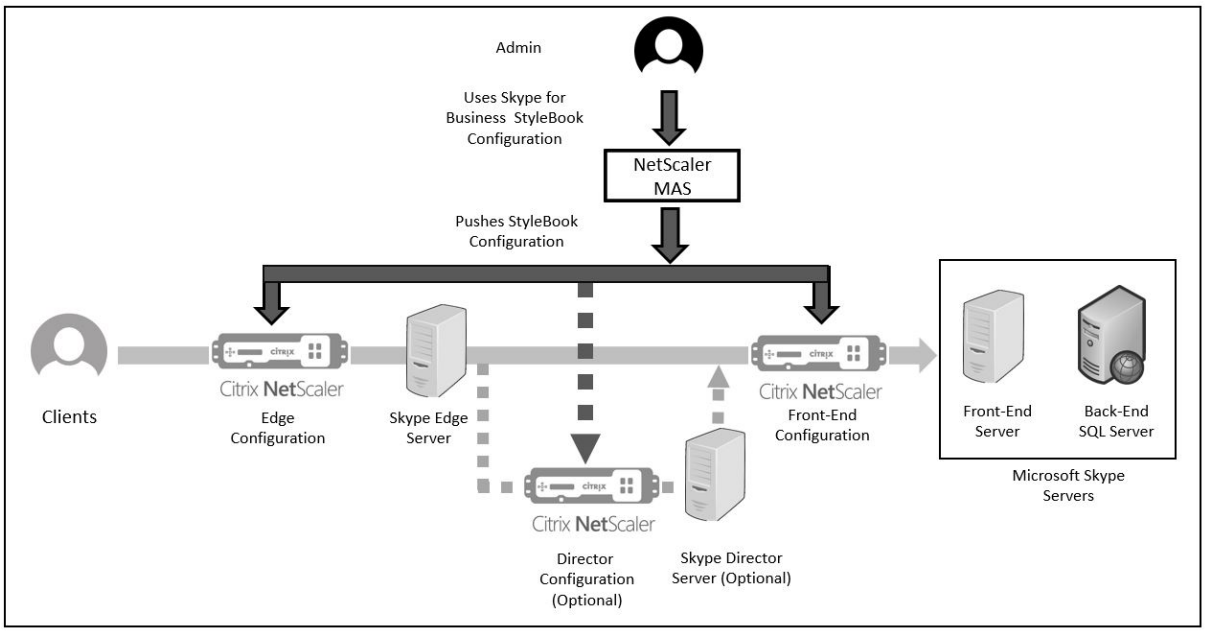
- Access Edge は、SIP トラフィックを処理し、外部接続を認証し、リモート接続を許可し、フェデレーション接続を許可します。
- Web Conferencing。これは、データ会議パケットを処理し、外部ユーザーに Skype for Business へのアクセスを許可します。
- A/V Conferencing。これは、A/V 会議パケットを処理し、音声とビデオ、アプリ共有、およびファイル転送の機能を外部ユーザーにも使用できるようにします。
- XMPP Proxy。これは、XMPP パケットを処理し、XMPP ベースのサーバーまたはクライアントに Skype for Business への接続を許可します。

Director サーバー

Skype for Business 2015 における Director サーバーの主要機能は、エンドポイントを認証し、ユーザーを各自のアカウントが含まれているプールに「案内する」ことです。Skype for Business 2015 では、ディレクターはスタンドアロンサーバー上で完全に専用の特定の役割ですが、オプションのサーバーです。これにより、構成の展開や削除がより簡単になることで、セキュリティが促進されます。

ダイレクタは、複数のプールが存在する場合に最も役立ちます。これは、ディレクタがエンドポイントの認証を一元化できるためです。また、リモートユーザーについては、Director はエッジプールとフロントエンドプールとの間の追加のホップの役割を果たし、それによって攻撃に対する保護が強化されます。

次の図は、ネットワーク内の Skype サーバーの展開を示しています。



エンタープライズでの **NetScaler ADC** インスタンスの構成

次の表は、以下の手順に含まれるサンプル構成で使用されている IP アドレスの一覧です。

Skype for Business Servers	仮想 IP アドレス	サーバー IP アドレス	NetScaler ADC インスタンス
エッジサーバー	外部 VIP - 192.20.20.20	192.20.20.21; 192.20.20.22	10.102.29.141
	内部 VIP - 10.10.10.20	10.10.10.21; 10.10.10.22	
フロントエンドサーバー	10.10.10.10	10.10.10.11; 10.10.10.12	10.102.29.60
Director サーバー	10.10.10.30	10.10.10.31; 10.10.10.32	10.102.29.93

フロントエンドサーバーを設定するには

1. NetScaler Application Delivery Management（ADM）で、［アプリケーション］>［構成］の順に選択し、［新規作成］をクリックします。「**StyleBook** の選択」ページには、NetScaler ADM で使用できるすべての StyleBook が表示されます。下にスクロールして、**Microsoft Skype for Business 2015 StyleBook** を選択します。StyleBook がユーザーインターフェイスページとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。

2. エッジサーバーセクションに、ネットワーク内のすべてのエッジサーバーの次の仮想 IP (VIP) アドレスと IP アドレスを入力します。

   a) Access Edge、web conferencing Edge、および A/V Edge のために使用される、エッジサーバーの外部 VIP アドレスと IP アドレス。
   b) 内部ネットワークに接続されるエッジサーバーの内部 VIP アドレスと IP アドレス。
   c) ネットワーク内の 2 台の外部エッジサーバーと 2 台の内部エッジサーバー。

3. [フロントエンドサーバー] セクションで、Skype for Business フロントエンドサーバー用に作成する仮想フロントエンドサーバー (VIP) の IP アドレスを入力します。また、ネットワーク内のすべての Skype for Business フロントエンドサーバーの IP アドレスも入力します。
4. [ディレクターサーバー] セクションで、Skype for Business アプリケーション用に作成される Director サーバーの仮想 IP アドレス (VIP) を入力します。また、ネットワーク内のすべての Skype for Business Director サーバーの IP アドレスを入力します。高可用性のためには、少なくとも 2 台の Director サーバーを作成します。
5. 詳細設定セクションには、3 つの Skype サーバーの NetScaler ADC インスタンスで構成されているすべてのデフォルトポートが表示されます。

次の表は、すべてのデフォルトポートとプロトコルのリストです。

ラベル	ポート	プロトコル	説明
HTTP Port	80	HTTP	HTTPS が使用されないときに、フロントエンドサーバーから Web ファームの完全修飾ドメイン名 (Fully Qualified Domain Name：FQDN) への通信のために使用されます。
HTTPS ポート	443	HTTPS	フロントエンドサーバーから Web ファームの FQDN への通信のために使用されます。
AutoDiscover Internal Port	4443	HTTPS	AutoDiscover サインインのための HTTPS 通信（リバースプロキシから）と HTTPS フロントエンドプール内通信です。

ラベル	ポート	プロトコル	説明
RPC Port	135	DCOM およびリモートプロシージャコール（Remote Procedure Call：RPC）	ユーザーの移動、ユーザーレプリケーターの同期、アドレス帳の同期など、DCOM ベースの操作のために使用されます。
SIP Port	5061	TCP（TLS）	すべての内部 SIP 通信のためにフロントエンドサーバーによって使用されます。
SIP Focus Port	444	HTTPS、TCP	Focus（Skype 会議状態を管理するコンポーネント）と個々のサーバーとの間の HTTPS 通信のために使用されます。
SIP Group Port	5071	TCP	応答グループアプリケーションの受信 SIP 要求のために使用されます。
SIP AppSharing Port	5065	TCP	アプリケーション共有の受信 SIP リスニング要求のために使用されます。
SIP Attendant Port	5072	TCP	出席者の受信 SIP 要求のために使用されます（つまり、ダイヤルイン会議用）。
SIP Conf Announcement Port	5073	TCP	Skype for Business サーバーの会議お知らせサービスの受信 SIP 要求のために使用されます（つまり、ダイヤルイン会議用）。
SIP CallPark Port	5075	TCP	CallPark アプリケーションの受信 SIP 要求のために使用されます。
SIP Call Admission Port	448	TCP	Skype for Business サーバーの帯域幅ポリシーサービスによる通話受付管理のために使用されます。

ラベル	ポート	プロトコル	説明
SIP Call Admission TURN Port	5080	TCP	音声/ビデオエッジ TURN トラフィックの帯域幅ポリシーサービスによる通話受付管理のために使用されます。
SIP Audio Test Port	5076	TCP	音声テストサービスの受信 SIP 要求のために使用されます。
HTTPS External Port	443	HTTPS	内部 Web 会議へのリモートユーザーアクセスのための SIP/TLS 通信用、および内部メディアおよび A/V セッションにアクセスするための STUN/TCP 送受信メディア通信用の外部ポートとして使用されます。
HTTPS Internal Port	443	HTTPS	内部 Web 会議へのリモートユーザーアクセスのための SIP/TLS 通信用、および内部メディアおよび A/V セッションにアクセスするための STUN/TCP 送受信メディア通信用の内部ポートとして使用されます。
SIP External Remote Access Port	5061	TCP	リモートユーザーアクセスまたはフェデレーションのための SIP/MTLS 通信用の外部ポートとして使用されます。
SIP Internal Remote Access Port	5061	TCP	リモートユーザーアクセスまたはフェデレーションのための SIP/MTLS 通信用の内部ポートとして使用されます。
SIP External STUN UDP Port	3478	UDP	STUN/UDP 送受信メディア通信のための外部ポートとして使用されます。

ラベル	ポート	プロトコル	説明
SIP Internal STUN UDP Port	3478	UDP	STUN/UDP 送受信メディア通信のための内部ポートとして使用されます。
SIP Internal IM Port	5062		内部ファイアウォールを通過して送信方向に流れる IM 通信の SIP/MTLS 認証のための内部ポートとして使用されます。
HTTP Port	80	TCP	Director から Web ファームの FQDN への初期通信のために使用されます。
HTTPS ポート	443	HTTPS	Director から Web ファームの FQDN への通信のために使用されます。
AutoDiscover Internal Port	4443	HTTPS	AutoDiscover サインインのために HTTPS 通信（リバースプロキシから）と HTTPS Director プール内通信に使用されます。
SIP Internal Port	5061	TCP	サーバー間の通信とクライアント接続のために使用されます。

6. 「ターゲットインスタンス」セクションで、3 つの Skype for Business サーバーをデプロイする 3 つの異なる Citrix ADC インスタンスを選択します。

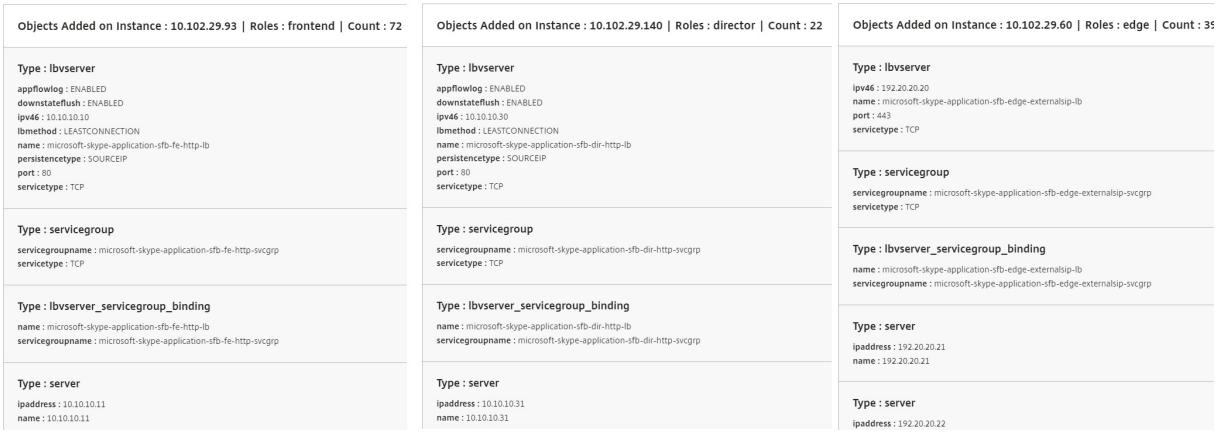
> 注
>
> 更新アイコンをクリックして、Citrix ADM で最近検出された Citrix ADC インスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。

7. 「作成」をクリック して、選択した Citrix ADC インスタンスで構成を作成します。

> ヒント
>
> インスタンスで実際の構成を実行する前に、［**Dr**y Run］を選択して、ターゲットインスタンスに作成する必要のある構成オブジェクトを確認することをお勧めします。
>
> 構成が正常に作成されると、StyleBook により、25 台の負荷分散仮想サーバーが作成されます。つまり、ポートごとに、1 台の負荷分散仮想サーバーが 1 つのサービスグループとともに定義されます。そのサービスグループは、その負荷分散仮想サーバーにバインドされています。また、その構成では、フロントエンドサーバーが

> サービスグループのメンバーとして追加され、それらがそのサービスグループにバインドされます。作成されたサービスグループメンバーの数は、作成されたフロントエンドサーバーの数と等しくなります。

次の図は、各サーバーで作成されるオブジェクトを示しています。



Microsoft Exchange StyleBook

February 6, 2024

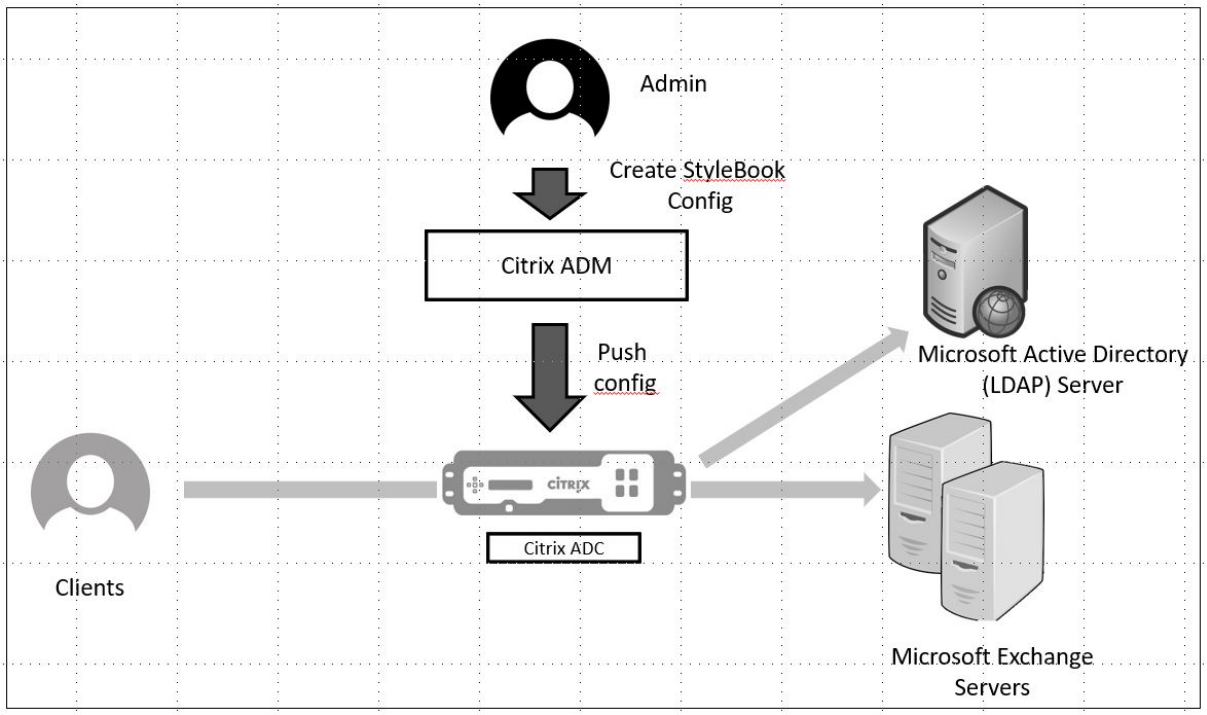
Microsoft Exchange 2016 StyleBook を使用して、ネットワーク内の Microsoft Exchange 2016 エンタープライズアプリケーションを最適化して保護する NetScaler ADC 構成を展開できます。Microsoft Exchange 2016 は、従業員やその他の利害関係者にメール、個人情報管理、およびメッセージングのサービスを提供するための主要なエンタープライズアプリケーションです。

Microsoft ExchangeStyleBook を使用して構成された **NetScaler ADC** 機能

Microsoft Exchange 2016 StyleBook は、Microsoft Exchange 2016 サーバー向けに以下の Citrix ADC 機能を有効化および構成します。

- 負荷分散 - 複数の Exchange サーバーを負荷分散できる、基本的な負荷分散です。
- コンテンツスイッチ - シングル IP アクセス、および正しい負荷分散仮想サーバーへのクエリのリダイレクトができるようになるコンテンツスイッチです。
- 書き換え - ユーザーを安全なページにリダイレクトします。
- SSL オフロード-SSL 処理を NetScaler ADC にオフロードするため、Exchange サーバーの負荷が軽減されます

次の図は、ネットワーク内の Exchange サーバーの展開を示しています。



前提条件

- 証明書ベースの認証の場合は、ネットワーク設定に含まれているアドレス可能なすべてのホストに、IP アドレスのみでなく解決できるドメイン名が必要となります。
- 必ず Microsoft Exchange 2016 サーバーの SIP ポートにアクセスできるようにしてください。

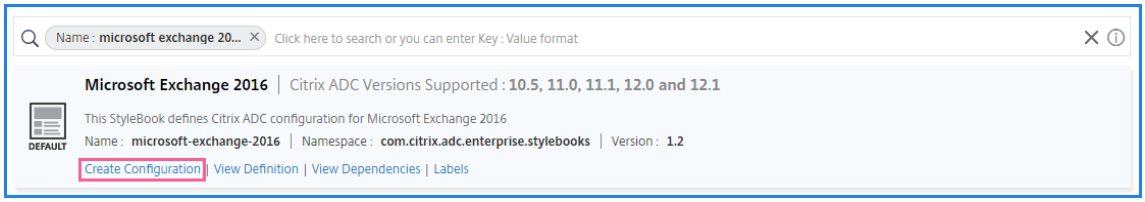
Microsoft Exchange StyleBook の設定

企業内の Microsoft Exchange StyleBook を構成して、NetScaler ADC 構成を展開します。

Microsoft Exchange アプリケーションを設定するには

1. NetScaler ADM で、［アプリケーション］>［**StyleBook**］に移動します。
2. **Microsoft Exchange 2016 StyleBook** を検索し、「構成の作成」をクリックします。

   StyleBook がユーザーインターフェイスフォームとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。



3. 以下のパラメーターに対して詳細を入力します。

   - **Exchange** アプリケーション名 -ネットワーク内の Microsoft Exchange アプリケーションの名前
   - **Exchange VIP** - Microsoft Exchange アプリケーションに対するクライアントリクエストを受信する Citrix ADC 上の仮想 IP アドレス
   - **Exchange Server** IP：ネットワーク内のすべての Exchange サーバの IP アドレス。

     IP アドレスをさらに追加する場合は、プラス (**+**) アイコンをクリックします。通常は、ネットワーク内で 2 つの Exchange サーバーが構成されます。

4.「交換証明書」セクションで、交換証明書を NetScaler ADM にアップロードします。証明書とキーファイルの両方の名前を入力し、ローカルストレージからアップロードします。キーファイルを暗号化するための秘密キーパスワードも指定できます。

   > 注**:**
   >
   > 証明書ファイルが「.pem」または「.der」形式であることを確認してください。NetScaler ADM は、他の形式のファイルを拒否します。

   証明書の有効期限の詳細や詳細設定を指定する場合は、「証明書の詳細設定」を選択します。

5. **Exchange Active Directory** 認証の構成 セクションで、データを入力して AD 設定を構成します。

   - **Active Directory** 認証 **VIP** -Citrix ADC アプライアンス上で AD (LDAP) 仮想サーバーを作成および構成するために使用される仮想 IP アドレス。
   - **Active Directory** サーバー **IP**-Active Directory ドメインコントローラーの IP アドレスです。
   - **Active Directory** ベースストリング-Active Directory の LDAP ベースストリング。たとえば、CN=Users,DC=CTXNSSFB,DC=COM などです。
   - **Active Directory LDAP** バインド識別名 **(DN)** -LDAP バインド識別名 (DN) を使用して、このオブジェクトを LDAP サーバー (AD) にバインドします。たとえば、「cn=Administrator,cn=Users,dc=acme,dc=com」などです。
   - **Active Directory LDAP** バインド識別名 **(DN)** パスワード -LDAP バインド識別名 (DN) は AD 認証のパスワードです
   - **Active Directory** ユーザー名属性 -ユーザー名の AD 属性。Citrix ADC は、LDAP 属性を使用して外部の Active Directory サーバーにクエリを実行します。たとえば、「sAMAccountName」などです。
   - **Active Directory** グループ属性名-LDAP サーバー上で設定されている LDAP グループ属性名。たとえば、LDAP のグループ属性には「memberOf」と入力します。
   - **Active Directory** サブ属性名 -LDAP サーバーで構成された LDAP サブ属性名。たとえば、LDAP のサブ属性は「cn」です。
   - **Active Directory** 認証ドメイン -認証に使用される AD/LDAP ドメイン名。たとえば、ctxnssfb.com などです。

6.「ターゲットインスタンス 」セクションで、この Exchange 構成を展開する Citrix ADC インスタンスを選択します。

> 注
>
> 最近検出された NetScaler ADC インスタンスを表示する場合は、更新アイコンをクリックします。

7.「作成」をクリックして構成ファイルを作成し、選択した Citrix ADC インスタンスで構成を実行します。

Citrix では、インスタンスで実際の構成を実行する前に、まず **Dry Run** を選択してターゲットインスタンスに作成された構成オブジェクトを確認することをお勧めします。

構成が正常に作成されると、StyleBook はコンテンツスイッチング仮想サーバー、5 つの負荷分散仮想サーバー、1 つの LDAP 認証仮想サーバーにバインドされた 1 つの LDAP ポリシーを作成します。また、対応するサービスグループが作成され、負荷分散仮想サーバーにバインドされます。

Microsoft SharePoint StyleBook

February 6, 2024

Microsoft SharePoint 2016 は、主にドキュメント管理機能とストレージシステムを提供する、主要なエンタープライズアプリケーションです。高度に構成可能であり、すべての主要 Web ブラウザーでサポートされています。

Microsoft SharePoint 2016 StyleBook を使用して、ネットワーク内の Microsoft SharePoint 2016 エンタープライズアプリケーションを最適化して保護する NetScaler ADC 構成を展開できます。

前提条件

- Microsoft SharePoint 2016
- NetScaler ADM、バージョン 12.0 以降
- NetScaler ADC、バージョン 10.5 以降

Microsoft の **SharePoint 2016 StyleBook** によって構成された **NetScaler ADC** の機能

Microsoft SharePoint 2016 StyleBook を使用して、Microsoft SharePoint 2016 の次の NetScaler ADC 機能を有効にして構成できます。

- 負荷分散
- コンテンツスイッチ
- レスポンダー
- 書き換え

- 圧縮
- 統合キャッシング

負荷分散

Citrix ADC 負荷分散は、要求をバックエンド SharePoint サーバーに均等に分散します。バックエンドサーバーをインテリジェントに監視することで、正常に動作していないサーバーに要求が送信されないようにします。

SharePoint 用 StyleBook では、12 台の負荷分散仮想サーバーが構成され、各仮想サーバーは、ドキュメント、画像、オーディオ、ビデオ、およびその他のファイルタイプなど、特定の種類のコンテンツの負荷分散要求専用となります。

SharePoint StyleBook は、SSL ベースの LB 仮想サーバーを構成することにより、SharePoint アプリケーションの SSL モードをサポートするようになりました。SSL がフロントエンドプロトコルとして選択されていることを確認します。仮想ポートは、デフォルトで 443 に設定されています。SSL を選択して、サービスグループ (SharePoint アプリケーションサーバー) をターゲットの負荷分散仮想サーバーにバインドすることもできます。バックエンドプロトコルはデフォルトで HTTP に設定されていることに注意してください。

コンテンツの切り替え

コンテンツスイッチ機能は、要求された特定種類の SharePoint コンテンツ（たとえば、ドキュメント、画像、およびオーディオまたはビデオファイル）に基づいて複数の負荷分散仮想サーバーにわたりクライアント要求を分散するために使用されます。コンテンツスイッチモジュールにより、受信トラフィックが、その種類のコンテンツを処理できる最適な負荷分散仮想サーバーに送られます。それにより、さまざまな最適化ポリシーをさまざまな種類のトラフィックに適用できます。たとえば、テキストドキュメントよりもさまざまな圧縮ポリシーやキャッシュポリシーをビデオに使用できます。

レスポンダー

NetScaler ADC インスタンスのレスポンダー機能を使用して、ユーザーを HTTP から HTTPS にシームレスにリダイレクトできます。レスポンダーは、カスタマイズされたエラーページを提供するように構成することもできます。レスポンダーポリシーは、アクションを実行する必要がある要求 (トラフィック) を決定し、各ポリシーを負荷分散仮想サーバーにバインドします。SharePoint 用 StyleBook には、ユーザーを HTTP の URL から HTTPS の URL にリダイレクトする構成が含まれています。

書き換え

書き換えモジュールは、要求/応答のヘッダー、URL、またはコンテンツを即座に変更するために使用されます。このモジュールは、トラフィック処理でインラインで動作します。それにより、特定のユースケースに応じてトラフィッ

クフローを変更できます。たとえば、書き換えにより、Web サイトのサーバーについて不要な情報が公開されることなく、要求されたコンテンツにアクセスできるようになります。

SharePoint 用 StyleBook では、書き換え機能は、ユーザーの要求から不要なヘッダーを削除するために使用されます。

圧縮

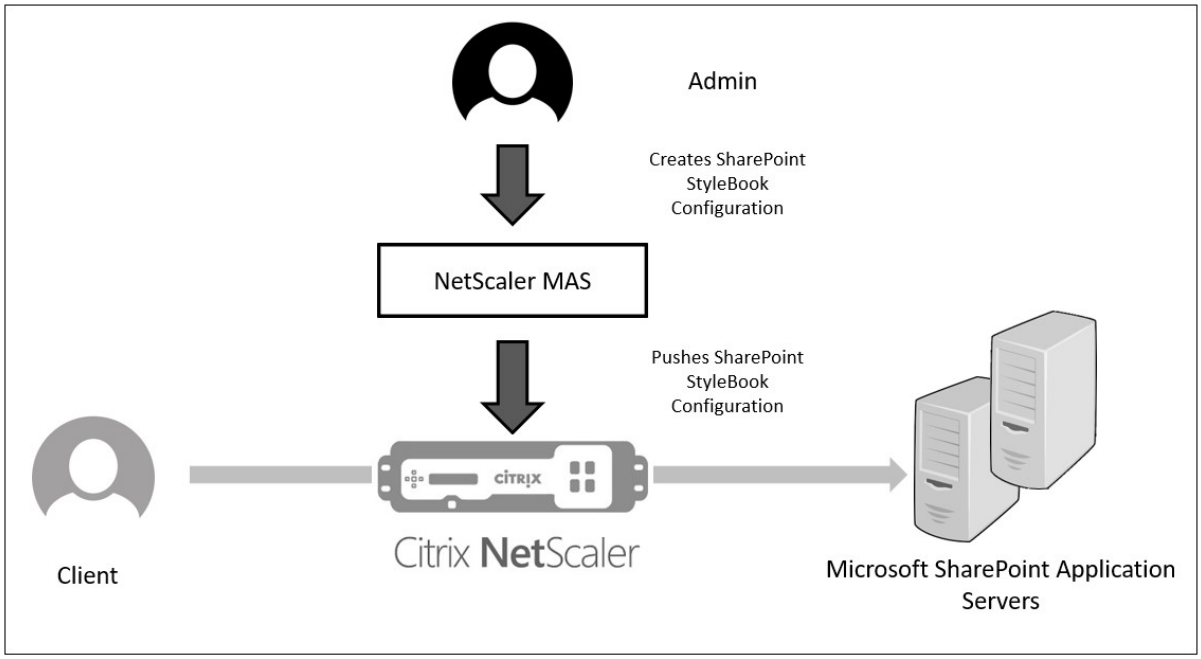
NetScaler ADC 圧縮エンジンは、圧縮可能なコンテンツを識別して圧縮します。このプロセスにより、データ転送時間が短縮され、クライアントに対するネットワーク帯域幅要件が減少するとともに、SharePoint コンテンツサーバー上の CPU サイクルが節約されます。NetScaler ADC インスタンスは、静的に生成されたデータと動的に生成されたデータの両方を圧縮できます。GZIP または DEFLATE 圧縮アルゴリズムが適用されることで、無関係で反復的な情報がサーバー応答から削除され、より簡潔で効率的な形式で元の情報が表されます。クライアントのブラウザーのデータ展開機能は、サポートされているアルゴリズム（GZIP、DEFLATE、またはこれら両方）によって異なります。

NetScaler ADC インスタンスは、HTML、XML、プレーンテキスト、カスケーディングスタイルシート（CSS）、および Microsoft Office ドキュメントのテキストを圧縮するように構成されていますが、GIF または JPG 形式の画像は圧縮しません。トラフィック圧縮の主な利点には、帯域幅コストの減少、WAN（Wide Area Network：ワイドエリアネットワーク）の遅延の減少、サーバーパフォーマンスの向上があります。

統合キャッシング

NetScaler ADC のインメモリキャッシュには、頻繁に要求されるコンテンツをユーザーに迅速に配信するために、SharePoint オブジェクトを保存できます。キャッシュされるコンテンツには、ダウンロードしたドキュメントや、オーディオ、ビデオ、および画像ファイルなどがあります。

次の図は、NetScaler ADM を使用して SharePointStyleBook 構成を展開する NetScaler ADC インスタンスによるネットワークフロントエンドでの SharePoint サーバーの展開を示しています。



SharePoint StyleBook の構成を展開する

次の作業は、ビジネスネットワークで Microsoft SharePoint 2016 StyleBook を展開する場合に役立ちます。

Microsoft SharePoint 2016 StyleBook をデプロイするには:

1. NetScaler ADM で、［アプリケーション］>［管理］>［構成］の順に選択し、［新規作成］をクリックします。

   「**StyleBook** の選択」ページには、NetScaler ADM で使用できるすべての StyleBook が表示されます。

2. 下にスクロールして [**Microsoft SharePoint 2016 StyleBook**] を選択します。

   > 注**:**
   >
   > NetScaler ADM で、「アプリケーション」>「構成」>「**StyleBooks**」に移動します。下にスクロールして Microsoft SharePoint 2016 StyleBook を探し、「構成を作成」をクリックします。

   StyleBook は、この StyleBook で定義されているすべてのパラメータの値を入力できるユーザーインタフェースフォームとして開きます。

   次のパラメーターの値を入力します:

   a) **SharePoint** アプリケーション名。ネットワーク内で展開する SharePoint 構成の名前です。

   b) **SharePoint** 仮想 **IP**。NetScaler ADC インスタンスが Microsoft SharePoint アプリケーションのクライアント要求を受信する仮想 IP アドレス。

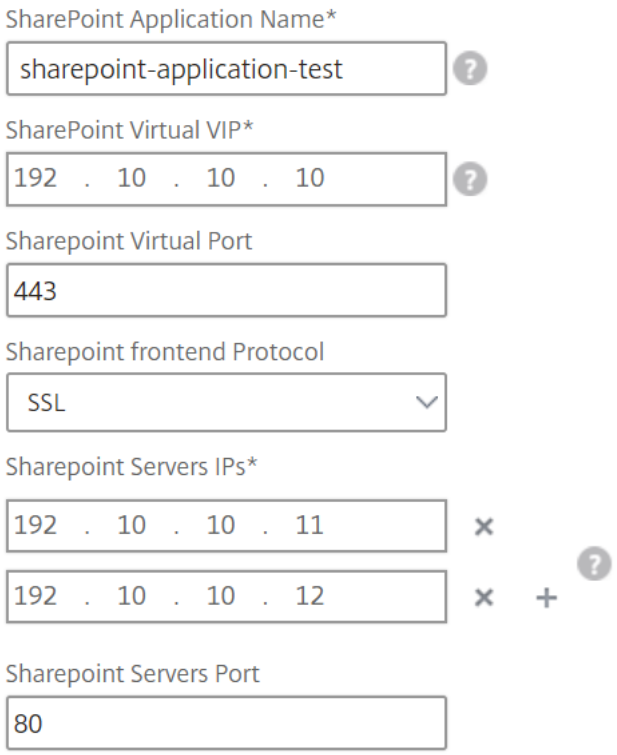
   c) **SharePoint** 仮想ポート。ユーザーが SharePoint アプリケーションにアクセスする際に使用する TCP ポート

d) **SharePoint** フロントエンドプロトコル。ドロップダウンリストから SharePoint フロントエンドプロトコルを選択します。使用可能なオプションは、HTTP または SSL です。

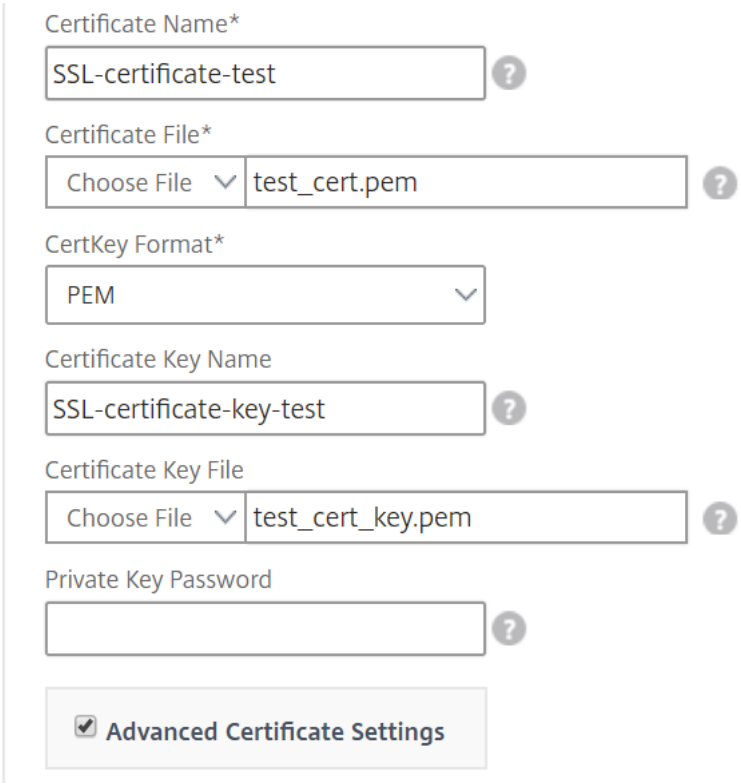
> 注:
>
> SSL を選択する場合は、この StyleBook の「SharePoint 詳細設定」セクションで「リライト構成」パラメータが有効になっていることを確認してください。

e) **SharePoint** サーバー **IP** ネットワーク内のすべての SharePoint サーバーの IP アドレス。

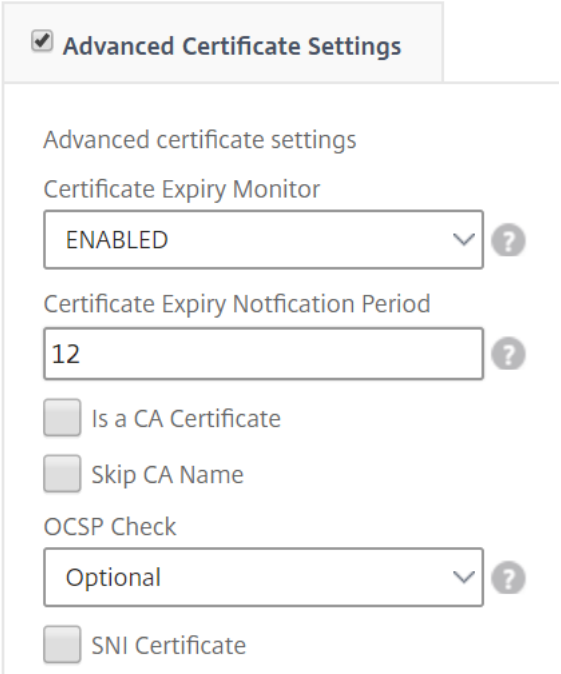
f) **SharePoint** サーバーポート。SharePoint サーバーで使用される TCP ポート番号です。デフォルト値は、80 です。必要な場合はこの値を編集できますが、必ず Microsoft SharePoint 2016 サーバー上でこのポートにアクセスできることを確認してください。



3. [**SSL** 証明書の設定] セクションで、[+] をクリックして SSL 証明書の名前と証明書キーを入力し、ローカルストレージフォルダからそれぞれのファイルを選択します。

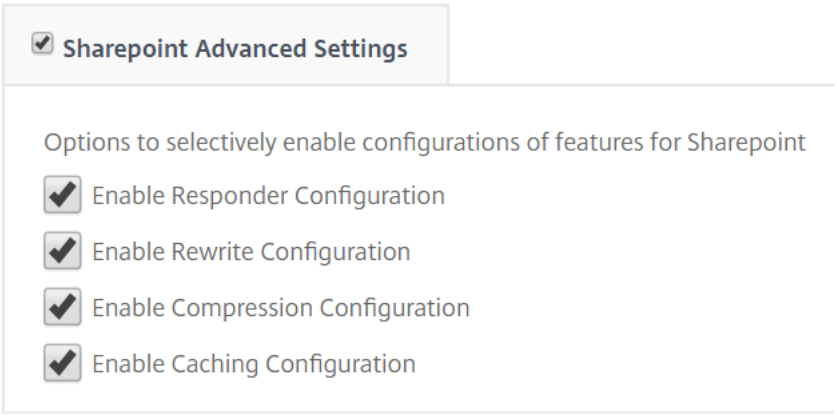


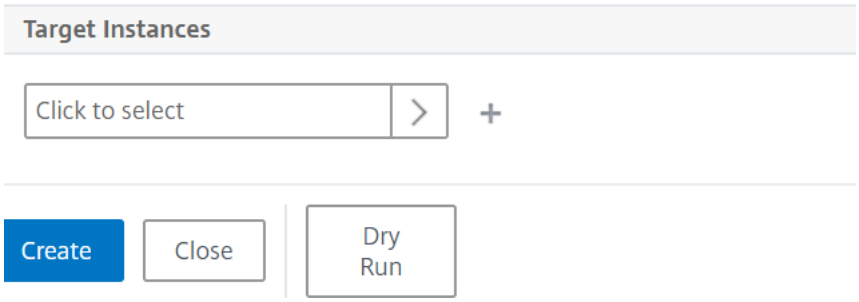
4. 必要に応じて、[証明書の詳細設定] をクリックして、SSL 証明書の有効期限の監視を有効または無効にします。証明書の有効期限監視を有効にする場合は、証明書の有効期限が近づくこの数日後に NetScaler ADM がアラームを発行するように日数を設定します。OCSP チェックをオプション機能または必須機能にするオプションもあります。



5. [SharePoint の詳細設定] セクションでは、NetScaler ADC インスタンスで構成する NetScaler ADC 機能を有効にできます。負荷分散機能とコンテンツスイッチ機能はインスタンス上でデフォルトで構成されますが、その他の機能（つまり、インスタンス上で構成する必要がある、レスポンダー構成、書き換え構成、圧縮構成、および統合キャッシュ構成）を選択できます。
6. 「ターゲットインスタンス」をクリックし、この SharePoint 構成を展開する NetScaler ADC インスタンスを選択します。「作成」をクリックして構成を作成し、選択した NetScaler ADC インスタンスに構成を展開します。

> 注
>
> 更新アイコンをクリックして、Citrix ADM で最近検出された Citrix ADC インスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。





> 注:
>
> Citrix では、実際の構成を実行する前に、「ドライラン」を選択して、ターゲットインスタンスに作成される構成オブジェクトを確認することをお勧めします。

構成が作成され、正常に展開されると、SharePoint 用 StyleBook により、1 台のコンテンツスイッチ仮想サーバーと 12 台の負荷分散仮想サーバーが作成されます。ポリシーとサービスグループも作成され、それらが負荷分散仮想サーバーにバインドされます。作成されるポリシーは、構成パックの作成中に StyleBook で選択した機能によって異なります。

NetScaler ADC インスタンスに定義されているオブジェクトの表示

NetScaler ADM で構成パックを作成すると、SharePoint StyleBook の NetScaler ADC インスタンスで作成されたすべてのオブジェクトを表示できます。[アプリケーション] > [管理] > [構成] に移動し、[作成されたオブジェクトを表示] をクリックします。次の図は、作成されたオブジェクトの一部を示しています。この例では、「NetScaler ADM から SharePointStyleBook 構成を展開する」に示されている IP アドレスが指定されています。

Type : lbvserver

appflowlog : DISABLED
backuppersistencetimeout : 20
downstateflush : DISABLED
ipv46 : 0.0.0.0
lbmethod : LEASTCONNECTION
name : sharepoint application test frontpage services lb
persistencebackup : SOURCEIP
persistencetype : COOKIEINSERT
port : 0
servicetype : HTTP
timeout : 20

Type : servicegroup

cip : DISABLED
cka : YES
cmp : NO
downstateflush : DISABLED
healthmonitor : NO
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp
servicetype : HTTP
sp : ON
state : ENABLED
tcpb : NO
useproxyport : NO
usip : NO

Type : lbvserver_servicegroup_binding

name : sharepoint-application-test-frontpage-services-lb
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.11
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.12
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : csaction

name : sharepoint-application-test-cs-frontpage-services-csaction
targetlbvserver : sharepoint-application-test-frontpage-services-lb

Type : cspolicy

action : sharepoint-application-test-cs-frontpage-services-csaction
policyname : sharepoint-application-test-cs-frontpage-services-cspol
rule : HTTP.REQ.HEADER("X-Vermeer-Content-Type").EXISTS

Type : csvserver_cspolicy_binding

name : sharepoint-application-test-cs
policyname : sharepoint-application-test-cs-frontpage-services-cspol
priority : 10

Microsoft ADFS proxy StyleBook

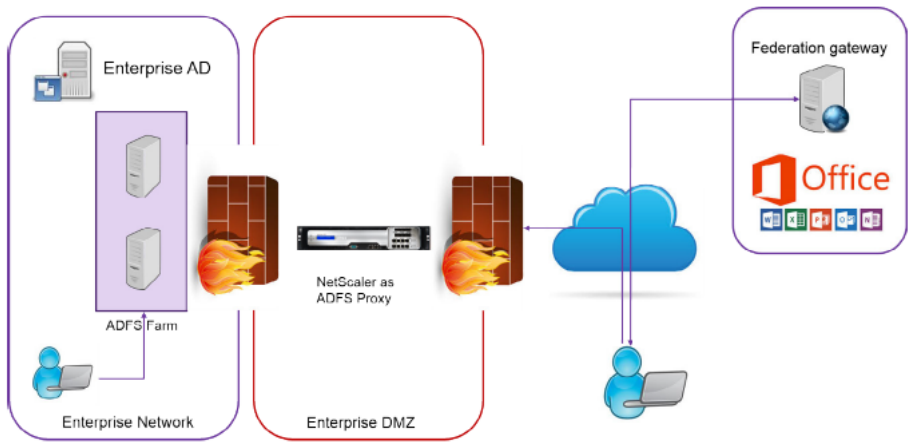
February 6, 2024

Microsoft™ ADFS プロキシは、内部のフェデレーション対応リソースとクラウドリソースの両方にシングルサインオンアクセスを提供することで重要な役割を果たします。クラウドリソースの一例が Office 365 です。ADFS プロキシサーバーの目的は、インターネットからアクセスできない ADFS サーバーに要求を受信および転送することです。ADFS プロキシはリバースプロキシで、通常は組織の境界ネットワーク (DMZ) にあります。ADFS プロキシは、リモートユーザーの接続とアプリケーションアクセスにおいて重要な役割を果たします。

NetScaler ADC には、フェデレーション ID の安全な接続、認証、および処理を可能にする正確なテクノロジーが搭載されています。NetScaler ADC を ADFS プロキシとして使用すると、DMZ に追加のコンポーネントを展開する必要がなくなります。

NetScaler Application Delivery Management（ADM）の Microsoft ADFS プロキシ StyleBook を使用すると、NetScaler ADC インスタンスで ADFS プロキシサーバーを構成できます。

次の図は、Citrix ADC インスタンスをエンタープライズ DMZ の ADFS プロキシサーバーとして展開しているところを示しています。



ADFS プロキシとして NetScaler ADC を使用する利点

1. 負荷分散と ADFS プロキシの両方のニーズに対応
2. 内部ユーザーアクセスシナリオと外部ユーザーアクセスシナリオの両方をサポート
3. 事前認証のための豊富なメソッドをサポート
4. ユーザーにシングルサインオン環境を提供します
5. アクティブプロトコルとパッシブプロトコルの両方をサポート

    a) アクティブなプロトコルアプリの例としては、Microsoft Outlook、Microsoft Skype for Business
    b) パッシブプロトコルアプリの例としては、Microsoft Outlook Web アプリ、Web ブラウザー

6. DMZ ベースの展開のための強化されたデバイス
7. Citrix ADC ADC のコア機能を追加して付加価値を高める

    a) コンテンツスイッチ
    b) SSL オフロード
    c) 書き換え
    d) セキュリティ (NetScaler ADC AAA)

プロトコルベースのアクティブなシナリオでは、Office 365 に接続して認証情報を入力できます。Microsoft フェデレーションゲートウェイは、アクティブなプロトコルクライアントに代わって (ADFS プロキシを介して) ADFS サービスにアクセスします。次に、ゲートウェイは基本認証 (401) を使用して認証情報を送信します。NetScaler ADC は、ADFS サービスにアクセスする前にクライアント認証を処理します。認証後、ADFS サービスはフェデレーションゲートウェイに SAML トークンを渡します。次に、フェデレーションゲートウェイはトークンを Office 365 に送信してクライアントアクセスを提供します。

パッシブクライアントの場合、ADFS プロキシ StyleBook は Kerberos 制約付き委任 (KCD) ユーザーアカウントを作成します。KCD アカウントは、Kerberos SSO 認証で ADFS サーバーに接続するために必要です。StyleBook は LDAP ポリシーとセッションポリシーも生成します。これらのポリシーは、パッシブクライアントの認証を処理する NetScaler ADC AAA 仮想サーバーに後でバインドされます。

StyleBook は、NetScaler ADC 上の DNS サーバーが ADFS 用に構成されていることを確認することもできます。

以下の構成セクションでは、アクティブプロトコルベースとパッシブプロトコルベースのクライアント認証の両方を処理するように NetScaler ADC を設定する方法について説明します。

構成の詳細

以下の表は、この統合を正常にデプロイするために最低限必要なソフトウェアバージョンを示しています。

Product	最低限必要なバージョン
Citrix ADC	11.0、エンタープライズ/プラチナライセンス

次の手順は、適切な外部および内部 DNS エントリが既に作成されていることを前提としています。

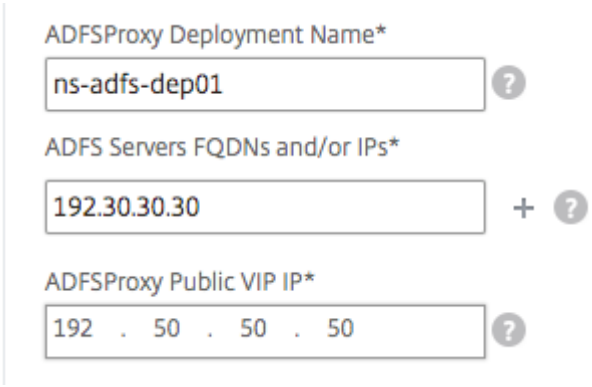
NetScaler ADM からの **Microsoft ADFS** プロキシ **StyleBook** 構成の展開

以下の手順は、Microsoft ADFS プロキシ StyleBook をビジネスネットワークに実装する際に役立ちます。

Microsoft ADFS プロキシ **StyleBook** をデプロイするには

1. NetScaler ADM で、［アプリケーション］>［**StyleBook**］に移動します。**StyleBook** ページには、Citrix ADM で使用できるすべての StyleBook が表示されます。
2. 下にスクロールして **Microsoft ADFS** プロキシ **StyleBook** を見つけてください。[構成を作成] をクリックします。
   StyleBook がユーザーインターフェイスページとして開き、この StyleBook で定義されているすべてのパラメーターの値を入力できます。
3. 次のパラメータに値を入力します。

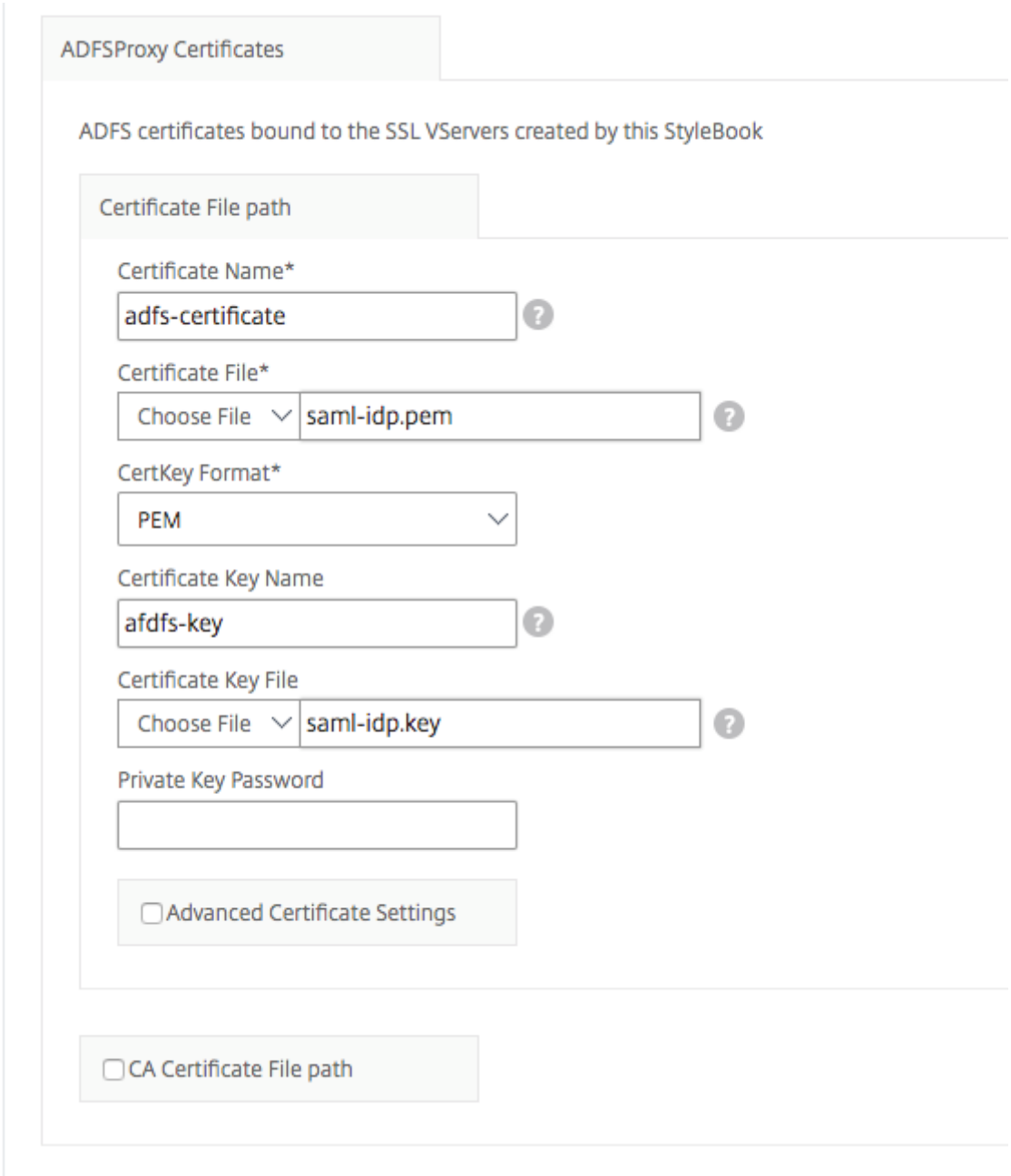
   a) **ADFS** プロキシ展開名。ネットワークに導入されている ADFS プロキシ構成の名前を選択します。
   b) **ADFS** サーバーの **FQDN** または **IP**。ネットワーク内のすべての ADFS サーバーの IP アドレスまたは FQDN (ドメイン名) を入力します。
   c) **ADFS** プロキシパブリック **VIP IP** ADFS プロキシサーバーとして NetScaler ADC 上のパブリック仮想 IP アドレスを入力します。



4. [**ADFS** プロキシ証明書] セクションで、SSL 証明書と証明書キーの詳細を入力します。

   この SSL 証明書は、NetScaler ADC インスタンスで作成されたすべての仮想サーバーにバインドされます。

   ローカルストレージフォルダからそれぞれのファイルを選択します。また、秘密キーのパスワードを入力して、暗号化された秘密キーを.pem 形式でロードすることもできます。



[証明書の詳細設定] チェックボックスをオンにすることもできます。ここでは、証明書の有効期限通知期間などの詳細を入力したり、証明書有効期限モニターを有効または無効にしたりできます。

5. **SSL** 証明書で **NetScaler ADC** に **CA** パブリック証明書をインストールする必要がある場合は、オプションで［SSL CA 証明書］チェックボックスをオンにできます。[証明書の詳細設定] セクションで [**CA** 証明書です] を選択していることを確認してください。
6. アクティブクライアントおよびパッシブクライアントの認証を有効にします。Active Directory でユーザー認証に使用されている DNS ドメイン名を入力します。その後、アクティブクライアントまたはパッシブクライアントのいずれか、あるいはその両方の認証を設定できます。

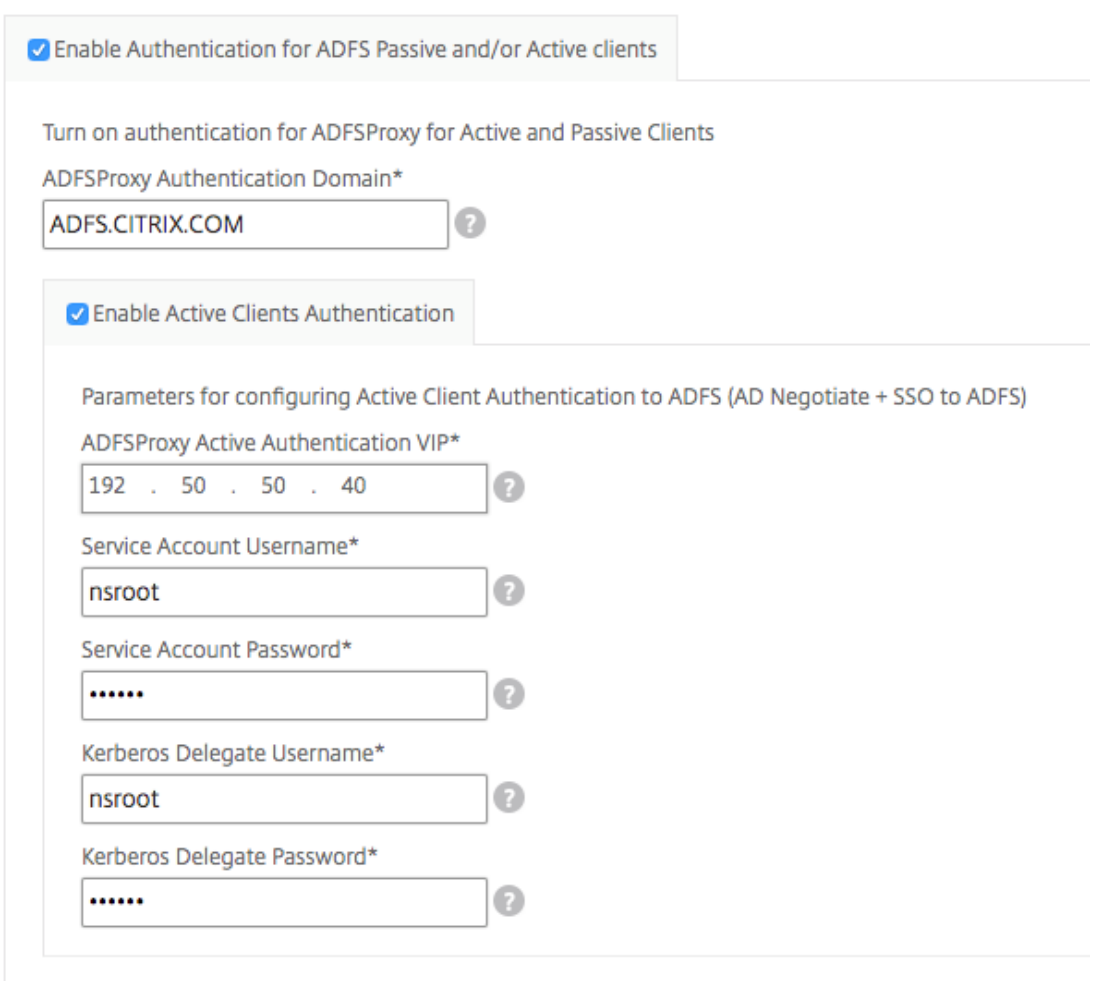
7. 次の詳細を入力して、アクティブなクライアントの認証を有効にします。

> 注:
>
> アクティブクライアントのサポートの設定は任意です。

a) **ADFS** プロキシアクティブ認証 **VIP** アクティブなクライアントが認証のためにリダイレクトされる NetScaler ADC インスタンス上の仮想認証サーバーの仮想 IP アドレスを入力します。

b) サービスアカウントのユーザー名。NetScaler ADC が Active Directory へのユーザーを認証するために使用するサービスアカウントのユーザー名を入力します。

c) サービスアカウントのパスワード。Active Directory に対するユーザーを認証するために NetScaler ADC が使用するパスワードを入力します。



8. 対応するオプションを有効にし、LDAP 設定を構成して、パッシブクライアントの認証を構成します。

> 注:
>
> パッシブクライアントのサポートの設定は任意です。

パッシブクライアントの認証を有効にするには、次の詳細を入力します。

a) **LDAP (Active Directory)** ベース。認証を許可する Active Directory (AD) 内にユーザーアカウントが存在するドメインの基本ドメイン名を入力します。たとえば、dc=netscaler、dc=com

b) **LDAP**（**Active Directory**）バインド **DN**。AD ツリーを参照する権限を持つドメインアカウント (構成を容易にするために電子メールアドレスを使用) を追加します。たとえば、CN= マネージャ、dc=netscaler、dc=com

c) **LDAP (Active Directory)** バインド **DN** パスワード。認証用のドメインアカウントのパスワードを入力します。

このセクションに値を入力する必要があるその他のフィールドは次のとおりです。

d) **LDAP** サーバ **(Active Directory) IP**。AD 認証が正しく機能するように、アクティブディレクトリサーバーの IP アドレスを入力します。

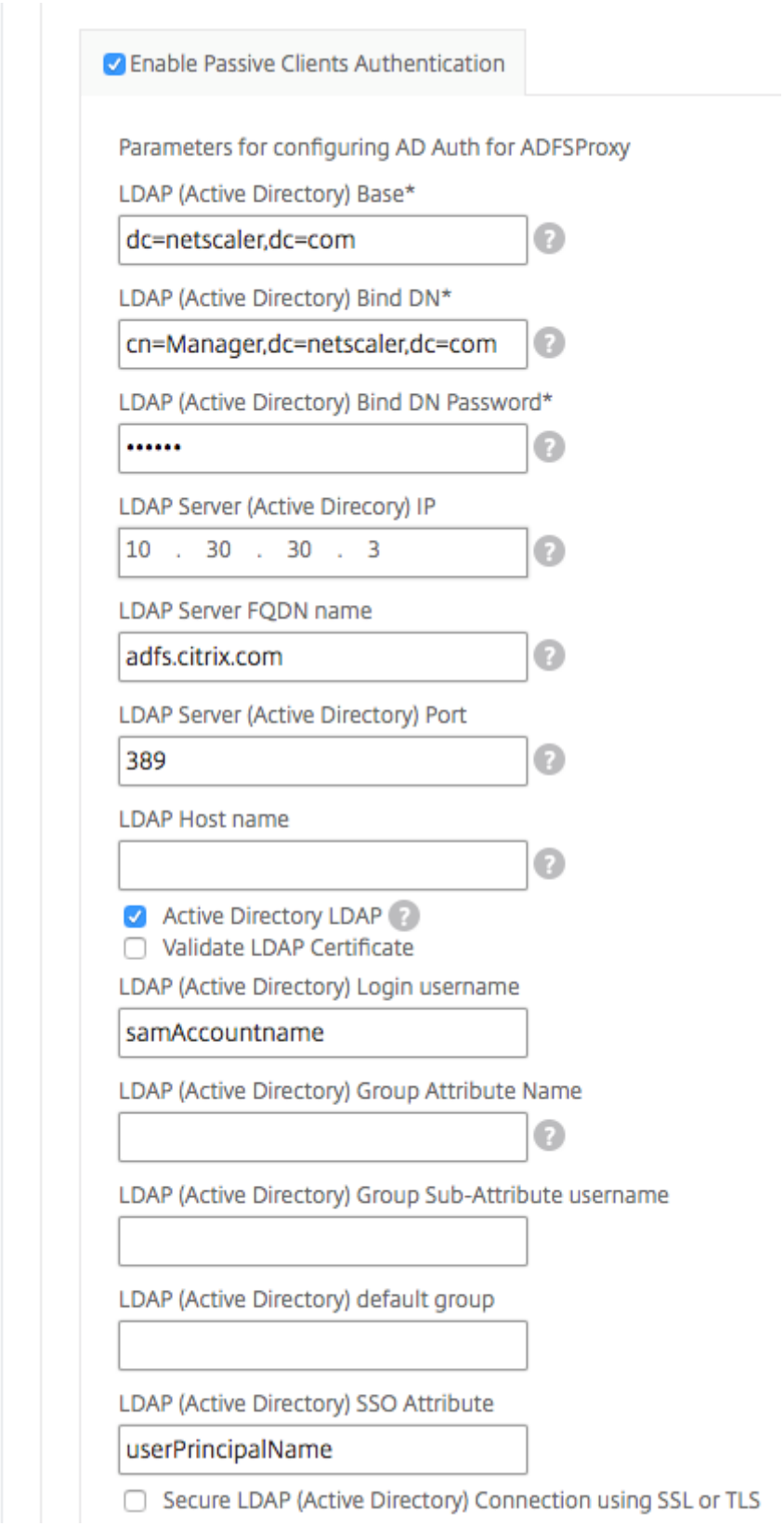
e) **LDAP** サーバーの **FQDN** 名。アクティブディレクトリサーバーの FQDN 名を入力します。FQDN 名はオプションです。ステップ 1 のように IP アドレスまたは FQDN 名を指定します。

f) **LDAP** サーバの **Active Directory** ポート。デフォルトでは、LDAP プロトコルの TCP ポートと UDP ポートは 389 ですが、セキュア LDAP の TCP ポートは 636 です。

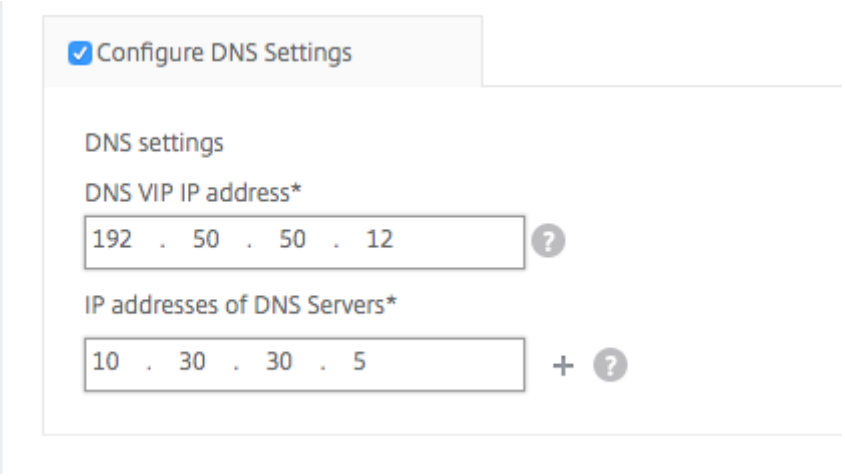
g) **LDAP**（**Active Directory**）ログインユーザ名。ユーザー名を「SAM アカウント名」として入力します。

h) **ADFS** プロキシパッシブ認証 **VIP**。パッシブクライアント用の ADFS プロキシ仮想サーバーの IP アドレスを入力します。

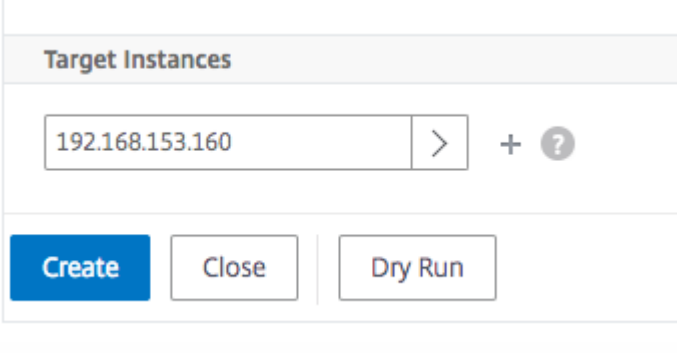
> 注**:**
>
> 「*」の付いたフィールドは必須です。



9. 必要に応じて、DNS サーバーの DNS VIP を構成することもできます。



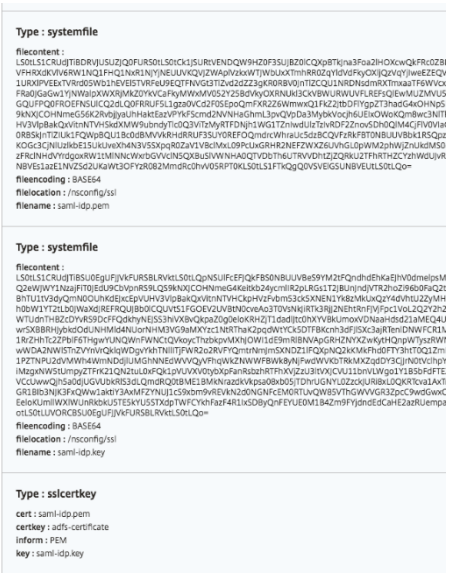
10. ［ターゲットインスタンス］をクリックし、この Microsoft ADFS プロキシ構成を展開する NetScaler ADC インスタンスを選択します。［作成］をクリックして構成を作成し、選択した NetScaler ADC インスタンスに構成を展開します。



> 注:
>
> Citrix では、実際の構成を実行する前に、「ドライラン」を選択することをお勧めします。まず、StyleBook によってターゲットの NetScaler ADC インスタンスに作成された構成オブジェクトを表示できます。その後、[作成] をクリックして、選択したインスタンスに設定をデプロイできます。

オブジェクトが作成されました

ADFS プロキシ構成が NetScaler ADC インスタンスに展開されると、いくつかの構成オブジェクトが作成されます。次の図は、作成されたオブジェクトのリストを示しています。



Objects Added on Instance : 192.168.153.160 | Count : 57

Type : nsfeature

Meta Properties
action : **enable**

feature : cs lb ssl rewrite aaa

Type : lbvserver

ipv46 : 192.50.50.12
name : ns-adfs-dep01-adfs-dns
port : 53
servicetype : DNS

Type : service

ip : 10.30.30.5
name : ns-adfs-dep01-dns-svc-1
port : 53
servicetype : DNS

Type : lbvserver_service_binding

name : ns-adfs-dep01-adfs-dns
servicename : ns-adfs-dep01-dns-svc-1

Type : authenticationnegotiateaction

domain : ADFS.CITRIX.COM
domainuser : nsroot
domainuserpasswd : nsroot
name : ns-adfs-dep01-negotiate-action

Type : authenticationpolicy

action : ns-adfs-dep01-negotiate-action
name : ns-adfs-dep01-negotiate-policy
rule : true

Type : aaakcdaccount

delegateduser : nsroot
kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
kcdpassword : nsroot
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
name : ns-adfs-dep01-adfs-auth401-tmsession-action
persistentcookie : ON
persistentcookievalidity : 3
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-auth401-tmsession-action
name : ns-adfs-dep01-adfs-auth401-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.40
maxloginattempts : 255
name : ns-adfs-dep01-adfs-auth401-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-auth401-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-negotiate-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-adfs-auth401-tmsession-policy
priority : 10

Type : authenticationldapaction

authentication : ENABLED
authtimeout : 30
followreferrals : OFF
ldapbase : dc=netscaler,dc=com
ldapbinddn : cn=Manager,dc=netscaler,dc=com
ldapbinddnpassword : nsroot
ldaploginname : samAccountname
name : ns-adfs-dep01-ldap-action
passwdchange : DISABLED
sectype : PLAINTEXT
serverip : 10.30.30.3
serverport : 389
ssonameattribute : userPrincipalName
svrtype : AD
validateservercert : NO

Type : authenticationpolicy

action : ns-adfs-dep01-ldap-action
name : ns-adfs-dep01-ldap-policy
rule : true

Type : aaakcdaccount

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
name : ns-adfs-dep01-adfs-ldap-tmsession-action
persistentcookie : OFF
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-ldap-tmsession-action
name : ns-adfs-dep01-adfs-ldap-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.30
maxloginattempts : 255
name : ns-adfs-dep01-adfs-ldap-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-ldap-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-ldap-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-adfs-ldap-tmsession-policy
priority : 10

Type : csvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-cs
port : 443
servicetype : SSL

Type : lbvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
port : 445
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : server

ipaddress : 192.30.30.30
name : 192.30.30.30

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") || HTTP.REQ.URL.CONTAINS("/federa

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
priority : 9800

Type : lbvserver

appflowlog : ENABLED
authentication : ON
authenticationhost : ADFS.CITRIX.COM
authn401 : OFF
authnvsname : ns-adfs-dep01-adfs-ldap-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
port : 446
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/ls/auth/integrated") || HTTP.REQ.URL.CONTAINS("/adfs/ls/wia")

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
priority : 9900

Type : lbvserver

appflowlog : ENABLED
authentication : OFF
authn401 : ON
authnvsname : ns-adfs-dep01-adfs-auth401-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
port : 444
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
rule : true

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
priority : 10000

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-cs

Type : rewritepolicylabel

labelname : ns-adfs-dep01-request-rewritepolicylabel
transform : HTTP_REQ

Type : rewritepolicylabel

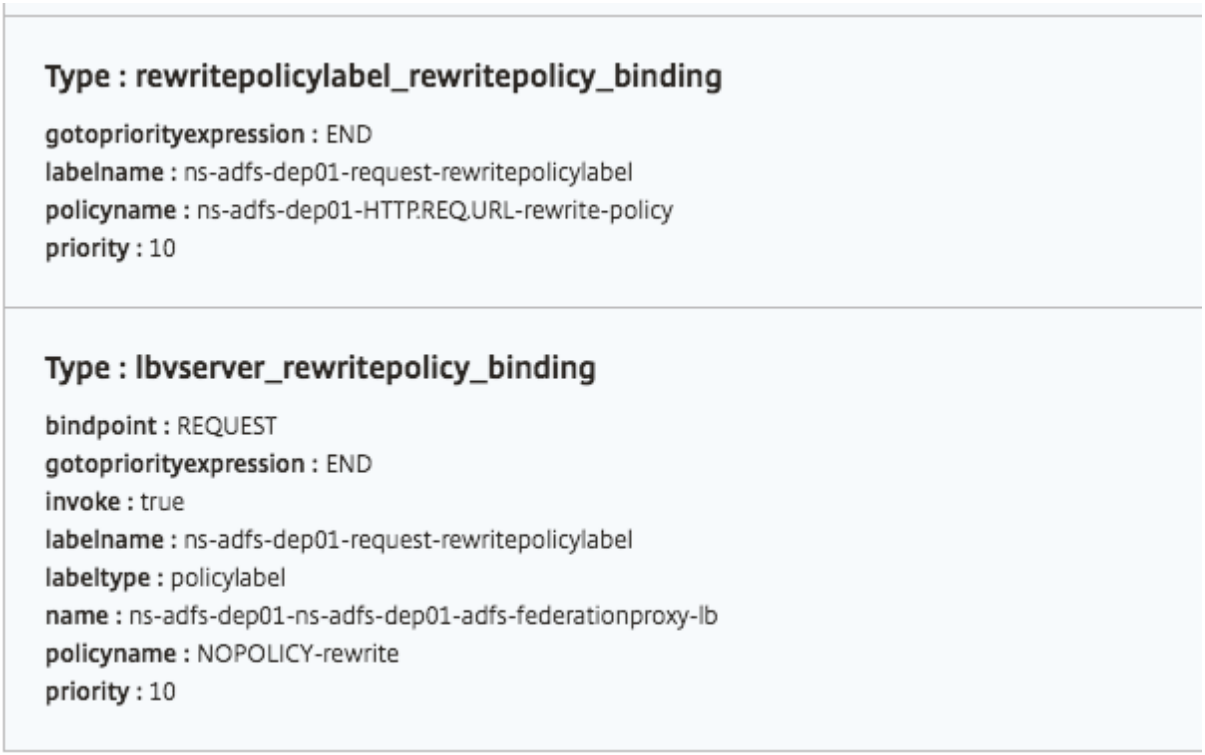
labelname : ns-adfs-dep01-response-rewritepolicylabel
transform : HTTP_RES

Type : rewriteaction

name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
stringbuilderexpr : "/adfs/services/trust/proxymex"
target : HTTP.REQ.URL
type : REPLACE

Type : rewritepolicy

action : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-policy
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") && (!HTTP.REQ.URL.CONTAINS("/trust/proxymex"))



Oracle e-business Stylebook

February 6, 2024

Oracle E-Business Suite は、統合されたグローバルなビジネス・アプリケーションの最も包括的なスイートです。このスイートは、組織がより良い意思決定を行い、コストを削減し、パフォーマンスを向上させることを可能にします。以下のアプリケーションで構成されています。

- エンタープライズリソースプランニング (ERP)
- 顧客関係管理 (CRM)
- サプライチェーン管理 (SCM)

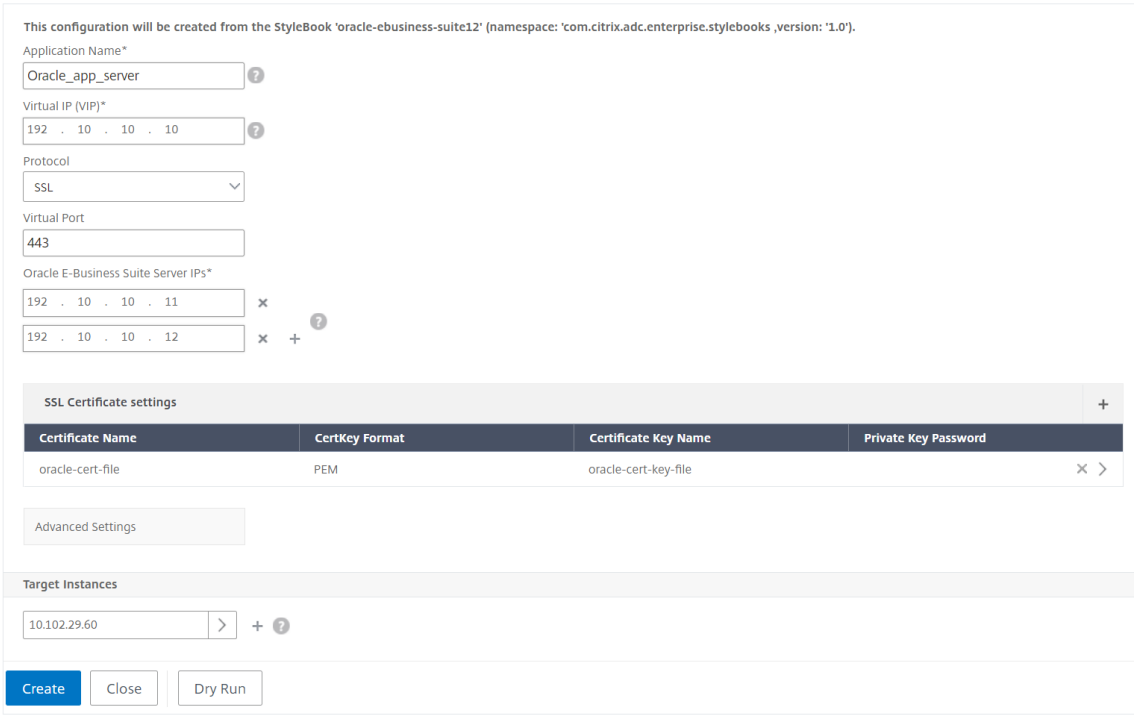
これらのコンピュータ・アプリケーションは、オラクルが開発または買収したものです。Oracle E-Business Suite 12.2 StyleBook を使用すると、選択した NetScaler ADC インスタンスに構成を展開できます。

この StyleBook は、負荷分散仮想サーバー、サービスグループ、およびサービスのリストで構成される負荷分散構成を作成します。また、サービスをサービスグループにバインドし、サービスグループを仮想サーバーにバインドできます。SSL を選択し、ローカルシステムから SSL ファイルとキーファイルを提供することで、暗号化された通信を選択できます。

Oracle E-Business Suite 12.2 の構成を作成するには

1. Citrix Application Delivery Management（ADM）で、「アプリケーション」>「構成」**>**「**StyleBooks**」に移動します。［**StyleBook** ］ページには、NetScaler ADM で使用可能なすべての StyleBook が表示されます。下にスクロールして、**Oracle E-Business Suite 12.2** を選択します。検索オプションを使用して StyleBook を検索することもできます。
2. StyleBook パネルの「構成を作成」をクリックします。
3. ロードバランサー設定セクションにロードバランサーアプリケーションの名前と仮想 IP アドレスを入力します。
4. 必要なプロトコルを選択します。ここには、HTTP と HTTPS/SSL の 2 つのオプションがあります。ポート番号を入力することもできます。
5. 負荷分散の対象となるネットワーク内のすべての Oracle E-Business Suite アプリケーションサーバーの IP アドレスを入力します。**+** をクリックして、さらにサーバの IP アドレスを追加します。
6. **SSL** 証明書の設定セクションで、ローカルストレージからそれぞれのファイルを選択します。**[** 証明書の詳細設定] チェックボックスをオンにすることもできます。ここでは、証明書の有効期限通知期間などの詳細を設定できます。証明書有効期限モニターを有効または無効にすることもできます。

   構成を作成する対象の NetScaler ADC インスタンスを選択し、［作成］をクリックします。



> ヒント
>
> 更新アイコンをクリックして、Citrix ADM で最近検出された Citrix ADC インスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。更新アイコンは現在、NetScaler

> ADM でのみ使用できます。

カスタム **StyleBook** の作成と使用

February 6, 2024

デプロイメント用に独自の StyleBook を作成し、それを CitrixApplication Delivery Management（ADM）にインポートして、構成オブジェクトを作成できます。また、API を使用して、StyleBook から構成を作成することもできます。

このドキュメントでは、次の内容について説明します。

はじめに

StyleBook の作成を始める前に、次の知識があることを確認してください。

- NITRO API。詳しくは、Nitro API のドキュメントを参照してください。
- YAML

StyleBook ファイルでは YAML 形式を使用します。YAML 形式の詳細については、「YAML 構文」を参照してください。

StyleBook を作成するときは、次に示す YAML のガイドラインに注意する必要があります。

- YAML では、大文字と小文字が区別されます。
- YAML では、インデントを適切に使用する必要があります。
- <spacebar> キーを使用して適切なインデントを作成します。<tab> キーは使用しないでください。<tab> キーを使用すると、StyleBook を MA Service にインポートする際にコンパイルエラーが発生します。
- 文字列を引用符で囲まないでください。文字列が句読点（ダッシュ、コロン、その他）を含む場合にのみ、文字列を引用符で囲ってください。数字を文字列として解釈する必要がある場合は、数字を引用符で囲むか、または StyleBook の組み込み関数 str() を使用します。
- YES/Yes/yes/Y/y/NO/no/No/n/N、ON/On/on/OFF/Off/off,、TRUE/true/truthy/FALSE/False/false/-falsely などのリテラルはブール値と見なされ、それぞれ真と偽と同等です。これらのリテラルを文字列として解釈するには、引用符で囲んでください。次に例を示します：
  - “YES”
  - “No”
  - “True”
  - “False” など。

> 注
>
> StyleBook ファイルを NetScaler ADM にインポートする前に、ファイルが YAML 形式に準拠しているかどうかを確認することをお勧めします。StyleBooks に組み込みの YAML バリデータを使用して、YAML コンテンツを検証およびインポートすることをお勧めします。
>
> StyleBook の設定では、作成 および 削除操作（**POST** および **DE** LETE HTTP メソッド）をサポートする Nitro 構成リソースのみを使用できます。詳しくは、Nitro API のドキュメントを参照してください。

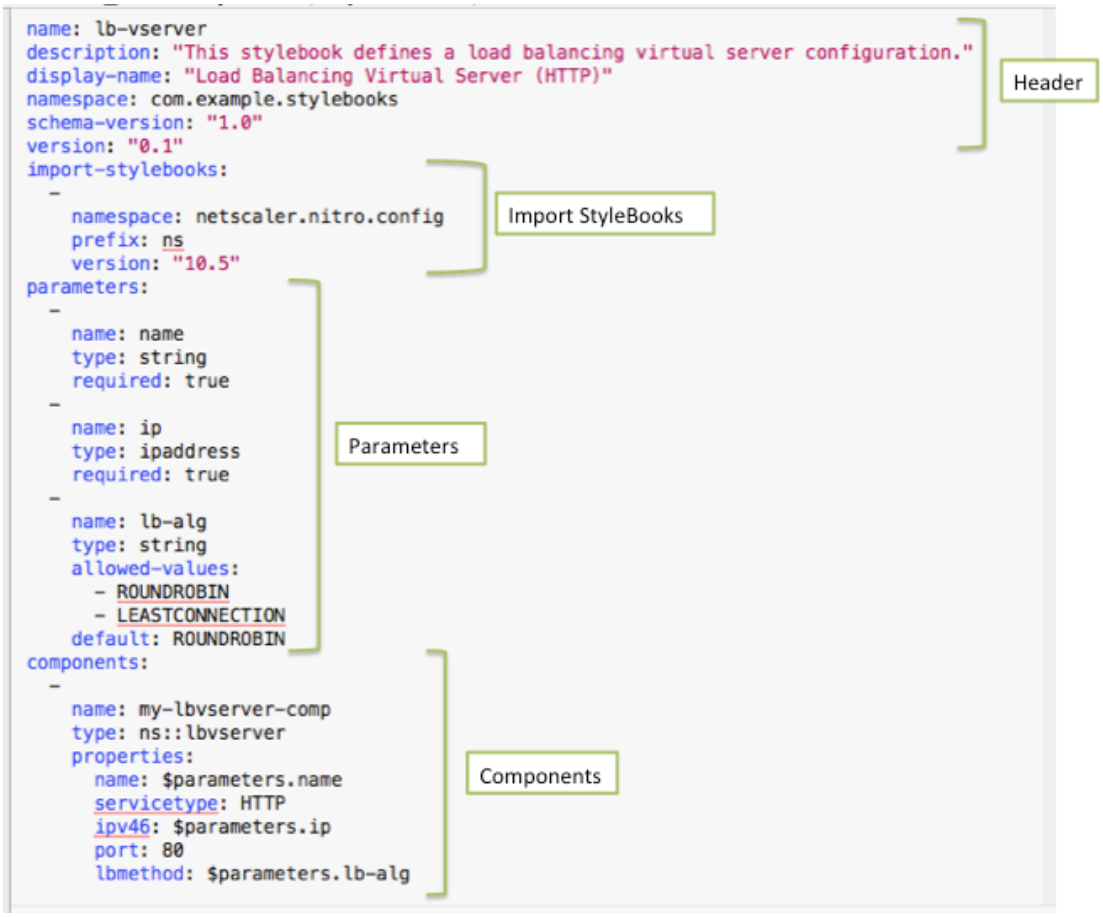
StyleBook の構造

StyleBook を作成するには、StyleBook の文法、構文、および構造を理解する必要があります。通常、StyleBook には、次のセクションが含まれます。

- ヘッダー: このセクションでは、StyleBook のアイデンティティを定義し、その機能を説明できます。これは必須セクションです。
- **Import StyleBooks**: このセクションでは、現在の StyleBook から参照する他の StyleBook を宣言できます。StyleBook を作成するには、NetScaler ADC NITRO 構成の StyleBooks または他の StyleBook をインポートする必要があります。これは必須セクションです。
- **Parameters**: このセクションでは、構成を作成するために必要な StyleBook のパラメーターを定義します。StyleBook では、このセクションに記述された入力が使用されます。これはオプションのセクションです。
- コンポーネント: このセクションでは、特定の構成用に StyleBook によって作成されるエンティティ (構成オブジェクト) を定義できます。このセクションは、StyleBook の中核です。Components では通常、Parameters セクションの入力値を使用して、StyleBook で生成される構成に適応させます。これはオプションのセクションです。

  StyleBook には、Parameters セクションと Components セクションのいずれか、または両方を記述できます。他の StyleBook で使用可能なパラメーターの一覧を定義する場合、Parameters セクションのみを含む StyleBook を作成すると便利です。これにより、一連の StyleBook 全体で、パラメーターグループが再利用しやすくなります。ユーザー入力を取得するパラメーターを定義せずに、StyleBook の属性値を指定する場合は、Components セクションのみを含む StyleBook を使用します。
- **Outputs**: Parameters セクションでは、StyleBook の入力を定義しましたが、この省略可能な Outputs セクションでは StyleBook の出力を定義します。構成を作成するユーザーは、この省略可能な Outputs セクションで指定したコンポーネントを、この StyleBook から、この StyleBook をインポートする他の StyleBook に公開できます。これにより、ユーザーおよびインポートする側の StyleBook は、公開されたコンポーネントのプロパティを参照できます。
- 操作:StyleBook には、StyleBook の一部である任意の仮想サーバー上の NetScaler ADM でアナリティクスを有効にするオプションセクションが含まれている場合があります。

次の図は、StyleBook の概略を簡単に示したものです。



次の例は、StyleBook の文法と構文について学び、より複雑な StyleBook の作成方法を理解するのに役立ちます。

- 負荷分散仮想サーバーを作成する StyleBook
- StyleBook による基本的な負荷分散構成の作成
- 複合 StyleBook の作成
- GUI 属性を使用して StyleBook をカスタマイズ

負荷分散仮想サーバーを作成する **StyleBook**

February 6, 2024

この例で設計する基本的な StyleBook では、プロトコルのタイプが HTTP で、ポート 80 でリッスンする負荷分散仮想サーバーを作成します。仮想サーバーの名前、IP アドレス、負荷分散方式の各パラメーターには、ユーザーが定義した値を指定できます（これらは StyleBook のパラメーターです）。

Header

StyleBook の先頭の 6 行は、Header セクションです。この例の場合、Header セクションは、次のように記述されています。

```
name: lb-vserver
description: This StyleBook defines a load balancing virtual server
   configuration.
display-name: Load Balancing Virtual Server (HTTP)
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

Header セクションには、次の情報が記述されています。

- **name**: この StyleBook の名前。
- **description**: この StyleBook の実行内容を示す説明。この説明は NetScaler ADM に表示されます。
- 表示名: NetScaler ADM に表示される StyleBook の説明的な名前。
- **namespace**: 名前空間は、StyleBook の一意の識別子の一部で、これにより名前の衝突を回避できます。
- **schema-version**: このリリースでは、値は常に「1.0」です。
- **version**: StyleBook のバージョン番号。バージョン番号は、StyleBook の更新時に変更できます。

name、**namespace**、および **version** の組み合わせにより、システム内で StyleBook が一意に識別されます。NetScaler ADM では、名前、名前空間、およびバージョンの組み合わせが同じ 2 つの StyleBook を使用することはできません。ただし、name と version が同じであっても namespace が異なる場合、または namespace と version が同じであっても name が異なる場合は、それらの 2 つの StyleBook を使用できます。

> 注
>
> StyleBook を更新して、version の番号が更新された場合を想定してください。別の StyleBook でこの StyleBook を参照している（つまりインポートしている）場合は、インポート元の StyleBook の正しいバージョン番号が使用されるように、別の StyleBook を確実に更新して、インポートされる StyleBook の正しいバージョンが使われるようにしてください。

StyleBook のインポート

ヘッダーの次のセクションは「import-stylebooks」と呼ばれます。このセクションで、現在の StyleBook で参照する他の StyleBook の名前空間とバージョン番号を宣言する必要があります。このセクションを記述すると、他の StyleBook をインポートして再利用できるため、StyleBook で同じ構成を再作成する必要がなくなります。

この例の場合、import-stylebooks セクションは、次のように記述されています。


```
import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
<!--NeedCopy-->
```

いずれかの NITRO 構成オブジェクトを直接使用する場合、StyleBook では、netscaler.nitro.config 名前空間を必ず参照する必要があります。この名前空間には、lbvServer など、すべての NetScaler ADC NITRO タイプが含まれています。ソフトウェアバージョン 10.5 以降がサポートされているため、StyleBook を使用して、リリース 10.5 以降を実行する任意の NetScaler ADC インスタンスで構成を作成して実行できます。

import-stylebooks セクションで使用されるプレフィックスは、名前空間とバージョンの組み合わせを示すための略語です。この場合、ns はバージョン 10.5 の netscaler.nitro.config を指します。StyleBook の以降のセクションでは、名前空間とバージョンを使用して、インポートされる StyleBook を示す代わりに、選択したプレフィックス文字列（上記の例では ns）を使用できます。

StyleBook で使用されるバージョンは、NetScaler ADC NITRO バージョンです。Nitro バージョン X をベースにした StyleBook を使用して、バージョン X 以降の任意の Citrix ADC を構成できます。

> 注
>
> StyleBook を使用してバージョン 10.5 以降の Citrix ADC インスタンスを構成できるようにするには、互換性を最大限に高めるために、Nitro 組み込み StyleBook（名前空間：netscaler.nitro.config、バージョン：10.5）を直接使用する StyleBook に Nitro 10.5 名前空間をインポートすることをお勧めします。

他の StyleBook をインポートする StyleBook は、インポートする StyleBook と同じかそれ以上のバージョンの Nitro バージョンをベースにしている必要があることが重要です。たとえば、Nitro バージョン 10.5 をベースにした StyleBook は、11.1 をベースにした StyleBook に依存したり、使用したり、インポートしたりすることはできません。しかし、バージョン 11.1 に基づく StyleBook は、11.1 未満のバージョンに基づく StyleBook をインポートすることができます。

StyleBook が Nitro 名前空間をまったくインポートしない可能性もあります。つまり、StyleBook は Nitro コンポーネントを直接定義する必要はありませんが、Nitro コンポーネントを定義する StyleBook をインポート（依存）できます。他の StyleBook をインポートする StyleBook は、依存関係の階層の中で常に最も高い Nitro バージョンを取得するため、そのバージョン以上の Citrix ADC を構成するために使用できます。

パラメーター

Parameters セクションでは、StyleBook で必要なすべてのパラメーターを宣言できます。StyleBook の作成者は、StyleBook のユーザーが指定する入力項目を決定する必要があります。この例の場合、ユーザーが、仮想サーバーの名前、IP アドレス、負荷分散方式を指定するように StyleBook を設計しました。

Parameters セクションは、次のようになっています。


```
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Name of the application configuration.
  required: true

 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: Application VIP that the clients access.
  required: true

-
  name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the load balancing algorithm (method) used for
     load balancing client request between the application servers.
  allowed-values:
   - ROUNDROBIN
   - LEASTCONNECTION
   default: ROUNDROBIN
<!--NeedCopy-->
```

> 注
>
> パラメーターのラベルを指定しない場合、NetScaler ADM はこのパラメーターを表示するときに名前属性を使用します。NetScaler ADM での表示方法を制御できるように、必ずパラメーターにラベルを定義する必要があります。
>
> ただし、API で使われる場合、パラメーターはその name で指定されます。

このセクションでは、**name** 属性の値で示される 3 つのパラメーターが宣言されています。**name** は仮想サーバー名、**ip** は仮想サーバーの IP アドレス、**lb-alg** は負荷分散方式を表します。

- **type**。これらのパラメータに指定できる値のタイプ。たとえば、name と lb-alg には、文字列値を使用できます。また、ip 値のタイプは、IP アドレスにする必要があります。StyleBook のパラメーターには、次のいずれかの組み込みタイプを指定できます。
- **string**。文字の配列。長さが指定されていない場合、文字列値には、任意の数の文字を使用できます。ただし、min-length 属性と max-length 属性を使用すれば、文字列タイプの長さを制限できます。
- **number**。整数値。min-value 属性と max-value 属性により、このタイプで使用できる最小数と最大数を指定できます。
- **boolean**。真でも偽でもかまいません。YAML では、すべてのリテラルがブール値（例：Yes または No）と見なされることに注意してください。

- **ipaddress**。有効な IPv4 または IPv6 アドレスを表す文字列。
- **tcp-port**。TCP ポートまたは UDP ポートを表す 0 から 65535 までの数値です。
- **password**。不透明/秘密の文字列値。NetScaler ADM でこのパラメータの値が表示される場合は、アスタリスク（*****）として表示されます。
- **certfile**。証明書ファイル。
- **keyfile**。証明書のプライベートキーファイル。
- **file**。このタイプのパラメータでは、ユーザーは証明書やキーファイルなどのファイルをアップロードする必要があります。
- **object**。複数の要素で構成され、これらの各要素はパラメータです。このタイプを使用すると、関連する複数のパラメーターを 1 つの親パラメーターの下にグループ化できます。
- **required**。パラメータが必須かオプションかを示します。true に設定すると、パラメーターは必須になります。その場合、ユーザーは、StyleBook を使った構成の作成時にこのパラメーターの値を指定する必要があります。デフォルトでは、すべてのパラメーターが任意です。この例では、**name** と **ip** は必須パラメータですが、**lb-alg** はオプションパラメータで、デフォルト値は「ROUNDROBIN」です。

任意のパラメーターにデフォルト値を割り当てるには、**default** 属性を使用します。構成の作成時、ユーザーが値を指定しない場合は、デフォルト値が使用されます。たとえば、**lb-alg** パラメーターのデフォルト値は、ROUNDROBIN です。

構成の作成時にユーザーが選択できる値を定義するには、**allowed-values** 属性を使用します。この例の場合、**lb-alg** パラメーターには、ROUNDROBIN および LEASTCONNECTION という 2 つの値が指定されています。

StyleBook をインポートして使用すると、NetScaler ADM はこれらの 3 つのパラメータを含むフォームが表示されます。name および ip に対して表示されるフィールドでは、文字列タイプと IP アドレスタイプの値を入力できます。lb-alg のフィールドは、ボックスの一覧として表示されます。デフォルトでは、ROUNDROBIN という値が選択されています。

> 注
>
> 組み込みタイプに加えて、パラメーターには他の StyleBook をタイプにすることができます。こうして他の StyleBook で定義されたパラメーターを再利用できます。

コンポーネント

この StyleBook の最後のセクションは、Components セクションです。Components セクションは、StyleBook で最も重要なセクションです。このセクションでは、StyleBook で作成する必要がある構成オブジェクトを定義します。

この例の場合、Components セクションは、次のように記述する必要があります。


```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

この例では、コンポーネントが 1 つのみ含まれています。コンポーネントの主要な属性は、name、type、および properties です。このコンポーネントで指定するプロパティは、コンポーネントのタイプによって決まります。コンポーネントには、次の 2 つのタイプがあります。

- ビルトインタイプ。このタイプはシステムによって提供され、定義する必要はありません。たとえば、NITRO エンティティタイプ「lbvserver」や「servicegroup」などです。この例では、組み込みのコンポーネントのタイプが使われています。
- 複合タイプ。このタイプは、作成して NetScaler ADM にインポートした StyleBook、または NetScaler ADM に同梱されているデフォルトの StyleBook です。複合 StyleBook の詳細については、「複合 StyleBook の作成」を参照してください。

この例では、**lbvserver-comp** というコンポーネントを定義しました。このコンポーネントのタイプは **ns:: lbvserver**(組み込みの Nitro タイプ) で、「ns」は import-stylebooks セクションで指定した名前空間 netscaler.nitro.config とバージョン 10.5 を指すプレフィックスで、「lbvserver」はこの名前空間の Nitro リソースです。

ここで定義されている **properties** は、「lbvserver」リソースの属性です。使用可能なすべての NetScaler ADC Nitro リソースとその属性の詳細については、NetScaler ADC NITRO REST API のドキュメントを参照してください。

このセクションのプロパティには、「lbvserver」リソースの必須属性が含まれています。そのため、これらの属性の値を指定できます。この例では、servicetype と port には静的な値が指定されていますが、name、ipv46、および lbmethod の各プロパティは、入力パラメーターから値を取得します。StyleBook の残りの部分では、を使用して、パラメータ・セクションで定義されたパラメータ名を参照できます。**$parameters.<parameter-name>** 式 (例: **$** パラメータ**.ip**) です。

> 注
>
> 慣例により、「インポート StyleBook」セクションでは、常にプレフィックス「ns」を使用して Citrix ADC Nitro 名前空間を指定します。これは必須ではありませんが、一貫性を保つためにお使いの StyleBook で慣例に従うことをお勧めします。

StyleBook を構築する

StyleBook の必須セクションをすべて定義しました。これらのセクションをまとめて、最初の StyleBook を作成します。StyleBook の内容をコピーして、テキストエディターに貼り付け、**lb-vserver.yaml** という名前でファイルを保存します。Citrix では、StyleBooks に組み込まれている YAML 検証ツールを使用して YAML コンテンツを検証およびインポートすることをお勧めします。

lb-vserver.yaml ファイルのすべての内容を次に示します。

```yaml
name: lb-vserver
namespace: com.example.stylebook
version: "1.0"
display-name: Load Balancing Virtual Server (HTTP)
description: "This stylebook defines a very simple load balancing HTTP
    virtual server configuration"
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
 -
  namespace: com.citrix.adc.stylebooks
  version: "1.0"
  prefix: stlb

parameters:
 -
  name: name
  label: "Application Name"
  description: "Give a name to the application configuration."
  type: string
  required: true
 -
  name: vip-ipaddress
  label: "Load Balancer IP Address"
  description: "The Application VIP that clients access"
  type: ipaddress
  required: true
 -
  name: lb-alg
  label: LB Algorithm
  description: Load Balancing Algorithm
  type: string
  default: ROUNDROBIN
  allowed-values:
   - ROUNDROBIN
   - LEAST-CONNECTION

components:
 -
```



```
43    name: lbvserver-comp
44    description: This StyleBook component (a Builtin Nitro StyleBook)
         builds a Citrix ADC load balancing virtual server configuration
         object.
45    type: ns::lbvserver
46    properties:
47     name: $parameters.name
48     ipv46: $parameters.vip-ipaddress
49     lbmethod: $parameters.lb-alg
50     servicetype: HTTP
51     port: 80
52  <!--NeedCopy-->
```

StyleBook を使用して構成を作成するには、NetScaler ADM にインポートしてから使用する必要があります。詳しくは、「ユーザー定義の StyleBook を使用する方法」を参照してください。

またこの StyleBook を他の StyleBook に（import-stylebooks 構造を使って）インポートすることもできます。または、次のセクションで説明されるように、より多くのパラメーターとコンポーネントを含むようにこの StyleBook を修正することもできます。

StyleBook による基本的な負荷分散構成の作成

February 6, 2024

前の例では、負荷分散仮想サーバーを作成するための基本的な StyleBook を作成しました。この StyleBook を別名で保存した後、基本的な負荷分散を構成するためのパラメーターとコンポーネントを追加して、StyleBook を更新します。この StyleBook ファイルを **basic-lb-config.yaml** という名前で保存します。

このセクションでは、負荷分散仮想サーバー、サービスグループ、およびサービス一覧からなる負荷分散の構成を作成する新しい StyleBook を設計します。また、サービスをサービスグループにバインドし、サービスグループを仮想サーバーにバインドできます。

Header

この StyleBook を作成するには、最初に Header セクションを更新する必要があります。このセクションは、負荷分散仮想サーバーの StyleBook 用に作成したセクションと似ています。Header セクションで、**name** の値を basic-lb-config に変更します。また、この StyleBook の適切な説明を記述して、**description** と **display-name** を更新します。**namespace** と **version** の値は、変更する必要はありません。name を変更したため、name、namespace、および version の組み合わせにより、この StyleBook の一意の識別子がシステム内に作成されます。

```
1  name: basic-lb-config
2  description: This StyleBook defines a simple load balancing
      configuration.
```



```
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

StyleBook のインポート

import-stylebooks セクションは、同じままです。このセクションでは、Nitro 構成オブジェクトを使用するために、netscaler.nitro.config 名前空間が指定されています。

```
import-stylebooks:
 -
 namespace: netscaler.nitro.config
 prefix: ns
 version: "10.5"
<!--NeedCopy-->
```

パラメーター

Parameters セクションを更新して、サービスまたはサーバーの一覧を定義するパラメーターと、サービスをリッスンするポートを定義するパラメーターを追加する必要があります。先頭の 3 つのパラメーター（name、ip、lb-alg）は、同じままです。

```
parameters:
 -
 name: name
 type: string
 label: Application Name
 description: Name of the application configuration
 required: true
  -
   name: ip
   type: ipaddress
   label: Application Virtual IP (VIP)
   description: Application VIP that the clients access
   required: true
  -
   name: lb-alg
   type: string
   label: LoadBalancing Algorithm
   description: Choose the load balancing algorithm used for load
      balancing client requests between the application servers.
     allowed-values:
     - ROUNDROBIN
     - LEASTCONNECTION
      default: ROUNDROBIN
  -
```



```
    name: svc-servers
    type: ipaddress[]
    label: Application Server IPs
    description: The IP addresses of all the servers of this application
    required: true
   -
    name: svc-port
    type: tcp-port
    label: Server Port
    description: The TCP port open on the application servers to receive
        requests.
    default: 80
<!--NeedCopy-->
```

この例では、アプリケーションのバックエンドサーバーを表すサービスの IP アドレスのリストを受け入れるように **svc-servers** パラメーターが追加されています。これは、**required: true** からわかるように、必須パラメーターです。2 番目のパラメーター、**svc-port** は、サーバーがリッスンするポート番号を示しています。ユーザーの指定がなければ、svc-port パラメーターのデフォルトのポート番号は 80 です。

コンポーネント

また、Components セクションを更新して、新しい 2 つのパラメーターを使用して完全な負荷分散構成を作成する追加コンポーネントを定義する必要があります。

この例の場合、Components セクションは、次のように記述する必要があります。

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg

components:
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
   name: $parameters.name + "-svcgrp"
   servicetype: HTTP

components:
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
```



```
25     name: $parent.parent.properties.name
26     servicegroupname: $parent.properties.name
27   -
28    name: members-svcg-comp
29    type: ns::servicegroup_servicegroupmember_binding
30    repeat: $parameters.svc-servers
31    repeat-item: srv
32    properties:
33     ip: $srv
34     port: str($parameters.svc-port)
35     servicegroupname: $parent.properties.name
36  <!--NeedCopy-->
```

この例では、元のコンポーネント **lbvserver-comp** (前の例の) に **svcg-comp** という子コンポーネントが追加されました。また、**svcg-comp** コンポーネントには 2 つの子コンポーネントがあります。コンポーネントを別のコンポーネント内にネストした場合、ネストされたコンポーネントは、親コンポーネントの属性を参照して構成オブジェクトを作成できます。ネストされたコンポーネントは、親コンポーネントでオブジェクトが作成されるたびに、1 つまたは複数のオブジェクトを作成できます。

svcg-comp コンポーネントは、リソース「servicegroup」の属性に指定された値を使用して、NetScaler ADC インスタンスにサービスグループを作成するために使用されます。この例では、servicetype には静的な値が指定されていますが、name は、入力パラメーターから値を取得します。パラメーターセクションで定義されているパラメーター名は、**$parameters.name+**「**-svcgrp**」という表記を使用して参照します。ここで、ユーザー定義名に**-svcgrp** を追加 (連結**)** します。

コンポーネント **svcg-comp** には、**lbvserver-svg-binding-comp** と **members-svcg-comp** という 2 つの子コンポーネントがあります。

最初の子コンポーネントである **lbvserver-svg-binding-comp** は、親コンポーネントによって作成されたサービスグループと、親の親コンポーネントによって作成された負荷分散仮想サーバー (lbvserver) との間で構成オブジェクトをバインドするために使用されます。$parent 表記（親参照とも呼ばれる）は、親コンポーネントのエンティティを参照するために使用されます。たとえば、サービスグループ名:$parent.properties.name は親コンポーネント svcg-comp によって作成されたサービスグループを指し、名前 ****:$parent.parent.properties.name** は親コンポーネントの親コンポーネント **lbvserver-comp** によって作成された仮想サーバーを指します。**

members-svcg コンポーネントは、親コンポーネントによって作成されたサービスグループにサービスのリスト間の設定オブジェクトをバインドするために使用されます。複数のバインディング設定オブジェクトを作成するには、StyleBook の **re** peat 構造を使用して、パラメータ **svc-**servers で指定されたサーバーのリストを反復処理します。繰り返し処理中、この **StyleBook** コンポーネントは、サービスグループ内の各サービス（繰り返し項目構造では **srv** と呼ばれます）に対して servicegroup_servicegroupmember_binding タイプの **Nitro** 構成オブジェクトを作成し、各 **Nitro** 構成オブジェクトの **ip** 属性を対応するサーバーの **IP** アドレスに設定します。

一般に、コンポーネントで **repeat** および **repeat-item** 構造を使用して、そのコンポーネントに同じタイプの複数の構成オブジェクトを構築させることができます。**repeat-item** コンストラクトに変数名 (srv など) を割り当てて、イテレーションの現在の値を指定できます。この変数名は、同じコンポーネントまたは子コンポーネントのプロパティで **$**として参照されます (<varname\ > 例:$srv)。

上記の例では、お互いの内部でコンポーネントのネスティングを使って、簡単に構成を組み立てています。この場合、コンポーネントのネスティングが構成を組み立てる唯一の方法ではありません。次に示すように、ネストしなくても同じ結果が得られる可能性があります。

```
components:
 -
  name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: str($parameters.svc-port)
   servicegroupname: $components.svcg-comp.properties.name
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
   name: $components.lbvserver-comp.properties.name
   servicegroupname: $components.svcg-comp.properties.name
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
  name: $parameters.name + "-svcgrp"
  servicetype: HTTP
<!--NeedCopy-->
```

ここでは、すべてのコンポーネントは同じレベルにあります（つまり、ネストされていません）が、達成される結果（生成された Citrix ADC 構成）は、以前に使用したネストされたコンポーネントと同じです。また、StyleBook のコンポーネントを宣言する順序が、構成オブジェクトの作成順序に影響を与えることはありません。この例では、**svcg-comp** と **lbvserver-comp** コンポーネントは、最後に宣言されたものであっても、**2** 番目のコンポーネント **lbvserver-svg-binding-comp** をビルドする前にビルドする必要があります。**2** 番目のコンポーネントにはこれらのコンポーネントへのフォワードリファレンスがあるためです。

> 注
>
> 慣例によって、StyleBooks、パラメーター、置換、コンポーネント、出力の名前は小文字です。複数の単語を含む場合は「-」文字で区分されます。たとえば、「lb-bindings」、「app-name」、「rewrite-config」などがあります。別の慣例としては、コンポーネント名には文字列「-comp」を末尾に付け加えます。

結果

新しい StyleBook に最後に追加するセクションは Outputs セクションです。Outputs セクションでは、この StyleBook を使用して構成を作成した後にユーザーに（または他の StyleBook で）公開する情報を指定します。たとえば、Outputs セクションでは、この StyleBook で作成される lbvserver および servicegroup 構成オブジェクトを公開することを指定できます。

```
outputs:
 -
  name: lbvserver-comp
  value: $components.lbvserver-comp
  description: The component that builds the Nitro lbvserver
     configuration object
 -
  name: servicegroup-comp
  value: $components.svcg-comp
  description: The component that builds the Nitro servicegroup
     configuration object
<!--NeedCopy-->
```

StyleBook の Outputs セクションは、必要に応じて記述します。StyleBook で必ずしも出力を返す必要はありません。ただし、内部コンポーネントを出力として返すと、この StyleBook をインポートするすべての StyleBook の柔軟性が向上します。このことは、複合 StyleBook の作成時にわかります。

> 注
>
> outputs セクションで、コンポーネントの単一のプロパティだけでなく、StyleBook のコンポーネントの全体を公開することが推奨されます（たとえば、$components.lbvserver-comp.properties.name という名前だけでなく、$components.lbvserver-comp 全体を公開します）。また出力には、特定の出力が何を表すかを説明する記述が追加されます。

StyleBook を構築する

StyleBook の必須セクションをすべて定義したので、それらをまとめて 2 番目の StyleBook を作成します。この StyleBook ファイルは、**basic-lb-config.yaml** という名前で既に保存されています。Citrix では、StyleBooks ページの組み込み YAML 検証ツールを使用して YAML コンテンツを検証およびインポートすることをお勧めします。

basic-lb-config.yaml のすべての内容を次に示します。

```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: This StyleBook defines a simple load balancing
   configuration.
schema-version: "1.0"

```



```
import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the loadbalancing algorithm (method) used for
     loadbalancing client requests between the application servers.
  allowed-values:
     - ROUNDROBIN
     - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: svc-servers
  type: ipaddress[]
  label: Application Server IPs
  description: The IP addresses of all the servers of this application
  required: true

components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
    servicegroupname: $parameters.name + "-svcgrp"
    servicetype: HTTP

 -
```



```
60    name: lbvserver-svg-binding-comp
61    type: ns::lbvserver_servicegroup_binding
62    properties:
63     name: $components.lbvserver-comp.properties.name
64     servicegroupname: $components.svcg-comp.properties.servicegroupname
65   -
66    name: members-svcg-comp
67    type: ns::servicegroup_servicegroupmember_binding
68    repeat: $parameters.svc-servers
69    repeat-item: srv
70    properties:
71     ip: $srv
72     port: 80
73     servicegroupname: $components.svcg-comp.properties.servicegroupname
74  outputs:
75  -
76    name: lbvserver-comp
77    value: $components.lbvserver-comp
78    description: The component that builds the Nitro lbvserver
          configuration object
79  -
80    name: servicegroup-comp
81    value: $components.svcg-comp
82    description: The component that builds the Nitro servicegroup
          configuration object
83  <!--NeedCopy-->
```

StyleBook を使用して構成を作成するには、NetScaler ADM にインポートしてから使用する必要があります。詳しくは、「ユーザー定義の StyleBook を使用する方法」を参照してください。

この StyleBook を他の StyleBook にインポートして、そのプロパティを使用することもできます。詳しくは、次のセクションで説明します。

複合 **StyleBook** の作成

February 6, 2024

StyleBook の重要かつ便利な特徴の 1 つは、別の StyleBook の構築ブロックとして使用できる点です。StyleBook は別の StyleBook にインポートできます。その StyleBook は、Nitro に組み込まれている StyleBook と同様に、**2** つ目の **StyleBook** のコンポーネントで使用されるタイプと呼ぶことができます。

たとえば、前のセクションで作成した basic-lb-config**StyleBook** を使用して、コンポジットサンプルという別の **StyleBook** を作成できます。「basic-lb-config」StyleBook を使用するには、新しい StyleBook 内の import-stylebooks セクションで、この StyleBook をインポートする必要があります。

StyleBook を構築する

新しい StyleBook は、次のようになります。

```
name: composite-example
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Virtual Server (HTTP/RoundRobin)
description: This StyleBook defines a RoundRobin load balancing
   configuration with a monitor.
schema-version: "1.0"
import-stylebooks:
  -
   namespace: netscaler.nitro.config
   version: "10.5"
   prefix: ns
  -
   namespace: com.example.stylebooks
   version: "0.1"
   prefix: stlb
parameters:
  -
    name: name
    type: string
    label: Application Name
    description: Give a name to the application configuration.
    required: true
  -
    name: ip
    type: ipaddress
    label: Application Virtual IP (VIP)
    description: The Application VIP that clients access
    required: true
  -
    name: svc-servers
    type: ipaddress[]
    label: Application Server IPs
    description: The IP addresses of all the servers of this
       application
    required: true

  -
    name: response-code
    type: string[]
    label: List of Response Codes
    description: List of Response Codes - Provide a list of response
       codes in integer.

components:
  -
    name: basic-lb-comp
    type: stlb::basic-lb-config
    description: This component's type is another StyleBook that builds
```



```
            the NetScaler lbvserver, servicegroups and services
          configuration objects.
47      properties:
48       name: $parameters.name
49       ip: $parameters.ip
50       svc-servers: $parameters.svc-servers
51    -
52       name: monit-comp
53       type: ns::lbmonitor
54       description: This component is a basic Nitro type (a Builtin
             StyleBook) that builds the NetScaler monitor configuration
             object.
55       properties:
56         monitorname: $parameters.name + "-mon"
57         type: HTTP
58         respcode: $parameters.response-code
59         httprequest: "'GET /'"
60         lrtm: ENABLED
61         secure: "YES"
62
63       components:
64          -
65            name: monit-svcgrp-bind-comp
66            type: ns::servicegroup_lbmonitor_binding
67            properties:
68              servicegroupname: $components.basic-lb-comp.outputs.
                    servicegroup-comp.properties.servicegroupname
69              monitor_name: $parent.properties.monitorname
70  <!--NeedCopy-->
```

import-stylebooks セクションで、名前空間とバージョンを指定して basic-lb-config StyleBook をインポートします。この StyleBook は、プレフィックス「stlb」で参照できます。

Components セクションでは、2 つのコンポーネントが定義されています。最初のコンポーネントは **stlb::basic-lb-config** タイプで、「basic-lb-config」は基本的な負荷分散設定を作成するために StyleBook で作成した StyleBook の名前です。このコンポーネントで定義されているプロパティは、basic-lb-config StyleBook で宣言されている必須パラメーターに対応しています。ただし、StyleBook の任意のパラメーター（必須とオプションの両方）を使用できます。lbvserver、サービスグループ、サービスとサービスグループのバインディングを再構築する代わりに、これらすべてを行う StyleBook をコンポーネントとしてインポートし、それを使用して新しい StyleBook にこれらの構成オブジェクトを作成します。

StyleBook は、Nitro リソース「lbmonitor」（組み込み StyleBook）の属性を使用して monitor 構成オブジェクトを作成する、2 番目のコンポーネント「monit-comp」を追加します。このコンポーネントは、最初のコンポーネントで作成された servicegroup に monitor をバインドするバインド構成オブジェクトを作成する、サブコンポーネント「monit-svcgrp-bind-comp」も持っています。「**basic-lb-config**」**StyleBook** で作成されたサービスグループコンポーネントは出力として公開されるため、この **StyleBook** には **$components.basic-lb-comp.outputs.servicegroup-comp** という表現を使用してアクセスできます。この例では、インポート先の StyleBook が、Outputs セクションを使用してインポート元の StyleBook のコンポーネントにアクセスする方法を示しています。この方法以外でアクセスすることはできません。

次に、StyleBook のコンテンツをコピーしてテキストエディターに貼り付け、そのファイルを **composite-example.yaml** として保存します。NetScaler ADM にファイルをインポートする前に、必ず YAML コンテンツを検証してください。次に、NetScaler ADM にインポートし、この StyleBook を使用して 1 つまたは複数の構成を作成します。

StyleBooks に組み込みの YAML バリデータを使用して、YAML コンテンツを検証およびインポートすることをお勧めします。

カスタム **StyleBook** での **GUI** 属性の使用

February 6, 2024

StyleBook のパラメータセクションに GUI 属性を追加して、NetScaler Application Delivery Management（ADM）に表示されるフィールドを直感的に表示できます。

例。label 属性を使用してパラメーターにわかりやすい名前を追加し、description 属性を使用してこのパラメーターにツールチップを追加できます。

```
name: ip
label: Virtual Server IP Address
description: IP address of the virtual server that represents the load
   balanced application.
type: ipaddress
required: true
<!--NeedCopy-->
```

例。オブジェクト型のパラメータがある場合は、**gui** 属性を使用してレイアウトを定義できます。この例の場合、レイアウトは折りたたみ可能なオブジェクトで、フィールドが 2 列で表示されます。

```
name: svcg-advanced
label: Advanced Application Server Settings
type: object
required: false
gui:
 collapse_pane: true
 columns: 2
<!--NeedCopy-->
```

例。object [] 型のパラメータ (オブジェクトのリスト) の概要ビューを、列を表す内部パラメータを含むテーブルとして表示することもできます。概要ビューに内部パラメータを含めたり除外したりするには、次のように GUI セクションの summary_display 属性を使用できます。

```
name: settings
label: Settings
type: object[]
parameters:
  -
```



```
    name: name
    label: Name
    description: Name of this setting
    type: string
    gui:
      summary_display: true
<!--NeedCopy-->
```

例。Citrix ADM の一部の StyleBook は、他の StyleBook の構成要素としてのみ使用されます。また、ユーザーがこれらの StyleBook から直接構成を作成しないようにすることもできます。これらの StyleBook は他の StyleBook の一部として使用されることになっているからです。StyleBook をプライベートとしてマークして、NetScaler ADM GUI で構成を作成するために StyleBook を直接使用しないようにします。

```
name: basic-lb-config
description: This stylebook defines a simple load balancing
   configuration.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
private: true
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

カスタム **StyleBook** を使用する

February 6, 2024

StyleBook を作成したら、NetScaler ADM にインポートして使用する必要があります。NetScaler ADM では、単一の StyleBook を YAML 形式でインポートすることも、複数の StyleBookYAML ファイルを.zip、.tgz、または.gz 形式でバンドルとしてインポートすることもできます。NetScaler ADM システムは、インポート時に StyleBook を検証します。これで、Stylebook を使用して構成を作成する準備が整いました。

NetScaler ADM には、StyleBook YAML コンテンツの作成に使用できる組み込みの YAML エディタもあります。YAML エディターを使用すると、Citrix ADM GUI 自体から YAML コンストラクトを検証できます。これらの検証チェックに個別のツールを使用する必要はありません。コンテンツは YAML 標準に照らして検証され、偏差が強調表示されます。その後、コンテンツを修正して、StyleBook を NetScaler ADM にインポートしてみることができます。ビルトインの YAML エディターには、独自の StyleBook を作成する際に 2 つの利点があります。

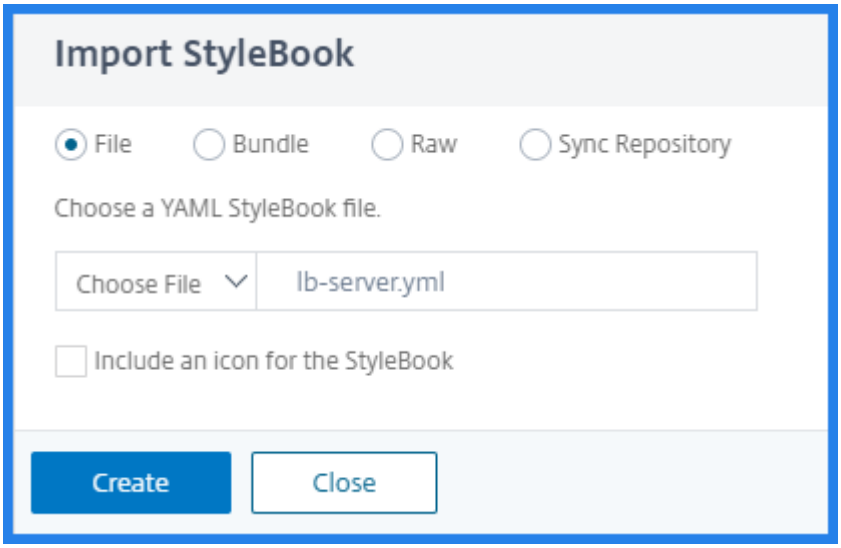
- 色分けされています。エディターには、YAML ガイドラインに従って解析された StyleBook コンテンツが表示されます。色分けにより、YAML コンテンツで定義されているキーと値を簡単に区別できます。
- **YAML** 検証です。入力時にコンテンツが YAML エラーに対して検証され、偏差が即座に強調表示されます。これにより、NetScaler ADM で StyleBook をインポートする前でも、YAML ガイドラインに準拠したテキストを作成できます。現在、エディターは YAML ガイドラインに従ってコンテンツを検証しています。コードの正確性と誤植は検証されません。

StyleBook のインポート

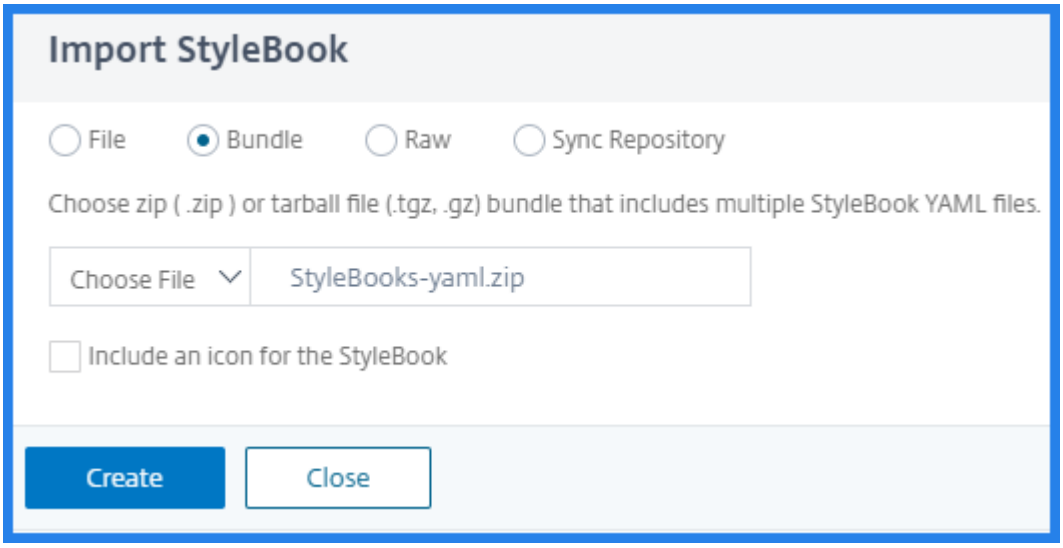
1. Citrix ADM で、「アプリケーション」>「構成」 > 「**StyleBook**」に移動し 、「新しい StyleBook のインポート」をクリック します。
2. StyleBook をインポートするには、3 つのオプションのいずれかをクリックします。

   a) ファイル。ローカルストレージから必要なファイルまたはファイルのバンドルを選択します。

   > 注
   >
   > : この例では、StyleBook で作成した「lb-vserver.yaml」StyleBook をインポート して、負荷分散仮想サーバーを作成します。

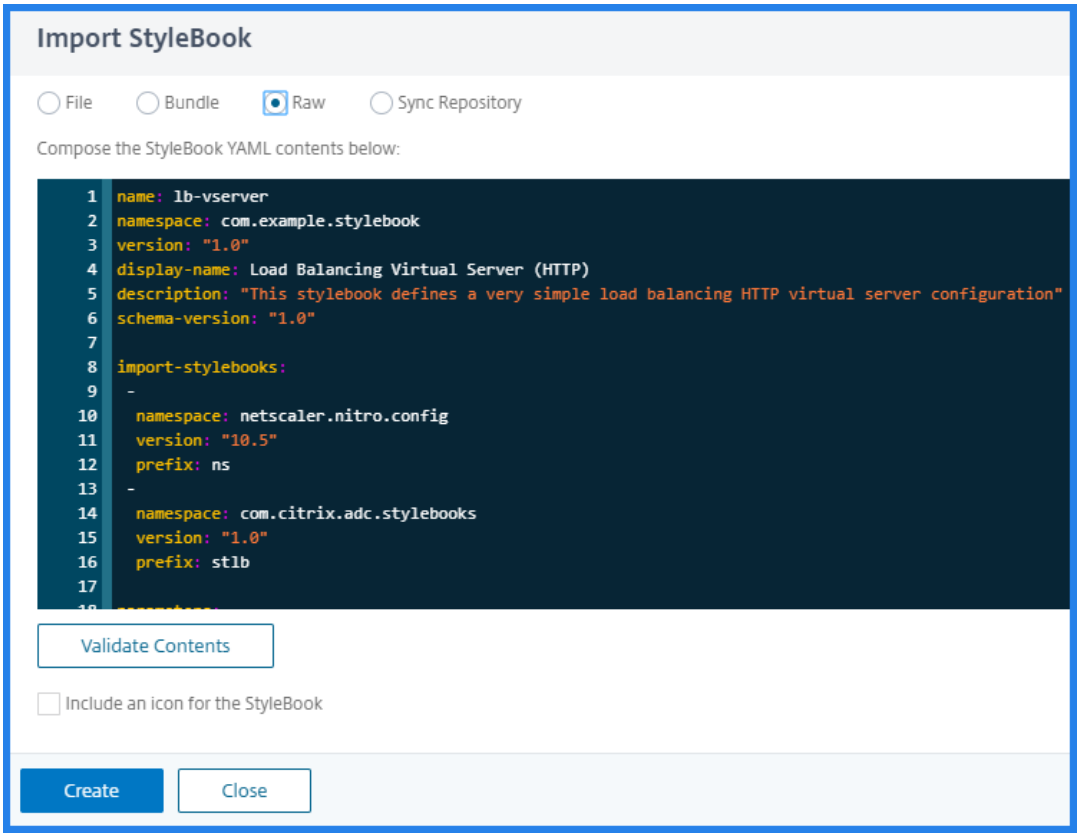
   b) バンドル。NetScaler ADM では、複数の StyleBook を YAML 形式でインポートできます。zip (.zip) 形式または tarball (.tgz、.gz) 形式で圧縮された YAML StyleBook ファイルを複数インポートできます。

c) 未加工。YAML エディターで StyleBook のコンテンツを作成します。

> 注
>
> StyleBook を作成する際は、次の知識があることを確認してください。
>
> - NITRO API
> - YAML

独自の StyleBook を作成する方法について詳しくは、「独自の StyleBook を作成する方法」を参照してください。



> 注
>
> :StyleBook YAML ファイルからコンテンツをコピーして貼り付けて、コンテンツを検証することもできます。

3. [**Create**] をクリックします。

NetScaler ADM は、StyleBook の文法に従って、すべての構文エラーと意味エラーについて StyleBook を検証するようになりました。エラーが発生した場合、StyleBook は NetScaler ADM にインポートされません。エラーがなければ、StyleBook は正常にインポートされ、StyleBooks ページに表示されるようになりました。StyleBook のヘッダーセクションで定義した表示名で StyleBook を識別できます。

> 注:
>
> ファイルのバンドルをインポートする場合、NetScaler ADM は圧縮されたフォルダーを解凍し、すべての StyleBook を検証します。
> 1 つの StyleBook ファイルが検証テストに失敗しても、バンドルはインポートされません。

StyleBook の文法とさまざまな構成と属性の構文について詳しくは、「StyleBook の文法」を参照 してください。

4. この StyleBook から構成を作成するには、「構成を作成」リンクをクリック します。StyleBook がユーザーインターフェイスページとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。
5. パラメータに必要な値を指定します。以下の例では、アプリケーション名 と ロードバランサーの **IP** アドレスフィールドが必須フィールド として表示され、ユーザー値を受け入れることができることがわかります。 **LB** アルゴリズムには選択できる値が 2 つしかなく、デフォルトで ROUNDROBIN が選択されています。
6. [ターゲットインスタンス] で、構成を実行する Citrix ADC インスタンスの IP アドレスをクリックして選択します。ターゲットインスタンスを必要な数だけ指定して、複数の NetScaler ADC で構成を展開することもできます。

実際に構成を作成する前に、Citrix ADC 上に作成される Citrix ADC（Nitro）構成オブジェクトを確認したい場合は、「ドライラン」をクリック します。設定が有効な場合は、指定した値に基づいて作成される設定オブジェクトが表示されます。この例では、この例の StyleBook では lbvserver タイプのオブジェクトが 1 つだけ作成されます。この lbvserver は、この基本的な StyleBook のサンプルで定義されている唯一のコンポーネントでした。後で [作成] をクリック して、選択した Citrix ADC インスタンスに実際に構成を作成できます。

作成が完了すると、新しい ConfigPack が [構成] ページに一覧表示されます。

> 注
>
> 更新アイコンをクリックして、NetScaler ADM で最近検出された NetScaler ADC インスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。

カスタム **StyleBook** の検索

Citrix ADM では、タイプに基づいて StyleBook を検索できるようになりました。つまり、デフォルトの StyleBook またはカスタム StyleBook のいずれかを検索できるようになりました。このオプションは、多数のデフォルト StyleBook の中からユーザー定義の StyleBook を検索する必要がある場合に特に役立ちます。

カスタム **StyleBook** を検索するには

1. NetScaler ADM で、［アプリケーション］>［構成］>［**StyleBook**］に移動します。
2. 右上にある検索アイコンをクリックします。

3. 表示される検索バーで、最初のリストから [タイプ] を選択し、次のオプションリストから [カスタム] を選択します。
4. NetScaler ADM では、ユーザー定義の StyleBook のみが表示されます。

NetScaler ADM にファイルをアップロードする StyleBook を作成する

February 6, 2024

Citrix Application Delivery Management（Citrix ADM）StyleBooks を使用すると、Citrix ADM GUI または API を使用して、ローカルファイルシステムから Citrix ADC インスタンスにあらゆる種類のファイルをアップロードする際に、とりわけ含めることができる Citrix ADC 構成を作成できます。これらのファイルは、証明書ファイルの例でも位置情報ファイルでもかまいません。これらのファイルをアップロードするディレクトリを指定することもできます。

StyleBook の設定

以下は、NetScaler ADC インスタンスに位置情報ファイルをアップロードする方法を説明する StyleBook の例です。地理ファイルは、地理的位置に基づいて静的近接を定義するために、GSLB 設定で通常使用されます。

StyleBook の作成 -1

```
name: upload-geolocations
namespace: com.citrix.adc.stylebooks.samples
version: "1.0"
display-name: GeoLocation File Upload
description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
schema-version: "1.0"

import-stylebooks:
-
 namespace: netscaler.nitro.config
 version: "11.1"
 prefix: ns

parameters:
-
 name: locationfile
 label: Location File
 description: The system file path of the geolocation file on Citrix
    ADM
 type: file
 required: true
```



```
21
22 components:
23 -
24  name: upload-file-comp
25  type: ns::systemfile
26  properties:
27     filename: $parameters.locationfile.filename
28     filelocation: "/var/netscaler/inbuilt_db/"
29     filecontent: base64.encode($parameters.locationfile.contents)
30 <!--NeedCopy-->
```

> 注:
>
> この例で使用されているパラメータはタイプファイルのものです。この StyleBook を NetScaler ADM にインポートして、ジオロケーションファイルをアップロードできます。

この StyleBook では、ファイルが Citrix ADM にすでに存在している必要があります（たとえば、scp などのユーティリティを使用して Citrix ADM に既にコピーしているはずです）。

NetScaler ADM ファイルシステムにファイルをコピーせずに、NetScaler ADM 経由で NetScaler ADC にファイルをアップロードする場合は、2 つの「文字列」パラメータを持つ StyleBook を構築できます。1 つは NetScaler ADC で使用するファイル名を指定し、もう 1 つは NetScaler ADC の内容を指定するものです。ファイルを作成し、upload-file-comp コンポーネントでこれら 2 つのパラメータを使用します。以下は、位置情報ファイルをアップロードするための代替 StyleBook です。

StyleBook を構築する-2

```
1  name: upload-geolocations-alt
2  namespace: com.citrix.adc.stylebooks.samples
3  version: "1.0"
4  display-name: GeoLocation File Upload
5  description: This StyleBook is used to upload a geolocation file to
      Citrix ADC
6  schema-version: "1.0"
7
8  import-stylebooks:
9   -
10   namespace: netscaler.nitro.config
11   version: "11.1"
12   prefix: ns
13
14 parameters:
15  -
16   name: filename
17   label: Location Filename
18   description: The name of the location file on the Citrix ADC
19   type: string
20   required: true
21  -
```



```
  name: filecontents
  label: Location File Contents
  description: The contents of the location file
  type: string
  required: true

components:
 -
  name: upload-file-comp
  type: ns::systemfile
  properties:
   filename: $parameters.filename
   filelocation: "/var/Citrix ADC/inbuilt_db/"
   filecontent: base64.encode($parameters.filecontents)
<!--NeedCopy-->
```

ファイルをアップロードするための構成の作成

以下の手順では、選択した NetScaler ADC インスタンスに、上記の最初の StyleBook を使用して位置情報ファイルをアップロードする構成を作成します。

ファイルをアップロードするための設定を作成するには:

1. NetScaler ADM で、［アプリケーション］>［構成］に移動し、［新規作成］をクリックします。「StyleBook の選択」ページには、NetScaler ADM で使用できるすべての StyleBook が表示されます。下方向にスクロールして、インポートした StyleBook を選択します。

   StyleBook パラメーターは、この StyleBook で定義されているすべてのパラメーターの値を入力できるユーザーインターフェイスページとして表示されます。

2. ロードバランサーの基本設定セクションにロードバランサーの名前と仮想 IP アドレスを入力します。
3. [ロケーションファイル] セクションで、ファイルの名前または場所を入力します。

   > 注
   >
   > : Citrix ADM では、ファイルが現在のテナントのフォルダーのみにあることを確認してください。任意のファイル転送プロトコルを使用して、Citrix ADM ファイルシステムにファイルをコピーします。

4. ターゲットインスタンスにアクセスする前に、ユーザー認証情報を入力するように求められる場合があります。
5. 構成を作成する対象の NetScaler ADC インスタンスを選択し、［作成］をクリックします。

> 注:
>
> インスタンスで実際の構成を実行する前に、［**Dry Run**］を選択して、ターゲットインスタンス上に作成された構成オブジェクトをチェックすることをお勧めします。

コンフィグパックの作成が成功すると、ファイルは Citrix ADC インスタンスのファイルシステムの /var/netscaler/inbuilt_db/ という場所に保存されます。

> 注
>
> 更新アイコンをクリックして、NetScaler ADM で最近検出された NetScaler ADC インスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。

Citrix ADM API を使用してコンフィグパックを作成する

Citrix ADM API を使用して、選択した Citrix ADC インスタンスにファイルをアップロードする構成パックを作成することもできます。API の使用方法の詳細については、「API を使用して任意のファイルタイプをアップロードする構成を作成する方法」を参照してください。

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

February 6, 2024

SSL プロトコルを使用する StyleBook の構成を作成する場合、SSL 証明書ファイルと証明書キーファイルを StyleBook パラメーターの要求に応じてアップロードする必要があります。StyleBook では、NetScaler ADM GUI を使用して、SSL ファイルとキーファイルをローカルシステムから直接アップロードできます。NetScaler ADM API を使用して、NetScaler ADM によってすでに管理されている証明書ファイルとキーファイルをアップロードすることもできます。

StyleBook の設定

このドキュメントは、**SSL** 証明書とキーファイルをアップロードするためのコンポーネントを備えた独自の **StyleBook**-負荷分散仮想サーバー（**SSL**）
を作成するのに役立ちます。ここで例として提供している StyleBook は、選択した NetScaler ADC インスタンス上に基本的な負荷分散仮想サーバー構成を作成します。この構成は SSL プロトコルを使用します。この StyleBook を使用して構成を作成するには、仮想サーバーの名前と IP アドレスを指定し、負荷分散方法のパラメーターを選択し、仮想サーバーの証明書ファイルと証明書キーファイルをアップロードするか、すでに存在する証明書ファイルと証明書キーファイルを使用する必要があります NetScaler ADM に存在します。これらは下記のとおり、「parameters」セクションで指定されます。

```
parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
```



```
    type: ipaddress
    required: true
  -
    name: lb-alg
    type: string
    allowed-values:
      - ROUNDROBIN
      - LEASTCONNECTION
    default: ROUNDROBIN
  -
    name: certificate
    label: "SSL Certificate File"
    description: "The file name of the SSL certificate file"
    type: certfile
  -
    name: key
    label: "SSL Certificate Key File"
    description: "The file name of the server certificate's private key
       file"
    type: keyfile
<!--NeedCopy-->
```

下記のとおり、StyleBook のコンポーネントセクションに 2 つのコンポーネントが作成されます。「my-lbvserver-comp」コンポーネントのタイプは ns::lbvserver です。

- 「ns」は、import-stylebooks セクションで指定した、組み込みの名前空間 netscaler.nitro.config バージョン 10.5 を参照するプレフィックスです。
- 「lbvserver」はこの名前空間の組み込み StyleBook です。これは、同じ名前の Citrix ADC NITRO 負荷分散仮想サーバーリソースに対応します。

2 番目のコンポーネント「lbvserver-certificate-comp」は stlb:: vserver-certs-binds タイプです。プレフィックス「stlb」は StyleBook の import-stylebooks セクションで指定された、名前空間「com.citrix.adc.stylebooks」バージョン 1.0 を参照します。名前空間「com.citrix.adc.stylebooks」がフォルダーと考えることができるのであれば、「vserver-certs-binds」はフォルダー中の他の StyleBook（またはファイル）です。名前空間「com.citrix.adc.stylebooks」にある StyleBook は、NetScaler ADM の一部として出荷されます。

ユーザー定義の StyleBook で使用される「vserver-certs-binds」StyleBook を使用すると、証明書とキーファイルをターゲットの NetScaler ADC インスタンスにアップロードし、証明書とキーファイルを適切な仮想サーバーにバインドすることによって、証明書を簡単に構成できます。このコンポーネントのプロパティは、lb 仮想サーバーの名前と、configpack の作成時に提供する SSL 証明書の名前です。

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name
   servicetype: SSL
   ipv46: $parameters.ip
   port: 443
```



```
    lbmethod: $parameters.lb-alg
  -
   name: lbvserver-certificate-comp
   type: stlb::vserver-certs-binds
   description: Binds lbvserver with server certificate
   properties:
    vserver-name: $components.my-lbvserver-comp.properties.name
    certificates:
     -
      cert-name: $parameters.name + "-lb-cert"
      cert-file: $parameters.certificate
      ssl-inform: PEM
      key-name: $parameters.name + "-key"
      key-file: $parameters.key
<!--NeedCopy-->
```

API を使ってこういった StyleBook から構成を作成する場合は、ファイル名だけを使うようにしてください（フルファイルパスではなく）。これらのファイルは、NetScaler ADM の証明書フォルダーとキーファイルフォルダーに既にあるはずです。アップロードされた SSL 証明書ファイルは、NetScaler ADM の /var/mps/tenants/…に保存されます/ns_ssl_certs ディレクトリで、SSL 証明書キーファイルは /var/mps/tenants/…に保存されています NetScaler ADM の /ns_ssl_keys ディレクトリ。

SSL ファイルをアップロードするための構成の作成

以下の手順では、上記で指定した StyleBook の SSL プロトコルを使用して、選択した NetScaler ADC インスタンス上に基本的な負荷分散仮想サーバー構成を作成します。この手順を使用して、NetScaler ADM で SSL 証明書ファイルと証明書キーファイルをアップロードできます。

ファイルをアップロードする構成を作成するには

1. NetScaler ADM で、[アプリケーション] > [構成] **>** [**StyleBook**] に移動します。 **StyleBook** ページには、Citrix ADM で利用できるすべての StyleBook が表示されます。
2. 下にスクロールして [負荷分散仮想サーバー **(SSL)**] を選択するか 、検索フィールドに「負荷分散仮想サーバー **(SSL)** 」と入力して **Enter** キーを押します。
3. StyleBook パネルで「設定を作成」リンクをクリックします。

   StyleBook パラメーターは、この StyleBook で定義されているすべてのパラメーターの値を入力できるユーザーインターフェイスページとして表示されます。
4. ロードバランサーの基本設定セクションにロードバランサーの名前と仮想 IP アドレスを入力します。
5. **SSL** 証明書の設定セクションで、ローカルストレージフォルダからそれぞれのファイルを選択します。または、NetScaler ADM 自体にあるファイルを選択することもできます。
6. 構成を作成する対象の NetScaler ADC インスタンスを選択し、[作成] をクリックします。

> 注:
>
> 更新アイコンをクリックして、NetScaler ADM で最近検出された NetScaler ADC インスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。
>
> Citrix ADM では、Citrix ADM の一部として付属している次のデフォルトの StyleBook を使用すると、SSL 証明書とキーをアップロードして SSL サポートを作成できます。
>
> - HTTP/SSL 負荷分散 StyleBook（lb）
> - HTTP/SSL 負荷分散（監視あり）StyleBook（lb-mon）
> - HTTP/SSL コンテンツスイッチアプリケーション（監視あり）（cs-lb-mon）
> - CS、LB、および SSL 機能を使ったサンプルアプリケーション StyleBook（sample-cs-app）
>
> 上記の StyleBook で説明されたものと同じ方法で SSL 証明書を使用する、ご自身の StyleBook を作成することも可能です。

StyleBook を構築する

lb-vserver-ssl.yaml ファイルのすべての内容を次に示します。

```
name: lb-vserver-ssl
description: "This stylebook defines a load balancing virtual server
   configuration."
display-name: "Load Balancing Virtual Server (SSL)"
namespace: com.example.ssl.stylebooks
schema-version: "1.0"
version: "0.1"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
 -
  namespace: com.citrix.adc.stylebooks
  prefix: stlb
  version: "1.0"

parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
  type: string
```



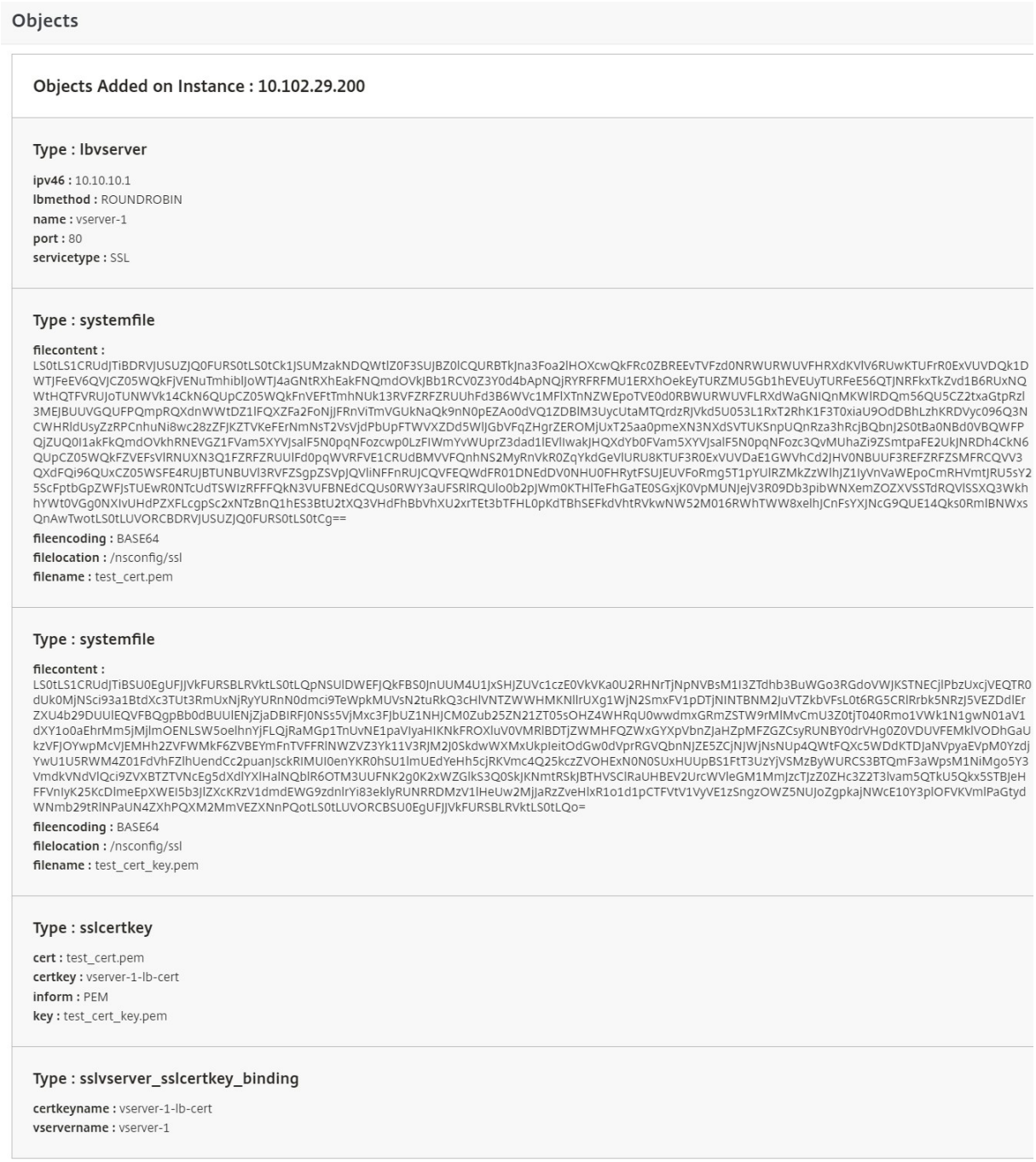
```
30    allowed-values:
31      - ROUNDROBIN
32      - LEASTCONNECTION
33    default: ROUNDROBIN
34   -
35    name: certificate
36    label: "SSL Certificate File"
37    description: "The file name of the SSL certificate file"
38    type: certfile
39   -
40    name: key
41    label: "SSL Certificate Key File"
42    description: "The file name of the server certificate's private key
          file"
43    type: keyfile
44
45  components:
46   -
47    name: my-lbvserver-comp
48    type: ns::lbvserver
49    properties:
50      name: $parameters.name
51      servicetype: SSL
52      ipv46: $parameters.ip
53      port: 443
54      lbmethod: $parameters.lb-alg
55   -
56    name: lbvserver-certificate-comp
57    type: stlb::vserver-certs-binds
58    description: Binds lbvserver with server certificate
59    properties:
60     vserver-name: $ components.my-lbvserver-comp.properties.name
61     certificates:
62      -
63       cert-name: $parameters.name + "-lb-cert"
64       cert-file: $parameters.certificate
65       ssl-inform: PEM
66       key-name: $parameters.name + "-key"
67       key-file: $parameters.key
68  <!--NeedCopy-->
```

NetScaler ADM API を使用した構成パックの作成

Citrix ADM API を使用して、選択した Citrix ADC インスタンスに証明書ファイルとキーファイルをアップロードする構成パックを作成することもできます。API の使用方法の詳細については、「API を使用して 証明書とキーファイルをアップロードするための設定を作成する方法」を参照してください。

NetScaler ADC インスタンスに定義されているオブジェクトの表示

Citrix ADM で StyleBook 構成パック（構成パック）を作成したら、［作成されたオブジェクトを表示］をクリックして、ターゲットの Citrix ADC インスタンスで作成されたすべての Citrix ADC オブジェクトを表示します。



StyleBook で定義された仮想サーバーでの分析の有効化とアラームの設定

February 6, 2024

操作コンストラクトを使用して、StyleBook の一部である任意の仮想サーバーコンポーネントによって処理されるトラフィックトランザクションのすべてまたは一部に関する appflow レコードを収集するように Citrix ADM Analytics を構成できます。また、このような操作構成を使用して、アラームを構成し、仮想サーバーが管理するトラフィックの詳細な情報を取得できます。

次の例は、StyleBook の Operations セクションを示しています。

```
operations:
  analytics:
   -
    name: lbvserver-ops
    properties:
    target: $components.basic-lb-comp.outputs.lbvserver
    filter: HTTP.REQ.URL.CONTAINS("catalog")
   -
    alarms:
     -
      name: lbvserver-alarm
      properties:
      target: $outputs.lbvserver
      email-profile: $parameters.emailprofile
      sms-profile: "NetScalerSMS"

    rules:
     -
      metric: "total_requests"
      operator: "greaterthan"
      value: 25
      period-unit: $parameters.period
     -
       metric: "total_bytes"
       operator: "lessthan"
       value: 60
       period-unit: "day"
<!--NeedCopy-->
```

分析セクションの属性は、Citrix ADM 分析機能に、ターゲットプロパティで識別される仮想サーバーコンポーネント上のアプリケーションフローレコードを収集するように指示するために使用されます。また、NetScaler ADC ポリシー式を受け入れるフィルタプロパティを指定して、仮想サーバー上で収集される appflow レコードの要求をフィルタリングすることもできます。

この StyleBook から構成パックを作成すると、Citrix ADM 分析機能は、構成パックの作成プロセスで作成されたときに指定された仮想サーバー上のアプリケーションフローレコードを収集するように構成されます。

alarms セクションの属性は、アラーム生成のしきい値を設定し、ターゲットプロパティが指定する仮想サーバーの

通知を送信するために使用されます。上の例では、email-profile と sms-profile のプロパティが通知を送信する場所を指定するために使用されています。rules セクションはしきい値を定義します。たとえば、ユーザーが定義した期間に、仮想サーバーが処理する要求の合計が 25 件を超えた場合、アラームが設定され、通知が送信されます。「period-unit」はアラームをトリガーする頻度を指定します。これは、日、時間、または毎週の値を取ることができます。

測定基準値としきい値の比較を用いる場合、次の演算子を使用できます。

- 「greaterthan」:「>」を示します
- 「Lessthan」:「<」を示します
- 「greaterthanequal」:「>=」を示します
- 「lessthanequal」:「<=」を示します

StyleBook では、メトリックスに API 名が使用され、NetScaler ADM 分析 GUI に表示される名前は使用されません。

構成パックの一部として作成された仮想サーバーで収集されたデータを表示および分析する方法については、NetScaler ADM Analytics のドキュメントを参照してください。

インスタンスロール

February 6, 2024

Citrix Application Delivery Management（ADM）では、1 つのアプリケーションに対して複数の Citrix ADC インスタンスを構成する必要がある場合がありますが、各 ADC インスタンスをそれらに展開するには異なる構成が必要な場合もあります。このような場合の例は、Microsoft Skype for BusinessStyleBook のデフォルトです。

StyleBook は現在、構成パックを作成して同じ構成を複数の Citrix ADC インスタンスに適用する機能をサポートしています。構成がすべての ADC インスタンスで同一であるようなシナリオを対称構成と呼ぶことができます。

StyleBooks の「インスタンスロール」機能を使用すると、非対称構成、つまり複数の ADC インスタンスに適用できるが、異なる ADC インスタンスには異なる構成を適用できる構成パックを作成できます。

インスタンスロール機能付きの StyleBook を使用して構成パックを作成する場合、構成パック内の各 ADC インスタンスに異なる役割を割り当てることができます。このロールは、ADC インスタンスが受け取る構成パックの設定オブジェクトを決定します。

注意事項:

- StyleBook のインスタンスロールのセットは、StyleBook の作成時に定義されます。
- ロールは、構成パックを作成または更新するときに特定の ADC インスタンスに割り当てられます。

「ターゲットロール」セクション

StyleBook に「target-roles」と呼ばれる新しいセクションが導入されました。このセクションには、StyleBook でサポートされているすべてのロールが宣言されています。

このセクションは通常、StyleBook の「Import-StyleBooks」セクションの後、パラメーターセクションの前に配置されます。

次の StyleBook の例では、「ターゲットロール」セクション内に A と B の 2 つのロールが定義されています。

```
target-roles:

  -
   name: A
   name: B
     min-targets: 2
     max-targets: 5
<!--NeedCopy-->
```

ロール B は、min-target と max-target という 2 つのオプションのサブプロパティも定義していることがわかります。

これら 2 つのサブプロパティはオプションですが、min-targets は、この StyleBook から構成パックを作成するときにこのロールに割り当てる必要がある ADC インスタンスの最小必須数を指定し、最大ターゲットは、この StyleBook から構成パックを作成するときにこのロールを割り当てることができる ADC インスタンスの最大数を指定します。

これらのサブプロパティが指定されていない場合、そのロールに設定できる ADC インスタンスの数に制限はありません。min-targets = 0 の場合、そのロールに関連付けられた設定はオプションであり、min-targets = 1 の場合、その設定は必須であり、そのロールに対して少なくとも 1 つの ADC インスタンスを設定する必要があります。

ロール「デフォルト」

明示的に定義されたロールに加えて、すべての StyleBook が持つ暗黙的なロールがあり、そのロールはデフォルトロールとして呼び出されます。このロールは、StyleBook の他のロールと同様に使用できます。構成パックを作成するときに、ADC インスタンスに特定のロールが割り当てられていない場合、インスタンスは暗黙的に「デフォルト」ロールに割り当てられます。これで、インスタンスは「default」ロールを持つコンポーネントによって生成された設定オブジェクトを受け取ります。

ロールを持つコンポーネント

StyleBook がサポートできるロール（「デフォルト」ロールを含む）を定義したら、そのロールを StyleBook のコンポーネントセクションで使用できます。コンポーネントを特定の役割を果たす ADC インスタンスにのみデプロイする場合は、次のコンポーネントの例に示すように、コンポーネントの一部として roles 属性を指定できます。


```
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
<!--NeedCopy-->
```

上記の例では、コンポーネントは「lbvserver」を生成し、このインスタンスはロール A を演じるインスタンスにデプロイされます。コンポーネントのロール属性はリストであり、コンポーネントには複数のロールを割り当てることができることに注意してください。これらのロールは、StyleBook の「ターゲットロール」セクションで宣言されていたはずです。

注：StyleBook 内のコンポーネントがロール属性を指定しない場合、そのコンポーネントによって生成された構成オブジェクトは、ロールに関係なくすべての NetScaler ADC インスタンスに作成されます。この機能を効果的に使用して、構成パックのすべてのインスタンスに適用できる構成オブジェクトを作成できます。

A と B の 2 つのロールが定義されている StyleBook があり、4 つのコンポーネントが含まれていると仮定します。

- コンポーネント C1 にはロール A と B があります。
- コンポーネント C2 にはロール B があります。
- コンポーネント C3 にはロールが定義されていません
- コンポーネント C4 には「デフォルト」の役割があります

この StyleBook のコンポーネントセクションを以下に示します。

```
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
```



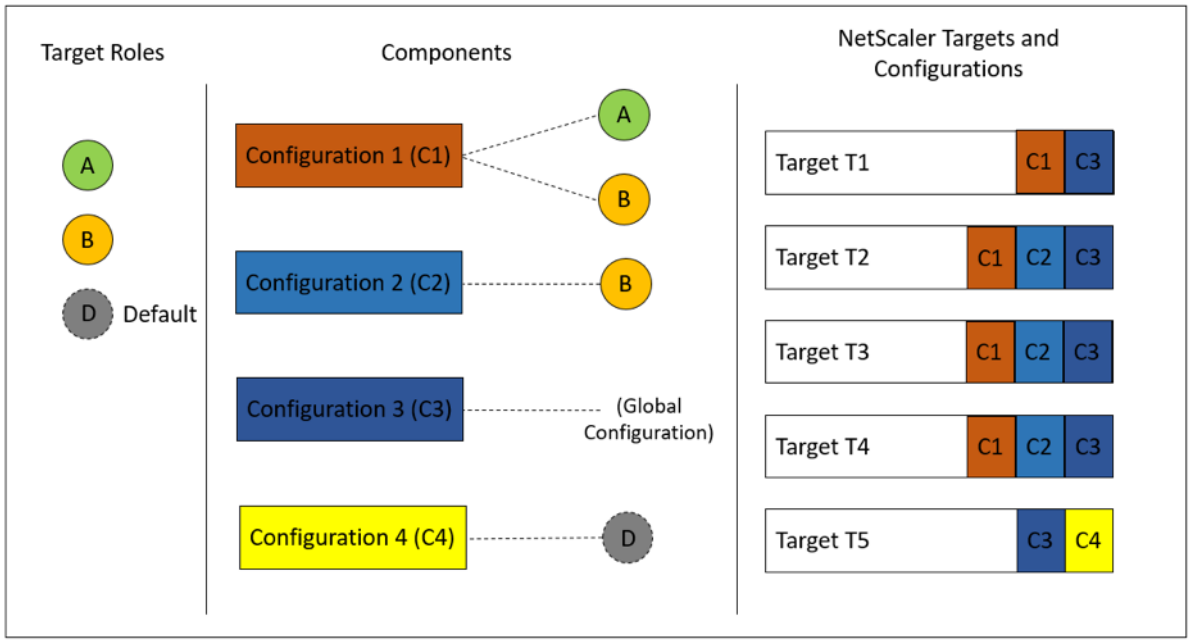
```
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
      port: 80
<!--NeedCopy-->
```

コンポーネント C3 にはロールが定義されていないことに注意してください。つまり、コンポーネントはロールに関係なくすべてのインスタンスにデプロイされます。一方、コンポーネント C4 には「default」というロールがあります。つまり、明示的なロールが割り当てられていないインスタンスに適用されます。

ここで、この StyleBook を使用して構成パックを作成し、それを 5 つの ADC インスタンスにデプロイするとします。この段階では、次の方法でインスタンスにロールを割り当てることができます:

- ロール A はインスタンス T1、T2、T3、T4 に割り当てられます
- ロール B はインスタンス T2、T3、T4 に割り当てられます
- インスタンス T5 にはロールが割り当てられていません

次の図は、役割の割り当てをまとめたもので、各 ADC インスタンスが受け取る構成を示しています。



コンポーネント C3 は、ロールに関係なくすべてのインスタンスにデプロイされます。これは、このコンポーネントには roles 属性がないためです。

構成パックを作成するときに「ドライラン」機能を使用して、各 ADC インスタンスで作成される役割と構成オブジェクトの正しい割り当てを表示および確認することもできます。

StyleBook を構築する

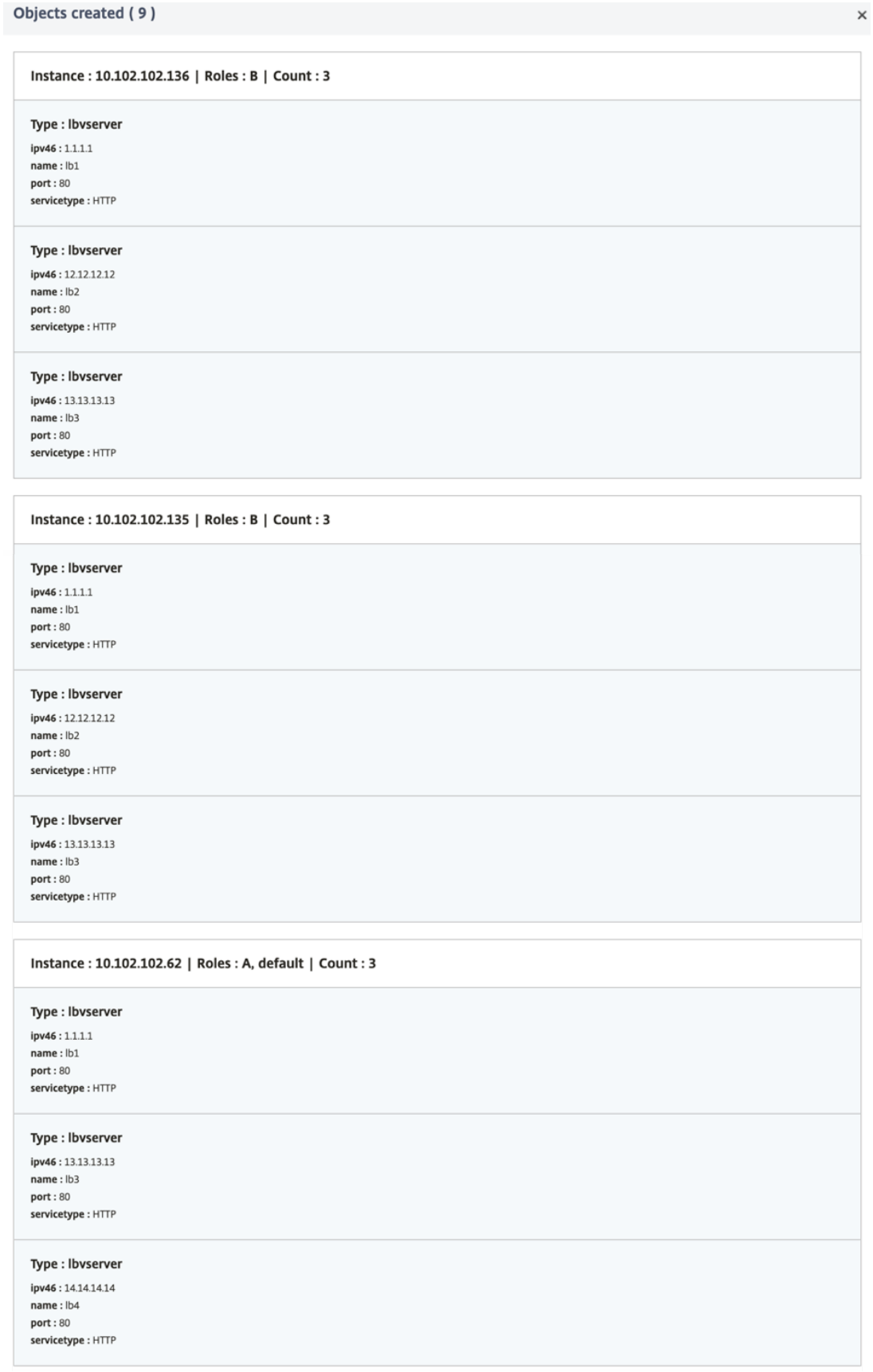
StyleBook「デモターゲットロール」の全コンテンツを以下に示します:

```
---
name: demo-target-roles
namespace: com.example.stylebooks
version: "1.2"
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: appname
    type: string
    required: true
    key: true
target-roles:
  -
    name: A
  -
```



```
    name: B
    min-targets: 2
    max-targets: 5
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
      port: 80
<!--NeedCopy-->
```

以下の画像は、サンプル構成パック用に作成されたオブジェクトを示しています。



API の使用

REST API を使用する場合、構成パックを作成または更新するときに、次のように各 ADC インスタンスのロールを指定できます。「targets」ブロックで、個々のコンポーネントを展開する特定の NetScaler ADC インスタンスの UUID を指定します。

```
"targets": [
            {

             "id": "<ADC-UUID>",
             "roles": ["A"]
             }
 ,
           ]
<!--NeedCopy-->
```

参考のために、完全なサンプル REST API が提供されています。

POST/<ADM-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpack

```
{

  "configpack": {

     "parameters": {

     "appname": "app1"
     }
 ,
     "targets": [
        {

          "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",
        "roles": ["A"]
         }
 ,
        {

          "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",
          "roles": ["A", "B"]
         }
 ,
        {

          "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",
          "roles": ["A", "B"]
         }
 ,
        {

          "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
```



```
            "roles": ["A", "B"]
           }
 ,
          {

            "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
            "roles": ["default"]
           }

        ]
       }

 }

<!--NeedCopy-->
```

StyleBook を作成して非 CRUD 操作を実行する

February 6, 2024

StyleBook は、NetScaler ADC インスタンス上で必要な構成オブジェクトを計算することによって、NetScaler ADC 構成を管理します。これらのオブジェクトは、ConfigPack を作成または更新するたびにインスタンスから追加、更新、または削除されます。つまり、「望ましい状態」を指定するときです。

ただし、一部の Citrix ADC 構成オブジェクトは、作成、更新、削除（CRUD 操作）以外のいくつかの操作をサポートしています。たとえば、ロードバランサーオブジェクト（lbvserver）または Citrix ADC 機能オブジェクト（nsfeature）は、「有効化」または「無効化」操作をサポートできます。同様に、Citrix ADC 証明書キーは、証明書を別の証明書にリンクまたはリンク解除するための「リンク」および「リンク解除」操作をサポートしています。NetScaler ADC オブジェクトに対するこれらの操作は、非 CRUD 操作と呼ばれます。このセクションでは、StyleBook を使用して、それらをサポートする設定オブジェクトに対して非 CRUD 操作を実行する方法について説明します。

> 注:
>
> 設定オブジェクト間のバインディング (たとえば、証明書キーを lbvserver にバインドする) は、CRUD 以外の操作とは見なされません。これは、Nitro バインディングはそれ自体が設定オブジェクトとして表現されるためです。これらのオブジェクトは、他の NetScaler ADC 構成オブジェクトと同様に作成および削除されます。

CRUD 以外のオペレーションのサポート

「メタプロパティ」と呼ばれる新しい構成が、「プロパティ」構成と同じレベルでコンポーネントに追加されます。この構成でサポートされる唯一の属性は、現在「action」と呼ばれています。この属性は、その構成オブジェクトでサポートされている「enable」や「disable」のような値を取ることができます。


```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  meta-properties
   action: enable
   properties:
    name: $parameters.name
    servicetype: HTTP
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

上記の例では、「my-lbvserver-comp」コンポーネントのタイプは「ns:: lbvserver」です。「ns」は、インポート StyleBook のセクションで指定した名前空間 netscaler.nitro.config とバージョン 10.5 を指すプレフィックスです。「lbvserver」は、この名前空間の NITRO リソースです。暗黙的なアクションとして、LBV サーバーは最初に StyleBook によって作成され、次に「enable」操作が実行されます。

メタプロパティで指定されたアクションは、ConfigPack の作成時にのみ構成オブジェクトに対して実行されます。ConfigPack を更新しても、CRUD 以外のアクションは実行されません。

> 注:
>
> action 属性の値は、動的に評価される StyleBook 式であってはなりません。

API を使用して StyleBook から設定を作成する

February 6, 2024

StyleBook を作成したら、それを Citrix Application Delivery Management（ADM）にインポートして、Citrix ADM または Citrix ADM API を使用して使用する必要があります。NetScaler ADM はインポート時に StyleBook を検証し、検証が成功すると、StyleBook の NetScaler ADM カタログに StyleBook が表示され、構成の作成に使用できます。

StyleBook API を使用して、この StyleBook に基づいて構成を作成できるようになりました。curl コマンドラインツールや Postman chrome ブラウザ拡張機能などの任意のツールを使用して、Citrix ADM に HTTP リクエストを送信できます。

例 1

負荷分散仮想サーバーを作成するために、StyleBook で作成した「lb-vserver」StyleBook について考えてみます。REST API を使用して、この StyleBook から次のように構成パックを作成します。


```
POST

https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/lb-vserver/configpacks

<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters": {

      "name": "lb1",
      "ip": "10.102.117.31"
     }
 ,
    "target_devices":
    [
      {

        "id": "deecee30-f478-4446-9741-a85041903410"
       }

    ]
 }

 }

<!--NeedCopy-->
```

この HTTP リクエストでは、ID（例:”deecee30-f478-4446-9741-a85041903410”）は、負荷分散仮想サーバー lb1 が IP アドレス 10.102.117.31 が作成される NetScaler ADC インスタンスのインスタンス ID です。NetScaler ADC インスタンスのインスタンス ID は NetScaler ADM から取得されます。

NetScaler ADM によって管理されるインスタンスの ID を取得するには、NetScaler ADM API を使用します。たとえば、IP アドレスが 192.168.153.160 の Citrix ADC インスタンスのインスタンス ID を取得するには、次の API を使用できます。

```
GET https://<MAS-IP>/nitro/v1/config/ns?filter=ip_address
   :192.168.153.160
<!--NeedCopy-->
```

```
Accept: application/json
<!--NeedCopy-->
```

応答ではペイロード内に ID が含まれています。


```
200
OK
Content-Type: application/json
{

  "errorcode": 0,
  "message": "Done",
  "operation": "get",
  "resourceType": "ns",
  "username": "nsroot",
  "tenant_name": "Owner",
  "resourceName": "",
  "ns":
  [
    {

    "is_grace": "false",
    "hostname": "",
    "std_bw_config": "0",
    "gateway_deployment": "false",
    …"id": "deecee30-f478-4446-9741-a85041903410",
    ...
    }

 ]
 }

<!--NeedCopy-->
```

構成 (configpack) が正常に作成されると、次の HTTP 応答が返されます。

```
200 OK
Content-Type: application/json
{

  "configpack":
  {

    "config_id": "1460806080"
   }

 }

<!--NeedCopy-->
```

これで、ID 1460806080 を使用して一意に識別される最初の構成 (コンフィグパック) が作成されました。この ID を使用して、構成のクエリ、更新、削除を行えます。

例 **2**

同じ StyleBook を使用して別の構成または構成パックを作成し、同じまたは異なる Citrix ADC インスタンスで実行できます。この例では、別の構成を作成し、仮想サーバーに異なる名前と IP アドレスを指定します。また、負荷分散の方法として LEASTCONNECTION を指定します。この構成を 2 つの NetScaler ADC インスタンスにデプロイします。

HTTP 要求は次のとおりです。

```
POST

https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/lb-vserver/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters":
    {

      "name": "lb2",
      "ip": "10.102.117.32",
      "lb-alg": "LEASTCONNECTION"
     }
 ,
    "target_devices"
    [
     {
 "id": "deecee30-f478-4446-9741-a85041903410" }
 ,
     {
 "id": "debecc60-d589-4557-8632-a74032802412" }

    ]
   }

 }

<!--NeedCopy-->
```

この HTTP リクエストでは、IP アドレス 10.102.117.32 の負荷分散仮想サーバー lb2 が、ids “deecee30-f478-4446-9741-a85041903410”と”debecc60-d589-4557-8632-a74032802412”で表される 2 つの NetScaler ADC インスタンスに作成されます。

構成パックが正常に作成されると、次の HTTP 応答が受信されます。


```
200 OK
Content-Type: application/json
{

   "configpack":
  {

     "config_id": "1657696292"
   }

 }

<!--NeedCopy-->
```

この新しいコンフィグパックの ID は 165769629 が異なります。この ID を使用することで、この構成を更新または削除できます。

例 3

「基本的な負荷分散の構成を作成するための StyleBook」で作成した「basic-lb-config」StyleBook を参考にします。REST API を使用して、この StyleBook から次のように構成パックを作成します。

```
POST

http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example
    .stylebooks/0.1/basic-lb-config/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters":
    {

      "name": "myapp",
      "ip": "10.70.122.25",
      "svc-servers":
      ["192.168.100.11","192.168.100.12"],
       "svc-port": 8080
     }
 ,
    "target_devices":
    [
     {

      "id": "deecee30-f478-4446-9741-a85041903410"
      }
```



```
,
    {

     "id": "debecc60-d589-4557-8632-a74032802412"
     }

   ]
  }

}

<!--NeedCopy-->
```

この HTTP リクエストでは、2 つの NetScaler ADC インスタンスで負荷分散構成が実行されます。これらの NetScaler ADC インスタンスにログオンして、仮想サーバーと 2 つのサービスがバインドされたサービスグループが作成されているかどうかを確認できます。

例 **4**

「複合 StyleBook の作成」で作成した複合 StyleBook の **composite-example** を参考にします。REST API を使用して、この StyleBook から次のように構成パックを作成します。

```
POST http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters": {

      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53"]
     }
,
    "target_devices":
    [
    {

      "id": "deecee30-f478-4446-9741-a85041903410"
     }
,
    {

      "id": "debecc60-d589-4557-8632-a74032802412"
```



```
      }

    ]
   }

 }

<!--NeedCopy-->
```

この HTTP リクエストでは、構成は ID で表される 2 つの NetScaler ADC インスタンスに作成されます。NetScaler ADC インスタンスにログオンすると、「複合例」StyleBook にインポートされた「basic-lb-config」StyleBook で作成された構成オブジェクトを表示できます。また、「composite-example」StyleBook の一部だった「myapp-mon」という新しい HTTP モニターも表示されます。

構成パックが正常に作成されると、次の HTTP 応答が受信されます。

```
200 OK
Content-Type: application/json{

  "configpack": {

    "config_id": "4917276817"
   }

 }

<!--NeedCopy-->
```

構成の更新

たとえば、IP アドレスが 10.102.29.54 の新しいバックエンドサーバーを負荷分散仮想サーバー myapp に追加してこの構成を更新するには、以下のように API を使用して構成パックを更新します。

```
PUT http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks/4917276817
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack": {

    "parameters": {

      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]
   }
 ,
```



```
  "target_devices":
  [
    {

    "id": "deecee30-f478-4446-9741-a85041903410"
     }
 ,
  {

    "id": "debecc60-d589-4557-8632-a74032802412"
   }

]
 }

 }

<!--NeedCopy-->
```

構成パックが正常に更新されると、次の HTTP 応答が受信されます。

```
200 OK
Content-Type: application/json
{

   "configpack": {

     "config-id": "4917276817"
   }

 }

<!--NeedCopy-->
```

構成の削除

この構成を（すべての Citrix ADC インスタンスから）削除するには、次のように API を使用して構成パックを削除します。

```
DELETE http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks/4917276817
<!--NeedCopy-->
```

```
Accept: application/json
<!--NeedCopy-->
```

コンフィグパックが正常に削除されると、次の HTTP 応答が受信されます。

```
200 OK
Content-Type: application/json
{
```



```
4
5     "configpack": {
6
7       "config_id": "4917276817"
8     }
9
10   }
11
12  <!--NeedCopy-->
```

Citrix ADC インスタンスにログオンして、この構成パックに含まれるすべての構成オブジェクトが削除されていることを確認できます。

すべての NetScaler ADC インスタンスからではなく、特定の NetScaler ADC インスタンスから構成を削除する場合は、上記の構成パックの更新操作を使用し、JSON ペイロードの「target_devices」属性を変更して、特定の NetScaler ADC インスタンス ID を削除します。

API を使用して証明書とキーファイルをアップロードする設定を作成する

February 6, 2024

StyleBook API を使用して、この StyleBook に基づいて構成を作成します。curl コマンドラインツールや Postman chrome ブラウザ拡張機能などの任意のツールを使用して、HTTP リクエストを NetScaler Application Delivery Management（ADM）に送信できます。

SSL 証明書と証明書キーファイルを NetScaler ADM にアップロードする StyleBook を作成する方法で証明書とキーファイルをアップロードするために作成した StyleBook の例を考えてみましょう。REST API を使用して、この StyleBook から次のように構成パックを作成します。

```
1  POST
2
3  https://<MAS_IP_Address>/stylebook/nitro/v1/config/stylebooks/com.
       citrix.adc.stylebooks/1.0/lb-mon/configpacks?mode=async
4  <!--NeedCopy-->
```

```
1  Content-Type: application/jsonAccept: application/json {
2
3     "configpack": {
4
5         "parameters": {
6
7             "lb-appname": "lbmon",
8             "lb-virtual-ip": "13.1.11.10",
9             "lb-virtual-port": "80",
10            "lb-service-type": "HTTP",
11            "svc-service-type": "HTTP",
12            "svc-servers": [
```



```
                {

                    "ip": "14.1.1.15",
                    "port": "80"         }

        ],
            "certificates": [
                {

                    "cert-name": "server_cert",
                    "cert-file": "server_cert.pem",
                    "ssl-inform": "PEM",
                    "key-name": "server_key",
                    "key-file": "server_key.pem",
                    "cert-password": "secret",
                    "cert-advanced": {

                        "is-ca-cert": false,
                        "skip-ca-name": false
            }

          }

        ],
            "lb-advanced": {

                "flush-on-state-down": "ENABLED",
                "auth-params": {

                    "authentication": "OFF",
                    "authentication-http-401": "OFF"
          }
  ,
                "appflow-log": "ENABLED",
                "algorithm": "LEASTCONNECTION"
         }
  ,
            "svcg-advanced": {

                "svc-client-ip": "DISABLED",
                "svc-use-source-ip": "NO",
                "svc-use-proxy-port": "NO",
                "svc-surge-protection": "OFF",
                "svc-client-keepalive": "NO",
                "svc-tcp-buffering": "NO",
                "svc-compression": "NO",
                "svc-state": "ENABLED",
                "svc-downstate-flush": "DISABLED",
                "svc-enable-health-monitor": "NO"
          }

       }
  ,
```



```
        "targets": [
            {

                "id": "8c158e7a-0087-423f-91b0-0ccf16de552a"
        }

     ]
    }

 }

<!--NeedCopy-->
```

このコンフィグパックは、ID 8c158e7a-0087-423f-91b0-0ccf16de552a を使用して一意に識別されます。この ID を使用して、構成のクエリ、更新、削除を行えます。configpack が正常に更新されると、証明書ファイルとキーファイルが NetScaler ADM ファイルシステムにアップロードされます。

API を使用して任意のファイルタイプをアップロードする設定を作成する

February 6, 2024

Citrix Application Delivery Management（ADM）API を使用して、選択した Citrix ADC インスタンスにファイルをアップロードする構成パックを作成することもできます。

「NetScaler ADC MA Service にファイルをアップロードする StyleBook を作成する方法」で、あらゆる種類のファイルをアップロードするために作成した StyleBook の例を考えてみましょう。上記のトピックの例のように、構成パックを作成し、Citrix ADM 上のロケーションファイルのファイルパスとして「locationfile」パラメーターの値を指定します。
REST API を使用して、次のようにこの StyleBook からコンフィグパックを作成します。

```
POST

https://<mas_ip>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.
    stylebooks.samples/1.0/upload-geolocations/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

   "configpack":
   {

      "parameters": {

         "locationfile": "/var/mps/tenants/root/files/ /
          custom_geolocations.csv"
```



```
      }
 ,
      "targets": [
         {

            "id": "5e540839-cd6c-437e-ac53-7d49bc2602b5"
        }

    ]
   }

 }

<!--NeedCopy-->
```

API を使用してカスタム StyleBook をインポートする

February 6, 2024

StyleBook API を使用して、カスタム StyleBook を NetScaler Application Delivery Management（ADM）にインポートできるようになりました。curl コマンドラインツールや Postman chrome ブラウザ拡張機能などの任意のツールで、REST API を使用してこの StyleBook から構成パックを次のように作成します。たとえば、example-lb という名前の StyleBook をインポートして、NetScaler ADC インスタンスでロードバランサー構成を作成できます。

```
HTTP Method: POST
URL: http://<mas-ip>/stylebook/nitro/v1/config/stylebooks
Headers:
Content-Type: application/json
Accept: application/json
RequestBody:
{

       "stylebook":
  {

     "file_name": "example-lb.yaml",
     "source": "<base64-contents>",
     "encoding": "base64"
   }

 }

<!--NeedCopy-->
```

ここで、「ソース」属性の値は、StyleBook ファイルのコンテンツの base64 エンコーディングです。たとえば、https://www.browserling.com/tools/file-to-base64 StyleBook ファイルの YAML コンテンツをオンライン

ツールに貼り付けて base64 文字列を取得し、それを上記の「source」属性の値として使用できます。

この API 呼び出しを使用すると、複数の StyleBook ファイルを含む圧縮された tarball ファイル（.tgz ファイル）を 1 つの API オペレーションでアップロードすることもできます。そのためには、file_name 属性を.tgz ファイル名に、source 属性の値を.tgz ファイルの内容の base64 エンコーディングに変更するだけです。

ツールで API が正常に実行されると、StyleBook が NetScaler ADM にインポートされたことを示す次の応答が表示されます。

```
200 OK
<!--NeedCopy-->
```

レスポンス本文**:**

```
{


  "stylebook":
{


    "name": "example-lb",

    "namespace": "com.example.stylebook",

    "version": "1.0"

   }


 }

<!--NeedCopy-->
```

API を使用してカスタム StyleBook をダウンロードする

February 6, 2024

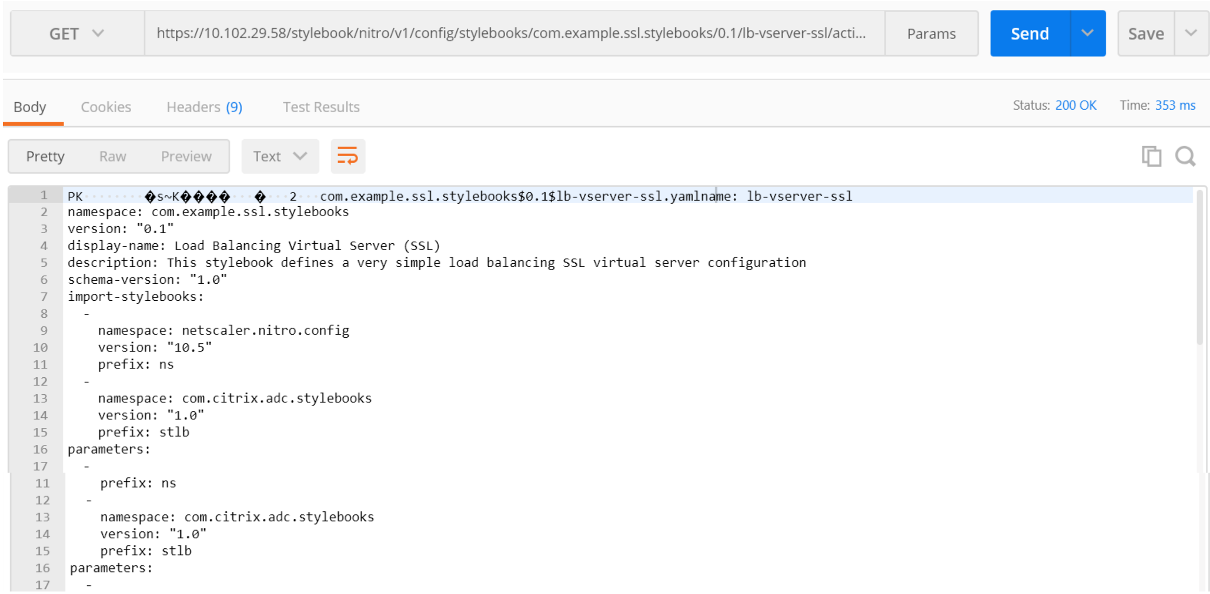
以下の StyleBook REST API を提供することで、カスタム StyleBook をダウンロードできます。

```
GET

https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
   VERSION>/<NAME>/actions/download
<!--NeedCopy-->
```

IP アドレス、名前、バージョン、名前空間のフィールドを変更した後は、curl コマンドラインツールや Postman chrome ブラウザ拡張機能など、どのツールでも API を実行できます。


```
GET

https://10.102.29.58/stylebook/nitro/v1/config/stylebooks/com.example.
    ssl.stylebooks/0.1/lb-vserver-ssl/actions/download`
<!--NeedCopy-->
```

.yaml 形式の StyleBook がダウンロードされます。



API を使用してカスタム StyleBook を削除する

February 6, 2024

カスタム StyleBook を削除するには、次の StyleBook REST API を指定します。

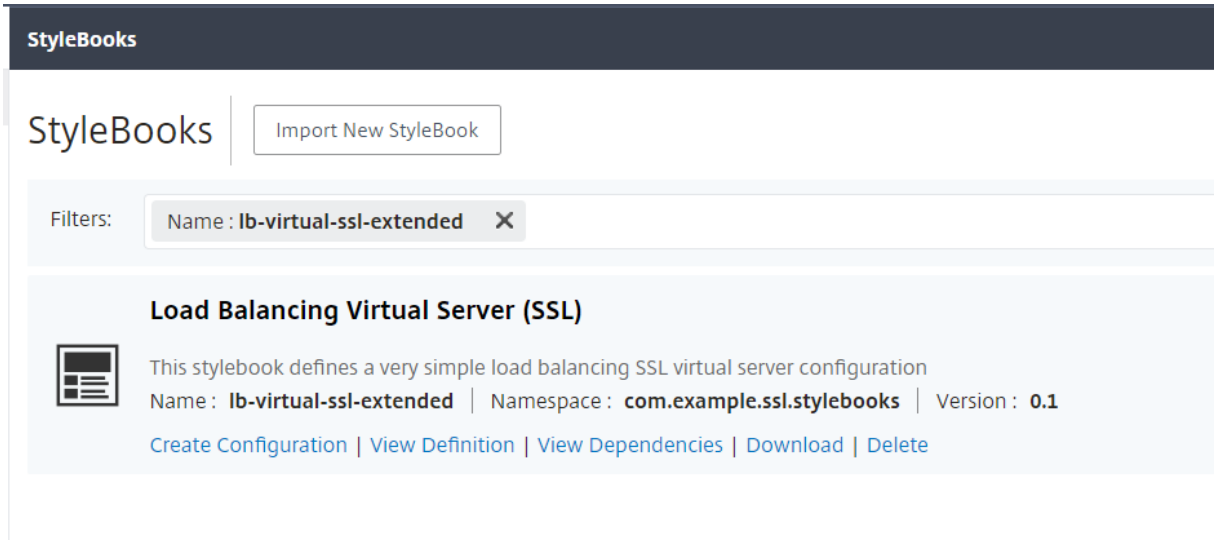
```
DELETE

https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
    VERSION>/<NAME>?dependencies=true
<!--NeedCopy-->
```

URL の依存関係クエリパラメータが指定されていないか、その値が false に設定されている場合、StyleBook の依存関係は削除されません（StyleBook 自体のみが削除されます）。

HTTP 応答ステータスコード 200 を受け取った場合は、カスタム StyleBook（およびその依存関係）が Citrix ADM から正常に削除されたことを意味します。

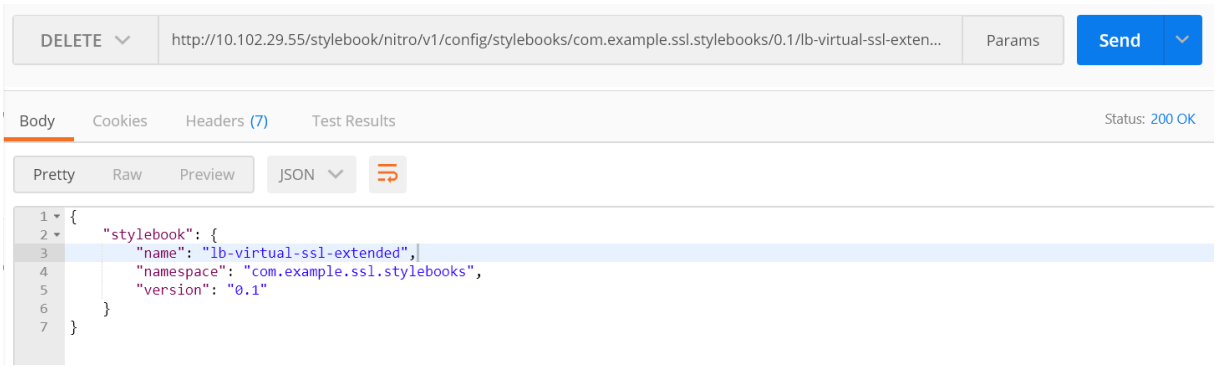
> 注:
>
> MA サービス内の他の StyleBook が依存しているカスタム StyleBook は削除できません。

たとえば、Citrix ADM で「lb-virtual-ssl-extended」という名前の StyleBook を作成したとします。後でその StyleBook を削除することにしました。

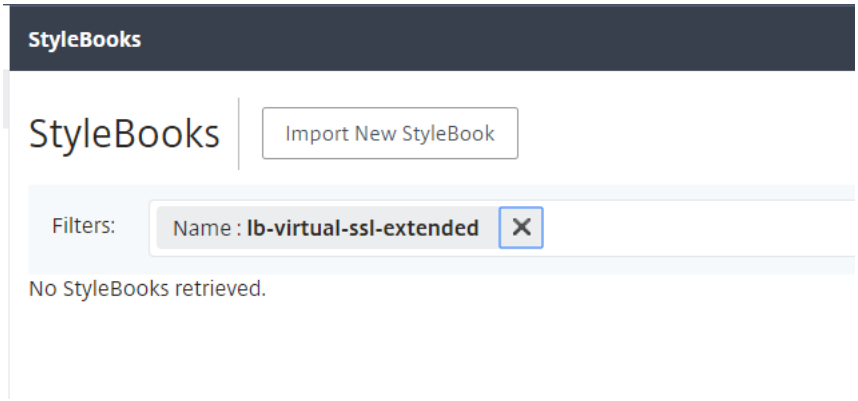


IP アドレス、名前、バージョン、名前空間のフィールドを変更した後は、curl コマンドラインツールや Postman chrome ブラウザ拡張機能など、どのツールでも API を実行できます。

https://10.102.29.55/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-virtual-ssl-extended?dependencies=falseを削除する



StyleBook が NetScaler ADM から削除されます。



StyleBook の文法

February 6, 2024

独自の StyleBook をデザインして CitrixApplication Delivery Management（ADM）にインポートし、Citrix ADM GUI または API を使用して構成を作成できます。独自の StyleBook を作成するには、まず、使用できるさまざまな構造および属性の文法と構文について理解しておく必要があります。

このドキュメントでは、StyleBook の作成時に使用できるさまざまな構造および参照について説明します。

次の表のセクション名、構造名、または参照名をクリックすると、詳細が表示されます。

–	–
[Header](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/header-section.html)	[StyleBook のインポート](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/import-stylebooks-section.html)
[Parameters](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parameters-section.html)	[パラメータ-デフォルトソース構成](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parameters-default-sources-construct.html)
[Substitutions](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/substitutions.html)	[Components](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/components.html)
[オプションのプロパティ](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/optional-properties.html)	[ヘルパーコンポーネント](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/helper-components.html)
[プロパティデフォルトソース](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/properties-default-sources.html)	[ネストされたコンポーネ

ン　　ト](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/nested-components.html) |
[条件構成](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/condition-construct.html)	[repeat 構造](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/repeat-construct.html)
[繰り返し条件構成](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/repeat-condition-construct.html)	[Outputs](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/outputs.html)
[ネストされた繰り返し](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/nested-repeats.html)	[親　参　照](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parent-reference.html)
[パラメータ参照](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parameter-reference.html)	[置換参照](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/substitutions-reference.html)
[コンポーネントのリファレンス](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/components-reference.html)	[Operations](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/operations.html)
[変数参照](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/variable-reference.html)	[Alarms](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/alarms.html)
[分　析](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/analytics.html)	[組み込み関数](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/built-in-functions.html)
[式](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/expressions.html)	[依存関係の検出](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/dependency-detection.html)
インプレース補間

> 注
>
> リピートアイテム、リピートインデックス、または置換関数の引数を定義する際には、次の予約語を使用してユーザー定義変数に $ という名前を付けないでください。<var-name>
>
> - stylebook、parameters、substitutions、components、properties、outputs、parent、self、operations、analytics、alarms
> - repeat-item, repeat-item-0, repeat-item-1, repeat-item-2
> - repeat-index, repeat-index-0, repeat-index-1, repeat-index-2
> - デフォルト
> - roles, role, targets, target
> - context、parent-context、parent_context

独自の StyleBook を設計する方法とその例については、「独自の StyleBook の作成方法」を参照してください。

Header

February 6, 2024

StyleBook の先頭の 6 行は、Header セクションです。このセクションでは、StyleBook の ID を定義し、StyleBook の実行内容を記述できます。これは必須セクションです。

次の表は、Header セクションの属性について説明しています。

属性	[説明]
–	–
name	StyleBook を識別する名前。この属性は必須です。
説明	StyleBook の実行内容を定義する説明。この説明は NetScaler ADM GUI に表示されます。これはオプションの属性です。
display-name	StyleBook を識別するための任意の名前。この名前は NetScaler ADM GUI に表示されます。これはオプションの属性です。
author	StyleBook を作成した作成者また組織。これはオプションの属性です。
namespace	名前空間は、StyleBook の一意の識別子の一部で、これにより名前の衝突を回避できます。namespace には任意の文字列を指定できますが、StyleBook のセットを作成したまたは所有している会社、部門または部署の名前を使用することをお勧めします。たとえば、次の形式を使用できます <company>.<department>.<unit>.stylebooks。これは必須属性です。
version	StyleBook のバージョン番号。バージョン番号は、StyleBook の更新時に変更できます。異なるバージョンの StyleBook を共存させることができます。これは必須属性です。
schema-version	StyleBook スキーマのバージョン。NetScaler ADM の現在のリリースでは「1.0」という値を使用します。これは必須属性です。
private	この属性を true に設定すると、NetScaler ADM GUI に StyleBook は表示されません。これは、他の StyleBook の構築ブロックである StyleBook で有用な設定であり、ユーザーが直接使用するものではありません。これはオプションの属性です。デフォルト値は、false です。

例:

```
      name: lb
    description: "This stylebook defines a sample load balancing
    configuration."
    display-name: "Load Balancing StyleBook (HTTP)"
    author: Mike Smith (ACME Infra team)
    namespace: com.example.stylebooks
    schema-version: "1.0"
    version: "0.1"
<!--NeedCopy-->
```


name、namespace、および version の組み合わせにより、システム内で StyleBook が一意に識別されます。NetScaler ADM では、名前、名前空間、およびバージョンの組み合わせが同じ 2 つの StyleBook を使用することはできません。ただし、name と version が同じであっても namespace が異なる場合、または namespace と version が同じであっても name が異なる場合は、それらの 2 つの StyleBook を使用できます。

StyleBook のインポート

February 6, 2024

これは StyleBook の第 2 セクションで、現在の StyleBook から参照するほかの StyleBook を宣言できます。このセクションを記述すると、他の StyleBook をインポートして再利用できるため、StyleBook で同じ構成を再作成する必要がなくなります。これは必須セクションです。

現在の StyleBook で参照する StyleBook の名前空間とバージョン番号を宣言する必要があります。いずれかの NITRO 構成オブジェクトを直接使用する場合、StyleBook では、netscaler.nitro.config 名前空間を必ず参照する必要があります。この名前空間には、lbvserver サービスやモニターなど、すべての Citrix ADC NITRO タイプが含まれています。NetScaler ADC バージョン 10.5 以降の StyleBook がサポートされています。つまり、StyleBook を使用して、リリース 10.5 以降を実行するすべての NetScaler ADC インスタンス上で構成を作成および実行できます。

import-stylebooks セクションで使用される **prefix** 属性は、名前空間とバージョンの組み合わせを示すための略語です。たとえば、「ns」プレフィックスを使用して、名前空間 netscaler.nitro.config とバージョン 10.5 を示すことができます。StyleBook の以降のセクションでは、StyleBook を名前空間とバージョンで示すたびにこの名前空間とバージョンを使用する代わりに、選択したプレフィックス文字列と、StyleBook を一意に識別する名前を使用できます。

例:

```
      import-stylebooks:
       -
         namespace: netscaler.nitro.config
         version: "10.5"
         prefix: ns
      -
       namespace: com.acme.stylebooks
        version: "0.1"
        prefix: stlb
<!--NeedCopy-->
```

上の例では、最初に定義されているプレフィックスは ns で、名前空間 netscaler.nitro.config とバージョン 10.5 を示します。2 番目に定義されているプレフィックスは stlb で、名前空間 com.acme.stylebooks とバージョン 0.1 を示します。

プレフィックスを定義した後は、特定の名前空間とバージョンに属するタイプまたは StyleBook を示すたびに、**< 名前空間の略語 >::< タイプ名 >** という表記を使用できます。たとえば、**ns::lbvserver** は、名前空間

netscaler.nitro.config、バージョン 10.5 で定義されているタイプ lbvserver を示します。タイプ名 > 名前空間の略語 >

同様に、com.acme.stylebooks 名前空間にあるバージョン「0.1」の StyleBook を示す場合は、**stlb::** という表記を使用できます。

> 注
>
> 慣例により、プレフィックス「ns」は、NetScaler ADC NITRO 名前空間を参照するために使用されます。

パラメーター

February 6, 2024

このセクションでは、構成を作成するために必要な StyleBook のすべてのパラメーターを定義します。StyleBook では、このセクションに記述された入力が使用されます。このセクションはオプションですが、ほとんどの StyleBook で必要になります。StyleBook を使用して Citrix ADC インスタンスで構成を作成するときにユーザーに回答してもらいたい質問を定義するには、パラメーターセクションを検討してください。

StyleBook を Citrix ADM にインポートして構成を作成すると、GUI は StyleBook のこのセクションを使用して、定義したパラメーターの値を入力するフォームを表示します。

次のセクションでは、このセクションの各パラメータに指定する必要がある属性について説明します。

name

定義するパラメーターの名前。英数字名を指定できます。

名前はアルファベットで始まる必要があり、追加でアルファベット、数字、ハイフン（-）、またはアンダースコア（_）を含めることができます。

StyleBook の作成時に、この「name」属性を使用して、$parameters.< 名前 > という表記でほかのセクションのパラメーターを参照できます。名前 >

必須? はい

ラベルに貼り付けます

ADM GUI でこのパラメータの名前として表示される文字列。

必須? いいえ

説明

パラメーターの使用目的について説明するヘルプ文字列。ユーザーがこのパラメータのヘルプアイコンをクリックすると、ADM GUI にこのテキストが表示されます。

必須? いいえ

種類

そのパラメーターで使用できる値のタイプ。パラメータには、
次の組み込み型のいずれかを使用できます。

- string：文字の配列。長さが指定されていない場合、文字列値には、任意の数の文字を使用できます。ただし、min-length 属性と max-length 属性を使用すれば、文字列タイプの長さを制限できます。
- number：整数。min-value 属性と max-value 属性により、このタイプで使用できる最小数と最大数を指定できます。
- boolean：true と false のいずれかを設定できます。YAML では、すべてのリテラルがブール値（例：Yes または No）と見なされることに注意してください。
- ipaddress：有効な IPv4 アドレスまたは IPv6 アドレスを示す文字列。
- tcp-port：TCP ポートまたは UDP ポートを示す 0～65535 の数値。
- password：不透明な秘密の文字列値を表します。Citrix ADM GUI にこのパラメーターの値が表示される場合、アスタリスク（*****）として表示されます。
- certfile：証明書ファイルを表します。これにより、ADM GUI を使用して StyleBook 構成を作成するときに、ローカルシステムからファイルを直接アップロードできます。アップロードされた証明書ファイルは /var/mps/tenants/ ディレクトリに保存されます ADM の /ns_ssl_certs。

  証明書ファイルは、ADM が管理する証明書のリストに追加されます。
- keyfile：証明書キーファイルを表します。これにより、Citrix ADM GUI を使用して StyleBook 構成を作成するときに、ローカルシステムからファイルを直接アップロードできます。アップロードされた証明書ファイルは /var/mps/tenants/ ディレクトリに保存されます Citrix ADM の /ns_ssl_keys。

  証明書キーファイルは、Citrix ADM が管理する証明書キーのリストに追加されます。
- file：ファイルを表します。
- object：このタイプは、関連する複数のパラメーターを 1 つの親要素の下にグループ化する場合に使用します。親パラメーターのタイプとして「object」を指定する必要があります。タイプが「object」のパラメーターにはネストされた「Parameters」セクションを含めることができ、そのセクションに含まれるパラメーターを記述できます。
- 別の StyleBook：このタイプのパラメータを使用すると、このパラメータは、その値が StyleBook で定義されているパラメータの型であることを期待します。

パラメータには、型の末尾に「[]」を追加することで、上記
のいずれかの型のリストである型を指定することもできます。たとえば、タイプ属性が string [] の場合、このパラメーターは
文字列のリストを入力として受け取ります。この StyleBook から構成を作成するときに、
このパラメータに文字列を 1 つ、2 つ、または複数の文字列を指定できます。

必須? はい

キー

true または false を指定して、このパラメーターが StyleBook のキーパラメーターかどうかを示します。

StyleBook で「キー」パラメーターとして定義できるパラメーターは 1 つだけです。

同じ StyleBook から（同じまたは異なる Citrix ADC インスタンスで）異なる構成を作成すると、各構成でこのパラメーターの値は
異なります。

デフォルト値は false です。

必須? いいえ

必須

true または false を指定して、パラメーターが必須か、任意かを示します。true
に設定した場合、パラメータは必須であり、ユーザーは構成の作成時にこの
パラメータの値を指定する必要があります。

NetScaler ADM GUI により、このパラメーターに有効な値が指定されます。

デフォルト値は false です。

必須? いいえ

> 注 パラメータにおよびが`type: object`ある`required: false`場合、このパラメータのサブパラメータは評価されません。

サブパラメータのデフォルト値を有効にする場合は、メイン`required: true`パラメータを次のように設定します。

```
    type: object
    required: true
    gui:
      collapse_pane: true
<!--NeedCopy-->
```

collapse_pane 属性は、ユーザーがペインを展開しない限り、UI でオブジェクトとそのサブパラメーターを折りたたんで表示します。

allowed-values

型が「string」に設定されている場合、この属性を使用して、パラメータの有効な値のリストを定義します。

NetScaler ADM GUI から構成を作成する場合、ユーザーはこのリストからパラメーター値を選択するように求められます。

例 **1**:

名前:IP アドレス

type: string

許容値:

- SOURCEIP
- ウエストチップ
- NONE

例 **2**:

名前:TCP ポート

type: tcp-port

許容値:

- 80
- 81
- 8080

サンプル **3**:

(tcp-port のリスト。リストの各要素は、許可された値
で指定された値のみを持つことができます)

name: tcpports

タイプ:TCP ポート []

許容値:

- 80
- 81
- 8080
- 8081

必須? いいえ

デフォルト

任意のパラメーターにデフォルト値を割り当てるには、この属性を使用します。構成の作成時に、ユーザーが値を指定しない場合、デフォルト値が使用されます。

Citrix ADM GUI から構成を作成するときに、ユーザーがデフォルト値のないパラメーターに値を入力しない場合、そのパラメーターには値が設定されません。

例 **1**:

名前: タイムアウト

タイプ: 番号

デフ・アダルト:20

例 **2**:

(パラメータのデフォルト値は値のリストです):

name: protocols

タイプ: 文字列 []

default:

- TCP
- UDP
- IP

サンプル **3**:

名前: タイムアウト

タイプ: 番号

デフ・アダルト:20

例 **4**:

名前:TCP ポート

type: tcp-port

デフ・アダルト:20

必須? いいえ

pattern

この属性を使用して、パラメータの型が「string」の場合に、このパラメータの有効な値のパターン（正規表現）を定義します。

例:

名前: アプリ名

type: string

パターン:「[A-Z] +」

必須? いいえ

min-value

種類が「number」または「tcp-port」のパラメーターの最小値を定義するには、この属性を使用します。

例:

名前: オーディオポート

type: tcp-port

最小値:5000

数値の最小値は負でもかまいませんが、tcp-port の最小値は
負であってはなりません。

必須? いいえ

max-value

この属性を使用して、「number」または
「tcp-port」タイプのパラメータの最大値を定義します。

定義されている場合、最大値は最小値より大きくなければなりません。

例:

名前: オーディオポート

type: tcp-port

最小値:5000

最大値:15000

必須? いいえ

min-length

この属性を使用して、「string」
タイプのパラメータに受け入れられる値の最小長を定義します。

値として定義される文字の最小長は 0 以上でなければ
なりません。

例:

名前: アプリ名

type: string

最小長さ:3

必須? いいえ

max-length

種類が「string」のパラメーターに入力できる値の最大文字数を定義するには、
この属性を使用します。

値の最大長は、min-length で
定義された文字の長さ以上でなければなりません。

例:

名前: アプリ名

type: string

最大長:64

必須? いいえ

min-items

この属性を使用して、リストであるパラメータ内の項目の最小数
を定義します。

項目の最小数はゼロ以上でなければなりません。

例:

name: server-ips

タイプ:IP アドレス []

min-items: 2

必須? いいえ

max-items

リストであるパラメータ内の項目の最大数を定義するには、
この属性を使用します。

項目の最大数は、定義されている場合は最小項目数より大きくなければなりません。

例:

name: server-ips

タイプ:IP アドレス []

min-items: 2

最大アイテム数:250

必須? いいえ

gui

この属性を使用して、Citrix ADM GUI の「オブジェクト」タイプのパラメータの
レイアウトをカスタマイズします。

必須? いいえ

columns

これは gui 属性のサブ属性です。これを使用して、Citrix ADMGUI に表示する
列の数を定義します。

必須? いいえ

updatable

これは gui 属性のサブ属性です。これを使用して、構成の作成後にパラメーター
を更新できるかどうかを指定します。

値を false に設定すると、構成の更新時にパラメーターフィールドが灰色表示になります。

必須? いいえ

collapse_pane

これは gui 属性のサブ属性です。これを使用して、このオブジェクトパラメータのレイアウト
を定義するペインが折りたたみ可能かどうかを指定します。

値を true に設定すると、ユーザーはこの親パラメーターの下にある子パラメーターを展開したり折りたたんだりできるようになります。

例:

```
    gui:

     collapse_pane: true

     columns: 2

     updatable: false
<!--NeedCopy-->
```

Parameters セクション全体の例:

```
parameters:

   -

      name: name

      label: Name

      description: Name of the application

      type: string

      required: true

       -

         name: ip

         label: IP Address

         description: The virtual IP address used for this application

         type: ipaddress

         required: true

      -

         name: svc-servers

         label: Servers

         type: object[]

         required: true

         parameters:
```



```
38
39              -
40
41                 name: svc-ip
42
43                 label: Server IP
44
45                 description: The IP address of the server
46
47                 type: ipaddress
48
49                 required: true
50
51                  -
52
53                    name: svc-port
54
55                    label: Server Port
56
57                    description: The TCP port of the server
58
59                    type: tcp-port
60
61                    default: 80
62
63        -
64
65            name: lb-alg
66
67            label: LoadBalancing Algorithm
68
69            type: string
70
71            allowed-values:
72
73              - ROUNDROBIN
74
75              - LEASTCONNECTION
76
77            default: ROUNDROBIN
78
79        -
80
81            name: enable-healthcheck
82
83            label: Enable HealthCheck?
84
85            type: boolean
86
87            default: true
88  <!--NeedCopy-->
```

次の例では、一覧のすべての属性と、前のセクションで説明した値を定義しています。

“‘YAML
名: 機能リスト

タイプ: 文字列 []**

最小長さ:1

最大長:3

最小アイテム:1

最大アイテム数:3

パターン:「[A-Z] +」

allowed-values:

-小さじ

-ポンド

-個

デフォルト:

-ポンド

パラメータ-デフォルトソース構成

February 6, 2024

この構造を使用すると、ほかの StyleBook のパラメーター定義を再利用できます。

パラメーターまたはパラメーターグループを複数の StyleBook で繰り返し使用するシナリオについて考えてみます。新しい StyleBook を作成するたびにこれらのパラメーターを再定義することを避けるために、パラメーターを一度定義してから、**parameters-default-sources** 構造を使用して、これらのパラメーターを必要とする StyleBook にその定義をインポートできます。

たとえば、StyleBook の多くで仮想 IP を構成する必要がある場合は、新しく作成する各 StyleBook で仮想 IP に関連する同じパラメーターの定義が必要になることがあります。代わりに、「vip-params」のような名前の StyleBook を別途作成し、この StyleBook で次の例に示すように、仮想 IP に関連するすべてのパラメーターを定義できます。

```
-
name: vip-params
namespace: com.acme.commontypes
version: "1.0"
description: This StyleBook defines a typical virtual IP config.
private: true
schema-version: "1.0"
parameters:
```



```
9          -
10              name: lb-appname
11              label: Load Balanced Application Name
12             description: Name of the Load Balanced application
13              type: string
14              required: true
15         -
16              name: lb-virtual-ip
17              label: Load Balanced App Virtual IP address
18              description: Virtual IP address representing the Load
       Balanced application
19              type: ipaddress
20              required: true
21         -
22              name: lb-virtual-port
23              label: Load Balanced App Virtual Port
24              description: TCP port representing the Load Balanced
       application
25              type: tcp-port
26              default: 80
27         -
28              name: lb-service-type
29              label: Load Balanced App Protocol
30              description: Protocol used for the Load Balanced application
       .
31              type: string
32              default: HTTP
33              required: true
34              allowed-values:
35                   - HTTP
36                   - SSL
37                   - TCP
38 <!--NeedCopy-->
```

その後、これらのパラメーターを使用するその他の StyleBook を作成できます。以下に、このような StyleBook の例を示します。

```
1        -
2        name: acme-biz-app
3        namespace: com.acme.stylebooks
4        version: "1.0"
5        description: This stylebook defines the Citrix ADC configuration
       for Biz App
6        schema-version: "1.0"
7        import-stylebooks:
8          -
9            namespace: com.acme.commontypes
10           prefix: cmtypes
11           version: "1.0"
12       parameters-default-sources:
13             - cmtypes::vip-params
14       parameters:
15           -
```



```
            name: monitorname
            label: Monitor Name
            description: Name of the monitor
            type: string
            required: true
          -
            name: type
            label: Monitor Type
            description: Type of the monitor
            type: string
            required: true
            allowed-values:
              - PING
              - TCP
              - HTTP
              - HTTP-ECV
              - TCP-ECV
              - HTTP-INLINE
<!--NeedCopy-->
```

StyleBook acme-biz-app では、まず「import-stylebooks」セクションを使用して、vip-params StyleBook の名前空間とバージョンをインポートします。次に、**parameters-default-sources** 構造を追加して、StyleBook 名、つまり vip-params を指定します。これにより、StyleBook vip-params のパラメーターをこの StyleBook で直接定義するのと同じ効果が得られます。

parameters-default-sources は一覧であり、一覧の各項目が StyleBook であると想定されるので、複数の StyleBook のパラメーターを含めることができます。

ほかの StyleBook のパラメーターを含めることができるだけでなく、Parameters セクションを使用して独自のパラメーターを定義することもできます。StyleBook のパラメーターの一覧全体は、ほかの StyleBook のパラメーターとこの StyleBook で定義したパラメーターの組み合わせになります。したがって、式 **$parameters** はこのパラメーターの組み合わせを参照します。

パラメーターがインポートした StyleBook と現在の StyleBook の両方で定義されている場合は、現在の StyleBook 内の定義によって別の StyleBook からインポートした定義が上書きされます。インポートしたパラメーターの一部を必要に応じてカスタマイズし、残りのパラメーターをそのまま使用することで、この動作を効果的に活用できます。

parameters-default-sources 構造は、次に示すようにネストされたパラメーターでも使用できます。

```
parameters:
    -
      name: vip-details
      label: Virtual IP details
      description: Details of the Virtual IP
      type: object
      required: true
      parameters-default-sources:
              - cmtypes::vip-params
<!--NeedCopy-->
```


これは、StyleBook vip-params のパラメーターをこの StyleBook の vip-details パラメーターの子パラメーターとして直接追加する場合と同様です。

自動置換

February 6, 2024

Substitutions セクションは、StyleBook のほかの部分で StyleBook を読み取りやすくするために使用できる、複雑な式の省略名を定義するために使用されます。また、このセクションは、StyleBook で同じ式または値を複数回使用する場合にも役立ちます（定数値など）。この値に置換名を使用すると、この値を変更する必要があるときに、StyleBook に出現するすべての箇所で値を更新するのではなく（この方法ではエラーが発生しやすくなります）、置換値のみを更新できます。

置換は、このドキュメントの後の例で示すように、値のマッピングの定義にも使用できます。

一覧の各置換はキーと値で構成されます。 値には、単純な値、式、関数、またはマップを指定できます。

次の例では、2 つの置換が定義されています。1 つ目は、8181 の省略名として使用できる「http-port」です。置換を使用することで、この値を StyleBook のほかの部分で、8181 ではなく **$substitutions.http-port** として参照できるようになります。

置換:

```
http-port: 8181
```

これにより、ポート番号のニーモニック名を指定できるほか、その使用回数に関係なく、このポート番号を StyleBook 内の 1 か所で定義できます。ポート番号を 8080 に変更する場合は、Substitutions セクションで変更すると、ニーモニック名 http-port を使用しているすべての箇所にその変更が適用されます。次の例は、コンポーネントで置換を使用する方法を示しています。

```
components:
 -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
          name: $parameters.name + "-lb"
          servicetype: HTTP
          ipv46: $parameters.ip
          port: \*\*$substitutions.http-port\*\*
          lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

置換は複雑な式にすることもできます。次の例は、2 つの置換で式を使用する方法を示しています。

```
substitutions:
  app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS
  app-name: str("acme-") + $parameters.name + str("-app")
```



```
<!--NeedCopy-->
```

また、置換式では、次の例に示すように既存の置換式を使用することもできます。

```
substitutions:
  http-port: 8181
  app-name: str("acme-") + $parameters.name + str($substitutions.http-
   port) + str("-app")
<!--NeedCopy-->
```

置換のもう 1 つの便利な機能がマップで、キーを値にマップできます。以下は、マップ置換の例です。

```
substitutions:
    secure-port:
        true: int("443")
        false: int("80")
    secure-protocol:
        true: SSL
        false: HTTP
<!--NeedCopy-->
```

次の例は、マップ secure-port および secure-protocol を使用する方法を示しています。

```
components:
 -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
          name: $parameters.name + "-lb"
          servicetype: \*\*$substitutions.secure-protocol[$parameters.
   is-secure]\*\*
          ipv46: $parameters.ip
          port: \*\*$substitutions.secure-port[$parameters.is-secure
   ]\*\*
          lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

つまり、StyleBook のユーザーがパラメーター is-secure にブール値「true」を指定するか、Citrix ADM GUI でこのパラメーターに対応するチェックボックスを選択した場合、このコンポーネントの servicetype プロパティには **SSL** という値が割り当てられ、ポートプロパティには値 **443** が割り当てられます。ただし、ユーザーがこのパラメーターに「false」を指定するか、Citrix ADM GUI の対応するチェックボックスをオフにすると、servicetype プロパティには **HTTP** という値が割り当てられ、ポートには **80** という値が割り当てられます。

次の例は、置換を関数として使用する方法を示しています。置換関数は 1 つまたは複数の引数を取ることができます。引数は、string、number、ipaddress、boolean などの単純な型にする必要があります。

置換:

form-lb-name(name): $name + “-lb”

この例では、「name」という文字列引数を取り、それを使用して名前引数の文字列に「-lb」** という接尾辞を付けた新しい文字列を作成する置換関数「form-lb-name」を定義します。この置換関数を使用する式は、次のように記

述することができます。

$substitutions.form-lb-name(“my”)

これは、「my-lb」を返します。

別の例を考えてみましょう。

置換:

cspol-priority(priority): 10100 - 100 * $priority

置換 cspol-priority は、priority という引数を受け取って値の計算に使用する関数です。StyleBook のほかの部分で、この置換を次の例に示すように使用できます。

```
components:
  -
    name: cspolicy-binding-comp
    type: ns::csvserver_cspolicy_binding
    condition: not $parameters.is-default
    properties:
         name: $parameters.csvserver-name
         policyname: $components.cspolicy-comp.properties.policyname
         priority: $substitutions.cspol-priority($parameters.pool.
   priority)
<!--NeedCopy-->
```

置換は、キーと値で構成することもできます。値には、単純な値、式、関数、マップ、一覧、またはディクショナリを指定できます。

以下は、値がリストである‘slist’という置換の例です。

```
substitutions:
  slist:
    - a
    - b
    - c
<!--NeedCopy-->
```

置換の値には、以下の「sdict」という置換の例に示すように、キーと値のペアのディクショナリも指定できます。

```
substitutions:
  sdict:
    a: 1
    b: 2
    c: 3
<!--NeedCopy-->
```

一覧とディクショナリを組み合わせると、もっと複雑な属性を作成できます。たとえば、「slistofdict」という名前の置換はキーと値のペアの一覧を返します。

```
  slistofdict:
    -
```



```
      a: $parameters.cs1.lb1.port
      b: $parameters.cs1.lb2.port
    -
      a: $parameters.cs2.lb1.port
      b: $parameters.cs2.lb2.port
<!--NeedCopy-->
```

しかし、次の例では、置換「sdictoflist」はキーと値のペアを返します。ここでも値は別の一覧です。

```
  sdictoflist:
    a:
      - 1
      - 2
    b:
      - 3
      - 4
<!--NeedCopy-->
```

コンポーネントでは、これらの置換は condition、properties、repeat、repeat-condition 構造で使用できます。

次のコンポーネントの例では、置換を使用して properties を指定する方法を示します。

```
    properties:
      a: $substitutions.slist
      b: $substitutions.sdict
      c: $substitutions.slistofdict
      d: $substitutions.sdictoflist
<!--NeedCopy-->
```

値が一覧またはディクショナリの置換を定義するユースケースは、コンテンツスイッチ仮想サーバーや複数の負荷分散仮想サーバーを構成する場合です。同一の cs 仮想サーバーに関連付けされたすべての lb 仮想サーバーはまったく同じ構成を持つことができるため、置換一覧およびディクショナリを使用してこの構成を作成し、各 lb 仮想サーバーでの構成の繰り返しを避けることができます。

次の例では、コンテンツスイッチ仮想サーバー構成を作成する cs-lb-mon StyleBook の置換とコンポーネントを示します。cs-lb-mon StyleBook のプロパティを構成しながら、複雑な置換「lb-properties」で cs 仮想サーバーに関連付けた lb 仮想サーバーのプロパティを指定します。「lb-properties」置換は、名前、サービスの種類、仮想 IP アドレス、ポート、サーバーをパラメーターとして取り、値としてキーと値のペアを生成する関数です。「cs-pools」コンポーネントで、この置換の値を各プールの lb-pool パラメーターに割り当てます。

```
substitutions:
  cs-port[]:
    true: int("80")
    false: int("443")
  lb-properties(name, servicetype, vip, port, servers):
    lb-appname: $name
    lb-service-type: $servicetype
    lb-virtual-ip: $vip
    lb-virtual-port: $port
    svc-servers: $servers
```



```
    svc-service-type: $servicetype
    monitors:
      -
        monitorname: $name
        type: PING
        interval: $parameters.monitor-interval
        interval_units: SEC
        retries: 3
components:
  -
    name: cs-pools
    type: stlb::cs-lb-mon
    description: | Updates the cs-lb-mon configuration with the
    different pools provided. Each pool with rule result in a dummy LB
    vserver, cs action, cs policy, and csvserver_cspolicy_binding
    configuration.
    condition: $parameters.server-pools
    repeat: $parameters.server-pools
    repeat-item: pool
    repeat-condition: $pool.rule
    repeat-index: ndx
    properties:
      appname: $parameters.appname + "-cs"
      cs-virtual-ip: $parameters.vip
      cs-virtual-port: $substitutions.cs-port($parameters.protocol == "
    HTTP")
      cs-service-type: $parameters.protocol
      pools:
        -
          lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP"
    , "0.0.0.0", 0, $pool.servers)
          rule: $pool.rule
          priority: $ndx + 1
<!--NeedCopy-->
```

置換マップ:

キーを値にマップする置換を作成できます。たとえば、各プロトコル（キー）に使用するデフォルトポート（値）を定義するシナリオを考えてみましょう。このタスクでは、次のように置換マップを記述します。

```
substitutions:
     port:
          HTTP: 80
          DNS: 53
          SSL: 443
<!--NeedCopy-->
```

この例では、HTTP は 80 に、DNS は 53 に、SSL は 443 にマップされます。パラメーターとして与えられた特定のプロトコルのポートを取得するには、次の式を使用します。

$substitutions.port [$parameters.protocol]

この式は、ユーザーが指定したプロトコルに基づいて値を返します。

- キーが HTTP の場合、この式は 80 を返します。
- キーが DNS の場合、この式は 53 を返します。
- キーが SSL の場合、この式は 443 を返します。
- キーがマップ内に存在しない場合、この式はいずれの値も返しません。

コンポーネント

February 6, 2024

StyleBook の components 構造は、StyleBook で最も重要なセクションです。このセクションでは、作成する必要がある構成オブジェクトを定義します。この構造を使用すると、同じ種類の構成オブジェクトを 1 つまたは複数作成できます。

components 構造では、Parameters セクションの入力値を使用して、StyleBook で生成される構成に適応させることができます。このセクションはオプションですが、ほとんどの StyleBook で Components セクションが記述されています。

次の表は、コンポーネントの主要な属性を示しています。

属性	説明
name	コンポーネントの名前。英数字名を指定できます。名前はアルファベットで始まる必要があり、追加でアルファベット、数字、ハイフン（-）、またはアンダースコア（_）を含めることができます。
説明	StyleBook におけるこのコンポーネントの役割の説明。
種類	このコンポーネントで指定するプロパティはタイプによって決まります。コンポーネントには 2 種類のタイプがあります。** 組み込みタイプ **: このタイプはシステムによって提供され、定義する必要はありません。たとえば、NITRO エンティティタイプ「lbvserver」や「servicegroup」などです。コンポーネントに組み込みの type 属性がある場合、NetScaler ADC 上にそのタイプの構成オブジェクトが作成されます。たとえば、コンポーネントが組み込みタイプ「lbvserver」を参照している場合、このコンポーネントは、構成の対象である Citrix ADC インスタンス上に負荷分散仮想サーバーを作成します。** 複合タイプ **: このタイプは、作成して NetScaler ADM にインポートした既存の StyleBook を指します。コンポーネントにコンポジットタイプ属性がある場合、参照先の StyleBook で指定されているすべての構成オブジェクトが、構成のターゲットである NetScaler ADC インスタンスに作成されます。これにより、それぞれが最終構成の一部を作成する複数の StyleBook を組み合わせて使用できるようになります。複合 StyleBook について詳しくは、「[複合 StyleBook の作成](/ja-jp/netscaler-application-delivery-management-software/12-1/stylebooks/how-to-create-custom-stylebooks)」を参照してください。
properties	コンポーネントの type 属性で使用できるサブ属性。コンポーネントに対して有効なプロパティは、そのタイプによって決まります。組み込みタイプの場合、有効なプロパティは対応する NITRO オブジェクトのプロパティまたは属性です。コンポーネントのタイプが別の StyleBook である場合（つまり複合タイプの場合）、プロパティはその StyleBook で定義されているパラメーターに対応します。

例:

```
components:
   -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
         name: $parameters.name
         servicetype: HTTP
         ipv46: $parameters.ip
         port: 80
         lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

この例では、my-lbvserver-comp という名前のコンポーネントが定義されています。このコンポーネントのタイプは、ns::lbvserver（組み込みタイプ）です。ここで「ns」は、import-stylebooks セクションで指定された名前空間の netscaler.nitro.config とバージョン 10.5 を示すプレフィックス、「lbvserver」は、この名前空間の NITRO リソースです。

このセクションのプロパティには、「lbvserver」リソースの 4 つの必須属性と 1 つのオプション属性（lbmethod）が含まれています。そのため、これらの属性の値を指定できます。この例では、servicetype と port には静的な値が指定されていますが、name、ipv46、および lbmethod の各プロパティは、入力パラメーターから値を取得します。parameters セクションで定義されているパラメータ名は、$parameters を使って参照します。\ <name\ > 記法。たとえば、$parameters.ip のように指定します。

> 注
>
> NITRO リソースの種類の属性名（コンポーネントのプロパティ）には、小文字を使用する必要があります。そうしないと、StyleBook のインポートに失敗します。

ヘルパーコンポーネント

February 6, 2024

StyleBook のコンポーネントセクションの主な用途は、Nitro 組み込みタイプ、または実際の構成オブジェクトを作成する他の StyleBook を使って、構成オブジェクトを生成することです。ヘルパーコンポーネントは、それ自身では構成オブジェクトを構築しません。ヘルパーコンポーネントは、パラメーターオブジェクト、他のコンポーネントのプロパティ、または他のコンポーネントの出力などを入力として、それらを他の形式に変換します。これが後に他のコンポーネントで使用されて、実際の構成オブジェクトが生成されます。ヘルパーコンポーネントには 2 種類あり、オブジェクトタイプとコンポーネントセクションを含まない他の StyleBook です。

次の例は、Citrix ADC インスタンスでモニター（lb-mon-comp）を使用して負荷分散サーバーを作成するために使用される StyleBook のスニペットを示しています。


```
parameters:
  -
    name: appname
    type: string
  -
    name: ips
    type: ipaddress[]
  -
    name: vip
    type: ipaddress

components:
  -
    name: help-comp
    type: cmtypes::server-ip-port-params
    repeat:
      repeat-list: $parameters.ips
      repeat-item: server-ip
    properties:
      ip: $server-ip
      port: 80
 -
    name: lb-mon-comp
    type: stlb::lb-mon
    properties:
      lb-appname: $parameters.appname
      lb-virtual-ip: $parameters.vip
      lb-virtual-port: 80
      lb-service-type: HTTP
      svc-service-type: HTTP
      svc-servers: $components.help-comp.properties
<!--NeedCopy-->
```

パラメーターセクションにはアプリケーションの名前と負荷分散サーバーの IP アドレスを入力することができます。lb-mon-comp コンポーネントセクションでは、lb-mon StyleBook の svc-servers パラメーターには、それぞれの項目が ip と port の 2 つのサブパラメーターを持つオブジェクトの一覧が予期されます。

ただし、この StyleBook のパラメーターセクションは、$parameters.ips を使ってサーバー IP のみを受け取ります。この StyleBook では、すべてのサーバーがポート 80 で実行されると想定されています。lb-mon StyleBook を使って負荷分散構成を作成するには、$parameters.ips をオブジェクトの一覧に変換する必要があります。これは上記の例ではヘルパーコンポーネント、help-comp を使って実現されます。help-comp コンポーネントのタイプは server-ip-port-params StyleBook です。この StyleBook はコンポーネントを持ちません。結果として、構成オブジェクトを作成しません。help-comp は $parameters.ips 上にリピート一覧を作成し、$parameters.ips の各項目に対して ip と port（80 に静的に設定）からなるオブジェクトを構築します。そうして help-comp は IP アドレスの一覧を、後で lb-mon-comp で svc-servers プロパティを割り当てるために使用できるオブジェクトの一覧に変換します。help-comp の結果は、lb-mon-comp の svc-servers プロパティに割り当てられます。

オプションのプロパティ

February 6, 2024

コンポーネントのプロパティは、式からその値を取得する場合があります。式はパラメーター参照などの単純式の場合もあれば、より複雑な式の場合もあります。このプロパティ値の設定は、コンポーネントではオプションです。式から実際の値が返される場合にのみプロパティの値を設定し、値が返されない場合はこのプロパティを設定しなくてもかまいません。

たとえば、設定するプロパティの 1 つが、型を ns::lbvserver とするコンポーネントの lbmethod（負荷分散アルゴリズム）であるとします。プロパティ lbmethod の値は、次に示すようにユーザーが指定したパラメーター値から取得されます。

```
components
  -
      name: lbvserver_comp
      type: ns::lbvserver
      properties:
        name: $parameters.lb-appname + "-lb"
        servicetype: $parameters.lb-service-type
        ipv46: $parameters.lb-virtual-ip
        port: 80
        lbmethod: $parameters.lb-advanced.algorithm
<!--NeedCopy-->
```

ここで、パラメータ **lb-advanced.algorithm** がオプションのパラメータであることを考えてみましょう。また、オプションであるためにユーザーがこのパラメータの値を指定しない場合、式 **$parameters.lb-advanced.algorithm** は空白の値に評価されます。そのため、lbmethod プロパティに無効な値が渡されます。このような状況を回避するには、次のようにプロパティ名に「?」のサフィックスを付けて、プロパティにオプションであることを示す注釈を付けることができます。

```
components
   -
     name: lbvserver_comp
     type: ns::lbvserver
     properties:
       name: $parameters.lb-appname + "-lb"
       servicetype: $parameters.lb-service-type
       ipv46: $parameters.lb-virtual-ip
       port: 80
       lbmethod?: $parameters.lb-advanced.algorithm
<!--NeedCopy-->
```

「?」を使用すると、右側の式がなしに評価された場合、このプロパティは省略されます。この例では、次のように定義されたコンポーネントと同等になります。

```
components
  -
```



```
    name: lbvserver_comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb-appname + "-lb"
      servicetype: $parameters.lb-service-type
      ipv46: $parameters.lb-virtual-ip
      port: 80
<!--NeedCopy-->
```

lbmethod はオプションであるため、それを省略しても有効なコンポーネントになります。lbmethod は、「ns::lbvserver」型で定義されている場合、そのデフォルト値を取得する場合があります。

プロパティ-デフォルトソース構成

February 6, 2024

properties-default-sources 構造は parameters-default-sources 構造に似ています。parameters-default-sources 構造では StyleBook で（他の StyleBook から）既存のパラメーターを再利用できますが、properties-default-sources 構造ではユーザーが既存のソースに基づいてコンポーネントのプロパティを指定できます。

コンポーネントのプロパティは、StyleBook のさまざまなセクションに分散される可能性があります。たとえば、オブジェクトのパラメーター、オブジェクトを返す置換、ほかのコンポーネントのプロパティ、またはほかのコンポーネントの出力からプロパティが取得されることがあります。このような場合は、コンポーネントの定義で、StyleBook のほかのセクションで発生するプロパティを再定義する必要があります。明らかに、これは冗長でエラーにつながる可能性があります。この問題に対応するために、properties-default-sources 構造を使用できます。properties-default-sources 構造は、各項目がコンポーネントのプロパティのソースを識別する一覧です。

たとえば、lbvserver 構成を作成するコンポーネントを考えてみましょう。このコンポーネントは、以下のように lbvserver のプロパティを定義する必要があります。

```
parameters:
  -
    name: lb
    type: ns::lbvserver
components:
  -
    name: lb-comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb.name
      ipv46: $parameters.lb.ipv46
      port: $parameters.lb.port
      servicetype: $parameters.lb.servicetype
      lbmethod: $parameters.lb.lbmethod
<!--NeedCopy-->
```


上記の例では、components セクションで定義されているすべてのプロパティの値は $parameters.lb オブジェクトから取得されていることに注目してください。これらのプロパティは 1 つのソースから取得されますが、StyleBook で再定義されています。さらに、lbvserver の構成に関連する $parameters.lb オブジェクトに新しいサブパラメーターが追加された場合は、新しいサブパラメーターに対応する新しいプロパティを追加するために lb-comp コンポーネントを更新する必要があります。

プロパティの再定義を避け、コンポーネントのすべての関連プロパティを properties セクションで明示的にリストすることなく取得するために、properties-default-sources 構造を使用できます。上の例は、次のように記述することもできます。

```
parameters:
  -
    name: lb
    type: ns::lbvserver
components:
  -
    name: lb-comp
    type: ns::lbvserver
    properties-default-sources:
      - $parameters.lb
<!--NeedCopy-->
```

上の例では、properties-default-sources 構造を使用することでコンポーネント定義のサイズが小さくなり、そのためにコンポーネントを簡潔に定義できています。さらに、コンポーネントのプロパティのソースが変更されるたびに、変更内容が自動的に反映されます。たとえば、「persistesetype」という名前の新しいプロパティが $parameters.lb オブジェクトに追加された場合、persistencetype は lbvserver のプロパティであるため、デフォルトで lb-comp の構成に追加されます。このように、properties-default-sources 構造は、コンポーネントのプロパティのソースに対して行われる変更を気にすることなくコンポーネントを定義できる動的なインターフェイスを提供します。

コンポーネントのプロパティの計算

このセクションでは、コンポーネントで properties-default-sources 構造を使用した場合にプロパティがどのように取得されるかについて説明します。はじめに、StyleBooks コンパイラがコンポーネントの種類（上の例では lbvserver）に基づいてコンポーネントのプロパティの一覧を識別します。次に、コンパイラはこれらのプロパティを複数のソースから（コンポーネントの properties-default-sources セクションに）定義されている順に取得します。プロパティが複数のソースに存在する場合は、最後のソースに出現するプロパティがほかのプロパティより優先されます。最後に、properties-default-sources 構造を使用して取得されたプロパティは、コンポーネントの properties セクションで上書きすることができます。component セクションの定義は、少なくとも properties-default-sources セクションまたは properties セクションを持つ必要があることに気付くことが重要です。両方のセクションを持つこともできます。

ネストされたコンポーネント

February 6, 2024

コンポーネントを別のコンポーネント内にネストした場合、ネストされたコンポーネントは、親コンポーネントによって作成される構成オブジェクトまたはコンテキストを参照してその構成オブジェクトを作成できます。ネストされたコンポーネントは、親コンポーネントでオブジェクトが作成されるたびに、1 つまたは複数のオブジェクトを作成できます。コンポーネントを別のコンポーネント内にネストしても、作成される構成オブジェクト間に関係は生じません。ネストを使用すると、親コンポーネントの既存のコンテキスト内で構成オブジェクトを作成するコンポーネントのタスクが容易になります。

例:

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
   properties:
      name: $parameters.name + "-lb"
      servicetype: HTTP
      ipv46: $parameters.ip
      port: 80
      lbmethod: $parameters.lb-alg
      components:
        -
         name: my-svcg-comp
         type: ns::servicegroup
         properties:
            name: $parameters.name + "-svcgrp"
            servicetype: HTTP
         components:
            -
              name: lbvserver-svg-binding-comp
              type: ns::lbvserver_servicegroup_binding
              properties:
                name: $parent.parent.properties.name
                servicegroupname: $parent.properties.name
                  -
                    name: members-svcg-comp
                    type: ns::servicegroup_servicegroupmember_binding
                    repeat:
                      repeat-list: $parameters.svc-servers
                      repeat-item: srv
                    properties:
                      ip: $srv
                      port: str($parameters.svc-port)
                      servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

この例では、複数レベルのネストが使用されています。コンポーネント my-lbvserver-comp が、my-svcg-comp

という名前の子コンポーネントを持っています。また、my-svcg-comp コンポーネントは、その内部に 2 つの子コンポーネントを持っています。my-svcg-comp コンポーネントは、組み込みの NITRO リソースタイプ「サービスグループ」の属性に値を指定することにより、Citrix ADC インスタンス上にサービスグループ構成オブジェクトを作成するために使用されます。my-svcg コンポーネントの最初の子コンポーネントである lbvserver-svg-binding-comp は、親コンポーネントが作成したサービスグループと、さらにその親のコンポーネントが作成した負荷分散仮想サーバー（lbvserver）をバインドするために使用されます。$parent 表記（親参照とも呼ばれる）は、親コンポーネントのエンティティを参照するために使用されます。2 番目の子コンポーネントである members-svcg-comp は、親コンポーネントが作成したサービスグループにサービス一覧をバインドするために使用されます。このバインドを実行するには、StyleBook の repeat 構造を使用して、svc-servers パラメーターに指定されたサービス一覧を反復処理します。repeat 構造については、「repeat 構造」を参照してください。

同じ構成オブジェクトを、コンポーネントのネストを使用せずに作成することもできます。追加の情報および例については、「基本的な負荷分散の構成を作成するための StyleBook」を参照してください。

条件構成

February 6, 2024

condition 構造を使用すると、コンポーネントを条件付きにすることができます。condition 構造の値は、true または false に評価されるブール式です。条件が true になる場合、このコンポーネントを使用して構成オブジェクトが作成されます。条件が false になる場合、このコンポーネントはスキップされ、構成オブジェクトの作成には使用されません。多くの場合、ブール式はパラメーター値に基づきます。

例:

```
components:
      -
        name: servicegroup-comp
        type: ns::servicegroup
        condition: $parameters.svc-server-ips
        properties:
              name: $parameters.name + "-svcgrp"
              servicetype: HTTP
<!--NeedCopy-->
```

この例では、ユーザーがオプションのパラメーター svc-server-ips に値を指定すると、StyleBook エンジンによってコンポーネント servicegroup-comp が処理されます。条件が false になる場合、つまり、ユーザーがこのパラメーターに値を指定しなかったためにこのパラメーターに null 値が割り当てられ、false に評価された場合は、StyleBook エンジンでこのコンポーネントの存在が無視され、サービスグループは作成されません。

ブール式は、StyleBook でサポートされる任意の有効な式に基づいて設定できます（たとえば、別のコンポーネントが存在するかどうかや、パラメーターに特定の値が指定されているかどうかなど）。

次の例では、条件が true に評価された場合に、NITRO タイプ ns::systemfile の構成オブジェクトを作成します。

例:

```
    components
         -
           name: pem_key_files
           type: ns::systemfile
           condition: "$components.der-certificate-files-comp or
    $components.pem-certificate-files-comp"
           properties:
                 filecontent: $certificate.keyfile.contents
                 fileencoding: "BASE64"
                 filelocation: "/nsconfig/ssl"
                 filename: $certificate.keyfile.filename
<!--NeedCopy-->
```

この例では、条件は複雑な「OR」式です。StyleBook 内の他の 2 つのコンポーネントが処理されている（スキップされていない）場合にのみ、この構成オブジェクトを StyleBook で作成し、コンポーネント間の依存関係を作成します。

repeat 構造

February 6, 2024

コンポーネントの **repeat** 構造を使用して、同じタイプの複数の構成オブジェクトを作成できます。

次の例では、**members-svcg-comp** コンポーネントは、親コンポーネントが作成したサービスグループにサービス一覧をバインドするために使用されます。各サーバーをサービスグループにバインドする構成オブジェクトを作成するには、**repeat** 構造を使用して、**svc-servers** パラメーターに指定されたサービス一覧を反復処理します。繰り返し処理中に、コンポーネントはサービスグループ内の各サービス **(**繰り返し項目構造では ****srv** と呼ばれる) に **servicegroup_servicegroupmember_binding** タイプの NITRO オブジェクトを作成し、各 NITRO オブジェクトの IP 属性を対応するサービスの IP アドレスに設定します。**

例:

```
components:
  -
      name: my-lbvserver-comp
      type: ns::lbvserver
      properties:
           name: $parameters.name + "-lb"
           servicetype: HTTP
           ipv46: $parameters.ip
           port: 80
           lbmethod: $parameters.lb-alg
          components:
                -
                   name: my-svcg-comp
                   type: ns::servicegroup
```



```
15                      properties:
16                           name: $parameters.name + "-svcgrp"
17                           servicetype: HTTP
18                      components:
19                            -
20                            name: lbvserver-svg-binding-comp
21                            type: ns::lbvserver\servicegroup\binding
22                            properties:
23                                  name: $parent.parent.properties.name
24                                  servicegroupname: $parent.properties.
      name
25                            -
26                            name: members-svcg-comp
27                            type: ns::servicegroup\servicegroupmember\
      binding
28                            repeat:
29                              repeat-list: $parameters.svc-servers
30                              repeat-item: srv
31                            properties:
32                                   ip: $srv
33                                   port: $parameters.svc-port
34                                   servicegroupname: $parent.properties.
      name
35  <!--NeedCopy-->
```

リピートはそれ自体がオブジェクトであり、** リピートリストとリピートアイテムはリピートオブジェクトの属性です ** 。

- repeat-list は、コンポーネントが反復する一覧を識別する必須の属性です。
- repeat-item はオプションで、反復処理中の現在の項目にフレンドリ名を付けるために使用されます。

指定しない場合は、**$repeat-item** という式を使用して現在のアイテム にアクセスできます。上の例の最後のコンポーネントは、次のように記述することもできます:

```
1             -
2             name: members-svcg-comp
3             type: ns::servicegroup_servicegroupmember_binding
4             repeat:
5               repeat-list: $parameters.svc-servers
6             properties:
7                    ip: $repeat-item
8                    port: $parameters.svc-port
9                    servicegroupname: $parent.properties.name
10  <!--NeedCopy-->
```

リスト上で現在の項目を白く反復して参照できるだけでなく、**repeat-index** を使用してリスト内の項目の現在のインデックスを参照することもできます。次の例では、**repeat-index** を使用して、現在のインデックスに基づいてポート番号を計算します。

```
1               name: services
2               type: ns::service
3               repeat:
```



```
                repeat-list: $parameters.app-services
                repeat-item: srv
            properties:
                ip: $parameters.app-ip
                port: $parameters.base-port + repeat-index
                servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

repeat-item 構文と同様 に、イテレーションの現在のインデックスを参照する別の変数名を割り当てることができます。前の例は次の例と同等です:

```
      -
            name: services
            type: ns::service
            repeat:
                repeat-list: $parameters.app-services
                repeat-item: srv
                repeat-index: idx
            properties:
                ip: $parameters.app-ip
                port: $parameters.base-port + $idx
                servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

繰り返し条件構成

February 6, 2024

repeat-condition 構造は repeat 構造の反復処理ごとに評価され、その結果によって、構成オブジェクトをその反復処理で作成するか次の反復処理に進むかが決定されます。次の例は、repeat-condition 構造の使用方法を示しています。

例:

```
components
   -
      name: der-key-files-comp
      type: ns::systemfile
      repeat:
      repeat-list: $parameters.certificates
      repeat-item: certificate
        repeat-condition: $certificate.ssl-inform == DER
        properties:
         filecontent: base64($certificate.keyfile.contents)
         fileencoding: BASE64
         filelocation: /nsconfig/ssl
         filename: $certificate.keyfile.file
<!--NeedCopy-->
```


この例では、der-key-files-comp コンポーネントはユーザーが指定したすべての証明書を反復処理しますが、DER エンコーディングの証明書に対応する構成オブジェクトのみを作成します。反復処理ごとに repeat-condition 式が評価され、証明書のエンコーディングのタイプが DER かどうかがテストされます。タイプが DER でない場合、現在の反復処理では構成オブジェクトは作成されず、反復処理は一覧の次の証明書に進みます。

ネストされた繰り返し

February 6, 2024

repeat 構造をネストにして使用することで、コンポーネントの定義に応じて各コンポーネントに複数の repeat 構造を含めることができます。2 レベルのネストになった repeat 構造を考えます。外側のリスト（最初の repeat-list）の要素ごとに、内側のリスト（2 番目の repeat-list）の要素すべてに対して repeat リストを作成できます。StyleBook コンパイラでは、ネストになった repeat は最大で 3 つまでサポートされます。各 repeat レベルには、repeat-item 属性および repeat-index 属性を関連付けます。repeat-item 属性と repeat-index 属性はともにオプションです。また、repeat ごとに repeat-condition を指定することもできます。

例:

```
parameters:
  -
      name: vips
      type: ipaddress[]
  -
      name: vip-ports
      type: tcp-port[]
components:
  -
      name: lbvservers-comp
      type: ns::lbvserver
      repeat:
         repeat-list: $parameters.vips
         repeat-item: ip
         repeat:
              repeat-list: $parameters.vip-ports
              repeat-item: port
      properties:
         name: str("lb-") + str($ip) + '-' + str($port)
         servicetype: HTTP
         ipv46: $ip
         port: $port
<!--NeedCopy-->
```

上記の例では、$parameters.vips の項目ごとに、$parameters.vip-ports の項目すべてに対して反復処理を行います。つまり、$parameters.vips で指定した ipaddress ごとに、$parameters.vip-ports で指定したすべてのポートに対して lbvserver 構成オブジェクトを作成します。properties セクションでは、IP アドレスとポートの組

み合わせにプレフィックス「lb」を付けたオブジェクト名を定義しています。このため、反復処理のたびに、$ip と $port の結合により一意の IP アドレスとポート番号の組み合わせが定義されます。

repeat-item 属性を指定していない場合、コンパイラではこの属性のデフォルト値が生成されます。repeat-item のデフォルト値は、repeat レベルごとにそれぞれ $repeat-item、$repeat-item-1、$repeat-item-2 となります。同様に、repeat-index 属性を指定していない場合、コンパイラではこの属性のデフォルト値が生成されます。repeat-index のデフォルト値は、repeat レベルごとにそれぞれ $repeat-index、$repeat-index-1、$repeat-index-2 となります。

以下の例では、ネストになった repeat オブジェクトで repeat-item 属性および repeat-index 属性を指定していない場合の命名規則を示します。

例:

```
components:
-
      name: lbvservers-comp
      type: ns::lbvserver
      repeat:
          repeat-list: $parameters.vips
          repeat:
             repeat-list: $parameters.vip-ports
      properties:
         name: str("lb-") + str($repeat-item) + '-' + str($repeat-item
    -1)
          servicetype: HTTP
          ipv46: $repeat-item
          port: $repeat-item-1
<!--NeedCopy-->
```

結果

February 6, 2024

Outputs セクションでは、StyleBook によってすべての構成オブジェクトが正常に作成された後にユーザーに公開する情報を指定します。StyleBook の Outputs セクションは、必要に応じて記述します。StyleBook で必ずしも出力を返す必要はありません。ただし、内部コンポーネントを出力として返すと、この StyleBook をインポートするすべての StyleBook の柔軟性が向上します。このことは、複合 StyleBook の作成時にわかります。

次の表は、Outputs セクションで使用する属性を示しています。

属性	説明	固定
name	公開する構成オブジェクトに対応する出力の名前。	はい

属性	説明	固定
説明	出力について説明するテキスト文字列。	いいえ
value	この属性では、StyleBook によって返される値の抽出方法を指定します。	はい

例:

```
outputs:
 -
   name: lbvserver
   description: LBVServer component
   value: $components.my-lbvserver-comp
 -
   name: svc-grp
     description: ServiceGroup name
     value: $components.my-svcg.properties.name
<!--NeedCopy-->
```

この例では、StyleBook で作成される **lbvserver** コンポーネントとサービスグループの名前（**name**）を公開します。**lbvserver** という出力の値はコンポーネント **my-lbvserver-comp** です。同様に、**svc-grp** という出力の値は、コンポーネント **my-svcg** によって作成されたサービスグループの名前です。

パラメータ参照

February 6, 2024

コンポーネント構成では、パラメーターセクションで定義されているパラメーターを`$parameters.<parametername>`表記法を使用して参照します。`<parametername>`それ自体にパラメータが含まれている場合 (type が object の場合)、表記法`$parameters.<parametername>.<sub-parametername>`などを使う必要があります。

例:

```
parameters:
  -
    name: name
    label: Name
    type: string
    required: true
     -
      name: vip
      label: Virtual IP and Port
      type: object
```



```
      required: true
      parameters:
        -
          name: ip
          label: Virtual IP
          description: The Virtual IP Address
          type: ipaddress
          required: true
            -
              name: port
              label: The Virtual Port
              description: The TCP port for the Virtual IP
              type: tcp-port
              default: 80
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
       name: $parameters.name
       servicetype: HTTP
       ipv46: $parameters.vip.ip
       port: $parameters.vip.port
<!--NeedCopy-->
```

親参照

February 6, 2024

ネストされたコンポーネントを使用している場合は、$parent 表記を使用して親コンポーネントを参照できます。親コンポーネントで repeat 構造を使用して複数の構成オブジェクトを作成し、反復処理ごとに子コンポーネントでほかの構成オブジェクトを作成する場合、$parent 表記は常に親コンポーネントの現在の反復処理を参照します。たとえば、$parent.properties.name は、親が現在の反復処理で作成する構成オブジェクトの name プロパティを参照します。

例:

```
components:
 -
   name: my-lbvserver-comp
   type: ns::lbvserver
   properties:
     name: $parameters.name + "-lb"
     servicetype: HTTP
     ipv46: $parameters.ip
     port: 80
     lbmethod: $parameters.lb-alg
     components:
```



```
        -
          name: my-svcg-comp
          type: ns::servicegroup
          properties:
            name: $parameters.name + "-svcgrp"
            servicetype: HTTP
            components:
             -
               name: lbvserver-svg-binding-comp
               type: ns::lbvserver_servicegroup_binding
               properties:
                  name: $parent.parent.properties.name
                  servicegroupname: $parent.properties.name
                    -
                      name: members-svcg-comp
                      type: ns::servicegroup_servicegroupmember_binding
                      repeat: $parameters.svc-servers
                      repeat-item: srv
                      properties:
                        ip: $srv
                        port: str($parameters.svc-port)
                        servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

また、親の親のプロパティにアクセスしてコンポーネントの階層を上方向に移動し、最上位レベルのコンポーネントまで遡ることもできます。たとえば、コンポーネント **lbvserver-svg-binding-comp** のプロパティ名は、**$parent.parent** 表記を使用して、その親の親である my-lbvserver-comp コンポーネントのプロパティ名から値を取得します。

コンポーネントのリファレンス

February 6, 2024

components コンストラクトでは、**$components** を使って **StyleBook** の最上位コンポーネントを参照します。 \ <componentname\ > 記法。トップレベルコンポーネント内にネストされたコンポーネントがある場合、**$components** という表記法が使用されます。**\.components <componentname\ >**。\ <component-name\ > でそれらを参照するなどです。

例:

```
components:
 -
    name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
           name: $parameters.name + "-lb"
           servicetype: HTTP
           ipv46: $parameters.ip
```



```
            port: 80
            lbmethod: $parameters.lb-alg
  -
     name: my-svcg-comp
     type: ns::servicegroup
     properties:
          name: $parameters.name + "-svcgrp"
          servicetype: HTTP
  -
     name: members-svcg-comp
     type: ns::servicegroup_servicegroupmember_binding
     repeat: $parameters.svc-servers
     repeat-item: srv
     properties:
        ip: $srv
          port: str($parameters.svc-port)
          servicegroupname: $components.my-svcg-comp.properties.name
  -
     name: lbvserver-svg-binding-comp
     type: ns::lbvserver_servicegroup_binding
     properties:
            name: $components.my-lbvserver-comp.properties.name
            servicegroupname: $components.my-svcg-comp.properties.name
<!--NeedCopy-->
```

この例では、**my-svcg-comp** コンポーネントと **my-lbvserver-comp** コンポーネントを作成してから、最後のコンポーネントである **lbvserver-svg-binding-comp** を作成する必要があります。この最後のコンポーネントには、これらのコンポーネントへの参照が含まれるからです。これらの参照は、**$components** で示されるコンポーネント参照を使用して提供されます。\ <componentname\ >。

置換参照

February 6, 2024

コンポーネントセクションまたは操作セクションでは、代替セクションで定義されている代替を**$substitutions.<substitution-name>**表記法を使用して参照します。たとえば、**$substitutions.http-port** のように指定します。

代替がマップの場合、マップ内のエレメントを**$substitutions.<substitutions-name>[<map-key>]**と呼ぶことができます。たとえば、**$substitutions.protocol-map[$parameters.port]**のようになります。

変数参照

February 6, 2024

コンポーネントの repeat 構造と repeat-item 構造を使用して複数の構成オブジェクトを作成するときに、repeat-item 構造に変数名を割り当てることができます。その後、この変数は、そのコンポーネントのプロパティ内または子コンポーネント内の表記法**$\<varname\>**を使用して参照できます。コンポーネントで repeat-item 構造を省略して repeat 構造を使用する場合は、$repeat-item というデフォルトの変数を使用して反復処理項目にアクセスできます。

例:

```
components:
  -
    name: server-members-comp
    type: ns::server
    condition: $parameters.svc-server-domain-names
    repeat: $parameters.svc-server-domain-names
    repeat-item: server-name
    properties:
      name: $server-name + "-server"
      domain: $server-name
    components:
      -
         name: service-members-comp
         type: ns::service
         properties:
           name: $server-name + "-service"
           servername: $parent.properties.name
           servicetype: $parameters.svc-service-type
           port: $parameters.svc-server-port
<!--NeedCopy-->
```

上の例では、repeat-item 構造に変数名 server-name が割り当てられています。この変数名は、同じコンポーネントのプロパティと子コンポーネント**$\<varname\>**のプロパティで参照されます。

オペレーション

February 6, 2024

操作は StyleBook のオプションセクションです。このセクションでは、すべてまたは一部のトラフィックトランザクションに関する AppFlow レコードを収集するように CitrixApplication Delivery Management（ADM）分析を構成できます。StyleBook を使用して NetScaler ADC インスタンス上に作成された仮想サーバーは、これらのトラフィックトランザクションを処理します。このセクションでは、仮想サーバーで特定のトラフィック条件が満たされたときにアラームをトリガーするように NetScaler ADM を構成することもできます。

StyleBooks を使用して NetScaler ADM を構成して、次のようにリストされているさまざまな NetScaler ADM Insights からトラフィック統計を収集できます。

- Web Insight
- Security Insight
- HDX Insight
- Citrix Gateway Insight

サポートされる仮想サーバは、ロードバランシング、コンテンツスイッチング、および VPN 仮想サーバです。

Web Insight と Security Insight の両方、またはどちらか一方を有効化して、負荷分散またはコンテンツスイッチング仮想サーバーの分析に使用します。ただし、VPN 仮想サーバーの場合は、HDX Insight と NetScaler Gateway Insight の両方を有効にする必要があります。

StyleBooks を介して Citrix ADC インスタンスで有効になっている Citrix ADM Insight はすべて、IPFIX プロトコル（AppFlow）を使用してインスタンスから Citrix ADC にデータを送信します。

また、Web Insight を有効にすると、負荷分散およびコンテンツスイッチング仮想サーバーで「クライアント側測定」が有効になります。

例 **1**:

次の例は、VPN 仮想サーバー上で HDX Insight と Citrix Gateway Insight の両方を有効にするための操作セクションを StyleBook に記述する方法を示しています。

```
name: simple-vpn-ops
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
description: Test StyleBook to enable hdxinsight and gatewayinsight on
   a VPN vserver
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
components:
    -
        name: vpnvserver-comp
        type: ns::vpnvserver
        properties:
            name: str("vpn-") + str($current-target.ip)
            servicetype: SSL
            ipv46: 1.1.21.37
            port: 443
operations:
    analytics:
        -
            name: comp-ops
            properties:
                target: $components.vpnvserver-comp
```



```
                  filter: "true"
                  insights:
                    -
                   type: hdxinsight**
                    -
                      type: gatewayinsight
outputs:
  -
    name: myvpns
    value: $components.vpnvserver-comp
<!--NeedCopy-->
```

例 **2**:

次の例は、StyleBook に操作セクションを記述して、負荷分散仮想サーバー上で Web Insight と SurityInsight の両方を有効にする方法を示しています。

```
name: simple-lb-ops
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
description: Test StyleBook to enable webinsight and securityinsight on
    LB vserver
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
components:
    -
        name: lbvserver-comp
        type: ns::lbvserver
        properties:
            name: str("lb-") + str($current-target.ip)
            servicetype: HTTP
            ipv46: 1.1.21.37
            port: 80
operations:
    analytics:
        -
            name: comp-ops
            properties:
                target: $components.lbvserver-comp
                filter: "true"
                 insights:
                 -
                  type: webinsight
                   -
                  type: securityinsight
outputs:
  -
    name: mylbs
    value: $components.lbvserver-comp
```



```
<!--NeedCopy-->
```

分析

February 6, 2024

Operations セクションの analytics サブセクションには、Components セクションと似たような構造があります。分析セクションの各要素は、StyleBook によって作成された 1 つ以上の仮想サーバーの NetScaler ADM Analytics 機能を構成するために使用されます。

analytics セクションの要素には次の属性があります。

属性	説明	固定
name	分析要素の名前。	はい
説明	この要素の内容を説明するテキスト文字列。	いいえ
condition	ブール式。この条件が false に評価された場合、分析要素全体がスキップされます。	いいえ
リピート	リストを反復します。	いいえ
repeat-condition	ブール式。式が false に評価されると、現在の反復がスキップされます。	いいえ
repeat-item	現在の反復の項目の名前。	いいえ
repeat-index	現在の反復の指数値の名前。	いいえ
properties	分析のプロパティの一覧。	はい
target	一覧のいずれかのプロパティ。ターゲット表現は、分析が収集される NetScaler ADC で構成された仮想サーバーの名前です。	はい
filter	一覧のいずれかのプロパティ。この属性の値は、分析を収集する仮想サーバー上の要求をフィルタリングするために使用される NetScaler ADC の高度なポリシー表現です。デフォルトでは、分析データは仮想サーバーを通過するすべてのトラフィックで収集されます。	いいえ

例:

```
operations:

  analytics:

    -

    name: lbvserver-ops-comp

    properties:

    target: $components-basic-lb-comp.outputs.lbvserver-name

    filter: HTTP.REQ.URL.CONTAINS("catalog")
<!--NeedCopy-->
```

分析セクションの各属性を使用して、NetScaler ADM Analytics 機能に、ターゲットプロパティで識別される仮想サーバー上のアプリフローレコードを収集するように NetScaler ADC インスタンスを構成するように指示します。

アラーム

February 6, 2024

Operations セクションの alarms サブセクションは、analytics サブセクションと同様の構造と同じ属性を持ちます。唯一異なるのは properties 属性です。(properties 属性以外の) すべての属性の一覧については、「analytics」を参照してください。

alarms サブセクションでは次のプロパティを使用できます。

属性	説明	固定
target	アラームが構成されている NetScaler ADC で構成された仮想サーバーの名前に評価される式。	はい
email-profile	NetScaler ADM Analytics 機能で定義され、アラームがトリガーされたときに通知する電子メールアドレスのリストを含む電子メールプロファイルの名前。	いいえ (email-profile または sms-profile のどちらかを定義する必要があります)

属性	説明	固定
sms-profile	NetScaler ADM Analytics 機能で定義され、アラームがトリガーされたときに通知する電話番号のリストを含む SMS プロファイルの名前。	いいえ（email-profile または sms-profile のどちらかを定義する必要があります）
rules	target プロパティで定義した仮想サーバーに対するアラームをトリガーする条件を定義する規則の一覧。	はい
metric	rules の属性。NetScaler ADC 仮想サーバーに関連して追跡したいメトリックの名前。	はい
operator	rules の属性。測定基準と値の比較に使用する演算子。有効な演算子は「greaterthan」および「lessthan」です。	はい
value	rules の属性。演算子を使用して測定基準と比較するしきい値。測定基準値がこのしきい値を超えると、関連するアラームがトリガーされます。	はい
period-unit	rules の属性。アラームの規則条件が満たされている場合にユーザーに通知する頻度。day、hour、weekly の値を使用できます。つまり、規則条件が満たされている場合、アラームは period-unit に 1 回の頻度で送信されます（1 日に 1 回など）。	はい

次の表は、NetScaler ADC 仮想サーバーに関して追跡されるメトリックのリストを示しています。

カウンター | 説明 | 詳細な説明 |NetScaler ADM 計算
|–|–|–|–|
|VPN 仮想サーバーの場合：|
total_requests|VPN セッションの合計起動数 | ユーザーが指定した期間内に、この VPN 仮想サーバーで起動されたアクティブなセッションの合計数。| 新しいセッションの起動ごとに増分される、単調増加カウンター |
app_count	VPN アプリケーションの起動数	ユーザーが指定した期間内に、この VPN 仮想サーバーで起動された一意の VPN アプリケーションの合計数。	新しいアプリケーションの起動ごとの単調増加カウンター
app_launch_duration	VPN アプリケーションの起動時間	アプリケーションの起動にかかった平均時間（ミリ秒単位）	この VPN 仮想サーバーで起動された、すべての VPN アプリケーションの起動時間から算出された平均値
その他の仮想サーバー (CS、LB、Auth、GSLB)		

Total_requests| 要求数 | 要求数 | 前回のアプライアンスの再起動以降、または仮想サーバーの作成後のいずれか新しい方から、この仮想サーバーに対するクライアント要求の数。| カウンタは単調に増加し、この仮想サーバーへの新しいリクエストごとに増加します。||
合計バイト | バイト | 指定された時間間隔に仮想サーバーから Citrix ADM に転送された合計バイト数。| この仮想サーバーによって処理された合計バイト数を考慮して、カウンタが単調に増加している。||
アプリケーション _ 応答時間 | 応答時間 | 仮想サーバーの平均応答時間。| アプライアンスの最後の再起動以降 (または仮想サーバーの作成後)、いずれか最後の方から、この仮想サーバーが受信したすべての要求の応答時間の平均値。|

StyleBook の alarms セクションの例:

```
operations:
alarms:
 -
  name:lbvserver_alarm
  properties:
  target: $outputs.lbvserver
  email-profile: $parameters.emailprofile
  sms-profile: "NetScalerSMS"
     rules:
      -
        metric: "total_requests"
        operator: "greaterthan"
        value: 25
        period-unit: weekly
        -
          metric: "total_bytes"
          operator: "lessthan"
          value: 1024
          period-unit: day

<!--NeedCopy-->
```

式

February 6, 2024

StyleBook の最も強力な機能の 1 つに、式の使用があります。さまざまなシナリオで StyleBook の式を使用して動的な値を計算できます。次の例は、パラメーター値をリテラル文字列と連結する式を示しています。

例:

$parameters.appname + “-mon”

この式では、appname という名前のパラメーターを取得して文字列「-mon」と連結します。

次の種類の式がサポートされています。

算術式

- 加算 (+)
- 減算 (-)
- 乗算 (*)
- 除算 (/)
- モジュロ (%)

例:

- 2 つの数字の加算：$parameters.a + $parameters.b
- 2 つの数字の乗算：$parameters.a * 10
- ある数を別の数で除算した後の余りを見つける：

15% 10 件が 5 件見つかりました

文字列式

- 2 つの文字列を連結する (+)

例:

2 つの文字列を連結してください:str (「app-」) + $parameters.appname

一覧式

2 つのリスト（+）をマージします

例:

- 2 つの一覧を連結：$parameters.external-servers + $parameters.internal-servers
- $parameters.ports-1 が [80, 81] で、$parameters.port-2 が [81, 82] の場合、$parameters.ports-1 + $parameters.ports-2 の結果は [80, 81, 81, 82] になります。

関係式

- ==: 2 つのオペランドが等しいかどうかをテストして、等しい場合は true を、異なる場合は false を返します。
- !=: 2 つのオペランドが異なるかどうかをテストして、異なる場合は true を、等しい場合は false を返します。
  - ：最初のオペランドが 2 番目のオペランドより大きい場合は true を返し、それ以外の場合は false を返します。

> - =: 1 つ目のオペランドが 2 つ目のオペランド以上である場合は true を、それ以外の場合は false を返します。

- <: 1 つ目のオペランドが 2 つ目のオペランドよりも小さい場合は true を、それ以外の場合は false を返します。
- <=: 1 つ目のオペランドが 2 つ目のオペランド以下である場合は true を、それ以外の場合は false を返します。

例:

- 等価演算子の使用:$parameters.name = =「abcd」
- 非等値演算子の使用: $parameters.name != “default”
- 他の関係演算子の例
  - 10 > 9
  - 10 >= 10
  - 0 < 9
  - 10 <= 9
  - 10 == 10
  - 10 != 1

論理 **(**ブーリアン**)** 表現

- and: 論理積演算子。両方のオペランドが true の場合、結果は true となり、それ以外の場合は false となります。
- or: 論理和演算子。いずれかのオペランドが true の場合、結果は true となり、それ以外の場合は false となります。
- not: 単項演算子。オペランドが true の場合、結果は false となり、オペランドが false の場合、結果は true となります。
- in: 最初の引数が第 2 引数の部分文字列かどうかをテストします
- in: 項目がリストの一部であるかどうかをテストします

> 注
>
> 文字列が数値に変換でき、数値が文字列に変換できる場合は、キャスト式を入力できます。同様に、TCP ポートを数値に型変換でき、IP アドレスを文字列に型変換できます。

演算子の前後には区切り記号を使う必要があります。区切り記号は次のように使えます。

> - 演算子の前：スペース、タブ、カンマ、(、)、[、]
> - 演算子の後：スペース、タブ、(、[
> - 例：
> - abc + def
> - 100 % 10
> - 10 > 9

式の種類の検証

StyleBook エンジンはコンパイル時により強力な種類のチェックができるようになりました。つまり、StyleBook を書くときに使われる式は、構成パックの作成時ではなくて、StyleBook 自身のインポート時に検証されます。

パラメーター、置換、コンポーネント、コンポーネントのプロパティ、コンポーネントの出力、ユーザー定義変数 (repeat-item、repeat-index、代替関数への引数) などへの参照はすべて、その存在とタイプについて検証されます。

タイプチェックの例:

以下の例では、lbvserver の StyleBook のポートプロパティの予期される種類は tcp-port です。Citrix Application Delivery Management（ADM）の以前のリリースでは、StyleBook コンパイラが値を文字列として計算し、StyleBook がインポートされて実行されていました。今では、コンパイル時に種類の検証が行われます（インポート時）。コンパイラは文字列と tcp-port が互換性のない種類であることを発見し、StyleBook コンパイラはエラーを返し、StyleBook のインポートまたは移行に失敗します。

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: str("80")
      servicetype: HTTP

You should now declare this as a number for the compiler to
   successfully compile this StyleBook.

  port: 80
<!--NeedCopy-->
```

無効な式のフラグ付けの例:

以前のリリースでは、無効な式がプロパティ名に割り当てられている場合、コンパイラは無効な式を検出せず、StyleBook を NetScaler ADM にインポートすることができました。これで、この StyleBook が Citrix ADM に

インポートされると、コンパイラーはそのような無効な式を識別してフラグを立てます。その結果、StyleBook は Citrix ADM にインポートされません。

この例では、lb-sg-binding-comp component の名前のプロパティに割り当てられた式は次の通りです: $components.lbvserver-comp.properties.lbvservername。ただし、コンポーネント lbvserver-comp には lbvservername と呼ばれるプロパティはありません。以前の NetScaler ADM リリースでは、コンパイラはこの式を許可し、正常にインポートされていました。実際の失敗はこの StyleBook を用いて構成パックを作成するときに起こります。ただし、インポート中にこの種のエラーが特定され、StyleBook は NetScaler ADM にインポートされません。こういったエラーを手動で修正し、StyleBook をインポートする必要があります。

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.lbvservername
      servicegroupname: $components.sg-comp.properties.servicegroupname
<!--NeedCopy-->
```

インデックスの一覧

一覧のアイテムは直接インデックスすることでアクセスできます。

** 式 **	** 説明 **
$components.test-lbs[0]	test-lbs コンポーネントの最初のアイテムを参照します。
$components.test-lbs [0] .properties.p1	test-lbs コンポーネントの最初のアイテムのプロパティ p1 を参照します。
$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname	servicegroups コンポーネントの 2 番目のアイテムのプロパティ servicegroupname を参照しますが、これは lbcomps コンポー

ネントの最初のアイテムからの出力です。|
|

インプレイス補間

February 6, 2024

文字列の一部を、StyleBook 式で置き換えることができるようになりました。文字列式が StyleBook コンパイラで評価されるときに、StyleBook 式を使用した文字列の部分がその式の値で置き換えられます。文字列に StyleBook 式を含めるには、次のように記述します。

“…%{…}%…”

「%{」と「}%」で囲んだ文字が StyleBook 式となります。こうした式は、「インプレース補間」と呼ばれます。

例として、「lb-%{$parameters.appname}%-svc」という StyleBook 式のインプレース補間を用いた文字列式を考えます。文字列式の値は、補間式の値によって決まります。**$parameters.appname** に「app1」が割り当てられていることを考えてみましょう。次に、この文字列式は **lb-app1-svc** と評価されます。この機能を使用することで、値を文字列式に直接入力するのではなく、ユーザー定義値に応じて決めることができます。

インプレース補間の実用的な使用例としては、StyleBook のポリシー式のパラメーター化があります。HTTP URL に特定の語句（この例では「jpeg」）が含まれているかどうかをチェックするポリシー式を記述するシナリオを考えます。

この場合、記述するポリシー式は「HTTP.REQ.URL.CONTAINS(\“jpeg\”)」となります。

ここで、StyleBook に文字列パラメーター（この例では $parameters.url-object）を追加して、HTTP URL のオブジェクトをパラメーター化できます。ポリシー式は、このパラメーターに基づいて記述する必要があります。この目的を達成するには、文字列連結を使用します。式は次のようになります。

str(“HTTP.REQ.URL.CONTAINS(\”” + $parameters.url-object + “\”)”)

$parameter.url-object に「csv」が代入されている場合、上記の式の値は「HTTP.REQ.URL.CONTAINS(\“csv\”)」となります。しかし、こうした式は読みにくいものです。インプレース補間を使用することで、こうしたパラメーター化を読みやすくわかりやすいものにすることができます。

インプレース補間を使用した式は次のようになります。

str(“HTTP.REQ.URL.CONTAINS(%{quotewrap($parameters.url-object)}%)”)

上記の式では、インプレース補間を使用して $parameters.url-object の値の前後に内部引用を追加しています。この式の結果は先ほどのものと同じですが、より直感的で、実際の結果に近い形になっています。

補間式内で使用できる型

補間式の内側では、boolean、number、tcp-port、ipaddress、および string の各型の値が生成される式を使用できます。生成された値は、補間式が結果に置き換えられるときに自動で文字列へ変換されます。

文字列式には補間を含めないことも、1 個以上の補間を含めることもできます。順次補間で、文字列式の各部分を異なる StyleBook 式に置き換えることができます。たとえば、文字列 lb-%{$parameters.appname}%-%{$parameters.vip}% では、$parameters.appname が「app1」、$parameters.vip が「1.1.1.1」の場合、lb-app1-1.1.1.1 が返されます。

文字列式では、入れ子補間もサポートされています。つまり、補間式を別の補間式の内側に入れ子にして、ある式の値を別の式の入力にすることができます。

たとえば、「% {lb-% {$parameters.port + 1}%}%」という文字列を考えてみましょう。

$parameters.port が 80 の場合、内部文字列「**% {$parameters.port + 1}%**」は「lb-81」を返します。ここでは、この式は別の補間式の中に入れ子になっています。

以下の表に、さまざまな種類の補間を例と対応する結果とともに示します。例で使用しているパラメーターの値は次のとおりです。

- $parameters.appname: “lb1”
- $parameters.vip: “1.1.1.1”
- $parameters.n1: 1
- $parameters.n2: 3

単純な補間

式	結果
lb-%{$parameters.appname}%-def	lb-lb1-def

自動型変換

式	結果
lb-%{1}%	lb-1
lb-%{$parameters.vip}%	lb-1.1.1.1
lb-%{true}%	lb-True

式	結果

順次補間

式	結果
% {$parameters.appname} %-% {str ($parameters.appname)}%	lb1-lb1
lb-%{1}%-%{2}%	lb-1-2

入れ子補間

式	結果
% {abc-% {$parameters.n1 + 1}%}%	abc-2
str(“%{abc-%{$parameters.n1}%}%-%{$parameters.n2}%”)	bc-1-3

quotewrap を使用した補間

式	結果
str(“%{quotewrap(abcd)}%”)	“abcd
str(“%{quotewrap(https://)} %+HTTP.REQ.HOSTNAME+HTTP.REQ.URL")	“«code class=” language-plaintext highlighter-rouge” >https://” +HTTP.REQ.HOSTNAME+HTTP.REQ.URL</code>

補間式のエスケープ文字列

文字「% {」または「}%」が文字列の一部である場合、StyleBook コンパイラがこれらを補間タグとして評価しないように、エスケープ文字として”\”を指定する必要があります。

例:

str(“%{\%{ + str($parameters.vip) + }\%}%”) returns “%{1.1.1.1}%” if $parameters.vip is 1.1.1.1

以下の表に、その他の式と結果を示します。

カテゴリ	式	結果
補間のエスケープ	str(“%{str($parameters.n1) + }%}%”)	1}%
	lb-%{str($parameters.n1) + }%}%	lb-1}%
	” %{str($parameters.n1) + \” }\%\” }%”	1}%

組み込み関数

February 6, 2024

StyleBook の式では組み込み関数が使用できます。

たとえば、組み込み関数 str() を使用して数字を文字列に変換できます。

str($parameters.order)

また、組み込み関数 int() を使用して文字列を整数に変換することもできます。

int($parameters.priority)

以下は、StyleBook の式でサポートされる組み込み関数とその使用例の一覧です。

str()

str () 関数は入力引数を文字列値に変換します。

許可される引数の種類は次のとおりです。

- string

- 番号
- TCP-port
- ブーリアン型
- IP アドレス

例:

- “set-“+ str(10) returns “set-10”
- str(10) returns “10”
- str(1.1.1.1) は”1.1.1.1”を返します
- str (T true) は「T true」を返します。
- str(mas) は”mas”を返します

int()

int () 関数は、文字列、数値、または tcpport を引数に取り、整数を返します。

例:

- int(“10”) returns 10
- int(10) returns 10

bool()

bool () 関数は引数として任意の型を取ります。引数の値が false、空、または存在しない場合、この関数は false を返します。

それ以外の場合は true を返します。

例:

- bool(true) returns “true”
- bool(false) は”false”を返します
- bool ($parameters.a) は、次の場合に false を返します。
- $parameters.a が偽であるか、空であるか、または存在しません。

len()

len () 関数は文字列またはリストを引数に取り、文字列の文字数またはリスト内の項目数を返します。

例 **1**:

次のように置換を定義した場合、

items: [“123”，“abc”，“xyz”]

len($substitutions.items) は 3 を返します

例 **2**:

len(“netscaler mas”) returns 13

サンプル **3**:

len ($parameters.vips) は、$parameters.vip に
値 [‘1.1.1.1’、’1.1.1.2’、’1.1.1.3’] が割り当てられている場合は 3 を返します。

min()

min () 関数は、リストまたは一連の数字または tcp-ports を引数に取り、最小の項目を返します。

一連の番号**/tcp** ポートを使用する例:

- min(80, 100, 1000) returns 80
- min(-20, 100, 400) returns -20
- min(-80, -20, -10) returns -80
- min(0, 100, -400) returns -400

番号**/tcp-**ポートのリストを持つ例:

- サポート $parameters.ports は TCP ポートのリストで、値は [80、81、8080] です。

  min ($parameters.ports) は 80 を返します。

max()

max () 関数は、リストまたは一連の数字または tcp-ports を引数に取り、最大の項目を返します。

一連の番号**/tcp** ポートを使用する例:

- max(80, 100, 1000) returns 1000
- max(-20, 100, 400) returns 400
- max(-80, -20, -10) returns -10
- max(0, 100, -400) returns 100

番号**/tcp-**ポートのリストを持つ例:

- $parameters.ports は tcp-port の一覧で、[80, 81, 8080] の値があるとします。

  max ($parameters.ports) は 8080 を返します。

bin()

bin () 関数は引数として数値を取り、その数値を 2 進形式で表す文字列を返します。

式の例:

bin(100) returns “0b1100100”

oct()

oct () 関数は引数として数値を取り、その数値を 8 進形式で表す文字列を返します。

式の例:

oct(100) returns “0144”

hex()

hex () 関数は引数として数値を取り、その数値を 16 進形式で表す小文字の文字列を返します。

式の例:

hex(100) returns “0x64”

lower()

lower () 関数は文字列を引数に取り、同じ文字列を小文字で返します。

例:

lower(“MAS”) returns “mas”

upper()

upper () 関数は文字列を引数に取り、同じ文字列を大文字で返します。

例:

upper (「netscaler_mas」) は「ネットスケーラー _MAS」を返します

sum()

sum () 関数は、数値または tcpports のリストを引数に取り、リスト内の数値の合計を返します。

例 **1**:

置換を次のように定義した場合:
置換:

- 番号リスト:
  - 11
  - 22
  - 55

  sum ($ 置換. 数値リスト) は 88 を返します

例 **2**:

$parameters.ports が [80, 81, 82] の場合、sum ($parameters.ports) は 243 を返します

pow()

pow () 関数は 2 つの数値を引数に取り、1 番目の引数を 2 番目の引数で
累乗した数値を返します。

例:

pow(3,2) returns 9

ip()

ip 関数は引数として文字列または ipaddress を受け取り、入力値に基づく IP アドレスを返します。

例:

- ip(“2.1.1.1”) returns “2.1.1.1”
- ip(3.1.1.1) は”3.1.1.1”を返します

base64.encode()

base64.encode () 関数は文字列引数を取り、base64 でエンコードされた文字列を返します。

例:

base64.encode(“abcd”) は”YWJjZA==”を返します

base64.decode()

Base64 Decode 関数は引数として Base64 でエンコードされた文字列を受け取り、デコードされた文字列を返します。

例:

base64.decode(“YWJjZA==”) は” abcd” を返します

exists()

exists 関数は任意の種類の引数を受け取り、ブーリアン型を返します。入力にいずれかの値がある場合、戻り値は True です。入力引数に値がない (つまり、値がない) 場合、戻り値は False です。

$parameters.monitor がオプションのパラメーターであるとします。構成パックを作成するときにこのパラメーターに値を入力すると、exists($parameters.monitor) は True を返します。

それ以外の場合は False を返します。

filter()

filter () 関数は 2 つの引数を取ります。

引数 1: 1 つの引数を受け取ってブーリアン型の値を返す置換関数です。

引数 2: 一覧です。

この関数は、最初の引数の置換関数に渡されたときに各要素が「True」と評価される元のリストのサブセットを返します。

例:

置換関数を次のように定義したとします。

置換:

```
1  x(a): $a != 81
```

入力値が 81 でない場合、この関数は True を返します。それ以外の場合は False を返します。

仮に、

$parameters.ports は [81、80、81、89]

filter($substitutions.x, $parameters.ports) は、一覧から 81 のアイテムをすべて削除して、[80, 89] を返します。

if-then-else()

関数 if-then-else () は 3 つの引数を取ります。

引数 1：ブール式

引数 2：任意の式

引数 3：任意の式（オプション）

引数 1 の式で True に評価された場合、この関数は引数 2 として指定された式の値を返します。

それ以外の場合は、引数 3 が指定されている場合、この関数は引数 3 の式の値を返します。

引数 3 が指定されていない場合、この関数は値を返しません。

例 **1**:

$parameters.servicetype に値”HTTP”がある場合、if-then-else($parameters.servicetype == HTTP, 80, 443) は”80”を返します。それ以外の場合、この関数は「443」を返し
ます。

例 **2**:

if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport) returns the value of “$parameters.hport”if $parameters.servicetype has value “HTTP.”

それ以外の場合、関数は「$parameters.sport」の値を返します。

サンプル **3**:

$parameters.servicetype に値”HTTP”がある場合、if-then-else($parameters.servicetype == HTTP, 80) は”80”を返します。

それ以外の場合、関数は値を返しません。

join()

join () 関数は次の 2 つの引数を取ります。

引数 1：数字、tcp-port、文字列、または ipaddress の一覧

引数 2：区切り文字列（オプション）

この関数は、引数 1 として指定された一覧の要素を 1 つの文字列に結合します。この文字列の各要素は、引数 2 として指定された区切り文字列で区切られます。引数 2 が指定されない場合、一覧の要素は 1 つの文字列として結合されます。

例:

- $parameters.ports は [81, 82, 83] です。

- デリミタ引数付き:

  join ($parameters.ports, ‘-‘) は「81-82-83”を返します

- デリミタ引数なし:

  join ($parameters.ports) は「818283」を返します

map()

map 関数は、次の 2 つの引数を受け取ります。

引数 1：任意の関数

引数 2：要素の一覧

この関数は、リスト内の各要素が引数 2 の対応する要素にマップ関数 (引数 1) を適用した結果であるリストを返します。

引数 1 で許可される関数は次のとおりです。

- 1 つの引数を取る組み込み関数:

  base64.encode, base64.decode, bin, bool, exists, hex, int, ip, len, lower, upper, oct, quotewrap, str, trim, upper, url.encode, url.decode

- 1 つ以上の引数を受け取る置換関数。

例:

$parameters.nums が [81, 82, 83] であるとします。

- 組み込み関数 str を使用した map

  map(str, $parameters.nums) は [“81”, “82”, “83”] を返します

  map 関数の結果は文字列の一覧であり、文字列の各要素は、入力した一覧 ($parameters.nums) の対応する要素に str 関数を適用して処理されています。

- 置換関数を使用した map

  - Substitutions:

    10 (ポート) の追加:$ ポート + 10

  - 表現:

    マップ ($substitutions.add-10,

    $parameters.nums) は数値のリストを返します:
    [91, 92, 93]

この map 関数の結果は数字の一覧であり、各要素は、入力した一覧 ($parameters.nums) の対応する要素に、置換関数 $substitutions.add-10 を適用して処理されています。

quotewrap()

quotewrap 関数は、引数として文字列を受け取り、入力値の前後に二重引用符を追加してから文字列を返します。

例:

クォートラップ (「mas」) は「”mas “」を返します

replace()

replace 関数は、次の 3 つの引数を受け取ります。

引数 1: 文字列

引数 2: 文字列

引数 3: 文字列（オプション）

この関数は、引数 1 の中にある引数 2 のすべてのアイテムを引数 3 で置き換えます。

引数 3 が指定されない場合、引数 2 のすべてのアイテムが引数 1 から削除されます（つまり、空の文字列で置き換えられます)。

文字列の一部を、別の文字列の一部で置き換えます。

- replace(‘abcdef’ , ‘def’ , ‘xyz’) returns “abcxyz”.
  - 「def」のすべての出現は「xyz」に置き換えられます。
- replace(‘abcdefabc’ , ‘def’) returns “abcabc”.
  - 3 つ目の引数がないため、”def” は結果の文字列から削除されています。

trim()

trim 関数は、入力文字列から前後のスペースを削除した文字列を返します。

例:

トリム (‘abc’) は「abc」を返します

truncate()

truncate 関数は、次の 2 つの引数を受け取ります。

引数 1: 文字列

引数 2: 数字

この関数は、引数 1 の入力文字列を、引数 2 で指定された長さに切り捨てた文字列を返します。

例:

truncate(‘netscaler mas’, 9) returns “netscaler”

url.encode

url.encode 関数は、RFC 3986 に基づき、ASCII 文字セットを使用して文字が変換された文字列を返します。

例:

url.encode(“a/b/c”) returns “a%2Fb%2Fc”

url.decode

url.decode 関数は、RFC 3986 に基づき、URL エンコードされた引数を通常の文字列にデコードした文字列を返します。

例:

url.decode(“a%2Fb%2Fc”) returns “a/b/c”

is-ipv4 ()

is-ipv4 () 関数は IP アドレスを引数に取り、IP アドレスが IPv4 形式の場合は「true」を返します。

is-ipv4 (10.10.10.10) は「True」を返します

is-ipv6 ()

is-ipv6 () 関数は IP アドレスを引数に取り、IP アドレスが IPv6 形式の場合は「true」を返します。

is-ipv6 (2001: DB8::) は「True」を返します

依存関係の検出

February 6, 2024

StyleBook のコンポーネントでは、同じ StyleBook に含まれる別のコンポーネントのプロパティまたはセクションを参照できます。コンポーネントはそれ自体が完成されたブロックであるため、実行する必要のある順序どおりに記

載されていない場合があります。StyleBook コンパイラはコンポーネントの記載順をチェックして、論理順で実行します。

例:

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
 -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.name
      servicegroupname: $components.sg-comp.properties.servicegroupname
-
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
<!--NeedCopy-->
```

上記の例では、定義された 3 つのコンポーネントがあります- **lbvserver-comp**、**lb-sg-binding-comp**、および **sg-comp**。この StyleBook の実行時には、まず lbvserver-comp が作成されます。lb-sg-binding-comp は lbvserver-comp プロパティを参照しており、StyleBook で 2 番目に定義されているコンポーネントですが、この次に作成することはできません。これは、lb-sg-binding-comp にはまだ作成されていない sg-comp との依存関係もあるからです。このため、コンパイラはコンポーネントの作成時点でコンポーネントの依存関係が解決されるようにコンポーネントを並べ替え、並べ替えた順序でコンポーネントを実行します。上記の StyleBook の実行順は、lbvserver-comp、sg-comp、lb-sg-binding-comp のようになります。

したがって、StyleBook の作成者がコンポーネントの正確な順序を気にする必要はありません。コンポーネントはどのような順序で記載しても構いません。コンパイラにより、コンポーネント間の参照関係に基づいて適切なコンポーネントの実行順序が計算されます。この依存関係の検出と並べ替えは、substitution セクションおよび outputs セクションにも適用されることに注意してください。

循環依存関係

コンポーネントは別のコンポーネントを参照することがあるため、StyleBook の定義では依存関係の循環が生じる可能性があります。たとえば、コンポーネント A がコンポーネント B で定義されているプロパティを参照しており、さらにコンポーネント B がコンポーネント A で定義されているプロパティを参照している場合などです。こうした依

存関係は、循環依存関係と呼ばれます。循環依存関係を自動で解決することはできません。StyleBook の作成者が手動で StyleBook の定義を修正し、こうした循環依存関係を解消する必要があります。コンパイラは循環依存関係を特定することができ、循環依存関係が存在する場合にはレポートします。

以下の例に、コンポーネントの循環依存関係を示します。

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $components.lb-sg-binding-comp.properties.name
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
     name: mylb
      servicegroupname: $components.sg-comp.properties.servicegroupname
  -
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: $components.lbvserver-comp.properties.servicetype
<!--NeedCopy-->
```

上の例では、lbvserver-comp、lb-sg-binding-comp、sg-comp の 3 つのコンポーネントがあります。**lbvserver-comp** は **lb-sg-binding-comp** に依存し、**lb-sg-binding comp** は **sg-comp** に依存し、**sg-comp** は **lbvserver-comp** に依存します。このように、これらのコンポーネント間で依存関係の循環が生じており、この循環は自動で解決できません。このため、この StyleBook は実行できません。StyleBook コンパイラはこれを検出し、StyleBook が NetScaler ADM にインポートされないようにします。

インスタンス管理

February 6, 2024

インスタンスは、NetScaler Application Delivery Management（ADM）を使用して管理、監視、トラブルシューティングを行うことができる Citrix Application Delivery Controller（ADC）アプライアンスです。インスタンスを監視するには、NetScaler ADM にインスタンスを追加する必要があります。インスタンスは、Citrix ADM の設定時に追加することも、後で追加することもできます。NetScaler ADM にインスタンスを追加すると、継続的にポーリングされ、後で問題の解決やレポートデータとして使用できる情報を収集します。

インスタンスは、静的グループまたはプライベート IP ブロックとしてグループ化できます。インスタンスの静的グループは、設定ジョブなどの特定のタスクを実行する場合に便利です。プライベート IP ブロックは、地理的な場所に基づいてインスタンスをグループ化します。

インスタンスを追加する

インスタンスは、Citrix ADM サーバーを初めて設定するときに追加することも、後で追加することもできます。インスタンスを追加するには、各 NetScaler ADC インスタンスのホスト名または IP アドレス、または IP アドレスの範囲を指定する必要があります。

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

NetScaler ADM サーバーにインスタンスを追加すると、サーバーは暗黙的にインスタンスのトラップ先として自身を追加し、インスタンスのインベントリを収集します。詳細については、「NetScaler ADM がインスタンスを検出する方法」を参照してください。

インスタンスを追加したら、[ネットワーク] > [ダッシュボード] に移動し、[すべてのインスタンス**]** をクリックすることでインスタンスを削除できます。[Instances] ページで、削除するインスタンスを選択し、[**Remove**] をクリックします。

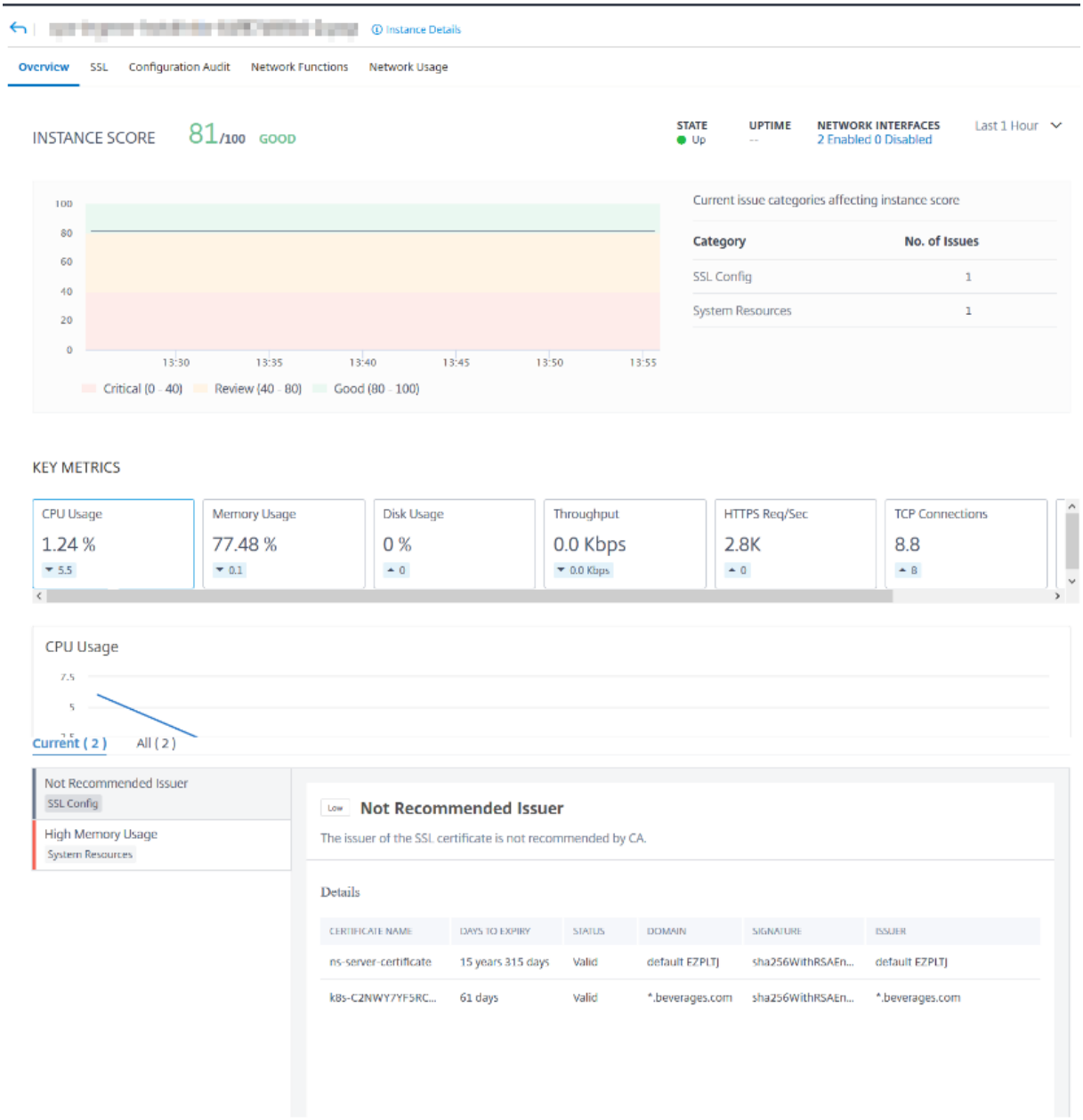
インスタンスダッシュボードの使用方法

NetScaler ADM のインスタンスごとのダッシュボードには、選択したインスタンスのデータが表形式とグラフ形式で表示されます。ポーリングプロセス中にインスタンスから収集されたデータは、ダッシュボードに表示されます。

デフォルトでは、1 分ごとに、マネージインスタンスがデータ収集のためにポーリングされます。状態、1 秒あたりの HTTP リクエスト数、CPU 使用率、メモリ使用量、スループットなどの統計情報は、NITRO 呼び出しを使用して継続的に収集されます。管理者は、収集したデータをすべて 1 つのページに表示し、インスタンス内の問題を特定し、すぐに修正するためのアクションを実行できます。

特定のインスタンスのダッシュボードを表示するには、[ネットワーク] > [インスタンス] に移動します。概要からインスタンスタイプを選択し、表示するインスタンスを選択し、[**Dashboard**] をクリックします。

次の図は、インスタンス単位のダッシュボードに表示されるさまざまなデータの概要を示しています:



- 概要。概要タブには、選択したインスタンスの CPU とメモリの使用量が表示されます。インスタンスによって生成されたイベントとスループットデータを表示することもできます。IP アドレス、ハードウェアと LOM のバージョン、プロファイルの詳細、シリアル番号、連絡先などのインスタンス固有の情報もここに表示されます。さらに下にスクロールすると、選択したインスタンスで使用できるライセンスされた機能と、そのインスタンスで設定されたモードが表示されます。
- **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 つのレポートのみが表示されますが、画面の右下隅にある「+」アイコンをクリックしてパフォーマンスレポートを追加できます。

グローバルに分散したサイトの監視

February 6, 2024

ネットワーク管理者は、さまざまな地域に展開されたネットワークインスタンスを必要に応じて監視および管理する必要があります。ただし、地理的に分散したデータセンターでネットワークインスタンスを管理する場合、ネットワークの要件を評価することは容易ではありません。

NetScaler Application Delivery Management（ADM）のジオマップは、サイトをグラフィカルに表現し、ネットワーク監視エクスペリエンスを地理的に分類します。また、ネットワークインスタンスの分布を場所ごとに表示し、ネットワークの問題を監視することもできます。

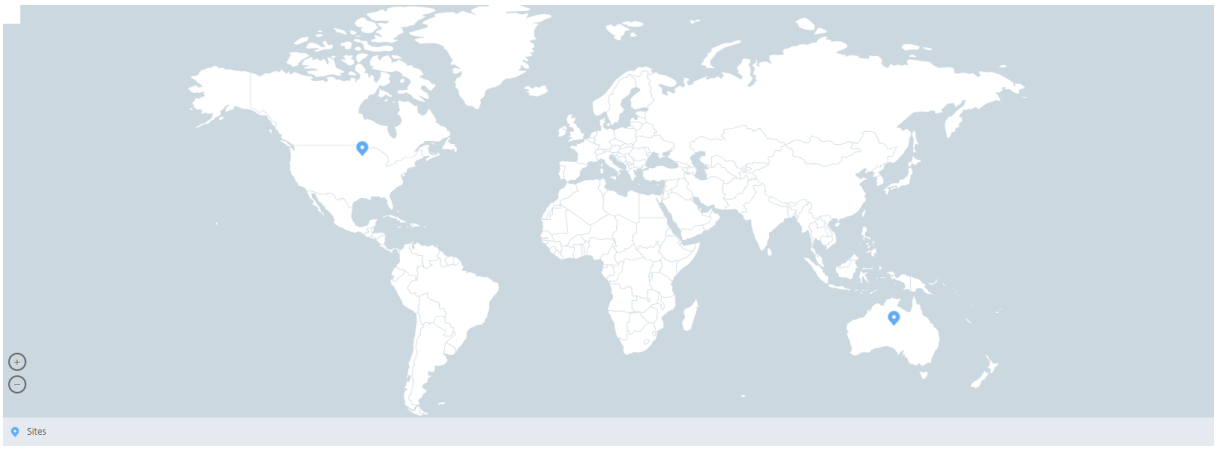
次のセクションでは、NetScaler ADM でデータセンターを監視する方法について説明します。

NetScaler ADM サイトは、特定の地理的な場所にある Citrix Application Delivery Controller（ADC）インスタンスを論理的にグループ化したものです。たとえば、あるサイトが Amazon Web Services（AWS）に割り当てられ、別のサイトが Azure™ に割り当てられる場合があります。さらに別のサイトがテナントの敷地内にホストされています。NetScaler ADM は、すべてのサイトに接続されているすべての NetScaler ADC インスタンスを管理および監視します。NetScaler ADM を使用して、管理対象インスタンスから送信される syslog、AppFlow、SNMP、およびそのようなデータを監視および収集できます。

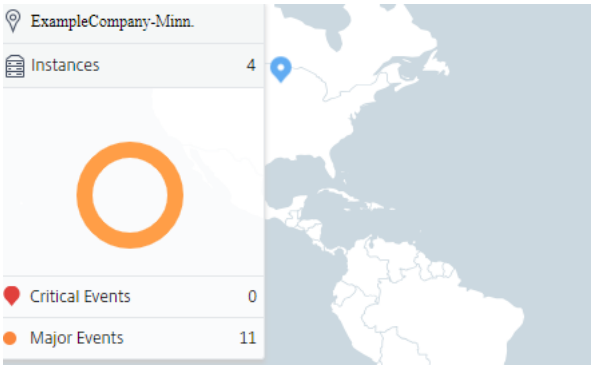
NetScaler ADM のジオマップでは、サイトをグラフィカルに表示できます。ジオマップでは、ネットワークモニタリング体験を地域ごとに分類することもできます。ジオマップを使用すると、場所ごとにネットワークインスタンスの分布を視覚化し、すべてのネットワーク問題を監視できます。ネットワーク > ダッシュボードページに移動すると、世界地図上に作成されたサイトを視覚的に表示できます。

使用例

ある大手携帯電話会社 ExampleCompany は、リソースとアプリケーションのホスティングを民間のサービスプロバイダーに頼っていました。同社はすでに 2 つの拠点を構えていました。1 つは米国のミネアポリスに、もう 1 つはオーストラリアのアリススプリングスにあります。この画像では、2 つのマーカーが 2 つの既存のサイトを表していることがわかります。



マーカーには、各サイトのアプリケーション数を示す数値も表示されます。これらのマーカーをクリックすると、各サイトの詳細情報が表示されます。

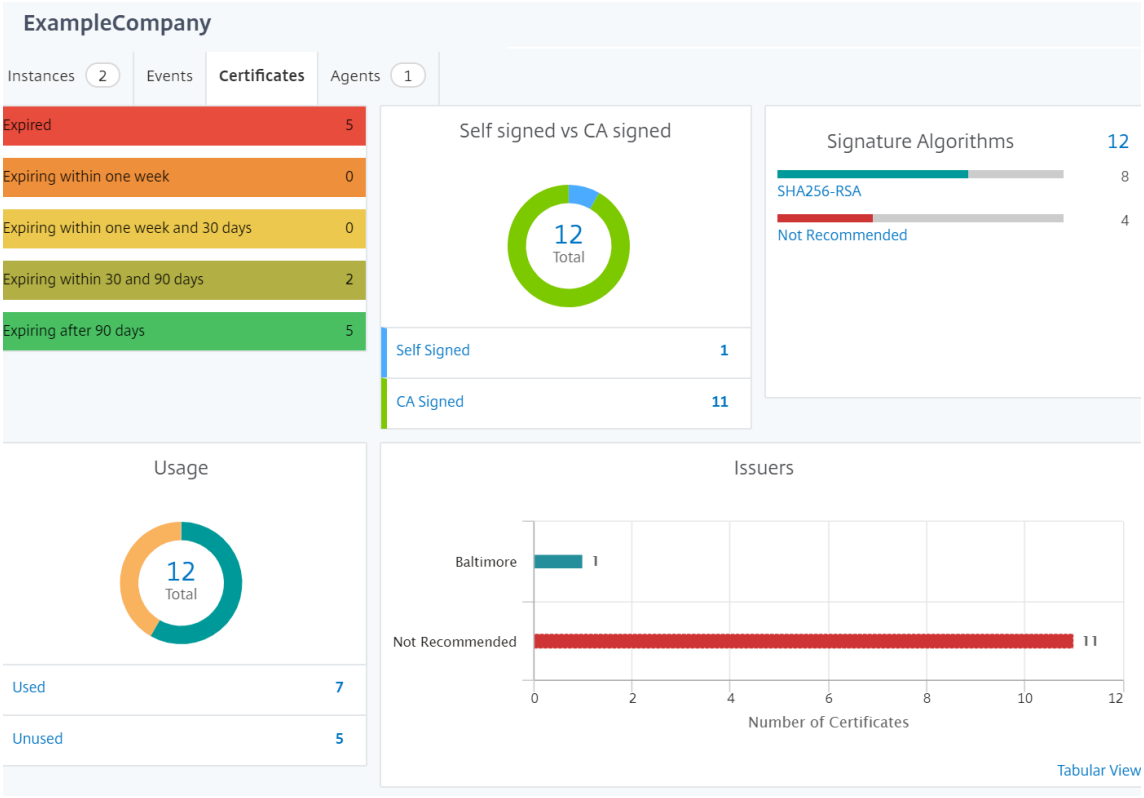


タブをクリックして、詳細情報を表示します。

- 「インスタンス」タブ: このタブには以下が表示されます。
  - 各ネットワークインスタンスの IP アドレス
  - インスタンスのタイプ
  - それらに関する重大なイベントの数
  - NetScaler ADC インスタンスで発生した重要なイベントとすべてのイベント。
- イベントタブ: インスタンスで発生した重大イベントと重要イベントのリストを表示します。
- 「証明書」タブ: このタブには以下が表示されます。

  - すべてのインスタンスの証明書のリスト
  - 有効期限ステータス
  - 重要な情報と、使用中の多くの証明書の上位 10 インスタンス。

- [**Agents**] タブ: インスタンスがバインドされているエージェントのリストを表示します。



ジオマップの設定

ExampleCompany は、インドのバンガロールに 3 つ目のサイトを作成することにしました。同社は、重要度の低い社内 IT アプリケーションの一部をバンガロールオフィスにオフロードして、クラウドをテストしたいと考えていました。同社は AWS クラウドコンピューティングサービスを使用することにしました。

管理者は、最初にサイトを作成し、次に NetScaler ADM に NetScaler ADC インスタンスを追加する必要があります。また、インスタンスをサイトに追加し、エージェントを追加し、エージェントをサイトにバインドする必要があります。NetScaler ADM は、NetScaler ADC インスタンスとエージェントが属するサイトを認識します。

NetScaler ADC インスタンスの追加について詳しくは、「インスタンスの追加」を参照してください。

サイトを作成するには、次の手順に従います。

NetScaler ADM にインスタンスを追加する前にサイトを作成します。位置情報を提供することで、サイトを正確に見つけることができます。

[ネットワーク] > [サイト] に移動し 、[追加] をクリック します。

1. **[** サイトの作成] ページで、次の情報を指定します。

   a) サイトタイプ: データセンターを選択します。

   > 注
   >
   > サイトは、プライマリデータセンターまたはブランチとして機能できます。適宜選択してください。

   b) タイプ: リストから AWS をクラウドプロバイダーとして選択します。

   > 注**:**
   >
   > [既存の **VPC** をサイトとして使用する] チェックボックスをオンにします。

   c) サイト名: サイトの名前を入力します。

   d) 市区町村: 市区町村を入力します。

   e) 郵便番号: 郵便番号を入力します。

   f) 地域: 地域を入力します。

   g) 国: 国を入力してください

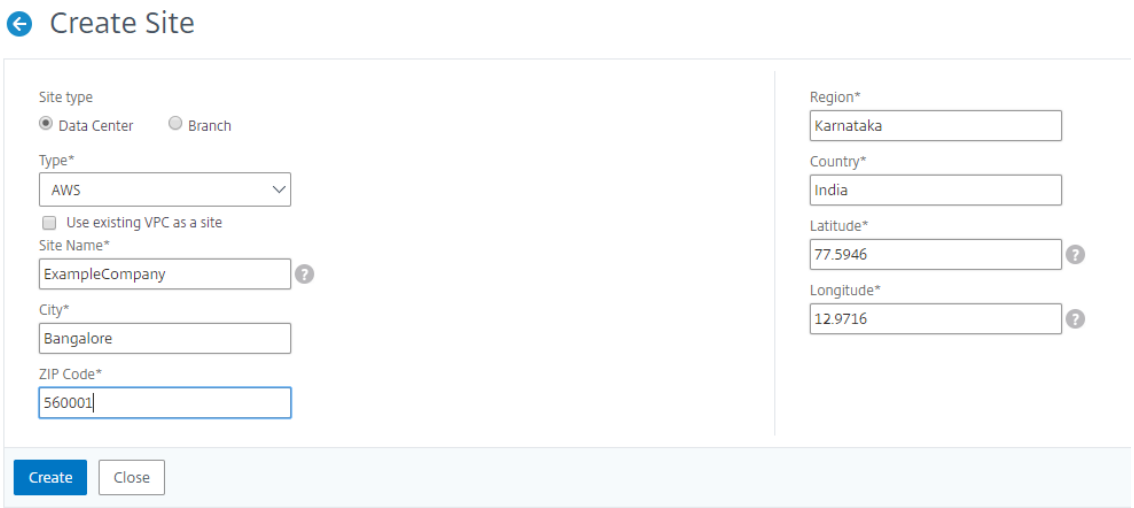
   h) 緯度: 位置の緯度を入力します。

      南緯には負の値を指定します。例: `-77.5946`

   i) 経度: 位置の経度を入力します。

      西経には負の値を指定します。例: `-12.9716`

2. [**Create**] をクリックします。

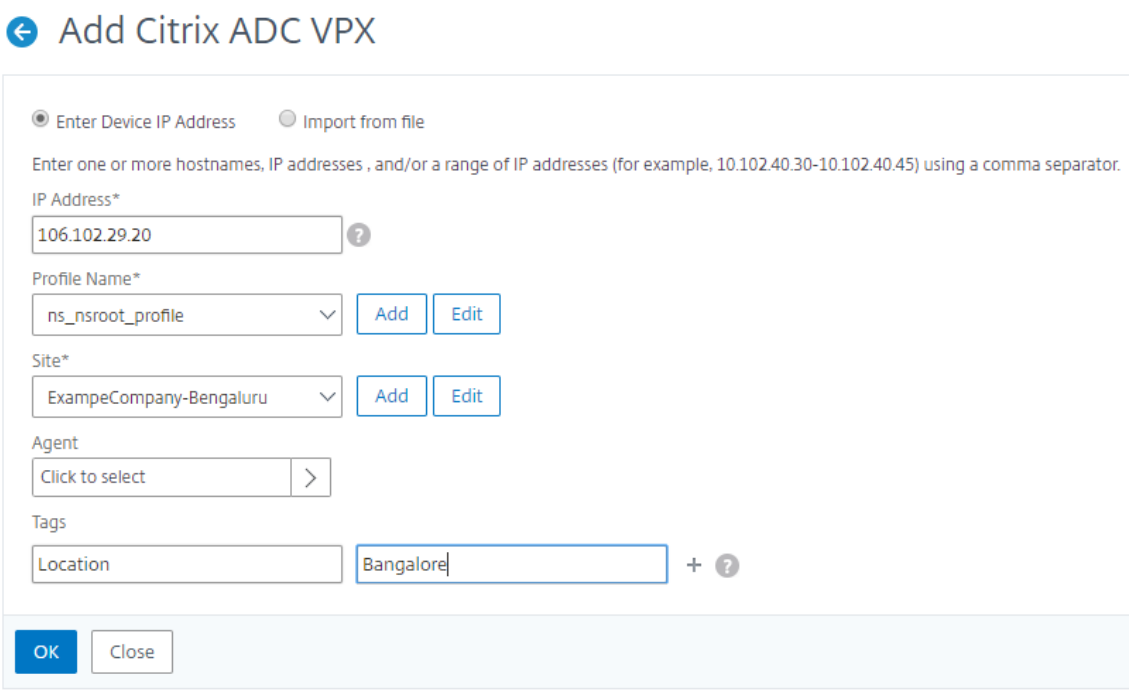


インスタンスを追加してサイトを選択するには**:**

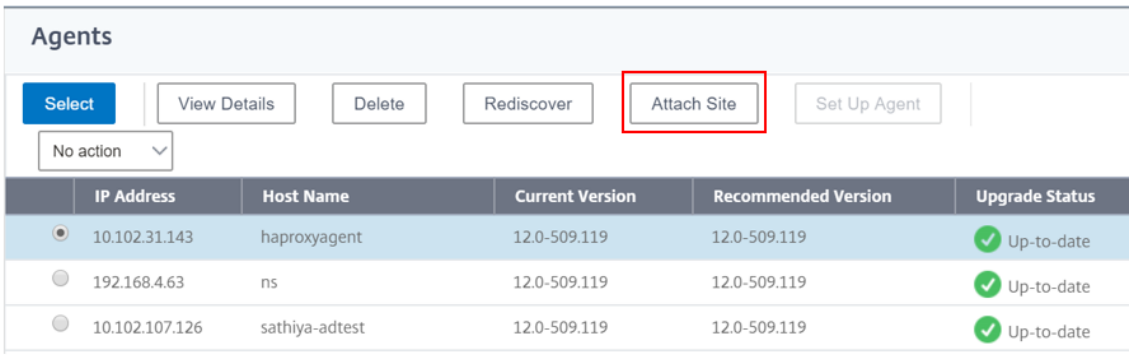
サイトを作成したら、NetScaler ADM にインスタンスを追加する必要があります。以前に作成したサイトを選択するか、サイトを作成してインスタンスを関連付けることもできます。

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、[ネットワーク] > [インスタンス] に移動します。
2. 作成するインスタンスのタイプを選択し、[**Add**] をクリックします。
3. [**NetScaler ADC VPX** の追加] ページで、IP アドレスを入力し、リストからプロファイルを選択します。
4. リストからサイトを選択します。サイトフィールドの横にある **+** 記号をクリックしてサイトを作成するか、編集アイコンをクリックしてデフォルトサイトの詳細を変更できます。
5. 右矢印をクリックし、表示されるリストからエージェントを選択します。



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。



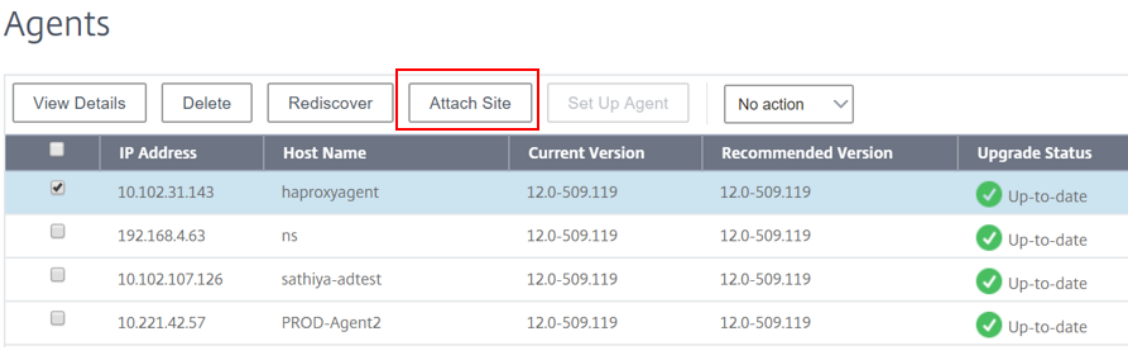
1. リストからサイトを選択し、[保存] をクリックします。

1. [**OK**] をクリックします。

[ネットワーク] > **[**エージェント] に移動して、エージェントをサイトに接続することもできます。

NetScaler ADM エージェントをサイトに関連付けるには:

1. Citrix ADM で、[ネットワーク] > [エージェント] に移動します。
2. エージェントを選択し、[サイトの接続] をクリックします。



1. サイトを関連付けて、[保存] をクリックします。

NetScaler ADM は、バンガロールサイトに追加された NetScaler ADC インスタンスと、他の 2 つのサイトのインスタンスの監視を開始します。

タグを作成してインスタンスに割り当てる方法

February 6, 2024

Citrix Application Delivery Management（ADM）では、Citrix アプリケーション Delivery Controller（ADC）インスタンスをタグに関連付けることができるようになりました。タグは、インスタンスに割り当てることができるキーワードまたは単語の用語です。タグは、インスタンスに関するいくつかの追加情報を追加します。タグは、インスタンスを説明するのに役立つメタデータと考えることができます。タグを使用すると、これらの特定のキーワードに基づいてインスタンスを分類および検索できます。1 つのインスタンスに複数のタグを割り当てることもできます。

以下のユースケースは、インスタンスのタグ付けがどのようにモニタリング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、英国にあるすべてのインスタンスを識別できます。ここでは、キーを「Country」、値を「UK」とするタグを作成できます。このタグは、英国にあるすべてのインスタンスを検索および監視するのに役立ちます。
- ユースケース **2**: ステージング環境にあるインスタンスを検索する場合。ここでは、キーを「Purpose」、値を「Staging_NS」とするタグを作成できます。このタグは、ステージング環境で使用されているすべてのインスタンスを、クライアント要求が実行されているインスタンスから分離するのに役立ちます。

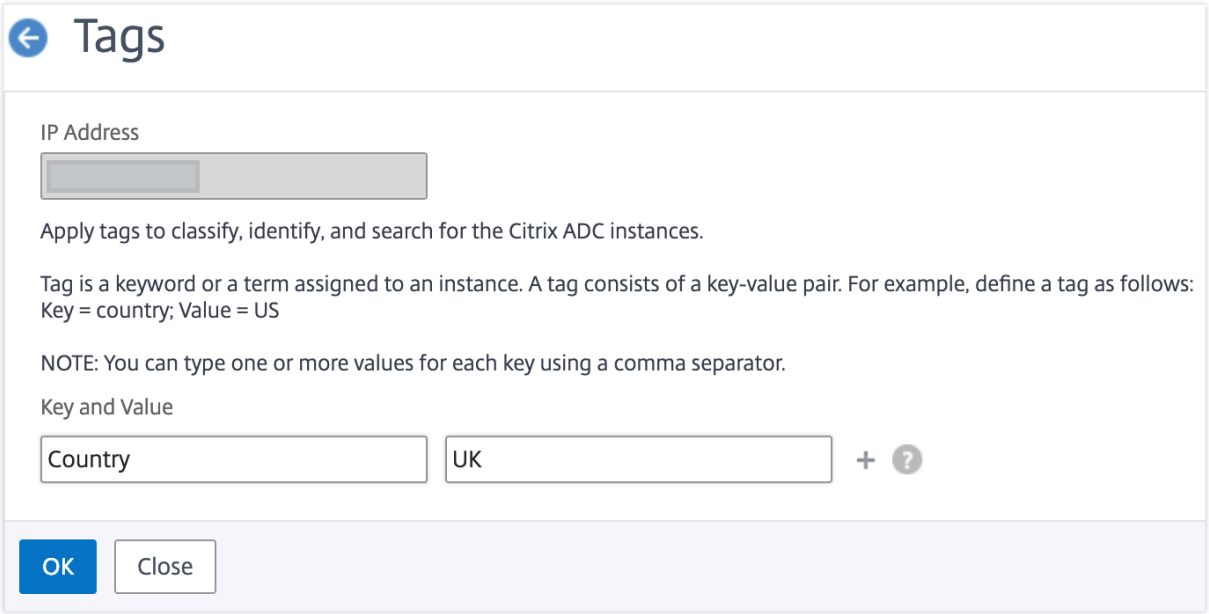
- ユースケース **3**: 英国のスウィンドン地域にあり、David T. が所有している Citrix ADC インスタンスのリストを確認したい場合を考えてみましょう。これらすべての要件に対応するタグを作成し、それをこれらの条件を満たすすべてのインスタンスに割り当てることができます。

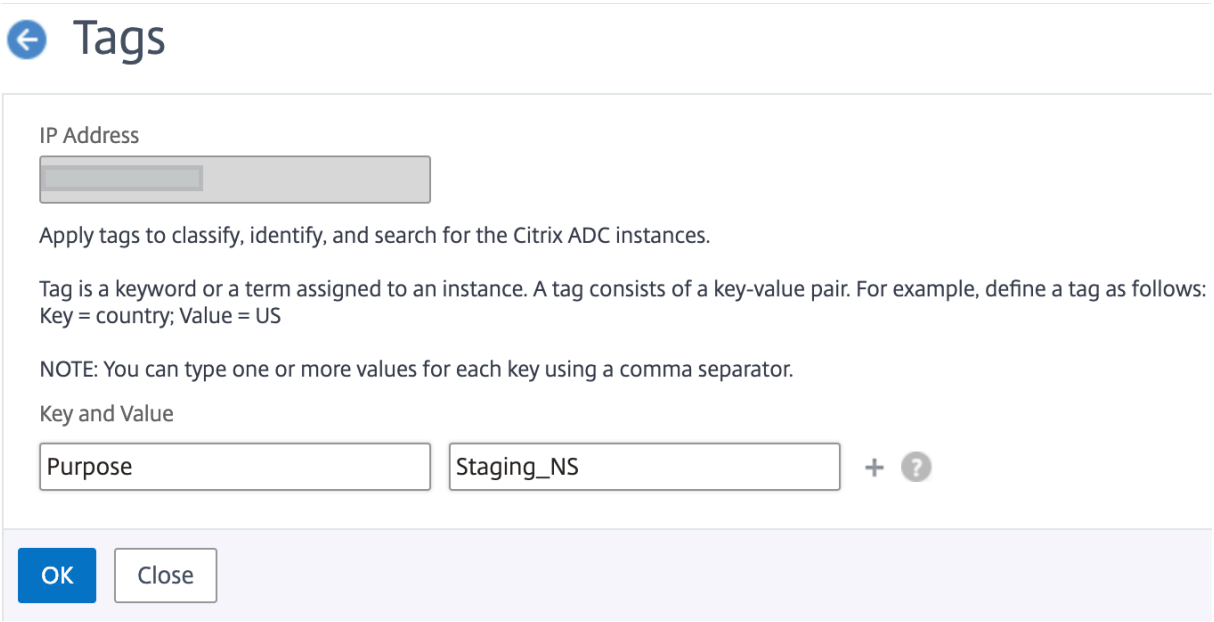
NetScaler ADC VPX インスタンスにタグを割り当てるには:

1. NetScaler ADM で、［ネットワーク］>［インスタンス］**>**［**NetScaler ADC**］に移動します。
2. ［**NetScaler ADC VPX** ］タブを選択します。
3. 必要な Citrix VPX を選択します。
4. [タグ] をクリックします。
5. タグを作成して「**OK**」をクリックします。

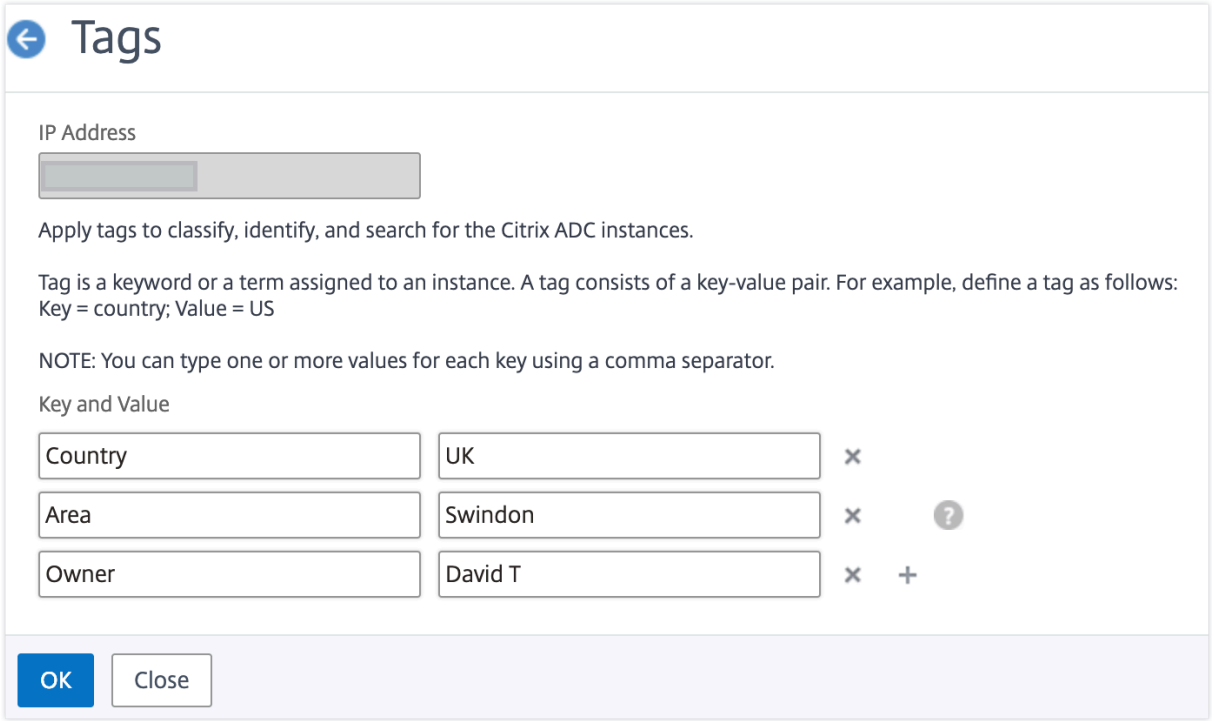
表示される [タグ] ウィンドウでは、作成したすべてのキーワードに値を割り当てることによって、独自の「キーと値」のペアを作成できます。

たとえば、次の画像は、作成されたいくつかのキーワードとその値を示しています。独自のキーワードを追加し、各キーワードに値を入力できます。



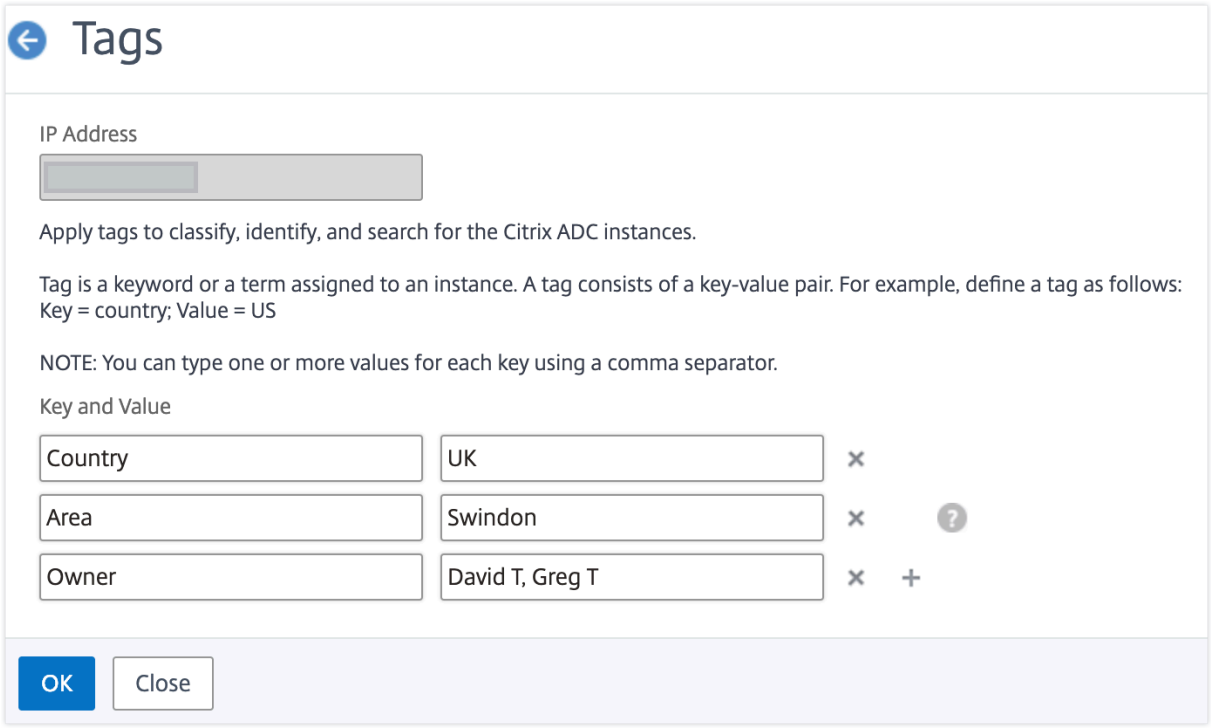


「+」をクリックして複数のタグを追加することもできます。複数の意味のあるタグを追加すると、インスタンスを非常に効率的に検索できます。



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

Citrix Application Delivery Management（ADM）が多数の Citrix 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。タグとは、NetScaler ADC インスタンスに関する追加の説明を追加するために、NetScaler ADC インスタンスに割り当てることができる用語またはキーワードです。これで、NetScaler ADC インスタンスをタグに関連付けることができます。これらのタグを使用すると、NetScaler ADC インスタンスをより適切に識別および検索できます。

- **[プロパティ]**。NetScaler ADM で追加された各 NetScaler ADC インスタンスには、そのインスタンスに関連付けられたデフォルトのパラメータまたはプロパティがいくつかあります。たとえば、各インスタンスには独自のホスト名、IP アドレス、バージョン、ホスト ID、ハードウェアモデル ID などがあります。これらのプロパティの値を指定して、インスタンスを検索できます。

たとえば、バージョン 12.0 にあり、稼働状態にある NetScaler ADC インスタンスのリストを調べたい場合を考えてみましょう。ここでは、インスタンスのバージョンと状態はデフォルトプロパティによって定義されます。

12.0 バージョンとインスタンスの稼働状態の他に、所有しているインスタンスを検索することもできます。「所有者」タグを作成し、そのタグに値「David T」を割り当てることができます。タグの作成と割り当て方法について詳しくは、「タグの作成とインスタンスへの割り当て方法」を参照してください。

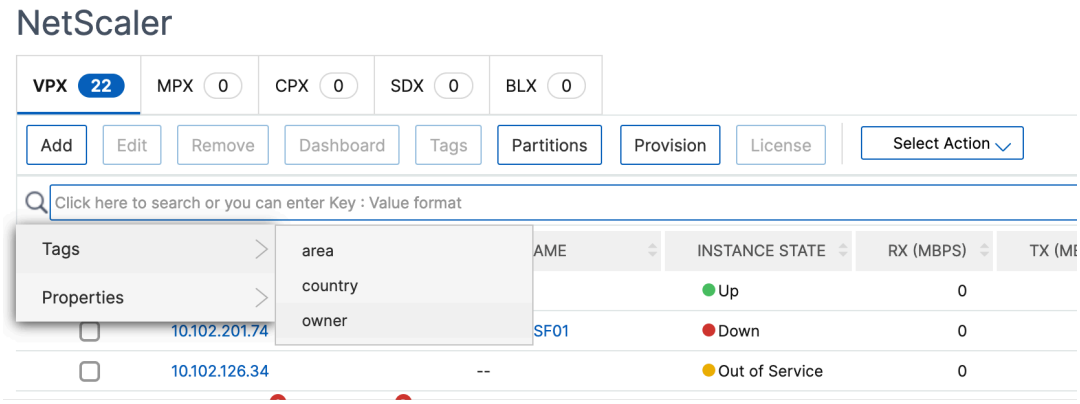
タグとプロパティの組み合わせを使用して、独自の検索条件を作成できます。

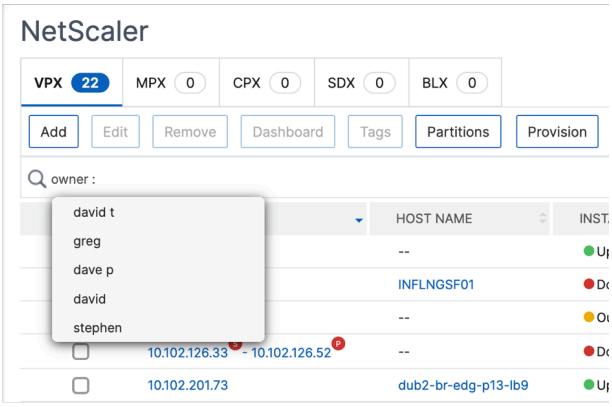
NetScaler ADC VPX インスタンスを検索するには

1. Citrix ADM で、[ネットワーク] > [インスタンス] > **[**Citrix ADC**] > [VPX] タブに移動します。
2. 検索フィールドをクリックします。検索式は、タグまたはプロパティを使用するか、両方を組み合わせて作成できます。

   次の例は、検索式を効率的に使用してインスタンスを検索する方法を示しています。

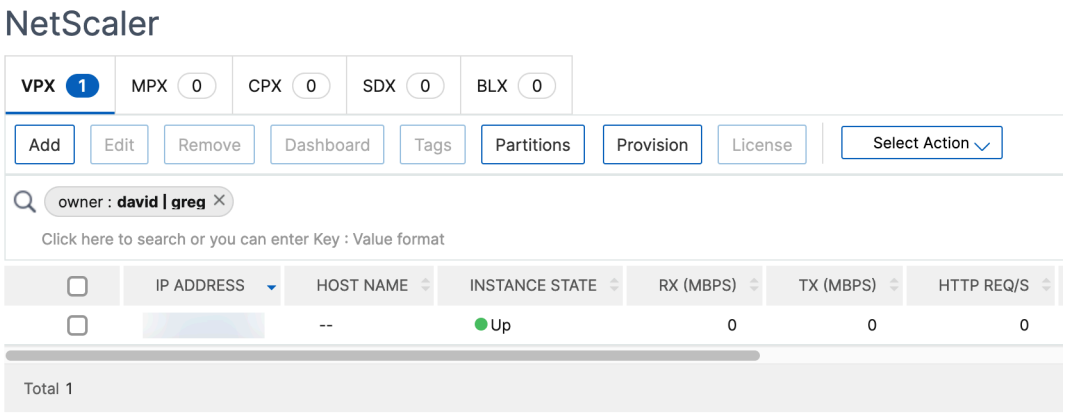
   a) [タグ] オプションを選択し、[所有者] を選択します。「デビッド T.」を選択します。



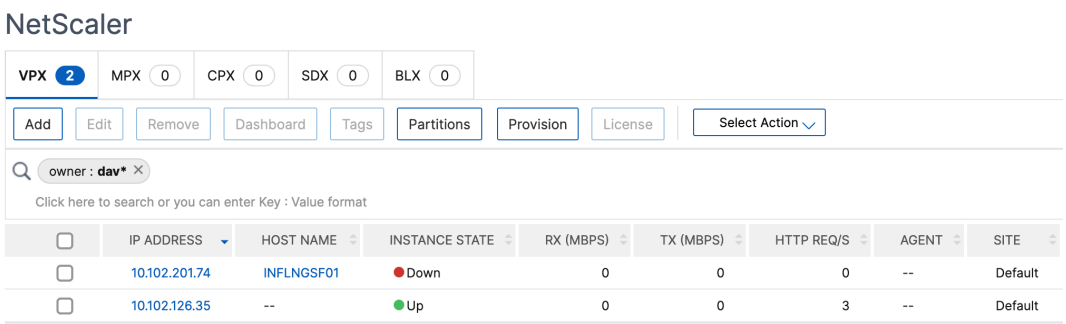


NetScaler ADM では、検索式で正規表現とワイルドカード文字がサポートされています。

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

Citrix アプリケーション Delivery Controller（ADC）インスタンスの管理パーティションを構成して、組織内のさまざまなグループに同じ Citrix ADC インスタンス上の異なるパーティションを割り当てることができます。ネットワーク管理者を割り当てて、複数の Citrix ADC インスタンス上の複数のパーティションを管理できます。

Citrix Application Delivery Management（ADM）を使用すると、管理者が所有するすべてのパーティションを単一のコンソールからシームレスに管理できます。これらのパーティションは、他のパーティション構成を中断することなく管理できます。

複数のユーザーが異なる管理パーティションを管理できるようにするには、グループを作成し、それらのグループにユーザーとパーティションを割り当てる必要があります。各ユーザーは、そのユーザーが属するグループ内のパーティションのみを表示および管理できます。各管理パーティションは、NetScaler ADM ではインスタンスと見なされます。NetScaler ADC インスタンスを検出すると、その NetScaler ADC インスタンスに構成されている管理パーティションが自動的にシステムに追加されます。

2 つの Citrix VPX インスタンスがあり、各インスタンスに 2 つのパーティションが設定されているとします。たとえば、NetScaler ADC インスタンス 10.102.216.49 にはパーティション _1、パーティション _2、パーティション _3 があり、NetScaler ADC インスタンス 10.102.29.120 には p1 と p2 があります。

パーティションを表示するには、［ネットワーク］**>**［インスタンス］**>**［**NetScaler ADC**］**>**［**VPX**］の順に選択し、［パーティション］をクリックします。

ユーザ p1 には、10.102.29.120-p1 および 10.102.216.49-パーティション _1 というパーティションを割り当てることができます。また、ユーザー p2 をパーティション 10.102.29.80-p2、10.102.216.49-Partition_2、10.102.216.49-Partition_3 の管理に割り当てることができます。

次に、user-p1 と user-p2 という 2 つのユーザーを作成し、それらのユーザーを、それぞれのために作成されているグループに割り当てる必要があります。

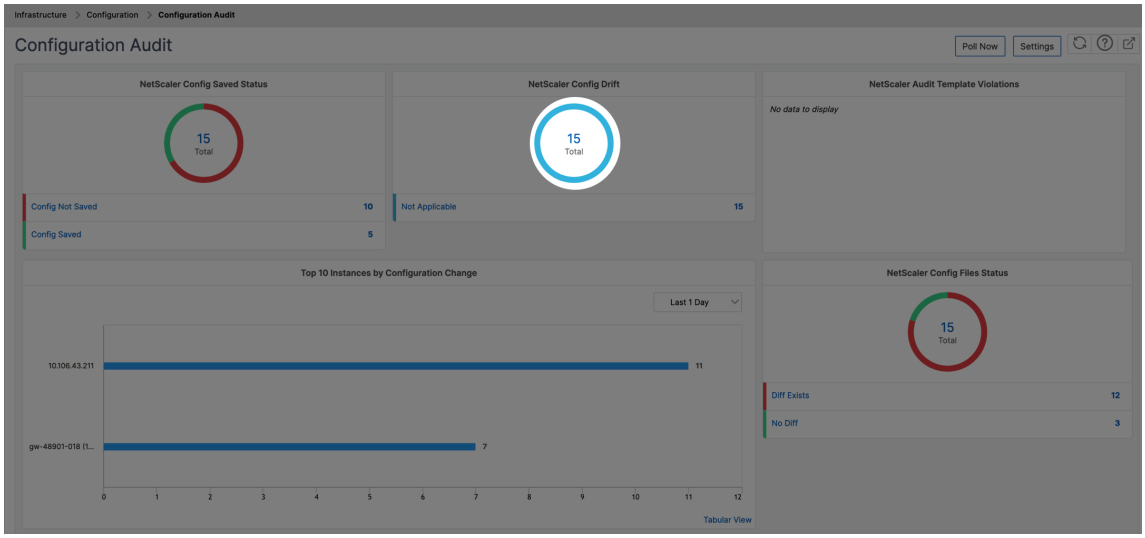
まず、適切な権限 (管理者権限など) を持つ 2 つのグループを作成し、各グループに必要な管理パーティションインスタンスを含める必要があります。たとえば、システムグループ partition1-admin を作成し、Citrix ADC 管理パーティション 10.102.29.120-p1 と 10.102.216.49-Partition_1 をこのグループに追加します。また、システムグループ partition2-admin を作成し、Citrix ADC 管理パーティション 10.102.29.120-p2、10.102.216.49-Partition_2、10.102.216.49-Partition_3 をこのグループに追加します。

管理パーティションを作成したら、改訂履歴差分機能と管理パーティションの監査テンプレート機能を監査目的で使用することもできます。

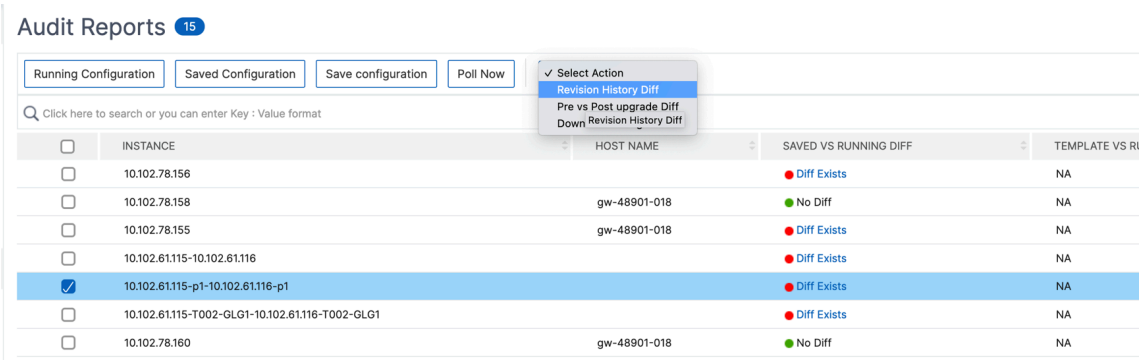
管理パーティションのリビジョン履歴の違いにより、パーティション化された Citrix ADC インスタンスの最新の 5 つの構成ファイルの違いを表示できます。構成ファイルを相互に比較したり（たとえば、構成リビジョン-1 と構成リビジョン -2)、構成リビジョンを使用して現在実行/保存されている構成と比較したりできます。構成の違いとともに、修正構成も示されています。すべての修正コマンドをローカルフォルダにエクスポートし、設定を修正できます。

改訂履歴の差異を表示する手順は、次のとおりです。

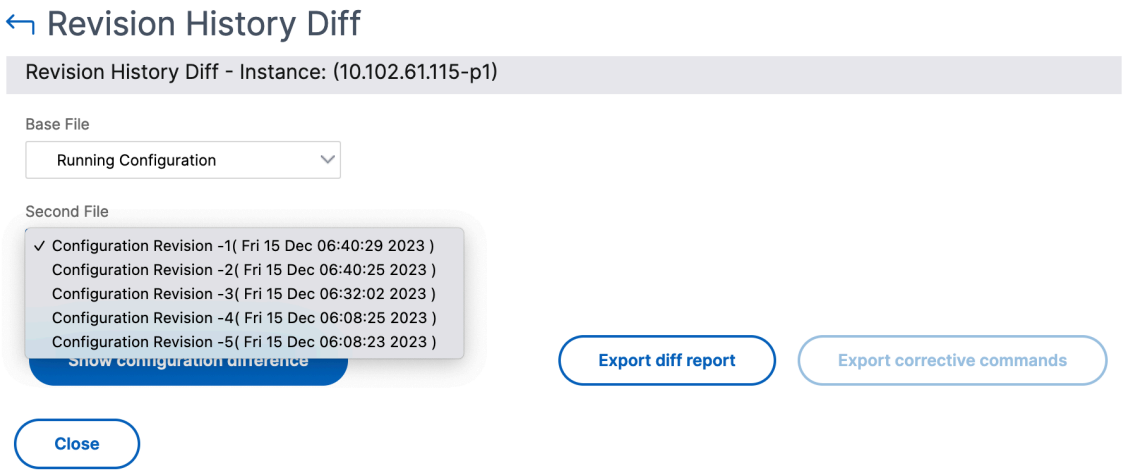
1. ［ネットワーク**] > [**構成監査**]** に移動します。インスタンスの構成ステータスを表すドーナツグラフ内をクリックします。表示される［監査レポート］ページで、パーティション分割された NetScaler ADC インスタンスをクリックします。



2. [操作] メニューから、[リビジョン履歴の差分] をクリックします。

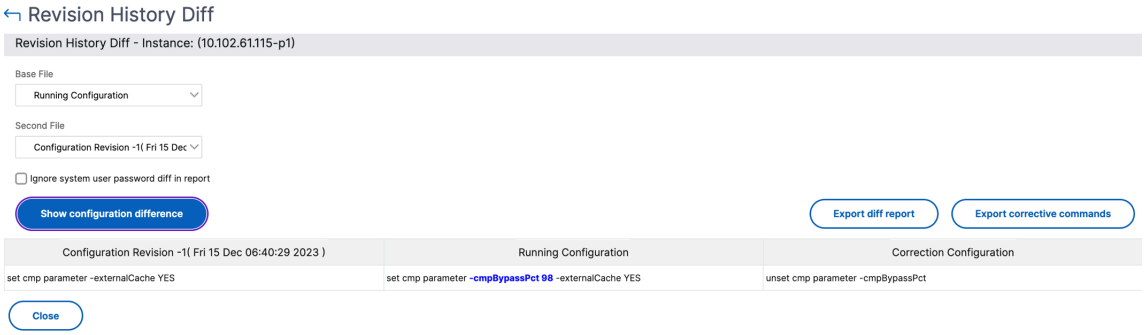


3. [リビジョン履歴の差分] ページで、比較するファイルを選択します。たとえば、[保存された構成] と [構成リビジョン-1] を比較し、[構成の違いを表示] をクリックします。



4. 次に示すように、選択したパーティション分割された NetScaler ADC インスタンスの最新の 5 つの構成ファ

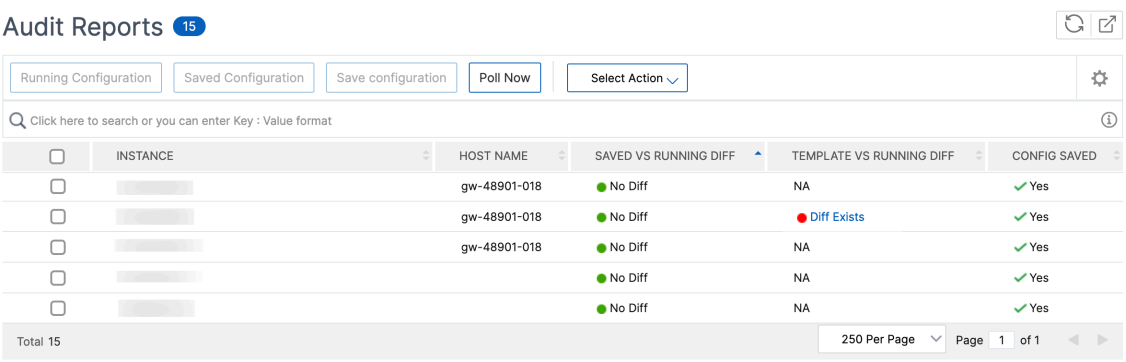
イルの違いを確認できます。修正構成コマンドを表示し、これらの修正コマンドをローカルフォルダにエクスポートすることもできます。これらの修正コマンドは、構成を目的の状態 (比較に使用されている構成ファイル) にするためにベースファイルに対して実行する必要があるコマンドです。



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構成に違いがある場合、その違いはハイパーリンクとして表示されます。ハイパーリンクをクリックすると、相違点が表示されます（存在する場合）。構成の違いとともに、修正構成も示されています。また、すべての修正コマンドをローカルフォルダにエクスポートして、設定を修正することもできます。

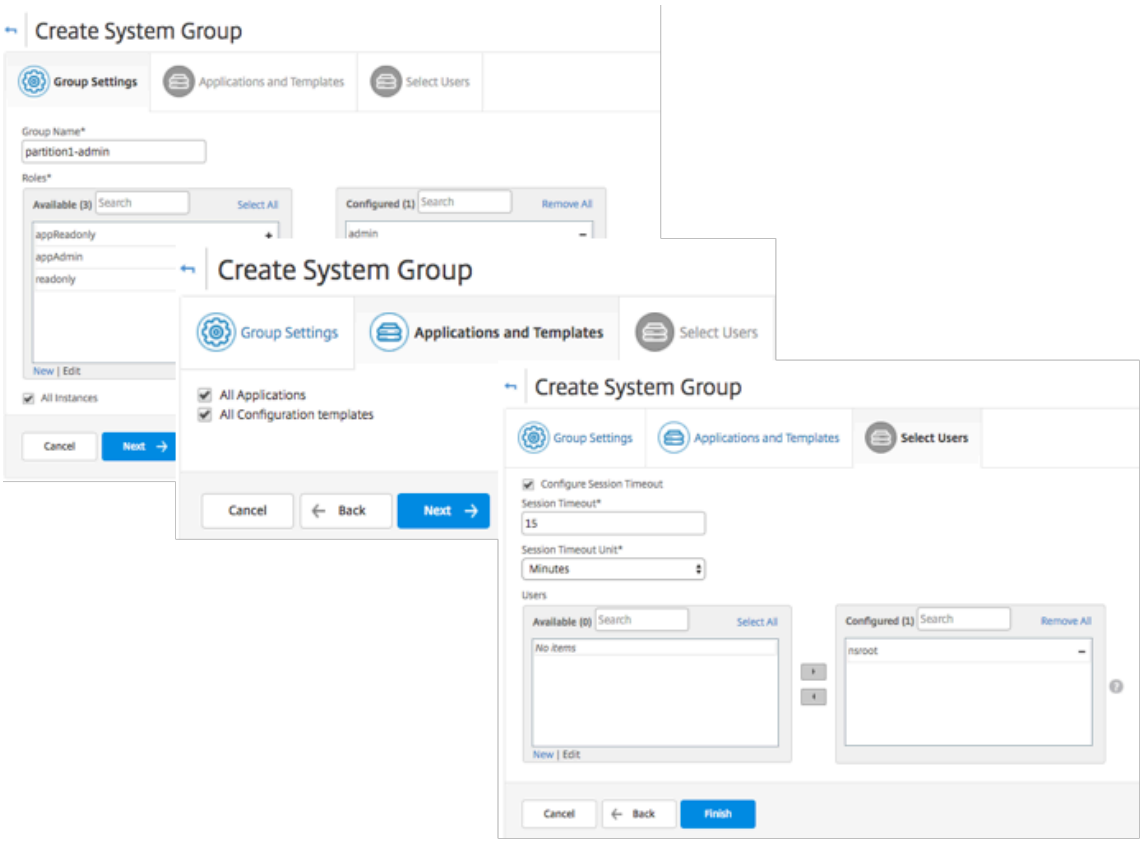
グループを作成するには、次の手順に従います。

1. [システム] > [ユーザー管理] > [グループ] に移動し、[追加] をクリックします。
2. **[** システムユーザーの作成] ページで、次の項目を指定します。

   - グループ設定タブ: グループ名とロール権限を入力します。特定のインスタンスへのアクセスを許可するには、「**All Instances**」チェックボックスをオフにし、「Select Instances」ページでインスタンスを選択します。

- 「アプリケーションとテンプレート」タブ: このグループをすべてのアプリケーションと構成テンプレートで使用できます。
- [ユーザーの選択] タブ: このグループに追加するユーザーを選択します。「**Available** 」テーブルの「**New** 」リンクをクリックすると、新しいユーザーを作成できます。必要に応じて、セッションタイムアウトを構成します。ここでは、ユーザーがアクティブな状態でいられる期間を構成できます。

3. [完了] をクリックします。



ユーザーを作成するには、次の手順に従います。

1. [システム] > [ユーザー管理] > [ユーザー] に 移動し、[追加] をクリックします。
2. **[** システムユーザーの作成] ページで、ユーザー名とパスワードを指定します。必要に応じて、外部認証を有効にすることや、セッションタイムアウトを構成することができます。
3. 「使用可能」リストのグループ名を「構成済み」リストに追加して、ユーザーをグループに割り当てます。
4. [**Create**] をクリックします。

ログアウトして、user-p1 の資格情報でログオンします。管理および監視が割り当てられた管理パーティションのみを表示、管理することができます。

NetScaler ADC インスタンスのバックアップと復元

February 6, 2024

NetScaler ADC インスタンスの現在の状態をバックアップし、後でバックアップしたファイルを使用して同じ状態に復元できます。インスタンスをアップグレードする前に、または予防的な理由により、常にインスタンスをバックアップする必要があります。安定したシステムのバックアップを使用すると、不安定になった場合に、安定した状態に復元できます。

NetScaler ADC インスタンスでバックアップおよびリストアを実行する方法は複数あります。GUI と CLI を使用して、Citrix ADC 構成を手動でバックアップおよび復元できます。Citrix ADM を使用して自動バックアップと手動復元を実行することもできます。

NetScaler ADM は、NITRO コールとセキュアシェル（SSH）プロトコルとセキュアコピー（SCP）プロトコルを使用して、管理対象 NetScaler ADC インスタンスの現在の状態をバックアップします。

NetScaler ADM は完全なバックアップを作成し、次の NetScaler ADC インスタンスタイプを復元します。

- Citrix SDX
- Citrix VPX
- Citrix MPX

詳細については、「ADC インスタンスのバックアップと復元」を参照してください。

> 注
>
> - NetScaler ADM では、NetScaler ADC 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-->
```

ディスク領域が使用できないことによる問題を回避するために、このディレクトリには最大 50 個のバックアップファイルを保存できます。

NetScaler ADC インスタンスをバックアップおよび復元するには、まず NetScaler ADM でバックアップ設定を構成する必要があります。設定を構成したら、1 つの Citrix ADC インスタンスまたは複数のインスタンスを選択して、これらのインスタンスの構成ファイルのバックアップを作成できます。必要に応じて、これらのバックアップファイルを使用して Citrix ADC インスタンスを復元することもできます。

インスタンスのバックアップ設定の構成

［インスタンスのバックアップ設定］ページでは、選択した NetScaler ADC インスタンスまたは複数のインスタンスをバックアップするための NetScaler ADM の設定を構成できます。

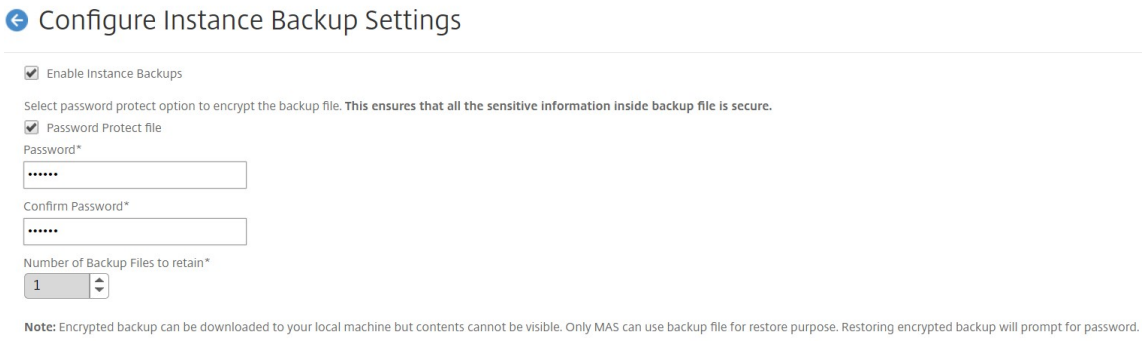
NetScaler ADM で、［システム］>［システム管理］に移動します。右側のペインの [インスタンス設定] で、**[** インスタンスバックアップ設定] を選択し、以下を指定します。

1. インスタンスバックアップを有効にする：デフォルトでは、NetScaler ADM は NetScaler ADC インスタンスのバックアップを作成するために有効になっています。インスタンスのバックアップファイルを作成しない場合は、このオプションをクリアしてください。
2. パスワード保護ファイル:(オプション) パスワード保護オプションを選択して、バックアップファイルを暗号化します。バックアップファイルを暗号化すると、バックアップファイル内のすべての機密情報が安全に保たれます。

   > 注
   >
   > 暗号化されたバックアップファイルはローカルマシンにダウンロードできますが、NetScaler ADM GUI またはテキストエディタで開くことはできません。このファイルは、Citrix ADM だけで取得して使用できます。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。

3. 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。Citrix ADC インスタンスの現在の状態のバックアップファイルを最大 50 個保持できます。デフォルトでは、バックアップファイルは 3 つです。

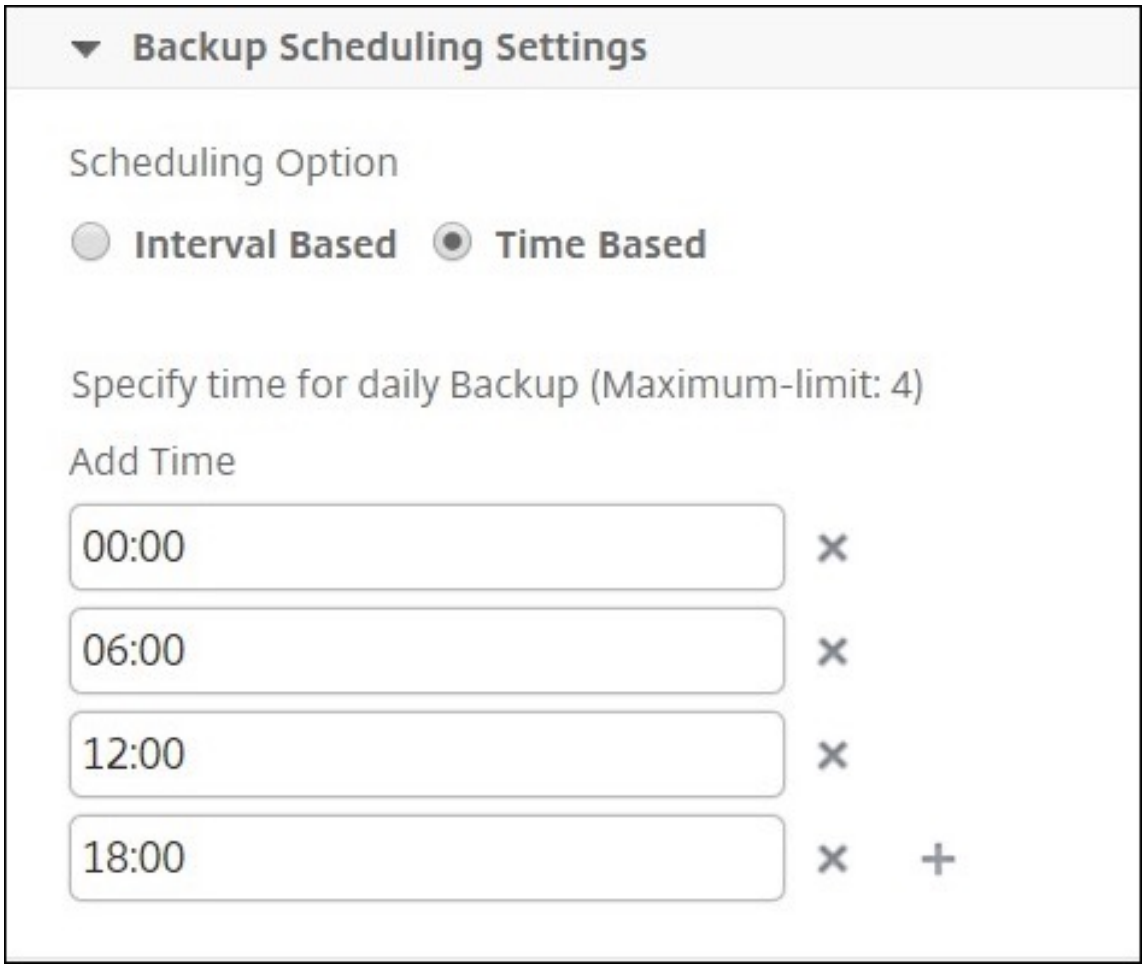
   > 注
   >
   > 各バックアップファイルには、ある程度のストレージ要件があります。要件に応じて、NetScaler ADC バックアップファイルを最適な数の NetScaler ADM に保存することをお勧めします。

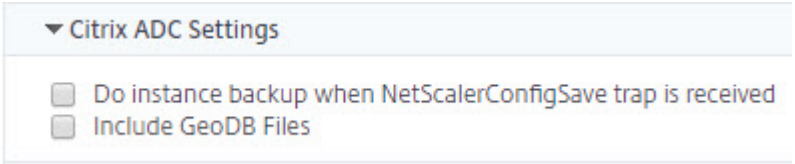
4. バックアップのスケジュール設定: (オプション) バックアップファイルの作成には 2 つのオプションがありますが、一度に使用できるオプションは 1 つだけです。

   a) デフォルトのバックアップスケジュールオプションは「間隔ベース」です。指定した間隔が経過すると、Citrix ADM にバックアップファイルが作成されます。デフォルトのバックアップ間隔は 12 時間です。

b) スケジュール・バックアップのタイプを「時間ベース」に変更することもできます。このオプションでは、バックアップが実施される時刻を「時：分」形式で指定します。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。



5. **NetScaler ADC** 設定：（オプション）デフォルトでは、NetScaler ADM は「NetScalerConfigSave」トラップを受信したときにバックアップファイルを作成しません。ただし、Citrix ADC インスタンスが Citrix ADM に「NetScalerConfigSave」トラップを送信するたびに、バックアップファイルを作成するオプションを有効にできます。Citrix ADC インスタンスは、インスタンスの構成が保存されるたびに「NetScalerConfigSave」を送信します。
6. ジオデータベースファイル:(オプション) デフォルトでは、Citrix ADM はジオデータベースファイルをバックアップしません。このオプションを有効化して、これらのファイルもバックアップファイルを作成することができます。



7. 外部転送：（オプション）NetScaler ADM では、NetScaler ADC インスタンスのバックアップファイルを外

部の場所に転送できます。

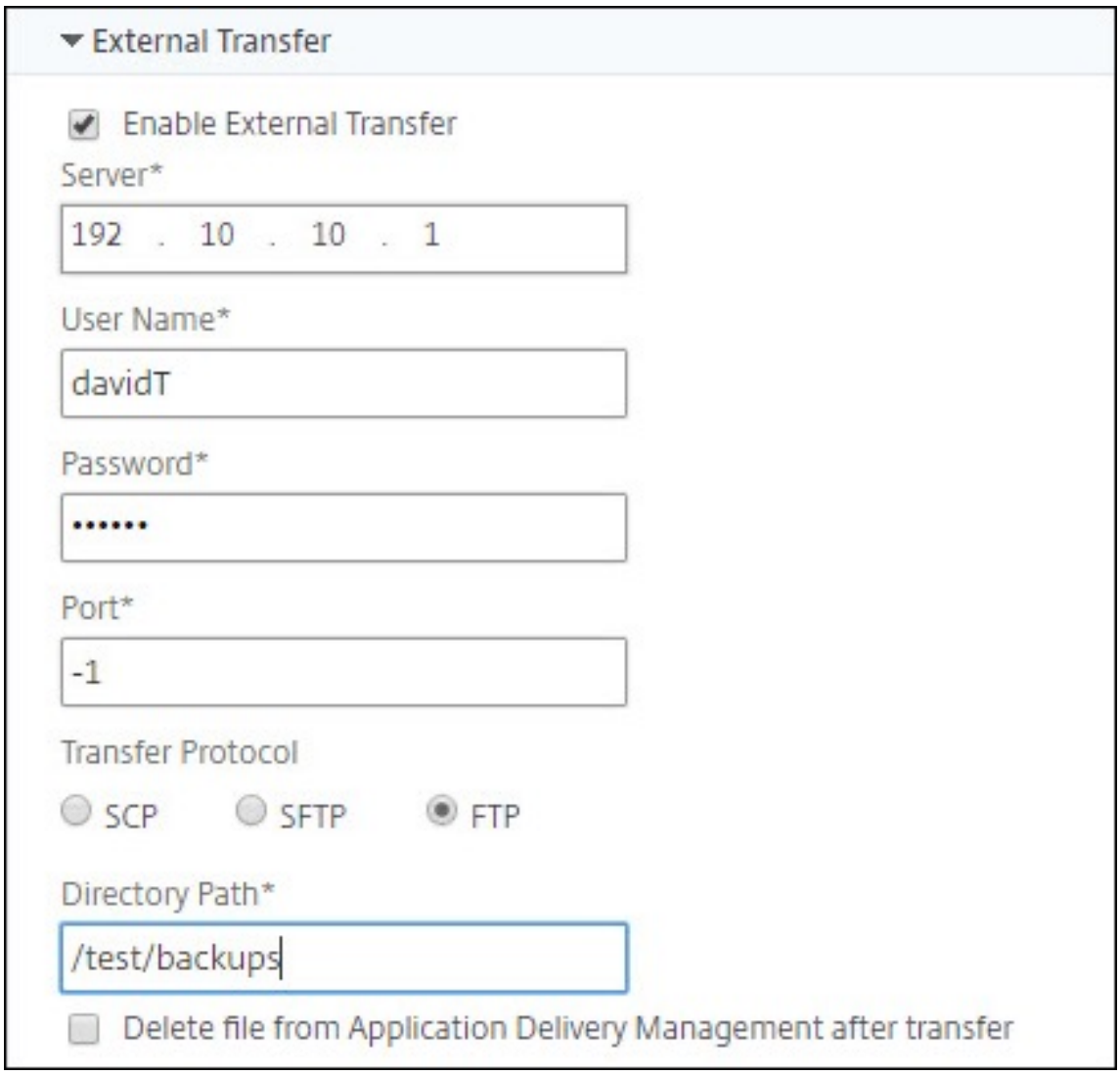
a) ロケーションの IP アドレスを指定します。

b) バックアップファイルの転送先となる外部サーバーのユーザー名とパスワードを指定します。

c) 転送プロトコルとポート番号を指定します。

d) ファイルを保存する必要があるディレクトリパスを指定できます。

e) バックアップファイルを外部サーバーに転送した後、Citrix ADM から削除することもできます。



> 注
>
> Citrix ADM は、選択した Citrix ADC インスタンスのいずれかでバックアップが失敗すると、SNMP トラップまたは Syslog 通知をそれ自体に送信します。

Citrix ADNetScaler ADM を使用して、選択した **NetScaler ADC** インスタンスのバックアップを作成する

選択した NetScaler ADC インスタンスまたは複数のインスタンスをバックアップする場合は、次のタスクを実行します。

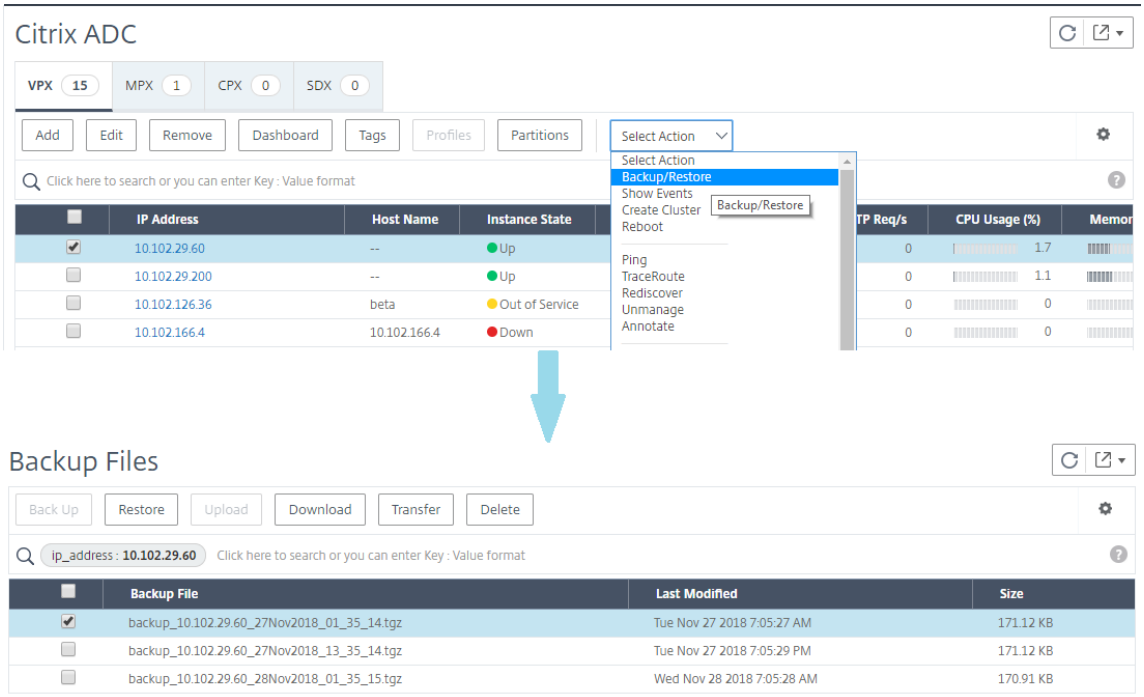
1. Citrix ADM で、［ネットワーク］> ［インスタンス］に 移動します。［インスタンス］で、画面に表示するインスタンスのタイプ（Citrix VPX など）を選択します。
2. バックアップするインスタンスを選択します。
   - MPX および VPX インスタンスの場合は、「アクションの選択」リストから「バックアップ/復元」を選択します。
   - SDX インスタンスの場合は、[バックアップ/復元] をクリックします。
3. [ファイルのバックアップ] ページで、[バックアップ] をクリックします。
4. セキュリティを強化するためにバックアップファイルを暗号化するかどうかを指定できます。パスワードを入力するか、[インスタンスバックアップ設定] ページで以前に指定したグローバルパスワードを使用できます。
5. [続行] をクリックします。

NetScaler ADM を使用して **NetScaler ADC** インスタンスを復元する

> 注:NetScaler ADC インスタンスが HA
>
> ペアになっている場合は、次の点に注意する必要があります。
>
> - バックアップファイルの作成元と同じインスタンスを復元します。たとえば、HA ペアのプライマリインスタンスからバックアップが作成されたシナリオを考えてみましょう。復元プロセス中は、プライマリインスタンスではなくなった場合でも、必ず同じインスタンスを復元してください。
> - プライマリ ADC インスタンスで復元プロセスを開始すると、プライマリインスタンスにアクセスできなくなり、セカンダリインスタンスが **STAYSECONDARY** に変更されます。プライマリインスタンスで復元プロセスが完了すると、セカンダリ ADC インスタンスは **STAYSECONDARY** モードから **ENABLED** モードに変わり、再び HA ペアの一部になります。復元プロセスが完了するまで、プライマリインスタンスでダウンタイムが発生する可能性があります。

以前に作成したバックアップファイルを使用して NetScaler ADC インスタンスを復元するには、次のタスクを実行します。

1. [ネットワーク] > **[**インスタンス] に移動し、復元するインスタンスを選択して、[バックアップを表示] をクリック します。
2. [バックアップファイル] ページで、復元する設定を含むバックアップファイルを選択し、[復元] をクリックします。



NetScaler ADM を使用して **NetScaler ADC SDX** アプライアンスを復元する

Citrix ADM では、Citrix ADC SDX アプライアンスのバックアップには次のものが含まれます。

- アプライアンスでホストされている NetScaler ADC インスタンス
- SVM SSL 証明書とキー
- Instance の削除設定（XML 形式）
- Instance のバックアップ設定（XML 形式）
- SSL 証明書ポーリング設定（XML 形式）
- SVM データベースファイル
- SDX 上に存在するデバイスの NetScaler ADC 構成ファイル
- NetScaler ADC ビルドイメージ
- NetScaler ADC XVA イメージ。これらのイメージは次の場所に保存されます。
  `/var/mps/sdx_images/`
- SDX 単一バンドルイメージ（SVM+XS）
- サードパーティのインスタンスイメージ（プロビジョニングされている場合）

NetScaler ADC 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する必要があります。アプライアンスの復元中に、現在の構成全体は削除されます。

別の NetScaler ADC SDX アプライアンスのバックアップを使用して NetScaler ADC SDX アプライアンスをリストアする場合は、復元プロセスを開始する前に、ライセンスを追加し、バックアップファイル内の設定と一致するようにアプライアンスの管理サービスのネットワーク設定を構成してください。

バックアップされた Citrix ADC SDX プラットフォームのバリアントが、復元しようとしているものと同じであることを確認してください。異なるプラットフォーム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、バックアップしたバージョンが RMA バージョンと同じかそれ以上であることを確認してください。

バックアップしたファイルから SDX アプライアンスを復元するには:

1. Citrix ADM GUI で、[ネットワーク**] > [**インスタンス**] > [Citrix ADC**] に移動します。
2. [バックアップ**/**復元] をクリックします。
3. 復元したい同じインスタンスのバックアップファイルを選択します。
4. 「バックアップを再パッケージ化」をクリックします。

   SDX アプライアンスをバックアップすると、ネットワーク帯域幅とディスク容量を節約するために、XVA ファイルとイメージは別々に保存されます。そのため、SDX アプライアンスを復元する前に、バックアップしたファイルを再パッケージする必要があります。

   バックアップファイルを再パッケージすると、SDX アプライアンスを復元するためにバックアップされたすべてのファイルが一緒に含まれます。再パッケージされたバックアップファイルにより、SDX アプライアンスが正常に復元されます。
5. 再パッケージするバックアップファイルを選択し、[**Restore**] をクリックします。

セカンダリ **NetScaler ADC** インスタンスへのフェイルオーバーを強制する

February 6, 2024

たとえば、プライマリの Citrix Application Delivery Controller（ADC）インスタンスを交換またはアップグレードする必要がある場合は、強制的にフェイルオーバーを実行する必要があります。プライマリインスタンス、セカンダリインスタンスのいずれからでもフェ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。

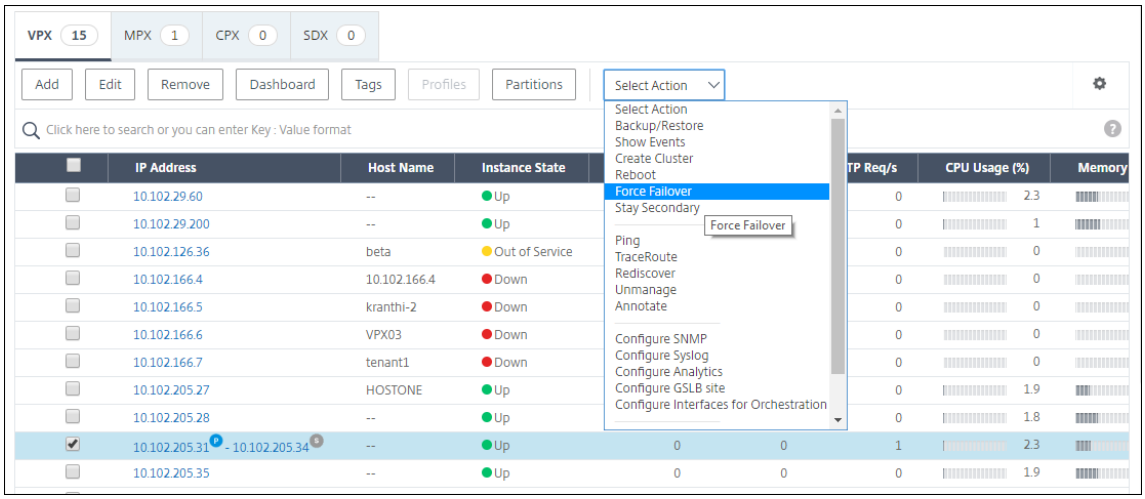
- セカンダリインスタンスが無効または非アクティブである。セカンダリインスタンスが非アクティブの場合、状態が UP になるまで待ってからフェールオーバーを強制してください。
- セカンダリを維持するようにセカンダリインスタンスが構成されている。

NetScaler ADC インスタンスは、強制フェールオーバーコマンドを実行したときに潜在的な問題を検出すると、警告メッセージを表示します。メッセージには警告の要因に関する情報が含まれており、手順を進める前に確認が求められます。

プライマリインスタンスまたはセカンダリインスタンスでフェールオーバーを強制できます。

Citrix ADNetScaler ADM を使用してセカンダリ **NetScaler ADC** インスタンスにフェイルオーバーを強制するには:

1. Citrix Application Delivery Management（ADM）で、[ネットワーク] > [インスタンス] > **[****Citrix ADC**] > [**VPX**] タブに移動し、インスタンスを選択します。
2. 選択したインスタンスの種類にリストされているインスタンスから、HA セットアップを構成するインスタンスを選択します。
3. 「アクション」メニューから、「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。

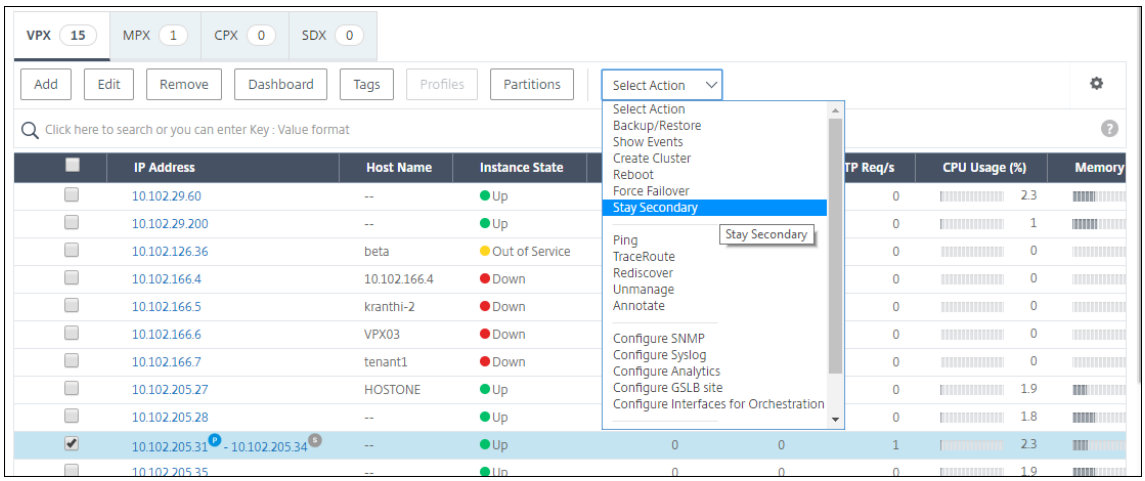
たとえば、プライマリノードをアップグレードする必要があり、アップグレード処理に数秒かかるとします。アップグレード中、プライマリノードは数秒間ダウンしますが、セカンダリノードに処理を引き継がせたくありません。セカンダリノードでプライマリノードの障害を検出しても、引き続きセカンダリノードとして稼働するようにしたいと考えています。

セカンダリノードを強制的にセカンダリのまま維持すると、プライマリノードがダウンしても、セカンダリのまま維持されます。HA ペアの一方のノードのステータスをセカンダリのまま強制的に維持すると、そのノードは、HA 状態マシン遷移には参加しません。ノードのステータスは、STAYSECONDARY として表示されます。

> 注
>
> システムをセカンダリのまま強制的に維持する場合、その強制を実施するプロセスは、伝播も同期もされません。コマンドを実行するノードのみが対象となります。

NetScaler ADM を使用してセカンダリ **NetScaler ADC** インスタンスをセカンダリとして保持するように構成するには:

1. Citrix Application Delivery Management（ADM）で、[ネットワーク] > [インスタンス] > **[**Citrix ADC**] > [**VPX**] タブに移動し、インスタンスを選択します。
2. 選択したインスタンスの種類にリストされているインスタンスから、HA セットアップを構成するインスタンスを選択します。
3. 「アクション」メニューから「セカンダリーを維持」を選択します。
4. [**Yes**] をクリックして、「Stay Secondary」アクションの実行を確定します。



インスタンスグループの作成

February 6, 2024

インスタンスグループを作成するには、最初にすべての Citrix アプリケーション Delivery Controller（ADC）インスタンスを Citrix アプリケーションデリバリー管理（ADM）に追加する必要があります。インスタンスを正常に追加した後で、デバイ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。インスタンスグループを作成することによって、グループ化されたすべてのインスタンスに対して、アップグレード、バックアップ、復元などの操作を同時に実行できます。各インスタンス上で個別に操作を実行する必要はありません。

Citrix ADM を使用してインスタンスグループを作成するには**:**

1. NetScaler ADM で、［ネットワーク］>［インスタンスグループ］の順に選択し、［追加］をクリックします。
2. インスタンスグループに名前を付け、リストからインスタンスファミリーを選択します。
3. インスタンスファミリーメニューからインスタンスタイプを選択します。
4. [インスタンスを選択] をクリックし、表示されるウィンドウからインスタンスを選択します。
5. ［作成］をクリックします。

複数の **Citrix VPX** インスタンスの再検出

February 6, 2024

Citrix Application Delivery Management（ADM）セットアップで複数の Citrix VPX インスタンスを再検出できるようになりました。以前は、再検出できた Citrix VPX インスタンスは 1 つだけでした。複数の Citrix VPX インスタンスの最新の状態と構成を確認したい場合は、それらのインスタンスを再検出できます。NetScaler ADM サーバーはすべての Citrix VPX インスタンスを再検出し、Citrix Application Delivery Controller（ADC）インスタンスに到達可能かどうかを確認します。

複数の **Citrix VPX** インスタンスを再検出するには:

1. Web ブラウザで、Citrix ADM サーバーの IP アドレス（たとえば、http://192.168.100.1）を入力します。
2. ［**User Name**］と ［**Password**］の各フィールドに管理者の資格情報を入力します。デフォルトの管理者の資格情報は nsroot と nsroot です。
3. [ネットワーク] > [インスタンス] > [**NetScaler ADC**] > [**VPX**] タブに移動し、再検出するインスタンスを選択します。
4. **[** アクションの選択**]** メニューで、[再検出] をクリックします。
5. 再検出ユーティリティを実行するための確認メッセージが表示されたら、[はい] をクリックします。

   各 Citrix VPX インスタンスの再検出の進行状況が画面に表示されます。

インスタンスの管理解除

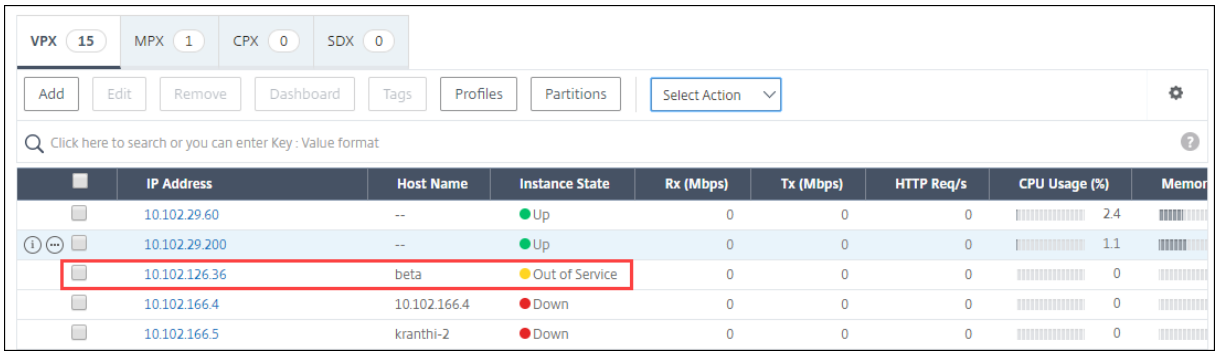
February 6, 2024

Citrix Application Delivery Management（ADM）とネットワーク内のインスタンス間の情報交換を停止したい場合は、インスタンスを管理解除できます。

インスタンスの管理を解除するには、次の手順に従います。

[ネットワーク] > [インスタンス] > **[**Citrix ADC**] > [VPX] タブに移動します。インスタンスのリストで、インスタンスを右クリックして [**UnManage**] を選択するか、インスタンスを選択し、[Select **Action]** リストから [**UnManage**] を選択します。

次の図に示すように、選択したインスタンスのステータスが [**Out of Service**] に変わります。



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

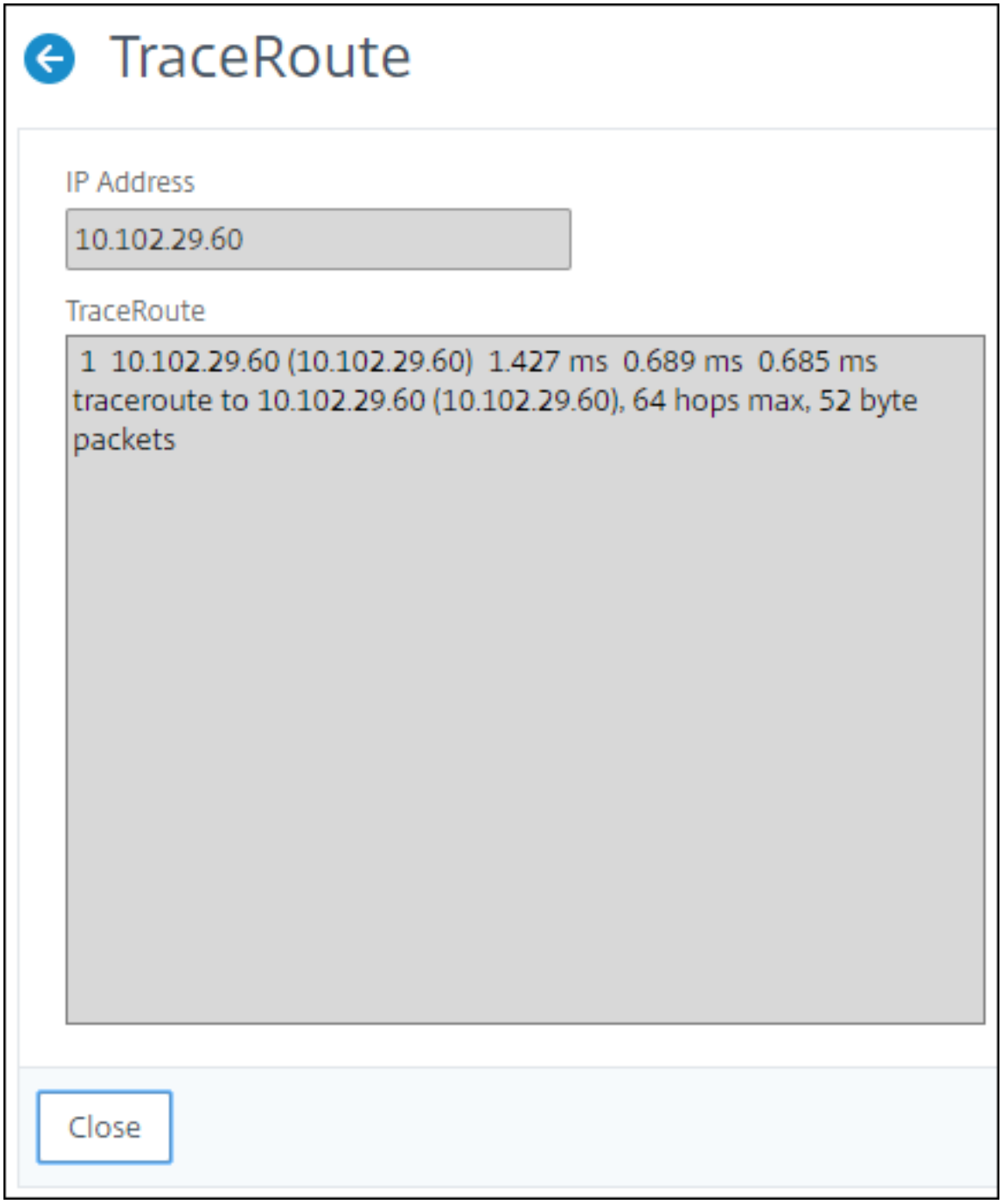
Citrix Application Delivery Management（ADM）からインスタンスへのパケットのルートをトレースすることで、インスタンスに到達するために必要なホップ数などの情報を確認できます。Traceroute では、ソースから宛先までのパケットのパスがトレースされます。これには、ルート内の各エンティティのホスト名と IP アドレスと共に、ネットワークホップの一覧が表示されます。

また、Traceroute では、あるホップから別のホップへパケットが移動するのにかかる時間が記録されます。パケットの転送に中断があった場合は、traceroute によって、問題が存在する場所が示されます。

インスタンスのルートをトレースするには:

1. Citrix ADM で、[ネットワーク] > [インスタンス] > **[**Citrix ADC**] > [**VPX**] タブに移動します。
2. インスタンスのリストで、インスタンスを右クリックして [**TraceRoute**] を選択するか、インスタンスを選択し、[アクションの選択] メニューから [**TraceRoute**] をクリックします。

［TraceRoute］メッセージボックスに、インスタンスへのルート、および各ホップでかかった時間（ミリ秒単位）が表示されます。



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、そのインスタンスがトラップまたはイベントを受信するためのトラップ宛先として暗黙的に追加します。

イベントは、管理対象 Citrix ADC インスタンスでのイベントまたはエラーの発生を表します。たとえば、システム障害や構成の変更があった場合、イベントが生成され、NetScaler ADM サーバーに記録されます。NetScaler ADM で受信したイベントは、［イベントの概要］ページ（［ネットワーク］> ［イベント］）に表示され、すべてのアクティブなイベントは［イベントメッセージ］ページ（［ネットワーク］> ［イベント］> ［イベントメッセージ］）に表示されます。

Citrix 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さまざまな重大度のアラームを生成し、メッセージとして表示します。メッセージの中には、早急な対応が必要なものもあります。たとえば、システム障害のイベント重要度は「Critical」に分類され、早急な対応が必要になります。

特定のイベントを監視するように規則を構成できます。ルールにより、Citrix ADC インフラストラクチャ全体で生成される多数のイベントを簡単に監視できます。

特定の条件で規則を構成し、規則にアクションを割り当てることで、一連のイベントにフィルターを適用できます。生成されたイベントが規則のフィルター条件を満たす場合、規則に割り当てられたアクションが実行されます。フィルタを作成できる条件は、重大度、NetScaler ADC インスタンス、カテゴリ、障害オブジェクト、構成コマンド、メッセージです。

また、イベントについて、そのイベントが解決されるまで特定の間隔で通知を複数回表示するように設定することもできます。追加の措置として、件名とユーザーメッセージを指定して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も可能です。

イベントダッシュボードの使用

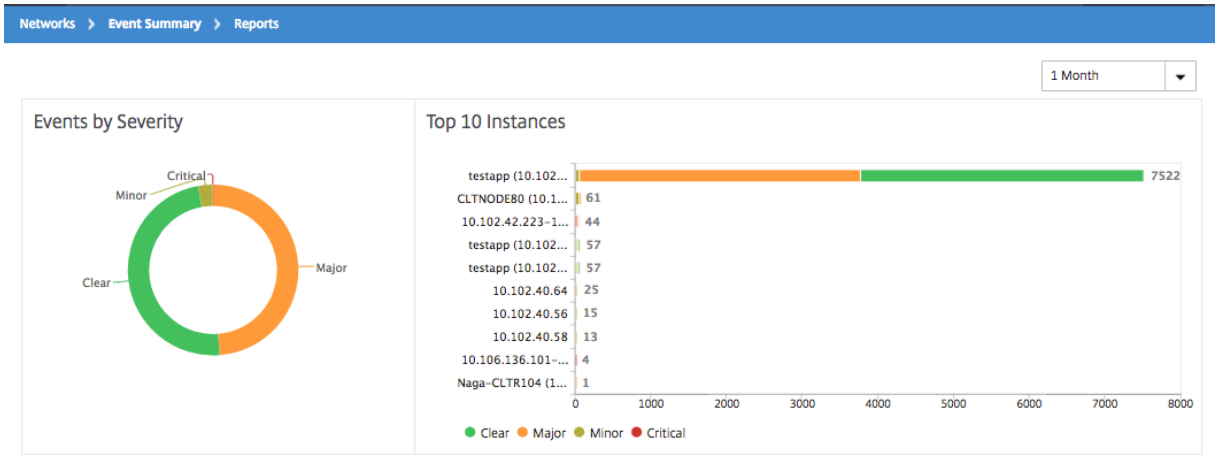
February 6, 2024

ネットワーク管理者は、Citrix Application Delivery Controller（ADC）インスタンスの構成変更、ログイン条件、ハードウェア障害、しきい値違反、エンティティ状態の変化などの詳細を、特定のインスタンスでのイベントとその重大度とともに表示できます。NetScaler Application Delivery Management（ADM）のイベントダッシュボードを使用すると、すべての NetScaler ADC インスタンスの重要なイベントの重大度について生成されたレポートを表示できます。

イベント・ダッシュボードで詳細を表示するには、次の手順に従います。

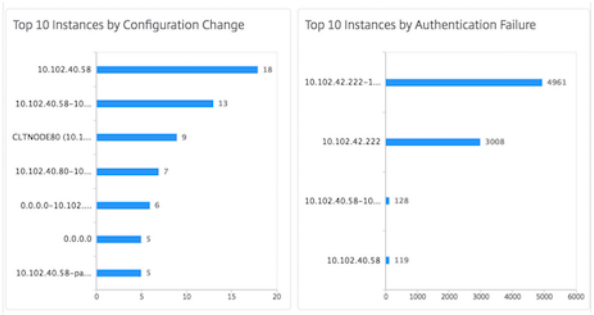
[ネットワーク] > [イベント] > [レポート] に移動します。

ダッシュボードの［Top 10 Devices］グラフには、各インスタンスで生成されたイベントの数に基づき、上位 10 個のインスタンスが表示されます。グラフのインスタンスをクリックすると、イベントの重要度についてさらに詳しく確認できます。

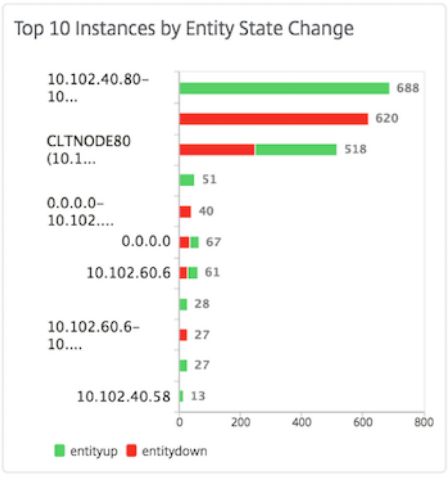


Citrix ADC インスタンスタイプ（[ネットワーク] > [イベント] > [レポート] > [NetScaler/NetScaler **SDX/NetScaler SD**-WANWO]）に移動すると詳細が表示され、次の内容が表示されます。

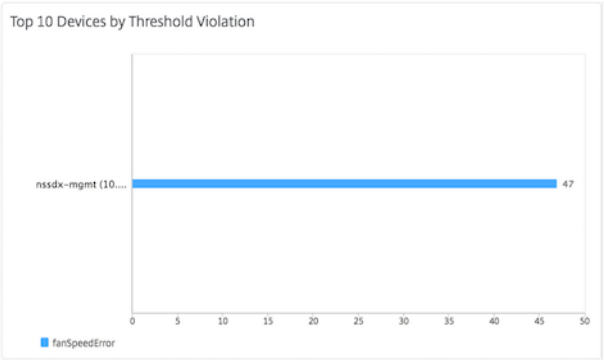
- ハードウェアエラー件数上位 10 デバイス
- 構成変更件数上位 10 デバイス
- 認証エラー件数上位 10 デバイス



- 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

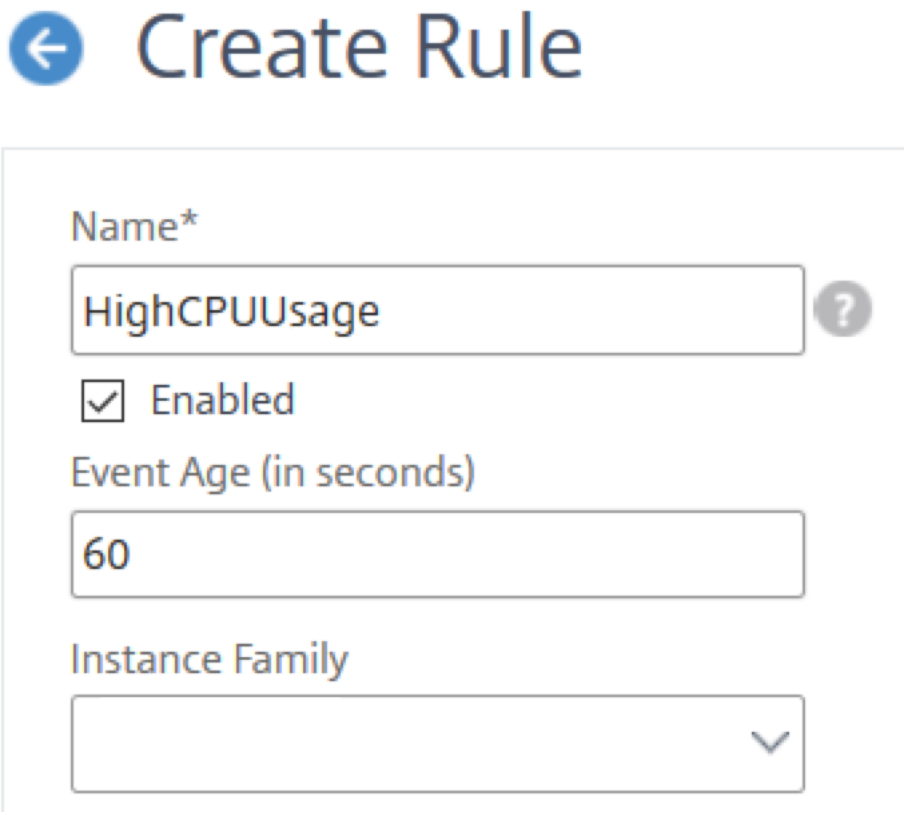
イベントの経過時間オプションを設定して、時間間隔 (秒単位) を指定できます。NetScaler ADM は、設定された期間までアプライアンスを監視し、イベントの経過時間が設定された期間を超えた場合にのみイベントを生成します。

> 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と、エンティティ名、ステータスの変更、時間などの詳細が記載された電子メール通知が届きます。

NetScaler ADM でイベントの経過期間を設定するには:

1. Citrix ADM で、［ネットワーク］>［イベント］>［ルール］に移動し、［追加］をクリックします。
2. ［**Create Rule**］ページで規則パラメーターを設定します。
3. イベント期間を秒数で指定します。



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、[Sever **ity]** セクションでそれぞれの重大度 を設定してください。上記の例では、エンティティアップ、エンティティダウン、およびエンティティトラップを選択します。

イベントフィルタをスケジュールする

February 6, 2024

ルールのフィルターを作成した後、生成されたイベントがフィルター条件を満たすたびに Citrix Application Delivery Management（ADM）サーバーに通知を送信させたくない場合は、毎日、毎週、または毎月などの特定の時間間隔でのみフィルターがトリガーされるようにスケジュールできます。

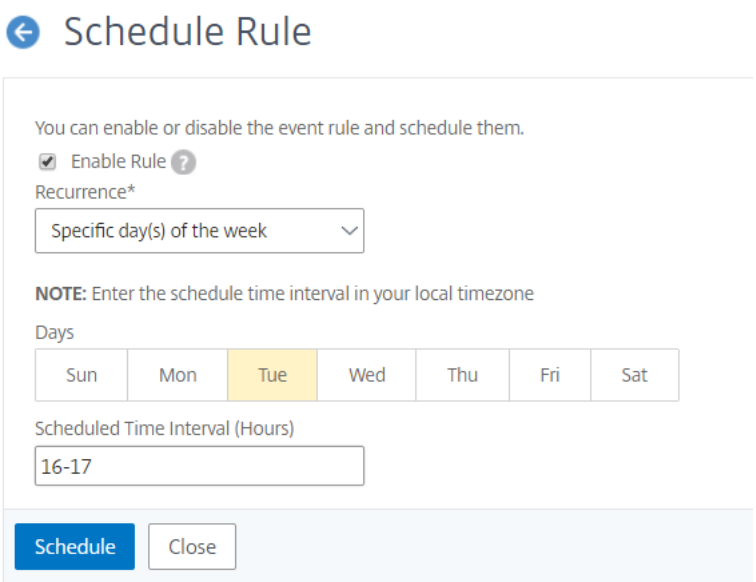
たとえば、インスタンスの複数のアプリケーションを対象に、異なるタイミングでシステムメンテナンスのスケジュールを指定している場合、それらのインスタンスによって複数のアラームが生成される可能性があります。

これらのアラームのフィルターを構成し、これらのフィルターの電子メール通知を有効にした場合、Citrix ADM が

これらのトラップを受信すると、サーバーは大量の電子メール通知を送信します。このようなサーバーによるメール通知の送信を特定期間に限定するには、フィルターにスケジュールを指定します。

NetScaler ADM を使用してフィルタをスケジュールするには:

1. Citrix ADM で、［ネットワーク］>［イベント］>［ルール］に移動します。
2. スケジュールを指定するフィルターの対象となっている規則を選択し、［**View Schedule**］をクリックします。
3. ［**Scheduled Rule**］ページの［**Schedule**］をクリックして、次のパラメーターを指定します。
   - **Enable Rule** - このチェックボックスをオンにして、スケジュール指定対象のイベント規則を有効にします。
   - **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) —ルールをスケジュールする時間 (24 時間形式を使用)。
4. ［**Schedule**］をクリックします。



イベントに対して繰り返し電子メール通知を設定する

February 6, 2024

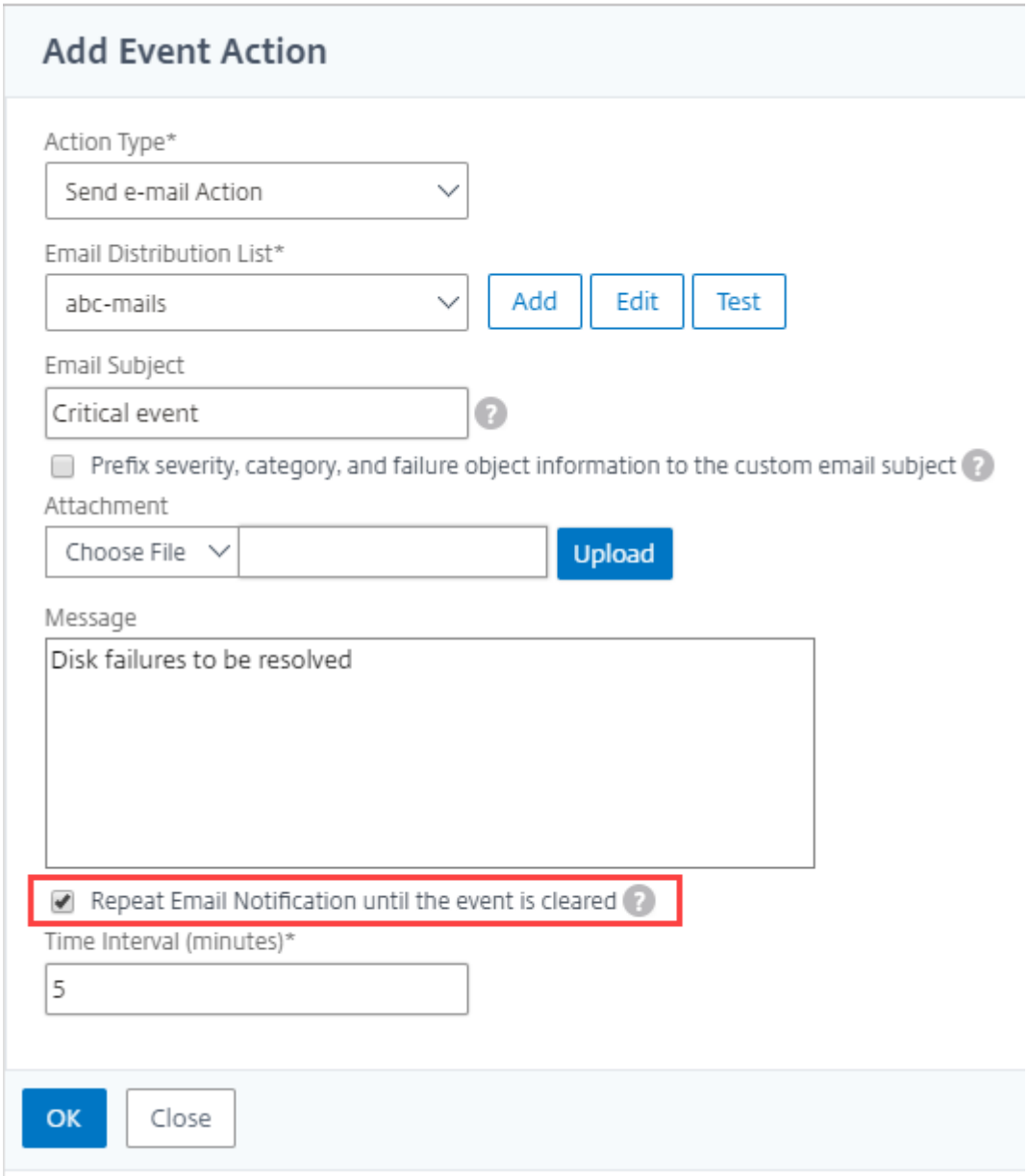
すべての重大なイベントに対応し、重要なメール通知を見落とさないために、指定した条件を満たすイベント規則に関して、連続してメール通知を送信するように指定できます。たとえば、ディスクエラーを伴うインスタンスに対するイベント規則を作成し、問題が解決するまで通知するようにする場合、それらのイベントに関して連続メール送信を指定できます。

これらのメール通知は、受信者が通知を見たことを確認するか、イベント規則が解除されるまで、定義された間隔で繰り返し送信されます。

> 注
>
> イベントを自動的にクリアできるのは、同等の「クリア」トラップが設定され、Citrix Application Delivery Controller（ADC）インスタンスから送信された場合のみです。
>
> イベントを手動でクリアするには、次の操作を行います。
>
> - [ネットワーク] **>** [イベント] **>** [イベント概要] に移動し、カテゴリを選択し、カテゴリ内のイベントを選択して [クリア] をクリックします。
> - または、[ネットワーク] **>** [イベント] **>** [イベントメッセージ] に移動します。インスタンスタイプを選択し、下のグリッドからイベントを選択し、[**Clear**] をクリックします。

NetScaler ADM から繰り返し電子メール通知を設定するには：

1. Citrix Application Delivery Management（ADM）で、［ネットワーク］>［イベント］>［ルール］に移動し、［追加］をクリックしてルールを作成します。
2. ［**Create Rule**］ページで規則パラメーターを設定します。
3. 「イベントルールアクション」で、「アクションを追加」をクリックします。次に、**** アクションタイプドロップダウンリストから「電子メールを送信アクション ** 」を選択し、電子メール配布リストを選択します。
4. 構成した規則と受信イベントが適合したときに、カスタマイズした件名とユーザーメッセージを追加し、添付ファイルをメールにアップロードすることもできます。
5. ［**Repeat Email Notification until the event is cleared**］チェックボックスをオンにします。



イベントを抑制する

February 6, 2024

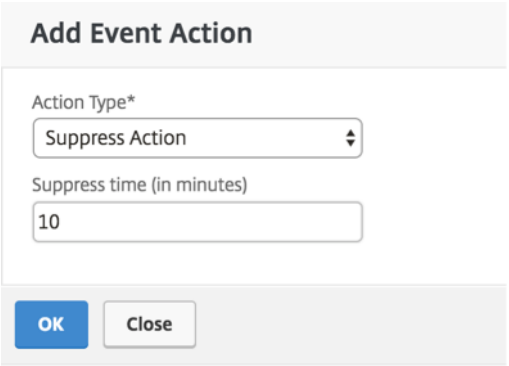
Suppress Action イベントアクションを 選択すると、イベントを抑制またはドロップする期間を分単位で設定できます。最短で 1 分間イベントを非表示にできます。

NetScaler ADM を使用してイベントを抑制するには:

1. Citrix Application Delivery Management（ADM）で、［ネットワーク］>［イベント］>［ルール］に移動

します。［追加］をクリックします。

2. 規則を作成するために必要なすべてのパラメーターを指定します。
3. ［**Event Rule Actions**］の［**Add Action**］をクリックして、イベントの通知アクションを割り当てます。
4. 「イベントアクションの追加」ページで、「アクションタイプ」ドロップダウンから「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

2018 年 5 月 24 日

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、Citrix アプリケーション Delivery Controller（ADC）インフラストラクチャ全体で生成される多数のイベントを簡単に監視できます。

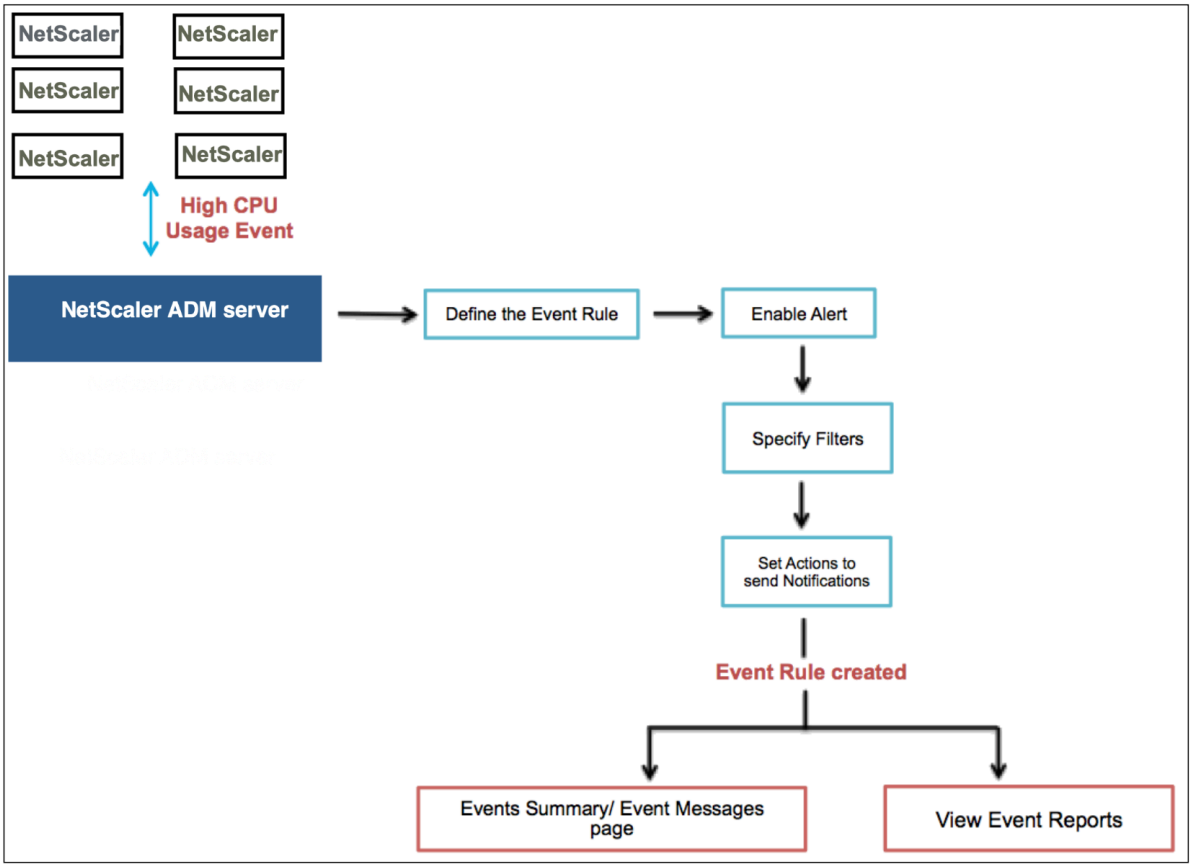
特定の条件で規則を構成し、規則にアクションを割り当てることで、一連のイベントにフィルターを適用できます。生成されたイベントが規則のフィルター条件を満たす場合、規則に割り当てられたアクションが実行されます。フィルタを作成できる条件は、重大度、NetScaler ADC インスタンス、カテゴリ、障害オブジェクト、構成コマンド、メッセージです。

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。
- **SMS** 送信アクション: フィルター条件に一致するイベントごとにショートメッセージサービス (SMS) メッセージを送信します。
- **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**:** ジョブの実行は、指定したフィルター条件に一致するイベントに対して行われます。

- 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。

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、件名、ユーザーメッセージ、添付ファイルを指定してメールをカスタマイズすることも可能です。



たとえば、管理者は、特定の NetScaler ADC インスタンスの「高い CPU 使用率」イベントを監視して、NetScaler ADC インスタンスの停止につながる可能性があるとします。インスタンスをモニターする規則を作成して、「高 CPU 使用率」カテゴリのイベントが発生した場合にメール通知を送信するアクションを指定できます。イベントが生成されるたびに通知が行われないように、午前 11 時から午後 11 時までなどの特定の時間にこの規則を実行するようスケジュール設定します。

イベント規則の構成では以下の作業を行います。

1. 規則を定義する
2. 規則の検出対象イベントの重要度を選択する
3. イベントのカテゴリを指定する
4. ルールを適用する NetScaler ADC インスタンスの指定
5. エラーオブジェクトを指定する
6. 追加のフィルターを指定する
7. 規則でイベントが検出された場合に実行するアクションを指定する

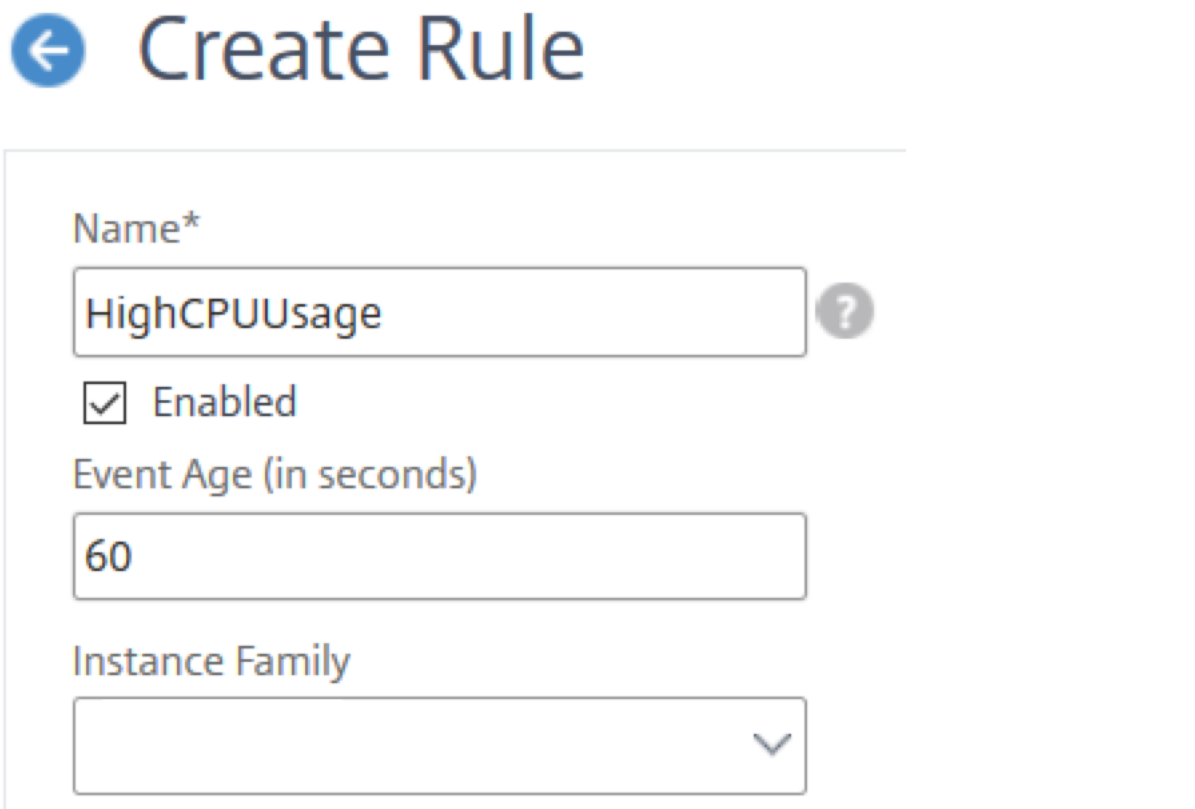
ステップ **1-**イベントルールを定義する

[ネットワーク] > [イベント] > [ルール] に移動し、[追加] をクリックします。ルールを有効にする場合は、「ルールを有効にする」チェックボックスを選択します。

イベント経過時間オプションを設定して、Citrix Application Delivery Management（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。

上記の例に基づいて、Citrix ADC インスタンスで「CPU 使用率が高い」イベントが 60 秒以上発生するたびに、電子メールで通知を受け取りたい場合があります。イベントの経過時間を 60 秒に設定すると、Citrix ADC インスタンスで「CPU 使用率が高い」イベントが 60 秒以上発生するたびに、イベントの詳細が記載された電子メール通知が届きます。

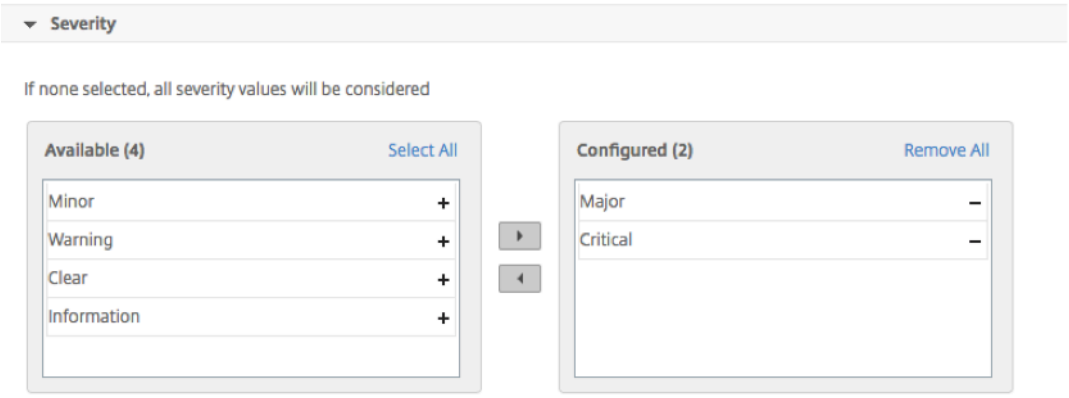


イベントルールをデバイスファミリーでフィルタリングして、Citrix ADM がイベントを受信する Citrix ADC インスタンスを追跡することもできます。

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。

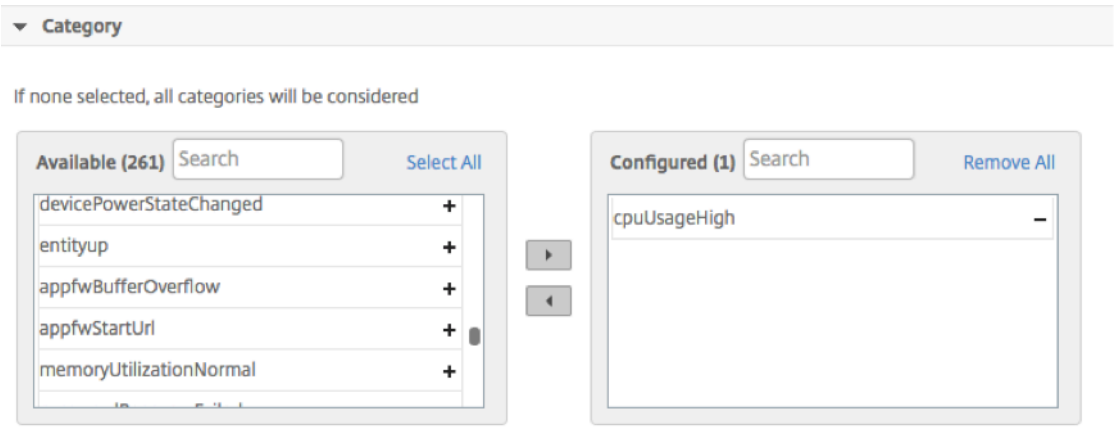


> 注
>
> 汎用イベントとエンタープライズ固有のイベント双方に対して、重要度を構成できます。NetScaler ADM で管理されている NetScaler ADC インスタンスのイベントの重要度を変更するには、［ネットワーク］>［イベント］>［イベント設定］に移動します。イベントの重大度を設定する カテゴリ を選択し、[Configure Severity] をクリックします。新しい重大度レベルを割り当てて、[**OK**] をクリックします。

手順 **3 -** イベントカテゴリを指定する

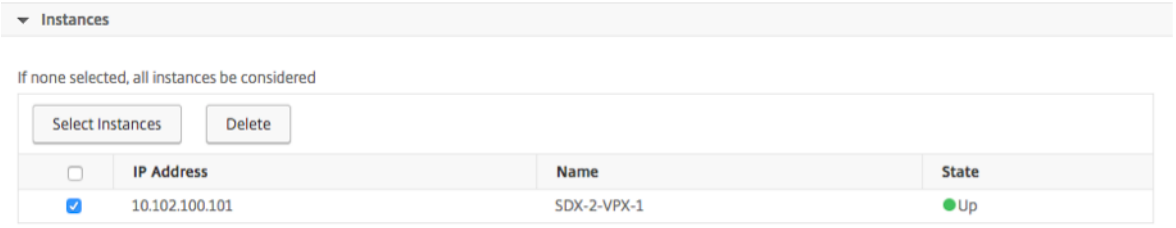
NetScaler ADC インスタンスによって生成されるイベントのカテゴリを指定できます。すべてのカテゴリは、NetScaler ADC インスタンスに作成されます。これらのカテゴリは、イベントルールの定義に使用できる NetScaler ADM にマッピングされます。考慮するカテゴリを選択し、「使用可能」(Available) テーブルから「構成済み」(構成済み) テーブルに移動します。

先ほどの例では、表示されるテーブルで［cpuUsageHigh］をイベントカテゴリとして選択します。



ステップ **4-NetScaler ADC** インスタンスの指定

イベントルールを定義する NetScaler ADC インスタンスの IP アドレスを選択します。「インスタンス」セクションで、「インスタンスを選択」をクリックします。[**Select Instances]** ページで、インスタンスを選択し、[**Select**] をクリックします。

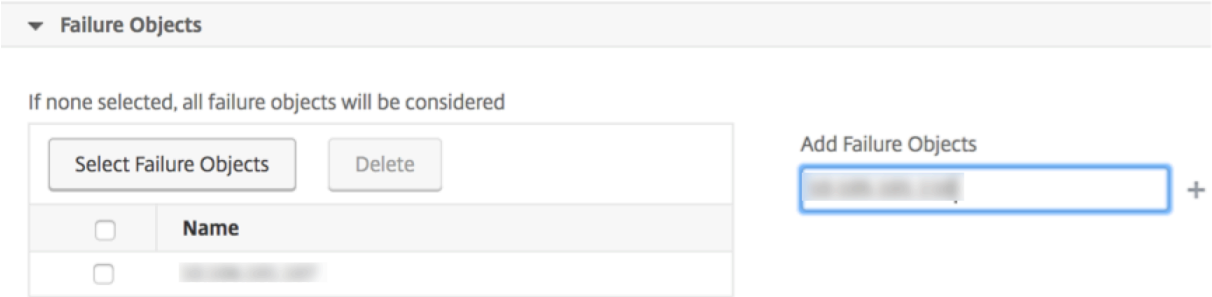


ステップ **5-**障害オブジェクトの選択

エラーオブジェクトを表示されるボックスの一覧から選択するか、イベントが生成されるエラーオブジェクトを追加することができます。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。

エラーオブジェクトはイベントの処理方法に影響を与え、通知されたとおりの問題がエラーオブジェクトに反映されるようにします。このオブジェクトを使用すると、単にイベントをありのままレポートするのではなく、問題を素早く突き止めてエラーの原因を特定することができます。たとえば、ユーザーのログインに問題が生じた場合、エラーオブジェクトはユーザー名またはパスワード（「nsroot」など）になります。

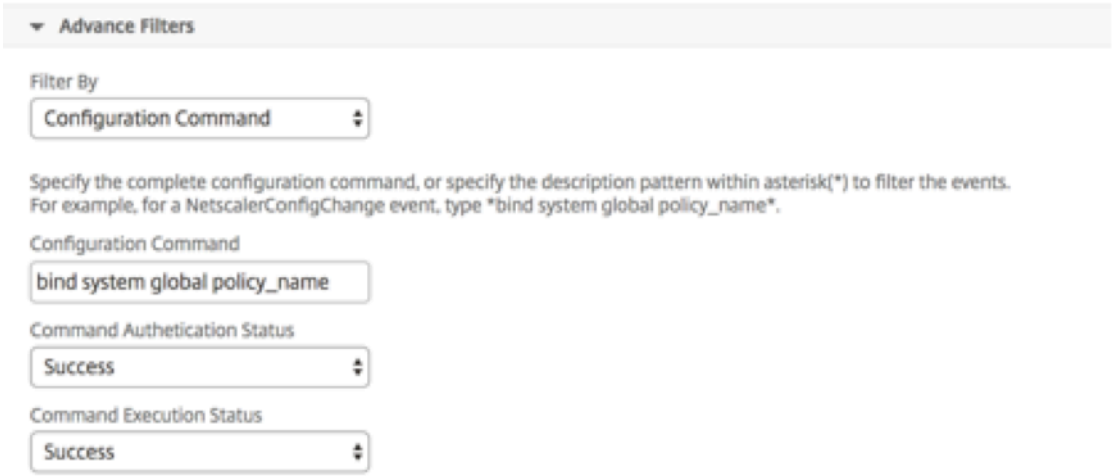
このリストには、すべてのしきい値関連のイベントではカウンター名、すべてのエンティティ関連のイベントではエンティティ名、証明書関連のイベントでは証明書名などが含まれます。



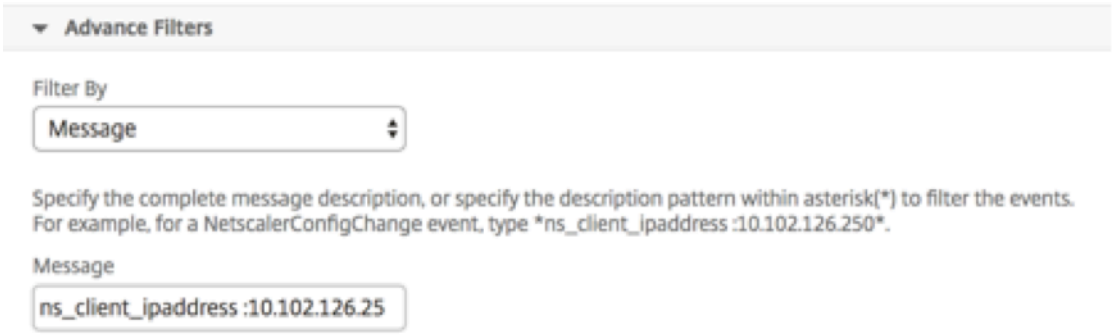
ステップ **6-**追加のフィルターを指定する

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-設定コマンド全体を指定するか、アスタリスク (*) 内の説明パターンを指定してイベントをフィルタリングできます。コマンドに加えて、コマンドの認証状態や実行状態によりイベントをさらに絞り込むこともできます。たとえば、NetScalerConfigChange イベントの場合は、「* バインドシステムグローバルポリシー名 *」と入力します。



- メッセージ-メッセージの完全な説明を指定するか、アスタリスク (*) 内の説明パターンを指定してイベントをフィルタリングできます。
  たとえば、NetscalerConfigChange イベントの場合は、「*ns_クライアント_ipaddress: 10.102.126.250*」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。

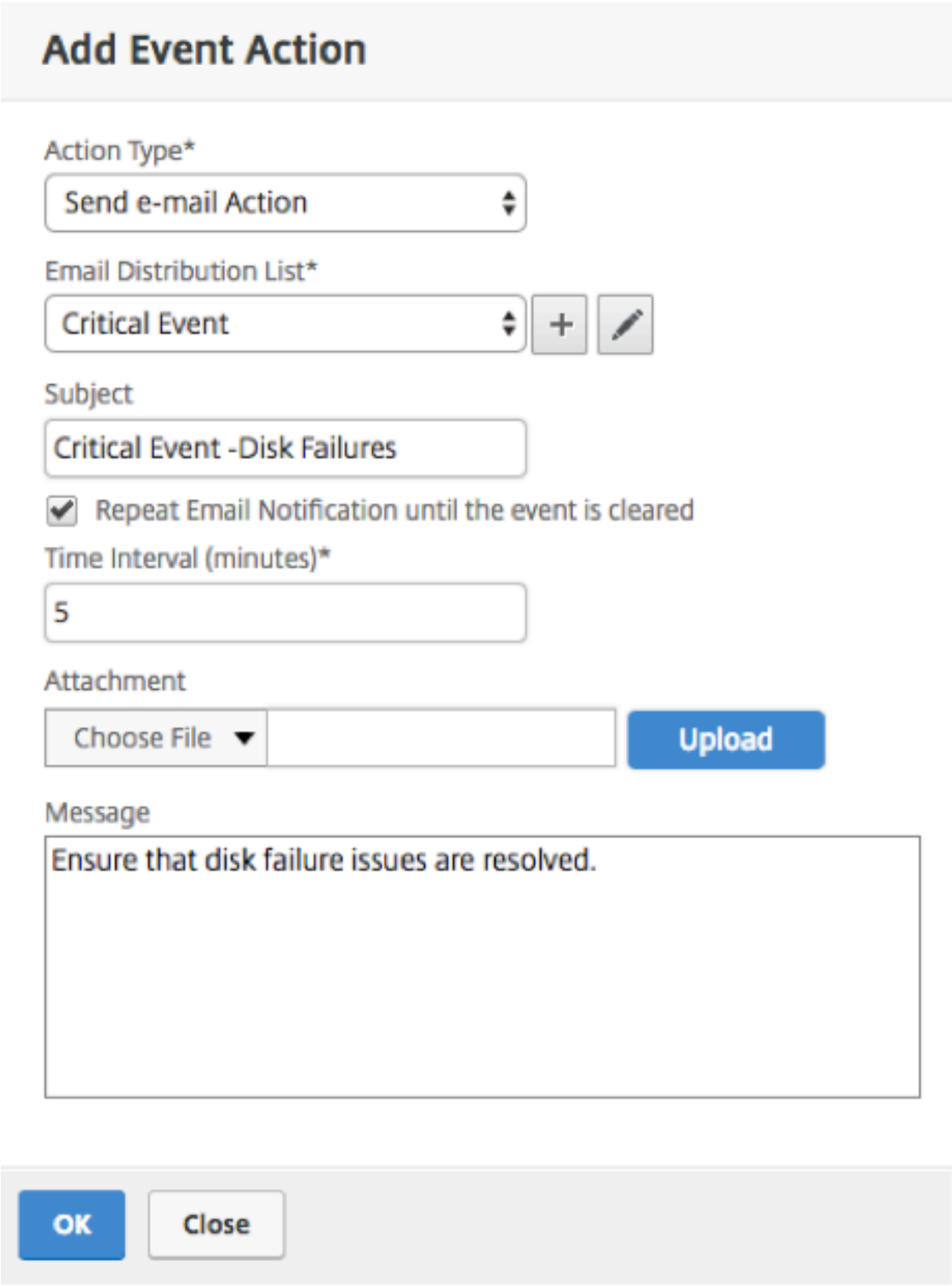
- Send e-mail Action
- Send Trap Action
- Send SMS Action
- Run Command Action
- Execute Job Action
- Suppress Action

メールイベント規則アクションを設定するには:

［Send e-mail Action］イベントアクションタイプを選択した場合、定義したフィルター条件をイベントが満たしたときにメールが送信されます。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信リストを作成するか、過去に作成したメール配信リストを選択できます。

カスタマイズした件名とユーザーメッセージを追加し、構成した規則に受信イベントが適合したときに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。

このオプションを使用すると、「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選択して、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。



トラップイベント規則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）を定義した場合、定義したフィルター条件をイベントが満たしたときに特定のトラップリスナーにトラップメッセージが送信されます。

SMS イベント規則アクションを設定するには：

「**SMS** アクションを送信」イベントアクションタイプを選択すると、フィルター条件に一致する各イベントのショートメッセージサービス (SMS) メッセージが表示されます。SMS サーバーまたは SMS プロファイルの詳細を指定して SMS 配信リストを作成するか、過去に作成した SMS 配信リストを選択できます。

Run Command Action を設定するには：

[コマンドアクションの実行] 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。たとえば、管理対象ライセンスの構成変更が行われたときに重要度が「Critical」のイベントが発生した場合、コマンドスクリプトを実行できます。

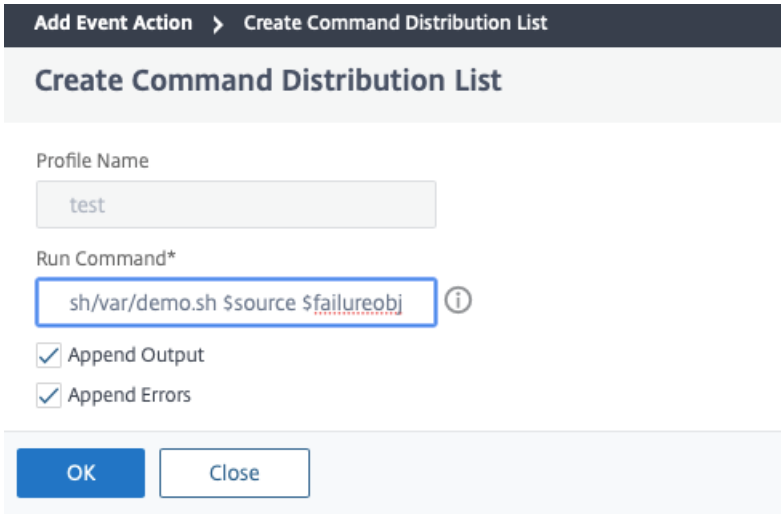
また、「コマンドアクションを実行」スクリプトに次のパラメータを設定することもできます。

パラメーター	説明
$source	このパラメーターは、受信したイベントのソース IP アドレスに相当します。
$category	このパラメーターは、フィルターのカテゴリで定義したトラップのタイプに相当します。
$entity	このパラメーターは、イベント生成の対象となるエンティティのインスタンスまたはカウンターに相当します。このパラメーターには、しきい値関連のイベントではカウンター名、エンティティ関連のイベントではエンティティ名、すべての証明書関連のイベントでは証明書名が含まれます。
$severity	このパラメーターは、イベントの重要度に相当します。
$failureobj	エラーオブジェクトはイベントの処理方法に影響を与え、通知されたとおりの問題がエラーオブジェクトに反映されるようにします。このオブジェクトを使用すると、単にイベントをありのままレポートするのではなく、問題を素早く突き止めてエラーの原因を特定することができます。

> 注
>
> コマンドの実行の際には、これらのパラメーターは実際の値に置き換えられます。

Citrix ADM で「コマンドアクションを実行」イベントアクションを設定するには：

1. 「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」ドロップダウンから「****** コマンドアクション ** を実行」を選択します。
2. 「コマンド配布リストの作成」ページで、プロファイル名と実行するコマンドを指定します。指定したコマンドは、定義したフィルター条件をイベントが満たしたときに実行されます。

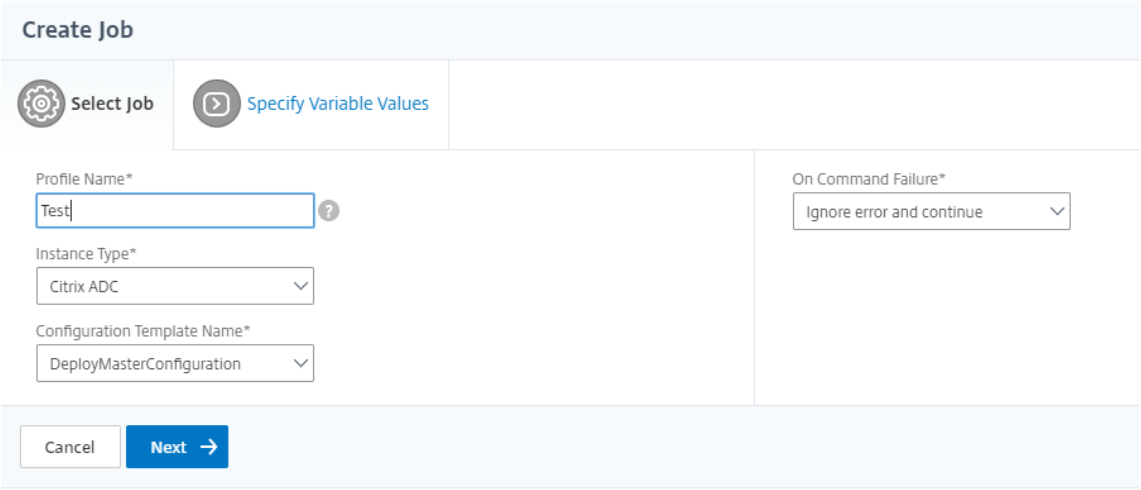


> 注
>
> コマンドスクリプトの実行時に生成された 出力 と エラー（存在する場合）を **NetScaler ADM** サーバーのログファイルに保存する場合は、[**Append** Output] オプションと [Append Errors] オプションを有効にできます。これらのオプションを有効にしない場合、Citrix ADM はコマンドスクリプトの実行中に生成されたすべての出力とエラーを破棄します。

[**Execute Job Action**] を設定するには:

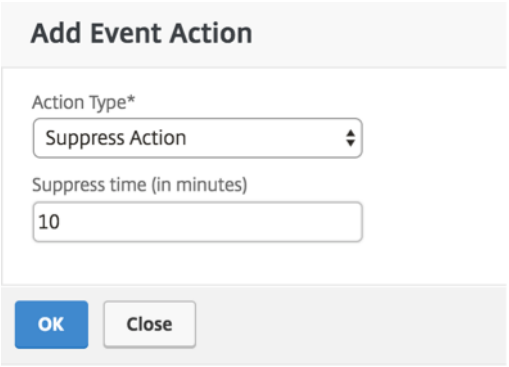
構成ジョブを含むプロファイルを作成すると、ジョブは、指定したフィルター条件に一致するイベントとアラームに対して、Citrix ADC、Citrix SDX、Citrix SD-WAN WO インスタンスの組み込みジョブまたはカスタムジョブとして実行されます。

1. 「イベントルールアクション」で「アクションを追加」をクリックし、「アクションタイプ」メニューから「ジョブアクションを実行」を選択します。
2. 定義したフィルター条件をイベントが満たした場合に実行するジョブを指定して、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。



[**Suppress Action**] 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。



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 ADC インスタンスで発生するイベントの報告された重大度を変更する

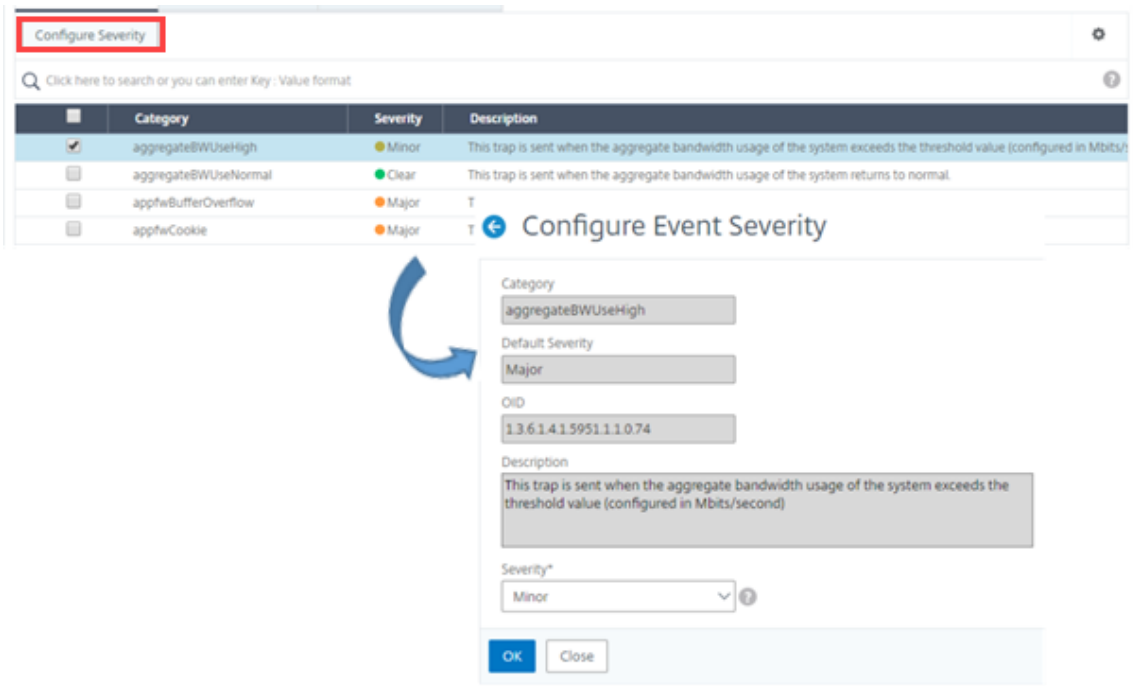
February 6, 2024

すべてのデバイスで生成されたイベントのレポート機能を管理できます。これにより、特定のインスタンスの特定のイベントに関するイベント詳細を確認したり、イベントの重要度に基づいてレポートを表示したりできます。デフォルトの重要度設定を使用したイベント規則を作成できます。また、重要度設定を変更できます。汎用イベントとエンタープライズ固有のイベント双方に対して、重要度を構成できます。

重要度レベルは、Critical、Major、Minor、Warning、Clear で定義できます。

イベントの重大度を変更するには、次の手順に従います。

1. [ネットワーク] > [イベント] > [イベント設定] に移動します。
2. 変更する Citrix Application Delivery Controller（ADC）インスタンスタイプのタブをクリックします。次に、リストからカテゴリを選択し、[重要度の設定] をクリックします。
3. [**Configure Event Severity**] でボックスの一覧から重要度レベルを選択します。
4. [**OK**] をクリックします。

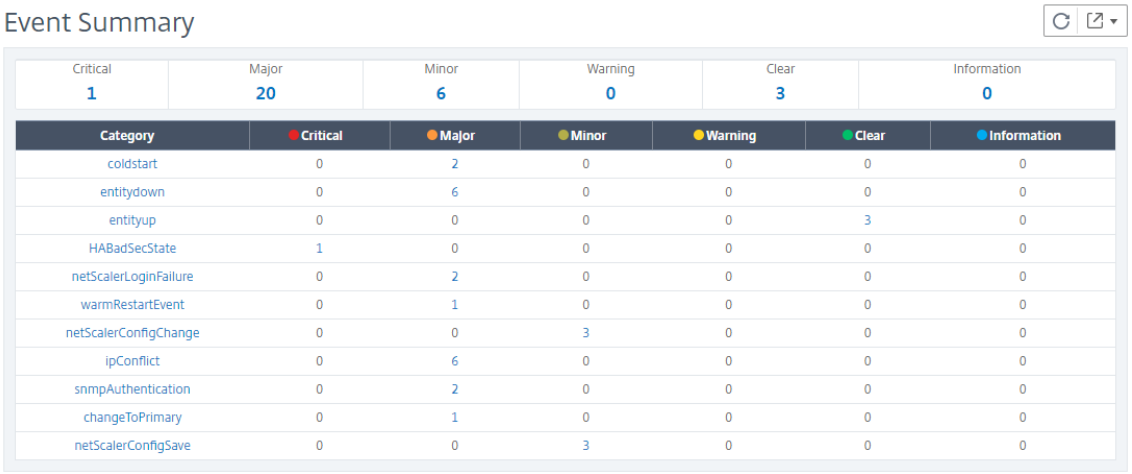


イベントの概要の表示

February 6, 2024

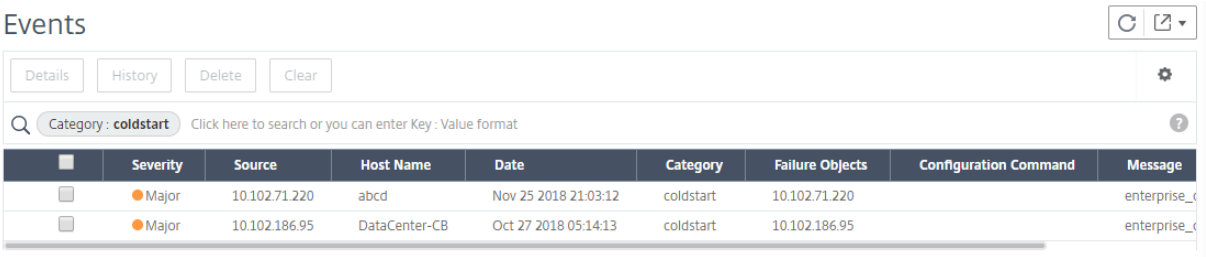
[イベントの概要] ページを表示して、NetScaler Application Delivery Management（ADM）サーバーで受信したイベントとトラップを監視できるようになりました。[ネットワーク] > [イベント] に移動します。[Events Summary] ページには、以下の情報が表形式で表示されます。

- **NetScaler ADM** が受信したすべてのイベントの概要。イベントはカテゴリ別にリスト表示され、各列にそれぞれの重要度（Critical、Major、Minor、Warning、Clear、Information）が表示されます。たとえば、Citrix Application Delivery Controller（ADC）インスタンスがダウンし、NetScaler ADM サーバーへの情報の送信を停止すると、クリティカルなイベントが発生します。このイベント中には、インスタンスがダウンした理由やダウン時間などを示す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、「
イベント」ページに移動します。このページでは、「カテゴリ」や「重要度」などのフィルタがあらかじめ選択されています。このページには、NetScaler ADC インスタンスの IP アドレスとホスト名、トラップを受信した日付、カテゴリ、障害オブジェクト、構成コマンドの実行、メッセージ通知など、イベントに関する詳細情報が表示されます。



イベントの重大度と **SNMP** トラップの詳細を表示します

February 6, 2024

Citrix Application Delivery Management（ADM）でイベントとその設定を作成すると、そのイベントは［イベントの概要］ページにすぐに表示されます。同様に、Citrix ADM サーバーに追加されたすべての Citrix Application Delivery Controller（ADC）インスタンスの状態、稼働時間、モデル、およびバージョンを、インフラストラクチャダッシュボードで詳細に表示および監視できます。

Infrastructure ダッシュボードでは、無関係な値をマスクして、重要度、正常性、稼働時間、モデル、NetScaler ADC インスタンスのバージョンなどの情報をより簡単に表示および監視できるようになりました。

たとえば、重要度レベルが「緊急」のイベントはまれにしか発生しない場合があります。しかしながら、ネットワー

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 based events** ページが表示されます。このページには、選択した期間にクリティカルイベントが発生したタイミングに関するすべての詳細 (インスタンスソース、日付、カテゴリ、およびクリティカルイベントが発生したときに送信されたメッセージ通知) が表示されます。

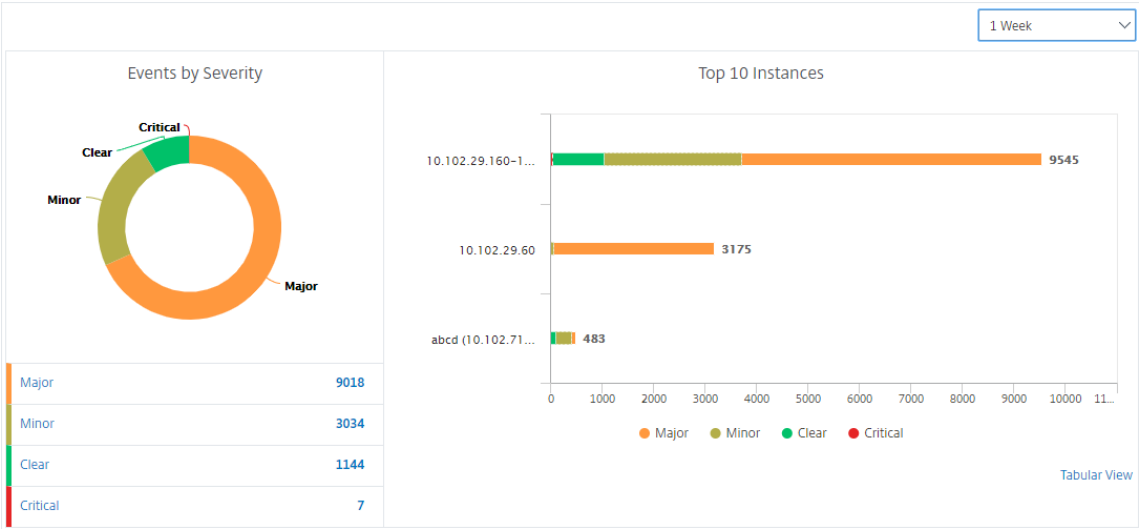
同様に、Citrix VPX インスタンスの正常性をダッシュボードに表示できます。インスタンスが稼働していた時間をマスクし、インスタンスが稼働停止していた時間のみを表示できます。グラフをクリックすると、そのインスタンスのページが表示され、サービス外 フィルタが既に適用され、ホスト名、1 秒あたりに受信した HTTP リクエストの数、CPU 使用率などの詳細が表示されます。インスタンスを選択して、その特定の Citrix インスタンスのダッシュボードで詳細を確認することもできます。

NetScaler ADM で特定のイベントを重要度別に選択するには:

1. 管理者の資格情報を使用して NetScaler ADM にログオンします。
2. [ネットワーク**] > [**ダッシュボード**]** に移動します。

   または

   [ネットワーク**] > [**イベント**] > [**レポート] に移動します。
3. ページの右上隅のメニューから、重大度別にイベントを表示する期間を選択します。

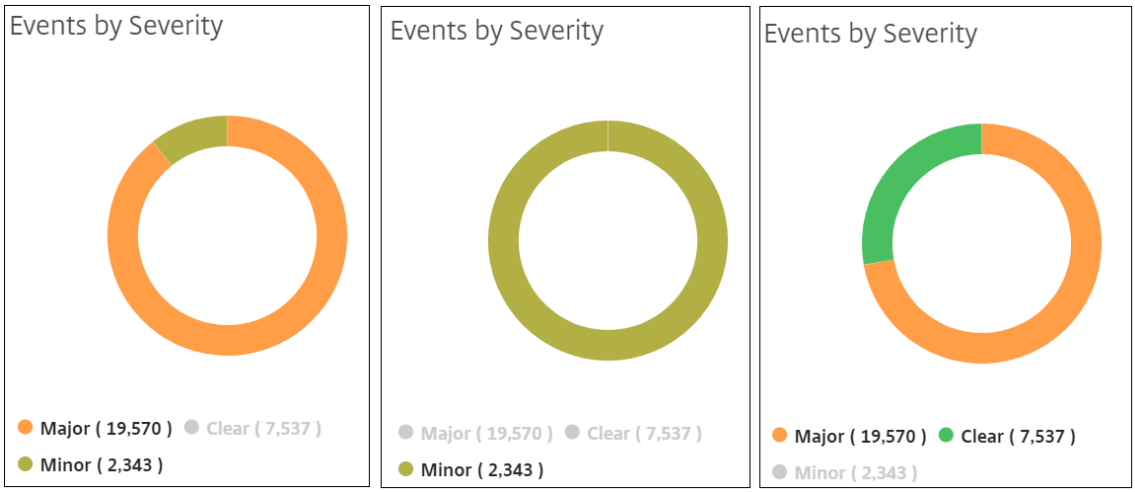


4. [**Events by Sev**erity] ドーナツグラフには、すべてのイベントが重要度別に視覚的に表示されます。異なる種類のイベントは異なる色が付いたセクションとして表され、各セクションの長さは、その種類の重要度の合計イベント数に対応しています。
5. ドーナツチャートの各セクションをクリックすると、対応する重要度ベースの イベントページが表示されます。このページには、選択した期間における選択した重要度に関する次の詳細が表示されます。

   - インスタンスのソース
   - イベントの日付

- NetScaler ADC インスタンスによって生成されるイベントのカテゴリ
- 送信されたメッセージ通知

> 注
>
> ドーナツグラフの下には、チャートに表示されている重大度のリストが表示されます。デフォルトでは、ドーナツグラフには、すべての重要度タイプのすべてのイベントが表示されます。そのため、一覧内のすべての重要度タイプが強調表示されます。選択した重要度をより簡単に表示して監視するには、重要度タイプを切り替えます。



NetScaler ADM で **NetScaler ADC SNMP** トラップの詳細を表示するには:

管理対象の NetScaler ADC インスタンスから受信した各 SNMP トラップの詳細を、［イベント設定］ページで NetScaler ADM サーバーに表示できるようになりました。[ネットワーク] > [イベント] > [イベント設定**]** に移動します。インスタンスから受信した特定のトラップについては、タブ形式で次の詳細を表示できます。

- カテゴリ-イベントが属するインスタンスのカテゴリを指定します。
- 重大度：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。

syslog メッセージのエクスポート

February 6, 2024

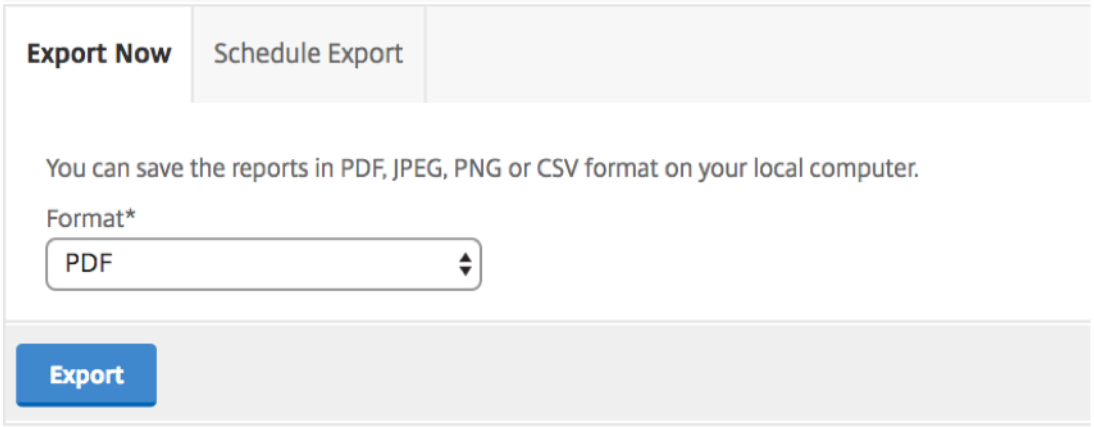
サーバー上で受信されたすべての syslog メッセージのエクスポートをスケジュールすることで、NetScaler Application Delivery Management（ADM）にログインせずに syslog メッセージを表示できるようになりました。Citrix アプリケーション Delivery Controller（ADC）インスタンスで生成された syslog メッセージは、PDF、CSV、PNG、および JPEG 形式でエクスポートできます。また、指定した電子メールアドレスにさまざまな間隔でこれらのレポートをエクスポートするようにスケジュールすることもできます。

> 注
>
> Syslog サーバーの構成、Syslog のデータと時刻の形式、および Citrix ADM での Syslog メッセージの表示方法の詳細については、「監査情報の表示」を参照してください。

Syslog メッセージを表示するには、[ネットワーク] > [イベント] > [**Syslog** メッセージ] に移動し ます。右側のペインの [Syslog **Viewer**] で、 表示したい Syslog メッセージをモジュール、イベントタイプ、重大度、および送信元 IP アドレスでフィルタリングできます。[適用] をクリック して Syslog メッセージを生成します。

NetScaler ADM を使用して **syslog** メッセージレポートをエクスポートするには:

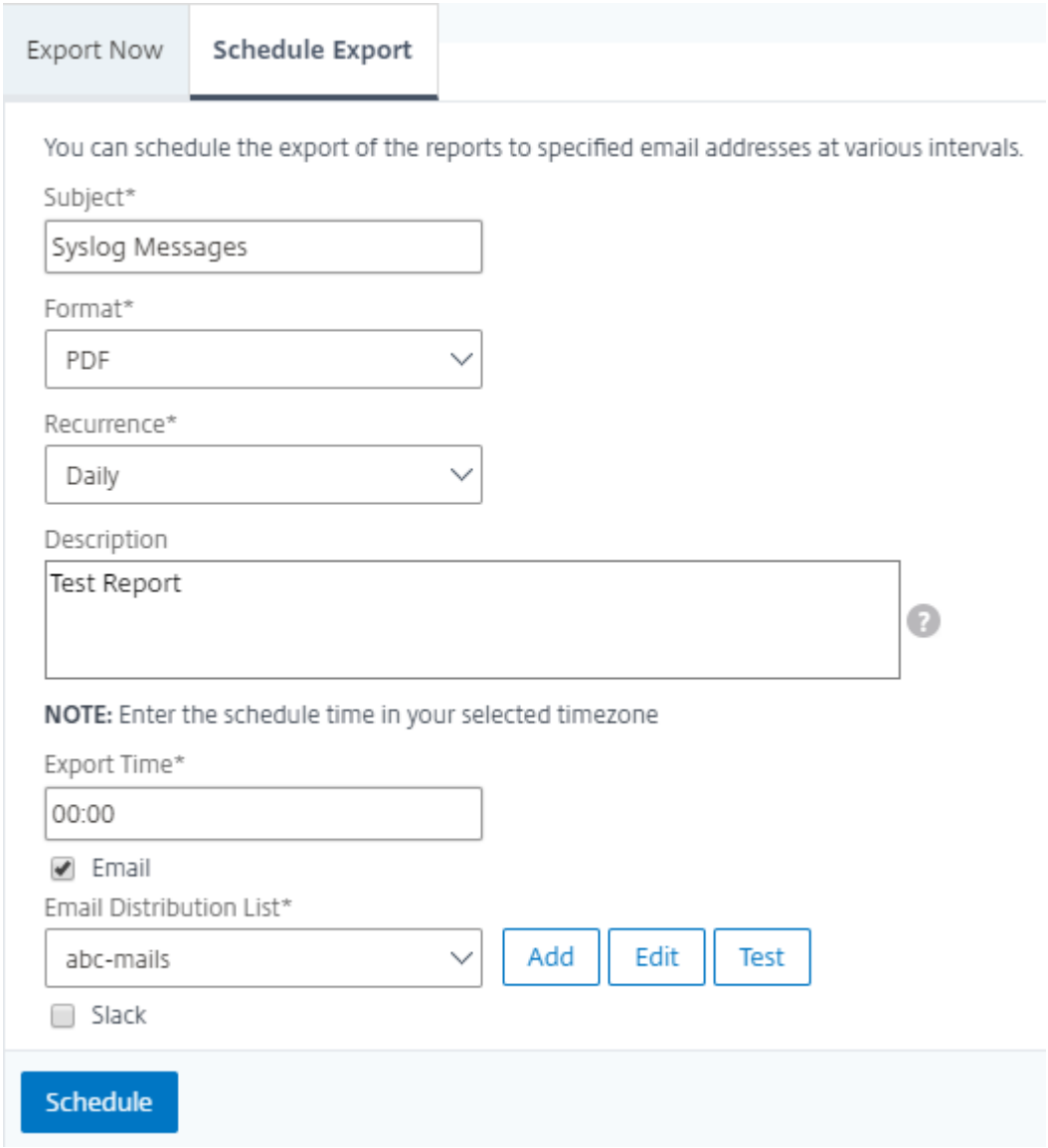
1. [ネットワーク] > [イベント] > [**Syslog** メッセージ] に移動します。
2. [Syslog Messages] ページの右側のペインで、右上隅にある [Export] をクリックします。
3. [今すぐエクスポート] タブで、必要な形式を選択し、[エクスポート] をクリックします。



NetScaler ADM を使用して **syslog** メッセージレポートのエクスポートをスケジュールするには:

1. [ネットワーク] > [イベント] > [**Syslog** メッセージ] に移動します。
2. 「**Syslog** メッセージ」ページの右側のペインで、「エクスポート」をクリックします。
3. [レポートのスケジュール] タブで、次のパラメータを設定します。
   - 説明: レポートをエクスポートする理由を説明するメッセージ。
   - フォーマット: レポートをエクスポートする フォーマット。
   - 繰り返し: レポートをエクスポートする 間隔。
   - エクスポート時間: レポートをエクスポートする時間。現地時間帯の時間を 24 時間形式で入力します。

- 電子メール配布リスト: 電子メールでレポートを受信する受信者のリスト。表示されるボックスの一覧からメール配布リストを選択します。電子メールは、レポートが生成されスケジュールの時間基準が満たされると送信されます。 新しいメール配布リストを作成する場合は、「**+**」をクリックして、メールサーバーとメールプロファイルの詳細を指定します。



NetScaler ADM を使用してイベントプルーニング設定を構成する方法

Citrix ADM サーバーのデータベースに保存されるイベントメッセージデータの量を制限するには、Citrix 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] > [システム管理] に移動します。[インスタンス設定**]** で、[イベント**] [**プルーニング設定] をクリック します。Citrix ADM サーバーにデータを保持する時間間隔を日単位で入力し、「**OK**」をクリックします。

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、CitrixApplication Delivery Management（ADM）は、構成済みの Citrix アプリケーション Delivery Controller（ADC）インスタンスから送信されたすべての syslog メッセージを受信します。表示する必要のないメッセージの数が大量になる場合もあります。たとえば、情報レベルのすべてのメッセージを表示する必要がない場合があります。必要のない一部の syslog メッセージを破棄できるようになりました。いくつかのフィルターを設定することで、NetScaler ADM に届く Syslog メッセージの一部を抑制できます。Citrix ADM は、条件に一致するすべてのメッセージをドロップします。これらのドロップされたメッセージは NetScaler ADM GUI には表示されません。また、これらのメッセージはお客様の NetScaler ADM データベースにも保存されません。

いくつかのフィルターを設定することで、NetScaler ADM に届くログに記録された Syslog メッセージの一部を抑制できます。syslog メッセージを非表示にするために使用できる 2 つのフィルターは、重要度とファシリティです。特定の NetScaler ADC インスタンスまたは複数のインスタンスからのメッセージを抑制することもできます。また、NetScaler ADM でメッセージを検索および非表示にするテキストパターンを指定することもできます。Citrix ADM は、条件に一致するすべてのメッセージをドロップします。これらのドロップされたメッセージは NetScaler ADM GUI には表示されません。また、これらのメッセージは顧客データベースにも保存されません。それにより、ストレージサーバー上のかなりの領域が節約されます。

syslog メッセージを非表示にするためのいくつかのユースケースを次に示します。

- 情報レベルのすべてのメッセージを無視する場合は、レベル 6（情報）を非表示にします。
- ファイアウォールのエラー条件のみを記録する場合は、レベル 3（エラー）以外のすべてのレベルを非表示にします。

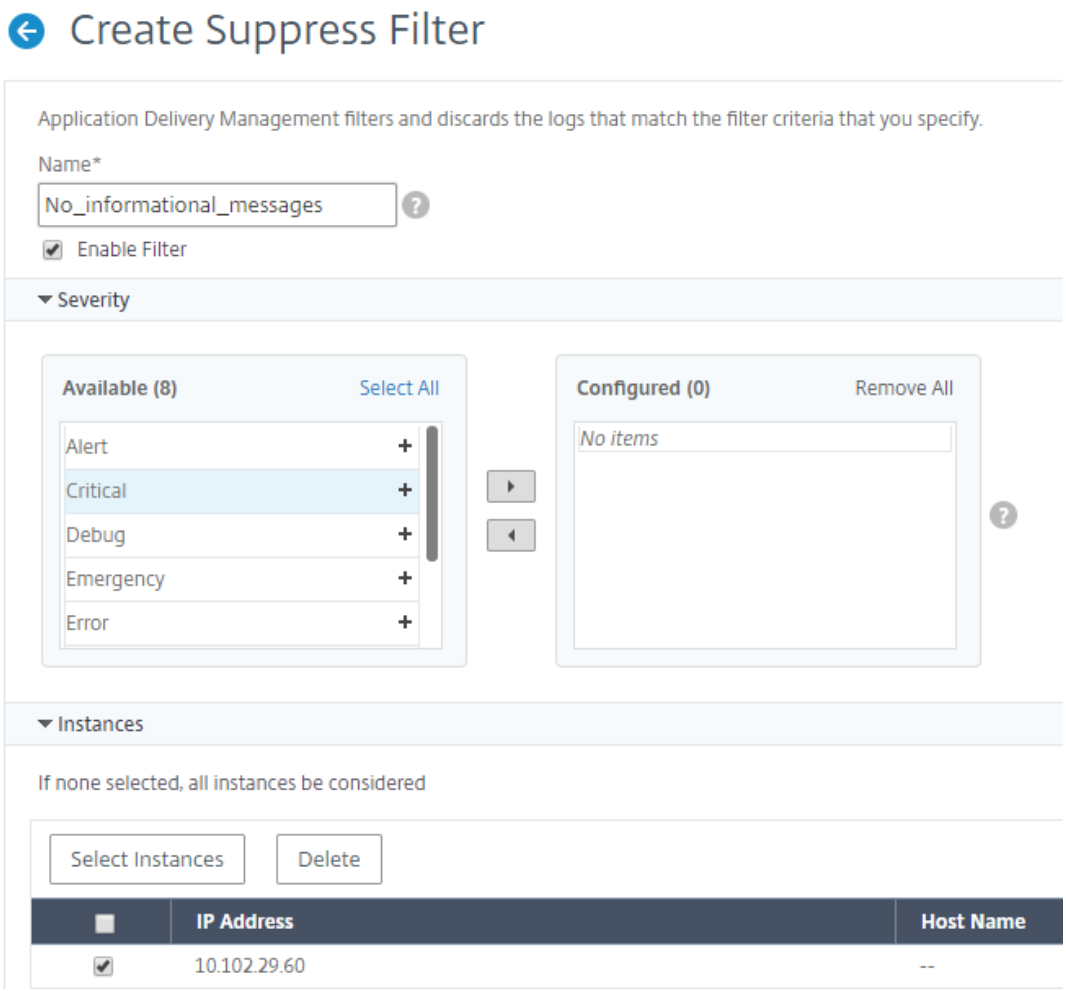
フィルタの作成による **syslog** メッセージの抑制

1. Citrix ADM で、［ネットワーク］> ［イベント］> ［**Syslog** メッセージ］> ［フィルターの抑制］に移動します。
2. 「抑制フィルタの作成」ページで、次の情報を更新します。
   a) 名前 -フィルタ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。

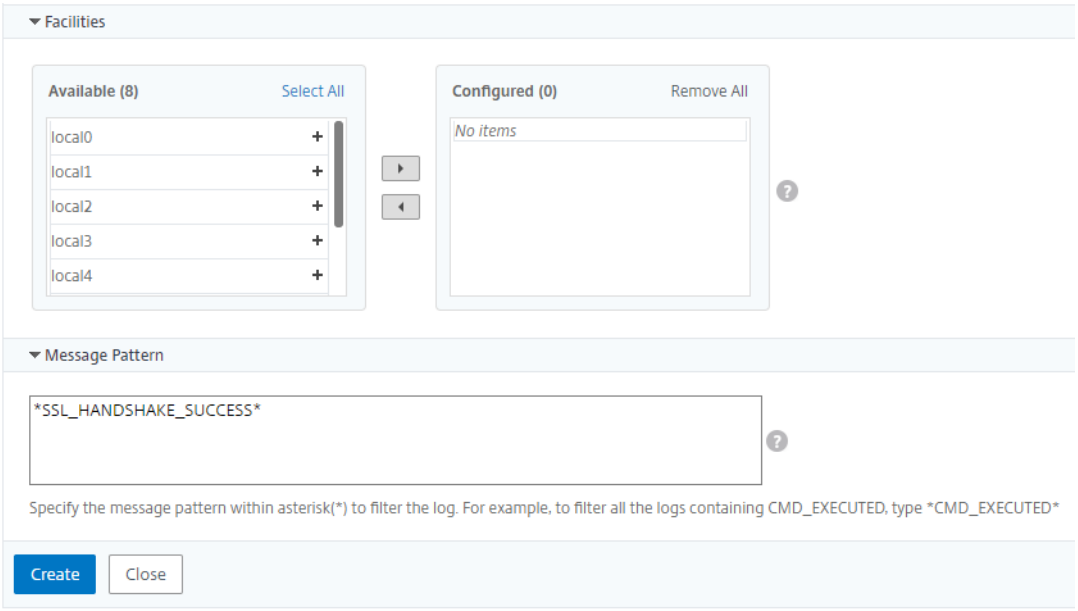
   b) 重要度 -メッセージを非表示にする必要があるログレベルを選択して追加します。たとえば、受信した情報メッセージを表示する必要がない場合は、［Informational］を選択してそれらのメッセージを非表示にします。

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. [ネットワーク] > [イベント] > [**Syslog** メッセージ] > [フィルタの抑制] に移動し、[フィルタの抑制] ページでフィルタを選択して [編集] をクリックします。
2. [抑制フィルタの構成] ページで、[フィルタの有効化] チェックボックスをオフにしてフィルタを無効にします。

インスタンスイベントのプルーニング設定の構成

February 6, 2024

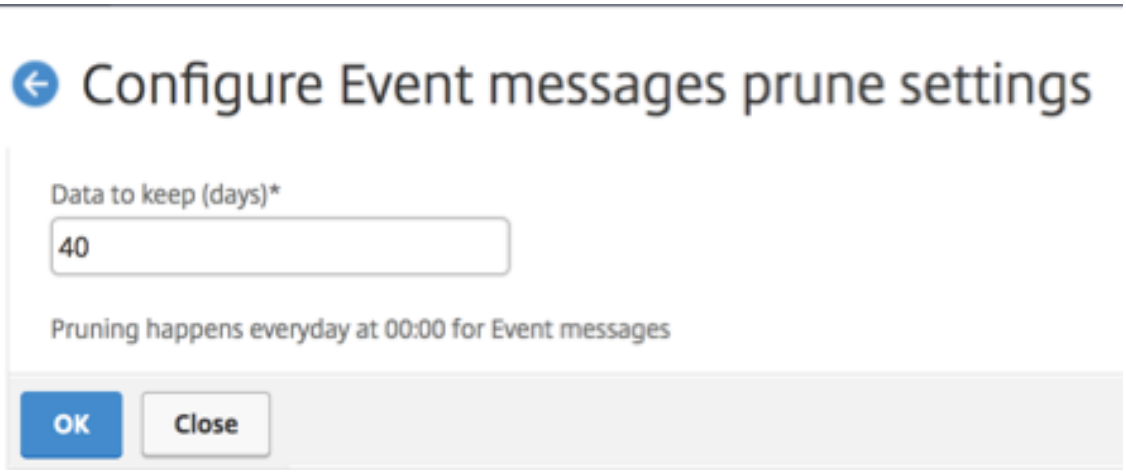
Citrix Application Delivery Management（ADM）サーバーによって管理される Citrix アプリケーション Delivery Controller（ADC）インスタンスは、イベントメッセージデータを継続的に送信して Citrix ADM に保存します。NetScaler ADM でネットワークレポートデータ、イベント、監査ログ、タスクログを保持する間隔を指定できます。デフォルトでは、これらのデータは 24 時間ごとに（00:00 の時刻に）削除されます。

> 注
>
> 指定できる値は 40 日を超えることも、1 日未満にすることもできません。

インスタンスイベントのプルーニング設定を構成するには:

1. [システム] > [システム管理] に移動します。

2. 「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。



SSL ダッシュボード

February 6, 2024

NetScaler Application Delivery Management（ADM）により、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。Citrix ADM SSL ダッシュボードとその機能を使い始めるには、SSL 証明書とは何か、Citrix 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。

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。

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。

- 認可された認証局 (CA) から
- NetScaler ADC アプライアンスで新しい SSL 証明書とキーを生成する

NetScaler ADM は、すべての管理対象 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します。SSL Dashboard では、証明書の発行者、キーの強度、署名アルゴリズム、期限切れまたは未使用の証明書などを追跡するのに役立つグラフを表示できます。また、仮想サーバーで実行されている SSL プロトコルの分布および各サーバーで有効化されているキーも確認できます。

また、証明書の有効期限が近づいたときに通知を設定し、その証明書を使用する NetScaler ADC インスタンスに関する情報を含めることもできます。

NetScaler ADC インスタンスの証明書を CA 証明書にリンクできます。ただし、同じ CA 証明書にリンクする証明書のソースと発行元が同じであることを確認してください。証明書を CA 証明書にリンクしたら、それらのリンクを解除できます。

SSL ダッシュボードの使用

February 6, 2024

Citrix Application Delivery Management（ADM）の SSL 証明書ダッシュボードを使用して、証明書の発行者、主な強み、および署名アルゴリズムを追跡するのに役立つグラフを表示できます。SSL 証明書ダッシュボードには、次の項目を示すグラフも表示されます。

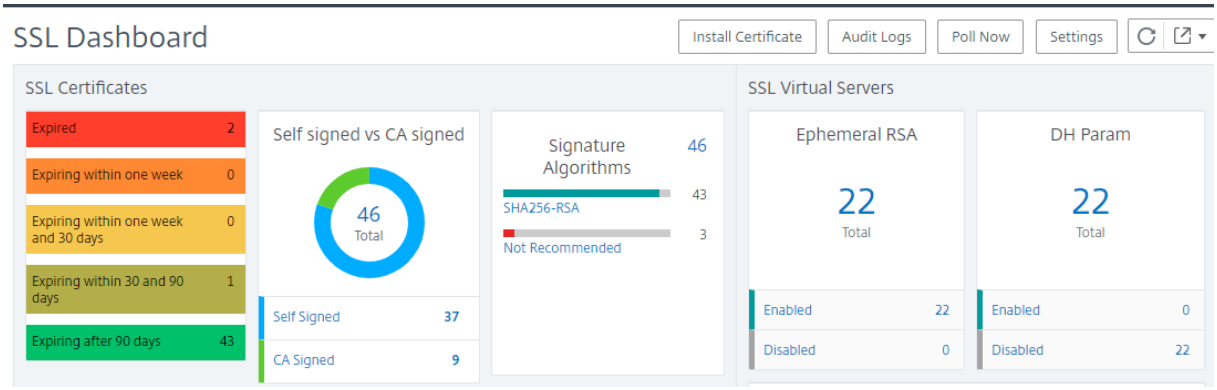
- 証明書が有効期限切れになるまでの日数
- 使用されている証明書および未使用の証明書の数
- 自己署名および CA 署名の証明書の数
- 発行者数
- 署名アルゴリズム
- SSL プロトコル
- 使用中の証明書件数上位 10 インスタンス

SSL 証明書を監視するには

会社に SSL ポリシーがあり、すべての証明書に最低 2048 ビットのキー強度が必要であり、信頼できる CA 機関がそれを承認する必要があるなど、特定の SSL 証明書要件を定義している場合は、Citrix ADM SSL ダッシュボードを使用して証明書を監視できます。

別の例として、新しい証明書をアップロードしたが、それを仮想サーバーにバインドするのを忘れた場合について述べます。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。［Usage］で、インストールされている証明書の数、および使用されている証明書の数を確認できます。さらにグラフをクリックすると、証明書名、それが使用されているインスタンス、その有効性、その署名アルゴリズムなどを確認できます。

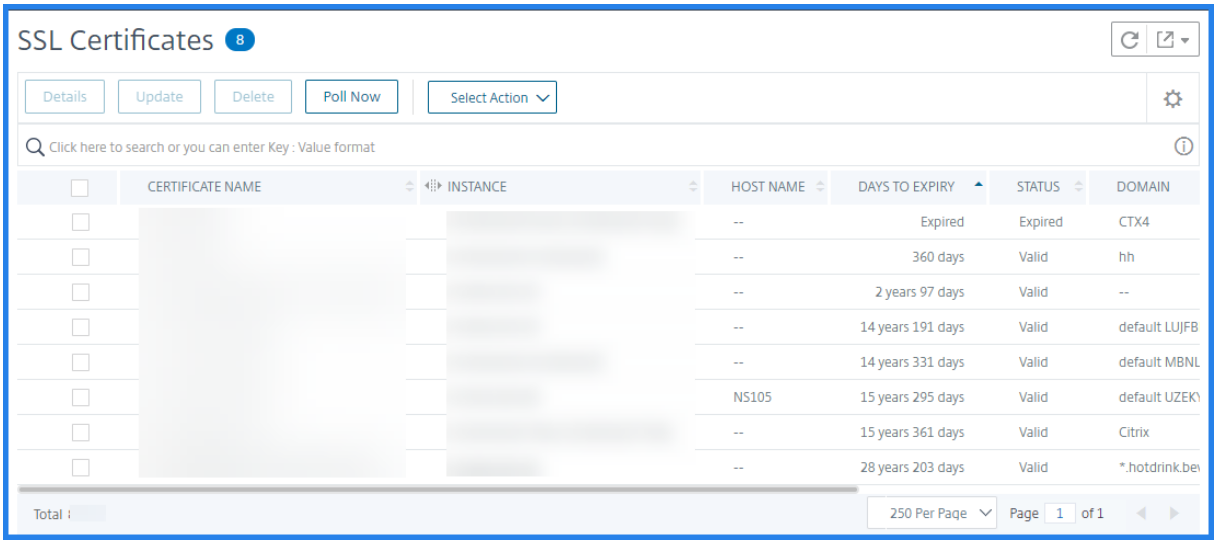
NetScaler ADM で SSL 証明書を監視するには、［ネットワーク］>［**SSL** ダッシュボード］に移動します。



NetScaler ADM では、SSL 証明書をポーリングし、インスタンスのすべての SSL 証明書を直ちに NetScaler ADM に追加できます。そのためには、[ネットワーク] > [**SSL** ダッシュボード] に移動し、[今すぐ投票] をクリックします。[**Poll Now**] ページが表示され、ネットワーク内のすべての Citrix Application Delivery Controller（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オプションが表示されます。

Citrix ADM SSL ダッシュボードを使用して、Citrix ADC SSL 証明書、SSL 仮想サーバー、および SSL プロトコルの詳細を表示または監視できます。「合計」数はリンクになっています。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、ユーザーが「自己署名 vs. CA signed」をクリックすると、新しいウィンドウが開き、NetScaler ADC インスタンス上の 52 の SSL 証明書の詳細が表示されます。



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 ポリシーを使用して監視するプロトコルを指定できます。サポートされているプロトコルは、SSLv2、SSLv3、TLS1.0、TLS1.1、および TLS1.2 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一覧が表示されます。

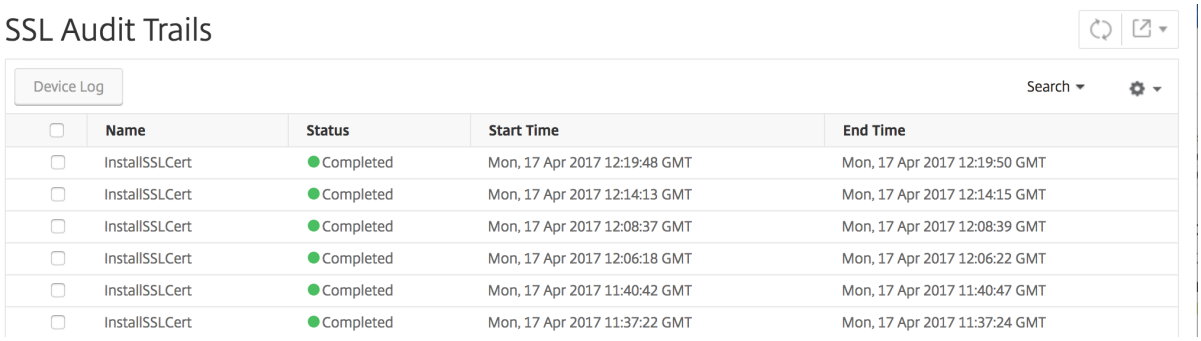
SSL ダッシュボード上で Diffie-Hellman（DH）または Ephermeral RSA キーが有効または無効になると、ドーナツグラフが表示されます。これらのキーにより、1024 ビットの証明書の場合のように、サーバー証明書でエクスポ

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。当該グラフをクリックすると、DH または Ephemeral RSA キーが有効になっている仮想サーバーの一覧が表示されます。

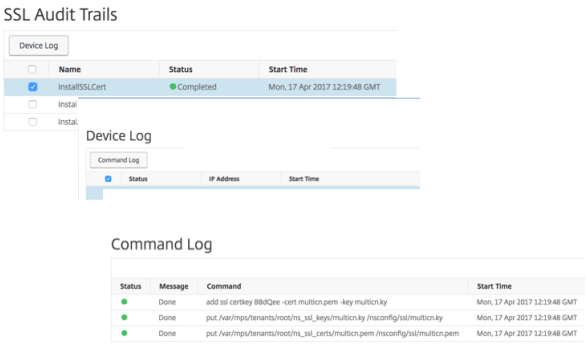
SSL 証明書の監査記録を表示するには

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 Citrix ADM で実行された特定の操作の監査ログを表示するには、［ネットワーク］>［SSL ダッシュボード］**>**［**SSL** 監査証跡］に移動します。



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、その操作が実行されたインスタンス、およびそのインスタンス上で実行されたコマンドを表示できます。

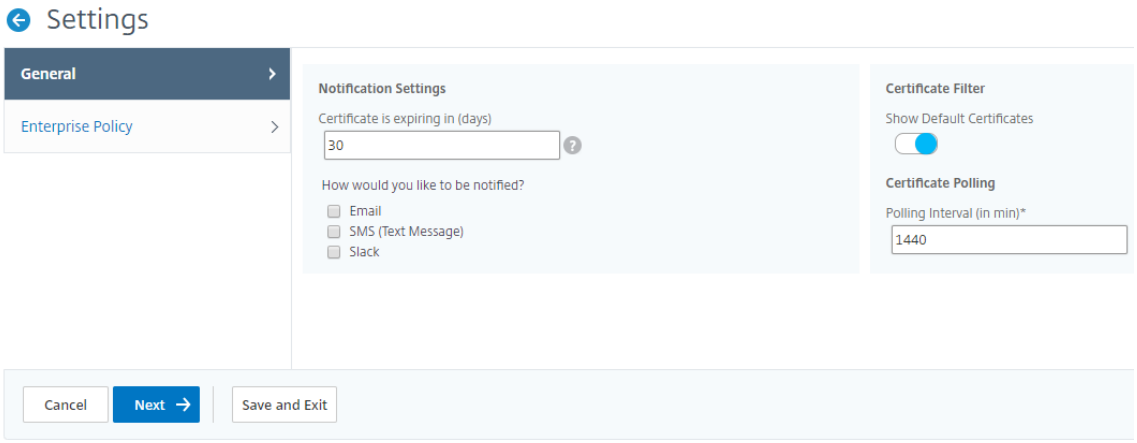


SSL ダッシュボードでデフォルトの **NetScaler ADC** 証明書を除外するには

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［ネットワーク］>［**SSL** ダッシュボード］に移動します。
2. [**SSL** ダッシュボード] ページで、[設定] をクリックします。
3. **[** 設定] ページで、[一般] を選択します。
4. 証明書の有効期限が切れるまでの日数を入力して、証明書の有効期限切れに関する通知を受け取ります。
5. 通知方法を選択し、それぞれのプロファイルを作成します。
6. [証明書フィルタ] セクションで、[既定の証明書を表示する] チェックボックスをオフにし、[保存して終了] をクリックします。



SSL 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。

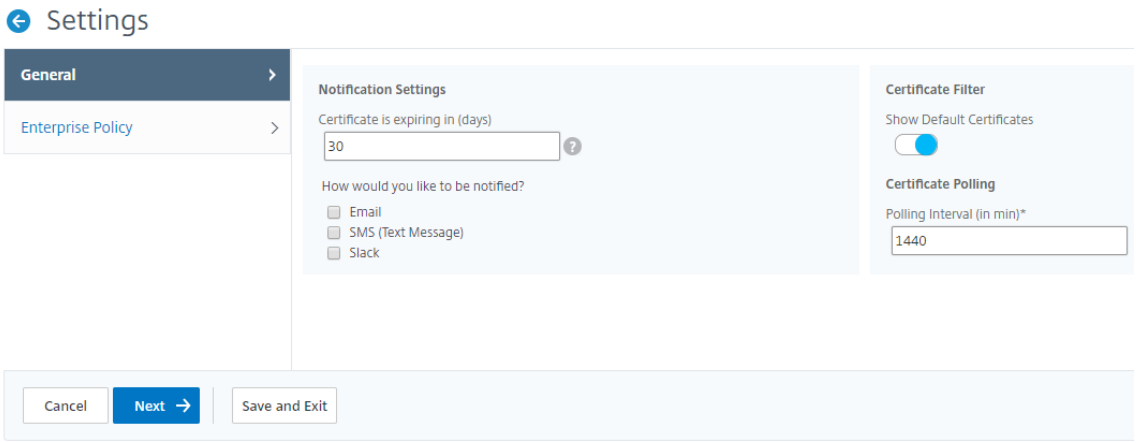
NetScaler ADM からの通知を設定するには：

1. NetScaler Application Delivery Management（ADM）で、［ネットワーク］>［**SSL** ダッシュボード］に移動します。
2. [**SSL** ダッシュボード] ページで、[設定] をクリックします。
3. [**SSL** 設定] ページで、[編集] アイコンをクリックします。
4. ［**Notification Settings**］セクションで、有効期限の何日前に通知を送信するかを指定します。

5. 送信する通知の種類を選択します。ボックスの一覧メニューから通知の種類と配布リストを選択します。通知の種類を次に示します。

   - **Email** - メールサーバーとプロファイルの詳細を指定します。証明書の有効期限が近づくと、メールがトリガーされます。
   - **SMS** - ショートメッセージサービス（SMS）サーバーとプロファイルの詳細を指定します。証明書の有効期限が近づくと、SMS メッセージがトリガーされます。
   - **Slack** -Slack プロファイルの詳細を指定します。

6. [保存して終了] をクリックします。



SSL 証明書の有効期限が切れると、NetScaler ADM が SSL 証明書の有効期限トラップを外部トラップ送信先サーバーに送信するようになりました。Citrix ADM は、次の 2 つの条件が満たされるとトラップを送信します。

- SSL ダッシュボード設定ページで証明書の有効期限が切れる日数を設定しました。
- トラップの宛先が追加されました。

トラップ送信先は、[システム] > [**SNMP**] > [トラップ送信先] に移動して設定できます。トラップが送信される宛先 SNMP サーバの IP アドレスを入力します。ポート番号を入力し、コミュニティストリングとして「public」（引用符なし）を入力します。

インストールされた証明書を更新する

February 6, 2024

認証局（CA）から更新された証明書を受け取ったら、個々の Citrix Application Delivery Controller（ADC）インスタンスにログオンしなくても、Application Delivery Management（ADM）から既存の証明書を更新できます。

NetScaler ADM から **SSL** 証明書、キー、またはその両方を更新するには：

1. NetScaler ADM で、［ネットワーク］>［**SSL** ダッシュボード］に移動します。
2. いずれかのグラフをクリックして、SSL 証明書の一覧を表示します。
3. ［**SSL Certificates**］ページで証明書を選択し、［**Update**］をクリックします。または、SSL 証明書をクリックして詳細を表示し、[**SSL** 証明書] ページの右上隅にある [更新] をクリックします。
4. ［**Update SSL Certificate**］ページで、証明書およびキーに必要な変更を加えて、［**OK**］をクリックします。

NetScaler ADC インスタンスへの **SSL** 証明書のインストール

February 6, 2024

Citrix アプリケーション Delivery Controller（ADC）インスタンスに SSL 証明書をインストールする前に、証明書が信頼できる CA によって発行されていることを確認してください。また、証明書キーのキー強度が 2048 ビット以上であり、キーが安全な署名アルゴリズムで署名されていることを確認します。

別の **NetScaler ADC** インスタンスから **SSL** 証明書をインストールするには:

また、選択した NetScaler ADC インスタンスから証明書をインポートして、NetScaler Application Delivery Management（ADM）GUI から他のターゲット NetScaler ADC インスタンスに適用することもできます。

1. [ネットワーク] > [**SSL** ダッシュボード**]** に移動します。
2. SSL ダッシュボードの右上隅にある [インストール] をクリックします。
3. **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。

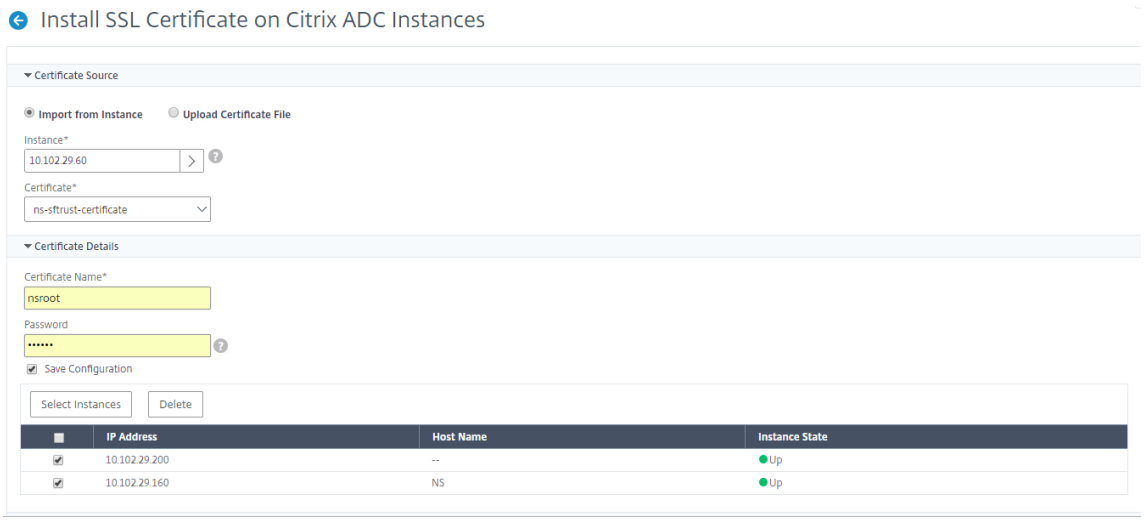
   a) [証明書のソース
   ] [インスタンスからインポート] オプションを選択します。

      - 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

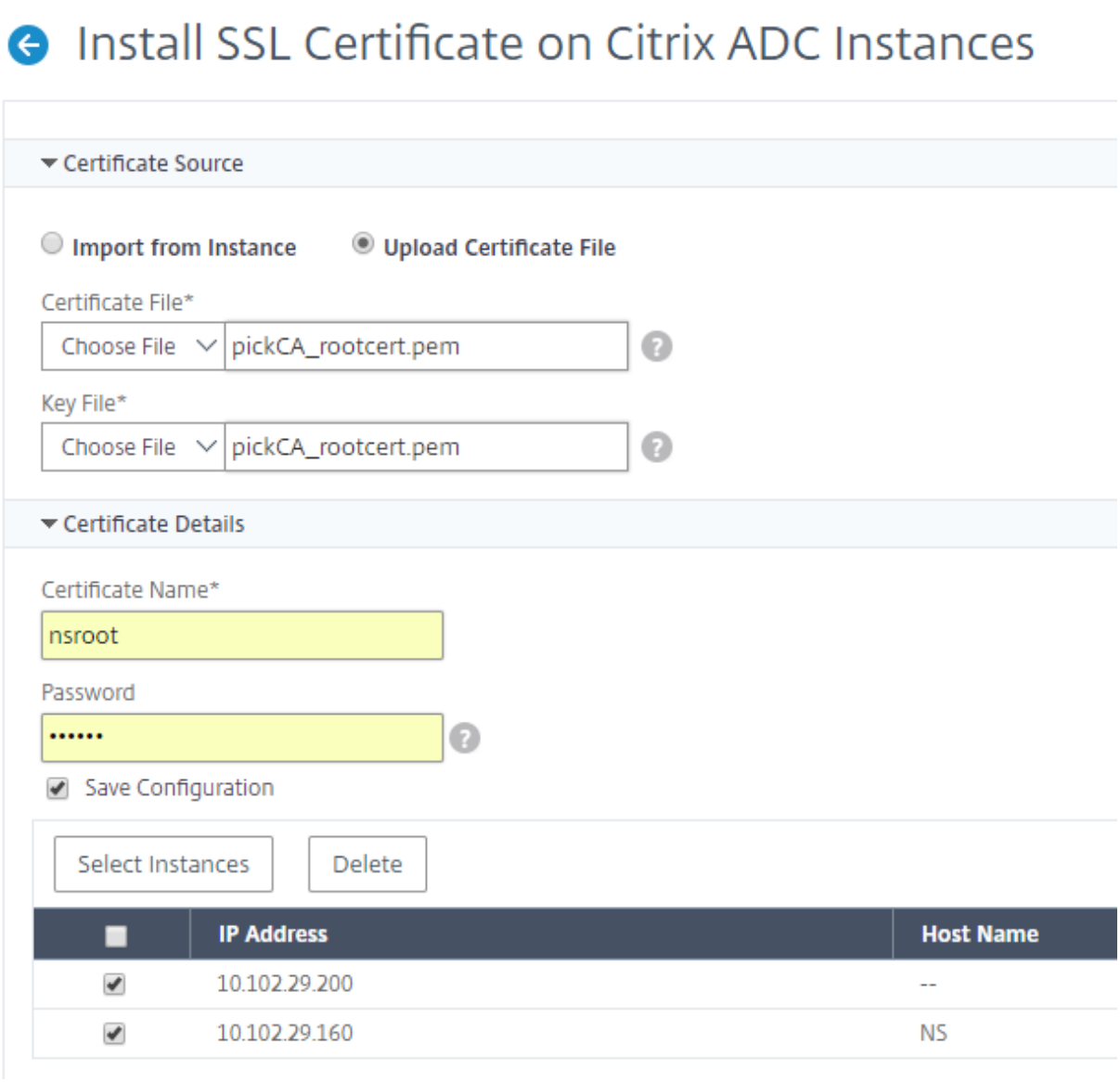
      - 証明書名。証明書キーの名前を指定します。
      - パスワード。プライベートキーを暗号化するためのパスワード。このオプションを使用して、暗号化された秘密キーをアップロードできます。

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 ADC 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、［ネットワーク］>［**SSL** ダッシュボード］に移動します。
2. ダッシュボードの右上隅にある［**Install**］をクリックします。
3. **NetScaler** インスタンスに **SSL** 証明書をインストール する］ページで、［証明書ファイルのアップロード］を選択し、次のパラメーターを指定します。
   - 証明書ファイル - [ローカル]（ローカル マシン）または [アプライアンス]（証明書ファイルは NetScaler ADM 仮想インスタンス上に存在する必要があります）を選択して、SSL 証明書ファイルをアップロードします。
   - **Key File** - キーファイルをアップロードします。
   - **Certificate Name** - 証明書のキーの名前を指定します。
   - **Password** - 秘密キーを暗号化するためのパスワード。このオプションを使用して、暗号化された秘密キーをアップロードできます。
   - インスタンスの選択-証明書をインストールする Citrix ADM インスタンスを選択します。
4. 今後使用するために構成を保存するには、[構成を保存] チェックボックスをオンにします。
5. ［**OK**］をクリックします。



証明書署名要求（**CSR**）の作成

February 6, 2024

CSR（Certificate Signing Request：証明書署名要求）は、証明書が使用されるサーバー上で生成される暗号化済みテキストのブロックです。CSR には、組織名、共通名（ドメイン名）、地域、国など、証明書に格納される情報が含まれています。

NetScaler ADM を使用して **CSR** を作成するには：

1. NetScaler Application Delivery Management（ADM）で、［ネットワーク］>［**SSL** ダッシュボード］に移動します。

2. いずれかのグラフをクリックしてインストールされている SSL 証明書のリストを表示し、CSR を作成する証明書を選択し、[Select **Action]** リストから **[**Create CSR**] を選択します ** 。
3. [**Create Certificate Signing Request (CSR)**] ページで、CSR の名前を指定します。
4. 次のいずれかを行います:
   - **Upload a key** - [**I have a Key**] オプションを選択します。キーファイルをアップロードするには、[ローカル]（ローカル マシン）または [アプライアンス]（キーファイルは NetScaler ADM 仮想インスタンスに存在している必要があります）を選択します。
   - キーの作成 -「キーがありません」オプションを選択し、次のパラメータを指定します。

暗号化アルゴリズム	キーの種類。たとえば、RSA などがあります。
キーファイル名	RSA キーが保存されたファイル名。
キーサイズ	キーサイズ（ビット）。
公開指数値	表示されるドロップダウンリストから [**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. 次のページに詳細情報が表示されます。デフォルト値を変更せずに CSR を作成する場合は、[**Continue**] をクリックします。

> 注
>
> 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。
>
> 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。CSR を送信してきた電子メールのアドレスに、CA は有効な証明書を返信します。

SSL 証明書のリンクとリンク解除

February 6, 2024

複数の証明書をまとめて関連付けて、証明書パッケージを作成します。証明書を別の証明書に関連付けるとき、1 番目の証明書の発行者が 2 番目の証明書のドメインと一致しなければなりません。たとえば、証明書 A を証明書 B に関連付ける場合、証明書 A の「発行者」は証明書 B の「ドメイン」と一致する必要があります。

NetScaler ADM を使用して **SSL** 証明書を別の証明書にリンクするには:

1. NetScaler Application Delivery Management（ADM）で、[ネットワーク] > [**SSL** ダッシュボード] に移動します。
2. いずれかのグラフをクリックして、SSL 証明書の一覧を表示します。
3. 関連付ける証明書を選択して、[**Action**] ボックスの一覧から [**Link**] を選択します。
4. 一致する証明書の一覧から関連付ける対象の証明書を選択して、[**OK**] をクリックします。

> 注
>
> 一致する証明書がない場合は「No certificate found to link.」というメッセージが表示されます。

NetScaler ADM を使用して **SSL** 証明書のリンクを解除するには:

1. NetScaler ADM で、[ネットワーク] > [**SSL** ダッシュボード] に移動します。
2. いずれかのグラフをクリックして、SSL 証明書の一覧を表示します。
3. 関連付けられているいずれかの証明書を選択し、[**Action**] ボックスの一覧から [**Unlink**] をクリックします。
4. [**OK**] をクリックします。

> 注
>
> 選択した証明書が別の証明書に関連付けられていない場合、「Certificate does not have any CA link.」というメッセージが表示されます。

エンタープライズポリシーの構成

February 6, 2024

エンタープライズポリシーを構成し、すべての信頼できる CA、安全な署名アルゴリズムを追加し、NetScaler Application Delivery Management（ADM）で証明書キーの推奨キー強度を選択できます。Citrix Application Delivery Controller（ADC）インスタンスにインストールされた証明書のいずれかがエンタープライズポリシーに

追加されていない場合、SSL 証明書ダッシュボードには、それらの証明書の発行元が「推奨されません」と表示されます。

また、証明書のキー強度が、企業のポリシーで推奨されているキー強度と同じでない場合、SSL 証明書のダッシュボードには、これらのキーの強度が［Not Recommended］として表示されます。

NetScaler ADM でエンタープライズポリシーを構成するには:

1. Citrix ADM で、［インフラストラクチャ］>［**SSL** ダッシュボード］に移動し、［設定］をクリックします。
2. SSL 設定のページで、編集アイコンをクリックし、信頼できるすべての認証機関と安全な署名アルゴリズムを追加して、証明書のキーの推奨キー強度を選択します。
3. ［**Save**］をクリックして、企業のポリシーを保存します。

NetScaler ADC インスタンスからの **SSL** 証明書のポーリング

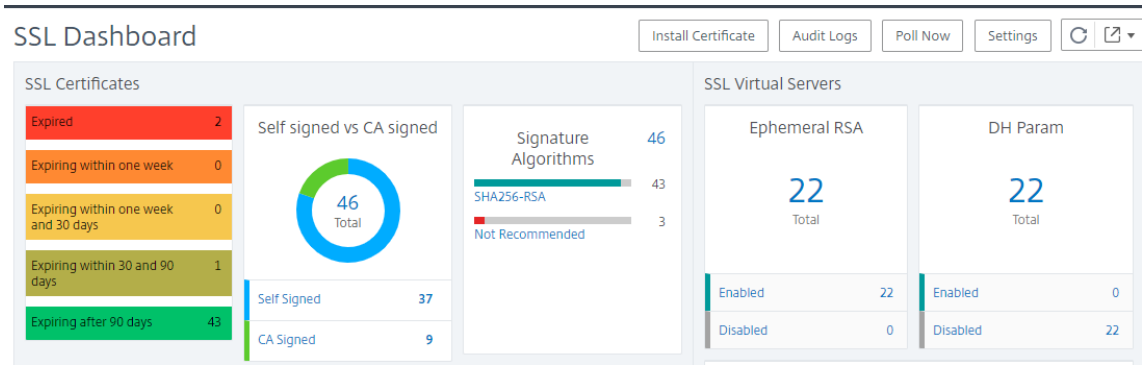
February 6, 2024

Citrix の Application Delivery Management（ADM）は、NITRO コールとセキュアコピー（SCP）プロトコルを使用して、24 時間に 1 回、SSL 証明書を自動的にポーリングします。SSL 証明書を手動でポーリングして、Citrix Application Delivery Controller（ADC）インスタンスに新しく追加された SSL 証明書を見つけることもできます。すべての NetScaler ADC インスタンスの SSL 証明書をポーリングすると、ネットワークに大きな負荷がかかります。

すべての NetScaler ADC インスタンスの SSL 証明書をポーリングする代わりに、選択した 1 つまたは複数のインスタンスの SSL 証明書のみを手動でポーリングできます。

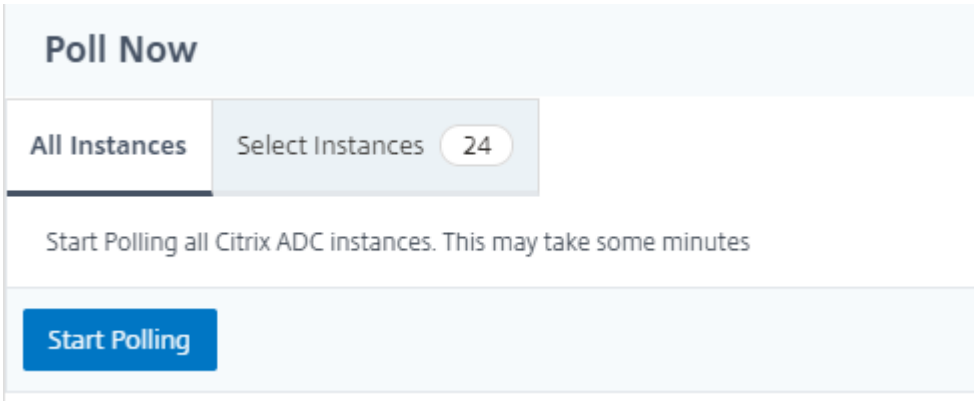
NetScaler ADC インスタンスで **SSL** 証明書をポーリングするには:

1. NetScaler ADM で、［ネットワーク］>［**SSL** ダッシュボード］に移動します。
2. [**SSL** ダッシュボード] ページの右上隅にある [今すぐポーリングする] をクリックします。

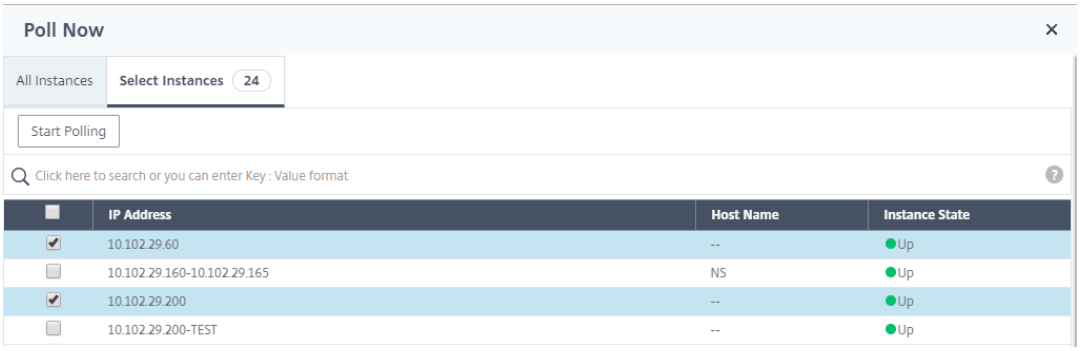


3. **Poll Now** ページが表示され、ネットワーク内のすべての Citrix ADC インスタンスをポーリングするか、選択したインスタンスをポーリングするかを選択できます。

a) すべての Citrix ADC インスタンスの SSL 証明書をポーリングするには、［すべてのインスタンス］タブを選択し、［ポーリング開始］をクリックします。



b) 特定のインスタンスをポーリングするには、**[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。**



構成ジョブ

February 6, 2024

NetScaler Application Delivery Management（NetScaler ADM）構成管理プロセスにより、ネットワーク内の複数の Citrix Application Delivery Controller（ADC）インスタンス間で、構成の変更、システムのアップグレード、およびその他のメンテナンスアクティビティを適切に複製できます。

Citrix ADM では、これら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、システムに対するコマンドと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

新しいジョブを作成しながら設定テンプレートを作成し、構成コマンドのセットをテンプレートとして保存できます。これらのテンプレートは、[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。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ことも、後で実行するようにジョブにスケジュールを指定することもできます。

インスタンス

Citrix ADC リリース 11.0 以降を実行している Citrix SDX インスタンスのシングルバンドルアップグレードを実行できます。シングルバンドルのアップグレードを実行するには、NetScaler ADM 組み込みタスクを使用します。実行中の構成または保存された構成を抽出し、同じタイプの別の Citrix ADC インスタンスでコマンドを実行することで、Citrix 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 を使用すると、独自の CLI コマンドを入力することも、記録して再生ボタンを使用して Citrix ADC セッションからコマンドを取得することもできます。ジョブを実行すると、選択したインスタンスの ns.conf の変更が記録され、NetScaler ADM にコピーされます。

関連トピック

- 構成ジョブで SCP（put）コマンドを使う方法
- 設定ジョブで変数を使用する方法
- 修正コマンドから構成ジョブを作成する方法
- 設定テンプレートを使用して監査テンプレートを作成する方法
- 記録と再生を使用して構成ジョブを作成する方法
- NetScaler ADM でマスター構成テンプレートを使用する方法

構成ジョブの作成

February 6, 2024

ジョブとは、1 つまたは複数の管理対象インスタンスに対して作成および実行できる構成コマンドのセットです。Citrix Application Delivery Management（ADM）GUI を使用して、[インスタンス間で構成を変更したり、ネットワーク上の複数のインスタンスで構成を複製したり](https://docs.citrix.com/ja-jp/netscaler-mas/11-1/configuration-jobs-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. [ネットワーク**] > [**構成ジョブ**]** に移動します。
2. [ジョブの作成] をクリックします。
3. 「ジョブの作成」ページの「構成を選択」タブで、ジョブ名を指定し、ドロップダウンリストからインスタンスタイプを選択します。

4. 「構成ソース」ドロップダウンリストで、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」ドロップダウンリストから、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アンドドロップします。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、マスター構成、録音と再生、インスタンス、ファイルがあります。

   > 注
   >
   > Deploy Master Configuration ジョブテンプレートを初めて追加し、次に別のタイプのテンプレートを追加すると、ジョブテンプレート全体がマスター設定タイプになります。

5. 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。設定ジョブの編集中に、後で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。
6. これらのパラメーターにさまざまな値を割り当てることや 1 つのジョブを複数のインスタンスにわたって実行することができるようになる変数を定義できます。構成ジョブの作成または編集中に定義したすべての変数を、1 つの統合ビューで確認できます。「変数 をプレビュー」タブをクリックすると 、構成ジョブの作成または編集時に定義した単一の統合ビューで変数をプレビューできます。
7. 「インスタンスの 選択」 タブで、構成監査を実行するインスタンスを選択し、「次へ」をクリック します。
8. [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。
9. ［次へ］をクリックします。
10. 各インスタンスで実行されるコマンドは、[ジョブプレビュー] タブで評価および 検証でき ます。ロールバックコマンドを評価するには、「ロールバックコマンドをプレビュー」チェックボックスを選択します。
11. [実行] タブで 、ジョブを今すぐ実行するか、後でジョブを実行するようにスケジュールするかを選択します。また、コマンドが失敗した場合に Citrix ADM が実行するアクションも選択する必要があります。

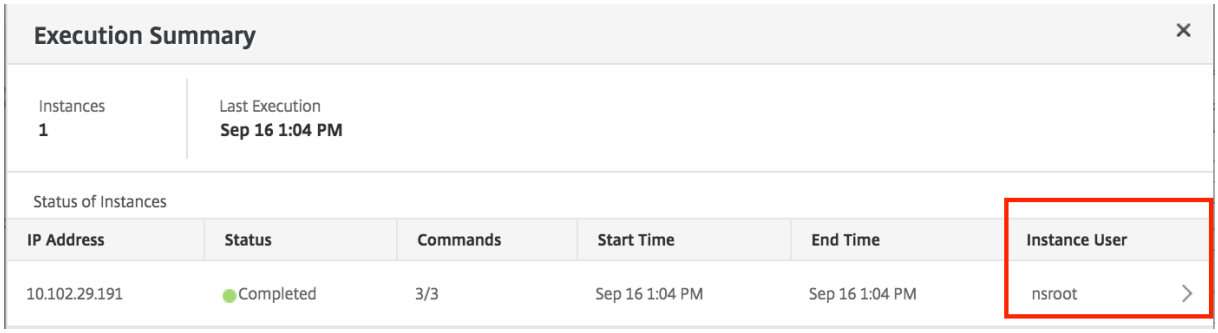
ジョブのメール通知を送信するには**:**

ジョブを実行またはスケジュールするたびにメール通知が送信されるようになりました。メール通知には、ジョブの成否と関連事項などの詳細が記載されます。

ジョブを作成したら、［Execute］タブの［Receive Execution Report Through］セクションで、［**Email**］チェックボックスをオンにします。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。

実行要約の詳細を表示する手順は、次のとおりです。

[ネットワーク] > [構成ジョブ] に移動します。ジョブを選択して［**Details**］をクリックします。[**Execution Summary**] をクリックすると、ジョブを実行したインスタンスのステータス、ジョブで実行されたコマンド、ジョブの開始時刻と終了時刻、およびインスタンスユーザーの名前が表示されます。



レコードアンドプレイを使用して構成ジョブを作成する

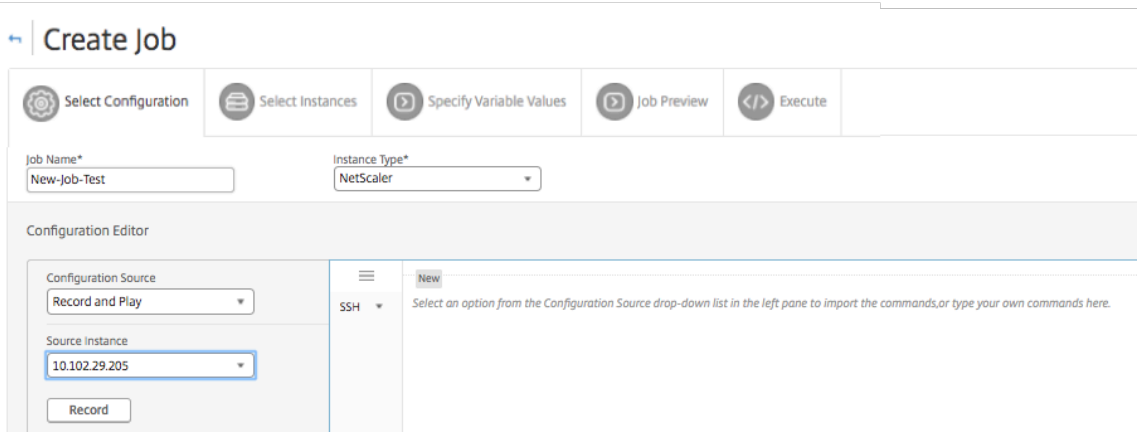
February 6, 2024

NetScaler GUI による NetScaler インスタンスの構成に慣れていると、正確な CLI コマンドを思い出して構成タスクを作成し、それを複数の NetScaler インスタンスで実行するのが面倒に感じる場合があります。

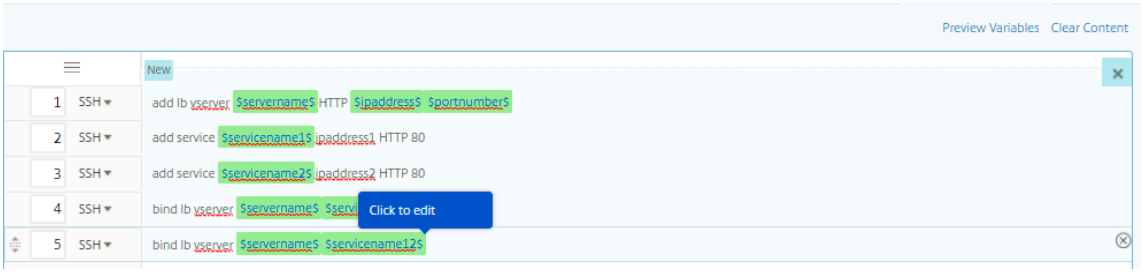
NetScaler ADM を使用すると、NetScaler インスタンスの GUI を使用して実行された構成タスクを記録し、CLI コマンドに変換できます。変換された CLI コマンドから構成タスクを作成し、複数のインスタンスでそのタスクを実行できます。

GUI による構成を記録して構成タスクに変換するには

1. ［**Networks**］**>** ［**Configuration Jobs**］の順に選択してから、［**Create Job**］をクリックします。
2. ジョブ名とインスタンスのタイプを指定します。
3. 「設定ソース」リストから「記録して再生」を選択し、構成を記録するソースインスタンスを選択します。［**Record**］をクリックします。



4. **NetScaler** の **GUI** が開きます。構成タスクに含める機能と設定を構成します。次に、NetScaler GUI ウィンドウを閉じて、[**Configuration Editor**] の [**Stop**] をクリックします。左ペインにコマンドがリンクとして表示されます。コマンドを右ペインにドラッグアンドドロップし、[**Next**] をクリックします。

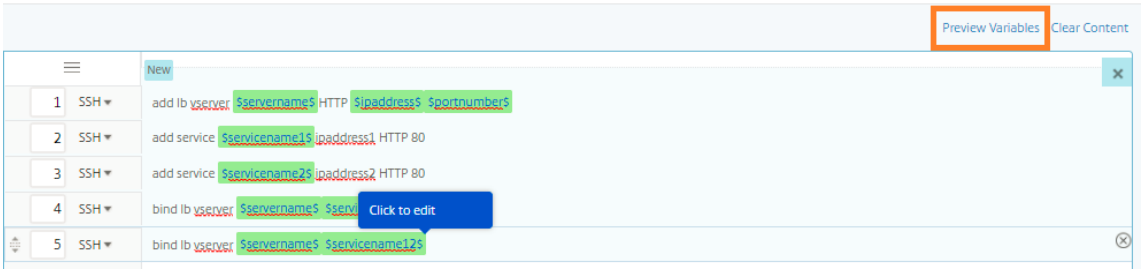


その後、構成レーションエディタでコマンドを並べ替えたり、並べ替えたりすることができます。コマンドラインをドラッグアンドドロップすることで、コマンドをある行から別の行に移動できます。テキストボックスでコマンドライン番号を変更するだけで、コマンドラインを 1 行から任意のターゲットラインに移動または再配置することもできます。

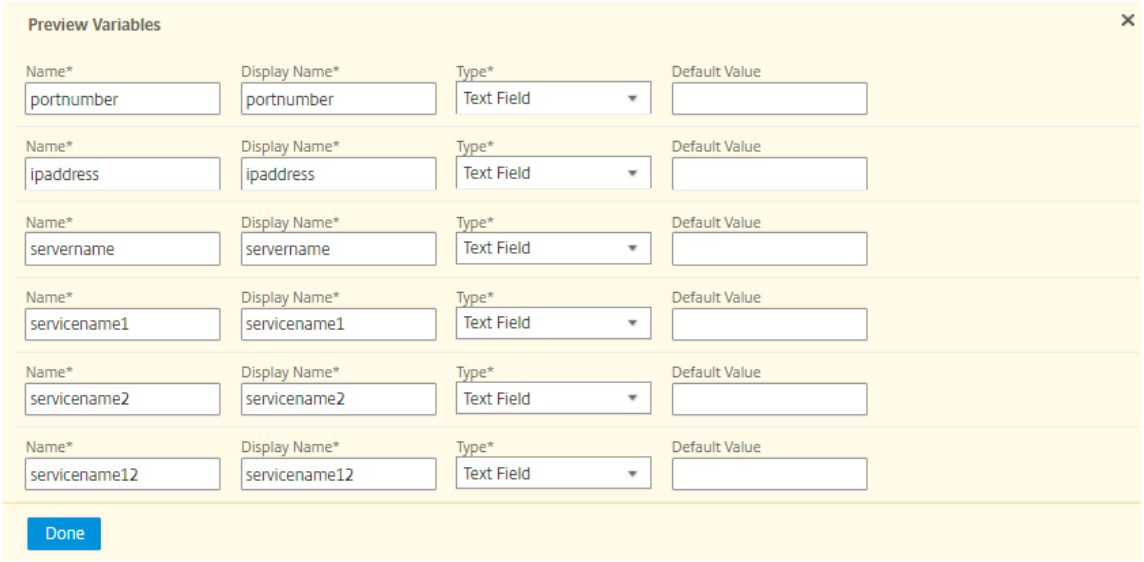
5. 構成ジョブの作成または編集中に定義したすべての変数を、1 つの統合ビューで確認できます。
6. 次のいずれかの操作を行って、すべての変数を 1 つの統合ビューに表示します。

   - 構成ジョブを作成するときに、[ネットワーク] **>** [構成ジョブ] に移動し、[ジョブの作成] を選択します。[**Create Job**] ページでは、構成ジョブの作成時に追加したすべての変数を確認できます。
   - 構成ジョブの編集中に、[ネットワーク] **>** [構成ジョブ] に移動し、ジョブ名を選択して [編集] をクリックします。[ジョブの構成] ページでは、構成ジョブの作成時に追加されたすべての変数を確認できます。

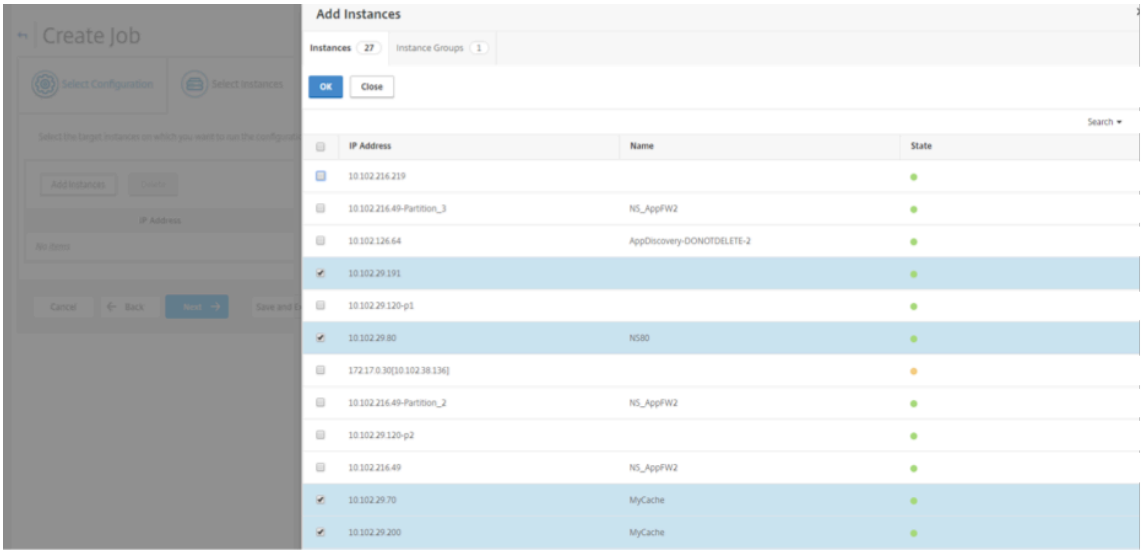
7. 次に、「変数のプレビュー」タブをクリックすると、構成ジョブの作成または編集中に定義した単一の統合ビューで変数をプレビューできます。



8. 新しいポップアップウィンドウが表示され、名前、表示名、タイプ、デフォルト値などの変数のすべてのパラメータが表形式で表示されます。これらのパラメータを編集および修正することもできます。パラメータを編集または変更したら、[完了] ボタンをクリックします。



9. [**Add Instance**s] をクリックし、構成ジョブを実行するインスタンスを選択します。[**OK**] をクリックし、[次へ] をクリックします。



10. コマンドで変数を指定した場合は、**[Specified Variable Value**s] タブで、次のいずれかのオプションを選

択して、インスタンスの変数を指定します:

- 変数値の入力ファイルをアップロード**:**「入力キー ファイルをダウンロード」をクリック して入力ファイルをダウンロードします。入力ファイルで、コマンドで定義した変数の値を入力し、NetScaler ADM サーバーにファイルをアップロードします。
- すべてのインスタンスに共通の変数値: 変数の値を入力します。選択したテンプレートによって、変数は変わります。

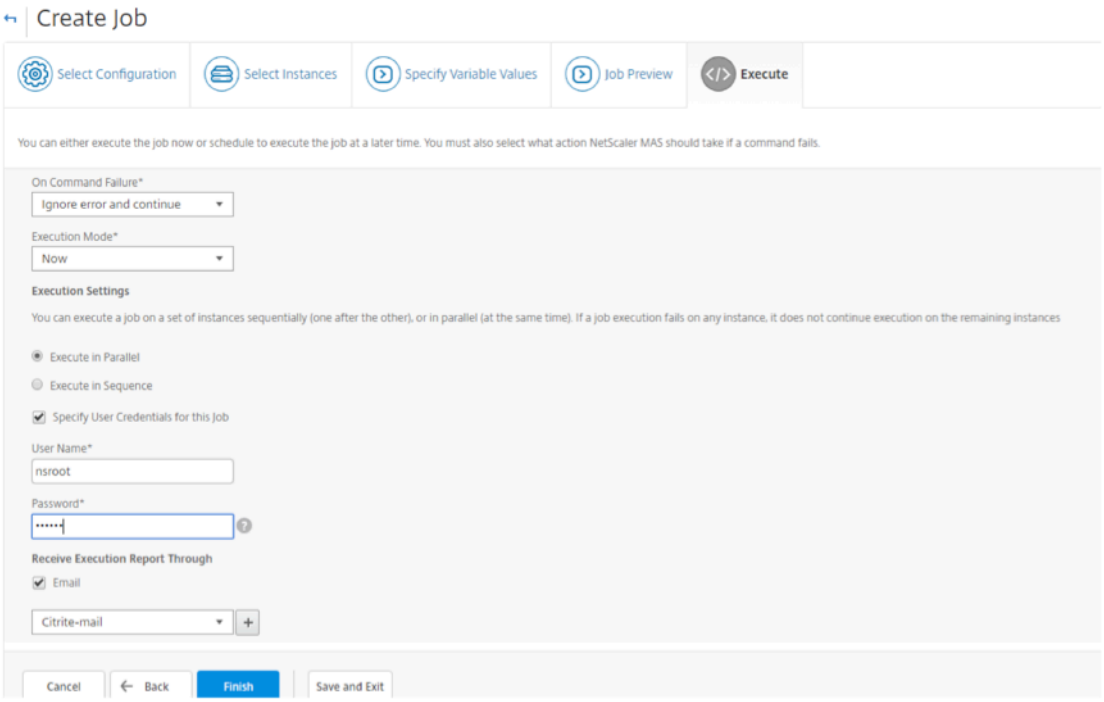
変数値を含む入力ファイルは、設定ジョブで (同じファイル名で) 保持されます。設定ジョブの作成または編集中に、以前に使用およびアップロードした入力ファイルを表示および編集できます。

構成ジョブの作成中に実行された構成ジョブを表示するには、[ネットワーク**] > [**構成ジョブ] に移動し、[ジョブの作成] をクリックします。**[** ジョブの作成] ページ。[変数値の指定] タブで、[すべてのインスタンスに共通の変数値] オプションを選択し、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします（同じファイル名を維持します)。

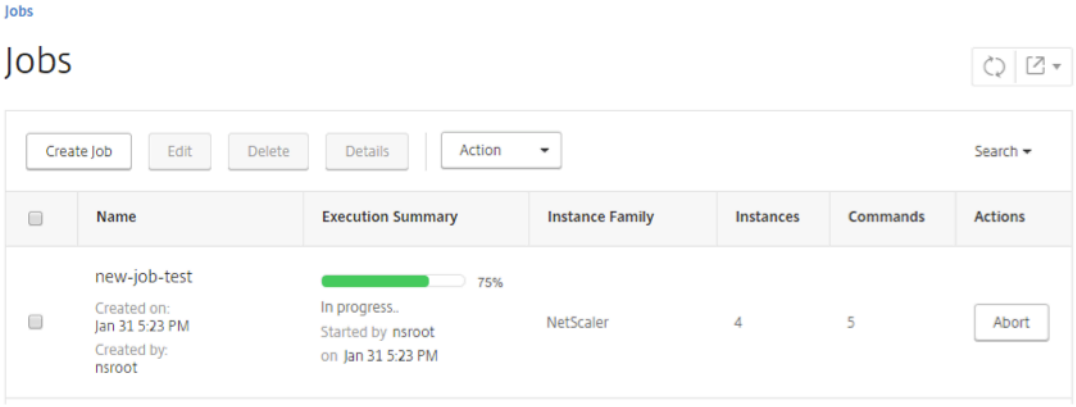
構成ジョブの編集中に実行済みの構成ジョブを表示するには、[ネットワーク**] > [**構成ジョブ] に移動し、ジョブ名を選択して [編集] をクリックします。[ジョブの設定] ページの [変数値の指定] タブで、[すべてのインスタンスに共通変数値] オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします (同じファイル名を使用)。10. [**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。

11. [**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および確認できます。
12. [**Execute**] タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。コマンドが失敗した場合に Citrix ADM が実行するアクションを選択することもできます。

    権限のあるユーザーに管理対象インスタンス上でのジョブの実行を許可するように選択することもできます。また、その他の詳細と共にジョブの成功や失敗に関してメール通知を送信するかどうかを選択できます。



13. [**Jobs**] ページでは、すべてのインスタンスでの設定タスク実行の進行状況を表示できます。



構成ジョブを使用して、1 つのインスタンスから複数のインスタンスに構成を複製する

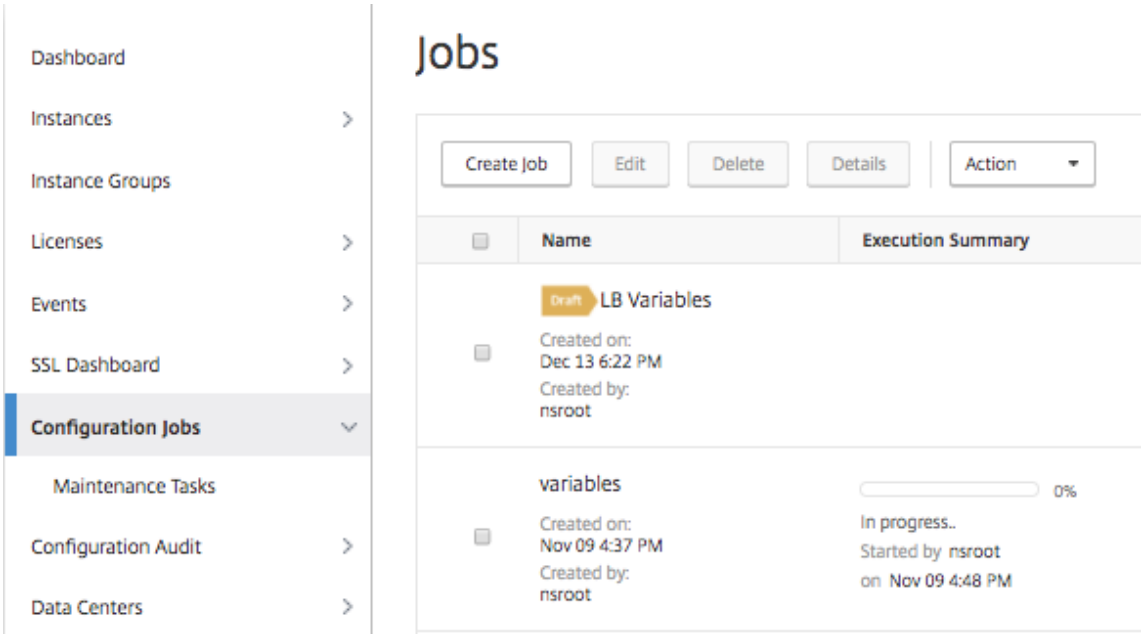
February 6, 2024

Citrix ADM の構成ジョブ機能を使用して、NetScaler インスタンスから特定の構成を抽出し、それを複数のインスタンスに複製できます。

たとえば、展開環境の NetScaler インスタンスで負荷分散とフロントエンド最適化（FEO）の両方を構成している場合があります。しかし、ここで、FEO 構成のみを他の NetScaler インスタンスに複製する必要があります。

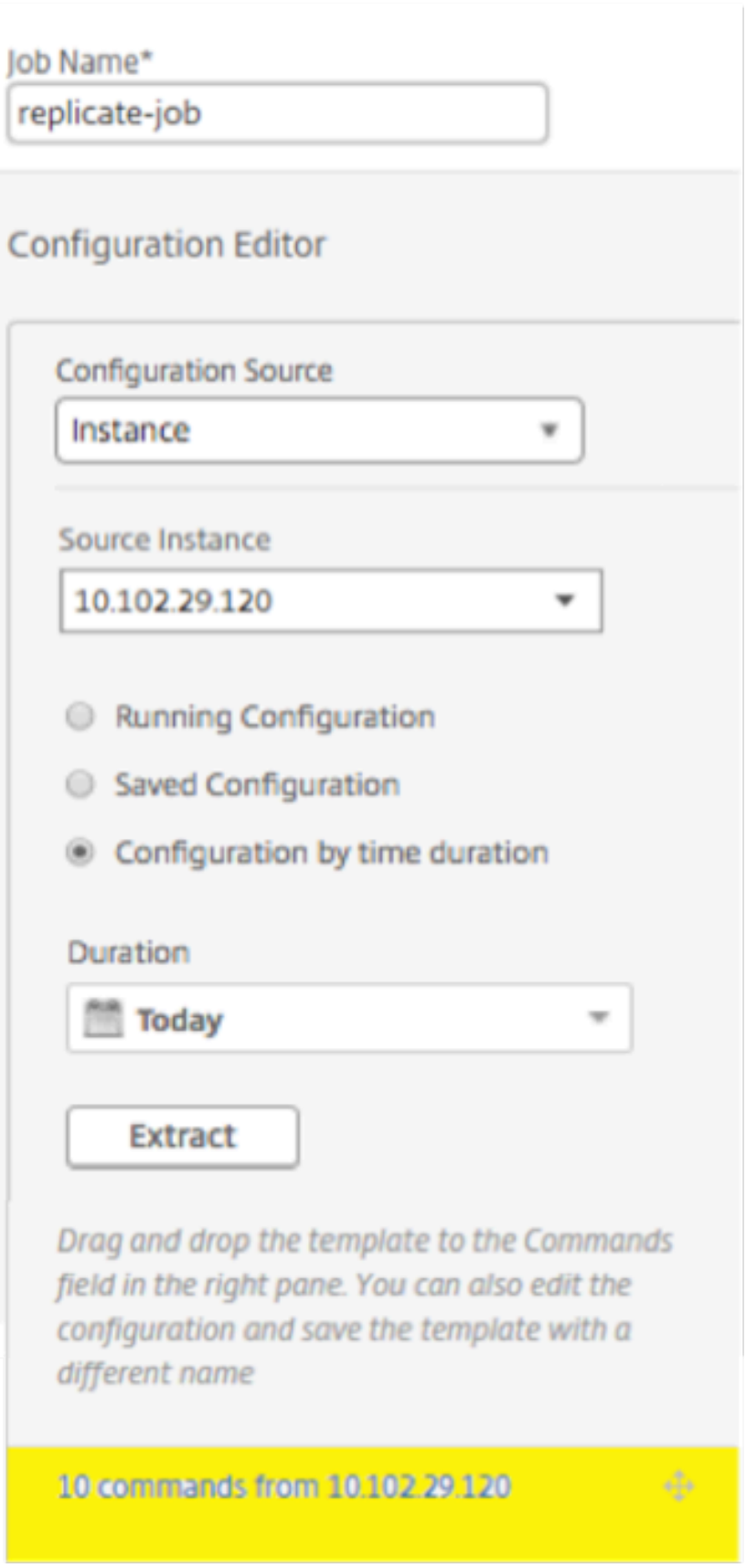
あるインスタンスから他の **NetScaler** インスタンスに構成を取得して複製するには：

1. ［**Networks**］>［**Configuration Jobs**］の順に選択してから、［**Create Job**］をクリックします。



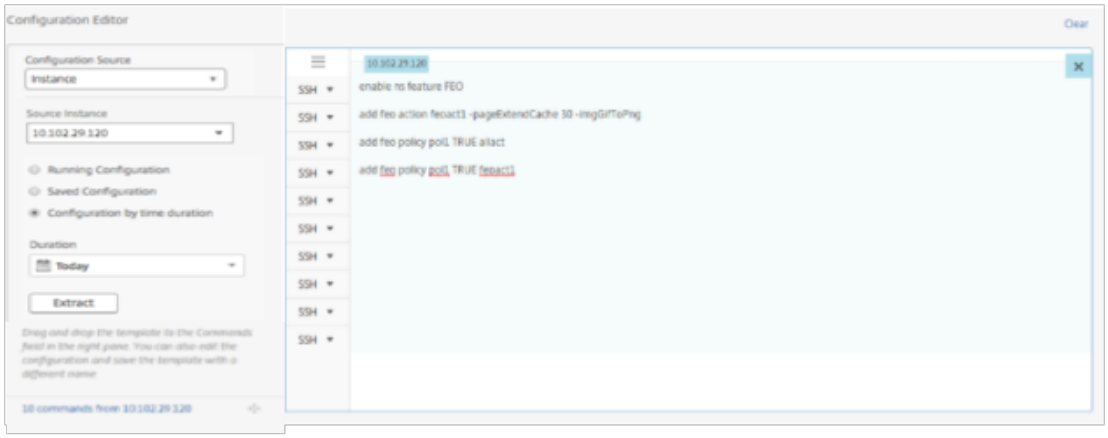
2. ジョブ名とインスタンスのタイプを指定します。
3. 構成ソースとして [インスタンス] を選択し、構成を複製するソースインスタンスを選択します。抽出する設定のタイプを選択します。[期間による構成] を選択した場合は、この構成を実行した期間を設定し、[抽出] をクリックします。

   選択した期間にそのインスタンスで実行されたコマンドの数が次の図のように画面に表示されます。



4. コマンドを右ペインのコマンドフィールドにドラッグアンドドロップします。

FEO に関するコマンドのみを保持します。負荷分散に関するコマンド、または他のすべての構成に関するコマンドは手動で削除し、［**Next**］をクリックします。



5. [**Add Instanc** es] をクリックし、FEO 設定を適用するインスタンスを追加します。「**OK**」をクリックし、次に「次へ」をクリックします。
6. コマンドに変数を指定した場合は、［Specify Variable Values］タブで［**Download Input Key File**］をクリックします。ダウンロードしたファイルで、変数の値を指定し、NetScaler ADM にファイルをアップロードします。
7. [**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。
8. ［**Execute**］タブで［**Finish**］をクリックすると、選択した NetScaler インスタンスでジョブが実行されます。

構成ジョブでの変数の使用

February 6, 2024

構成ジョブとは、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。複数のインスタンスで同じ構成を実行する場合は、構成内で使用されているパラメーターに対して、さまざまな値を使用できます。これらのパラメーターにさまざまな値を割り当てることや 1 つのジョブを複数のインスタンスにわたって実行することができるようになる変数を定義できます。

たとえば、負荷分散仮想サーバーを追加し、2 つのサービスを追加し、それらのサービスをその仮想サーバーにバインドするという、基本的な負荷分散構成を考えてみましょう。ここでは、2 つのインスタンスで同じ構成を使用するが、仮想サーバーとサービスの名前および IP アドレスに異なる値を使用する必要があるとします。これを実現するには、変数を使用して仮想サーバーとサービスの名前および IP アドレスを定義することで、構成ジョブ機能を使用します。

この例では、次のコマンドと変数を使用します。

lb 仮想サーバーサーバー名 HTTP IP アドレス ポート番号を追加

サービス名 1、IP アドレス **1** 、HTTP 80 を追加

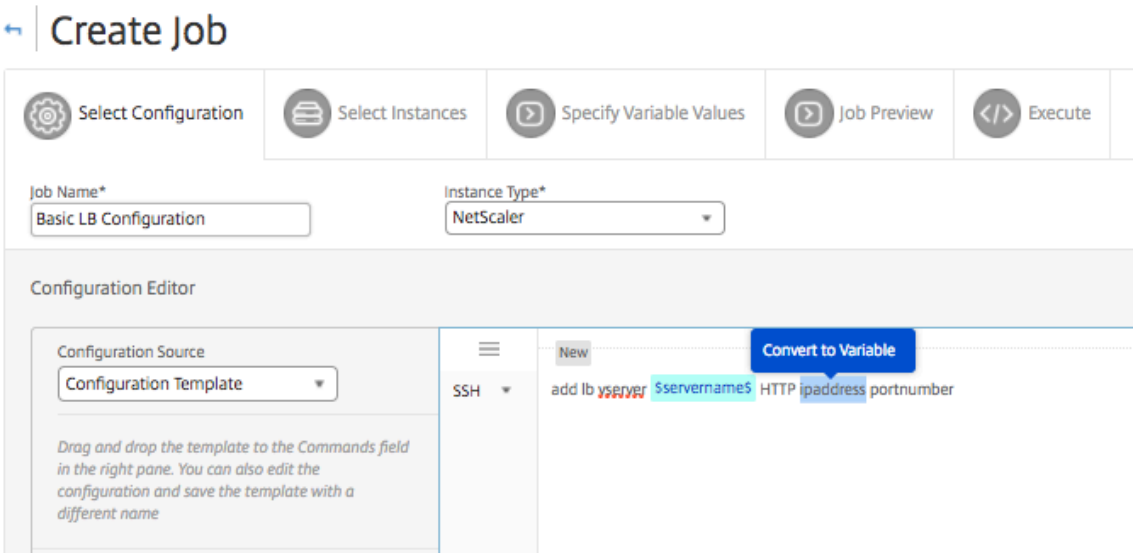
サービス名/サービス名/**2** IP アドレス**/2** HTTP 8.0 を追加

bind lb vserver サーバ名サービス名 **1**

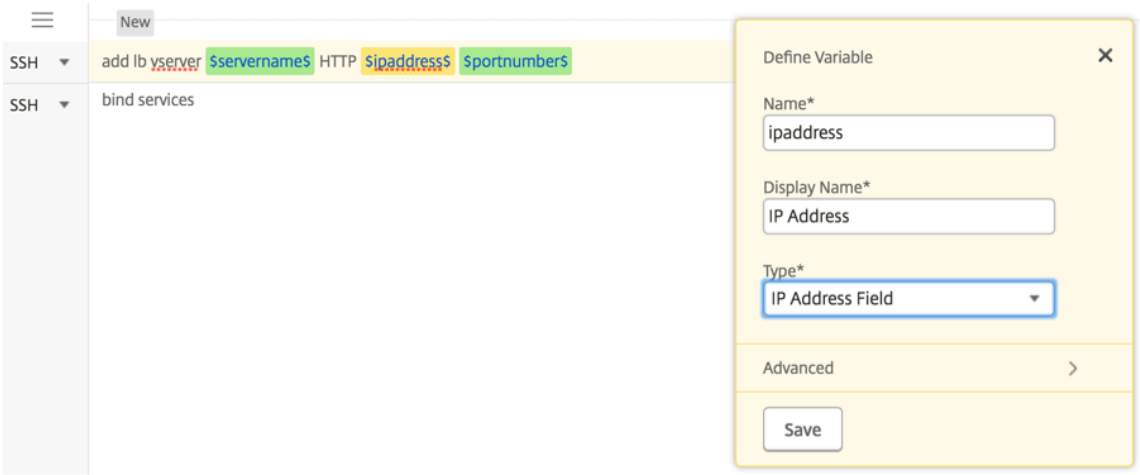
bind lb vserver サーバー名サービス名 **2**

NetScaler ADM で変数を定義して構成ジョブを作成するには:

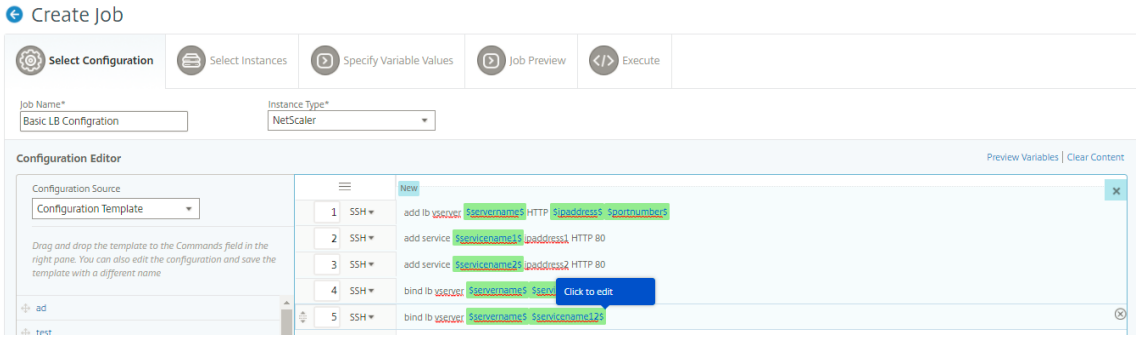
1. [ネットワーク] > [構成ジョブ] に移動します。
2. [ジョブの作成] をクリックします。
3. **Create Job** ページで、ジョブの名前、インスタンスタイプ、設定タイプなどのカスタムジョブパラメータを選択します。
4. [Configuration Editor] でコマンドを入力して、負荷分散仮想サーバー、2 つのサービスを追加し、それらのサービスをその仮想サーバーにバインドします。変数に変換する値をダブルクリックして選択し、[変数に変換] をクリックします。たとえば、負荷分散サーバーの *IP* アドレスの *IP* アドレスを選択し、次の図に示すように [変数に変換] をクリックします。



5. 変数の値がドル記号で囲まれたら、変数をクリックして、名前、表示名、種類など、変数の詳細をさらに指定します。変数のデフォルト値をさらに指定する場合は、「詳細」(**Advanced**) オプションをクリックすることもできます。[保存] をクリックし、[次へ] をクリックします。



残りのコマンドを入力し、すべての変数を定義します。

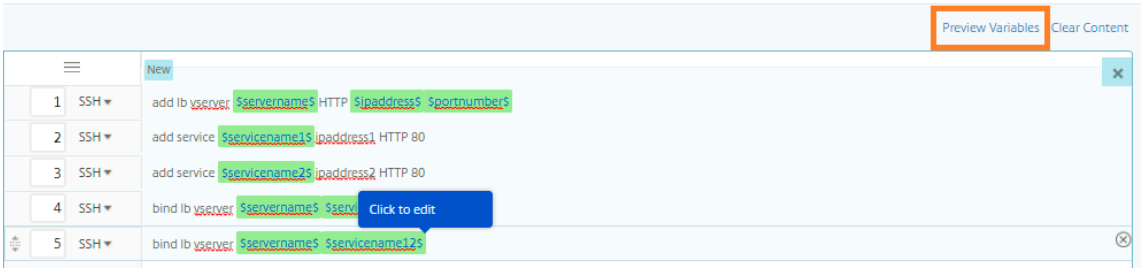


6. 構成ジョブの作成または編集中に定義したすべての変数を、1 つの統合ビューで確認できます。

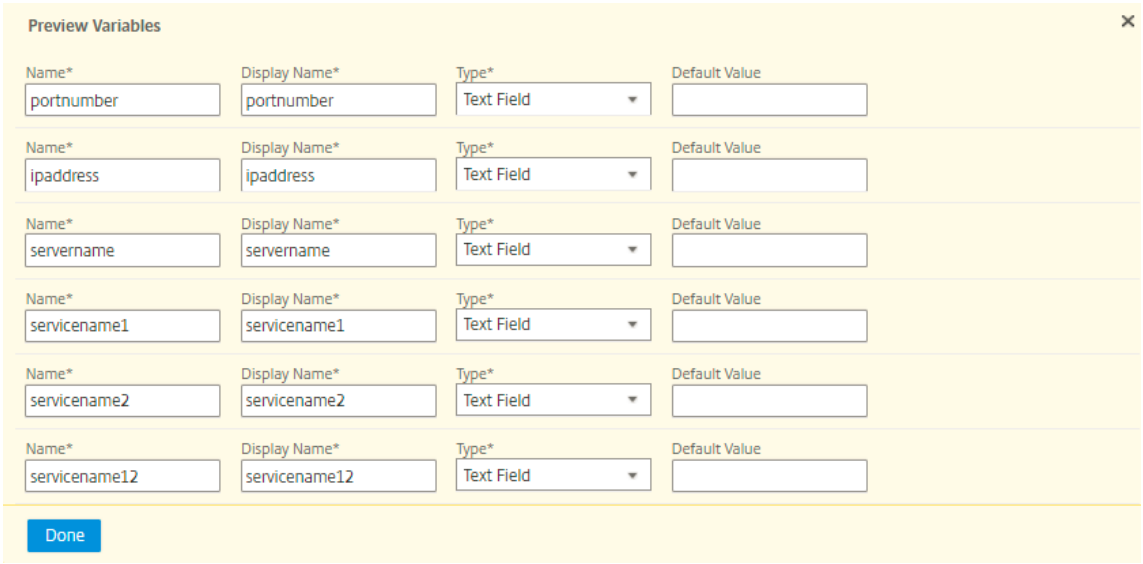
7. 次のいずれかの操作を行って、すべての変数を 1 つの統合ビューに表示します。

   - 構成ジョブを作成するときに、[ネットワーク**] > [**構成ジョブ] に移動し、[ジョブの作成] を選択します。[**Create Job**] ページでは、構成ジョブの作成時に追加したすべての変数を確認できます。
   - 構成ジョブの編集中に、[ネットワーク**] > [**構成ジョブ] に移動し、ジョブ名を選択して [編集] をクリックします。[ジョブの構成] ページでは、構成ジョブの作成時に追加されたすべての変数を確認できます。

8. 次に、「変数のプレビュー」タブをクリックすると、構成ジョブの作成または編集中に定義した単一の統合ビューで変数をプレビューできます。



9. 新しいポップアップウィンドウが表示され、名前、表示名、タイプ、デフォルト値などの変数のすべてのパラメータが表形式で表示されます。これらのパラメータを編集および修正することもできます。パラメータを編集または変更したら、[完了] ボタンをクリックします。



10. その後、構成レーションエディタでコマンドを並べ替えたり、並べ替えたりすることができます。コマンドラインをドラッグアンドドロップすることで、コマンドをある行から別の行に移動できます。テキストボックスでコマンドライン番号を変更するだけで、コマンドラインを 1 行から任意のターゲットラインに移動または再配置することもできます。

11. 構成ジョブを実行するインスタンスを選択します。

12. 「変数値の指定」タブで、「変数値の入力ファイルをアップロード」オプションを選択し、「入力キーファイルのダウンロード」をクリックします。例では、各インスタンス上のサーバー名、サーバーとサービスの IP アドレ

ス、ポート番号、およびサービス名を指定する必要があります。ファイルを保存し、アップロードします。値が正確に定義されていない場合は、システムによってエラーがスローされる場合があります。

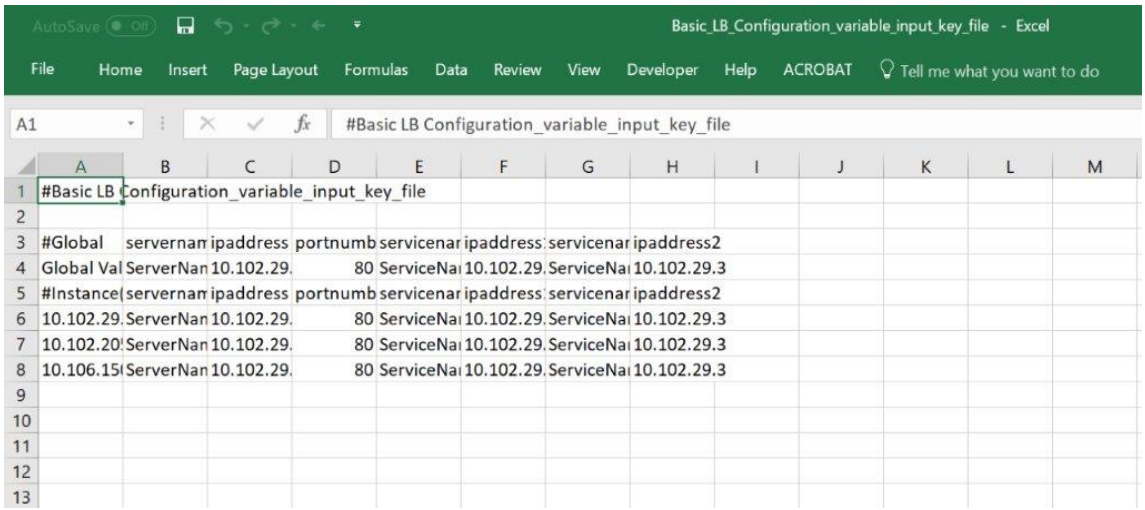
13. 入力キーファイルはローカルシステムにダウンロードされ、以前に選択した各 NetScaler インスタンスの変数値を指定して編集できます。［アップロード］をクリックして入力キーファイルを Citrix ADM にアップロードします。［次へ］をクリックします。入力キーファイルがローカルシステムにダウンロードされ、以前に選択した各 NetScaler インスタンスの変数値を指定することで編集できます。

    > 注：入力キーファイルでは、変数は 3 つのレベルで定義されています。
    >
    > - グローバルレベル
    > - インスタンスグループレベル
    > - インスタンスレベル

    グローバル変数は、すべてのインスタンスに適用される変数値です。インスタンスグループレベルの変数値は、グループで定義されているすべてのインスタンスに適用されます。インスタンスレベルの変数値は、特定のインスタンスにのみ適用されます。

    NetScaler ADM では、インスタンスレベルの値が最優先されます。個々のインスタンスの変数に値が提供されていない場合、NetScaler ADM はグループレベルで提供された値を使用します。グループレベルで値が指定されていない場合、NetScaler ADM はグローバルレベルで提供された変数値を使用します。3 つのレベルすべてにわたって変数の入力を指定すると、NetScaler ADM はインスタンスレベル値をデフォルト値として使用します。

14.「アップロード」をクリックして、入力キーファイルを Citrix ADM にアップロードします。［次へ］をクリックします。



> 重要
>
> Mac から CSV ファイルをアップロードすると、CSV ファイルはコンマではなくセミコロンで保存されます。これにより、入力ファイルをアップロードしてジョブを実行すると、設定が失敗します。Mac を使用している場合は、テキストエディタを使用して必要な変更を行い、ファイルをアップロードします。

15. すべてのインスタンスに共通の変数値を指定し、「アップ ロード」をクリック して入力キーファイルを Citrix ADM にアップロードすることもできます。

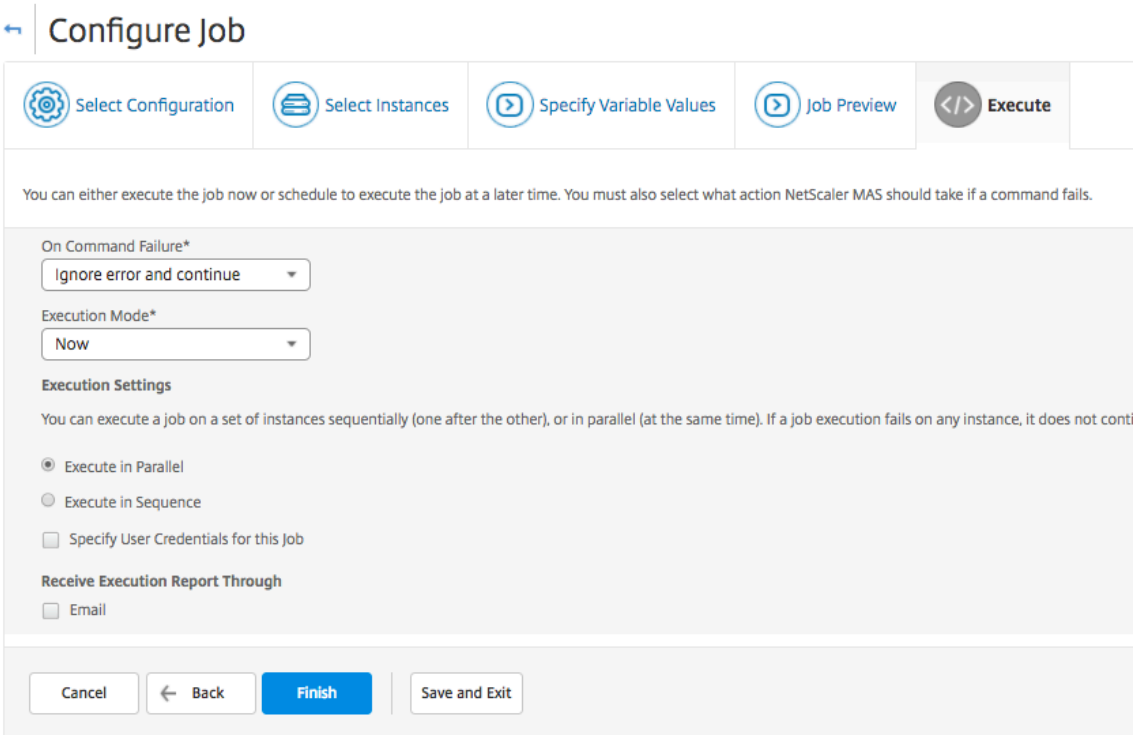
    変数値を含むキー入力ファイルは、設定ジョブで (同じファイル名で) 保持されます。設定ジョブの作成または編集中に、以前に使用およびアップロードした入力ファイルを表示および編集できます。

    構成ジョブの作成中に実行された構成ジョブを表示するには、[ネットワーク**] > [**構成ジョブ] に移動し、[ジョブの作成] をクリックします。**[** ジョブの作成] ページ。[変数値の指定] タブで、[すべてのインスタンスに共通の変数値] オプションを選択し、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします（同じファイル名を維持します）。

    構成ジョブの編集中に実行済みの構成ジョブを表示するには、[ネットワーク**] > [**構成ジョブ] に移動し、ジョブ名を選択して [編集] をクリックします。[ジョブの設定] ページの [変数値の指定] タブで、[すべてのインスタンスに共通変数値] オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします（同じファイル名を維持します）。

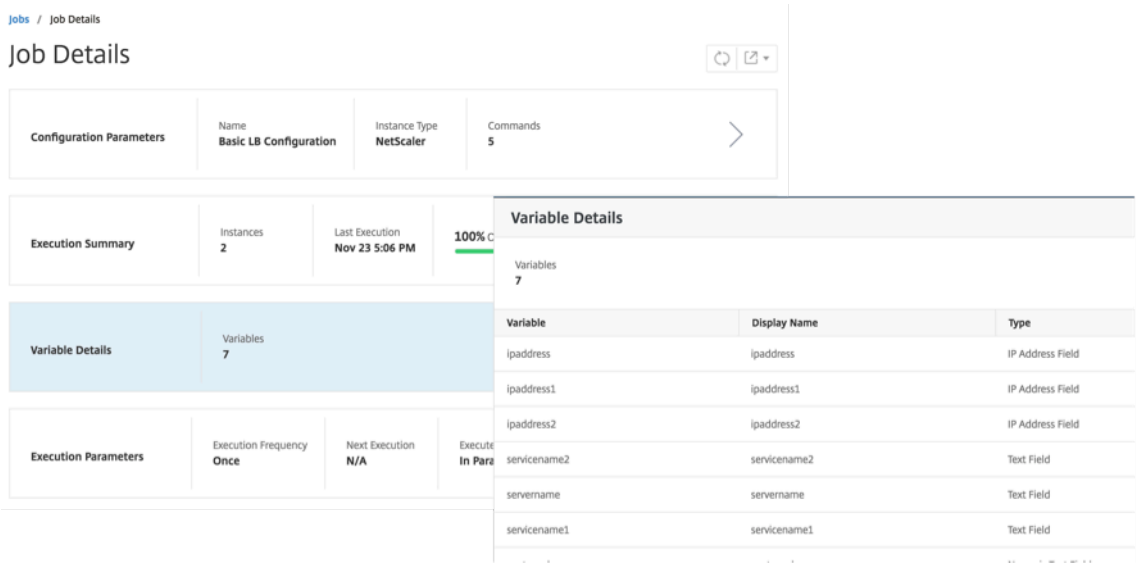
16. [**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。

17. [実行] タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。また、コマンドが失敗した場合に Citrix ADM が実行するアクションや、ジョブの成功または失敗に関する電子メール通知を他の詳細とともに送信するかどうかを選択することもできます。



ジョブを設定して実行したら、[ネットワーク] > [設定ジョブ] に移動し、先ほど設定したジョブを選択すると、ジョブの詳細が表示されます。 [詳細] をクリックし、[変数の詳細] をクリックすると、ジョブに追加された変数のリス

トが表示されます。



> 注
>
> **STEP 5** で変数に指定した値は、ジョブを保存して終了するとき、または後でジョブを実行するようにスケジュールするときに、NetScaler ADM によって保持されます。

修正コマンドからの構成ジョブの作成

February 6, 2024

NetScaler Application Delivery Management（ADM）の監査テンプレート機能を使用して、管理対象の NetScaler ADC インスタンスの構成変更を監視し、構成エラーのトラブルシューティングを行うことができます。

監査テンプレートを用いた構成変更の監査の通常のワークフローは、以下の手順で構成されます。

1. インスタンス構成を監査するための有効/期待される Citrix ADC コマンドのセットを含む監査テンプレートを作成します。
2. 監査テンプレートを実行する NetScaler ADC インスタンスを選択して、実行構成と予想される構成の違いがないか確認します。
3. 差分と修正コマンドを理解し、[Create Job] 機能を利用して、インスタンスの構成を必要な状態にします。

複数の管理者が 5 つの NetScaler ADC インスタンスを管理しているシナリオを考えてみましょう。これらの管理者すべてが、既存のインスタンスの構成に、変更が必要になれば更新するとします。スーパー管理者は他の管理者からの変更にかかわらず、特定の重要な構成の設定は触れられずに保持されることを確保したいと考えます。このユースケースでは、スーパー管理者が Citrix ADC インスタンスに存在すると予想される構成のテンプレートを作成し、そ

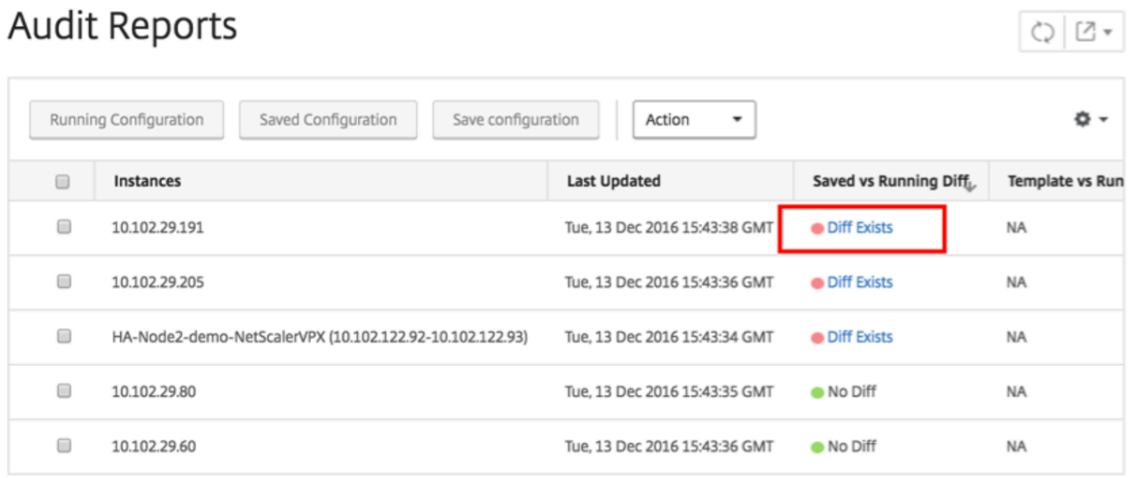
れをインスタンスに対して実行します。NetScaler ADM は監査テンプレート構成と実行構成を比較し、[構成監査] ダッシュボードで不一致を報告します。

一部のインスタンスの構成に変更があることに気付いた場合は、NetScaler ADM 修正コマンド機能を使用して、特定の NetScaler ADC インスタンス用の変更および修正された構成コマンドを含む構成ジョブを作成できます。

監査テンプレート設定と構成実行の間に相違がある場合は、「監査レポート」(Audit Report) ページに「差分」(**Diff Exist** s) ステータスメッセージが表示されます。「相違の出口」リンクをクリックすると、「構成の差分」ページが表示され、修正コマンドを表示できます。また、これらの修正コマンドを使用して構成ジョブを作成し、それを特定の Citrix ADC インスタンスで実行して、目的の構成に戻すこともできます。

NetScaler ADM 修正コマンドで構成ジョブを作成するには

1. [ネットワーク] > [構成監査] に移動します。
2. [構成監査] ページで、2 つのドーナツチャートのいずれかの中をクリックして、[監査レポート] ページにアクセスします。
3. 設定コマンドを修正するインスタンスの「**Diff Exists** 」リンク（表の「保存済みと実行中の相違点」列の下）をクリックします。[**Configuration Diff**] ページが表示され、そのインスタンスの [保存された設定]、[実行設定]、[修正設定] の相違点が一覧表示されます。



4. 「ジョブの作成」をクリックして、「ジョブの作成」ページに移動します。このページには、修正コマンドがあらかじめ入力されています。構成ジョブの作成方法については、「NetScaler ADM で構成ジョブを作成する方法」を参照してください。

ある **NetScaler** インスタンスから別のインスタンスに実行および保存された構成を複製する

February 6, 2024

2018 年 5 月 24 日

NetScaler インスタンスの構成を他のインスタンスに複製できるようになりました。NetScaler ADM でジョブを構成する場合は、構成ソースとしてインスタンスを選択し、選択したインスタンスの実行中または保存された構成を選択します。

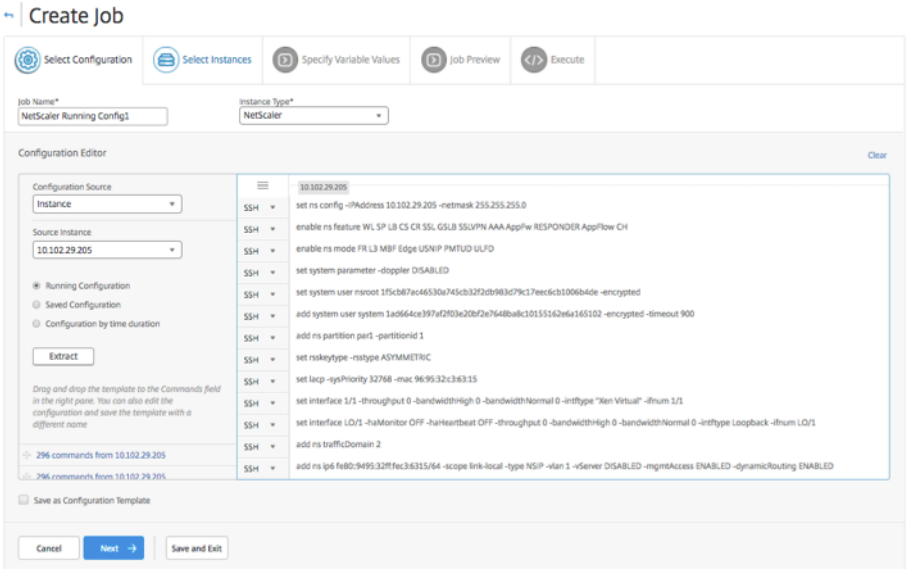
たとえば、NetScaler ADM 実行構成］を選択して［抽出］をクリックすると、選択した NetScaler インスタンスに実行構成を検索する要求が送信され、テンプレートとして表示されます。テンプレートは、右側のペインの [**Command** s] フィールドにドラッグアンドドロップできます。コマンド、パラメーター、およびインスタンスを変更できます。

あるインスタンスの実行および保存された構成コマンドを **NetScaler ADM** 上の別のインスタンスにレプリケートするには:

1. [ネットワーク] > [構成ジョブ] に移動し、[ジョブの作成] をクリックします。
2. ジョブ名とインスタンスのタイプを指定します。たとえば、ジョブの名前として NetScaler Running Config1 を指定し、インスタンスタイプを *NetScaler* として指定します。
3. [構成ソース] として [インスタンス] を選択し、他のインスタンスに構成をレプリケートするソース・インスタンスを選択します。
4. 次の 3 つのオプションが表示されます:
   - ［Running Configuration］
   - ［Saved Configuration］

- [Configuration by time duration]

5. 「実行構成」を選択し、「抽出」をクリックします。そのインスタンス上で実行されている、実行中の構成コマンドの数が表示されます。



6. 右側のペインの **Commands** フィールドにコマンドをドラッグアンドドロップします。
7. [Commands] フィールドでコマンドを編集できます。たとえば、抽出されたコマンドが NetScaler インスタンスのセットアップのためのコマンドだとします。これには、パーティションの追加、負荷分散のセットアップ、サービスへの負荷分散サーバーのバインドが含まれているとします。パーティションなしで新しい NetScaler インスタンスをセットアップするようにコマンドを編集できます。したがって、パーティションを削除するには、パーティションの作成に関連するコマンドを手動で削除し、[次へ] をクリックします。
8. [**Add Instances**] をクリックし、実行中の設定コマンドを適用するインスタンスを追加します。「**OK**」をクリックし、「次へ」をクリックします。
9. コマンドで変数を指定した場合は、[変数値の指定] タブで [入力キーファイルのダウンロード] をクリックします。ダウンロードしたファイルで、変数の値を指定し、NetScaler ADM にファイルをアップロードします。
10. [**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。

11. [実行] タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。また、コマンドが失敗した場合に Citrix ADM が実行するアクションを選択したり、ジョブの成功または失敗に関する電子メール通知を他の詳細とともに送信したりすることもできます。

実行された構成ジョブを再利用

February 6, 2024

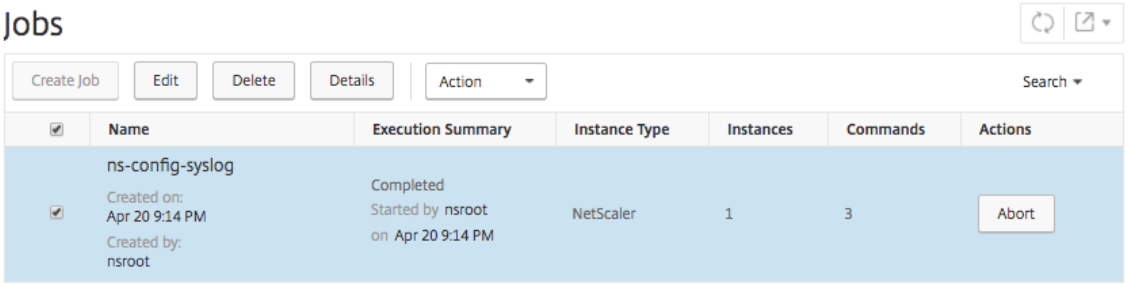
設定ジョブを使用すると、1 つ以上の管理対象インスタンスで実行できる設定コマンドのセットを作成できます。また、保存した構成ジョブのコマンド、パラメーター、構成ソース、インスタンスを変更してから、そのジョブの同様のセットを実行することもできます。これは、同じコマンドセットを別のインスタンスで実行する必要がある場合や、ジョブでエラーが発生してそれ以降の実行が停止する場合に役立ちます。

Citrix Application Delivery Management（ADM）には、完了したジョブを再実行する機能があります。この機能を使用すると、実行が完了したジョブの名前を変えることなく、ジョブを再実行できます。

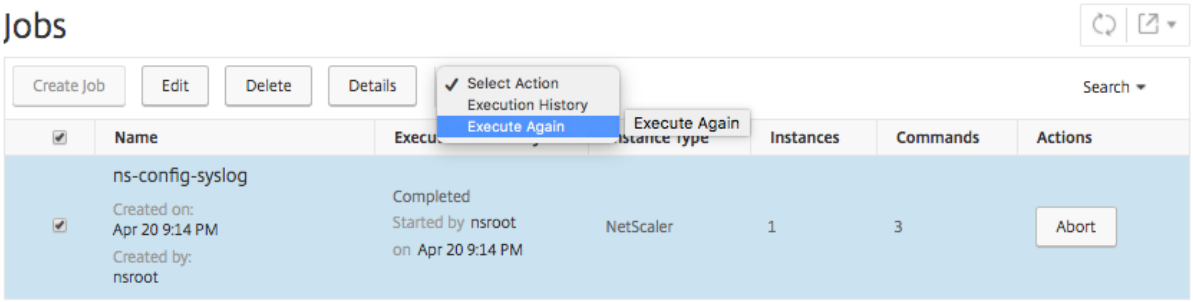
> 注**:** 再実行できるのは、実行モードが「Now」のときに実行されたジョブだけです。

完了したジョブを編集するには、次の手順に従います。

1. Citrix ADM ホームページから、［ネットワーク ］**>**［構成ジョブ］に移動します。
2. 「ジョブ」ページで、「実行サマリー」が「完了」と表示されるジョブを選択し、「編集」をクリックします。スケジュール指定された構成ジョブも編集できます。
3. ［**Configure Job**］ページで、［Job Name］と［Instance Type］が編集できないことを確認できます。構成ソースをはじめとするその他のフィールドの変更、インスタンスの追加、変数値の編集、実行設定の指定を行うことができます。
4. [完了] をクリックして、構成ジョブを再度実行します。



> 注
>
> ジョブを選択し、もう一度 [**Execute**] をクリックすると、ソース、インスタンス、コマンドを変更せずにジョブを実行することもできます。これは、同じインスタンス群に対して同じコマンドセットを実行する必要がある場合に便利です。場合によっては、ジョブがサーバー側から一時的なエラーが発生し、ジョブを再度実行する必要がある場合があります。



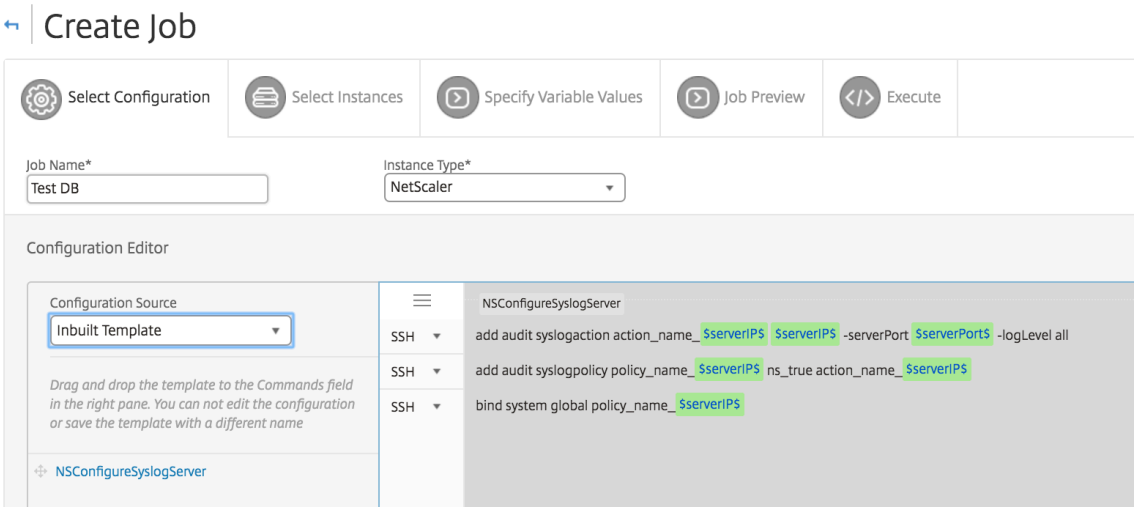
組み込みテンプレートを使用して作成されたジョブをスケジュールする

February 6, 2024

組み込みテンプレートオプションを使用して、ジョブにスケジュールを指定できます。ジョブとは、管理対象インスタンスで実行できる一連の構成コマンドのことです。たとえば、組み込みのテンプレートオプションを使用して、syslog サーバを設定するジョブをスケジュールします。ジョブをすぐに実行するか、後で実行するようにジョブをスケジュールすることもできます。

Citrix Application Delivery Management（**ADM**）で組み込みテンプレートを使用してジョブをスケジュールするには

1. NetScaler ADM で、［ネットワーク］>［構成ジョブ］の順に選択し、［ジョブの作成］をクリックします。
2. [**Create Job**] ページの [**Select Configuration**] タブで、[**Job Name**] を指定し、ドロップダウンリストから [**Instance Type**] を選択します。
3. 「構成ソース」ドロップダウンリストから「作り込みテンプレート」を選択します。*****NSConfigureSyslogServer** コマンドを右側のペインにドラッグアンドドロップし、[次へ]** をクリックします。



4. [インスタンスの選択] タブで、[インスタンスの追加] をクリックし、ジョブを実行するインスタンスを選択し、[**OK**] をクリックします。
5. ［次へ］をクリックします。［**Specify Variable Values**］タブで次のいずれかのオプションを選択してインスタンスの変数を指定します。

   - 入力ファイルからの変数値 -入力ファイルをダウンロードして、コマンドで定義した変数の値を入力します。次に、ファイルを Citrix ADM サーバーにアップロードします。

- **Common variable values for all instances** - Syslog サーバーの IP アドレスとポートを指定します。

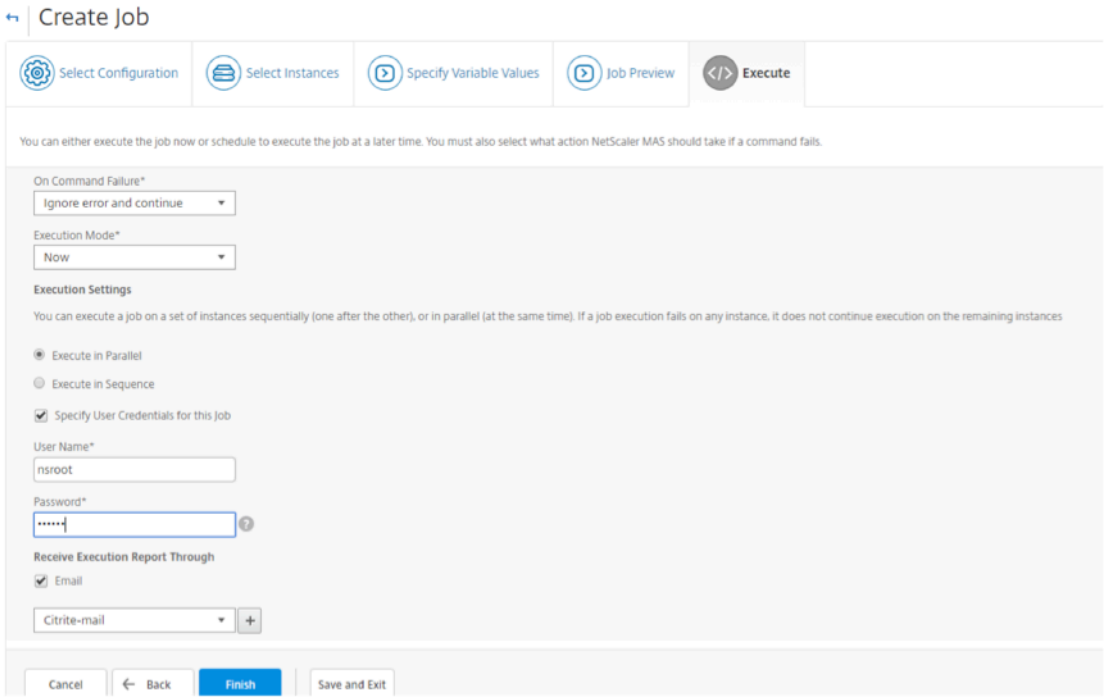
6. [**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。
7. [次へ] をクリックします。
8. [実行] タブで、次の条件を設定します:

   - **On Command Failure** - コマンドにエラーが発生した場合、エラーを無視してジョブの実行を継続するか、ジョブの実行を停止するか選択できます。実行するアクションをボックスの一覧から選択します。
   - 実行モード -ジョブを今すぐ実行することも、後で実行するようにスケジュールすることもできます。後でジョブをスケジュールする場合は、そのジョブの実行頻度設定を指定する必要があります。ジョブに定めるスケジュールをボックスの一覧から選択します。

9. また、[実行設定] で必要なメソッドを選択することで、一連のインスタンスでジョブを順次または並行して実行することもできます。いずれかのインスタンスでジョブの実行にエラーが発生した場合、残っているインスタンスに続行することはありません。

   権限のあるユーザーにマネージドインスタンスでのジョブの実行を許可することを選択できます。ジョブの成功または失敗に関する電子メール通知は、他の詳細とともに送信することもできます。

10. [完了] をクリックします。



メンテナンス・ジョブを使用した **NetScaler ADC SDX** インスタンスのアップグレード

February 6, 2024

NetScaler リリース 11.0 以降を実行している NetScaler ADC SDX インスタンスのシングルバンドル・アップグレードを実行できます。シングルバンドルのアップグレードを実行するには、NetScaler ADM 組み込みタスクを使用します。この組み込みタスクを使用して、NetScaler SDX 管理サービス、Citrix Hypervisor、および Citrix Hypervisor のサプリメントパックとホットフィックスをアップグレードできます。

NetScaler ADM を使用して **NetScaler ADC SDX** インスタンスをアップグレードするには:

1. [ネットワーク] > [構成ジョブ] > [メンテナンスジョブ] に移動します。
2. [ジョブの作成] をクリックします。［ジョブの作成］ページで、**NetScaler SDX** のアップグレード組み込みタスクを選択して、NetScaler SDX インスタンスをアップグレードします。[続行] をクリックします。
3. 1 つまたは複数 の NetScaler アプライアンス のアップグレードページの「インスタンスの 選択 」タブで、ジョブ名 を指定し、「インスタンスの 追加」をクリック します。
4. アップグレードするターゲットインスタンスまたはインスタンスグループを選択します。
5. NetScaler ADC インスタンスまたはインスタンスグループを追加したら、［次へ］をクリックして、選択したインスタンスでアップグレード前の検証を開始します。画面に、各 NetScaler インスタンスの事前検証の進行状況がレポートされます。
6. ［アップグレード **NetScaler ADC** アプライアンスの変更］ページで、［アップグレード］タブを選択します。ソフトウェアイメージメニューから 、ローカル（ローカル マシン）または アプライアンス （ビルドファイルは Citrix ADM に存在する必要があります）を選択します。
7. また、検証前のアップグレードエラーが発生しているインスタンスがあるかどうかを確認することもできます。これらのエラーは、メッセージ形式で表示されます。メッセージでは、ディスクスペース、ハードディスクドライブ、およびユーザーのカスタマイズに関するエラーが示されます。事前検証アップグレードチェックに失敗したインスタンスの使用を続行しない場合は、そのインスタンスを削除できます。インスタンスを削除するには、インスタンスを選択して [削除] をクリック します。
8. [**Schedule Task**] タブでは、アップグレード・プロセスを今すぐ実行したり、後日スケジュールを設定したりできる実行の詳細を設定することもできます。NetScaler SDX インスタンスをバックアップするか、実行レポートを電子メールで受信するか、HA のノードを 2 段階アップグレードするかを選択することもできます。

HA のノードの 2 段階アップグレードでは、アップグレードをすぐに実行するか、ノードを次々に更新する時間をスケジュールするかを選択できます。ノードの同期と伝播は、両方のノードが正常にアップグレードされるまで無効になります。

Citrix SD-WAN WANOP インスタンスの構成ジョブの作成

February 6, 2024

ジョブとは、管理対象インスタンスに対して作成およびスケジュール設定できる構成コマンドのセットです。Citrix SD-WAN WANOP インスタンスの場合、次のオプションを使用してジョブを作成できます。

- 構成テンプレート: 構成エディターを使用して CLI コマンドを入力し、構成をテンプレートとして保存し、それを使用してジョブを設定できます。
- 組み込みテンプレート: 構成テンプレートのリストから選択できます。これらのテンプレートには CLI コマンドの構文が用意されており、変数の値を指定できます。組み込みテンプレートは、説明とともに下の表に一覧表示されます。
- ファイル: ローカルマシンから設定ファイルをアップロードし、ジョブを作成できます。

ジョブが作成されると、ジョブをすぐに実行することも、後で実行するようにジョブをスケジュール設定することもできます。また実行頻度も設定できます。

組み込みテンプレート	説明
EnableCloudBridgeWANOpt	Citrix SD-WAN WANOP アプライアンスを介したトラフィックを有効にします。
DisableCloudBridgeWANOpt	Citrix SD-WAN WANOP アプライアンスを経由するトラフィックを無効にします。
RestartCloudBridgeWANOpt	Citrix SD-WAN WANOP アプライアンスを再起動します。
RestoreConfig	Citrix SD-WAN WANOP アプライアンスの構成を復元します。
AddLink	リンクを作成または定義することで、SD-WAN WANOP アプライアンスはリンクの混雑や損失を防ぎ、トラフィックシェーピングを実行できます。リンク上で送受信される最大帯域幅を定義できます。また、LAN 側 または WAN 側のトラフィックを指定することもできます。
ConfigureBandwidth	帯域幅の制限と他の帯域幅管理の設定を設定します。
AddUser	特権を割り当てる新しいユーザーを追加します。
AddUserAdvancedPlatform	新しいユーザーを追加すると、AddUser テンプレートでは利用できない権限を割り当てることが できます。
AddService-class	1 つ以上のサービスクラスフィルターを使用して Citrix SD-WAN WANOP アプライアンスの サービスクラスを作成し、有効にします。

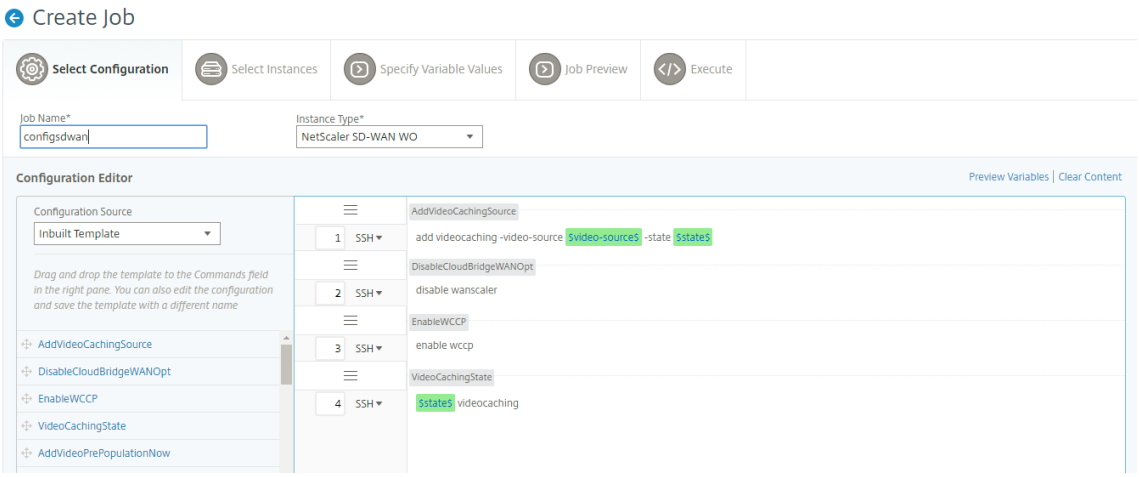
組み込みテンプレート	説明
SetApplication	アプリケーション分類子の定義を設定します。
AddorRemoveVideoCachingPorts	ビデオ ソースがデータを送受信できるポート番号を追加または削除します。デフォルトポートは 80 です。
RemoveVideoCachingSource	1 つ以上のビデオキャッシュソースを削除します。ビデオソースの IP アドレスまたはドメイン名を指定します。
RemoveAllVideoCaching	すべての利用可能なビデオキャッシュソースを削除します。
VideoCachingState	Citrix SD-WAN WANOP アプライアンスのビデオキャッシュ機能を 有効または無効にします。
ClearVideoCaching	ビデオキャッシュまたはビデオキャッシュ統計情報のいずれかをクリアします。
SetVideoCaching	キャッシュされるオブジェクトの最大サイズを設定します。この制限を超えるオブジェクト はキャッシュされません。デフォルトでは、キャッシュオブジェクトの最大サイズは 100 MB です。
AddVideoCachingSource	ビデオソースの IP アドレスまたはドメイン名を追加します。そのソースのビデオキャッシュを有効または無効にするオプション が含まれています。
ConfigureRemoteLicenseServer	集中ライセンスサーバーを構成します。ライセンスサーバモデル、IP アドレス、およびポート番号を指定 します。
ConfigureLocalLicenseServer	ライセンスサーバーの場所をローカルに設定します。
InstallCACert	Citrix SD-WAN WANOP アプライアンスに CA 証明書をインストールします。証明書名、ファイル名、およびキーストアのパスワードを指定します。
InstallCombinedCerKey	統合された SSL 証明書とキーのペアファイルをインストールします。
InstallSeperateCertKey	SSL 証明書とキーを別のファイルとしてインストールします。
EnableWCCP	WCCP 展開モードを有効にします。
AddWCCPServiceGroup	Citrix SD-WAN WANOP アプライアンスの新しい WCCP サービスグループ定義を追加します。
DisableWCCP	WCCP 展開モードを無効にします。
AddTrafficShapingPolicy	Citrix SD-WAN アプライアンスのトラフィックシェーピングポリシーを作成します。このポリシーはネットワーク帯域幅を制御します。

組み込みテンプレート	説明
SetTrafficShapingPolicy	Citrix SD-WAN WANOP アプライアンスのトラフィックシェーピングポリシーを変更します。このポリシーはネットワーク帯域幅を制御します。
AddVideoPrePopulation	ビデオの事前入力エントリを作成します。これにより、ビデオを事前にダウンロード してキャッシュできます。いつビデオをキャッシュするかも指定できます。
UpdateVideoPrePopulation	いつビデオをキャッシュするかを指定する、ビデオの事前設定エントリを変更します。
AddVideoPrePopulationNow	ビデオのプリポピュレーションを設定して、ビデオをすぐにダウンロードしてキャッシュできるよう にします。URL から 動画をダウンロードしてキャッシュする方法を制御できます。
VideoPrePopulationState	ビデオの事前設定を変更、開始、更新、および削除します。
ConfigureSyslogServer	syslog サーバーの IP アドレスとポート番号を設定します。
ConfigureAlert	アラートレベルを構成します。

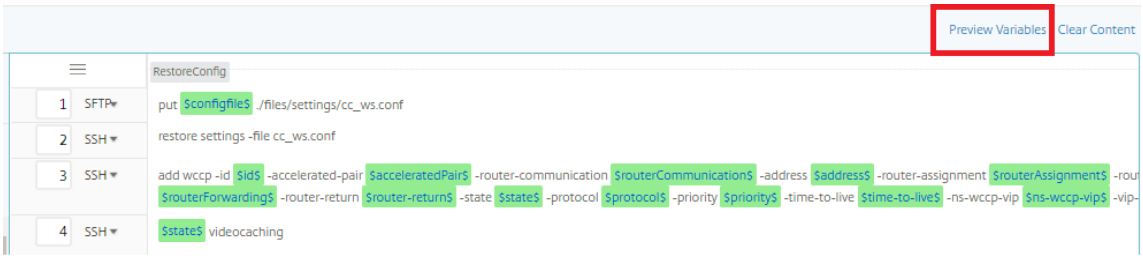
Citrix SD-WAN WANOP インスタンスの構成ジョブを作成するには:

1. Citrix ADM で、［ネットワーク］> ［構成ジョブ］に移動し、［ジョブの作成］をクリックします。
2. [ジョブの作成] ページの [構成の選択] タブで、[ジョブ名] を指定します。
3.「インスタンスタイプ」フィールドで、「**Citrix SD-WAN WO**」を選択します。
4.「構成ソース」ドロップダウンリストで、ジョブを作成するオプションを選択します。

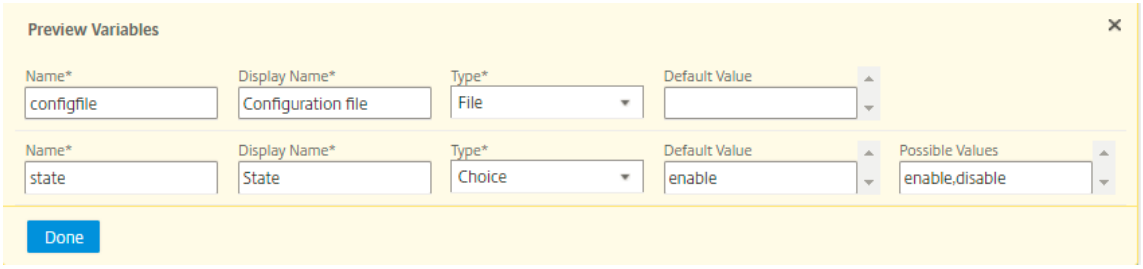
> 注
>
> [構成テンプレートとして保存] を選択し、名前を指定して構成をテンプレートとして保存し、再利用します。



5. 構成ジョブの作成または編集中に定義したすべての変数を、1 つの統合ビューで確認できます。
6. 次のいずれかの操作を行って、すべての変数を 1 つの統合ビューに表示します。
   - 構成ジョブを作成するときに、[ネットワーク**] > [**構成ジョブ] に移動し、[ジョブの作成] を選択します。[**Create Job**] ページでは、構成ジョブの作成時に追加したすべての変数を確認できます。
   - 構成ジョブの編集中に、[ネットワーク**] > [**構成ジョブ] に移動し、ジョブ名を選択して [編集] をクリックします。[ジョブの構成] ページでは、構成ジョブの作成時に追加されたすべての変数を確認できます。
7. 次に、「変数のプレビュー」タブをクリックすると、構成ジョブの作成または編集中に定義した単一の統合ビューで変数をプレビューできます。



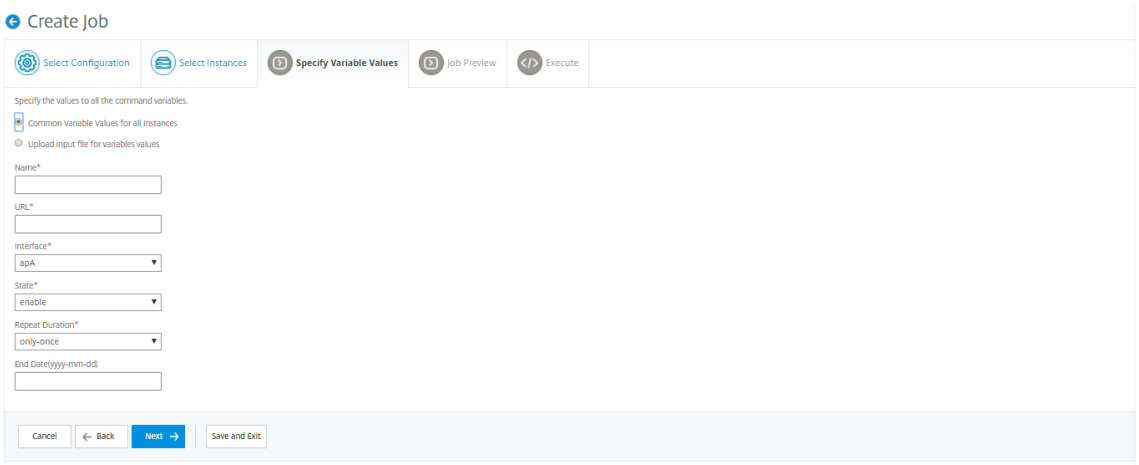
8. 新しいポップアップウィンドウが表示され、名前、表示名、タイプ、デフォルト値などの変数のすべてのパラメータが表形式で表示されます。これらのパラメータを編集および修正することもできます。パラメータを編集または変更したら、[完了] ボタンをクリックします。



9. [次へ] をクリック し、[インスタンスの 選択] タブで [インスタンスの追加**]** をクリック します。ジョブを実行するインスタンスを選択し、「**OK**」をクリック します。

10. [次へ] をクリック し、[変数値 を指定] タブで次のオプションのいずれかを選択して、インスタンスの変数を指定します。

    - 変数値の入力ファイルをアップロード**:**「入力キー ファイルをダウンロード」をクリック して入力ファイルをダウンロードします。入力ファイルで、コマンドで定義した変数の値を入力し、NetScaler ADM サーバーにファイルをアップロードします。
    - すべてのインスタンスに共通の変数値: 変数の値を入力します。選択したテンプレートによって、変数は変わります。



    変数値を含む入力ファイルは、設定ジョブで (同じファイル名で) 保持されます。設定ジョブの作成または編集中に、以前に使用およびアップロードした入力ファイルを表示および編集できます。

    構成ジョブの作成中に実行された構成ジョブを表示するには、[ネットワーク**] > [**構成ジョブ**]** に 移動し、**[**ジョブの作成] をクリック します。**[** ジョブの作成] ページ。「変数値の指定」タブで、「すべてのインスタンスの共通変数値」オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします（同じファイル名を維持します)。

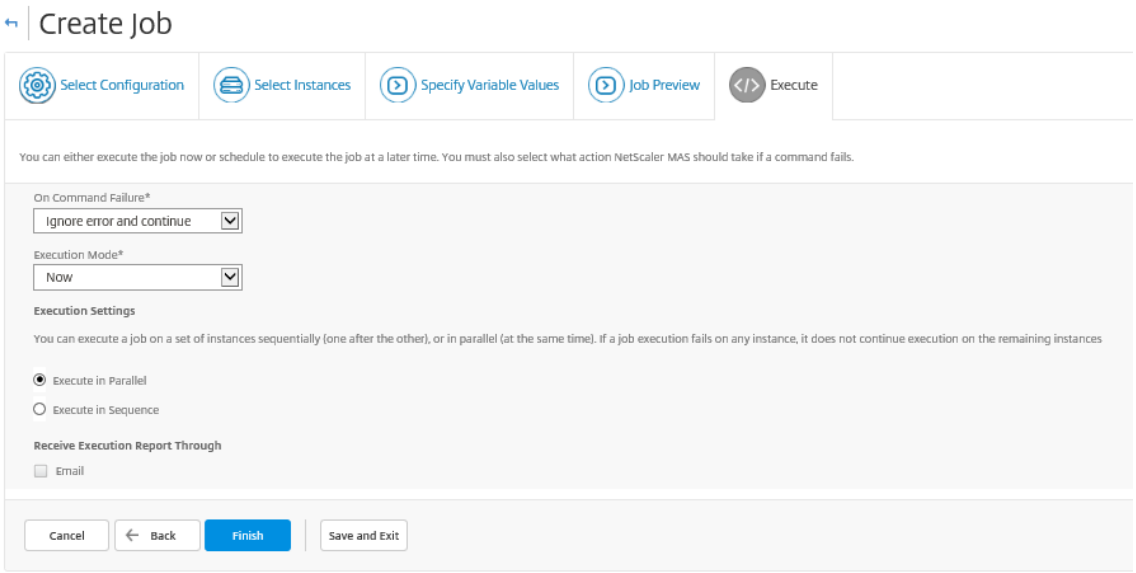
    構成ジョブの編集中に実行済みの構成ジョブを表示するには、[ネットワーク**] > [**構成ジョブ] に移動し、[ジョブ名] を選択して [編集] をクリックします。[ジョブの設定] ページの [変数値の指定] タブで、[すべてのインスタンスの共通変数値] オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします（同じファイル名を使用)。

11. [次へ] をクリックすると、[ジョブプレビュー] タブでジョブとして実行されるコマンドを評価および検証できます。

12. [次へ] をクリックし、[実行] タブで、次の条件を設定します。

    - コマンドが失敗した場合: コマンドが失敗した場合の対処方法: エラーを無視してジョブを続行するか、ジョブの実行を停止します。ボックスの一覧からアクションを選択します。
    - 実行モード: ジョブをすぐに実行するか、後で実行するようにスケジュールします。後で実行するようにスケジュールを指定する場合、ジョブの実行頻度の設定を指定する必要があります。「実行頻度」ドロッ

プダウン・リストから、ジョブが従うスケジュールを選択します。



13. [実行設定] で、ジョブを順番に (次々に) 実行するか、並行して (同時に) 実行するかを選択します。
14. ジョブ実行レポートを受信者のリストに電子メールで送信するには、「実行レポートの受信」セクションの「電子メール」チェックボックスを選択します。表示されるボックスの一覧から電子メール配布リストを選択します。メール配信リストを作成するには、**+** アイコンをクリックし、受信者のメールアドレスとメールサーバーの詳細を入力します。
15. ［完了］をクリックします。

マスター構成テンプレートの使用

February 6, 2024

マスター構成テンプレートを使用すると、複数の NetScaler ADC インスタンスにマスター構成を作成して展開できます。

管理者は、構成を変更し、ライセンス、証明書、およびその他のファイルを ADC インスタンスに保存することができます。新しい構成をマスター構成テンプレート（.conf ファイル）として保存できます。

マスター構成テンプレートを ADC インスタンスから保存するには、次のいずれかを実行できます：

- コマンドプロンプトに対して、s **ave ns config** と入力します。構成は、インスタンスのフラッシュメモリ内の/nsconfig/ns.conf ファイルに保存されます。
- インスタンスの GUI から、[診断] > [設定の表示] に移動します。保存する構成の種類を選択します。たとえば、インスタンスの保存済み設定を保存する場合は、[**Saved configuration n**] を選択します。「ファイルにテキストを保存」リンクをクリックして、’ns.conf’ ファイルをローカルマシンに保存します。

新しいジョブの作成時に「DeployMasterConfiguration」構成テンプレートを使用してマスター構成テンプレートをデプロイすると、コマンドを追加したり、既存のコマンドを変更したり、入力ファイルにさまざまな変数値を指定したりすることで、特定の ADC インスタンスごとにさらにカスタマイズできます。

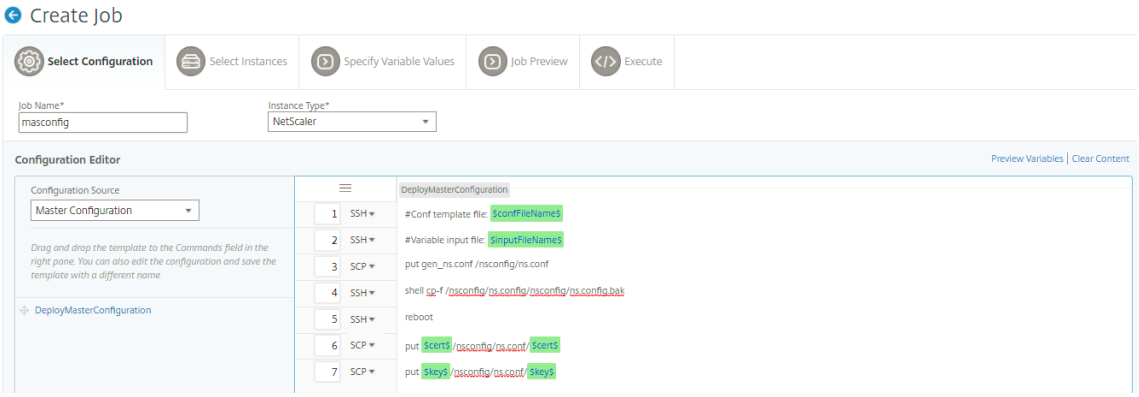
たとえば、管理者として、さらに ns.conf ファイルに ADC インスタンスに証明書キーをアップロードし、マスター設定もデプロイできます。

> 重要
>
> Citrix ADC CPX インスタンス、クラスタ内で構成されたインスタンス、またはパーティション化された ADC インスタンスでは、DeployMasterConfiguration テンプレートを使用して構成ジョブを実行することはできません。

NetScaler ADM でマスター構成構成構成テンプレートを使用して構成ジョブを作成するには:

1. Citrix ADM で、[ネットワーク] > [構成ジョブ] に移動し 、[ジョブの作成] をクリック します。
2. [**Create Job**] ページの [**Select Configuration**] タブで、[**Job Name**] を指定し、ドロップダウンリストから [**Instance Type**] を選択します。
3. 「構成ソース」ドロップダウンリストから「マスター構成」を選択します。DeployMasterConfiguration テンプレートのコマンドを右側のペインにドラッグアンドドロップします。右側のペインでは、コマンドを追加、変更、削除することもできます。[次へ] をクリックします。

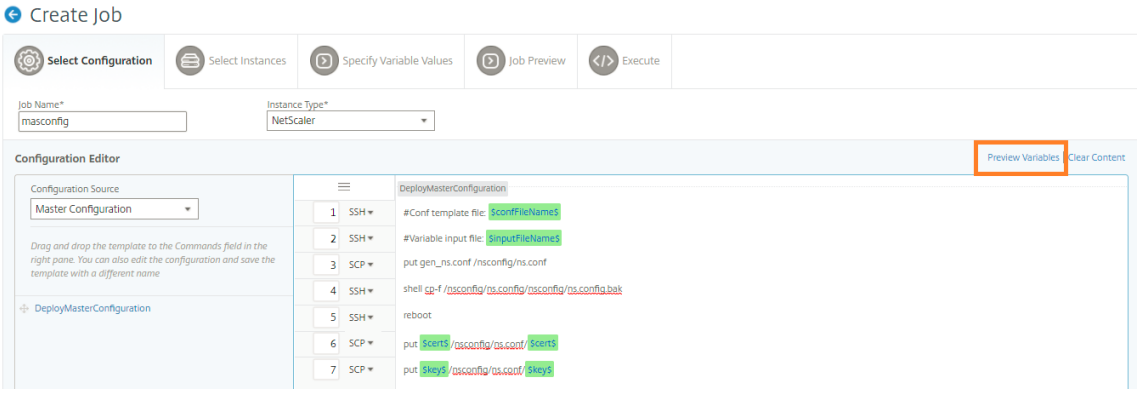
   > 注
   >
   > p ***ut*** コマンドを追加して、入力ファイルをテンプレートに追加できます。例では、構成テンプレートファイルと変数入力ファイルに加えて、証明書とキーファイルをアップロードする必要があります。



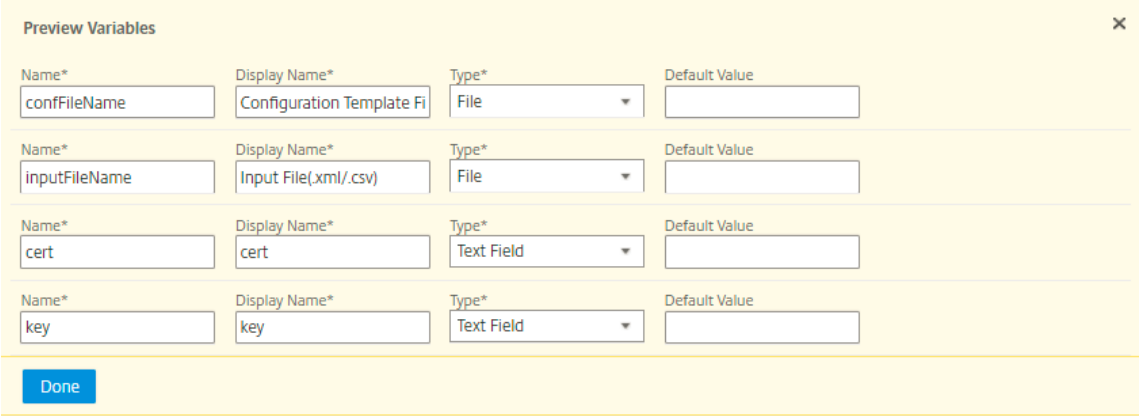
4. 構成ジョブの作成または編集中に定義したすべての変数を、1 つの統合ビューで確認できます。
5. 次のいずれかの操作を行って、すべての変数を 1 つの統合ビューに表示します。

   - 構成ジョブを作成するときに、[ネットワーク**] > [**構成ジョブ] に移動し、[ジョブの作成] を選択します。[**Create Job**] ページでは、構成ジョブの作成時に追加したすべての変数を確認できます。
   - 構成ジョブの編集中に、[ネットワーク**] > [**構成ジョブ] に移動し、ジョブ名を選択して [編集] をクリックします。[ジョブの構成] ページでは、構成ジョブの作成時に追加されたすべての変数を確認できます。

6. 次に、「変数のプレビュー」タブをクリックすると、構成ジョブの作成または編集中に定義した単一の統合ビューで変数をプレビューできます。



7. 新しいポップアップウィンドウが表示され、名前、表示名、タイプ、デフォルト値などの変数のすべてのパラメータが表形式で表示されます。これらのパラメータを編集および修正することもできます。パラメータを編集または変更したら、[完了] ボタンをクリックします。



8. 構成ジョブを実行するインスタンスを選択し、[**Next**] をクリックします。
9. [変数値の指定] タブで、次のファイルをアップロードします。

   - 設定テンプレートファイル **(.conf)** -ADC インスタンスから抽出した.conf ファイルをアップロードします。
   - 入力ファイルのアップロード **(.xml/csv)** -コマンドで定義した変数の値を含む入力ファイルをアップロードします。

   ここでは、使用例としてサンプルの xml ファイルを用意しています。xml ファイルに、使用している ADC インスタンスに対応する詳細が含まれていることを確認します。

```
<?xml version="1.0" encoding="UTF-8" ?>

<properties>

<!--
```

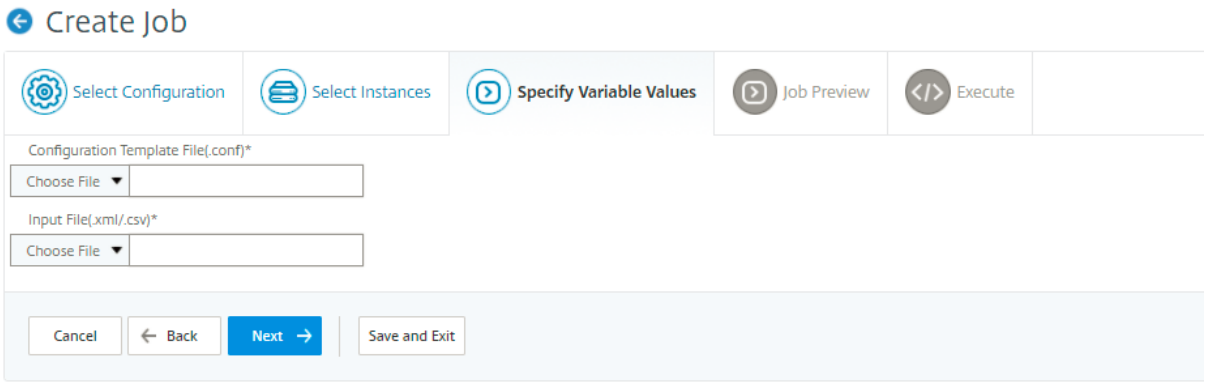


```
6
7  Provide inputs for all the parameters defined in the master config
       file.
8
9  -  global. This tag contains all the common parameters and value.
10
11 -  devicegroup. This tag contains all the instance group specific
      parameters and values.
12
13 If the same parameters are defined in global and instance tags,
      the instance specific parameters value will take precedence
      over the instance group. The instance group specific parameters
       value will take precedence over global parameters in the
      execution.
14
15 -  name. This attribute represents the name of the instance group.
16
17 -  device. This tag contains all the instance specific parameters
      and value.
18
19 If the same parameters are defined in global and instance tags,
      the instance specific parameters value will take precedence in
      the execution.
20
21 -  name. This attribute represents the IP Address of the instance.
       Host name is not supported for the attibute.
22
23 HA pair should be represented as <primaryip>-<secondaryip>.
      Example 10.102.2.1-10.102.2.2
24
25 In the template file, the parameter name must be specified within
      the dollar sign,Example: $NSIP$, $CC_Trap_Dest$ and parameters
      names are case sensitive.
26 -->
27
28 <global>
29
30 </global>
31 <devicegroup name="BLR_DEVS">
32 </devicegroup>
33 <device name="10.106.101.209">
34 <param name="IP" value="10.106.101.209"/>
35 </device>
36
37 <!-- HA PAIR-->
38 <!--<device name="10.102.43.154-10.102.43.155">
39 <param name="NSIP" value="10.102.43.154"/>
40 <param name="HostName" value="NS43HA"/>
41 <param name="LBSERVER" value="haserver43http"/>
42 <param name="SNMPTrapDest" value="10.102.43.130"/>
43 </device>-->
44 </properties>
45
```



```
46  <!--NeedCopy-->
```

10. ［次へ］をクリックします。

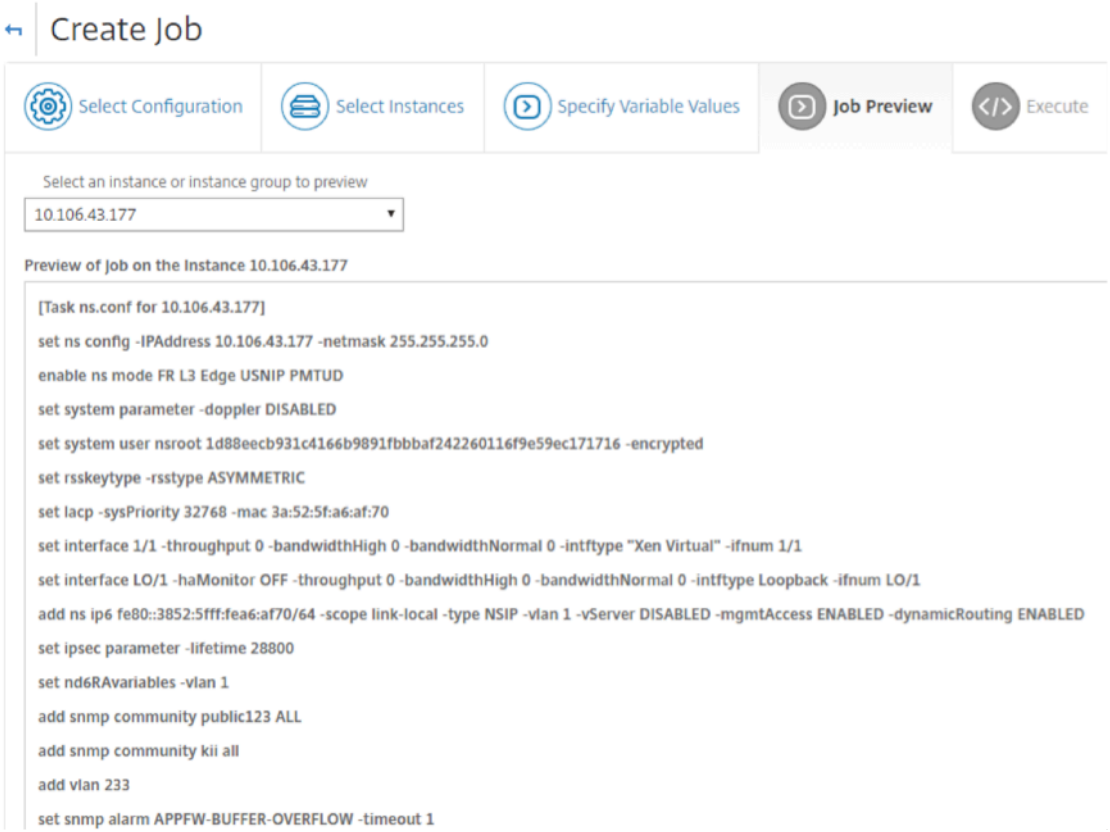


変数値を含む入力ファイルは、設定ジョブで (同じファイル名で) 保持されます。設定ジョブの作成または編集中に、以前に使用およびアップロードした入力ファイルを表示および編集できます。

構成ジョブの作成中に実行された構成ジョブを表示するには、[ネットワーク**] > [**構成ジョブ] に移動し、[ジョブの作成] をクリックします。**[** ジョブの作成] ページ。[変数値の指定] タブで、[すべてのインスタンスに共通の変数値] オプションを選択し、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします（同じファイル名を維持します）。

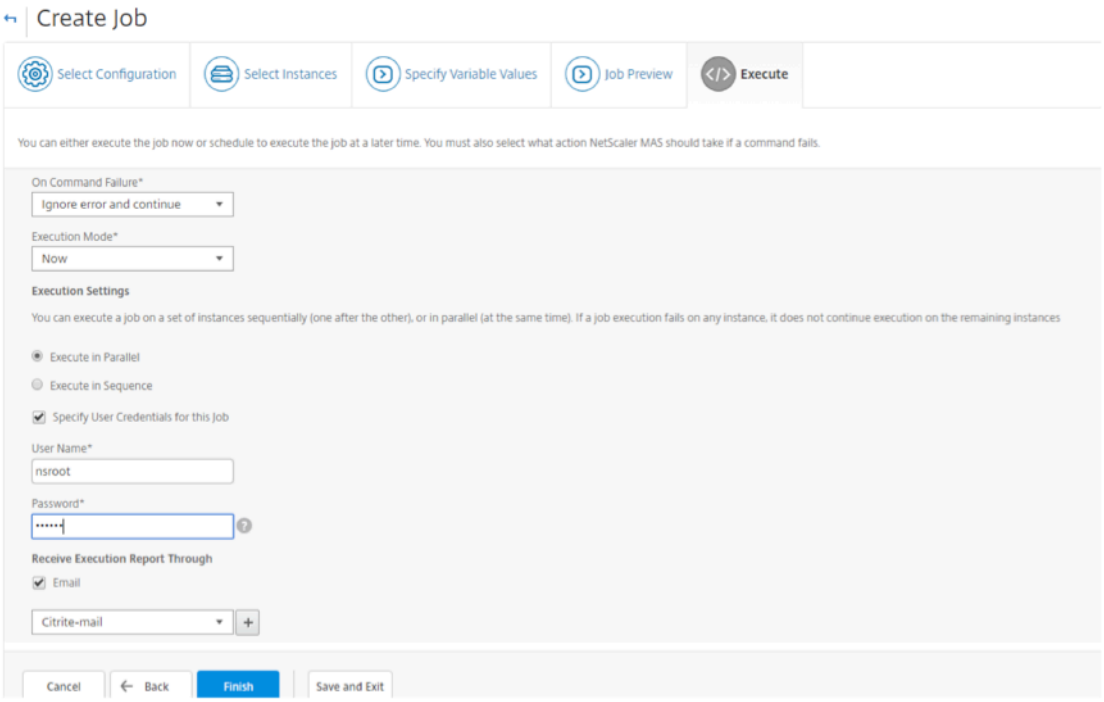
構成ジョブの編集中に実行済みの構成ジョブを表示するには、[ネットワーク**] > [**構成ジョブ] に移動し、ジョブ名を選択して [編集] をクリックします。[ジョブの設定] ページの [変数値の指定] タブで、[すべてのインスタンスに共通変数値] オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします（同じファイル名を維持します）。

1. [**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価して確認し、[**Next**] をクリックします。



2. [実行] タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。コマンドが失敗した場合に Citrixx ADM が実行するアクションを選択することもできます。

   権限のあるユーザーに管理対象インスタンス上でのジョブの実行を許可するように選択することもできます。また、その他の詳細と共にジョブの成功や失敗に関してメール通知を送信するかどうかを選択できます。



ジョブを実行した後、[ネットワーク] > [構成ジョブ] に移動し 、先ほど設定したジョブ を選択すると、ジョブの詳細が表示されます。 [詳細] をクリックし 、[実行 の概要] をクリックしてジョブの詳細を確認します。インスタンスをクリックすると、コマンドログが表示され、ジョブで実行されたコマンドが表示されます。

Command Log

Status	Command	Message
✓	put /var/mps/tenants/root/config_mgmt/MySSLCert.crt /nsconfig/ssl/MySSLCert.crt	Done
✓	put /var/mps/tenants/root/config_mgmt/MySSLCertKey.key /nsconfig/ssl/MySSLCertKey.key	Done
✓	shell cp -f /nsconfig/ns.conf /nsconfig/ns.conf.bak	Done
✓	#Conf template file: NS12_0_41_Template.conf	Done
✓	#Variable input file: NS12_0_41_AnswerKey.xml	Done
✓	put /var/mps/tenants/root/config_mgmt/ns_##7A818EB30E94FAA36144CC5F0782E06A13C3122F6BC67B32190444FC6F06.conf /nsconfig/ns.conf	Done
✓	shell	Done
✓	reboot	Done

ジョブを使用して **NetScaler ADC** インスタンスをアップグレードする

February 6, 2024

NetScaler Application Delivery Management（ADM）を使用して、1 つ以上の NetScaler ADC インスタンスをアップグレードできます。インスタンスをアップグレードする前に、NetScaler ADC インスタンスに正しいビルドファイルとドキュメントファイルをアップロードしていることを確認してください。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。

メンテナンスタスクを作成して NetScaler ADC インスタンスをアップグレードすると、次の操作を実行できます。

- 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。事前検証チェックは、次のチェックで構成されます。

    1. NetScaler ADC インスタンスに既存のカスタマイズがあるかどうかを確認し、カスタマイズを削除します。アップグレードプロセスの完了後に、すべてのカスタマイズを再適用できます。
    2. NetScaler ADC インスタンスのディスク使用量を確認します。ディスク使用が 80% を超えている場合は、ディスクスペースをクリーンアップします。
    3. NetScaler ADC インスタンスのディスクハードウェアの問題を確認します。

- NetScaler ADC HA ペアのアップグレードを 2 段階で実行します。

    1. ノードでアップグレードタスクをただちに実行することも、後で実行するようにスケジュールすることもできます。
    2. もう一方のノードのアップグレードを後でスケジュールします。このスケジュールは、最初のノードがアップグレードされた後に行う必要があります。

NetScaler ADC HA ペアをアップグレードするときは、次の点に注意してください。

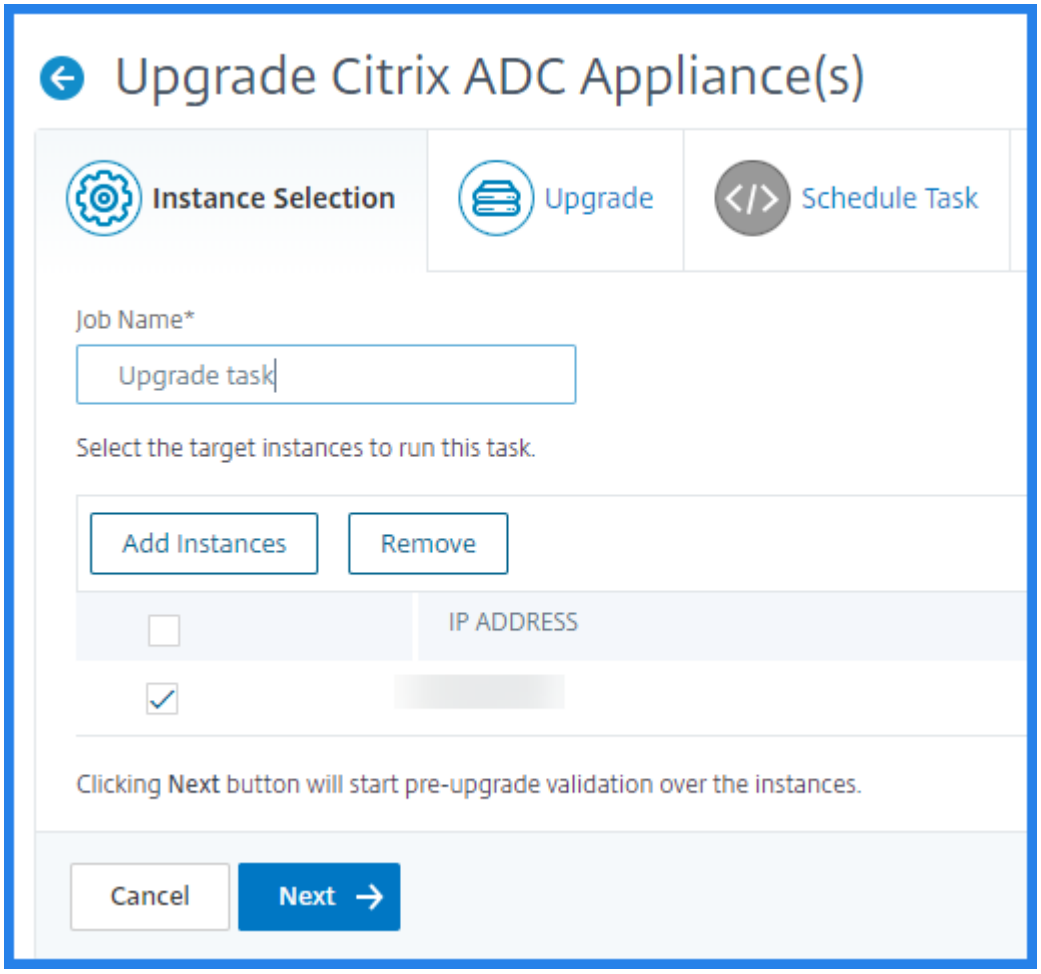
- 現在、HA ペアの 2 番目のノードが最初にアップグレードされ、1 番目のノードのアップグレードは後で実行されるようにスケジュールされています。
- ノードの同期と伝播は、両方のノードが正常にアップグレードされるまで無効になります。
- 両方のノードをアップグレードした後、HA ペアのノードが異なるビルドまたはバージョンにある場合、実行履歴にエラーメッセージ (HA Sync が有効になっていないことを示す) が表示されます。

NetScaler ADC インスタンスをアップグレードするメンテナンスタスクを作成するには:

> 注
>
> 上位バージョンから下位バージョンへの ADC のアップグレードはサポートされていません。たとえば、NetScaler ADC インスタンスが 13.0 82.x の場合、ADC インスタンスを 13.0 79.x または他の以前のバージョンにダウングレードすることはできません。

1. [ネットワーク] > [構成ジョブ] > [メンテナンスジョブ] に移動します。
2. [メンテナンスジョブ] ページで、[ジョブの作成] をクリックします。
3. ［メンテナンスジョブの作成］ページで、［**NetScaler ADC** のアップグレード**/ NetScaler ADC HA** のアップグレード］を選択し、［続行］をクリックします。

4. 1 つ以上の［NetScaler ADC アプライアンスのアップグレード］ページの［インスタンスの選択］タブで、［ジョブ名］を指定し、［インスタンスの追加］をクリックします。



5. アップグレードするターゲットインスタンスまたはインスタンスグループを選択します。

   注

   - NetScaler ADC インスタンスを高可用性モードでアップグレードするには、プライマリインスタンスまたはセカンダリインスタンスのいずれかの IP アドレスを選択する必要があります。ただし、アップグレードには常にプライマリノードを使用することをお勧めします。
   - NetScaler ADC インスタンスをクラスターモードでアップグレードするには、クラスター IP アドレスを選択します。

6. NetScaler ADC インスタンスまたはインスタンスグループを追加したら、[次へ] をクリックして、選択したインスタンスでアップグレード前の検証を開始します。画面には、各 NetScaler ADC インスタンスの事前検証の進行状況が報告されます。

7. [**NetScaler ADC** アプライアンスのアップグレード］ページで、［アップグレード］タブを選択します。［ソフトウェアイメージ］メニューから、［ローカル］（ローカルマシン）または［アプライアンス］（ビルドファイルは NetScaler ADM に存在する必要があります）を選択します。

8. また、検証前のアップグレードエラーが発生しているインスタンスがあるかどうかを確認することもできます。これらのエラーは、メッセージ形式で表示されます。メッセージでは、ディスクスペース、ハードディスクド

ライブ、およびユーザーのカスタマイズに関するエラーが示されます。

事前検証アップグレードチェックに失敗したインスタンスの使用を続行しない場合は、そのインスタンスを削除できます。インスタンスを削除するには、インスタンスを選択し、[**Delete**] をクリックします。

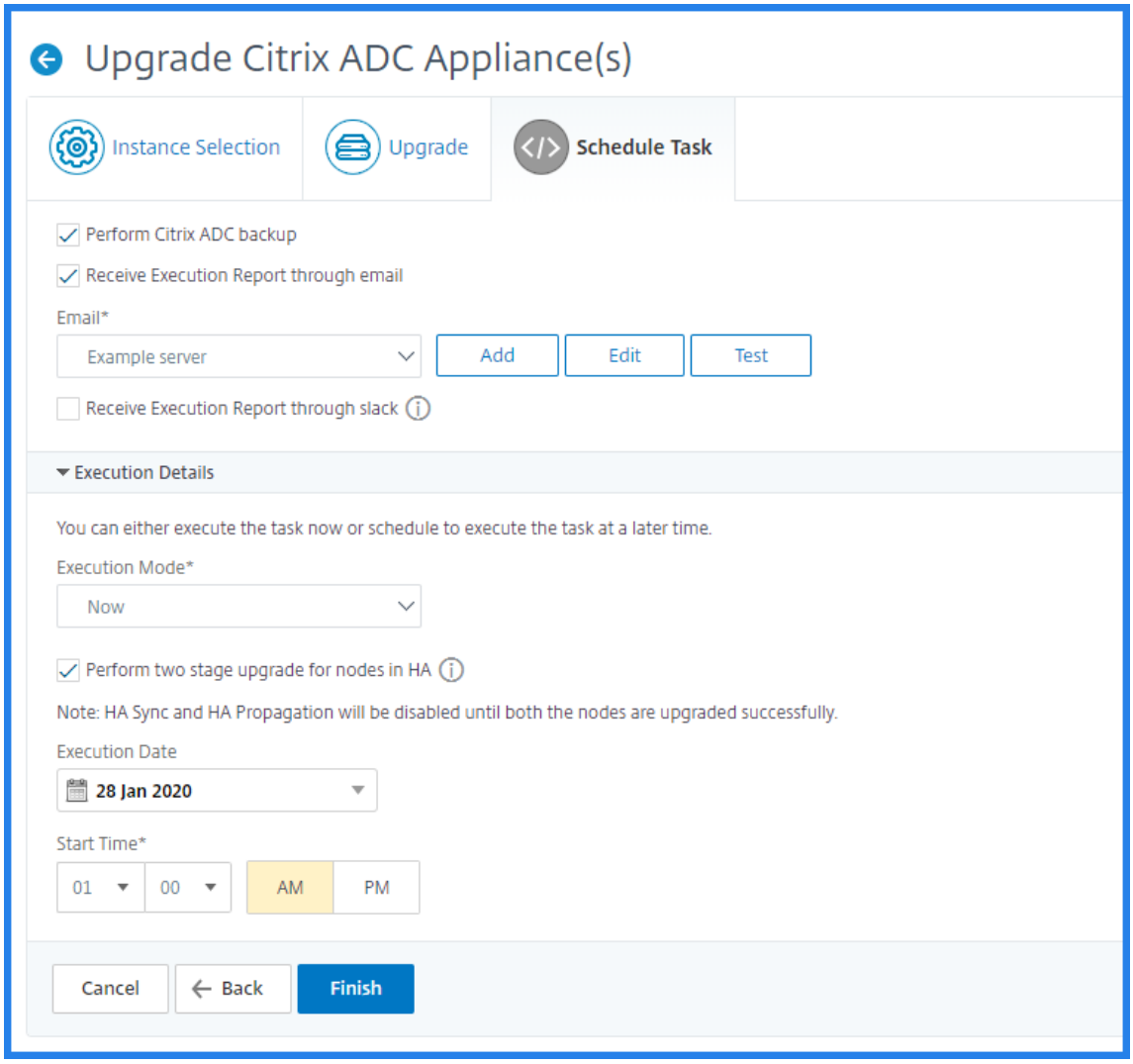
1. ［次へ］をクリックします。

   > 注
   >
   > NetScaler ADC インスタンスのアップグレード前の検証チェックに合格した場合にのみ、アップグレードプロセスを続行することを強くお勧めします。

2. [タスクのスケジュール] タブでは、アップグレードプロセスを今すぐ実行したり、後でスケジュールしたりできる実行の詳細を設定することもできます。
3. 電子メール通知を有効にして、NetScaler ADC インスタンスのアップグレードの実行レポートを受け取ることができます。「実行レポートを電子メールで受信」チェックボックスをクリックして、電子メール通知を有効にします。電子メール配布リストを作成するには、次の手順を実行します。

   - **+** アイコンを選択してメール配布リストを作成します。
   - **[**電子メール配布リストの作成] ページで、電子メール配布リストの [名前] を指定します。電子メール通知を電子メールサーバに送信するために使用する SMTP メールサーバを追加します。[差 出 人] ボックスに、メッセージの送信元の電子メールアドレスを追加します。[宛先] ボックスに、メッセージを送信する 1 つまたは複数のアドレスを追加します。また、メッセージのコピーやコピーの送信先となる電子メールアドレスを追加して、これらのアドレスをメッセージまたはコピーに表示しないようにすることもできます。［作成］をクリックします。電子メール同報リストを作成したら、[**Finish**] をクリックして設定プロセスを完了します。

4. [**Schedule Task**] タブでは、HA のノードに対して 2 段階のアップグレードを実行することもできます。アップグレードをすぐに実行することも、ノードを 1 つずつ更新する時間をスケジュールすることもできます。ノードの同期と伝播は、両方のノードが正常にアップグレードされるまで無効になります。



構成テンプレートを使用した監査テンプレートの作成

February 6, 2024

前に構成テンプレートとして保存した構成コマンドを使用して、特定の NetScaler インスタンスに適用できる監査テンプレートを作成できるようになりました。監査テンプレートの作成中には、前に保存した構成テンプレートを [Commands] フィールドにドラッグアンドドロップし、要件に合うようにそのテンプレートを編集できます。その後、その監査テンプレートを特定の NetScaler インスタンスに適用できます。NetScaler ADM は、これらのインスタンスを監査テンプレートと比較し、不一致を報告します。このプロセスは、エラーを識別し、直ちに修正するために役立ちます。

新しいジョブを作成しながら設定テンプレートを作成し、構成コマンドのセットをテンプレートとして保存できます。これらのテンプレートを [ジョブの作成] ページで保存すると、[テンプレートの作成] ページに自動的に表示されま

す。

たとえば、負荷分散仮想サーバーを追加し、2 つのサービスを追加し、それらのサービスをその仮想サーバーにバインドするという、基本的な負荷分散構成を考えてみましょう。

この例では、次のコマンドを使用します。

add lb vserver **servername** HTTP **ipaddress portnumber**

サービスサービスの追加 **1 IP** アドレス **1** HTTP 80

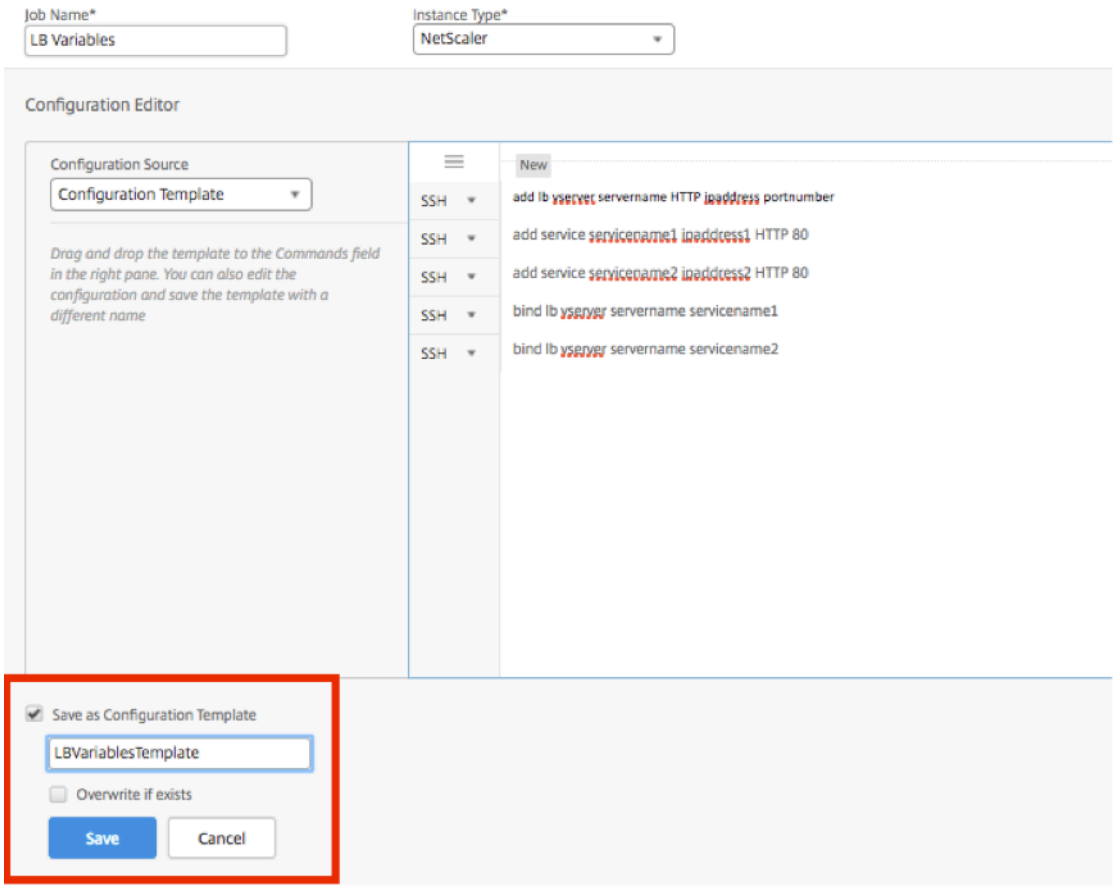
サービスサービスの追加 **2 IP** アドレス **2** HTTP 80

バインド lb v **server** サーバ名サービス名 **1**

バインド lb v **server** サーバ名サービス名 **2**

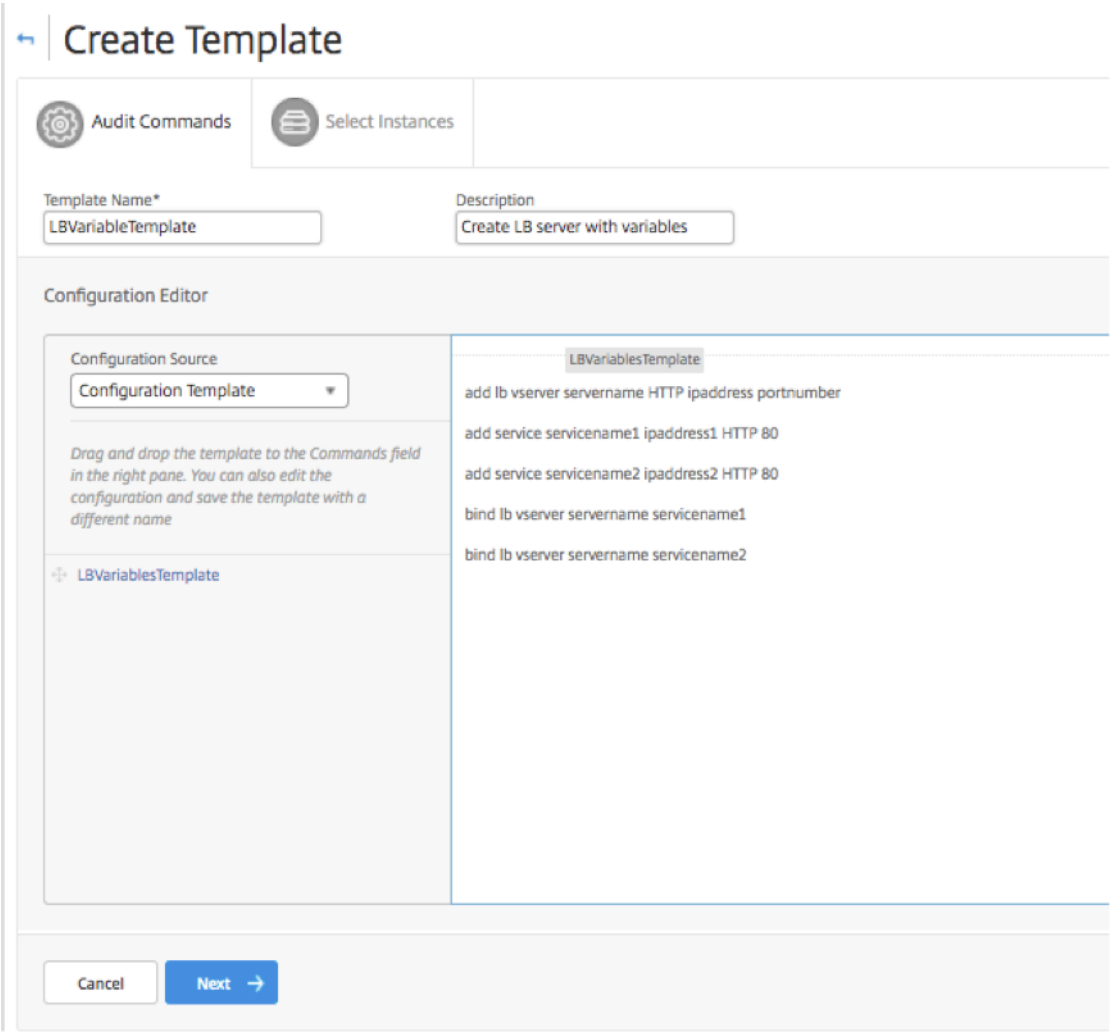
NetScaler ADM で構成テンプレートを保存するには:

1. [ネットワーク] > [構成ジョブ] に移動し、[ジョブの作成] をクリックします。
2. [**Create Job**] ページで、ジョブ名とインスタンスタイプを指定します。
3. 構成ソースとして **[Configuration Template]** を選択し、**[Commands]** フィールドに上記の例のようなコマンドを入力します。
4. 「構成テンプレートとして保存」チェックボックスを選択し、テンプレートの名前を指定します。同じ名前が付いた他のテンプレートが存在する場合はそれを上書きすることを選択できます。
5. ［保存］をクリックします。



構成テンプレートを使用して **NetScaler ADM** で監査テンプレートを作成するには:

1. [ネットワーク] > [構成監査] > [監査テンプレート] に移動し、[追加] をクリックします。
2. [テンプレートの作成] ページで、テンプレート名の名前を指定し、説明を入力します。
3. 「構成ソース」リストから「構成テンプレート」を選択し、テンプレートを右側のペインの「コマンド」フィールドにドラッグアンドドロップします。構成を編集し、テンプレートを別の名前で保存することもできます。［次へ］をクリックします。
4. **[**インスタンスの選択] タブで [インスタンスを追加] をクリックし、設定を実行するインスタンスを追加します。［**OK**］をクリックします。
5. ［完了］をクリックします。



監査テンプレートは、[Audit Templates] ボックスの一覧に表示され、指定したインスタンスの構成に対して 12 時間ごとに実行されます。

設定ジョブで **SCP (put)** コマンドを使用する

February 6, 2024

Citrix ADM の構成ジョブ機能を使用して、構成ジョブの作成、電子メール通知の送信、作成されたジョブの実行ログの確認を行うことができます。ジョブとは、管理対象インスタンスに対して作成および実行できる構成コマンドのセットです。たとえば、デバイスのアップグレードのために構成ジョブを使用できます。

NetScaler ADM の構成ジョブでは、Secure Shell（SSH）コマンドを使用してインスタンスを構成し、Secure Copy（SCP）を使用してファイルを安全に転送するように構成ジョブを構成できます。SCP は、SSH プロトコルに基づいています。構成ジョブに含めることができる SCP コマンドの 1 つは、「put」コマンドです。構成ジョブで

「put」コマンドを使用して、システムのローカルディレクトリに保存されている 1 つ以上のファイルを NetScaler ADM にアップロードまたは転送し、次に NetScaler インスタンスまたはインスタンス上のディレクトリに転送できます。

> 注：ファイルは Citrix ADM にアップロードされ、後で選択した NetScaler インスタンスにコピー（配置）されます。アップロードされたファイルは NetScaler ADM に保存され、ジョブが削除されたときにのみ削除されます。これは、後で実行するようにスケジュールされているジョブの場合に、必要になります。

このコマンドの構文を次に示します：

```
put <local_filename> <remote_path/remote_filename>
```

各項目の意味は次のとおりです。

<local_filename> は、アップロードするローカルファイルの名前です。

<remote_path/remote_filename> はリモートディレクトリへのパスと、そのディレクトリにコピーされるときにファイルに割り当てる名前です。

構成ジョブの作成中に、ローカルファイル名とリモートファイル名のパラメーターを変数に変換できます。これにより、ジョブを実行するたびに、同じ一連の NetScaler インスタンスのために、これらのパラメーターに異なるファイルを割り当てることができます。また、1 つのファイルをジョブ内の複数の位置で使用しており、そのファイルの名前を変更する必要がある場合は、すべての位置でファイル名を変更するのではなく、変数を再定義できます。

put コマンドを使用して、設定ジョブでファイルをアップロードするには、次の手順を実行します。

1. [ネットワーク] > [構成ジョブ] に移動します。
2. [ジョブ] ページで、[ジョブの作成] をクリックします。
3. [ジョブの作成] ページで、[ジョブ名] フィールドにジョブの名前を入力し、[構成エディタ] ペインで [put] コマンドを入力します。

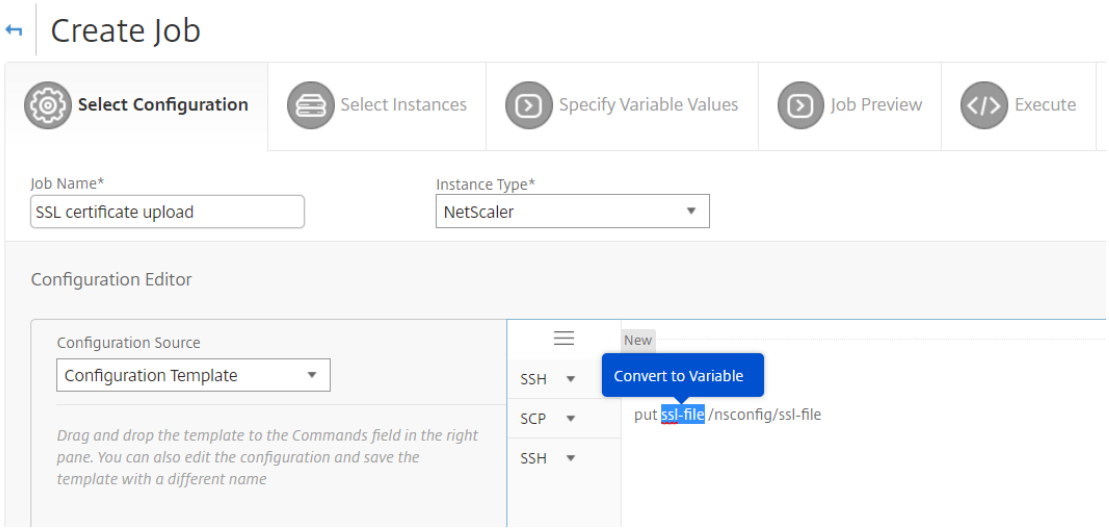
   たとえば、ローカルシステム上に保存されている SSL 証明書ファイルを複数の NetScaler インスタンスにコピーする構成ジョブを作成する必要がある場合は、特定のファイルの名前の代わりに変数を使用する「put」コマンドを追加し、変数のタイプを「ファイル」として定義できます。

   ```
   1 put ssl-file /nsconfig/ssl-file
   2 <!--NeedCopy-->
   ```

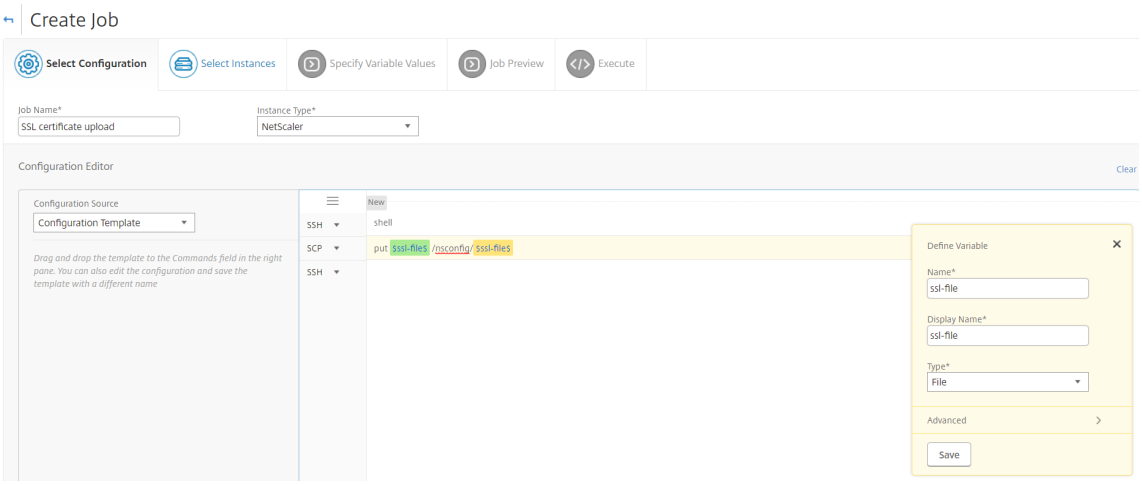
   この例の説明を次に示します。

   - ssl-file - これは、NetScaler インスタンスにアップロードする必要があるファイルの名前です。
   - /nsconfig/ssl-file - これは、タスクの実行後に ssl-file が格納される、インスタンス上の目的フォルダーです。

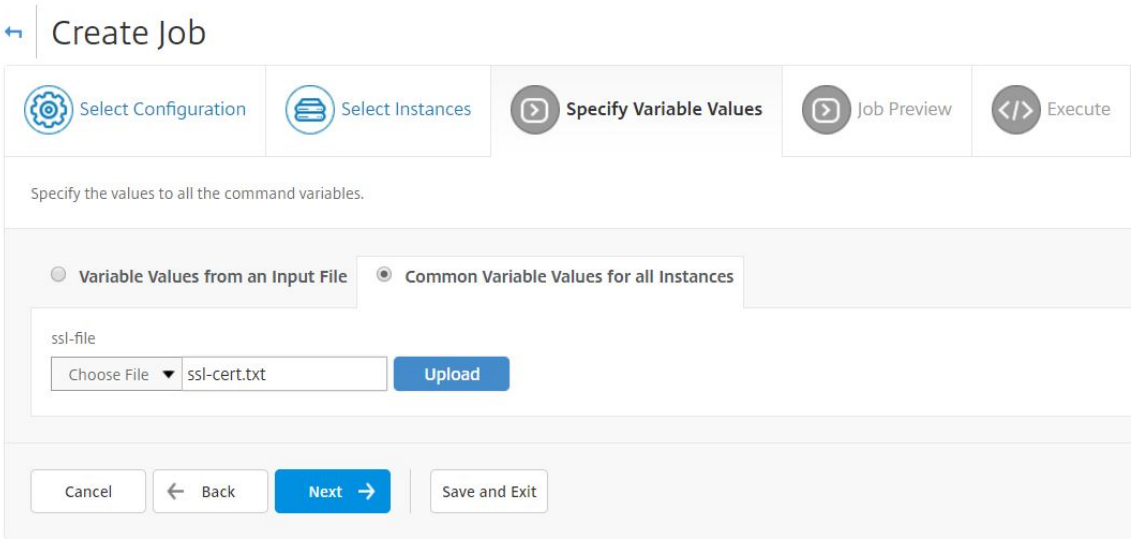
4. 先ほど入力したコマンドで、変数に変換するファイル名を選択し、次の図に示すように「変数に 変換」をクリック します。



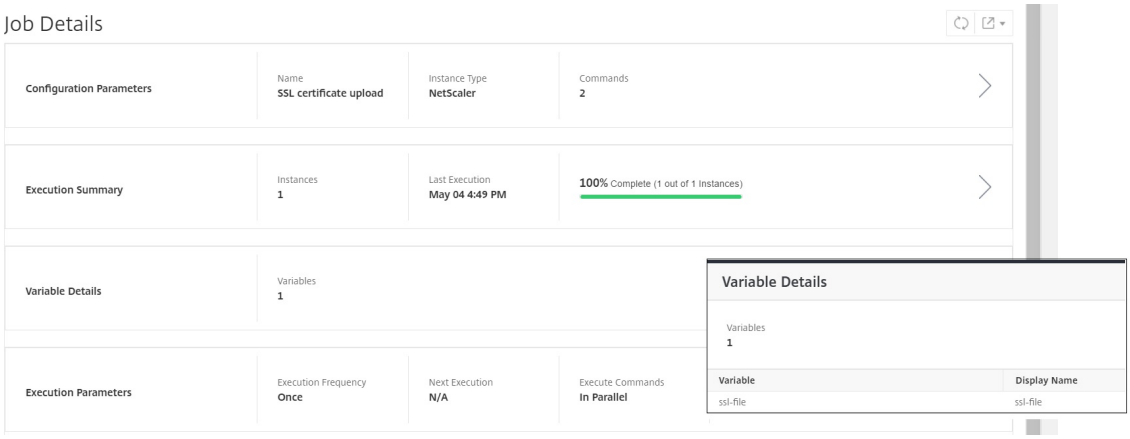
5. ファイル名がドル記号 (変数であることを示す) で囲まれていることを確認し、変数をクリックします。
6. 名前、表示名、タイプなど、変数の詳細を指定します。
7. [タイプ] ドロップダウンリストから [ファイル] を選択します。[保存] をクリックします。変数を「ファイル」タイプとして宣言すると、ファイルを NetScaler ADM にアップロードできます。



8. [次へ] をクリック し、ファイルのコピー先の NetScaler インスタンスを選択します。
9. [変数値の指定] タブで、[すべてのインスタンスの共通変数値] セクションを選択し、システム上のローカルストレージからファイルを選択し、[アップロード] をクリックして NetScaler ADM にファイルをアップロードし、[次へ] をクリックします。



10. [**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。
11. [実行] タブで は、ジョブを今すぐ実行することも、後で実行するようにスケジュールすることもできます。コマンドが失敗した場合に Citrix ADM が実行するアクションを選択することもできます。また、ジョブの成功または失敗、およびその他の詳細について通知を受け取るように、メール通知を作成できます。[完了] をクリックします。
12. ジョブの詳細は、[ネットワーク] > [構成ジョブ] に 移動し、 構成したばかりのジョブを選択すると表示されます。[詳細] をクリックし、[変数の詳細] をクリックして、ジョブに追加された変数を一覧表示します。



組み込みテンプレートを使用して構成されたジョブを再スケジュールする

February 6, 2024

Citrix Application Delivery Management（ADM）の組み込みテンプレートを使用して、スケジュールしたジョ

ブを再スケジュールできます。たとえば、コマンドが失敗した場合に NetScaler ADM が実行する必要があるアクションを変更できます。エラーを無視して続行するように設定していた場合、その設定を、1 つのコマンドが失敗したらすべての成功したコマンドをロールバックするように変更できます。

NetScaler ADM で組み込みテンプレートを使用して構成されたジョブを再スケジュールするには

1. NetScaler ADM で、［ネットワーク］>［構成ジョブ］に移動します。
2. インスタンスを編集、追加、または削除するジョブを選択し、変数値を指定してから、実行アクションと設定を変更します。
3. ［**Finish**］をクリックしてジョブを再スケジュールします。

> 注
>
> ジョブを選択して [**Execute Again**] をクリックすると、ソース、インスタンス、コマンドを変更せずにジョブを実行することもできます。これは、同じインスタンス群に対して同じコマンドセットを実行する必要がある場合に便利です。サーバー側の問題でジョブで一時的なエラーが発生すると、ジョブを再実行しなければならないことがあります。

構成ジョブでの構成監査テンプレートの再利用

February 6, 2024

管理者は、ジョブを作成して構成監査を実行するときに、構成コマンドを再利用可能な構成テンプレートのセットとして保存できるようになりました。構成ジョブで作成および保存された構成テンプレートは、構成監査で使用して、特定の Citrix ADC インスタンスに適用できる監査テンプレートを作成できます。同様に、構成監査モジュールで作成された監査テンプレートは、構成ジョブとして実行できるように、構成ジョブで使用できます。テンプレート内で行われた変更は、構成ジョブモジュールと構成監査モジュールの両方で表示されるようになりました。

以前は、構成ジョブテンプレートと構成監査テンプレートを同じ構成のために別々に作成し、別のファイルとして保存する必要がありました。このため、テンプレートの作成時と保守時に同じ作業を繰り返す必要がありました。

Citrix Application Delivery Management（ADM）では、このテンプレートをシステムに保存して、構成ジョブでも監査テンプレートを使用できるようにします。ここでは、監査テンプレートを構成ジョブの作成に使用できます。上記のように、テンプレートは、構成ジョブと構成監査との間で区別なく使用できます。

たとえば、負荷分散仮想サーバーを追加し、2 つのサービスを追加し、それらのサービスをその仮想サーバーにバインドするという、基本的な負荷分散構成を考えてみましょう。

この例では、次のコマンドを使用します。


```
add lb vserver servername HTTP ipaddress portnumber

add service servicename1 ipaddress1 HTTP 80

add service servicename2 ipaddress2 HTTP 80

bind lb vserver servername servicename1

bind lb vserver servername servicename2
<!--NeedCopy-->
```

構成監査でのテンプレートの作成と構成ジョブでのその使用

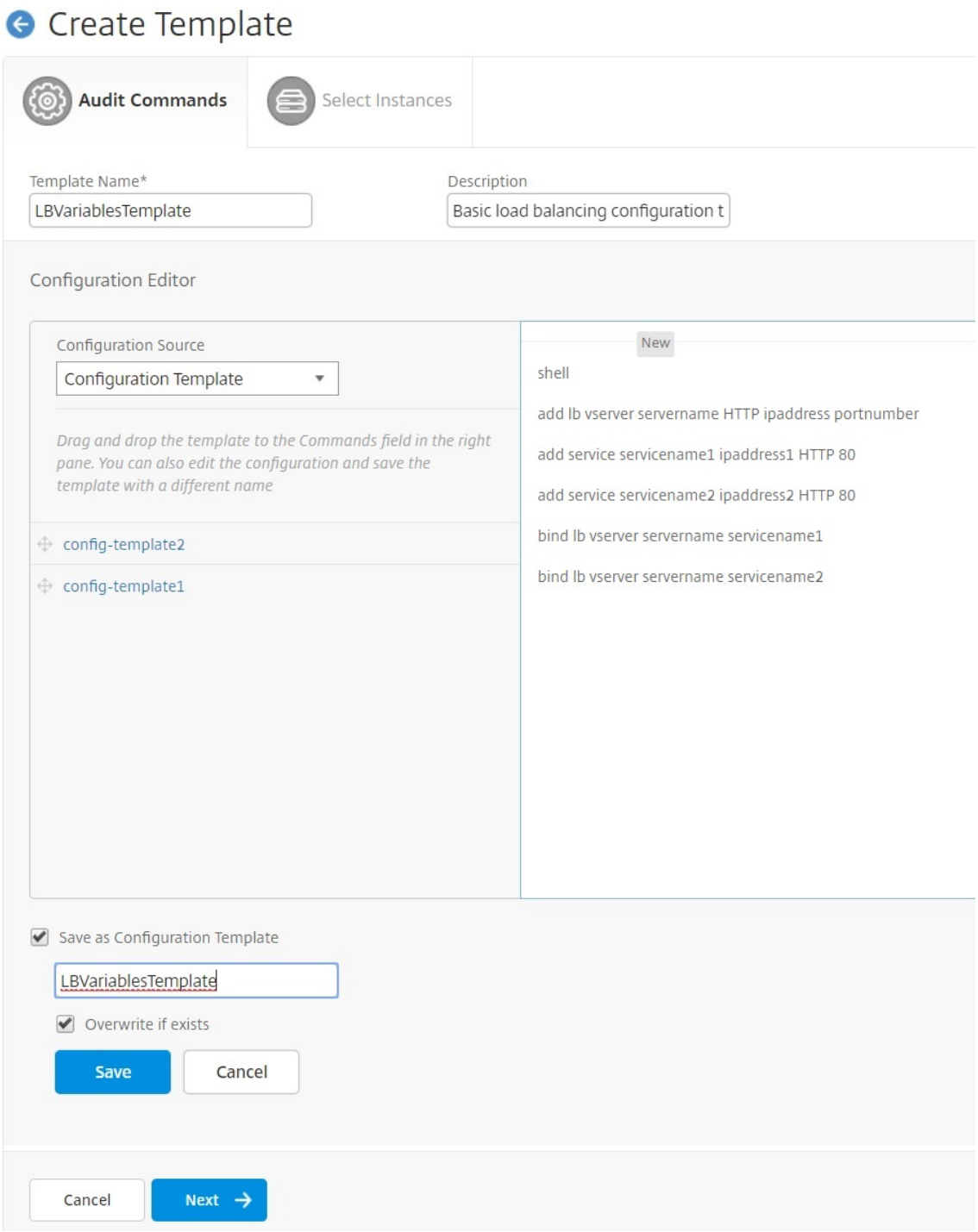
次のタスクを実行して、構成監査モジュールでテンプレートを作成し、それを構成ジョブモジュールで再利用します。

監査テンプレートを作成するには、次の手順に従います。

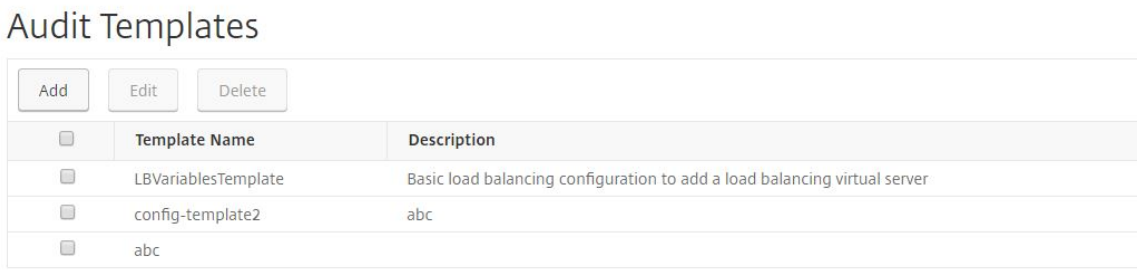
1. Citrix ADM で、[ネットワーク] **>** [構成監査] **>** [監査テンプレート] に移動し 、[追加] をクリック します。
2. **[** テンプレートの作成] ページで、テンプレート名を指定します。[説明] フィールドに、テンプレートの詳細情報を追加することもできます。
3. [**Commands**] ペインで、例のコマンドを入力します。
4. 「構成テンプレートとして保存」チェックボックスを選択し、テンプレートの名前を指定します。たとえば、このテンプレートに「LBVariablesTemplate」という名前を付けます。同じ名前が付いた他のテンプレートが存在する場合はそれを上書きすることを選択できます。

   > **注:** 監査テンプレート名は、設定テンプレート名と同じでもかまいません。

5. [保存] をクリックし、[次へ] をクリックします。



6. ［次へ］をクリックします。
7. **[**インスタンスの選択] タブで、これらの構成コマンドを実行する **Citrix ADC** インスタンスを選択し、［完了］をクリックします。新しいテンプレートが監査テンプレートの一覧に表示されるようになります。



8. これらの構成コマンドを実行するには、[ネットワーク] > [構成ジョブ] に移動し、 [ジョブの作成] をクリックします。前に作成した監査テンプレートは、構成テンプレートとして一覧に表示されます。

構成ジョブで監査テンプレートを再利用するには、次の手順に従います。

1. ジョブの名前を入力してインスタンスタイプを選択し、テンプレートをコマンドペインにドラッグアンドドロップします。

   構成ジョブの作成中に、ローカルファイル名とリモートファイル名のパラメーターを変数に変換できます。これにより、ジョブを実行するたびに、同じ Citrix ADC インスタンスセットのこれらのパラメータに異なるファイルを割り当てることができます。

2. 入力したコマンドで、変数に変換するファイル名を選択し、[変数に変換] をクリックします。
3. [**Select Inst** ances] タブで、これらのコマンドを実行するインスタンスを選択します。
4. コマンドで 変数を指定した場合は、**[Specify Variable Valu** es] タブで、次のいずれかのオプションを選択して、インスタンスの変数を指定します。

   - 入力ファイルからの変数値-入力ファイルをダウンロードして、コマンドで定義した変数の値を入力し、そのファイルを Citrix ADM サーバーにアップロードします。
   - [Common variable values for all instances] - syslog サーバーの IP アドレスとポートを指定します。

5. 「ジョブプレビュー」タブでは、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証して、「次へ」をクリックします。
6. 「実行」タブで、「完了」をクリックして構成ジョブを実行します。この時点で、別のサービスをこの負荷分散サーバーに追加して、そのサービスをそのサーバーにバインドする必要がある場合は、コマンドページでコマンドを編集し、保存することができます。
7. 「監査テンプレート」にナビゲートし、「追加」をクリックします。
8. 「LBVariablesTemplate」テンプレートをコマンドペインにドラッグアンドドロップします。そのテンプレートが新しいコマンドで更新されたことがわかります。

監査テンプレートは、[Audit Templates] ボックスの一覧に表示され、指定したインスタンスの構成に対して 12 時間ごとに実行されます。これで、テンプレートを作成し、構成ジョブモジュールと構成監査モジュールとの間で再使用できるようになりました。

構成テンプレートのインポートとエクスポート

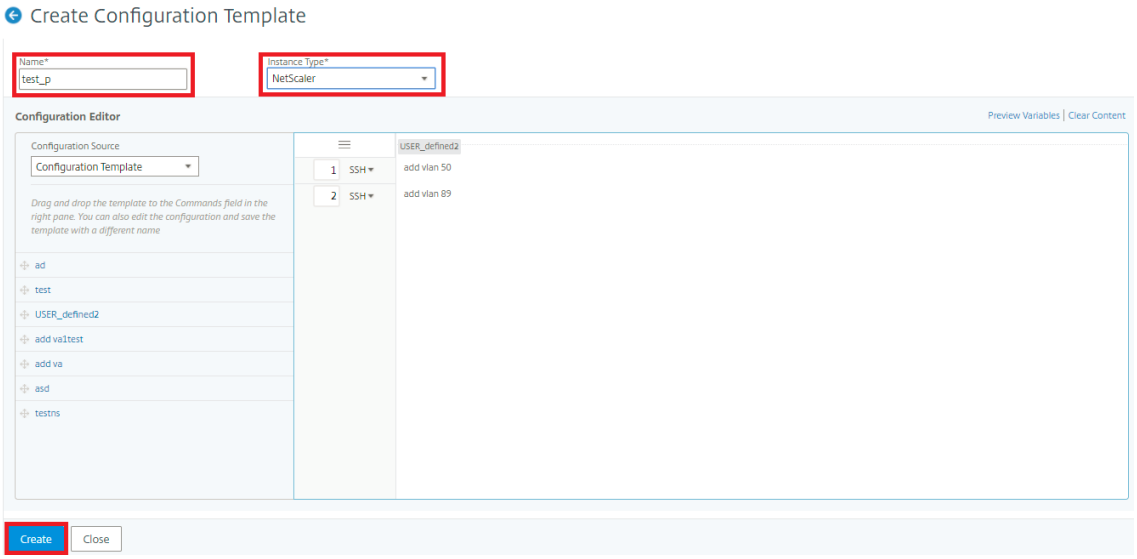
February 6, 2024

構成テンプレートは、どの Citrix Application Delivery Management（ADM）からでもエクスポートできます。また、将来いつでも同じまたは別の Citrix ADM にファイルをインポートできます。設定テンプレートデータ (設定コマンド、変数定義、パラメータなど) は失われません。

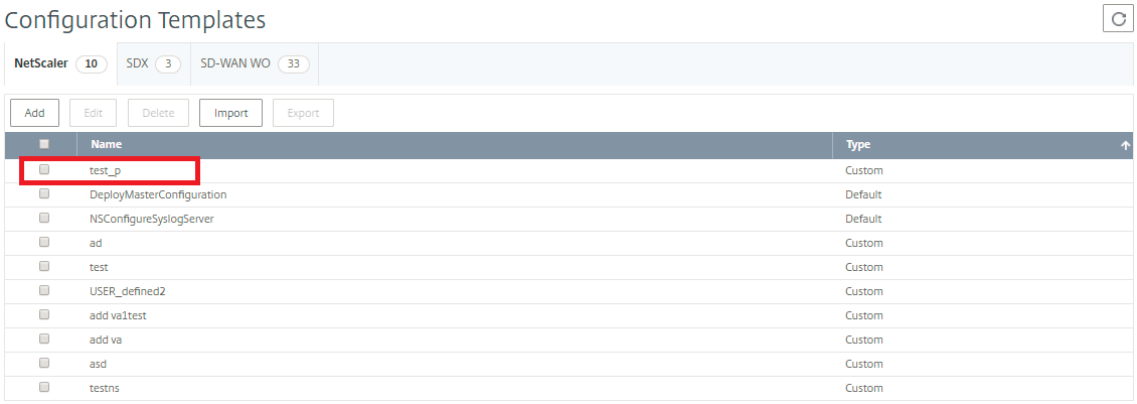
構成テンプレートを **.json** ファイル形式にエクスポートし、ローカルフォルダに保存できます。構成テンプレートをインポートできます。**JSON** ファイルを Citrix ADM に保存します。このファイルは新しい場合もあれば、同じまたは別の Citrix ADM からエクスポートしたファイルである場合もあります。

構成テンプレートをエクスポートするには、次の手順に従います。

1. [ネットワーク] **>** [構成ジョブ] **>** [構成テンプレート] に移動します。
2. 「追加」ボタンをクリックして、構成テンプレートを作成します。
3. [**Create Configuration Template**] ページで、設定テンプレート名を指定し、インスタンスタイプを選択します。[構成エディタ] で、ドロップダウンメニューから [構成テンプレート] として構成ソースを選択します。既存の構成テンプレートを構成エディターにドラッグアンドドロップできます。[作成] をクリックします。



4. [ネットワーク] **>** [構成ジョブ] **>** [構成テンプレート] に移動して、構成テンプレートのリストに作成されたテンプレートを表示します。

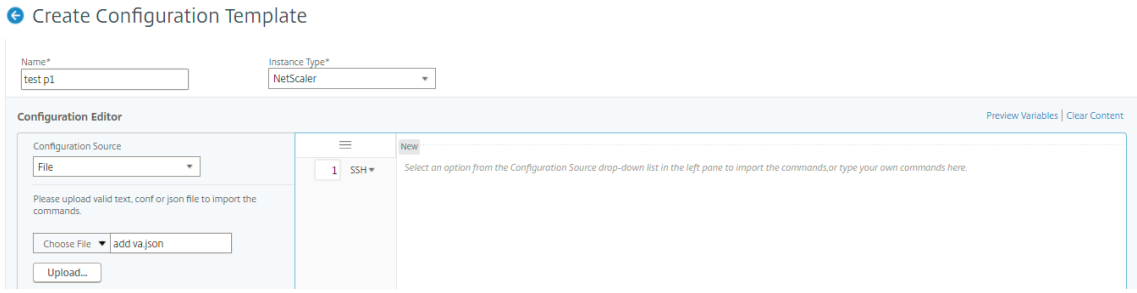


5. 新しく作成した構成テンプレートを選択し、[**Export**] ボタンをクリックします。

対応する構成テンプレートが **.json** 形式でローカルシステムにダウンロードされます。

構成テンプレートをインポートするには、次の手順に従います。

1. [ネットワーク] **>** [構成ジョブ] **>** [構成テンプレート] に移動し、[インポート] ボタンをクリックします。構成テンプレートの **.json** ファイルがあるパスを選択し **.json** ファイルをアップロードします。エクスポート済みの **.json** ファイルをアップロードすることをお勧めします。
2. 構成エディターの [ファイル] オプションを使用して構成テンプレートをインポートすることもできます。
3. 構成エディターのドロップダウンメニューから [ファイル] を選択します。
4. [ファイルを選択] (**.json** files) をローカルシステムからアップロードし、設定テンプレートをアップロードします。**JSON** ファイル。



> 注
>
> - 新しくインポートされたテンプレートはすべて、新しい ID 文字列で保存されます。
> - 構成テンプレートをインポートできるのは、ファイルが **json** 形式で保存されている場合だけです。**.json** ファイル以外の構成テンプレートをローカルシステムからインポートすると、エラーが表示され、ファイルのインポートに失敗します。

メンテナンス・ジョブ

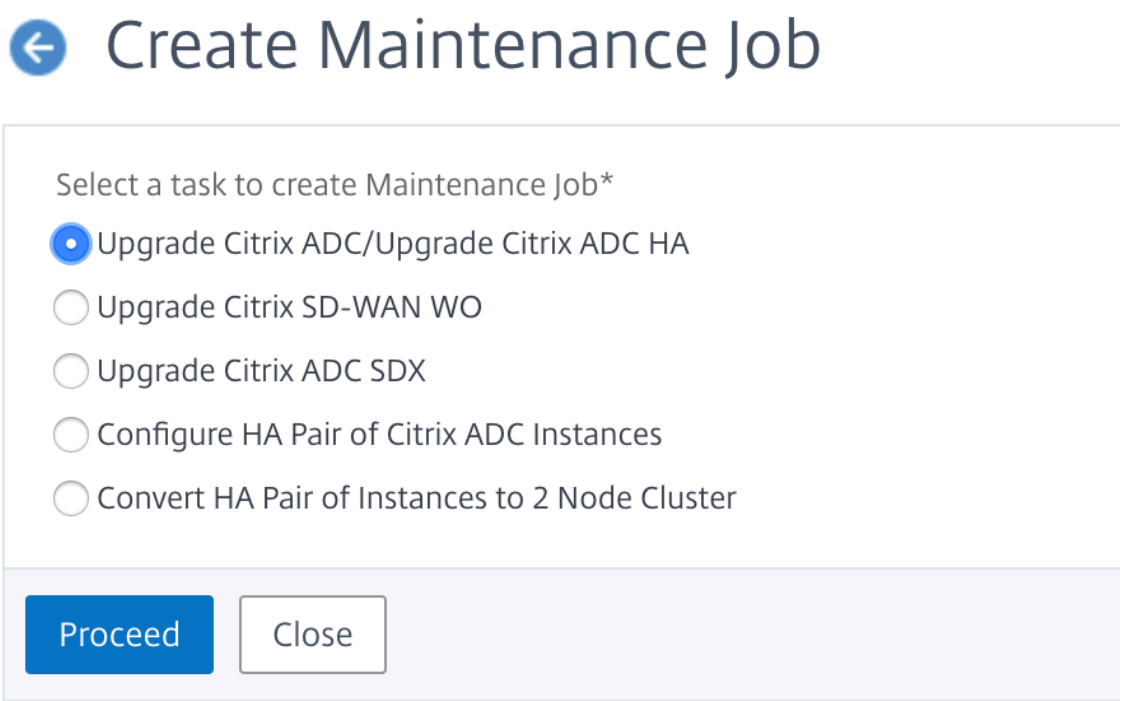
February 6, 2024

Citrix ADM を使用して次のメンテナンスジョブを作成できます。その後、特定の日時にメンテナンスジョブをスケジュールできます。

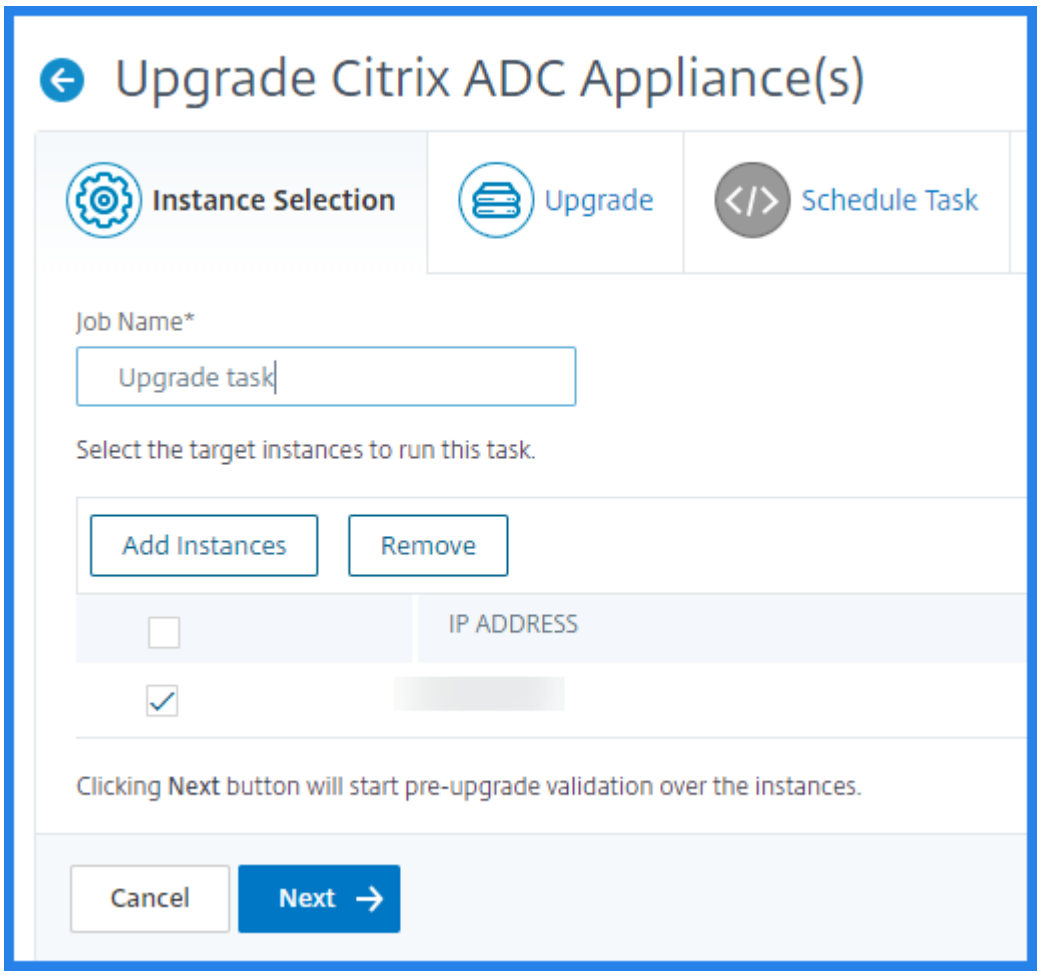
- NetScaler ADC インスタンスのアップグレード
- Citrix SD WAN-WO インスタンスのアップグレード
- NetScaler ADC SDX インスタンスのアップグレード
- NetScaler ADC インスタンスの HA ペアを構成する
- インスタンスの HA ペアを 2 ノードクラスタに変換

NetScaler ADC インスタンスのアップグレードをスケジュールする

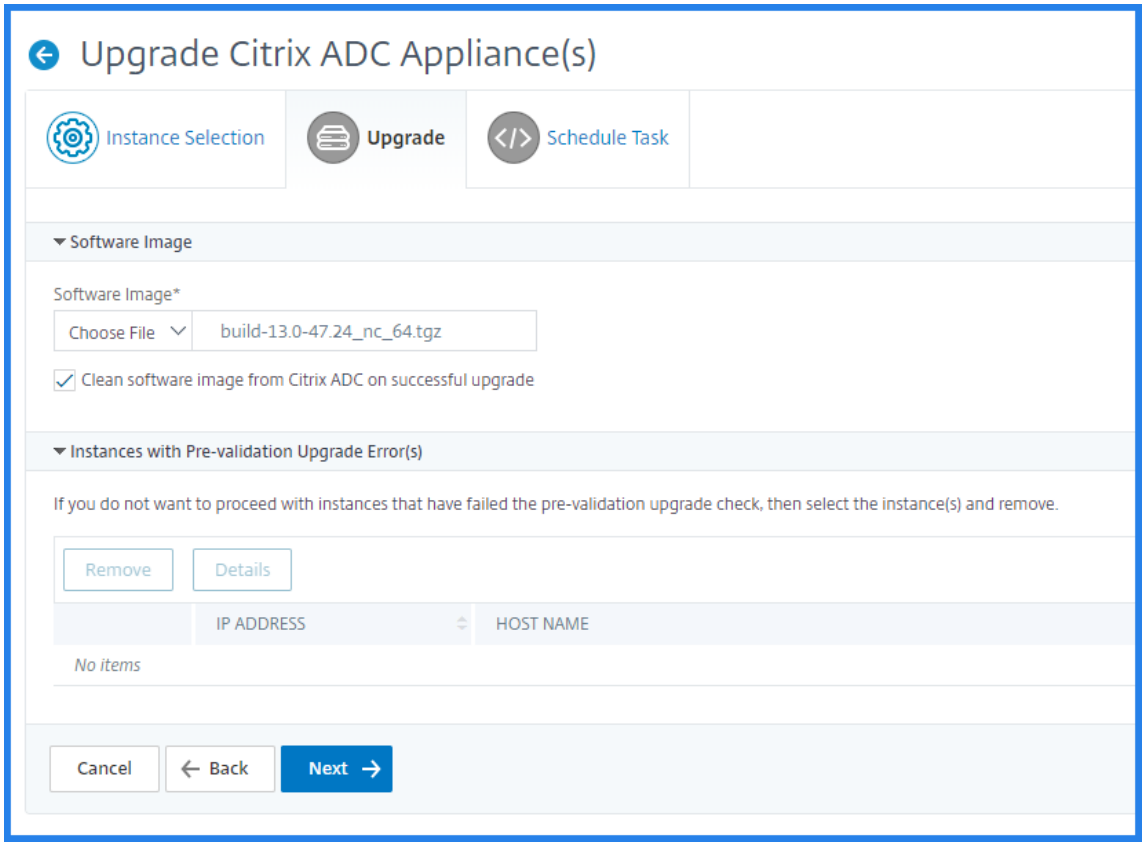
1. [ネットワーク] > [構成ジョブ] > [メンテナンスジョブ] に移動します。[ジョブの作成] ボタンをクリックします。
2. ［メンテナンスタスクの作成］ページで、［Citrix ADC HA のアップグレード**/Citrix ADC HA** のアップグレード］を選択し、［続行］をクリックします。



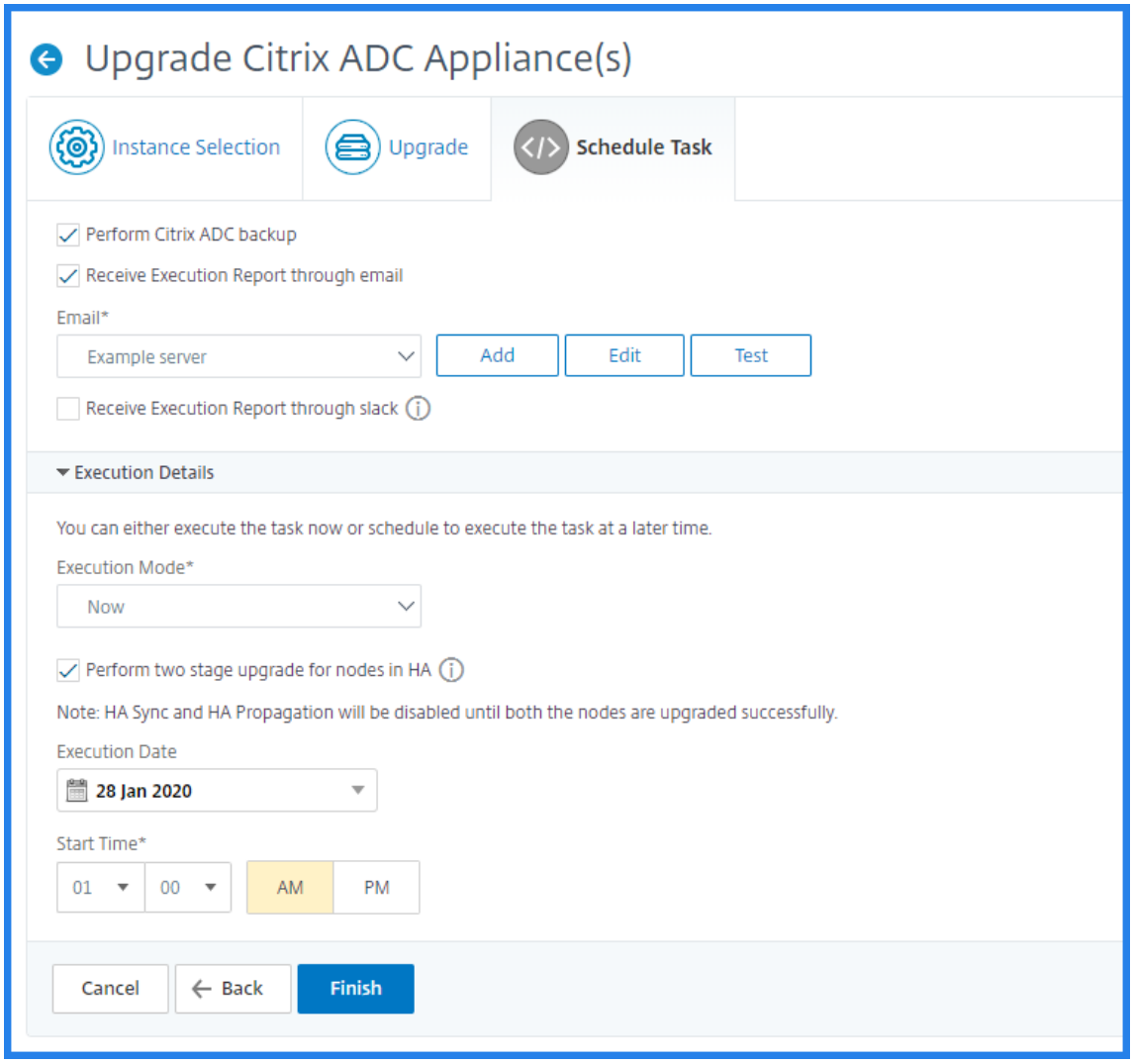
3. 「Citrix ADC アプライアンスのアップグレード」ページの「インスタンスの選択」タブで、アップグレードプロセスを実行する Citrix ADC インスタンスを追加します。[**Next**] をクリックして、選択したインスタンスでアップグレード前の検証を開始します。



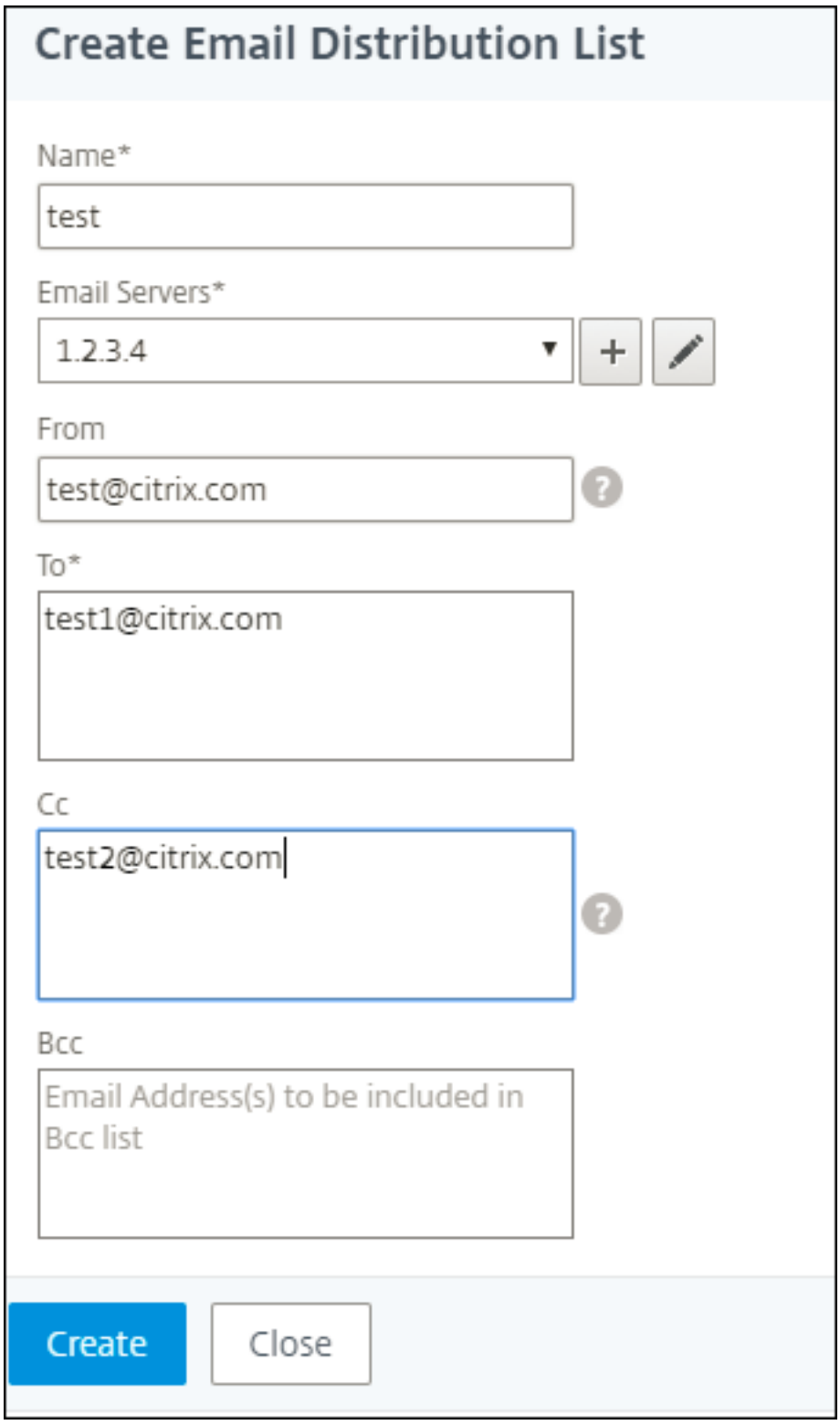
4. ［アップグレード］タブの［ソフトウェアイメージ］リストで、［ローカル］（ローカルマシン）または［アプライアンス］（ビルドファイルは Citrix ADM 仮想アプライアンスに存在する必要があります）を選択します。



5. 電子メール通知を有効にして、NetScaler ADC インスタンスのアップグレードの実行レポートを受け取ることができます。「実行レポートを電子メールで受信」チェックボックスをクリックして、電子メール通知を有効にします。
6. アイコンを選択してメール配布リストを作成します。
7. Citrix ADC インスタンスを今すぐアップグレードするには、実行モードリストから「**Now**」を選択します。
8. Citrix ADC インスタンスを後でアップグレードするには、実行モードリストから「後で」を選択します。次に、Citrix ADC インスタンスをアップグレードするための実行日と開始時間を選択できます。

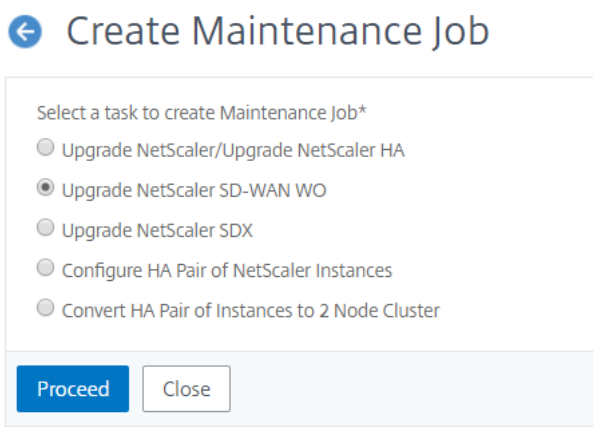


9. 「メール配布リストの作成」ページで、メール配布リストの名前を指定します。電子メール通知を電子メールサーバに送信するために使用する SMTP メールサーバを追加します。[差 出 人] ボックスに、メッセージの送信元の電子メールアドレスを追加します。[宛先] ボックスに、メッセージを送信する 1 つまたは複数のアドレスを追加します。また、メッセージのコピーやコピーの送信先となる電子メールアドレスを追加して、これらのアドレスをメッセージまたはコピーに表示しないようにすることもできます。[作成] をクリックします。電子メール同報リストを作成したら、[**Finish**] をクリックして設定プロセスを完了します。

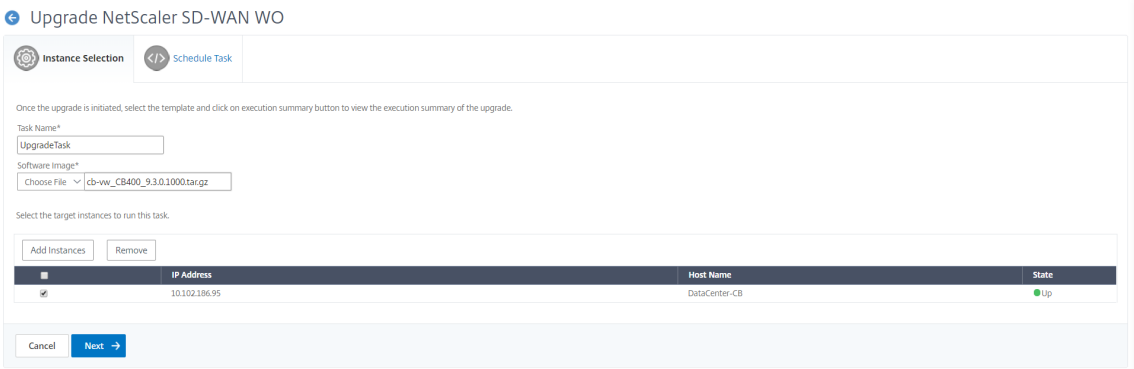


Citrix SD-WAN WO インスタンスのアップグレードのスケジュール設定

1. Citrix ADM で、[ネットワーク] > [構成ジョブ] **>** [メンテナンスジョブ] に移動します。[ジョブの作成] ボタンをクリックします。
2. 「メンテナンスジョブの作成」ページで、「**Citrix SD-WAN WO** のアップグレード」を選択し、「続行」をクリックします。

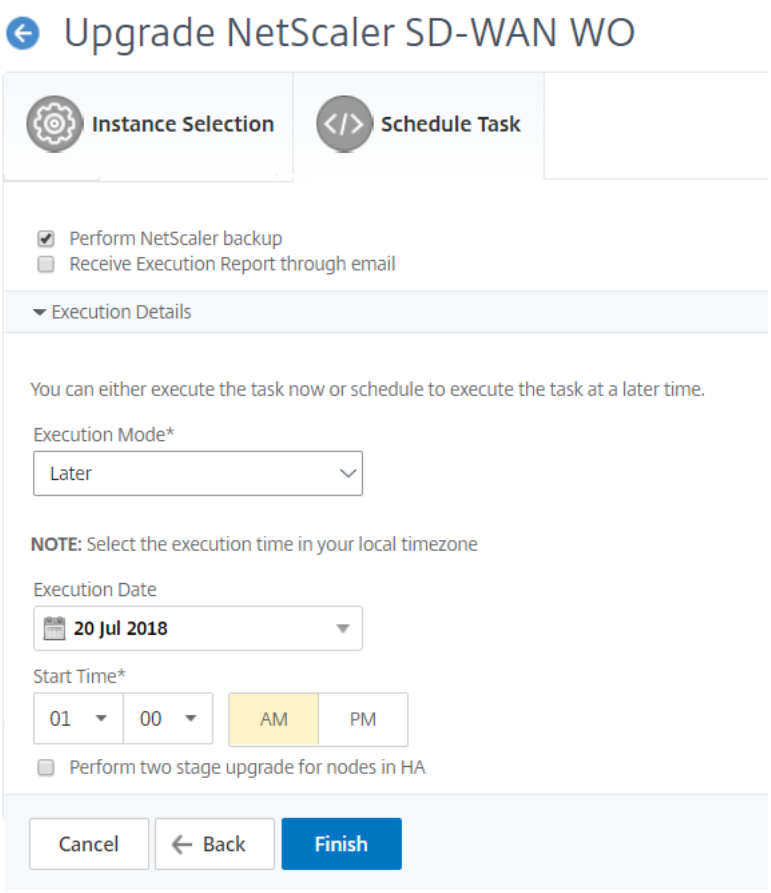


3. 「**Citrix SD-WAN WO** のアップグレード」ページの「インスタンスの選択」タブで、タスク名を追加します。ソフトウェアイメージリストから、ローカル（ローカルマシン）またはアプライアンス（ビルドファイルは Citrix MAS 仮想アプライアンスに存在する必要があります）を選択します。アップグレードプロセスを実行する Citrix SD-WAN WO インスタンスを追加します。[次へ] をクリックします。



4. Citrix SD-WAN WO インスタンスを今すぐアップグレードするには、実行モードリストから「Now」を選択します。[完了] をクリックします。
5. Citrix SD-WAN WO インスタンスを後でアップグレードするには、実行モードリストから「後で」を選択します。次に、Citrix SD-WAN WO インスタンスのアップグレードの実行日と開始時間を選択できます。
6. 電子メール通知を有効にして、Citrix SD-WAN WO インスタンスのアップグレードの実行レポートを受け取ることができます。「実行レポートを電子メールで受信」チェックボックスをクリックして、電子メール通知を有効にします。

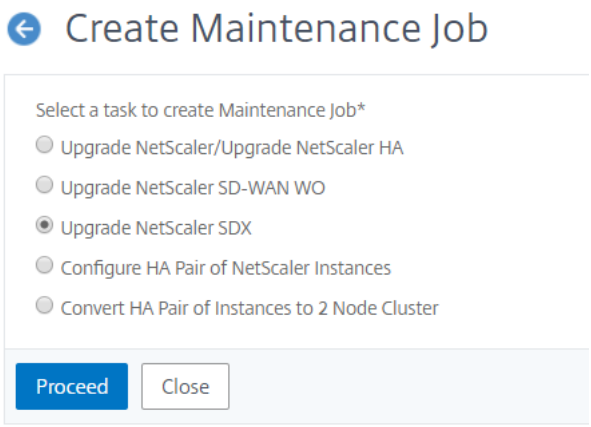
7. **+** アイコンを選択して、メール配布リストを作成します。



8. **[** 電子メール配布リストの作成] ページで、電子メール配布リストの名前を指定します。メール通知をメールサーバーに送信するために使用する SMTP メールサーバーを追加します。[差 出 人] ボックスに、メッセージの送信元の電子メールアドレスを追加します。「宛先」ボックスに、メッセージを送信する 1 つまたは複数のアドレスを追加します。また、メッセージのコピーやコピーを送信する電子メールアドレスを 1 つまたは複数追加できます。これらのアドレスは、メッセージやコピーに表示されません。[作成] をクリックします。電子メール同報リストを作成したら、[**Finish**] をクリックして設定プロセスを完了します。

NetScaler ADC SDX インスタンスのアップグレードをスケジュールする

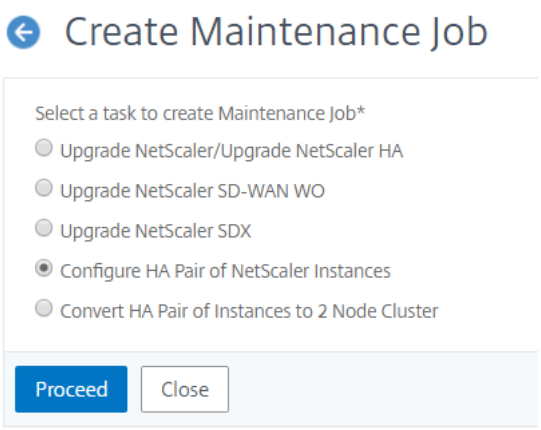
1. Citrix ADM で、[ネットワーク] > [構成ジョブ] **>** [メンテナンスジョブ] に移動します。[ジョブの作成] ボタンをクリックします。
2. [メンテナンスジョブの作成] ページで、[**NetScaler ADC SDX** のアップグレード] を選択し、[続行] をクリックします。



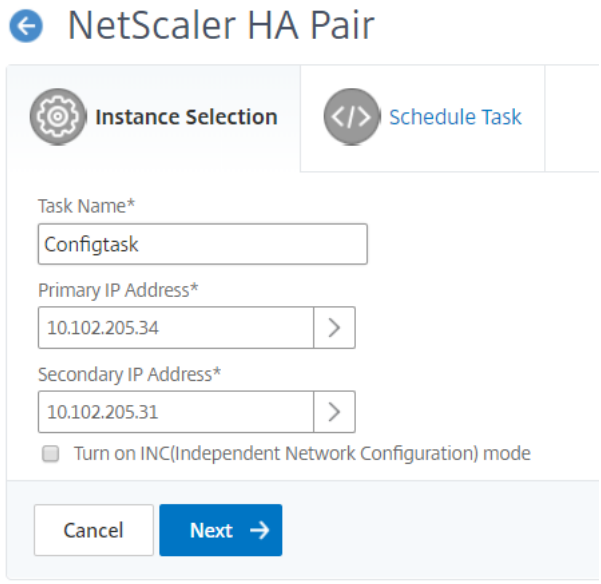
3. [**NetScaler ADC SDX** アプライアンスのアップグレード］ページの［インスタンスの選択］タブで、［タスク名］を追加します。ソフトウェアイメージリストから、ローカル（ローカルマシン）またはアプライアンス（ビルドファイルが NetScaler ADM 仮想アプライアンスにある必要があります）を選択します。アップグレードプロセスを実行する NetScaler ADC SDX インスタンスを追加します。［次へ］をクリックします。
4. 電子メール通知を有効にして、NetScaler ADC SDX インスタンスのアップグレードの実行レポートを受け取ることができます。「実行レポートを電子メールで受信」チェックボックスをクリックして、電子メール通知を有効にします。
5. **+** アイコンを選択して、メール配布リストを作成します。
6. Citrix ADC SDX インスタンスを今すぐアップグレードするには、実行モードリストから「Now」を選択します。［完了］をクリックします。
7. Citrix ADC SDX インスタンスを後でアップグレードするには、実行モードリストから「後で」を選択します。その後、NetScaler ADC SDX インスタンスをアップグレードするための実行日と開始時刻を選択できます。
8. **[** 電子メール配布リストの作成] ページで、電子メール配布リストの名前を指定します。メール通知をメールサーバーに送信するために使用する SMTP メールサーバーを追加します。[差 出 人] ボックスに、メッセージの送信元の電子メールアドレスを追加します。「宛先」ボックスに、メッセージを送信する 1 つまたは複数のアドレスを追加します。また、メッセージのコピーやコピーを送信する電子メールアドレスを 1 つまたは複数追加できます。これらのアドレスは、メッセージやコピーに表示されません。［作成］をクリックします。電子メール同報リストを作成したら、[**Finish**] をクリックして設定プロセスを完了します。

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. [ネットワーク] > [構成ジョブ] > [メンテナンスジョブ] に移動します。[ジョブの作成] ボタンをクリックします。
2. ［メンテナンスジョブの作成］ページで、**NetScaler ADC** インスタンスの高可用性ペアの構成］を選択し、［続行］をクリックします。



3. [**NetScaler ADC** 高可用性ペア] ページの [インスタンスの選択] タブで、[タスク名] を追加します。プライマリ IP アドレスとセカンダリアドレスを入力し、[**Next**] をクリックします。

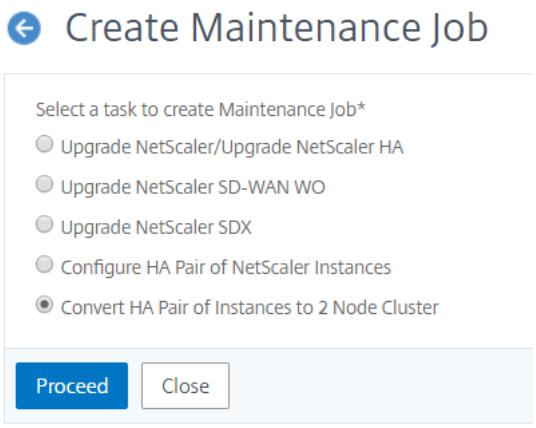


4. [タスクのスケジュール] タブで、NetScaler ADC HA ペアを今すぐ構成するか、後で構成するかを選択できます。
5. Citrix ADC HA ペアを今すぐ構成するには、実行モードリストから「Now」を選択します。電子メール通知を有効にして、NetScaler ADC HA ペアの実行レポートを受信できます。「実行レポートを電子メールで受信」チェックボックスをクリックして、電子メール通知を有効にします。
6. Citrix ADC HA ペアを後で構成するには、「実行モード」リストから「後で」を選択します。その後、eExecution 日と開始時刻を選択できます。電子メール通知を有効にして、NetScaler ADC HA ペアの実行レポートを受信できます。「実行レポートを電子メールで受信」チェックボックスをクリックして、電子メール通知を有効にします。
7. **+** アイコンを選択して、メール配布リストを作成します。

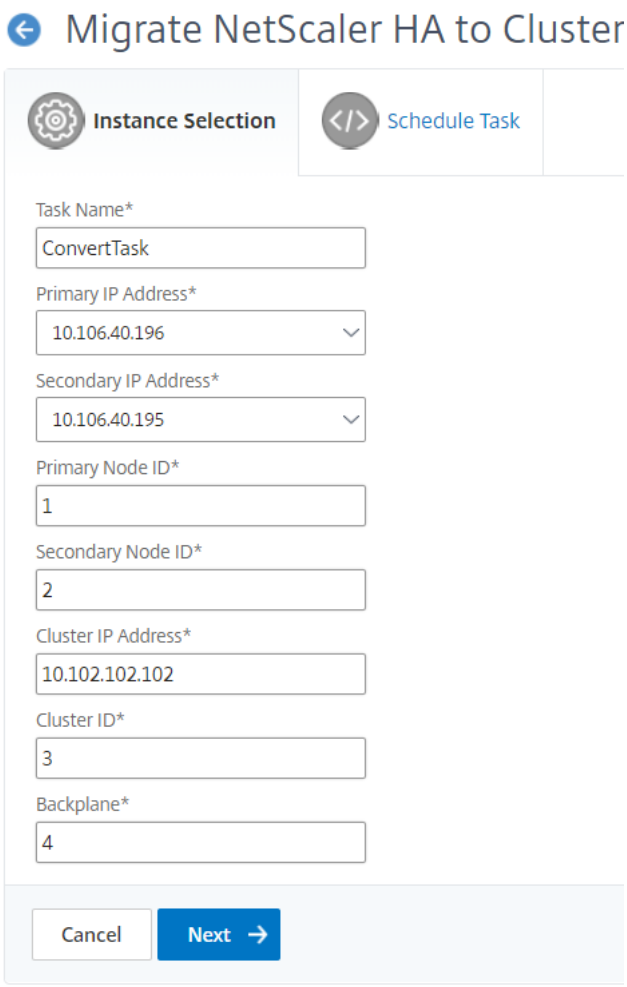
8. 「メール配布リストの作成」ページで、メール配布リストの名前を指定します。メール通知をメールサーバーに送信するために使用する SMTP メールサーバーを追加します。「差出人」ボックスに、メッセージの送信元の電子メールアドレスを追加します。「宛先」ボックスに、メッセージを送信する 1 つまたは複数のアドレスを追加します。また、メッセージのコピーやコピーを送信する電子メールアドレスを 1 つまたは複数追加できます。これらのアドレスは、メッセージやコピーに表示されません。［作成］をクリックします。電子メール同報リストを作成したら、[**Finish**] をクリックして設定プロセスを完了します。

インスタンスの **HA** ペアをクラスタに変換するスケジュールを設定する

1. [ネットワーク] > [構成ジョブ] > [メンテナンスジョブ] に移動します。[ジョブの作成] ボタンをクリックします。
2. [メンテナンスジョブの作成] ページで、[**HA** ペアの **2** ノードクラスタに変換] を選択し、[続行] をクリックします。



3. ［**NetScaler ADC HA** をクラスターに移行 する］ページの［インスタンスの選択］タブで、［タスク名］を追加します。プライマリ IP アドレス、セカンダリアドレス、プライマリノード ID、セカンダリノード ID、クラスタ IP アドレス、クラスタ ID、およびバックプレーンを指定します。［次へ］をクリックします。



4. ［タスクのスケジュール］タブでは、NetScaler ADC HA をクラスターに移行するか、後で移行するかを選択できます。
5. Citrix ADC HA ペアを後で構成するには、「実行モード」リストから「後で」を選択します。その後、実行日と開始時間を選択できます。電子メール通知を有効にして、NetScaler ADC HA ペアの実行レポートを受信できます。「実行レポートを電子メールで受信」チェックボックスをクリックして、電子メール通知を有効にします。
6. **+** アイコンを選択して、メール配布リストを作成します。
7. **[** 電子メール配布リストの作成] ページで、電子メール配布リストの名前を指定します。メール通知をメールサーバーに送信するために使用する SMTP メールサーバーを追加します。「差出人」ボックスに、メッセージの送信元の電子メールアドレスを追加します。「宛先」ボックスに、メッセージを送信する 1 つまたは複数のアドレスを追加します。また、メッセージのコピーやコピーを送信する電子メールアドレスを 1 つまたは複数追加できます。これらのアドレスは、メッセージやコピーに表示されません。［作成］をクリックします。電子メール同報リストを作成したら、[**Finish**] をクリックして設定プロセスを完了します。

構成監査

February 6, 2024

このドキュメントには、以下が含まれます。

- 監査テンプレートの作成
- 監査レポートの表示
- 複数インスタンスにまたがる監査構成の変更
- ネットワーク構成に関するアドバイスの表示
- NetScaler インスタンスの構成監査をポーリングする方法

監査テンプレートの作成

February 6, 2024

ネットワークのパフォーマンスを最適化するため、特定の構成を特定のインスタンス上で実行する場合があります。また、管理対象の Citrix Application Delivery Controller（ADC）インスタンス間の構成変更の監視、構成エラーのトラブルシューティング、および突然のシステムシャットダウン後に未保存の構成の回復も行う必要があります。特定のインスタンスで監査する特定の構成を持つ監査テンプレートを作成できます。Citrix Application Delivery Management（Citrix ADM）は、これらのインスタンスを監査テンプレートと比較し、構成に不一致がある場合は報告します。構成の不一致があると、Citrix ADM は構成差分レポートを生成します。これにより、不要な構成変更のトラブルシューティングと修正が可能になります。

監査テンプレートの実行を自動化するには、

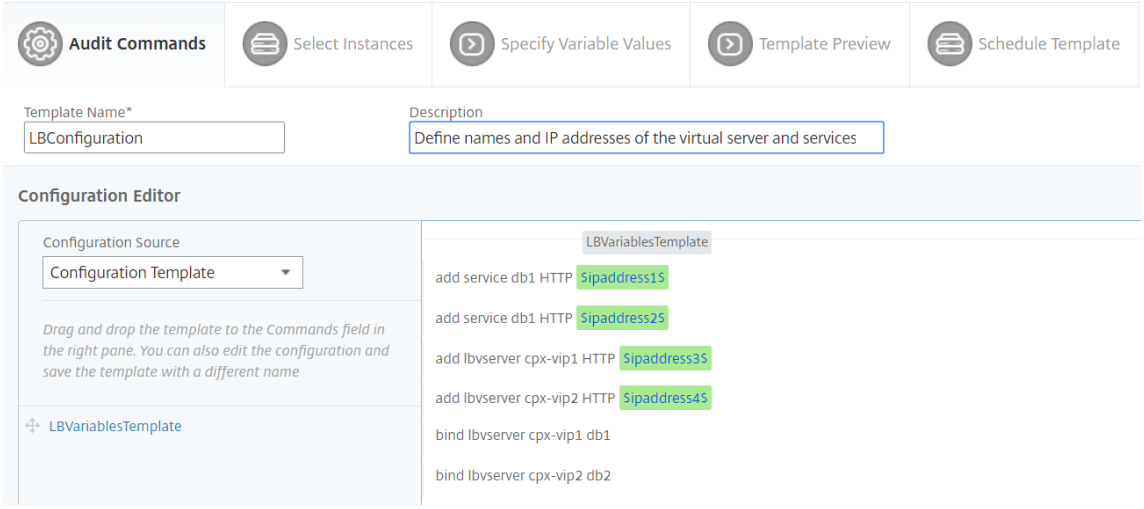
- テンプレートを実行する時間のスケジュールを設定する
- Citrix ADM がテンプレートを実行する頻度を設定します。テンプレートは、毎日、週の特定の日、または月の特定の日に実行できます。

また、NetScaler ADM によって生成された差分レポートを、構成可能な特定の電子メールアドレスに送信するオプションもあります。このオプションを使用すると、ユーザーはレポートをメール添付ファイルとして受信できます。ユーザーが NetScaler ADM にログオンしてレポートを手動でエクスポートする必要はありません。

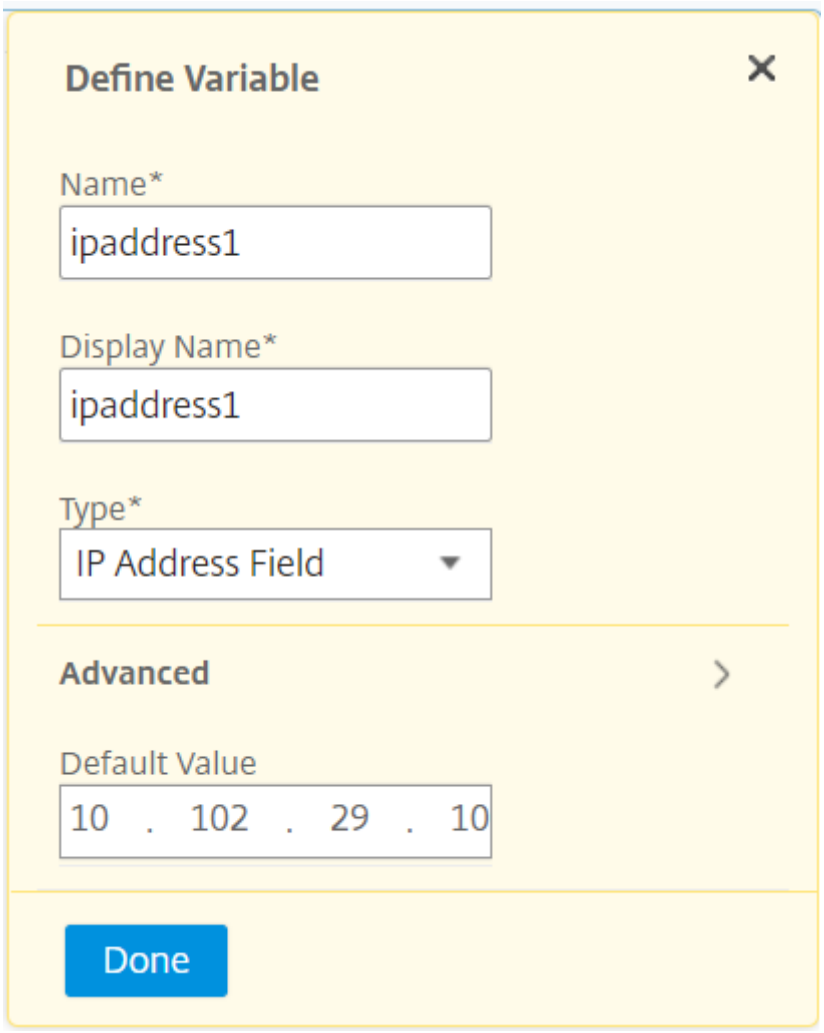
監査テンプレートを作成するには、次の手順に従います。

1. [ネットワーク] > [構成監査**] > [**監査テンプレート] に移動し 、[追加] をクリック します。
2. [テンプレートの作成] ページおよび [監査コマンド] タブで、テンプレート名とその説明を指定します。

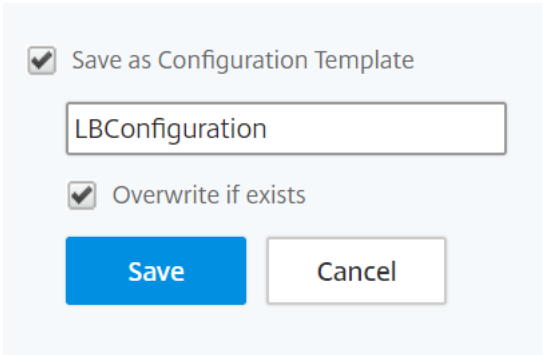
3. [構成エディタ] ページで、コマンドを入力し、コマンドを構成テンプレートとして保存します。既存のテンプレートを左ペインからエディタにドラッグすることもできます。
4. 変数に変換する値を選択し、[変数に変換] をクリックします。たとえば、負荷分散サーバーの IP アドレス「ipaddress1」を選択し、「変数に変換」をクリックします。この変数は、下の図のように「$」で囲まれています。



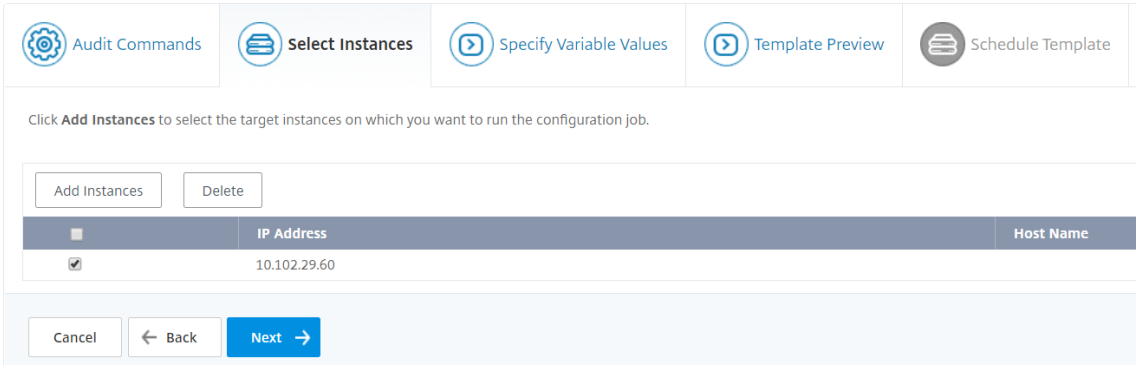
「変数の定義」(Define Variable) ウィンドウで、この変数のプロパティ (名前、表示名、変数のタイプ) を設定します。変数のデフォルト値をさらに指定する場合は、「詳細」(**Advanced**) オプションをクリックします。



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。

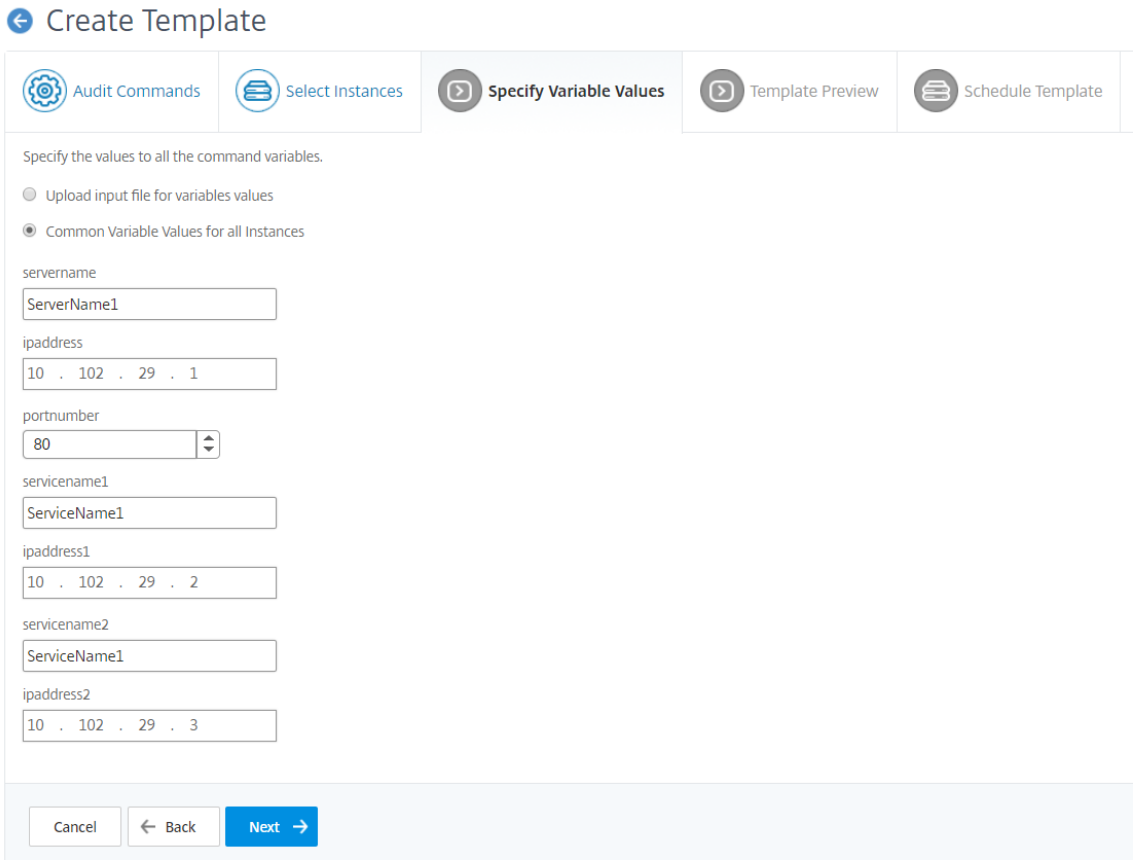


7. [変数値の指定] タブには、次の 2 つのオプションがあります。

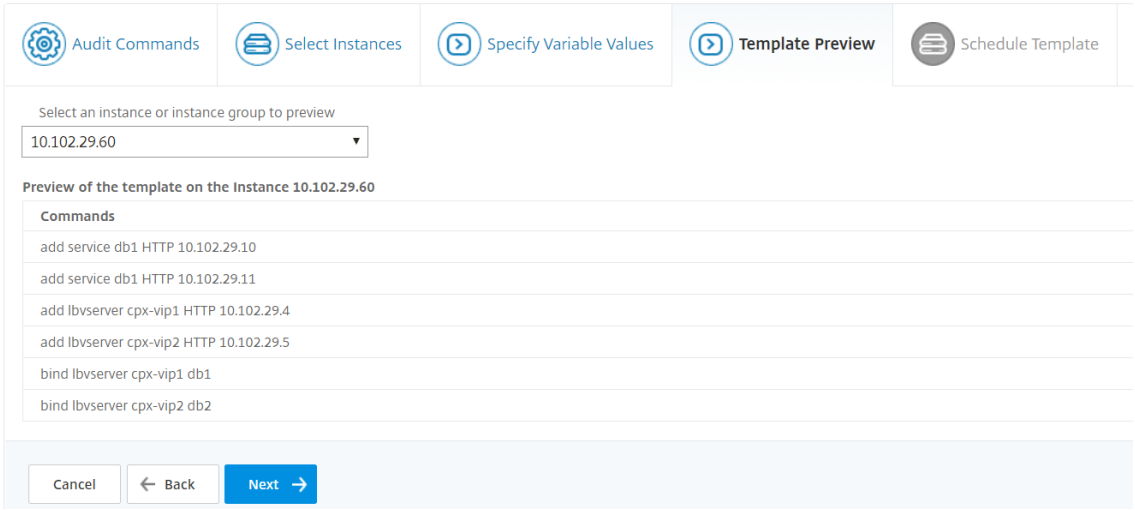
   a) 入力ファイルをダウンロードして、コマンドで定義した変数の値を入力し、NetScaler ADM サーバーにファイルをアップロードします。

   b) すべてのインスタンスに定義した変数に共通の値を入力します。

8. [次へ] をクリックします。



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。



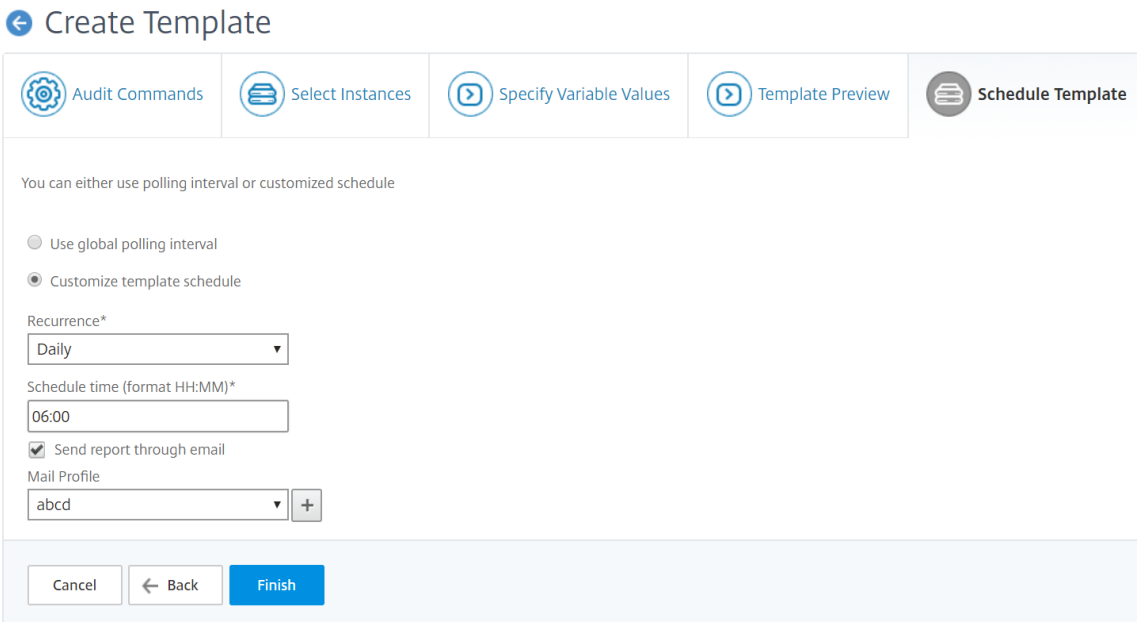
10. [**Schedule Template**] タブには、テンプレートの実行をスケジュールし、差分レポートを送信するようにメールアドレスを設定する次のオプションがあります。

    - 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。

      > 注:
      >
      > NetScaler ADM でグローバルポーリング間隔を構成するには、［ネットワーク］>［構成監査］>［監査テンプレート］の順に選択し、［グローバルポーリング間隔］をクリックします。［ポーリング間隔］フィールドに、Citrix ADM がインスタンスをグローバルにポーリングする時間を分単位で入力します。

    - テンプレート集計表をカスタマイズします。このオプションを使用して、テンプレートを実行する必要がある時間と頻度を設定します。
    - レポートを電子メールで送信。このオプションを使用して、差分レポートをメールの添付ファイルとして送信するメールプロファイルを設定します。

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。

監査レポートを表示する

February 6, 2024

Citrix Application Delivery Management（Citrix ADM）では、構成監査セクションで構成監査差分レポートを表示およびダウンロードできます。設定監査セクションでは、すべてのインスタンスおよびインスタンスごとに概要レポートをエクスポートできます。また、インスタンスとテンプレートのペアごとに詳細な差分レポートをエクスポートすることもできます。

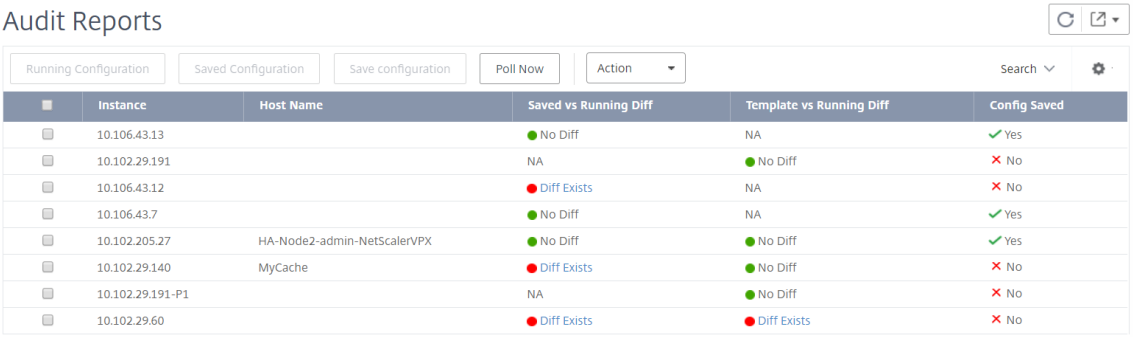
[Audit Templates] リストに表示される監査テンプレートは、指定したインスタンスの設定に対してスケジュールされた時刻に実行されます。［構成監査］ダッシュボードの ［**NetScaler Config Drift** ］グラフには、保存されていない構成に対して保存された構成の変更に関する詳細な情報が表示されます。**NetScaler Config Drift** チャートをクリックすると、次の監査レポートページに「Diff Exists（差分あり）」と「差分なし」の両方を示すインスタンスのリストが表示されます。Citrix ADM によって表示される差分レポートをダウンロードできます。

NetScaler ADM では、差分のレポートの自動エクスポートをメール添付ファイルとしてスケジュールするオプションも用意されています。レポートのエクスポートをスケジュールする方法の詳細については、「監査テンプレートの作成」を参照してください。

構成監査レポートをエクスポートするには、次の手順に従います。

1. NetScaler ADM で、［ネットワーク］>［構成監査］に移動します。

2. [構成監査] ページで、**NetScaler ADC** の構成ドリフトグラフ内をクリックします。
3. 「監査レポート」ページには、相違があるインスタンスが一覧表示されます。このページには、構成実行に違いがないインスタンスのリストも表示されます。

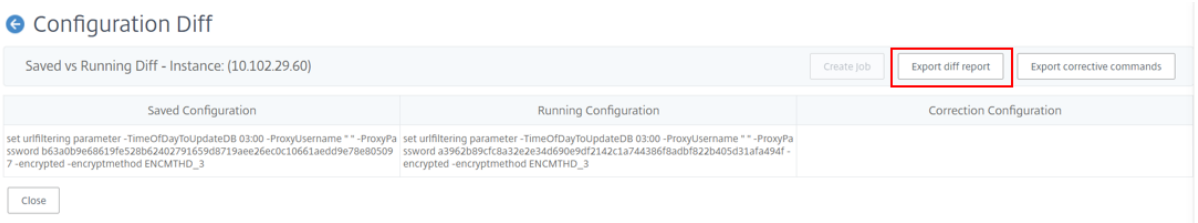


画像では、一部のインスタンスでは差分が 保存済みと実行差分 にのみ存在し、一部のインスタンスでは差分が テンプレートと実行差分にのみ存在することがわかります。場合によっては、保存された差分と実行中の差分とテンプレートと実行中の差分の両方に違いがあります。

保存された差分と実行中の差分比較

インスタンスに保存された設定と、そのインスタンスで現在実行中の設定との相違のレポートを表示できます。たとえば、[保存済みと実行中の ** 相違の比較] で、インスタンスの [相違が存在する] をクリックします。**

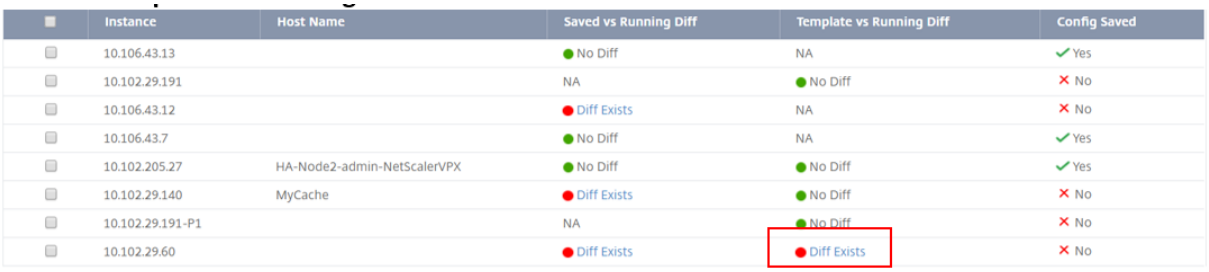
ここでは、そのインスタンスの構成実行差分に対する、保存された構成のレポートを確認できます。



[差分レポートのエクスポート] をクリックして、差分レポートの.csv ファイルをダウンロードします。[修正コマンドのエクスポート] をクリックして、コマンドを.txt ファイルにエクスポートすることもできます。その後、構成ジョブから関連する Citrix ADM インスタンスでコマンドを実行して、そのインスタンスの構成を修正できます。

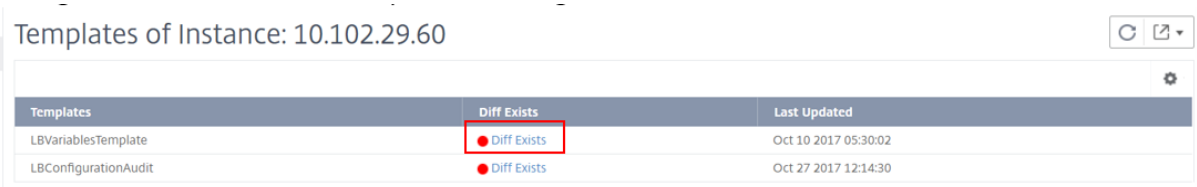
テンプレートと実行中の差分

テンプレートと実行差分 には、デフォルトのテンプレートである 保存済みと実行差分 以外のすべてのテンプレートが含まれます。テンプレートと実行構成の違いを確認できます。たとえば、「テンプレート」と「実行中差分」のインスタンスの **1** つに対して「差分」をクリックします。

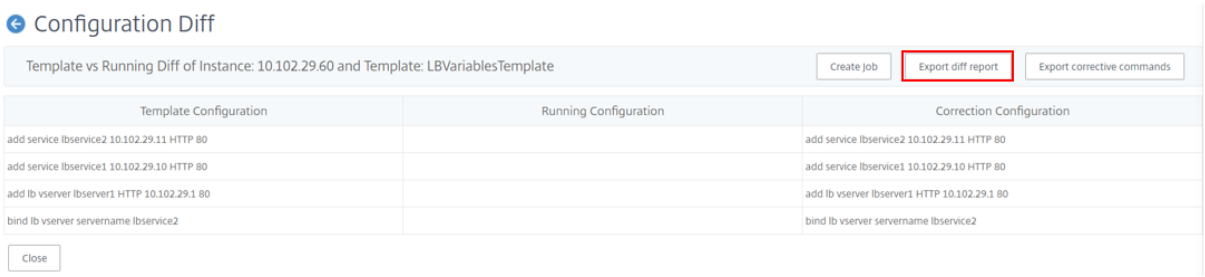


Instance	Host Name	Saved vs Running Diff	Template vs Running Diff	Config Saved
10.106.43.13		No Diff	NA	Yes
10.102.29.191		NA	No Diff	No
10.106.43.12		Diff Exists	NA	No
10.106.43.7		No Diff	NA	Yes
10.102.205.27	HA-Node2-admin-NetScalerVPX	No Diff	No Diff	Yes
10.102.29.140	MyCache	Diff Exists	No Diff	No
10.102.29.191-P1		NA	No Diff	No
10.102.29.60		Diff Exists	Diff Exists	No

これで、2 つのテンプレートに diff が表示され、NetScaler ADM インスタンスはテンプレートが探しているものとは異なる構成になっていることがわかります。



もう一度「相違が存在する」をクリックします。次の図は、テンプレートが探している設定と、そのようなコマンドが設定されていないか、削除されていないために空白になっている実行構成を示しています。また、修正設定や、設定を修正するために実行するコマンドも表示されます。



[差分レポートのエクスポート] をクリックして、差分レポートの.csv ファイルをダウンロードします。[修正コマンドのエクスポート] をクリックして、コマンドを.txt ファイルにエクスポートすることもできます。その後、CLI でコマンドを実行して、そのインスタンスの設定を修正できます。

次の図は、システムにダウンロードされる.csv diff ファイルの例を示しています。

#Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate		
Template Configuration	Running Configuration	Correction Configuration
add service lbservice2 10.102.29.11 HTTP 80		add service lbservice2 10.102.29.11 HTTP 80
add service lbservice1 10.102.29.10 HTTP 80		add service lbservice1 10.102.29.10 HTTP 80
add lb vserver lbserver1 HTTP 10.102.29.1 80		add lb vserver lbserver1 HTTP 10.102.29.1 80
bind lb vserver servername lbservice2		bind lb vserver servername lbservice2

インスタンス間の設定変更の監査

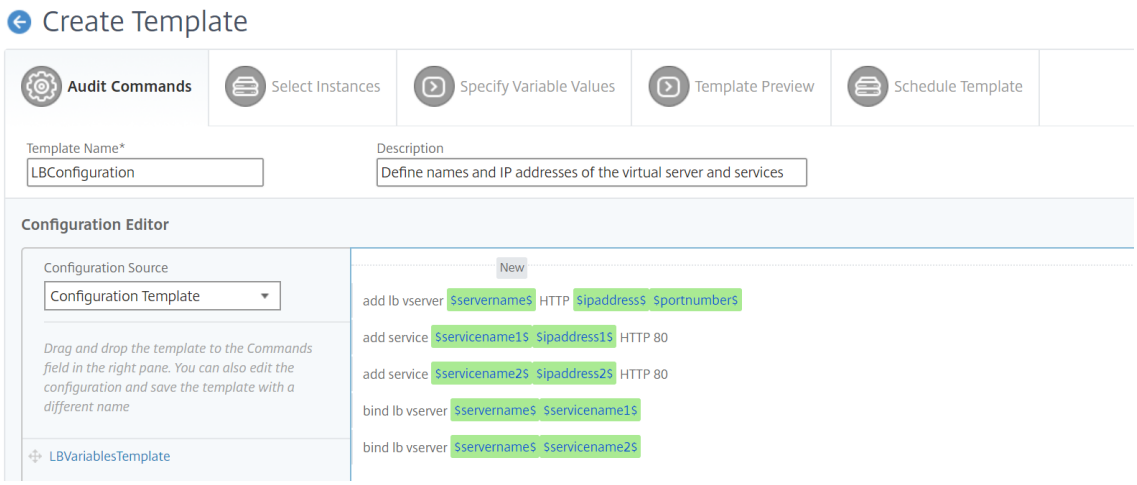
February 6, 2024

ネットワークのパフォーマンスを最適化するため、特定の構成を特定のインスタンス上で実行する場合があります。また、管理対象の Citrix Application Delivery Controller（ADC）インスタンス間の構成変更の監視、構成エラーのトラブルシューティング、および突然のシステムシャットダウン後に未保存の構成の回復も行う必要があります。特定のインスタンス上で実行する特定の構成の監査テンプレートを作成できます。NetScaler Application Delivery Management（NetScaler ADM）は、これらのインスタンスを監査テンプレートと比較し、構成に不一致があるかどうかを報告します。これにより、エラーのトラブルシューティングと修正が可能になります。

テンプレートを実行する時間をスケジュールすることで、監査テンプレートの実行を自動化できます。Citrix ADM がテンプレートを実行する頻度を設定することもできます。テンプレートは、毎日、週の特定の日、または月の特定の日に実行できます。Citrix ADM によって生成された差分レポートを、構成可能な指定された電子メールアドレスに送信することもできます。このオプションを選択すると、ユーザーはレポートをメール添付ファイルとして受信します。ユーザーが NetScaler ADM にログオンしてレポートを手動で確認する必要はありません。

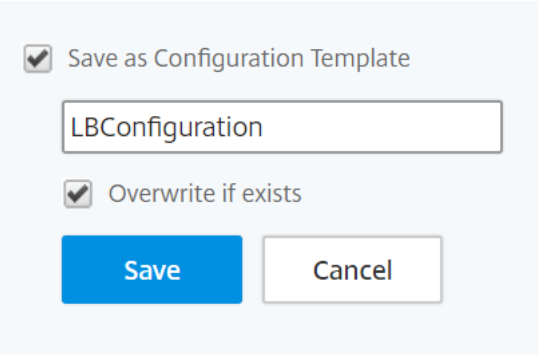
監査テンプレートを作成するには、次の手順に従います。

1. [ネットワーク] > [構成監査] > [監査 テンプレート] に移動し 、[追加] をクリック します。
2. [テンプレートの作成] ページおよび [監査コマンド] タブで、テンプレート名とその説明を指定します。
3. 構成エディタでコマンドを入力し、構成テンプレートとしてコマンドを保存します。エディターの左側のペインから既存のテンプレートをドラッグアンドドロップ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 「ipaddress」の IP アドレスを選択し、下図のように [変数 に変換] をクリック します。

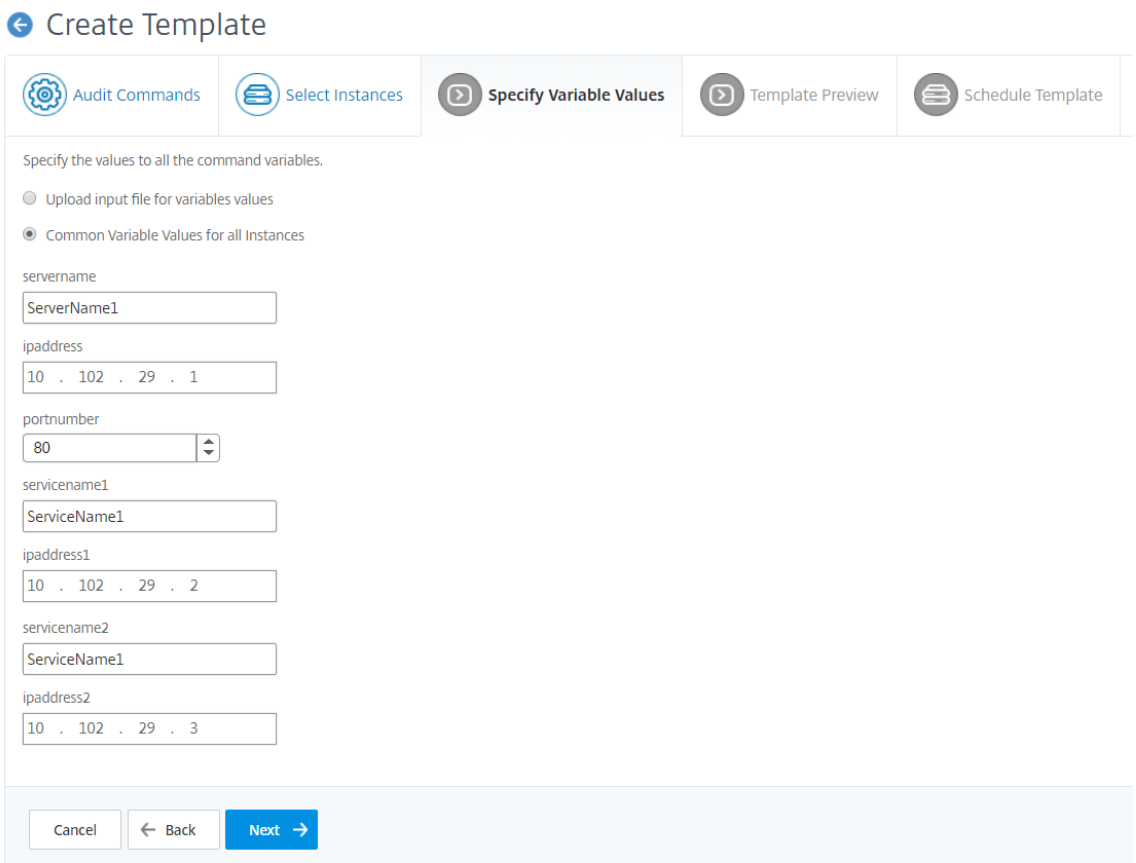


   変数のデフォルト値をさらに指定する場合は、「詳細」(**Advanced**) オプションをクリックします。

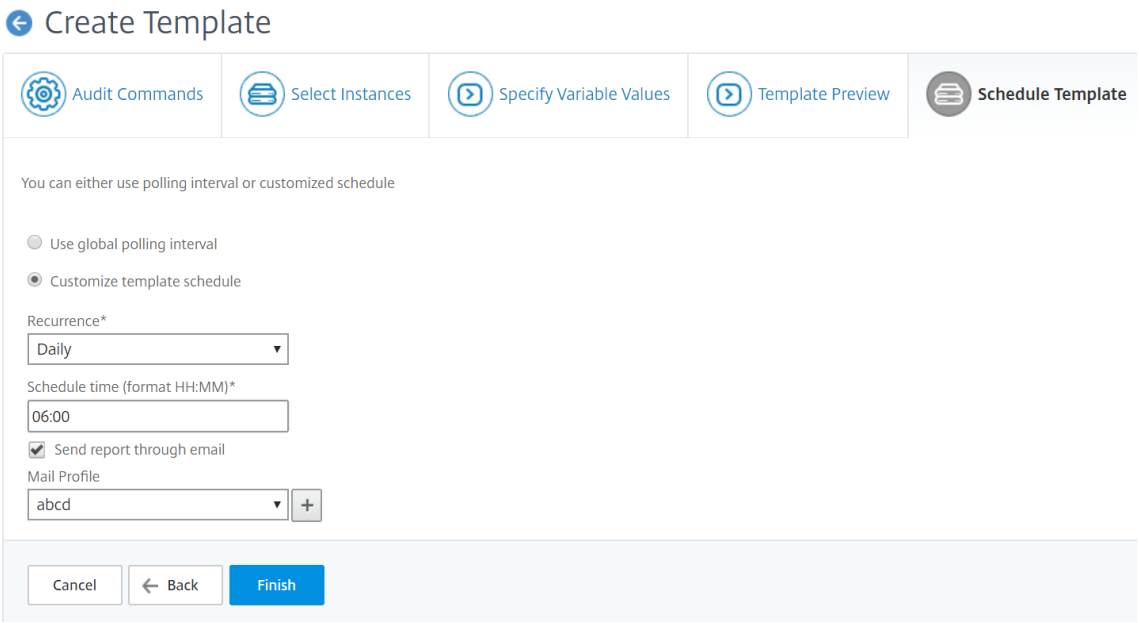
   コマンドを構成テンプレートとして保存することもできます。



5. [保存] をクリックし、[次へ] をクリックします。
6. [**Select Instanc** es] タブで、設定監査を実行するインスタンスを選択します。
7. [変数値の指定] タブには、次の 2 つのオプションがあります。
   a) 入力ファイルをダウンロードして、コマンドで定義した変数の値を入力し、NetScaler ADM サーバーにファイルをアップロードします。
   b) すべてのインスタンスに定義した変数に共通の値を入力します。
8. ［次へ］をクリックします。



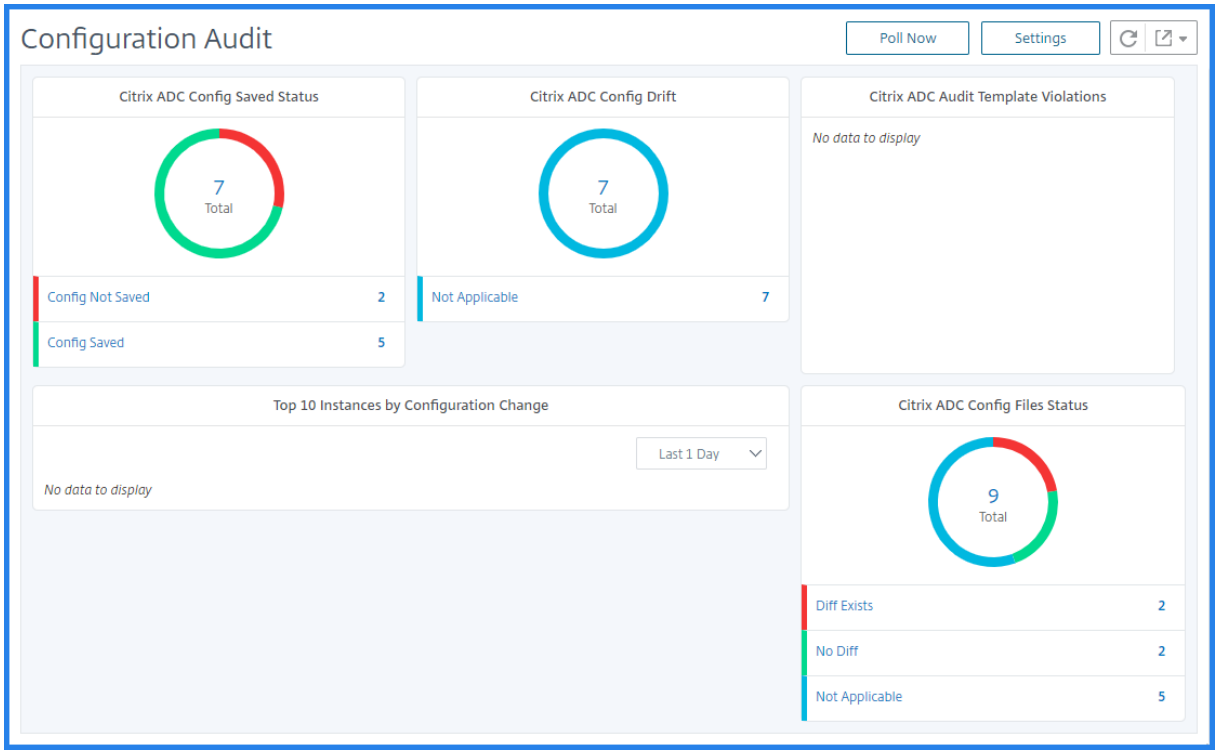
9. [**Template Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。［次へ］をクリックします。
10. スケジュールテンプレートタブには、テンプレートの実行を自動化する 3 つのオプションと、差分レポートを送信するメールアドレスがあります。
    - グローバルポーリング間隔を使用します。このオプションを選択すると、NetScaler ADM でグローバルに設定されたインスタンス上でテンプレートを一度に実行します。
    - テンプレート集計表をカスタマイズします。このオプションを使用して、テンプレートを実行する必要がある時間と頻度を設定します。
    - レポートを電子メールで送信。このオプションを使用して、差分レポートをメールの添付ファイルとして送信するメールプロファイルを設定します。
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。

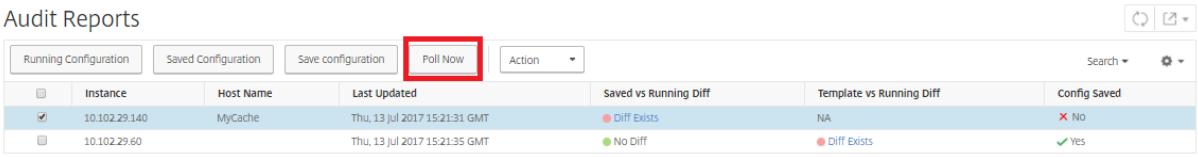
設定変更の詳細の表示

また、［Configuration Audit］ダッシュボードを使用して、構成変更回数の多い上位 10 インスタンス、保存された構成の数と保存されていない構成の数など、構成変更に関する詳細情報を表示できます。



また、NetScaler ADM では、構成監査を手動でポーリングし、インスタンスのすべての構成監査を直ちに NetScaler ADM に追加します。そのためには、[ネットワーク] > [構成監査] に移動し、[今すぐ投票] をクリックします。ポップアップページの [今すぐ投票] に、ネットワーク内のすべての Citrix ADC インスタンスをポーリングするか、選択したインスタンスをポーリングするかを選択できます。

特定のインスタンスに対して監査を強制することもできます。それには、[**NetScaler Config Saved Status**] 表、または [**NetScaler Config Drift**] 表をクリックします。「監査レポート」ページでインスタンスを選択し、「アクション」リストで「Poll Now」を選択します。



構成監査通知を設定するには:

1. [ネットワーク] > [構成監査] に移動します。
2. [構成の監査] ページで、[設定] をクリックします。
3. [**Notification Settings**] ページで、[**Edit**] アイコンをクリックして、通知設定を有効にします。
4. [**Enabled**] チェックボックスをオンにして、ボックスの一覧からメール配布リストを選択します。[**+**] アイコンをクリックしてメールサーバーの詳細を指定することによって、メール配布リストを作成することもできます。

ネットワーク構成に関する設定アドバイスを取得

February 6, 2024

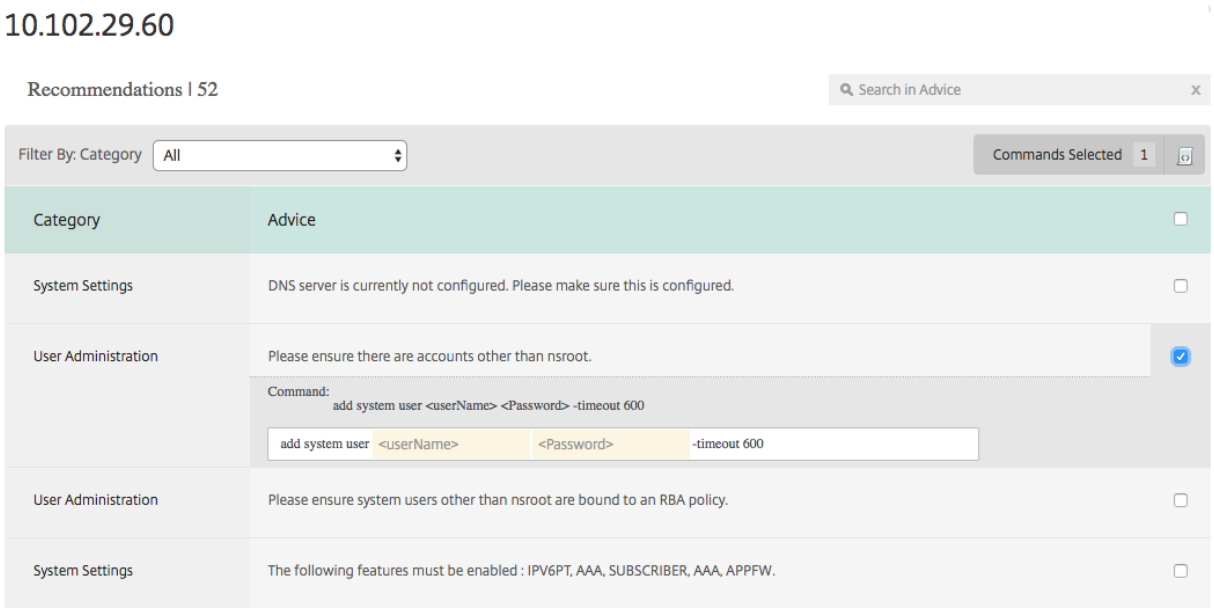
アプリケーションのパフォーマンスを最適化できるように、Citrix Application Delivery Controller（ADC）インスタンスを最適な構成でセットアップします。ただし、標準的ではない構成が含まれる場合、アプリケーションのパフォーマンスが低下することがあります。

アプリケーションのパフォーマンスを最適化するために、NetScaler Application Delivery Management（NetScaler ADM）は NetScaler ADC インスタンス構成を分析し、推奨事項を提供します。NetScaler ADM から推奨される構成を適用できます。

NetScaler ADC インスタンスを分析するには：

1. [ネットワーク] > [構成監査] **> [** 構成アドバイス] に移動します。
2. 次のいずれかを行います：
   - ［**Upload Configuration File**］をクリックし、ネットワークインスタンスの構成ファイルをアップロードします。
   - ［デバイスの選択］をクリックし、分析する NetScaler ADC インスタンスを選択します。

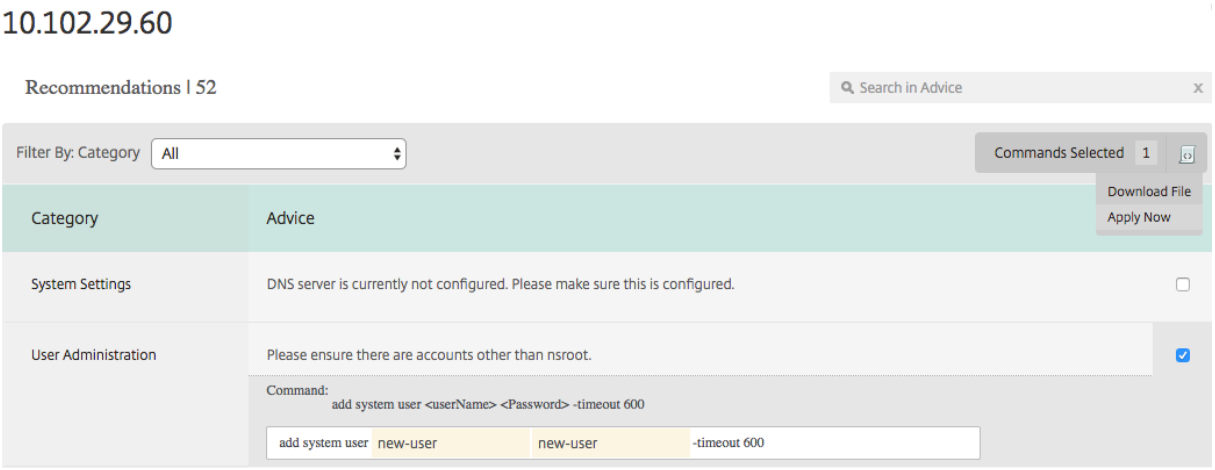
Citrix ADM はインスタンスの構成を分析し、以下の画像に示すように構成に関する推奨事項のリストを提供します。構成のアドバイスの隣にあるチェックボックスをオンにすると、修正コマンドが表示されます。



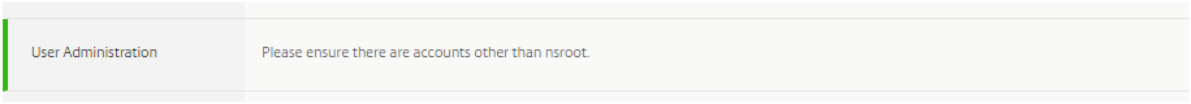
構成を更新する場合は、次の図に示すように、修正コマンドの変数に値を指定して、［**Apply Now**］をクリックします。

> 注:
>
> ここに記載されているコマンドは、推奨事項に過ぎません。読み取りおよび書き込みアクセス権を持つユーザーは、この機能を使用して任意のコマンドを編集できる場合があります。コマンドを編集してはいけないと思われるユーザーには、制限付きの特権アクセスを許可してください。

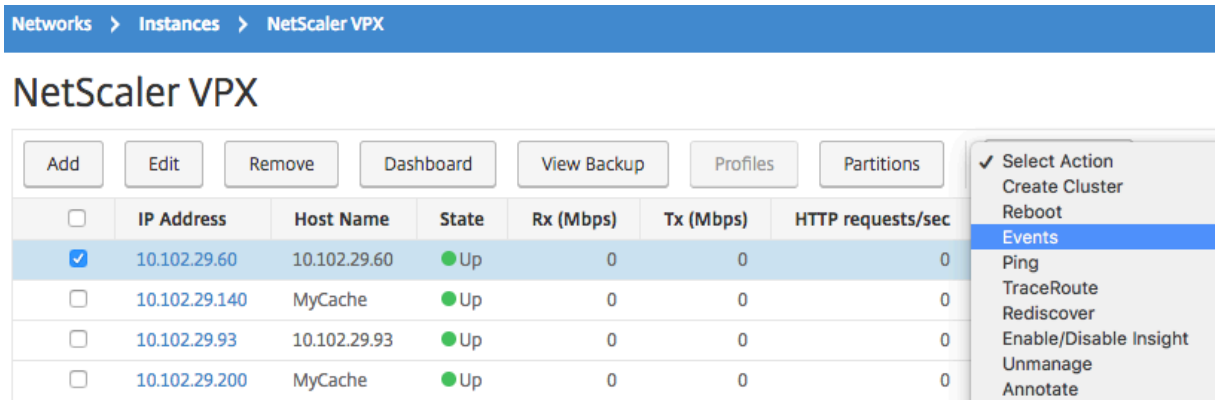
10.102.29.60



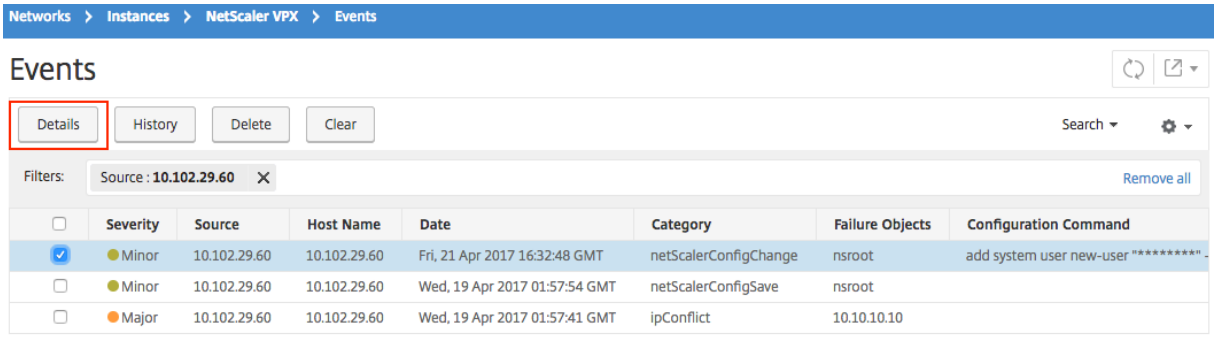
ネットワークインスタンスでコマンドが正常に実行されると、アドバイスの隣にあるチェックボックスが消えます。



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、[ネットワーク] > **[**インスタンス] に移動し**、**<Instance_Type>** 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] をクリックします。



[**Events**] ページでは、構成変更の詳細を表示できます。



NetScaler ADC インスタンスの構成監査をポーリングする

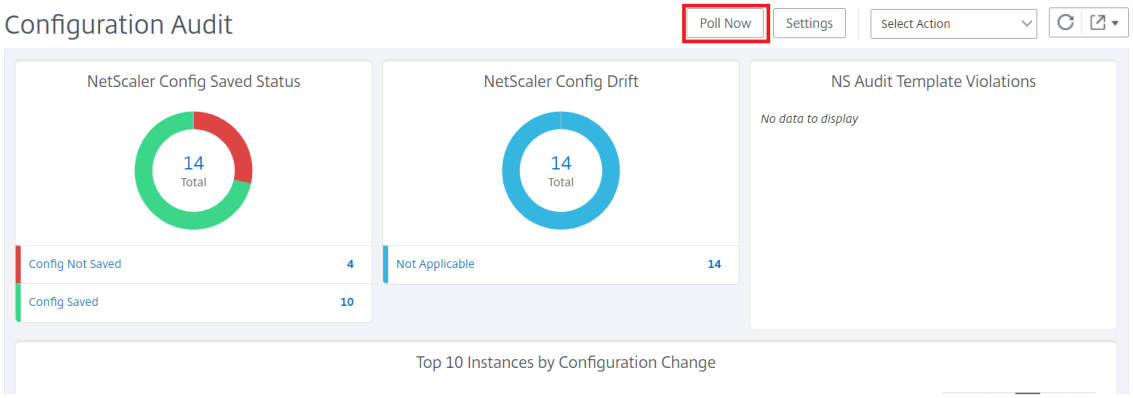
February 6, 2024

Citrix Application Delivery Management（Citrix ADM）は、Citrix アプリケーション Delivery Controller（ADC）インスタンスで発生した構成変更を確認するために、10 時間ごとに構成監査を自動的にポーリングします。構成監査を手動でポーリングして最近の変更を検出することもできますが、すべての NetScaler ADC インスタンスの構成をポーリングすると、ネットワークに大きな負荷がかかります。

NetScaler ADC インスタンスの構成監査全体をポーリングする代わりに、選択した 1 つまたは複数のインスタンスの構成監査のみを手動でポーリングできます。

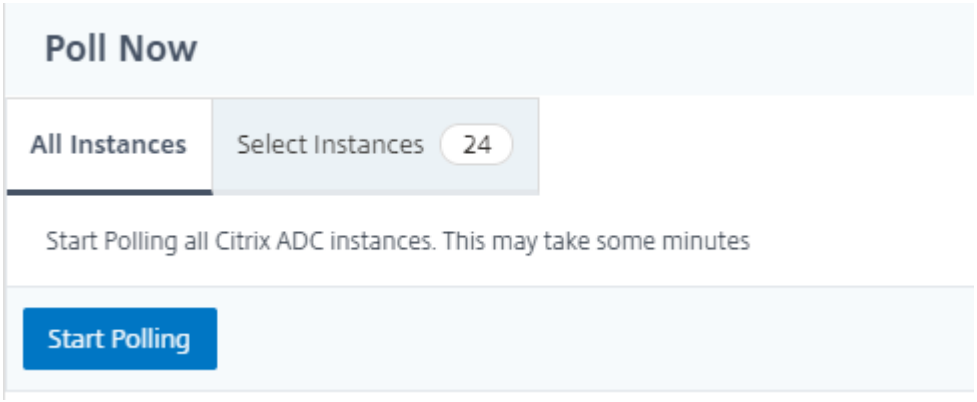
NetScaler ADC インスタンスの構成監査をポーリングするには：

1. NetScaler ADM で、［ネットワーク］>［構成監査］に移動します。
2. [構成の監査] ページの右上隅にある [今すぐポーリングする] をクリックします。

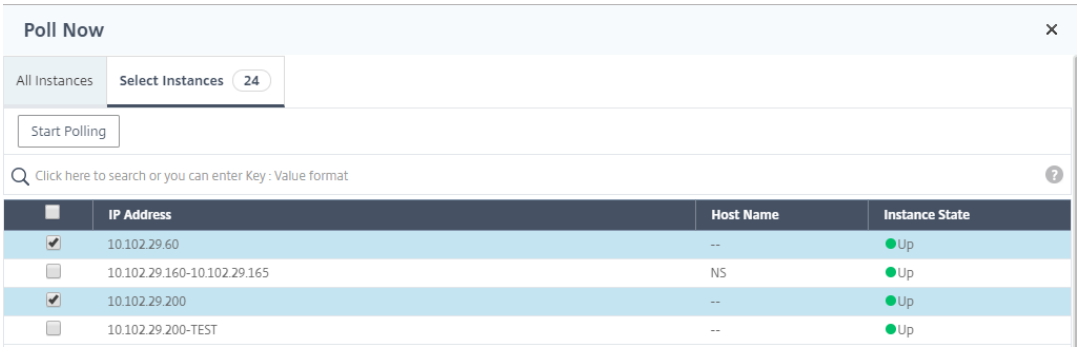


3. ［**Poll Now** ］ページが表示され、ネットワーク内のすべての NetScaler ADC インスタンスをポーリングするか、選択したインスタンスをポーリングするかを選択できます。

   a) すべての NetScaler ADC インスタンスをポーリングするには、［すべてのインスタンス］タブを選択し、［ポーリング開始］をクリックします。



b) 特定のインスタンスをポーリングするには、**[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 Citrix Application Delivery Controller (ADC) インスタンスの構成が変更されるたびに、構成ファイルが更新されます。インスタンスは ConfigChange SNMP トラップを Application Delivery Management (Citrix ADM) に送信します。インスタンスが ConfigChange SNMP トラップを送信するときに、そのインスタンスに対して NetScaler ADM で構成監査を実行するように設定できます。

監査テンプレート設定と構成実行の間に相違がある場合は、「監査レポート」(Audit Report) ページに「差分」(Diff Exist s) ステータスメッセージが表示されます。「相違の出口」リンクをクリックすると、「構成の差分」ページが表示され、修正コマンドを表示できます。これらの修正コマンドを使用して構成ジョブを作成し、それを特定の Citrix ADC インスタンスで実行できます。設定ジョブを実行すると、インスタンスは目的の設定に戻ります。修正コマンドから構成ジョブを作成する方法の詳細については、「NetScaler ADM で修正コマンドから構成ジョブを作成する方法」を参照してください。

ConfigChange SNMP トラップの受信時に構成監査テンプレートを実行するには、次の手順に従います。

NetScaler ADM では、NetScaler ADM で構成監査テンプレートを実行するオプションを有効にできます。

1. NetScaler ADM で、［ネットワーク］>［構成監査］に移動します。
2.「構成監査」ページの「設定」をクリック します。
3.「構成変更の監査設定」セクションの編集アイコンをクリックします。
4.「**NetScalerConfigChange** イベントの受信時に構成監査を行う」チェックボックスを選択します。

> 注**:**
>
> これはすべてのインスタンスのグローバル設定です。NetScaler ADM は、将来 NetScalerConfigChange SNMP トラップを受信するすべてのインスタンスに対して構成監査を実行します。

1.「監査テンプレートを実行するための遅延時間 (分単位)」フィールドに、分数を入力します。NetScaler ADM は、そのインスタンスによって ConfigChange SNMP トラップを受信すると、この時間が経過すると、NetScaler ADC インスタンス上で構成監査テンプレートを実行します。

ネットワーク機能

February 6, 2024

ネットワーク機能機能を使用すると、管理対象の Citrix Application Delivery Controller（ADC）インスタンスで構成されたエンティティの状態を監視できます。負荷分散仮想サーバーのトランザクション詳細、接続詳細、スループットなどの統計を表示できます。また、メンテナンスの計画時にはエンティティを有効または無効にすることもできます。

ネットワーク機能ダッシュボードには、次のグラフが表示されます。

- クライアント接続が多い上位 5 つの仮想サーバー
- サーバー接続が多い上位 5 つの仮想サーバー
- スループット（MB/秒）が高い上位 5 つの仮想サーバー
- スループット（MB/秒）が低い下位 5 つの仮想サーバー
- 仮想サーバーが多い上位 5 つのインスタンス
- 仮想サーバーの状態
- 負荷分散仮想サーバーの正常性
- プロトコル

負荷分散エンティティのレポートを生成する

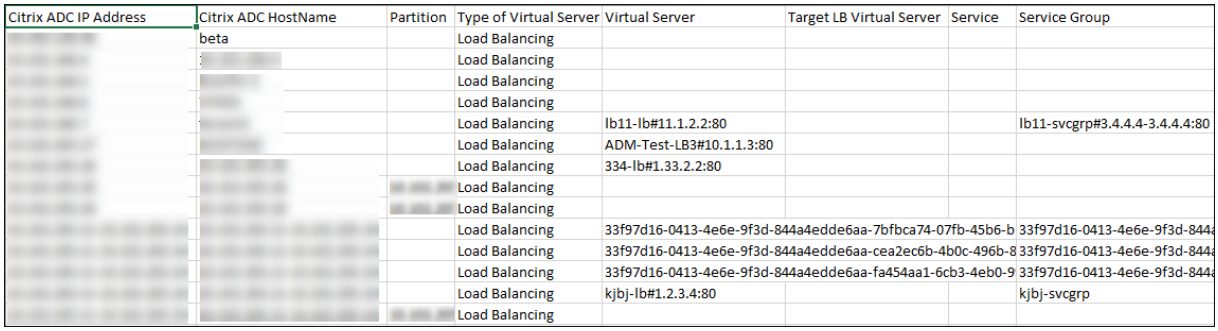
February 6, 2024

Citrix Application Delivery Management（ADM）では、Citrix アプリケーション Delivery Controller（ADC）インスタンスエンティティのレポートをすべてのレベルで表示できます。NetScaler ADM ／ネットワーク機能でダウンロードできるレポートには、統合レポートと個別レポートの 2 種類があります。

統合レポート：NetScaler ADC インスタンスで管理されているすべてのエンティティの統合レポートまたは要約レポートをダウンロードして表示できます。

このレポートでは、NetScaler ADC インスタンス、パーティション、およびネットワークに存在する対応する負荷分散エンティティ（仮想サーバー、サービスグループ、サービス）間のマッピングを大まかに確認できます。

次の画像は、概要レポートの例を示しています。



Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	beta		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#3.4.4.4-3.4.4.4:80
[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-b			33f97d16-0413-4e6e-9f3d-844
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8			33f97d16-0413-4e6e-9f3d-844
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-9			33f97d16-0413-4e6e-9f3d-844
[redacted]	[redacted]		Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
[redacted]	[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:Citrix ADC インスタンスの IP アドレスがレポートに表示されます
- **NetScaler** ホスト名：ホスト名がレポートに表示されます。
- パーティション: 管理パーティションの IP アドレスが表示されます。
- 仮想サーバー:<name_of_the_virtual_server>#virtual_IP_address: port_number
- サービス:<name_of_the_service>#service-IP_Address: Port_Number
- サービスグループ:<name_of_service_group>#Server_Member1_IP_Address: Port、server_Member2_IP_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 ADC インスタンスに対して構成されていないことを示します。

個別レポート: すべてのインスタンスとエンティティの独立したレポートをダウンロードして表示することもできます。たとえば、負荷分散仮想サーバー、負荷分散サービス、負荷分散サービスグループのいずれかのみ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、［ネットワーク］>［ネットワーク機能］>［負荷分散］に移動します。
2. 負荷分散ページで、  。
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。

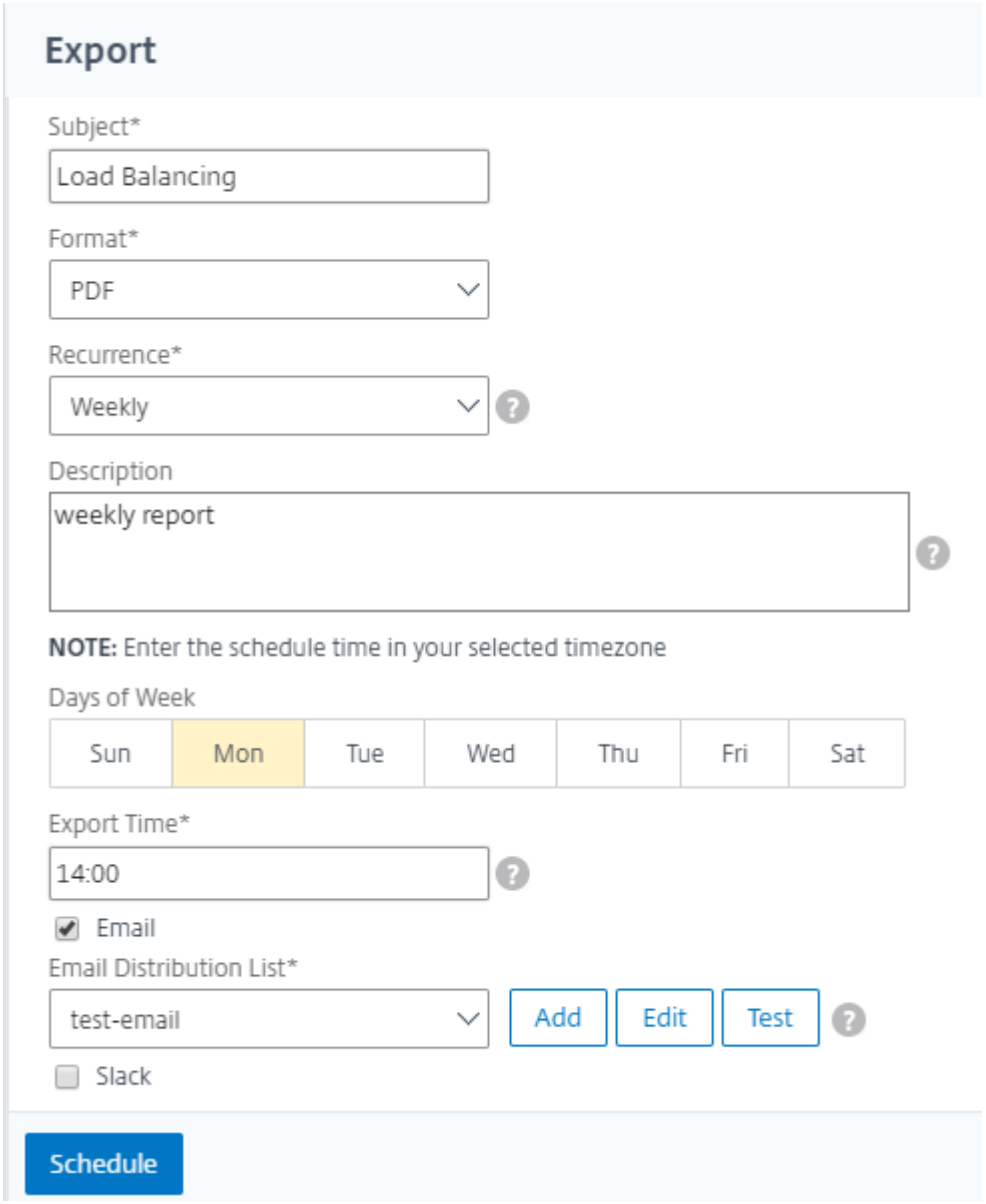
   b) レポートの生成とエクスポートを定期的にスケジュールするには、「レポートのスケジュール」タブを選択します。レポート生成の繰り返し設定を指定し、レポートのエクスポート先のメールプロファイルを作成します。

      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。

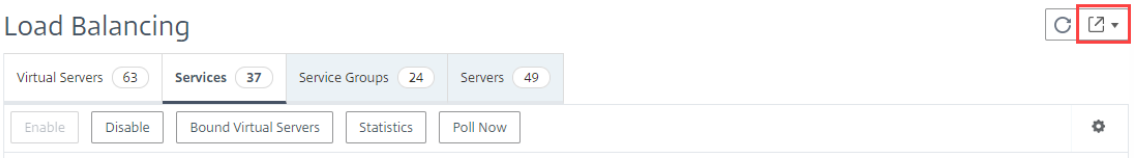


> 注
>
> [毎月の繰り返し] を選択した場合は、レポートをスケジュールするすべての日をカンマで区切って入力します。

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. Citrix ADM で、［ネットワーク］>［ネットワーク機能］>［負荷分散］**>**［サービス］に移動します。
2. [サービス] ページで、右上隅にある [エクスポート] ボタンをクリックします。



a) この瞬間にレポートを生成して表示する場合は、[**Export Now**] タブを選択します。

b) レポートの生成とエクスポートを定期的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

Citrix Application Delivery Management（ADM）では、負荷分散、コンテンツスイッチング、キャッシュリダイレクト、グローバルサーバー負荷分散（GSLB）、認証、NetScaler Gateway などの特定のネットワーク機能に関する包括的なレポートを生成できます。このレポートを使用すると、ネットワークに存在する Citrix ADC インスタンス、パーティション、および対応するバインドされたエンティティ（仮想サーバー、サービスグループ、サービス）間のマッピングの概要を把握できます。これらのレポートは、.csv ファイル形式でエクスポートできます。

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

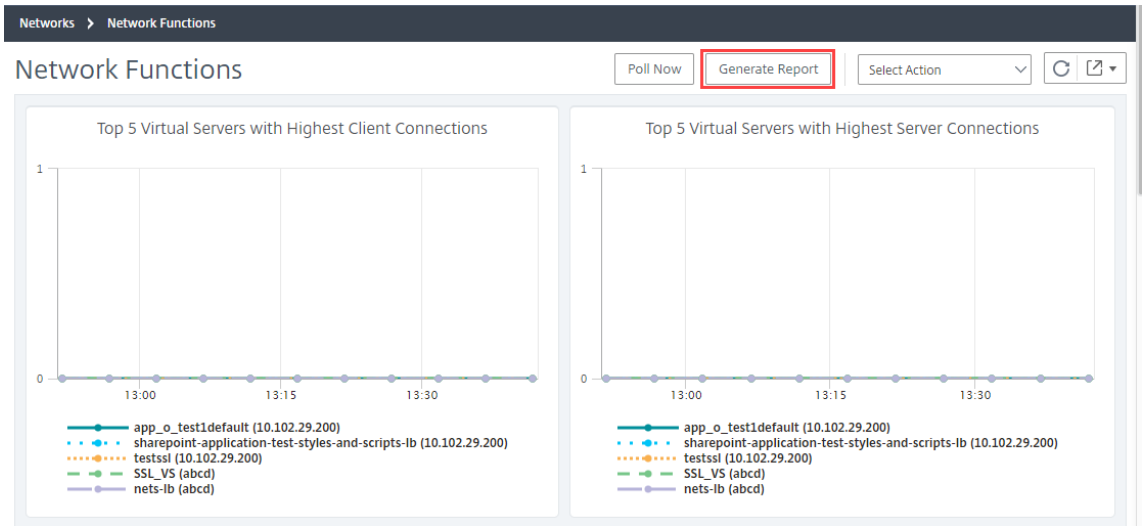
これらのレポートを指定のメールアドレスに異なる間隔でエクスポートするようにスケジュールできます。

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。

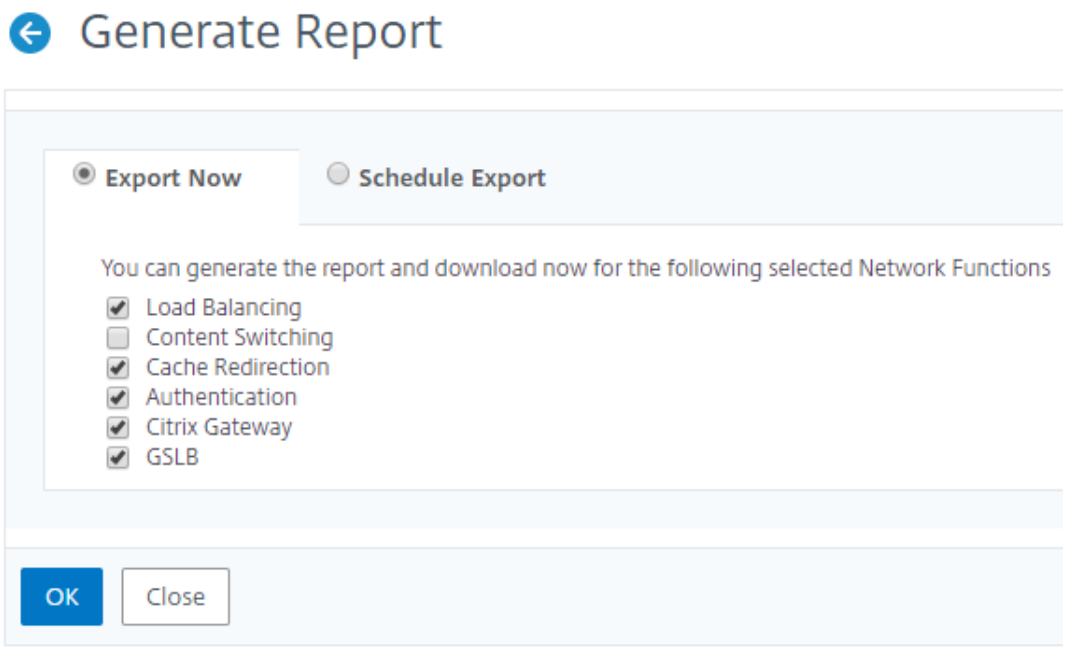
ネットワーク機能レポートをエクスポートおよびスケジュールする手順は、次のとおりです。

1. [ネットワーク] > [ネットワーク機能] に移動します。
2. [ネットワーク機能] ページの右ペインで、ページの右上隅にある [レポートの生成] をクリックします。



3. [レポートの生成] ページには、次の 2 つのオプションがあります:

   a)「今すぐエクスポート」タブを選択し、「**OK**」をクリックします。レポートがシステムにダウンロードされます。



次の図は、ネットワーク機能レポートの例を示しています。

NetScaler ADC IP Address	NetScaler ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
10.	10.		Load Balancing	lb_test_1#10.10.10.10:80		adm_metric_collector_svc_10.106.171.41#10.106	
10.	10.		Load Balancing	lbvs_511#51.1.1.1:80		test_1#10.102.61.105:80	
10.	10.		Load Balancing	lbvs_521#52.1.1.1:80		test_1#10.102.61.105:80	
10.	10.		Load Balancing	SG_HS_DNS_MON#1.2.22.2:80			sc1
10.	10.		Load Balancing	SG_HS_DNS_MONgdvfffs#1.3.4.5:80			
10.	10.		Load Balancing	atest94#1.1.1.11:80			
10.	10.		Load Balancing	lbvs1_101#1.10.1.1:80			
10.	10.		Load Balancing	lbvs1_1010#1.10.1.10:80			
10.	10.		Load Balancing	lbvs1_10100#1.10.1.100:80			
10.	10.		Load Balancing	lbvs1_10101#1.10.1.101:80			
10.	10.		Load Balancing	lbvs1_10102#1.10.1.102:80			
10.	10.		Load Balancing	lbvs1_10103#1.10.1.103:80			

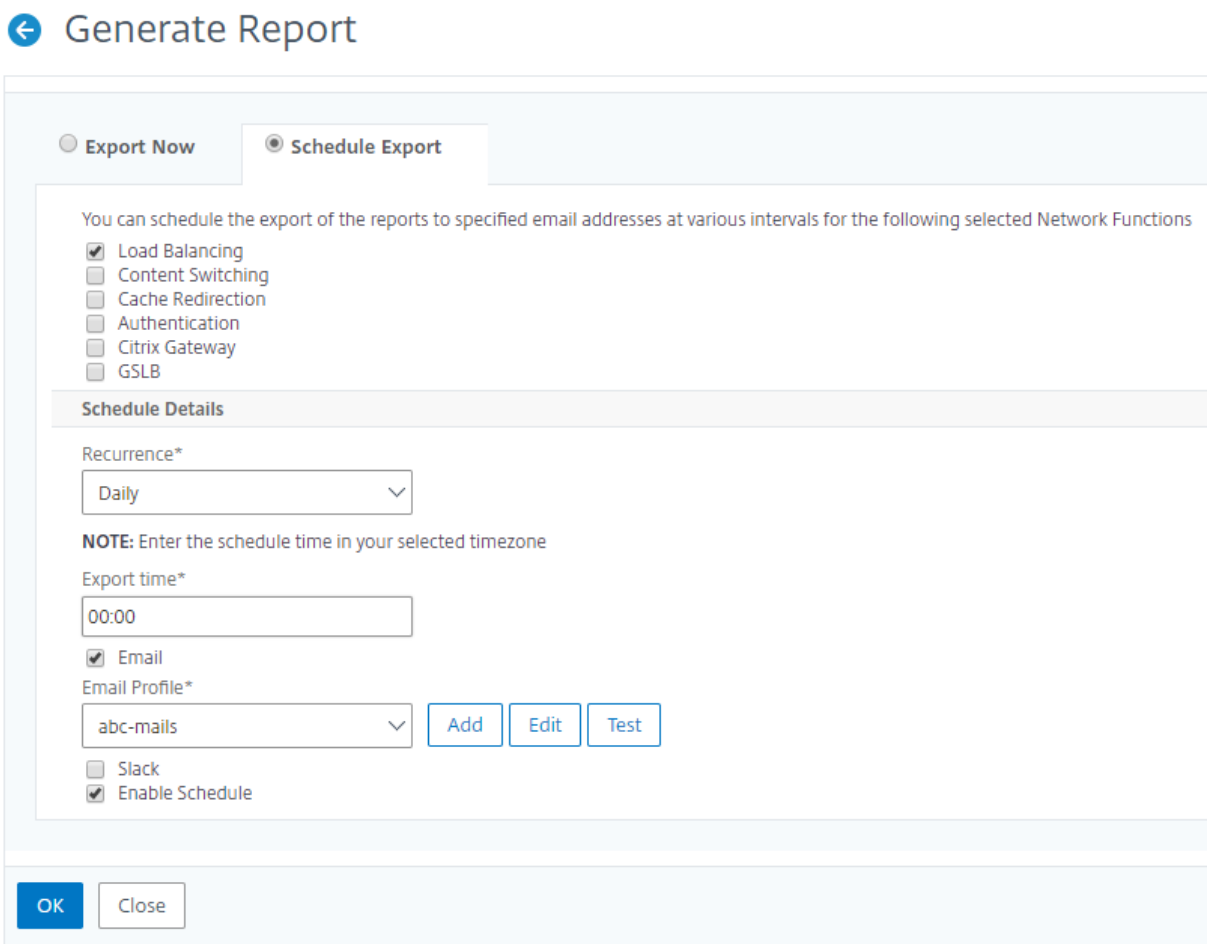
b) レポートの生成とエクスポートを定期的にスケジュールするには、[レポートのスケジュール] タブを選択します。レポート生成の繰り返し設定を指定し、レポートのエクスポート先のメールプロファイルを作成します。

   i. 繰り返し-ドロップダウンリストボックスから [毎日]、[毎週]、または [毎月] を選択します。

   ii. 繰り返し時間-時間を 24 時間形式で時間: 分として入力します。

   iii. メールプロファイル-ドロップダウンリストボックスからプロファイルを選択するか、**+** をクリックしてメールプロファイルを作成します。

[スケジュールを有効にする] をクリックしてレポートをスケジュールし、[**OK**] をクリックします。「スケジュールを有効にする」チェックボックスをクリックすると、選択したレポートを生成できます。



ネットワークレポート作成

February 6, 2024

Citrix Application Delivery Management（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（ADC）インスタンスをデプロイして、トラフィックの負荷分散、コンテンツの切り替え、または圧縮も行っています。ネットワークのパフォーマンスは、アプリケーションのパフォーマンスに影響を与える可能性があります。アプリケーションのパフォーマンスを維持し続けるには、ネットワークパフォーマンスを定期的に監視し、すべてのリソースが最適に使用されていることを確認する必要があります。

NetScaler ADM では、グローバルレベルのインスタンスだけでなく、仮想サーバーやネットワークインターフェイスなどのエンティティのレポートを生成できるようになりました。インスタンスファミリーは、NetScaler ADC インスタンスと SD-WAN インスタンスの両方で構成されます。レポートを生成できる仮想サーバーは次のとおりです。

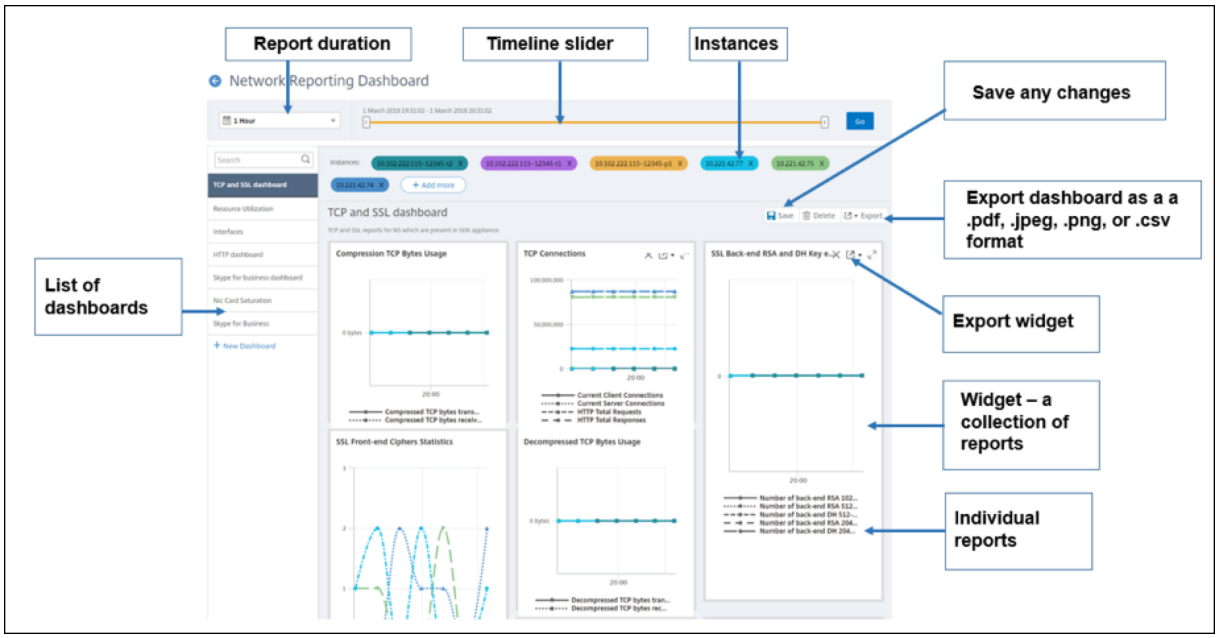
- 負荷分散サーバー

- コンテンツ・スイッチ・サーバ
- キャッシュリダイレクト
- 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。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。

各ダッシュボードを複数のウィジェットでカスタマイズして、さまざまなレポートを表示できます。ウィジェットは、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時刻と繰り返しをスケジュールすることもできます。レポートの送信先となる電子メール配布リストを設定することもできます。

ダッシュボードの上部にある [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。

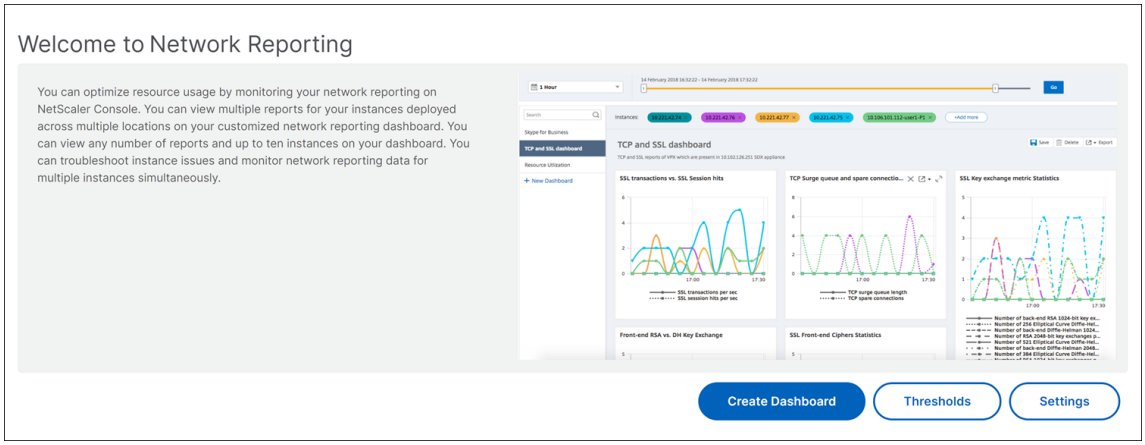
をクリックしてインスタンスを削除するか、レポートにインスタンスを追加できます。ただし、現在、Citrix ADM では 10 個のインスタンスのレポートを表示できます。

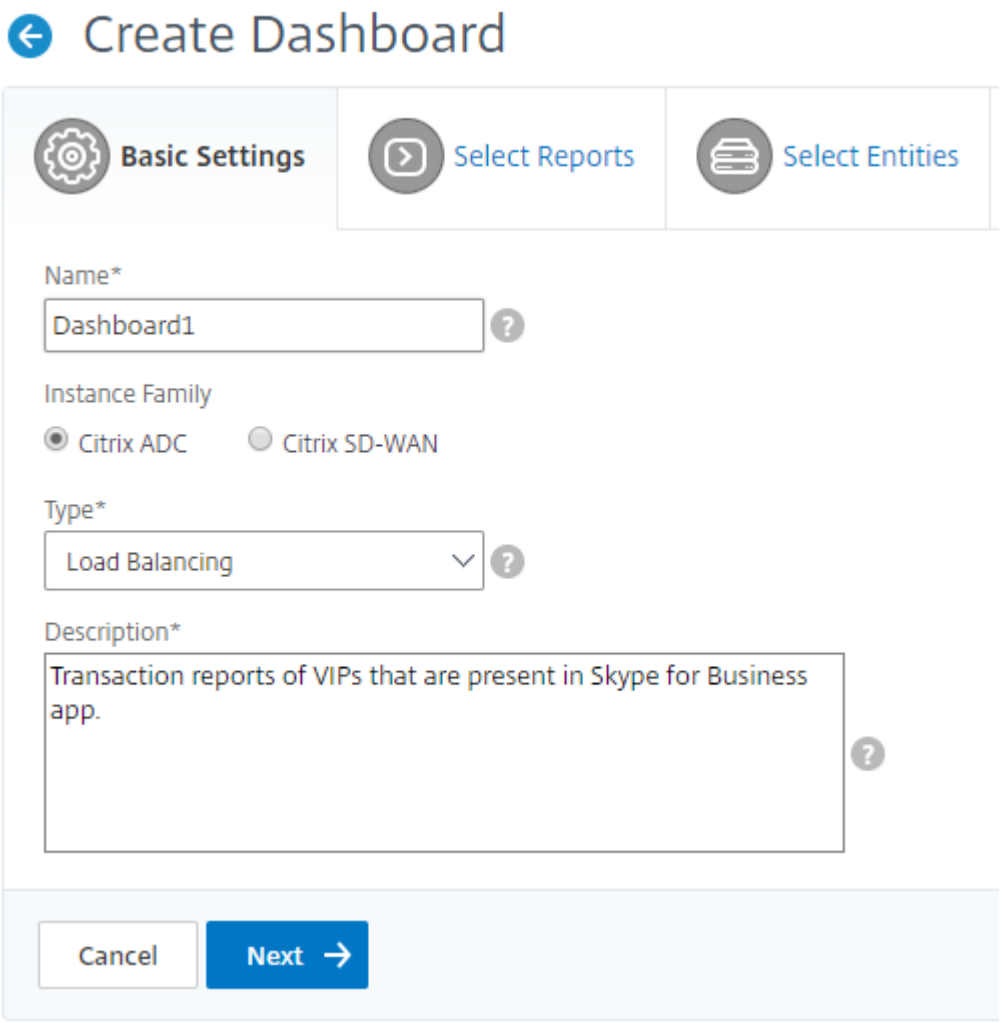
ダッシュボード全体を.pdf、.jpeg、.png、.csv 形式でシステムにエクスポートすることもできます。ダッシュボードに加えられた変更はすべて保存する必要があります。［保存］をクリックして変更を保存します。

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には

1. NetScaler ADM で、［ネットワーク］>［ネットワークレポート］に移動します。

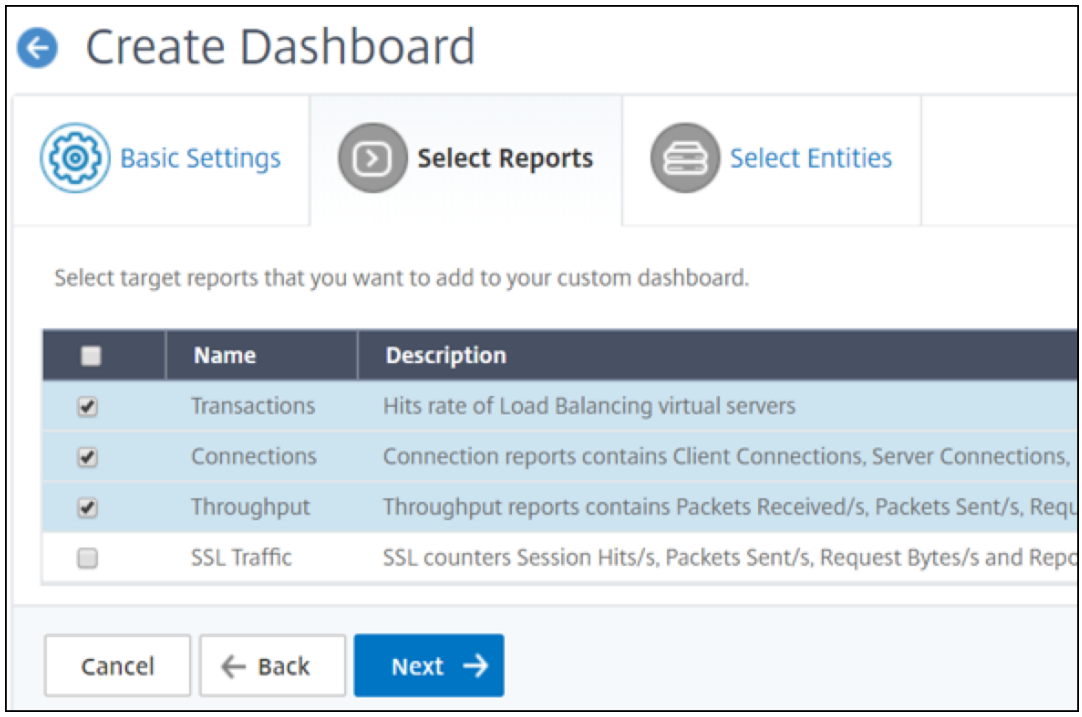




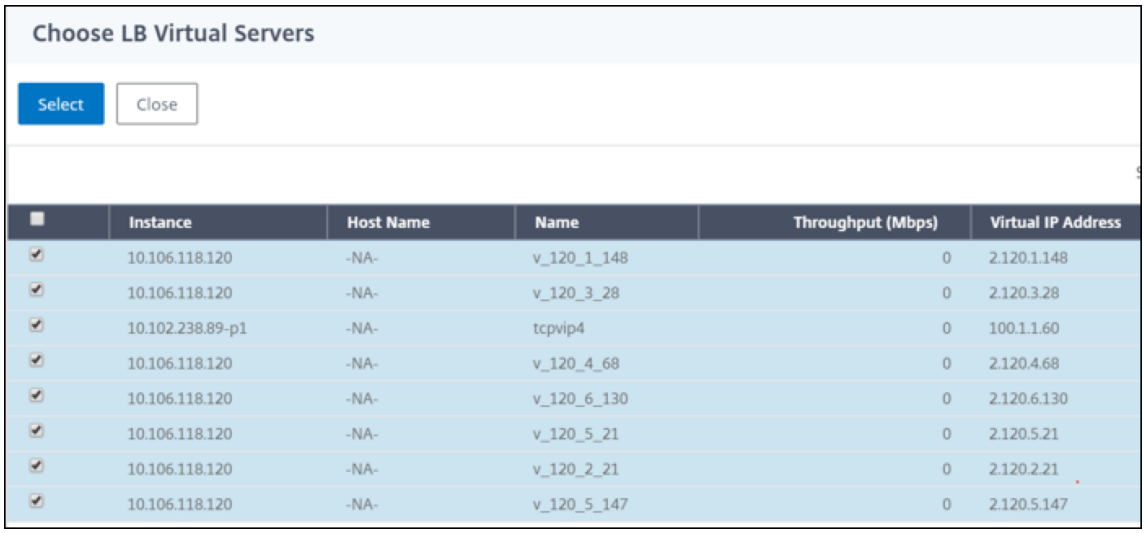
2. **[** レポートの選択] タブで、必要なレポートを選択します。この例では、トランザクション、接続、スループットを選択できます。［次へ］をクリックします。
3. 既存のダッシュボードを表示するには、[ダッシュボードの表示] をクリックします。[ネットワークレポートダッシュボード] ページが開き、すべてのダッシュボードとレポートウィジェットを表示できます。
4. ダッシュボードを作成するには、[ダッシュボードの作成] をクリックします。
5. **[**ダッシュボードの作成] ページが開きます。
6. 「基本設定」タブで、次の詳細を入力します。
    a) 名前。ダッシュボードの名前を入力します。
    b) インスタンスファミリー。インスタンスのタイプ (Citrix ADC または Citrix SD-WAN) を選択してください
    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。

e) ［次へ］をクリックします。



7. **[** エンティティの選択] タブで、[追加] をクリックします。
8. スライドして表示される [**LB** 仮想サーバーの選択] ウィンドウで、監視する仮想サーバーをいくつでも選択します。



> 注
>
> 「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」タブには対応するエンティティが表示されます。たとえば、グローバルを選択すると、インスタンスを追加できます。

9. ［作成］をクリックします。

TCP と **SSL** のダッシュボードが作成され、選択したすべてのレポートが表示されます。

> 注**:**
>
> 現在のところ、凡例またはフィルタに加えた変更は保存できません。

ネットワークレポートのエクスポート

ウィジェットレポートは.pdf、.png、.jpeg、または.csv 形式でエクスポートできますが、ダッシュボード全体は.pdf、.jpeg、または.png 形式でのみエクスポートできます。

> 注
>
> 読み取り専用権限を持っている場合、NetScaler ADM でレポートをエクスポートすることはできません。NetScaler ADM でファイルを作成したり、ファイルをエクスポートしたりするには、編集権限が必要です。

ダッシュボード・レポートをエクスポートするには、次の手順に従います。

1. [ネットワーク] > [ネットワークレポート] に移動します
2. [ダッシュボードの表示] をクリックして、作成したすべてのダッシュボードを表示します。
3. 左側のペインで、ダッシュボードをクリックします。この例では、「ダッシュボード **1**」をクリックします。
4. ページの右上隅にあるエクスポートボタンをクリックします。
5. [今すぐエクスポート] タブで、必要な形式を選択し、[エクスポート] をクリックします。

ネットワークレポートをスケジュールするときに、[Subject] 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間に作成されたレポートには、この文字列が名前として付けられます。

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。

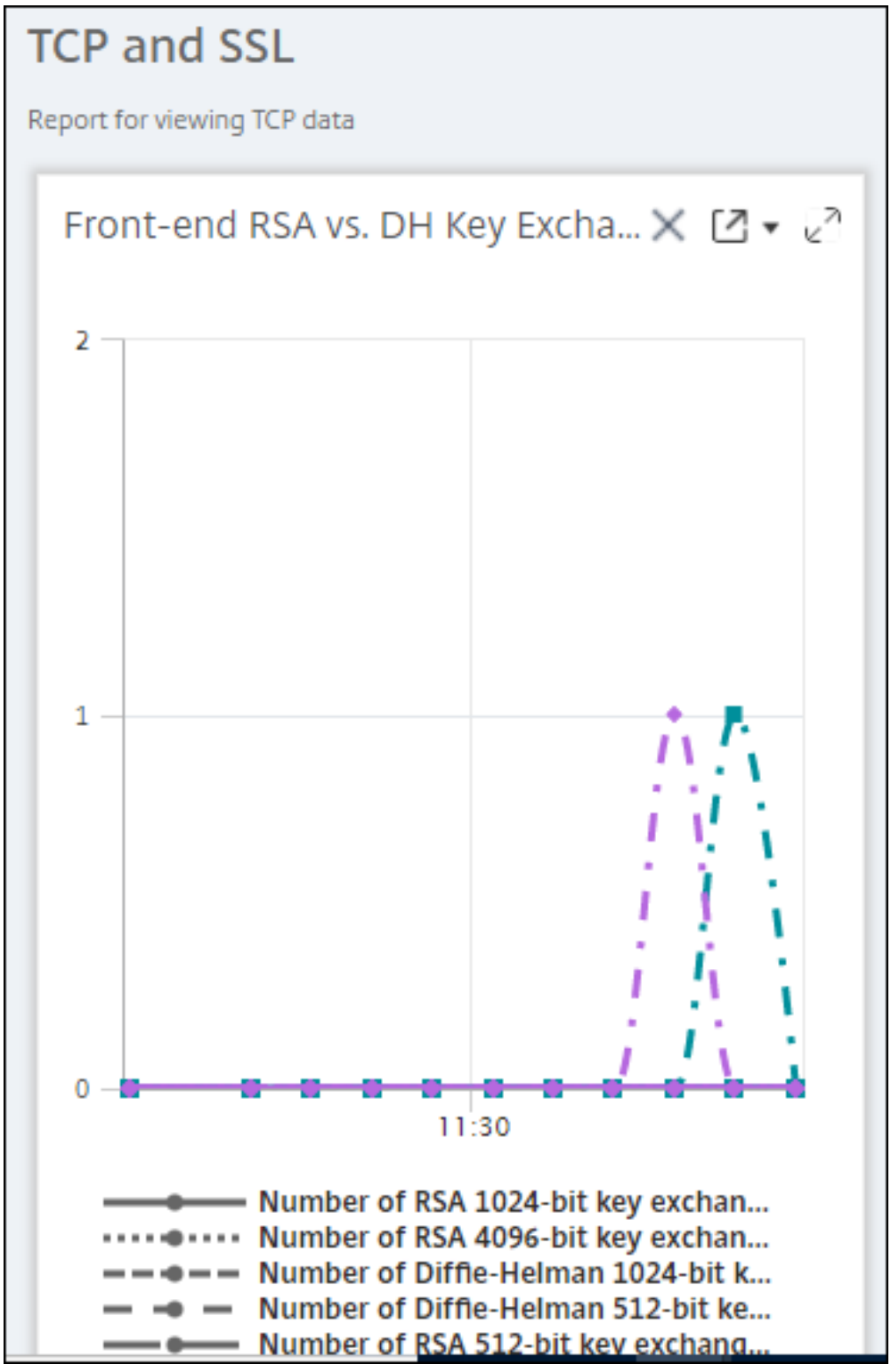
> 注**:**
>
> 現在、このオプションはレポートのエクスポートをスケジュールしている場合にのみ使用できます。即座にエクスポートするときに、レポートに見出しを追加することはできません。

ダッシュボード・レポートをエクスポートするには、次の手順に従います。

1. [ネットワーク] > [ネットワークレポート] に移動します
2. [ダッシュボードの表示] をクリックして、作成したすべてのダッシュボードを表示します。
3. 左側のペインで、ダッシュボードをクリックします。この例では、「ダッシュボード **1**」をクリックします。
4. ページの右上隅にあるエクスポートボタンをクリックします。
5. [今すぐエクスポート] タブで、必要な形式を選択し、[エクスポート] をクリックします。**

ウィジェット・レポートをエクスポートするには、次の手順に従います。

1. [ネットワーク] > [ネットワークレポート**]** に移動します。
2. [ダッシュボードの表示] をクリックして、作成したすべてのダッシュボードを表示します。
3. 左側のペインで、ダッシュボードをクリックします。この例では、[**TCP** と **SSL]** 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、「フロントエンド RSA vs.」を選択します。**DH** キー交換。
5. ページの右上隅にある [エクスポート] ボタンをクリックします。
6. [今すぐエクスポート] タブで、必要な形式を選択し、[エクスポート] をクリックします。



NetScaler ADM でネットワークレポートのしきい値を管理する方法

NetScaler ADC インスタンスの状態を監視するには、カウンタにしきい値を設定し、しきい値を超えたときに通知を受け取ることができます。NetScaler ADM では、しきい値を設定したり、表示、編集、削除したりできます。

たとえば、コンテンツスイッチング仮想サーバーの Connections カウンターが指定された値に達したときに電子メール通知を受け取ることができます。特定のインスタンスタイプのしきい値を定義できます。選択したインスタンスから特定のカウンタメトリックスに対して生成するレポートを選択することもできます。

カウンタの値が（ルールで指定されている）閾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指定された重要度のイベントが生成されます。カウンター値が正常と見なされる値に戻ると、イベントはクリアされます。これらのイベントは、[ネットワーク] > [イベント] > **[**** レポート**]** に移動すると表示できます。「レポート」ページで、「重要度別のイベント ** 」ドーナツをクリックすると、イベントを重要度別に表示できます。

また、しきい値を超えたときに電子メールや SMS メッセージを送信するなど、アクションをしきい値に関連付けることもできます。

しきい値を作成するには

1. Citrix ADM で、［ネットワーク］>［ネットワークレポート］>［しきい値］に移動します。［**Thresholds**］の［**Add**］をクリックします。

    1.「しきい値の作成」ページで、次の詳細を指定します。

        - しきい値名。しきい値の名前。
        - インスタンスタイプ。Citrix ADC または Citrix SD-WAN WO を選択してください。
        - レポート名。このしきい値に関する情報を提供するパフォーマンスレポートの名前。

    2. また、イベントを生成またはクリアするタイミングを指定するルールを設定することもできます。「ルールの設定」セクションでは、次の詳細を指定できます。

        - メトリック。しきい値を設定する指標を選択します。
        - コンパレータ。比較器を選択して、監視対象値が閾値以上か、それ以下かをチェックします。
        - しきい値。イベントの重要度を計算する基準となる値を入力します。たとえば、現在のクライアント接続の監視対象の値が 80%に達すると、重大なイベント重大度を持つイベントを生成することができます。この場合、しきい値として 80 を入力します。「重大度」イベントは、[ネットワーク] > [イベント] > **[**** レポート **] に移動すると表示できます。「レポート」ページで、「重要度別のイベント」ドーナツをクリックすると、イベントを重要度別に表示できます。
        - 明確な価値。値をクリアするタイミングを示す値を入力します。たとえば、監視対象の値が 50%に達すると、現在のクライアント接続のしきい値をクリアすることができます。この場合、クリア値として 50 を入力します。

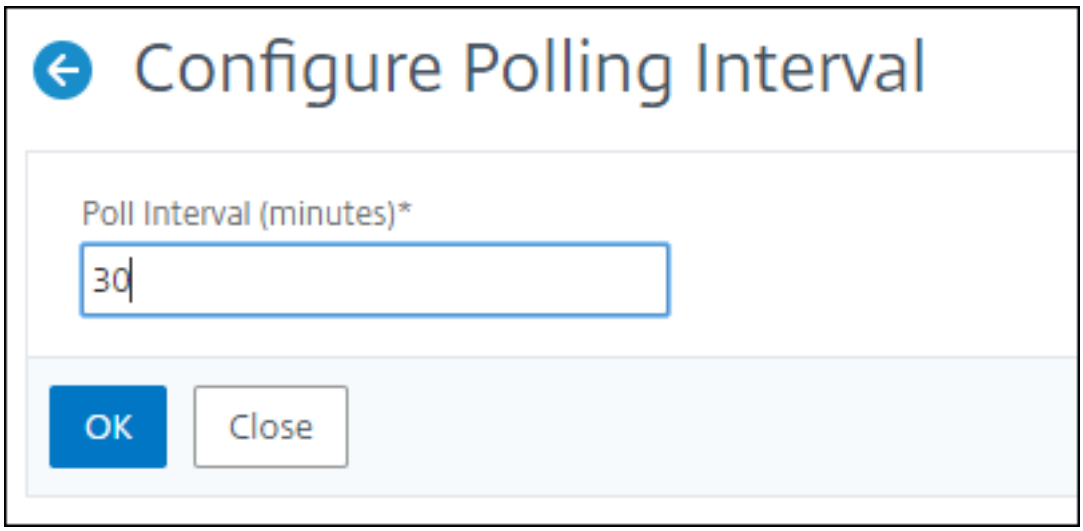
- イベントの重要度。閾値に設定するセキュリティレベルを選択します。

3. しきい値を設定するインスタンスの IP アドレスを選択します。
4. 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。
5. 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。
6. オプションで、メール通知や SMS 通知などのアクションを設定できます。
7. ［作成］をクリックします。

ネットワークレポートのパフォーマンスポーリング間隔の設定

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。これにより、カウンター情報などのインスタンスの統計が取得され、分単位、時間単位、日単位、または週単位で集計されます。この集計データを事前定義されたレポートで表示できます。

パフォーマンスポーリング間隔を設定するには、[ネットワーク] > [ネットワークレポート] に移動し、**[**ポーリング間隔の 設定] をクリック します。ポーリング間隔は 5 分未満または 60 分を超えることはできません。



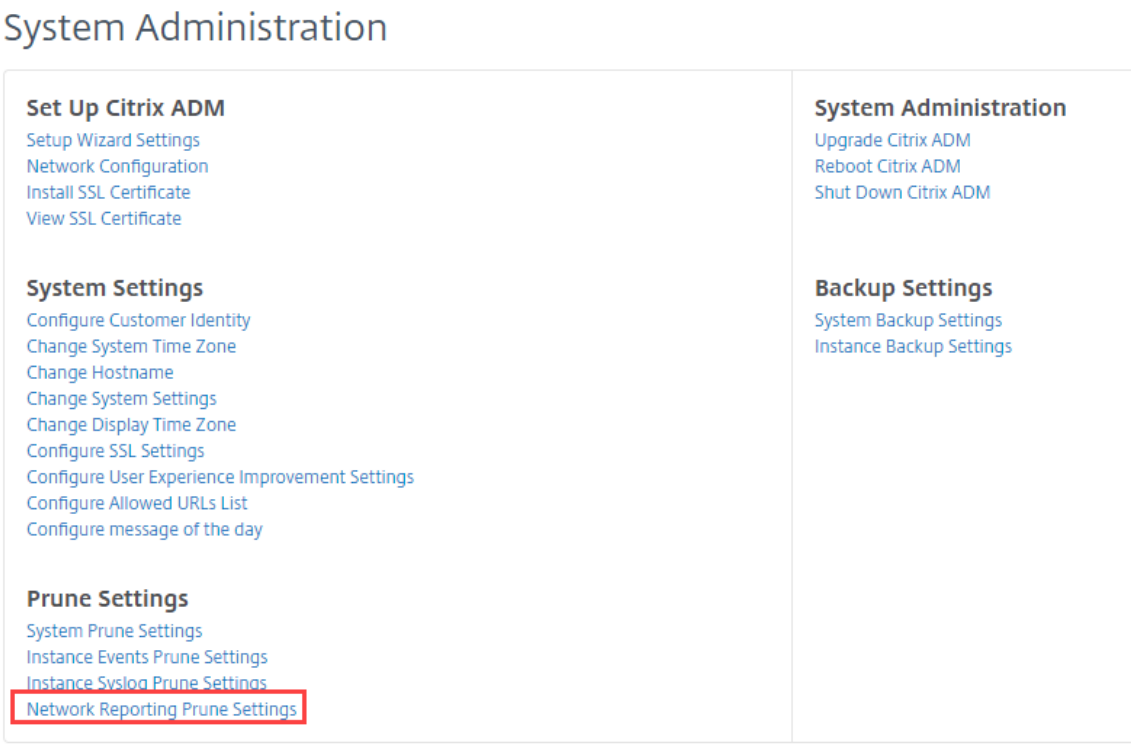
ネットワークレポートプルーニング設定の構成

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。これにより、Citrix ADM サーバーのデータベースに保存されるネットワークレポートデータの量が制限されます。デフォルトでは、ネットワークが履歴データをレポートする場合、プルーニングは 24 時間ごと（01.00 時間ごと）実行されます。

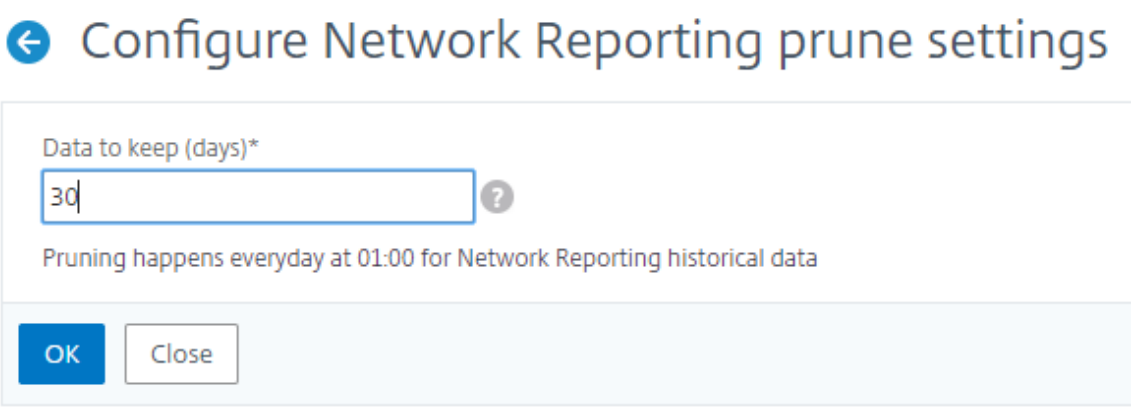
> 注
>
> : 指定できる値は 90 日を超えることも、1 日未満にすることもできません。

ネットワークレポーティングプルーニング設定を構成するには:

1. [**System**] > [**System Administration**] の順に選択します。プルーニング設定で、ネットワークレポートプルーニング設定をクリックします。



2. 「ネットワークレポーティングプルーニング設定の構成」ページで、データを保持する日数を指定し、「**OK**」をクリックします。



すべてのネットワークレポートパフォーマンスデータは、選択した日数の間、Citrix ADM データベースに保持されます。

分析

February 6, 2024

Citrix ADM Analytics 機能を使用すると、Citrix ADC のさまざまな洞察を簡単かつスケーラブルに調べて、アプリケーションのパフォーマンスを分析および改善できます。NetScaler ADM では、1 つ以上の分析機能を同時に使用できます。

次の表では、Citrix ADM でサポートされているさまざまな分析機能について説明します。

分析機能	説明
Web Insight	Web Insight を使用すると、エンタープライズ Web アプリケーションを可視化し、Citrix ADC のすべての Web アプリケーションを監視できます。管理者は、アプリケーションを統合的かつリアルタイムで監視できます。
HDX insight	HDX Insight は、NetScaler ADC を通過する ICA トラフィックのエンドツーエンドの可視性を提供します。HDX Insight を使用すると、クライアントとネットワークの遅延メトリクス、履歴レポート、エンドツーエンドのパフォーマンスデータをリアルタイムで表示し、パフォーマンス問題のトラブルシューティングを行うことができます。
Gateway Insight	Gateway Insight は、アクセスモードに関係なく、NetScaler Gateway へのログオン時にすべてのユーザーが遭遇した障害を可視化します。
Security Insight	Security Insight は、アプリケーションのセキュリティ状況を判断し、是正処置を実施してアプリケーションを保護するための統一管理コンソールソリューションです。
SSL Insight	SSL Insight は、安全な Web トランザクション（HTTPS）を可視化し、Citrix ADC のすべての安全な Web アプリケーションを監視できるようにします。管理者は、安全なウェブトランザクションを統合的かつリアルタイムかつ履歴的に監視できます。
TCP Insight	TCP Insight は、データ転送におけるネットワークの輻輳を回避するために Citrix ADC インスタンスで使用される最適化手法と輻輳制御戦略（またはアルゴリズム）のメトリックを監視するための簡単でスケーラブルなソリューションを提供します。

分析機能	説明
Video Insight	Video Insight 機能は、Citrix ADC アプライアンスで使用されるビデオ最適化手法のメトリックを監視して、カスタマーエクスペリエンスと運用効率を向上させるための簡単でスケーラブルなソリューションを提供します。
WAN Insight	WAN Insight の分析機能を使用すると、管理者はデータセンターと Branch WAN 最適化アプライアンス間を流れる高速および非高速の WAN トラフィックを容易に監視できます。また、WAN Insight は、ネットワーク上のクライアント、アプリケーション、ブランチを可視化して、ネットワークの問題を効果的にトラブルシューティングできるようにします。

ライセンス要件

February 6, 2024

次の表は、NetScaler ADM のさまざまな分析レポートを表示するための NetScaler ADC インスタンスのライセンス要件を示しています。

NetScaler ADM アナリティクスの機能	Citrix ADC ライセンス要件
Web Insight	Citrix ADM に関する Web Insight レポートは、すべての Citrix ADC ライセンスエディション（スタンダード/エンタープライズ/プラチナ）でサポートされています。
HDX Insight	Citrix ADM の HDX Insight レポートは、エンタープライズエディション（1 時間未満のレポート用）またはプラチナエディション（無制限のレポート用）のいずれかの Citrix ADC ライセンスでサポートされています。注**:** Standard ライセンスエディションはサポートされていません。

NetScaler ADM アナリティクスの機能	Citrix ADC ライセンス要件
Security Insight	Citrix ADM のセキュリティインサイトレポートは、プラチナエディションまたはアプリファイアウォールライセンスのあるエンタープライズエディションでサポートされています。注**:** 標準ライセンスエディションおよびスタンドアロン App Firewall ライセンスはサポートされていません。
SSL Insight	Citrix ADM の SSL インサイトレポートは、すべての Citrix ADC ライセンスエディション（スタンダード/エンタープライズ/プラチナ）でサポートされています。
Gateway Insight	Citrix ADM の Gateway Insight レポートは、エンタープライズエディション（1 時間未満のレポート用）またはプラチナエディション（無制限のレポート用）のいずれかの Citrix ADC ライセンスでサポートされています。注**:** Standard ライセンスエディションはサポートされていません。
TCP Insight	TCP Insight レポートは、すべての Citrix ADC ライセンスエディション（スタンダード/エンタープライズ/プラチナ）でサポートされています。
Video Insight	NetScaler ADM に関するビデオインサイトレポートは、Citrix ADC プレミアム（VPX-T 1000 シリーズ、VPX-T）エディションでサポートされています。
WAN Insight	Citrix ADM に関する WAN インサイトレポートは、Citrix SD-WAN WO エディション (WAN 最適化エディション) でサポートされています。

ログストリームの概要

February 6, 2024

NetScaler ADC インスタンスは AppFlow レコードを生成し、データセンター内のすべてのアプリケーショントラフィックの中央制御ポイントとなります。IPFIX とログストリームは、Citrix ADC インスタンスから Citrix ADM にこれらの AppFlow レコードを転送するプロトコルです。詳細については、AppFlowを参照してください。

- IPFIX (IPFIX) は、RFC 5101 で定義されているオープンなインターネット技術タスクフォース (IETF) 規格である。IPFIX は、一方向のデータフローに使用される信頼性の低いトランスポートプロトコルである UDP プ

ロトコルを使用しています。IPFIX は UDP プロトコルを使用するため、IPFIX 標準に準拠すると、NetScaler ADM でより多くのリソースを処理することになります。

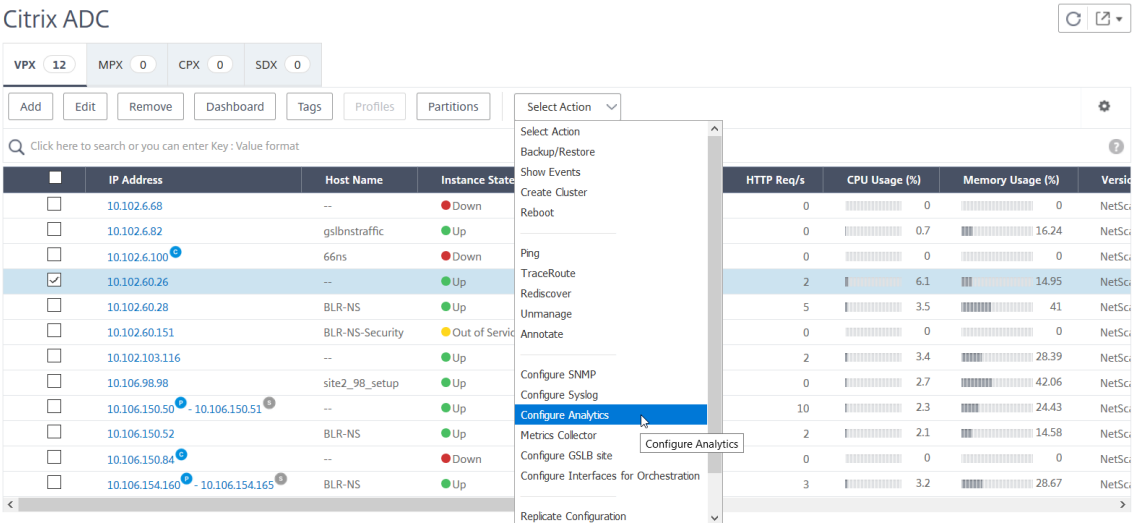
- Logstream は、Citrix が所有するプロトコルで、分析ログデータを Citrix ADC インスタンスから Citrix ADM に効率的に転送するためのトランスポートモードの 1 つとして使用されます。Logstream は信頼性の高い TCP プロトコルを使用しており、データ処理に必要なリソースも少なくて済みます。

11.1 ビルド **47.14** から **11.1** ビルド **62.8** までの CitrixADC では、Logstream が Web インサイト（HTTP）を有効にするデフォルトのトランスポートモードであり、IPFIX が他のインサイトを有効にする唯一のトランスポートモードです。**12.0** から最新バージョンまでの **Citrix ADC** バージョンでは、トランスポートモードとしてログストリームまたは IPFIX のいずれかを選択できます。

> 注
>
> Citrix ADM のバージョンとビルドは、Citrix ADC 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、Citrix ADC 12.1 ビルド 50.28/50.31 以前をインストールしている場合は、Citrix ADM 12.1 ビルド 50.39 がインストールされていることを確認してください。

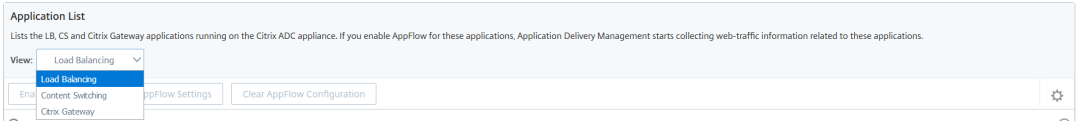
Citrix ADM で分析を有効にしているときに通信モードとしてログストリームを使用するには:

1. [ネットワーク] > [インスタンス] > [**Cit**rix ADC] に移動し、分析を有効にする NetScaler ADC インスタンスを選択します。
2. **[** アクションの選択] リストから、[**Analytics** の設定] を選択します。

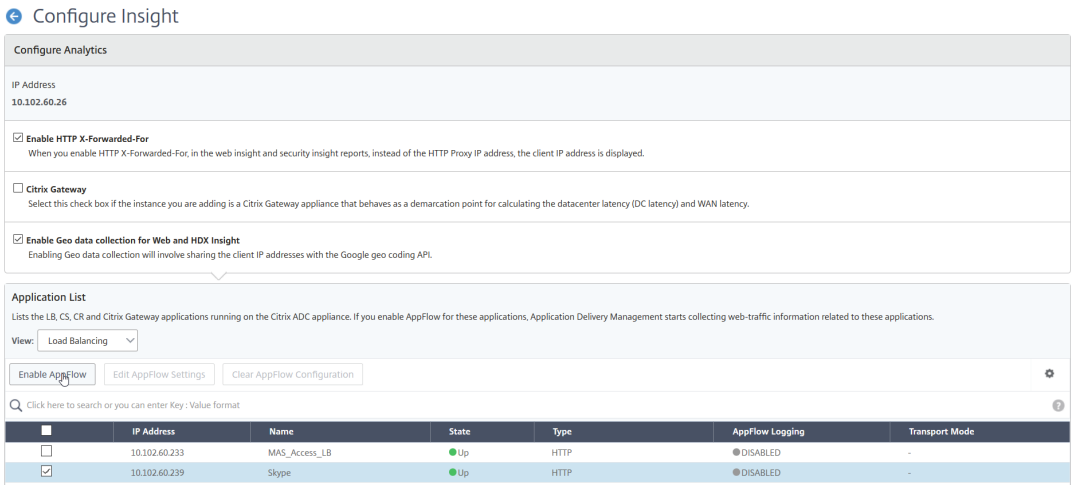


3. [** Insight の設定 **] ページで、次の操作を行います。

   a) ロードバランシングまたはコンテンツスイッチングの アプリケーションリスト を選択します。



b) 仮想サーバーを選択し、[**AppFlow** を有効にする] をクリックします。

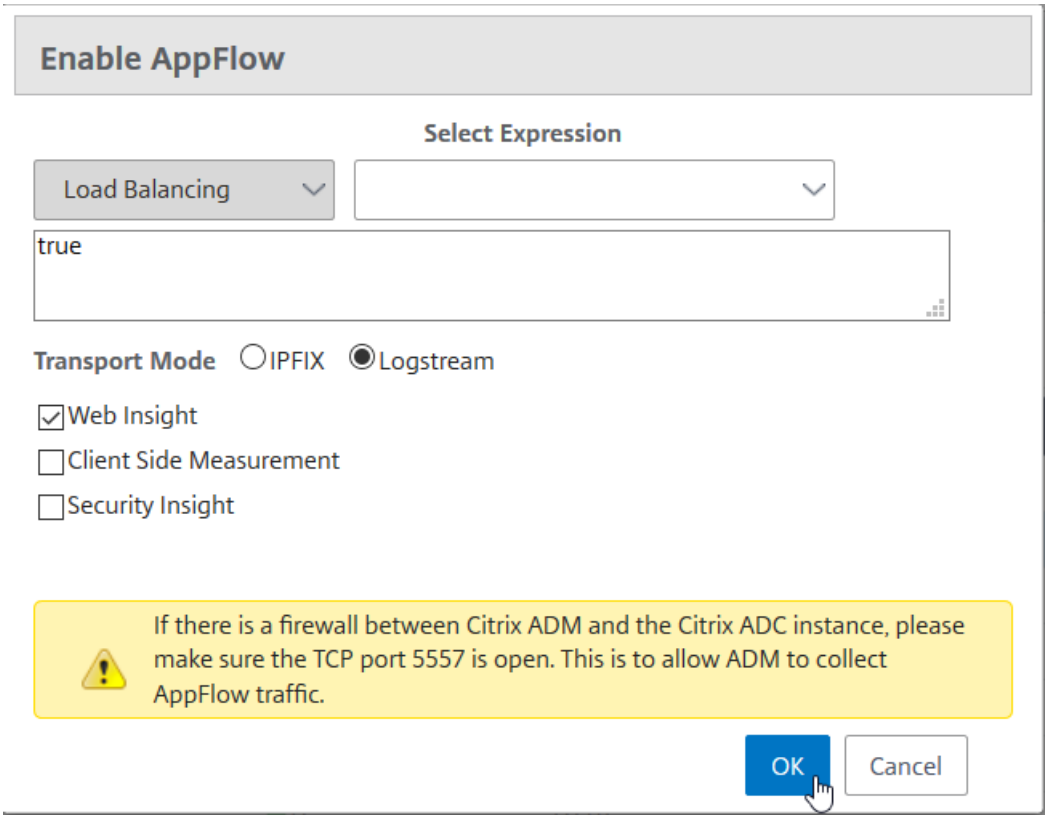


4. [AppFlow を有効にする] ダイアログボックスで、次の操作を行います。

- テキストボックスに **true** と入力します。
- 転送モードとして [ログストリーム] を選択します。

> 注
>
> Citrix では、トランスポートモードとして Logstream を選択することをお勧めします。

- インサイトタイプを選択し、「**OK**」をクリックします。



次の表では、転送モードとして Logstream をサポートする Citrix ADM の機能について説明します:

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

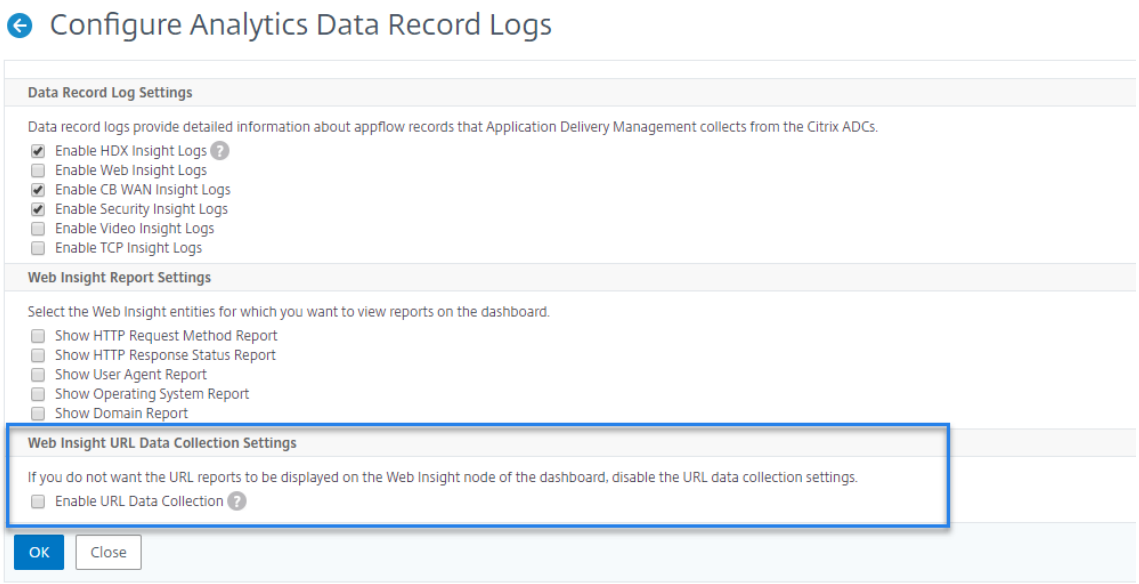
URL データ収集を無効にする

February 6, 2024

CitrixApplication Delivery Management（ADM）のダッシュボードの Web Insight ノードに URL レポートを表示したくない場合は、URL データ収集を無効にできます。

NetScaler ADM からの URL データ収集を無効にするには

1. Citrix ADM で、［分析］>［設定］に移動し、［分析データレコードログの設定］をクリックします。
2. ［**Web Insight URL Data Collection Settings**］セクションで［**Enable URL Data Collection**］オプションがオンになっている場合は、このチェックボックスをオフにします。
3. ［**OK**］をクリックします。



しきい値およびアラートの作成

February 6, 2024

しきい値とアラートを設定して、Citrix ADC インスタンスの状態を監視できます。カウンターにしきい値を設定して、インスタンスや管理対象インスタンスのエンティティを監視できます。

カウンターの値がしきい値を超えると、Citrix Application Delivery Management（ADM）はパフォーマンス関連の問題を通知するイベントを生成します。カウンターの値がしきい値で指定されているクリア値に一致するとイベントは消去されます。これは、そのしきい値が通常の状態に戻ったことを意味します。

しきい値にアクションを割り当てることもできます。アクションには、アラート、メール、SMS 通知の送信があります。しきい値を超えると、Citrix ADM は、アラートの有効化や電子メールまたは SMS 通知の送信など、ユーザーが定義したアクションを自動的に実行します。

NetScaler ADM を使用してしきい値およびアラートを作成するには

1. NetScaler ADM で、[**Analytics**] > [設定] > [しきい値] に移動します。[**Thresholds**] の [**Add**] をクリックします。
2. 「しきい値の作成」ページで、次の詳細を指定します。
   - **Name** - しきい値の構成の名前
   - トラフィックタイプ—しきい値を設定するトラフィックのタイプ。
   - **Entity** - しきい値構成時のカテゴリまたはリソースの種類
   - **Reference Key** - トラフィックの種類とエンティティの選択に基づいて自動的に生成される値
   - **Duration** - しきい値構成時の間隔
   - **[Configure** Rule]：しきい値を構成するメトリックのルール。
   - 通知設定-しきい値を有効にし、しきい値を超えたときに電子メール、Slack、SMS などのさまざまなチャネルで通知を受け取ります。
3. [作成] をクリックします。

HDX insight では、構成されたしきい値にすべてのエンティティが違反した場合にのみアラートが生成される、複数のしきい値を設定することもできます。

適応しきい値の設定

February 6, 2024

アダプティブしきい値機能によって、各 URL の最大ヒット数のしきい値が設定されます。URL の最大ヒット数が、その URL に設定されたしきい値を超えると、外部 Syslog サーバーに Syslog メッセージが送信されます。しきい値の間隔は、日単位または週単位で指定できます。

しきい値は、次のように計算されます。

しきい値 = 最大ヒット数 **×** しきい値乗数

各項目の意味は次のとおりです：

- 最大ヒット数：URL のヒットの最大数。
- しきい値乗数：ユーザーが定義する整数値（デフォルト：2）。

Citrix ADM を使用してアダプティブしきい値を作成するには

1. Citrix ADM で、［分析］>［設定］>［適応しきい値］に移動し、［追加］をクリックします。
2.「適応しきい値」ページで、次のパラメータを指定します。
    - **Name** - しきい値名
    - エンティティ -URL
    - **Duration** - しきい値の期間（日または週）
    - しきい値乗 数-URL の適応しきい値を取得するために、指定した URL の最大ヒット数を乗算するユーザー定義の整数。

データベースの永続性の構成

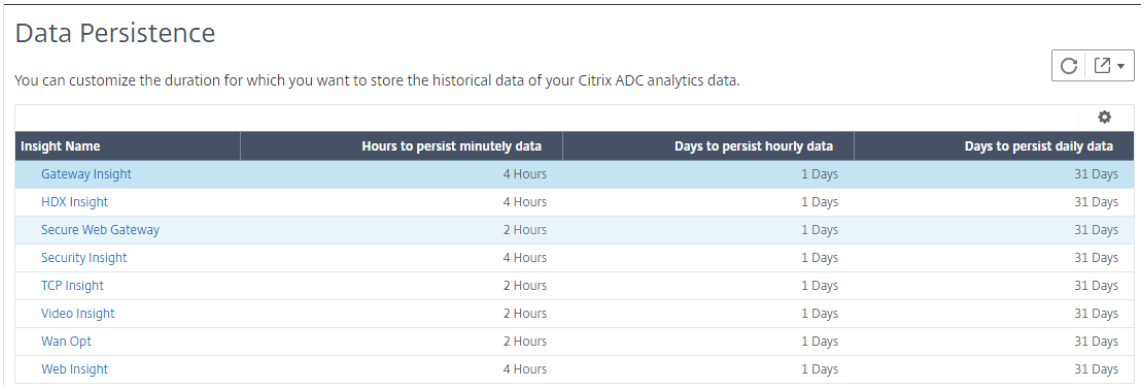
February 6, 2024

Citrix Application Delivery Management（ADM）でデータベース永続性を構成すると、Citrix ADC 分析データの履歴データを保存する期間をカスタマイズできます。分析の履歴データには、次のデータベース永続性タイプを選択できます。

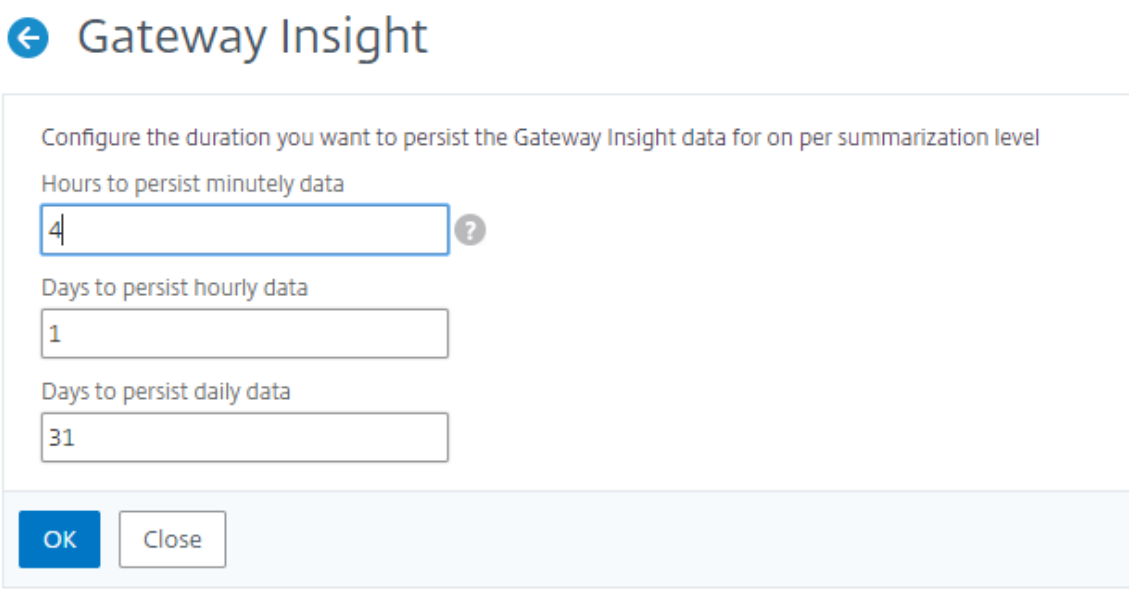
- 分単位のデータを保持するのにかかる時間
- 時間単位のデータを保存する日数
- 毎日データを保持する日数

データベースパーシスタンスを設定するには

1. [**Analytics**] > [設定] > [データベースの永続性] に移動します。
2. データベースの永続性を設定したいインサイトタイプをクリックします。



3. Citrix ADM で Insight データを保持する期間を指定します。たとえば、Gateway Insight に関して、分析の分単位の履歴データを 2 時間保存したり、時間単位のデータを 1 日保存したりできます。



Analytics のセルフサービス診断

February 6, 2024

Citrix Application Delivery Management（ADM）は、セルフサービス診断を実行して、以下の分析機能について、管理対象インスタンスのライセンスと構成の問題を特定します。

- Web Insight
- HDX Insight
- Gateway Insight

- Security Insight
- Secure Web Gateway 分析

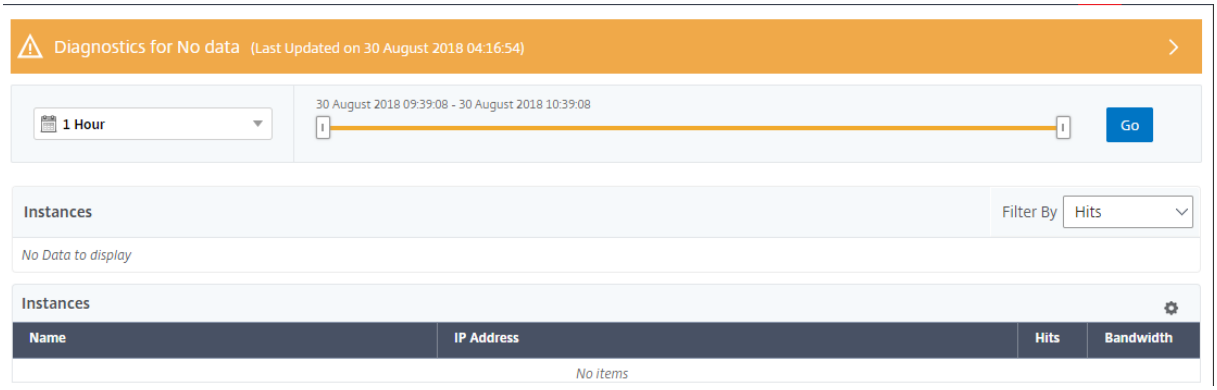
セルフサービス診断は 12 時間ごとに実行され、指定した分析機能ごとに問題が見つかった場合に診断レポートを生成します。診断レポートには、問題の原因、問題の種類、および問題を解決するための是正措置が記載されています。セルフサービス診断により、問題をより迅速に特定してトラブルシューティングできます。

たとえば、AppFlow ポリシーが仮想サーバーにバインドされていない場合、または仮想サーバーにライセンスがない場合、NetScaler ADM は Web Insight 監視に必要なデータを取得しません。セルフサービス診断は問題を特定し、診断レポートを生成します。診断レポートを表示して問題を確認し、修正アクションを実行できます。

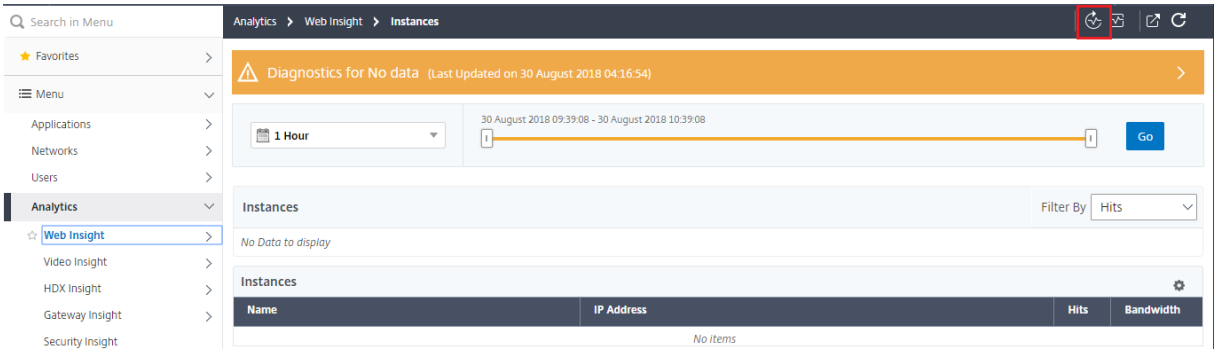
診断レポートを表示する

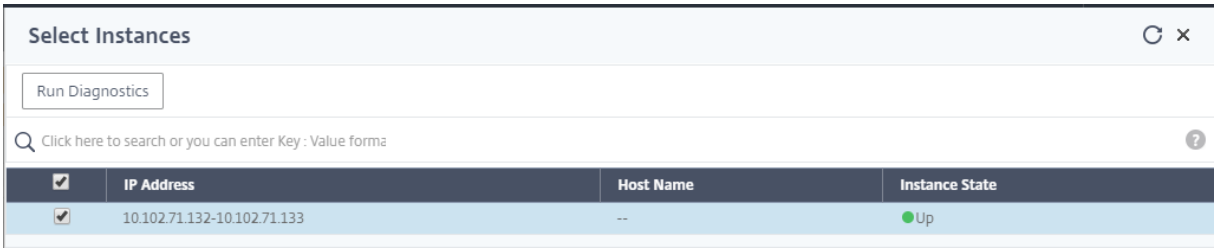
指定した分析機能の診断レポートを表示するには、NetScaler ADM ダッシュボードでそれぞれの分析ノードに移動する必要があります。

たとえば、Web Insight の診断レポートを表示するには、[分析] **>** [Web インサイト] に移動します。[Web Insight] ページで、[診断の表示] アイコンを選択します。



問題をチェックする場合は、インスタント診断を実行することもできます。[診断を実行] をクリックします。インスタンスを選択し、[**Run Diagnostics**] を選択します。





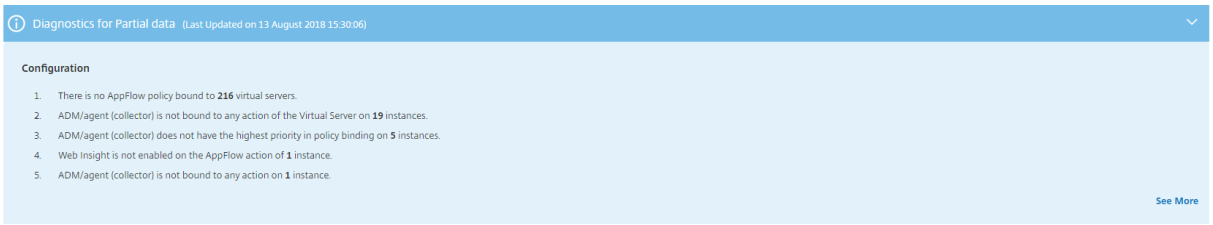
診断レポートの分析

セルフサービス診断では、問題の重要度に応じて、診断レポートがオレンジ色または青色の背景で表示されます。

オレンジ色の背景の診断レポートは、青色の背景よりも重要度が高いことを示しています。

たとえば、NetScaler ADC インスタンスには 5 つの仮想サーバーが設定されています。どの仮想サーバーでも AppFlow パラメーターを有効にしていない場合、NetScaler ADM は分析用の Web Insight および Security Insight トラフィックを受信しません。セルフサービス診断では、構成の問題が重大であることが特定されます。診断レポートは、Web Insight と Security Insight 機能でオレンジ色の背景で表示されます。

いずれかの仮想サーバーで AppFlow を有効にしている場合、NetScaler ADM は分析用のデータを受信します。少なくとも 1 つの仮想サーバーが分析のためにトラフィックを送信しているため、青色の背景で診断レポートが表示されます。

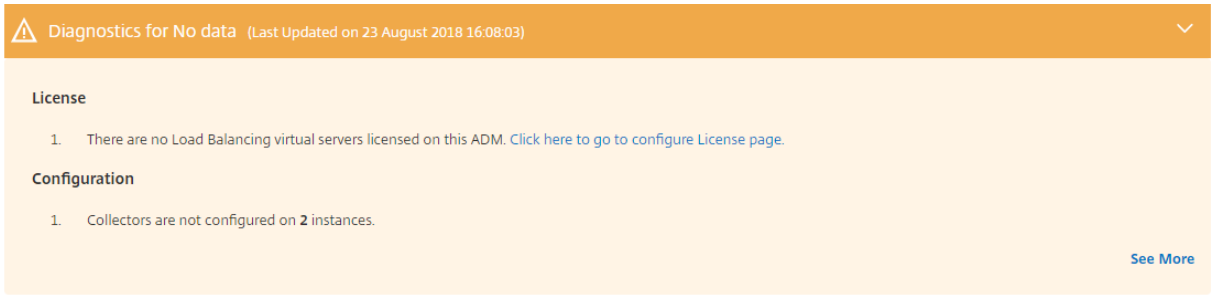


> 重要：セルフサービス診断では、トラフィックフローはチェックされません。管理対象インスタンスの指定した分析機能に関連するライセンスまたは設定の問題のみをチェックします。仮想サーバーを経由するアクティブなトラフィックがないため、分析データが表示されないことがあります。

診断レポートには、概要ページと詳細情報ページがあります。

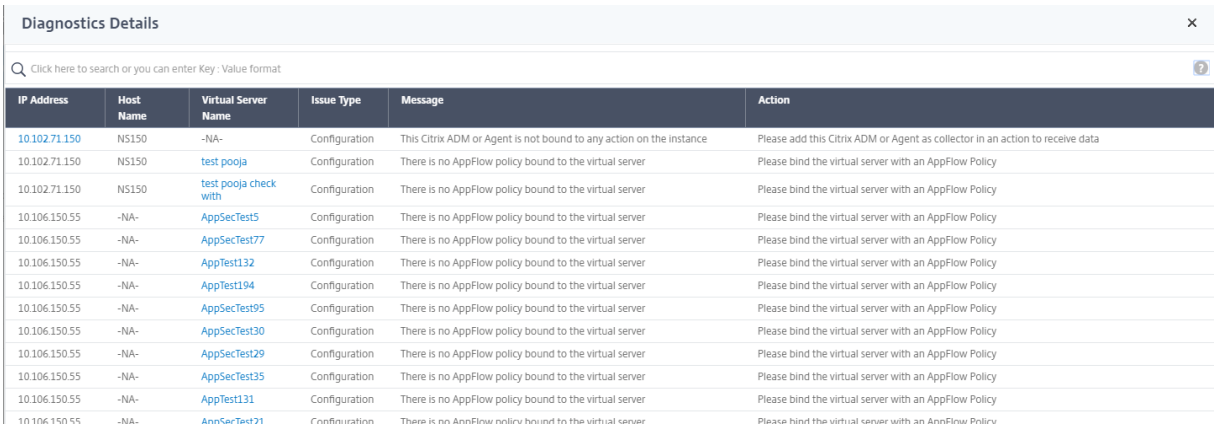
概要ページには、問題の種類 (ライセンスまたは構成) の概要が表示されます。このページには、関連する設定ページに移動するハイパーリンクが含まれている場合があります。

たとえば、NetScaler ADM でライセンスされた負荷分散仮想サーバーがない場合、概要ページには［システムライセンス］ページへのハイパーリンクが表示されます。

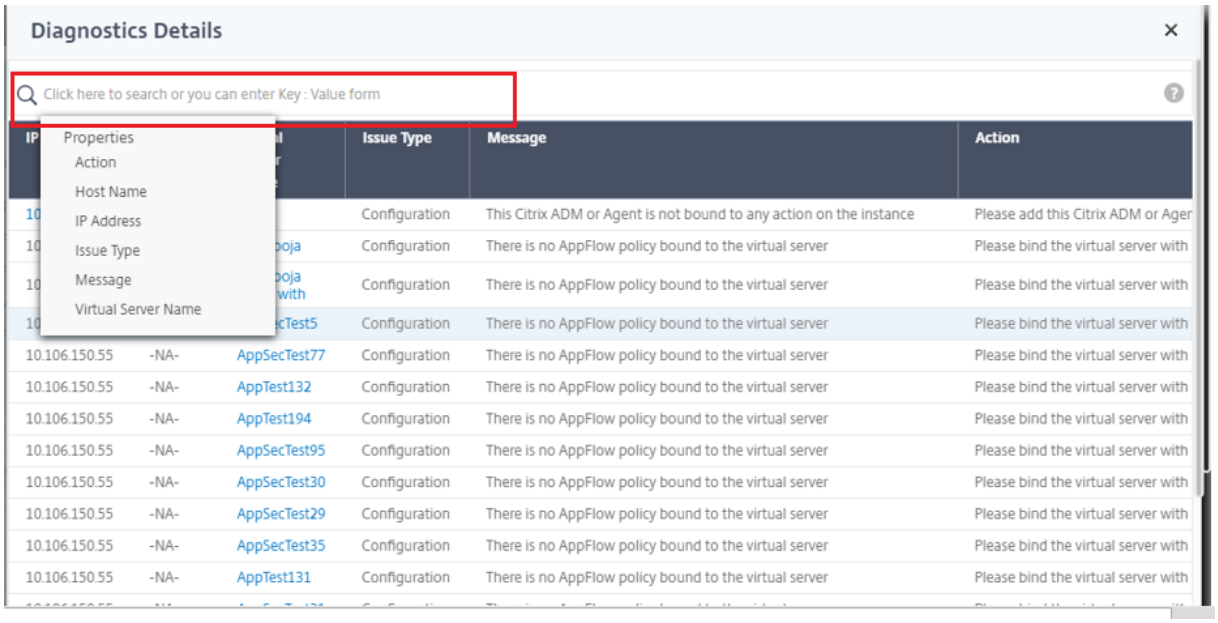


問題に関する詳細情報を表示するには、サマリページの [詳細 を表示] をクリックします。

詳細情報ページには、問題に関する完全な情報と、実行する必要があるアクションが推奨されます。各問題に対するハイパーリンクをクリックして、管理対象インスタンスまたは仮想サーバーを構成できます。



アクション、ホスト名、IP アドレス、問題の種類などに基づいて問題を検索することもできます。



問題を解決したら、インスタント診断を実行して最新の診断レポートを生成する必要があります。

Web Insight

February 6, 2024

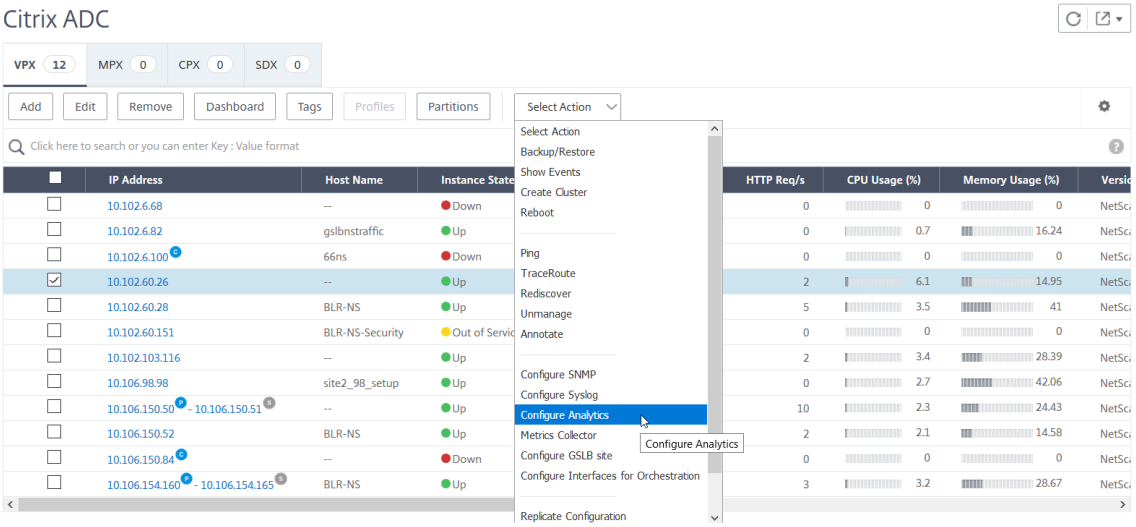
Web Insight を使用すると、管理者は Citrix ADC インスタンスによって提供されるすべての Web アプリケーションを監視できます。管理者は、Citrix ADC インスタンスからアプリケーションを統合的かつリアルタイムで監視できます。Web Insight は、クライアントネットワークの遅延やサーバーの応答時間などの重要な情報を提供し、アプリケーションのパフォーマンスを確実に監視および改善します。分析に使用されるデータは、Citrix ADC インスタンスによって処理される各 HTTP、HTTPS トランザクションからキャプチャされます。分析データにより、環境内の Citrix ADC インスタンス、アプリケーション、URL、クライアント、およびサーバーのパフォーマンスを分析できます。

Web Insight を使用してデータを表示できるユースケースには、次のようなものがあります。

- SharePoint などのアプリケーションへのアクセス中に遅延が発生しているクライアントのリスト
- 1 時間以内に最もヒット数が多かったアプリケーション
- クライアントからアクセスされたアプリケーションと URL のリスト
- 特定のクライアントが使用するオペレーティングシステムとブラウザ
- エラー関連の応答を最も多く送信するアプリケーションまたはサーバー
- 特定のクライアントでのアクセシビリティの問題
- 特定のクライアントからの少数のアプリケーションまたはすべてのアプリケーションにおけるアクセシビリティの問題
- 特定のクライアントやバックエンドサーバーから遅くなるアプリケーションのページはほとんどありません
- 特定のクライアントおよびバックエンドサーバーからアクセスすると、アプリケーションが遅くなる

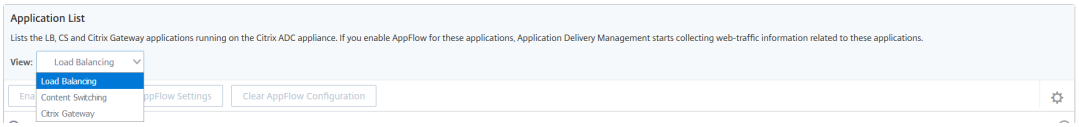
選択したインスタンス上の特定の仮想サーバーに対して Web Insight を有効にして、Web アプリケーション上のトラフィックを監視できます。Web Insight 機能は、NetScaler ADM の仮想サーバーの統計情報を提供します。Web Insight を有効にするには、次の手順に従います。

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. [ネットワーク] > [インスタンス] > [**Cit**rix ADC] に移動し、分析を有効にする NetScaler ADC インスタンスを選択します。
3. **[** アクションの選択] リストから、[**Analytics** の設定] を選択します。

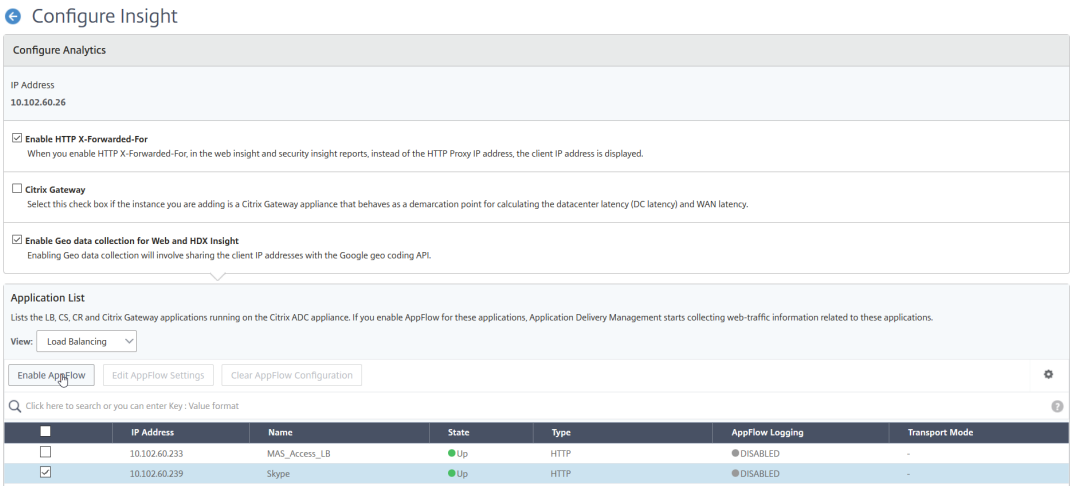


4. [** Insight の設定 **] ページで、次の操作を行います。

   a) ロードバランシングまたはコンテンツスイッチングの アプリケーションリスト を選択します。



   b) 仮想サーバーを選択し、[**AppFlow** を有効にする] をクリックします。

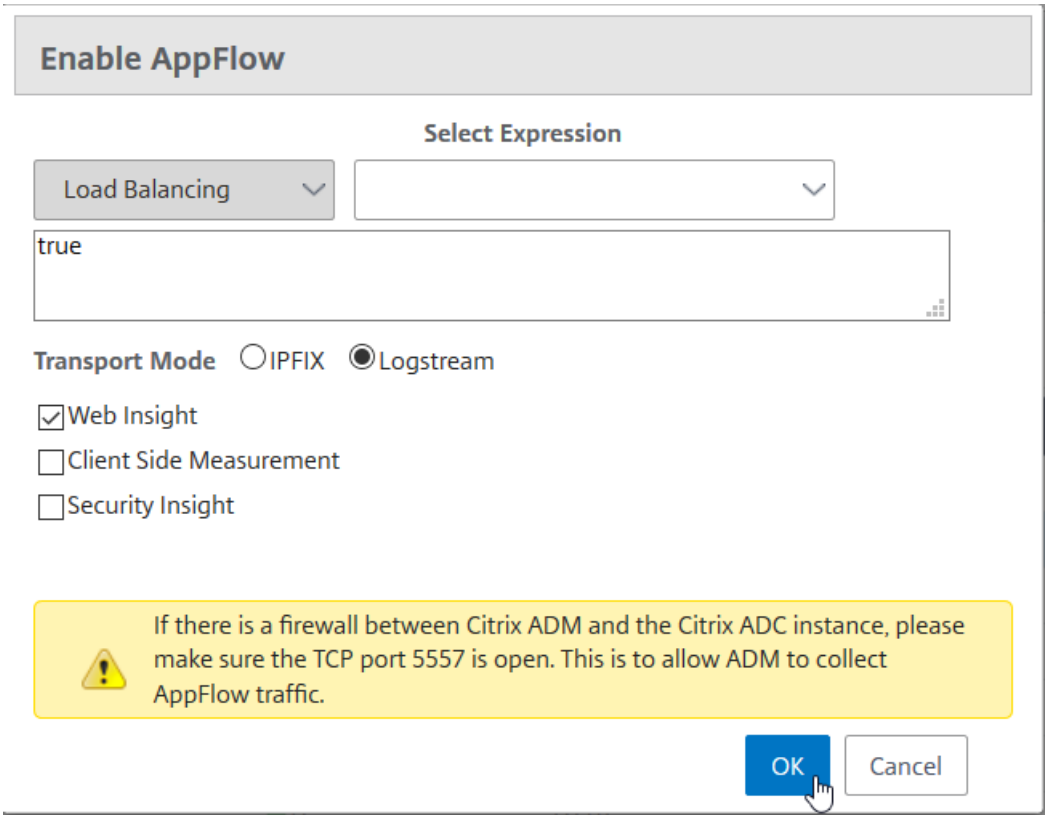


5. [AppFlow を有効にする] ダイアログボックスで、次の操作を行います。

   - テキストボックスに **true** と入力します。
   - 転送モードとして [ログストリーム] を選択します。

     > 注：Citrix では、転送モードとして Logstream を選択することを推奨しています。

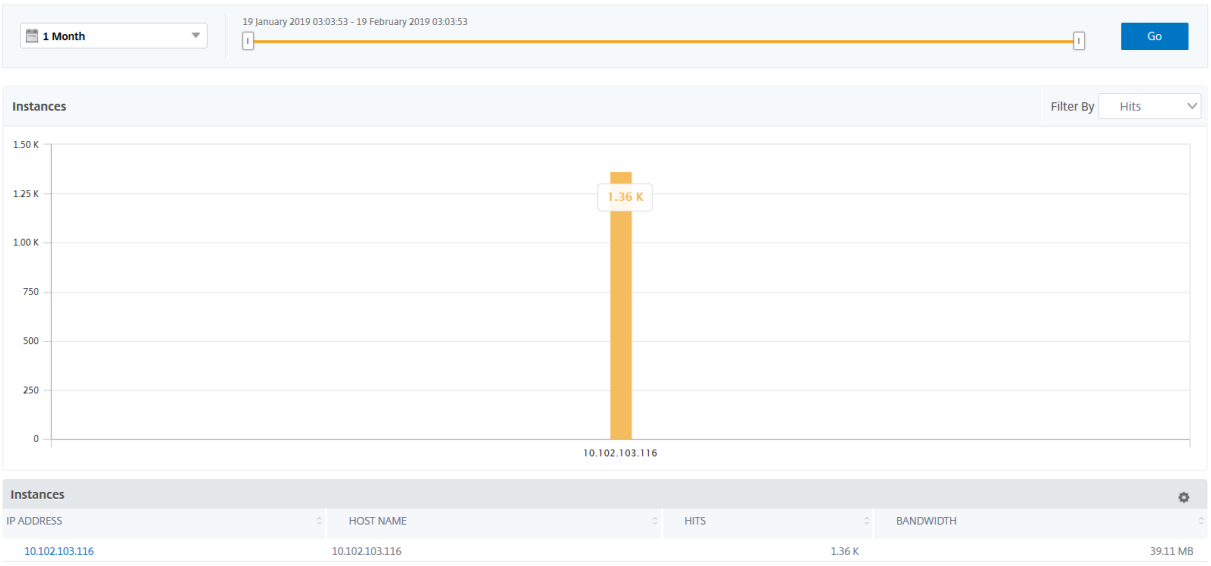
   - [**Web Insight**] を選択し、[**OK**] をクリックします。



Web アプリケーションの問題を分析する

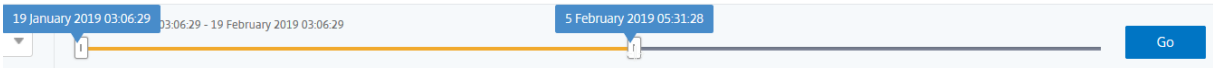
管理者が特定する必要がある一般的な問題の 1 つは、遅延の問題です。管理者は、遅延の問題がサーバーネットワーク、クライアントネットワーク、またはサーバーの応答時間にあるかどうかを確認する必要があります。Citrix ADM を使用すると、[分析] > [**Web** インサイト] に移動してこの情報を特定できます。

[**Analytics**] > [**Web Insight**] に移動すると、Web Insight が有効になっている NetScaler ADC インスタンスが表示されます。IP アドレス、ホスト名、合計ヒット数、帯域幅など、インスタンスの詳細情報を表示できます。



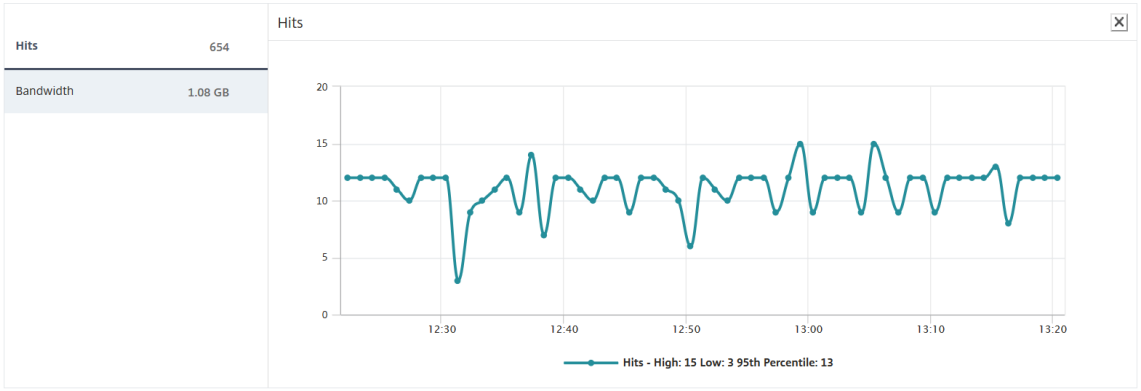
リストを使用して、インスタンスのインサイトを表示する期間を選択できます。

スライダを使用して時間をカスタマイズし、[**Go**] をクリックして結果を表示することもできます。

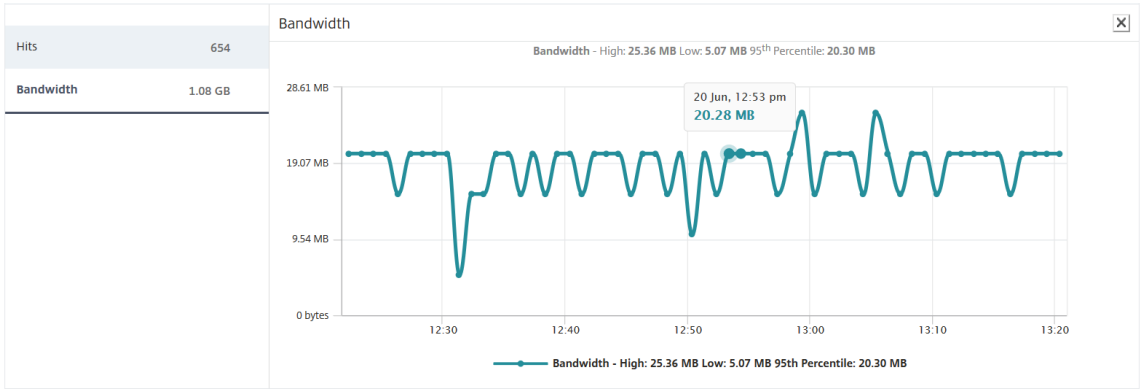


グラフまたはインスタンスの IP アドレスをクリックすると、インスタンスに関する詳細情報が表示されます。次のインサイトを表示できます。

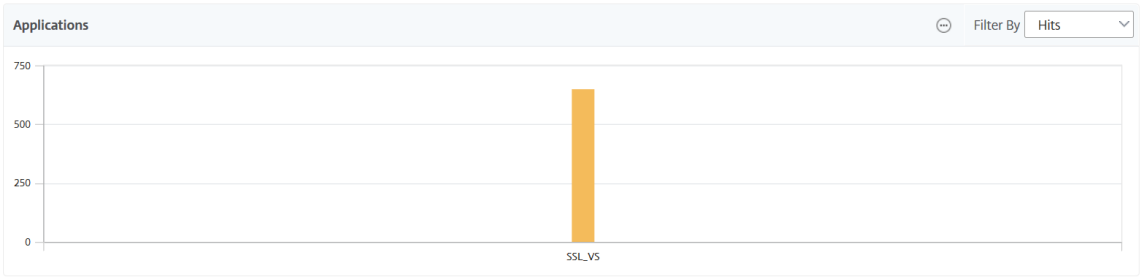
- 総ヒット数



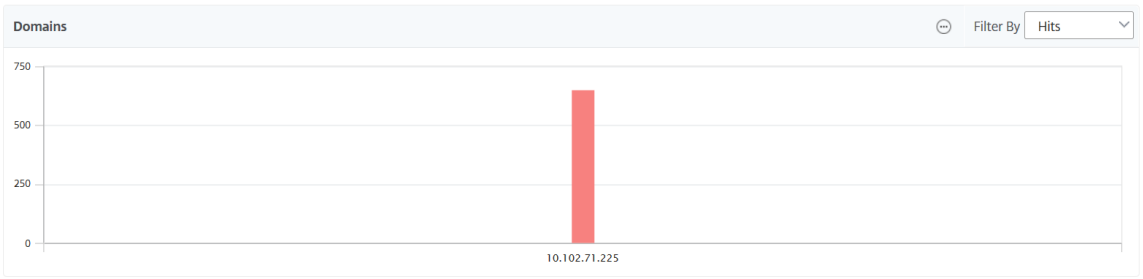
- 帯域幅



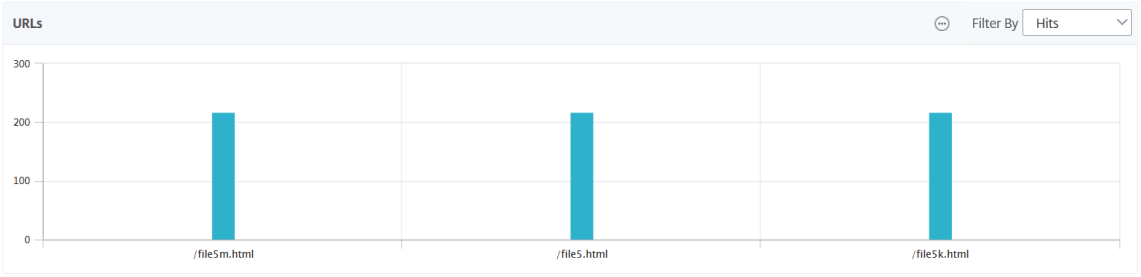
- アプリケーション



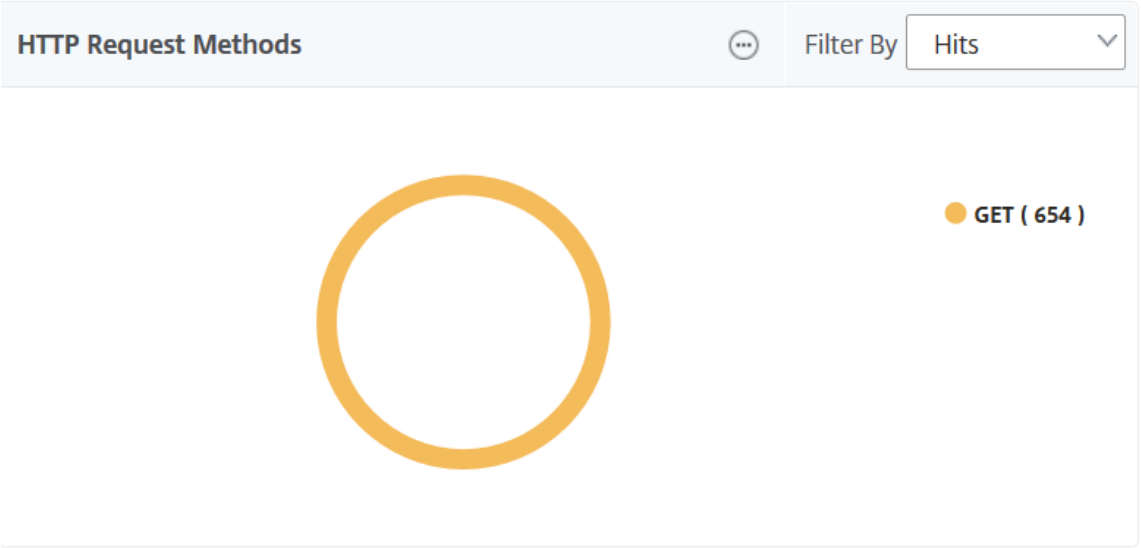
- ドメイン



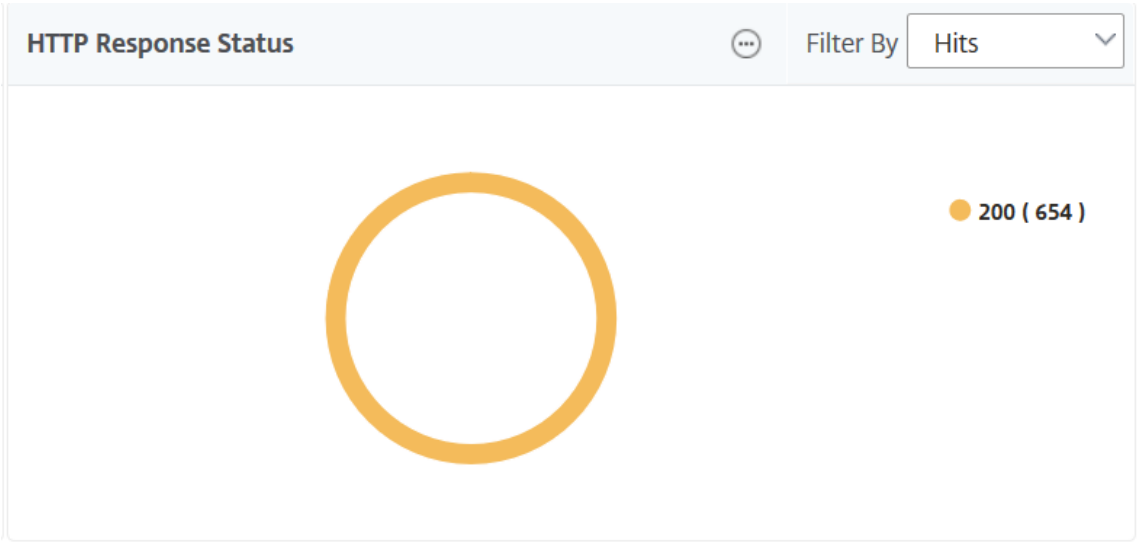
- **URL**



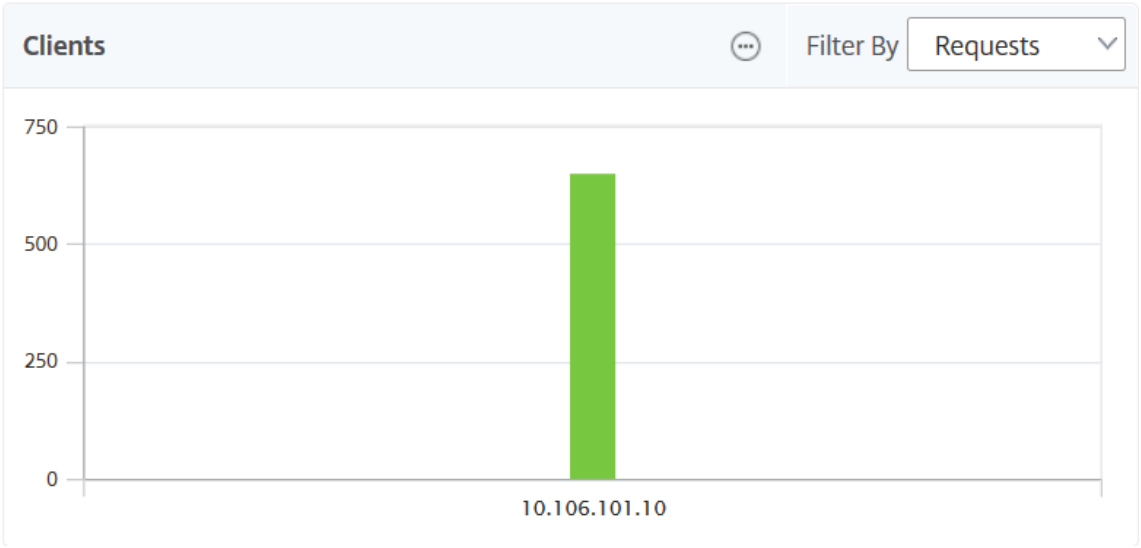
- **HTTP** 要求メソッド



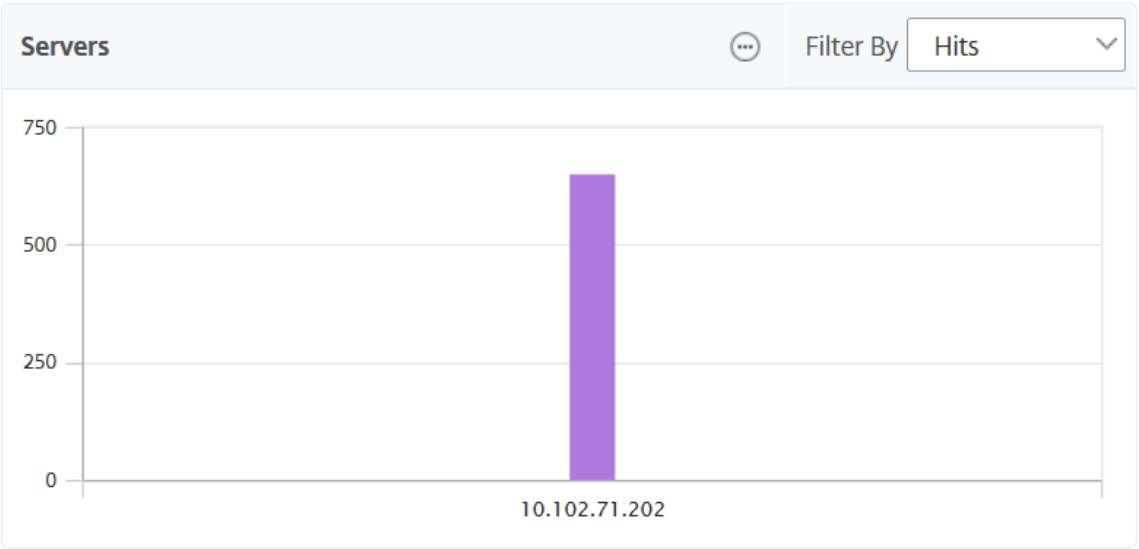
- **HTTP** 応答の状態



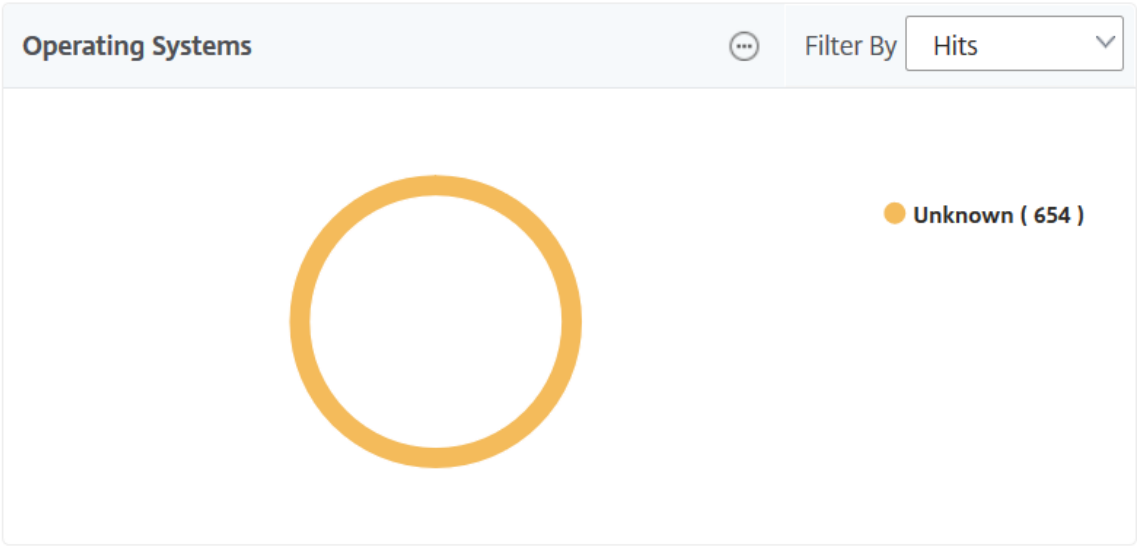
- クライアント



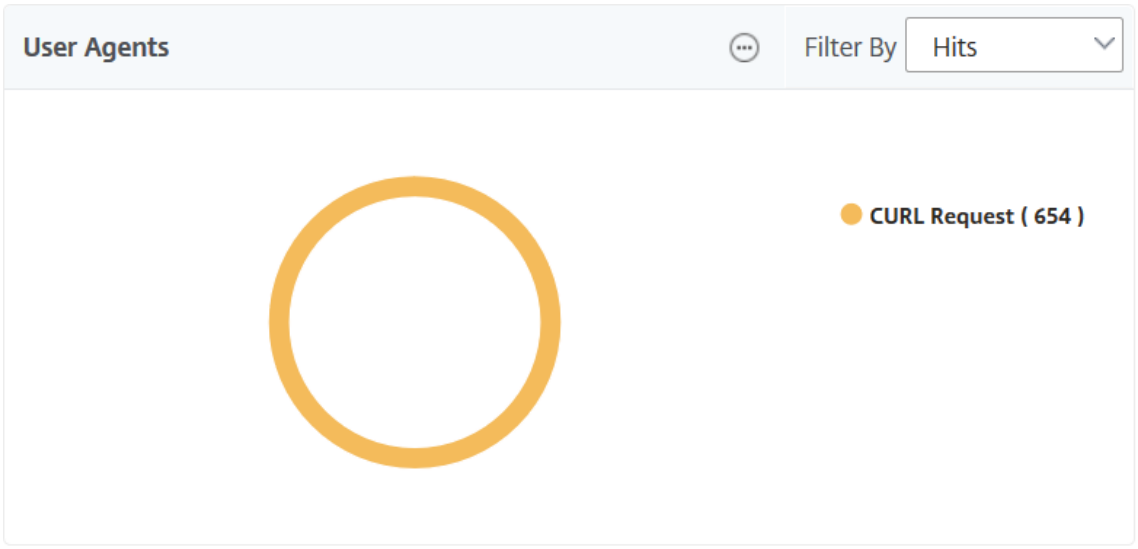
- サーバー



- オペレーティング システム

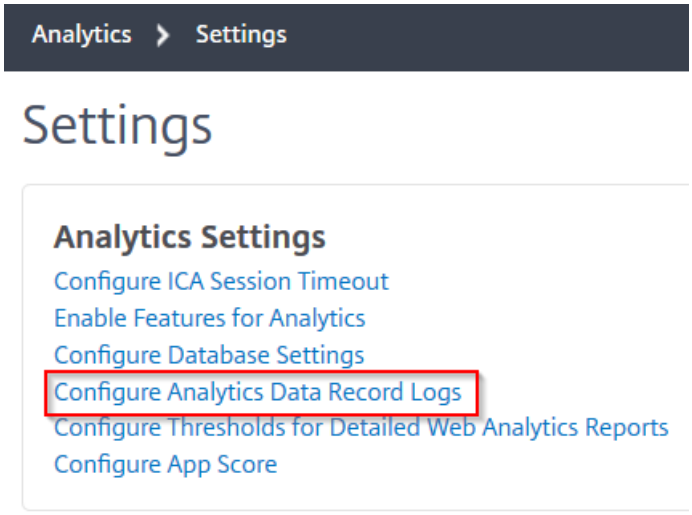


- ユーザー エージェント

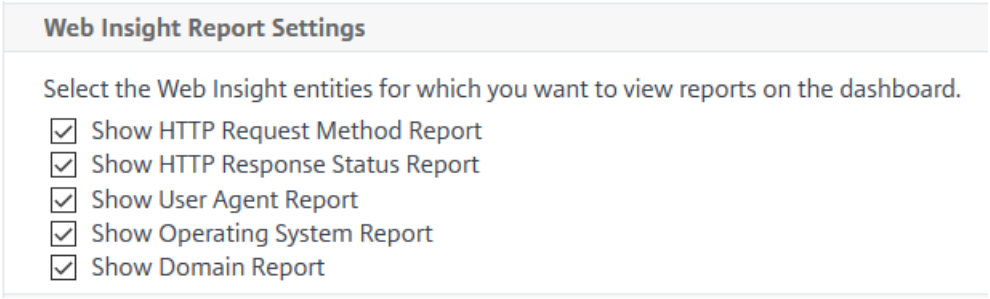


GUI でレポートを表示する **Web Insight** エンティティ を選択することもできます。

1. [アナリティクス] > [**Web** インサイト] > [設定] に移動します。
2. [**Analytics** データレコードログの構成] をクリックします。



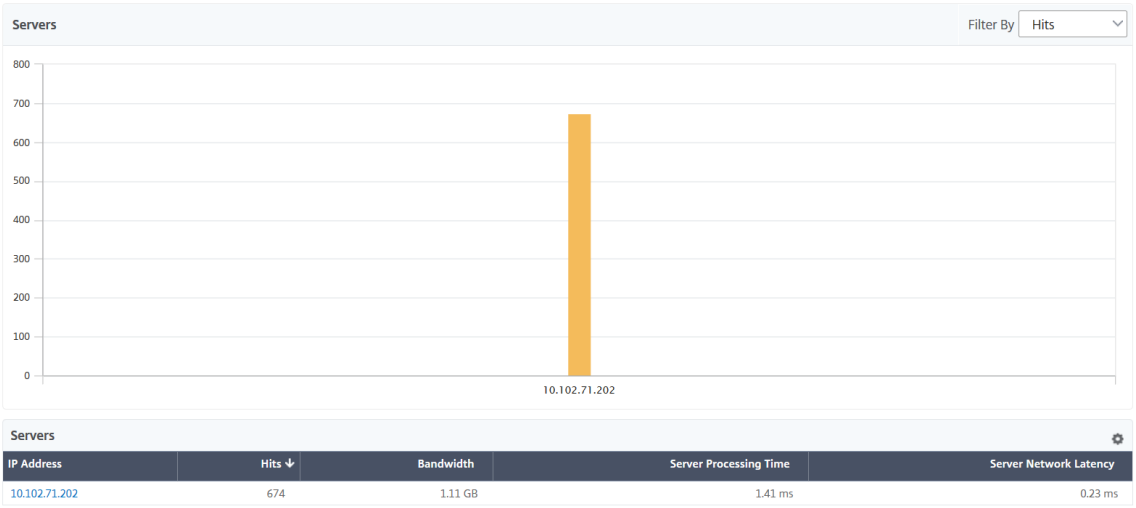
3. [**Web Insight** レポートの設定] で、GUI でレポートを表示するエンティティを選択します。



4. [**OK**] をクリックします。

詳細な分析を行うには、GUI の Web Insight の下にある各インサイトカテゴリをクリックします。たとえば、構成済みサーバーの問題をチェックする場合は、次のようにします。

1. [分析] > [**Web** インサイト] > [サーバー] に移動します。
2. 「サーバー」ページには、設定されているすべてのサーバーが表示されます。
3. グラフの IP アドレスをクリックします。テーブルから IP アドレスをクリックすることもできます。



選択したサーバーの詳細なインサイトビューが表示されます。このビューから、次のような複数のインサイトを確認できます。

- サーバーが受信したヒットの総数
- 帯域幅
- サーバー処理時間
- サーバーネットワークの待ち時間
- サーバー用に構成された仮想サーバー
- サーバーにアクセスしているクライアントの総数
- サーバーから提供された応答コードの総数

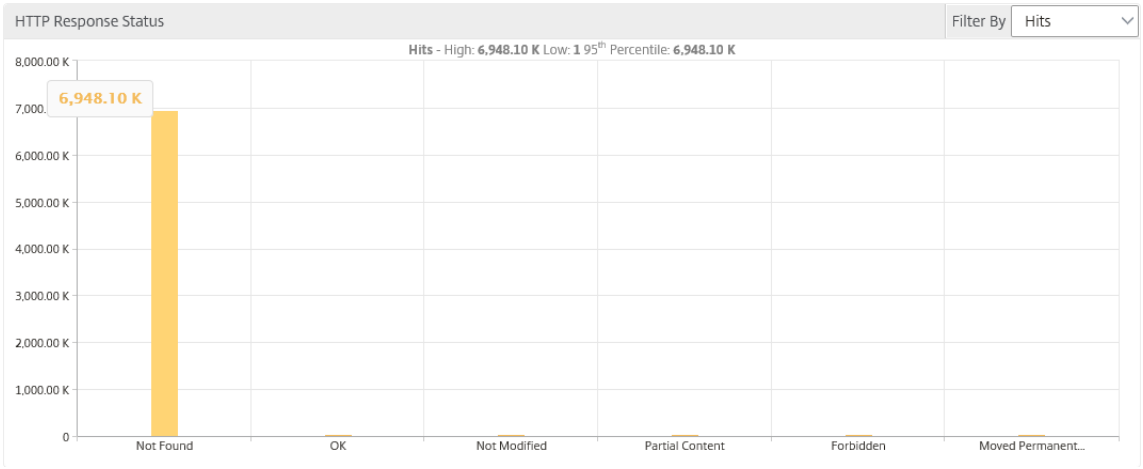
ユースケース **1**-内部サーバーエラー

Web アプリケーションのアクセス不能エラー 500 がユーザーに発生しているシナリオを考えてみましょう。エラー 500（見つかりません）は、Web サーバー上の問題を示す HTTP 応答ステータスエラーですが、サーバーは問題を明示的に示しません。実際の問題を特定して掘り下げるには:

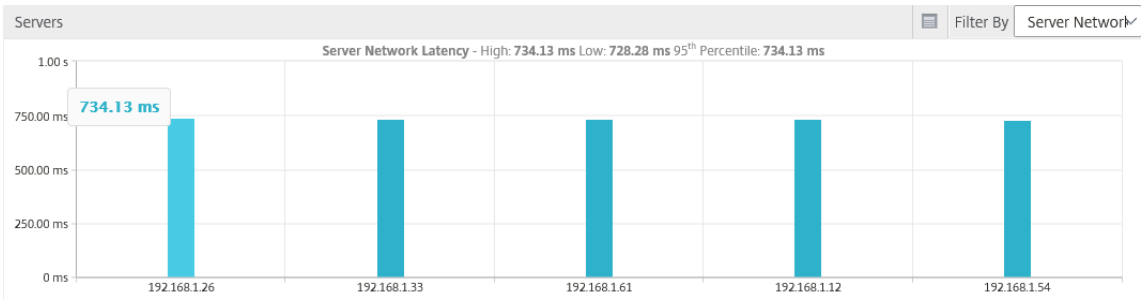
1. [**Analytics**] > [**Web Insight**] > [応答ステータス] に移動します。

   ダッシュボードページが表示されます。ダッシュボードには、処理された HTTP トランザクションの成功と失敗を分析するために使用できるメトリックが表示されます。

2. グラフで [見つかりません] をクリックします。



3. 下にスクロールして [サーバー] グラフを表示し、[フィルタ] リストから [サーバーネットワーク遅延] を選択します。



グラフは、すべてのアプリケーションサーバーが Web アプリケーションの取得に問題を抱えていたため、Web サーバーの応答時間が長くなっていることを示しています。この問題は、Web サーバーがどのサーバーからの要求にも応答しないことが原因である可能性があります。

ユースケース **2-Web** アプリケーションへのアクセスが遅いユーザーの場合

Web アプリケーションが 10 台の異なる Web サーバーでホストされているシナリオを考えてみましょう。複数のユーザーが同時にアプリケーションにアクセスすると、1 人以上のユーザーがアプリケーションの動作が遅くなることがあります。管理者は、次のシナリオを分析して問題の根本原因を理解する必要があります。

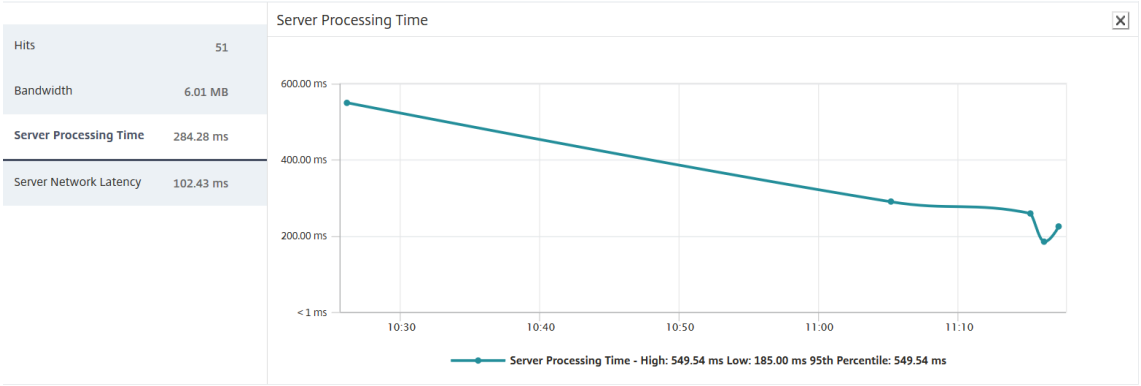
シナリオ **1-**サーバーの処理時間:

複数のリクエストが 10 台のウェブサーバーに同時に届いた場合、リクエストの読み込みにかかる時間は以下によって異なります。

- キュー内のリクエスト数。
- HTTP トランザクションを処理するために各リクエストによって消費される帯域幅。

  サーバーグラフは、サーバーによって処理されたリクエストに対する各サーバーの処理時間を理解するのに役立ちます。同様に、アプリケーショングラフには、ヒット数、応答時間、および各 HTTP トランザクションで消費された帯域幅が表示されます。

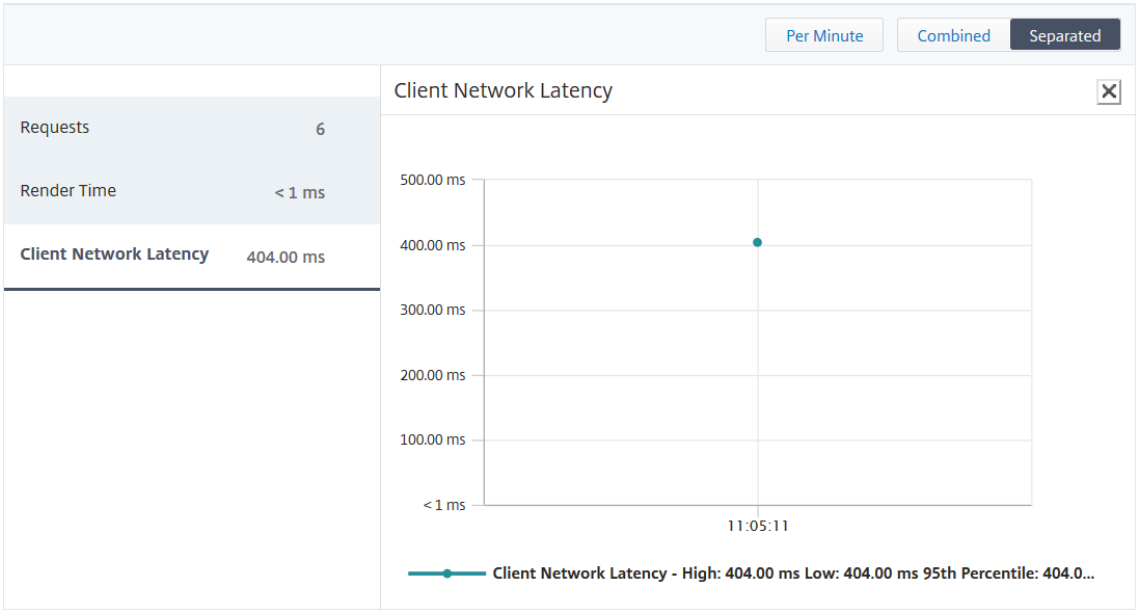
1. [分析] > [**Web** インサイト] > [サーバー] に移動します。
2. グラフからサーバーを選択します。
3. サーバーの処理時間を 分析するには、[サーバーの処理時間] をクリックします。



シナリオ **2-**クライアントの待ち時間:

アプリケーションの応答時間と合計ヒット数が、アプリケーションアクセスが遅くなる原因である可能性があります。クライアントネットワーク遅延を確認し、クライアントネットワーク遅延のメトリックを分析できます。根本原因を分析するには:

1. [アナリティクス] > [**Web** インサイト] > [クライアント] に移動します。
2. グラフからクライアントを選択します。
3. [クライアントネットワーク遅延] をクリックして、高遅延を分析します。



この例では、管理者として、クライアントネットワークのレイテンシーが高いことを示すため、クライアントネットワークからの問題の根本原因を確認できます。

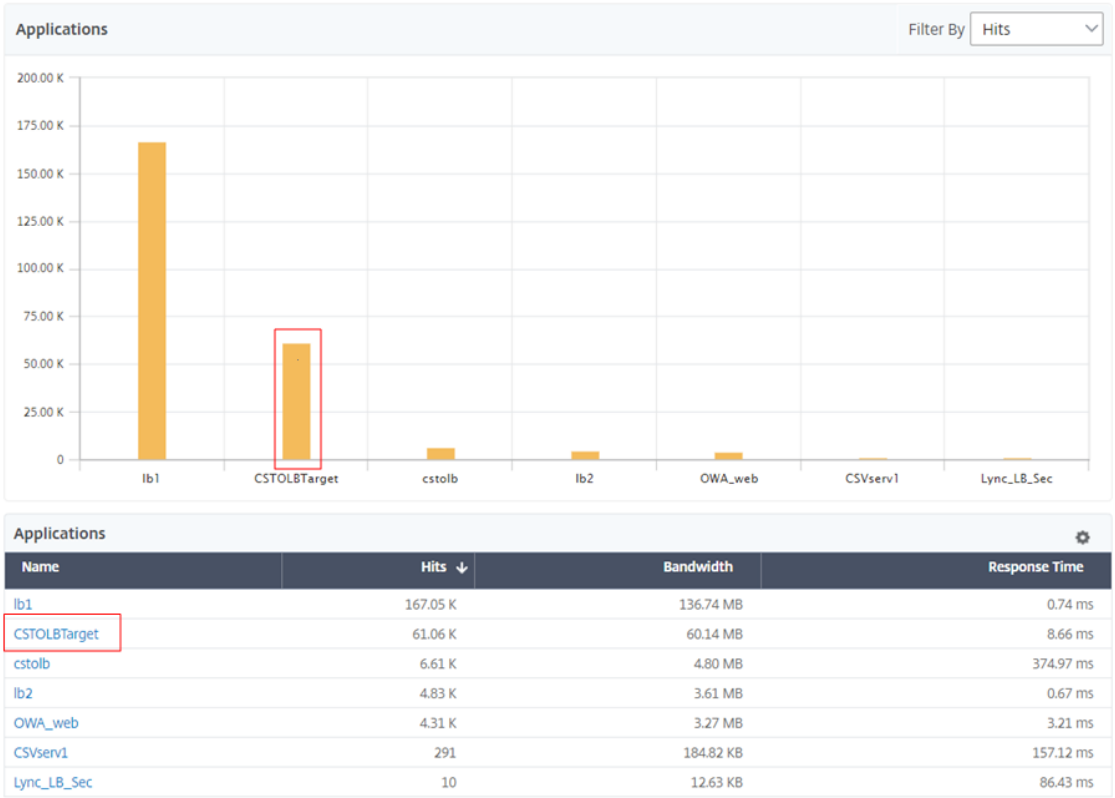
ユースケース **3-Web** アプリケーションへのアクセスが遅い

Windows ユーザー用の Web サーバーと Mac ユーザー用の Web サーバーがあり、ユーザーが Web アプリケーションへのアクセスが遅いと報告しているシナリオを考えてみましょう。管理者は、次のようなことを認識しているはずです。

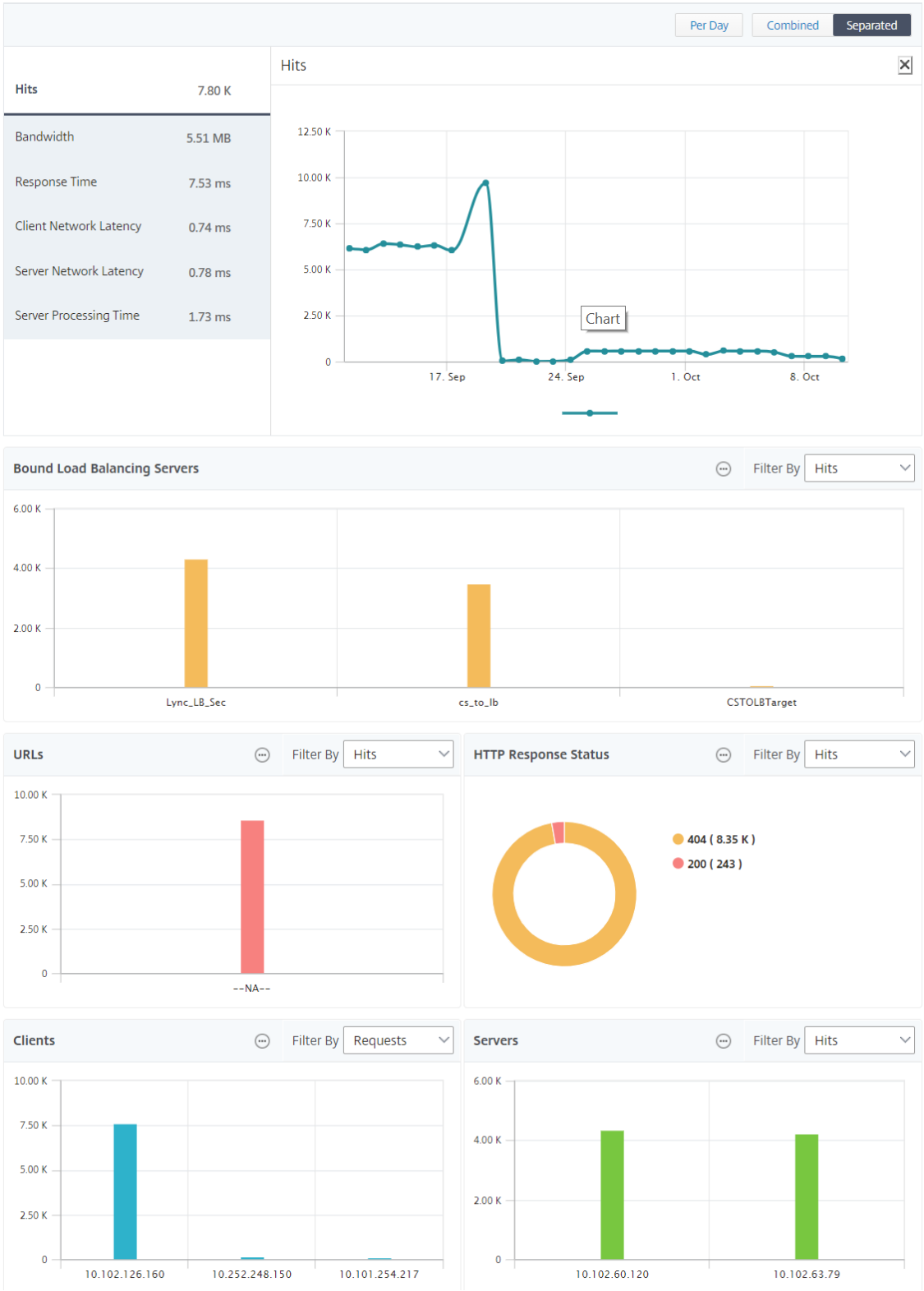
- Windows ユーザー用のコンテンツスイッチ仮想サーバーを構成しました。
- Mac ユーザー用のコンテンツスイッチング仮想サーバーを設定しました。
- Windows および Mac ユーザーに基づいてリクエストをリダイレクトするように、仮想サーバーにバインドされた関連サービスを構成しました。

Web アプリケーションの速度低下問題の根本原因を分析するには:

1. [分析] > [**Web** インサイト **] > [** アプリケーション**]** に移動します。
2. コンテンツスイッチング仮想サーバーを選択します。
   たとえば、イメージ内の「CSolbTarget」アプリケーションは、他の負荷分散仮想サーバーにバインドされたコンテンツスイッチング仮想サーバーです。



3. コンテンツスイッチング仮想サーバーをクリックして、他の負荷分散仮想サーバーを表示します。テーブル内のアプリケーション名をクリックすることもできます。



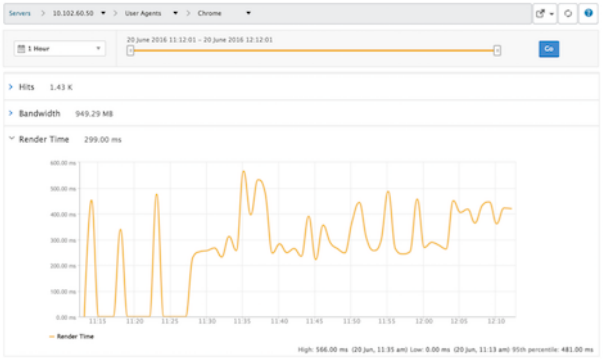
バインドされた負荷分散サーバーをクリックして、それらのアプリケーションの Web Insight の詳細を表示できます。

ブラウザとオペレーティングシステムのインサイトを分析

Web Insight を使用すると、L7 遅延の問題を分離して、モバイルデバイスの使用状況を理解できます。管理者にとって、この洞察は、ユーザーベース全体でさまざまなオペレーティングシステムが採用されていることを理解するのに役立ちます。

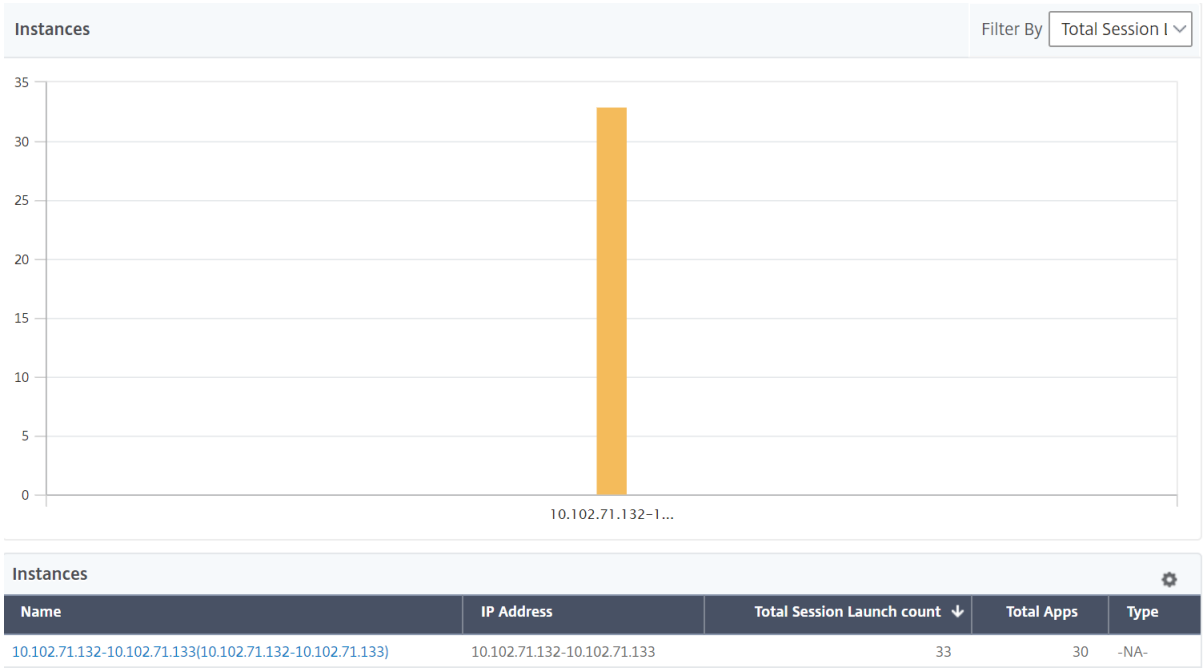
[**Analytics**] > [**Web Insight**] > [オペレーティングシステム] に移動して、ユーザーアクセスが遅くなる理由と、特定のブラウザー間の非互換性が原因であるかどうかを確認してください。また、特定のクライアントで使用されているオペレーティングシステムや、アクセスされているブラウザーを確認することもできます。さらには、さまざまなブラウザー間でレンダリング時間を比較したり、特定のブラウザーにドリルダウンし、そのブラウザーで最も高速にレンダリングされるアプリケーションページを確認したりできます。

たとえば、Google Chrome を選択し、特定のアプリケーションの URL ページごとに対応するレンダリング時間を確認できます。

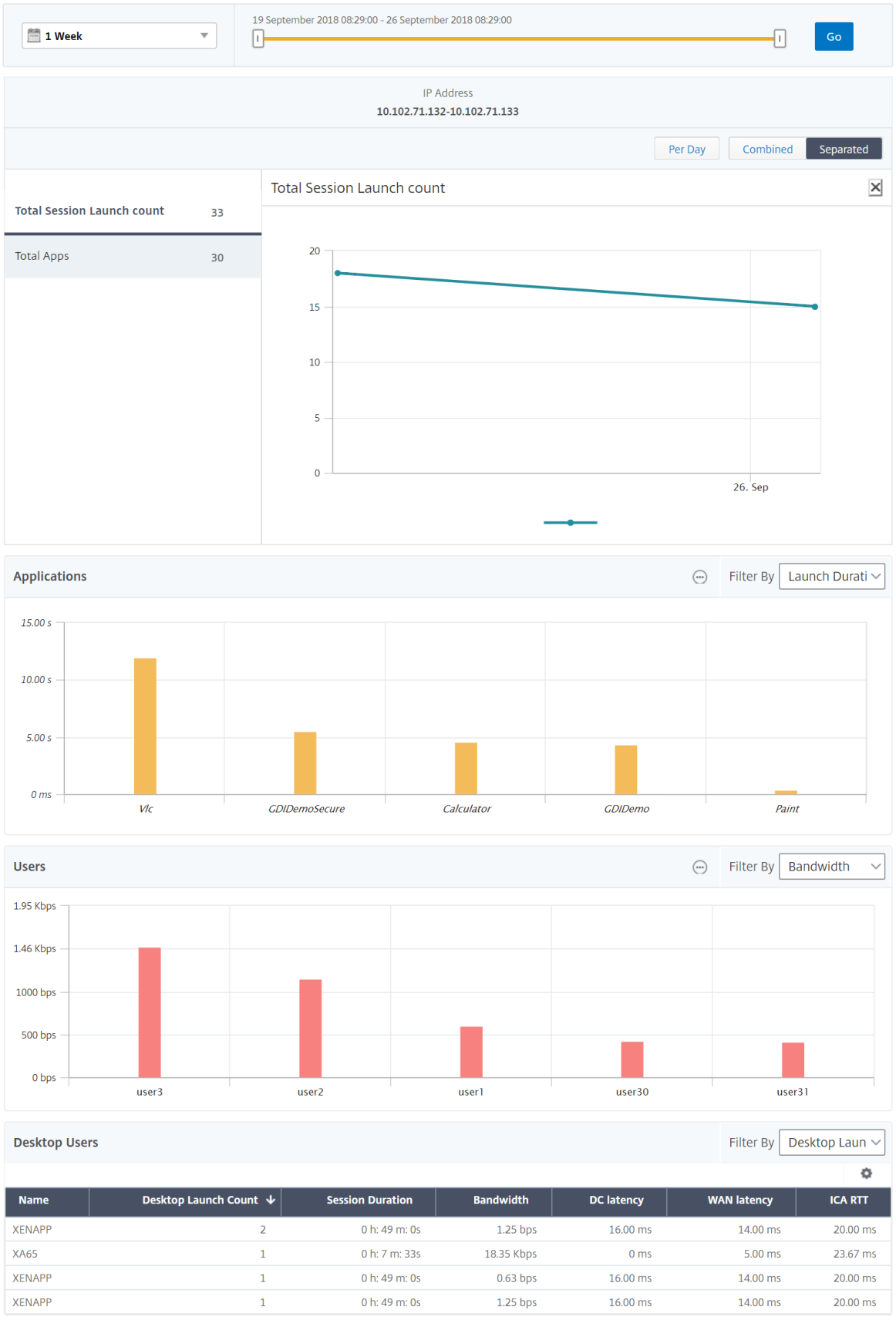


高可用性モードでデプロイされた **NetScaler ADC** インスタンス

Citrix ADM は、高可用性モードでデプロイされた ADC インスタンスのレポートを提供します。高可用性モードのインスタンスの集約レポートは、すべての分析でサポートされます。



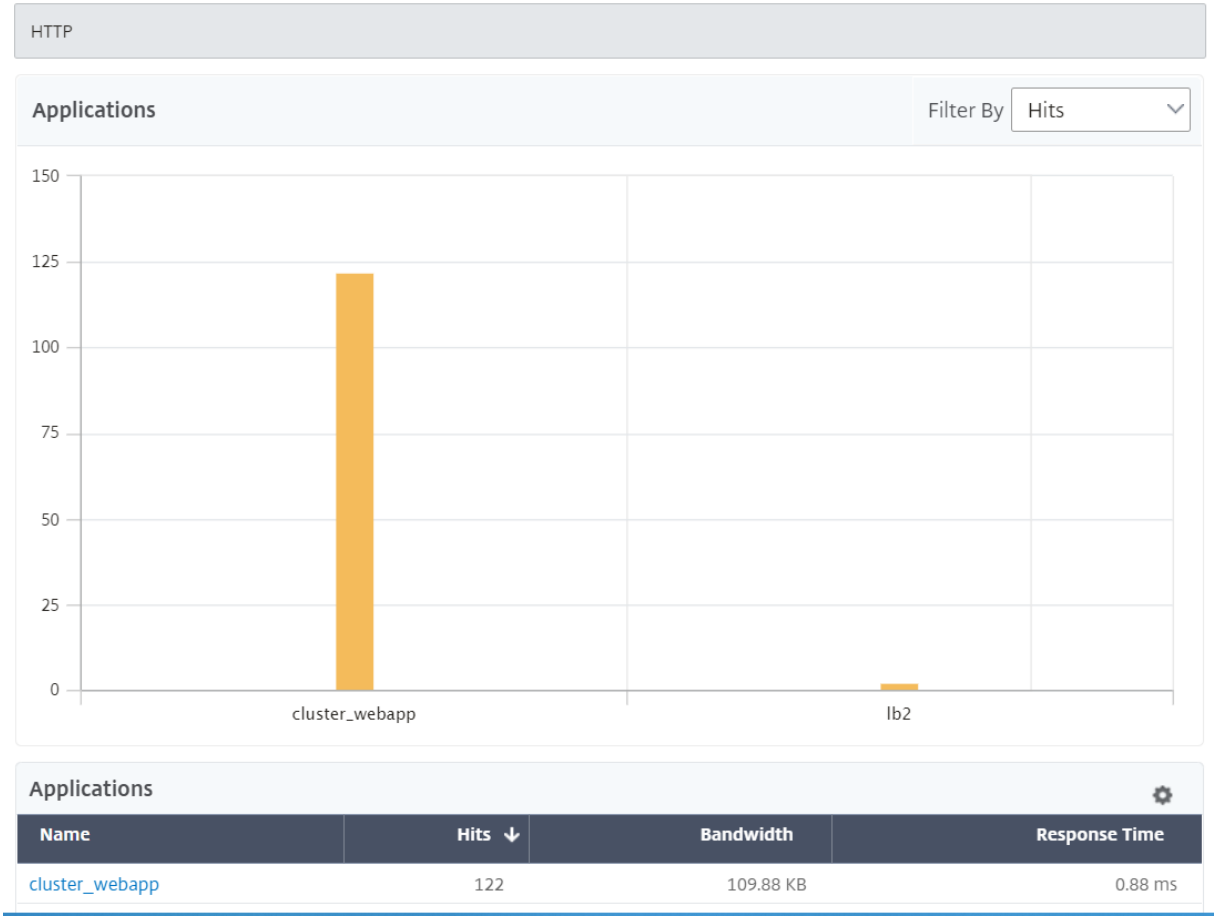
高可用性のインスタンスの名前をクリックすると、詳細が表示されます。



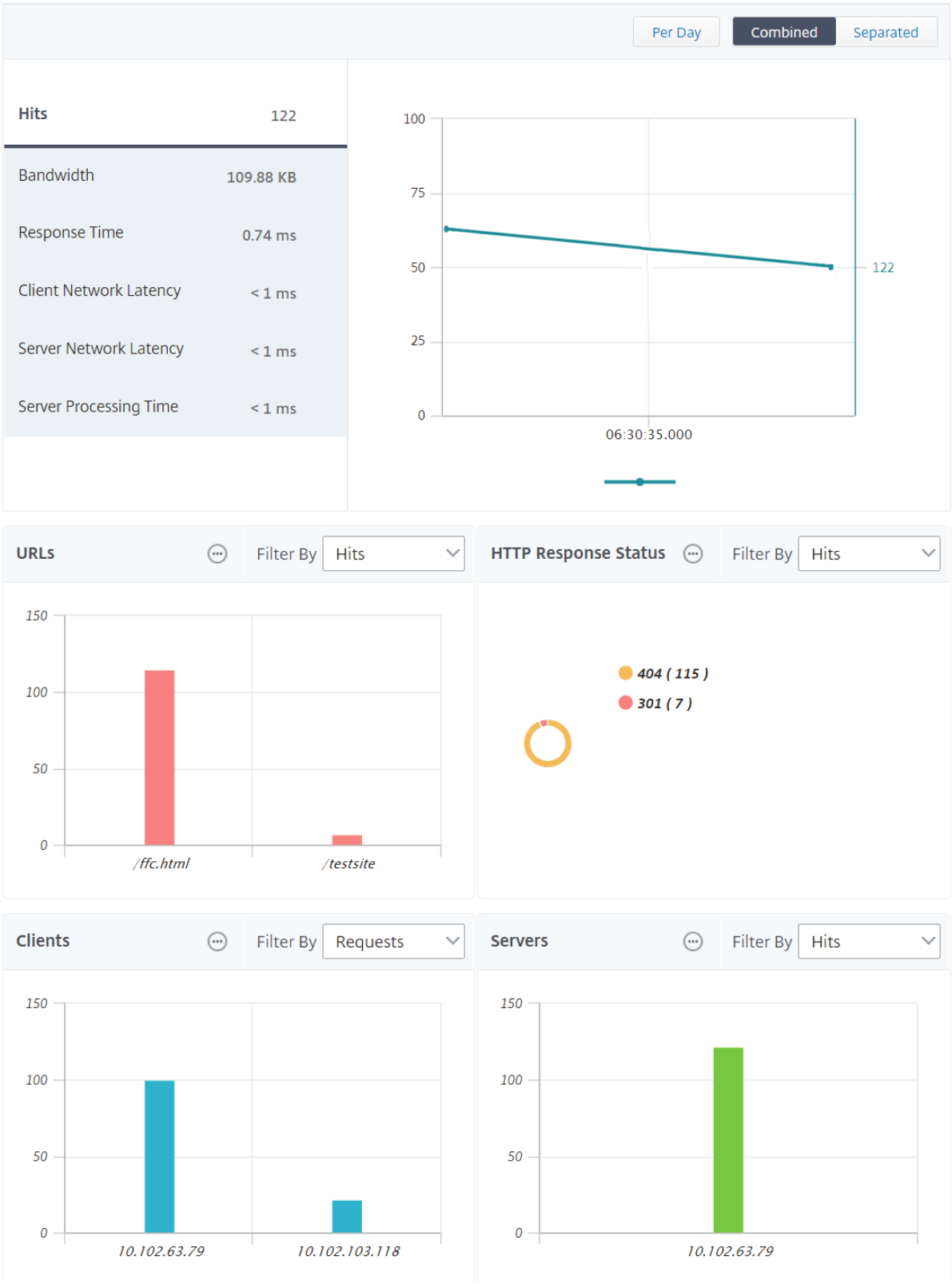
Name	Desktop Launch Count	Session Duration	Bandwidth	DC latency	WAN latency	ICA RTT
XENAPP	2	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms
XA65	1	0 h: 7 m: 33s	18.35 Kbps	0 ms	5.00 ms	23.67 ms
XENAPP	1	0 h: 49 m: 0s	0.63 bps	16.00 ms	14.00 ms	20.00 ms
XENAPP	1	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms

クラスターモードでデプロイされた **NetScaler ADC** インスタンス

Citrix ADM は、クラスターモードでデプロイされた ADC インスタンスのレポートを提供します。クラスターモードのインスタンスの集約レポートは、すべての分析でサポートされます。



CLIP ホスト名をクリックして、クラスターモードでデプロイされた ADC インスタンスに関するすべての詳細を表示することもできます。



> 注
>
> - Citrix ADM 12.1 ビルド 503.x にアップグレードする前に以前に収集されたすべてのデータは、データが保持されるまでの間、独立したレポートとして引き続き表示されます。
> - クラスタモードでデプロイされた ADC インスタンスの場合、オブザベーションドメイン ID/オブザベーションドメイン名は CLIP ホスト名と CLIP に置き換えられます。以前に収集されたすべてのデータは、引き続き観測ドメイン ID/観測ドメイン名を報告します。

Web インサイトジオマップ構成

NetScaler ADM ジオマップ機能は、マップ上の異なる地理的場所にわたる Web アプリケーションの使用状況を表示します。管理者は、この情報を使用して、アプリケーション使用率の傾向を把握し、容量計画を立てることができます。

Geomap は、国、州、都市に固有の以下の指標に関する情報を提供します。

- 合計ヒット数：アプリケーションがアクセスされた合計回数。
- 帯域幅: クライアント要求の処理中に消費された合計帯域幅
- 応答時間：クライアント要求への応答の送信に要した平均時間。

ジオマップは、次のようないくつかのユースケースに対応するために使用できる情報を提供します。

- アプリケーションにアクセスするクライアント数が最大であるリージョン
- 応答時間が最も長い地域
- 最も帯域幅を消費するリージョン

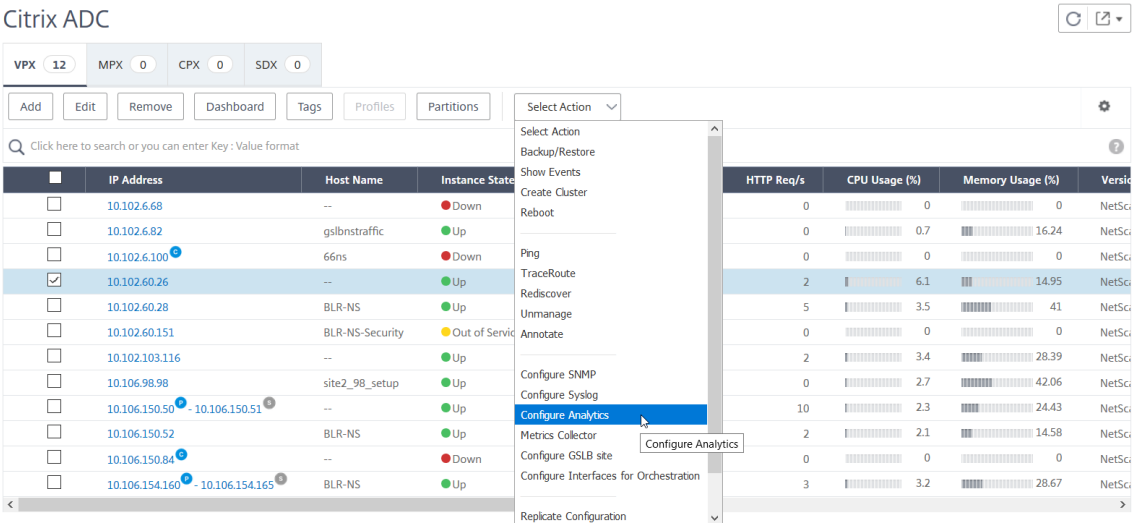
Citrix ADM には、プライベート IP アドレスまたはパブリック IP アドレスのジオマップを構成するオプションが用意されています。

プライベート **IP** アドレスのジオマップの構成

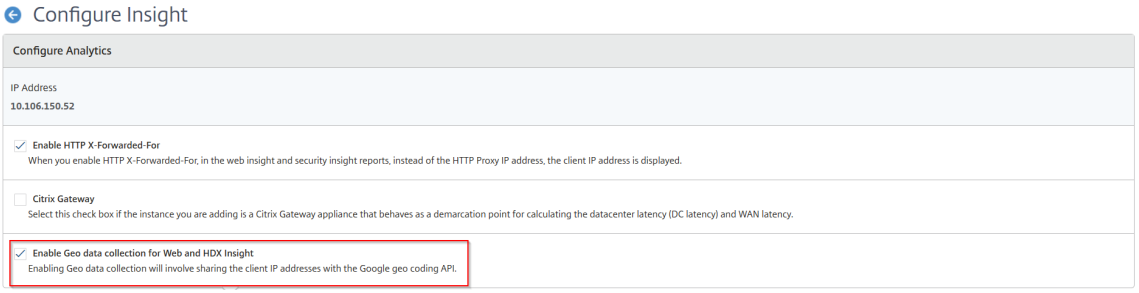
ジオマップ上のプライベート IP アドレスから発信された Web アプリケーションのトラフィックを表示するには、まずプライベート IP アドレスブロックを作成し、次に geo データ収集を有効にする必要があります。

地理データ収集を有効にするには：

1. [ネットワーク] > **[**** インスタンス**] > [**Citrix ADC**] に移動し、Citrix ADC インスタンスを選択します。
2. **[** アクションの選択] リストから、[**Analytics** の設定] を選択します。



3. [**Insight** の構成] ページで、[**Web** および **HDX Insight** の地域データ収集を有効にする] を選択します。



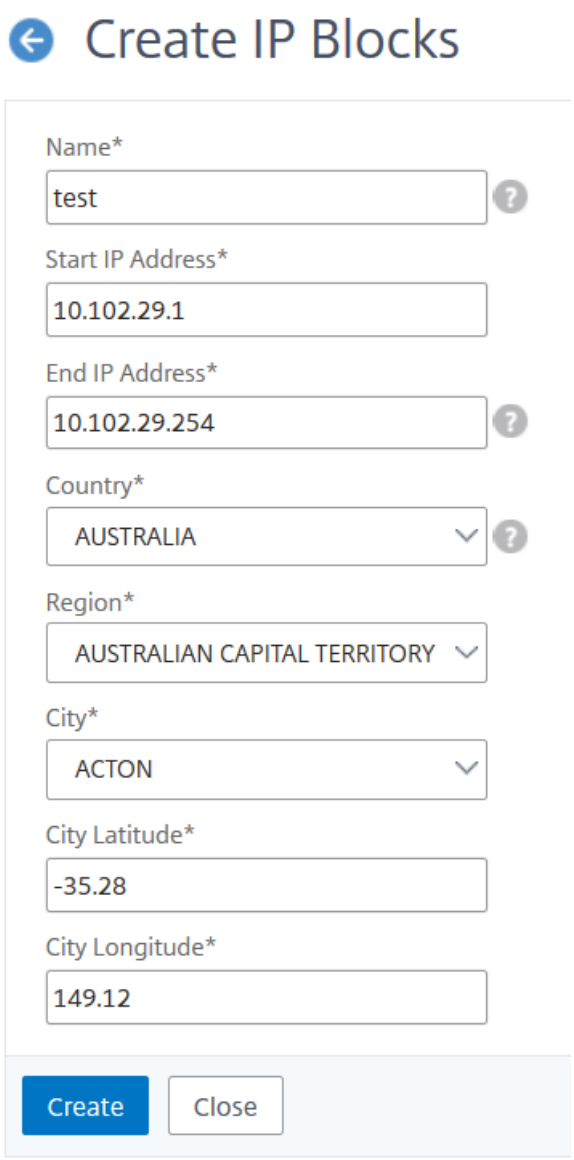
プライベート **IP** ブロックを作成する　NetScaler ADM は、クライアントのプライベート IP アドレスが NetScaler ADM サーバーに追加されると、クライアントの場所を認識できます。たとえば、クライアントの IP アドレスが A 市に関連付けられたプライベート IP アドレスブロックの範囲内にある場合、NetScaler ADM はこのクライアントの A 市町からトラフィックが発信していることを認識します。

IP ブロックを作成するには、次の手順を実行します。

1. Citrix ADM で、[分析] > [設定] > [**IP** ブロック] に移動し、[追加] をクリックします。
2. [**IP** ブロックの作成] ページで、次のパラメータを指定します。
    - 名前。プライベート IP ブロックの名前を指定してください
    - **IP** アドレスを開始します。IP ブロックの最下位 IP アドレス範囲を指定します。
    - 終了 **IP** アドレス。IP ブロックの最大の IP アドレス範囲を指定します。
    - カントリー。リストから国を選択します。
    - 地域。国に基づいて地域は自動入力されますが、地域を選択できます。
    - 市。地域に基づいて都市は自動入力されますが、都市を選択できます。

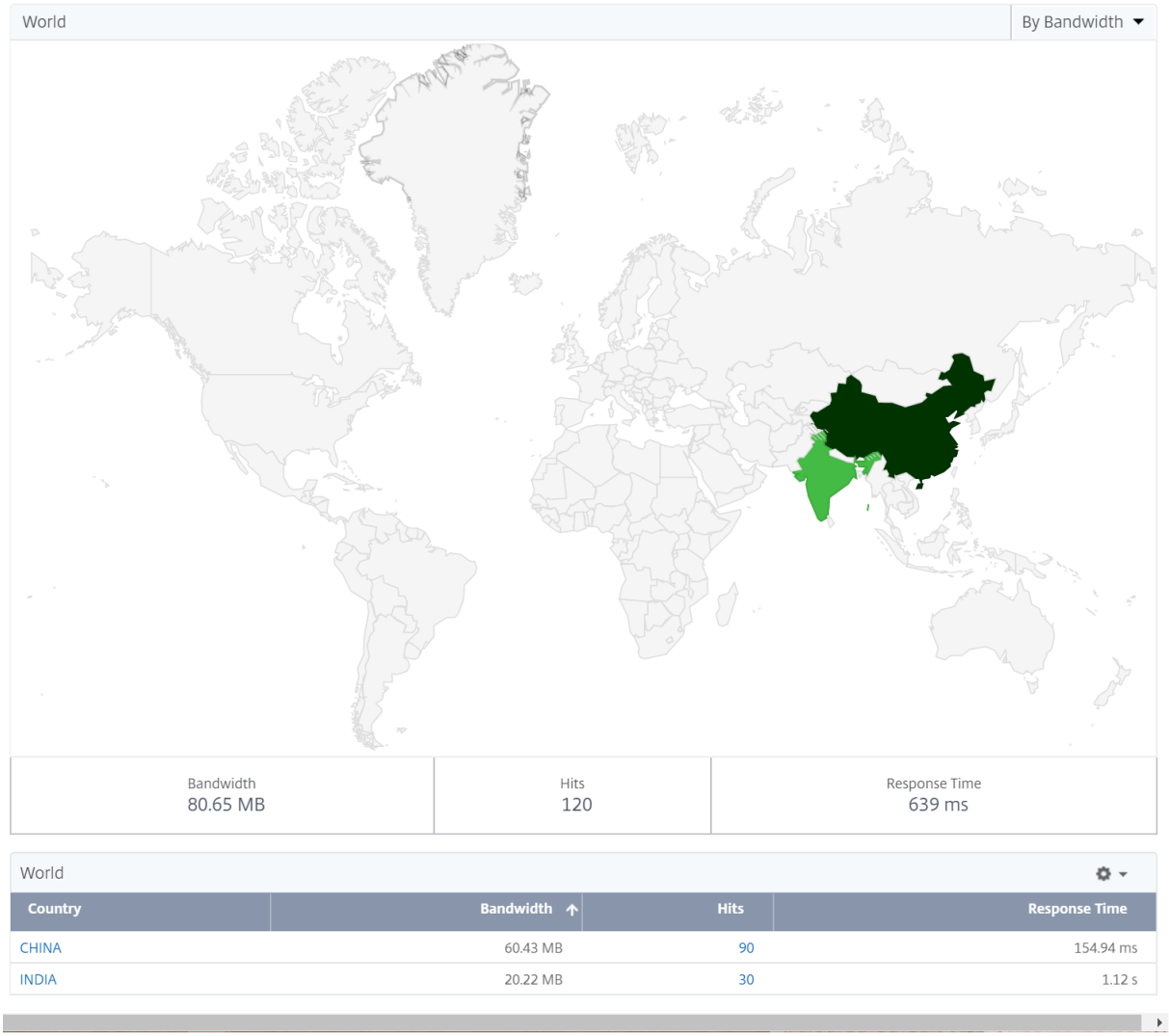
- ** 都市の緯度と都市の経度 **。選択した都市に基づいて、緯度と経度が自動的に入力されます。

3. [**Create**] をクリックすると、作業が終了します。



パブリック **IP** ブロック　Citrix ADM は、クライアントがパブリック IP アドレスを使用している場合、クライアントの場所を認識することもできます。NetScaler ADM には組み込みの場所 CSV ファイルがあり、これはクライアントの IP アドレス範囲に基づいて場所と一致します。パブリック IP ブロックを使用する場合、唯一の要件は、[Configure Insight] ページから geo データ収集を有効化する必要があることです。

> 注
>
> NetScaler ADM では、特定の地理的位置のジオマップを表示するためにインターネット接続が必要です。GeoMap を.pdf、.png、または.jpg 形式でエクスポートするには、インターネット接続も必要です。



このダッシュボードのレポートをエクスポートするには、次の手順に従います。

このページのレポートをエクスポートするには、このページの右上にある エクスポート アイコンをクリックします。[エクスポート] ページでは、次のいずれかの操作を実行できます:

1. [今すぐエクスポート] タブを選択します。レポートを PDF、JPEG、PNG、または CSV 形式で表示して保存します。
2. [スケジュールエクスポート] タブを選択します。レポートを毎日、毎週、または毎月スケジュールして、メールまたはスラックメッセージでレポートを送信します。

> 注
>
> - [毎週 の繰り返し] を選択した場合は、レポートをスケジュールする平日を選択してください。
> - [毎月の繰り返し] を選択した場合は、レポートをスケジュールするすべての日をカンマで区切って入力します。

しきい値の構成

しきい値を作成して、しきい値を超えるたびに通知を受け取ることができます。一般的な導入環境では、しきい値を次のように設定できます。

- さまざまなアプリケーションメトリックをトラッキング
- 計画を促進
- アプリケーションの指標値が設定されたしきい値を超えると通知を受け取る

しきい値を設定するには:

1. [アナリティクス] > [設定] > [しきい値] に移動します。
2. 「しきい値」ページで、「追加」をクリックします。

   「しきい値の作成」ページが表示されます。
3. 次の詳細を指定します:

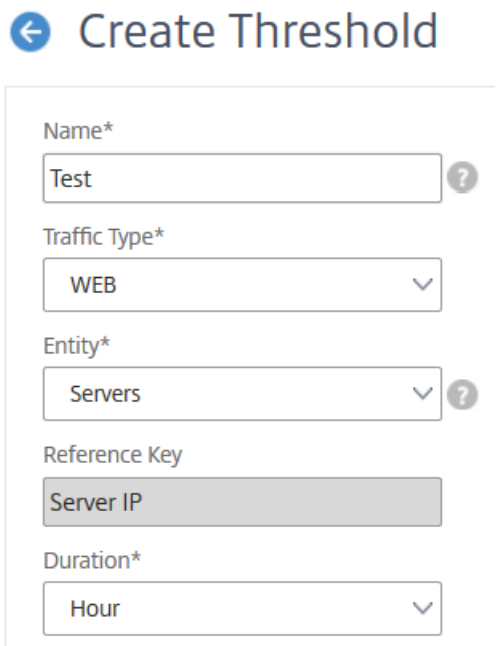
   a) 名前-イベントを作成する名前を指定します。

   b) トラフィックタイプ-リストから [WEB] を選択します。

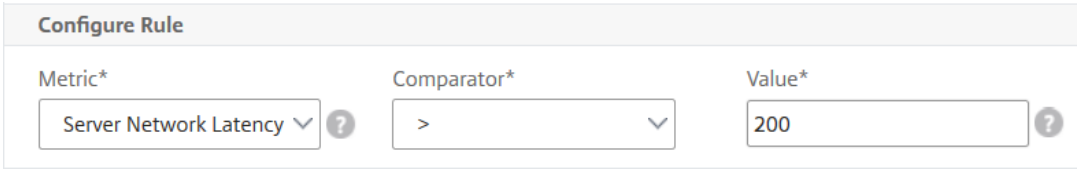
   c) エンティティ -リストから、カテゴリまたはリソース・タイプを選択します。デフォルトでは、「アプリケーション」がエンティティとして選択されます。

   d) 参照キー -参照キーは、選択したトラフィックタイプとエンティティに基づいて自動的に生成されます。

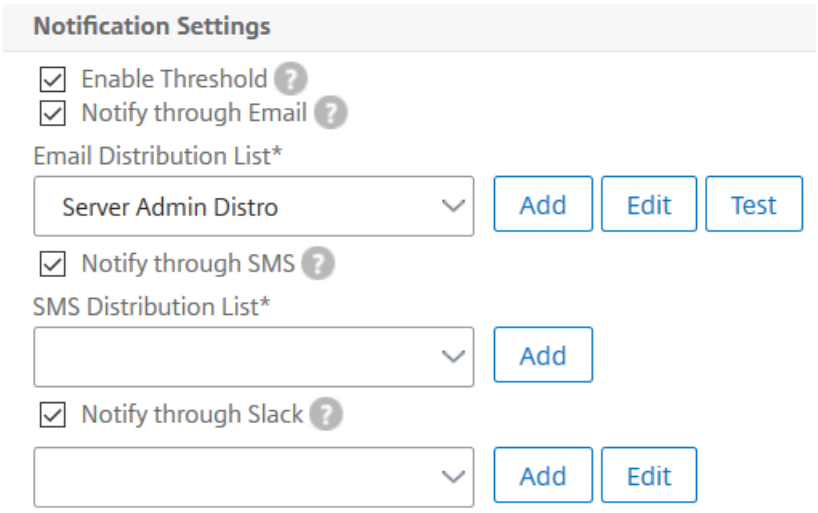
   e) 期間-一覧から、エンティティを監視する時間間隔を選択します。エンティティは、1 時間、1 日、または 1 週間の期間を監視できます。



f) [**Configure Rule**] セクションで、メトリック、必要なコンパレータを選択してルールを作成し、しきい値を指定します。



g) [通知の設定] セクションで、[しきい値の有効化] を選択し、アラートを取得するアラート・モードを選択します。



4. [作成] をクリックします。

HDX Insight

February 6, 2024

HDX Insight は、NetScaler ADC を通過する Citrix Virtual Apps and Desktops への HDX トラフィックのエンドツーエンドの可視性を提供します。管理者は、HDX Insight を通じて、リアルタイムのクライアントとネットワークの遅延測定基準、履歴レポート、エンドツーエンドのパフォーマンスデータを確認し、パフォーマンスの問題をトラブルシューティングできます。リアルタイムの可視性と履歴データの両方を利用できるため、NetScaler Application Delivery Management（ADM）はさまざまなユースケースをサポートできます。

データを表示するには、Citrix Gateway 仮想サーバーで AppFlow を有効にする必要があります。AppFlow は、IPFIX プロトコルまたは LogStream メソッドによって配信することができます。

> 注:ICA ラウンドトリップ時間の計算を記録できるようにするには、次のポリシー設定を有効にします:

- ICA 往復計算

- ICA ラウンドトリップ計算間隔
- アイドル接続の ICA 往復計算

個々のユーザーをクリックすると、選択した期間内に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）が表示されます。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のマッピングなど、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。

「**HDX Insight** 」>「アプリケーション」の順に選択し、「起動期間」をクリックして、アプリケーションの起動に要した時間を表示することもできます。**HDX Insight-**Users に移動して、接続しているすべて のユーザーのユーザーエージェントを表示することもできます。

> 注：HDX Insight は、ソフトウェアバージョン 12.0 で実行されている NetScaler ADC インスタンスで構成された管理パーティションをサポートしています。

次のシンクライアントが HDX Insight をサポートしています。

- WYSE Windows ベースのシンクライアント
- WYSE Linux ベースのシンクライアント
- WYSE Thinos ベースのシンクライアント
- 10Zig Ubuntu ベースのシンクライアント

パフォーマンス遅延問題の根本原因の特定

シナリオ **1**

ユーザーが Citrix Virtual Apps and Desktops にアクセスする際に遅延が発生しています。

遅延の原因として考えられるのは、サーバーネットワークの遅延、サーバーネットワークに起因する ICA トラフィックの遅延、またはクライアントネットワークの遅延です。

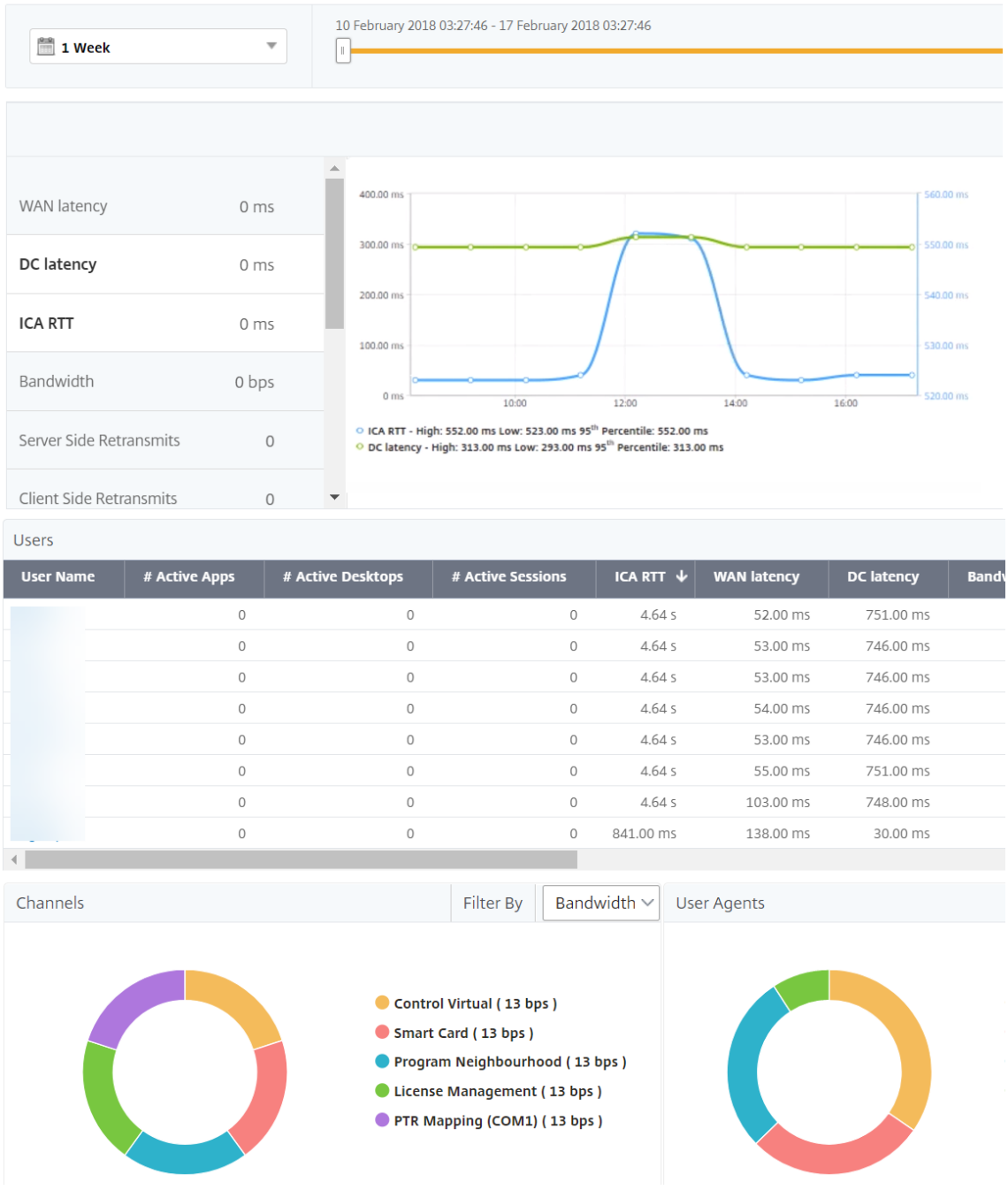
問題の根本原因を特定するために、次の測定基準を分析します。

- WAN 遅延
- DC の遅延
- ホストの遅延

クライアント・メトリックを表示する手順は、次のとおりです。

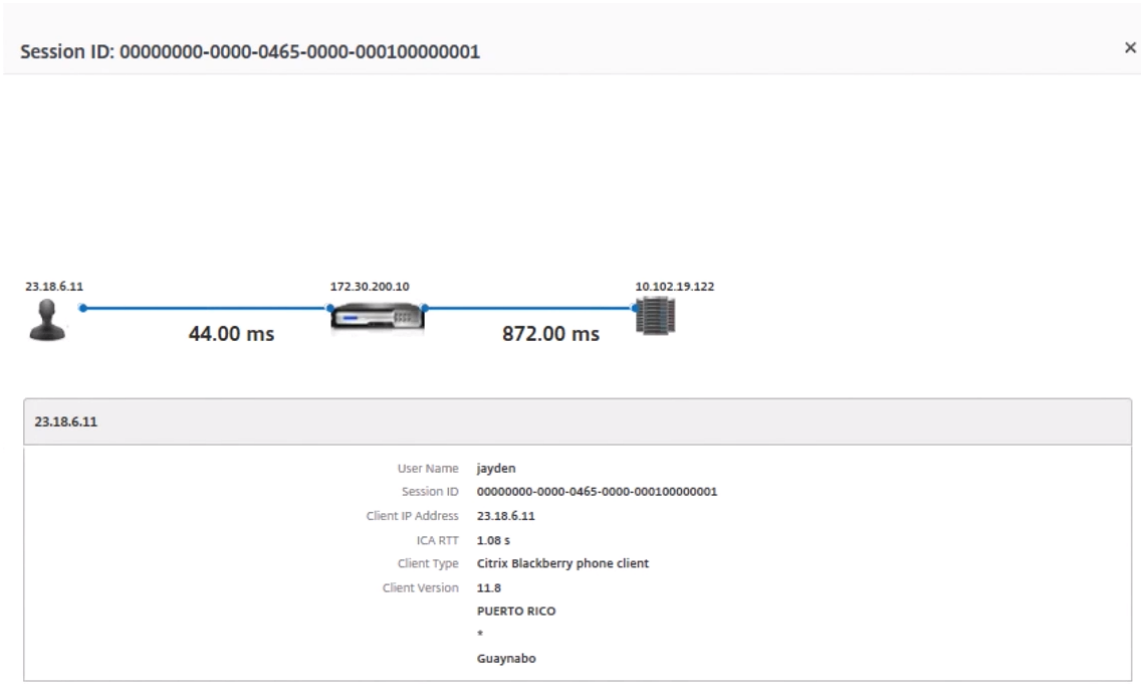
1. [**Analytics**] タブで、[**HDX Insight**] > [ユーザー] に移動します。
2. 下にスクロールして、ユーザー名を選択し、リストから期間を選択します。期間は、1 日、1 週間、1 か月にすることができます。また、データを表示する期間をカスタマイズすることもできます。

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**

Citrix Virtual Apps またはデスクトップでアプリケーションを起動する際に遅延が発生する

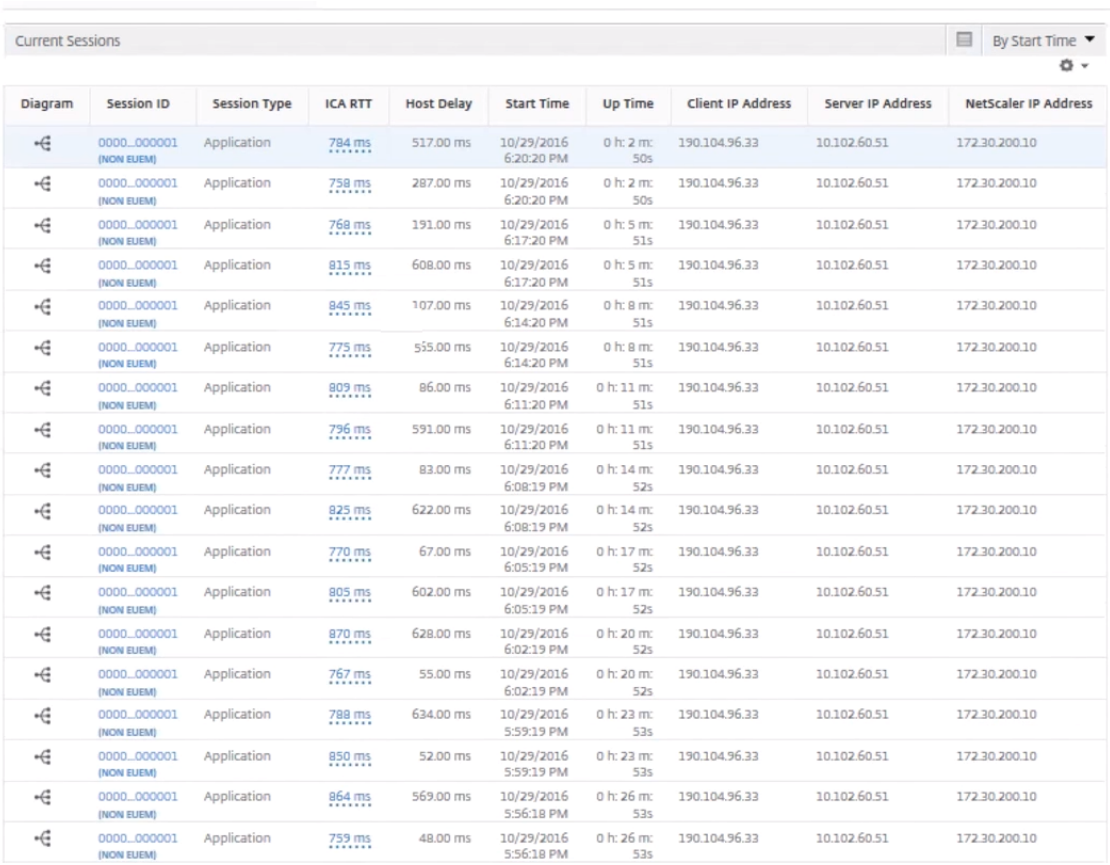
遅延の原因として考えられるのは、サーバーネットワークの遅延、サーバーネットワークに起因する ICA トラフィックの遅延、クライアントネットワークの遅延、またはアプリケーションの起動にかかる時間です。

問題の根本原因を特定するために、次の測定基準を分析します。

- WAN 遅延
- DC 遅延
- ホスト遅延

ユーザー・メトリックを表示する手順は、次のとおりです。

1. ［分析］タブで、［**HDX Insight** ］>［ユーザー］に移動します。
2. 下にスクロールして、該当するユーザー名をクリックします。
3. グラフに示されている該当するセッションの WAN の遅延、DC の遅延、RTT の値を書き留めます。
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 Citrix ADM を使用している場合、HDX Insight は WAN ジッターやサーバー側再送信などの追加のユーザーメトリックも表示します。これらの指標を表示するには、**[**Analytics**] > [HDX Insight**] > [ユーザー]** の順に選択し、ユーザー名を選択します。ユーザーの測定基準がグラフの隣の表に表示されます。

HDX Insight 用ジオマップ

Citrix ADM Geomaps 機能は、地理的に異なる場所でのアプリケーションの使用状況を地図上に表示します。この情報を使用して、管理者は、さまざまな地理的な場所でのアプリケーション使用状況の傾向を把握できます。

特定の地理的場所または LAN のジオマップを表示するように Citrix ADM を構成するには、その場所のプライベート IP 範囲（開始 IP アドレスと終了 IP アドレス）を指定します。

HDX Insight でジオロケーションマップから履歴とアクティブなユーザーの詳細も表示できます。[分析] > [**HDX Insight**] に移動し、マップの [世界] セクションで、詳細を確認したい国または地域をクリックします。更に情報を表示するために、市と州でドリルダウンすることができます。

データセンターの **geomap** を設定するには、次の手順に従います。

[**Analytics**] タブで、[設定] > [**IP** ブロック] に移動し、特定の場所のジオマップを設定します。

使用例

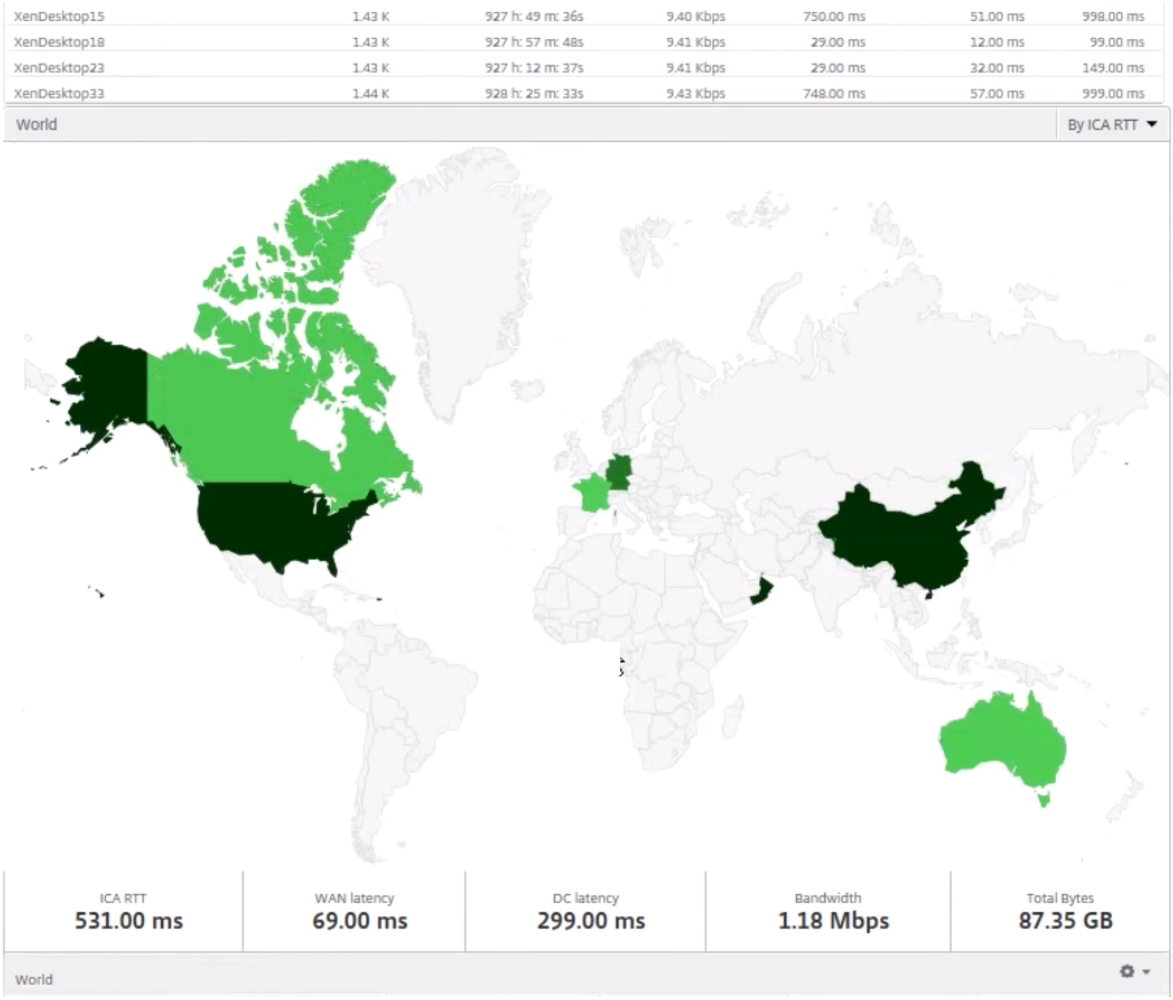
このシナリオでは 2 つのブランチオフィスを持つ ABC という名前の企業を扱います。ABC はサンタクララとインドにブランチオフィスがあります。

サンタクララのユーザーは、Sclara.x.com の Citrix Gateway アプライアンスを使用して VPN トラフィックにアクセスします。インドのユーザーは、India.x.com の Citrix Gateway アプライアンスを使用して VPN トラフィックにアクセスします。

サンタクララでは、午前 10 時から午後 5 時などの特定の時間帯に SClara.x.com に接続し、VPN トラフィックにアクセスします。ほとんどのユーザーは同じ NetScaler Gateway にアクセスするため、VPN への接続に遅延が生じます。そのため、一部のユーザーは Sclara.x.com ではなく India.x.com に接続します。

トラフィックを分析する NetScaler ADC 管理者は、ジオマップ機能を使用して、サンタクララオフィスのトラフィックを表示できます。このマップから、サンタクララオフィスの応答時間が非常に長いことがわかります。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 Citrix 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

Citrix ADC インスタンスにエンタープライズ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、Citrix ADM for HDX Insight に設定されたしきい値はトリガーされません。

HDX Insight データ収集の有効化

February 6, 2024

HDX Insight は、NetScaler ADC インスタンスまたは Citrix SD-WAN アプライアンスを通過する ICA トラフィックをこれまでにないエンドツーエンドで可視化することで、NetScaler Application Delivery Management

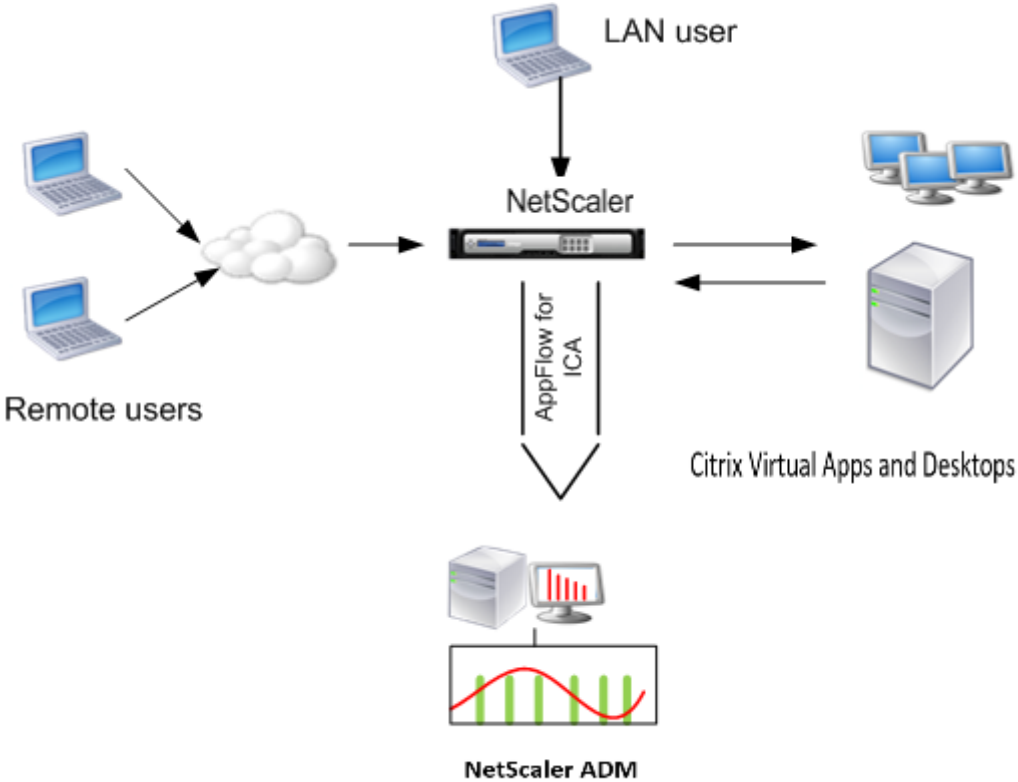
(ADM) Analytics が卓越したユーザーエクスペリエンスを提供できるようにします。HDX Insight は、ネットワーク、仮想デスクトップ、アプリケーション、アプリケーションファブリック向けの優秀かつ有能なビジネスインテリジェンスとエラー分析機能を提供します。HDX Insight はユーザーの問題を優先度によってすぐに選別すると同時に、仮想デスクトップ接続に関するデータを収集し、AppFlow レコードを生成して、それらをビジュアルレポートとして提示します。

NetScaler ADC でデータ収集を有効にする構成は、導入トポロジーにおけるアプライアンスの位置によって異なります。

LAN ユーザーモードで展開された Citrix ADC を監視するためのデータ収集の有効化

Citrix Virtual Apps and Desktops アプリケーションにアクセスする外部ユーザーは、Citrix Gateway で自分自身を認証する必要があります。ただし、内部ユーザーは NetScaler Gateway にリダイレクトする必要がない場合があります。また、透過モードの展開では、管理者が手動でルーティングポリシーを適用して、要求が NetScaler ADC アプライアンスにリダイレクトされるようにする必要があります。

これらの課題を克服し、LAN ユーザーが Citrix Virtual 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。



> 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 Citrix ADC アプライアンスを監視するには、まず Citrix ADC アプライアンスを NetScaler Insight インベントリに追加し、AppFlow を有効にしてから、ダッシュボードにレポートを表示します。

NetScaler ADC アプライアンスを NetScaler ADM インベントリに追加した後、データ収集のために AppFlow を有効にする必要があります。

> 注
>
> - ADC インスタンスでは、[システム] > [**AppFlow**] > [コレクター] に移動して、コレクター（つまり、Citrix ADM）が稼働しているかどうかを確認できます。NetScaler ADC インスタンスは、NSIP を使用して AppFlow レコードを NetScaler ADM に送信します。ただし、インスタンスは SNIP を使用して NetScaler ADM との接続を確認します。そのため、SNIP がインスタンスに設定されていることを確認してください。
> - NetScaler ADM 構成ユーティリティを使用して、LAN ユーザーモードで展開された NetScaler ADC でデータ収集を有効にすることはできません。
> - コマンドとその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 ADC** アプライアンスでデータ収集を構成するには：

コマンドプロンプトで、次の操作を行います：

1. アプライアンスにログオンします。
2. プロキシ IP およびポートを指定してフォワードプロキシキャッシュリダイレクト仮想サーバーを追加します。また、サービスタイプとして HDX を指定します。

   add cr vserver <name> <servicetype> [<ipaddress> <port>] [-cacheType <cachetype>] [- cltTimeout <secs>]

   例

   ```
   add cr vserver cr1 HDX 10.12.2.2 443  -cacheType FORWARD  -
      cltTimeout 180
   <!--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 or OFF)]

   add vpn trafficPolicy <name> <rule> <action>

   例

   ```
   add vpn trafficAction act1 tcp -HDX ON

   add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
   <!--NeedCopy-->
   ```


3. NetScaler ADM を NetScaler ADC アプライアンスの 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
   <!--NeedCopy-->
   ```

4. AppFlow アクションを作成して、コレクターを関連付けます。

   add appflow action <name> **-collectors** <string> …

   例:

   ```
   add appflow action act -collectors MyInsight
   <!--NeedCopy-->
   ```

5. トラフィック生成の規則を指定するための AppFlow ポリシーを作成します。

   add appflow policy <policyname> <rule> <action>

   例:

   ```
   add appflow policy pol true act
   <!--NeedCopy-->
   ```

6. グローバルバインドポートに AppFlow ポリシーをバインドします。

   bind appflow global <policyname> <priority> **-type** <type>

   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、タイプの値を ICA_REQ_OVERRIDE または ICA_REQ_DEFAULT にする必要があります。

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:

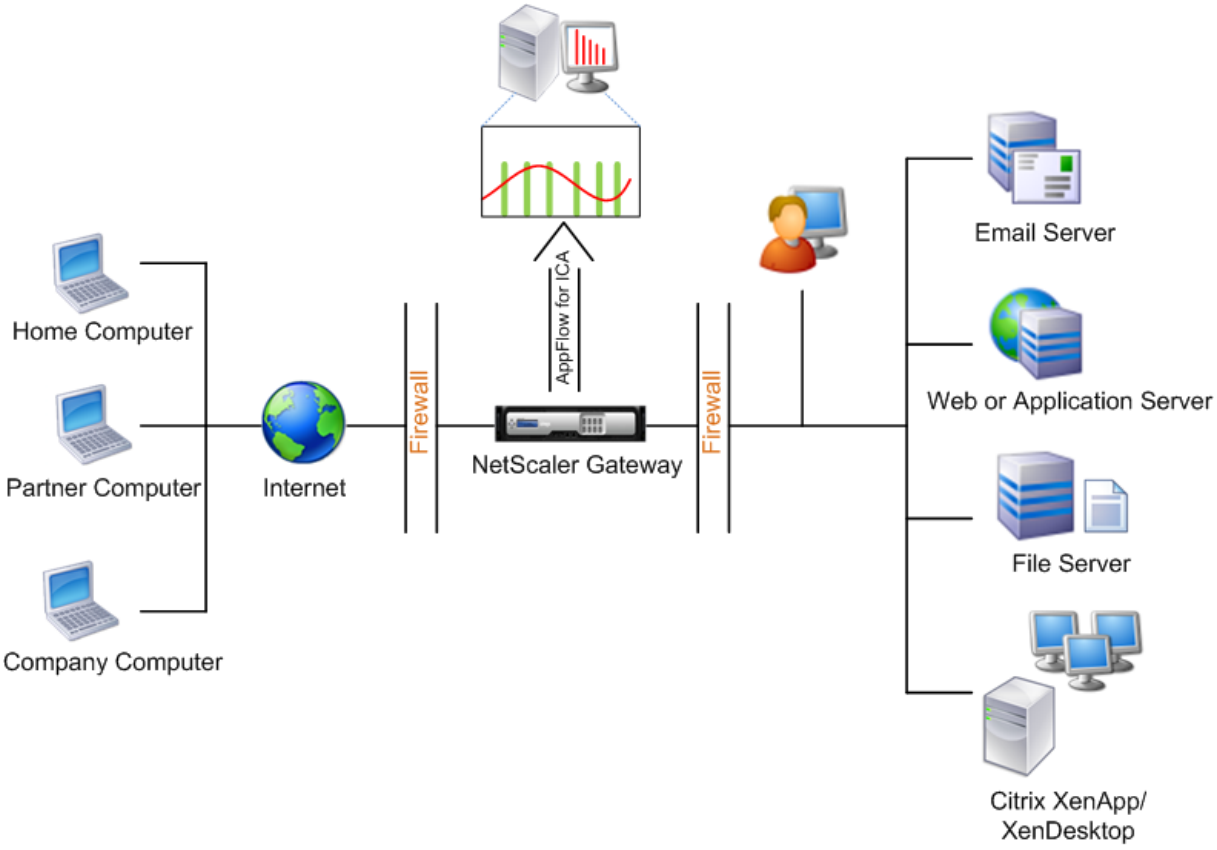
   ```
   set appflow param -flowRecordInterval 60
   <!--NeedCopy-->
   ```

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 **Citrix 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、ユーザーは仮想プライベートネットワーク（VPN）を介して NetScaler ADC アプライアンスにアクセスします。

レポートの収集を開始するには、NetScaler Gateway アプライアンスを Citrix Application Delivery Management（ADM）インベントリに追加し、ADM で AppFlow を有効にする必要があります。



NetScaler ADM から **AppFlow** 機能を有効にするには:

1. Web ブラウザで、Citrix ADM IP アドレス（例: http://192.168.100.1）を入力します。
2. [**User Name**] と [**Password**] に管理者の資格情報を入力します。
3. [ネットワーク] > [インスタンス] に移動し、分析を有効にする NetScaler ADC インスタンスを選択します。
4. 「アクションの選択」ドロップダウンから、「**Analytics** の設定」を選択します。
5. 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。
6. 「**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。

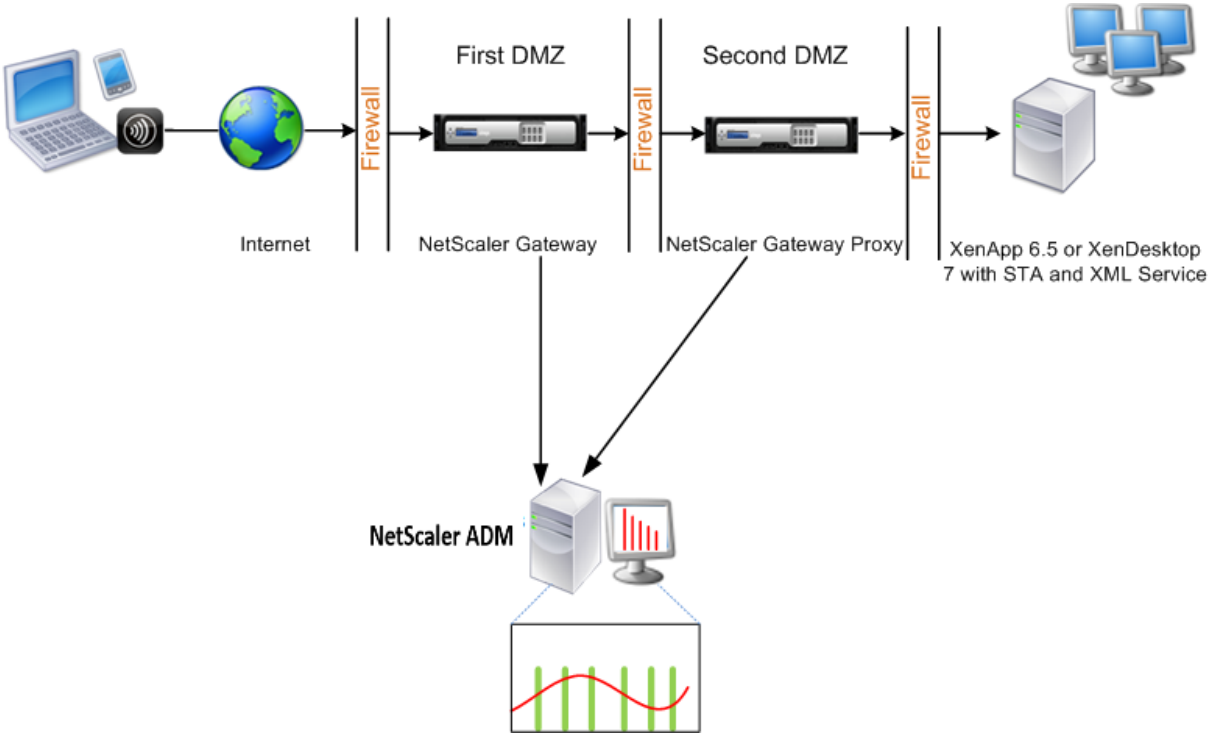
7. [**OK**] をクリックします。

> 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>
> - アプリフローアクションを追加 \ <name\ > -コレクター \ <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。

ダブルホップモードで展開された **Citrix Gateway** アプライアンスのデータ収集を有効にする

NetScaler Gateway のダブルホップモードでは、攻撃者が複数のセキュリティゾーンまたは非武装地帯（DMZ）に侵入してセキュアネットワークのサーバーに到達する必要があるため、組織の内部ネットワークをさらに保護できます。ICA 接続が通過するホップ（NetScaler Gateway アプライアンス）の数と、各 TCP 接続のレイテンシーの詳細と、クライアントが認識する ICA レイテンシーの合計とどのようにフェア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、内部ネットワーク内のサーバーへのアクセスを制御します。

2 つ目の DMZ の NetScaler Gateway は、NetScaler Gateway プロキシデバイスとして機能します。この NetScaler Gateway により、ICA トラフィックが 2 番目の DMZ を通過して、サーバーファームへのユーザー接続を完了できます。

NetScaler ADM は、最初の DMZ の NetScaler Gateway アプライアンスに属するサブネットか、2 番目の DMZ の NetScaler Gateway アプライアンスに属するサブネットのいずれかに展開できます。上の画像では、最初の DMZ の NetScaler ADM と NetScaler Gateway が同じサブネットにデプロイされています。

ダブルホップモードでは、NetScaler ADM は 1 つのアプライアンスから TCP レコードを、もう 1 つのアプライアンスから ICA レコードを収集します。Citrix Gateway アプライアンスを Citrix ADM インベントリに追加してデータ収集を有効にすると、各アプライアンスはホップカウントと接続チェーン ID を追跡してレポートをエクスポートします。

NetScaler ADM がレコードをエクスポートするアプライアンスを識別するために、各アプライアンスはホップ数で指定され、各接続は接続チェーン ID で指定されます。ホップカウントは、トラフィックがクライアントからサーバーに流れる NetScaler Gateway アプライアンスの数を表します。接続チェーン ID は、クライアントとサーバー間のエンドツーエンド接続を表します。

NetScaler ADM は、ホップカウントと接続チェーン ID を使用して、両方の NetScaler Gateway アプライアンスからのデータを相互に関連付け、レポートを生成します。

このモードで展開された Citrix Gateway アプライアンスを監視するには、まず Citrix Gateway を Citrix ADM イ

ンベントリに追加し、Citrix ADM で AppFlow を有効にしてから、Citrix 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。このような状況を解決するには、最初の Citrix Gateway アプライアンスの 1 つで AppFlow for ICA を有効にし、次に 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。この作業を行うことにより、一方のアプライアンスは ICA AppFlow レコードをエクスポートし、もう一方のアプライアンスは TCP AppFlow レコードをエクスポートします。これにより、ICA トラフィックを解析するときの処理時間も短縮されます。

NetScaler ADM から **AppFlow** 機能を有効にするには:

1. Web ブラウザで、Citrix ADM IP アドレス（例：http://192.168.100.1）を入力します。
2. ［**User Name**］と ［**Password**］に管理者の資格情報を入力します。
3. [ネットワーク] > [インスタンス] に移動し、分析を有効にする NetScaler ADC インスタンスを選択します。
4. 「アクションの選択」ドロップダウンから、「**Analytics** の設定」を選択します。
5. 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。
6. 「**AppFlow** を有効にする」フィールドに「**true**」と入力し、ICA トラフィック用の **ICA/TCP** 、TCP トラフィック用の ICA/TCP をそれぞれ選択します。

   > 注： Citrix ADC アプライアンスの各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、Citrix ADM ダッシュボードにはレコードが表示されません。

7. ［**OK**］をクリックします。

データをエクスポートするための **NetScaler Gateway** アプライアンスの設定

NetScaler Gateway アプライアンスをインストールした後、NetScaler Gateway アプライアンスで次の設定を構成して、レポートを NetScaler ADM にエクスポートする必要があります。

- 第 1 および第 2 の DMZ にある NetScaler Gateway アプライアンスの仮想サーバーが相互に通信するように構成します。
- 2 番目の DMZ の NetScaler Gateway 仮想サーバーを、最初の DMZ の NetScaler Gateway 仮想サーバーにバインドします。
- 2 つ目の DMZ で NetScaler Gateway でダブルホップを有効にします。
- 2 番目の DMZ の NetScaler Gateway 仮想サーバーでの認証を無効にします。
- いずれかの NetScaler Gateway アプライアンスで ICA レコードをエクスポートできるようにします

- 他の NetScaler Gateway アプライアンスが TCP レコードをエクスポートできるようにします。
- 両方の NetScaler Gateway アプライアンスで接続チェーンを有効にします。

コマンドラインインターフェイスを使用した **Citrix Gateway** の構成:

1. 最初の DMZ の NetScaler Gateway 仮想サーバーが、2 番目の DMZ の NetScaler Gateway 仮想サーバーと通信するように構成します。

   add vpn nextHopServer <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 Gateway 仮想サーバーを、最初の DMZ の NetScaler Gateway 仮想サーバーにバインドします。最初の DMZ の NetScaler Gateway で次のコマンドを実行します。

   bind vpn vserver <name> **-nextHopServer** <name>

   bind vpn vserver vs1 -nextHopServer nh1

3. 2 つ目の DMZ の NetScaler Gateway でダブルホップと AppFlow を有効にします。

   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 Gateway アプライアンスで TCP レコードをエクスポートできるようにします。

   bind vpn vserver<name> [**-policy**<string>**-priority**<positive_integer>] [**-type**<type>]

   bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type OTHERTCP_REQUEST

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. 両方の NetScaler Gateway アプライアンスで接続チェーンを有効にします:

   set appFlow param [**-connectionChaining** (ENABLED or DISABLED)]

   set appflow param -connectionChaining ENABLED

構成ユーティリティを使用した **NetScaler Gateway** の構成:

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) 右側のペインで仮想サーバーをダブルクリックし、[Advanced]グループで[**Published Applications**]を展開します。

c) ［ネクストホップサーバー］をクリックし、ネクストホップサーバーを 2 つ目の NetScaler Gateway アプライアンスにバインドします。

2. 2 つ目の DMZ で NetScaler Gateway でダブルホップを有効にします。

a) ［構成］タブで［**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 番目の DMZ の NetScaler Gateway 上の仮想サーバーでの認証を無効にします。

a)「構成」タブで 「 **Citrix Gateway** 」を展開 し、「仮想サーバー」をクリック します。

b) 右側のペインで仮想サーバーをダブルクリックし、基本設定グループで 編集アイコンをクリックします。

c) ［**More**］を展開し、［**Enable Authentication**］をオフにします。

4. Citrix Gateway アプライアンスのいずれかで TCP レコードをエクスポートできるようにします。

a)「構成」タブで 「 **Citrix Gateway** 」を展開 し、「仮想サーバー」をクリック します。

b) 右側のペインで仮想サーバーをダブルクリックし、［Advanced］グループで［Policies］を展開します。

c)「+ 」アイコンをクリックし 、「ポリシーの 選択」ドロップダウンリストで「**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** 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。

5. 他の NetScaler Gateway アプライアンスで ICA レコードをエクスポートできるようにします:

a)「構成」タブで 「 **Citrix Gateway** 」を展開 し、「仮想サーバー」をクリック します。

b) 右側のペインで仮想サーバーをダブルクリックし、「詳細設定」グループで「ポリシー」を展開 します。

c)「+ 」アイコンをクリックし 、「ポリシー の 選択」ドロップダウンリストで「**AppFlow** 」を選択 し、「タイプ を選択」ドロップダウンリストから「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] をクリックし ます。

c) ［**Connection Chaining**］を選択し、［**OK**］をクリックします。

7. 最初の DMZ の NetScaler Gateway を構成して、2 番目の DMZ の NetScaler Gateway と通信し、2 番目の DMZ の NetScaler Gateway を最初の DMZ の NetScaler Gateway にバインドします。

a) ［構成］タブで ［**NetScaler Gateway**］を展開し、［仮想サーバー］をクリックします。

b) 右側のペインで仮想サーバーをダブルクリックし、[詳細設定**]** グループで [公開 アプリケーション] を展開 します。

c) ［ネクストホップサーバー］をクリックし、ネクストホップサーバーを 2 番目の NetScaler Gateway アプライアンスにバインドします。

8. 2 つ目の DMZ で NetScaler Gateway でダブルホップを有効にします。

a) ［構成］タブで ［**NetScaler Gateway**］を展開し、［仮想サーバー］をクリックします。

b) 右側のペインで仮想サーバーをダブルクリックし、[基本設定] グループで編集アイコンをクリックします。

c)「詳細」を 展開 し、「ダブルホップ 」を選択 して「**OK**」をクリック します。

9. 2 番目の DMZ の NetScaler Gateway 上の仮想サーバーでの認証を無効にします。

a)「構成」タブで 「 Citrix Gateway 」を展開 し、「仮想サーバー」をクリック します。

b) 右側のペインで仮想サーバーをダブルクリックし、基本設定 グループで 編集アイコンをクリックします。

c) ［**More**］を展開し、［**Enable Authentication**］をオフにします。

10. Citrix Gateway アプライアンスのいずれかで TCP レコードをエクスポートできるようにします。

a) ［構成］タブで ［**Citrix Gateway**］を展開し、［仮想サーバー］をクリックします。

b) 右側のペインで仮想サーバーをダブルクリックし、[詳細設定] グループで [ポリシー] を展開 します。

c)「**+**」アイコンをクリックし 、「ポリシー の 選択」ドロップダウンリストから「**AppFlow** 」を選択 し、「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。

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」ドロップダウンリストで「**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** 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。

12. 両方の NetScaler Gateway アプライアンスで接続チェーンを有効にします。

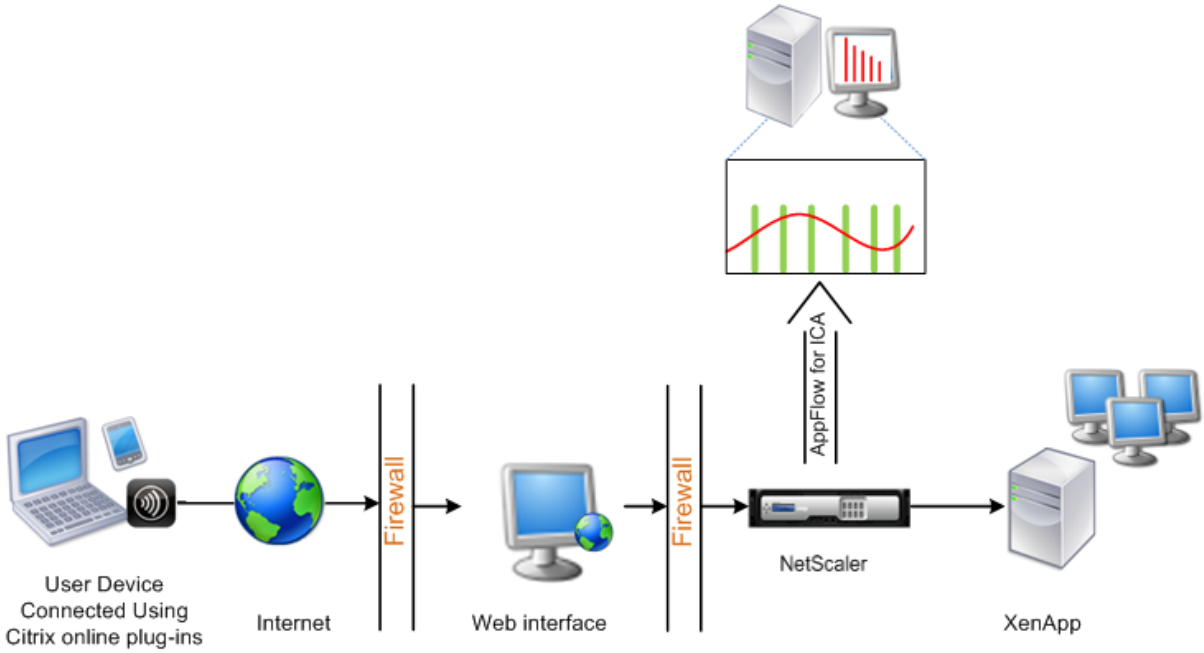
透過モードで展開された **NetScaler ADC** を監視するためのデータ収集の有効化

NetScaler ADC を透過モードで展開すると、クライアントは仮想サーバーを介さず、直接サーバーにアクセスできます。NetScaler ADC アプライアンスが Citrix Virtual Apps and Desktop 環境にトランスペアレントモードで展開されている場合、ICA トラフィックは VPN 経由で送信されません。

NetScaler ADC を NetScaler ADM インベントリに追加した後、データ収集のために AppFlow を有効にする必要があります。データ収集を有効にできるかどうかは、デバイスとモードによって決まります。その場合は、Citrix ADM を AppFlow コレクターとして各 Citrix ADC アプライアンスに追加する必要があります。また、アプライアンスを通過するすべてまたは特定の ICA トラフィックを収集するように Appflow ポリシーを構成する必要があります。

> 注
>
> - NetScaler ADM 構成ユーティリティを使用して、透過モードで展開された NetScaler ADC でデータ収集を有効にすることはできません。
> - コマンドとその使用法について詳しくは、「コマンドリファレンス」を参照してください。
> - ポリシー式については、「ポリシーと式」を参照してください。

次の図は、NetScaler ADC が透過モードで展開された場合の NetScaler ADM のネットワーク展開を示しています。



コマンドラインインターフェイスを使用して **NetScaler ADC** アプライアンスでデータ収集を構成するには:

コマンドプロンプトで、次の操作を行います:

1. アプライアンスにログオンします。
2. NetScaler ADC アプライアンスがトラフィックをリッスンする 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 Insight Center を Citrix ADC アプライアンスの 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： Citrix ADC アプライアンスに設定されている AppFlow コレクターを表示するには 、**show appflow** collector コマンドを使用します。

4. AppFlow アクションを作成して、コレクターを関連付けます。

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

例:

add appflow action act -collectors MyInsight

5. トラフィック生成の規則を指定するための AppFlow ポリシーを作成します。

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

例:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. グローバルバインドポートに AppFlow ポリシーをバインドします。

```
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、タイプの値を ICA_REQ_OVERRIDE または ICA_REQ_DEFAULT にする必要があります。

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-->
```

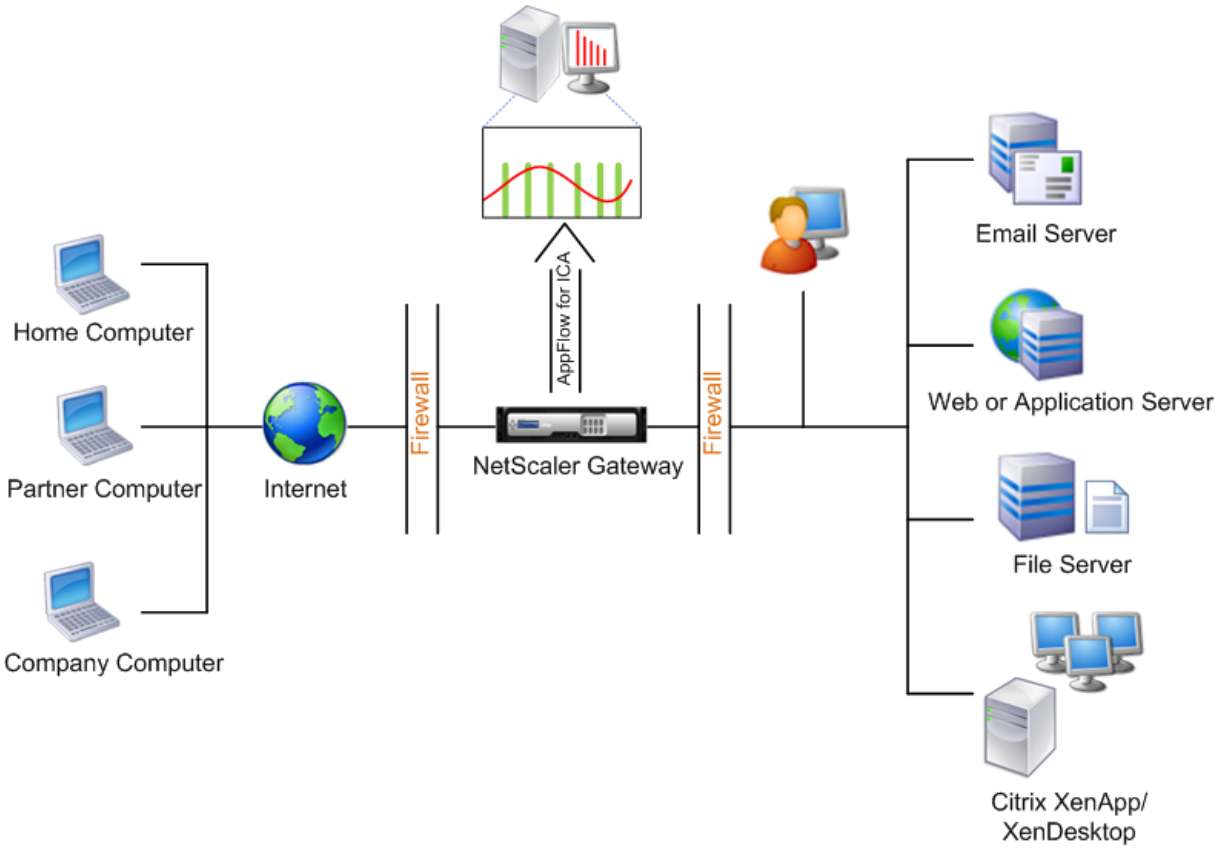
8. 構成を保存します。種類：`save ns config`

シングルホップモードで展開された **NetScaler Gateway** アプライアンスのデータ収集を有効にする

February 6, 2024

NetScaler Gateway をシングルホップモードで展開すると、ネットワークのエッジになります。Gateway インスタンスは、デスクトップ配信インフラストラクチャへのプロキシ ICA 接続を提供します。シングルホップは、最も単純で最も一般的な導入方法です。シングルホップモードは、外部ユーザーが組織内の内部ネットワークにアクセスしようとした場合にセキュリティを確保します。
シングルホップモードでは、ユーザーは仮想プライベートネットワーク（VPN）を介して NetScaler ADC アプライアンスにアクセスします。

レポートの収集を開始するには、NetScaler Gateway アプライアンスを Citrix Application Delivery Management（ADM）インベントリに追加し、ADM で AppFlow を有効にする必要があります。



ADM から **AppFlow** 機能を有効にするには:

1. Web ブラウザで、Citrix ADM IP アドレス（例: http://192.168.100.1）を入力します。
2. ［**User Name**］と ［**Password**］に管理者の資格情報を入力します。

3. [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」ドロップダウンから「**Insight** の有効化/無効化」を選択します。
5. **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。
6. 「**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。
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>
> - アプリフローアクションを追加 \ <name\ > -コレクター \ <string\ >
> - set appflow param -flowRecordInterval <secs>
> - disable ns feature AppFlow
> - enable ns feature AppFlow
> - add appflow policy <name> <rule> <expression>
> - set appflow policy <name> -rule <expression>
> - bind vpn vserver <vsname> -policy <string> -type <type> >-priority <positive_integer>
> - set vpn vserver <name> -appflowLog ENABLED
> - save ns config

EUEM 仮想チャネルデータは、NetScaler ADM がゲートウェイインスタンスから受信する HDX Insight データの一部です。EUEM 仮想チャネルは、ICA RTT に関するデータを提供します。EUEM 仮想チャネルが有効になっていない場合でも、残りの HDX Insight データは NetScaler ADM に表示されます。

透過モードで展開された **NetScaler ADC** を監視するためのデータ収集を有効にする

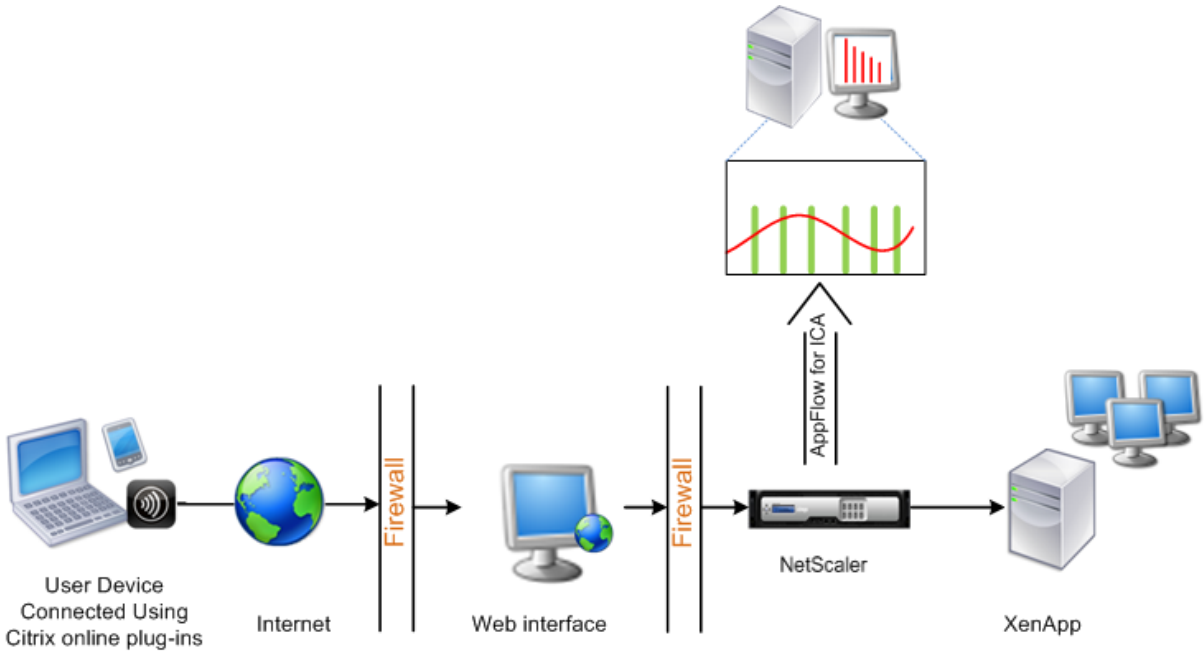
February 6, 2024

NetScaler ADC を透過モードで展開すると、クライアントは、仮想サーバーを介さずに直接サーバーにアクセスできます。NetScaler ADC アプライアンスが Citrix Virtual Apps and Desktops 環境でトランスペアレントモードで展開されている場合、ICA トラフィックは VPN 経由で送信されません。

NetScaler ADC を NetScaler ADM インベントリに追加した後、データ収集のために AppFlow を有効にする必要があります。データ収集を有効にできるかどうかは、デバイスとモードによって決まります。その場合は、Citrix ADM を AppFlow コレクターとして各 NetScaler アプライアンスに追加し、アプライアンスを通過するすべてまたは特定の ICA トラフィックを収集するように Appflow ポリシーを構成する必要があります。

> 注
>
> - 透過モードで展開された NetScaler ADC では、Citrix ADM 構成ユーティリティを使用して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 ADC をトランスペアレントモードで展開したときの Citrix 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 アプライアンスの AppFlow コレクターとして、NetScaler Insight Center を追加します。

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

例:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

> 注: NetScaler アプライアンス上で構成されている AppFlow コレクターを表示するには 、**show** appflow collector コマンドを使用します。

4. AppFlow アクションを作成して、コレクターを関連付けます。

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

例:

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. トラフィック生成の規則を指定するための AppFlow ポリシーを作成します。

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

例:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. グローバルバインドポートに AppFlow ポリシーをバインドします。

```
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、タイプの値を ICA_REQ_OVERRIDE または ICA_REQ_DEFAULT にする必要があります。

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。

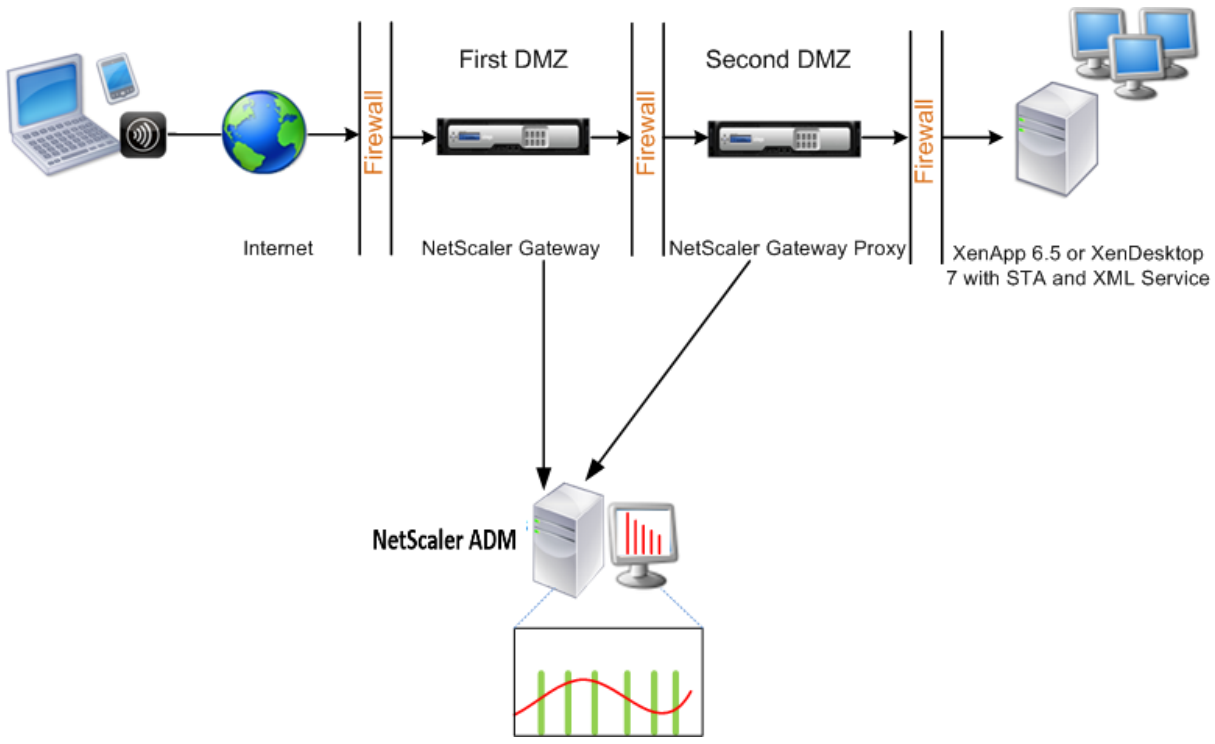
```
save ns config
<!--NeedCopy-->
```

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。

図 3：ダブルホップモードで展開される NetScaler ADM



最初の DMZ の NetScaler Gateway は、ユーザー接続を処理し、SSL VPN のセキュリティ機能を実行します。この NetScaler Gateway は、ユーザー接続を暗号化し、ユーザーの認証方法を決定し、内部ネットワーク内のサーバーへのアクセスを制御します。

2 つ目の DMZ の NetScaler Gateway は、NetScaler Gateway プロキシデバイスとして機能します。この NetScaler Gateway により、ICA トラフィックが 2 番目の DMZ を通過して、サーバーファームへのユーザー接続を完了できます。

NetScaler ADM は、最初の DMZ の NetScaler Gateway アプライアンスに属するサブネットか、2 番目の DMZ の NetScaler Gateway アプライアンスに属するサブネットのいずれかに展開できます。上の画像では、最初の DMZ の NetScaler ADM と NetScaler Gateway が同じサブネットにデプロイされています。

ダブルホップモードでは、NetScaler ADM は 1 つのアプライアンスから TCP レコードを、もう 1 つのアプライアンスから ICA レコードを収集します。Citrix Gateway アプライアンスを Citrix ADM インベントリに追加してデータ収集を有効にすると、各アプライアンスはホップカウントと接続チェーン ID を追跡してレポートをエクスポートします。

NetScaler ADM がレコードをエクスポートするアプライアンスを識別するために、各アプライアンスはホップ数で指定され、各接続は接続チェーン ID で指定されます。ホップカウントは、トラフィックがクライアントからサーバーに流れる NetScaler Gateway アプライアンスの数を表します。接続チェーン ID は、クライアントとサーバー間のエンドツーエンド接続を表します。

NetScaler ADM は、ホップカウントと接続チェーン ID を使用して、両方の NetScaler Gateway アプライアンスからのデータを相互に関連付け、レポートを生成します。

このモードで展開された Citrix Gateway アプライアンスを監視するには、まず Citrix Gateway を Citrix ADM インベントリに追加し、Citrix ADM で AppFlow を有効にしてから、Citrix 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。この作業を行うことにより、一方のアプライアンスは ICA AppFlow レコードをエクスポートし、もう一方のアプライアンスは TCP AppFlow レコードをエクスポートします。これにより、ICA トラフィック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」ドロップダウンから「**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 トラフィック用の **ICA/TCP** 、TCP トラフィック用の ICA/TCP をそれぞれ選択します。

   > 注： NetScaler アプライアンスの各サービスまたはサービスグループに対して AppFlow ロ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 ダッシュボードにレコードは表示されません。

5. [**OK**] をクリックします。

データをエクスポートするための **NetScaler Gateway** アプライアンスの設定

NetScaler Gateway アプライアンスをインストールした後、NetScaler Gateway アプライアンスで次の設定を構成して、レポートを NetScaler ADM にエクスポートする必要があります。

- 第 1 および第 2 の DMZ にある NetScaler Gateway アプライアンスの仮想サーバーが相互に通信するように構成します。
- 2 番目の DMZ の NetScaler Gateway 仮想サーバーを、最初の DMZ の NetScaler Gateway 仮想サーバーにバインドします。
- 2 つ目の DMZ で NetScaler Gateway でダブルホップを有効にします。
- 2 番目の DMZ の NetScaler Gateway 仮想サーバーでの認証を無効にします。
- いずれかの NetScaler Gateway アプライアンスで ICA レコードをエクスポートできるようにします
- 他の NetScaler Gateway アプライアンスが TCP レコードをエクスポートできるようにします。
- 両方の NetScaler Gateway アプライアンスで接続チェーンを有効にします。

コマンドラインインターフェイスを使用した **Citrix Gateway** の設定:

1. 最初の DMZ の NetScaler Gateway 仮想サーバーが、2 番目の DMZ の NetScaler Gateway 仮想サーバーと通信するように構成します。

---

add vpn nextHopServer [**-secure**(ON OFF)] [**-imgGifToPng**] …

```
add vpn nextHopServer nh1 10.102.2.33 8443 -secure ON
<!--NeedCopy-->
```

2. 2 番目の DMZ の NetScaler Gateway 仮想サーバーを、最初の DMZ の NetScaler Gateway 仮想サーバーにバインドします。最初の DMZ の NetScaler Gateway で次のコマンドを実行します。

   bind vpn vserver <name> **-nextHopServer** <name>

```
bind vpn vserver vs1 -nextHopServer nh1
<!--NeedCopy-->
```


3. 2 つ目の DMZ の NetScaler Gateway でダブルホップと AppFlow を有効にします。

set vpn DISABLED)] [**- appflowLog** (DISABLED)]
vserver [**- doubleHop** (ENABLED
ENABLED

```
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 Gateway アプライアンスで TCP レコードをエクスポートできるようにします。

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
bind vpn vserver vpn1 -policy appflowpol1 -priority 101  -type
   OTHERTCP_REQUEST
<!--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. 両方の NetScaler Gateway アプライアンスで接続チェーンを有効にします:

set appFlow DISABLED)]
param [**-connectionChaining** (ENABLED

```
set appflow param -connectionChaining ENABLED
<!--NeedCopy-->
```

構成ユーティリティを使用して **Citrix Gateway** を構成する方法:

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**］を展開して［仮想サーバー］をクリックします

b) 右側のペインで仮想サーバーをダブルクリックし、[Advanced]グループで[**Published Applications**]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 つ目の DMZ で NetScaler Gateway でダブルホップを有効にします。

a) ［構成］タブで［**NetScaler Gateway**］を展開し、［仮想サーバー］をクリックします。

b) 右側のペインで仮想サーバーをダブルクリックし、基本設定グループで 編集アイコンをクリックします。

c) ［**More**］を展開し、［**Double Hop**］を選択して［**OK**］をクリックします。

3. 2 番目の DMZ の NetScaler Gateway 上の仮想サーバーでの認証を無効にします。

a)「構成」タブで 「 **Citrix Gateway** 」を展開 し、「仮想サーバー」をクリック します。

b) 右側のペインで仮想サーバーをダブルクリックし、[基本設定] グループで編集アイコンをクリックします。

c) ［**More**］を展開し、［**Enable Authentication**］をオフにします。

4. Citrix Gateway アプライアンスのいずれかで TCP レコードをエクスポートできるようにします。

a)「構成」タブで 「 **Citrix Gateway** 」を展開 し、「仮想サーバー」をクリック します。

b) 右側のペインで仮想サーバーをダブルクリックし、［Advanced］グループで［Policies］を展開します。

c) [+] アイコンをクリックし、[ポリシーの選択] リストから [**AppFlow**] を選択し、[タイプの選択] リストから [その他の **TCP** 要求] を選択します。

d) [続行] をクリックします。

e) ポリシーのバインドを追加して、［**Close**］をクリックします。

5. 他の NetScaler Gateway アプライアンスで ICA レコードをエクスポートできるようにします:

a)「構成」タブで 「 **Citrix Gateway** 」を展開 し、「仮想サーバー」をクリック します。

b) 右側のペインで仮想サーバーをダブルクリックし、「詳細設定」グループで「 ****** ポリシー ******」を展開 します。

c) [+] アイコンをクリックし、[ポリシーの選択] ドロップダウンリストから [**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。

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) 右側のウィンドウの [設定] で、[**Appflow** 設定の変更] をクリックします。

c) [**Connection Chaining**] を選択し、[**OK**] をクリックします。

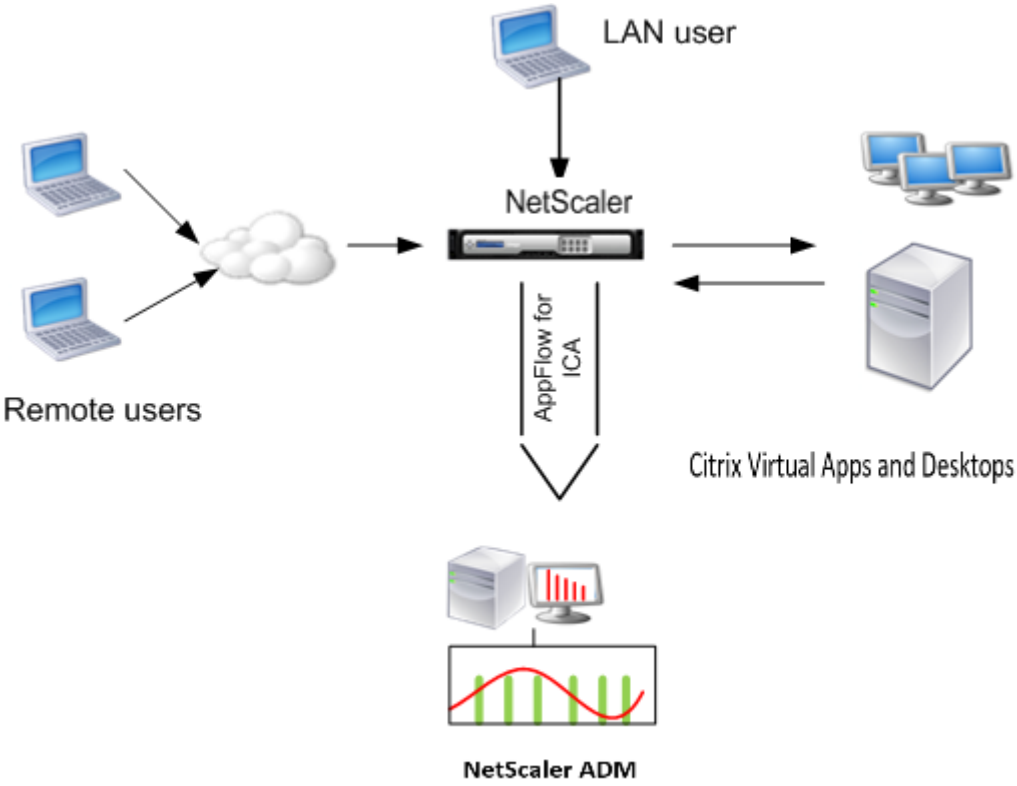
LAN ユーザーモードで展開された **NetScaler ADC** を監視するためのデータ収集を有効にする

February 6, 2024

Citrix Virtual Apps and Desktops アプリケーションにアクセスする外部ユーザーは、Citrix Gateway で自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、Citrix 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、NetScaler アプライアンスを LAN ユーザーモードで展開できます。

図 4: LAN ユーザーモードで展開される NetScaler ADM



> 注
>
> Citrix ADM と Citrix ゲートウェイ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 Citrix アプライアンスを監視するには、まず Citrix アプライアンスを NetScaler Insight インベントリに追加し、AppFlow を有効にしてから、ダッシュボードにレポートを表示します。

Citrix アプライアンスを Citrix ADM インベントリに追加したら、データ収集のために AppFlow を有効にする必要があります。

> 注
>
> - Citrix ADM 構成ユーティリティを使用して、LAN ユーザーモードで展開された NetScaler ADC でデータ収集を有効にすることはできません。
> - コマンドとその使用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 NetScaler ADC アプライアンスの AppFlow コレクタとして追加します。

```
add appflow collector** \<name\> \*\*-IPAddress\*\* \\<ip\\_addr
   \\>
<!--NeedCopy-->
```

例:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

4. AppFlow アクションを作成して、コレクターを関連付けます。

```
add appflow action** \<name\> \*\*-collectors\*\* \<string\> ...
<!--NeedCopy-->
```

例:

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. トラフィック生成の規則を指定するための AppFlow ポリシーを作成します。

```
add appflow policy** \<policyname\> \<rule\> \<action\>
<!--NeedCopy-->
```

例:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. グローバルバインドポートに AppFlow ポリシーをバインドします。

```
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、タイプの値を ICA_REQ_OVERRIDE または ICA_REQ_DEFAULT にする必要があります。

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

Citrix Application Delivery Management（ADM）に関する HDX Insight を使用すると、Citrix ADC インスタンスを通過する HDX トラフィックを監視できます。NetScaler ADM では、Insight トラフィックの監視に使用するさまざまなカウンターのしきい値を設定できます。また、NetScaler ADM でルールを構成し、アラートを作成することもできます。

HDX トラフィックの種類は、アプリケーション、デスクトップ、ゲートウェイ、ライセンス、ユーザーなどのさまざまなエンティティに関連付けられます。すべてのエンティティには、それらに関連付けられた異なるメトリックを含めることができます。たとえば、アプリケーションエンティティは、ヒット数、アプリケーションによって消費された帯域幅、およびサーバーの応答時間に関連付けられています。ユーザーエンティティは、WAN 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 ミリ秒以下でなければなりません
- 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 ミリ秒以下でなければなりません

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、まず監視するエンティティを選択する必要があります。次に、ルール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 Citrix ADM に表示したり、モバイルデバイスでアラートを電子メールまたは SMS として受信したりできるようにすることができます。最後の 2 つの操作では、NetScaler ADM で電子メールサーバーまたは SMS サーバーを構成する必要があります。

閾値グループは、ユーザーエンティティの地理固有の監視のためにジオロケーションにバインドすることもできます。

ユースケースの例

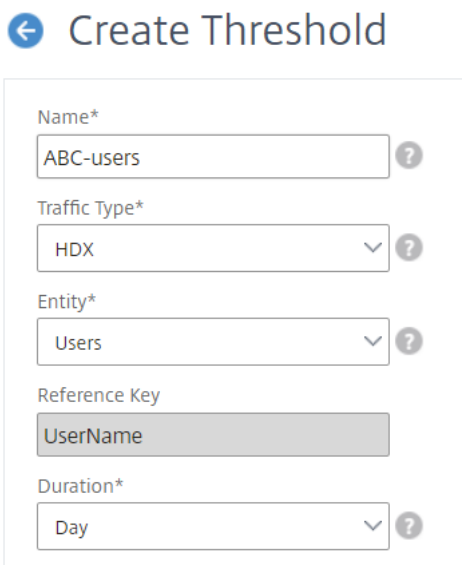
ABC Inc. はグローバル企業で、50 カ国以上にオフィスを構えています。同社は、シンガポールとカリフォルニア州に Citrix Virtual Apps and Desktops をホストする 2 つのデータセンターを持っています。同社の従業員は、NetScaler Gateway および Citrix GSLB ベースのリダイレクトを使用して、世界中の Citrix Virtual Apps and Desktops にアクセスします。ABC Inc. の Citrix Virtual Apps and Desktops 管理者である Eric は、すべてのオフィスのユーザーエクスペリエンスを追跡して、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の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いれば、データセンターから遠く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、データセンターの近くの場所の ICA RTT は 5〜10 ミリ秒ですが、遠隔地の ICA RTT は約 100 ミリ秒です。

HDX Insight のしきい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しきい値ルールグループを設定し、エリアごとの違反について電子メールまたは SMS で警告を受けることができます。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。

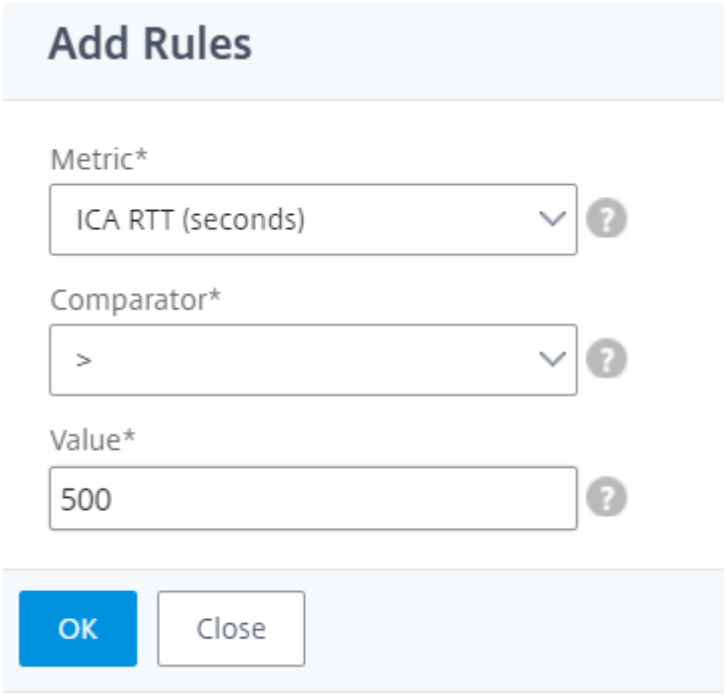
NetScaler ADM を使用してしきい値ルールグループを作成し、**HDX Insight** のアラートを構成するには:

1. Citrix ADM で、[**Analytics**] > [設定] > [しきい値] に移動します。[しきい値] ページが表示されたら、[追加] をクリックします。
2. [**Create Thresholds and Alerts**] ページで次の詳細を指定します。
   a) 名前。NetScaler ADM がアラートを生成するイベントを作成するための名前を入力します。
   b) トラフィックタイプ。ドロップダウンリストボックスから、[HDX] を選択します。
   c) エンティティ。ドロップダウン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。ドロップダウン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。

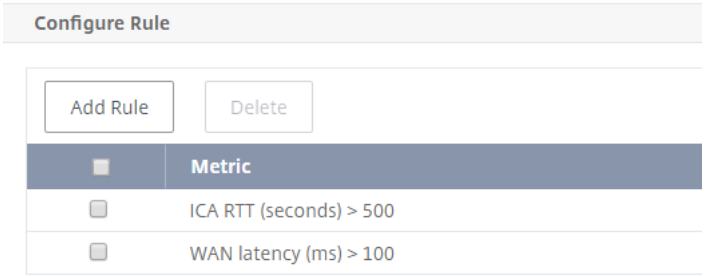


3. すべてのエンティティのしきい値ルールグループを作成しています。

   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。

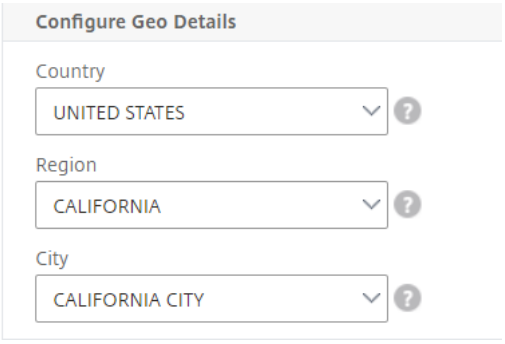


複数のルールを作成して、各エンティティを監視できます。1 つのグループに複数のルールを作成すると、個々のルールではなく、しきい値ルールのグループとしてエンティティを監視できます。[**OK**] をクリックしてウィンドウを閉じます。



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: 選択した期間内に Citrix Virtual Apps and Desktops にアクセスするすべてのユーザーのレポートを表示します。
- アプリケーション**:** アプリケーションの総数のレポートと、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。

> 注
>
> ［ライセンス］の値は、Citrix SD-WAN アプライアンスには適用されません。

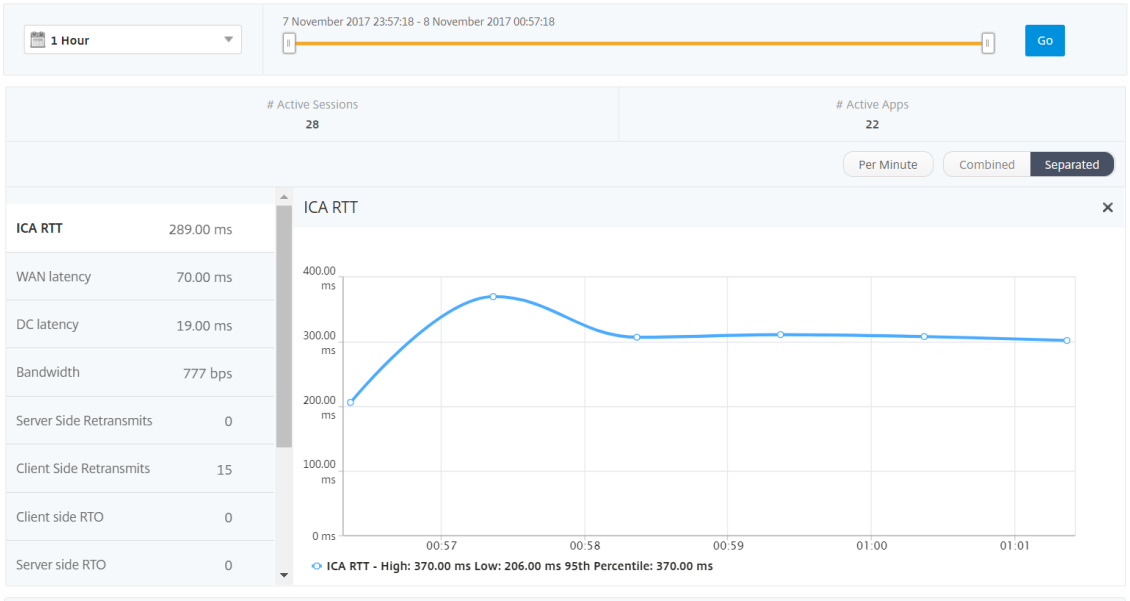
ユーザービューのレポートとメトリクス

2017 年 11 月 6 日

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. サポートされている Web ブラウザを使用して、NetScaler ADM にログオンします。
2. **Analytics** > **HDX Insight** > ユーザー



[User] ビューのレポートとメトリックは、次のセクションで構成されています。

- [Summary] ビュー
- [Per User] ビュー
- Per User Session ビュー

[**Summary**] ビュー

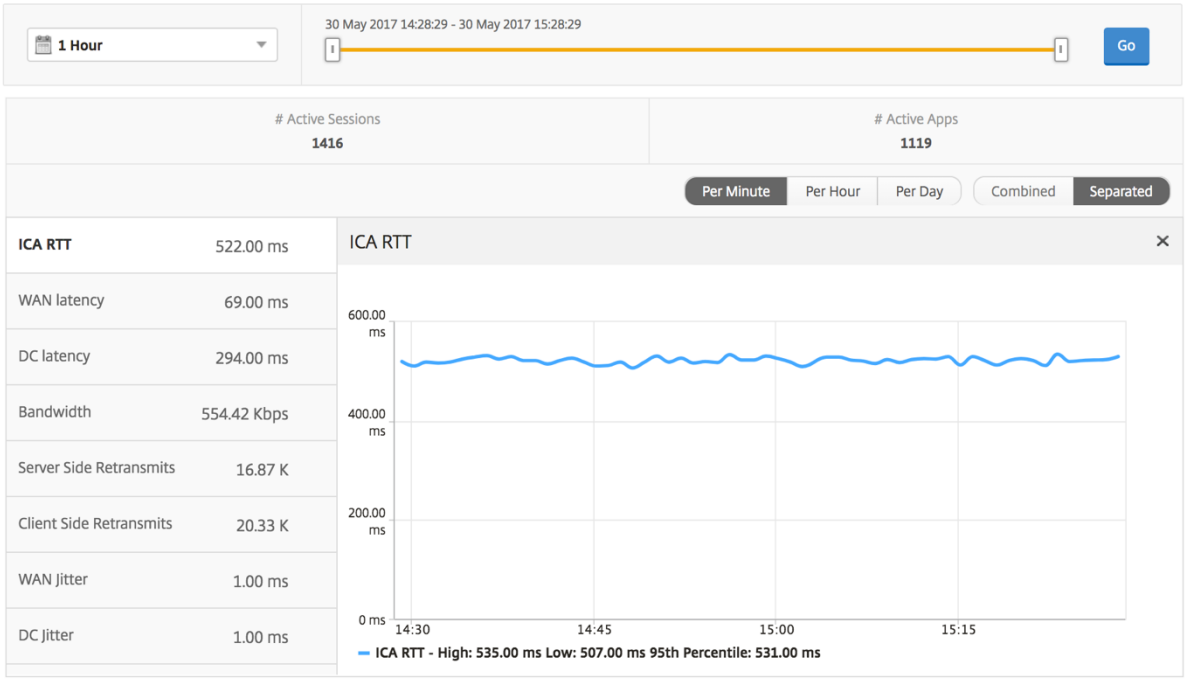
[Summary] ビューには、選択した期間中にログインしたすべてのユーザーのレポートが表示されます。このビューのすべてのメトリック/レポートには、特に指定のない限り選択した期間のメトリック/レポートに対応する値が表示されます。

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 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。



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 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。

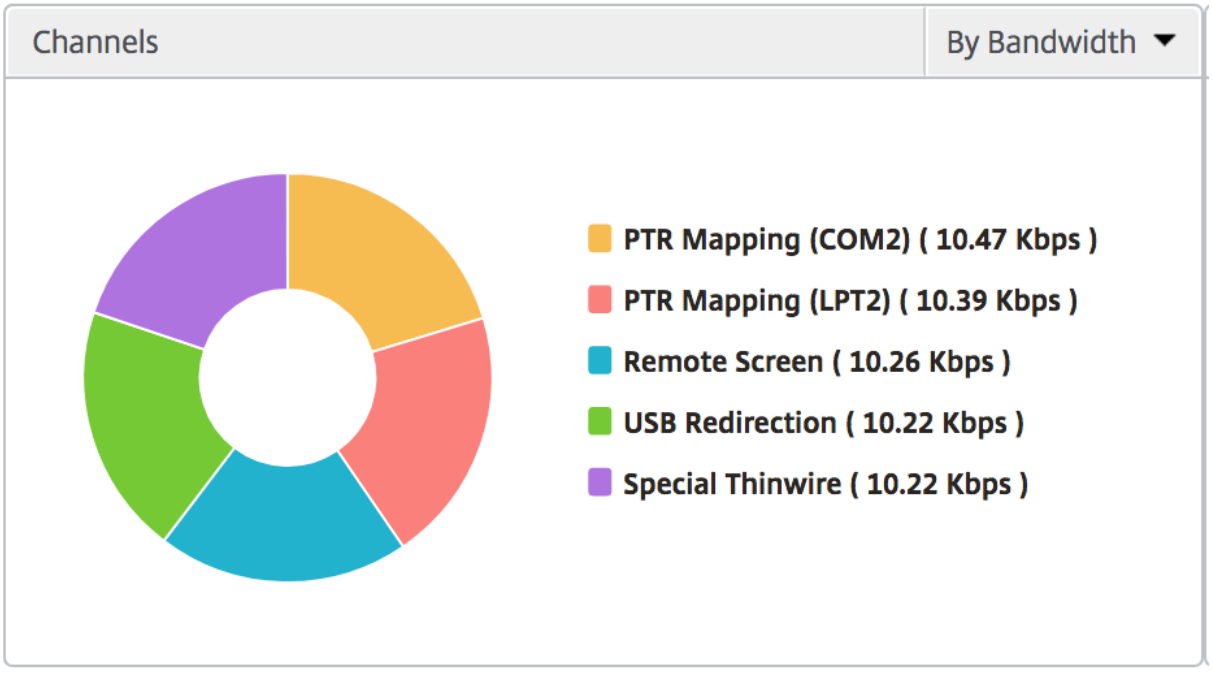
メトリックス	説明
クライアント側の再転送	NetScaler ADC とエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	NetScaler ADC とエンドユーザー間の接続で再送信タイムアウトが発生した回数。
Server side fast RTO	NetScaler ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。
クライアント側のゼロ ウィンドウ サイズ イベント	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

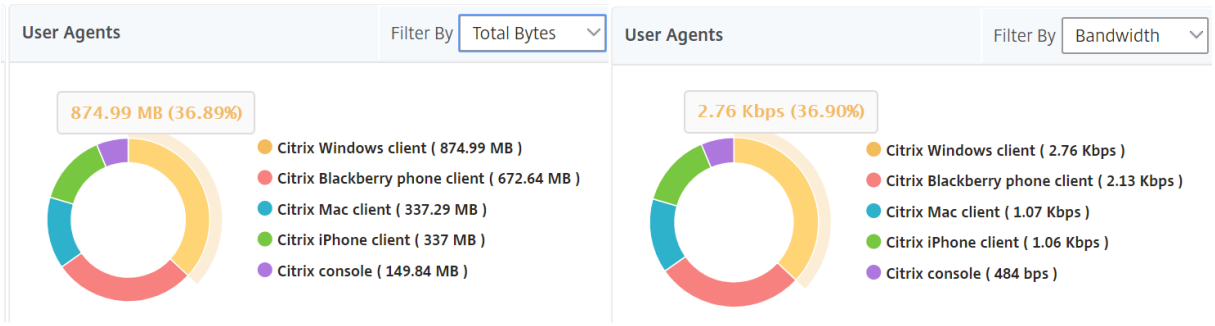
User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	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、各レシーバクライアントが消費する全体の帯域幅/合計バイトをドーナツチャートの形式で表します。グラフ内の色付きの各セグメントは、1 つの受信側クライアントを表します。

セグメントの長さは、その受信側クライアントでアプリケーションを起動するユーザーの数によって異なります。また、帯域幅または合計バイト数でメトリックをソートすることもできます。



各セグメントをクリックすると、その受信側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

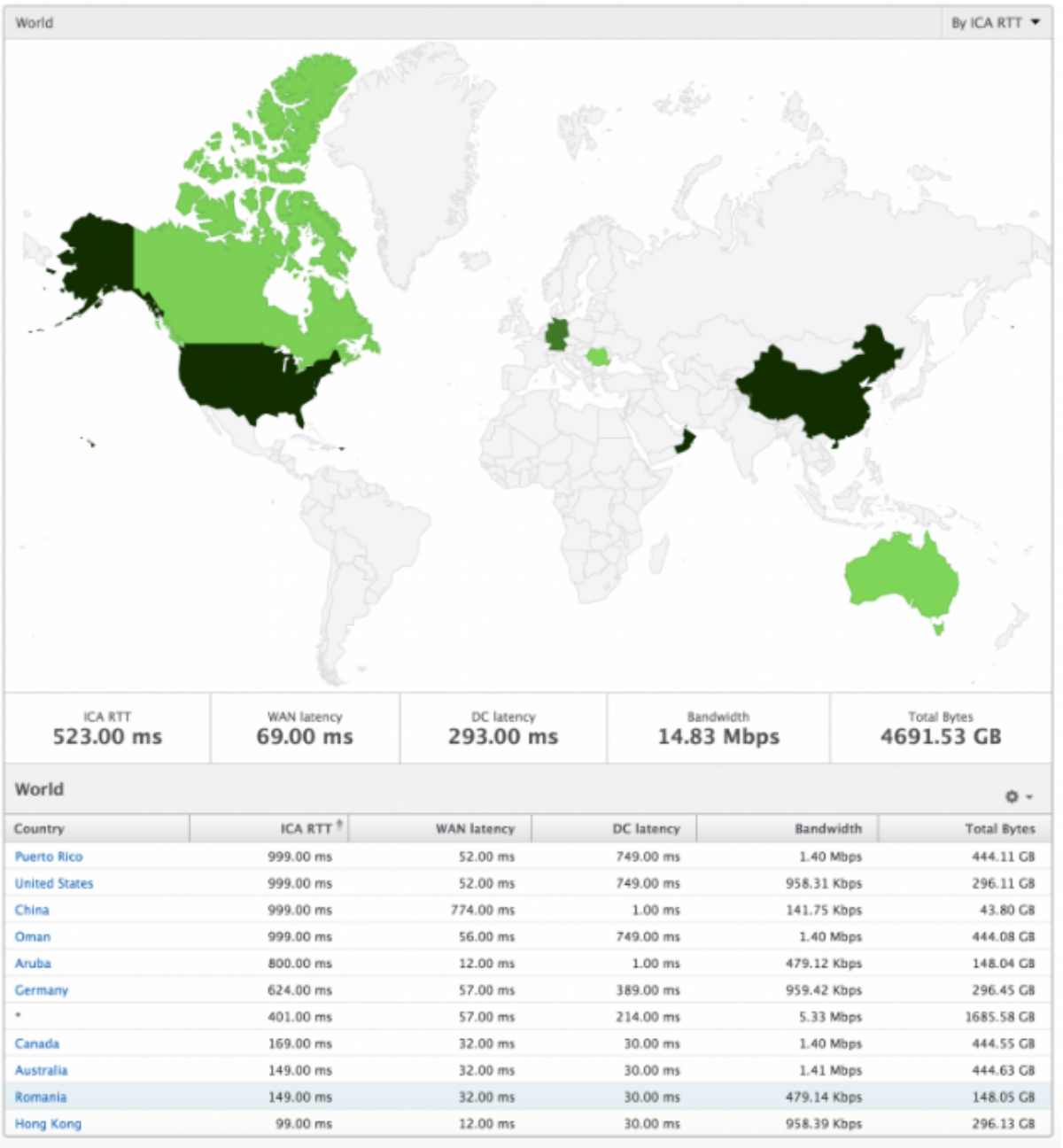
Name	Server Side Retransmits	ICA RTT	Client SRTT	Session Reconnect	Latency	Clientside zero window size event	Server SRTT
c1\daniel	0	149.44	1		149.44	0	
ryan	5071	4640	1		4640	0	
ramas	0	994.71	1		994.71	0	

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。

World Map　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。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. [**Analytics**] > [**HDX Insight**] > [ユーザー] に移動します。

3.［User Summary］レポートで目的のユーザーを選択します。

折れ線グラフ　折れ線グラフには、指定した期間における選択したユーザーのメトリックすべての概要が表示されます。

現在/終了したセッションレポート　このレポートは、選択したユーザーの現在/終了済みのユーザーセッションすべてに関係します。これらのメトリクスは、開始時間、セッション再接続、および ACR 数でソートできます。

メトリックス	説明
セッション ID	ICA セッションの一意の ID。
セッションの種類	アプリケーション/デスクトップ。
状態	緑はアクティブなセッション、赤は非アクティブなセッション。
ホストの遅延	サーバーネットワークが原因で NetScaler ADC を通過する ICA トラフィックの平均遅延。
間隔あたりの帯域幅	特定の期間にセッションで使用された帯域幅です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
インターバルあたりのバイト数	特定の期間にセッションで使用されたバイト数。
開始時刻	セッションの開始時間。
アップタイム	セッションの実行時間
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	レシーバタイプ-Citrix Windows クライアント
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値（［Yes］または［No］）。セッションがマルチストリーム ICA かどうかを表します。
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。たとえば、NetScaler Gateway のユーザー/透過モードなどです。
国	セッションが確立された国。

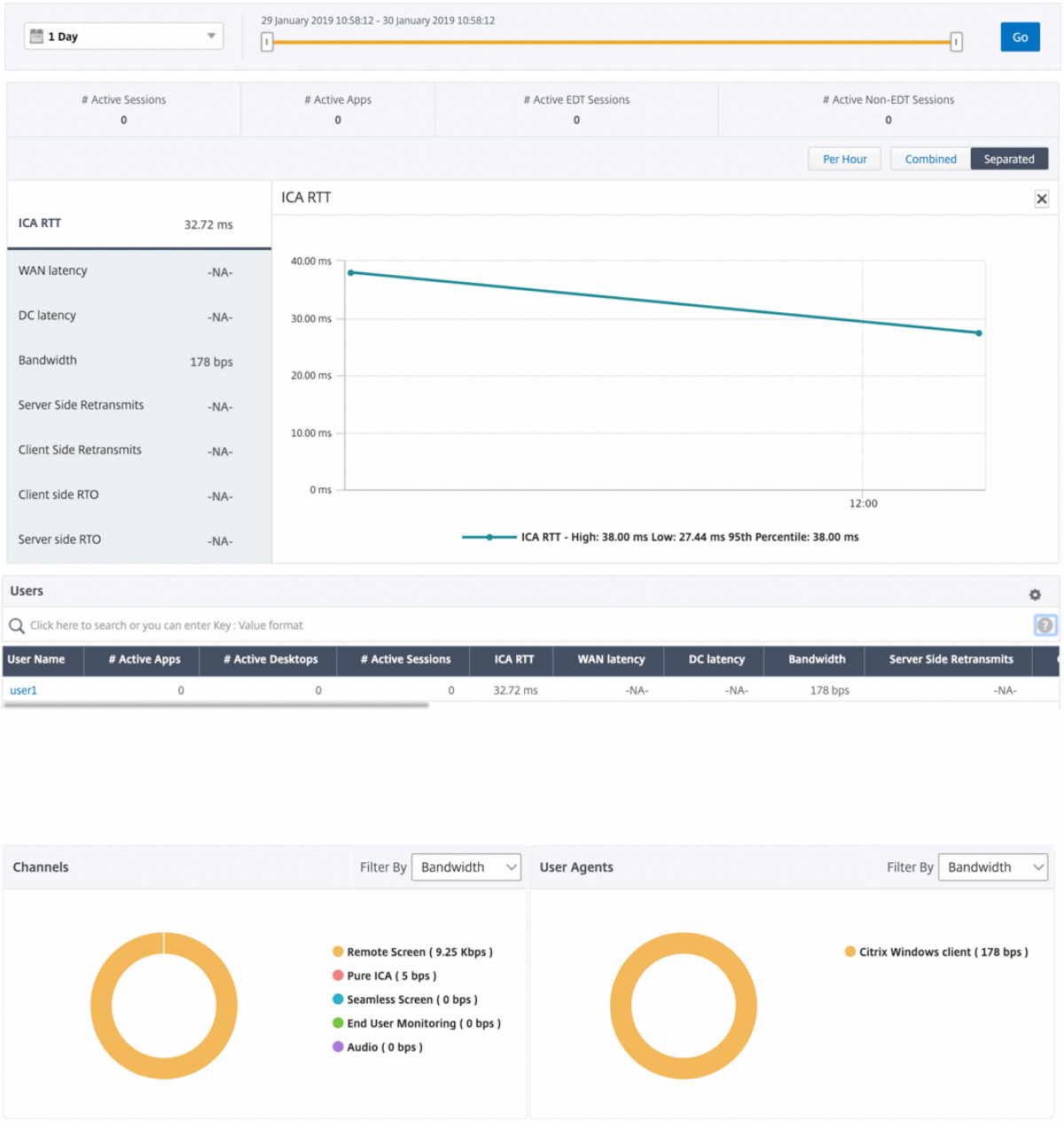
メトリックス	説明
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。
ICA 往復時間	ICA RTT は、Citrix Virtual 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。

メトリックス	説明
Server side fast RTO	NetScaler ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。

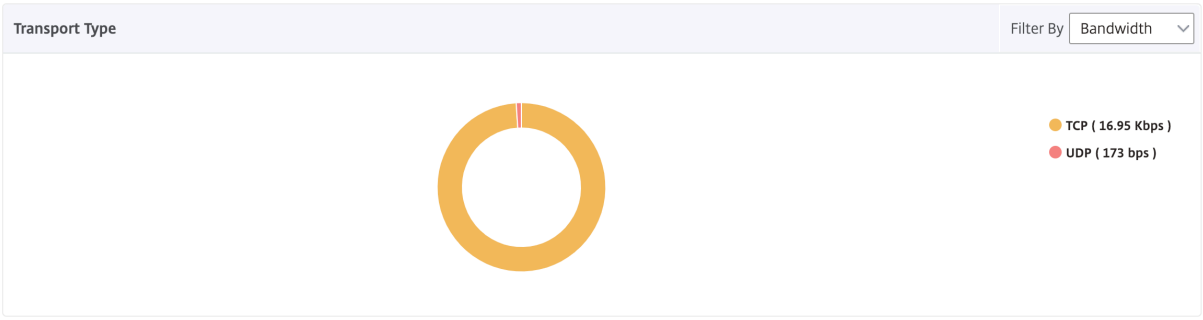
HDX Insight での **EDT** のサポート

NetScaler Application Delivery Management（ADM）では、HDX Insight ight の分析を表示するための啓発データトランスポート（EDT）がサポートされるようになりました。つまり、ADM は UDP と TCP の両方のプロトコルをサポートするようになりました。NetScaler Gateway の EDT サポートにより、Citrix Receiver を実行しているユーザーの仮想デスクトップの高品位セッション内ユーザーエクスペリエンスが保証されます。

HDX Insight は、アクティブセッションレポートの一部として、EDT セッションと非 EDT セッションの数を表示するようになりました。「ユーザー」(Users) テーブルには、システム内のすべてのユーザーの詳細なレポートが表示されます。この表には、WAN レイテンシー、DC レイテンシー、再送信、RTO などのメトリックが示されています。これらのメトリックのいくつかは、現在 TCP スタックから計算されるため、EDT セッションを持つユーザーには使用できません。したがって、これらは「NA」として表示されます。



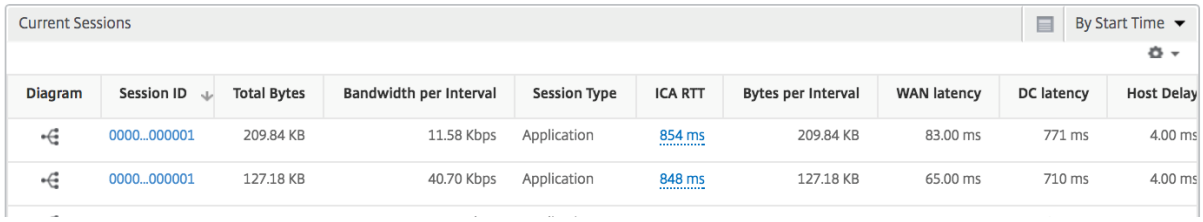
新しいドーナツグラフが導入され、ユーザーが使用したプロトコルの種類に基づいて、ユーザーが消費した帯域幅と合計バイト数を確認できるようになりました。

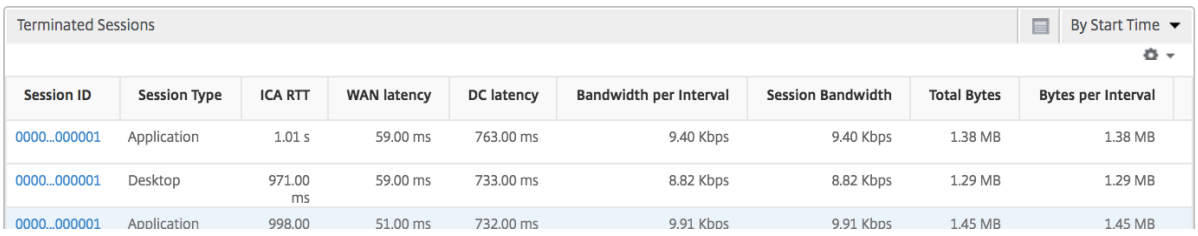


> 注
>
> HDX Insight の EDT は、リリース 12.1 ビルド 50.28 の NetScaler ADM でサポートされ、リリース 12.1 ビルド 49.23 の ADC インスタンスで使用できます。

NetScaler ADM 12.0 以降から入手可能な **HDX Insight** メトリック:

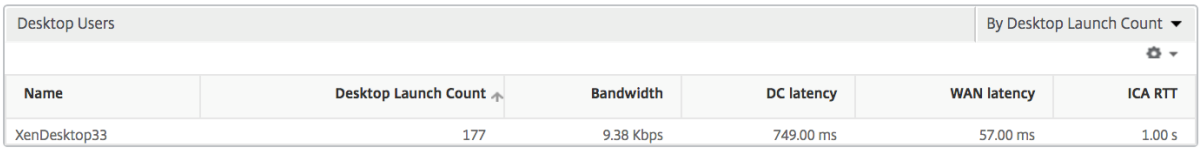
L7 Client-side Latency	ICA クライアントと NetScaler ADC インスタンスの間で観測された平均 L7 遅延時間。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。
L7 Server-side Latency	NetScaler ADC デバイスと Citrix Virtual Apps の間で観察された平均 L7 遅延。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。
違反の最大遅延	定義済みしきい値の違反が一定期間に発生した場合の、L7 遅延の最大値。
平均侵害待ち時間	システムが「L7 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。



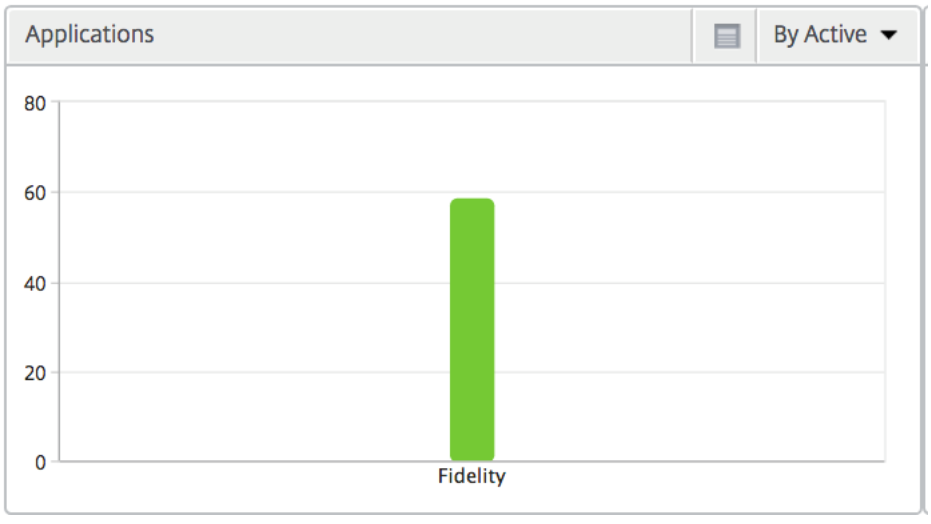


デスクトップユーザー　この表は、特定のユーザーの Citrix Virtual Desktop セッションに関する洞察を示しています。以下のメトリクスは［Desktop Launch Count］および［Bandwidth］を基準にしてソートできます。

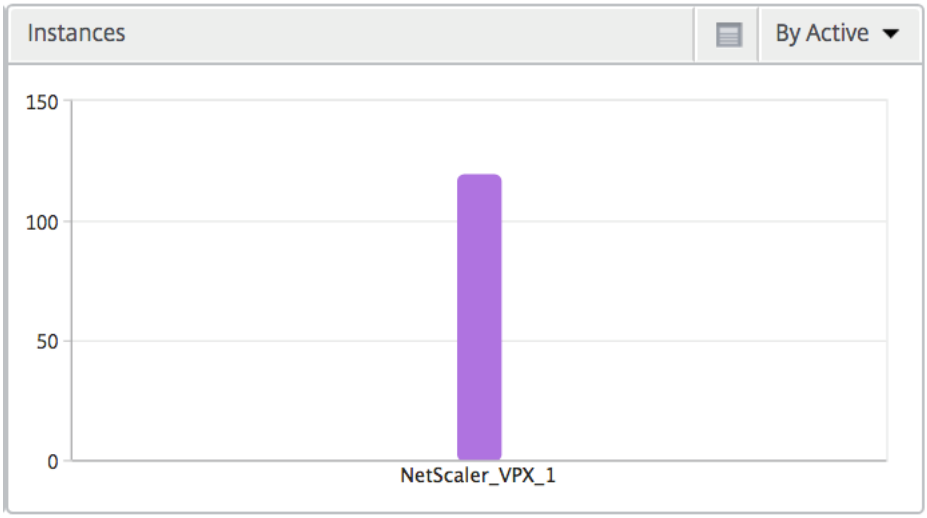
メトリックス	説明
名前	Citrix Virtual Desktops の名前。
デスクトップ起動回数	デスクトップが起動された回数です。
帯域幅	選択した期間中にエンドツーエンドの通信にかかった 1 秒あたりの合計バイト数。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps 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。



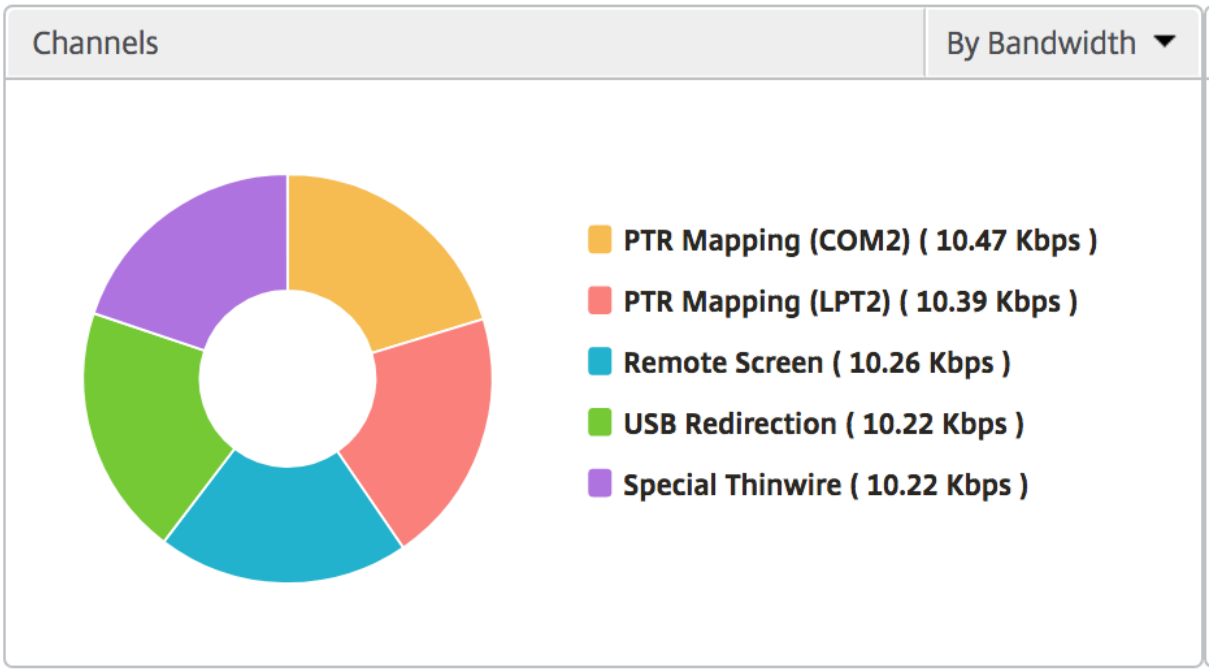
アプリケーション　［Active］、［Total Session Launch Count］、［Total App Launch Count］、［Launch Duration］で並べ替えることができる、アプリを表す棒グラフ。



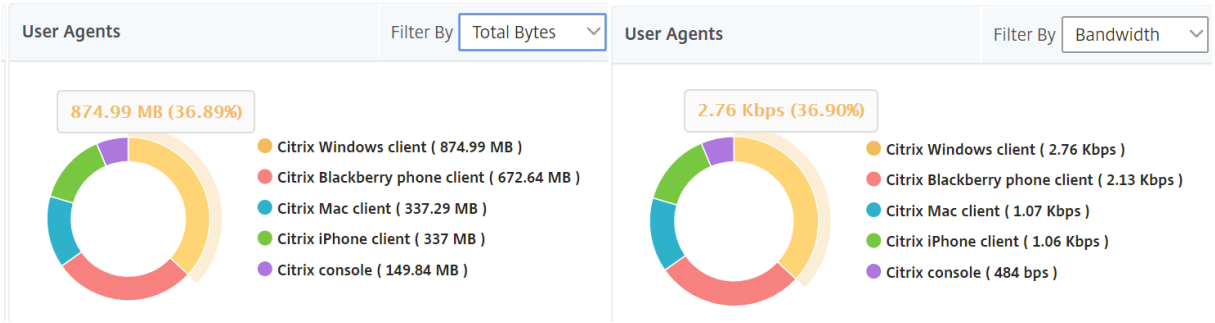
インスタンス　NetScaler ADC インスタンスをアクティブおよび合計アプリでソートした棒グラフ



チャネル　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。



ユーザーごと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。

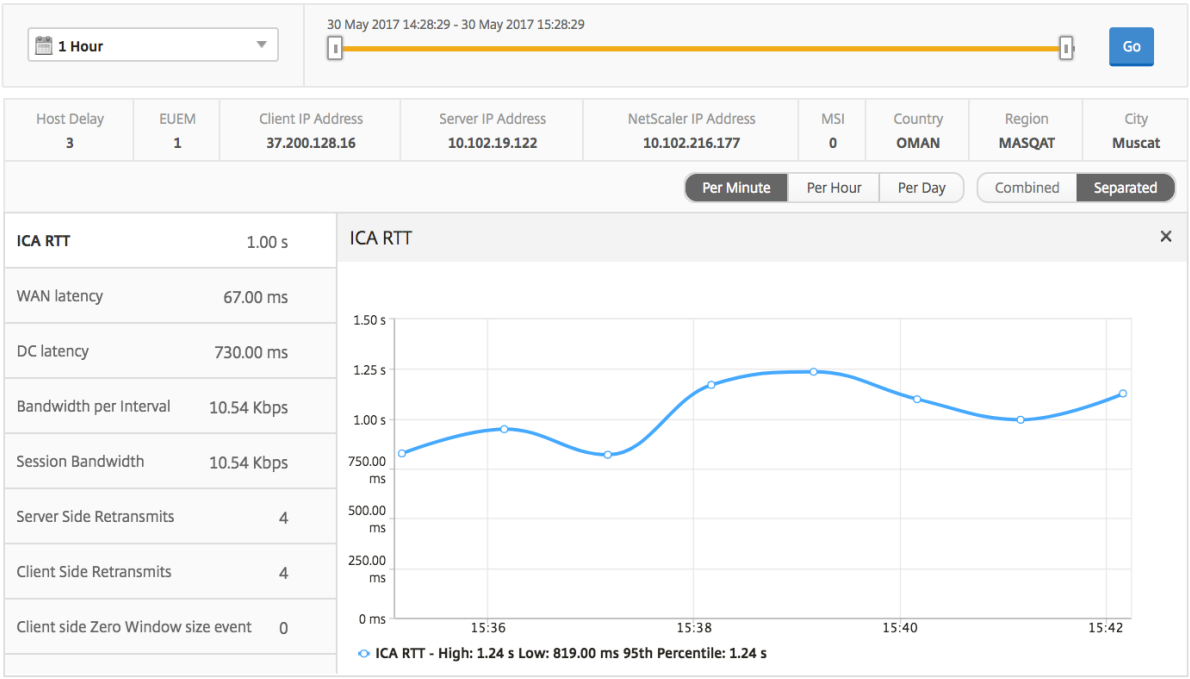
選択したユーザーのセッションのメトリックを表示する手順は、次のとおりです。

1. サポートされている Web ブラウザを使用して、NetScaler ADM にログオンします。
2. [**Analytics**] > [**HDX Insight**] > [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。

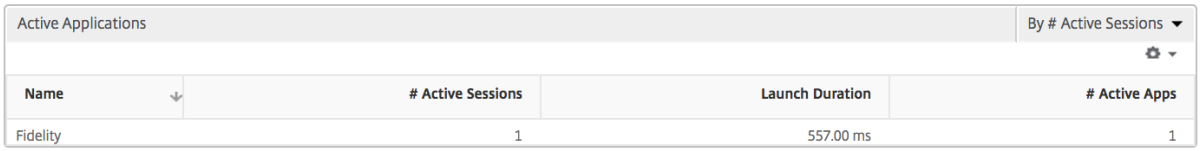
時系列グラフ

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 Apps 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。

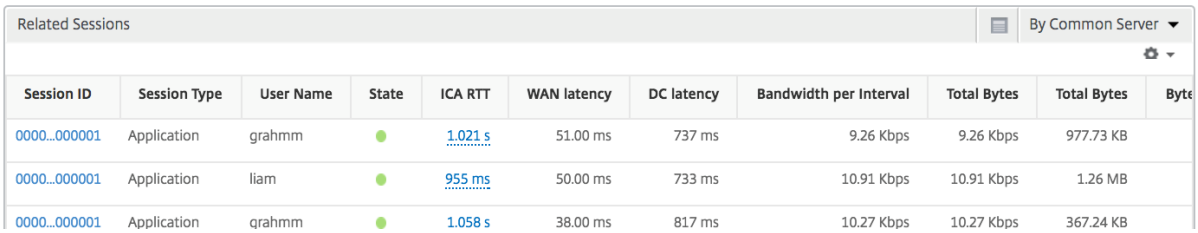
メトリックス	説明
クライアント側の再転送	NetScaler ADC とエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	NetScaler ADC とエンドユーザー間の接続で再送信タイムアウトが発生した回数。
Server side fast RTO	NetScaler ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。
間隔あたりの帯域幅	特定の期間にセッションで使用された帯域幅です。
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。



Active Applications 「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。このリレーションシップは、共通サーバーまたは共通 NetScaler ADC として選択できます。



アプリケーションビューのレポートとメトリクス

このビューのレポートとメトリックは、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. サポートされている Web ブラウザを使用して、NetScaler ADM にログオンします。
2. 「**Analytics** 」>「**HDX Insight** 」>「アプリケーション」の順に選択します。

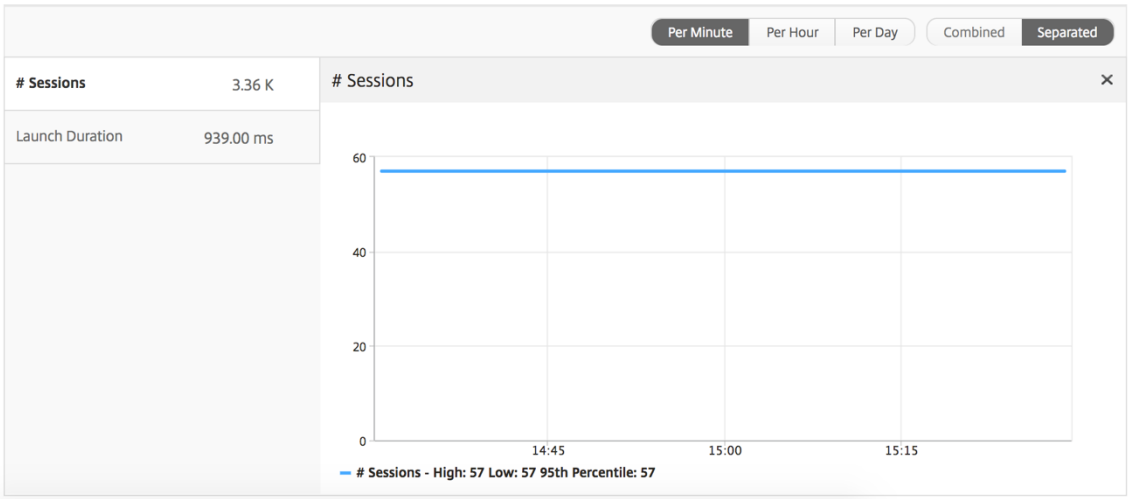
［**Summary**］ビュー

Summary ビューには、選択した期間中にログインしたすべてのアプリケーションのレポートが表示されます。

以下のメトリクスとレポートでは、明確な記載がない限り選択した期間の対応する値が表示されます。

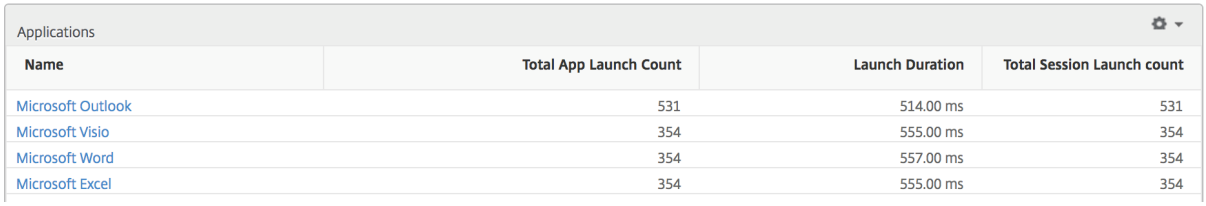
折れ線グラフ

メトリック	説明
セッション	特定の期間の合計セッション数。
起動時間	アプリケーションの起動にかかった平均時間。



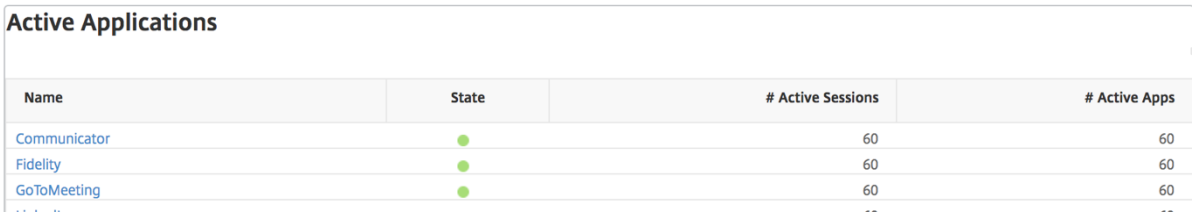
アプリケーション概要レポート

メトリックス	説明
名前	Citrix Virtual Apps 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 Apps 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 Apps 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

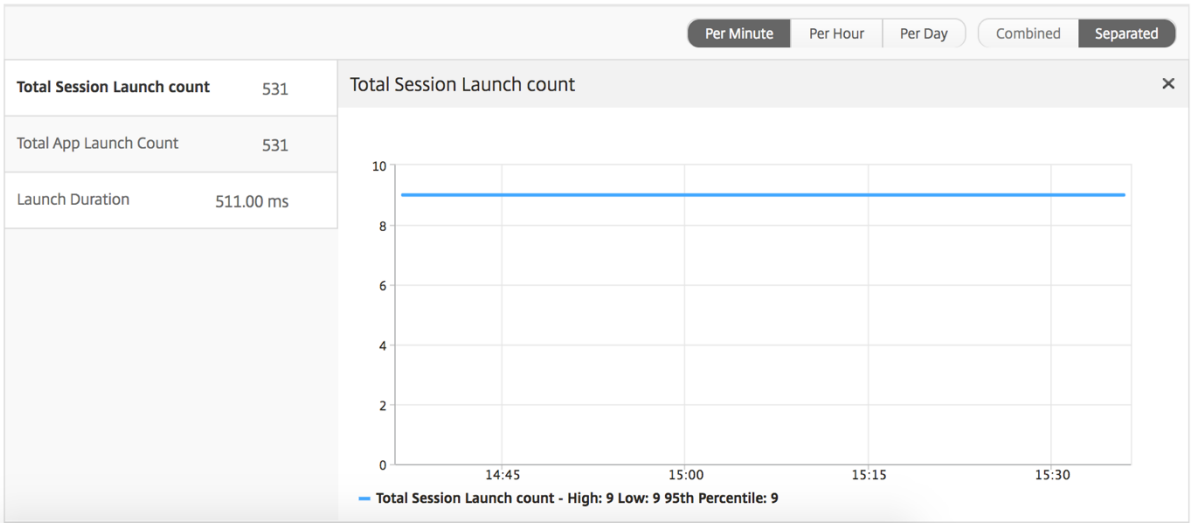
メトリックス	説明
名前	Citrix Virtual Apps の名前。
状態	アプリケーションの状態を表示します。緑-アクティブ、赤-非アクティブ
アクティブなセッション数	特定の期間にこのアプリケーションを使用したアクティブなユーザーセッション数。
アクティブなアプリケーション数	このアプリケーションのアクティブなセッション数。



しきい値レポート　しきい値レポートは、選択した期間にエンティティがアプリケーションとして選択された場合に違反したしきい値の数を示します。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。



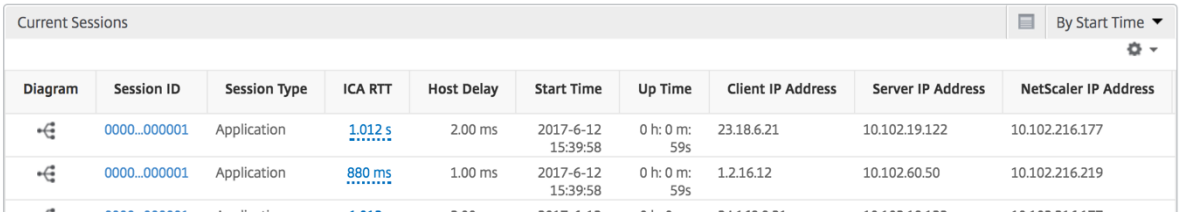
現在のセッションレポート

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。

メトリックス	説明
ホストの遅延	サーバーネットワークが原因で NetScaler ADC を通過する ICA トラフィックの平均遅延。
間隔あたりの帯域幅	特定の期間にセッションで使用された帯域幅です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
インターバルあたりのバイト数	特定の期間にセッションで使用されたバイト数。
開始時刻	セッションの開始時間。
アップタイム	セッションの実行時間
クライアント IP アドレス	エンドユーザーの IP。
サーバー IP アドレス	バックエンド/Citrix Virtual Apps サーバー IP。
NetScaler IP Address	NetScaler の管理 IP（NSIP）。
クライアントの種類	レシーバタイプ-Citrix Windows クライアント
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値（[Yes］または［No]）。セッションがマルチストリーム ICA かどうかを表します。
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。たとえば、NetScaler Gateway のユーザー/透過モードなどです。
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。

メトリックス	説明
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。
サーバー側の再転送	NetScaler ADC とバックエンドサーバー間の接続で再送信されたパケットの数。
クライアント側の再転送	NetScaler ADC とエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
クライアント側のゼロ ウィンドウ サイズ イベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがア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。

メトリックス	説明
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 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。



[アプリケーションセッションごと] 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。

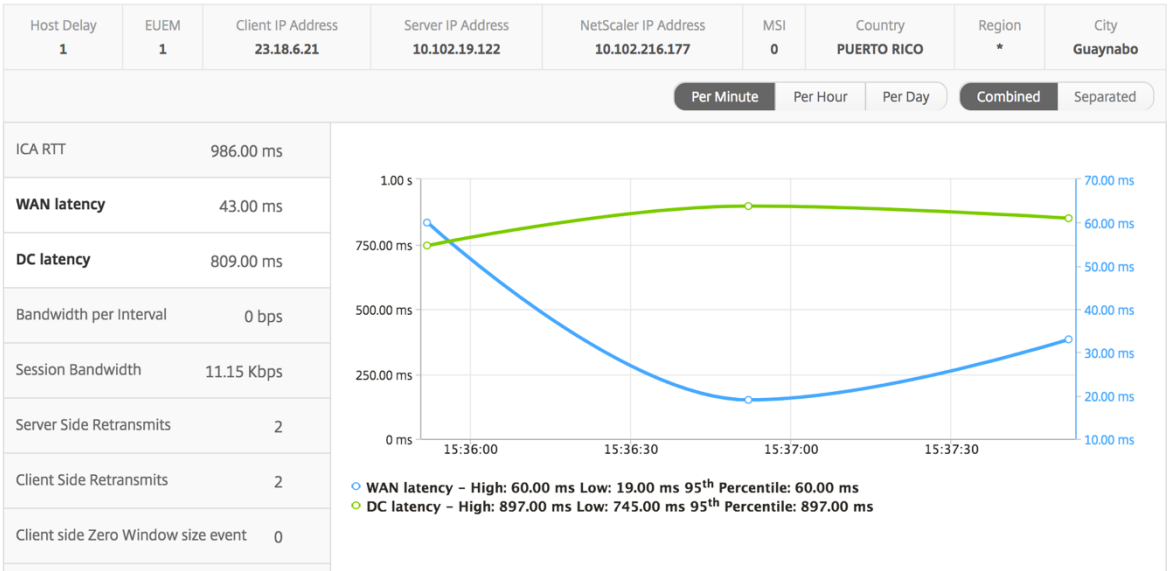
セッション・レポートを表示するには、次の手順に従います。

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. 「**Analytics**」>「**HDX Insight**」>「アプリケーション」の順に選択します。
3. Application Summary レポートから特定のユーザーを選択します。
4. Current Sessions レポートからセッションを選択します。

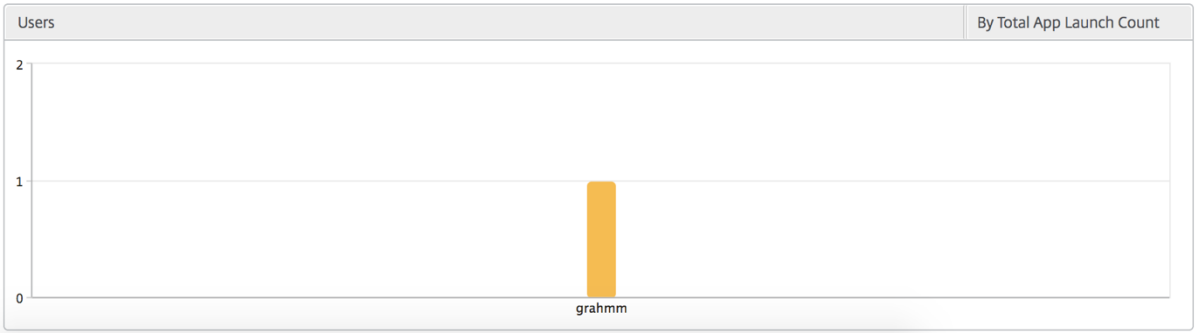
折れ線グラフ

メトリック	説明
セッション再接続	セッションが再接続された回数。
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。

メトリック	説明
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまで。
サーバー側のゼロ ウィンドウ サイズ イベント	ネットワークのサーバー側に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。
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とメトリクス

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. [アナリティクス] > [**HDX Insight**] > [デスクトップ] に移動します。

[**Summary**] ビュー

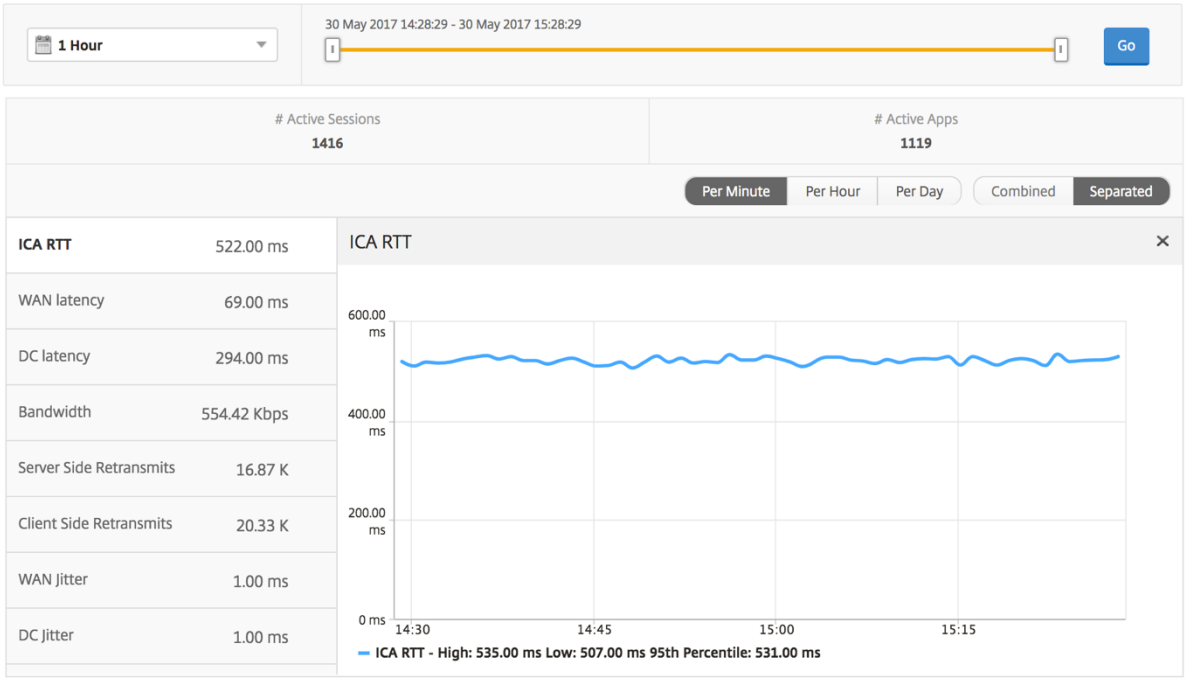
概要ビューには、選択したタイムライン中にログインしたすべての Citrix Virtual Desktops のレポートが表示されます。

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

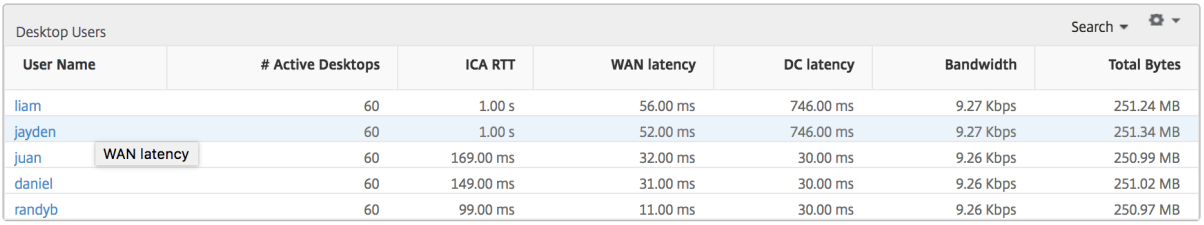
メトリック	説明
アクティブセッション	この数字は、アクティブな Citrix Virtual Apps and Desktops セッションの数を示します。
アクティブなアプリケーション数	この数字は、アクティブな Citrix Virtual Apps セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。

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 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。



デスクトップサマリーレポート

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 Desktops 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。

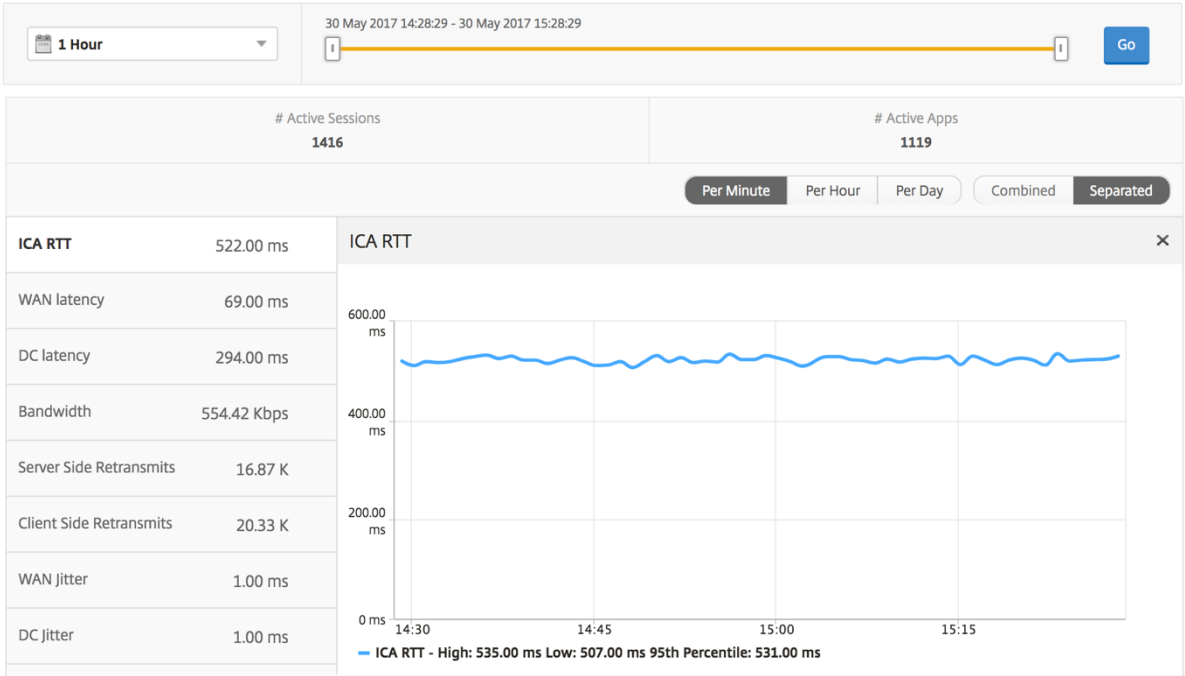
特定のデスクトップビューに移動するには**:**

1. サポートされている Web ブラウザを使用して、Citrix ADM にログオンします。
2. [分析**] > [HDX Insight] > [**デスクトップ] に移動します。
3. デスクトップの概要レポートから特定のデスクトップを選択します。

折れ線グラフ

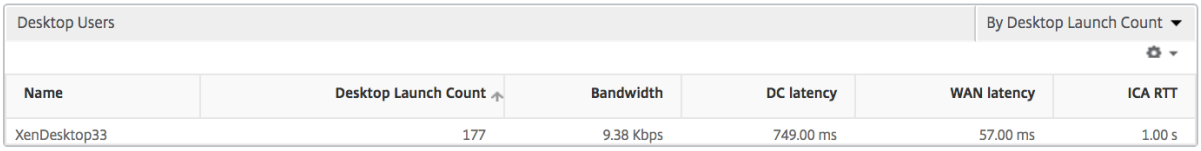
メトリック	説明
アクティブセッション	この数字は、アクティブな Citrix Virtual Apps and Desktops セッションの数を示します。
アクティブなアプリケーション数	この数字は、アクティブな Citrix Virtual Apps セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC か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。

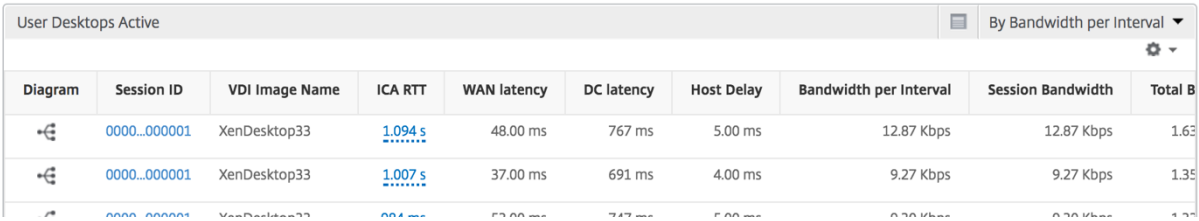


ユーザーデスクトップアクティブ/非アクティブレポート　以下のメトリクスは、[Bandwidth per Interval]、[Session Reconnects]、および［ACR Counts］を基準にしてソートできます。

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 ADC を通過する ICA トラフィックの平均遅延。
間隔あたりの帯域幅	特定の期間にセッションで使用された帯域幅です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
インターバルあたりのバイト数	特定の期間にセッションで使用されたバイト数。
開始時刻	セッションの開始時間。
アップタイム	セッションの実行時間

メトリックス	説明
クライアント IP アドレス	エンドユーザーの IP。
サーバー IP アドレス	バックエンド/Citrix Virtual Apps サーバー IP。
NetScaler IP Address	NetScaler の管理 IP（NSIP）。
クライアントの種類	レシーバタイプ-Citrix Windows クライアント
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値（[Yes］または［No]）。セッションがマルチストリーム ICA かどうかを表します。
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。たとえば、NetScaler Gateway のユーザー/透過モードなどです。
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。

メトリックス	説明
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。
サーバー側の再転送	NetScaler ADC とバックエンドサーバー間の接続で再送信されたパケットの数。
クライアント側の再転送	NetScaler ADC とエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
クライアント側のゼロ ウィンドウ サイズ イベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがア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	



[デスクトップセッションごと] ビュー

デスクトップごとのセッションビューでは、選択した特定の Citrix Virtual Desktop セッションのレポートが表示されます。

デスクトップ・セッション・ビューに移動するには:

1. サポートされている Web ブラウザを使用して、Citrix ADM にログオンします。

2. [分析**] > [HDX Insight] > [**デスクトップ] に移動します。
3. デスクトップ 概要レポートから特定のデスクトップを選択します。
4. 現在のセッションレポートからセッションを選択します。

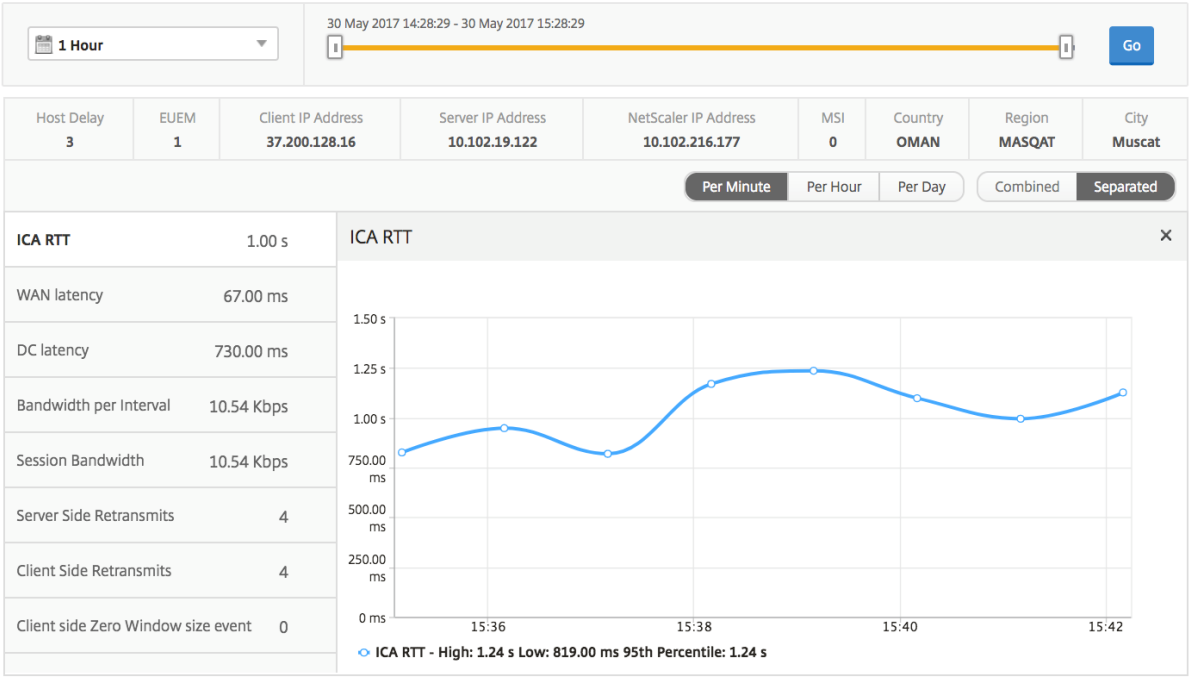
時系列グラフ　［Per User Session］ビューには、選択したユーザーのセッションに関するレポートが表示されます。

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. [**Analytics**] > [**HDX Insight**] > [ユーザー] に移動します。
3.「ユーザー 概要レポート」セクションから特定のユーザー を選択します。
4.「現在のセッション」または「終了したセッション」列からセッションを選択します。

メトリック	説明
セッション再接続	この数字は、アクティブな Citrix Virtual Apps and Desktops セッションの数を示します。
ACR 数	この数字は、アクティブな Citrix Virtual Apps 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。

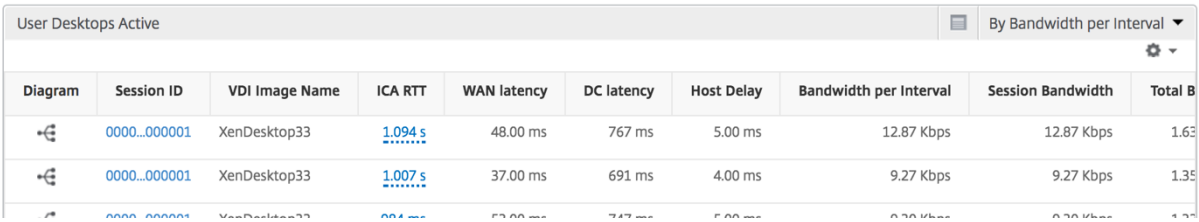


関連デスクトップセッションレポート　以下のメトリクスは、[Bandwidth per Interval]、[Session Reconnects]、および［ACR Counts］を基準にしてソートできます。

メトリックス	説明
セッション ID	ICA セッションの一意の ID。
セッションの種類	アプリケーション/デスクトップ。
状態	緑はアクティブなセッション、赤は非アクティブなセッション。
ホストの遅延	サーバーネットワークが原因で NetScaler ADC を通過する ICA トラフィックの平均遅延。

メトリックス	説明
間隔あたりの帯域幅	特定の期間にセッションで使用された帯域幅です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
インターバルあたりのバイト数	特定の期間にセッションで使用されたバイト数。
開始時刻	セッションの開始時間。
アップタイム	セッションの実行時間
クライアント IP アドレス	エンドユーザーの IP。
サーバー IP アドレス	バックエンド/Citrix Virtual Apps サーバー IP。
NetScaler IP Address	NetScaler の管理 IP（NSIP）。
クライアントの種類	レシーバタイプ-Citrix Windows クライアント
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値（[Yes］または［No]）。セッションがマルチストリーム ICA かどうかを表します。
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。たとえば、NetScaler Gateway のユーザー/透過モードなどです。
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。

メトリックス	説明
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、NetScaler Gateway と VDI、CVAD、または StoreFront サーバーの間です。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。
サーバー側の再転送	NetScaler ADC とバックエンドサーバー間の接続で再送信されたパケットの数。
クライアント側の再転送	NetScaler ADC とエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
クライアント側のゼロ ウィンドウ サイズ イベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがア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 ADC インスタンスに焦点を当てています。

[インスタンス**]** ビューにナビゲートするには、次の手順を実行します。

1. サポートされている Web ブラウザを使用して、NetScaler ADM にログオンします。
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

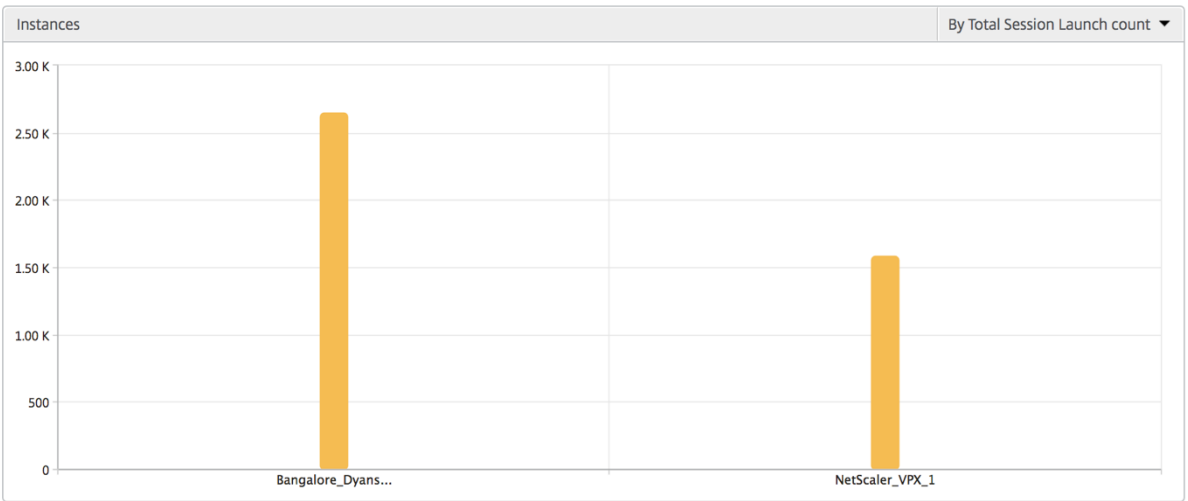
インスタンス概要ビュー

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。

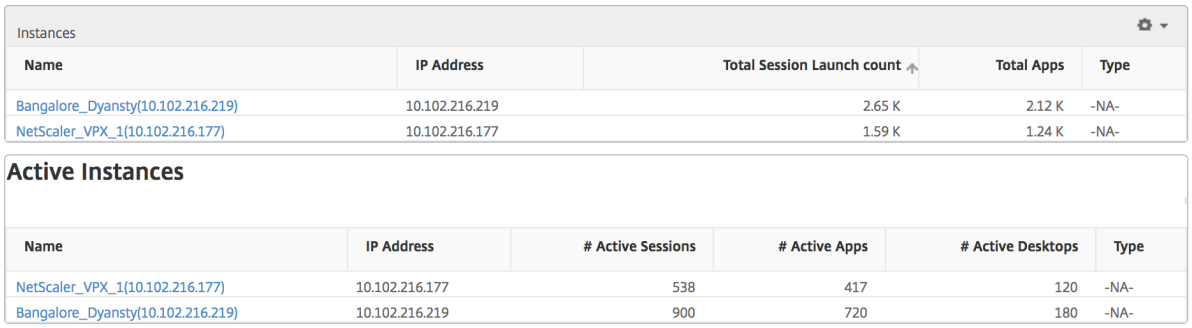
インスタンスバーグラフ

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にあるドロップダウンから選択できる合計アプリ。



インスタンス/アクティブインスタンスの概要レポート

メトリックス	説明
名前	NetScaler ADC インスタンスのホスト名。
IP アドレス	NetScaler の IP アドレスです。
セッションの起動数合計	特定の期間に作成された一意のユーザーセッションの合計数です。
アプリケーション合計数	特定の期間に起動された一意のアプリケーションの合計数です。
種類	-



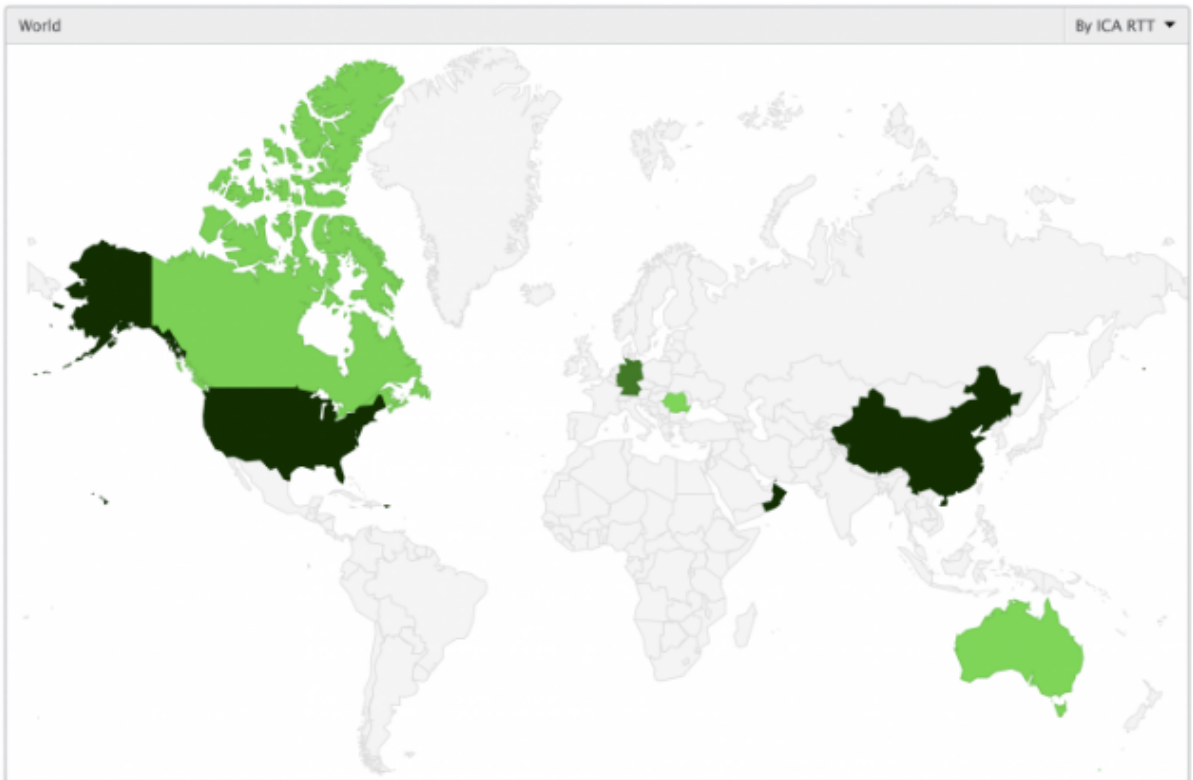
しきい値レポート　しきい値レポートは、選択した期間内に エンティティ がインスタンスとして選択された場合に、違反したしきい値の数を表します。詳細については、「しきい値の作成方法」を参照してください。

スキップフロー　スキップフローは、ICA 接続の解析が省略されたレコードのことです。これは、サポートされていない Citrix Virtual Apps and Desktops のバージョン、サポートされていないバージョンのレシーバーまたはレシーバータイプを使用するなど、複数の理由で発生する可能性があります。このテーブルでは、IP アドレスとスキップフロー数が示されます。こうしたセッションは監視対象から除外されるため、これらの Citrix Receiver はホワイトリストに登録しないことをお勧めします。

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。管理者にはシステムの［World］ビューが用意されており、地域をクリックするだけで特定の国、さらには都市へとドリルダウンすることができます。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［World Map］では以下の詳細を確認でき、各メトリックの密度がヒートマップ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

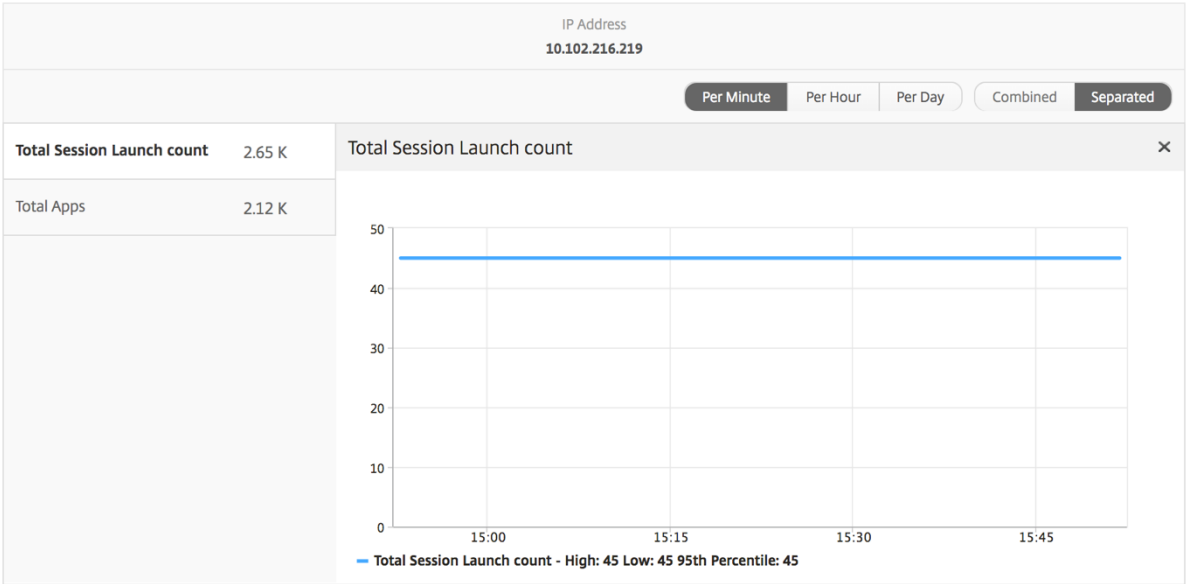
インスタンスごとのビューでは、選択した特定の NetScaler ADC インスタンスに関する詳細なエンドユーザーエクスペリエンスレポートが提供されます。

[インスタンス**]** ビューにナビゲートするには、次の手順を実行します。

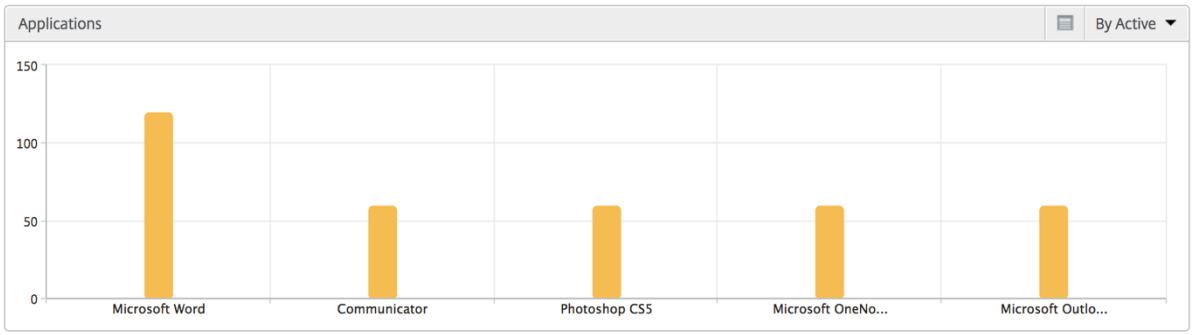
1. サポートされている Web ブラウザを使用して、NetScaler ADM にログオンします。
2. [分析**] > [HDX Insight] > [**インスタンス] に移動します。
3. インスタンスの概要レポートから特定のインスタンスを選択します。

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 Apps 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。

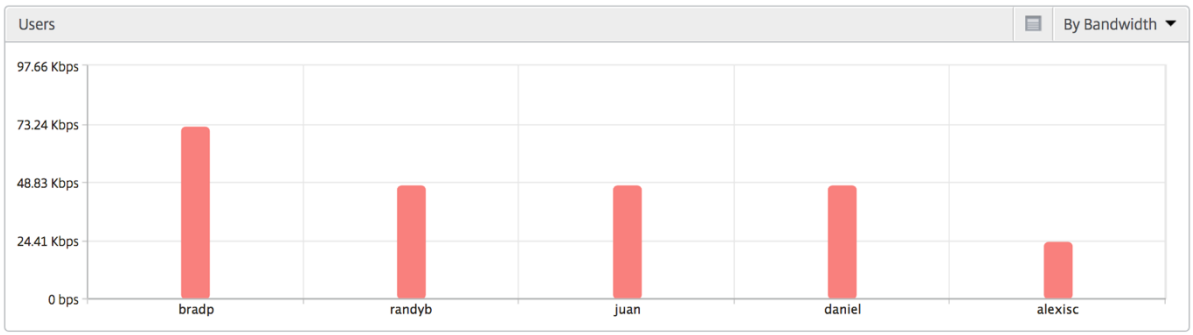


アプリケーション棒グラフ　アクティブなアプリ、合計セッション起動回数、合計アプリ起動回数、または起動期間の各基準別に上位 5 個のアプリケーションが示されます。



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。

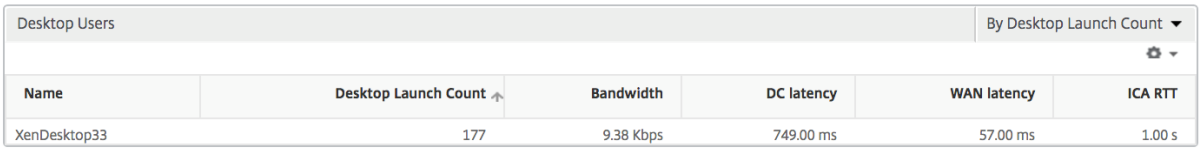
- 帯域幅
- WAN 遅延
- DC の遅延
- ICA 往復時間



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。

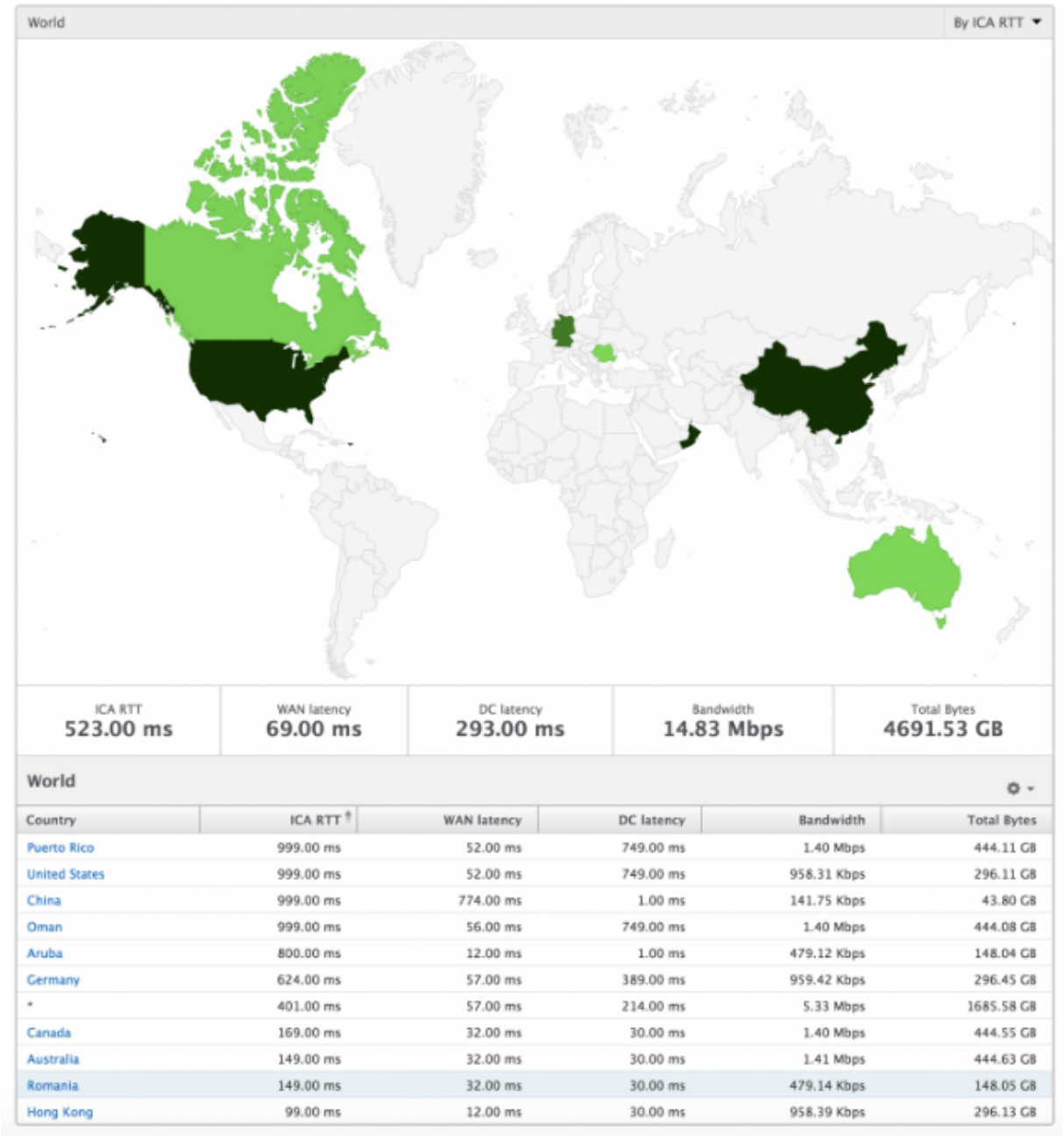
メトリックス	説明
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、NetScaler ADC からエンドユーザーまでです。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。



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。管理者にはシステムの［World］ビューが用意されており、地域をクリックするだけで特定の国、さらには都市へとドリルダウンすることができます。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［World Map］では以下の詳細を確認でき、各メトリックの密度がヒートマップ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

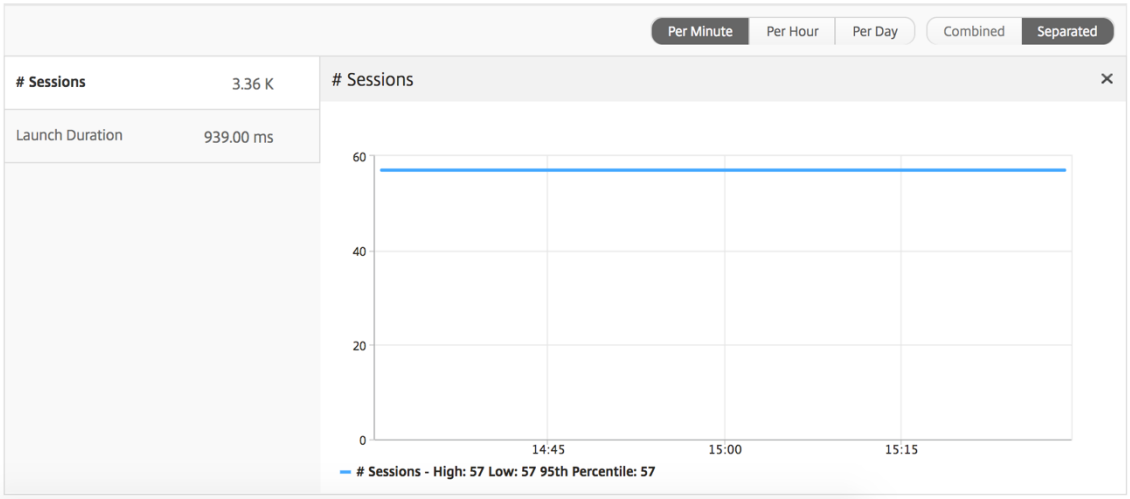
ライセンスビューには、NetScaler Gateway のライセンス情報が表示されます。

[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	選択した期間中に使用されている NetScaler Gateway CCU ライセンス。各カウントは、ユーザーセッションの数を表します。このカウントには、各ユーザーが起動したアプリケーションセッションおよびデスクトップセッションは含まれません。
総ライセンス数	お客様が利用できる NetScaler Gateway CCU ライセンスの合計数。



しきい値レポート　しきい値レポートは、選択した期間内に エンティティ がライセンスとして選択されている場合に、違反したしきい値の数を表します。詳細については、「しきい値の作成方法」を参照してください。

Application ビューのレポートとメトリック

February 6, 2024

このビューのレポートと指標は、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. サポートされている Web ブラウザを使用して、NetScaler ADM にログオンします。
2.「**Analytics** 」>「**HDX Insight** 」>「アプリケーション」の順に選択します。

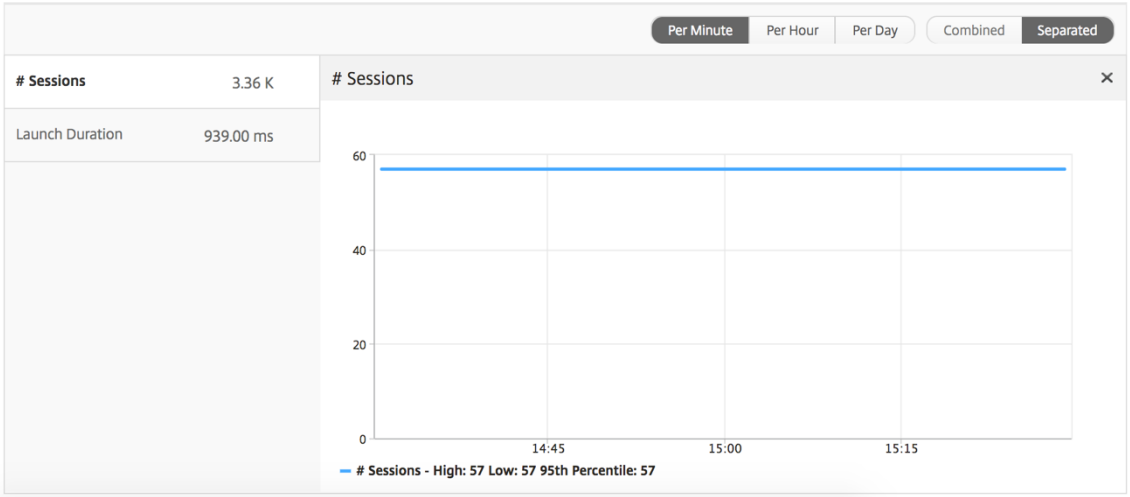
[**Summary**] ビュー

Summary ビューには、選択した期間中にログインしたすべてのアプリケーションのレポートが表示されます。

以下のメトリクスとレポートでは、明確な記載がない限り選択した期間の対応する値が表示されます。

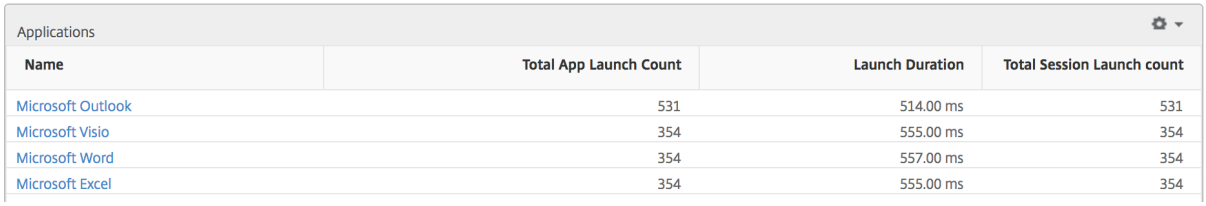
折れ線グラフ

メトリックス	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。



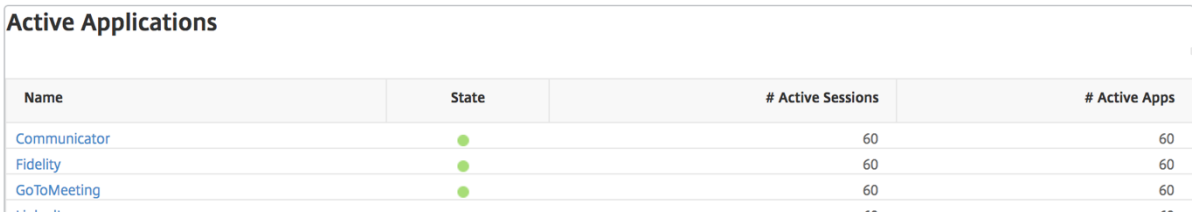
Applications Summary レポート

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 Apps 総数。
起動期間	Citrix 仮想アプリケーションの起動にかかった平均時間。



Active Application 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。

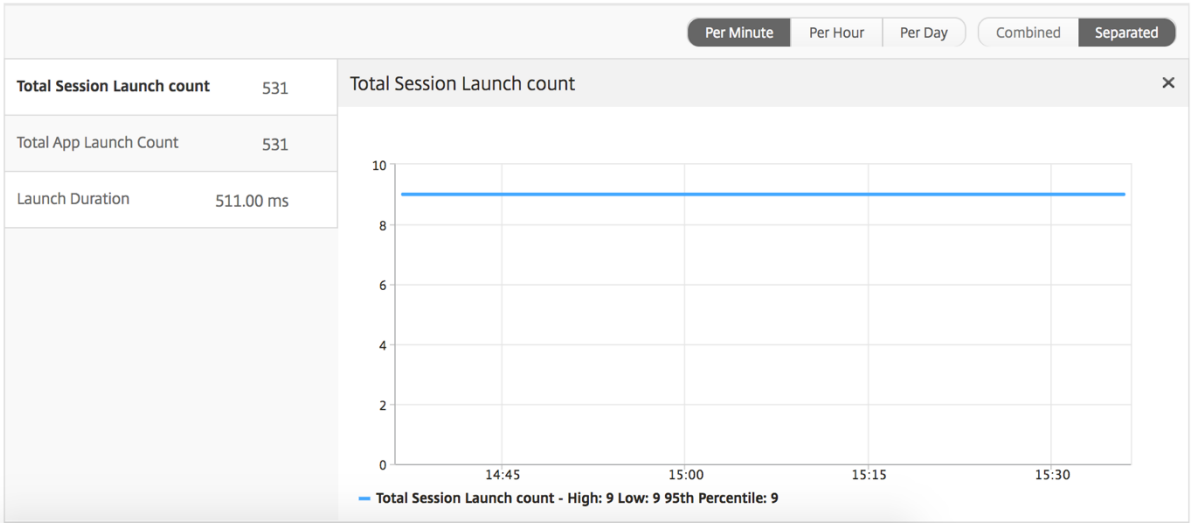


しきい値レポート

しきい値レポートは、選択した期間にエンティティがアプリケーションとして選択された場合に違反したしきい値の数を示します。 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。
起動時間	アプリケーションの起動にかかった平均時間。

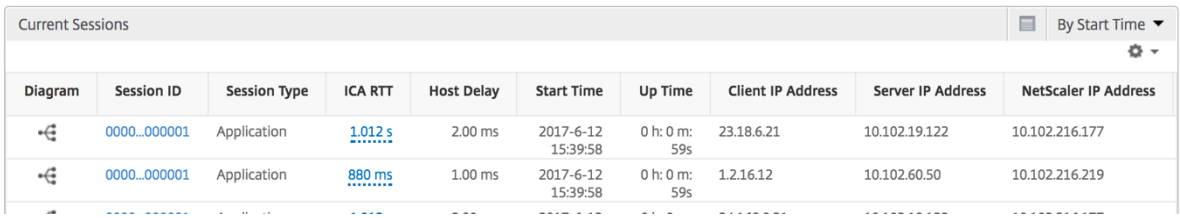


Current Sessions レポート

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	Citrix Receiver の種類（Citrix Windows クライアントなど）。
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値（[Yes] または [No]）。セッションがマルチストリーム ICA かどうかを表します。

メトリックス	説明
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。たとえば、NetScaler Gateway のユーザー/透過モードなどです。
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延です（すなわち NetScaler からエンドユーザー）。
DC 遅延	ネットワークのサーバー側に起因する遅延です（すなわち NetScaler からバックエンドサーバー）。
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 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。
ユーザー名	この特定の Citrix Virtual Apps 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 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。



Per Application Session ビュー

Per Application Session ビューには、選択した特定のアプリケーションセッションのレポートが表示されます。

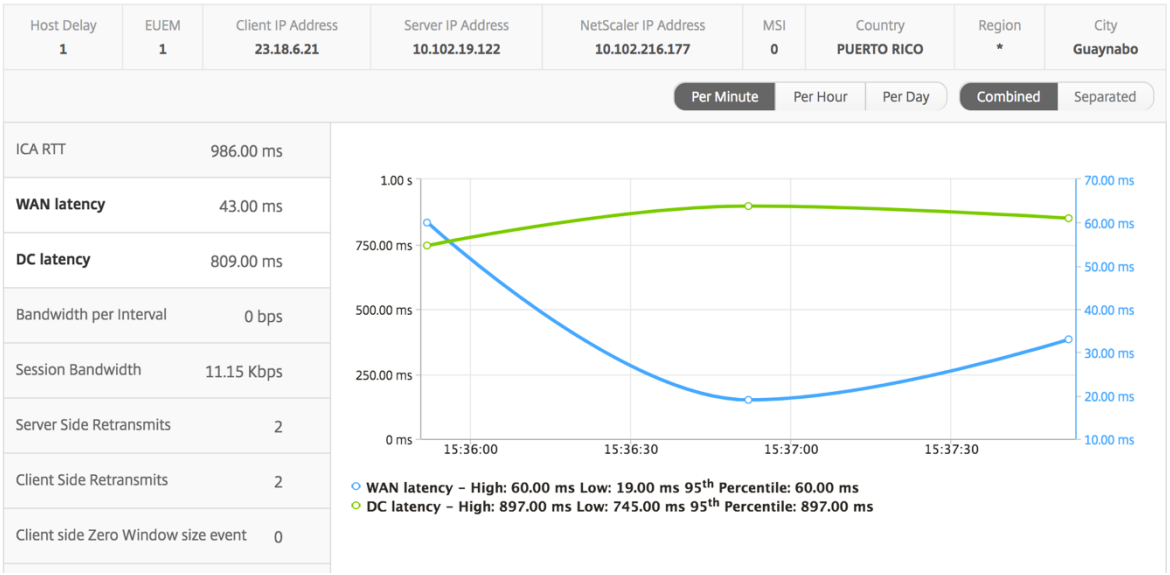
セッション・レポートを表示するには、次の手順に従います。

1. 「**Analytics** 」>「**HDX Insight** 」>「アプリケーション」の順に選択します。
2. Application Summary レポートから特定のユーザーを選択します。
3. Current Sessions レポートからセッションを選択します。

折れ線グラフ

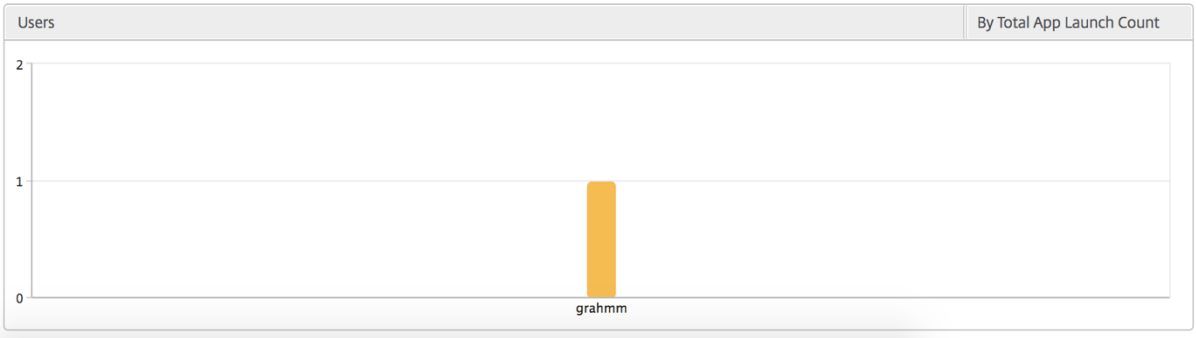
メトリックス	説明
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延です（すなわち NetScaler からエンドユーザー）。
サーバー側のゼロ ウィンドウ サイズ イベント	ネットワークのサーバー側に起因する遅延です（すなわち NetScaler からバックエンドサーバー）。
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 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。

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。



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. 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。

[**Summary**] ビュー

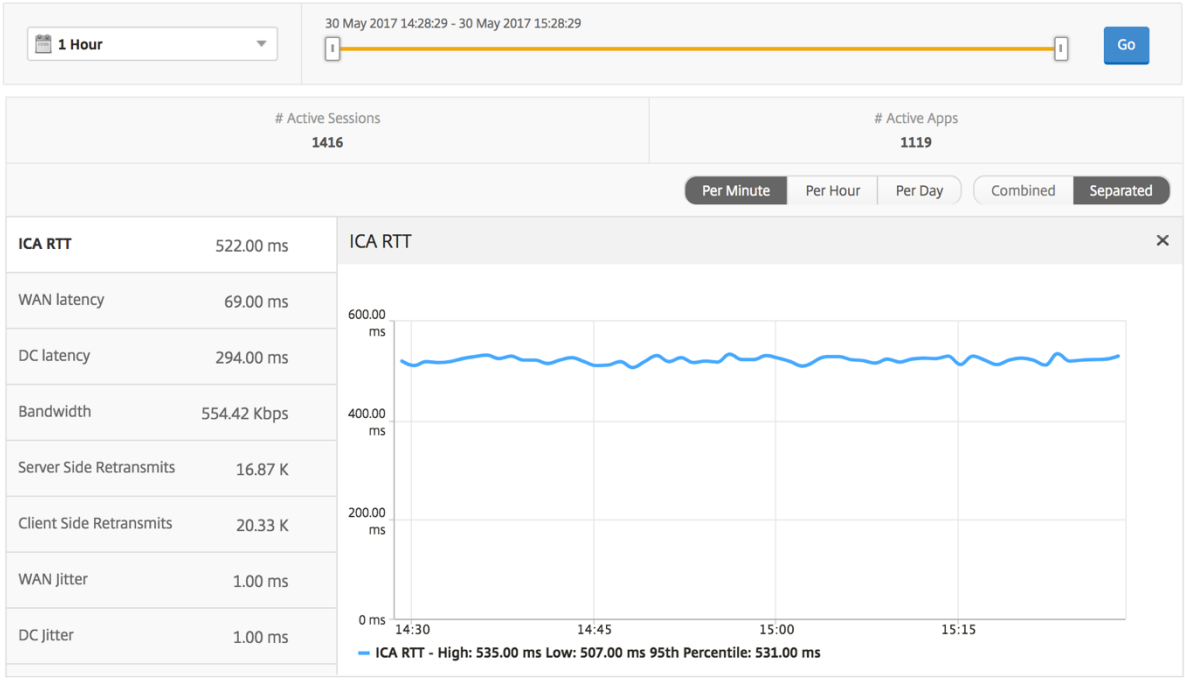
概要ビューには、選択したタイムライン中にログインしたすべての Citrix Virtual Desktops のレポートが表示されます。

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 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（すなわち NetScaler からエンドユーザー）。
DC 遅延	ネットワークのサーバー側に起因する遅延です（すなわち NetScaler からバックエンドサーバー）。
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。

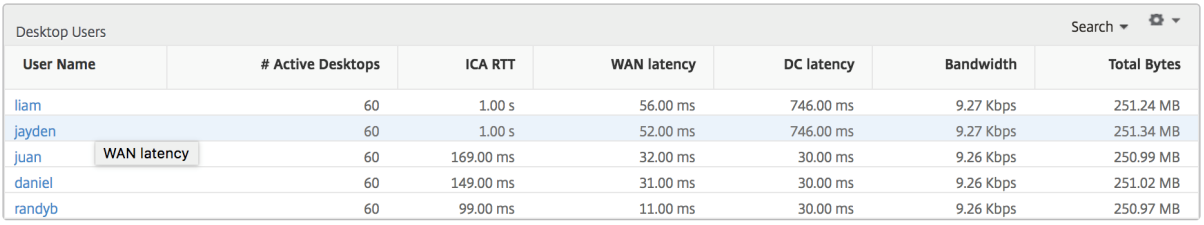
メトリックス	説明
Server side fast RTO	NetScaler とバックエンドサーバー間の接続で発生した再送信タイムアウトの回数です。
クライアント側のゼロ ウィンドウ サイズ イベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがアドバタイズした回数を表します。
サーバー側のゼロ ウィンドウ サイズ イベント	このカウンターは、TCP ウィンドウサイズがゼロであることをサーバーがアドバタイズした回数を表します。



デスクトップ概要レポート

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。

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（すなわち NetScaler からエンドユーザー）。
DC 遅延	ネットワークのサーバー側に起因する遅延です（すなわち NetScaler からバックエンドサーバー）。
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。

[**Per Dekstop**] 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。

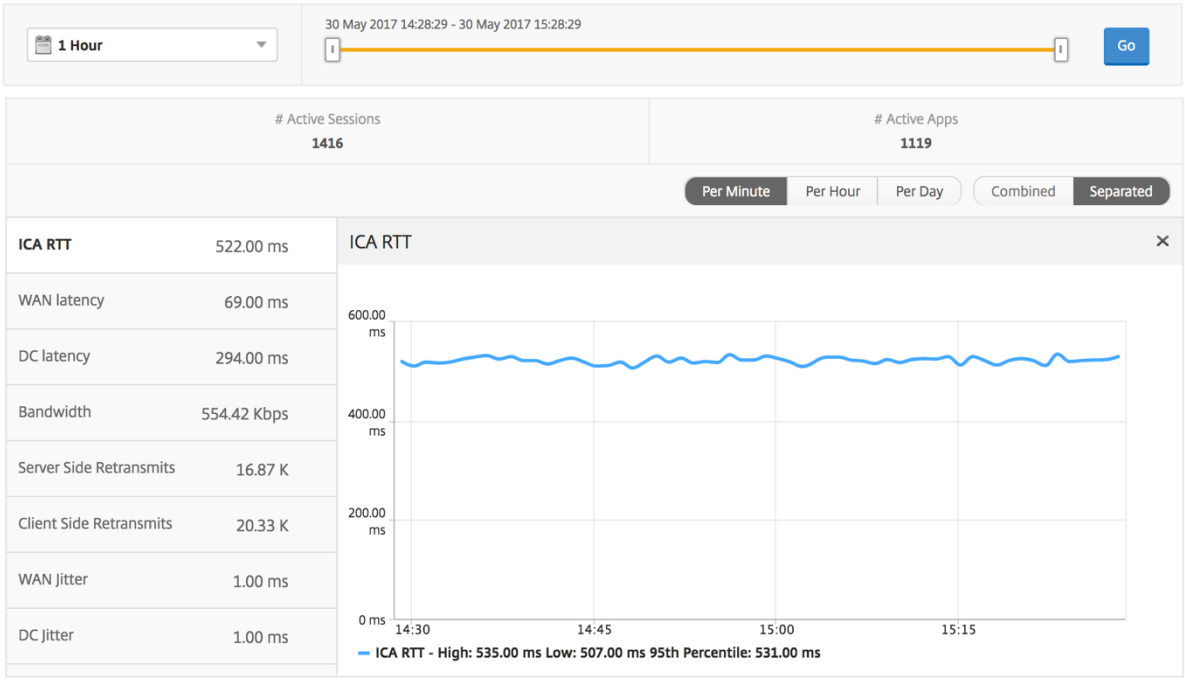
特定のデスクトップビューに移動するには**:**

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。

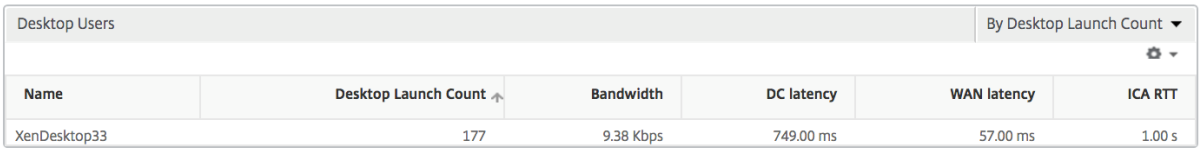
メトリックス	説明
アクティブなアプリケーション数	この数字は、アクティブな Citrix Virtual Apps セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延です（すなわち NetScaler からエンドユーザー）。
DC 遅延	ネットワークのサーバー側に起因する遅延です（すなわち NetScaler からバックエンドサーバー）。
帯域幅	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。



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（すなわち NetScaler からバックエンドサーバー）。
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（すなわち NetScaler からエンドユーザー）。
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。



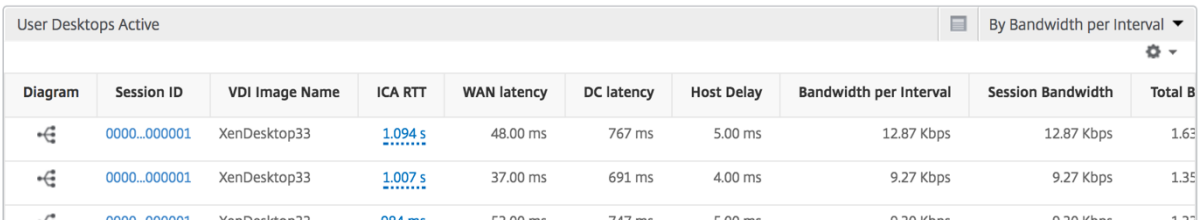
ユーザーデスクトップのアクティブ/非アクティブレポート

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	Citrix Receiver 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。

メトリックス	説明
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。たとえば、NetScaler Gateway のユーザー/透過モードなどです。
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延です（すなわち NetScaler からエンドユーザー）。
DC 遅延	ネットワークのサーバー側に起因する遅延です（すなわち NetScaler からバックエンドサーバー）。
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。

メトリックス	説明
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 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。
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	



[**Per Dekstop Session**] ビュー

デスクトップごとのセッションビューでは、選択した特定の Citrix Virtual Desktop セッションのレポートが表示されます。

デスクトップ・セッション・ビューに移動するには:

1. [アナリティクス] > [**HDX Insight**] > [デスクトップ] に移動します。
2. デスクトップ 概要レポートから特定のデスクトップを選択します。
3. 現在のセッションレポートからセッションを選択します。

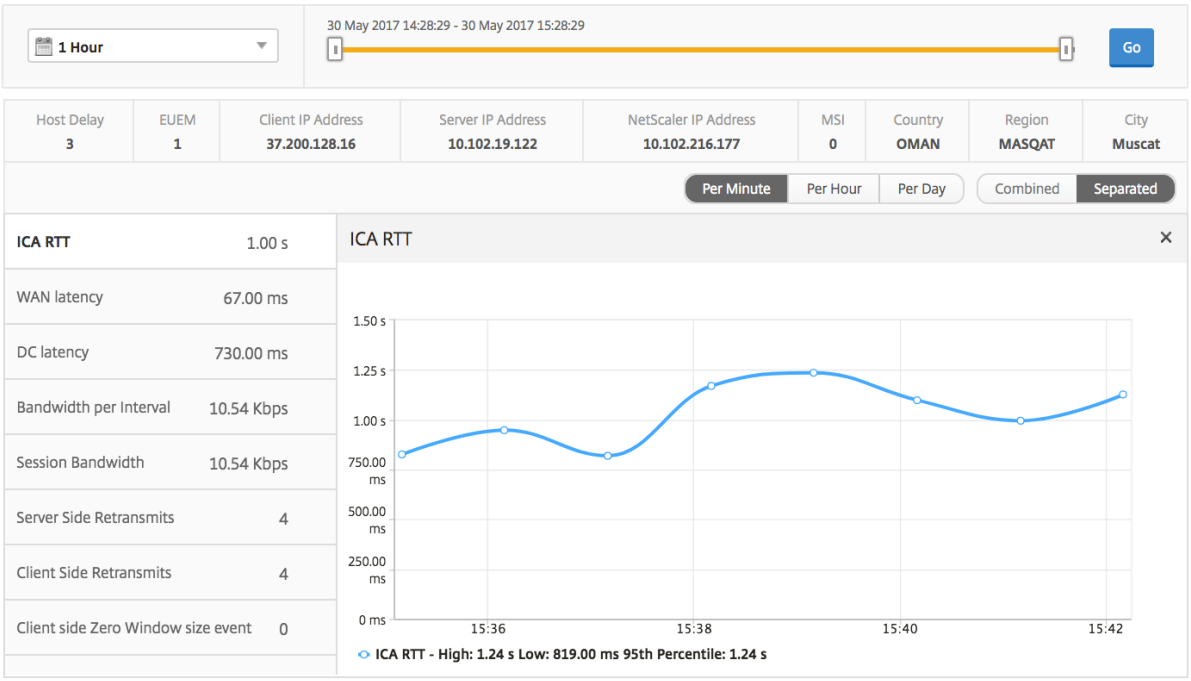
時系列グラフ

[Per User Session] ビューには、選択したユーザーのセッションに関するレポートが表示されます。

選択したユーザーのセッションのメトリックを表示する手順は、次のとおりです。

1. [**Analytics**] > [**HDX Insight**] > [ユーザー] に移動します。
2.「ユーザー 概要レポート」セクションから特定のユーザー を選択します。
3.「現在のセッション」または「終了したセッション」列からセッションを選択します。

メトリック	説明
セッション再接続	この数字は、アクティブな Citrix Virtual 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 Apps 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（すなわち NetScaler からエンドユーザー）。
DC 遅延	ネットワークのサーバー側に起因する遅延です（すなわち NetScaler からバックエンドサーバー）。
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。



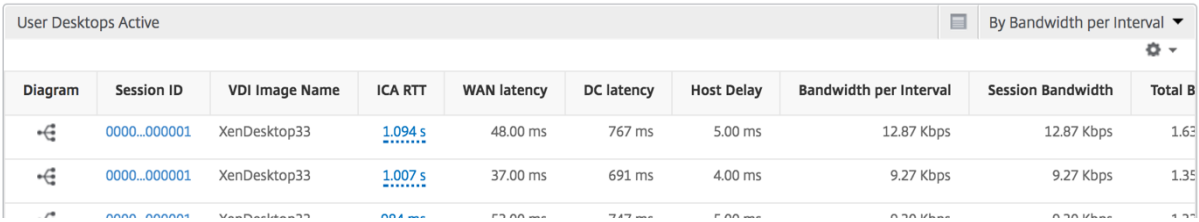
関連デスクトップセッションレポート

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。

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	Citrix Receiver の種類（Citrix Windows クライアントなど）。
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値（[Yes］または［No]）。セッションがマルチストリーム ICA かどうかを表します。
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。たとえば、NetScaler Gateway のユーザー/透過モードなどです。
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延です（すなわち NetScaler からエンドユーザー）。
DC 遅延	ネットワークのサーバー側に起因する遅延です（すなわち NetScaler からバックエンドサーバー）。
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 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。
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. サポートされている Web ブラウザを使用して、NetScaler ADM にログオンします。
2. **Analytics** > **HDX Insight** > ユーザー

[**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メトリック/レポートには、特に指定のない限り選択した期間のメトリック/レポートに対応する値が表示されます。

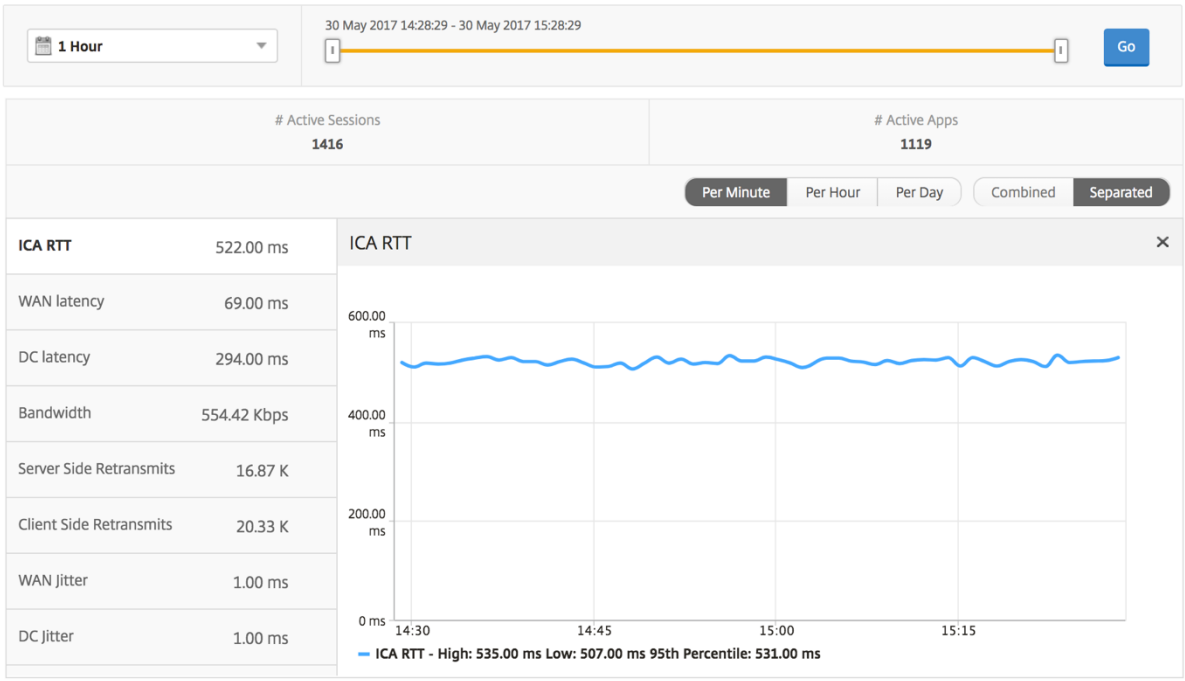
選択した期間を変更するには、次の手順に従います。

1. 期間のボックスの一覧またはスライダーを使用して、目的の期間を設定します。
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 Apps 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（すなわち NetScaler からエンドユーザー）。
DC 遅延	ネットワークのサーバー側に起因する遅延です（すなわち NetScaler からバックエンドサーバー）。
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。

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。
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。



[**User Summary**] 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 Apps and Desktops Desktops でそれぞれホスト されているアプリケーションまたはデスクトップを操作しているときにユーザーが経験するスクリーンラグです。

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（すなわち NetScaler からエンドユーザー）。
DC 遅延	ネットワークのサーバー側に起因する遅延です（すなわち NetScaler からバックエンドサーバー）。
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。
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。

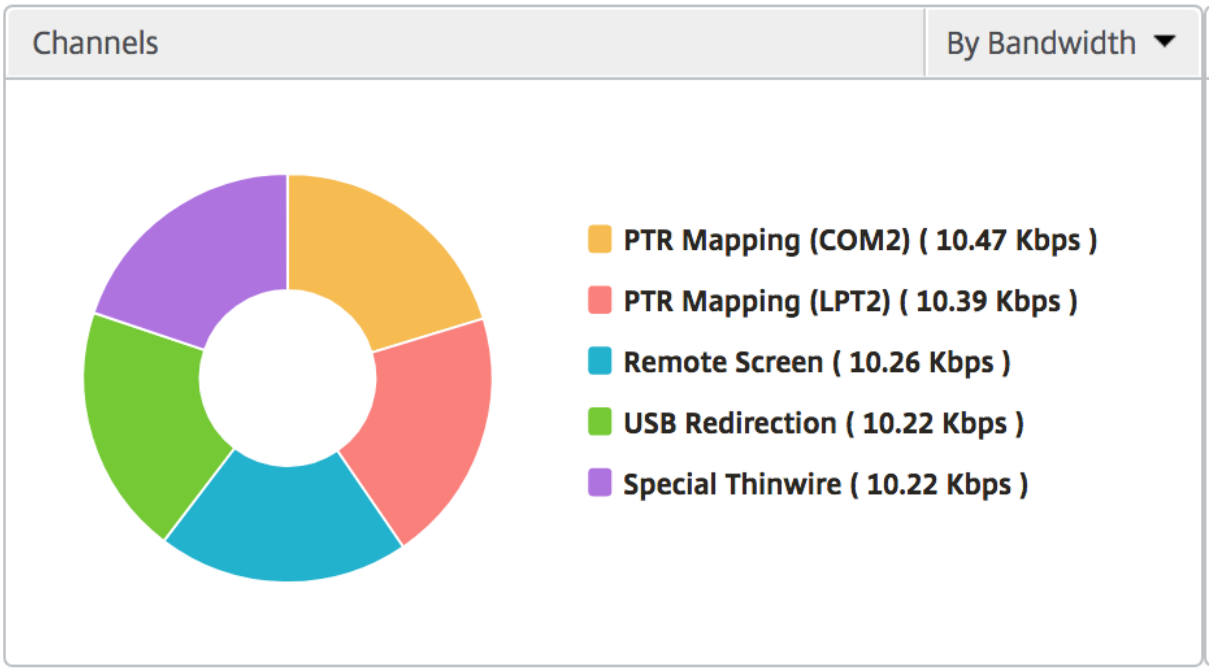
Users

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	

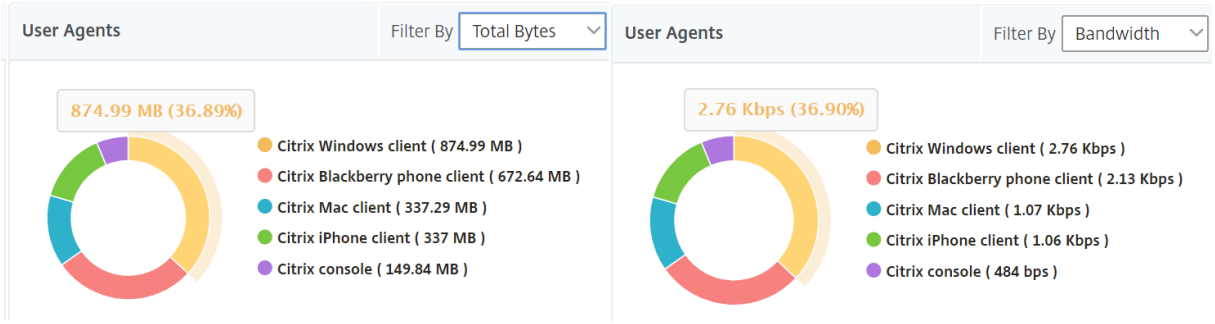
チャネル

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。



Thresholds Breach Count

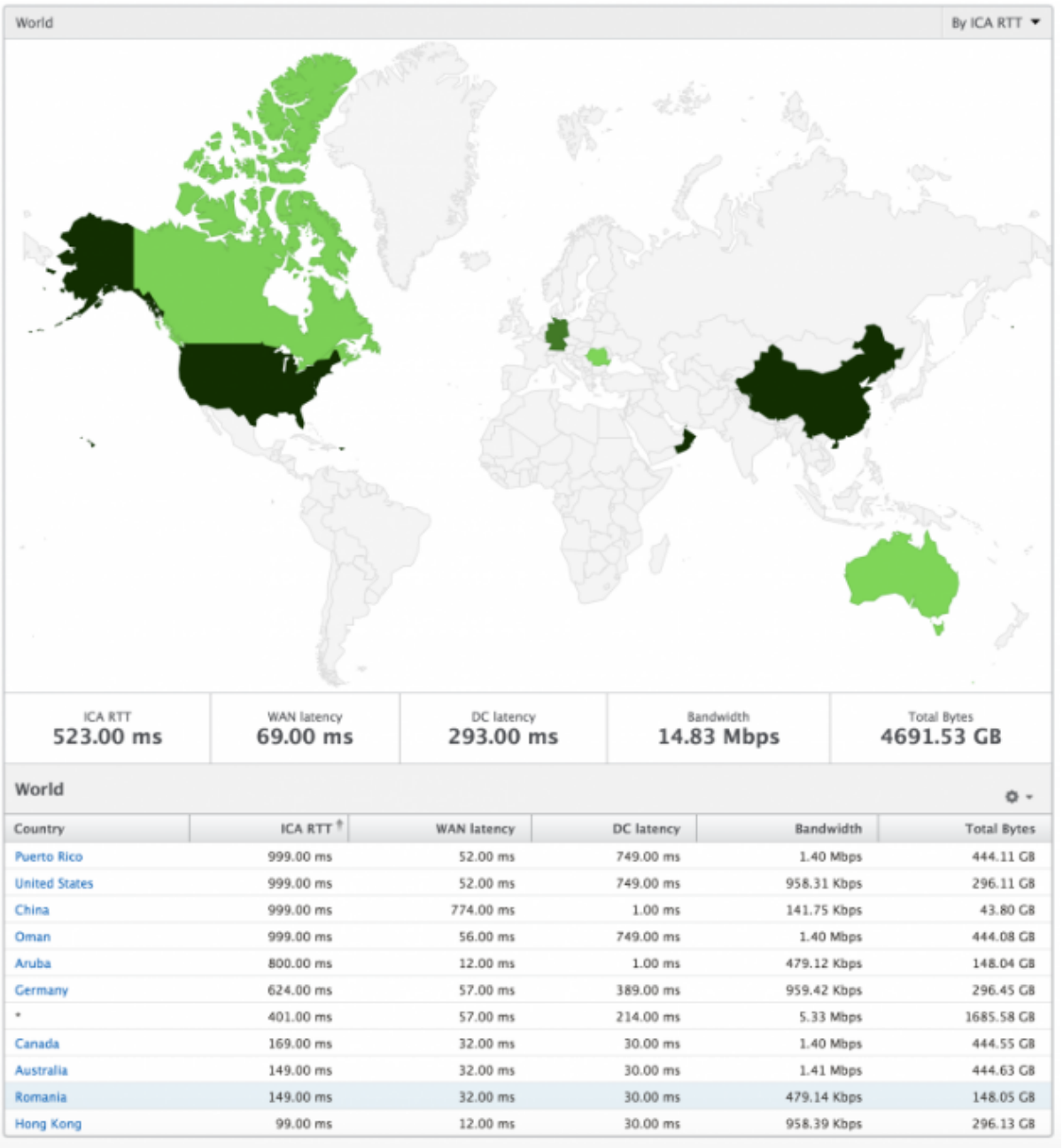
［Thresholds Breach Count］メトリックは、指定した期間において違反があったしきい値の数を表します。詳細については、「しきい値とアラートの作成方法」を参照してください。

World Map

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。管理者にはシステムの［World］ビューが用意されており、地域をクリックするだけで特定の国、さらには都市へとドリルダウンすることができます。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［World Map］では以下の詳細を確認でき、各メトリックの密度がヒートマップ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

[**Per User**] ビュー

[Per User] ビューには、選択した特定のユーザーについて詳細なエンドユーザーエクスペリエンスに関するレポートが示されます。

特定のユーザーのメトリックに移動する手順は、次のとおりです。

1. [**Analytics**] > [**HDX Insight**] > [ユーザー] に移動します。
2. [User Summary] レポートで目的のユーザーを選択します。

折れ線グラフ

折れ線グラフには、指定した期間における選択したユーザーのメトリックすべての概要が表示されます。

[**Current/Terminated Sessions**] 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	Citrix Receiver の種類（Citrix Windows クライアントなど）。
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値（[Yes] または [No]）。セッションがマルチストリーム ICA かどうかを表します。
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。たとえば、NetScaler Gateway のユーザー/透過モードなどです。

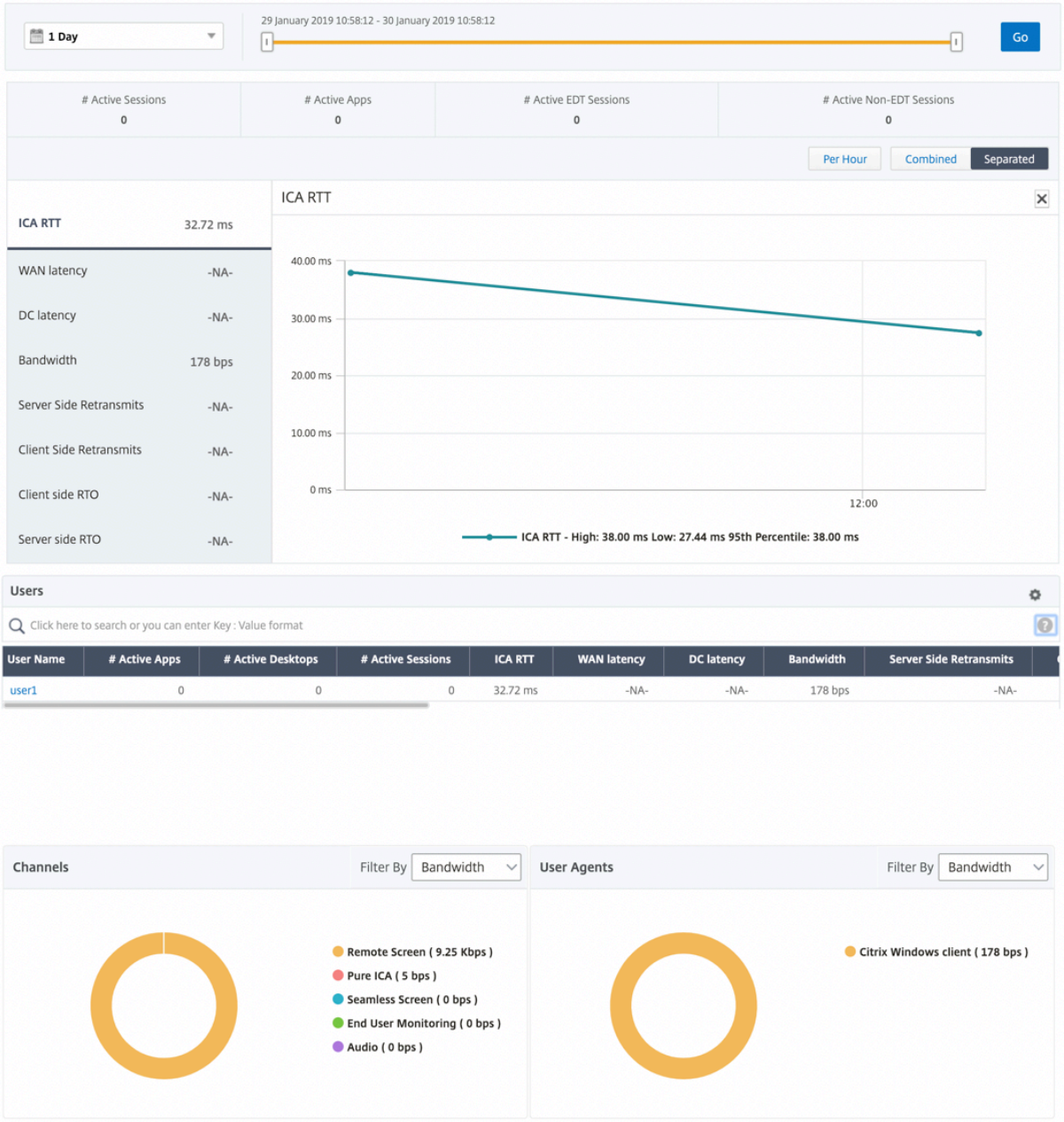
メトリックス	説明
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB ステータス	緑はアクティブ、赤は非アクティブ。
受け入れられる USB インスタンスの数	受け入れられた USB インスタンス数。
拒否された USB インスタンスの数	拒否された USB インスタンス数。
停止した USB インスタンスの数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェールオーバー	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps 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（すなわち NetScaler からエンドユーザー）。
DC 遅延	ネットワークのサーバー側に起因する遅延です（すなわち NetScaler からバックエンドサーバー）。
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。

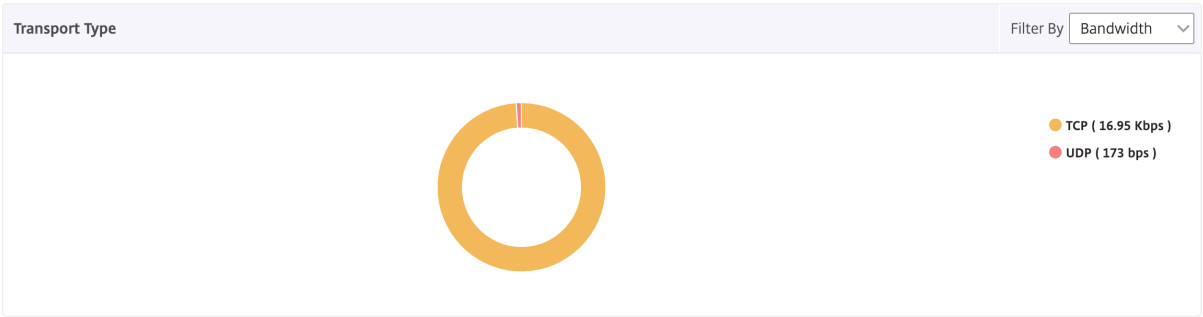
HDX Insight での **EDT** のサポート

NetScaler Application Delivery Management（ADM）では、HDX Insight ight の分析を表示するための啓発データトランスポート（EDT）がサポートされるようになりました。つまり、ADM は UDP と TCP の両方のプロトコルをサポートするようになりました。NetScaler Gateway の EDT サポートにより、Citrix Receiver を実行しているユーザーの仮想デスクトップの高品位セッション内ユーザーエクスペリエンスが保証されます。

HDX Insight は、アクティブセッションレポートの一部として、EDT セッションと非 EDT セッションの数を表示するようになりました。「ユーザー」(Users) テーブルには、システム内のすべてのユーザーの詳細なレポートが表示されます。この表には、WAN レイテンシー、DC レイテンシー、再送信、RTO などのメトリックが示されています。これらのメトリックのいくつかは、現在 TCP スタックから計算されるため、EDT セッションを持つユーザーには使用できません。したがって、これらは「NA」として表示されます。

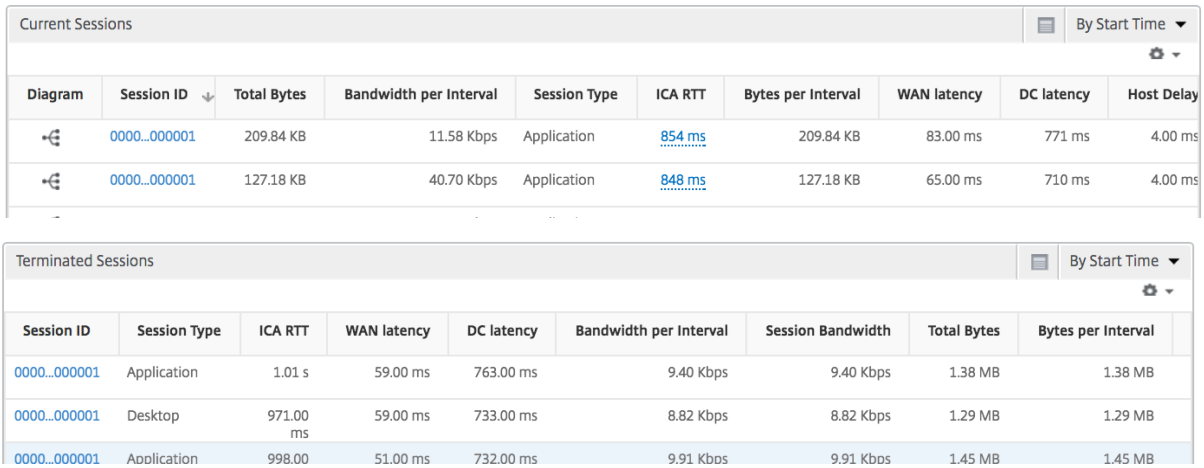


新しいドーナツグラフ が導入され、ユーザーが使用したプロトコルの種類に基づいて、ユーザーが消費した帯域幅と合計バイト数を確認できるようになりました。



NetScaler ADM 12.0 以降から入手可能な **HDX Insight** メトリック:

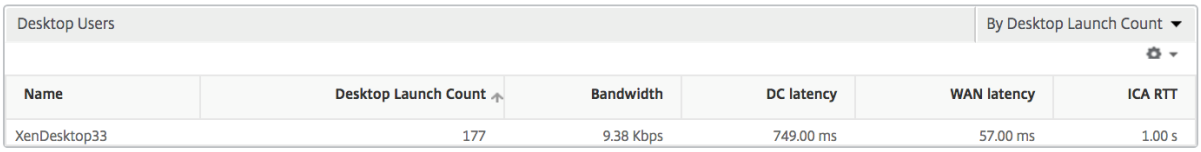
L7 Client-side Latency	ICA クライアントと NetScaler ADC インスタンスの間で観測された平均 L7 遅延時間。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。
L7 Server-side Latency	NetScaler ADC デバイスと Citrix Virtual Apps の間で観察された平均 L7 遅延。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。
違反の最大遅延	定義済みしきい値の違反が一定期間に発生した場合の、L7 遅延の最大値。
平均侵害待ち時間	システムが「L7 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

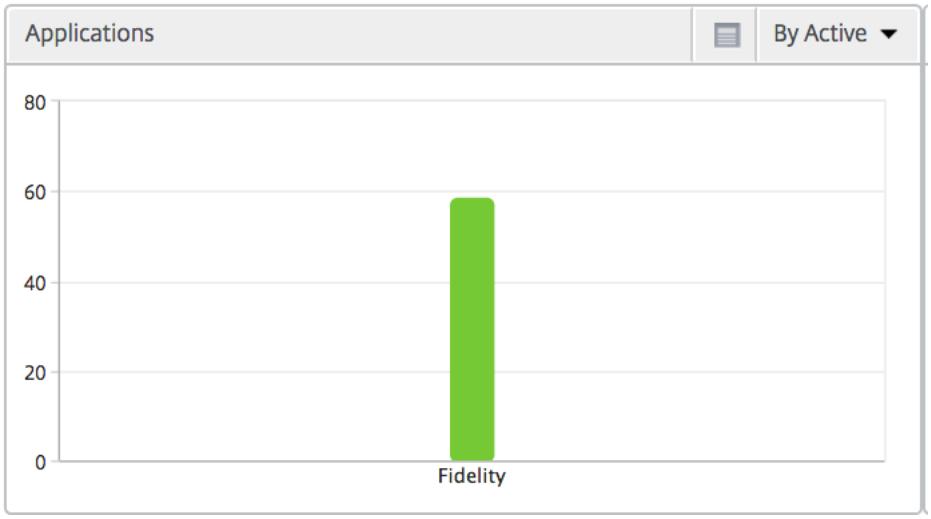
この表は、特定のユーザーの Citrix Virtual Desktop セッションに関する洞察を示しています。以下のメトリクスは［Desktop Launch Count］および［Bandwidth］を基準にしてソートできます。

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（すなわち NetScaler からバックエンドサーバー）。
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（すなわち NetScaler からエンドユーザー）。
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。



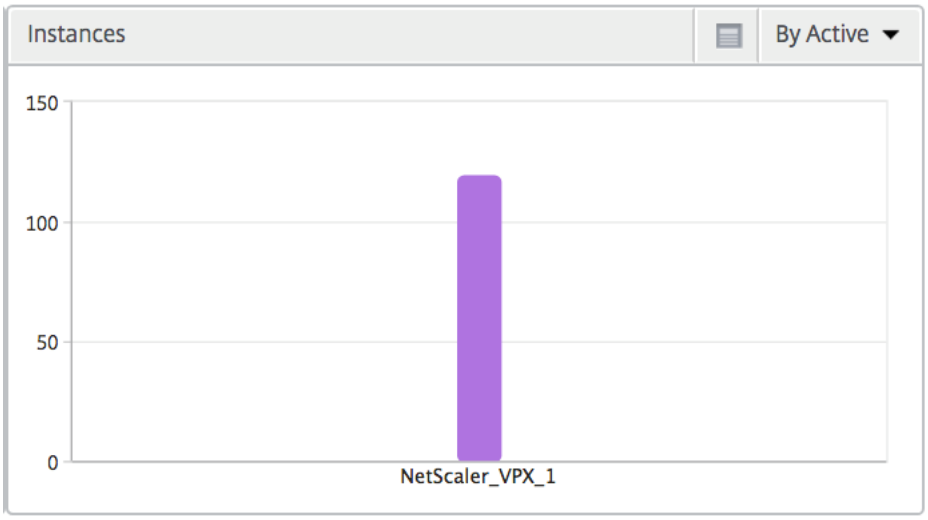
アプリケーション

[Active]、[Total Session Launch Count]、[Total App Launch Count]、[Launch Duration] で並べ替えることができる、アプリを表す棒グラフ。



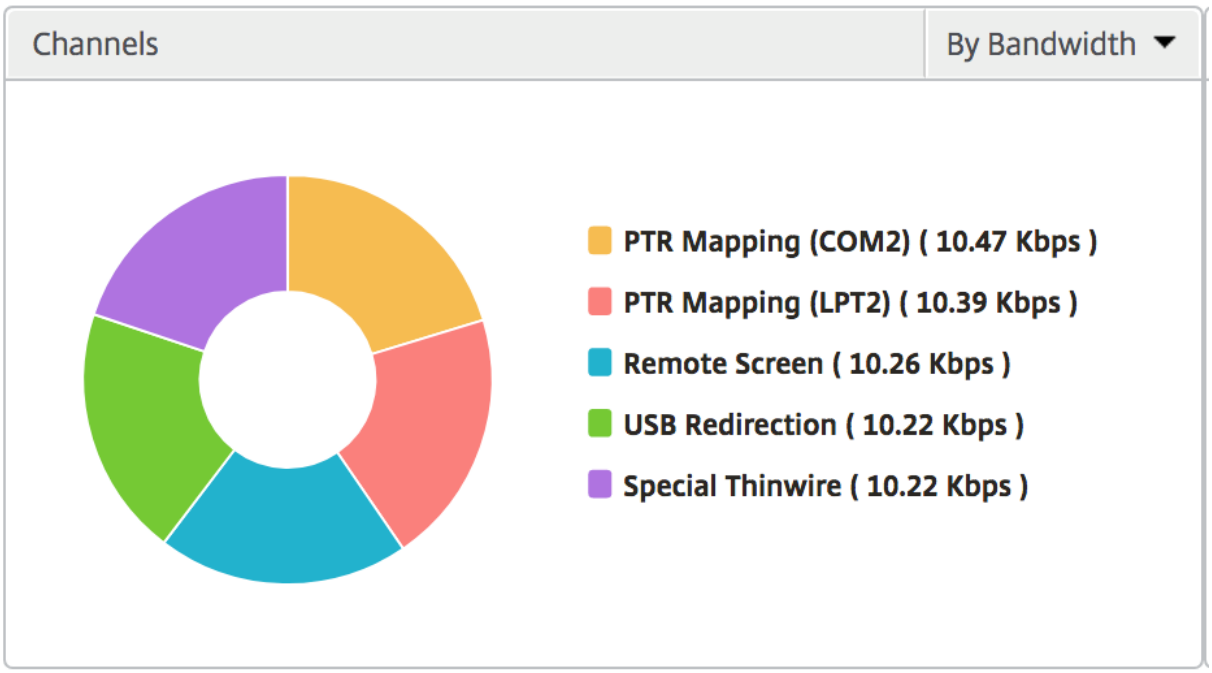
インスタンス

［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



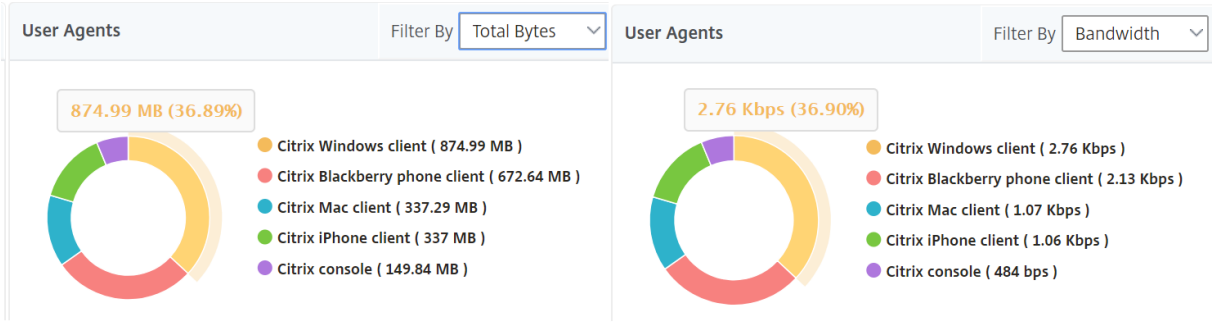
チャネル

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。



Per User Session ビュー

［Per User Session］ビューには、選択したユーザーのセッションに関するレポートが表示されます。

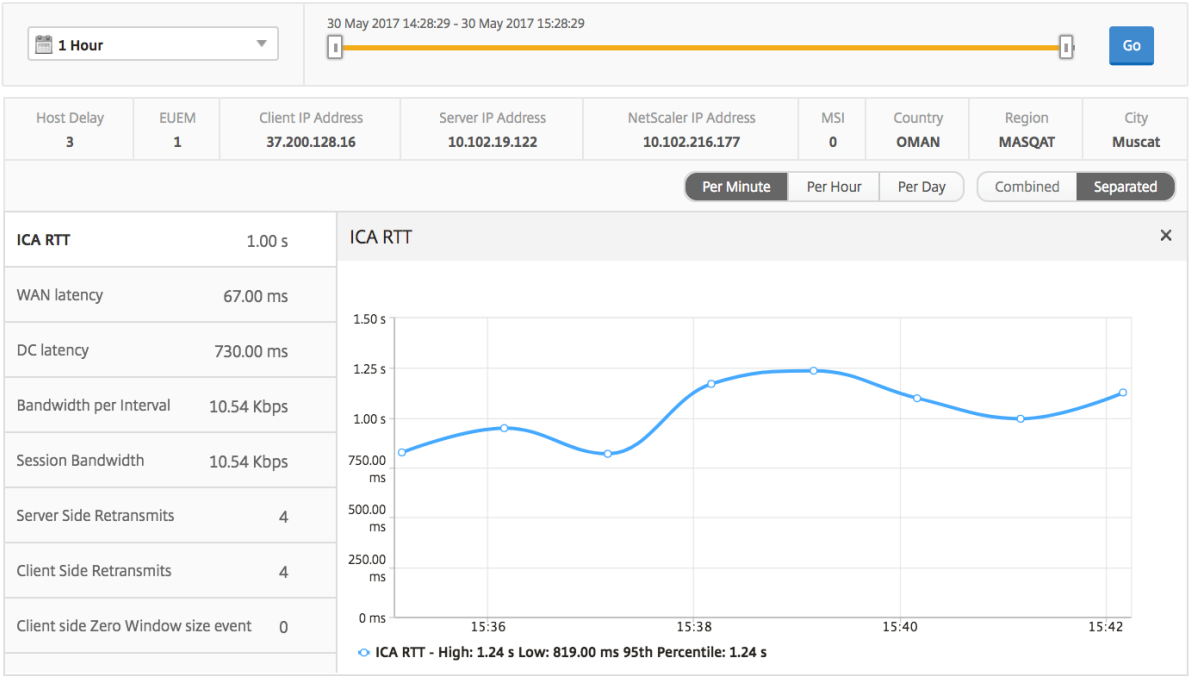
選択したユーザーのセッションのメトリックを表示する手順は、次のとおりです。

1. [**Analytics**] > [**HDX Insight**] > [ユーザー] に移動します。
2.「ユーザー 概要レポート」セクションから特定のユーザー を選択します。
3.「現在のセッション」または「終了したセッション」列からセッションを選択します。

時系列グラフ

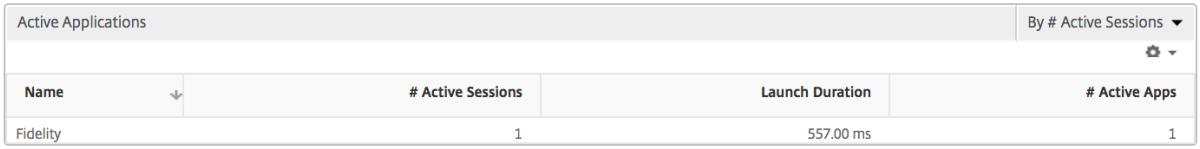
メトリックス	説明
セッション再接続	この数字は、アクティブな Citrix Virtual Apps and Desktops セッションの数を示します。
ACR 数	この数字は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延です（すなわち NetScaler からエンドユーザー）。
DC 遅延	ネットワークのサーバー側に起因する遅延です（すなわち NetScaler からバックエンドサーバー）。

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。



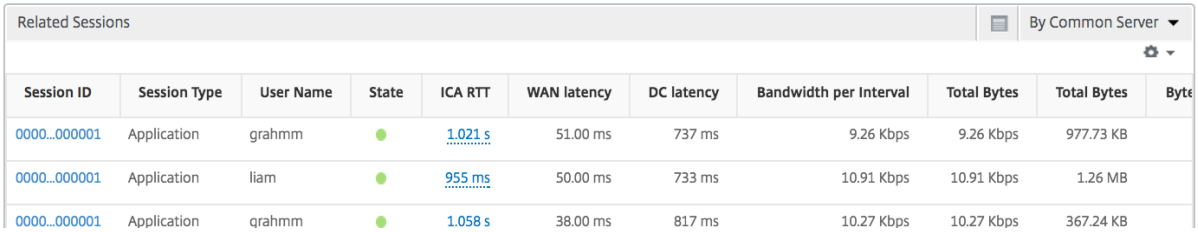
Active Applications

[Active Applications] 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およびメトリクスでは、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。

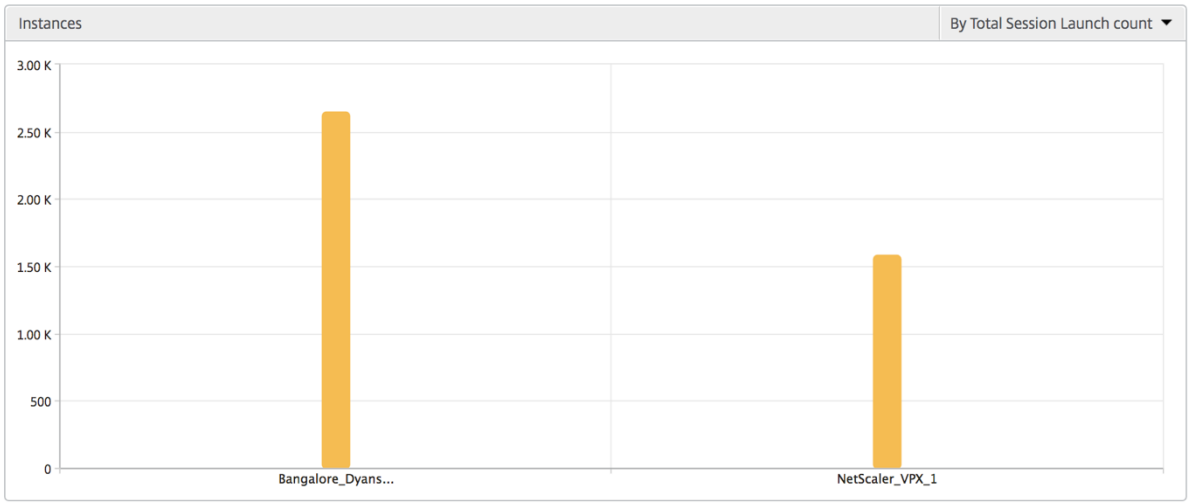
インスタンス概要ビュー

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。

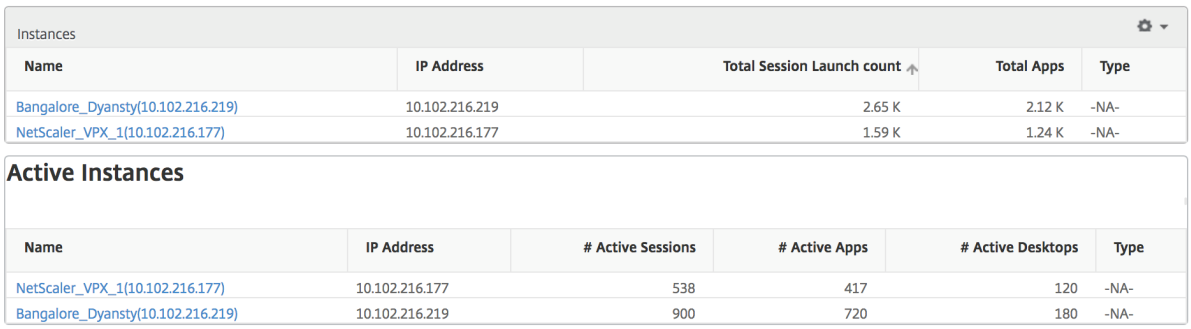
インスタンス棒グラフ

このグラフには、インスタンスと、グラフキャンバスの右上にあるドロップダウンから選択できる合計セッション起動回数および合計アプリ数が表示されます。



インスタンス/アクティブインスタンス概要レポート

メトリック	説明
名前	NetScaler インスタンスのホスト名。
IP アドレス	NetScaler の IP アドレスです。
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-

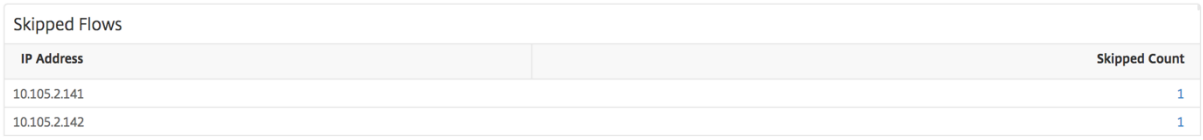
しきい値レポート

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。

スキップフロー

スキップフローは、ICA 接続の解析が省略されたレコードのことです。これは、サポートされていない Citrix Virtual Apps and Desktops s バージョンを使用している、サポートされていないバージョンのレシーバーまたはレシーバータイプを使用しているなど、複数の理由で発生する可能性があります。このテーブルでは、IP アドレスとスキップフロー数が示されます。こうしたセッションは監視対象から除外されるため、これらの Citrix Receiver はホワイトリストに登録しないことをお勧めします。

ICA 解析関連の問題について詳しくは、「**Error! Hyperlink reference not valid.** 」を参照してください。


Skipped Flows

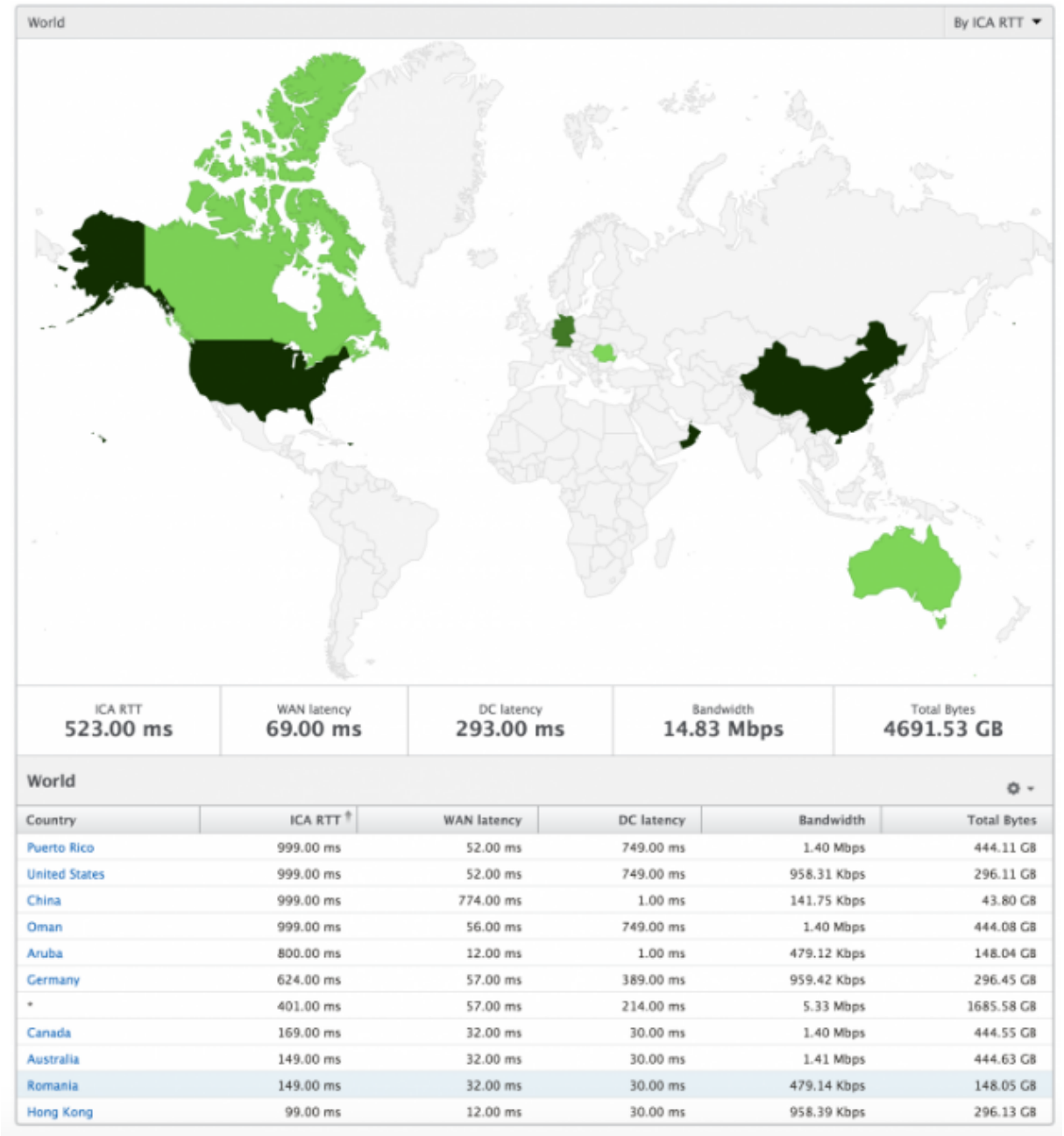
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

世界ビュー

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。管理者にはシステムの［World］ビューが用意されており、地域をクリックするだけで特定の国、さらには都市へとドリルダウンすることができます。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［World Map］では以下の詳細を確認でき、各メトリックの密度がヒートマップ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

インスタンス別ビュー

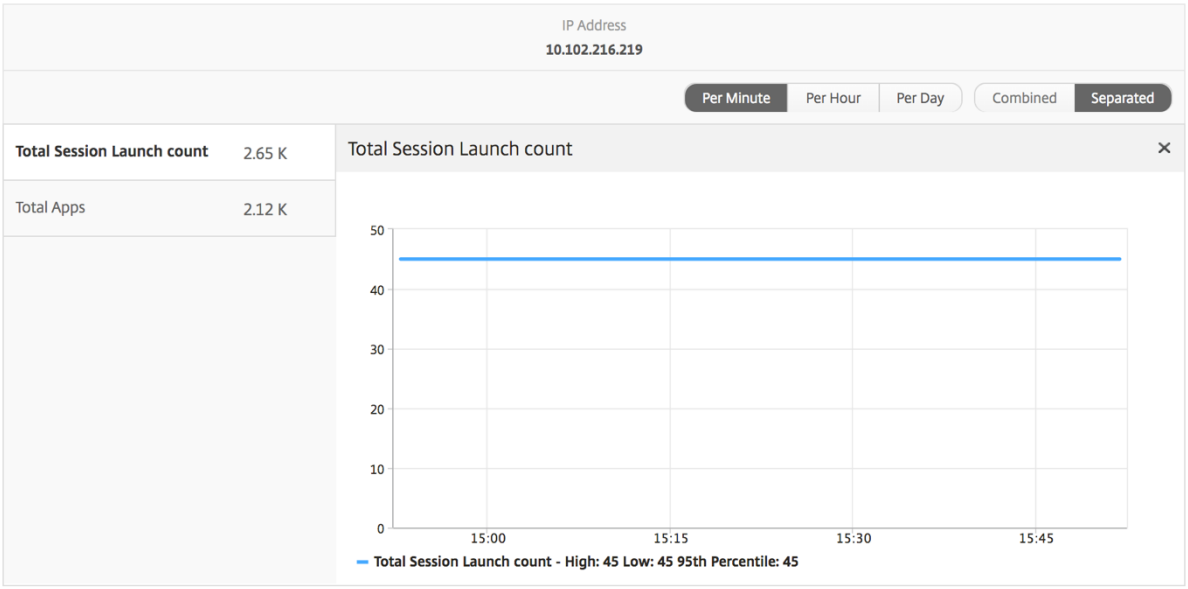
インスタンス別ビューには、選択した特定の NetScaler インスタンスの詳細なエンドユーザーエクスペリエンスに関するレポートが示されます。

[インスタンス**]** ビューにナビゲートするには、次の手順を実行します。

1. [分析] > [**HDX Insight**] > [インスタンス] に移動します。
2. インスタンスの概要レポートから特定のインスタンスを選択します。

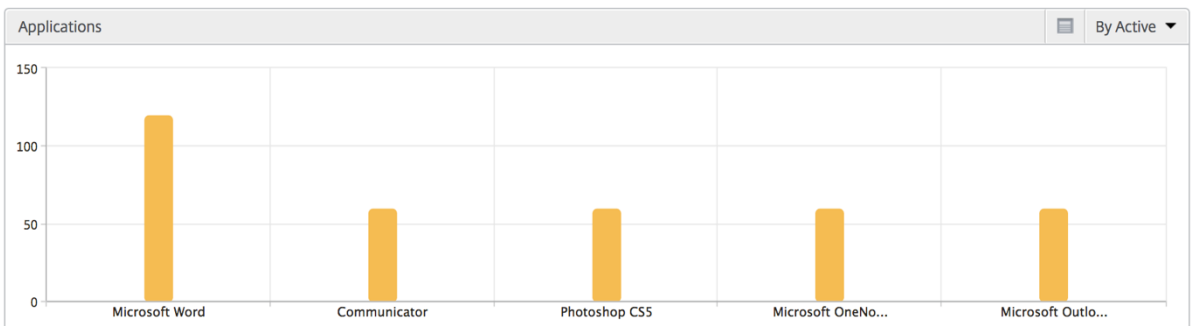
折れ線グラフ

メトリックス	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 Apps 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

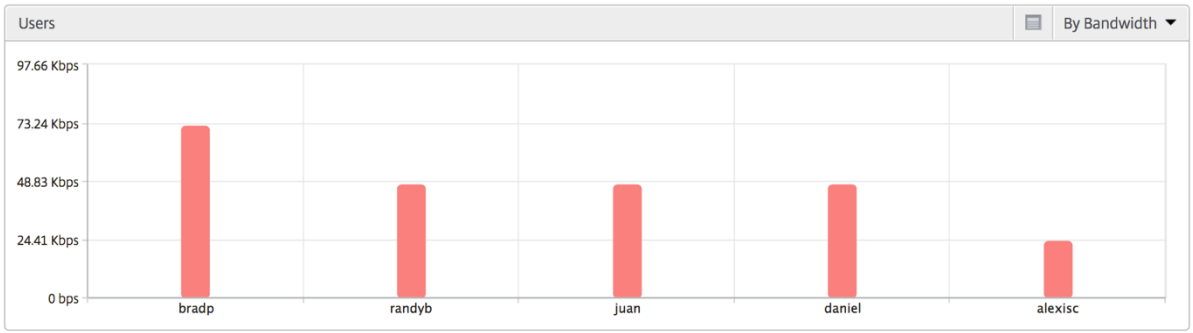
アクティブなアプリ、合計セッション起動回数、合計アプリ起動回数、または起動期間の各基準別に上位 5 個のアプリケーションが示されます。



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。

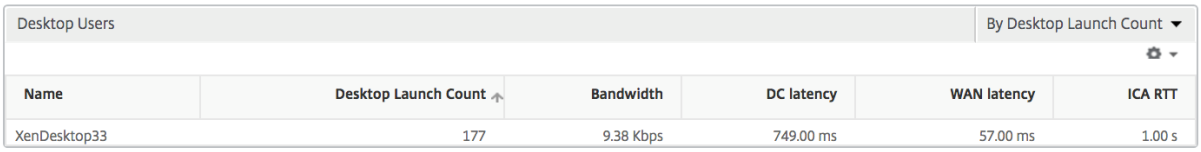
- 帯域幅
- WAN 遅延
- DC の遅延
- ICA 往復時間



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（すなわち NetScaler からバックエンドサーバー）。
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（すなわち NetScaler からエンドユーザー）。
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。

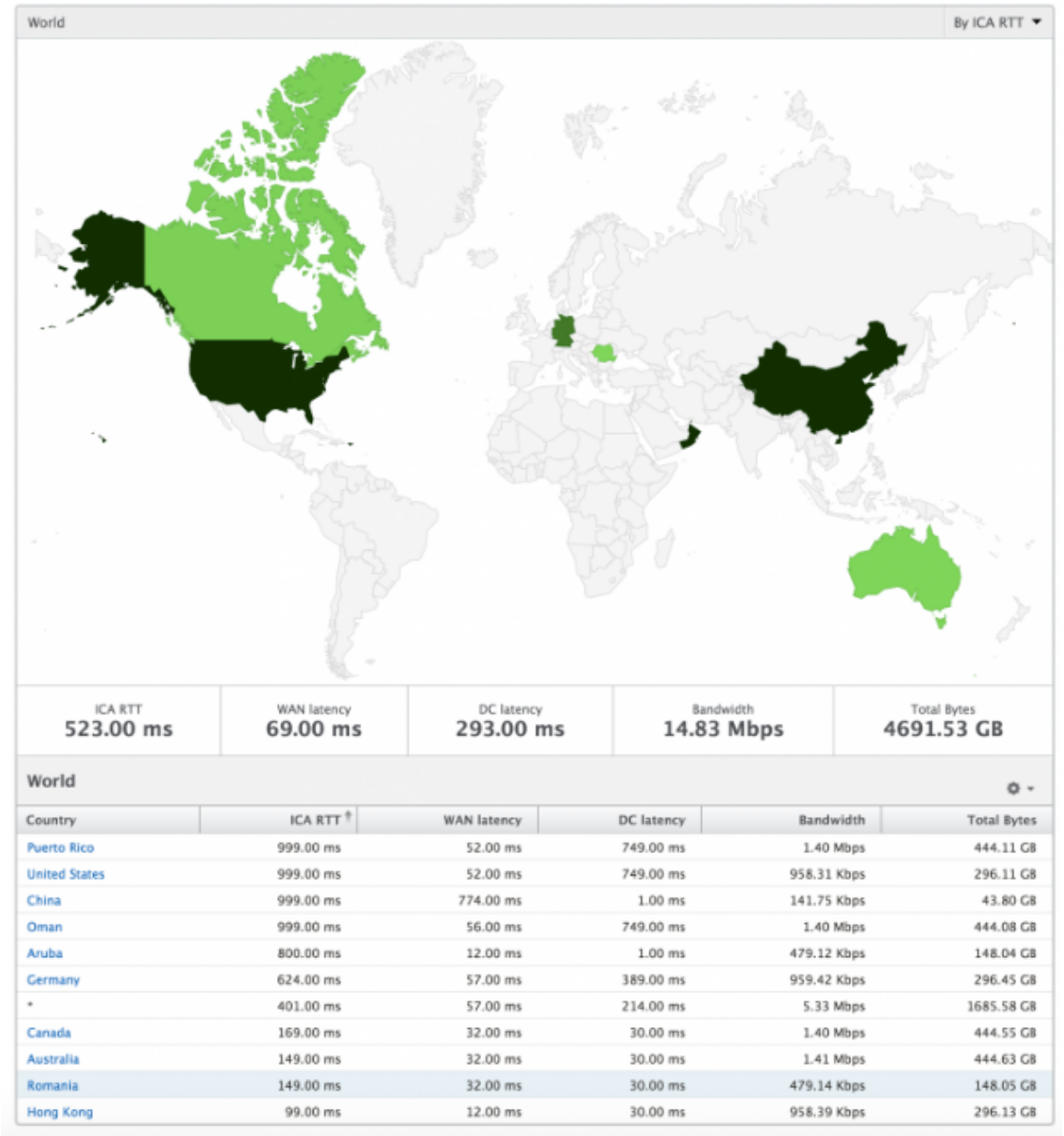


世界ビュー

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。管理者にはシステムの［World］ビューが用意されており、地域をクリックするだけで特定の国、さらには都市へとドリルダウンすることができます。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［World Map］では以下の詳細を確認でき、各メトリックの密度がヒートマップ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

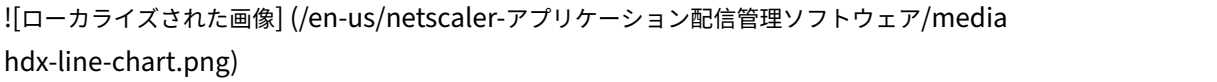
ライセンスビューには、NetScaler Gateway のライセンス情報が表示されます。

[ライセンス**]** ビューに移動するには、次の手順に従います。

1. サポートされている Web ブラウザーを使用して NetScaler MA Service ログオンします。
2. [分析] > [**HDX Insight**] > [ライセンス] に移動します。

折れ線グラフ

メトリックス	説明
使用中のライセンス	選択した期間中に使用されている NetScaler Gateway CCU ライセンス。各カウントは、ユーザーセッションの数を表します。このカウントには、各ユーザーが起動したアプリケーションセッションおよびデスクトップセッションは含まれません。
総ライセンス数	お客様が利用できる NetScaler Gateway CCU ライセンスの合計数。



しきい値レポート

しきい値レポートは、選択した期間内に エンティティ がライセンスとして選択されている場合に、違反したしきい値の数を表します。 詳細については、「 しきい値 とアラートの作成方法」を参照してください。

HDX Insight の問題のトラブルシューティング

February 6, 2024

HDX Insight ソリューションが期待どおりに機能しない場合、問題は次のいずれかにある可能性があります。トラブルシューティングについては、各セクションのチェックリストを参照してください。

- HDX Insight の構成。
- NetScaler ADC と NetScaler ADM 間の接続性。
- NetScaler ADC での HDX/ICA トラフィックのレコード生成。
- NetScaler ADM 内のレコードの設定。

HDX Insight 構成チェックリスト

- NetScaler ADC で AppFlow 機能が有効になっていることを確認します。詳細については、「AppFlow の有効化」を参照してください。
- NetScaler ADC の実行構成で HDX Insight 構成を確認します。

  コマンドを実行し`show running | grep -i <appflow_policy>`て HDX Insight の構成を確認します。バインドタイプが ICA REQUEST であることを確認します。たとえば、

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  透過モードの場合、バインドタイプは ICA_REQ_DEFAULT でなければなりません。たとえば、

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```

- シングルホップ/Access Gateway またはダブルホップ展開の場合は、HDX/ICA トラフィックが流れている VPN 仮想サーバーに HDX Insight AppFlow ポリシーがバインドされていることを確認してください。
- 透過モードまたは LAN ユーザーモードの場合は、ICA ポート 1494 と 2598 が設定されていることを確認します。
- Citrix Gateway または VPN 仮想サーバーの「appflowlog」パラメーターが Access Gateway またはダブルホップ展開で有効になっていることを確認します。詳しくは、「仮想サーバーに対する AppFlow の有効化」を参照してください。
- ダブルホップ NetScaler ADC で「接続チェーン」が有効になっていることを確認します。詳しくは、「データをエクスポートするための NetScaler Gateway アプライアンスの構成」を参照してください。
- 高可用性フェイルオーバー後、HDX Insight の詳細が解析されスキップされている場合は、ICA パラメータ「EnablesronHaFailover」が有効になっていることを確認します。詳しくは、「NetScaler ADC 高可用性ペアのセッション画面の保持」を参照してください。

NetScaler ADC と **NetScaler ADM** の間の接続チェックリスト

- NetScaler ADC で AppFlow コレクタのステータスを確認します。詳しくは、「NetScaler ADC と AppFlow Collector 間の接続状態を確認する方法」を参照してください。
- HDX Insight の AppFlow ポリシーヒットを確認します。

  コマンド`show appflow policy <policy_name>`を実行して AppFlow ポリシーヒットをチェックします。

  GUI で [システム**] > [AppFlow] > [**ポリシー**]** に移動して、AppFlow ポリシーのヒットを確認することもできます。

- AppFlow ポート 4739 または 5557 をブロックしているファイアウォールを検証します。

NetScaler ADC チェックリストでの **HDX/ICA** トラフィックのレコード生成

コマンド`tail -f /var/log/ns.log | grep -i "default ICA Message"`を実行してログを検証します。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 アプリ

  解決策：Citrix Workspace アプリをサポートされているバージョンにアップグレードしてください。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	デ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
116	NS_ICA_ERR_MEM_REDUC_CTX_ALLOC	エクスパンダーコンテキストのメモリ割り当てエラー
117	NS_ICA_ERR_ICA_OLD_SERVER	古いサーバー - 機能ブロックはサポートされていません
118	NS_ICA_ERR_PIR_MANY_FRAG	Packet Init 要求はフラグメント化されており、処理できません

スキップコード	エラーメッセージ	エラーの原因
119	NS_ICA_ERR_INIT_ICA_CAPS	ICA 機能初期化エラー
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	ICA ストリーム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_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
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	圧縮無効で、ホストには適用されません
134	NS_ICA_ERR_IDENT_PROTO	ICA または CGP プロトコルを識別できない、不正なレシーバーを使用している
135	NS_ICA_ERR_INVALID_SIGNATURE	ICA 署名またはマジックストリングが正しくありません
136	NS_ICA_ERR_PARSE_RAW	ICA ハンドシェイクパケットの解析中にエラーが発生しました

スキップコード	エラーメッセージ	エラーの原因
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	受信者 (クライアント) はホワイトリストに含まれていないため、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	クライアント再接続 Cookie が必要な制約を満たしていません
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	クライアントから受信した受信者バージョン文字列が無効です
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	クライアントから受け取った製品 ID が無効です
148	NS_ICA_ERR_V3_HDR_CORRUPT_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
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

スキップコード	エラーメッセージ	エラーの原因
156	NS_ICA_ERR_PURE_INVALID_EVENT	PURE チャネル解析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	CPR はリデューサーバージョン 3 をサポートしていません
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	CPR はクライアントはリデューサーバージョン 3 をサポートしていません
168	NS_ICA_ERR_ICAP_INSUFFBYTE	ICA ハンドシェイクで予期しないバイト数
169	NS_ICA_ERR_HIGHER_RECONSEQ	ピアポスト再接続による 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
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

スキップコード	エラーメッセージ	エラーの原因
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_RECONN_SEQ	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 HDXInsight 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。カウンターの詳細を表示するコマンド`nsconmsg -g hdx -d statswt0`を実行します。

HDX カウンタ名	目的	カテゴリ（統計/エラー/診断）
hdx_tot_ica_conn	NS によって検出されたピュア ICA 接続の総数を示します。クライアント PCB 上の ICA 署名に基づく ICA 接続が検出されるたびに増加します。	Stats
hdx_tot_cgp_conn	NS によって検出された CGP 接続の総数を示します（セッション信頼性オン）。クライアント PCB の CGP 署名に基づく CGP 接続が検出されるたびに増分されます。	Stats
hdx_dbg_tot_udt_conn	NS によって検出された UDP ICA 接続の総数を示します	Stats
hdx_dbg_tot_nsap_conn	NS が検出した NSAP がサポートする接続の総数を示します	Stats
skip_conn	ICA または CGP 署名が無効であるためにパーサーによってスキップされた ICA 接続の数を示します。	統計情報
hdx_dbg_active_conn	その時点でのアクティブな EDT/CGP/ICA 接続の合計数。	統計情報
hdx_dbg_active_nsap_conn	その時点でのアクティブな EDT/CGP/ICA NSAP 接続の総数。	統計情報
hdx_dbg_skip_appflow_disabled	AppFlow を無効にしたために AppFlow がセッションから接続解除されたインスタンスの総数	ステータス/診断
hdx_dbg_transparent_user	透過的なユーザーアクセスの総数	ステータス/診断
hdx_dbg_ag_user	Access Gateway のユーザーアクセスの総数	ステータス/診断
hdx_dbg_lan_user	LAN ユーザーモードアクセスの総数	ステータス/診断
hdx_basic_enc	基本暗号化を使用する ICA 接続の数を示します	ステータス/診断

HDX カウンタ名	目的	カテゴリ（統計/エラー/診断）
advanced_enc	高度な RC5 ベースの暗号化を使用する ICA 接続の数を示します	ステータス/診断
dx_dbg_wanscaler_on_clientside	クライアント側に Citrix SD-WAN がある CGP/ICA 接続の総数	ステータス/診断
hdx_dbg_wanscaler_on_serverside	Citrix SD-WAN サーバー側の CGP/ICA 接続の総数	ステータス/診断
reconnected_session	NetScaler ADC エラーのないクライアントからの再接続要求の総数	ステータス/診断
hdx_dbg_host_rejected_ns_reconnect	クライアントによる再接続要求を拒否したホストの総数	ステータス/診断
hdx_euem_available	エンドユーザーエクスペリエンスモニタリングチャネルが使用できる接続の数を示します。ICA RTT などの統計を収集するには、エンドユーザーエクスペリエンス監視チャネルが必要です。	ステータス/診断
hdx_err_disabled_sr	nsapimgr ノブを使用すると、セッションの信頼性が無効になります。セッションはこのセッションでは機能しません。	エラー
hdx_err_skip_no_msi	XA/XD サーバーに MSI 機能がありません。これは古いサーバーバージョンを示しており、HDX Insight はこの接続をスキップします。	エラー
hdx_err_skip_old_server	サポートされていない古いサーバーバージョン	エラー
hdx_err_clnt_not_whitelist	クライアントレシーバーがホワイトリストに含まれていないため、HDX Insight はこの接続をスキップします	エラー
hdx_sm_ica_cam_channel_disabled	SmartAccess ポリシーによって無効化された NS_ICA_CAM_CHANNEL の総数	診断
hdx_sm_ica_usb_channel_disabled	SmartAccess ポリシーによって無効にされた NS_ICA_USB_CHANNEL の総数	診断

HDX カウンタ名	目的	カテゴリ（統計/エラー/診断）
hdx_sm_ica_clip_channel_disabled	SmartAccess ポリシーによって無効化された NS_ICA_CLIP_CHANNEL の総数	診断
hdx_sm_ica_ccm_channel_disabled	SmartAccess ポリシーによって無効にされた NS_ICA_CCM_CHANNEL の総数	診断
hdx_sm_ica_cdm_channel_disabled	SmartAccess ポリシーによって無効にされた NS_ICA_CDM_CHANNEL の総数	診断
hdx_sm_ica_com1_channel_disabled	SmartAccess ポリシーによって無効にされた NS_ICA_COM1_CHANNEL の総数	診断
hdx_sm_ica_com2_channel_disabled	SmartAccess ポリシーによって無効にされた NS_ICA_COM2_CHANNEL の総数	診断
hdx_sm_ica_cpm_channel_disabled	SmartAccess ポリシーによって無効にされた NS_ICA_CPM_CHANNEL の総数	診断
hdx_sm_ica_lpt1_channel_disabled	SmartAccess ポリシーによって無効にされた NS_ICA_LPT1_CHANNEL の総数	診断
hdx_sm_ica_lpt2_channel_disabled	SmartAccess ポリシーによって無効にされた NS_ICA_LPT2_CHANNEL の総数	診断
dx_dbg_sm_ica_msi_disabled	SmartAccess ポリシーによって MSI が無効になっているケースの総数	診断
hdx_sm_ica_file_channel_disabled	SmartAccess ポリシーによって無効になっている NS_ICA_FILE_CHANNEL の総数	診断
hdx_dbg_usb_accept_device	受け入れられた USB デバイスの総数	診断
hdx_dbg_usb_reject_device	拒否された USB デバイスの総数	診断
hdx_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	なくなった USB デバイスの総数	診断
hdx_dbg_usb_device_stopped	停止した USB デバイスの総数	診断

nstrace 検証

CFLOW プロトコルをチェックして、NetScaler ADC から送信されるすべての AppFlow レコードを確認します。

NetScaler ADM チェックリスト内のレコードの移入数

- コマンド`tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"`を実行し、ログをチェックして、Citrix ADM が AppFlow レコードを受信していることを確認します。
- NetScaler ADC インスタンスが NetScaler ADM に追加されていることを確認します。
- NetScaler Gateway/VPN 仮想サーバーが NetScaler ADM でライセンスされていることを検証します。
- ダブルホップのマルチホップパラメータ設定が有効になっていることを確認してください。
- ダブルホップ展開では、NetScaler Gateway がセカンドホップに対してクリアされていることを確認します。

Citrix テクニカルサポートに連絡する前に

迅速に解決するには、Citrix テクニカルサポートに連絡する前に、次の情報があることを確認してください。

- 展開とネットワークトポロジの詳細。
- 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。
- クライアント側レシーバーのバージョン。
- 問題が発生したときのアクティブな ICA セッションの数。
- Citrix ADC コマンドプロンプトで`show techsupport`コマンドを実行してキャプチャ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。
- コマンドを実行して、システムの ARP テーブル内の`show arp`エントリを収集します。

既知の問題

HDX Insight の既知の問題については、NetScaler ADC リリースノートを参照してください。

Gateway Insight

February 6, 2024

NetScaler Gateway 展開では、ユーザーのアクセス詳細を可視化することは、アクセス障害の問題のトラブルシューティングに不可欠です。ネットワーク管理者は、ユーザーが NetScaler Gateway にログオンできないタイミングと、ユーザーアクティビティとログオン失敗の理由を知りたいが、通常、その情報はユーザーが解決の要求を送信しない限り利用できません。

Gateway Insight は、アクセスモードに関係なく、NetScaler Gateway へのログオン時にすべてのユーザーが遭遇した障害を可視化します。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数、アクティブなセッションの合計数、合計バイト数、アプリケーションが消費した帯域幅を表示できます。アプリケーションごとのユーザー、セッション、帯域幅、起動のエラーの詳細を表示できます。

Citrix Gateway アプライアンスに関連付けられているすべての Gateway が使用している Gateway の数、アクティブなセッションの数、合計バイト数、および帯域幅をいつでも表示できます。ゲートウェイごとの EPA、認証、SSO、アプリケーション起動のエラーについて表示できます。また、ゲートウェイに割り当てられたすべてのユーザーの詳細と、ユーザーのログオンアクティビティを表示できます。

すべてのログメッセージは NetScaler ADM データベースに保存されるため、いつでもエラーの詳細を表示できます。また、ログオンエラーの概要を表示して、エラーが発生したログオンプロセスの段階を特定できます。

注意事項

- Gateway Insight は次の展開においてサポートされています。
  - Access Gateway
  - Unified Gateway
- NetScaler ADM のリリースおよびビルドは、NetScaler Gateway アプライアンスのリリースおよびビルドと同じかそれ以降である必要があります。
- エンタープライズライセンスを持つ NetScaler ADC インスタンスについては、1 時間分の Gateway Insight レポートを表示できます。Gateway Insight レポートを 1 時間以上表示するには、プラチナライセンスが必要です。

制限事項

- 認証方法が証明書ベースの認証として構成されている場合、NetScaler Gateway Gateway は Gateway Insight をサポートしません。
- Gateway Insight レポートの場合、NetScaler ADC アプライアンスから地理的位置情報は提供されません。
- 仮想 ICA アプリケーションおよびデスクトップに関する成功したユーザーログオン、遅延、アプリケーションレベルの詳細は、HDX Insight Users ダッシュボードでのみ確認できます。
- ダブルホップモードでは、2 つ目の DMZ にある Citrix Gateway アプライアンスの障害を確認できません。
- RDP（Remote Desktop Protocol：リモートデスクトッププロトコル）のデスクトップアクセスの問題は報告されません。
- Gateway Insight は次の認証タイプでサポートされています。これら以外の認証タイプが使用されている場合、Gateway Insight に不一致が生じる可能性があります。
  - ローカル
  - LDAP
  - RADIUS
  - TACACS
  - SAML
  - ネイティブ OTP

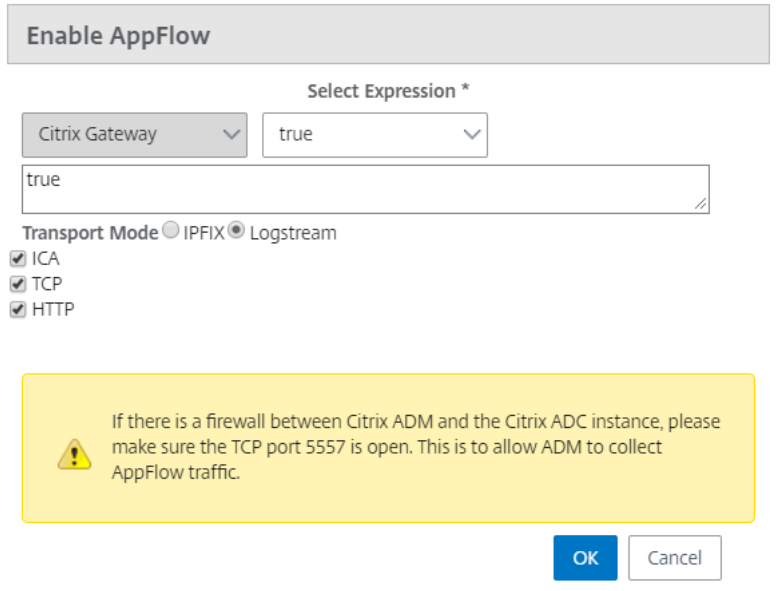
Gateway Insight の有効化

Citrix Gateway アプライアンスで Gateway インサイトを有効にするには、まず Citrix Gateway アプライアンスを Citrix ADM に追加する必要があります。次に、VPN アプリケーションを代表する仮想サーバー向けに AppFlow を有効にしてください。Citrix ADM へのデバイスの追加について詳しくは、「デバイスの追加」を参照してください。

> 注
>
> Citrix ADM のエンドポイント分析（EPA）エラーを表示するには、Citrix Gateway アプライアンス上で AppFlow 認証、承認、および監査ユーザー名ログを有効にする必要があります。

NetScaler ADM で仮想サーバーに対して **AppFlow** を有効にするには

1. NetScaler ADM にログオンします。
2. **[**** ネットワーク] > [インスタンス] に移動し、AppFlow を有効にするインスタンスを選択します。**
3. **[** アクションの選択] リストから、[**Analytics** の設定] を選択します。
4. ［**Insight** の構成］ページの［**Analytics** 構成］で、［**NetScaler Gateway**］を選択します。
5. AppFlow を有効にする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。
6. [**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。
7. [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
>
> IPFIX または`Logstream`のいずれかをトランスポートモードとして選択できます。

8. ［**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** の認証、承認、および監査ユーザー名ロギングを有効にするには

1. [構成**] > [**システム**] > [AppFlow] > [**設定] に移動し、[**AppFlow** 設定の変更] をクリックします。

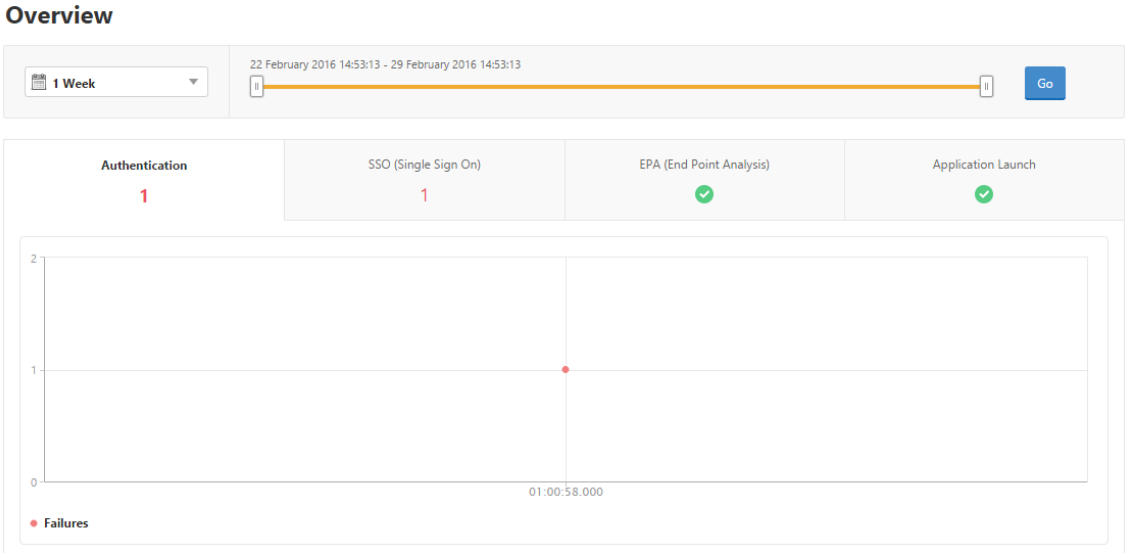
2. [**AppFlow** 設定の構成] 画面で、[**AAA** ユーザ名] を選択し、[**OK**] をクリックします。

Gateway Insight レポートの表示

Citrix ADM では、Citrix Gateway アプライアンスに関連するすべてのユーザー、アプリケーション、および Gateway のレポートを表示でき、特定のユーザー、アプリケーション、または Gateway の詳細を表示できます。「概要」セクションでは、EPA、SSO、認証、およびアプリケーション起動の失敗を表示できます。ユーザーがログオンに使用したさまざまなセッションモードの概要、クライアントの種類、時間ごとのログオンしたユーザーの数を表示することもできます。

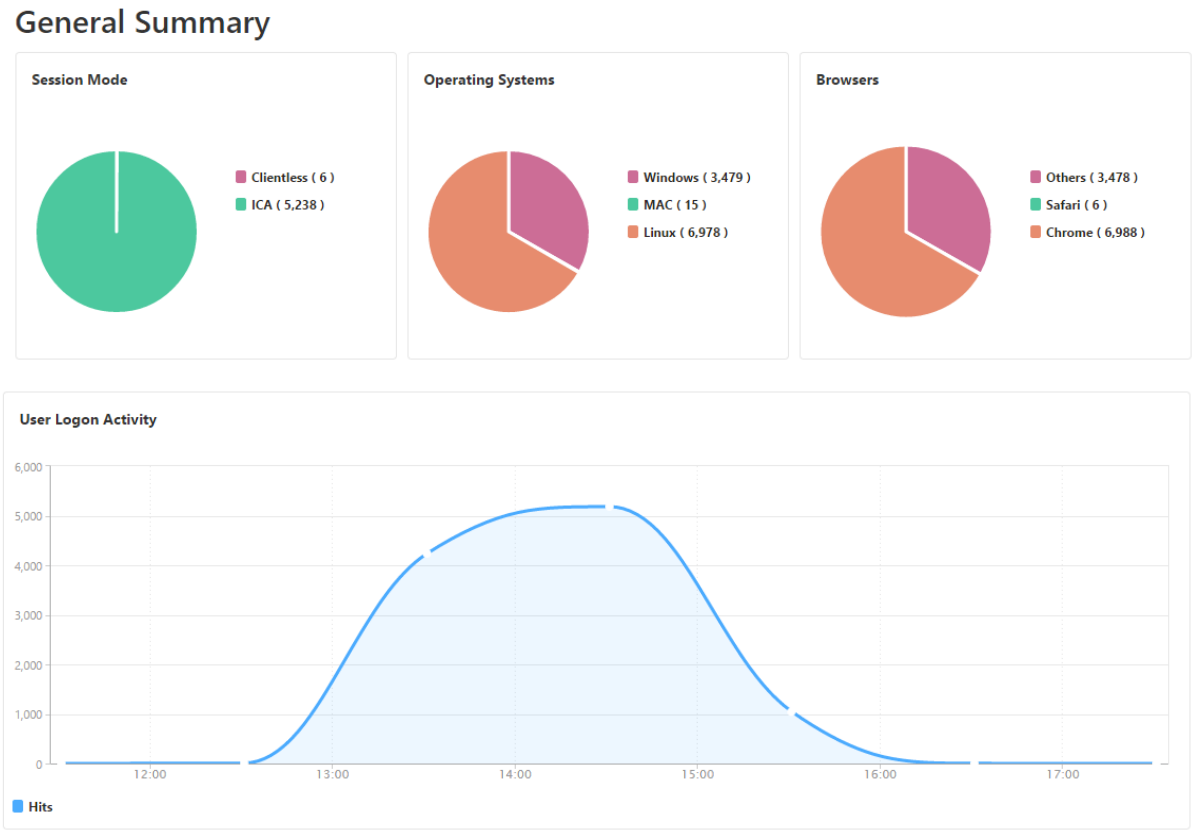
EPA、**SSO**、認証、承認、およびアプリケーションの起動の失敗を表示するには

1. NetScaler ADM で、[**Analytics] > [Gateway Insight**] に移動します。
2. ユーザーの詳細を表示する期間を選択します。時間スライダーを使用して選択する期間をカスタマイズできます。[**Go**] をクリックします。
3. [EPA (End Point Analysis)]、[Authentication]、[Authorization]、[SSO (Single Sign On)]、[Application Launch] タブのいずれかをクリックして、エラーの詳細を表示します。



セッションモード、クライアント、ユーザーの数の概要を表示するには

NetScaler ADM で、[**Analytics] > [Gateway Insight**] に移動し、下にスクロールしてレポートを表示します。

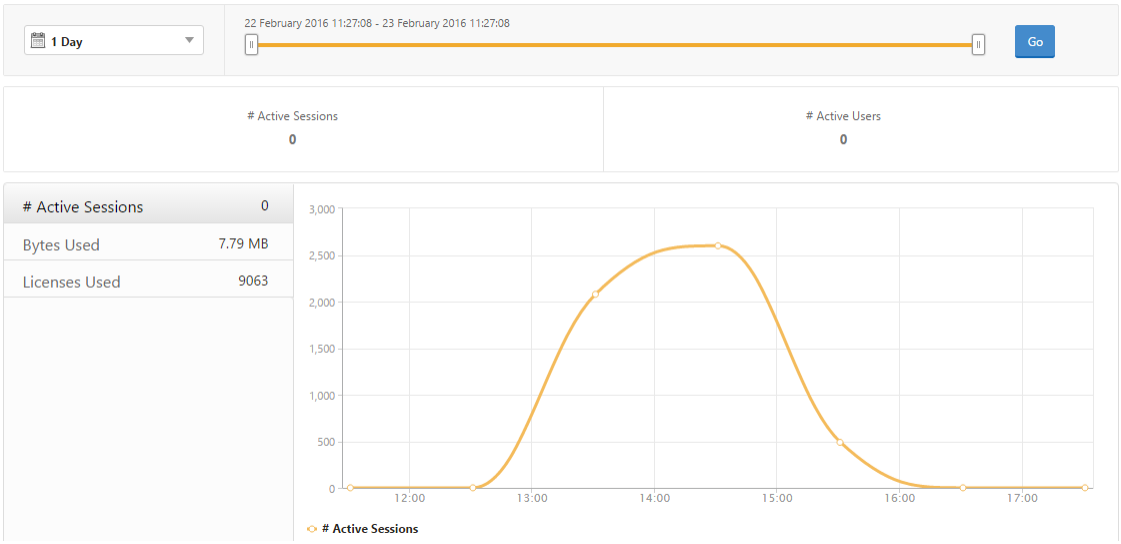


ユーザーの **Gateway Insight** レポートの表示

Citrix Gateway アプライアンスに関連付けられているすべてのユーザーのレポートを表示できます。ユーザーごとの EPA、認証、SSO、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。

ユーザーの詳細を表示するには

1. Citrix ADM で、［分析］**>**［**Gateway** インサイト］**>**［ユーザー］に移動します。
2. ユーザーの詳細を表示する期間を選択します。時間スライダーを使用して選択する期間をカスタマイズできます。［**Go**］をクリックします。
3. アクティブ・ユーザー数、アクティブ・セッション数、バイト数、および期間中にすべてのユーザーが使用したライセンスを表示できるようになりました。



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。

[Us **ers**] タブまたは [**Active Users**] タブで、[Us **ername**] 列のユーザーをクリックすると、EPA、認証、SSO、およびアプリケーションの起動の失敗、およびそのユーザーのその他の詳細を表示できます。

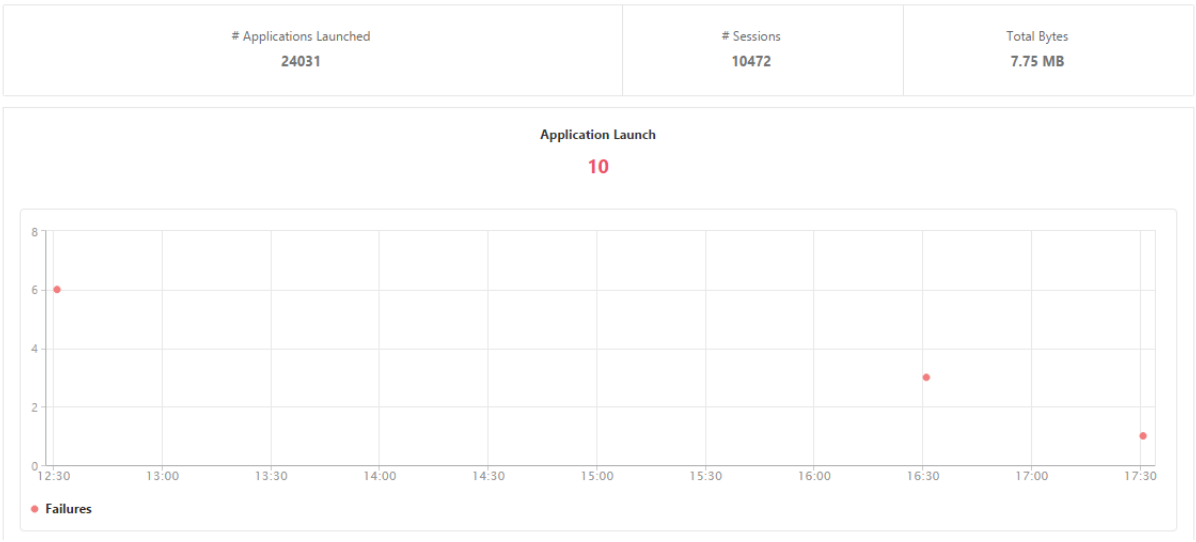
アプリケーションの **Gateway Insight** レポートの表示

起動されたアプリケーション数、アクティブなセッションの合計数、合計バイト数、アプリケーションが消費した帯域幅を表示できます。アプリケーションごとのユーザー、セッション、帯域幅、起動のエラーの詳細を表示できます。

アプリケーションの詳細を表示するには

1. NetScaler ADM で、［分析］ **>** ［**Gateway Insight**］ **>** ［アプリケーション］に移動します。
2. アプリケーションの詳細を表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。［**Go**］をクリックします。

起動されたアプリケーション数、アクティブなセッションの合計数、合計バイト数、アプリケーションが消費した帯域幅を表示できるようになりました。



下にスクロールすると、ICA とその他のアプリケーションによって使用されたセッション数、帯域幅、合計バイト数が表示されます。

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。

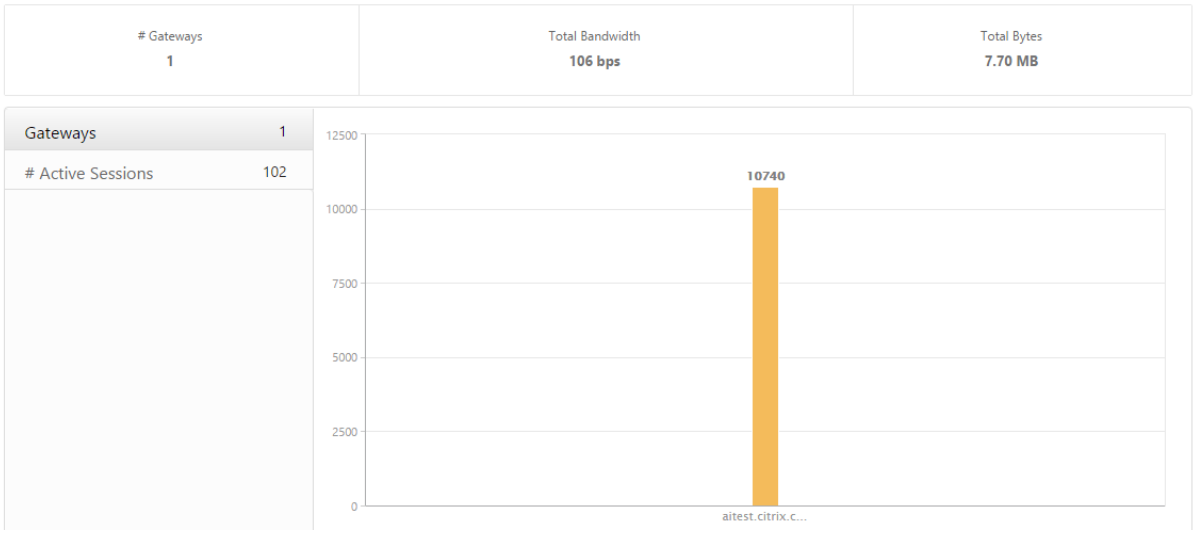
Gateway の **Gateway Insight** レポートの表示

NetScaler Gateway アプライアンスに関連付けられているすべての Gateway で使用されている Gateway の数、アクティブなセッションの数、合計バイト数、および帯域幅をいつでも表示できます。ゲートウェイごとの EPA、認証、SSO、アプリケーション起動のエラーについて表示できます。また、ゲートウェイに割り当てられたすべてのユーザーの詳細と、ユーザーのログオンアクティビティを表示できます。

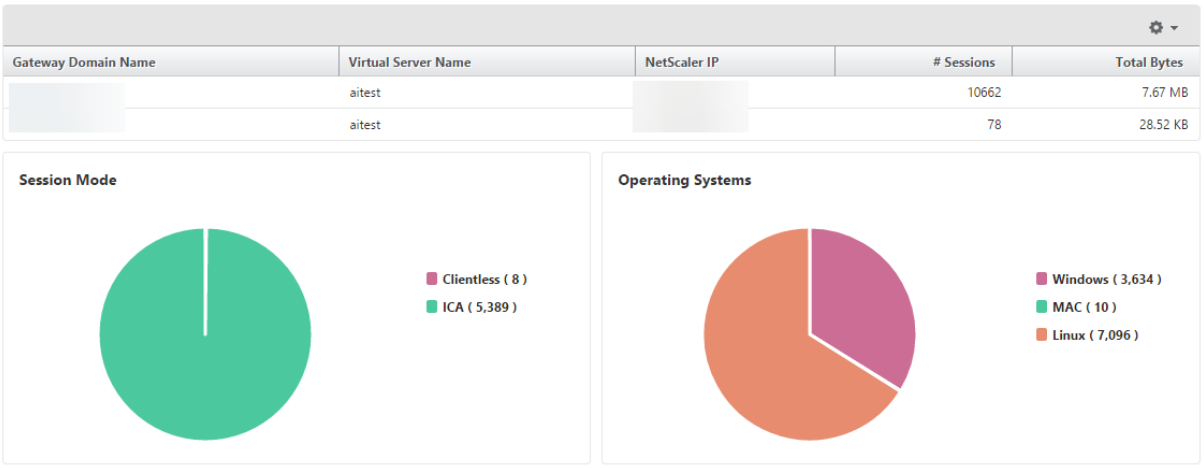
ゲートウェイの詳細を表示するには

1. **Citrix ADM** で、［分析］**>**［**Gateway** インサイト］**>**［**Gateway**］に移動します。
2. ゲートウェイの詳細を表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。［**Go**］をクリックします。

NetScaler Gateway アプライアンスに関連付けられたすべての Gateway で使用された Gateway 数、アクティブセッション数、合計バイト数、帯域幅をいつでも表示できるようになりました。



下にスクロールすると、Gateway ドメイン名、仮想サーバー名、NetScaler IP アドレス、セッションモード、合計バイト数などの Gateway の詳細が表示されます。



「Gateway **Domain Name**」列で **G** ateway をクリックすると、EPA、認証、シングル・サインオン、アプリケーション起動の失敗、および Gateway に関するその他の詳細を表示できます。

レポートのエクスポート

GUI に表示されるすべての詳細を含む Gateway Insight レポートは、PDF、JPEG、PNG、または CSV 形式でローカルコンピューターに保存できます。また、指定された電子メールアドレスへのレポートのエクスポートを、さまざまな間隔でスケジュール設定することができます。

> 注
>
> - 読み取り専用アクセス権のユーザーは、レポートをエクスポートすることができません。
> - 地理地図レポートは、NetScaler ADM がインターネットに接続されている場合にのみエクスポートされます。

レポートをエクスポートするには、次の手順に従います

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、[システム] > [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

あなたは Citrix ADM を介して Citrix Gateway アプライアンスを監視している Citrix Gateway 管理者であり、ユーザーがログインできない理由や、ログインプロセスのどの段階で障害が発生したかを確認したいと考えています。

NetScaler ADM では、ログインプロセスの次の段階でユーザーログインエラーの詳細を表示できます。

- 認証

- エンドポイント分析（EPA）
- シングルサインオン

NetScaler ADM では、特定のユーザーを検索して、そのユーザーの詳細をすべて表示できます。

ユーザーを検索するには、次の手順に従います。

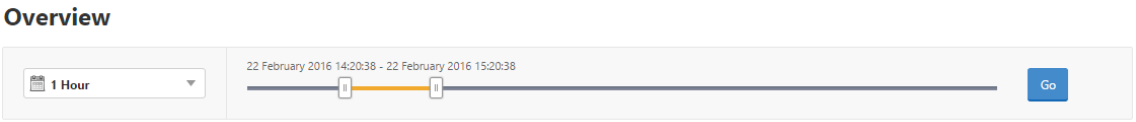
Citrix ADM で、［分析］**>**［**Gateway** インサイト］に移動し、［ユーザーの検索］テキストボックスで検索するユーザーを指定します。

認証の失敗

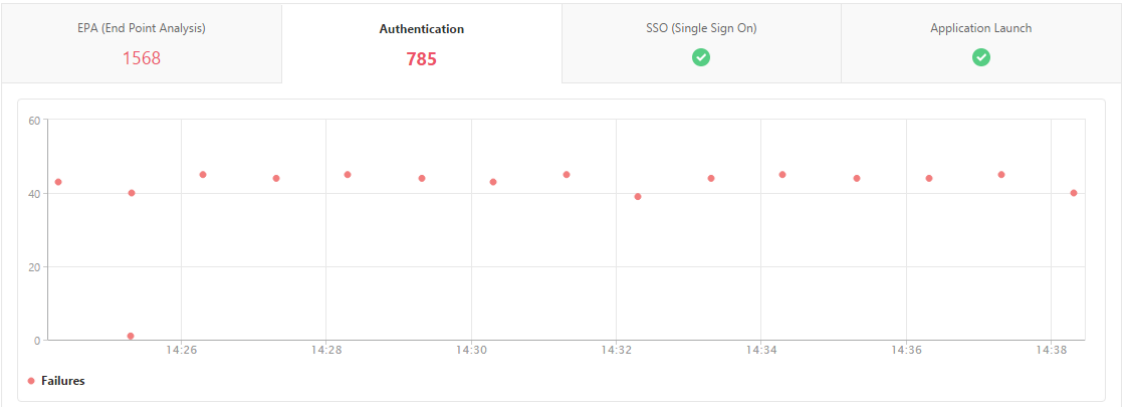
資格情報が正しくない、または認証サーバーから応答がないなどの認証エラーについて確認できます。2 段階認証を設定している場合、いずれの段階で認証できなかったのか、または両方の段階で認証できなかったのかを確認できます。

認証失敗の詳細を表示する手順は、次のとおりです。

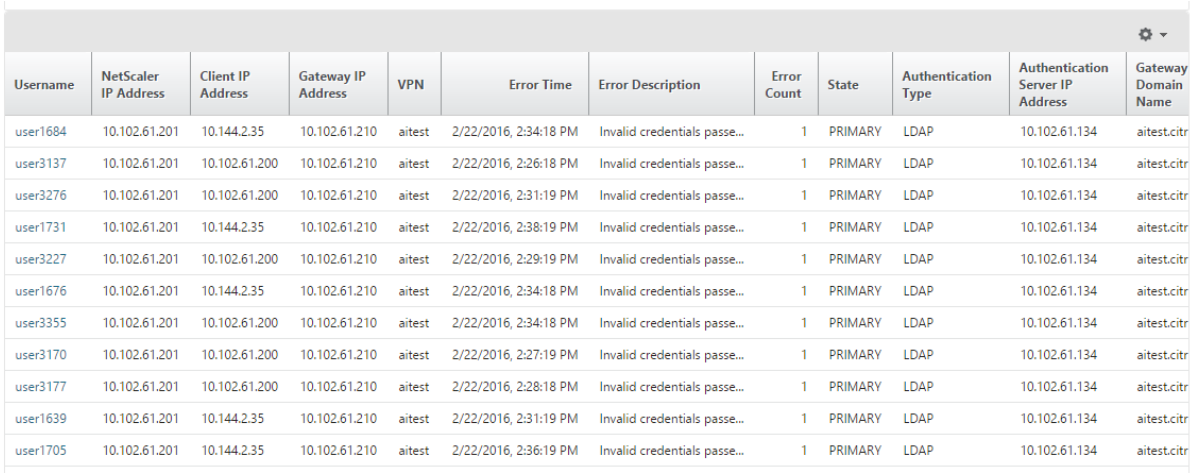
1. NetScaler ADM で、[**Analytics] > [Gateway Insight**] に移動します。
2. [概要] セクションで、認証エラーを表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。［**Go**］をクリックします。



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。



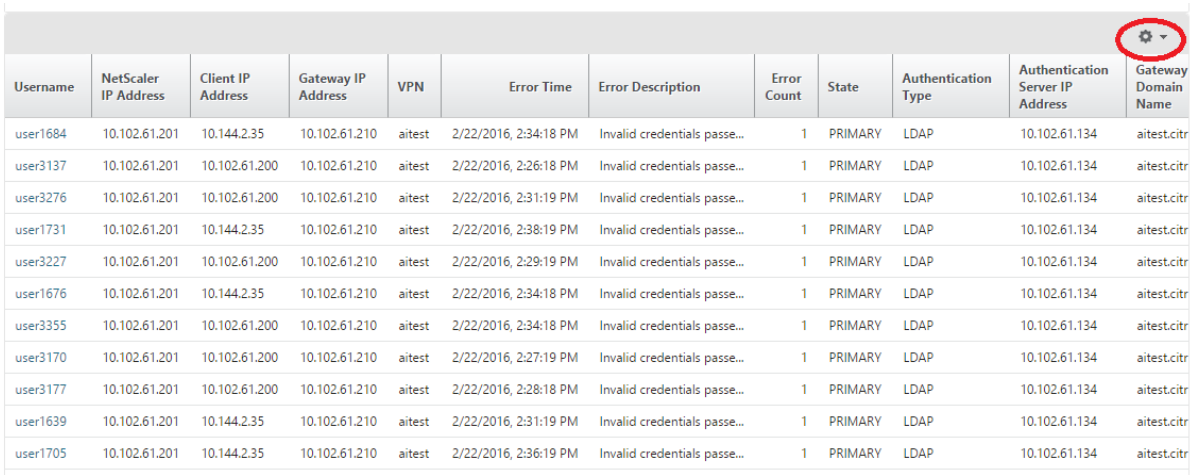
そのタブのまま下にスクロールすると、**Username**、**Client IP Address**、**Error Time**、**Authentication Type**、**Authentication Server IP Address** などの各認証エラーの詳細を表で確認できます。表の [エラーの説明] 列にはログオン失敗の理由が表示され、[状態] 列には、2 段階認証のどの段階でエラーが発生したかが表示されます。



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

[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。

次のスクリーンショットに示すように、下向き矢印を使用して、列を追加または削除するテーブルをカスタマイズできます。



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

EPA エラー

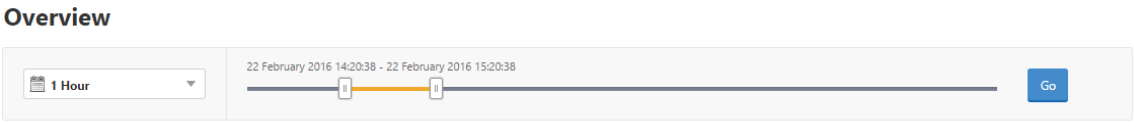
EPA の失敗は、認証前または認証後の段階で確認できます。

> 重要:
>
> - EPA の失敗は、クラシック式が設定されている場合にのみ報告されます。
> - 事前認証ポリシーまたは認証後ポリシーで高度な式が設定されている場合、EPA の失敗は報告されません。
> - EPA が nFactor 認証フローの要素の 1 つとして構成されている場合、EPA の失敗は報告されません。

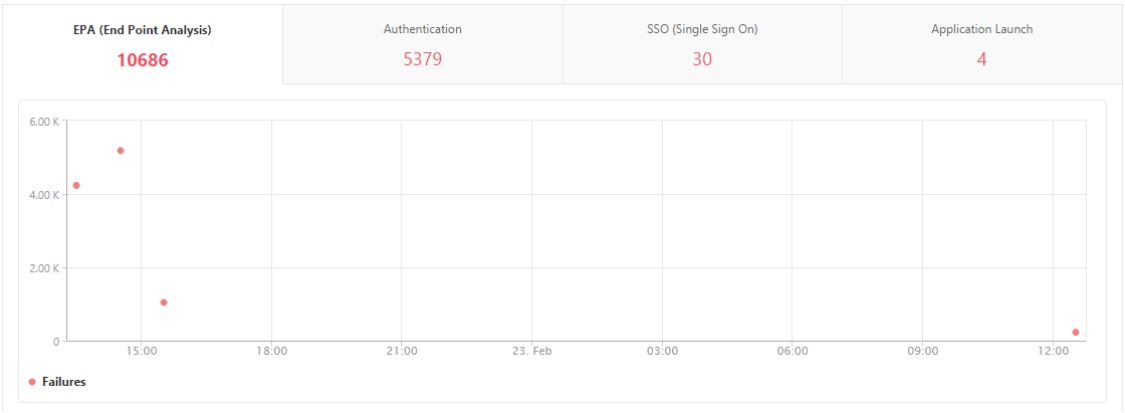
EPA 障害の詳細を表示するには、次の手順に従います。

1. NetScaler ADM で、[**Analytics] > [Gateway Insight**] に移動します。

2. [Overview] セクションで EPA エラーを表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。[**Go**] をクリックします。



3. [**EPA (**終点解析**)**] タブをクリックします。特定の時点における EPA エラーの数は、障害 グラフで表示できます。



そのタブのまま下にスクロールすると、**Username**、**NetScaler IP Address**、**Gateway IP Address**、**VPN**、**Error Time**、**Policy Name**、**Gateway Domain Name** などの各 EPA エラーの詳細を表で確認できます。表の [**Error Description**] 列には EPA エラーの理由が記載されており、[**Policy Name**] 列にはエラーの原因となったポリシーが示されています。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

[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。

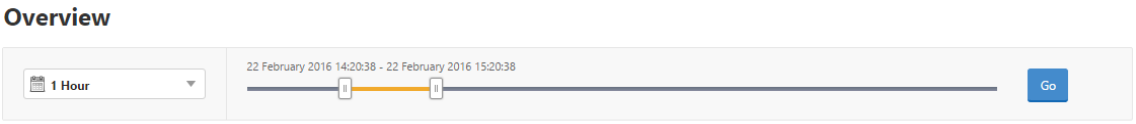
> 注
>
> 「ClientSecurity」式が VPN セッションポリシールールとして構成されている場合、NetScaler Gateway は EPA の失敗を報告しません。

SSO の障害

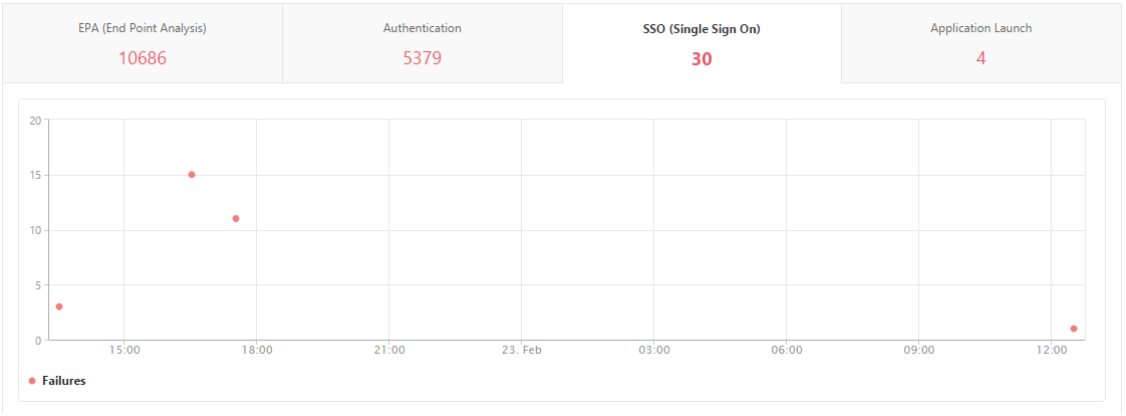
Citrix Gateway アプライアンスを介してアプリケーションにアクセスするユーザーのすべての SSO 障害を任意の段階で表示できます。

SSO 障害の詳細を表示するには、次の手順に従います。

1. NetScaler ADM で、[**Analytics] > [Gateway Insight**] に移動します。
2. [Overview] セクションで SSO エラーを表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。[**Go**] をクリックします。



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。

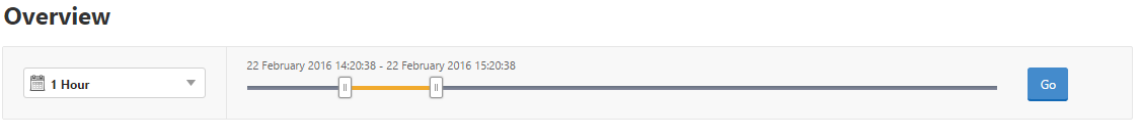
下向きの矢印を使用して、テーブルをカスタマイズして列を追加または削除できます。

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

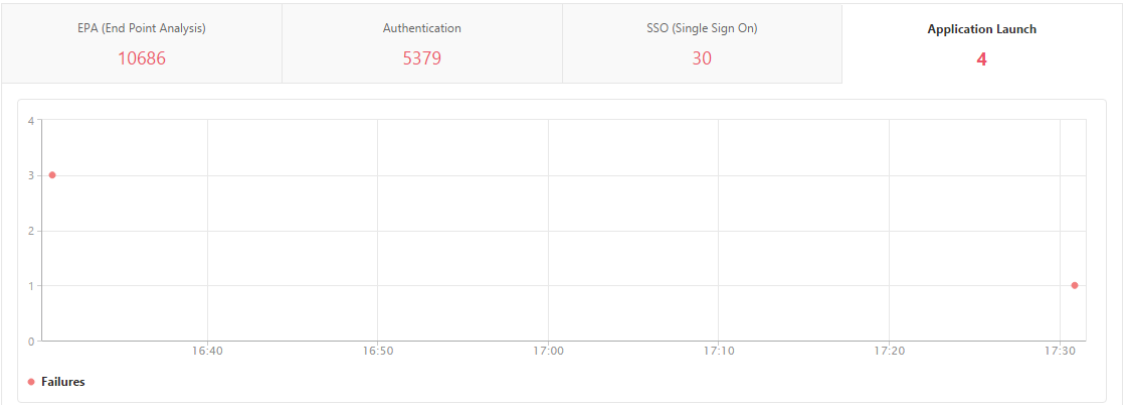
アプリケーションの起動に失敗した場合、Secure Ticket Authority（STA）または Citrix Virtual Apps サーバーにアクセスできない、STA チケットが無効であるなどの原因を把握できます。エラーの時間や詳細、STA 検証ができなかったリソースについて確認できます。

アプリケーションの起動失敗の詳細を表示するには、次の手順に従います。

1. NetScaler ADM で、[**Analytics] > [Gateway Insight**] に移動します。
2. 「概要」セクションで、SSO エラーを表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。[**Go**] をクリックします。



3. [アプリケーションの起動] タブをクリックします。[失敗] グラフでは、任意の時点でのアプリケーション起動の 失敗 数を表示できます。



そのタブのまま下にスクロールすると、**NetScaler IP Address**、**Error Time**、**Error Description**、**Resource Name**、**Gateway Domain Name** などの各アプリケーション起動エラーの詳細を表で確認できます。表の [**Error Description**] 列には STA サーバーの IP アドレスが、[**Resource Name**] 列には STA 検証ができなかったリソースの詳細が表示されています。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

[Us **ername**] 列でユーザーをクリックすると、アプリケーションの起動エラーとそのユーザーのその他の詳細を表示できます。

下向きの矢印を使用して、テーブルをカスタマイズして列を追加または削除できます。

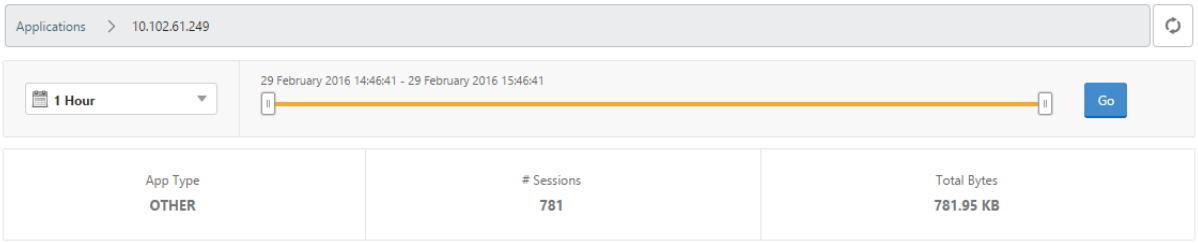
新しいアプリケーションを正常に起動した後、ユーザーは、そのアプリケーションによって消費された合計バイト数と帯域幅を表示したい

新しいアプリケーションを正常に起動したら、NetScaler ADM で、そのアプリケーションによって消費された合計バイト数と帯域幅を表示できます。

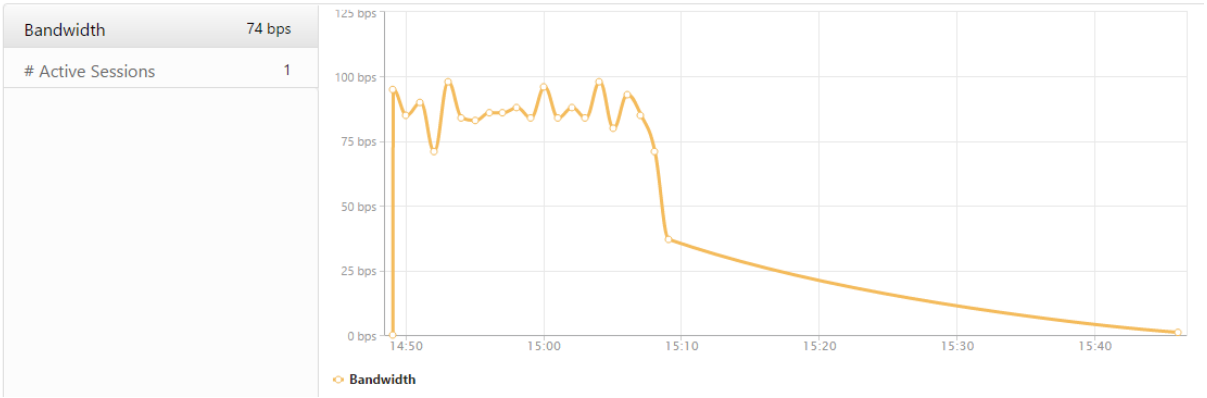
アプリケーションによって消費された合計バイト数と帯域幅を表示するには、次の手順を実行します。

NetScaler ADM で、[**Analytics] > [Gateway Insight] > [**アプリケーション] に移動し、下にスクロールして、[その他のアプリケーション] タブで詳細を表示するアプリケーションをクリックします。

そのアプリケーションが使用したセッション数と合計バイト数が表示されます。



そのアプリケーションが使用した帯域幅も表示されます。

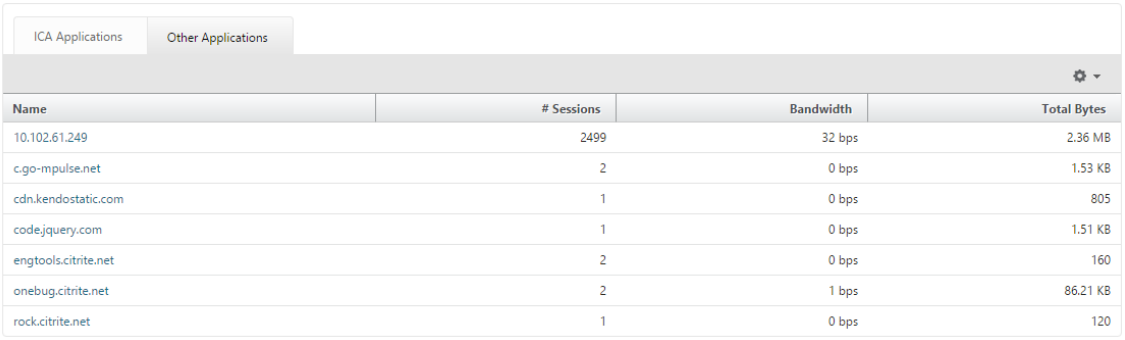


ユーザーが **NetScaler Gateway** に正常にログオンしたが、内部ネットワークの特定のネットワークリソースにアクセスできない

Gateway Insight では、ユーザーがネットワークリソースにアクセスできるかどうかを特定できます。また、エラーの原因となったポリシーの名前を確認できます。

リソースのユーザー・アクセスを表示するには、次の手順に従います。

1. Citrix ADM で、［分析］**>**［**Gateway** インサイト］**>**［アプリケーション］に移動します。
2. 表示される画面で下にスクロールし、[その他のアプリケーション] タブで、ユーザーがログオンできなかったアプリケーションを選択します。



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

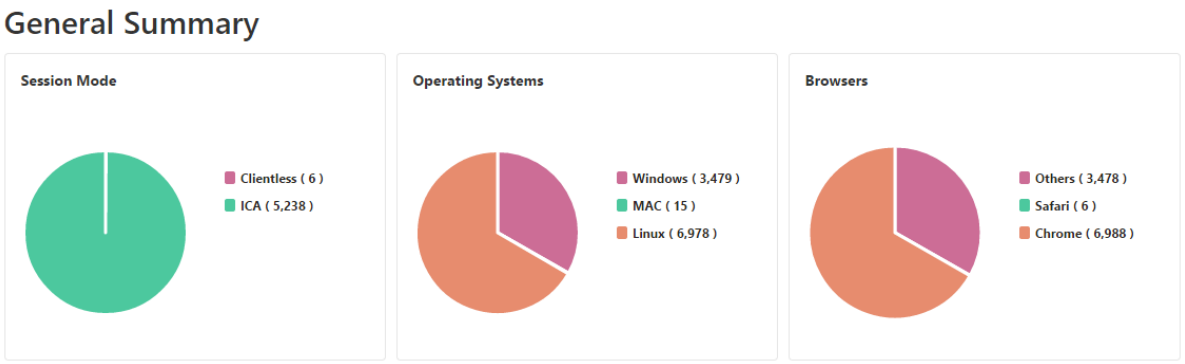
3. 下にスクロールすると、「ユーザー」テーブルに、そのアプリケーションにアクセスできるすべてのユーザーが表示されます。

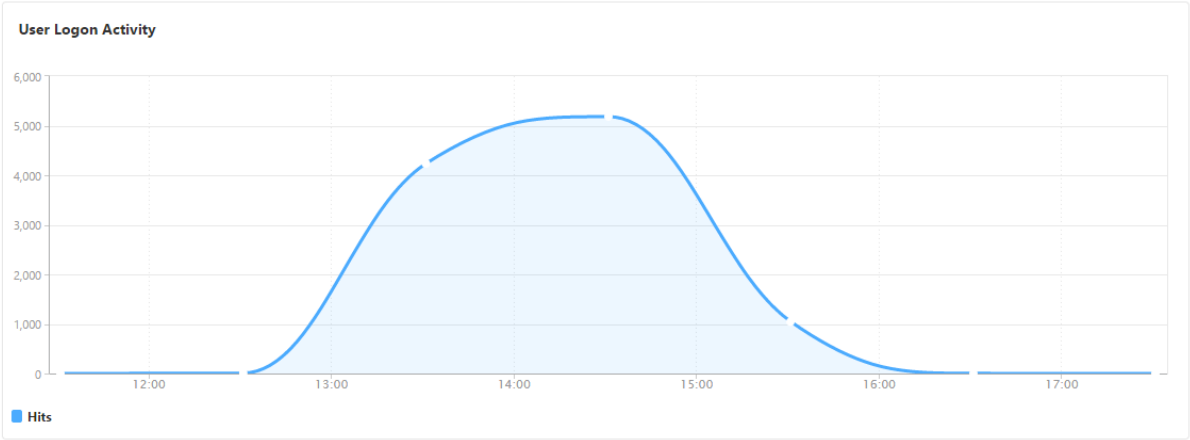
ユーザーが異なる **NetScaler Gateway** 展開環境を使用している場合や、異なるアクセスモードで **NetScaler Gateway** にログオンしている場合があります。管理者は、展開の種類とアクセスモードの詳細を表示できる必要があります

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、およびログオンしているユーザー数の概要を表示するには:

1. NetScaler ADM で、[**Analytics] > [Gateway Insight**] に移動します。
2. [概要] セクションで、下にスクロールして、[セッションモード**]**、**[**オペレーティングシステム**]**、**[**ブラウザ]、および [ユーザーログオンアクティビティ**]** の各グラフに、ユーザーがログオン するために使用するさまざまなセッションモード、クライアントの種類、および 1 時間ごとにログオンしたユーザー数が表示されます。





Gateway Insight の問題のトラブルシューティング

February 6, 2024

Gateway Insight ソリューションが期待どおりに機能しない場合は、次のいずれかに問題がある可能性があります。トラブルシューティングについては、各セクションのチェックリストを参照してください。

- Gateway Insight 設定。
- Citrix ADC と NetScaler ADM 間の接続に問題があります。
- NetScaler ADC でのレコード生成。
- NetScaler ADM での検証。

Gateway Insight 設定チェックリスト

- NetScaler ADC 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。

  コマンドを実行し`show running | grep -i <appflow_policy>`て、ゲートウェイインサイト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
  ```

- 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。
- Citrix ゲートウェイ/VPN 仮想サーバーの「アプリケーションフローログ」パラメータを確認してください。詳しくは、「仮想サーバーに対する AppFlow の有効化」を参照してください。

NetScaler ADC と **NetScaler ADM** の間の接続チェックリスト

- NetScaler ADC で AppFlow コレクタのステータスを確認します。詳しくは、「NetScaler ADC と AppFlow Collector 間の接続状態を確認する方法」を参照してください。
- Gateway Insight AppFlow ポリシーヒットをチェックします。

  コマンド`show appflow policy <policy_name>`を実行して AppFlow ポリシーヒットをチェックします。

  GUI で [システム] **> [AppFlow] > [**ポリシー**]** に移動して、AppFlow ポリシーのヒットを確認することもできます。
- AppFlow ポート 4739 または 5557 をブロックしているファイアウォールを検証します。

NetScaler ADC チェックリストでのレコード生成

- コマンドを実行し`nsconmsg -d stats -g ai_tot`、Citrix ADC の統計情報が増加しているかどうかを確認します。
- nstrace ログをキャプチャし、CFLOW パケットをチェックして、Citrix ADC が AppFlow レコードをエクスポートすることを確認します。

NetScaler ADM での検証

- コマンドを`tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"`実行してログをチェックし、Citrix 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。

Gateway Insight 統計

以下の Gateway Insight の統計情報を確認できます。

- 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

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。
- 問題発生中の Instrace キャプチャ。

既知の問題

ゲートウェイインサイトに関する既知の問題については、NetScaler ADC リリースノートを参照してください。

Security Insight

February 6, 2024

インターネットに接続している Web アプリケーションや Web サービスアプリケーションの攻撃に対する脆弱性が高まってきています。アプリケーションを攻撃から保護するには、脅威を可視化し、攻撃に関する実用的なデータをリアルタイムで把握し、対策に関する推奨事項を把握する必要があります。Security Insight は、アプリケーションのセキュリティ状況を判断し、是正処置を実施してアプリケーションを保護するための統一管理コンソールソリューションです。

> 注
>
> セキュリティインサイトは、バージョン 11.0 ビルド 65.31 以降で動作する Citrix ADC アプライアンスを搭載した Citrix Application Delivery Management（ADM）でサポートされています。

セキュリティインサイトの仕組み

Security Insight は、アプリケーションに関連するさまざまな脅威を把握できる直感的なダッシュボード型のセキュリティ分析ソリューションです。セキュリティインサイトは Citrix ADM に含まれており、アプリケーションファイ

アウォールと Citrix ADC システムのセキュリティ構成に基づいて定期的にレポートを生成します。このレポートには、アプリケーション別に次の情報が含まれています。

- 脅威指数：アプリケーションが Citrix ADC アプライアンスによって保護されているかどうかに関係なく、アプリケーションに対する攻撃の重要度を示す 1 桁の評価システム。アプリケーションに対する攻撃の重大度が高いほど、そのアプリケーションの脅威指数は大きくなります。この指数の範囲は 1〜7 です。

  脅威指数は攻撃情報に基づいています。違反の種類、攻撃のカテゴリ、場所、クライアントの詳細などの、攻撃に関連する情報により、アプリケーションに対する攻撃について正確かつ詳細に把握できます。違反情報は、違反または攻撃が発生した場合にのみ NetScaler ADM に送信されます。侵害や脆弱性が多いと、脅威指数の値が高くなります。

- 安全性指数：外部からの脅威や脆弱性からアプリケーションを保護するために、NetScaler ADC インスタンスをどのように安全に構成したかを示す 1 桁の評価システム。アプリケーションのセキュリティリスクが小さいほど、安全性指数は高くなります。この指数の範囲は 1〜7 です。

  安全指標では、アプリケーションファイアウォール構成と NetScaler ADC システムセキュリティ構成の両方が考慮されます。高い安全性指数値を得るためには、両方の構成を堅牢にする必要があります。たとえば、厳密なアプリケーションファイアウォールチェックが実施されているが、nsroot ユーザーの強力なパスワードなどの Citrix ADC システムのセキュリティ対策が採用されていない場合、アプリケーションには低い安全性指標値が割り当てられます。

- アクショナブルインフォメーション：脅威指数を低くし、安全性指数を高くするために必要な情報。これにより、アプリケーションのセキュリティは大幅に改善されます。たとえば、違反に関する情報、アプリケーションファイアウォールやその他のセキュリティ機能に関する既存の、または欠落しているセキュリティ構成、アプリケーションが攻撃されている割合を確認できます。

セキュリティインサイトの設定

Citrix ADM は、アプリケーションファイアウォールが構成されているすべての Citrix ADC インスタンスからのセキュリティインサイトをサポートします。

ADC インスタンスでセキュリティインサイトを設定するには、まずアプリケーションファイアウォールプロファイルとアプリケーションファイアウォールポリシーを設定します。その後、アプリケーションファイアウォールポリシーをグローバルにバインドできますが、Citrix ではポリシーを仮想サーバーにバインドすることをお勧めします。

Citrix ADM で分析を表示するには、インスタンスで AppFlow 機能を有効にし、AppFlow コレクター、アクション、およびポリシーを構成し、ポリシーをグローバルにバインドします。この場合も、アプリケーションファイアウォールポリシーをグローバルにバインドできますが、Citrix ではポリシーを仮想サーバーにバインドすることをお勧めします。また、Citrix ADM を使用して AppFlow 構成を ADC インスタンスにデプロイすることも推奨しています。コレクタを構成するときは、レポートを監視する NetScaler ADM サーバーの IP アドレスを指定する必要があります。

Citrix ADC インスタンスでセキュリティインサイトを設定するには：

1. 次のコマンドを実行して、アプリケーションファイアウォールのプロファイルとポリシーを構成し、アプリケーションファイアウォールポリシーをグローバルに、または負荷分散仮想サーバーにバインドします。

---

add appfw profile < 名前 > \[**-defaults** (basic advanced)]
名前 >

---

set appfw profile \< 名前\> \[**-startURLAction** \< 開始 URL アクション\> …\]

add appfw policy \< 名前\> \< 規則\> \< プロファイル名\>

bind appfw global \< ポリシー名\> \< 優先度\>

または、

bind lb vserver \<lb 仮想サーバー\> **-policyName** \< ポリシー\> **-priority** \< 優先度\>

```
add appfw profile pr_appfw -defaults advanced
set  appfw profile pr_appfw -startURLaction log stats learn
add appfw policy pr_appfw_pol "HTTP.REQ.HEADER("Host").EXISTS"
   pr_appfw
bind appfw global pr_appfw_pol 1
or,
bind lb vserver outlook  - policyName pr_appfw_pol  - priority  “20
   ”
<!--NeedCopy-->
```

2. 次のコマンドを実行して AppFlow 機能を有効化し、AppFlow コレクター、アクション、ポリシーを構成して、そのポリシーをグローバルに、または負荷分散仮想サーバーにバインドします。

add appflow collector \< 名前\> **-IPAddress** \<IP アドレス\>

---

set appflow param DISABLED)]
[**-SecurityInsightRecordInterval** < 秒 >]
\[**-SecurityInsightTraffic** (ENABLED 秒 >

アプリフローアクションを追加 **\ <**name\ > **-**コレクター \ <string\ >

add appflow policy \< 名前\> \< 規則\> \< アクション\>

bind appflow global \< ポリシー名\> \< 優先度\> \[\<goto 優先度式\>\] \[**-type** \< タイプ\>\]

または

bind lb vserver \< 仮想サーバー\> **-policyName** \< ポリシー\> **-priority** \< 優先度\>

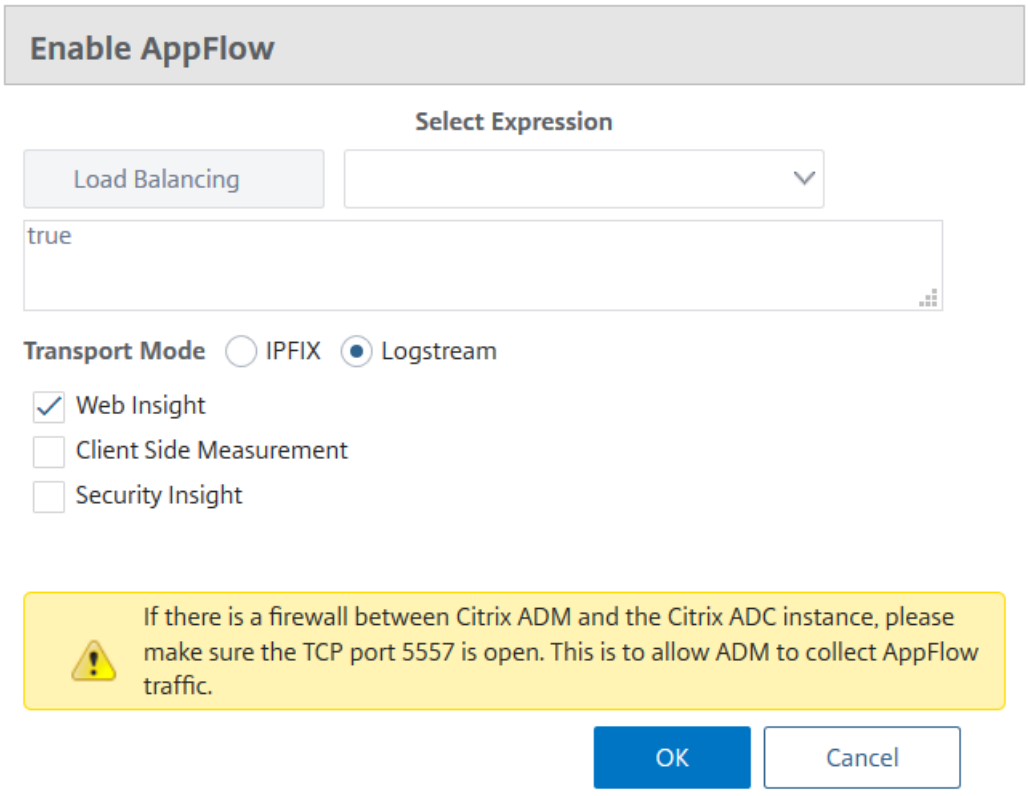
```
add appflow collector col -IPAddress 10.102.63.85
set appflow param  -SecurityInsightRecordInterval 600 -
   SecurityInsightTraffic ENABLED
```



```
3  add appflow action act1 -collectors col
4  add appflow action af_action_Sap_10.102.63.85 -collectors col
5  add appflow policy pol1 true act1
6  add appflow policy af_policy_Sap_10.102.63.85 true
      af_action_Sap_10.102.63.85
7  bind appflow global pol1 1 END -type REQ_DEFAULT
8  or,
9  bind lb vserver Sap  - policyName af_action_Sap_10.102.63.85  -
      priority  “20”
10 <!--NeedCopy-->
```

Citrix ADM から **AppFlow** を有効にするには:

1. Web ブラウザで、**Citrix 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. [ネットワーク] > [インスタンス] に移動し、AppFlow を有効にする NetScaler ADC インスタンスを選択します。
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. 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。
6. 「**AppFlow** を有効にする」フィールドに「**true**」と入力し、「セキュリティインサイト」を選択します。
7. [**OK**] をクリックします。



Security Insight レポートの地理的な場所を表示する

Security Insight レポートには、クライアントのリクエストが発生した正確な地理的場所が含まれます。Citrix ADM で地理的な場所を表示できます。Citrix ADC に組み込まれている地理データベースファイルには、ほとんどのパブリック IP アドレスが含まれています。このファイルは、Citrix ADC の **/var/netscaler/inbuilt_db** という場所にあります。

位置情報を有効にするには**:**

次のコマンドを実行して位置情報ログおよび CEF 形式でのログを有効にします。

- ロケーションファイルを追加 **<**Complete path with the DB filename>
- **set appfw settings -geoLocationLogging ON**
- **set appfw settings -CEFLogging ON**

地理データベースファイルで使用できない IP アドレスがある場合は、地理的位置の IP アドレスを追加できます。IP アドレスに加えて、都市名、州名、国名、および各場所の緯度と経度の座標を追加することもできます。

vi エディタなどのテキストエディタで geo データベースファイルを開き、すべての場所のエントリを追加します。

エントリは、次の形式で指定する必要があります。

```
\<start IP\>,\<end IP\>,,\<country\>,\<state\>,,\<city\>,,longitude,
latitude
```

例:

```
4.17.142.224,4.17.142.239,,US,New York,,Harrison,,73.7304,41.0568
<!--NeedCopy-->
```

IP レピュテーション

NetScaler Insight Center を使用して着信トラフィックの IP レピュテーションを監視および管理できます。悪意のある IP を追加するよう各種ポリシーを構成して、カスタマイズされたブロックリストを作成できます。

IP レピュテーションの設定と使用については、IP レピュテーションを参照してください。

IP レピュテーションの監視

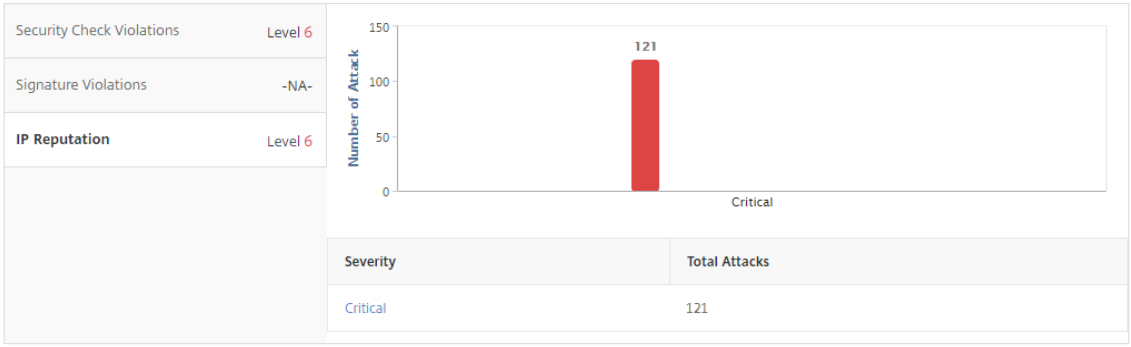
IP レピュテーション機能は、悪意のある IP アドレスに関する攻撃関連情報を提供します。たとえば、IP レピュテーションスコア、IP レピュテーションカテゴリ、IP レピュテーション攻撃時間、デバイス IP、およびクライアント IP アドレスに関する詳細がレポートされます。

IP レピュテーションスコアは、IP アドレスに関連付けられたリスクを示します。このスコアの範囲は次のとおりです。

IP レピュテーションスコア	リスクの程度
1–20	高リスク
21–40	疑わしい
41–60	中程度のリスク
61–80	低リスク
81–100	信頼できる

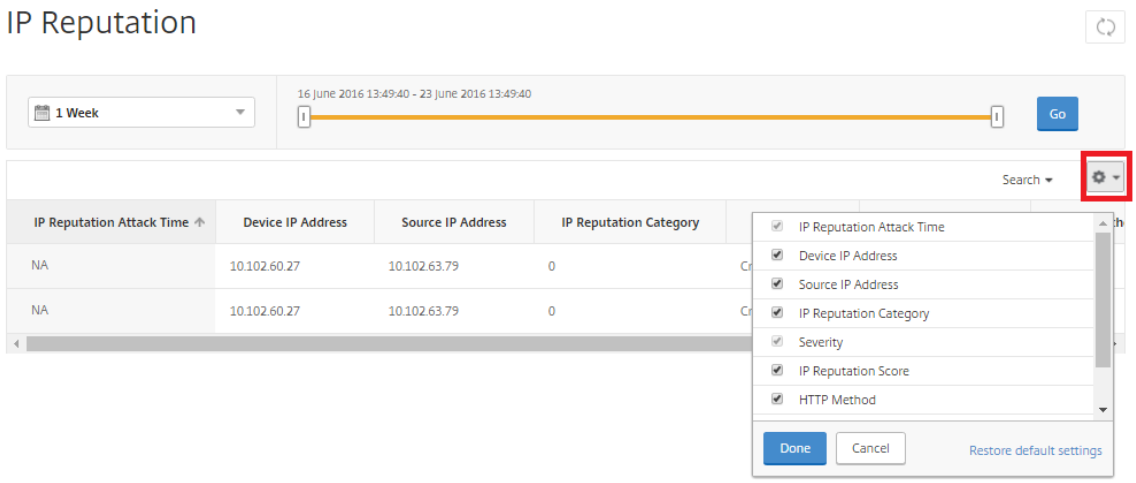
IP レピュテーションを監視するには、次の手順に従います。

1. [分析] > **[** セキュリティインサイト] に移動し、監視するアプリケーションを選択します。
2. [脅威インデックス] タブで、[**IP** レピュテーション**]** を選択します。



3. 重大度を選択して、そのレベルの攻撃の詳細を表示します。棒グラフをクリックするか、グラフの下の表をクリックします。
4. 詳細を表示する期間を選択します。時間スライダーを使用して選択する期間をカスタマイズできます。次に［**Go**］をクリックします。

5. 表示をカスタマイズするには、［Settings］をクリックします。



しきい値

Security Insight でアプリケーションの安全性指数と脅威指数のしきい値を設定および表示できます。

しきい値を設定するには**:**

1. [アナリティクス] > [設定] > [しきい値] に移動し、[追加] を選択します。
2. 「トラフィックタイプ」フィールドで「セキュリティ」としてトラフィックタイプを選択し、名前、期間、エンティティなどの他の適切なフィールドに必要な情報を入力します。
3. 「ルールを設定」セクションで、「メトリック」、「コンパレーター」、「値」の各フィールドを使用してしきい値を設定します。

   入力例:”Threat Index”“>”“5”
4. 通知設定で、通知タイプを選択します。
5. [作成] をクリックします。

しきい値違反を確認するには**:**

1. [分析] > **[** セキュリティインサイト ****] > [**** デバイス] に移動し、Citrix ADC インスタンスを選択します。
2. [アプリケーション] セクションの [Threshold **Breach]** 列には、各仮想サーバで発生したしきい値違反の数が表示されます。

セキュリティインサイトのユースケース

次のユースケースでは、Security Insight を使用して、アプリケーションの脅威環境を査定し、セキュリティ対策を向上する方法を説明します。

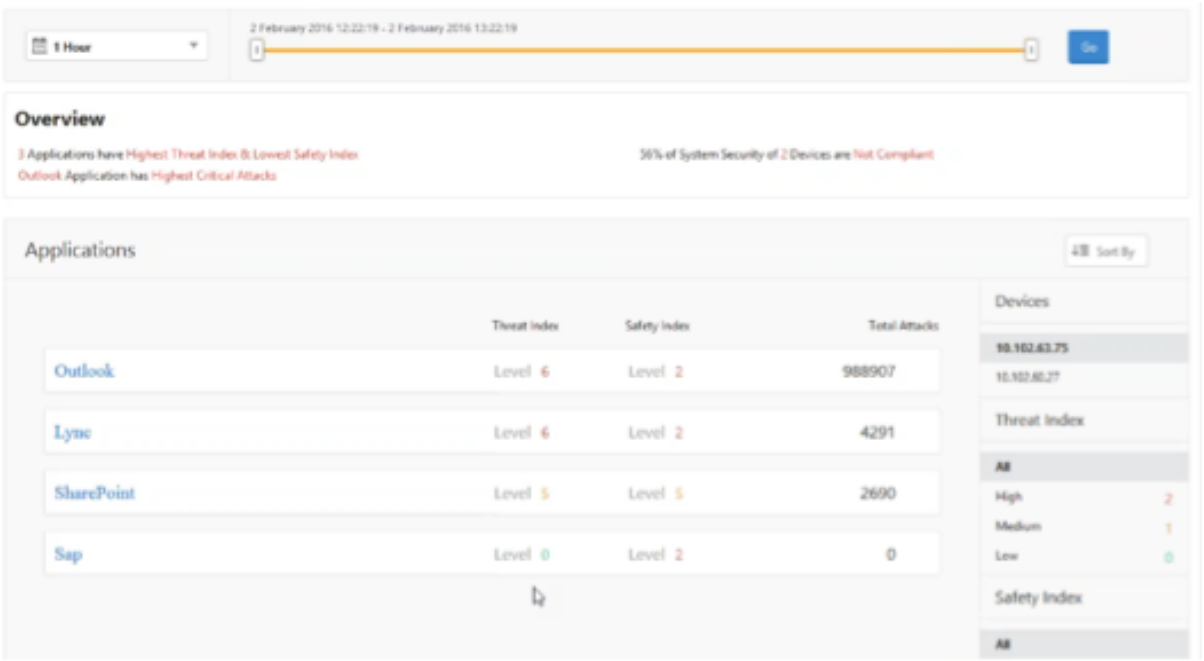
脅威環境の概要を把握する

このユースケースでは、攻撃にさらされる一連のアプリケーションがあり、脅威環境を監視するように NetScaler ADM を構成しています。脅威指数、安全性指数、およびアプリケーションで発生した可能性のある攻撃の種類と重大度を頻繁に確認する必要があります。このレビュー により、最も注意が必要なアプリケーションに最初に焦点を当てることができます。Security Insight ダッシュボードには、選択した期間および選択した NetScaler ADC デバイスについて、アプリケーションが経験した脅威の概要が表示されます。アプリケーションの一覧、脅威指数と安全性指数、選択した期間の攻撃回数の合計が表示されます。

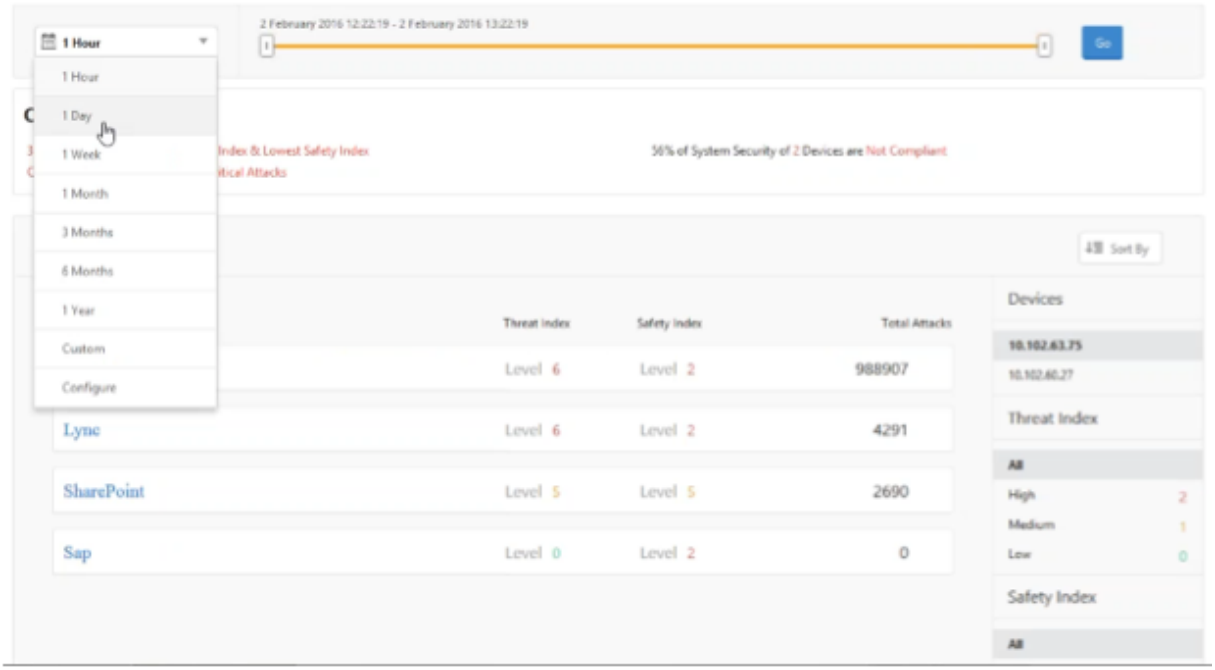
たとえば、Microsoft Outlook、Microsoft Lync、SharePoint、および SAP アプリケーションを監視しており、これらのアプリケーションの脅威環境の概要を確認するとします。

脅威環境の概要を取得するには、**NetScaler ADM** にログオンし、［**Analytics**］**>**［**Security Insight**］に移動します。

各アプリケーションの主要情報が表示されます。デフォルトの期間は 1 時間です。



異なる期間の情報を表示するには、左上のリストから期間を選択します。



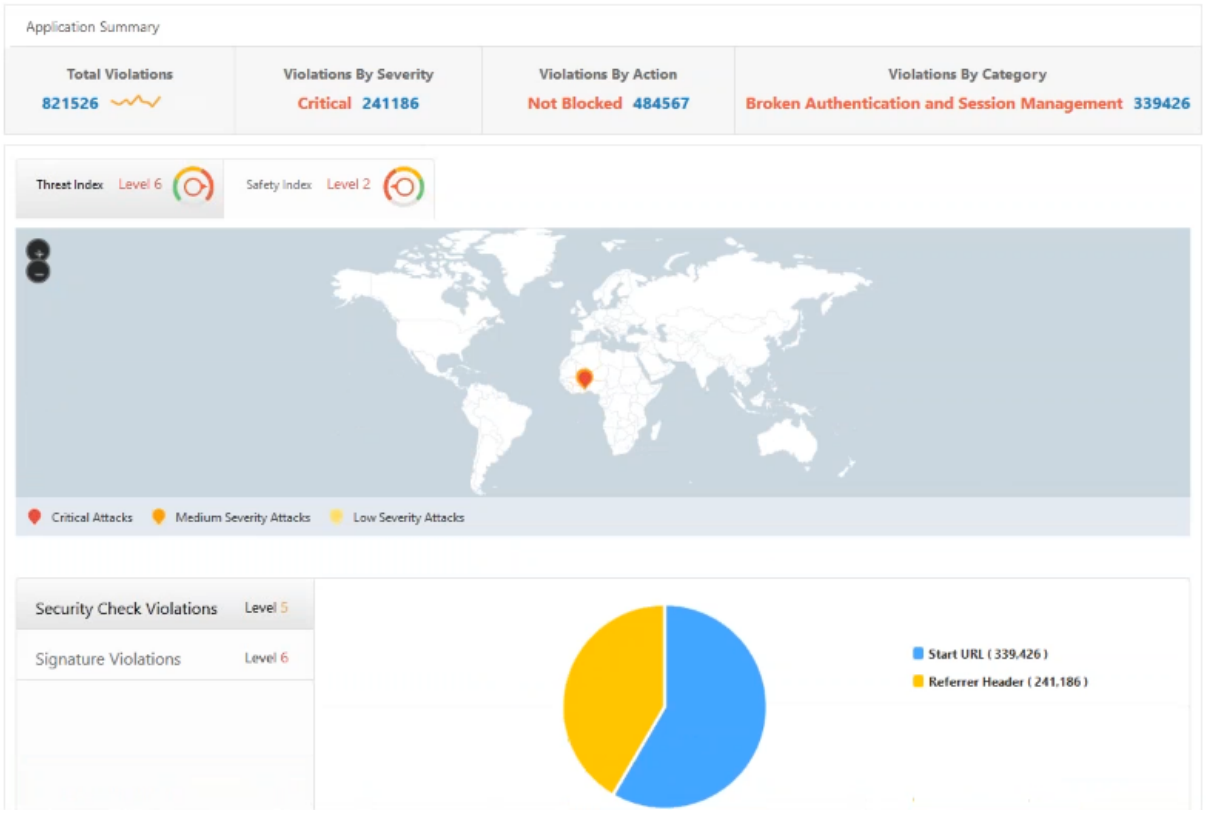
別の NetScaler ADC インスタンスの概要を表示するには、[デバイス] で、NetScaler ADC インスタンスの IP アドレスをクリックします。特定の列でアプリケーションの一覧を並べ替えるには、その列の見出しをクリックします。

アプリケーションが脅威にさらされる危険性を判断する

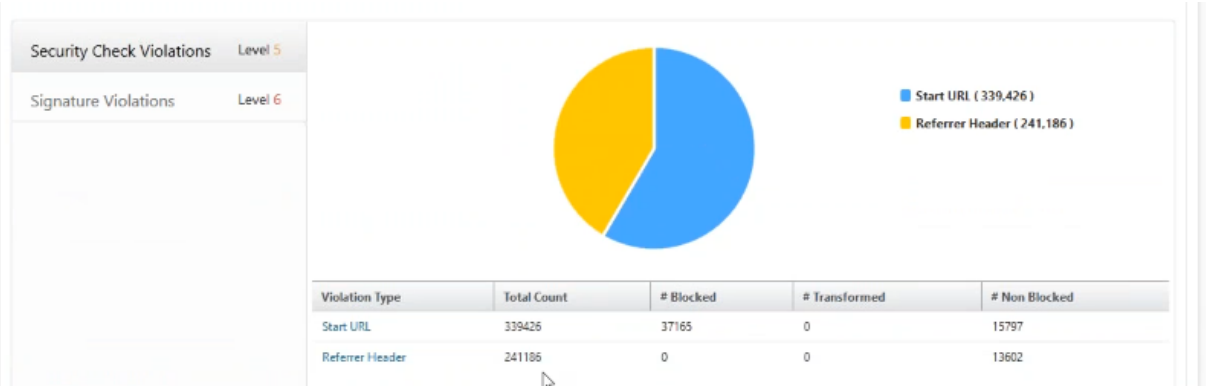
Security Insight ダッシュボードで脅威指数が高く安全性指数が低いアプリケーションを特定するには、保護を決定する前に脅威にさらされる危険性を判断する必要があります。つまり、指数値を下げている攻撃の種類と重大度を確認します。アプリケーションの脅威への露出度を判断するには、アプリケーションの概要を表示します。

この例では、Microsoft Outlook の脅威指数値が 6 になっており、この高い脅威指数の原因となっている要因を調べる必要があります。

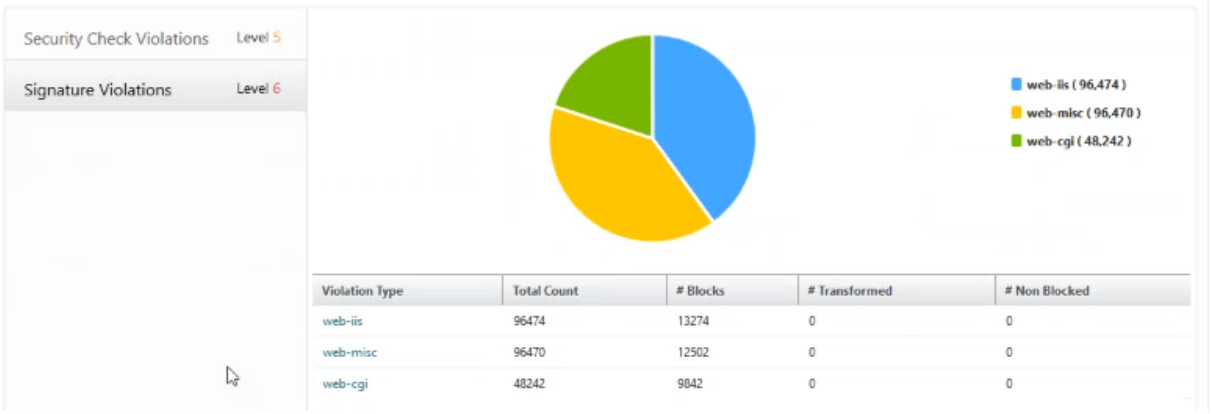
Microsoft Outlook の脅威への露出度を調べるには、[**Security Insight**] ダッシュボードで、[**Outlook**] をクリックします。アプリケーション概要に、サーバーの位置情報を特定する地図が含まれています。



[**Threat Index**] > [**Security Check Violations**] をクリックして、表示される違反情報を確認します。



[署名] [違反] をクリックし、表示される違反情報を確認します。

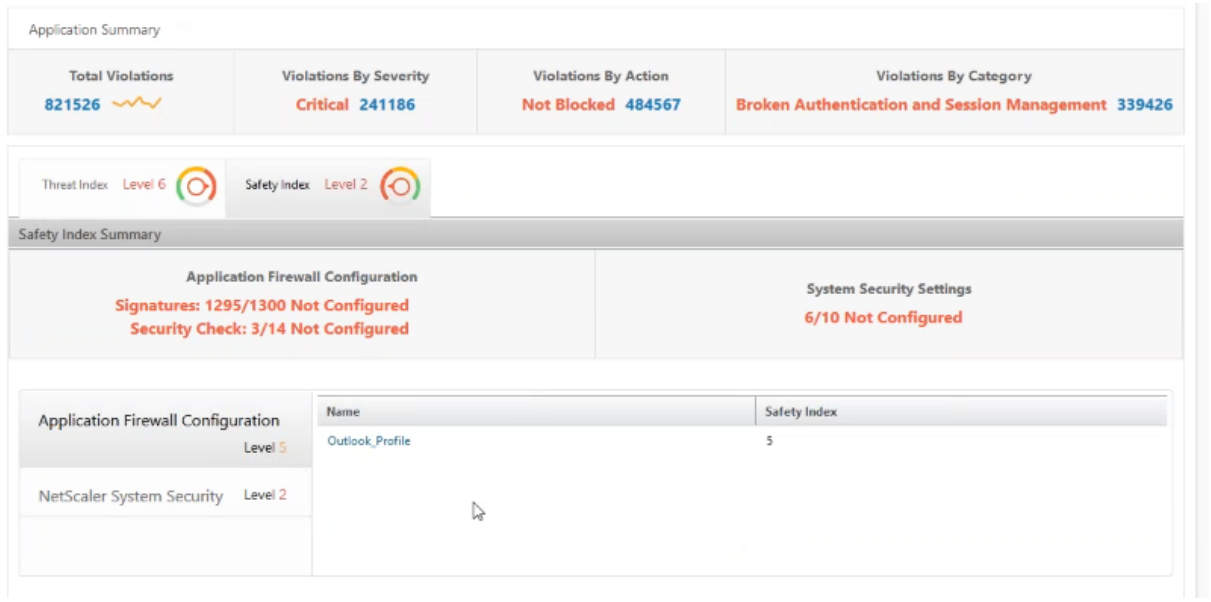


アプリケーションの既存のセキュリティ構成と欠落しているセキュリティ構成を判別する

アプリケーションの脅威への露出度を確認したら、そのアプリケーションに設定されているセキュリティ構成と欠落しているセキュリティ構成を確認します。この情報は、アプリケーションの安全性指数概要にドリルダウンすると表示されます。

安全性指数概要には、次のセキュリティ構成の有効性に関する情報が表示されます。

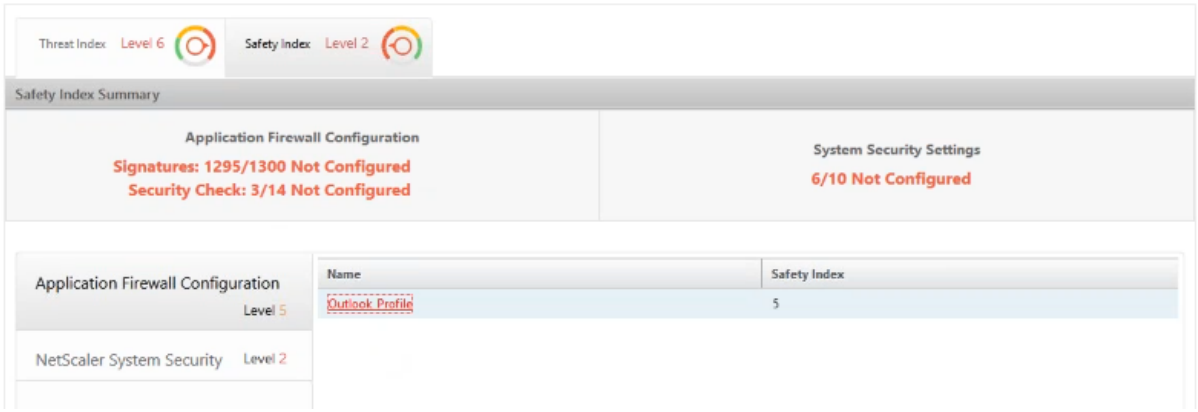
- アプリケーションファイアウォール構成。構成されていないシグネチャおよびセキュリティエンティティの数を表示します。
- **NetScaler** システムセキュリティ。構成されていないシステムセキュリティ設定の数を表示します。



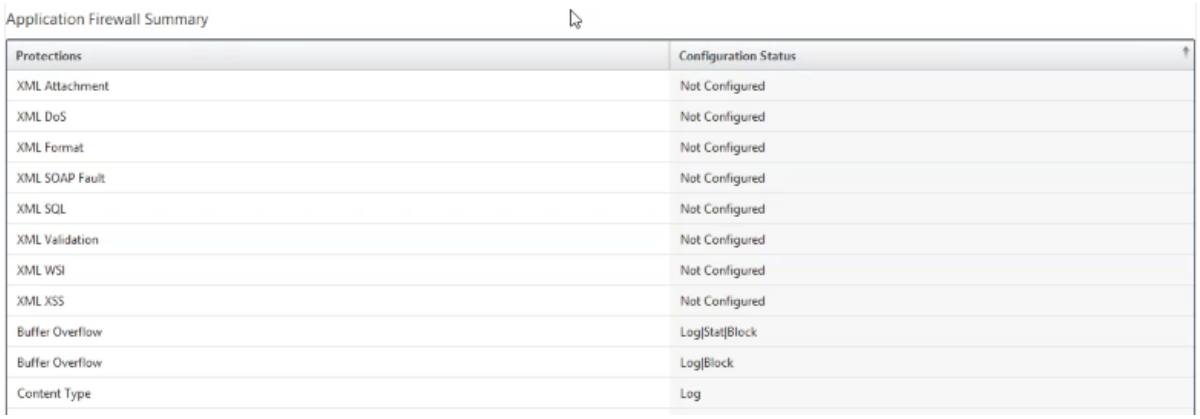
前出のユースケースでは、Microsoft Outlook の脅威への露出度（脅威指数値は 6）について調査しました。次に、Outlook に設定されているセキュリティ構成と、どのような構成を追加すれば脅威指数を改善できるのかを調べる必要があります。

[**Security Insight**] ダッシュボードで、[**Outlook**] をクリックし、[**Safety Index**] タブをクリックします。[**Safety Index Summary**] 領域に表示された情報を確認します。

[アプリケーションファイアウォールの構成] ノードで、[**Outlook_Profile**] をクリックし、セキュリティチェックと署名違反の情報を円グラフで確認します。



アプリケーションファイアウォール概要表で各保護タイプの構成ステータスを確認します。特定の列で表を並べ替えるには、列見出しをクリックします。

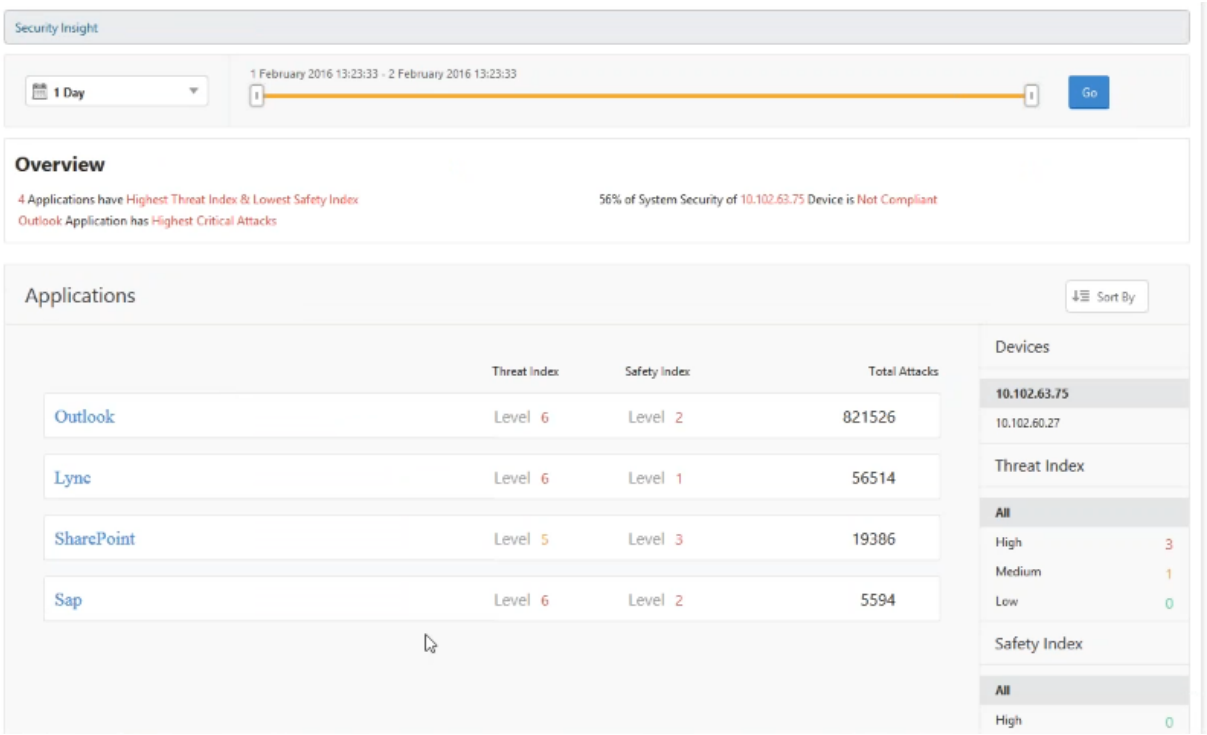


[**NetScaler System Security**] ノードをクリックして、システムセキュリティ設定と Citrix の推奨事項を確認し、アプリケーションの安全性指数を改善します。

即時の対応が必要なアプリケーションを特定

直ちに対処する必要があるアプリケーションとは、脅威指数が高く安全性指数が低いアプリケーションです。

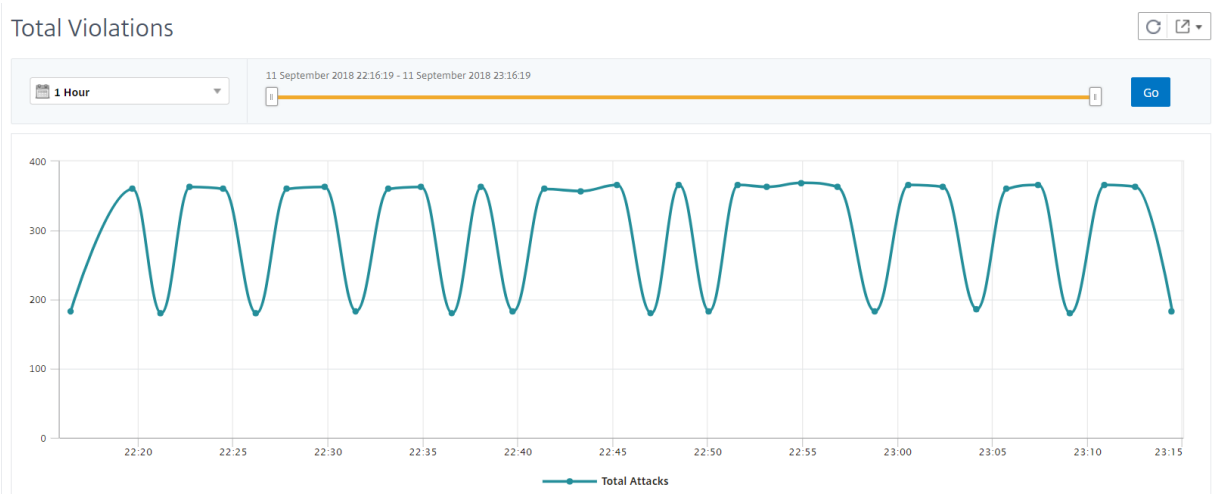
この例では、Microsoft Outlook と Microsoft Lync が高い脅威指数値（6）を示していますが、安全性指数は Lync のほうが低くなっています。したがって、最初に Lync に注意を払い、その後で Outlook の脅威環境を改善します。



特定の期間における攻撃の数を判別

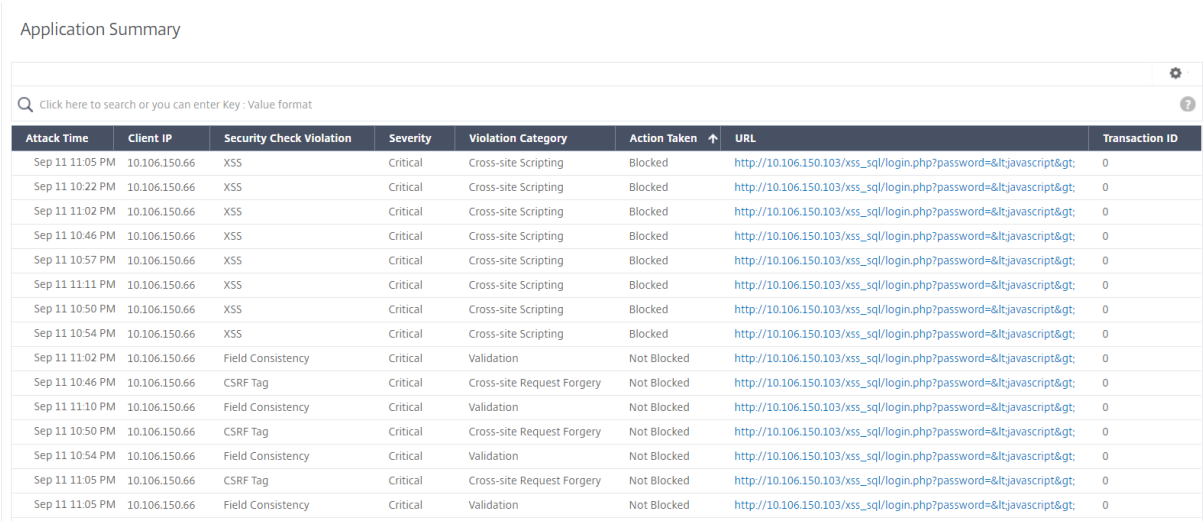
特定のアプリケーションで特定の時間帯に発生した攻撃の数や、指定した期間の攻撃発生率を調べてみます。

Security Insight ページで任意のアプリケーションをクリックし、[アプリケーションの概要] で違反の数をクリックします。違反合計ページには、1 時間、1 日、1 週間および 1 ヶ月の攻撃がグラフィカルに表示されます。



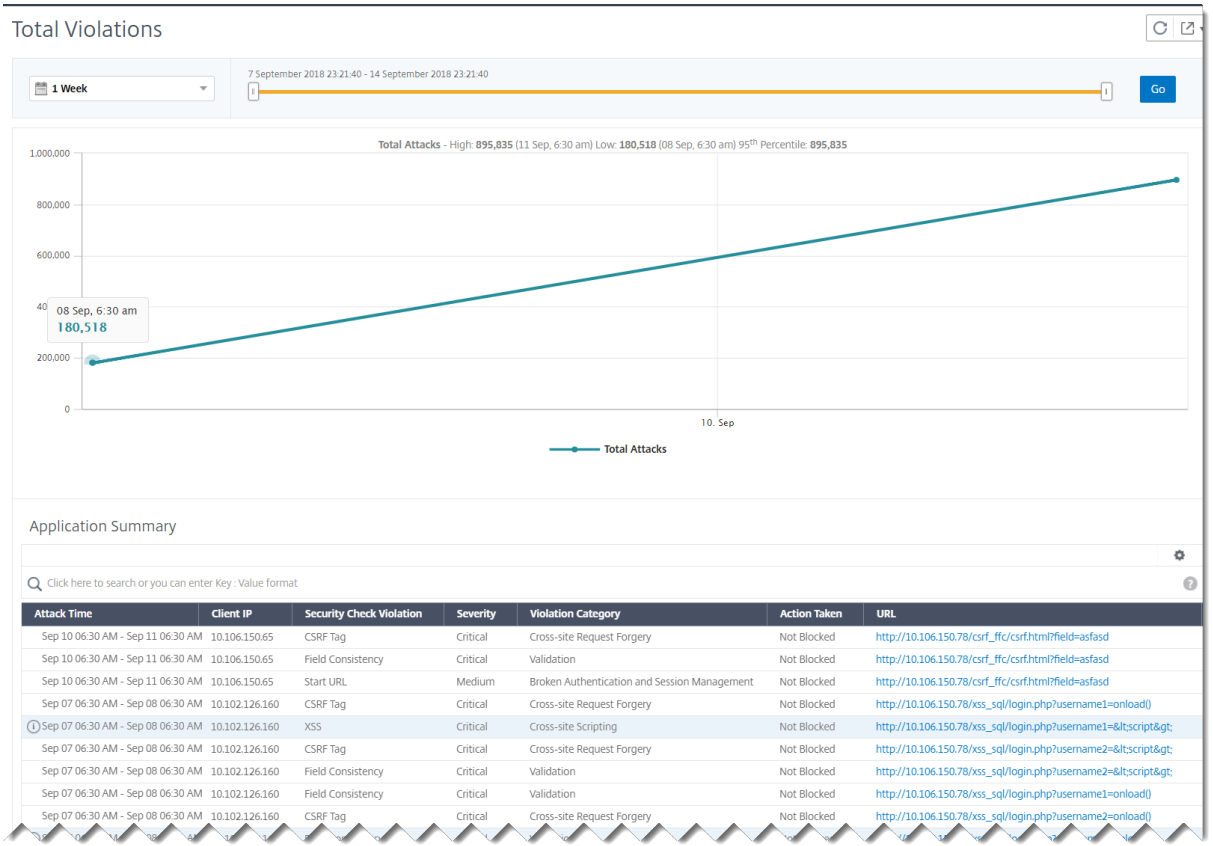
[アプリケーションの概要] テーブルには、攻撃の詳細が表示されます。それらのいくつかは以下のとおりです。

- アタックタイム
- 攻撃が発生したクライアントの IP アドレス
- 重要度
- 違反のカテゴリー
- 攻撃の発信元の URL、およびその他の詳細。



Attack Time	Client IP	Security Check Violation	Severity	Violation Category	Action Taken	URL	Transaction ID
Sep 11 11:05 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:22 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:02 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:46 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:57 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:11 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:50 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:54 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:02 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:46 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:10 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:50 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:54 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:05 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:05 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0

攻撃時間は、画像のように時間ごとのレポートでいつでも表示できますが、日次レポートや週次レポートでも、集計レポートの攻撃時間範囲を表示できるようになりました。期間リストから「1 日」を選択すると、セキュリティインサイトレポートには、集計されたすべての攻撃が表示され、攻撃時間が 1 時間の範囲で表示されます。「1 週間」または「1 ヶ月」を選択すると、すべての攻撃が集計され、攻撃時間が 1 日の範囲で表示されます。

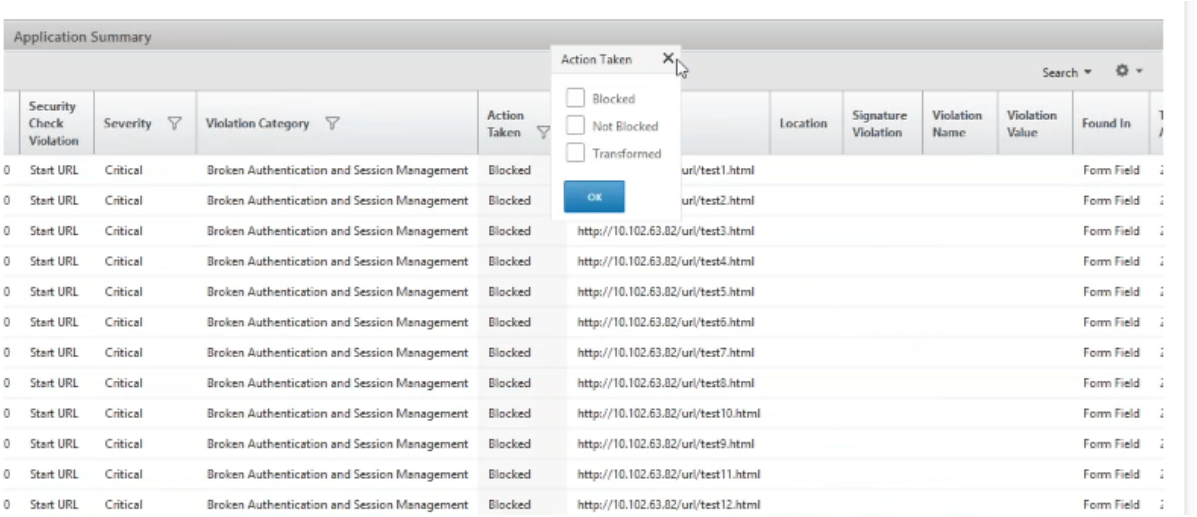


セキュリティ侵害に関する詳細情報の取得

アプリケーションに対する攻撃のリストを表示して、攻撃の種類と重大度、Citrix ADC インスタンスが実行したアクション、要求されたリソース、および攻撃の原因に関する洞察を得たい場合があります。

たとえば、Microsoft Lync に対する攻撃がブロックされた数、要求されたリソース、発信元の IP アドレスを調べます。

[**Security Insight]** ダッシュボードで、[**Lync] > [**違反総数] をクリックします。表の［**Action Taken**］列の見出しにあるフィルターアイコンをクリックし、［**Blocked**］を選択します。



要求されたリソースについて詳しくは、[**URL**] 列を参照してください。攻撃の発信元に関する情報を知りたい場合は、[**Client IP**] 列を確認します。

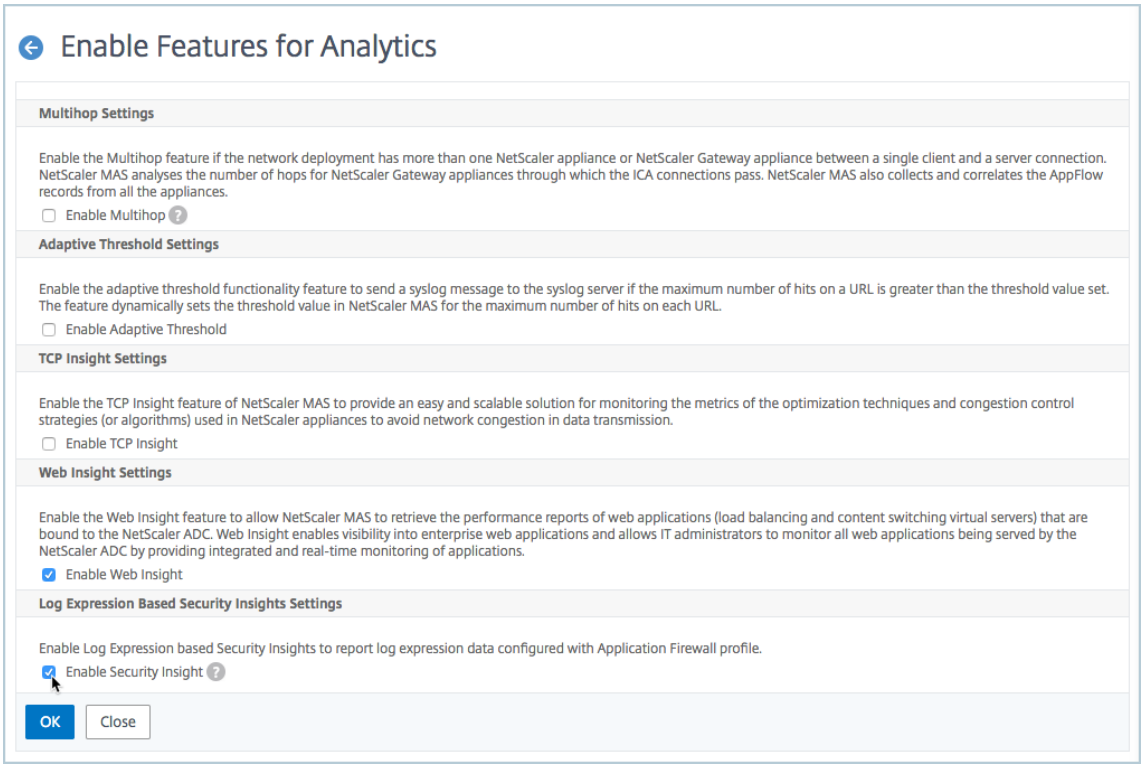
ログ式の詳細を表示する

Citrix ADC インスタンスは、アプリケーションファイアウォールプロファイルで構成されたログ式を使用して、企業内のアプリケーションに対する攻撃に対してアクションを実行します。セキュリティインサイトでは、Citrix ADC インスタンスで使用されるログ式に対して返された値を表示できます。これらの値には、リクエストヘッダー、リクエストボディなどが含まれます。ログ式の値とは別に、Citrix ADC インスタンスが攻撃に対するアクションを実行するために使用したアプリケーションファイアウォールプロファイルに定義されているログ式の名前とコメントを表示することもできます。

前提条件　次のことを確実にします。

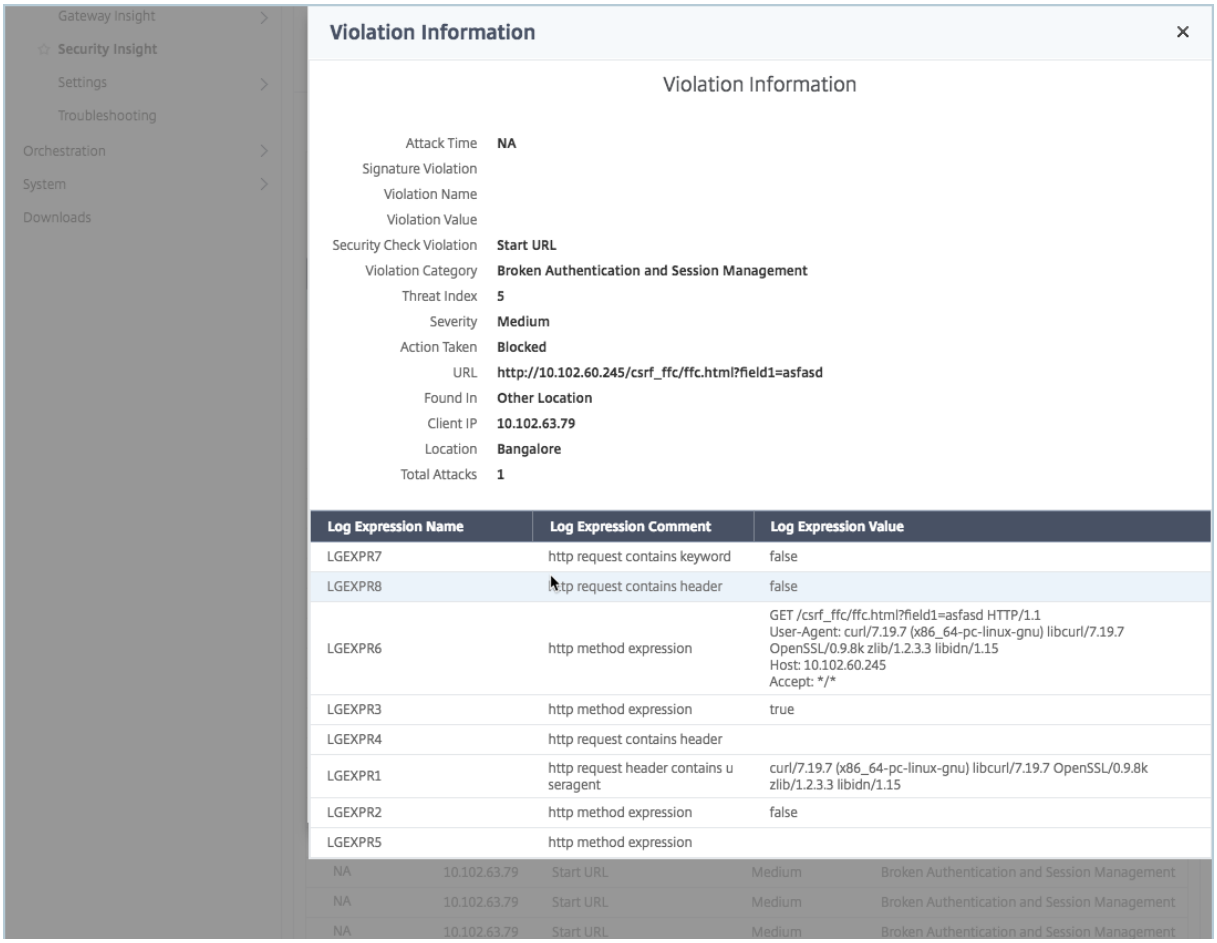
- アプリケーションファイアウォールプロファイルでログ式を設定します。詳しくは、「アプリケーションファイアウォール」を参照してください。
- Citrix ADM でログ式ベースのセキュリティインサイト設定を有効にします。以下を実行します:

  1. [アナリティクス**] > [**設定] に移動し、[アナリティクスの機能を有効にする**]** をクリックします。
  2. [Analytics の機能を有効にする] ページで、[ログ式ベースの **Security Insight** 設定**]** セクションの **[Security Insight** を有効にする] を選択し、[**OK**] をクリックします。



たとえば、企業内の Microsoft Lync に対する攻撃に対して実行したアクションについて、NetScaler ADC インスタンスによって返されるログ式の値を表示できます。

セキュリティインサイトダッシュボードで、[**Lync] > [**違反総数] に移動します。［アプリケーションの概要］表で URL をクリックすると、［違反 情報］ページで違反の完全な詳細が表示されます。ログ式名、コメント、および NetScaler ADC インスタンスがアクションに対して返す値が含まれます。

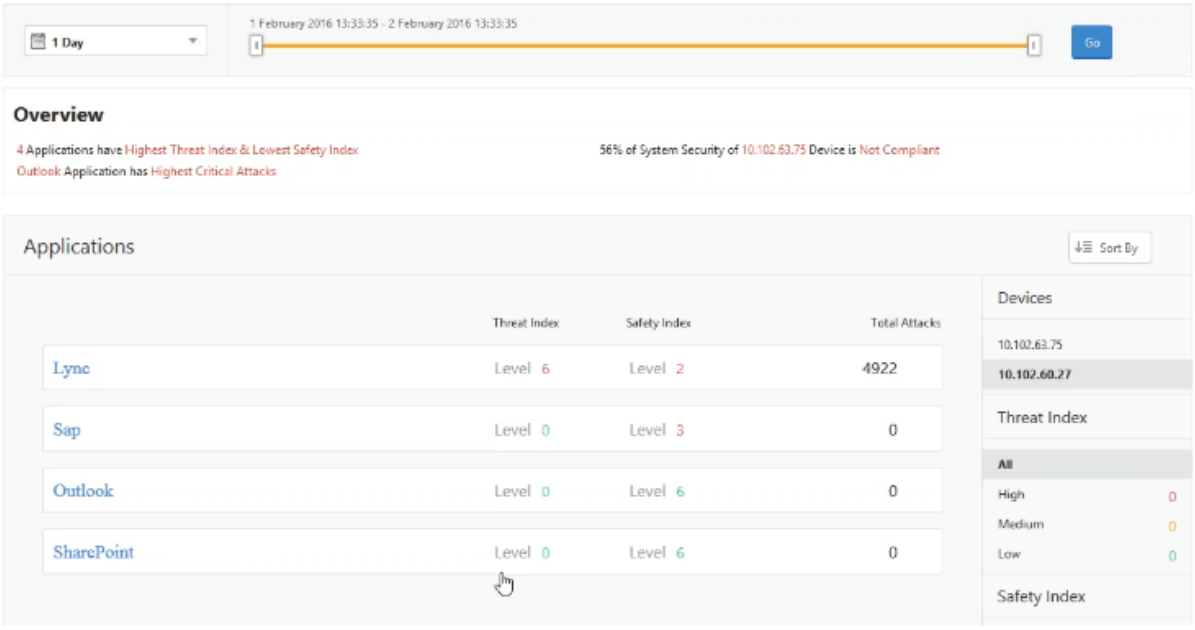


構成を展開する前に安全指数を決定してください

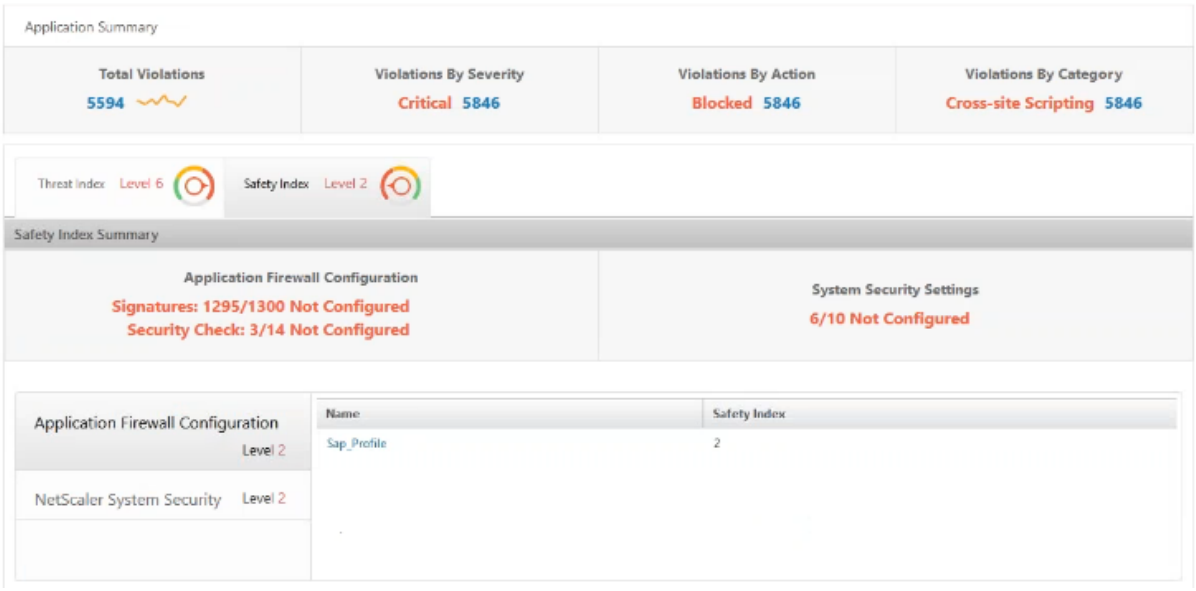
セキュリティ侵害は、NetScaler ADC インスタンスにセキュリティ構成を展開した後に発生しますが、展開する前にセキュリティ構成の有効性を評価することをお勧めします。

たとえば、IP アドレスが 10.102.60.27 の Citrix ADC インスタンス上の SAP アプリケーションの構成の安全性指数を評価したい場合があります。

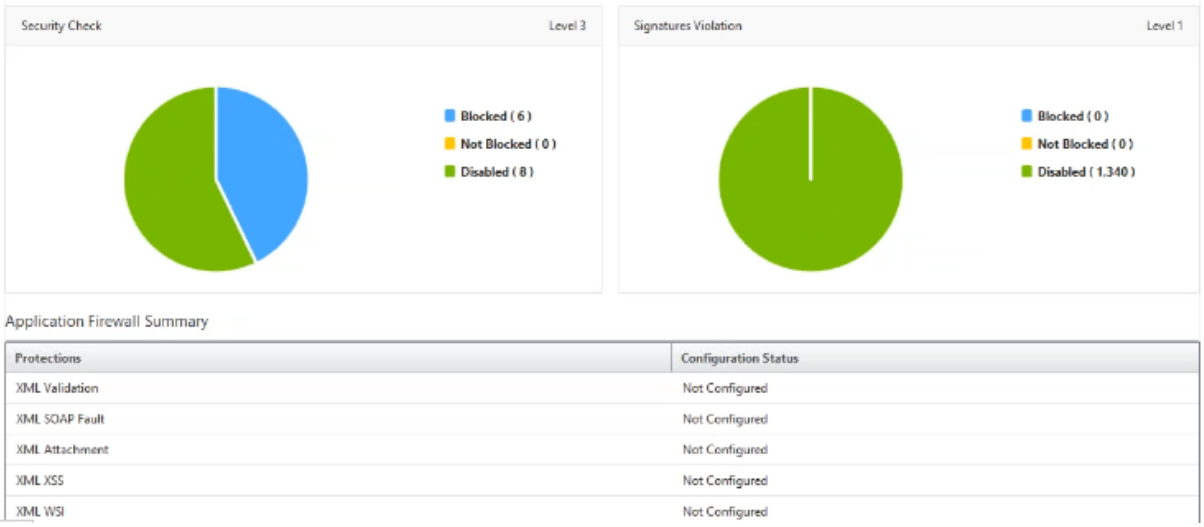
セキュリティインサイトダッシュボードの「デバイス **」で、構成した Citrix ADC インスタンスの IP アドレスをクリックします。脅威指数と攻撃総数はどちらも 0 になっています。脅威指数には、アプリケーションに対する攻撃の数と種類が直接反映されます。攻撃回数がゼロということは、アプリケーションがまったく脅威にさらされていないことを示しています。



［**Sap**］**>**［**Safety Index**］**>**［**SAP_Profile**］の順に選択して、表示される安全性指数情報を評価します。



アプリケーションファイアウォールの概要では、さまざまな保護設定の構成ステータスを確認できます。ログを記録する設定になっている場合や、構成されていない設定がある場合は、アプリケーションに割り当てられる安全性指数は低くなります。



SSL Insight

February 6, 2024

SSL Insight は、セキュアな Web トランザクション（HTTPS）を可視化し、IT 管理者は、セキュアな Web トランザクションのリアルタイムおよび履歴の統合監視を提供することで、NetScaler ADC によって提供されるすべてのセキュアな Web アプリケーションを監視できます。状態を把握することで管理者は以下の評価を行うことができます。

- 構成変更が顧客の使用に与える影響の特定: 管理者は、SSLv3 の無効化や RC4-MD5 などの暗号の削除などの構成変更がクライアントに与える影響を理解できます。そのためには、このプロトコルと暗号に関する履歴トランザクションデータを評価します。
- クライアントのパフォーマンスを定量化: 管理者は、使用された SSL 暗号化/プロトコルまたはネゴシエートされた証明書に基づいて、アプリケーションの応答時間への影響を把握できます。
- アプリケーションセキュリティ: セキュリティレベルの低いプロトコル、暗号、または弱いキー強度でトランザクションが実行されているアプリケーションがないかを評価します。

NetScaler ADC インスタンスで SSLAnalytics を有効にすると、SSL 統計情報が記録され、SSL トランザクションごとに記録されます。この統計により SSL フローの詳細が分かります。また、成功した接続はすべて CitrixApplication Delivery Management（ADM）
Analytics によってログに記録され、表示されます。

SSL Insight は、NetScaler ADM Analytics によって表示される次の重要な情報を提供します。

- SSL プロトコルのバージョンがネゴシエ
- ネゴシエートされた暗号と暗号強度

- 使用された証明書の署名ハッシュアルゴリズム
- 証明書の種類とサイズ
- SSL のフロントエンドおよびバックエンドのエラー

> 注
>
> SSL 接続が成功すると、SSL AppFlow のロギングは各トランザクションの最後に行われます。

前提条件

- SSL Insight を構成する NetScaler ADC インスタンスは、NetScaler ADC ソフトウェアリリース 11.1 51.21 以降を実行している必要があります。11.1 51.21 を実行する ADC インスタンスで次のコマンドを実行して、SSL Insight トランスポートタイプとして Logstream を有効にします。

1. `enable ns mode ulfd`
2. `add ulfd server <IP Address of the ADM>`

   バージョン 12.0 以降を実行する ADC インスタンスの場合は、ADM から AppFlow を有効にしながら、トランスポートタイプとして Logstream を選択します。

- NetScaler ADM バージョンとビルドは、NetScaler ADC のバージョンとビルドと同等かそれ以上でなければなりません。たとえば、NetScaler ADM 11.1 ビルド 61.7 をインストールしている場合は、NetScaler ADC 11.1 ビルド 60.14 以前がインストールされていることを確認します。

SSL Insight の構成

次の要素を有効にした場合、SSL Insight メトリックは Web Insight レポートに組み込まれます。

- 各 Citrix ADC インスタンスで AppFlow for Web Insight を有効にします。
- 各 Citrix ADC インスタンスで ULFD モードを有効にします。
- 各 NetScaler ADC インスタンスで必要な AppFlow パラメータを有効にします。

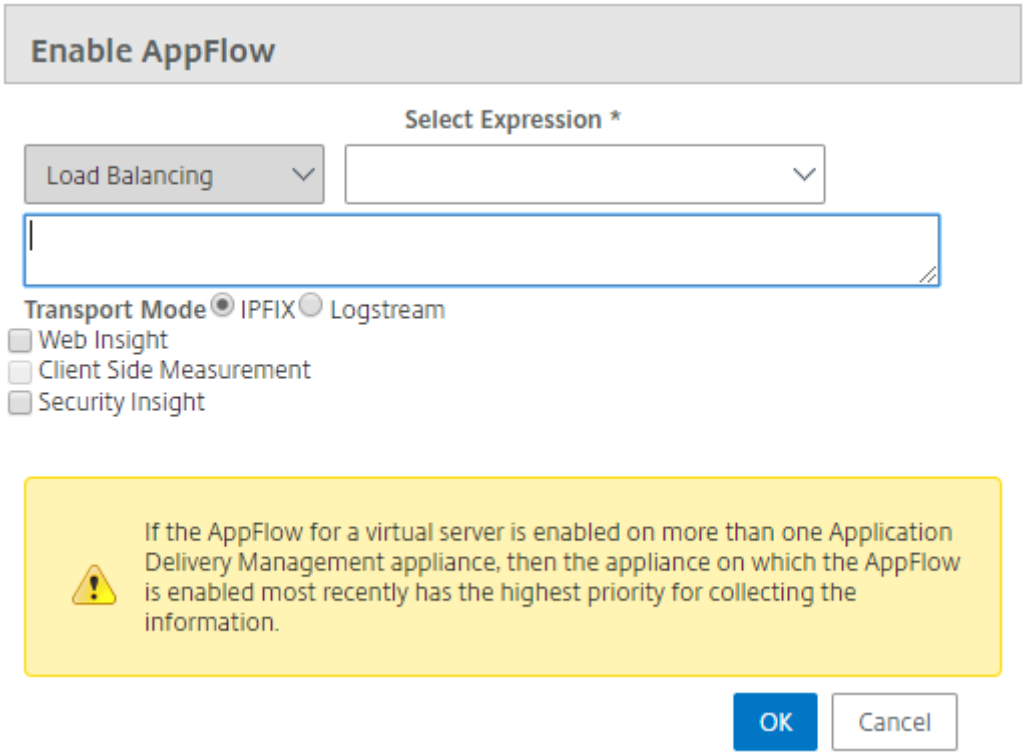
AppFlow 機能を有効にする

> 注
>
> AppFlow 機能は、Citrix ADM または各 Citrix ADC インスタンスから有効にできます。

NetScaler ADM から **AppFlow** 機能を有効にするには:

1. [ネットワーク] > [インスタンス] に移動し、分析を有効にする Citrix ADC インスタンスを選択します。

2. **[** アクションの選択] リストから、[**Analytics** の設定] を選択します。
3. 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、「ウェブインサイト」を選択します。
5. 各 Citrix ADC インスタンスで手順 3 から 6 を繰り返します。
6. [**OK**] をクリックします。



> 注
>
> 仮想サーバーの動作状態が［UP］以外の場合は、仮想サーバーでデータ収集を有効にできません。

NetScaler ADC GUI を使用して **AppFlow** 機能を有効にするには:

NetScaler ADC インスタンスの GUI で、［構成］>［システム］>［設定］の順に選択し、［高度な機能の構成］をクリックし、[**AppFlow**] を選択します。

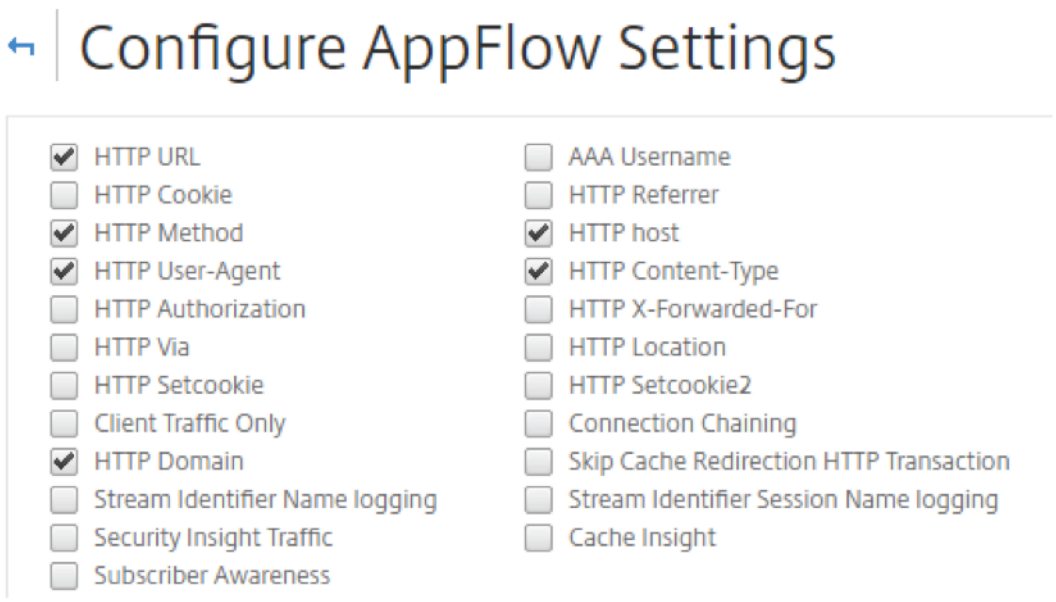
SSL インサイトパラメータの有効化

NetScaler ADC インスタンスごとに、一部の HTTP パラメーターを有効にして、NetScaler ADM で SSL Insight レコードを表示する必要があります。

Citrix ADC 構成ユーティリティから **SSL Insight** パラメーターを有効にするには:

1. 「構成」>「システム」>「**AppFlow**」に移動し、「**AppFlow** 設定の変更」をクリックします。

2. 「**HTTP** ドメイン」、「**HTTP** ホスト」、「**HTTP** メソッド」、「**HTTPURL**」、「**HTTP** ユーザーエージェント」、「**HTTP** コンテンツタイプ」のチェックボックスを選択します。
3. [**OK**] をクリックします。



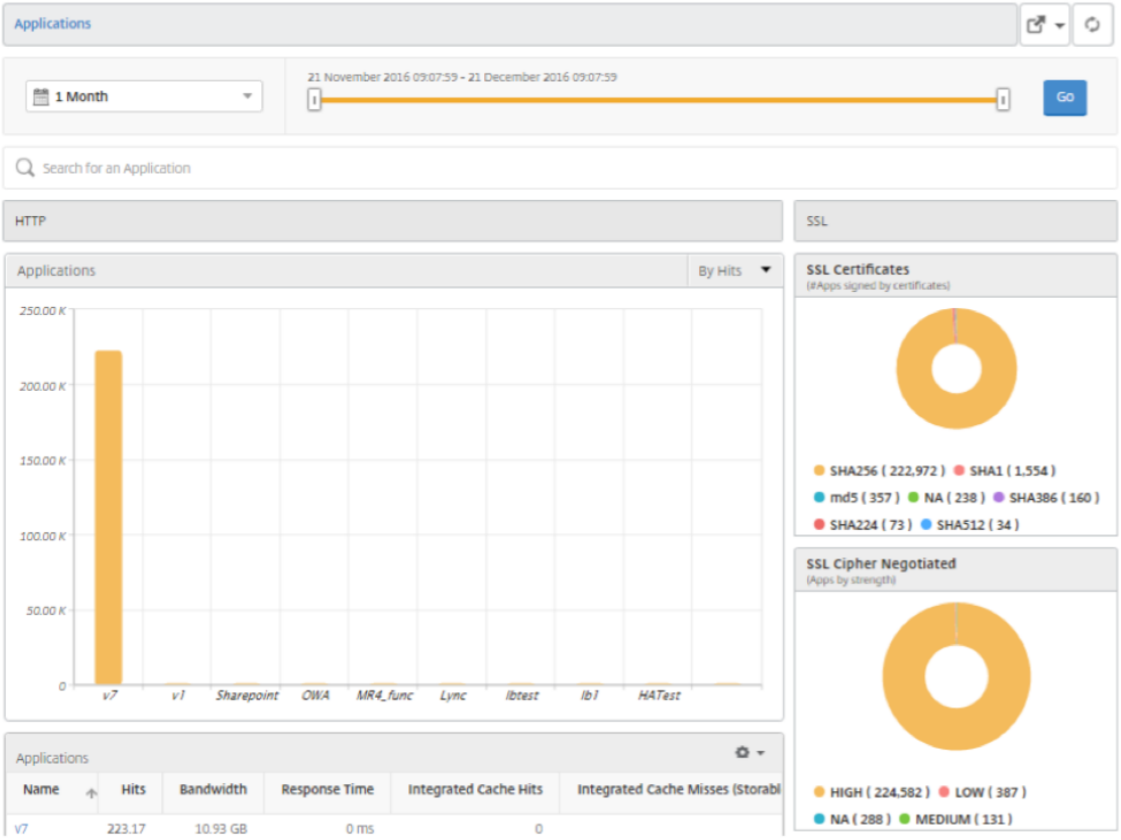
SSL Insight メトリックの表示

NetScaler ADM SSL Insight メトリックは、NetScaler ADC インスタンスが処理する SSL トランザクションのパフォーマンスを詳細に表示します。クライアント、サーバー、またはアプリケーションレベルの SSL Insight メトリック、および成功した SSL トランザクションおよび失敗した SSL トランザクションのメトリックを表示できます。これらのメトリックを使用して、Citrix ADC HTTPS 設定と SSL 証明書設定を分析して最適化し、パフォーマンスの問題を追跡できます。

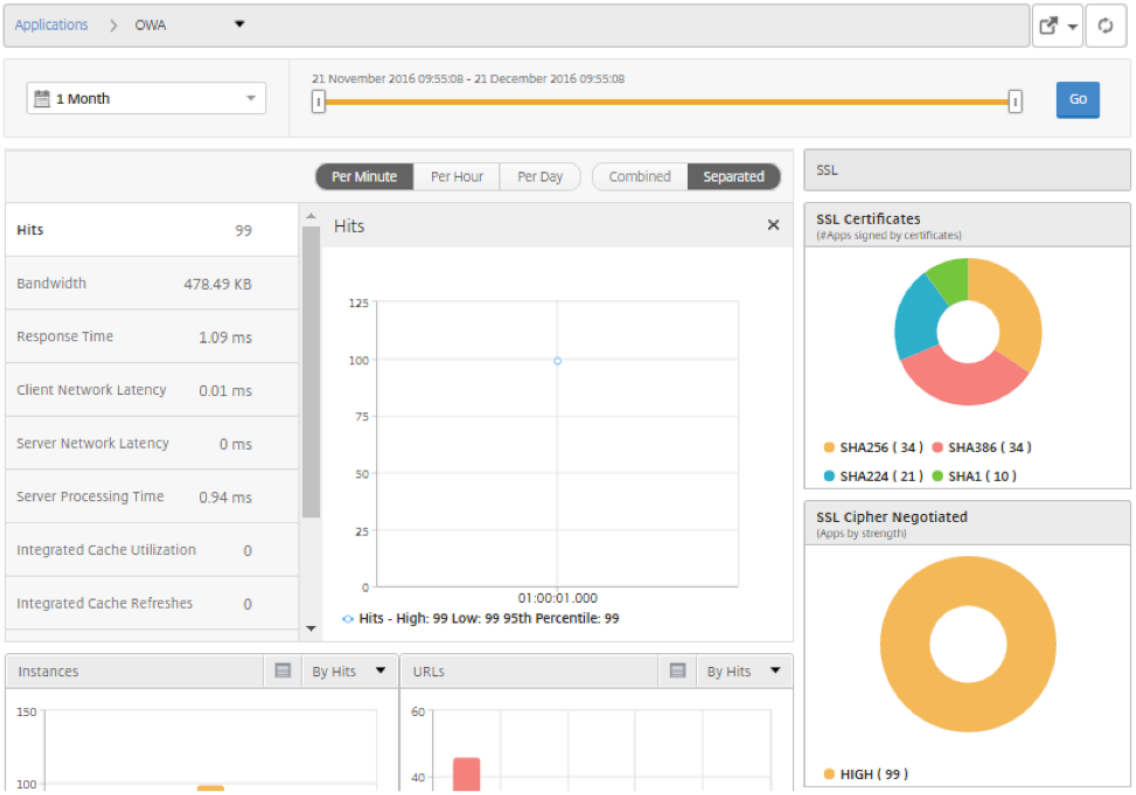
NetScaler ADM で **SSL Insight** メトリックスを監視するには:

1. 「分析」タブで「Web Insight」に移動し、「クライアント」、「サーバー」、または「アプリケーション」ノードをクリックすると、クライアント、サーバー、またはアプリケーションに関するメトリックがそれぞれ表示されます。
2. 左上のペインの期間リストから、指標を表示したい時間枠を選択します。期間は、スライダーを使用してカスタマイズできます。[**Go**] をクリックします。
3. SSL Insight のメトリックが円グラフとして表示されます。このグラフはクリックして詳細を確認できます。

> 注
>
> 円グラフには、すべてのアプリケーション、クライアント、またはサーバーのメトリックが表示されます。



4. 特定のアプリケーション、クライアント、またはサーバーの詳細を表示するには、棒グラフで対応する値をクリックします。



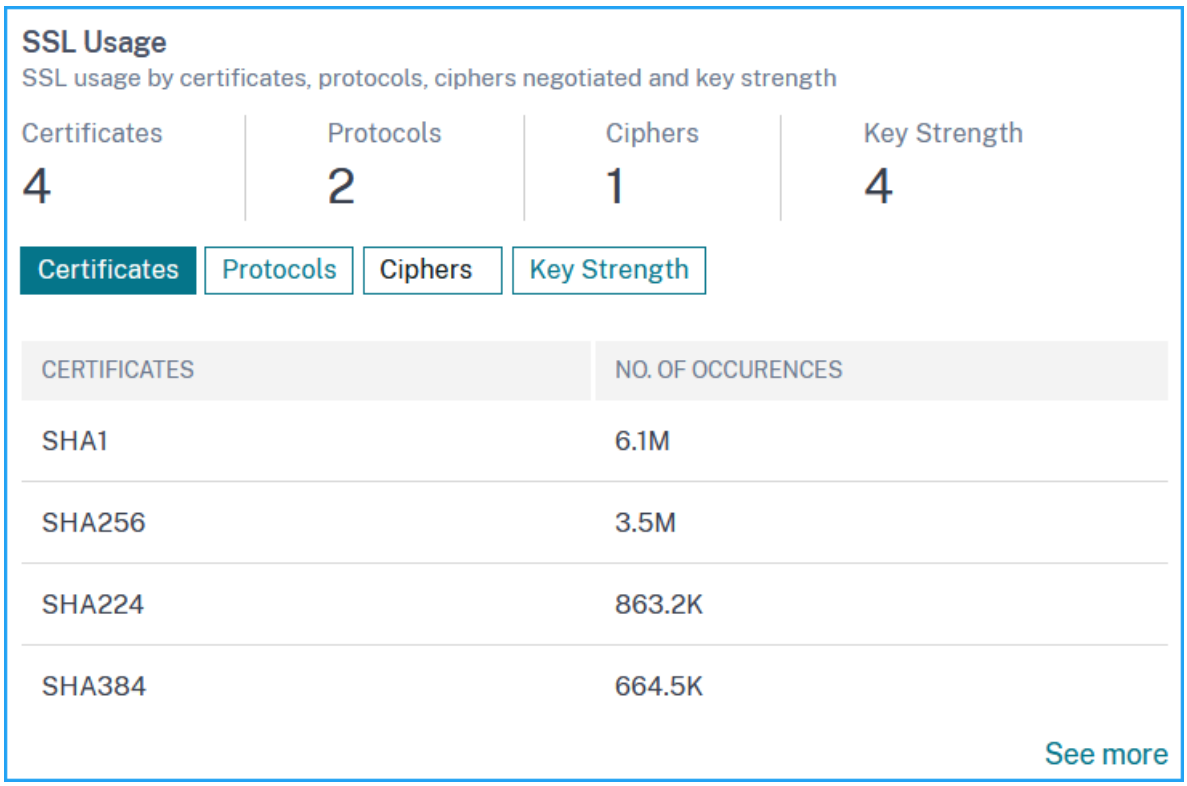
5. 失敗した SSL トランザクションを表示するには、［SSL］セクションのラジオボタンを選択します。

ユースケース**:** アプリケーション、クライアント、またはサーバーの **SSL** トランザクションの概要を把握する

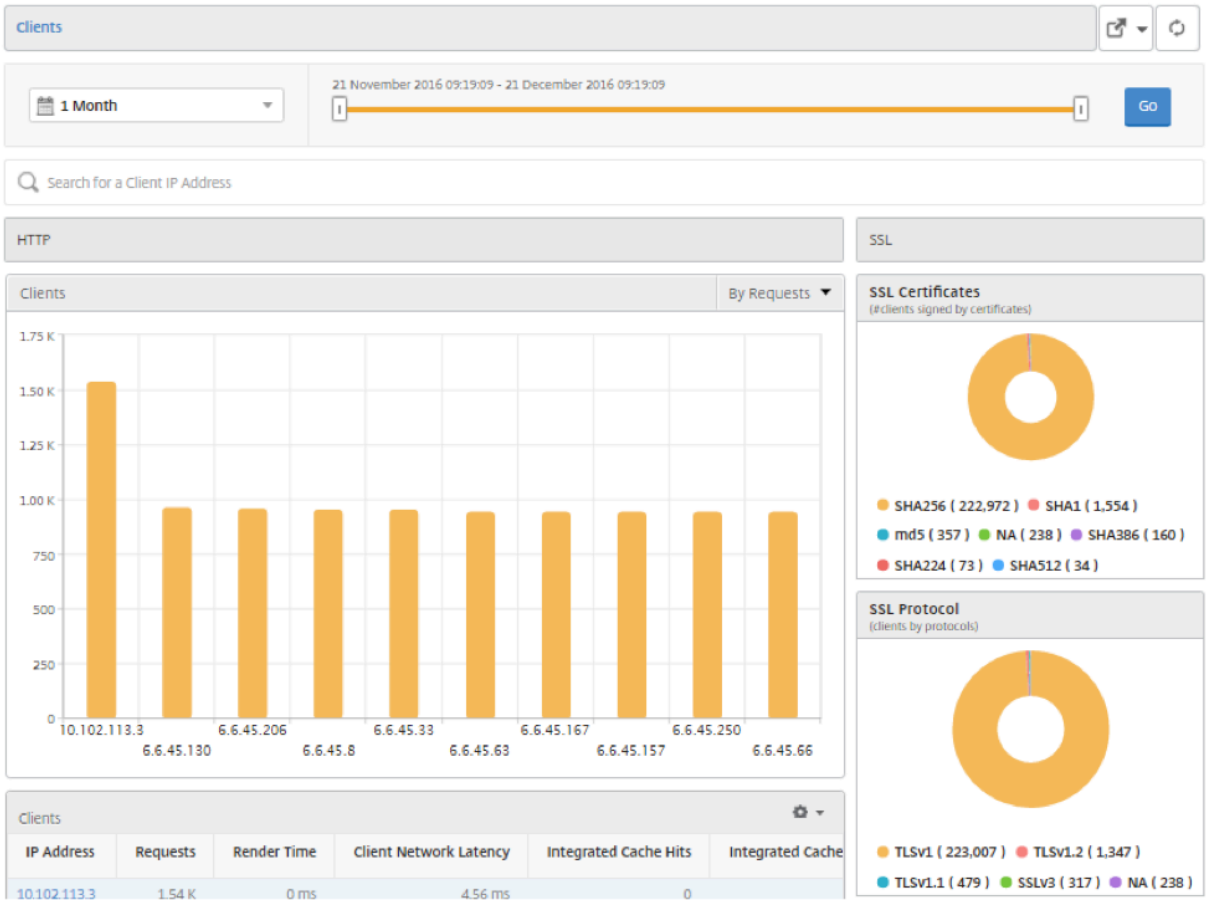
次のユースケースでは、Security Insight を使用して、アプリケーション、クライアント、およびサーバーのさまざまな SSL パラメーターの使用状況を評価し、セキュリティ対策を向上させる方法を説明します。

通信に SSL トランザクション（HTTPS）を使用している一連のアプリケーションがあり、SSL コンポーネントを監視するように NetScaler ADM を構成しているとします。最も注意が必要なアプリケーションに特に注意を払えるように、アプリケーションを頻繁に確認する必要があります。SSL インサイトダッシュボードには、選択した期間および選択した Citrix ADC デバイスについて、アプリケーションで使用されたさまざまな SSL パラメータの概要が表示されます。これには、次の種類のアカウントがあります:

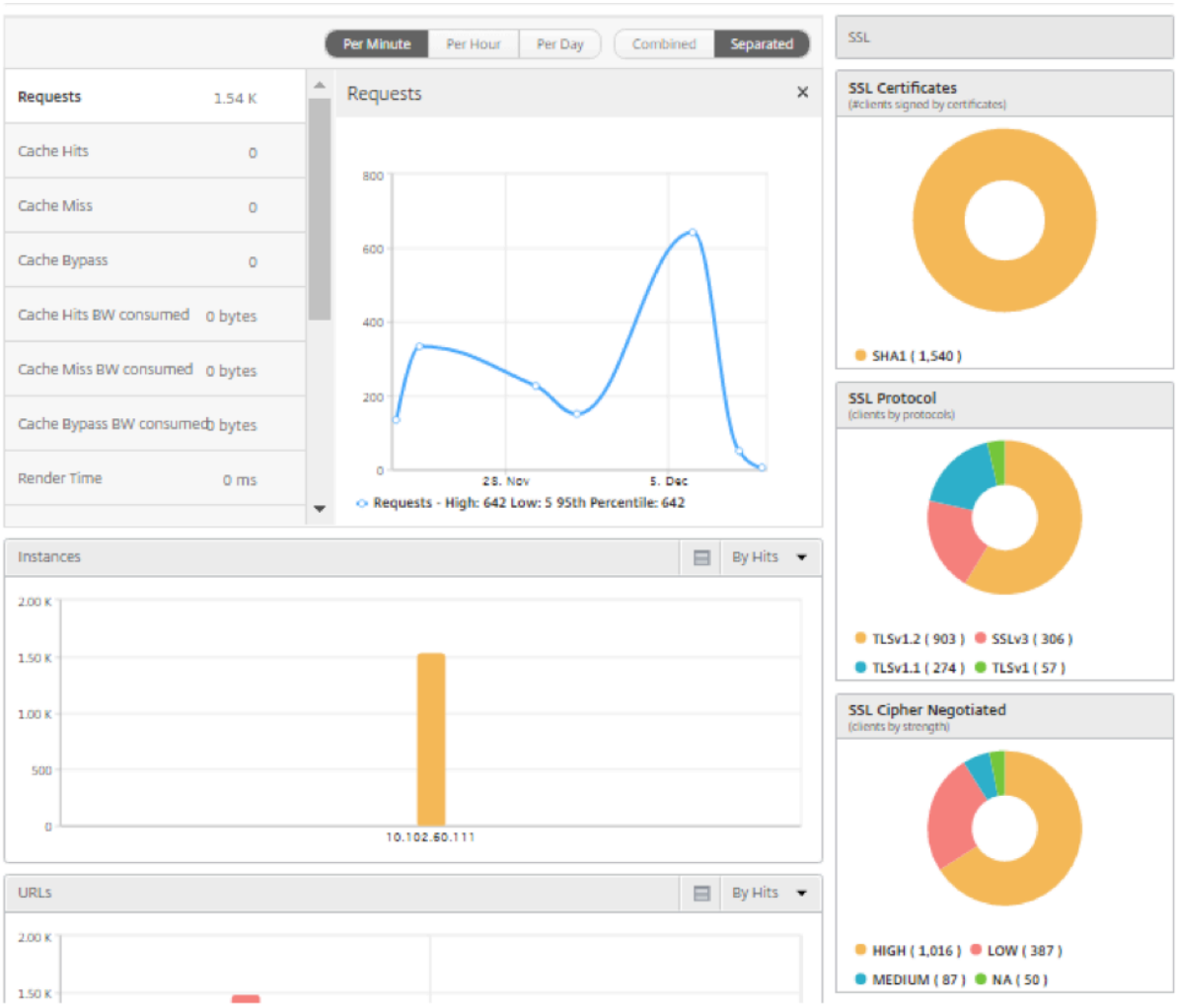
- SSL 証明書
- SSL プロトコル
- ネゴシエートされた SSL 暗号
- SSL キーの強度
- SSL 失敗 - フロントエンド
- SSL 失敗 - バックエンド



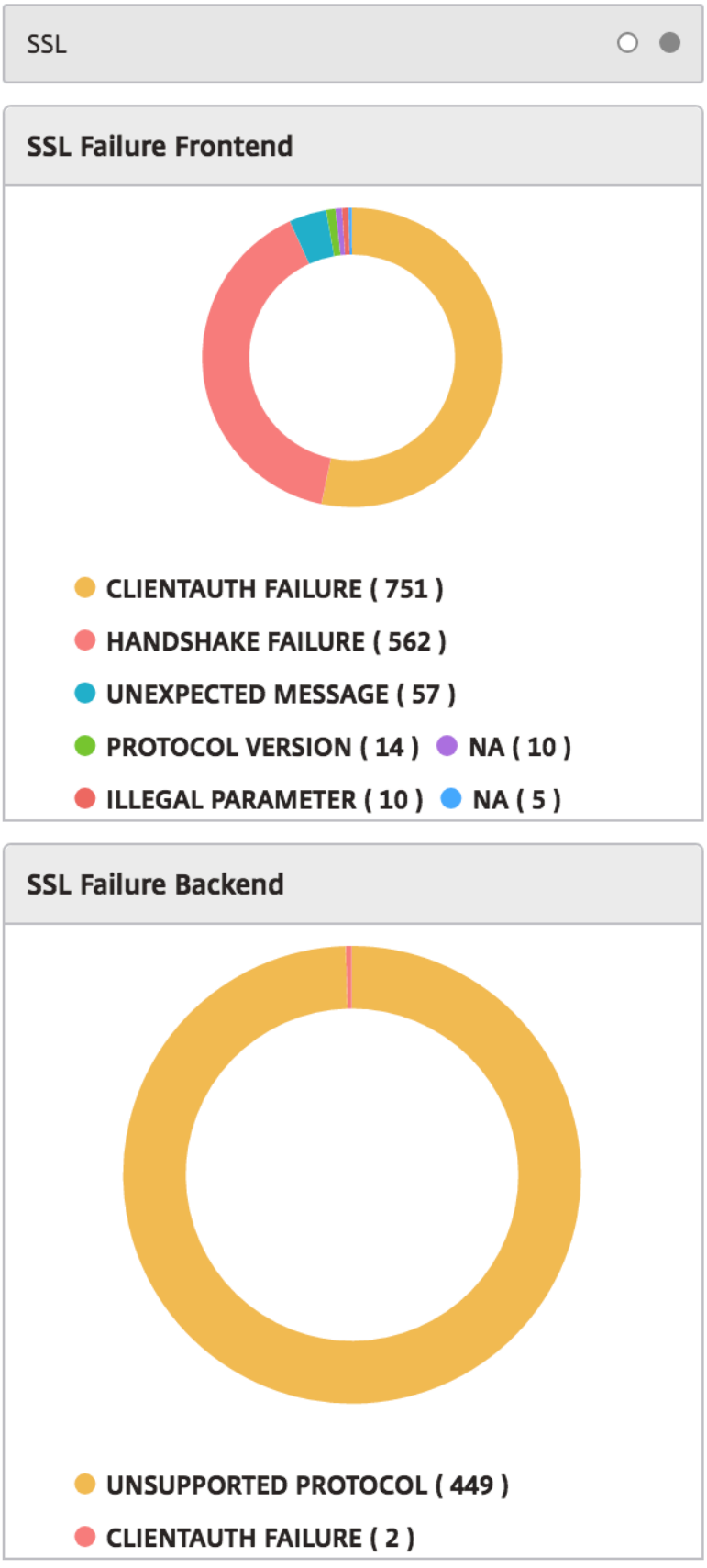
次の例では、クライアントの一覧（IP アドレスで識別）とクライアントごとの SSL ヒット数を確認できます。また、右側では、すべてのクライアントの SSL パラメーターを表示できます。



クライアントの SSL 詳細を表示するには、棒グラフまたはグラフの下の表でクライアントを選択します。次の例では、選択したクライアントのトランザクションで SHA1 SSL 証明書と 4 つの主要なプロトコル（TSLv1.2、TSLv1.1、TSLv1、SSLv3）が使用されています。さまざまな強度の暗号がネゴシエートされたことが分かります。色付けによって SSL プロトコルの強度が示されており、弱い暗号と強い暗号に関する情報が分かります。



同様に、失敗した **SSL** トランザクションに関する情報を表示するには、**[SSL]** セクションのオプションボタンを選択します。SSL フロントエンドとバックエンドの障害は、2 つの円グラフに別々に表示されます。次の例では、主要なバックエンド SSL エラーはハンドシェイク失敗であり、主要なフロントエンド SSL エラーは無効なパラメータであることを確認できます。



TCP Insight

February 6, 2024

Citrix Application Delivery Management（ADM）の TCP Insight 機能は、データ転送におけるネットワークの輻輳を回避するために Citrix ADC アプライアンスで使用される最適化手法と輻輳制御戦略（またはアルゴリズム）のメトリックを監視するための簡単でスケーラブルなソリューションを提供します。この機能では、TCP を最適化して、またはしないで TCP ファイルのダウンロードやアップロードのパフォーマンスを測定する「TCP スピードレポート」機能を使用します。

データボリューム、スループット、速度などの主要なトランスポート層メトリックを表示し、この情報を使用して Citrix ADC インスタンスが処理するトラフィック量を測定し、TCP Optimization の利点を検証できます。メトリックには、ストリーム方向（クライアントから Citrix ADC へ、および Citrix ADC からオリジンサーバーへ）、TCP ポート、および仮想 LAN ごとの内訳が表示されます。

前提条件

TCP Insight 機能の構成を開始する前に、以下の前提条件が満たされていることを確認してください。

- NetScaler ADC インスタンスは、ソフトウェアバージョン 11.1 ビルド 51.21 以降で実行されています。
- ソフトウェアバージョン 11.1 ビルド 51.21 以降で動作する NetScaler ADM がインストールされています。
- アプリケーション用に構成されているすべての仮想サーバーには、NetScaler ADM の管理と監視のライセンスが付与されます。
  NetScaler ADM ライセンスについて詳しくは、「ライセンス」を参照してください。

Citrix ADM のハードウェア要件:

コンポーネント	条件
RAM	8 GB
仮想 CPU	4 注: Citrix では、パフォーマンスを向上させるために 8 個の CPU を使用 することを推奨しています。
記憶域	120 GB 注: Citrix では、パフォーマンスを向上させるために 500 GB を使用 することをお勧めします。

TCP Insight の有効化

TCP Insight メトリックを表示する前に、NetScaler ADM でこの機能を有効にする必要があります。

TCP Insight を有効にするには:

1. 管理者の資格情報を使用して NetScaler ADM にログオンします。
2. [**Analytics**] > [設定] に移動し、[**Analytics** の機能を有効にする] をクリックします。
3. [**Analytics** の機能を有効にする] ページで、[**TCP Insight** を有効にする] を選択します。
4. 確認ウィンドウで、[**OK**] をクリックします。

Citrix ADM での **TCP** インサイトメトリクスの表示

NetScaler ADM で TCP Insight を有効にすると、トラフィックモード（インターネットまたはモバイルデータ)、データボリューム、スループット、インターフェイス、ポート、平均アップロード速度、平均ダウンロード速度などの主要なトランスポート層情報を表示できます。

NetScaler ADM で **TCP Insight** メトリックを表示するには:

[アナリティクス] > [**TCP** インサイト**]** に移動します。

棒グラフにマウスポインターを合わせると、対応するトランスポートテクニックのデータ量が表示されます。また、グラフの下の表にデータボリュームとその他のメトリックを表示できます。

> 注
>
> : 表の設定アイコンを使用して、グラフに表示される指標をカスタマイズできます。メトリックに関連する期間を選択したり、タイムスライダーを使用して期間を調整することもできます。

TCP Insight リストから選択して、インターフェイス、ポート、ビットレートなどのメトリックを表示することもできます。

使用例

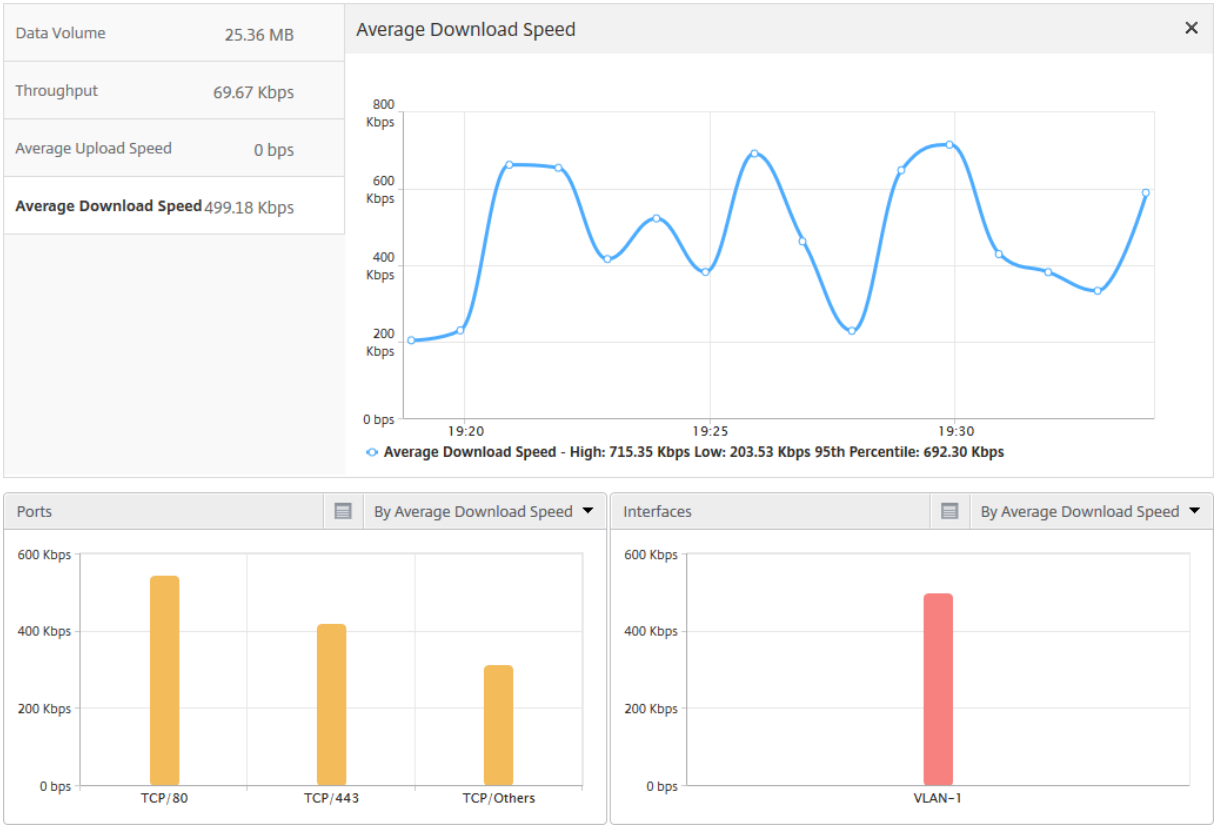
以下のユースケースは、NetScaler ADC アプライアンスで TCP Insight を使用する方法のいくつかを示しています。

- TCP 最適化のメリットを評価
- TCP パラメータの調整
- トラフィック量に対する TCP 最適化の影響を測定

TCP 最適化のメリットを評価

NetScaler ADC TCP 最適化は、モバイル（無線）または企業ネットワーク（インターネット）に実際にどの程度のメリットがありますか。TCP 経由で発生するデータ転送の速度を表示して、最適化されていないパフォーマンスと最適化されたパフォーマンスを比較できます。これらの測定は、ダウンロード方向とアップロード方向（常に無線/クライアント側から）や異なる宛先ポート（HTTP (80) と HTTPS (443)）で個別に表示されます。
TCP インサイトメトリクスを調べることで、TCP フローを最適化することで得られる速度の向上を定量化できます。

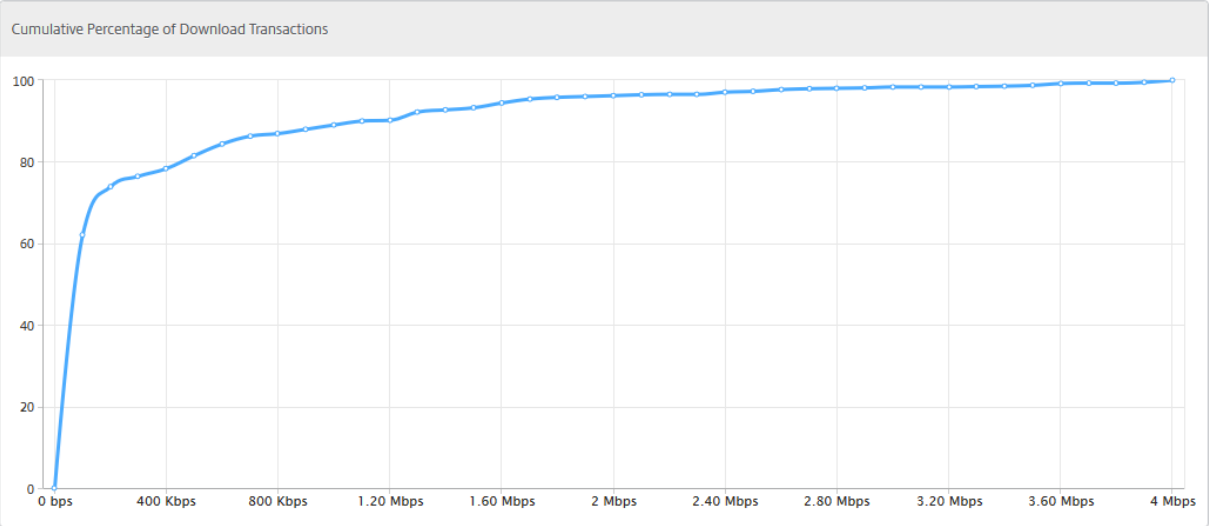
これらのパラメーターの概要を表示するには、NetScaler ADM にログオンし、[**TCP Insight**] タブをクリックします。次に、[側面] をクリックし、棒グラフまたはグラフの下の表から [インターネット] または [ラジオ] を選択します。



TCP パラメータの調整

異なる TCP プロファイルを使用すると、同じトラフィックから異なる出力が生成されます。このような状況では、NetScaler ADC がさまざまな TCP 最適化プロファイルを実行している期間の速度測定値を表示して比較したい場合があります。それらの結果を利用して、転送速度が上がるように TCP パラメーターを調整したり、特定のお客様のネットワークでのユーザー体験を最大限に高める TCP プロファイルを作成したりできます。

レポートを表示するには、NetScaler ADM にログオンします。次に、[**TCP Insight**] タブで [**Bit**rate] をクリックし、棒グラフまたはグラフの下のテーブルから目的のビットレートを選択します。

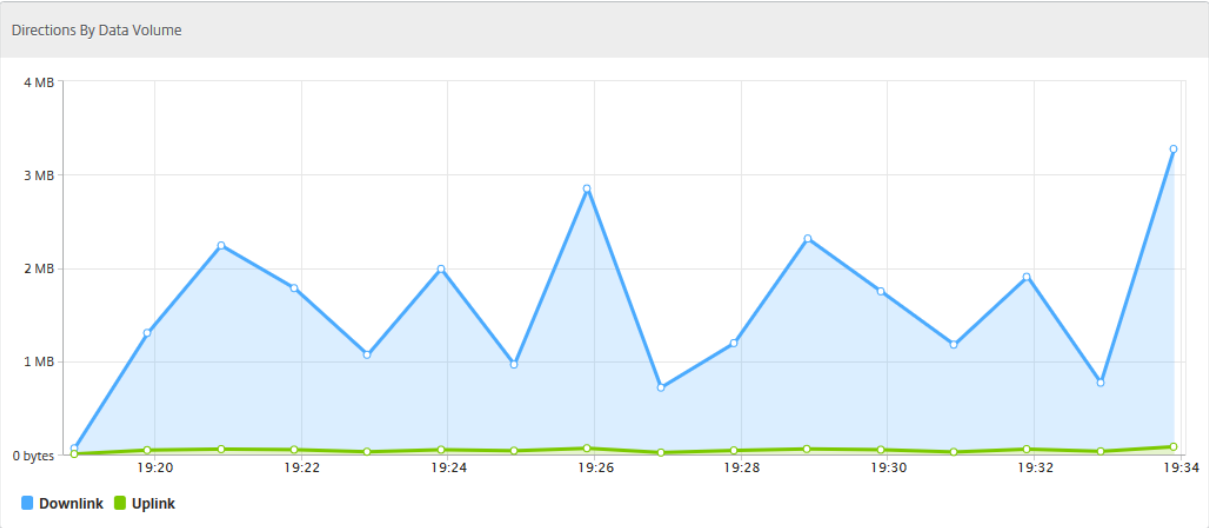


トラフィック量に対する **TCP** 最適化の影響を測定

NetScaler ADC インスタンスが処理する IP 層のデータ量/スループットの測定値をさまざまな期間で比較して、TCP 最適化が加入者のデータ消費に及ぼす影響を評価できます。測定は、ネットワークの各サイド（無線サイドとインターネットサイド）、さまざまなトラフィックセグメント（さまざまなインターフェイスや VLAN によって線引き）、各方向（ダウンリンクとアップリンク）、さまざまな宛先ポート（HTTP と HTTPS）に個別に適用できます。この比較を利用して、TCP 最適化によりサブスクライバーのデータ消費が促進されていることを確認できます。

測定値の概要を確認するには、NetScaler ADM にログオンし、「**TCP Insight** 」タブの「サイド」をクリックし、棒グラフまたはグラフの下の表から「インターネット」または「ラジオ」を選択します。

タイムリストから別の時間枠を選択することもできます。期間は、スライダーを使用してカスタマイズできます。

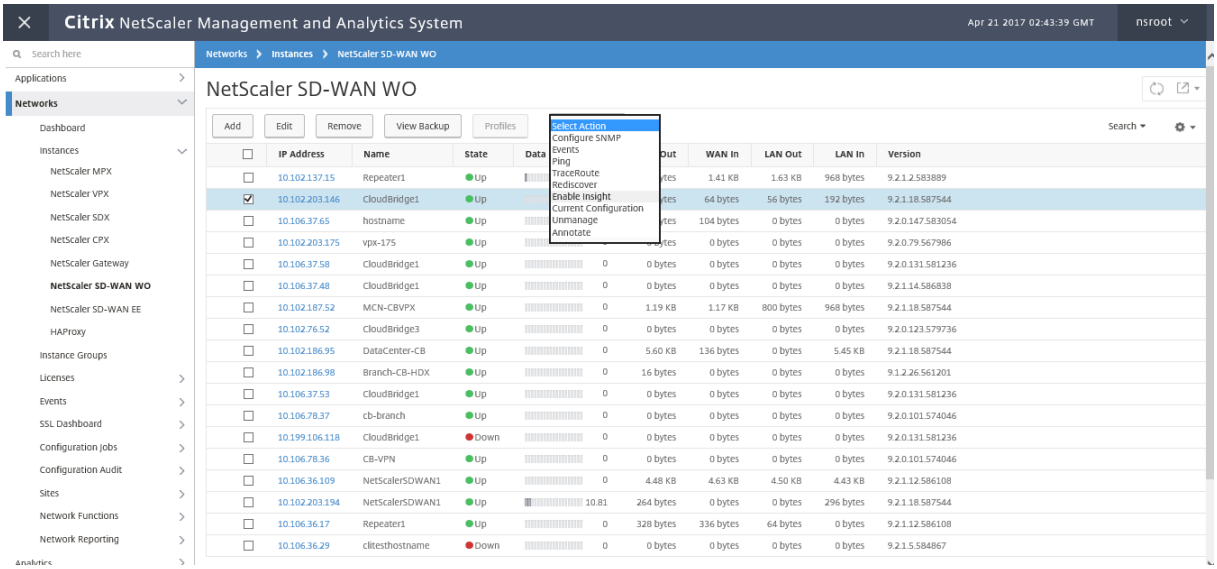


WAN Insight

February 6, 2024

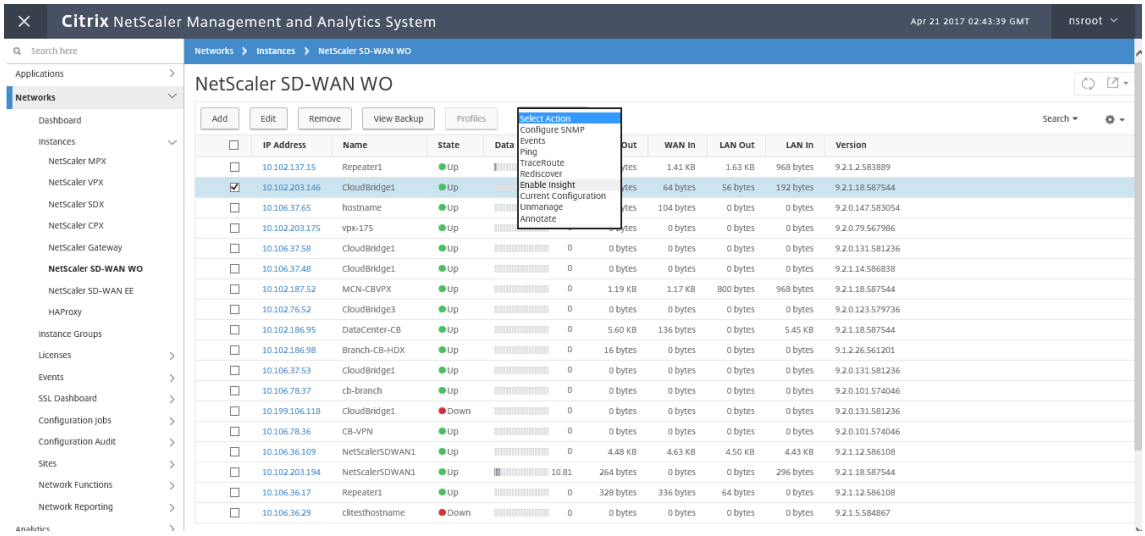
Citrix SD-WAN WAN 最適化（WO）アプライアンスは、データセンターとブランチサイト間のネットワーク全体のデータフローの効率を向上させることにより、WAN を介した多数のアプリケーションの配信を最適化します。WAN Insight の分析機能を使用すると、管理者はデータセンターと Branch WAN 最適化アプライアンス間を流れる高速および非高速の WAN トラフィックを容易に監視できます。WAN Insight では、ネットワーク上のクライアント、アプリケーション、ブランチの状態を把握し、ネットワーク問題を効果的にトラブルシューティングできます。利用できる場合には、ライブレポートおよび履歴レポートを使用して事前に問題に対処することもできます。

データセンター WAN 最適化アプライアンスで分析を有効にすると、NetScaler Application Delivery Management（ADM）がデータを収集し、データセンターとブランチ WAN 最適化アプライアンスのレポートと統計を提供できるようになります。



WAN 最適化アプライアンス上で分析を有効にするには:

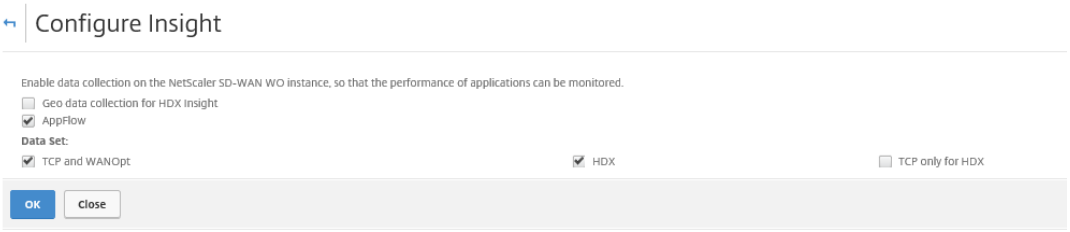
1. Web ブラウザで、Citrix ADM の IP アドレス（たとえば 、http://192.168.100.1）を入力します。
2.「ユーザー名 」フィールドと 「パスワード」フィールドに、管理者の資格情報を入力します。
3. [ネットワーク] > [インスタンス] > [**Citrix SD-WAN**] に移動し、SD-WAN WO インスタンスを選択します。



4. 「アクション を選択」ドロップダウンから、「アナリティクスの設定」を選択 します。
5. 必要に応じて以下のパラメーターを選択します。

   - **HDX Insight** の地理データ収集：クライアントの IP アドレスを Google Geo API と共有します。
   - **AppFlow**: WAN 最適化インスタンスからのデータ収集を開始します。

     - **TCP** および **WANopt**: TCP および WANopt インサイトレポートを提供します。
     - **HDX**: HDX Insight レポートを提供します。
     - **HDX** 用の TCP のみ:HDXInsight レポートにのみ TCP を提供します。



6. [**OK]** をクリックします。

WAN インサイトレポートを表示するには、次の手順を実行します。

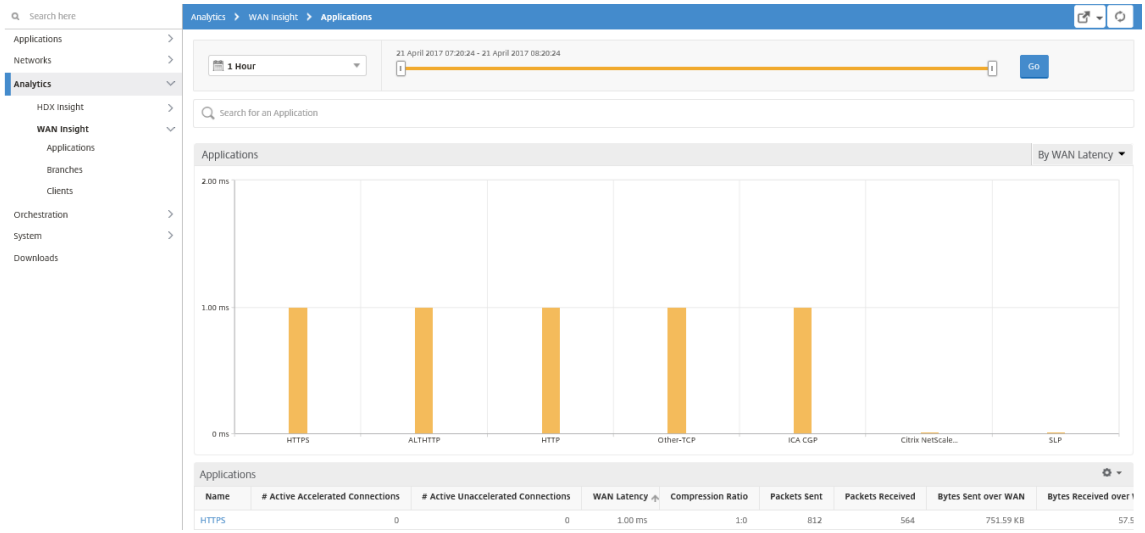
1. Web ブラウザで、Citrix ADM の IP アドレス（たとえば 、http://192.168.100.1）を入力します。
2. 「ユーザー名 」フィールドと「パスワード」フィールドに、管理者の資格情報を入力します。
3. [**Analytics**] > [**WAN Insight**] に移動します。

> 注
>
> WAN インサイトオプションは、SD-WAN WO インスタンスを NetScaler ADM に追加した後にのみ表

> 示されます。

次のレポートを表示できます。

- アプリケーション -選択した期間のすべてのアプリケーションの使用状況とパフォーマンスの統計を表示します。
- ブランチ -すべての WAN 最適化ブランチアプライアンスの使用状況とパフォーマンスの統計を表示します。
- **Clients** -各ブランチで、WAN 最適化アプライアンスにアクセスするすべてのクライアントの使用状況とパフォーマンスの統計情報を表示します。



次のメトリックが表示されます。

測定基準	説明
Active Accelerated Connections	アクセラレーションが有効なアクティブ WAN 接続の数です。
Active Unaccelerated Connections	アクセラレーションが無効なアクティブ WAN 接続の数です。
WAN 遅延	アプリケーションとの対話中にユーザーに生じる遅延（ミリ秒単位）です。
圧縮率	選択した期間におけるブランチオフィスアプライアンスとデータセンターアプライアンス間のデータ圧縮率です。
送信済みパケット	選択した期間に WAN 最適化アプライアンスからネットワーク経由で送信されたパケットの数です。
受信済みパケット	選択した期間に WAN 最適化アプライアンスがネットワークから受信したパケットの数です。
WAN で送信されたバイト数	選択した期間に Citrix WAN 最適化アプライアンスが WAN 経由で送信したバイト数。

測定基準	説明
WAN で受信したバイト数	選択した期間に WAN 最適化アプライアンスが WAN から受信したバイトの数です。
LAN RTO	選択した期間に WAN 最適化アプライアンスから LAN への再送信がタイムアウトになった回数です。
WAN RTO	選択した期間に WAN 最適化アプライアンスから WAN への再送信がタイムアウトになった回数です。
再送信パケット (LAN)	選択した期間に WAN 最適化アプライアンスから LAN ネットワークに再送信されたパケットの数です。
再送信パケット (WAN)	選択した期間に WAN 最適化アプライアンスから WAN ネットワークに再送信されたパケットの数です。

Video Insight

February 6, 2024

ビデオインサイト機能は、NetScaler ADC アプライアンスで使用されるビデオ最適化技術のメトリックを監視するための簡単でスケーラブルなソリューションを提供し、カスタマーエクスペリエンスと運用効率を向上させます。次のようなメリットがあります。

- ピーク時間における混雑時にネットワークを管理する。
- 動画再生の一貫性を向上させ動画の再生速度低下を抑える。
- 新しい動画サービスオファリング（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 ADC アプライアンスは、ビデオトラフィックを最適化する際に、ビデオビットレートを動的にペースさせる特別なメカニズムと、ランダムサンプリング手法を使用して、最適化手法による節約額を推定します。NetScaler ADC ビデオ最適化機能について詳しくは、「ビデオの最適化」を参照してください。NetScaler ADC アプライアンスを NetScaler Application Delivery Management（ADM）と統合すると、NetScaler ADC アプライアンスを流れるビデオデータから重要な情報が収集されます。この情報を使用することで、最適化している場合としていない場合の ABR 動画トラフィックのパフォーマンスを比較したり、最適化による削減率を求めたりすることができます。

> 注
>
> NetScaler ADM で提供される最適化されていないセッションの統計情報は、NetScaler ADC アプライアンスでランダムサンプリングで選択したセッションに対応します。ランダムサンプリングの詳細については、「ビデ

> オの最適化」を参照してください。

NetScaler ADM Video Insight は、次の種類のビデオトラフィックに関するメトリックを提供します。

- HTTP 経由でのプログレッシブダウンロード（PD）動画
- HTTP 経由の ABR 動画
- HTTPS 経由の ABR 動画
- QUIC 経由の YouTube ABR 動画

Video Insight の構成

> 注
>
> ビデオインサイトは、NetScaler ADC プレミアムライセンスを持つ NetScaler ADC インスタンスでサポートされます。NetScaler ADC Premium ライセンスは、NetScaler ADC Telco プラットフォーム（VPX T1000 および VPX-T）でサポートされています。

Citrix ADC インスタンスでビデオインサイトを構成するには、まず AppFlow 機能を有効にし、AppFlow コレクター、アクション、およびポリシーを構成して、ポリシーをグローバルにバインドします。コレクターを構成するときは、レポートを監視する Citrix ADM サーバーの IP アドレスを指定する必要があります。

NetScaler ADC インスタンスでビデオインサイトを構成するには、次のコマンドを実行して AppFlow プロファイルとポリシーを構成し、AppFlow ポリシーをグローバルにバインドします。

add appflow collector \< 名前\> **-IPAddress** \<IP アドレス\> **-port** < ポート番号 > **-Transport** logstream ポート番号 >

set appflow param -**videoInsight** ENABLED

add appflow action \< 名前\> **-collectors** \< 文字列\> **-videoAnalytics** ENABLED

add appflow policy \< 名前\> \< 規則\> \< アクション\>

bind appflow global \< ポリシー名\> \< 優先度\> \[\<goto 優先度式\>\] \[**-type** \< タイプ\>\]

enable ns mode ulfd

機能アプリフローを有効にする

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
```



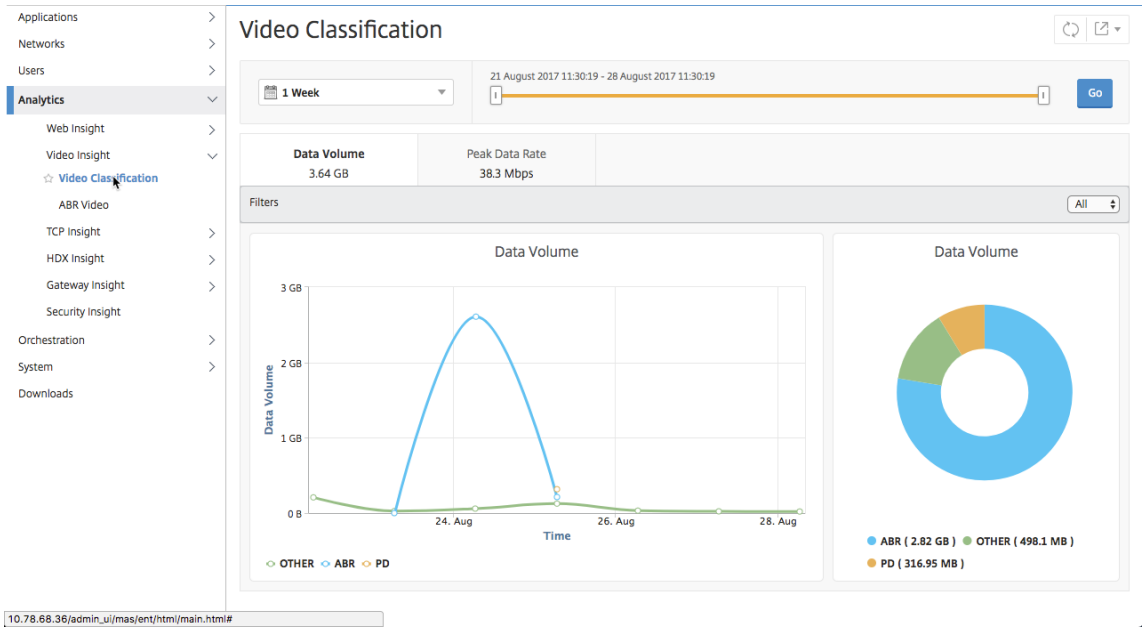
```
bind appflow global appol 1
enable ns mode ulfd
enable feature appflow
<!--NeedCopy-->
```

NetScaler ADM での **Video Insight** メトリックの表示

NetScaler ADM で Video Insight を有効にすると、ビデオの分類、データボリューム、ピークデータレート、ABR ビデオの再生などのビデオの最適化指標を表示できます。これらのメトリックにより、ネットワークを分析して動画を最適化し、サブスクライバーのエクスペリエンス、操作の効率、その他のパフォーマンス基準を改善することができます。

Citrix ADM でビデオインサイトメトリックを表示するには:

1. Web ブラウザで、Citrix ADM 仮想アプライアンスの IP アドレス（たとえば、http://192.168.100.1）を入力します。
2. [**User Name**] と [**Password**] に管理者の資格情報を入力します。
3. [**Analytics] > [Video Insight**] に移動します。



> 注
>
> グラフの凡例 **OTHER** によって提供される値は、選択したフィルタに応じて、ビデオトラフィックの非 ABR および PD 以外のデータを表します。
>
> - **All**： ビデオトラフィック内の非 ABR（HTTP、HTTPS、および QUIC）および非 PD（HTTP）データの合計。
> - **HTTP** —ビデオトラフィックの非 ABR データと非 PD データの合計。

- **HTTPS** —ビデオトラフィックの非 ABR ビデオデータの合計。
- **QUIC** —ビデオトラフィックの非 ABR ビデオデータの合計。

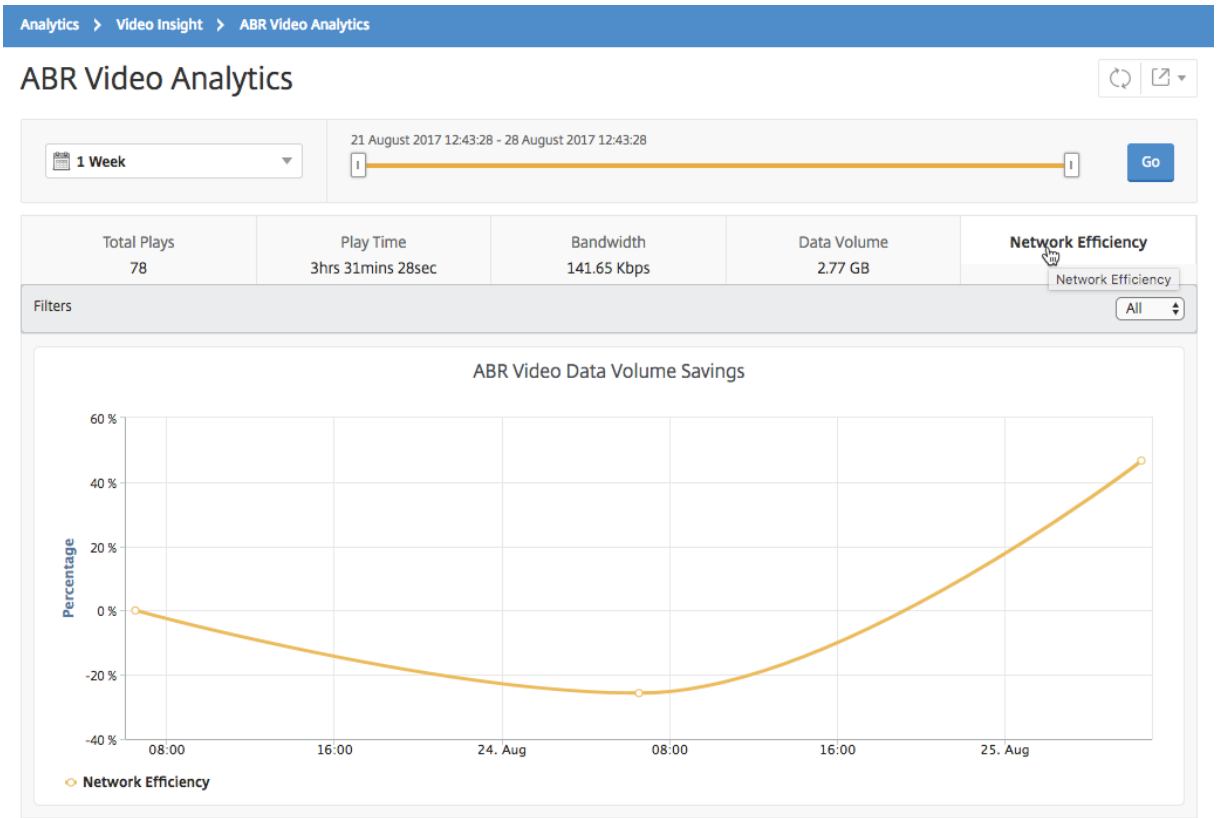
ネットワーク効率の表示

February 6, 2024

特定の時間枠について、Citrix Application Delivery Management（ADM）は、その時間枠における最適化されたビデオセッションと最適化されていないビデオセッションの比率を示すグラフを提供します。グラフには、最適化により削減された帯域幅の割合も表示されます。削減された帯域幅の割合は、次の式により計算されます。

保存帯域幅の割合 = 最適化された **ABR** ビデオデータボリュームの平均/最適化されていない **ABR** ビデオデータボリュームの平均。

最適化によって節約された帯域幅の割合を確認するには、Citrix ADM にログオンし、［分析］**>**［ビデオインサイト］に移動して、［**ABR** ビデオ］をクリックします。次に、右側のペインで、ボックスの一覧から期間を選択します。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。[**Go**] をクリックし、[ネットワーク効率] タブを選択します。



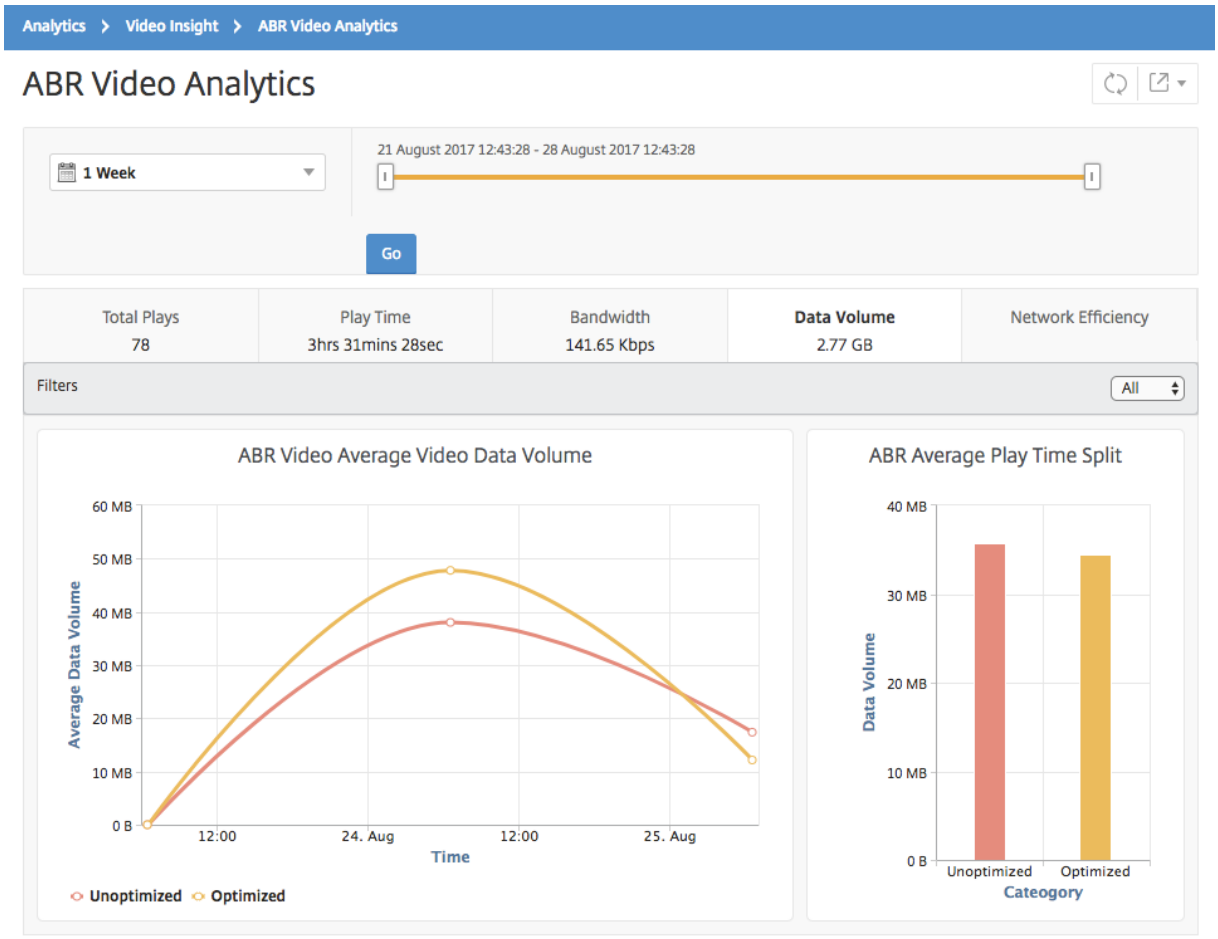
最適化された **ABR** ビデオと最適化されていない **ABR** ビデオで使用されるデータ量を比較する

February 6, 2024

Citrix Application Delivery Management（ADM）には、特定の期間に、最適化された ABR ビデオと最適化されていない ABR ビデオが使用したデータ量が表示されるため、2 つのボリュームを比較できます。

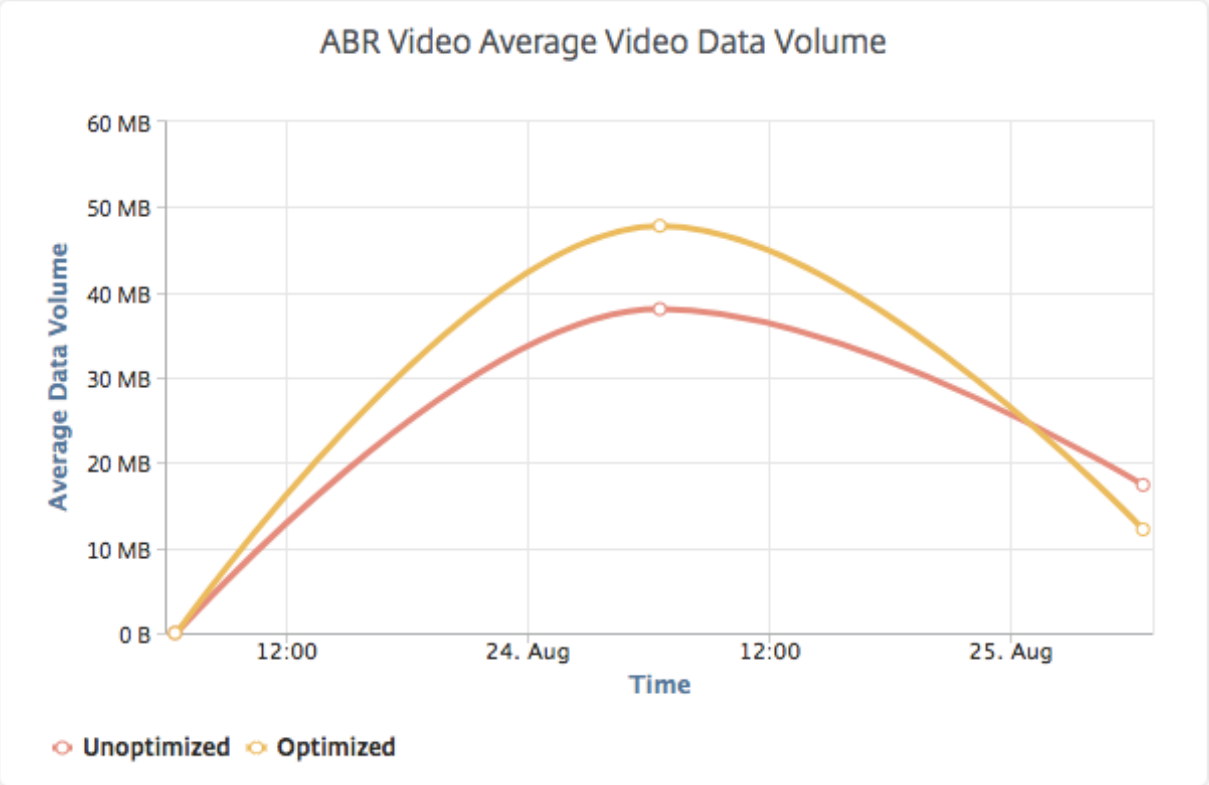
ABR ビデオで使用されているデータ量を確認するには、Citrix ADM にログオンし、［分析］**>**［ビデオインサイト］に移動して、［ABR ビデオ］をクリックします。次に、右側のペインで、ボックスの一覧から期間を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。「実行」をクリックし、「データボリューム」タブを選択します。

フィルタードロップダウンリストを使用して、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。



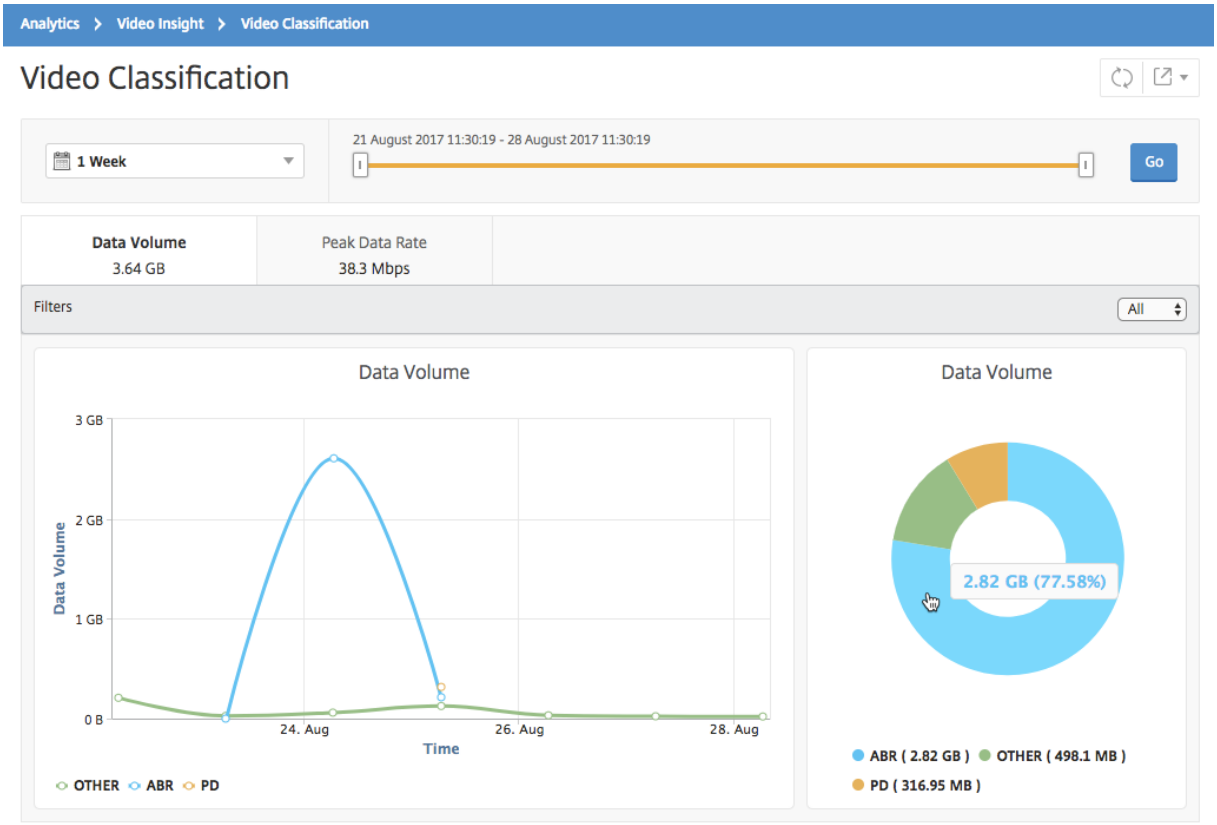
ストリーミングされる動画の種類とネットワークから消費されるデータ量の表示

February 6, 2024

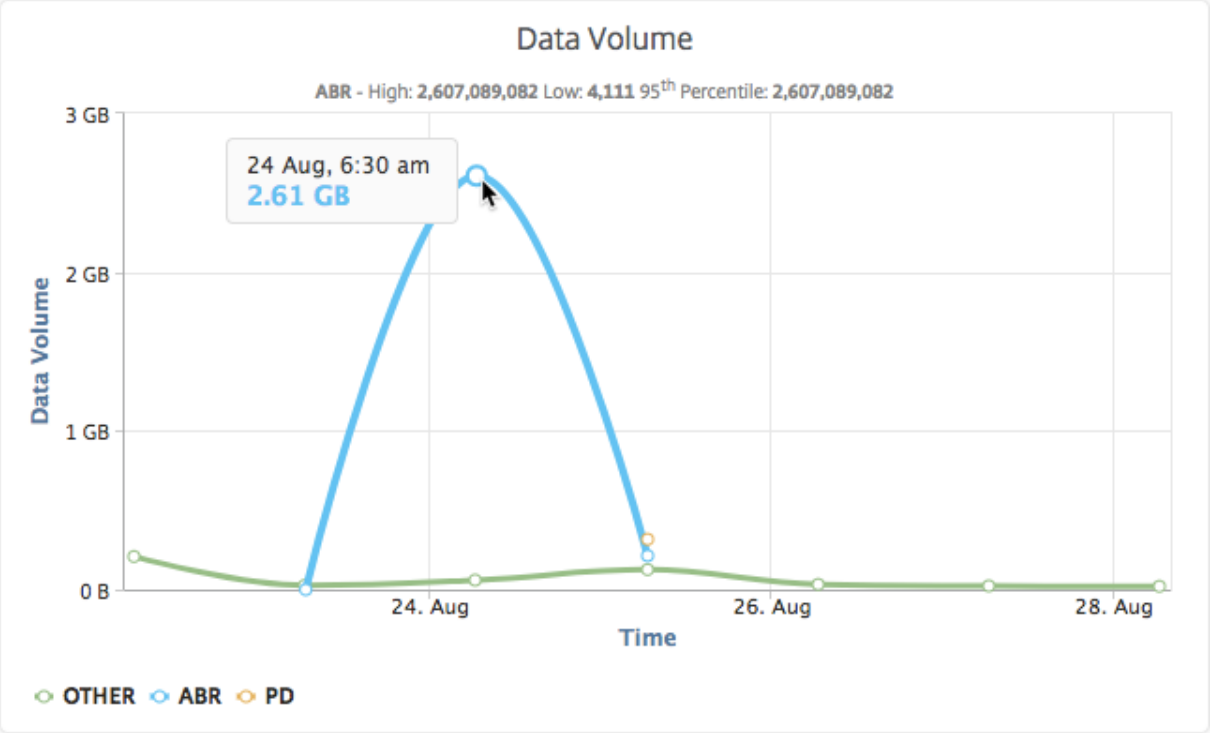
NetScaler ADC アプライアンスは、ネットワーク内の暗号化または暗号化されていないビデオトラフィック、およびビデオストリーミングの種類（PD または ABR）を検出します。NetScaler Application Delivery Management（ADM）では、これらのメトリックと、定義された期間内にビデオトラフィックによって消費されるデータ量が表示されます。

ビデオの種類と消費されたデータ量を確認するには、Citrix ADM にログオンし、[分析] **> [**ビデオインサイト**]** に移動して、**[** ビデオ分類] をクリックします。次に、右側のペインで、ボックスの一覧から期間を選択します。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。[**Go**] をクリックします。

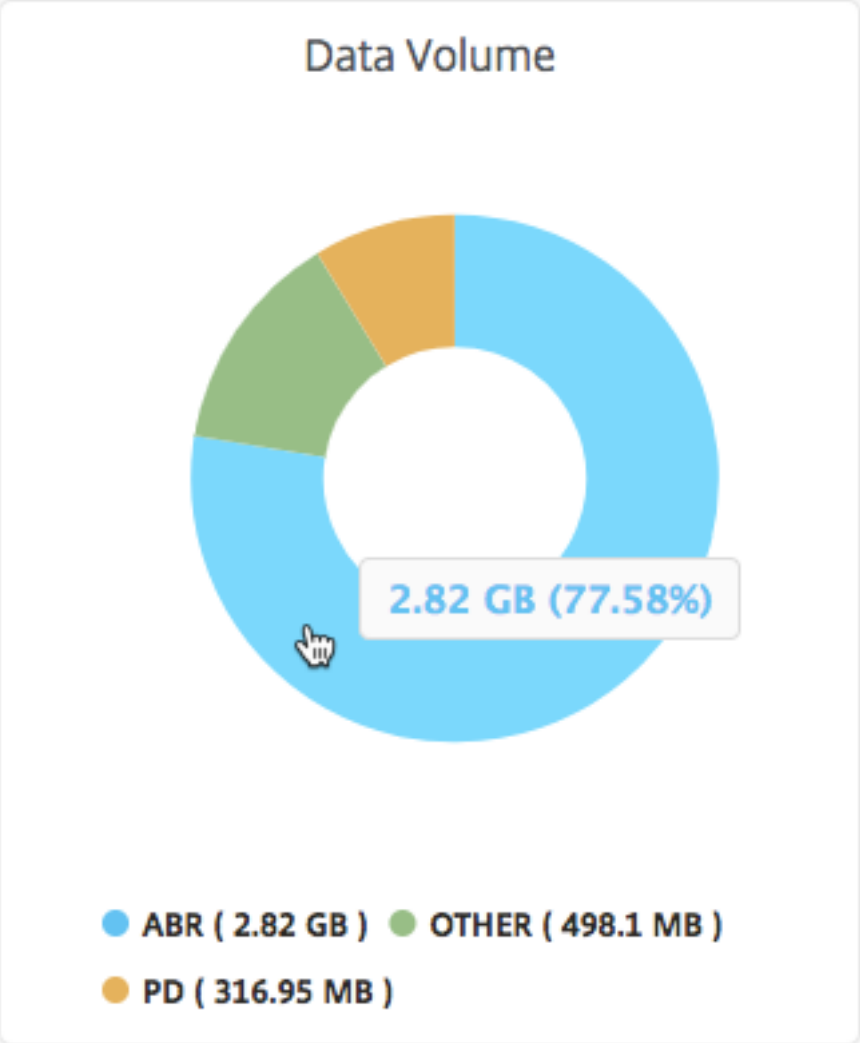
フィルタードロップダウンリストを使用して、HTTP、HTTPS、 または QUIC トラフィックを選択できます。



[**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。



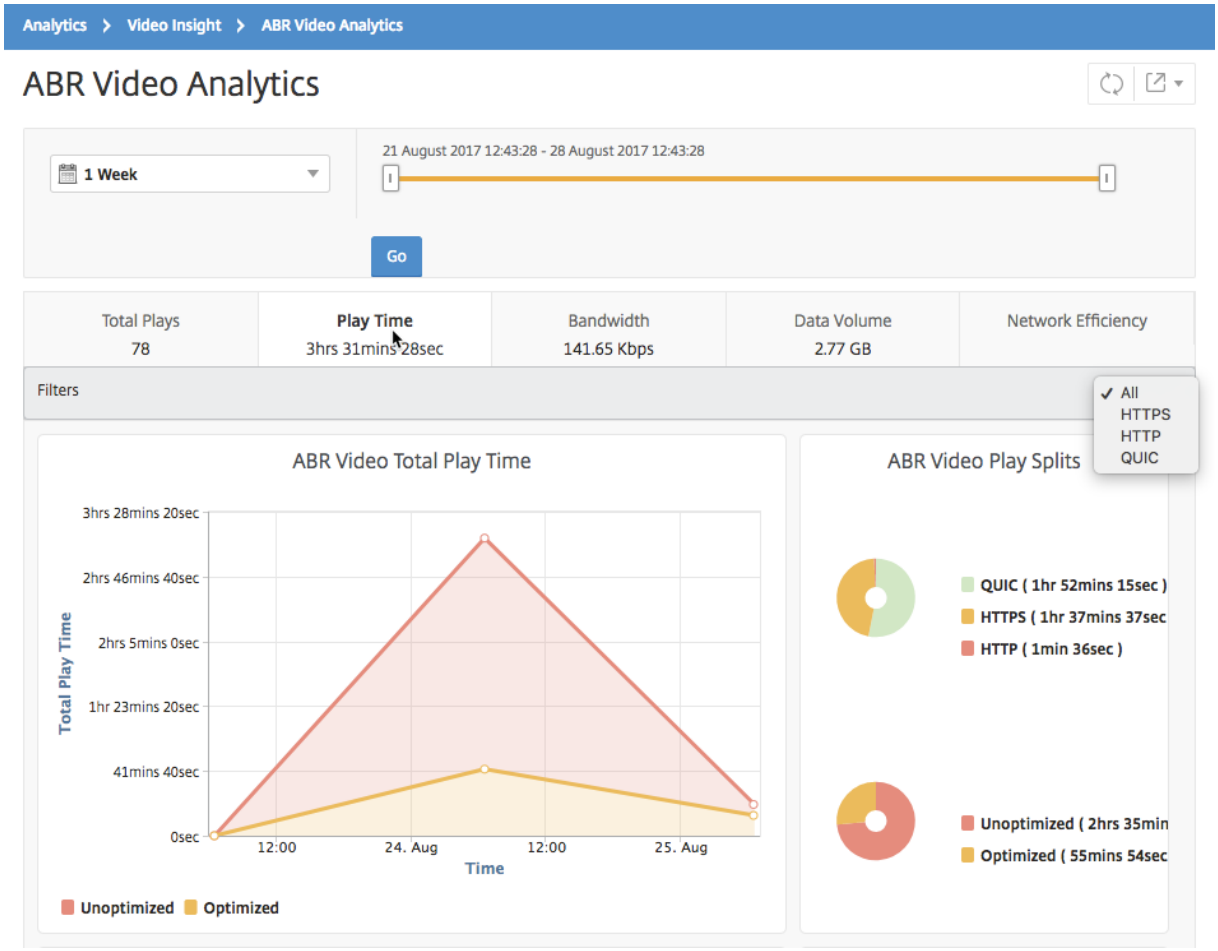
ABR ビデオの最適化と非最適化の再生時間を比較する

February 6, 2024

Citrix Application Delivery Management（ADM）は、特定の期間における ABR ビデオの再生時間を表示し、ネットワーク内の最適化された ABR ビデオと最適化されていない ABR ビデオの再生時間を比較することもできます。

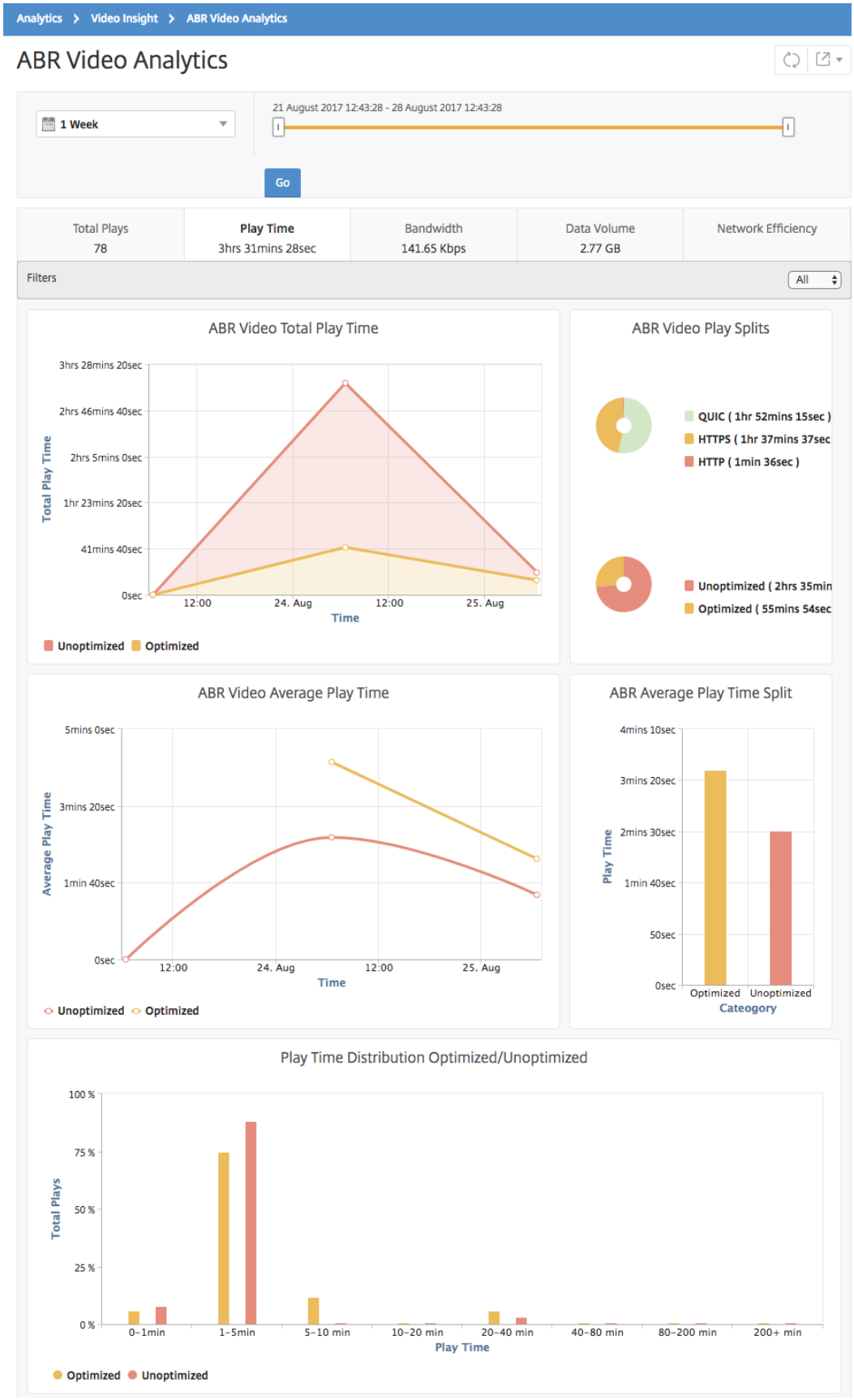
再生時間を確認するには、Citrix ADM にログオンし、「分析」**>**「ビデオインサイト」に移動して、「ABR ビデオ」をクリックします。次に、右側のペインで、ボックスの一覧から期間を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。[移動] をクリックし、[再生時間] タブを選択します。

フィルタードロップダウンリストを使用して、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、ネットワークから最適化および非最適化された ABR ビデオの再生の、合計再生時間。
- 暗号化および暗号化解除された ABR ビデオの再生時間の合計。
- 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

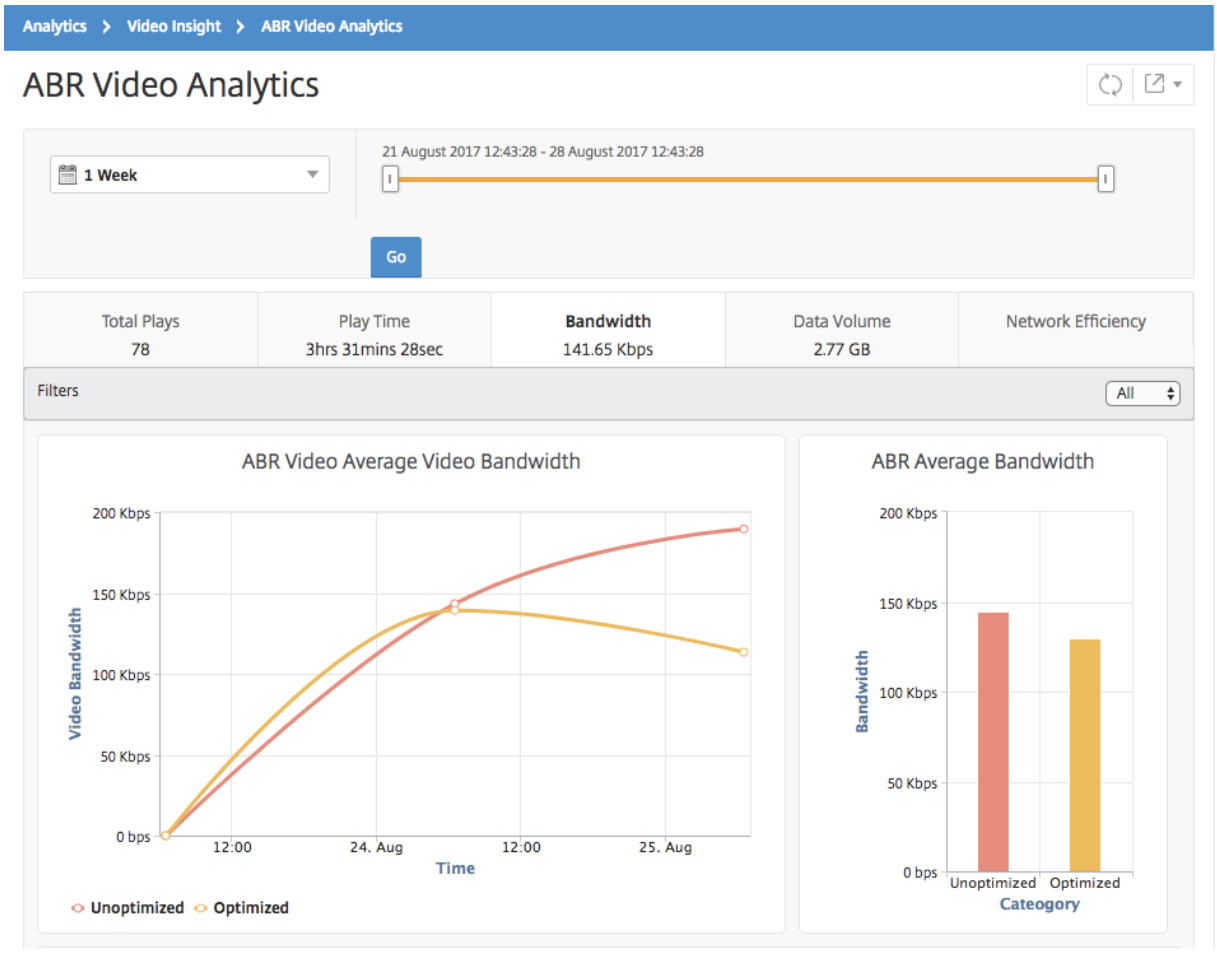
February 6, 2024

Citrix Application Delivery Management（ADM）は、特定の時間枠で ABR ビデオの最適化と非最適化によって消費される帯域幅を提供し、以下に基づいて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 ビデオの消費帯域幅を比較することもできます。

- 再生時間
- データ量

帯域幅消費量を確認するには、Citrix ADM にログオンし、「分析」**>**「ビデオインサイト」に移動して、「ABR ビデオ分析」をクリックします。次に、右側のペインで、ボックスの一覧から期間を選択します。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。[移動] をクリックし、[帯域幅] タブを選択します。

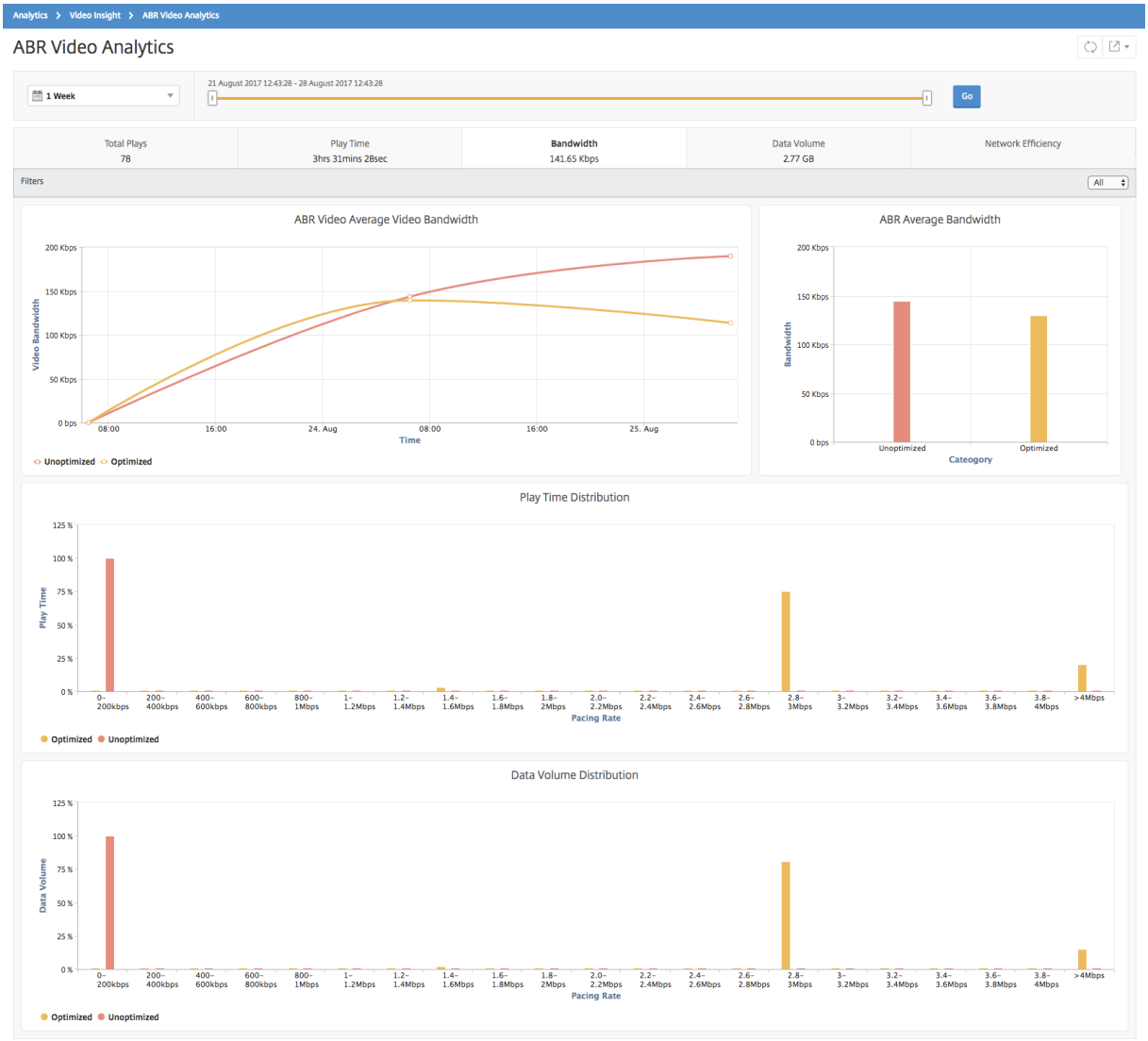
フィルタードロップダウンリストを使用して、HTTP、HTTPS、または QUIC ABR ビデオを選択できます。



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。



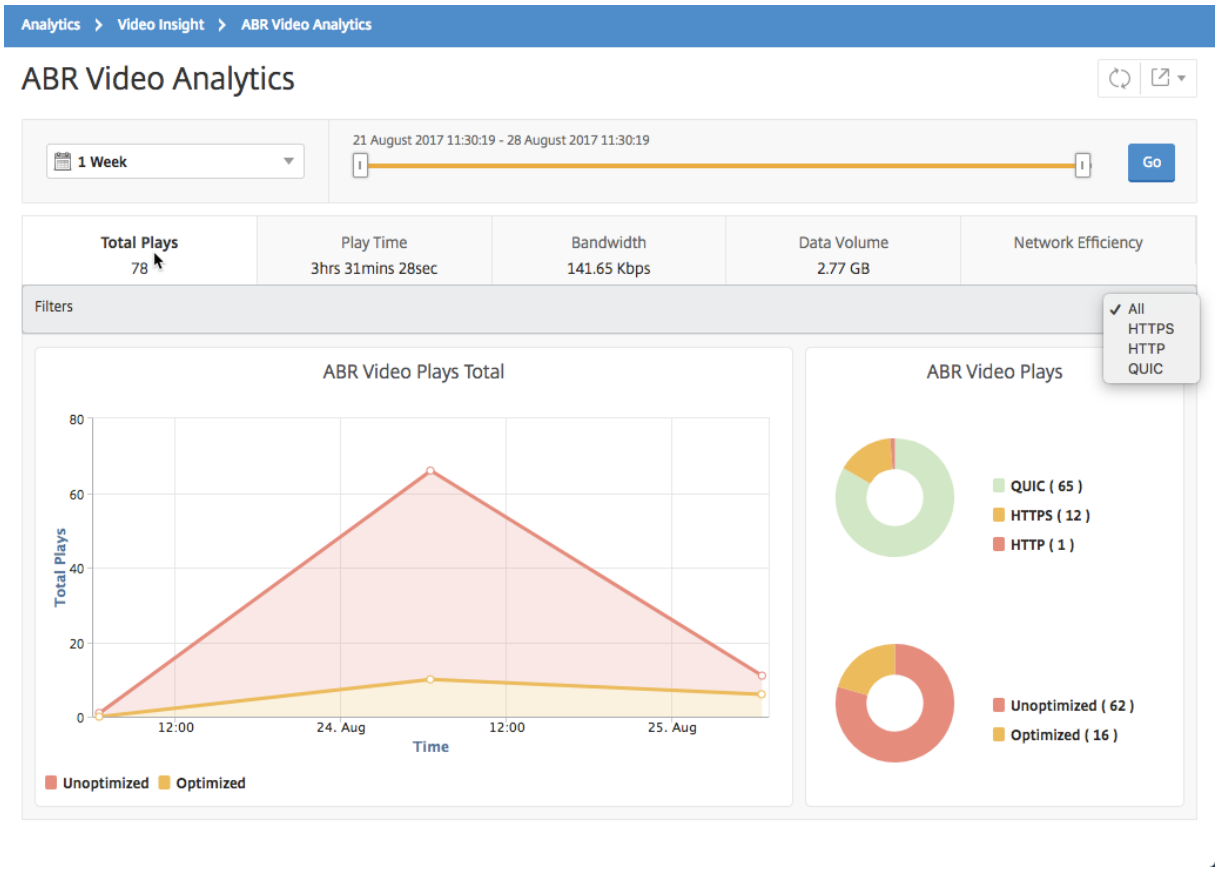
ABR ビデオの再生の最適化数と非最適化数を比較する

February 6, 2024

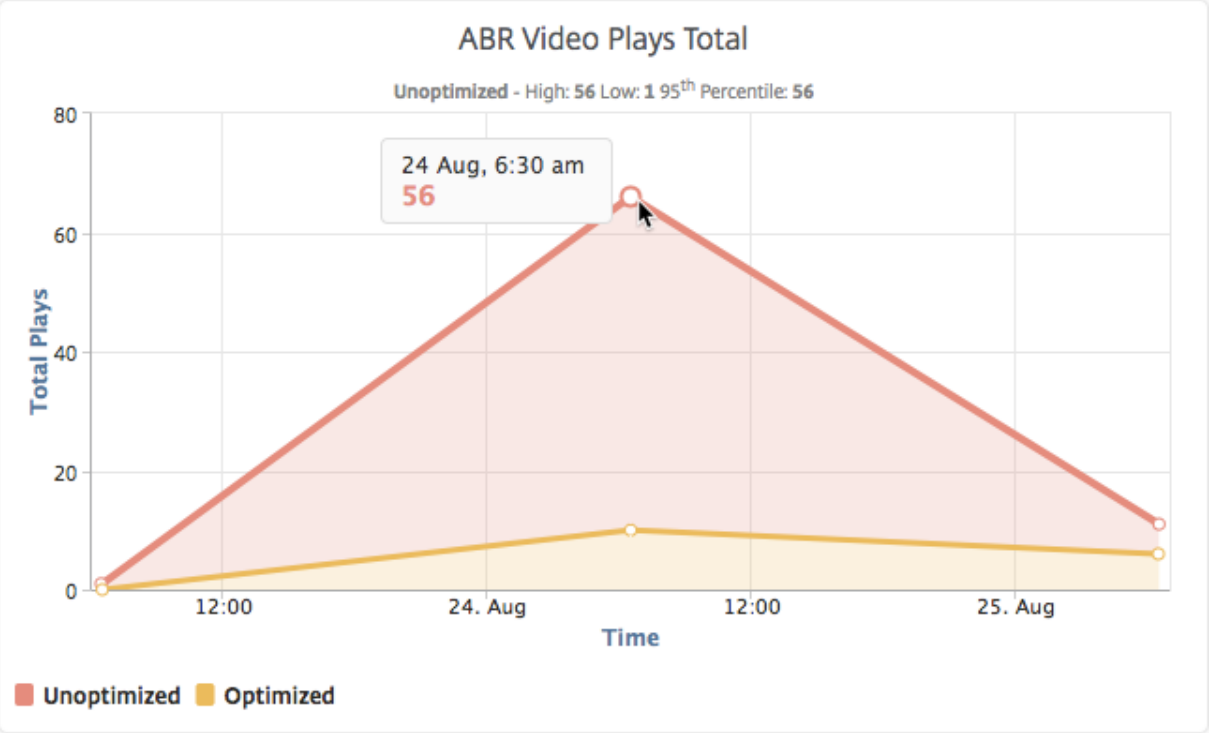
特定の期間において、NetScaler Application Delivery Management（ADM）は ABR ビデオの再生数を表示し、ネットワーク内の最適化された再生数と最適化されていない再生数を比較できます。

再生回数を確認するには、Citrix ADM にログオンし、[分析] > [ビデオインサイト] に移動して、[ABR ビデオ分析] をクリックします。次に、右側のペインで、ボックスの一覧から期間を選択します。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。[移動] をクリックし、[再生数] タブを選択します。

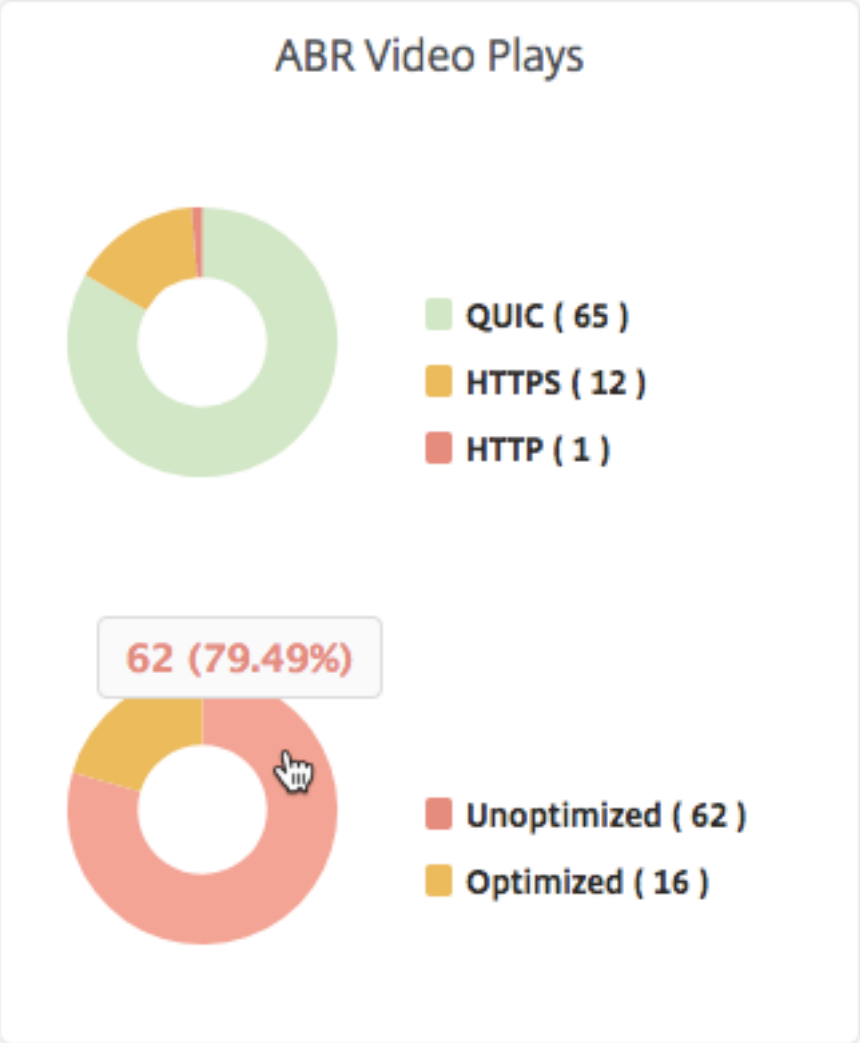
フィルタードロップダウンリストを使用して、HTTP、HTTPS、または QUIC ABR ビデオを選択できます。



[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。



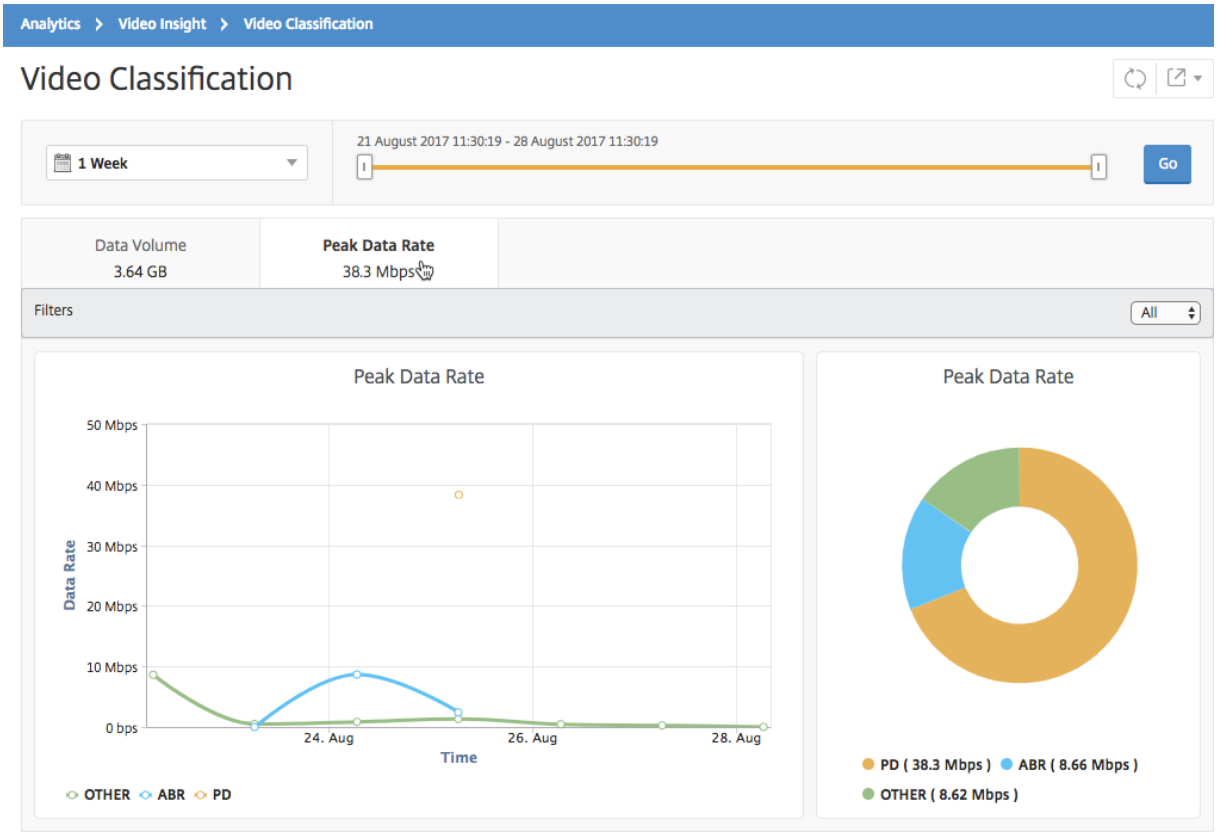
特定の時間枠のピークデータレートを表示する

February 6, 2024

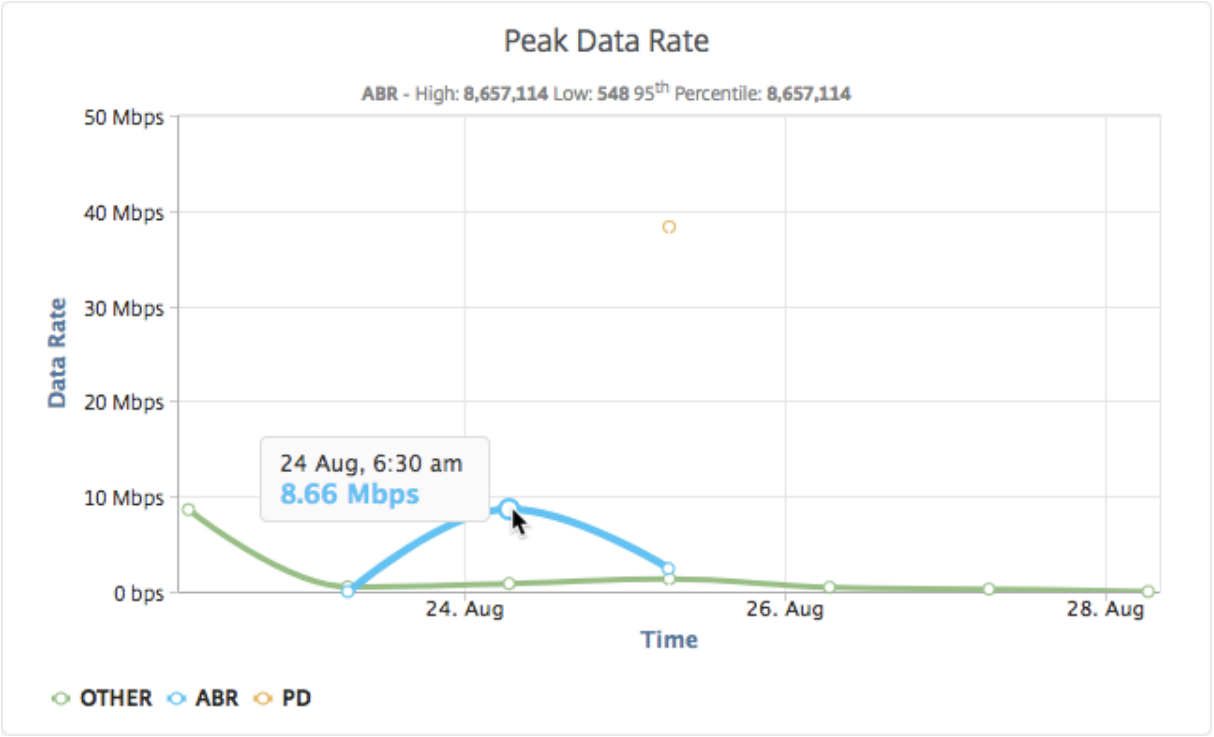
NetScaler Application Delivery Management（ADM）では、ネットワーク内のビデオトラフィックのピークスループットまたはデータレートが表示されます。

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、Citrix ADM にログオンし、［分析］**>**［ビデオインサイト］に移動して、［ビデオ分類］をクリックします。次に、右側のペインで、ボックスの一覧から期間を選択します。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。「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。

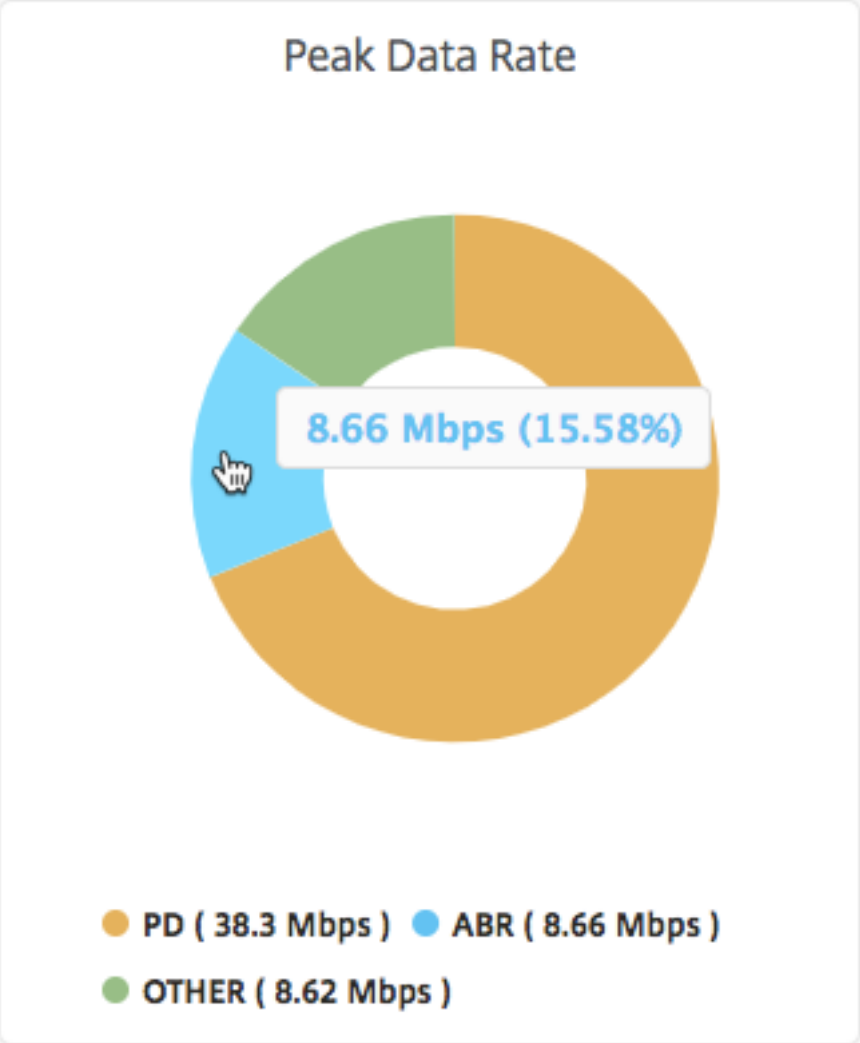
フィルタードロップダウンリストを使用して、HTTP、HTTPS、 または QUIC トラフィックを選択できます。



[**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。



Secure Web Gateway 分析

February 6, 2024

企業ネットワークのエッジにある Citrix Secure Web Gateway（SWG）アプライアンスは、インターネットプロキシとして機能します。このアプライアンスは透過プロキシモードまたは明示的プロキシモードで動作し、HTTPS を含むインターネットトラフィックの傍受を制御できるようにします。任意の要求を傍受するか、バイパスするか、禁止するかの決定は、アプライアンスに設定されたポリシーに基づいて行われます。ユーザーは社内ネットワークにログオンする前に認証されます。すべての要求と応答はユーザーにタグ付けされ、ユーザーのアクティビティはアプライアンスで記録されます。詳しくは、「Citrix Secure Web ゲートウェイ」を参照 してください。

Citrix Application Delivery Management（ADM）を Citrix SWG アプライアンスと統合すると、ログストリームを使用して、アプライアンス上でログに記録されたユーザーアクティビティとその後のレコードが Citrix ADM にエクスポートされます。NetScaler ADM は、訪問した Web サイトや消費された帯域幅など、ユーザーのアクティ

ビティに関する情報を照合して表示します。また、帯域幅の使用量と検出された脅威（マルウェアやフィッシングサイトなど）をレポートします。これらの主要なメトリックを使用して、ネットワークを監視し、Citrix SWG アプライアンスで修正アクションを実行できます。

Citrix SWG アプライアンスを **Citrix ADM** と統合するには：

1. Citrix SWG アプライアンスで、Secure Web Gateway を構成するときに、分析を有効にし、分析に使用する Citrix ADM インスタンスの詳細を指定します。
2. NetScaler ADM で、Citrix SWG アプライアンスをインスタンスとして NetScaler ADM に追加します。詳しくは、「NetScaler ADM へのインスタンスの追加」を参照してください。

ダッシュボード

February 6, 2024

2018 年 5 月 24 日

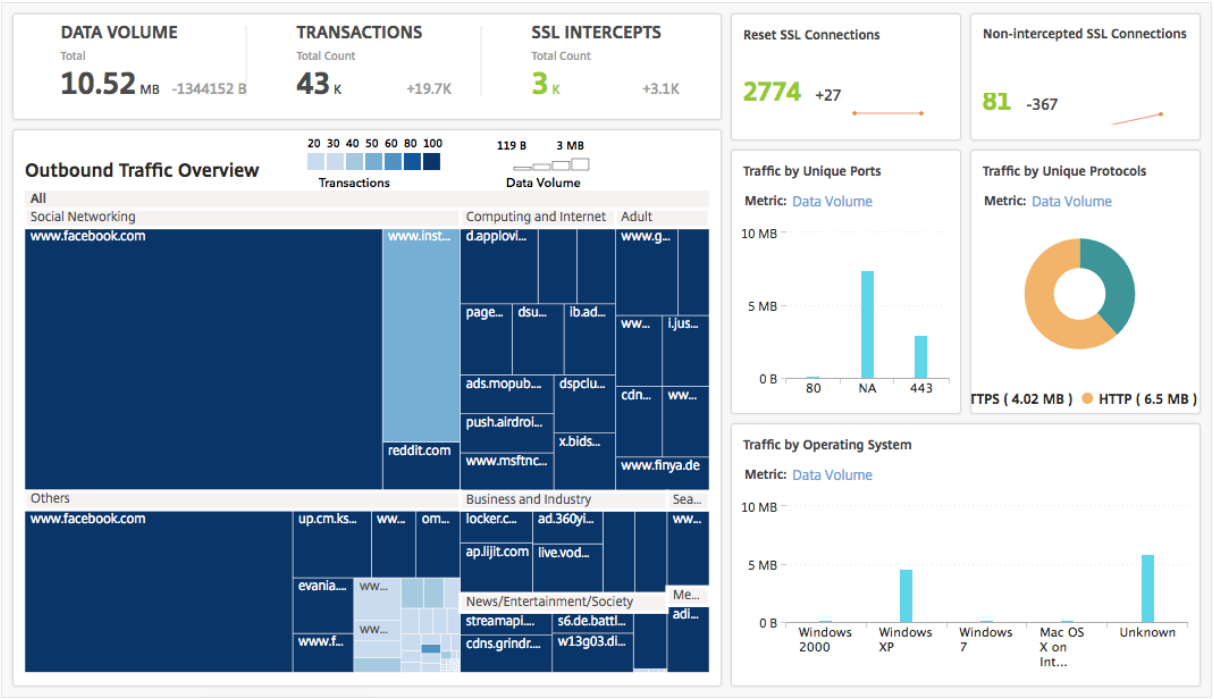
NetScaler Application Delivery Management（ADM）には、送信トラフィックダッシュボードとユーザーダッシュボードの **2** つのダッシュボードがあります。これらのダッシュボードには、組織内ネットワークからアクセスされた Web サイトとアプリケーション、およびネットワーク内のユーザーが実行したアクティビティの概要を示す複数のグラフが表示されます。

送信トラフィックダッシュボード

アウトバウンドトラフィックダッシュボード には、ネットワークからアクセスされた URL またはドメインの概要が表示されます。このダッシュボードでは、URL またはドメインで使用されたトランザクション数別またはデータボリューム別に URL とドメインの全体像を確認できます。
また、次のような詳細も表示されます。

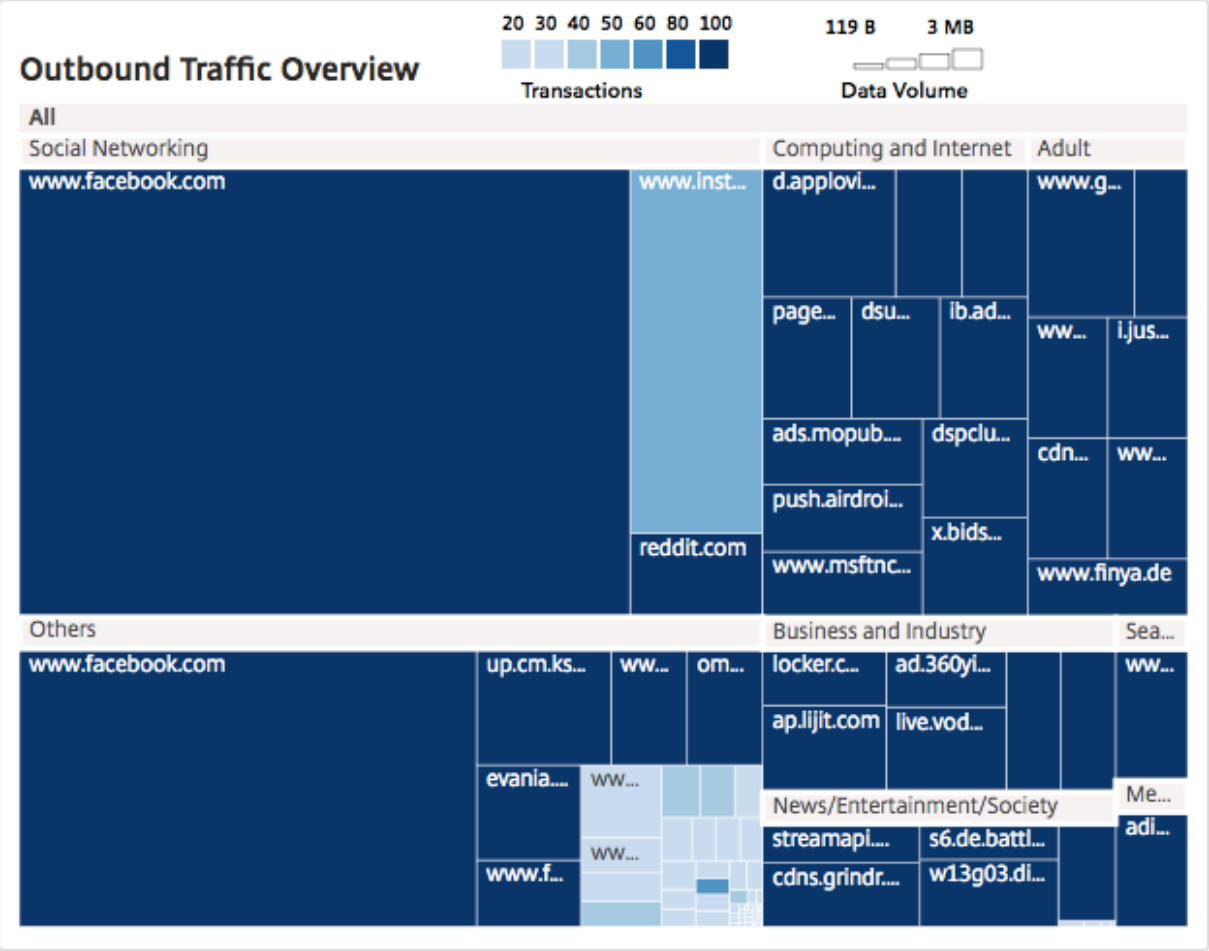
1. ネットワークからアクセスされた URL またはドメインで使用された帯域幅の量
2. ネットワークから URL およびドメインへのアクセス中に発生したトランザクション数
3. トランザクション中に Citrix SWG アプライアンスによってインターセプトされた SSL 接続の数。
4. トランザクション中に Citrix SWG アプライアンスによってインターセプトされなかった SSL 接続の数。
5. トランザクション中に Citrix SWG アプライアンスによってリセットされた SSL 接続の数。
6. トラフィックの送信に使用されたポート、Web トラフィックにより使用されたプロトコル、およびトラフィックの送信に使用されたクライアントオペレーティングシステムごとの Web トラフィックの送信量

アウトバウンドトラフィックダッシュボードにアクセスするには、「アプリケーション」>「アウトバウンドトラフィックダッシュボード」に移動します。



ネットワークからの送信トラフィックの確認

アウトバウンドトラフィックダッシュボード には、アウトバウンドトラフィックの概要 ペインがあります。アウトバウンドトラフィックの概要ペインでは、NetScaler ADM はアクセスされた URL またはドメインを「ショッピング」、「ニュース」、「ソーシャルネットワーキング」などのカテゴリに分類します。アウトバウンドトラフィックの概要ペインには、ネットワークからアクセスされた URL またはドメインが URL カテゴリのノードとして表示されます。ノードのサイズは、URL またはドメインへのアクセスで使用されたデータボリュームに応じて決まります。ノードの色は、URL またはドメインへのアクセス中に発生したトランザクションの回数を示しています。



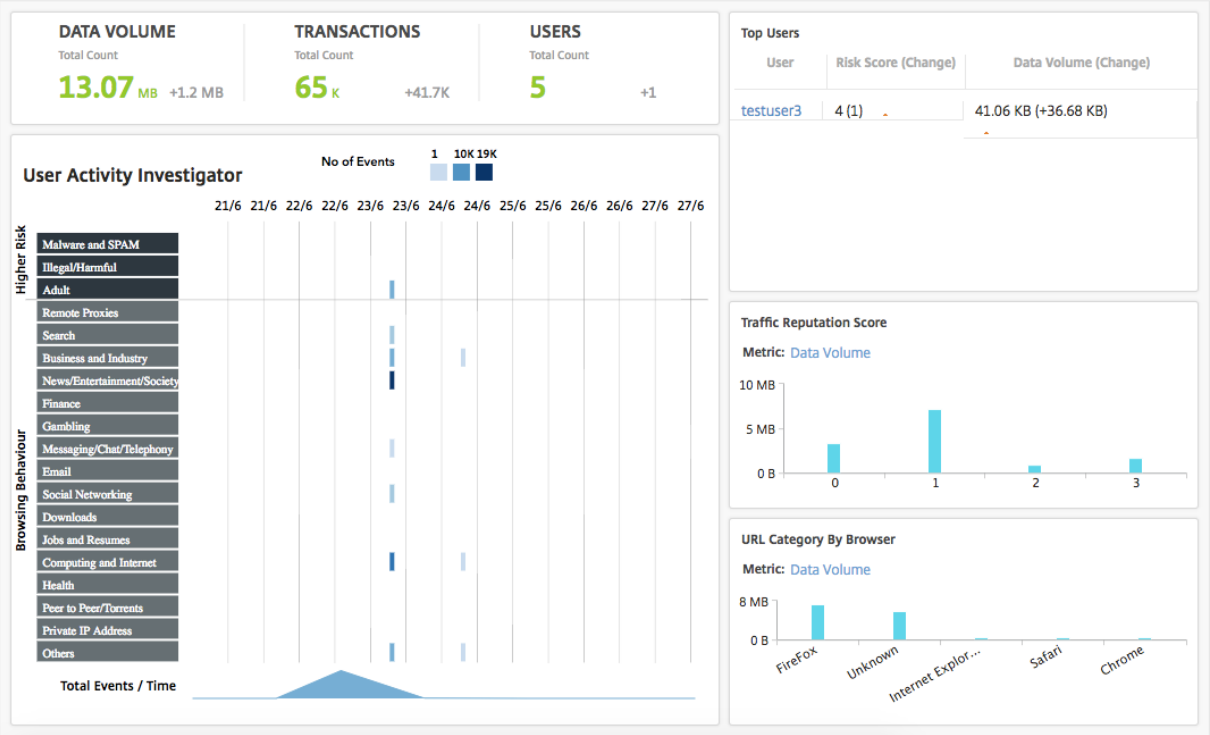
カテゴリーをクリックすると、指定時間内におけるそのカテゴリーに関連する詳細のみに絞り込んだグラフを表示できます。

ユーザーダッシュボード

ユーザー・ダッシュボード には、企業内のユーザーが実行したアクティビティの概要が表示されます。このダッシュボードにはキーメトリックが用意されており、これらを使用して以下を確認することができます。

1. 社内ユーザーのブラウジング行動
2. 社内ユーザーがアクセスした URL カテゴリ。
3. リスクスコアおよび使用帯域幅量に基づく上位 5 名のユーザー。リスクスコアについて詳しくは、「リスクスコア」を参照してください。
4. URL またはドメインへのアクセスに使用された Web ブラウザー。
5. トラフィックレピュテーションスコアに基づく、ユーザーにより生成された Web トラフィックの量

ユーザーダッシュボードにアクセスするには、「ユーザー」**>**「ダッシュボード」に移動します。

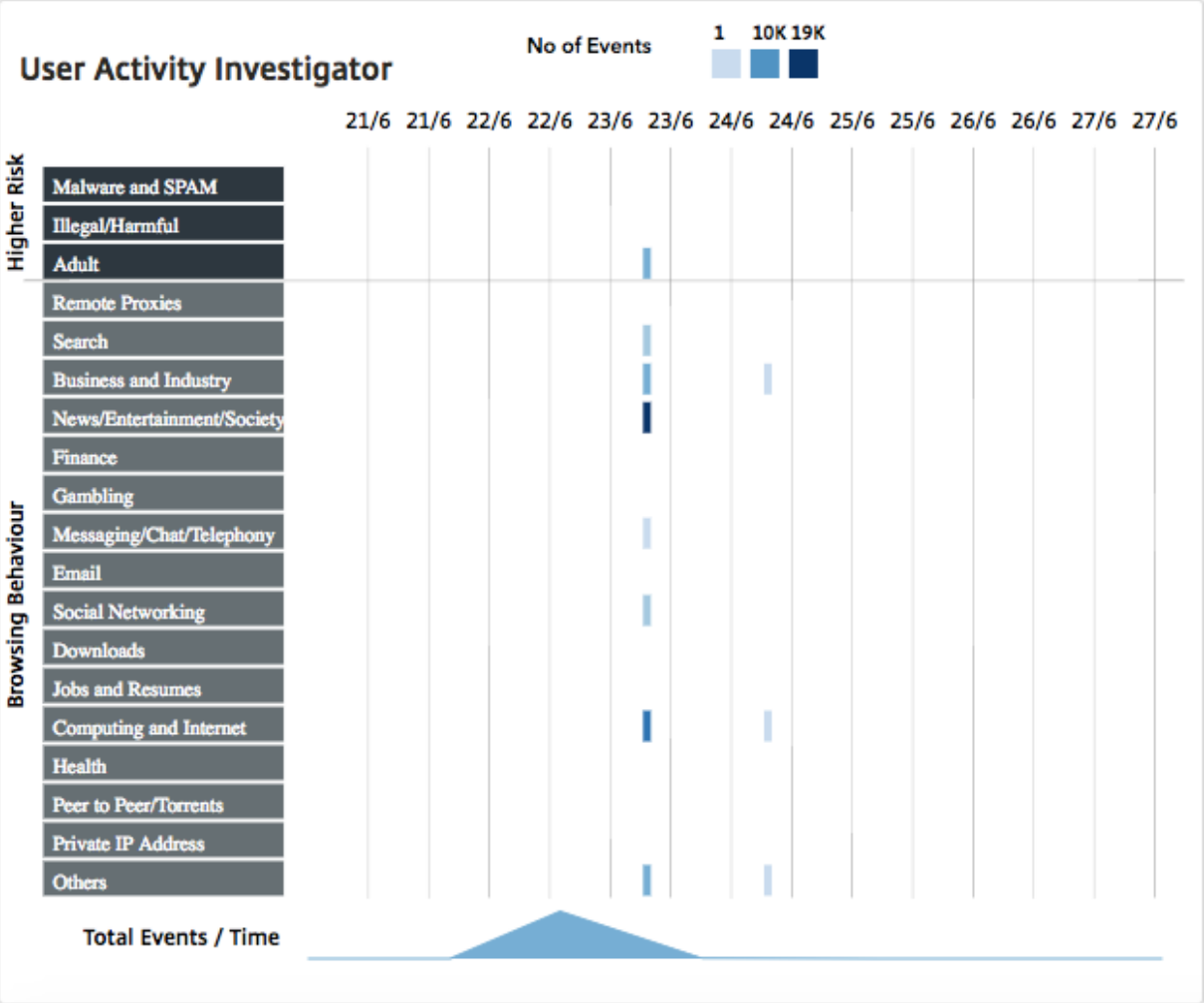


Top Users ペインでユーザーをクリックすると、グラフをフィルタリングして、指定した期間にユーザーが実行した Web アクティビティの詳細を表示できます。

User Activity Investigator

ユーザーダッシュボード には、ユーザーによって実行されたさまざまな **Web** アクティビティを表示する「**User Activity Investigator**」ペインがあります。このペインには、選択した時間内にユーザーがアクセスした URL カテゴリーと、URL カテゴリーごとの実行された各種イベントが表示されます。イベントをクリックすると、トランザクションレベルの詳細を確認できます。

User Activity Investigator は、URL カテゴリごとに、ユーザーの閲覧行動、ユーザーによるリスクの高いアクティビティ、トリガーされたイベントなどの重要な情報を表示します。イベントは、グラフ上に長方形の凡例として表示されます。凡例はそれぞれ、選択した期間が 1 時間の場合は 1 分間隔、選択した期間が 1 日の場合は 1 時間間隔で集計されます。



集計された凡例は、イベントの発生回数に応じて色分けされます。凡例にマウスポインターを重ねると、時間や選択した凡例について集計されたイベント数などの詳細が表示されます。グラフの期間は、期間のボックスから時間を選択することでカスタマイズできます。

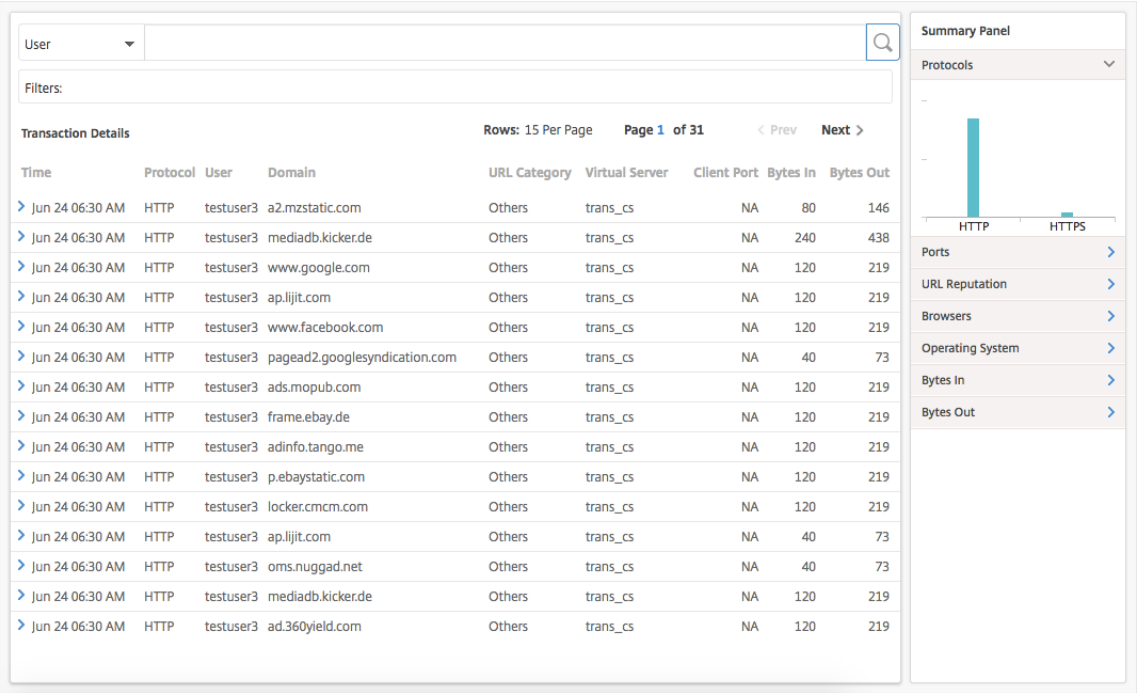
イベントをクリックすると、ドリルダウンしてトランザクションの詳細を確認できます。

User Transactions

[User Transactions] ペインには、ネットワーク内のユーザートランザクションの詳細が表示されます。このペインでは、以下のようなトランザクションレベルの詳細が示されます。

1. トランザクションの発生日時
2. トランザクションに使用されたプロトコル
3. ユーザー名
4. ユーザーがアクセスしたドメイン

5. URL カテゴリー
6. トランザクションの傍受に使用されたプロキシサーバー
7. クライアントポートの詳細
8. 受信バイト数
9. 送信バイト数



Summary panel 概要パネルには、トランザクションの詳細ペインに表示されるトランザクションのすべてのメトリックが表示されます。このパネルでは、メトリックを選択または選択解除することで、トランザクションの詳細ペインでトランザクションをソートして表示できます。概要パネルには次の指標が表示されます。

メトリックス	説明
プロトコル	トランザクションで使用されたプロトコル
ポート	トランザクションで使用されたポート
URL レピュテーション	URL レピュテーションスコア
Web ブラウザー	トランザクションで使用された Web ブラウザー
オペレーティングシステム	トランザクションで使用されたオペレーティングシステム
受信バイト数	Citrix SWG アプライアンスを介して受信したデータ量。

メトリックス	説明
送信バイト数	Citrix SWG アプライアンスを介して送信されたデータの量。

リスクスコア

リスクスコアは、NetScaler ADM で企業内のユーザーに関連するリスクを判断するために使用するスコアリングシステムです。Citrix ADM は、ネットワーク内のユーザーがアクセスする URL に Citrix SWG アプライアンスによって割り当てられた URL レピュテーションスコアに基づいてリスクスコアを割り当てます。URL レピュテーションスコアの詳細については、URL レピュテーションスコアを参照してください。次の表では、NetScaler ADM によって割り当てられるリスクスコアについて説明します。

リスクスコア	説明
1	ユーザーの Web アクティビティについて脅威は認められず異常ではありません。
2	ユーザーの Web アクティビティについて脅威は認められず異常でもありませんが、ユーザーは URL レピュテーションスコアが設定されていない「不明サイト」にアクセスしています。
3	ユーザーの Web アクティビティに脅威は検出されていませんが、ユーザーは潜在的な危険性があるサイトにアクセスしようとしたか、こうしたサイトと関係しています。
4	ユーザーが侵害を受けた可能性があります。
5	ユーザーの Web アクティビティは異常であり、ユーザーは既知の悪意のあるサイトにアクセスしました。

使用例

February 6, 2024

SSL インターセプションの監視

Citrix SWG アプライアンスを使用すると、暗号化されたアウトバウンドトラフィックを検査できます。アプライアンスに設定されたポリシーに基づいて、HTTPS 要求を傍受、バイパス、または禁止できます。NetScaler Application

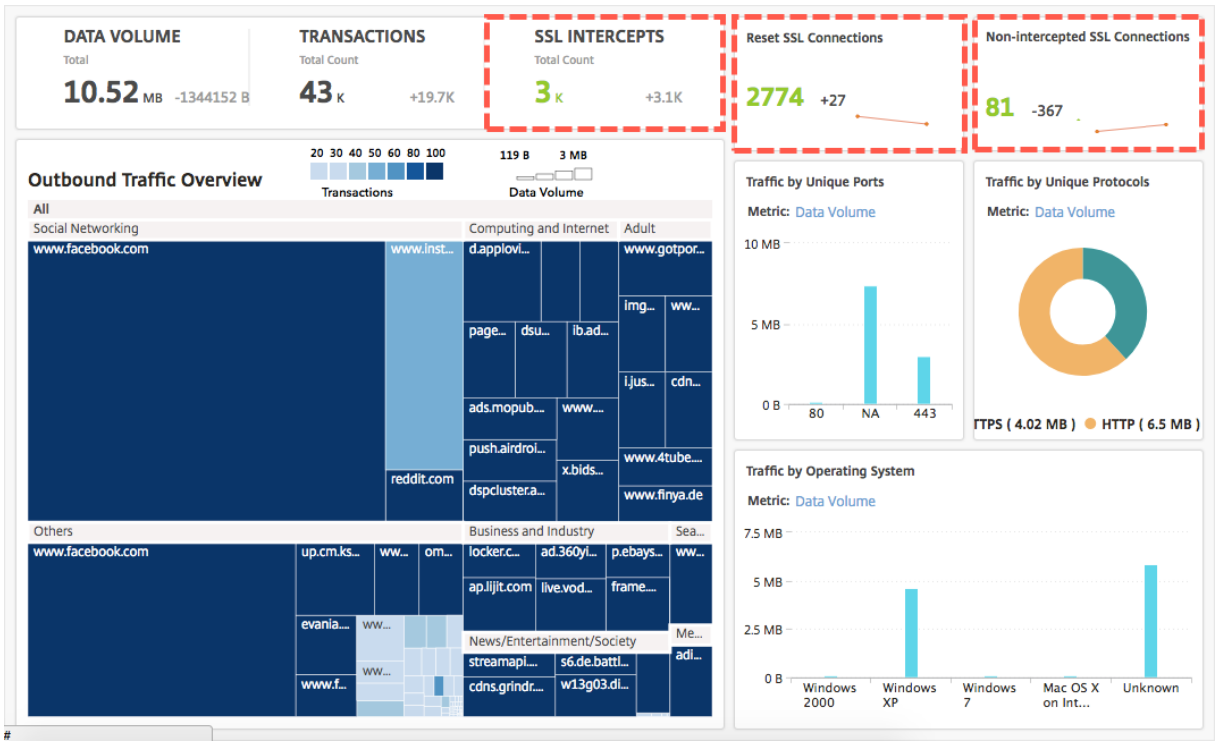
Delivery Management（ADM）では、選択した期間における 送信トラフィックダッシュボード の SSL 接続に関する次の詳細が提供されます。

- Citrix SWG アプライアンスによって傍受され、傍受されず、リセットされた SSL 接続の数
- SSL 接続のトランザクションの詳細

これらの詳細を使用して、Citrix SWG アプライアンスのポリシーをさらに微調整して、暗号化された送信トラフィックを効率的に検査できます。詳しくは、「Citrix Secure Web ゲートウェイ」を参照してください。

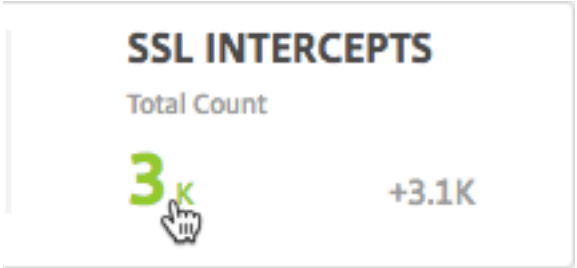
傍受された、傍受されていない、およびリセットされた **SSL** 接続の数を表示するには、以下を行います。

「アプリケーション」**>**「アウトバウンドトラフィックダッシュボード」に移動します。送信トラフィックダッシュボードに、傍受された、傍受されていない、およびリセットされた SSL 接続の数が表示されます。

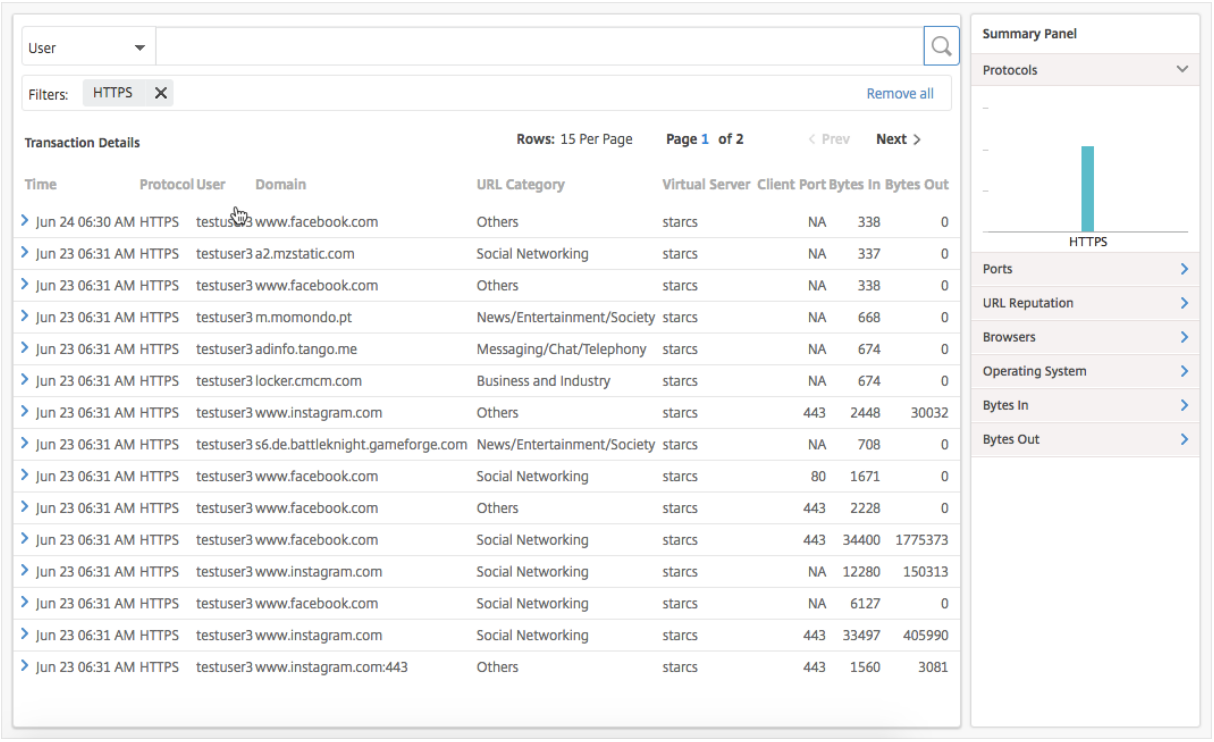


傍受された **SSL** 接続のトランザクションの詳細を表示するには、以下を行います。

1. 「アプリケーション」**>**「アウトバウンドトラフィックダッシュボード」に移動します。
2. 送信トラフィックダッシュボードで、「**SSL INTERCEPTS**」セクションの合計数をクリックします。



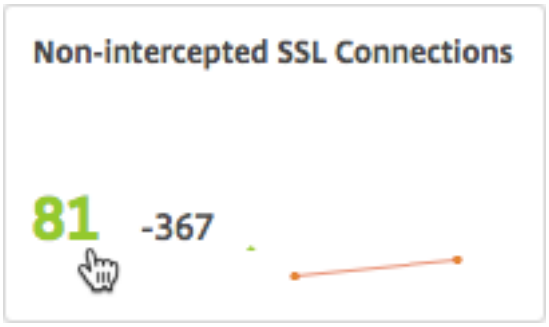
選択した期間中に傍受された SSL 接続のトランザクション詳細が、[トランザクション詳細] ページに表示されます。



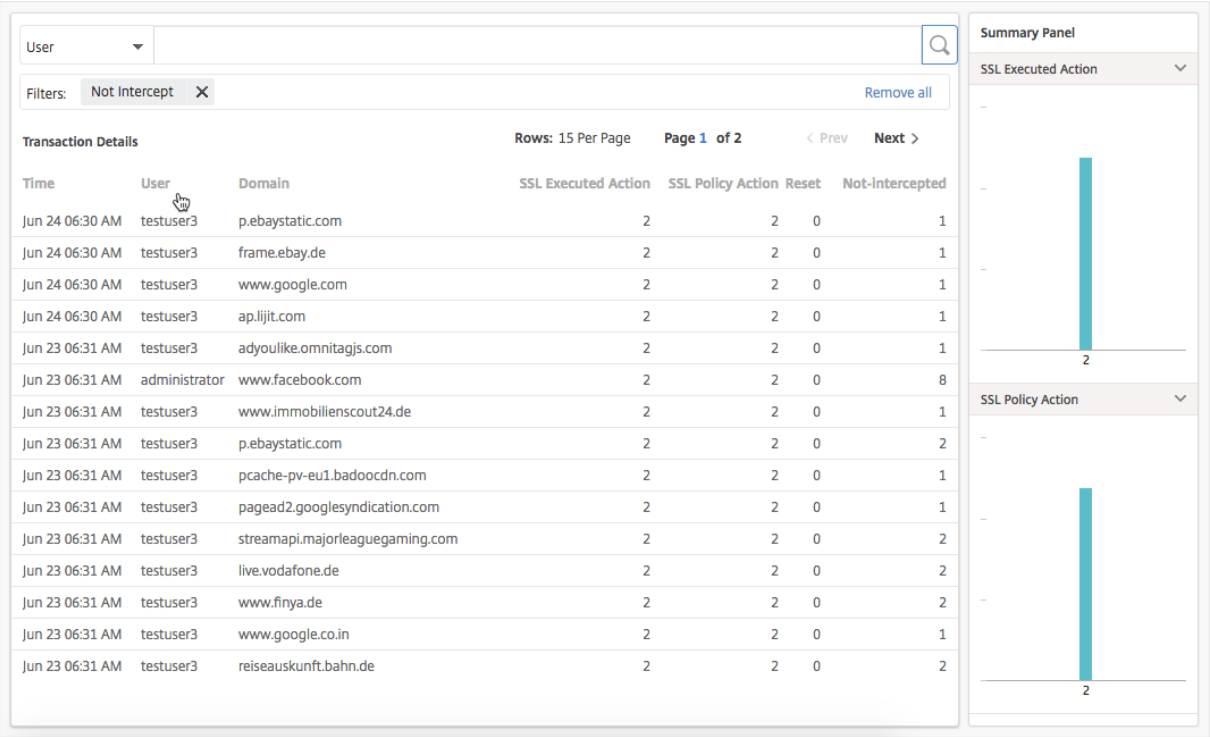
トランザクションの詳細をユーザーや URL カテゴリでさらにフィルターできます。

トラフィックが傍受されなかった **SSL** 接続のトランザクション詳細を表示するには:

1. 「アプリケーション」**>**「アウトバウンドトラフィックダッシュボード」に移動します。
2. 送信トラフィックダッシュボードで、代行受信されていない **SSL** 接続セクションの合計数をクリックします。



選択した期間中にトラフィックが傍受されなかった SSL 接続のトランザクションの詳細は、[**Transaction Details**] ページに表示されます。

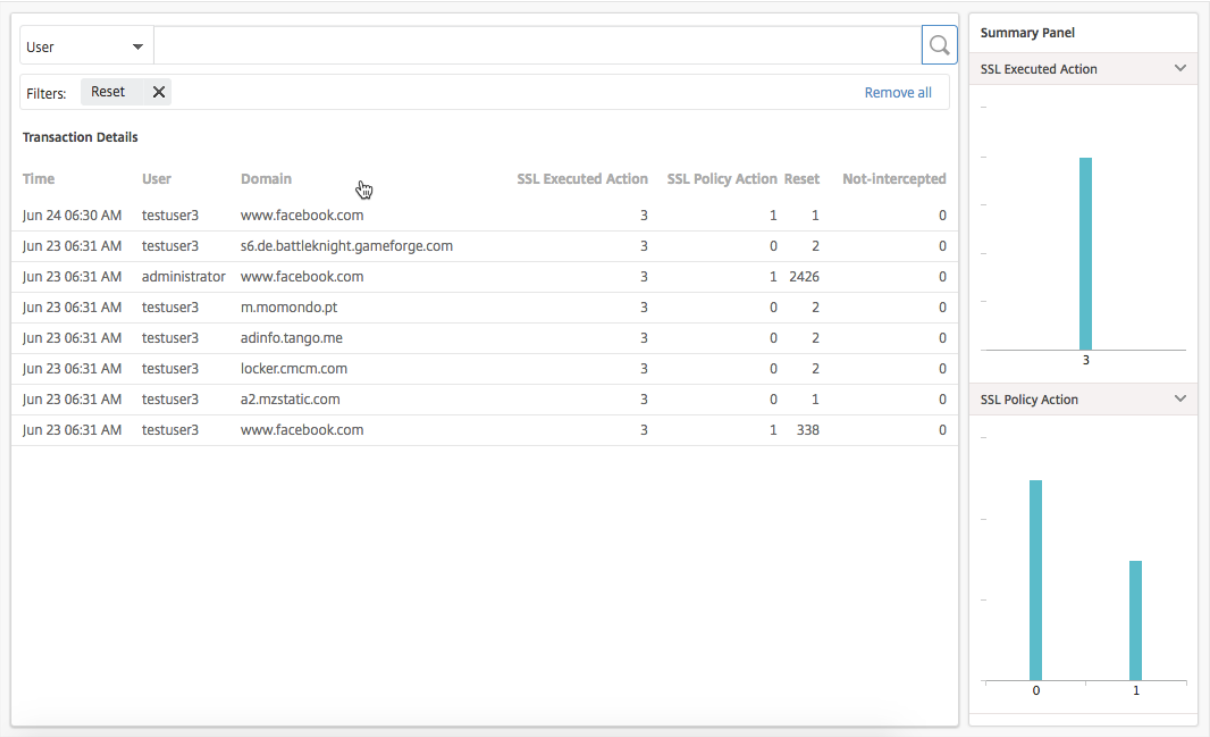


トランザクションの詳細をユーザーや URL カテゴリでさらにフィルターできます。

リセットされた **SSL** 接続のトランザクション詳細を表示するには:

1. 「アプリケーション」**>**「アウトバウンドトラフィックダッシュボード」に移動します。
2. 送信トラフィックダッシュボードで、[**SSL** 接続のリセット**]** セクションで合計数をクリックします。

選択した期間中にトラフィックが傍受されなかった SSL 接続のトランザクションの詳細は、[**Transaction Details**] ページに表示されます。



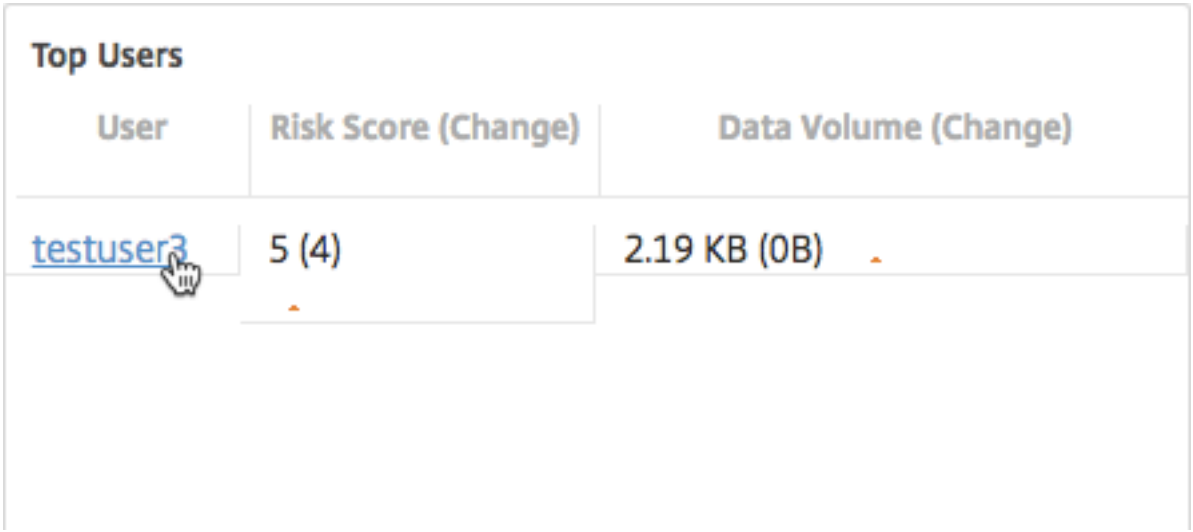
トランザクションの詳細をユーザーや URL カテゴリでさらにフィルターできます。

エンドポイントの検査

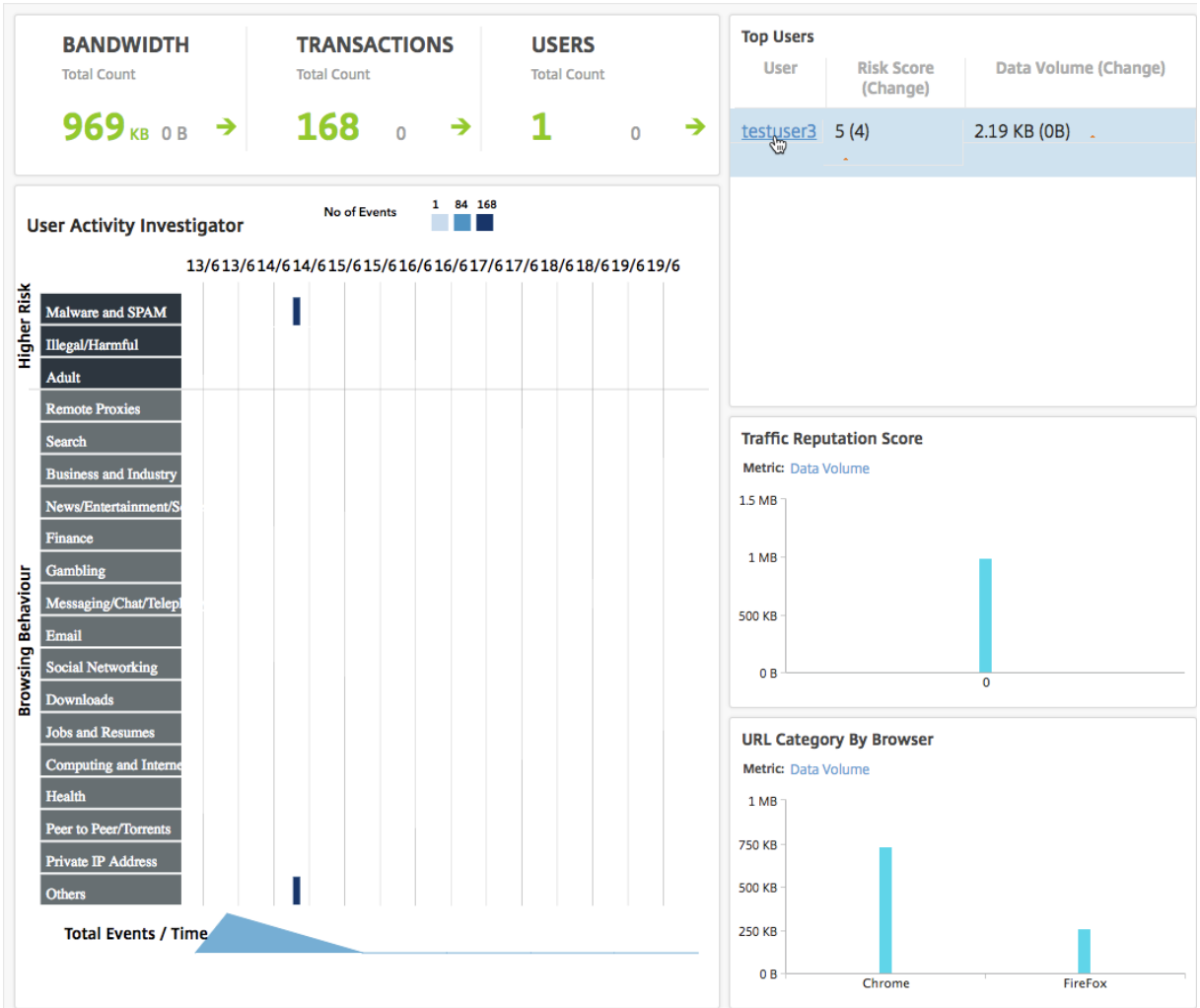
Citrix SWG アプライアンスで構成したポリシーは、企業で実行されたすべてのユーザーアクティビティをアプライアンスが記録する方法を指定します。NetScaler ADM は、次の項目を決定するために使用できる主要なメトリックを提供します。

1. 社内ユーザーのブラウジング行動
2. 社内ユーザーがアクセスした URL カテゴリ。
3. リスクスコアおよび使用帯域幅量に基づく上位 5 名のユーザー。リスクスコアの詳細については、「リスクスコア」を参照してください。
4. URL またはドメインへのアクセスに使用された Web ブラウザー。
5. トラフィックレピュテーションスコアに基づく、ユーザーにより生成された Web トラフィックの量

たとえば、ユーザー ID が testuser3 のユーザーが企業内のマルウェア関連サイトに常時アクセスしている場合、NetScaler ADM はそのユーザーをリスクの高いアクティビティユーザーとして識別し、より高いリスクスコアを割り当てます。testuser3 情報は、ユーザーダッシュボードの「上位ユーザー」セクションに表示されます。

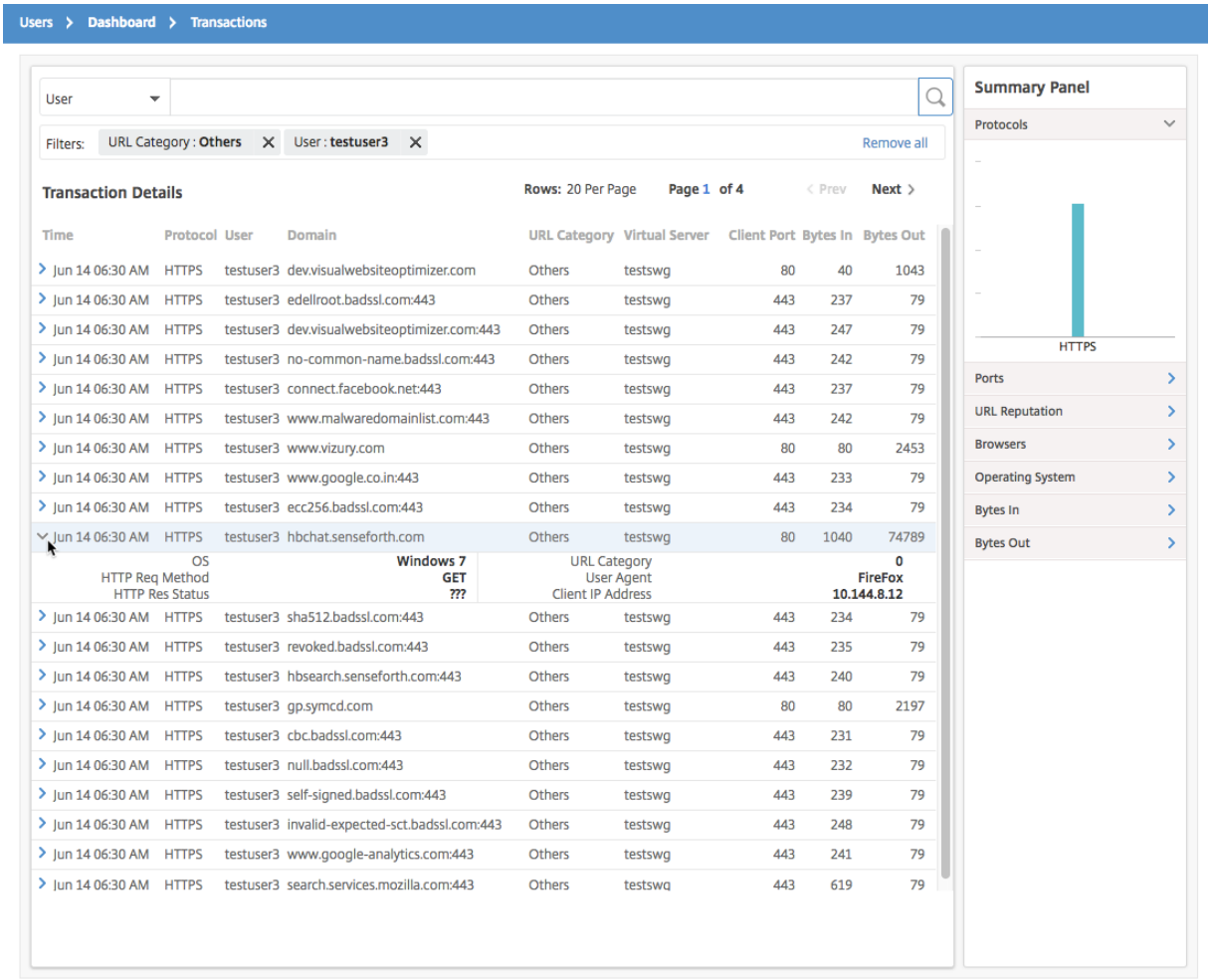


testuser3 をクリックすると、ユーザーダッシュボードをフィルタリングして、testuser3 に関連するすべての主要なメトリックを表示できます。



[ユーザーアクティビティの調査] ペインでは、testuser3 の高リスクアクティビティが、それぞれの URL カテゴリにイベントとして表示されます。

イベントにマウスでポイントしてイベント数を表示したり、イベントをクリックしてイベント中に発生したトランザクションを調査したりできます。

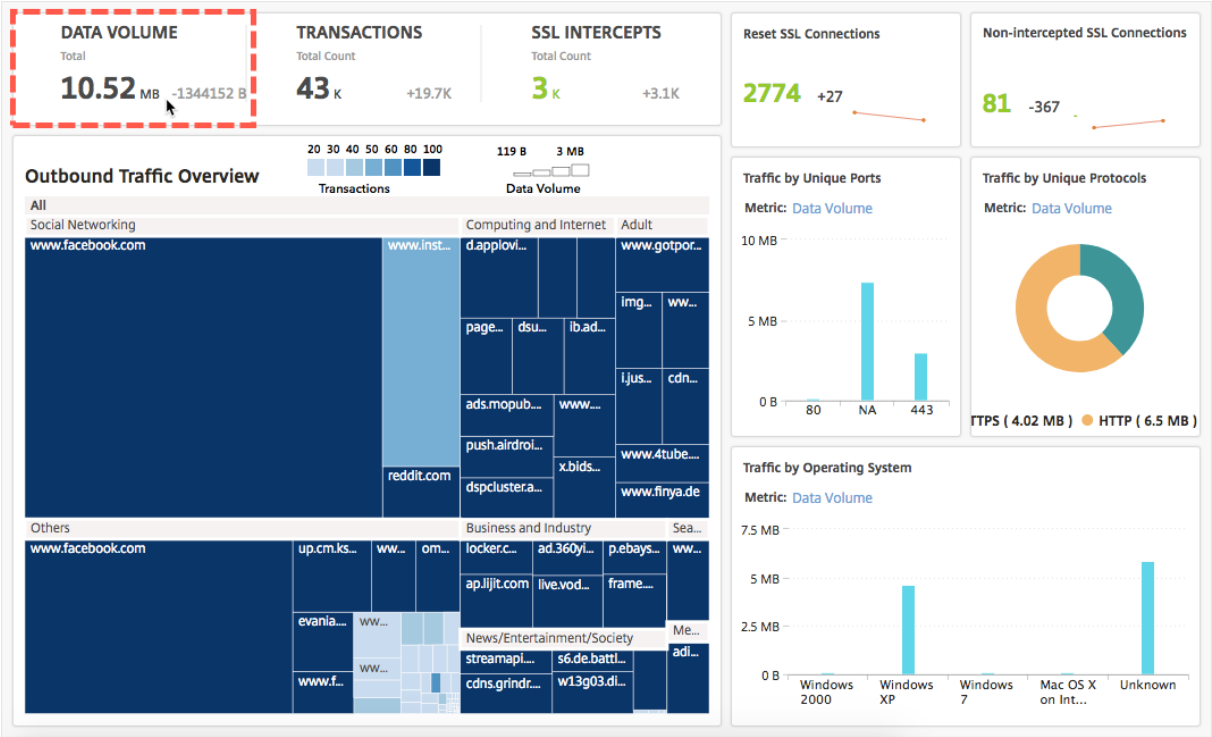


この情報を使用して、ユーザーのシステムがマルウェアに感染しているかどうかを判断したり、ユーザーの帯域幅消費パターンを把握して Citrix SWG ポリシーを微調整したりできます。詳しくは、Citrix Secure Web ゲートウェイのドキュメントを参照してください。

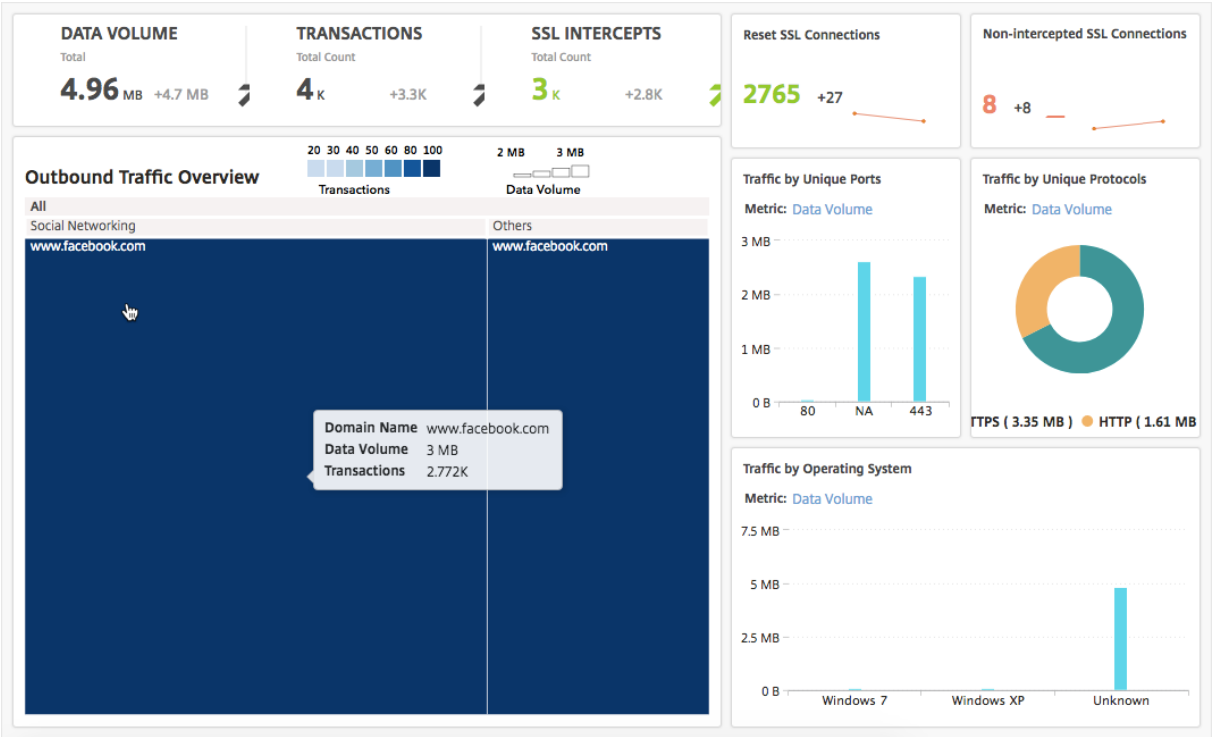
消費帯域幅のレポート

Outbound TrafficDashboard と **User Dashboard** には、企業ネットワークからアクセスした Web サイトやアプリケーション、およびネットワーク内のユーザーが実行したアクティビティをまとめた複数のグラフが用意されています。

アウトバウンドトラフィックダッシュボードには、ネットワークからアクセスされた URL またはドメインによるデータ量の消費の詳細が表示されます。「アプリケーション」>「アウトバウンドトラフィックダッシュボード」に移動します。「データボリューム」セクションに データボリュームの 詳細が表示されます。

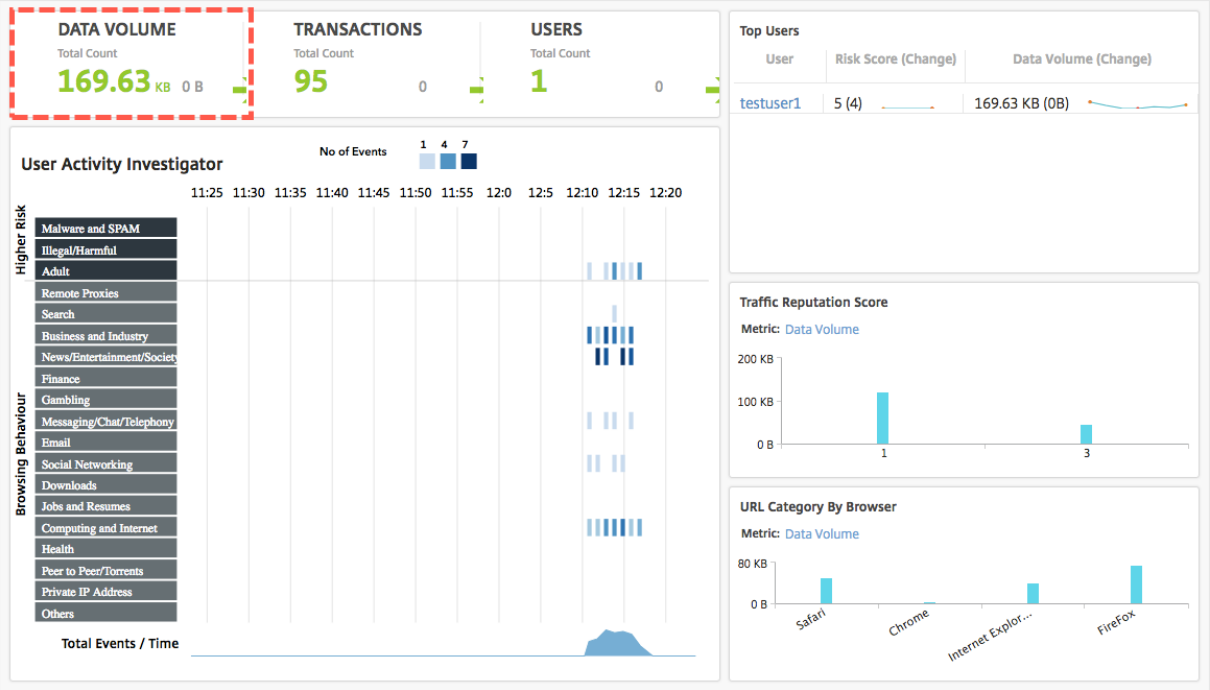


アウトバウンドトラフィック概要ペインでは、ドメインまたは URL をクリックすると、そのドメインまたは URL が消費するデータ量の詳細を表示できます。

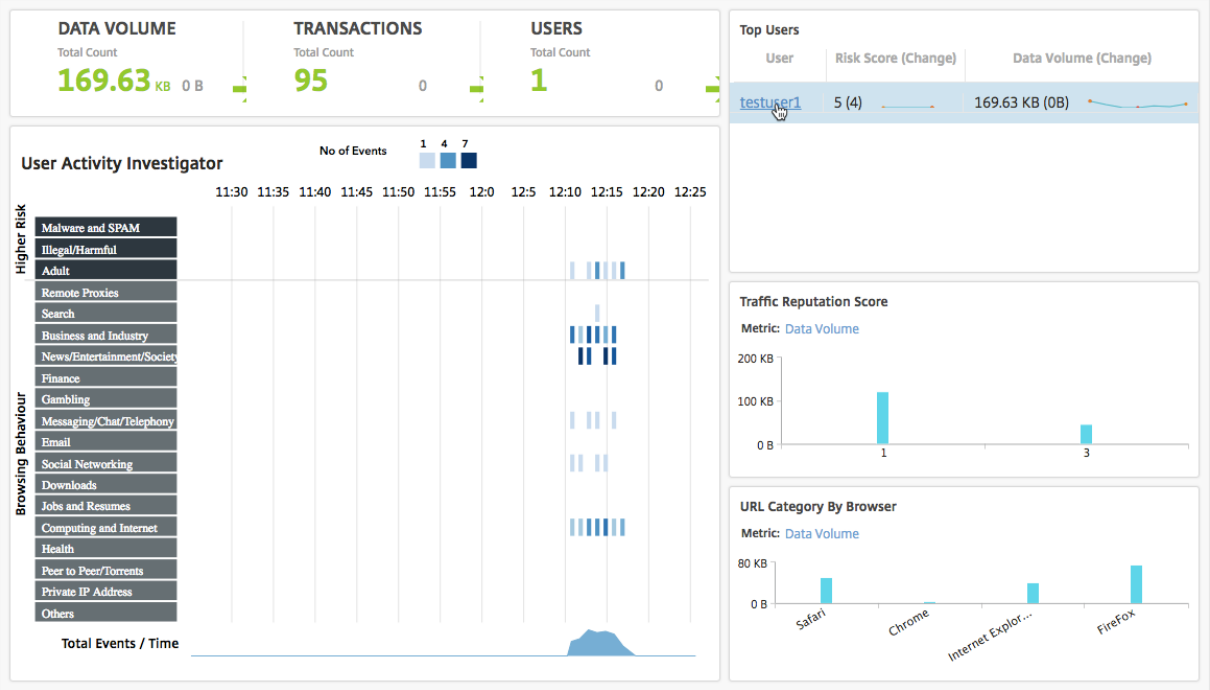


User Dashboard には、ネットワーク内のユーザが消費する帯域幅の詳細が表示されます。「ユーザー」>「ダッシュボード」に移動し、「ユーザー ダッシュボード」の「**D**ATA VOLUME」セクションにユーザーが消費した帯域幅の

詳細を表示します。



[**Top Users**] セクションからユーザーを選択すると、ユーザーが消費した帯域幅の詳細を表示できます。グラフ内の D **ATA VOLUME** セクションおよびその他の主要なメトリックは、選択したユーザーに対してフィルタリングされます。



これらの詳細を使用して、消費帯域幅とその消費理由を把握できます。たとえば、ユーザーがソーシャルネットワーキング Web サイトにアクセスしていて、そのために帯域幅が大量に消費されている場合、管理者は Citrix SWG ア

プライアンスにアクセスし、URL リスト機能を設定して Web サイトへのアクセスを制御できます。詳細については、「ユースケース: カスタム URL セットを使用した URL フィルタリング」トピックを参照してください。

送信トラフィック分散の表示

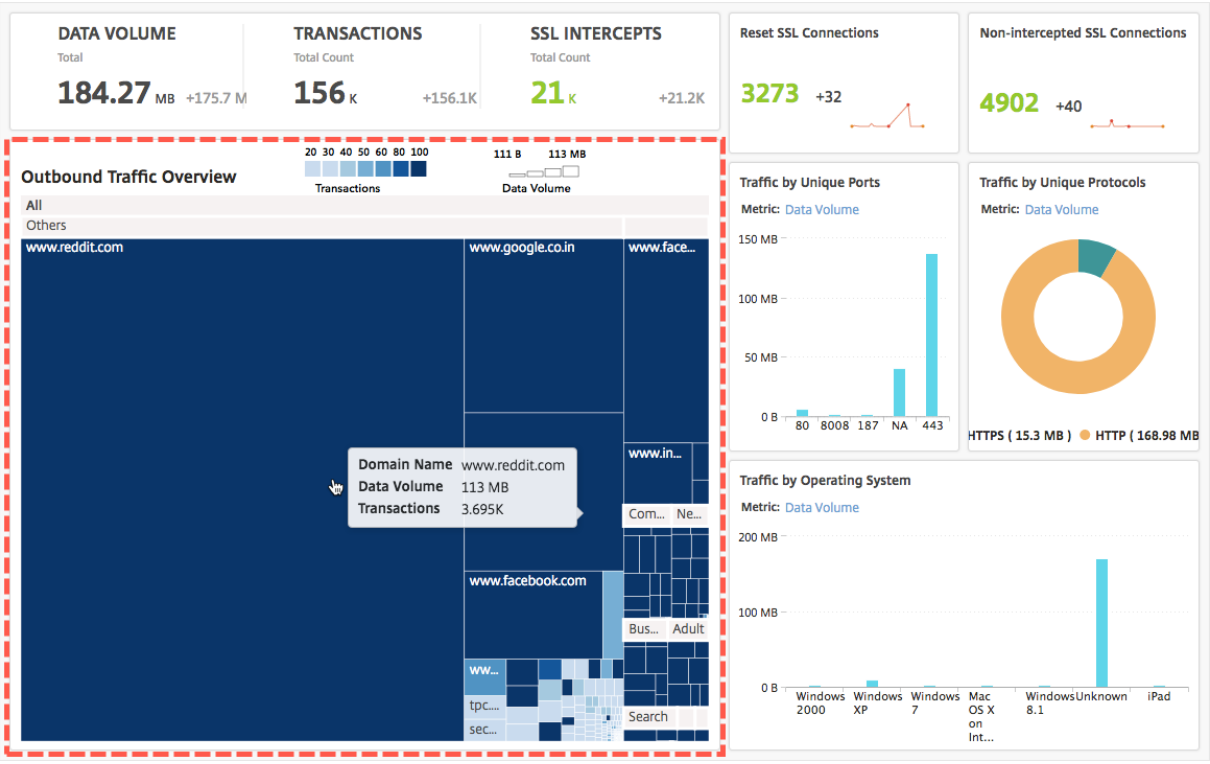
Citrix SWG アプライアンスには、ネットワークからアクセスされる URL を分類するために使用できる URL 分類およびフィルタリング機能があります。NetScaler ADM では、送信トラフィックダッシュボード に [送信トラフィックの概要] ペインが表示されます。NetScaler ADM では、［アウトバウンドトラフィックの概要］ペインで、アクセスした URL またはドメインがショッピング、ニュース、モバイルなどのカテゴリにグループ化され、ネットワーク内のアウトバウンドトラフィックの分布が表示されます。特定の期間について、URL をクリックして以下の事項を把握できます。

1. URL へのアクセスによって消費された帯域幅
2. URL にアクセス中に発生したトランザクション
3. URL にアクセス中に傍受された、傍受されていない、およびリセットされた SSL 接続の数

この情報により、送信トラフィックパターンを把握できるほか、特定の URL をブロックすべきかどうかなどの適切な意思決定を行うことができます。

アウトバウンドトラフィックの分布を表示するには:

「アプリケーション」**>**「アウトバウンドトラフィックダッシュボード」に移動します。[アウトボードトラフィックダッシュボード] の [アウトバウンドトラフィックの概要] ペインに URL が表示されます。



特定の URL の詳細を表示する場合には、その URL を選択します。

この情報を使用して、送信トラフィックパターンを把握し、SWG アプライアンスに設定された URL フィルターを使用して、ネットワークトラフィックを制御できます。詳細については、「URL フィルタリング」を参照してください。

オーケストレーション

February 6, 2024

SDN（Software Defined Networking：ソフトウェア制御ネットワーク）では、ネットワークをサポートするハードウェアに代わり、ソフトウェアアプリケーションコントローラーがネットワークとそのアクティビティを管理します。つまり SDN の場合、ネットワーク管理者は物理ネットワーク接続を論理ネットワーク接続に仮想化し、ソフトウェアベースの集中管理ツールを使用してネットワークサービスを管理できます。ネットワークエンジニアや管理者は、SDN を使用することで、頻繁に変わるビジネスの要件に対応できます。

よく知られている SDN のメリットには、トラフィックのプログラミング機能、優れたアジリティ、ポリシーに基づくネットワーク監視の設定、ネットワーク自動処理の実装がありますが、さらに SDN の特徴的なメリットとして次が挙げられます。

- 集中型ネットワークプロビジョニング
- 詳細なレベルによる優れたネットワークセキュリティ
- 運用コストの削減
- クラウド抽象化の促進
- コンテンツデリバリーの保証
- ネットワークダウンタイムの削減

Citrix アプリケーションデリバリー管理（ADM）は、さまざまなベンダーの SDN コントローラーと統合することにより、企業ネットワーク内の SDN をサポートします。Citrix ADM は、VMware NSX Manager とシスコアプリケーションポリシーインフラストラクチャコントローラ（APIC）の両方をサポートしています。

VMware NSX Manager

Citrix ADM は VMware ネットワーク仮想化プラットフォームと統合され、Citrix ADC サービスのデプロイ、構成、および管理を自動化します。この統合により、物理ネットワークトポロジに関連する従来の複雑さが解消され、vSphere/vCenter 管理者は Citrix ADC サービスをプログラムにより迅速に展開できるようになります。

VMware NSX Manager は、論理ファイアウォール、スイッチ、ルーター、ポートなどのネットワー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。

Citrix ADM のクラウドオーケストレーション機能により、Citrix ADC 製品と VMware NSX の統合が可能になり、次の機能が提供されます。

- 事前にプロビジョニングされたオンデマンドの VPX を、サービス挿入の一環として特定の Edge ゲートウェイに割り当てる。
- SSL や CS などの NetScaler ADC の高度な機能と、NSX 環境内で実行されているインスタンス上のアプリケーションテンプレートによる基本的な負荷分散を構成できます。
- サービス削除の一環として特定の Edge ゲートウェイから VPX の割り当てを解除し、同一の VPX を別の Edge ゲートウェイに再割り当てする。
- 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。
- クラウド管理者に単一ポイントでの管理を提供しつつ、マルチテナントの業務の分離およびセルフサービスの消費モデルを実現できる。
- NetScaler ADM API との統合が簡単で、将来の予期せぬ使用をサポートできます。

NetScaler ADM で VMware NSX Manager を構成する方法の詳細については、「NetScaler ADC アプライアンスと VMware NSX Manager の統合」を参照してください。

Cisco ACI のハイブリッドモード

Cisco ACI では、バージョン 1.3（2f）でハイブリッドモードのサポートが導入されています。ハイブリッドモードでは、アプリケーションポリシーインフラストラクチャコントローラー（APIC）を介してネットワーク自動化を実行しながら、L4-L7 構成を APIC のデバイスマネージャーとして機能する Citrix ADM に委任できます。

Citrix ADC ハイブリッドモードソリューションは、ハイブリッドモードのデバイスパッケージと Citrix ADM でサポートされています。APIC のハイブリッドモードデバイスパッケージをアップロードする必要があります。詳細については、「Cisco ACI のハイブリッドモードで NetScaler ADM を使用した NetScaler ADC オートメーション」を参照してください。

OpenStack: Citrix ADC インスタンスの統合

February 6, 2024

NetScaler Application Delivery Management（ADM）のクラウドオーケストレーション機能により、NetScaler ADC 製品と OpenStack プラットフォームを統合できます。OpenStack プラットフォームでこの機能を使用することで、OpenStack ユーザーは NetScaler ADC 負荷分散機能（LBaaS）を利用することができます。この後、OpenStack ユーザーは Citrix ADC インスタンスの OpenStack からロードバランサー構成をデプロイできます。

以下のセクションでは、Citrix ADM と OpenStack の統合ワークフローの機能について簡単に説明します。

オープンスタック中性子 **LBaaS** 用 **NetScaler ADC** ドライバ

OpenStack Neutron LBaaS プラグインには、OpenStack が Citrix ADM と通信できるようにする Citrix ADC ドライバーが含まれています。OpenStack はこのドライバーを使用して、LBaaS API を介して行われた負荷分散設定を NetScaler ADM に転送します。これにより、目的の NetScaler ADC インスタンスにロードバランサー設定が作成されます。また、OpenStack はドライバーを使用して Citrix ADM を定期的に呼び出し、すべての負荷分散構成のさまざまなエンティティ（VIP やプールなど）のステータスを Citrix ADC から取得します。OpenStack プラットフォーム用の Citrix ADC ドライバーソフトウェアは、Citrix ADM にバンドルされています。ドライバをダウンロードしてインストールするには、まず NetScaler ADM をインストールしてアプリケーションを起動する必要があります。

Citrix ADM と **OpenStack** を相互に登録する

まず、NetScaler ADM に OpenStack 情報を登録する必要があります。OpenStack コントローラー IP アドレスとクラウド管理ユーザーの認証情報、および OpenStack Citrix ADC ドライバーのユーザー認証情報を指定します。後で Neutron 設定ファイル (neutron.conf) の Citrix ADC_Driver セクションに同じログイン認証情報を指定して、OpenStack の Citrix ADC ドライバーが LB 構成中に Citrix ADM に接続できるようにすることができます。

OpenStack と Citrix ADM を相互に登録すると、両方が相互に通信できるようになります。また、OpenStack ユーザーは、OpenStack の既存の認証情報を使用して Citrix ADM ユーザーインターフェイスにログオンし、自分の LB 構成が Citrix ADC でどのように機能しているかを確認できます。

OpenStack におけるテナント

OpenStack では、テナントはプロジェクトとも呼ばれます。テナントはユーザーのグループであり、テナント（プロジェクト）は、分離されたユーザーグループに割り当てられるリソースのセット（コンピューティング、ネットワーク、ストレージなど）として定義されることもあります。

配置ポリシー

配置ポリシーにより、ユーザーが作成した各ロードバランサー構成で使用される Citrix ADC インスタンスを柔軟に決定できます。または、Citrix ADM には、OpenStack テナントに基づいて Citrix ADC インスタンスを割り当てるオプションも用意されています。

サービスパッケージ

サービスパッケージは、ポリシーおよび SLA と、デバイスまたは自動プロビジョニングの構成仕様、テナントおよび配置ポリシーがまとめられたものです。サービスパッケージは、通常、テナントに提供される分離ポリシーの条件で定義されています。

サービスパッケージに関するいくつかの重要点は次のとおりです。

- テナントを複数のサービスパッケージに含めることはできません。
- 複数のテナントを同一のサービスパッケージに割り当てることはできます。
- 自動プロビジョニング用に設定されたサービスパッケージでは、仮想 NetScaler ADC インスタンスは、1 つのプラットフォームタイプ（SDX プラットフォームまたは OpenStack Compute プラットフォーム）からのみ作成できます。

LBaaS V1 と **LBaaS V2** でサポートされる機能

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
  - Barbican（OpenStack のキーマネージャー）が管理する証明書による SSL オフロード
  - 証明書パッケージ（中間証明機関を含む）
  - SNI サポート

このドキュメントでは、以下の内容について説明します。

- ユースケースのシナリオ
- Citrix ADM と OpenStack ワークフローの統合
- Prerequisites
- Citrix ADM と OpenStack の事前構成タスク
- Horizon を使用した LBaaS V1 の構成手順
- コマンドラインを使用した LBaaS V2 の構成手順

- OpenStack での Citrix ADC VPX インスタンスの手動 Provisioning
- Citrix ADM と OpenStack Heat サービスの統合
- NetScaler ADM での OpenStack アプリケーションの監視

ユースケースシナリオ

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相互化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 Citrix ADM の両方をインストールして構成し、相互に連携できるように準備する必要があります。スティーブは、OpenStack に Example-SportsOnline という名前のテナントアカウントを作成し、そのテナントアカウントにリソースを割り当てる必要があります。また、リソースと構成を管理するために、Example-SportsOnline 用の複数のログオン資格情報（ユーザー）も作成する必要があります。これらの手順を経ると、トムが OpenStack に 2 台のサーバー、S1 と S2 を作成し、Example-SportsOnline.com のトラフィックを管理できるようになります。

スティーブは OpenStack の詳細を Citrix ADM に登録し、OpenStack のネットワークコンポーネントである Neutron で Citrix ADC LBaaS ドライバーを設定する必要があります。登録が完了すると、Citrix ADM は OpenStack のすべてのテナントの詳細を表示します。スティーブは、Citrix ADC LBaaS 機能を希望するユーザーのリストから Example-SportsOnline を選択し、Citrix ADM のロードバランサー構成に専用の Citrix ADC が割り当てられるようにトムを構成できます。

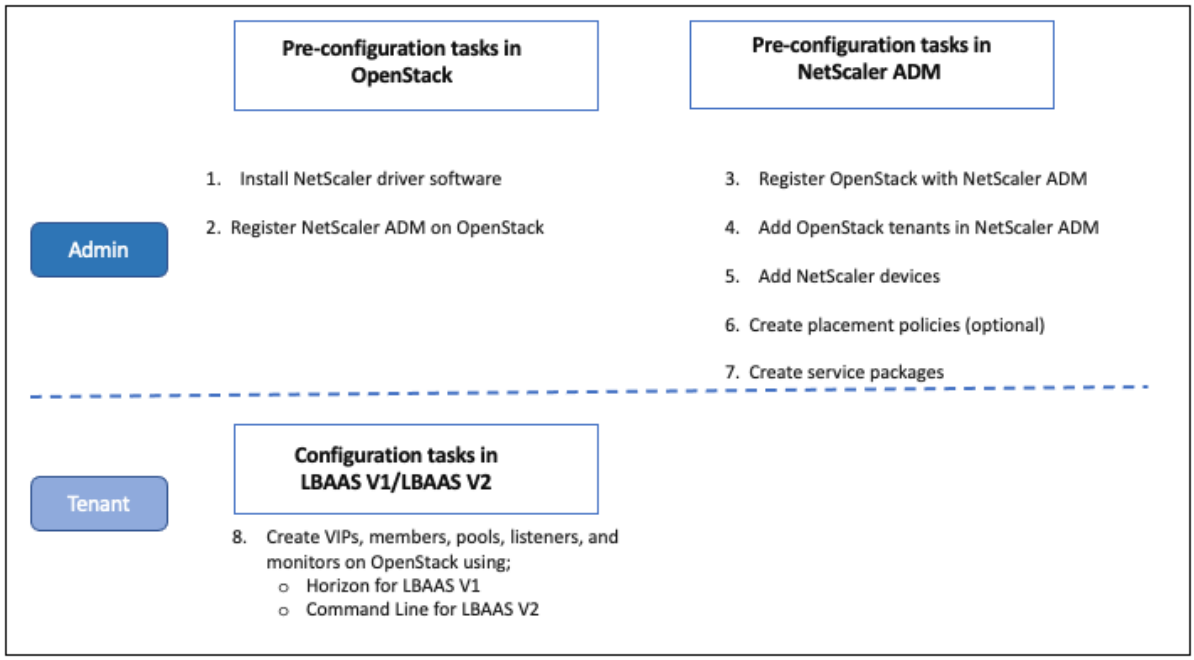
このため、スティーブは Citrix ADM ユーザーインターフェイスを使用して OpenStack のコンピューティングレイヤー（Nova）に Citrix ADC VPX インスタンスをプロビジョニングするか、トムが OpenStack で LB 構成を行うときに MAS が Citrix ADC VPX インスタンスをオンデマンドで自動プロビジョニングできるようにすることができます。いずれの場合も、Citrix ADM が VPX インスタンスを管理します。これを実現するために、スティーブは Citrix ADM でサービスパッケージを作成し、SLA でトムと合意したサービスパッケージの条件を定義します。たとえば、ロードバランサー構成を実現する専用インスタンスをトムに提供する場合、スティーブは「Dedicated」分離ポリシーを選択します。つまり、サービスパッケージでトムに対して非共有インスタンスを選択します。次に、多数の Citrix ADC VPX インスタンスをサービスパッケージに割り当て、Example-SportsOnline を、専用の Citrix ADC を必要とする他のテナントと一緒にサービスパッケージに関連付けます。その結果、トムが初めてロードバランサー構成を実行すると、Citrix ADM はサービスパッケージ内の Citrix ADC VPX インスタンスの 1 つを Example-SportsOnline に割り当てて、その構成をその Citrix ADC にも展開します。

これでトムは、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、Citrix ADC インスタンスにサービスグループおよび仮想サーバーとしてデプロイされます。Tom は、ヘルスモニターを作成してサーバーを監視し、いつでも稼働していて Citrix ADC からアクセスできるサーバーのみにアプリケーショントラフィックを送信することもできます。

OpenStack で作成された負荷分散設定が Citrix ADC インスタンスに実装されるようになりました。完全に構成されると、NetScaler ADC VPX インスタンスが負荷分散機能を引き継ぎ、アプリケーショントラフィックの受け入れを開始し、Tom によって作成されたサーバー S1 と S2 間のトラフィックの負荷分散を行います。

Citrix ADM と OpenStack ワークフローの統合

次のフローチャートは、LBaaS V1 および LBaaS V2 構成時に従う必要のあるワークフローです。



前提条件

February 6, 2024

Citrix ADC 仮想インスタンスを OpenStack プラットフォームと統合する前に、次の要件が満たされていることを確認してください。

NetScaler ADM および OpenStack ソフトウェア要件

- Citrix ADM 12.1 は、最小ハードウェア要件システムを満たす、サポートされているハイパーバイザーワークステーションにインストールされます。
- OpenStack コンポーネントがインストールされ、実行されています。
- Citrix ADM 12.1 は、ニュートン、オカタ、パイクの次の OpenStack バージョンをサポートしています。

NetScaler ADM ハードウェア要件

次の表は、Citrix ADC 仮想インスタンスをインストールするために OpenStack サーバーに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 または 100Mbps

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

NetScaler ADM および OpenStack での事前構成タスク

February 6, 2024

このセクションでは、Citrix Application Delivery Management（ADM）と OpenStack を設定する前に、事前設定タスクを実行するのに役立ちます。

Citrix ADM のインストール

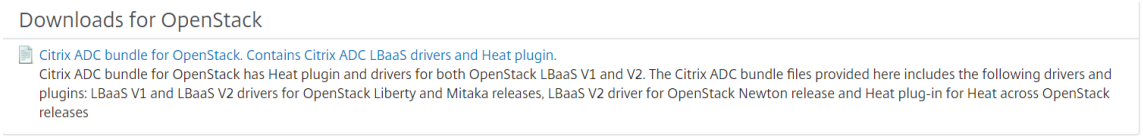
サポートされている Hypervisor に NetScaler ADM をインストールします。NetScaler ADM をダウンロードしてインストールする方法について詳しくは、「NetScaler ADM の展開」を参照してください。

NetScaler ADC ドライバーソフトウェアのインストールと **OpenStack** への **NetScaler ADM** 登録

Citrix ADM ダウンロードページから OpenStack 用の Citrix ADC バンドルをダウンロードします。

Citrix ADM GUI を使用して **OpenStack** プラットフォームに **Citrix ADC** ドライバーをインストールするには:

1. Citrix ADM で、「ダウンロード」をクリックします。Citrix ADM のダウンロードページには、ニュートン、オカタ、およびパイクの OpenStack バージョンに必要な **OpenStack** ソフトウェア用の **Citrix ADC** バンドルをダウンロードするためのリンクがあります。
2. 最新の Citrix ADC バンドル tar ファイルを OpenStack Controller の一時ディレクトリ (たとえば、/tmp) にダウンロードします。このバンドルには、すべての OpenStack リリース用の LBaaS V2 ドライバーと Heat プラグインが含まれています。



3. 次のコマンドを実行して、NetScaler ADC ドライバの tar ファイルからファイルを抽出します。
   ```
   tar -xvzf <name_of_tar_file>
   ```
4. OpenStack <Release Name> setup がある場合は、プロンプトで次のコマンドを入力します。

   ```
   cd <Release Name>
   ```

   例:

   ```
   cd Newton
   ```

5. 次のコマンドを実行してドライバをインストールし、Citrix ADM IP アドレス、OpenStack を Citrix ADM に登録したときに設定した Citrix ADC ドライバパスワード、およびプロトコルを指定します。

   ```
   ./install.sh --ip=<NetScaler_MAS_IP> --password=<password> --protocol=<protocol> --neutron-lbaas-path <neutron-lbaas-directory-path>
   ```

   単一ノード **OpenStack** のセットアップ例:

   ```
   ./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/opt/stack/neutron-lbaas
   ```

   マルチノード **OpenStack** セットアップ例:

   ```
   ./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/usr/lib/python2.7/site-packages
   ```


> 注
>
> システムの neutron-lbaas ディレクトリのパスは省略できます。このパスを指定すると、スクリプトによるドライバーの検索が容易になります。
>
> Citrix ADM が OpenStack に正常に登録されたら、OpenStack のユーザー認証情報を使用して Citrix ADM にログオンすることもできます。
>
> Citrix ADM が OpenStack に正常に登録されたら、OpenStack Neutron サービスを再起動します。

OpenStack を **Citrix ADM** に登録する

Citrix ADM GUI を使用して **OpenStack** を **Citrix ADM** に登録するには**:**

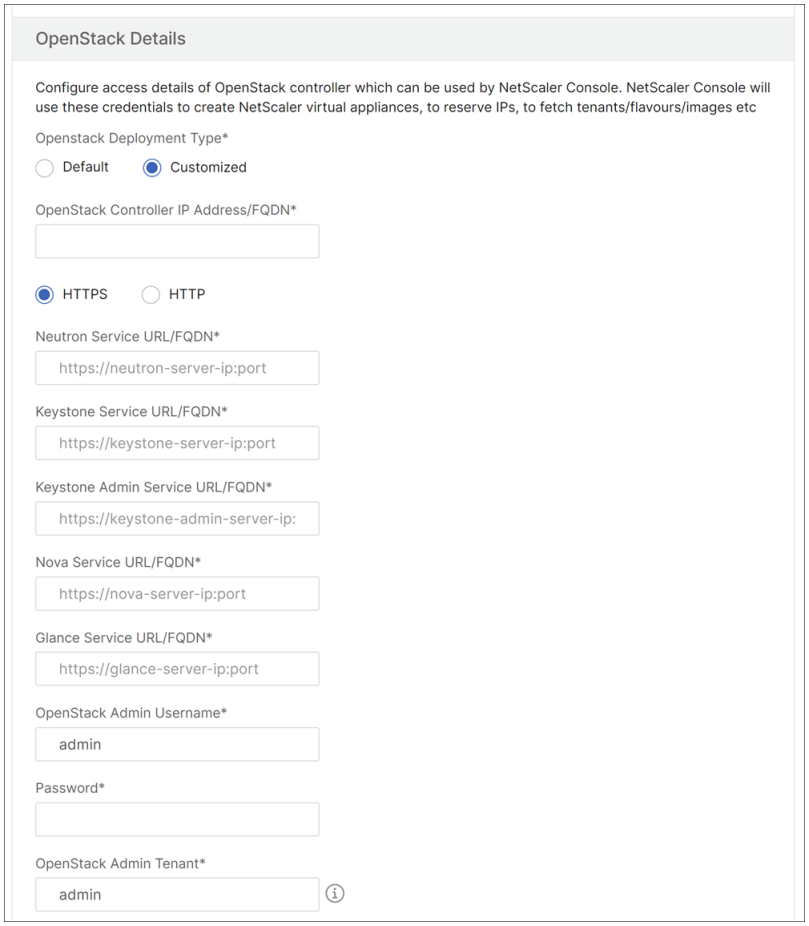
1. Citrix ADM で、［オーケストレーション］>［クラウドオーケストレーション］> ［OpenStack**］ に移動し ます。
2.「**OpenStack** の設定を設定」をクリックします。
3.「**OpenStack** 設定の構成」ページでは、Citrix ADM で OpenStack を設定するためのパラメータを設定できます。［Default］と［Customized］の 2 つのオプションがあります。

   OpenStack の Newton リリースと Ocata リリースでは、デフォルトまたはカスタマイズされたデプロイメントタイプを使用できます。ただし、Pike リリースでは、カスタマイズされたデプロイタイプを使用して OpenStack を Citrix ADM に登録する必要があります。

- 既定のデプロイタイプ

  OpenStack サービスがデフォルトポートで実行されている場合は、「デフォルト」を選択します。たとえば、Neutron サービスのデフォルトポートは 9696 で、Keystone サービスのデフォルトポートは 5000 です。

1. OpenStack Controller IP Address - OpenStack コントローラーの IP アドレス（KeyStone サービスと Neutron サービスはどちらもこの IP アドレスで到達可能である必要があります）。たとえば、IP アドレスを「10.102.205.23」と入力します。
2. OpenStack 管理者ユーザー名-OpenStack コントローラーの管理者ユーザー名。たとえば、「admin1」と入力します。
3. Password - OpenStack コントローラーの管理者ユーザーのパスワード。
4. OpenStack 管理テナント-OpenStack 上の管理テナントの名前。たとえば、「admin」と入力します。

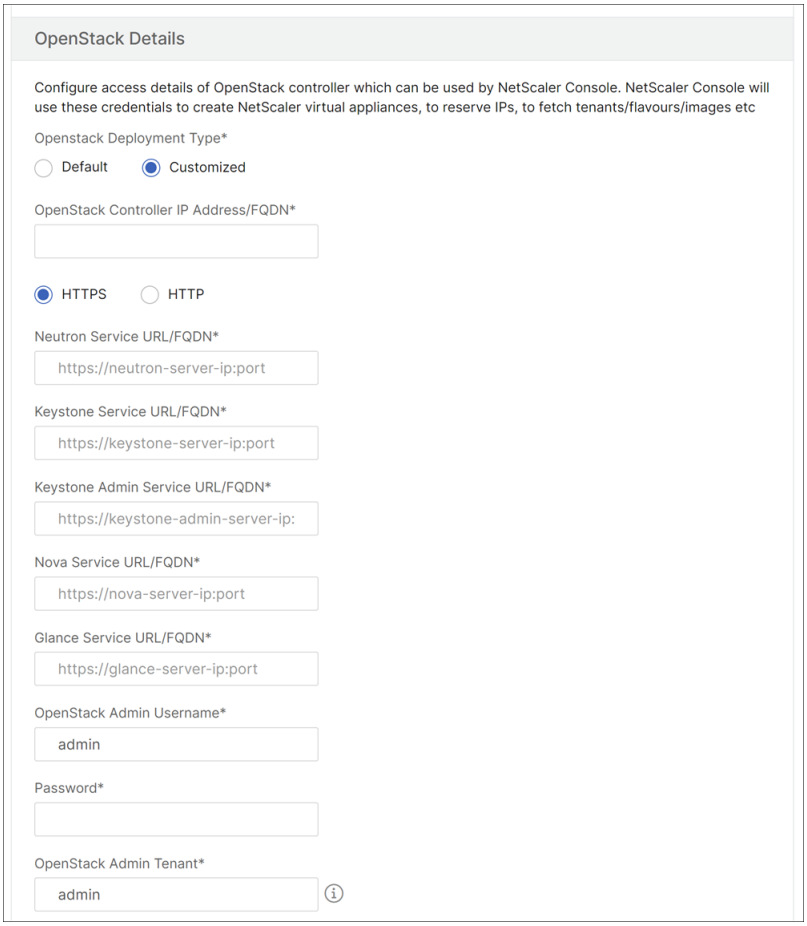


- カスタマイズされた展開の種類

  OpenStack サービスがデフォルトポートと異なるポートで実行されている場合は、デプロイタイプを **Customized** として選択します。サービスが異なるポートで実行されている場合は、ここでそのポートを指定します。OpenStack Newton および Ocata リリースを Citrix ADM に登録することは、OpenStack Pike リリースを登録することとは異なります。

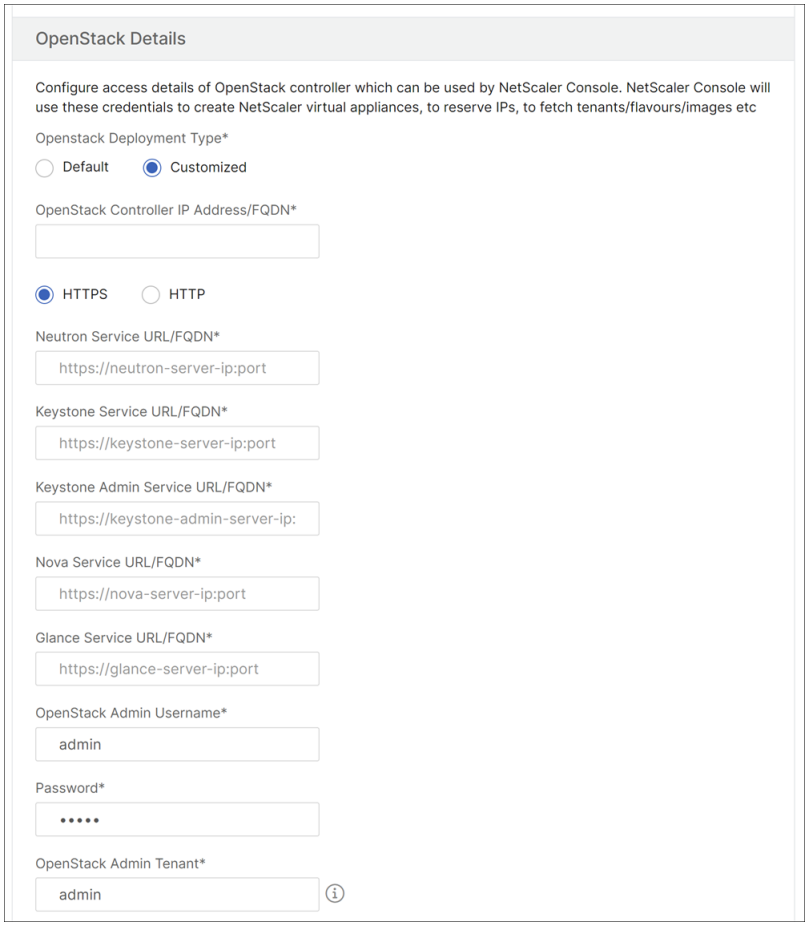
  OpenStack のニュートンとオカタのリリース**:**

  1. OpenStack の Newton リリースを登録する場合は、さまざまな OpenStack サービスのポート番号を指定します。
  2. デフォルト設定で先に指定したように、OpenStack 管理者のユーザー名、パスワード、および OpenStack 管理テナントのユーザー名を指定します。

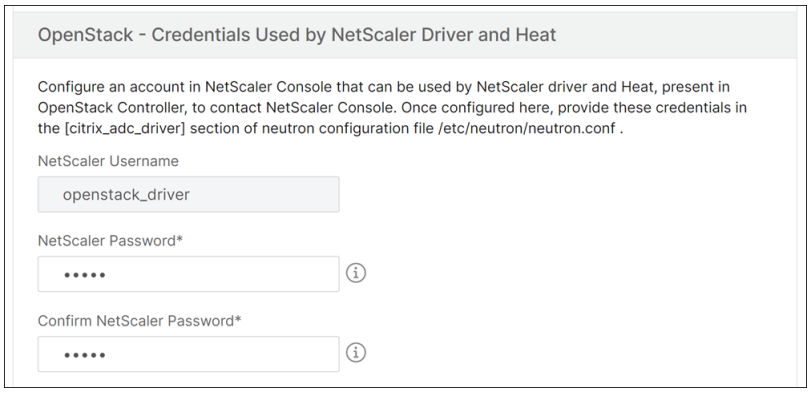


OpenStack の **Pike** リリース:

OpenStack の Pike リリースを登録する場合は、次の図に示すように、OpenStack サービスの詳細を入力します。また、デフォルト設定で OpenStack 管理者のユーザー名、パスワード、OpenStack 管理テナントのユーザー名を指定する必要があります。



1. 「**OpenStack Neutron LBaaS-NetScaler ADC** ドライバーが使用する資格情報」セクションで、OpenStack NetScaler ADC ドライバーのユーザーアカウントの NetScaler ADC ドライバーのパスワードを設定します。NetScaler ADM は、これらの資格情報を使用して、OpenStack NetScaler ADC ドライバーからの呼び出しを認証します。OpenStack コントローラーで Citrix ADC ドライバーインストールスクリプトを実行するときは、同じパスワードを指定する必要があります。



2. [**OK**] をクリックします。

OpenStack でのテナントの作成

OpenStack にプロジェクトまたはテナントを作成し、そのプロジェクトまたはテナントにユーザーを追加し、すべてのユーザーに役割を割り当てます。OpenStack の ID サービスである KeyStone が、OpenStack サービスごとに認証サービスを提供します。KeyStone 認証サービスでは、ドメイン、プロジェクト（テナント）、ユーザー、および役割の組み合わせを使用します。

OpenStack でプロジェクトを作成する方法や、他のタスクを実行する方法の詳細については、にある OpenStack のドキュメントを参照してください。http://docs.openstack.org/

OpenStack テナントの追加

1. Citrix ADM で、「オーケストレーション」>「クラウドオーケストレーション」>「**OpenStack**」>「**OpenStack** テナント 」に移動し、「追加」をクリック します。
2. ［**Add OpenStack Tenants**］ページで［**+Add**］をクリックして、OpenStack テナントを選択します。
3. ［**OK**］をクリックします。

OpenStack を統合するときに、事前プロビジョニングされたインスタンスと自動プロビジョニングされたインスタンスのどちらを使用するのかに応じて、次のどちらかのタスクを実行します。

- NetScaler ADC デバイスの事前プロビジョニング
- OpenStack でのネットスケーラー VP X デバイスの自動プロビジョニング

NetScaler ADC デバイスのプロビジョニング

OpenStack を統合するときに、事前プロビジョニングされたインスタンスと自動プロビジョニングされたインスタンスのどちらを使用するのかに応じて、次のどちらかのタスクを実行します。

- NetScaler ADC デバイスの事前プロビジョニング
- OpenStack でのネットスケーラー VP X デバイスの自動プロビジョニング

NetScaler ADC デバイスの事前プロビジョニング

Citrix ADC デバイスを Citrix Hypervisor、KVM、ESX などの任意のハイパーバイザープラットフォームにインストールし、そのインスタンスを Citrix ADM に追加します。次に、NetScaler ADM がこのデバイスを管理し、サーバーのトラフィックを負荷分散します。

既存の **Citrix ADC VPX** インスタンスを **Citrix ADM** に追加するには：

1. Citrix ADM で、［インフラストラクチャ］>［インスタンス］>［**Citrix ADC VPX**］に移動し、［追加］をクリック します。

2. ［**Citrix ADC VPX** の 追加］ページで、Citrix ADC VPX インスタンスの IP アドレスを指定し、［プロファイル名 ］リストからインスタンス プロファイルを選択します。インスタンスプロファイルには、Citrix ADC VPX へのログオンに使用される認証情報が含まれています。［+］アイコンをクリックして新規のインスタンスプロファイルを作成することもできます。[**OK]** をクリックします。

Citrix ADC デバイスの自動プロビジョニング

Citrix ダウンロードページから必要な Citrix ADC インスタンスイメージをダウンロードし、OpenStack イメージングサービスの Glance にアップロードします。Glance でイメージを利用できるようにすると、テナントにインスタンスを割り当てるときに、Citrix ADC インスタンスをオンデマンドで構成できます。

Citrix ADC VPX デバイスを **OpenStack** に自動プロビジョニングするには:

1. Citrix ADM で、［オーケストレーション］>［クラウドオーケストレーション］>［OpenStack**］に移動します。
2. 「デプロイ設定」をクリックします。
3. 次のパラメーターを設定します。

   a) 管理ネットワーク-自動プロビジョニングされた Citrix ADC VPX が接続されている OpenStack 上の管理ネットワークを選択します。

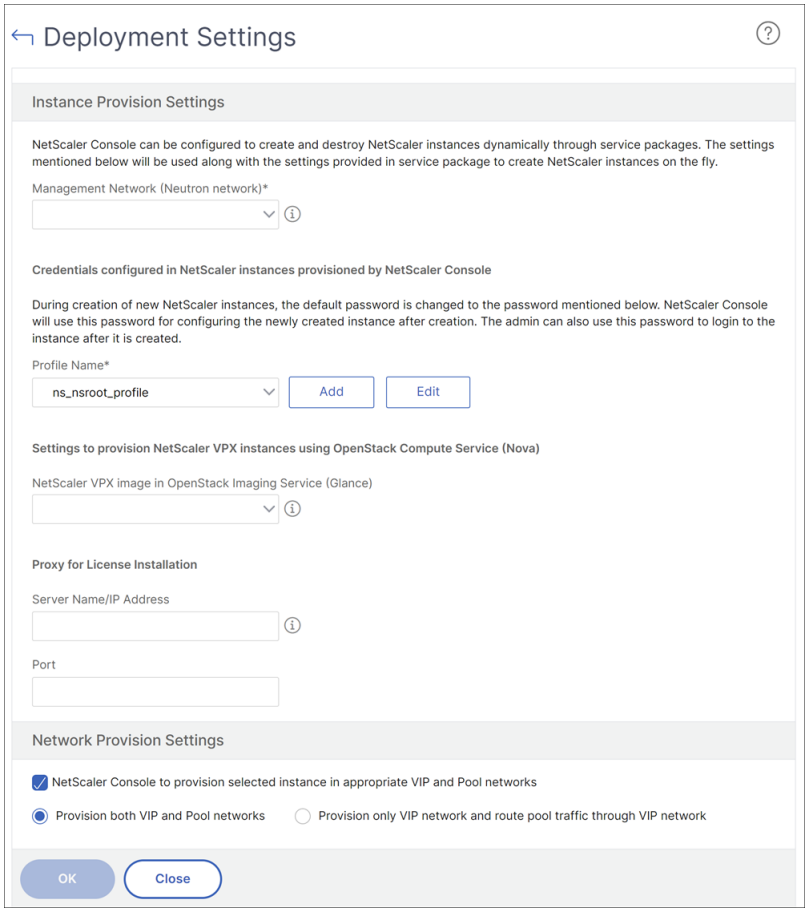
   b) Profile Name - ボックスの一覧からプロファイルを選択します。NetScaler ADM は、このプロファイルに含まれているパスワードを使用して、新しい自動プロビジョニングされた NetScaler ADC VPX インスタンスを構成します。

   c) ライセンス-新しい自動プロビジョニングされた Citrix ADC インスタンスのライセンス認証に使用される Citrix ADM ライセンスアクティベーションコード（LAC）を提供します。NetScaler ADM は、管理ネットワーク内の OpenStack コンピューティング上の NetScaler ADC インスタンスをプロビジョニングし、指定されたライセンスコードを使用してライセンスのインストールをトリガーします。次に、Citrix ADC インスタンスは、ここで指定した LAC を使用して Citrix Web サイトからライセンスファイルをダウンロードします。

   d) NetScaler ADC VPX イメージの概要-NetScaler ADC VPX インスタンスの作成に使用される OpenStack Glance で使用できる NetScaler ADC VPX イメージを選択します。

   e) プロキシ設定-ライセンスをインストールするための Citrix ADC プロキシサーバーの詳細を指定します。これは、Citrix ADC が管理ネットワーク経由でインターネットに直接アクセスできない場合に必要になることがあります。

4. [**OK]** をクリックします。



NetScaler ADM でのサービスパッケージの作成

Citrix ADM でテナント用のサービスパッケージを作成するには:

1. Citrix ADM で、［オーケストレーション］>［クラウドオーケストレーション］>［OpenStack**］**>**［**** サービスパッケージ］に移動し、［追加］をクリックします。
2. 「サービスパッケージ」ページで、次のパラメータを指定します。
   a) Name - サービスパッケージの名前。たとえば、「SVC-PKG-GOLD」と入力します。
   b) Citrix ADC インスタンス割り当て-サービスパッケージで定義されているインスタンス割り当てのタイプで、これに基づいて Citrix ADC インスタンスリソースがテナントに割り当てられます。[専用] を選択します。ポリシーの詳細については、「サービスパッケージ分離ポリシー」を参照してください。
   c) NetScaler ADC インスタンスのプロビジョニング: ［既存のインスタンス］を選択して、既存の NetScaler ADC インスタンスをテナントに割り当てます。構成中に Citrix ADC インスタンスを作成する場合は、「オンデマンドでインスタンスを作成」を選択します。
   d) Citrix ADC インスタンスタイプ- **Citrix ADC VPX** を選択します。

> 注
>
> :SDX プラットフォームでホストされている事前にプロビジョニングされた Citrix ADC インスタンスを割り当てるには、Citrix ADC VPX を選択します。

3. [続行] をクリックして、テナントをサービスパッケージに関連付けます。

> 注
>
> : **Citrix ADC** インスタンス を高可用性モードでデプロイする場合は、高可用性のために Citrix ADC インスタンス のプロビジョニングペアを有効にします。

4.「インスタンスの割り当て」セクションで、「追加」をクリックし、テナントに割り当てる Citrix ADC インスタンスを選択して、「続行」をクリックします。

5.「**OpenStack** テナント**/**プレイスメントポリシーの割り当て」セクションの「**OpenStack** テナント」で、「追加」をクリックしてテナントを選択します。

6.［**Continue**］、［**Done**］の順にクリックします。

> 注:
>
> ポリシーが見つからない場合、フォールバックメカニズムが復活し、NetScaler ADM はテナントに基づいて NetScaler ADC インスタンスを割り当てます。テナントがどのサービスパッケージにも含まれていない場合、NetScaler ADM は次のエラーメッセージを表示します。「テナント\ <admin\ > はどのサービスパッケージにも含まれておらず、デフォルトのサービスパッケージもありません。

配置ポリシーの作成（オプション）

分離ポリシーはテナントベースだけではありません。柔軟な配置ポリシーを作成することもできます。このポリシーは、テナント名またはテナント ID だけでなくその他のカスタム属性にも基づきます。

Citrix ADM でテナントの配置ポリシーを作成するには:

1. Citrix ADM で、［オーケストレーション］>［クラウドオーケストレーション］>［OpenStack**］**>**［**** 配置ポリシー］に移動し、［追加］をクリックします。

2.［**Add Placement Policy**］ページで、次のパラメーターを設定します。

   a) Name - 配置ポリシーの名前を入力します。

   b) Sample Expressions - 一覧から式のサンプルを選択します。これらのサンプルは、配置ポリシーを作成するのに役立ちます。

   c) Expression - このボックスには、前のボックスで選択したサンプル式に基づいて、ブール式を入力します。必要に応じてボックス名を編集します。

3.［**OK**］をクリックします。

Citrix ADC インスタンスからクライアントネットワーク経由でバックエンドサーバーへのトラフィックを有効にする

デフォルトでは、OpenStack オーケストレーションワークフローでは、NetScaler ADC インスタンスはロードバランサーまたはクライアントネットワーク、メンバーまたはサーバーネットワークに動的にバインドされます。

一部のデプロイメントでは、クライアントネットワーク経由でサーバーにアクセスでき、クライアントゲートウェイ経由でルーティングすることもできます。このような場合、Citrix ADC インスタンスをサーバーネットワークにバインドする必要はなく、クライアントネットワークにのみバインドする必要があります。

クライアントゲートウェイ経由のトラフィックを設定するには、次の設定を行います。

[オーケストレーション] > [クラウドオーケストレーション] > [**OpenStack**] > [デプロイ設定] に移動し、[VIP ネットワークのみをプロビジョニングし、**VIP** ネットワーク経由でプールトラフィックをルーティングする] オプションを選択します。

次に、Citrix ADM は、クライアントネットワークに SNIP を追加して Citrix ADC インスタンスをクライアントネットワークに構成し、さらにクライアントネットワークゲートウェイにデフォルトルートを追加します。これにより、インスタンスはクライアントゲートウェイを介してサーバーに到達できます。

Citrix ADC SDX プラットフォームにデプロイされた **Citrix ADC VPX** デバイスの自動プロビジョニング

Citrix ADM に Citrix ADC SDX プラットフォームを追加して、Citrix ADM がこのプラットフォーム上のインスタンスをオンデマンドでプロビジョニングできるようにします。

NetScaler ADC SDX プラットフォームにデプロイされた **NetScaler ADC** インスタンスを自動プロビジョニングするには:

1. Citrix ADM GUI で、［ネットワーク］ > ［インスタンス］ > ［**Citrix ADC SDX**］に移動し 、［追加］をクリック して Citrix ADC SDX プラットフォームを追加します。
2. [オーケストレーション] > [クラウドオーケストレーション] > [**OpenStack**] > [デプロイ設定**]** に移動します。
3. 管理ネットワーク セクションで 、自動プロビジョニングされた Citrix ADC SDX が接続されている OpenStack 上の管理ネットワークを選択します。
   a)「プロファイル名」で、ドロップダウンリストからプロファイルを選択します。NetScaler ADM は、このプロファイルに含まれているパスワードを使用して、新しい自動プロビジョニングされた NetScaler ADC VPX インスタンスを構成します。
   b) [**OK]** をクリックします。
4. Citrix ADC SDX プラットフォームを OpenStack でプロビジョニングするには、[オーケストレーション] > [クラウドオーケストレーション] > **[**OpenStack****] > [**サービスパッケージ ******] に移動し ます。
   a) [追加] をクリックして新しいサービスパッケージを作成します。

b) サービスパッケージの名前を入力します。

c) **Citrix ADC** インスタンス割り当て フィールドで、「専用」を選択 します。

d)「**Citrix ADC** インスタンス **Provisioning** 」フィールドで 「インスタンスをオンデマンドで作成」を選択 し、「自動プロビジョニングプラットフォーム」 フィールドで「**Citrix ADC SDX**」を選択 します。

e) デフォルトでは、Citrix ADC VPX インスタンスのみが Citrix ADC SDX プラットフォームにプロビジョニングされます。

f) [続行] をクリックします。

g) 自動プロビジョニング設定セクションで、リソースプロパティを設定します。

i. スループットフィールド。「1000 Mbps」と入力します。

ii. **NetScaler ADC** バージョン］フィールド。リストから、NetScaler ADC SDX プラットフォームに存在する NetScaler ADC VPX イメージの適切なバージョンを選択します。コマンドラインを使用した LBaaS V2 の設定

h) ［**NetScaler ADC SDX** プラットフォーム］セクションで、［追加］をクリックして SDX プラットフォームをサービスパッケージに追加します。

i) [続行] をクリックします。

j)「**OpenStack** テナントの設定」セクションで、「追加」をクリックしてテナントを追加します。[新規] をクリックして新しいテナントを追加することもできます。

k)「完了」をクリック します。

5. LBaaS V2 API を実装するには、Neutron LBaaS コマンドを使用します。いずれかの Neutron クライアントに接続して構成タスクを実行します。設定コマンドの実行方法の詳細については、「コマンドラインを使用した LBaaS V2 の設定」を参照してください。

Horizon を使用した **LBaaS V1** の設定

February 6, 2024

これでトムは、OpenStack Horizon ポータルにログオンして LBaaS プールを作成し、このプールのすべてのメンバーが存在するサブネットを選択できるようになりました。トムは仮想 IP（VIP）アドレスを追加して、自分で作成したプールに割り当てる必要があります。この操作は、コマンドラインまたは API 経由でも実行できます。トムのサーバーの外部クライアントは、割り当てられた Citrix ADC でホストされているこの VIP アドレスに接続でき、Citrix ADC はすべての要求を構成されたポート上のプールメンバーに配信します。

LBaaS プールメンバーは、選択したプールに追加される負荷分散サーバー群です。トムは、これらの各メンバーに重要度とポートを割り当てることができます。

ヘルスモニターを使用して、プールのすべてのメンバーのヘルス状況と機能状態を監視します。トムは、OpenStack 内にサーバーヘルス監視用テンプレートを作成できます。テンプレートには、遅延、タイムアウト、リトライ回数、メソッド、URL パス、成功時に返される HTTP コードを指定します。モニターを作成したら、トムはそのモニターを、作成済みのプールと関連付ける必要があります。

OpenStack でプールやその他の LBaaS 設定タスクを作成する方法の詳細については、OpenStack ドキュメントを参照してください。

> 重要
>
> OpenStack の Liberty リリースでは、LBaaS V1 はサポートされません。詳細については、「OpenStack リリースノート」を参照してください。

コマンドラインを使用した **LBaaS V2** の設定

February 6, 2024

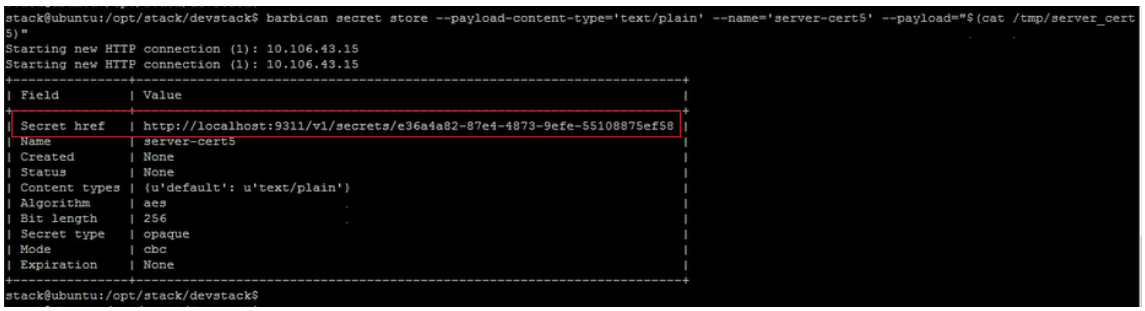
LBaaS V2 は、通常の負荷分散機能に加えて、Barbican で管理される証明書を使用した SSL オフロード、証明書パッケージ（中間認証機関を含む）、および SNI サポートに対応しています。LBaaS V2 では、構成タスクを実行するためのコマンドラインインターフェイスのみがサポートされます。LBaaS V2 API を実装するには、Neutron LBaaS コマンドを使用します。

> 注
>
> SSL オフロード機能が必要な場合は、証明書とキーを Barbican サービスにアップロードします。手順 1、2、3 は、SSL オフロードがサポートされている場合に実行してください。それ以外の場合は、手順 4から作業を続行して、ロードバランサー、リスナー、プール、メンバーを作成してください。

1. 次のコマンドを使用して Barbican サービスに証明書をアップロードします。

   barbican secret store –payload-content-type < コンテンツタイプ > --name < 証明書の名前 > --payload< 証明書の場所 > 証明書の場所 > 証明書の名前 > コンテンツタイプ >

   例: barbican secret store –payload-content-type=’ text/plain’ –name=’ hp_server_certificate’ –payload=” hp_server/tmp/server_certificate”



2. 次のコマンドを使用して、キーを Barbican サービスにアップロードします。

   barbican secret store –payload-content-type < コンテンツタイプ > --name < キーの名前 > --payload< キーの場所 > キーの場所 > キーの名前 > コンテンツタイプ >

   例：barbican secret store –payload-content-type='text/plain'–name='shp_server_key'–payload='' hp-server/tmp/server_key''

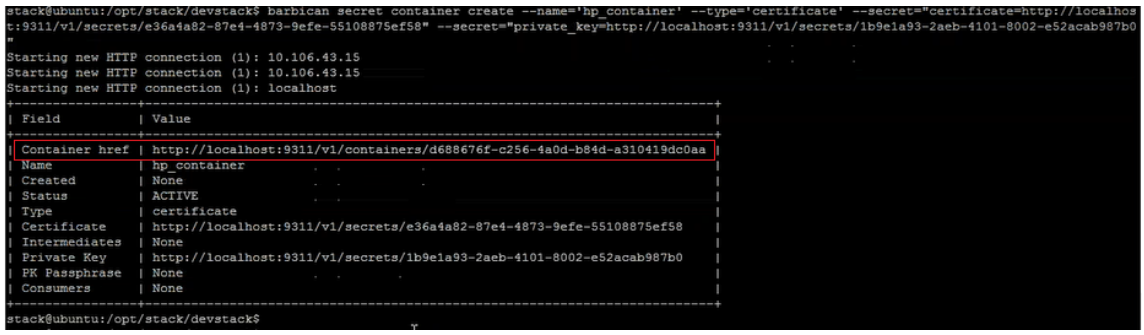
> 注
>
> 上記の 2 つの Barbican コマンドを実行して証明書とキーをロードすると、Secret href フィールドに場所または URL が表示されます。証明書とキーは、OpenStack がインストールされているシステムのこの場所に保存されます。手順 3 で Barbican サービスにコンテナを作成するときは、これらのリンクをコピーして、パラメーターとして指定します。

3. 次のコマンドを使用して、証明書とキーを保存するコンテナーを Barbican サービス内に作成します。

   このコマンドの < 証明書の URL> を、証明書のアップロード時に Secret href フィールドから取得した URL に置き換えます。同様に、< キーの URL> を、キーをアップロードするときに Secret href フィールドから取得した URL に置き換えます。キーの URL> 証明書の URL>

   barbican secret container create –name< コンテナの名前 > --type< コンテナのタイプ > --secret< 証明書の URL> --secret< キーの URL> キーの URL> 証明書の URL> コンテナのタイプ > コンテナの名前 >

   例: バービカン・シークレット・コンテナの作成–name='hp_container'–type='certificate'–secret="certificate=http://localhost:9311/v1/secrets/e36a4a82-87e4-4873-9efe-55108875ef58 --secret="private_key=http://localhost:9311/v1/secrets/1b9e1a93-2aeb-4101-8002-e52acab987b0



Container href の値をコピーします。手順 6 でリスナーを作成するときに、このリンクをコンテナに指定する必要があります。

4. OpenStack で環境変数を設定します。これらの変数を設定すると、OpenStack クライアントコマンドが OpenStack サービスと通信できるようになります。

   例:

   export OS_PASSWORD-hp

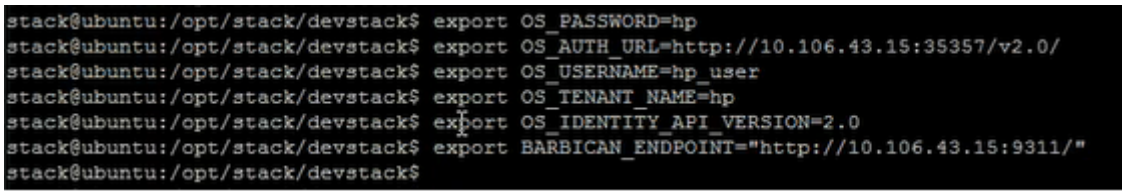
   export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/

   export OS_USERNAME=hp_user

   export OS_TENANT_NAME=hp

   export OS_IDENTITY_API_VERSION=2.0

   export BARBICAN_ENDPOINT=" http://10.106.43.15:9311/"

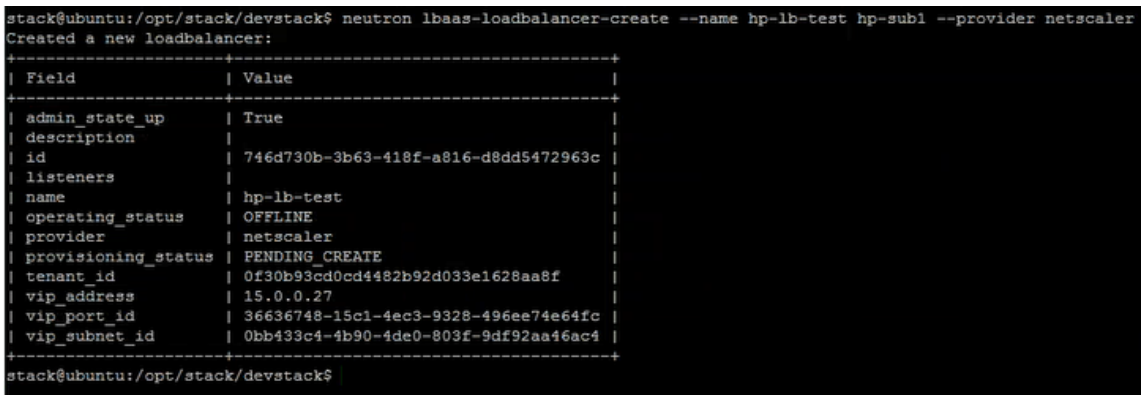


> 注
>
> ほかのコマンドを実行する前に、これらの変数を SSH セッションごとに設定します。OpenStack の環境変数について詳しくは、OpenStack の環境変数に関するドキュメントを参照してください。

5. 次のコマンドを使用してロードバランサーを作成します。

   <loadbalancer-name\ > <subnet-name\ >neutron lbaas-ロードバランサー-作成–name\\–provider\ <netscaler\ >

   例: neutron lbaas-loadbalancer-create –name hp-lb-test hp-sub1 –provider netscaler



   ロードバランサーが正常に作成されると、状態が PENDING_CREATE から ACTIVE に変わります。


```
+--------------------------------------+------------+-------------+---------------------+-----------+
| id                                   | name       | vip_address | provisioning_status | provider  |
+--------------------------------------+------------+-------------+---------------------+-----------+
| 0d5e8e17-41c2-41bb-aab5-2b3f8f5af4c5 | hp-lb8     | 15.0.0.25   | ACTIVE              | netscaler |
| 1092f752-aa25-4262-aacc-014725fe2921 | hp_lb3     | 15.0.0.19   | ACTIVE              | netscaler |
| 41dbe490-6d9c-4ce5-8d88-bb55953f5961 | hp-lb7     | 15.0.0.24   | ACTIVE              | netscaler |
| 746d730b-3b63-418f-a816-d8dd5472963c | hp-lb-test | 15.0.0.27   | ACTIVE              | netscaler |
| 9d65f6a4-5be5-44fd-a4bd-0808084557b0 | hp-lb1     | 15.0.0.18   | ACTIVE              | netscaler |
| cf8ee4b7-a9f5-41c5-a76a-cd2520e0a7a3 | hp-lb6     | 15.0.0.23   | ACTIVE              | netscaler |
| f7f7dd6e-28eb-40f2-b26c-e541138c6a06 | hp-lb4     | 15.0.0.20   | ERROR               | netscaler |
+--------------------------------------+------------+-------------+---------------------+-----------+
```

6. 以下のコマンドを使用してリスナーを作成します。

   neutron lbaas-listener-create –loadbalancer < ロードバランサーの名前 > --name < リスナーの名前 > --protocol < プロトコルのタイプ > --protocol-port < ポート番号 > --default-tls-container-id< コンテナの URL> コンテナの URL> ポート番号 > プロトコルのタイプ > リスナーの名前 > ロードバランサーの名前 >

   例: neutron lbaas-listener-create–name hp-lb-test-list –loadbalancer hp-lb-test–protocol TERMINATED_HTTPS–protocol-port 443–default-tls-container-id `http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa`

   > 注
   >
   > SSL オフロードをサポートしないリスナーを作成する場合は、コンテナの場所を指定せずに、次のコマンドを実行します。
   >
   > neutron lbaas-listener-create –loadbalancer < ロードバランサーの名前 > --name < リスナーの名前 > --protocol < プロトコルのタイプ > --protocol-port < ポート番号 > ポート番号 > プロトコルのタイプ > リスナーの名前 > ロードバランサーの名前 >

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-listener-create --name hp-lb-test-list --loadbalancer hp-lb-test --protocol TERMINATED_HTTPS --prot
ocol-port 443 --default-tls-container-id http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa
Created a new listener:
+-------------------------+--------------------------------------------------------------------------------+
| Field                   | Value                                                                          |
+-------------------------+--------------------------------------------------------------------------------+
| admin_state_up          | True                                                                           |
| connection_limit        | -1                                                                             |
| default_pool_id         |                                                                                |
| default_tls_container_id | http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa |
| description             |                                                                                |
| id                      | 734a0361-153d-4983-bc2c-55a3ec2ff6fb                                           |
| loadbalancers           | {"id": "746d730b-3b63-418f-a816-d8dd5472963c"}                                 |
| name                    | hp-lb-test-list                                                                |
| protocol                | TERMINATED_HTTPS                                                               |
| protocol_port           | 443                                                                            |
| sni_container_ids       |                                                                                |
| tenant_id               | 0f30b93cd0cd4482b92d033e1628aa8f                                               |
+-------------------------+--------------------------------------------------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

7. 次のコマンドを使用してプールを作成します。

   neutron lbaas-pool-create –lb-algorithm < アルゴリズムのタイプ > --listener < リスナーの名前 > --protocol < プロトコルのタイプ > --name < プールの名前 > プールの名前 > プロトコルのタイプ > リスナーの名前 > アルゴリズムのタイプ >

   例: neutron lbaas-pool-create –lb-algorithm LEAST_CONNECTIONS –listener demolistener –protocol http –name demopool


```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-pool-create --lb-algorithm ROUND_ROBIN --listener hp-lb-test-list --protocol HTTP --name hp-lb-test
-pool
Created a new pool:
+---------------------+----------------------------------------------+
| Field               | Value                                        |
+---------------------+----------------------------------------------+
| admin_state_up      | True                                         |
| description         |                                              |
| healthmonitor_id    |                                              |
| id                  | 714c44d0-5cf7-4ef8-b84d-f6d3a258c770         |
| lb_algorithm        | ROUND_ROBIN                                  |
| listeners           | {"id": "734a0361-153d-4983-bc2c-55a3ec2ff6fb"} |
| members             |                                              |
| name                | hp-lb-test-pool                              |
| protocol            | HTTP                                         |
| session_persistence |                                              |
| tenant_id           | 0f30b93cd0cd4482b92d033e1628aa8f             |
+---------------------+----------------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

8. 次のコマンドを使用してメンバーを作成します。

   neutron lbaas-member-create –subnet < サブネットの名前 > --address --protocol-port < ポート番号 > < プールの名前 > プールの名前 > ポート番号 > サブネットの名前 >

   例: neutron lbaas-member-create –subnet hp-sub1 –address 15.0.0.15 –protocol-port 80 hp-lb-test-pool

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15 --protocol-port 80 hp-lb-test-pool
Created a new member:
+----------------+--------------------------------------+
| Field          | Value                                |
+----------------+--------------------------------------+
| address        | 15.0.0.15                            |
| admin_state_up | True                                 |
| id             | ced7a563-5ecc-474f-8d2a-cb69923215b0 |
| protocol_port  | 80                                   |
| subnet_id      | 0bb433c4-4b90-4de0-803f-9df92aa46ac4 |
| tenant_id      | 0f30b93cd0cd4482b92d033e1628aa8f     |
| weight         | 1                                    |
+----------------+--------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

NetScaler ADM での OpenStack アプリケーションの監視

テナントは、OpenStack の認証情報を使用して NetScaler Application Delivery Management（ADM）にログオンし、OpenStack から作成された VIP とプールを任意のブラウザーから監視できます。URL は以下の形式で指定する必要があります。

http://\<mas_ip\>/\<admin_ui\>/mas/ent/html/cc_tenant_main.html

ここで <mas-ip-address>、は OpenStack に登録されている Citrix ADM IP アドレスです。

> 注
>
> - OpenStack VIP は Citrix ADM の仮想サーバーに対応しています。
> - オープンスタックプールは、Citrix ADM のサービスグループに対応しています。
> - OpenStack プールのメンバーは、NetScaler ADM のサービスグループメンバーに対応しています。

レイヤ 7 コンテンツスイッチングの構成

February 6, 2024

Citrix Application Delivery Management（ADM）は OpenStack と連携して、Citrix ADC インスタンスのレイヤー 7（L7）スイッチングまたはコンテンツベースのスイッチング機能を設定します。コンテンツスイッチは、指定した種類の要求を指定のサーバーに送信できるという点で単純な負荷分散とは異なります。Citrix ADC インスタンスをプロバイダーとして使用して OpenStack で L7 構成を作成すると、Citrix ADM は Citrix ADC インスタンスを割り当て、L7 構成に対応するコンテンツスイッチング構成とレスポンダー構成を展開します。その後、Citrix ADC インスタンスは、要求のアプリケーション層の特性に基づいてユーザー要求を分散し、負荷分散することができます。

OpenStack のレイヤー 7（L7）負荷分散機能では、負荷分散とコンテンツスイッチを組み合わせることで特定の種類のコンテンツを最適に配信できます。この機能ではコンテンツに適用可能なポリシーのみが実行されるようになり、ロードバランサーのパフォーマンスが改善されます。レイヤー 7 負荷分散では、アプリケーションインフラストラクチャの効率も向上できます。タイプ、URI、データに応じてコンテンツを分離できるため、アプリケーションインフラストラクチャへの物理リソースの割り当てを改善できます。たとえば、をブラウジングする`http://example-sports.com/about-us`エンドユーザーには、会社とサービスに関するコンテンツをホストするサーバーのプールからサービスを提供し、ブラウジングする`http://example-sports.com/shopping-cart-football`ユーザーには、ユーザーがオンラインで購入できる別のサーバープールがサービスを提供する必要があります。

L7 スイッチでは、ロードバランサーは、ユーザーからの HTTP 要求を受け付けてアプリケーションサーバーに配信するコンテンツスイッチ仮想サーバーとして実装されます。L7 スイッチまたはコンテンツスイッチでは、Web アプリケーションや Web サービスポータル、Web メールだけでなく、モバイル管理や異なる言語のコンテンツなども含むさまざまなバックエンドサービスにアクセス可能な単一のエントリポイントを設定できます。つまり、1 つのパブリック IP アドレスで、ユーザーに提供するサービスすべてに対応できるということです。

低レベルの負荷分散とは異なり、レイヤー 7 スイッチではプール内の全サーバーのコンテンツを同じにする必要はありません。L7 スイッチを使用するロードバランサーの構成では、アプリケーションサーバーまたはバックエンドサーバーとプールのコンテンツを違うものにする必要があります。L7 スイッチでは、URI やホスト、HTTP ヘッダーなど、アプリケーションメッセージに含まれるあらゆる要素を基に要求を送信できます。アプリケーションサーバーは、基本的に特定の種類のコンテンツのみを提供する必要があります。たとえば、あるサーバーでは画像のみ供給し、別のサーバーでは PHP や ASP などのサーバー側スクリプト言語を実行させ、さらに別のサーバーでは HTML、CSS、JavaScript などの静的コンテンツを供給するようにします。

L7 の規則

トラフィックの評価規則では以下の属性が定義されており、規則で定義されている値と比較されます。

- hostname：HTTP 要求のホスト名が、規則のこの値パラメーターと比較されます（「www.example-sports.com」など）。

- path：HTTP URI のパス部分が、規則のこの値パラメーターと比較されますたとえば、「www.example-sports.com/shopping-cart/football_pump.html」
- file_type：HTTP URI の最後の部分が、規則のこの値パラメーターと比較されます（txt、html、jpg、png、xls など）。
- header：キーパラメーターで定義されているヘッダーが、規則のこの値パラメーターと比較されます。
- cookie：キーパラメーターで指定されている Cookie が、規則のこの値パラメーターと比較されます。要求ヘッダーフィールドの Cookie 値には、該当する URL に格納されている情報の名前と値のペアが含まれています。一般的な構文は「Cookie: 名前 = 値」です。たとえば、値が「football-」で始まる「stores」という名前のクッキーを検索するルールは、「type = Cookie、compare_type=startsWith」、「key = storesvalue = football-」のようになります。

比較型

トラフィックの評価時には、L7 ポリシーにより以下の式と規則で定義されている値が比較されます。

- regex：Perl 型の正規表現マッチング
- starts_with：次で始まる文字列
- ends_with：次で終わる文字列
- contains：次を含む文字列
- equal_to：次に等しい文字列

> 注
>
> : ホスト名、パス、ヘッダー、および Cookie 属性はすべての比較タイプをサポートしますが、file_type 属性は regex と equal_to のみをサポートします。

L7 ポリシー

L7 ポリシーは受信 HTTP トラフィックを処理し、このポリシーで定義されているすべての規則が満たされている場合「true」を返します。

すべての L7 ポリシーで、規則はすべて AND 演算子により論理的に結合されます。要求はすべての規則を満たす必要があり、すべての規則が満たされた場合ポリシーは「true」値を返します。ロードバランサーが実行するアクションは、ポリシーから返される値に基づきます。アクションが同じ 2 つ目のポリシーを作成し、規則どうしで論理 OR 演算を行うことができます。

たとえば、単語「EXAMPLE-SPORTS」、「SPORTS-FOOTBALL」、または「EXAMPLE-FOOTBALL」を含む受信 HTTP 要求を許可するポリシーを作成し、ロードバランサーには、適切なアクションとして、要求されたコンテンツを提供する E コマース企業である Example-sports のサーバープールにこれらの要求を転送させるとします。同じ

アクションを実行するものの「example-sports」、「example-sports-football」、「example-football」とのマッチングを行う別のポリシーを作成します。ユーザーがこれら 6 個のキーワードのいずれかを含む HTTP 要求を送信すると、ロードバランサーはその要求を Example-Sports サーバーに転送します。

ポリシーの定義規則に応じて、L7 ポリシーでは以下のアクションのいずれかを行うことができます。

- プールへのリダイレクト - L7 ポリシーに関連付けられた規則で指定されているアプリケーションサーバープールに要求を転送します。これにより、ドメイン名に応じて要求を特定のロードバランサープールに送信するアプリケーション規則を作成できます。たとえば、example-football.com に対する要求を pool_1 に、example-sports-online_purchase.com に対する要求を pool_2 に送信するルールを作成できます。
- URL へのリダイレクト - クライアントを、Location 応答ヘッダーに新しい場所が設定されたリダイレクト HTTP 応答に送信します。Web ブラウザーのアドレスバーはこの新しい場所で更新され、新しい要求が発行されます。このアクションの使用例は多岐にわたります。たとえば、Web サイトのアドレスが変更された場合、ドロップを行うことなく要求を新しいアドレスにリダイレクトすることができます。また、Web サイトのメンテナンス中にユーザーを読み取り専用のサイトにリダイレクトすることも可能です。
- 拒否 - 要求を拒否し、それ以上のアクションを行いません。たとえば、401 Unauthorized 応答を返して、制限付き Web ページへのユーザーのアクセスを拒否することができます。

コンテンツスイッチの構成には、コンテンツスイッチ仮想サーバー、負荷分散仮想サーバーとサービスから成る負荷分散セットアップ、およびコンテンツスイッチポリシーが含まれます。コンテンツスイッチ仮想サーバーとコンテンツスイッチポリシーの作成後、各ポリシーをコンテンツスイッチ仮想サーバーにバインドします。ポリシーをコンテンツスイッチ仮想サーバーにバインドするときには、ターゲットとなる負荷分散仮想サーバーを指定します。要求がコンテンツスイッチ仮想サーバーに到達すると、仮想サーバーはその要求に対して関連するコンテンツスイッチポリシーを適用します。ポリシーの優先順位により、コンテンツスイッチ仮想サーバーにバインドされたポリシーを評価する順序を定義します。

リスナー ID が設定されているプールはすべて、トラフィックの迂回先となるデフォルト仮想サーバープールに割り当てることができます。プールとリスナーのバインドはゆるく、プールは L7 ポリシーの実装でのみリスナーと関連付けられます。プールは、リスナーに関連付けることなくロードバランサーの下に直接作成することもできます。この場合、作成されたプールは「pending_create」状態となります。L7 ポリシーとリスナーのバインドは密接であるため、プールを「active」状態にしてトラフィック要求の受信を開始するには、プール ID を含む L7 ポリシーを作成して実装する必要があります。

1 つのプールを複数の L7 ポリシーで提供できますが、1 つ以上のポリシーが関連付けられている場合プールは「active」のままとなります。最後のポリシーが削除されるとプールは「pending_create」状態に戻り、別のポリシーを作成して関連付けるまでその状態のままとなります。プール自体が削除されると、このプールが受信するはずであった HTTP 要求はすべてデフォルトプールにリダイレクトされます。

OpenStack L7 ポリシーと **Citrix ADC** エンティティ間のマッピング

OpenStack	Citrix ADC エンティティ	説明
REDIRECT_TO_POOL アクションが設定された L7 ポリシー	コンテンツスイッチポリシー > コンテンツスイッチアクション	Citrix ADM は、コンテンツスイッチング仮想サーバーにバインドされ、コンテンツの取得とユーザーへの表示のためのアプリケーションサーバーのターゲットプールを指定するコンテンツ切り替えアクションに関連付けられたコンテンツスイッチングポリシーを作成します。
REDIRECT_TO_URL アクションが設定された L7 ポリシー	レスポンダーポリシー > レスポンダーアクション	Citrix ADM は、コンテンツスイッチ仮想サーバーにバインドされ、ユーザーに表示するターゲット URL を指定するレスポンダーアクションに関連付けられたレスポンダーポリシーを作成します。
REJECT アクションが設定された L7 ポリシー	レスポンダーポリシー > 要求のドロップ	Citrix ADM は、コンテンツスイッチ仮想サーバーにバインドされ、要求をドロップするレスポンダーアクションに関連付けられたレスポンダーポリシーを作成します。

「true」と評価された L7 ポリシーのアクションが「create_pending」状態のプールにトラフィックをリダイレクトする場合、Citrix ADM は指定されたプールを負荷分散仮想サーバーとともに実装します。Citrix ADM は、L7 ポリシーからコンテンツスイッチングポリシーを作成し、対応するコンテンツスイッチアクションを使用して、そのプールに関連付けられた負荷分散仮想サーバーに要求をリダイレクトします。2 つ目の L7 ポリシーが同じプールにリダイレクトされると、Citrix ADM はコンテンツスイッチングポリシーとコンテンツスイッチアクションを作成して、プールに関連付けられている既存の負荷分散仮想サーバーにトラフィックをリダイレクトします。

ポリシーの順位付け

OpenStack での L7 ポリシーの評価は、ポリシーの優先度に従って行われます。デフォルトでは、OpenStack のポリシーは作成された順番に優先度が付けられます。最初に作成されたポリシーが「1」番となり、以降に作成されたポリシーには連続した番号が付けられます。ただし、ポリシーの優先順位を変更し、異なる優先度を割り当てることができます。ポリシーは常に優先度の順番に評価されます。特定の要求に最初に一致したポリシーが、常に最初に実行されます。

ポリシーを作成する場合、以下の点に注意してください。

- 新しいポリシーに既存のポリシーと同じ優先度を割り当てた場合、その優先度は新しいポリシーに設定されます。既存のポリシーの優先度は下がります。必要に応じて、ポリシーの評価順序を維持するために別のポリシーの優先度が下げられることもあります。
- 優先順位を指定せずに新しいポリシーを作成した場合、新しいポリシーはポリシーリストの末尾に追加されます。
- 新しいポリシーを作成し、リストに既に存在するポリシーの数よりも大きい順位を付けた場合、新しいポリシーはリストの末尾に追加されます。つまり、新しいポリシーには、次に利用可能な優先度が常に設定されます。たとえば、優先順位が 1、2、3 のポリシー A、B、C がある場合にポリシーを作成し優先順位として 8 を割り当てると、新しいポリシーの優先順位は 4 になります。
- リストにポリシーを追加するかリストからポリシーを削除すると、ポリシーの優先順位の値は 1 から順に連続して付け直されます。たとえば、優先順位の値が 1、2、3、4 のポリシー A、B、C、D がある場合にリストからポリシー B を削除すると、ポリシー C の優先順位が 2 となり、ポリシー D の優先順位は 3 となります。

Citrix ADM では、優先順位が 1 の csvserver に関連付けられたデフォルトポリシーが常に存在します。このデフォルトポリシーは、指定時点で lbvserver により処理される TCP 接続の数を指定するものです。したがって、対応するレスポンダーポリシーとコンテンツスイッチングポリシーが NetScaler ADC で作成されると、対応する L7 ポリシーの優先度よりも高い優先度が常に割り当てられます。たとえば、優先順位が 1 の L7 ポリシーを評価する場合、優先順位が 2 のコンテンツスイッチポリシーが作成されます。同様に、優先順位が 2 の L7 ポリシーを評価する場合、優先順位が 3 のレスポンダーポリシーが作成されます。

OpenStack では、「reject」ポリシーおよび「redirect_to_url」ポリシーが最初に評価され、その後に「redirect_to_pool」ポリシーが評価されます。NetScaler ADC インスタンスでは、レスポンダーポリシーは常に最初に評価され、リクエストを削除するか、リダイレクトされた Web アドレスをユーザーに提示します。コンテンツスイッチングポリシーは最後に評価されます。通常、コンテンツスイッチポリシーとレスポンダーポリシーが相互に排他的であれば、この評価順により競合が発生することはありません。つまり、2 つの L7 ポリシーの式を同じにしてはならないということです。こうした競合を避けるため、レスポンダーポリシーとコンテンツスイッチポリシーには派生した式を追加する必要があります。たとえば、「sports-football.com」に対する要求をすべて拒否する式と、「example-sports-football.com」に対する要求を許可する別の式を作成してください。要求を拒否するすべてのレスポンダーポリシーを評価リストの先頭に配置し、その後に Web リダイレクト用のレスポンダーポリシー、コンテンツスイッチポリシーの順となるように L7 ポリシーを作成してください。

Citrix ADM では、優先順位が 1 の csvserver に関連付けられたデフォルトポリシーが常に存在します。このデフォルトポリシーは、指定時点で lbvserver により処理される TCP 接続の数を指定するものです。したがって、対応するレスポンダーポリシーとコンテンツスイッチングポリシーが Citrix ADC で作成されると、対応する L7 ポリシーの優先度よりも高い優先度が常に割り当てられます。たとえば、優先順位が 1 の L7 ポリシーを評価する場合、優先順位が 2 のコンテンツスイッチポリシーが作成されます。同様に、優先順位が 2 の L7 ポリシーを評価する場合、優先順位が 3 のレスポンダーポリシーが作成されます。

OpenStack では、「reject」ポリシーおよび「redirect_to_url」ポリシーが最初に評価され、その後に「redirect_to_pool」ポリシーが評価されます。NetScaler ADC では、レスポンダーポリシーは常に最初に評価され、リクエストを削除するか、リダイレクトされた Web アドレスをユーザーに提示します。コンテンツスイッチング

ポリシーは最後に評価されます。通常、コンテンツスイッチポリシーとレスポンダーポリシーが相互に排他的であれば、この評価順により競合が発生することはありません。つまり、2 つの L7 ポリシーの式を同じにしてはならないということです。こうした競合を避けるため、レスポンダーポリシーとコンテンツスイッチポリシーには類似の派生式を追加する必要があります。たとえば、「sports-football.com」に対する要求をすべて拒否する式と、「example-sports-football.com」に対する要求を許可する別の式を作成してください。要求を拒否するすべてのレスポンダーポリシーを評価リストの先頭に配置し、その後に Web リダイレクト用のレスポンダーポリシー、コンテンツスイッチポリシーの順となるように L7 ポリシーを作成してください。

構成タスク

Neutron LBaaS コマンドを使用して、L7 ポリシーとアクションを実装します。

OpenStack で環境変数を設定し、ロードバランサーを作成します（例：LB1）。ロードバランサーを正常に作成できたら、リスナーとプール（例：L1、P1、P2）を作成しプールにメンバーとモニターを追加します。たとえば、P1 を L1 のデフォルトプールに設定し、P2 は LB1 に関連付け、アプリケーションサーバーを管理するプールにします。

コマンドラインを使用して LBaaS V2 を設定する方法の詳細については、「コマンドラインを使用した LBaaS V2 の設定」を参照してください。

以下のコマンドにより、ポリシーを定義して特定のアクションを定義します。

要求をドロップする **L7** ポリシーの作成

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <
    listener name> --action<action-name>
```

例：

neutron lbaas-l7policy-create –name policy11 –action REJECT –listener L1

上記のコマンドでは、要求を拒否するレスポンダーポリシー policy11 を作成して、コンテンツスイッチサーバーにバインドします。このポリシーには規則が作成されていないため、ポリシーは「false」と評価され要求が拒否されます。

特定の **URL** に要求をリダイレクトする **L7** ポリシーの作成

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <
    listener name> --action <action-name> --redirect-url <redirect-url>
```

例：

neutron lbaas-l7policy-create–name policy12 —action REDIRECT_TO_URL —listener admin-list1 —redirect-url `http://example-sports/about-us.html`

上記のコマンドでは、URL へ要求をリダイレクトするレスポンダーアクションを作成し、このアクションが設定されたレスポンダーポリシーを作成してコンテンツスイッチ仮想サーバーにバインドします。

```
neutron lbaas-l7rule-create --type HOST_NAME --compare-type CONTAINS --
    value <value-string> <L7 policy name>
```



```
2
3 neutron lbaas-l7rule-create --type PATH --compare-type CONTAINS --value
      <value-string> <L7 policy name>
```

上記 2 つの規則は AND 演算子により結合され、レスポンダーポリシーの式が導出されます。

プールに要求をリダイレクトする **L7** ポリシーの作成

```
1 neutron lbaas-l7policy-create --name <L7 policy name> --listener <
     listener name> --action <action-name> --redirect-pool <redirect-pool
     >
```

例:

neutron lbaas-l7policy-create –name policy13 –action REDIRECT_TO_POOL –listener admin-list1 –redirect-pool admin-pool2

この L7 ポリシーが最初のポリシーである場合、上記のコマンドでは LB1 とともに P2 が実装され、コンテンツスイッチリダイレクトアクションが作成されて要求が LB1 へリダイレクトされます。P2 が既に存在する場合、このコマンドではコンテンツスイッチリダイレクトアクションが作成され、要求が LB1 にリダイレクトされます。

OpenStack での NetScaler ADC VPX インスタンスの手動 Provisioning

February 6, 2024

一部の企業ネットワークでは、セキュリティ上の理由から、Citrix ADC VPX インスタンスが Citrix ライセンスサーバーに接続してライセンスを自動的にダウンロードすることができません。このようなシナリオでは、NetScaler ADC VPX インスタンスを OpenStack プラットフォームに手動でデプロイする必要があります。Citrix から受け取ったライセンスアクティベーションコード（LAC）を使用して、適切な Citrix ADC VPX ライセンスをダウンロードし、ローカルシステムに保存します。

OpenStack で **NetScaler ADC VPX** インスタンスを手動でプロビジョニングするには:

1. Citrix ADC ドライバソフトウェアをインストールし、OpenStack に Application Delivery Management（ADM）を登録する

   a) Citrix ADM で、[オーケストレーション] > [クラウドオーケストレーション] > [OpenStack**] に移動します。

   b)「**OpenStack** の設定を設定」をクリックします。「**OpenStack** 設定の構成」ページでは、Citrix ADM で OpenStack を設定するためのパラメータを設定できます。ここには、[デフォルト] と [カスタマイズ] の 2 つのオプションがあります。

   c) OpenStack サービスがデフォルトポートで実行されている場合は、[**Default**] をクリックします。

2. **[**オーケストレーション**] > [**** クラウドオーケストレーション ****] > [****OpenStack**] に移動し、[デプロイ設定] をクリックします。**

a) 管理ネットワーク-自動プロビジョニングされた Citrix ADC VPX が接続されている OpenStack 上の管理ネットワークを選択します。

b) プロファイル名 -ドロップダウンリストからプロファイルを選択します。NetScaler ADM は、このプロファイルに含まれているパスワードを使用して、新しい自動プロビジョニングされた NetScaler ADC VPX インスタンスを構成します。

c) Citrix ADC VPX イメージ・イン・グランス-Citrix ADC VPX インスタンスの作成に使用される OpenStack Glance で利用可能な Citrix ADC VPX イメージを選択します。ボックスの一覧には、OpenStack Glance に存在するイメージのみが表示されます。

3. Citrix ADM で、［オーケストレーション］> ［クラウドオーケストレーション］> ［OpenStack**］ > ［** サービスパッケージ］に移動し、［追加］をクリックします。

4.「サービスパッケージ」ページで、次のパラメータを指定します。

a) 名前：サービスパッケージの名前。たとえば、「SVC-PKG-GOLD」と入力します。

b) **Citrix ADC** インスタンス割り当て-サービスパッケージで定義されているインスタンス割り当てのタイプとして、[専用] または [パーティション] を選択します。

c) **Citrix ADC** インスタンス **Provisioning**-構成中に Citrix ADC インスタンスを作成するには、「オンデマンドでインスタンスを作成」を選択します。

d) 自動プロビジョニングプラットフォーム - **OpenStack Compute** を選択します。デフォルトでは、Citrix ADC VPX がインスタンスタイプとして選択されます。

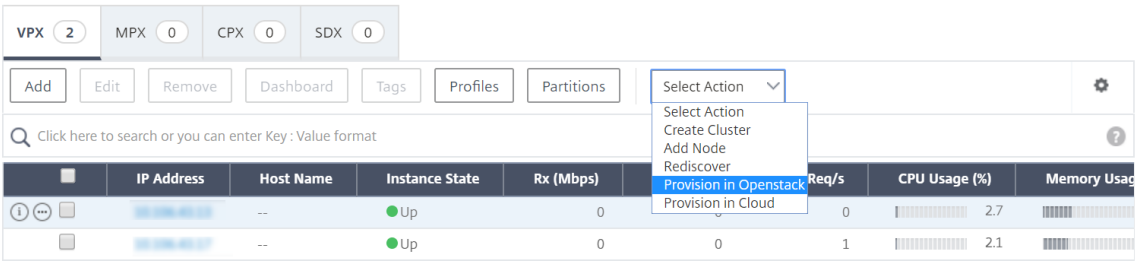
e) **OpenStack** テナント/プレースメントポリシーの割り当て-セクションの OpenStack テナントで [追加] をクリックし、テナントを選択します。

f) ［**Continue**］、［**Done**］の順にクリックします。

5. [システム] > [システム管理] > [システム設定の変更] に移動し、ドロップダウンリストから [**http**] を選択します。

6. [ネットワーク] > [インスタンス] > **[****Citrix ADC VPX**] に移動します。

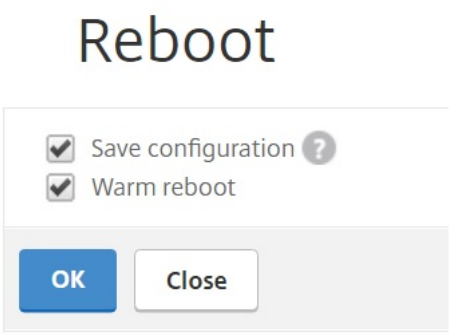
7. **NetScaler ADC VPX** ページで、［管理］ドロップダウンリストをクリックし、［デバイスのプロビジョニング］を選択します。



a) [**Device Provisioning**] ページで、デバイスの名前を入力し、前の手順で作成したサービスパッケージを選択します。

b) [**OK]** をクリックします。

8. **[**オーケストレーション**] > [**** クラウドオーケストレーション ****] > [**OpenStack**] > [リクエスト] タブに移動します。** リクエストを選択し、「タスク」をクリックしてタスクを表示します。タスクのステータスが [完了] に変わると、NetScaler ADC VPX が NetScaler ADM でプロビジョニングされます。
9. [ネットワーク] > [インスタンス] > **[Citrix ADC VPX**] に移動して、Citrix ADC VPX インスタンスが Citrix ADC VPX ページに表示されていることを確認します。
10. NetScaler ADC VPX インスタンスをクリックします。Citrix ADC VPX インスタンスがブラウザウィンドウで開いたら、インスタンスにログオンします。[構成] > [システム] > [ライセンス] に移動し、新しいライセンスを手動で追加します。新しいライセンスを追加する方法について詳しくは、「NetScaler ADC ライセンスの概要」を参照してください。
11. NetScaler ADC VPX インスタンスを再起動します。



12. 数分後、OpenStack にログオンし、[システム] > [インスタンス] で、NetScaler ADC VPX インスタンスが OpenStack にデプロイされていることがわかります。
13. LBaaS V2 API を実装するには、Neutron LBaaS コマンドを使用します。いずれかの Neutron クライアントに接続して構成タスクを実行します。設定コマンドの実行方法の詳細については、「コマンドラインを使用した LBaaS V2 の設定」を参照してください。

StyleBook を使用した **OpenStack** での **NetScaler ADC VPX** インスタンスのプロビジョニング

February 6, 2024

OpenStack オーケストレーションワークフローでは、Application Delivery Management（ADM）が「os-cs-lb-mon」StyleBook を使用して、OpenStack テナントに割り当てられた Citrix ADC インスタンスに LBaaS 構成をデプロイするようになりました。OpenStack ユーザーによって作成されたロードバランサーごとに、設定パックが作成されます。

OpenStack ワークフローの設定に StyleBooks を使用すると、次のようなメリットがあります。

- すべての設定オブジェクトを表示することで、視覚化が改善されました。
- ロールバックによる信頼性。
- さまざまな NetScaler ADC インスタンスタイプ（NetScaler ADC HA、パーティション、VPX、CPX、MPX など）のサポート。
- 独自の StyleBooks を使用して OpenStack テナントの設定をデプロイすることによるカスタマイズ。

NetScaler ADM 管理者として、［アプリケーション］>［構成］に移動して、NetScaler ADC インスタンスに展開されている構成パックを表示します。
次のタスクを実行できます。

- スクロールすると、ロードバランサーにデプロイされた「os-cs-lb-mon」設定パックが表示されます。
- 「os-cs-lb-mon」StyleBook パネルの「定義を表示」をクリックして、インスタンスにデプロイされている構成を確認します。
- ［オブジェクトの表示］をクリックして、インスタンスにデプロイされた NetScaler ADC オブジェクトまたはエンティティの一覧を表示します。

StyleBook を使用してインスタンスを **Provisioning** する前の注意点

NetScaler ADM 12.1 ビルド 49.23 以降、OpenStack オーケストレーションワークフローのアーキテクチャが更新されました。ワークフローでは、NetScaler ADM StyleBook を使用して NetScaler ADC インスタンスを構成するようになりました。バージョン 12.0 またはバージョン 12.1 ビルド 48.18 のいずれかから NetScaler ADM 12.1 ビルド 49.23 にアップグレードする場合は、次の移行スクリプトを実行する必要があります。

```
/mps/scripts/migration_scripts/migrate_configurations.py
<!--NeedCopy-->
```

- マイグレーションスクリプトを実行すると、既存の OpenStack 設定に対応する「os-cs-lb-mon」StyleBook の設定パックが作成されます。
- 以前のビルドから OpenStack 設定をデプロイした場合は、この移行スクリプトの実行が必須です。
- バージョン 12.1 ビルド 49.23 からの移行スクリプトを実行した後にのみ、「os-cs-lb-mon」StyleBook を使用してインスタンスに新しい構成をデプロイできます。
- OpenStack から試行されたすべての構成は、移行スクリプトが実行されるまで失敗します。

> 注
>
> - 移行スクリプトを実行すると、Citrix ADM の以前のビルドにダウングレードすることはできません。
> - OpenStack LBaaS V2 用の NetScaler ADC ドライバを最新バージョンにアップグレードしていることを確認します。最新の Citrix ADM 12.1 ビルド 49.23 に付属している Citrix ADC バンドルファイルを使用してください。

LBaaS V2 API を実装するには、Neutron LBaaS コマンドを使用します。任意の Neutron クライアントに接続し、設定タスクを実行します。設定コマンドの実行方法の詳細については、「コマンドラインを使用した LBaaS V2 の設定」を参照してください。

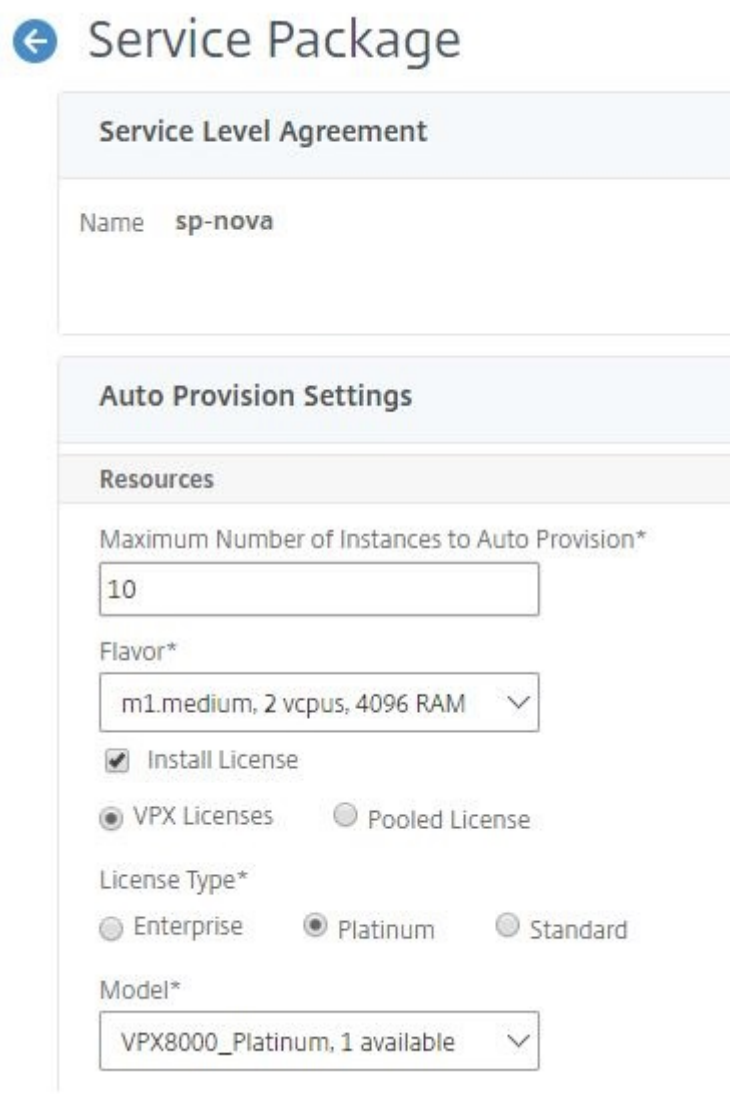
VPX チェックインとチェックアウトのライセンスおよび OpenStack 環境のプールライセンスのサポート

February 6, 2024

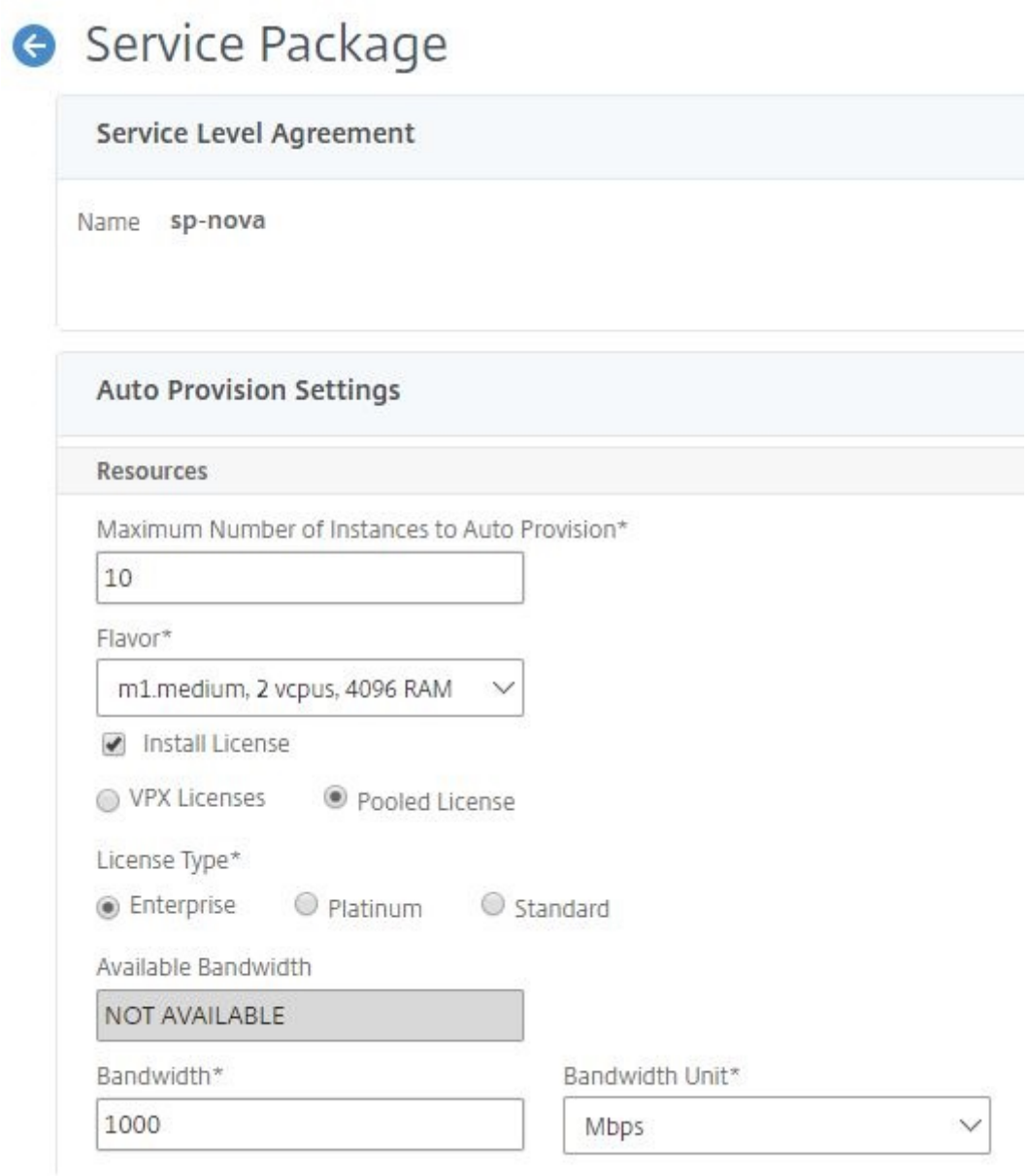
OpenStack オーケストレーションワークフローでは、**OpenStack** コンピュートでサービスパッケージを選択すると、NetScaler Application Delivery Management（ADM）がオンデマンドで NetScaler ADC VPX インスタンスを作成します。これで、Citrix ADM のオーケストレーション機能のサービスパッケージページが拡張され、オンデマンドで作成される Citrix ADC VPX インスタンスにインストールする必要のあるライセンスが提供されるようになりました。提供されるライセンスは、VPX チェックインおよびチェックアウトライセンスまたはプールライセンスのいずれかです。

この機能を使用するには、まず Citrix ADM にライセンスをアップロードしてから、OpenStack Compute を使用するサービスパッケージを作成する必要があります。

- チェックイン、チェックアウトライセンスの場合は、利用可能なさまざまなライセンスからインストールするライセンスを選択できます。



- プールライセンスの場合は、帯域幅とインストールするライセンスエディションのタイプの両方を選択できます。



NetScaler ADM をプロバイダーとして最初のロードバランサーを展開すると、NetScaler ADM によって NetScaler ADC VPX インスタンスが作成され、サービスパッケージで指定されたライセンスが新しく作成されたインスタンスにインストールされます。

また、既存の負荷分散インスタンスを削除すると、そのインスタンスは不要になります。インスタンスは廃止され、ライセンスは Citrix ADM に返却されます。これにより、Citrix ADM で利用可能なライセンスを最適に使用できます。

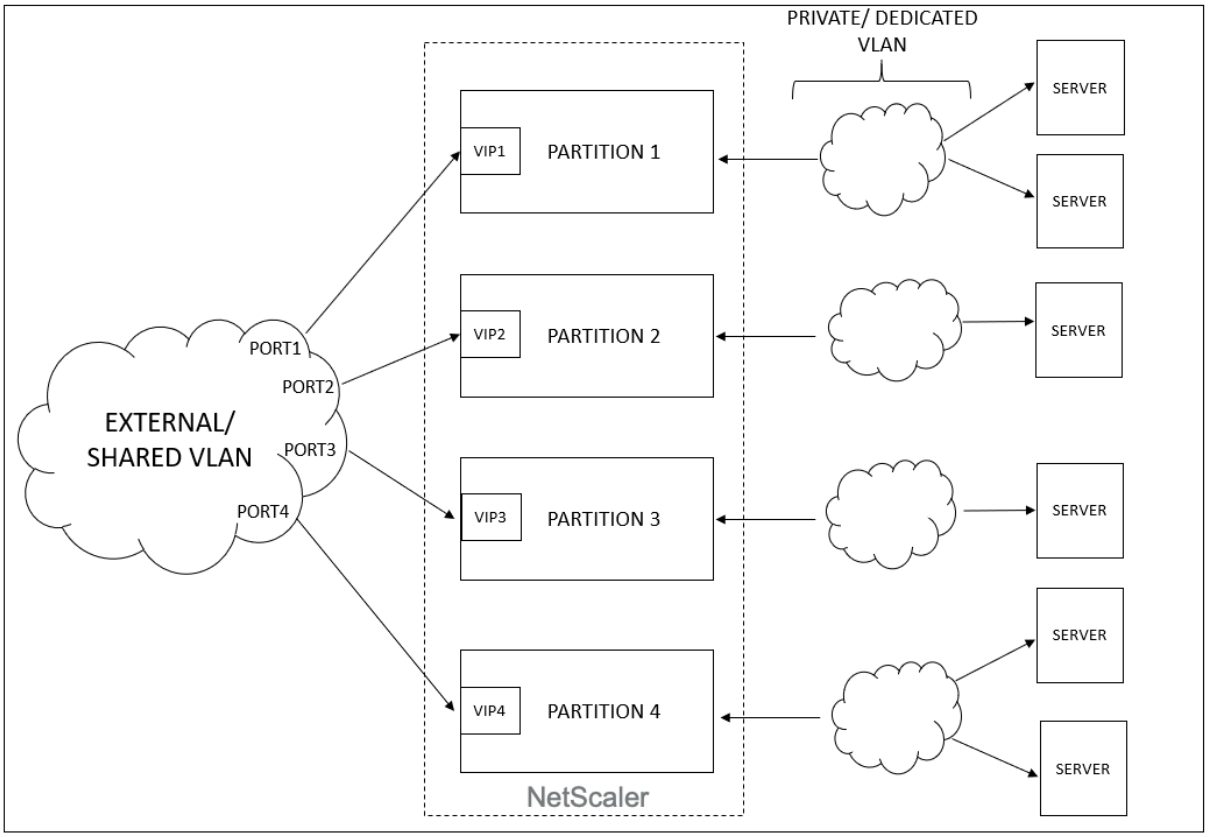
> 注
>
> ：Citrix ADM を高可用性モードで展開する場合は、ライセンスを現在のアクティブまたはプライマリの Citrix ADM、MAS-HA-1 にアップロードすることを検討してください。最初のリクエストを展開し、Citrix ADM が

> Citrix ADC VPX インスタンスを作成すると、インスタンスは MAS-HA-1 から必要なライセンスをチェックアウトします。後で、ライセンスを持たないセカンダリ Citrix ADM MAS-HA-2 が現在アクティブになっていると仮定します。現在、ADC VPX インスタンスは MAS-HA-2 からライセンスをチェックアウトできないため、新しいユーザー用にインスタンスを作成できません。
>
> このような場合は、MAS-HA-1 が稼働していて、現在のプライマリノードになっていることを確認してください。つまり、Citrix ADM を MAS-HA-2 から MAS-HA-1 に手動でフェールオーバーします。その後、OpenStack から設定を再試行する必要があり、インスタンスは適切なライセンスで再作成されます。NetScaler ADM 高可用性展開でのライセンスサポートについて詳しくは、「高可用性」を参照してください。

管理パーティションの共有 **VLAN** サポート

February 6, 2024

プライベートネットワークから接続するテナントの場合、Citrix Application Delivery Management（ADM）は分離ポリシーをサポートしているため、各テナントには独自の専用パーティション、専用 VLAN、および専用サーバーがあります。パブリックネットワークから接続するテナントの場合は、専用の VLAN を使用すると、大量の IP アドレスが必要になります。共有 VLAN では、各パーティション上に 1 つの仮想 IP アドレスを作成することで、1 つの IP サブネットを作成して、この問題を回避します。

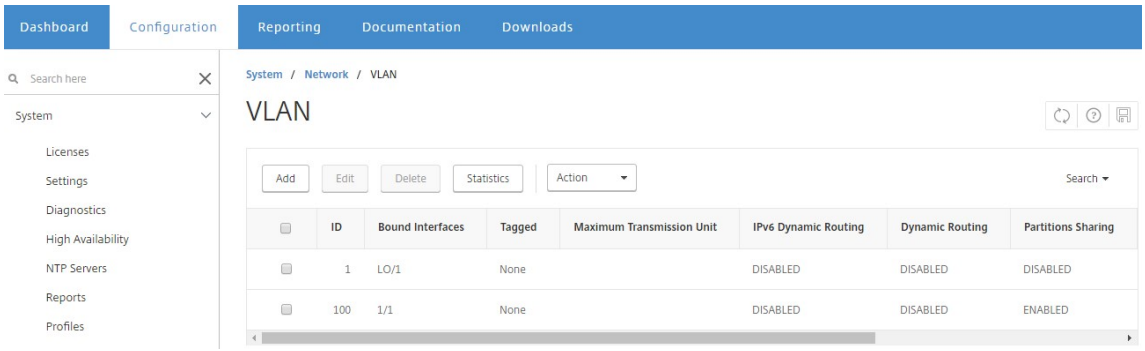


テナントが VIP またはリスナーを構成すると、そのテナントの NetScaler ADC デバイスに管理パーティションが作成されます。すべてのロードバランサー構成は、作成された admin パーティションにプッシュされます。テナントが共有ネットワークまたは外部ネットワークを使用してロードバランサーを作成している場合は、そのネットワークの VLAN が追加され、共有機能が有効化されます。別のテナントが同じ共有ネットワークを使用してロードバランサーを作成する場合、VLAN は Citrix ADC に再度追加されませんが、VLAN は 2 番目のパーティションにもバインドされます。したがって、同じ共有ネットワークを使用しているテナントには、同じ VLAN に結合されているパーティションが与えられます。

Citrix ADM は仮想デスティネーション MAC アドレスをサポートしています。テナントが VLAN を共有する場合、Citrix ADM は Citrix ADC デバイスのパーティションに異なる MAC アドレスを割り当てます。これにより、1 つの VLAN を、パーティション間、またはすべてのテナントおよびすべてのトラフィックドメイン間で共有できます。

Citrix ADC インスタンスからの共有 **VLAN** の設定

1. Citrix ADC インスタンスで、[構成 **] **> [** システム] > [ネットワーク]**> **[VLAN]** に移動し、**VLAN** プロファイルを選択し、**[** 編集] をクリックしてパーティション共有パラメータを設定します。
2. 「**VLAN** の設定」ページで、「パーティション共有」チェックボックスを選択します。
3. [**OK**] をクリックします。



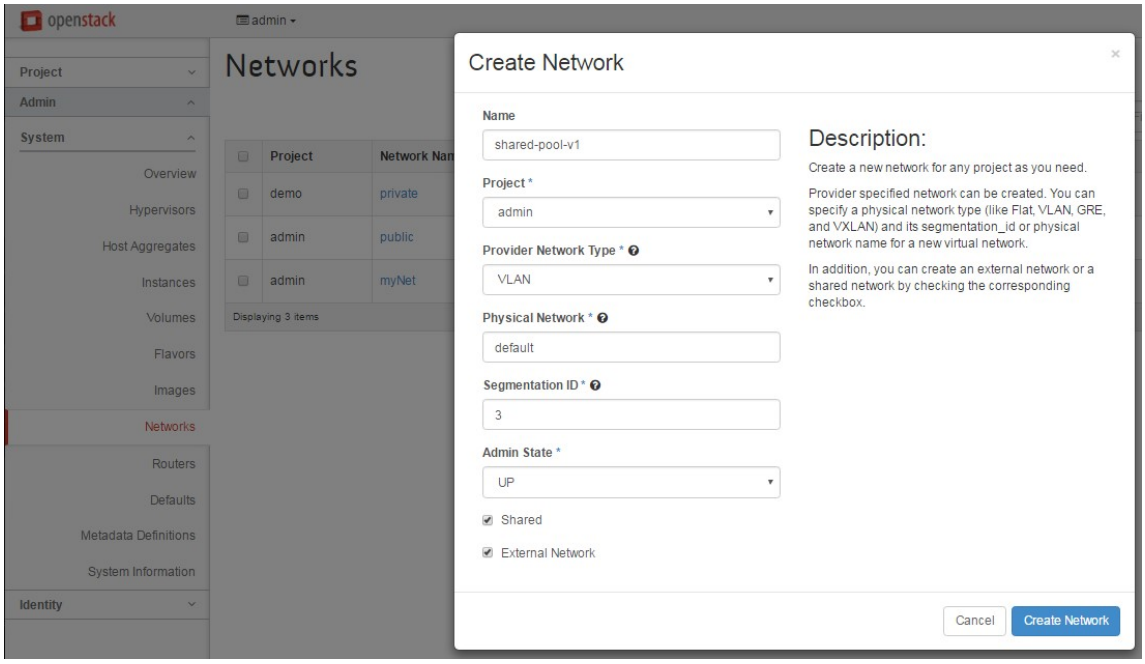
OpenStack Orchestration から共有 **VLAN** を構成する

1. OpenStack で、[管理] > [システム] > [ネットワーク] に移動し、[ネットワークの作成] をクリックします。
2. [**Create Network**] で、次のパラメーターを設定します。
   a) Name - ネットワークの名前を入力します。
   b) Project - ボックスの一覧からプロジェクトを選択します。
   c) プロバイダーネットワークタイプ-ドロップダウンリストから **VLAN** を選択します。これにより、仮想ネットワークが VLAN として確立されます。
   d) Physical Network - ここでデフォルトの物理ネットワークを選択します。このボックスは編集可能です。

e) Admin State - デフォルトでは、ネットワークの管理状態は UP です。

f) VLAN が共有されており、外部ネットワークを使用していることを定義するには、［**Shared**］と［**External**］を選択します。

3. ［**Create Network**］をクリックします。



試用版ライセンスのワークフロー

February 6, 2024

OpenStack オーケストレーションを使用した NetScaler ADC VPX インスタンスの自動プロビジョニングでは、NetScaler Application Delivery Management（ADM）は OpenStack コンピュートを使用して NetScaler ADC VPX インスタンスを起動します。新しくプロビジョニングされた Citrix ADC VPX インスタンスは、セットアップ中に Citrix ライセンスポータルにアクセスし、ライセンスアクティベーションコード（LAC）を使用してライセンスファイルを自動的にダウンロードしてインストールします。

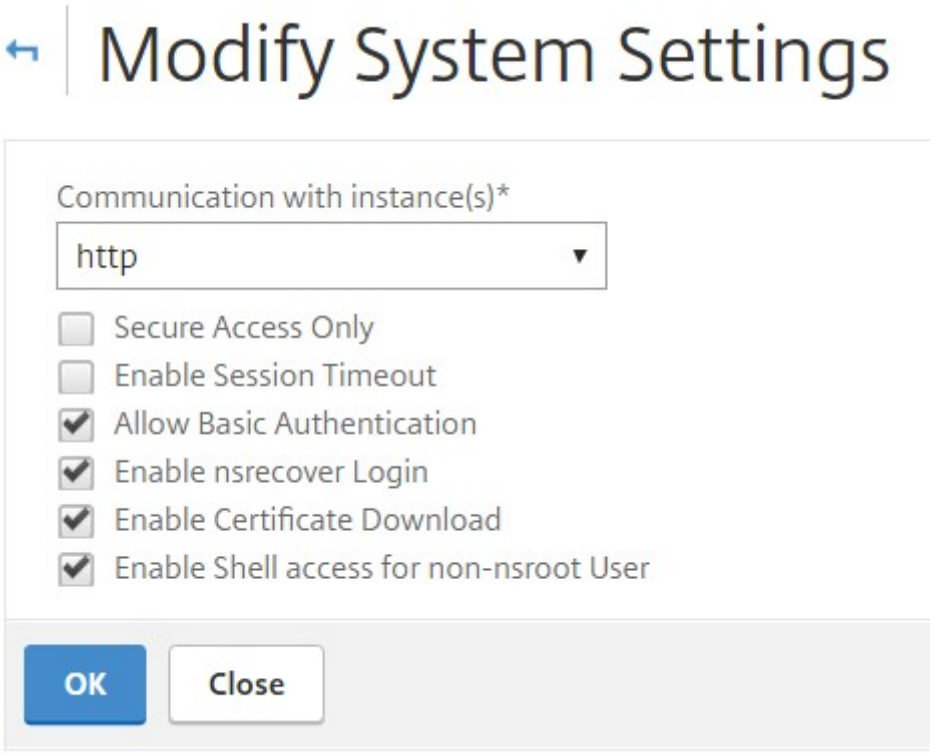
試用版ライセンス

テクニカルサポートスタッフは、Citrix ADM および Citrix ADC VPX デバイスを現場にインストールするときに試用版ライセンスを使用します。Citrix ADC VPX の試用版または評価版ライセンスは 90 日間有効です。複数の Citrix ADC を評価する必要がある場合、または 90 日後にテストを延長する必要がある場合は、新しい評価ライセンスをリクエストする必要があります。Citrix ADM は、試用版ライセンスファイルを自動的にインストールする代わりに、代

替ソリューションを提供します。ライセンスファイルを手動でダウンロードして Citrix ADC VPX にインストールすると、インスタンスのインストールを完了できます。

Citrix ADC VPX がインターネットに接続できない場合は、Citrix ADM を Citrix ライセンスポータルのプロキシサーバーとして動作するように構成し、ライセンスファイルをインストールします。

トライアルライセンスを持つ Citrix ADC VPX インスタンスは、HTTP でのみ Citrix ADM と通信できます。Citrix ADM で HTTP 通信を構成するには、[システム] > [システム管理] に移動し 、[システム設定の変更] をクリック します。ドロップダウンリストから「**http** 」を選択して通信方法を設定し、「**OK**」をクリックします。



OpenStack Heat サービスとの統合

February 6, 2024

OpenStack Neutron LBaaS を利用すると、負荷分散、SSL オフロード、コンテンツスイッチなどの主要な負荷分散サービスをアプリケーションで使用できます。LBaaS の管理は RESTful API により行い、この API を使用することでテナントで REST 呼び出しを実行し、LBaaS オブジェクトを作成、更新、削除できます。LBaaS では負荷分散サービスが提供されるため、オーケストレーションプロセス中により高度な NetScaler ADC 機能を使用することはできません。Citrix ADC Heat プラグインはこの制限を克服します。

Heat オーケストレーションサービス

OpenStack Heat オーケストレーションサービスでは、テンプレートに基づいて複雑なクラウドアプリケーションを展開することができます。クラウドアプリケーションのインフラストラクチャは、バージョン管理ツールで管理可能な Heat オーケストレーションテンプレート（HOT：Heat orchestration template）により、人間が読み取り/書き込み可能なテキストファイルで指定します。このテンプレートは、YAML という構造化言語を使用して記述します。HOT を使用することでほとんどの種類の OpenStack リソースを作成でき、このテンプレート内で定義したリソース間の関係を指定できます。Citrix ADC Heat プラグインを使用すると、任意の Citrix ADC インスタンスで高度なアプリケーションデリバリーコントローラー（ADC）機能を設定できます。

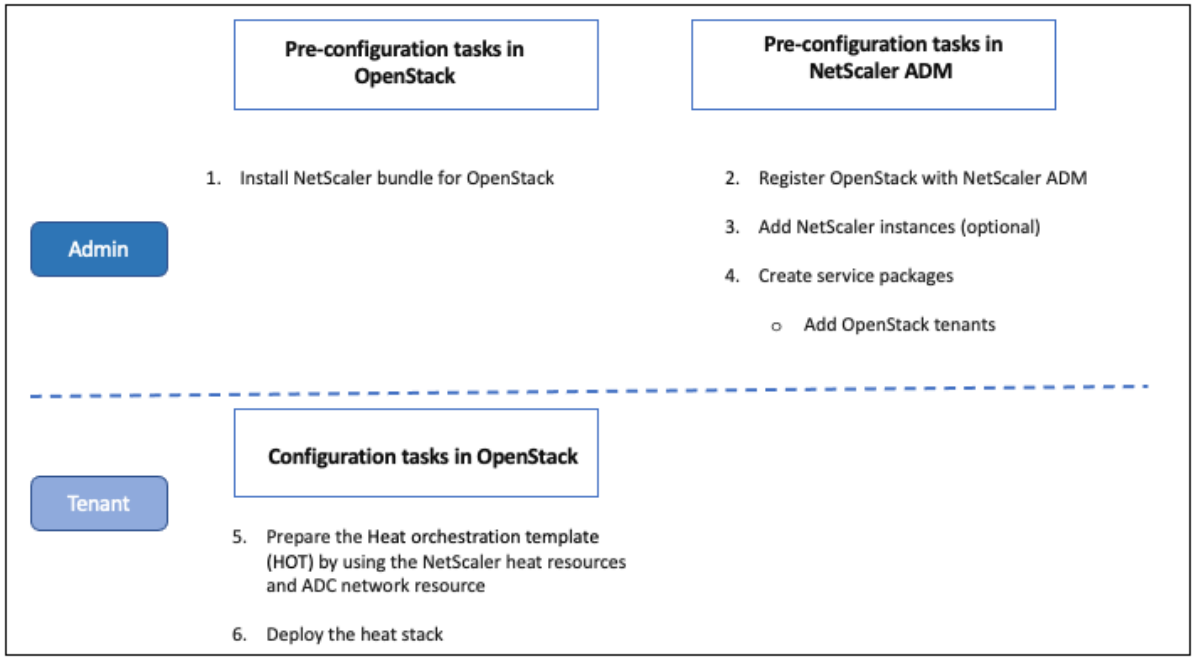
Citrix ADC StyleBook

Citrix Application Delivery Management（ADM）StyleBook を使用して、Citrix ADC 機能を作成および構成できます。Heat テンプレートと同様に、StyleBook も YAML で記述します。機能ごとに個別の StyleBook を作成でき、1 つの StyleBook を使用して複数の Citrix ADC インスタンスに構成を展開できます。

Citrix ADC と OpenStack の統合中、Citrix ADM はすべての Citrix ADM StyleBook を Heat サービスのリソースとして公開します。これには、Citrix ADM に同梱されている StyleBook と、ユーザーが後で作成した StyleBook の両方が含まれます。Heat テンプレートを使用すると、これらの StyleBooks リソースを使用して Citrix ADC の高度な機能を構成できます。

Heat を使用して **Citrix ADC** インスタンスを設定するためのワークフロー

以下のフローチャートに、Heat スタックを展開するワークフローを示します。



クラウド管理者として次のタスクを実行します。

OpenStack で **Heat** サービスを設定するには**:**

1. OpenStack 用 Citrix ADC バンドルのダウンロード

   Citrix ADC バンドルを OpenStack にインストールします。Citrix ADM で、「ダウンロード」に移動して Citrix ADC ドライバーバンドルをダウンロードし、バンドルを解凍して、バンドル内の Heat フォルダーの内容を OpenStack の Heat エンジンリソースディレクトリにコピーします。ディレクトリパスは次のとおりです。
   /opt/stack/heat/heat/engine/resources/netscaler_resources

2. heat.conf ファイルに「netscaler_plugin」セクションを作成し、そのセクションの以下のパラメーターを更新します。

   [netscaler_plugin]

   a) 通信が HTTP である場合、パラメーターは次のように設定します。

      NMAS_BASE_URI=<http://10.146.103.45:80>

      NMAS_USERNAME=

      NMAS_PASSWORD=

   b) 通信が https の場合、パラメータは次のように更新されます。

      NMAS_BASE_URIhttps://common_name_used_in_certificate

      NMAS_USERNAME=<openstack_driver_username

      NMAS_PASSWORD=<openstack_driver_password>

      SSL_CERT_VERIFY=<True_or_False>

      CERT_FILE_PATH=<path_of_the_certificate_file>

      ユーザーが ssl_cert_verify を「False」に設定すると、Citrix ADM はリクエスト呼び出しで verify=False を送信し、SSL 証明書の検証を無効にします。ssl_cert_verify が「True」に設定されていて、cert_file_path エントリが存在する場合、NetScaler ADM はリクエストの verify パラメータにこのパスを送信します。そうでない場合、NetScaler ADM は verify=true を送信します。

      > 注
      >
      > :
      >
      > Citrix ADM を「高可用性」モードでデプロイするには、heat.conf ファイル内の次のパラメーターを更新してください。NMAS_BASE_URI=<ip address of the front-end virtual server>

3. OpenStack で Heat サービスを再起動します。

OpenStack で Citrix ADC Heat サービスを再起動すると、定義されているすべての Citrix ADM StyleBook がリソースとして Heat にインポートされます。また、Citrix ADC ネットワークリソースと証明書リソースは、Citrix ADC Heat リソースとして OpenStack にインポートされます。

4. Citrix ADM を OpenStack に登録します。

   a) Citrix ADM で、「オーケストレーション」>「クラウドオーケストレーション」>「**OpenStack**」に移動し、「**OpenStack** 設定の構成」をクリックします。

   b) **OpenStack** の設定ページでは、OpenStack を設定するためのパラメーターを設定できます。[Default] と［Customized］の 2 つのオプションがあります。

   c) OpenStack サービスがデフォルトポートで実行されている場合は、「デフォルト」を選択します。以下のパラメーターを入力します。

      i. OpenStack コントローラーの IP アドレス

      ii. 管理者ユーザー名

      iii. パスワード

      iv. OpenStack 管理者テナント

      v. Citrix ADC ドライバーと Heat のパスワード

      > 注:
      >
      > これは heat.conf ファイルに入力したパスワード (NMAS_PASSWORD) と同じです。

5. サービスパッケージを作成し、テナントで SLA を定義します。

   OpenStack の登録時に、Citrix ADM でユーザーごとにテナントが作成され、テナント情報は LBaaS ドライバーと Heat プラグインの両方で使用されます。Heat プラグインはこの情報を使用して NetScaler ADM に連絡し、OpenStack に Heat リソースとして StyleBook をインポートします。

   > 注:
   >
   > NetScaler ADM および OpenStack でのサービスパッケージの作成およびその他の事前構成タスクの詳細については、「NetScaler ADM と OpenStack Platform の統合」を参照してください。

6. Citrix ADM 内の関連するすべての StyleBook がリソースとして OpenStack Heat にインポートされていることを確認してください。また、NetScaler ADC ネットワークリソースと NetScaler ADC 証明書リソースがリソースとして OpenStack Heat にインポートされることも確認します。

   > 注
   >
   > 現在、使用できるのは Citrix ADM に付属している StyleBook のみです。

   テナントは OpenStack で Heat テンプレートを作成して必要な Heat パラメーターの値を入力し、Heat スタックを展開できるようになりました。Heat スタックがデプロイされると、構成が Citrix ADM にプッシュされ、必要な Citrix ADC インスタンスが設定されます。

Heat テンプレートを準備して **Heat** スタックを起動するには**:**

1. OpenStack では、テナントで Heat リソースを使用して HOT を作成できます。
2. OpenStack Horizon では、テナント管理者はプロジェクト >**** オーケストレーション ** > スタックに移動して Heat テンプレートを作成し、Heat スタックを起動できます。HOT を作成するには 2 つの方法があります。

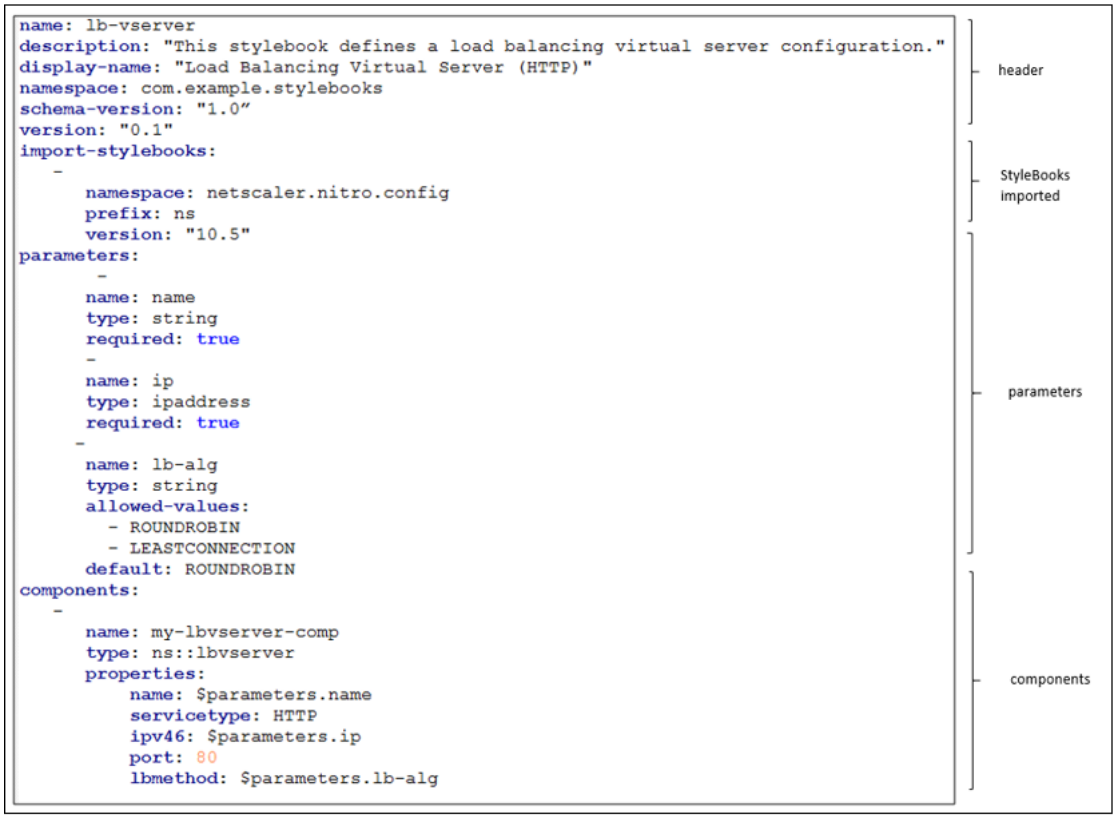
    - ファイル -ローカルディレクトリから更新されたテンプレートを選択します
    - 直接入力 -YAML コンテンツをテンプレートからコピーしてウィンドウに貼り付けます

    > 注**:**
    >
    > スタックのデプロイが成功すると、テナントはスタック変更テンプレートを使用してスタックを更新できます。ただし、スタックの作成中に初回設定したサブネット情報と仮想 IP アドレス（VIP：Virtual IP Address）を変更することはできません。

    テナントがスタックをデプロイしたら、NetScaler ADM で「オーケストレーション」>「クラウドオーケストレーション」>「**OpenStack**」>「リクエスト」の順に選択し、タスクのリストを確認します。また、Citrix ADM の「アプリケーション」>「構成」に移動して、Citrix ADC インスタンスが StyleBooks 構成パックの形式で正常に構成されていることを確認します。

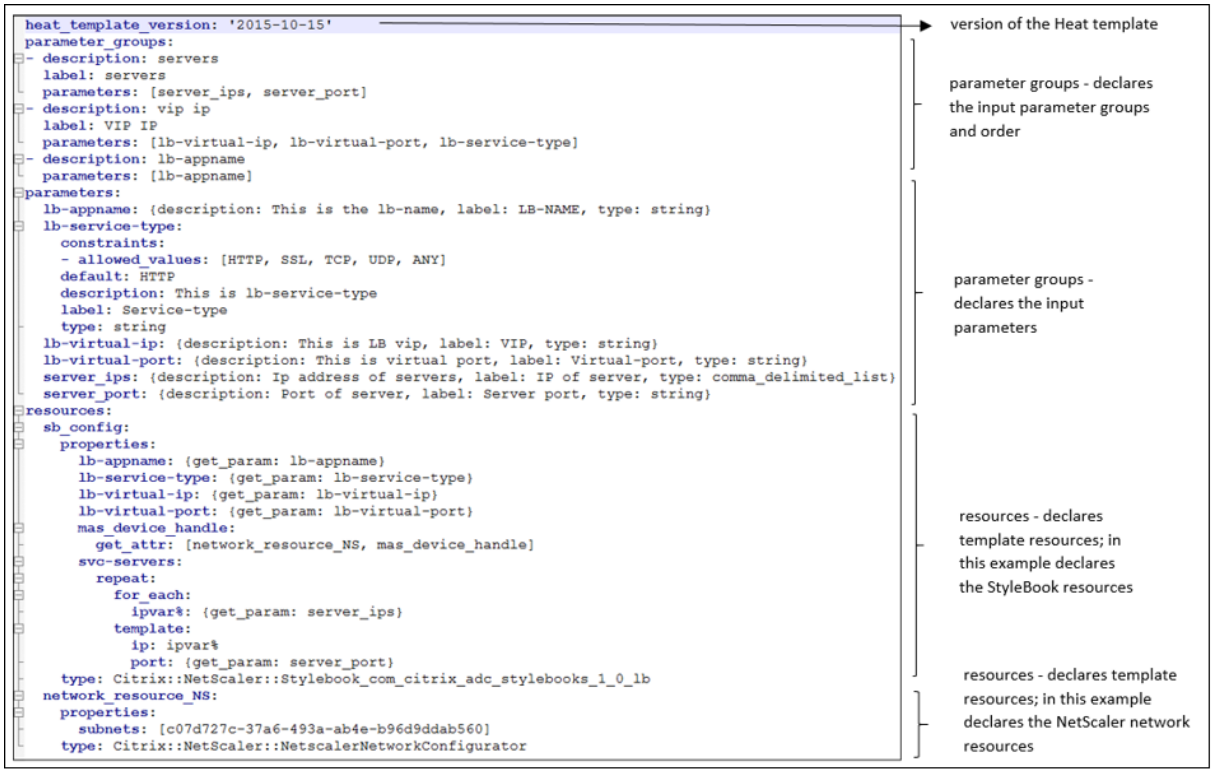
NetScaler ADM StyleBook の例:

次の図は、NetScaler ADM StyleBook の構成例とコンポーネントを簡単に説明したものです。NetScaler ADM StyleBooks および同梱されている StyleBook の使用方法の詳細については、「StyleBook」を参照してください。



Heat テンプレートの例**:**

次の図は、YAML で定義されている Heat テンプレートの構造を示し、Heat リソースとしてインポートされる StyleBooks リソースおよび NetScaler ADC ネットワークリソースを示します。



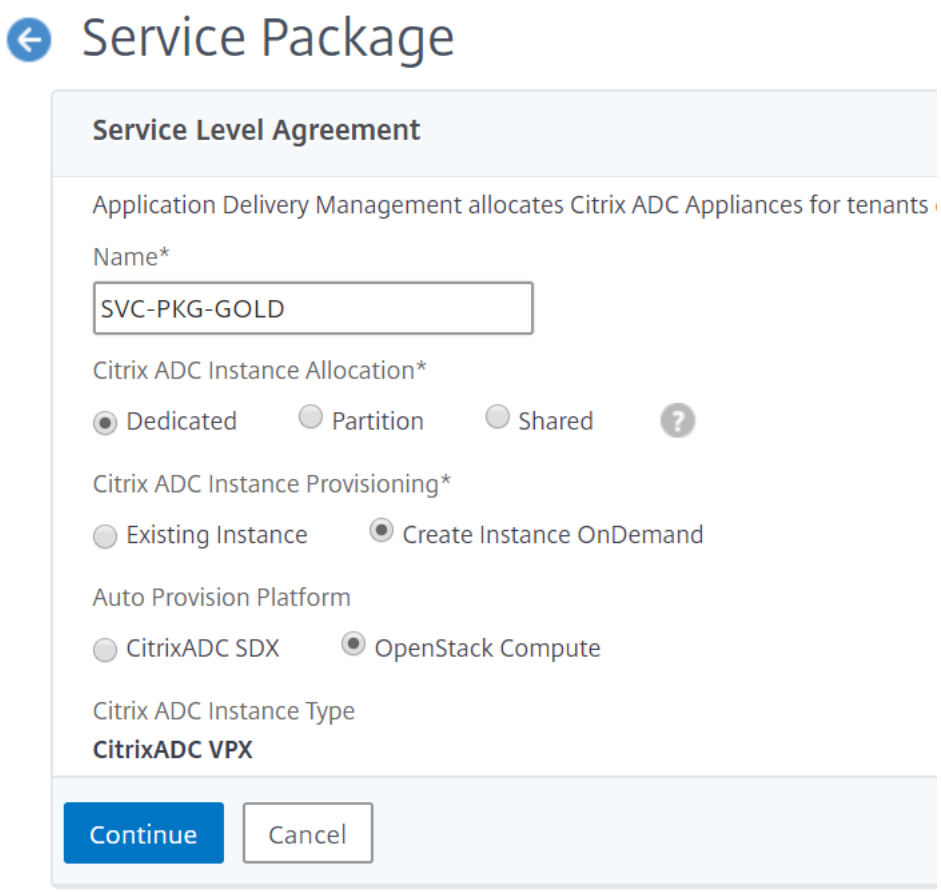
Heat サービスの詳細とテンプレートの作成方法については、OpenStack Heat のドキュメントを参照してください。

サービスパッケージの分離ポリシー

February 6, 2024

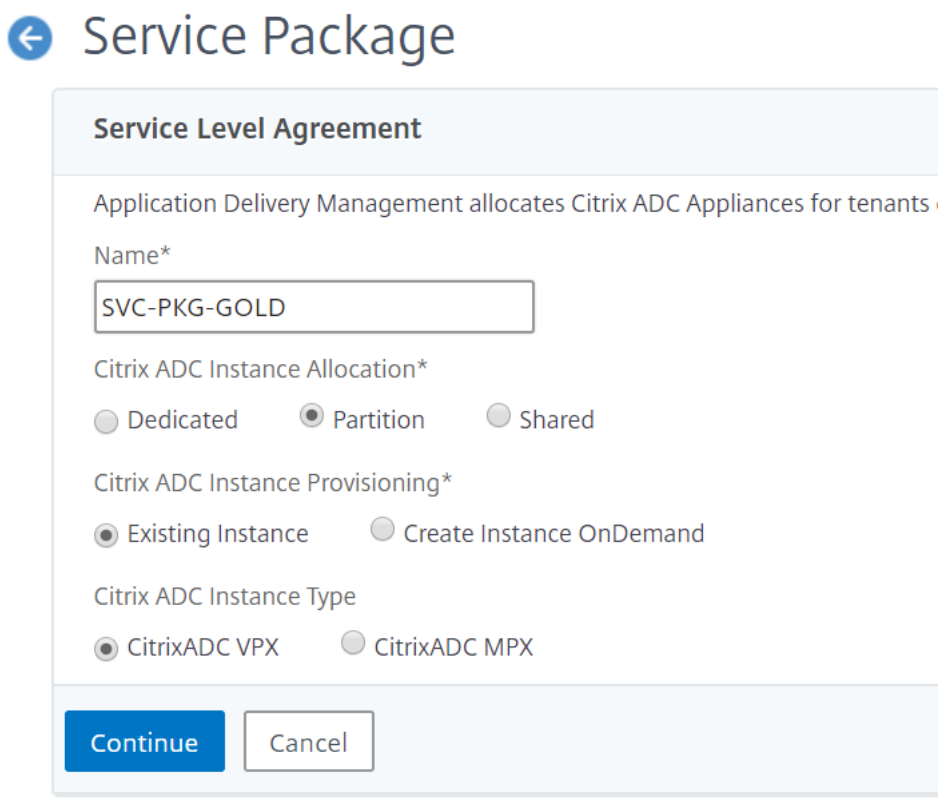
専用分離ポリシー

専用ポリシーの Citrix Application Delivery Management（ADM）サービスパッケージに関連付けられているすべてのテナントには、このサービスパッケージに含まれるインスタンスの中から Citrix ADC インスタンスが割り当てられます。この割り当てられた NetScaler ADC インスタンスは、他のテナントと共有されません。



パーティション分離ポリシー

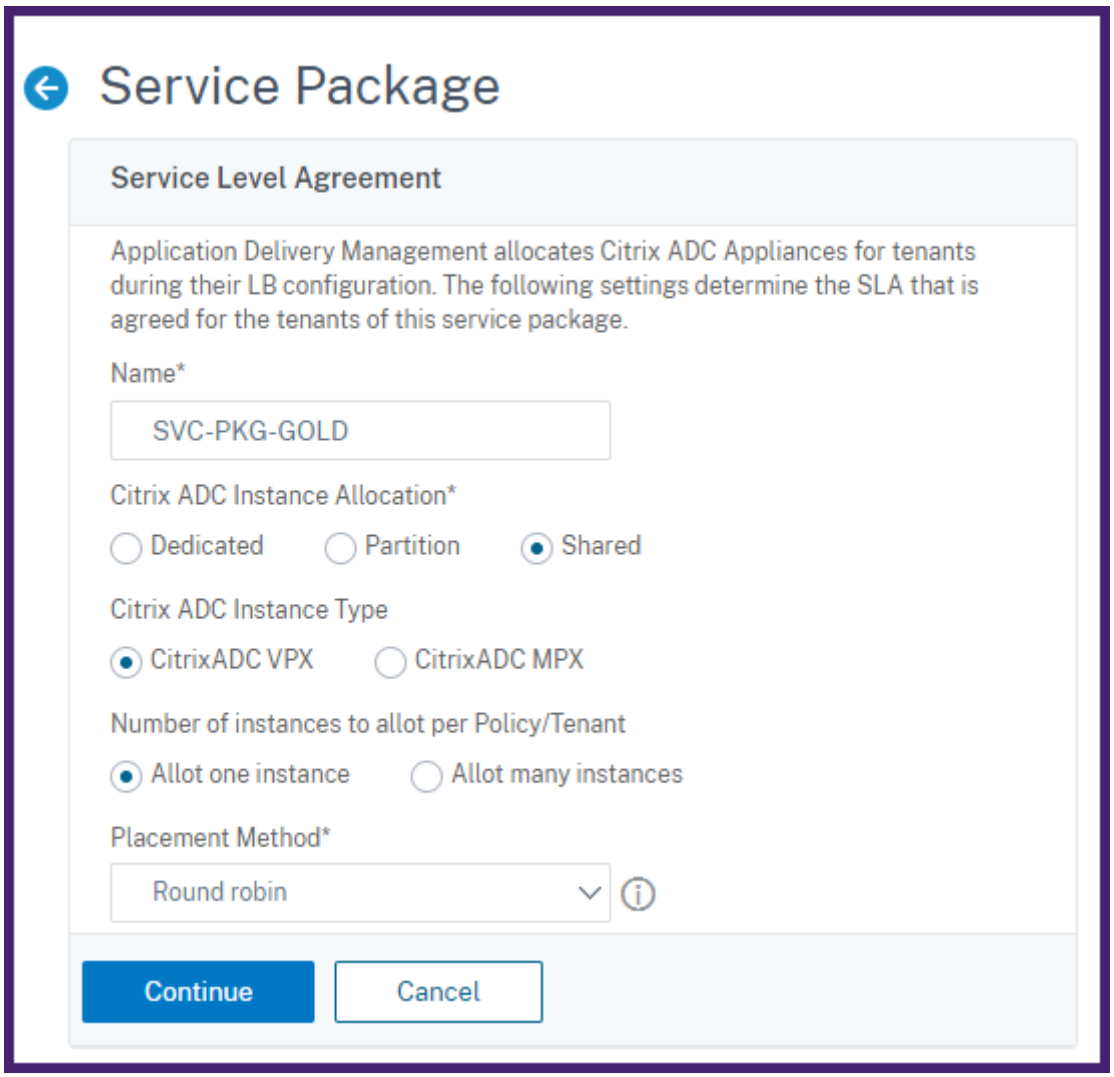
パーティションポリシーのサービスパッケージに関連付けられているすべてのテナントには、サービスパッケージの一部である NetScaler ADC インスタンスの専用の論理管理パーティションが割り当てられます。



共有分離ポリシー

サービスパッケージに関連付けられたテナントは、サービスパッケージの一部である Citrix ADC インスタンスを共有します。テナントのすべての構成は、1 つの Citrix ADC インスタンスに割り当てられます。このモードでは、複数のテナントからの構成を同じ Citrix ADC インスタンスでホストできます。デバイスタイプとして **Citrix ADC VPX** または **Citrix ADC MPX** を選択できます。サービスパッケージには、Citrix ADC インスタンスを 1 つだけ割り当てることも、複数のインスタンスを割り当てることもできます。つまり、複数のテナントが Citrix ADC デバイスの 1 つまたは複数の仮想インスタンスを共有できます。

> 注:
>
> NetScaler ADC SDX インスタンスは、NetScaler ADC VPX インスタンスとしてのみサービスパッケージに追加してください。これは、NetScaler ADC SDX には NetScaler ADC VPX がプロビジョニングされているためです。



> 注
>
> 柔軟な配置ポリシーを作成することもできます。その場合、テナント名またはテナント ID だけでなく、その他のカスタム属性にも基づいたポリシーにすることができます。柔軟な配置ポリシーについて詳しくは、「柔軟なポリシーベースのデバイス割り当て」を参照してください。

柔軟なポリシー・ベースのデバイス割り当て

February 6, 2024

Citrix Application Delivery Management（ADM）は、テナントと合意した SLA に基づいて、Citrix ADC 仮想インスタンスをテナントに割り当てます。テナントへの仮想インスタンス割り当てにおいて、インスタンスとテナントの関係は 1 対 1 です。データセンター内では、1 つのテナントを 1 つのサービスパッケージだけに割り当てることができます。

ただし、テナントが複数のインスタンスを必要とする場合や、テナントを基準にせず、ネットワーク ID やアプリケーションなどの要素に基づいてインスタンスを割り当てる場合も想定されます。このような場合、Citrix ADM では、ユーザー定義の式に基づいて配置ポリシーを正確に定義して、管理対象インスタンスの 1 つにロードバランサー構成を割り当てることができます。

配置ポリシーにより、ユーザーが作成した各ロードバランサー構成で使用される Citrix ADC インスタンスを柔軟に決定できます。Citrix ADM の柔軟な配置ポリシーは、テナントに基づいて Citrix ADC インスタンスを割り当てる既存の方法に追加のオプションを提供します。

> 注
>
> 手動でインスタンスをテナントに割り当てたり、作成された式に基づいてインスタンスを割り当てる配置ポリシーを使うことができます。1 つのサービスパッケージに対し、同時に両方の方法を使用することはできません。

配置ポリシーは、プールやロードバランサーなど、メインの LBaaS 構成のプロパティを通じて定義されたブール式に基づきます。Citrix ADM の配置ポリシーユーザーインターフェイスには、カスタマイズされたポリシーを定義するために選択できる定義済みの式が用意されています。さまざまな式に合わせて複数の配置ポリシーを作成できます。これにより、各テナントはテナントの要件で定義されている複数のデバイスを保有できます。

まずは、後で構成することとなるルートオブジェクトに適合する式を選択してください。ルートオブジェクトは、LBaaS V1 の場合はプールオブジェクト、LBaaS V2 の場合はロードバランサーオブジェクトです。そのため、Citrix ADM ポリシーベースのプレースメントは、LBaaS V1 API と V2 API の両方でサポートされています。その後、これらの配置ポリシーはサービスパッケージに割り当てられます。ルートオブジェクトがインスタンスに設定されると、モデルの後続のオブジェクトがインスタンスに追加されます。

たとえば、プール構成オブジェクトには次のプロパティがあります。

- tenant_id
- name
- 説明
- protocol
- lb_method
- subnet_id
- subname_name
- admin_state_up
- 状態
- network_id
- network_type
- segmentation_id

- subnet_cidr
- subnet_gateway_ip

次の例では、ポリシーの式を定義するプールプロパティを使用した式をいくつか示します。

1. プール名ベースのポリシー式

   設定 [“プール”] [“名前”] == “ハイエンドプール」

2. プールサブネット名ベースのポリシー式

   設定 [“プール”] [“サブネット名”] ==「us-west-payment-subnet1”

3. ロードバランサーのサブネット名ベースのポリシー式

   設定 [“ロードバランサー”] [“サブネット名”] ==「マスサブネット」

配置ポリシーの追加

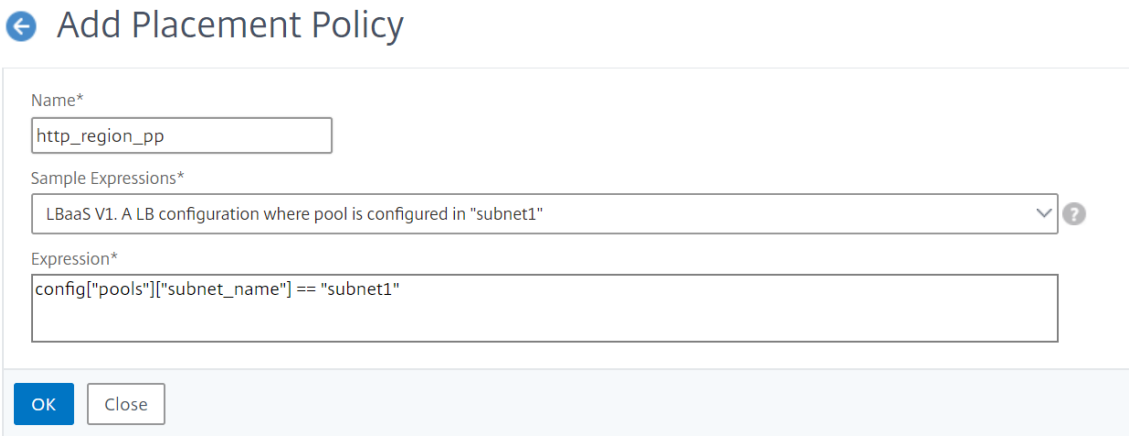
1. Citrix ADM ホームページから、[オーケストレーション] > [クラウドオーケストレーション] > [配置ポリシー] に移動し、[追加] をクリックします。
2. [**Add Placement Policy**] ページで、次のパラメーターを設定します。

   a) Name - 配置ポリシーの名前を入力します。

   b) Frequently Used Expressions - ボックスの一覧から式を選択します。

   c) Expression - 上のフィールドで選択した式に基づき、論理式（ブール式）がこのフィールドに表示されます。必要に応じてボックス名を編集します。

> 注:
>
> 複数のポリシーを作成する場合は、ポリシーが互いに排他的であることを確認してください。



3. [**OK**] をクリックします。

4. **[**** オーケストレーション] > [クラウドオーケストレーション] > [**OpenStack**] > [サービスパッケージ] に移動し、[追加] をクリックします。**

5.「サービスパッケージ」ページで、次のパラメータを設定します。

   a) 名前-サービスパッケージの名前を入力します

   b) 隔離ポリシー- 共有ポリシーを選択

      共有分離ポリシーでは、テナントのロードバランサー構成は、テナントに割り当てられたデバイス中において、他のテナントのロードバランサー構成と共存します。

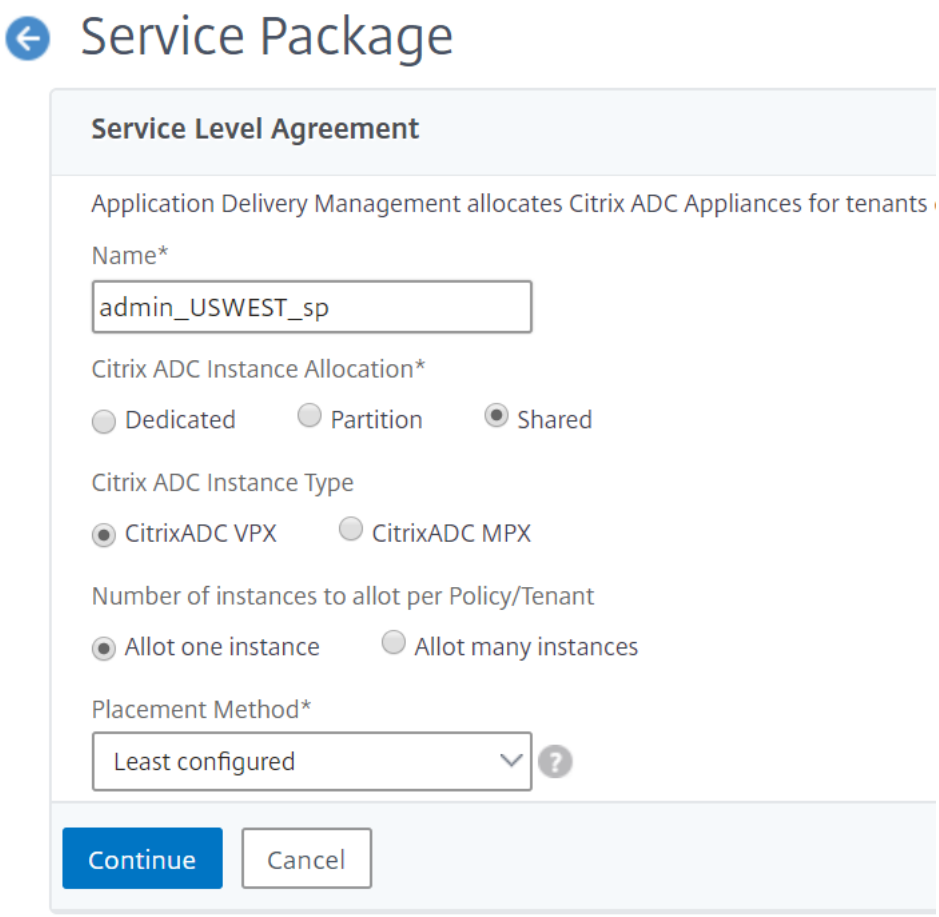
   c) デバイスタイプ - 事前にプロビジョニングされた **Citrix ADC VPX** または Citrix ADC **MPX** を選択してください

      テナントのすべてのロードバランサー構成を 1 つのデバイスに関連付ける場合は、[**Allot one device**] を選択します。テナントの各ロードバランサー構成を、配置ポリシーに基づいて複数のデバイスに配布する場合は、[**Allot many devices**] を選択します。

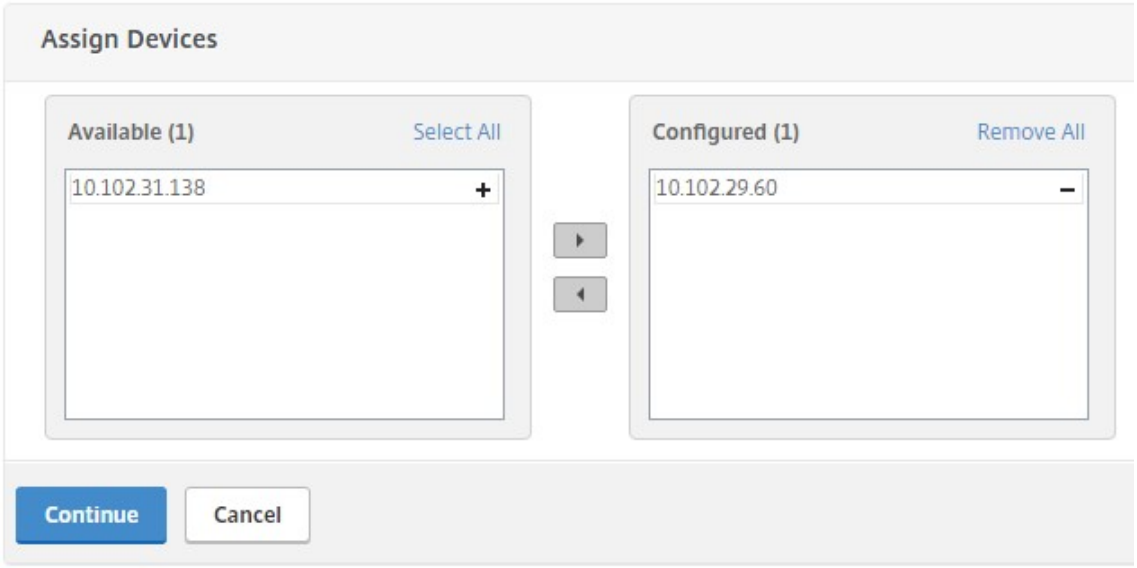
      > 注
      >
      > :Citrix ADC SDX には Citrix ADC VPX がプロビジョニングされているため、Citrix ADC SDX は Citrix ADC VPX インスタンスとしてのみサービスパッケージに追加する必要があります。

   d) 配置方法-「最小構成」を選択

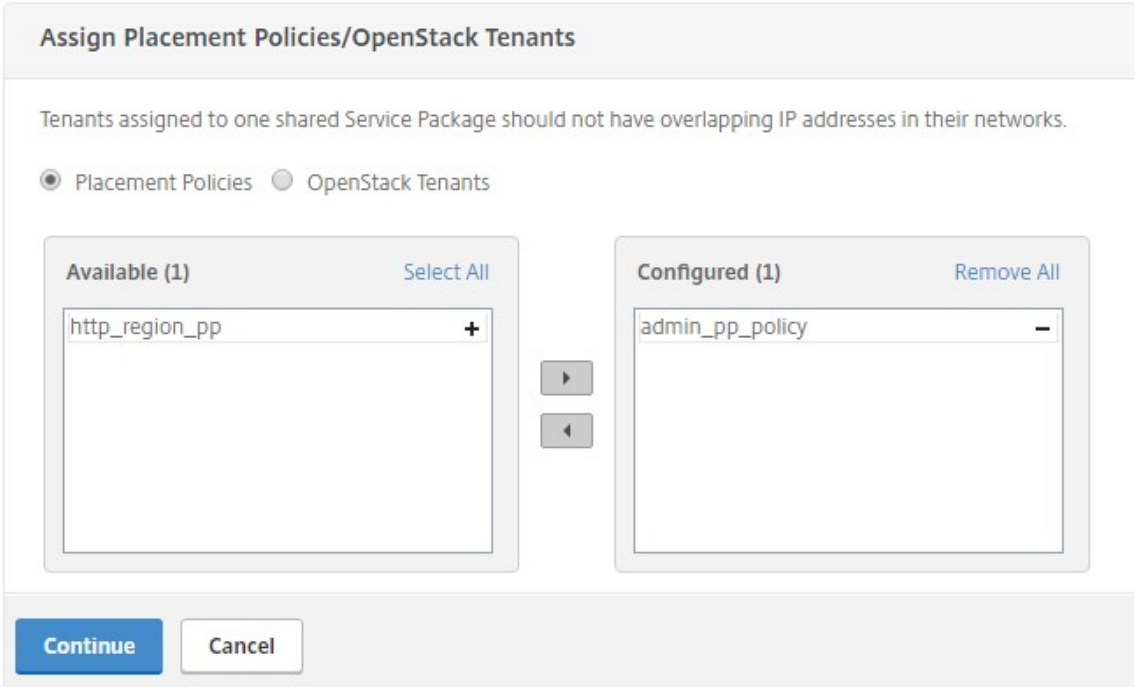
      「最小構成済み」を選択すると、その時点で構成されているプールメンバーの数が最も少ない NetScaler ADC インスタンスがテナントのデバイスとして選択されます。



6. ［続行］をクリックします。
7. ［デバイスの割り当て］セクションで、使用可能な NetScaler ADC デバイスを構成済みのデバイスリストに追加します。



8. ［続行］をクリックします。
9. **[** 配置ポリシーの割り当て**]/[OpenStack** テナント] セクションで、前に作成した配置ポリシーを追加します。



> 注:
>
> ポリシーが見つからない場合、フォールバックメカニズムが復活し、NetScaler ADM はテナントに基づいて NetScaler ADC インスタンスを割り当てます。テナントがどのサービスパッケージにも含まれていない場合、NetScaler ADM は次のエラーメッセージを表示します。「テナント\ <admin\ > はどのサービスパッケージにも含まれておらず、デフォルトのサービスパッケージもありません。

10. ［**Continue**］、［**Done**］の順にクリックします。

NSX Manager：NetScaler ADC インスタンスの手動 Provisioning

February 6, 2024

Citrix Application Delivery Management（ADM）は、VMware ネットワーク仮想化プラットフォームと統合して、Citrix ADC サービスの展開、構成、および管理を自動化します。この統合により、物理ネットワークトポロジに関連する従来の複雑さが解消され、vSphere/vCenter 管理者は Citrix ADC サービスをプログラムにより迅速に展開できるようになります。

この記事では、VMware NSX Manager と Citrix ADM の両方で実行する必要があるタスクのリストを示します。

> 注:
>
> VMware NSX for vSphere 6.2 以降がインストールおよび構成されていること、および負荷分散が必要なエッジゲートウェイ、分散論理ルーターおよび仮想マシンがすでに作成されていることを確認してください。

前提条件

- 最小要件を満たすハードウェアで VMware ESXi Version 4.1 以降をインストールします。
- 最小システム要件を満たす管理用のワークステーションに VMware Client をインストールします。
- 最小システム要件を満たす管理用のワークステーションに、VMware ESXi Version 4.1 に必要な VMware OVF Tool をインストールします。
- サポートされているハイパーバイザーのいずれかに NetScaler ADM をインストールします。

  サポートされているハイパーバイザーに NetScaler ADM ビルド 12.1 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、Citrix ADM 仮想アプライアンスをインストールするために VMware ESXi サーバーに必要な仮想コンピューティングリソースを示しています。

コンポーネント	条件
RAM	8 GB
仮想 CPU	8
記憶域	500 GB
仮想ネットワーク インターフェイス	1
スループット	1Gbps

> 注
>
> : 上記のメモリとハードディスクの要件は、ホスト上で他の仮想マシンが実行されていないことを考慮して、Citrix ADM を VMware ESXi サーバーに展開するためのものです。VMware ESXi サーバーのハードウェア要件は、サーバーで動作する仮想マシンの数によって異なります。

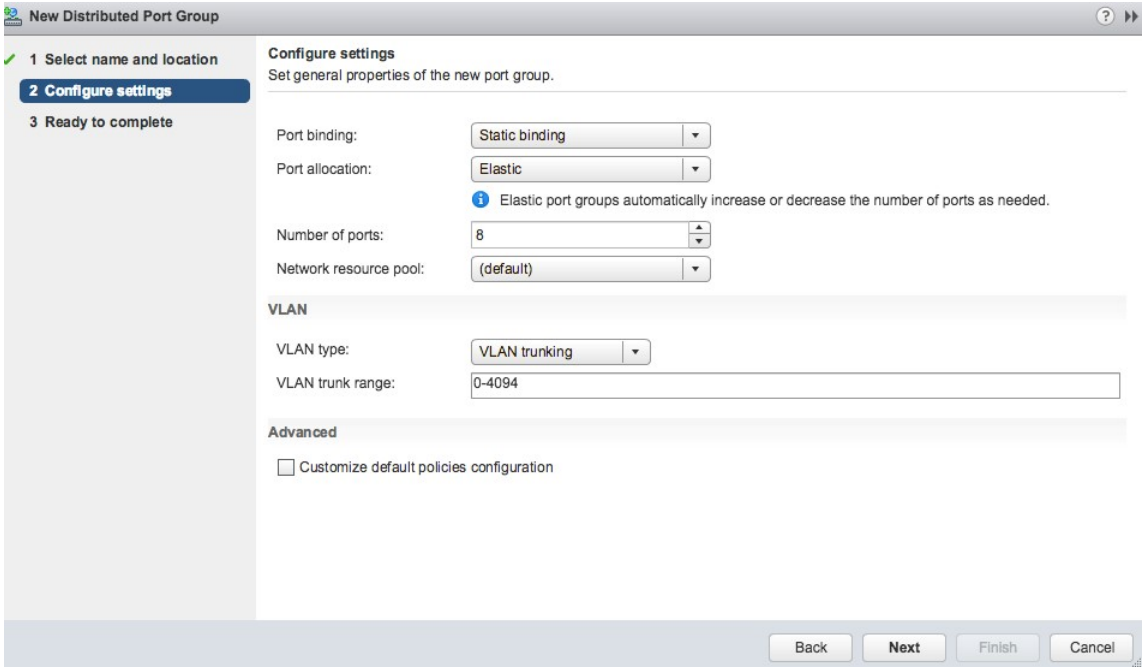
VMware NSX の構成

- 容量の異なる Citrix ADC VPX インスタンスのプールを作成し、さまざまなサービスパッケージに追加します。

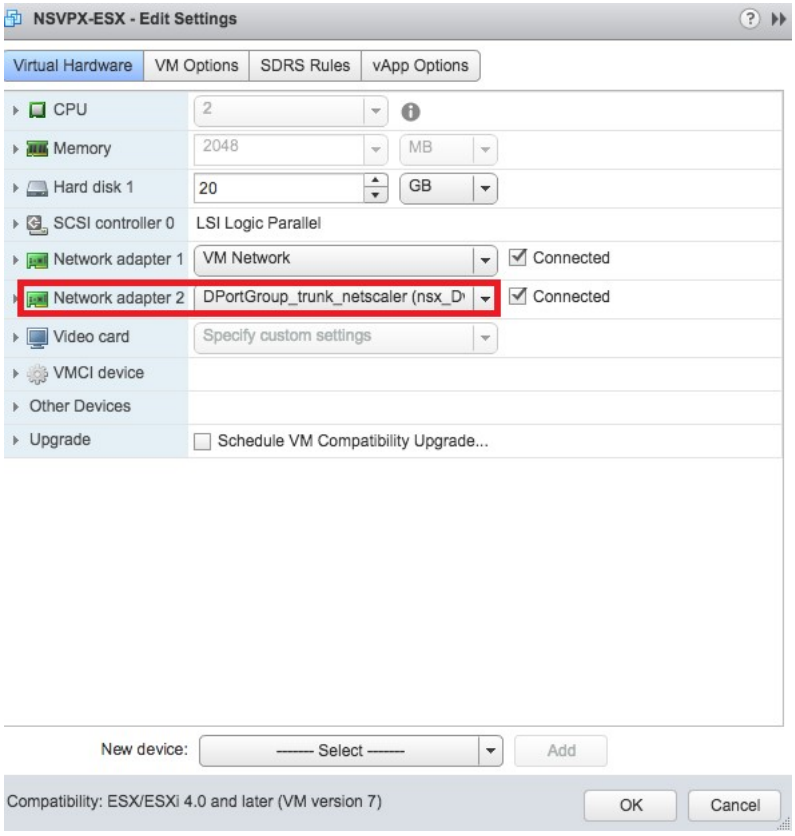
次に例を示します:

- VPX1000 (1 Gbps) の Citrix ADC VPX インスタンスを 5 つ作成します。これらのインスタンスは Gold サービスパッケージに追加されます。
- VPX10 (10 Mbps) の Citrix ADC VPX インスタンスを 5 つ作成します。これらのインスタンスは Bronze サービスパッケージに追加されます。

1. vSphere Client で [**Networking**] に移動し、たとえば「101-105」のように範囲を指定して、種類が VLAN トランク接続のポートグループを作成します（すべての範囲を設定することもできますが、必要な VLAN だけを対象として、種類が VLAN のポートグループを作成します）。

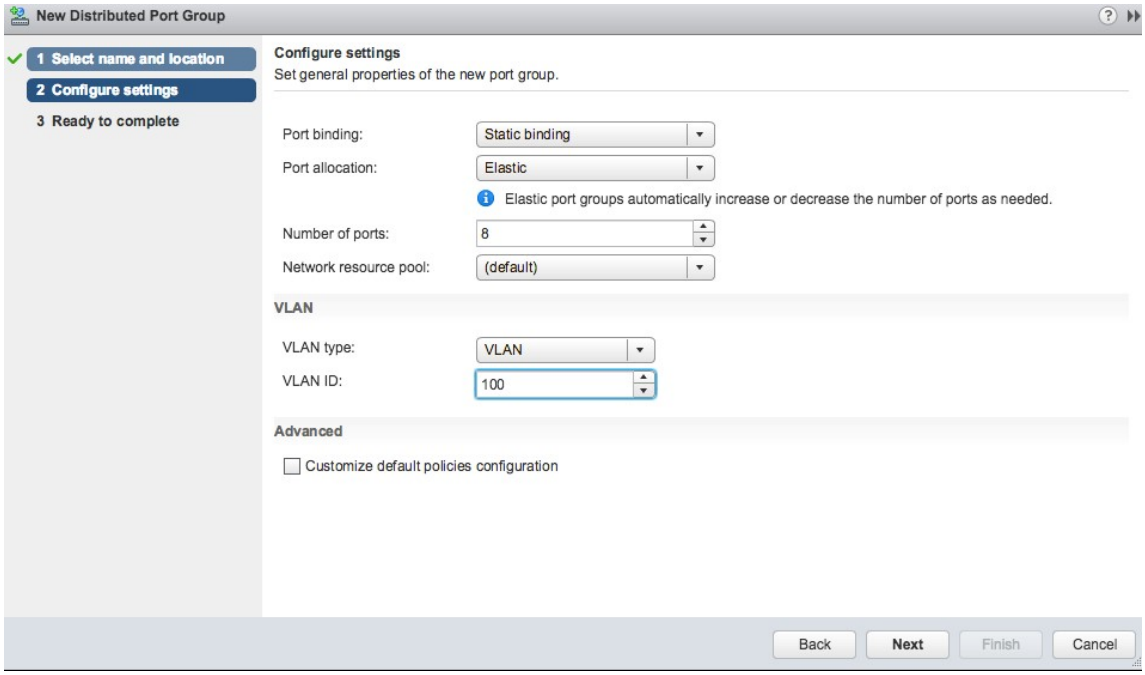


2. NetScaler ADC VPX インスタンスごとに新しいインターフェイスを作成し、上で作成した VLAN 範囲トランクポートグループに接続します。



3. vSphere Client で［**Networking**］に移動し、種類が VLAN のポートグループを作成します。

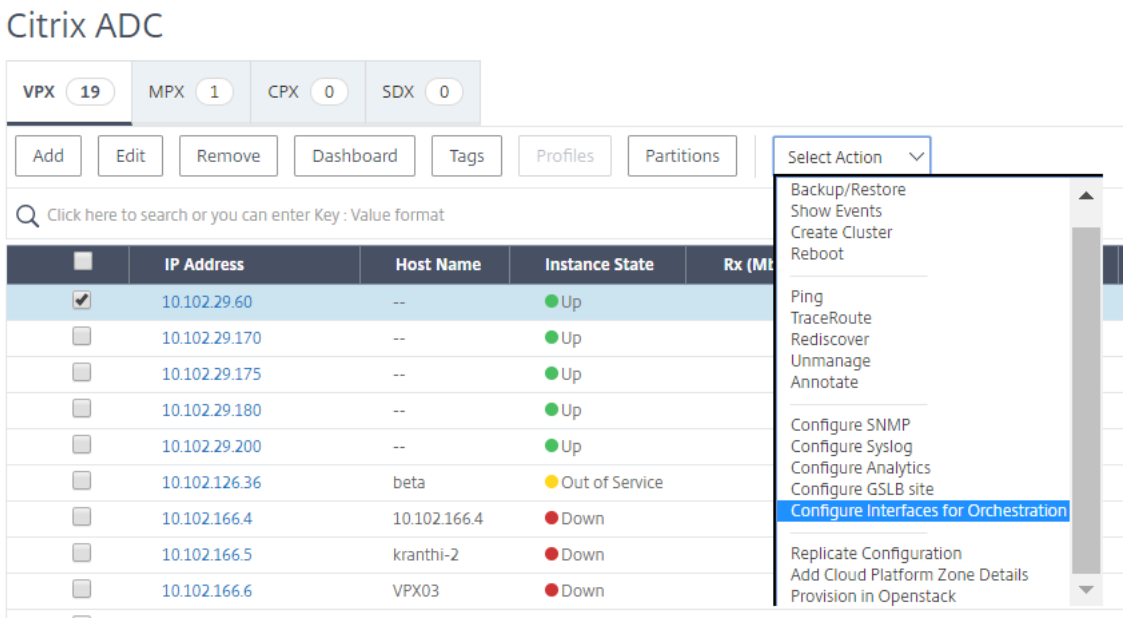
   たとえば、最初のトランク接続のポートグループを 101 から 105 の範囲で作成した場合、VLAN ごとに 1 つずつ、合計 5 つの VLAN ポートグループを作成します。VLAN 101 のポートグループ、VLAN102 のポートグループというように、VLAN 105 まで作成します。



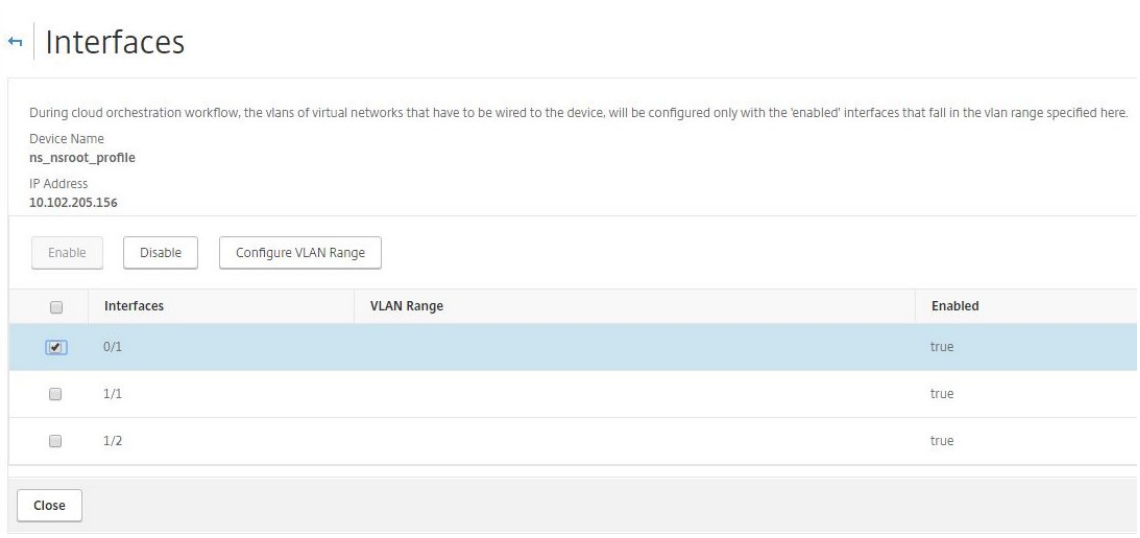
NetScaler ADM での **NetScaler ADC VPX** インスタンスの追加

Citrix ADC VPX インスタンスを Citrix ADM に追加し、各デバイスのトランクグループの VLAN 範囲を指定します。

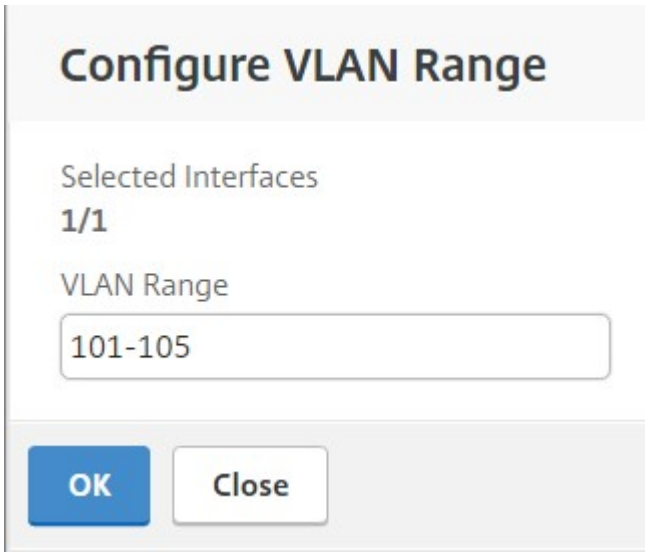
1. Citrix ADM で、[インフラストラクチャ] > [インスタンス] > **[**Citrix ADC VPX]** に移動し、**[**追加 **] をクリックします。
2. [**Citrix ADC VPX** の追加] ページで、インスタンスのホスト名、各インスタンスの IP アドレス、または IP アドレスの範囲を指定し、[プロファイル名] リストからインスタンスプロファイルを選択します。[+] をクリックして新しいインスタンスプロファイルを作成することもできます。
3. [**OK**] をクリックします。
4. Citrix ADC VPX ページのリストから新しく追加された **Citrix ADC VPX** インスタンスを選択し、アクションフィールドの下矢印ボタンをクリックします。[**Configure Interfaces for Orchestration**] を選択します。



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 Citrix ADM に登録して、それらの間の通信チャネルを作成します。

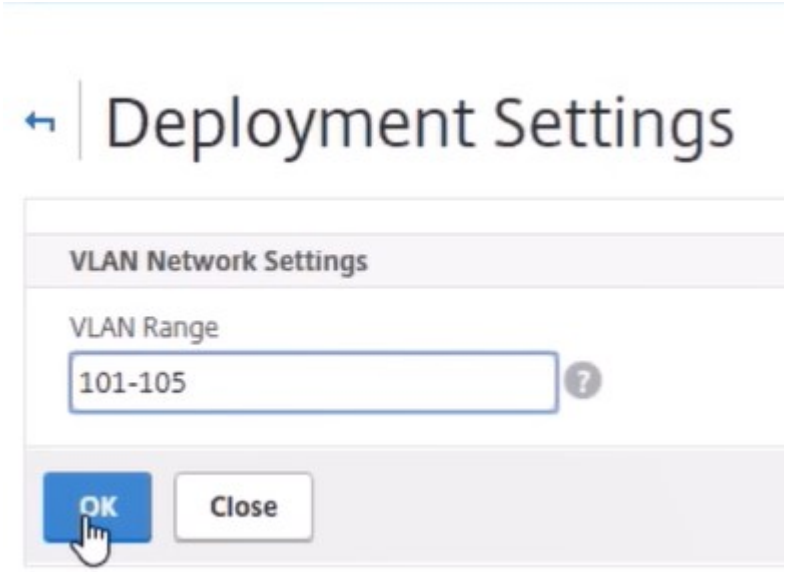
1. Citrix ADM で、ドロップダウンリストから ［オーケストレーション］> ［**SDN** オーケストレーション］> ［**VMware NSX Manager** ］に移動し、［**NSX Manager** 設定の構成］をクリック します。
2. **NSX Manager** の設定ページで、次のパラメータを設定します。

    a) NSX Manager IP Address - NSX Manager の IP アドレス

b) NSX Manager Username - NSX Manager の管理者ユーザー名

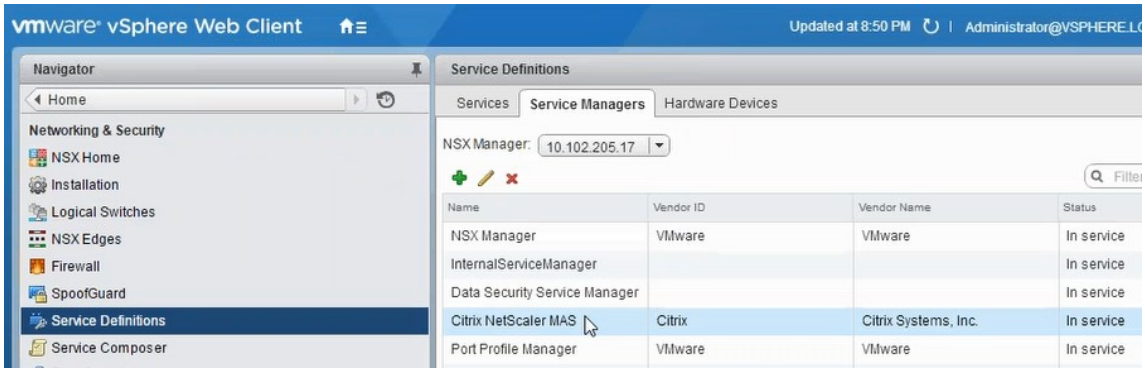
c) Password - NSX Manager の管理者ユーザーのパスワード

3. NSX Manager で使用される **Citrix ADM** アカウントセクションで、**NSX Manager** の Citrix ADC ドライバのユーザー名とパスワードを設定します。NetScaler ADM は、これらのログオン資格情報を使用して NSX Manager からのロードバランサー構成要求を認証します。
4. [**OK**] をクリックします。
5. [オーケストレーション] > [システム] > **[**デプロイ設定**]** に移動します。トランク接続のポートグループに構成されている VLAN の範囲を入力します。



6. vSphere Web Client で NSX Manager にログオンし、[サービス定義**] > [**サービスマネージャ] に移動します。

   Citrix Citrix ADM をサービスマネージャーの 1 人と見なすことができます。これは、登録が成功し、NSX Manager と NetScaler ADM の間に通信チャネルが確立されたことを示します。

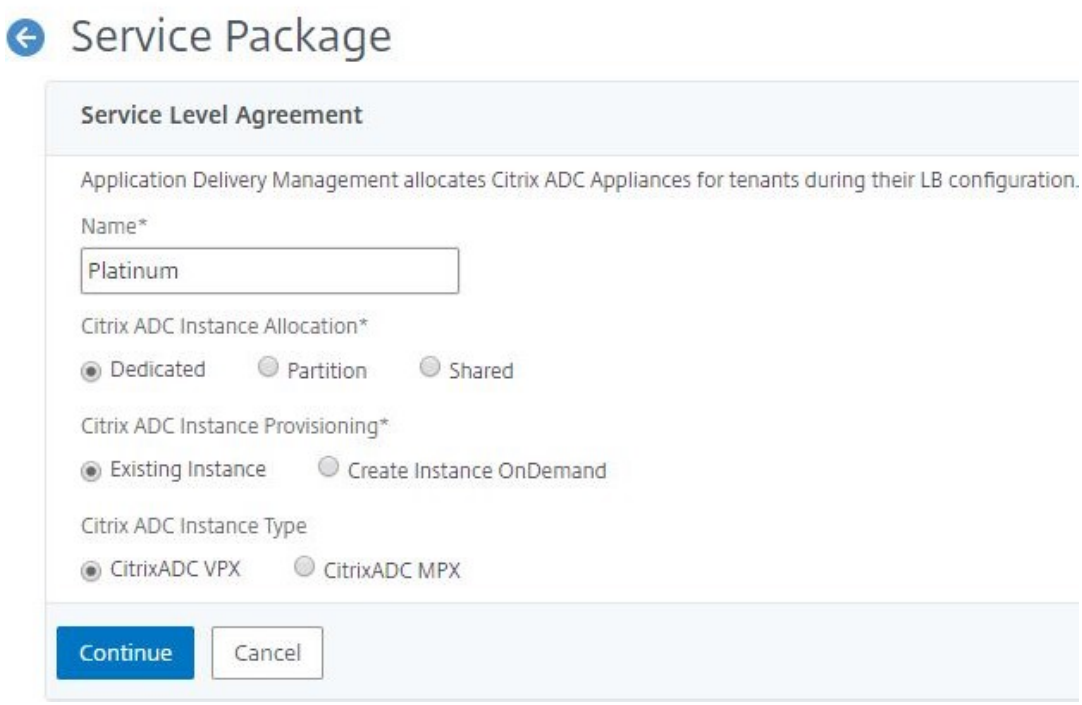


NetScaler ADM でのサービスパッケージの作成

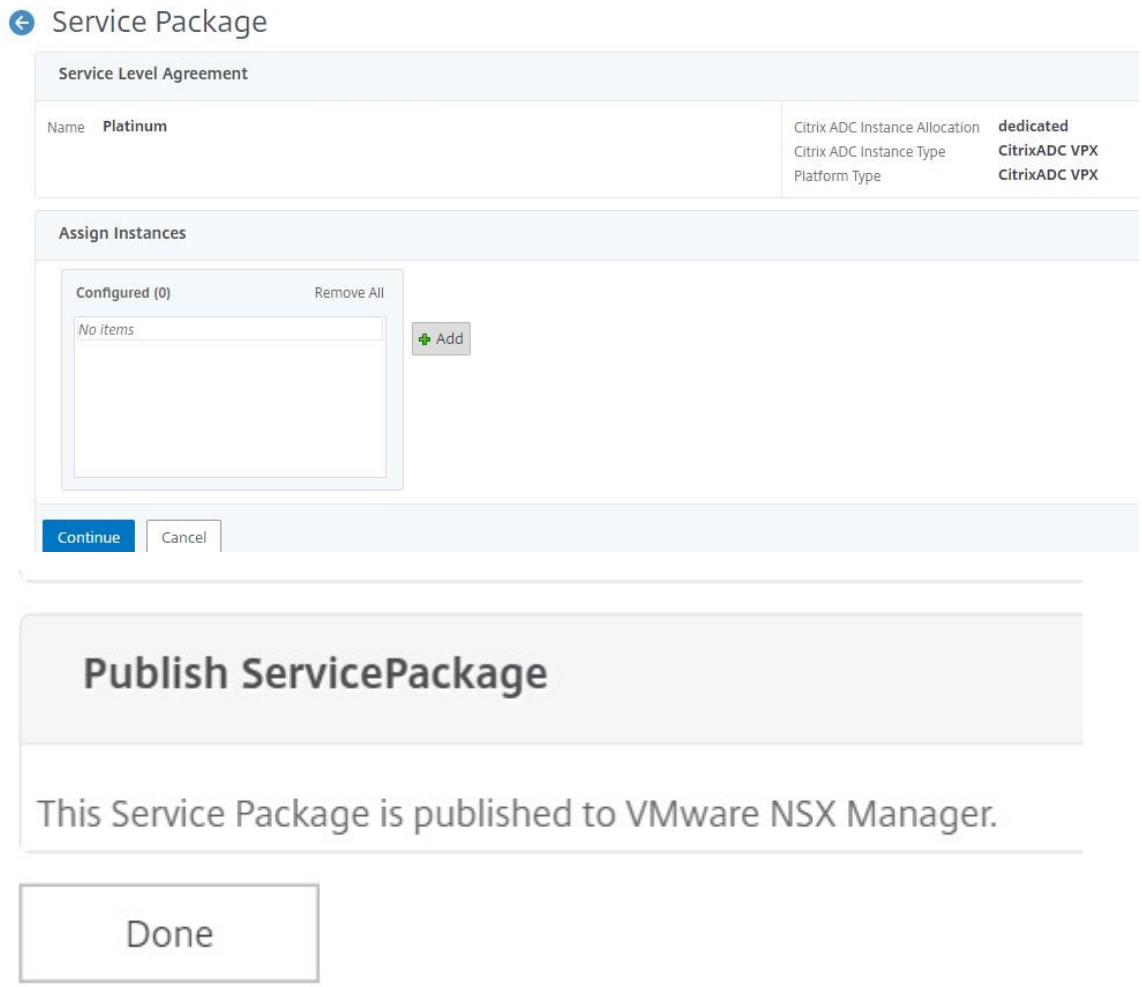
1. Citrix ADM で、[オーケストレーション] > [**SDN** オーケストレーション] > [**VMware NSX Manager**] > [サービスパッケージ] に移動し、[追加] をクリックして新しいサービスパッケージを追加します。
2. 「サービスパッケージ」ページの「基本設定」セクションで、次のパラメータを設定します。
   a) Name - サービスパッケージの名前を入力します。
   b) Isolation Policy - デフォルトでは、分離ポリシーは［Dedicated］に設定されています。
   c) デバイスタイプ—デフォルトでは、デバイスタイプは Citrix ADC VPX に設定されています

   > 注:
   >
   > これらの値は、このバージョンではデフォルトで設定されており、変更することはできません。

   d) ［続行］をクリックします。



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 Citrix ADC VPX インスタンスを Citrix ADM にオフロードできます。

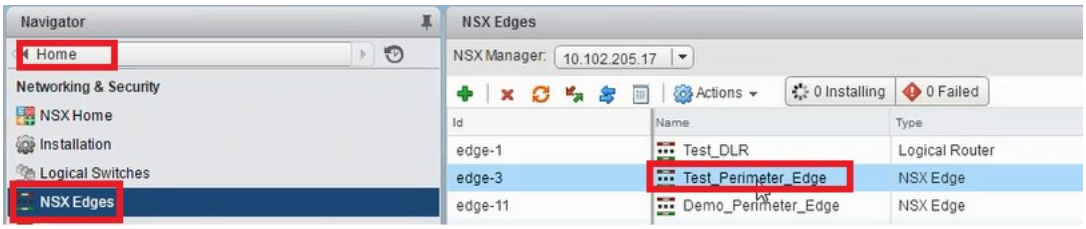
5. **vSphere Web Client** で **NSX Manager** にログインし、**[**** サービス定義**] > [**サービス] に移動します。**

   NetScaler ADM サービスパッケージが登録されていることがわかります。

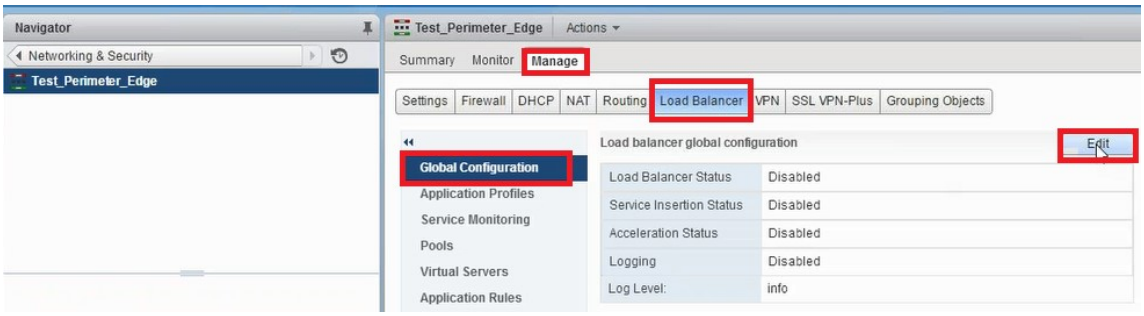
Edge 向けのロードバランサーサービスの挿入の実行

以前に作成した NSX Edge ゲートウェイにロードバランササービスの挿入を実行します（ロードバランシング機能を NSX LB から Citrix ADC にオフロードします）。

1. NSX Manager で、[ホーム] > [**NSX** エッジ] に移動し、構成したエッジ Gateway を選択します。

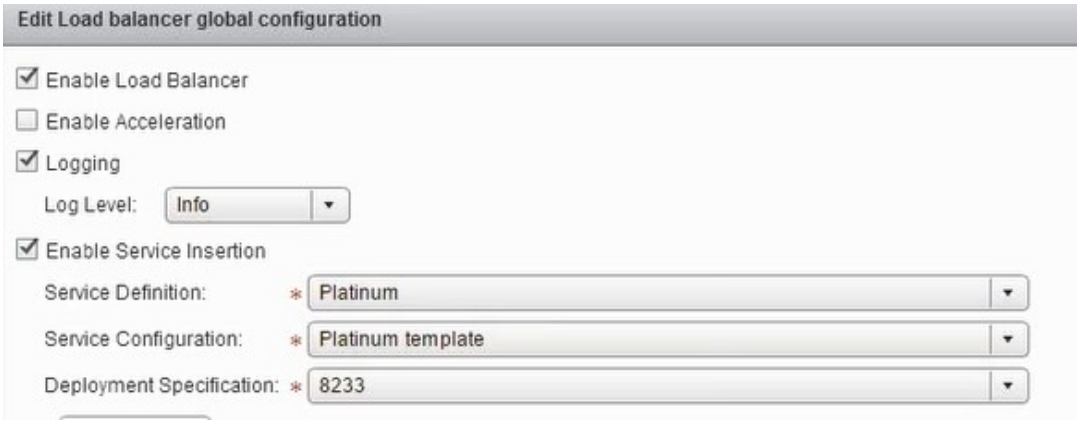


2. [管理] をクリックし、[ロードバランサ] タブで [グローバル構成] を選択し、[編集] をクリックします。

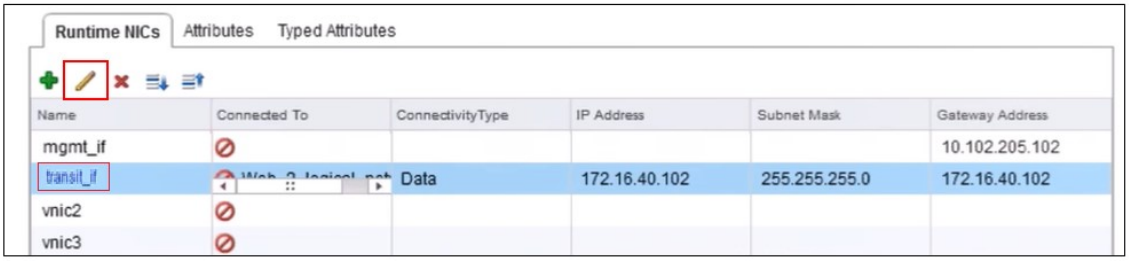


3. [ロードバランサを有効にする]、[ログ]、[サービス挿入を有効にする] の順に選択して有効にします。

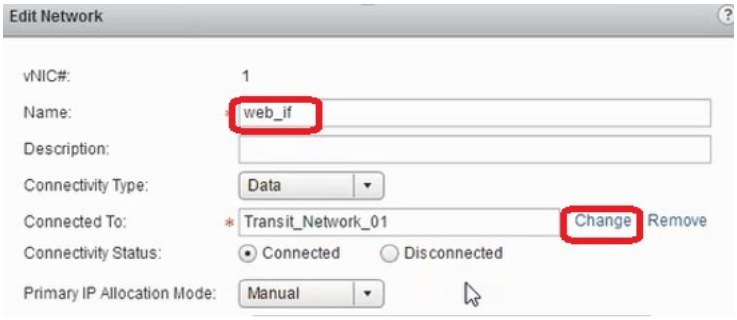
   a) [サービス定義**]** で、 NetScaler ADM で作成され、NSX Manager に公開されたサービスパッケージを選択します。



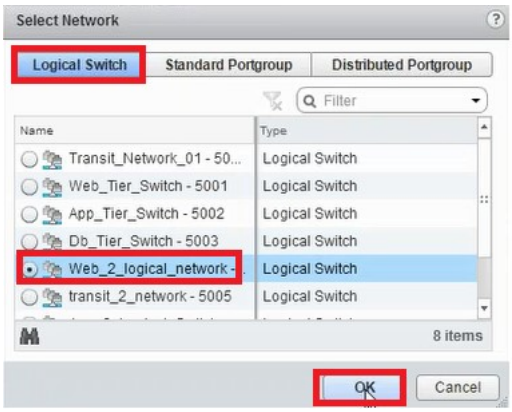
4. 既存のランタイム NIC を選択し、［編集］アイコンをクリックして、NetScaler ADC VPX が割り当てられているときに接続する必要があるランタイム NIC を編集します。



5. NIC の名前を編集し、[接続タイプ] を [データ] に指定して、[変更] をクリックします。

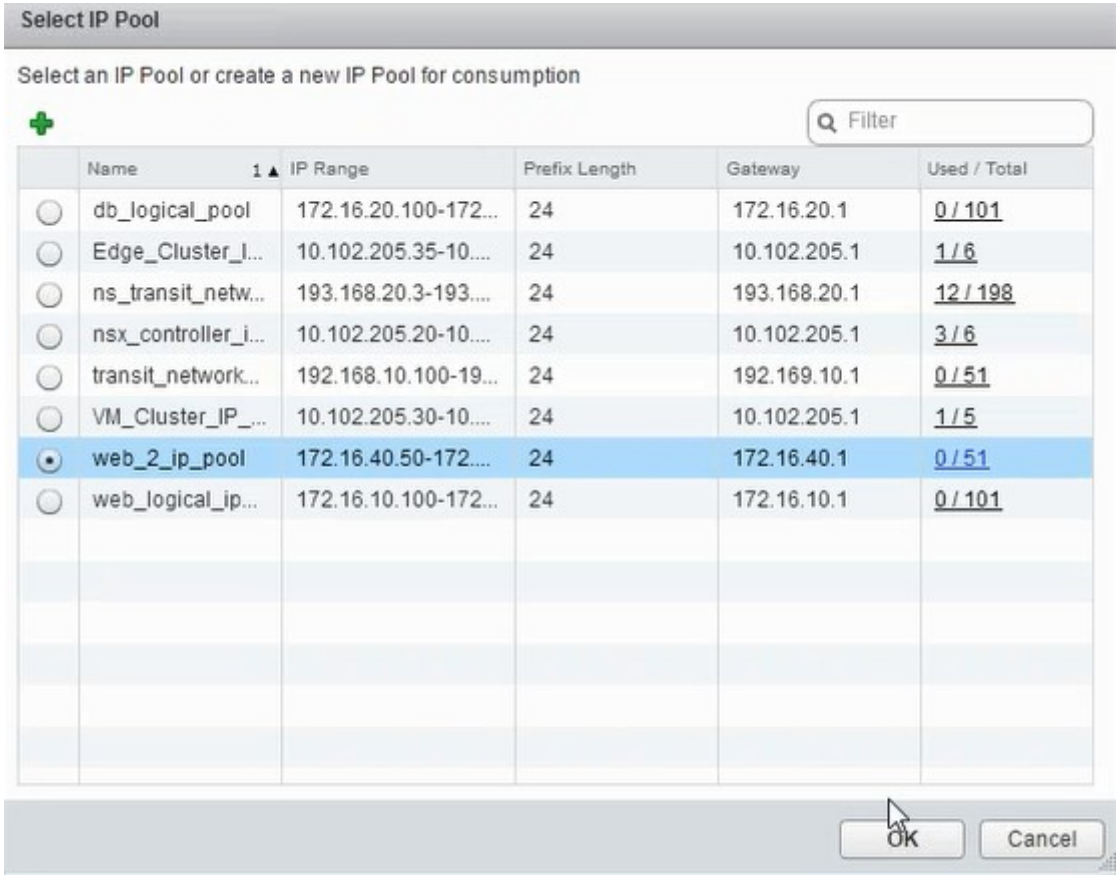


6. 適切な Web 論理スイッチを選択します。



7. [プライマリ **IP** 割り当てモード] で、ドロップダウンリストから [IP Pool] を選択し、[IP Pool] フィールドの下矢印ボタンをクリックします。

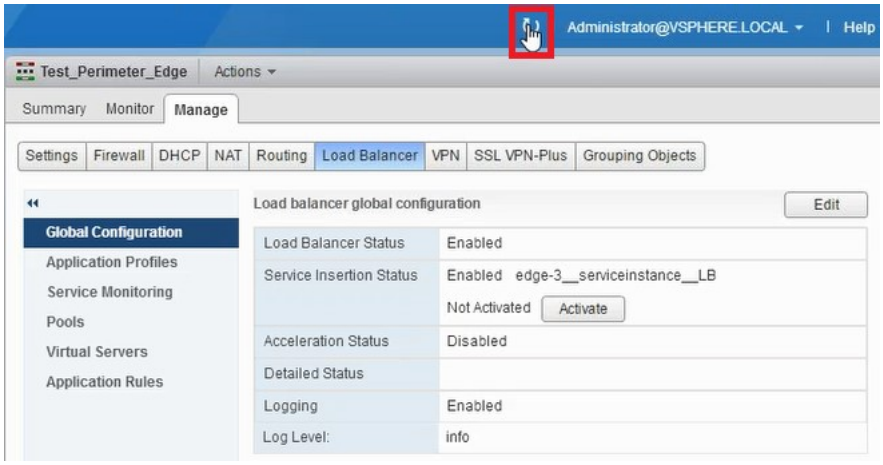
8. **[IP** プールの選択**]** ウィンドウで、適切な IP プールを選択し、[**OK**] をクリックします。

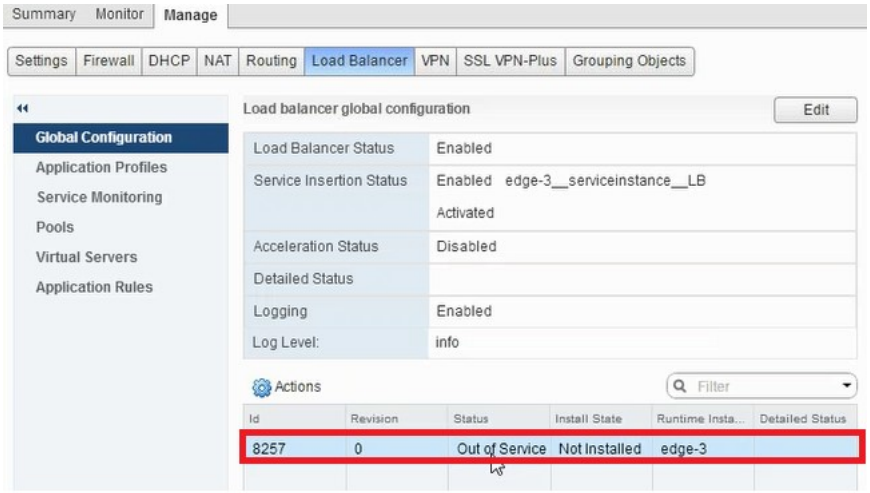


IP アドレスが取得され、NetScaler ADC VPX アプライアンスのソースネット IP アドレスとして設定されます。VXLAN を VLAN にマッピングするために、NSX Manager で L2 ゲートウェイが作成されます。

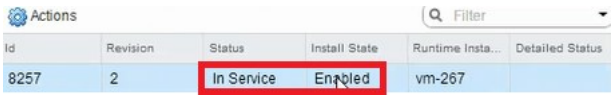
> （注
>
> ）すべてのデータインターフェイスはランタイム NIC として接続されており、分散論理ルーター用のインターフェイスの一部である必要があります。

9. ビューを更新して、実行時の作成を確認します。





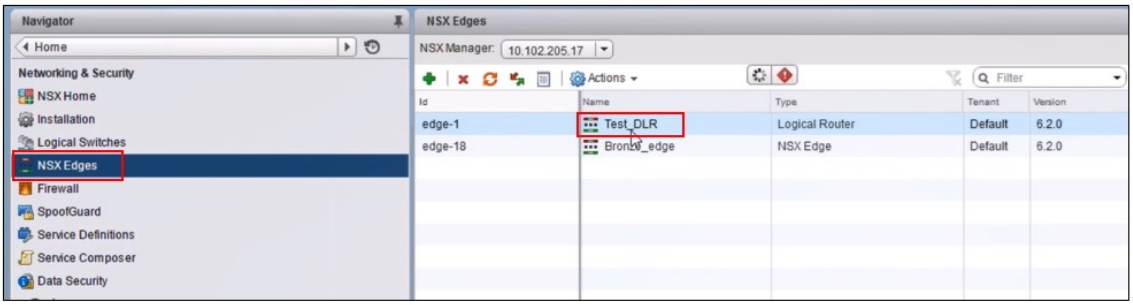
10. 仮想マシンの起動後、[状態] の値が [サービス 中] に変わり、[インストール状態] の値が [有効] に変わります。



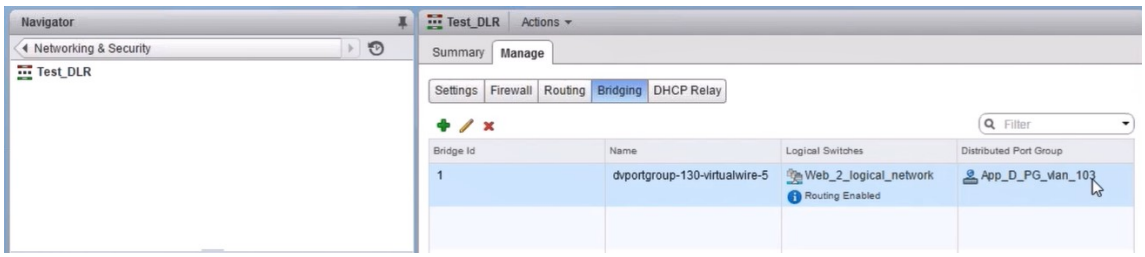
> 注:
>
> NetScaler ADM で、［オーケストレーション］>［リクエスト］に移動して、LB サービス挿入の完了の進行状況の詳細を確認します。

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。

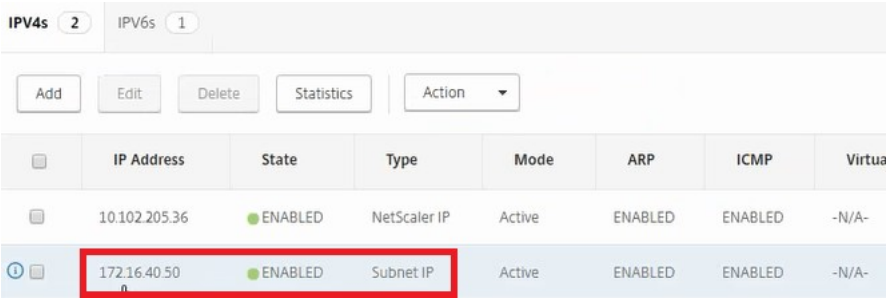


> 注:
>
> L2 Gateway は、データインターフェイスごとに作成されます。

割り当てられた **Citrix ADC** の表示

1. Citrix ADM に表示されている IP アドレスを使用して Citrix ADC VPX インスタンスにログオンします。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 **Citrix ADC VPX** インスタンスの設定

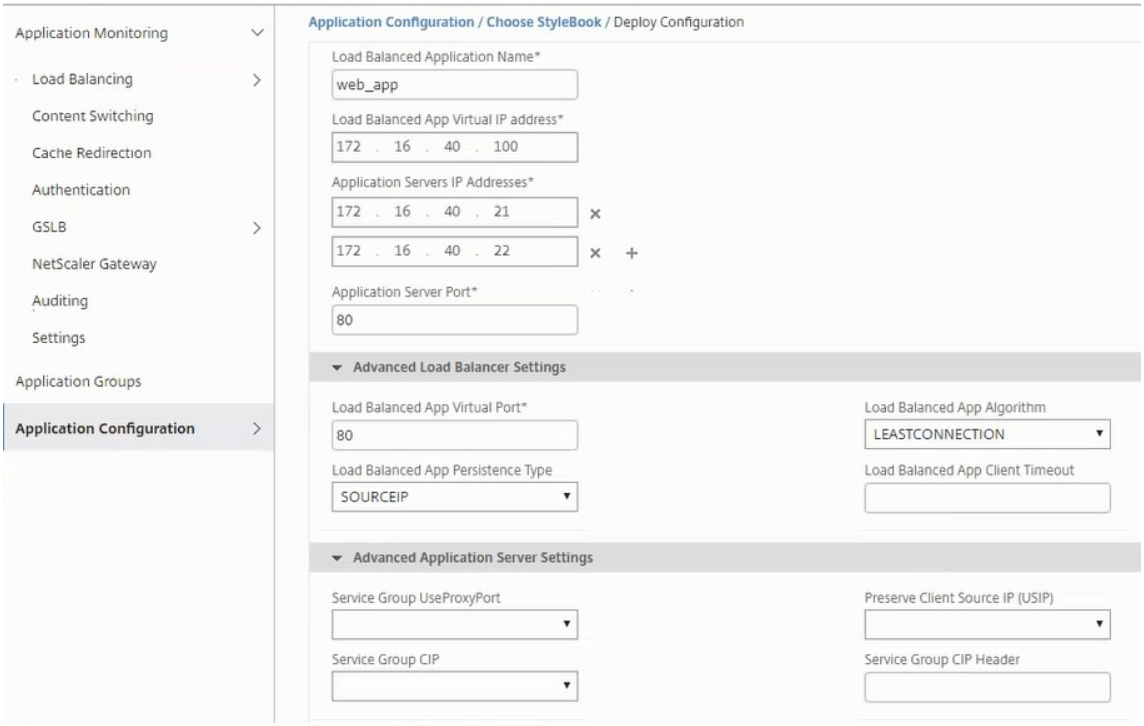
1. NetScaler ADM で、［オーケストレーション］ > ［**SDN** オーケストレーション］ > ［**NSX Manager** の構成］ > ［エッジゲートウェイ］ に移動します。

   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エッジゲートウェイに割り当てられている Citrix ADC インスタンス IP をメモしておきます。

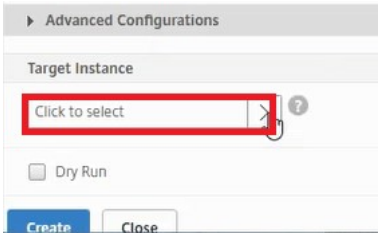
2. 新しい StyleBook を作成します。[アプリケーション] > [構成] に移動し、StyleBook をインポートして、リストから StyleBook を選択します。

   新しい StyleBook を作成する方法について詳しくは、「独自の StyleBook の作成」を参照してください。

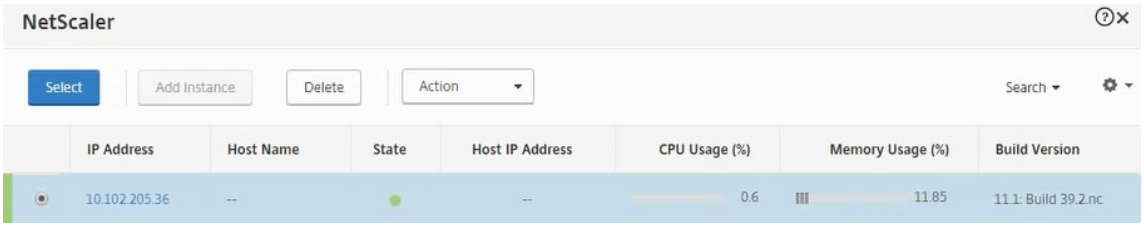
3. すべての必須パラメーターに対して値を指定します。



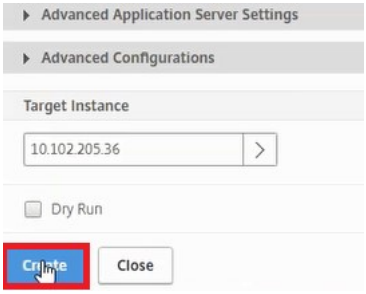
4. これらの構成設定を実行する NetScaler ADC VPX インスタンスを指定します。



5. 前述の IP インスタンスを選択し、[**Select**] をクリックします。

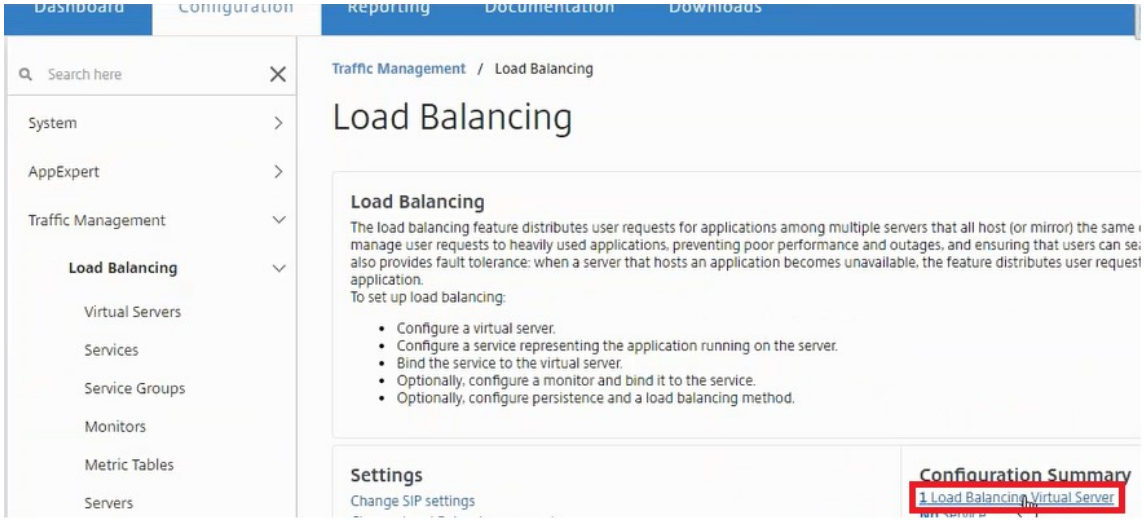


6. [**Create**] をクリックして、選択したデバイスに設定を適用します。

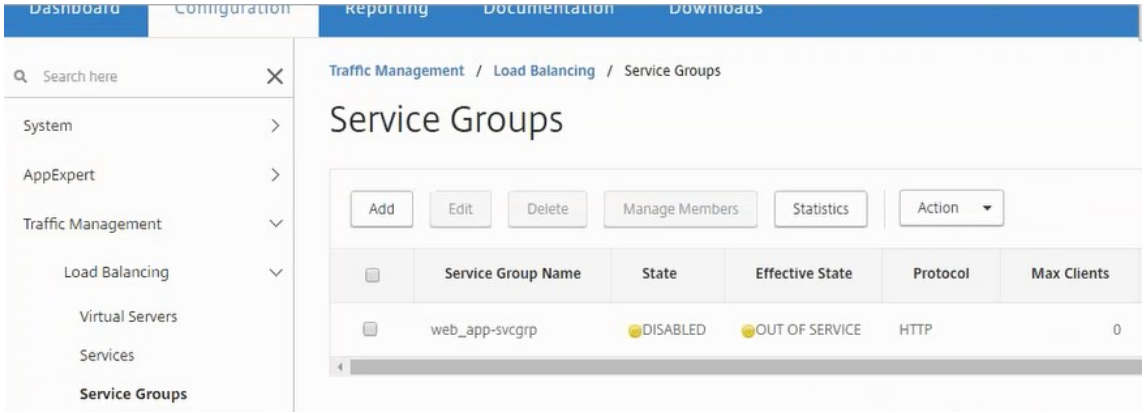


ロードバランサー構成の表示

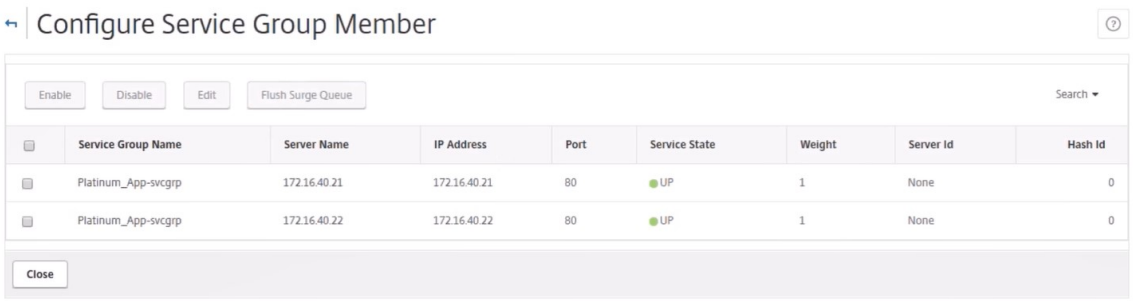
1. NetScaler ADC VPX インスタンスにログオンし、［構成］>［トラフィック管理］>［負荷分散］の順に選択し、作成された負荷分散仮想サーバーを表示します。



作成したサービスグループも表示できます。



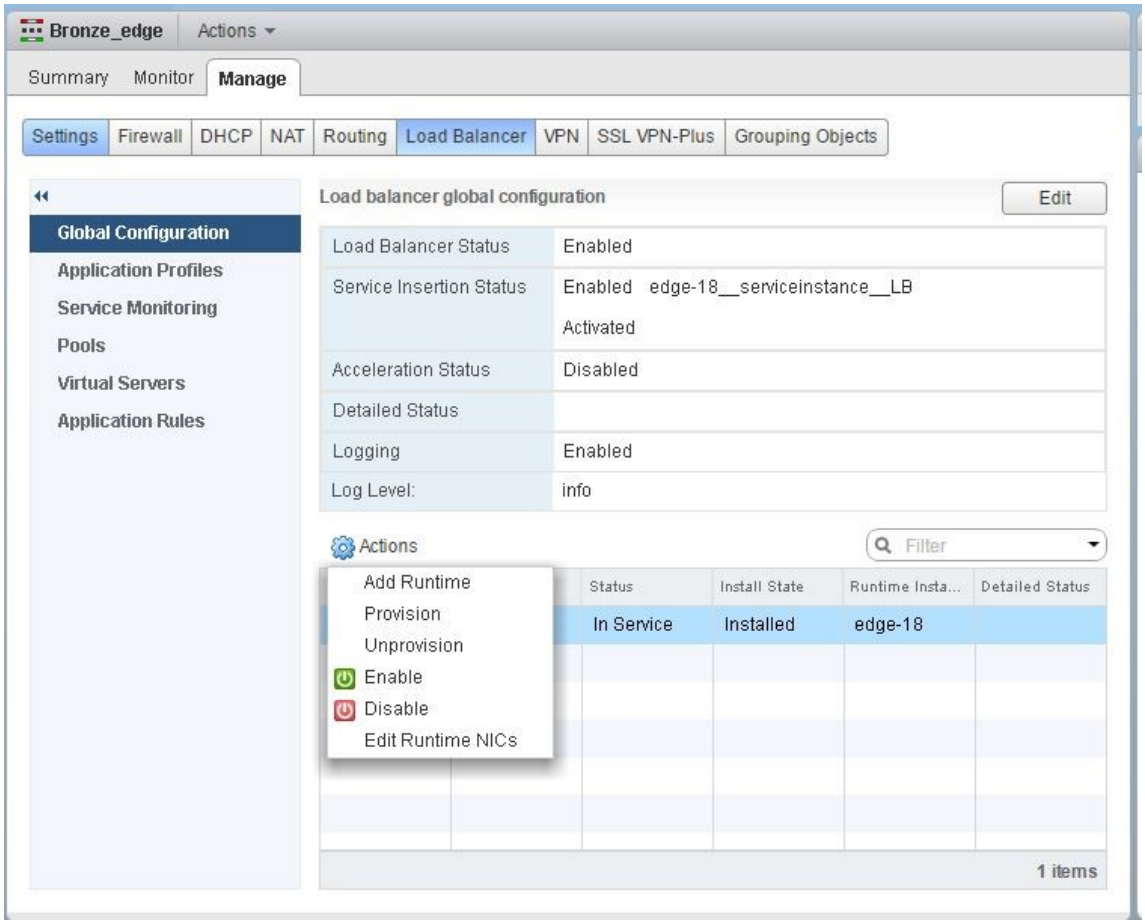
2. サービスグループを選択し、[メンバーの管理] をクリックします。サービスグループに割り当てられたメンバーが［**Configure Service Group Member**］ページに表示されます。



ロードバランサーサービスの削除

1. Citrix ADM で、［アプリケーション］>［構成］に移動し、［**X** ］アイコンをクリックしてアプリケーション構成を削除します。
2. vSphere Web Client で NSX Manager にログオンし、Citrix ADC VPX インスタンスが接続されているエッジゲートウェイに移動します。
3. [管理] > [ロードバランサー] > [グローバル設定] に移動し、ランタイムエントリを右クリックして、[プロビジョニング解除] をクリックします。

   > 注
   >
   > :NetScler MAS のエッジゲートウェイは NSX Manager のランタイムエントリに対応しています。



   NetScaler ADC VPX インスタンスがサービス外になります。
4. NetScaler ADM で、［オーケストレーション］>［**SDN** オーケストレーション］>［**NSX Manager** の構成］>［エッジゲートウェイ］に移動します。削除されたインスタンスに対する Edge ゲートウェイの割り当てが存在しないことを確認します。

NSX Manager：NetScaler ADC インスタンスの自動 Provisioning

February 6, 2024

概要

Citrix Application Delivery Management（ADM）は、VMware ネットワーク仮想化プラットフォームと統合して、Citrix ADC サービスの展開、構成、および管理を自動化します。この統合により、物理ネットワークトポロジに関連する従来の複雑さが解消され、vSphere/vCenter 管理者は Citrix ADC サービスをプログラムにより迅速に展開できるようになります。

VMware NSX Manager での負荷分散サービスの挿入および削除中に、Citrix ADM は Citrix ADC インスタンスを動的にプロビジョニングおよび破棄します。この動的プロビジョニングでは、Citrix ADC VPX ライセンスの割り当てを Citrix ADM で自動化する必要があります。Citrix ADC ライセンスが Citrix ADM にアップロードされると、Citrix ADM はライセンスサーバーの役割を果たします。

前提条件

> 注
>
> この統合は、**vSphere 6.1** 以前の **VMware NSX** でのみサポートされます。

- Citrix ADM、バージョン 12.1 は高可用性でセットアップされ、ESX にインストールされています。
- Citrix ADC VPX、バージョン 12.1
- Citrix ADC VPX インスタンス用 Citrix ADC VPX ライセンス、バージョン 12.1
- 最小要件を満たすハードウェアで VMware ESXi Version 4.1 以降をインストールします。
- 最小システム要件を満たす管理用のワークステーションに VMware Client をインストールします。
- 最小システム要件を満たす管理用のワークステーションに、VMware ESXi Version 4.1 に必要な VMware OVF Tool をインストールします。

Citrix ADM および Citrix ADC インスタンスの高可用性デプロイ

NetScaler ADM 高可用性セットアップをプロビジョニングするには、Citrix ダウンロードサイトからダウンロードした NetScaler ADM イメージファイルをインストールします。NetScaler ADM HA セットアップをプロビジョニングする方法の詳細については、「NetScaler ADM を高可用性で展開する」を参照してください。

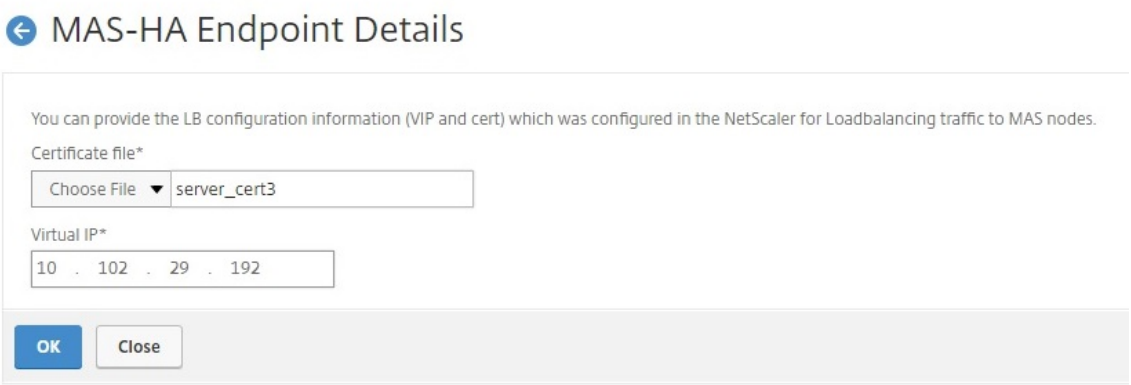
NetScaler ADM HA エンドポイントの詳細の設定

VMware NSX Manager を HA モードでデプロイされた Citrix ADM と統合するには、まず負荷分散 Citrix ADC インスタンスの仮想 IP アドレスを入力する必要があります。また、Citrix ADC 負荷分散仮想サーバーにある証明書ファイルを Citrix ADM ファイルシステムにアップロードする必要があります。

Citrix ADM で負荷分散構成情報を提供するには:

1. Citrix ADM HA ノードで、[システム] > [デプロイメント] に移動します。
2. 右上隅の [**HA** 設定] をクリックし、[**MAS-HA** 設定] ページで [**MAS-HA** エンドポイントの詳細] をクリックします。

3. **MAS-HA Endpoint 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 Citrix ADM サーバーを高可用性に設定すると、2 台のサーバーノードはアクティブ/パッシブモードになります。プライマリ Citrix ADM サーバノードにログオンして VMware NSX Manager を HA の Citrix ADM に登録し、それらの間の通信チャネルを作成します。

VMware NSX Manager を **HA** の **Citrix ADM** に登録するには:

1. プライマリ Citrix ADM サーバノードで、[オーケストレーション] > [**SDN** オーケストレーション] > [**VMware NSX Manager**] に移動します。

2. [**NSX Manager** の設定を設定**]** をクリックします。
3. **NSX Manager** の設定ページで、次のパラメータを設定します。
    a) NSX Manager IP Address - NSX Manager の IP アドレス
    b) NSX Manager Username - NSX Manager の管理者ユーザー名
    c) Password - NSX Manager の管理者ユーザーのパスワード
4.「NSX Manager が使用する Citrix ADM アカウント」セクションで、NSX Manager の Citrix ADC ドライバパスワードを設定します。
5. [**OK**] をクリックします。

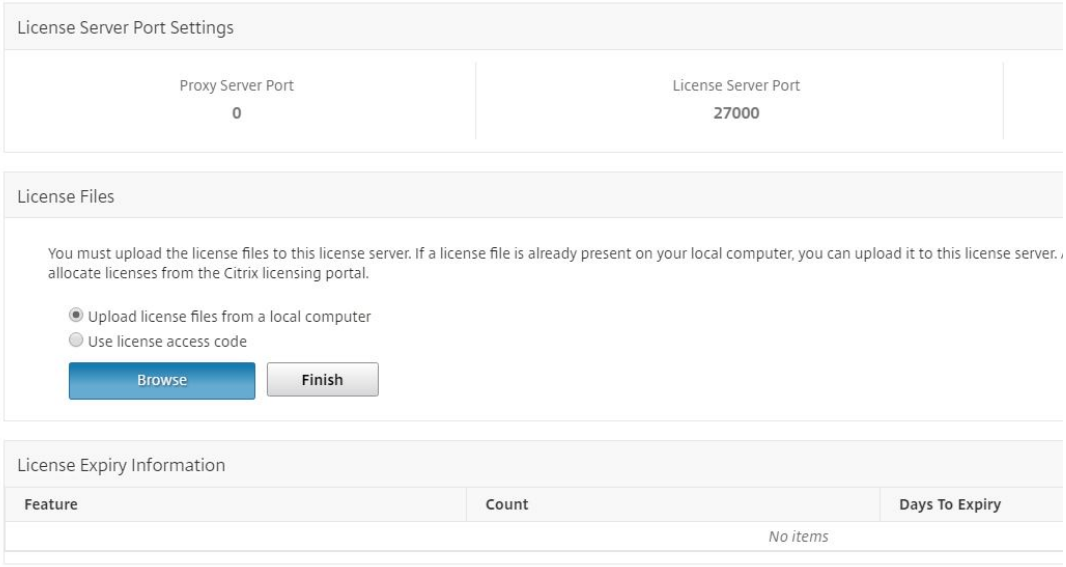
Citrix ADM でのライセンスのアップロード

NetScaler ADC VPX ライセンスを NetScaler ADM にアップロードすると、NSX とのオーケストレーション中に NetScaler ADM がインスタンスに自動的にライセンスを割り当てることができます。

NetScaler ADM にライセンスファイルをインストールするには:

1. Citrix ADM で、[ネットワーク] > [ライセンス] に移動します。
2. [ライセンスファイル] セクションで、次のいずれかのオプションを選択します。
    a) ローカルコンピュータからのライセンスファイルのアップロード**-**ローカルコンピュータに ライセンスファイルがすでに存在する場合は、NetScaler ADM にアップロードできます。ライセンスファイルを追加するには、[**Browse**] をクリックし、追加するライセンスファイル (.lic) を選択します。次に、[完了] をクリックします。
    b) ライセンスアクセスコードを使用する -購入したライセンスのライセンスアクセスコード（LAC）を Citrix から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 LAC 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。



Citrix ADC VPX イメージを **Citrix ADM** にアップロードする

NetScaler ADC イメージを NetScaler ADM に追加すると、NetScaler ADM がサービスパッケージで定義されているとおりにこれらのイメージを使用するようになります。

Citrix ADC VPX イメージを **Citrix ADM** にアップロードするには:

1. NetScaler ADM で、［オーケストレーション］>［**SDN** オーケストレーション］>［**VMware NSX** マネージャー］>［**ESX NSVPX** イメージ］に移動します。
2. ［アップロード］をクリックし、ローカルストレージフォルダーから NetScaler ADC VPX zip パッケージを選択します。

Citrix ADM でサービスパッケージを作成する

NetScaler ADM でサービスパッケージを作成して、NetScaler ADC リソースの割り当て方法を示す SLA のセットを定義します。

Citrix ADM でサービスパッケージを作成するには:

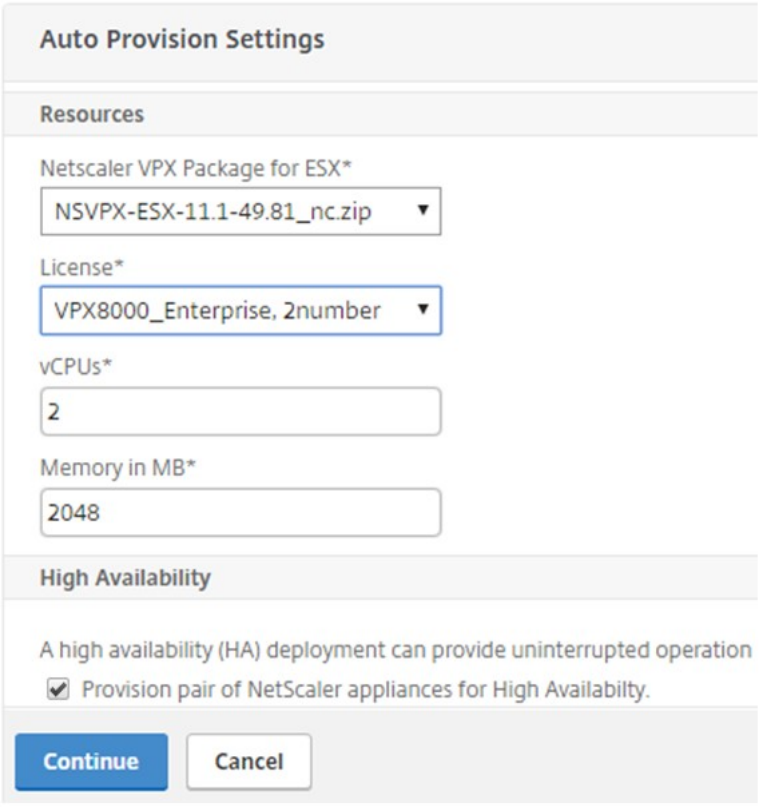
1. Citrix ADM で、[オーケストレーション] > [**SDN** オーケストレーション] > [**VMware NSX Manager**] > [サービスパッケージ] に移動し、[追加] をクリックして新しいサービスパッケージを追加します。
2. 「サービスパッケージ」ページの「基本設定」セクションで、次のパラメータを設定します。
    a) Name - サービスパッケージの名前。
    b) 隔離ポリシー-「専用」を選択
    c) Citrix ADC インスタンス Provisioning-「インスタンスをオンデマンドで作成」を選択します

d) 自動プロビジョニングプラットフォーム- **CitrixADC SDX** を選択

e)［**Continue**］をクリックします

3.［自動プロビジョニング設定］セクションで、最近アップロードした Citrix ADC VPX zip パッケージを選択して NSX プラットフォームにデプロイし、対応するライセンスを選択して、［続行］をクリックします。

> 注:
>
> ［高可用性］セクションで、NetScaler ADC インスタンスを高可用性用にプロビジョニングするチェックボックスをオンにします。



> 注
>
> 上の図のリストボックスに表示されているライセンスの名前、VPX8000_Enterprise, 2number は一例で、以下のように説明されています。
>
> - 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-消費可能な帯域幅は 8 GB
> - Enterprise - Citrix では Standard、Enterprise、Platinum という 3 種類のライセンスを提供しています。
> - 2 番号-このライセンスを使用して、2 つの NetScaler ADC VPX インスタンスを展開できます

> ［ライセンス］リストボックスに表示されるライセンスの 名前は、Citrix から購入したライセンスによって異なります。

4. ［続行］をクリックします。
5. サービスパッケージが NSX Manager に公開されます。NSX Manager で、[サービス定義**] > [**** サービスマネージャ ******] に移動します。Citrix ADM をサービスマネージャーの 1 人と見なすことができます。これは、登録が成功し、NSX Manager と Citrix ADM 間で双方向通信が確立されたことを示しています。

> 注
>
> ：高可用性展開の Citrix ADM では、ライセンスは Citrix ADM ライセンスサーバーノードにのみアップロードされます。NetScaler ADM ノードはアクティブ/パッシブモードです。

Edge のロードバランサーサービス挿入を実行する

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 ADC に負荷分散機能をオフロードします。

NSX Edge ゲートウェイにロードバランシングサービスを挿入するには**:**

1. NSX Manager で、[ホーム] > [ネットワークとセキュリティ] > [**NSX Edge**] に移動し、設定した Edge ゲートウェイをダブルクリックして選択します。
2. [管理] をクリックし、[ロードバランサ] タブで [グローバル構成] を選択し、[編集] をクリックします。
3. [ロードバランサーを有効にする] と [サービス挿入を有効にする] を選択して有効にします。
4. サービス定義で、NSX Manager に公開されたサービスパッケージを選択します。
5. 管理インターフェイス用に 1 つの仮想 NIC を、データインターフェイス用に 1 つ以上の仮想 NIC を設定します。構成に応じて、管理用およびデータ用のネットワークを選択します。

> 注**:**
>
> プライマリ IP 割り当てモードで IP プールオプションを選択します。Citrix ADM は、IP アドレスの手動割り当てまたは DHCP 割り当てをサポートしていません。

6. 更新アイコンをクリックすると、ランタイムの作成が表示されます。

> 注
>
> ： 高可用性デプロイでは 2 つの Citrix ADCVPX インスタンスをデプロイするため、NSX Manager には 2 つのランタイムが作成されます。
>
> 画面に表示される実行時間を確認するには、画面の更新が必要な場合があります。

7. ランタイムを選択し、「アクション」をクリックして、ポップアップメニューから「インストール」を選択します。高可用性展開であるため、同じことをもう 1 つのランタイムについても実行します。

8. 両方の仮想マシンが起動すると、[ステータス] の値が [サービス中] に変わり、[インストール状態] の値は [有効] に変わります。

   > 注:
   >
   > ステータスの変化を確認するには、画面の更新が必要な場合があります。

9. Citrix ADM で、［オーケストレーション］>［リクエスト］に移動して、サービス挿入完了の進行状況の詳細を確認します。ランタイムを作成および更新するリクエストが Citrix ADM に送信されたことがわかります。ランタイムが更新されたら、リクエストを選択して［タスク］ボタンをクリックすると、Citrix ADM が NSX Manager に追加されたことがわかります。

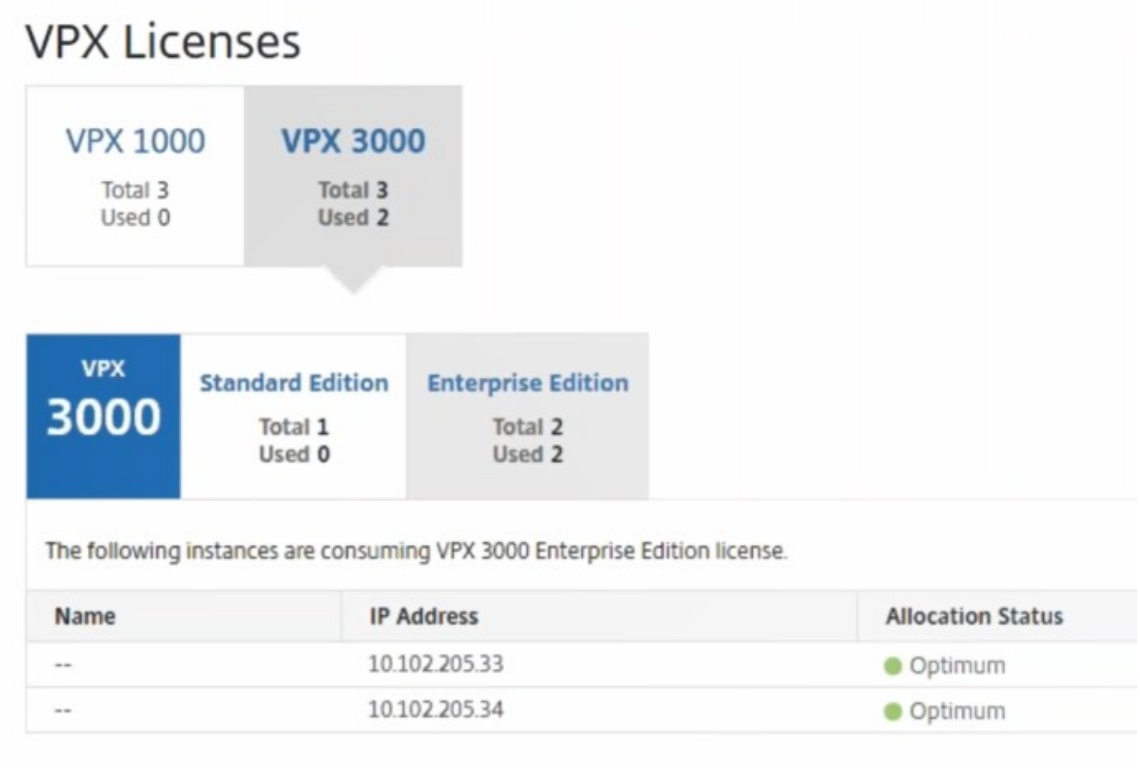
   HA の場合、Citrix ADM で 2 つのランタイムを作成して更新するリクエストが 2 回送信されます。両方のランタイムが更新されたら、両方のリクエストを選択して [タスク] ボタンをクリックすると、NSX Manager に 2 つの Citrix ADM HA ノードが追加されたことがわかります。

10. Citrix ADM で、[オーケストレーション] > [**SDN** オーケストレーション] > [**VMware NSX Manager**] > [エッジゲートウェイ] に移動します。右側のパネルでは、Citrix ADC VPX が NSX Edge ゲートウェイに追加されていることを確認できます。

    高可用性の場合、高可用性モードの 2 つの NetScaler ADC VPX インスタンスが NSX Edge Gateway に追加されていることがわかります。

11. Citrix ADM で、［ネットワーク］>［ライセンス］>［**VPX** ライセンス］に移動します。NetScaler ADC VPX ライセンスとインストールしたエディションを選択します。

    高可用性モードの NetScaler ADC VPX インスタンスは 2 つのライセンスを消費し、ステータスは以下のように画面に表示されます。



サービスの挿入が完了したら、StyleBook を使用して、次のいずれかの方法で NetScaler ADC インスタンスを構成できます。

- VMware NSX Manager GUI で Citrix ADC VPX のロードバランシングサービスを設定する
- Citrix ADM GUI で Citrix ADC VPX の負荷分散サービスを構成する

VMware NSX Manager GUI で **Citrix ADC VPX** のロードバランシングサービスを設定する

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。

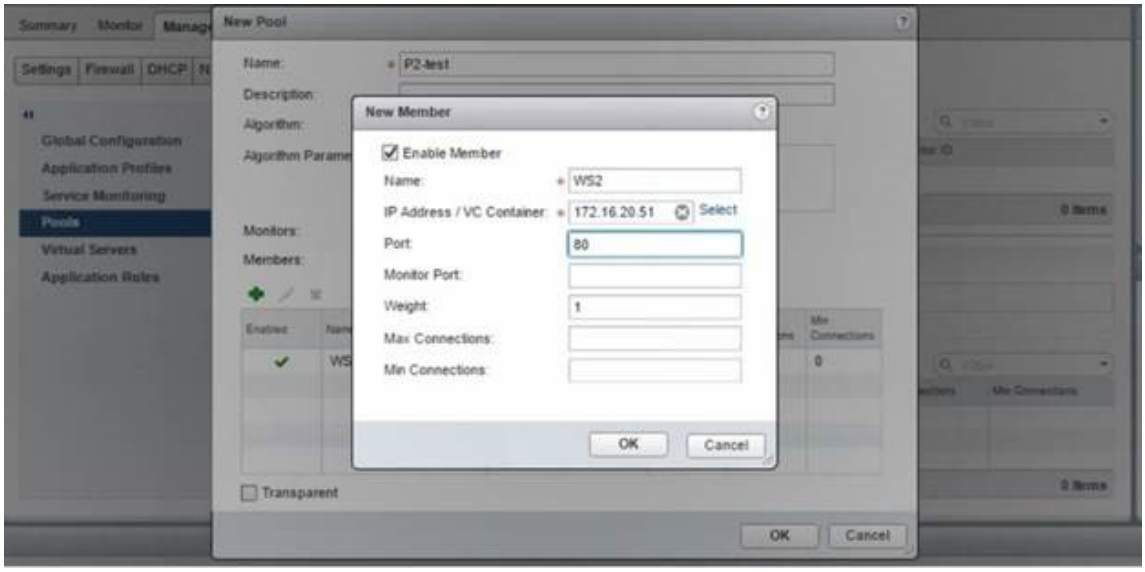
d) Members - ［+］をクリックしてプールにメンバーを追加し、［New Member］ウィンドウで必須パラメーターを入力します。

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。



仮想サーバーを作成する

仮想サーバーのセットを作成し、各仮想サーバーにプールを割り当てます。

1. 「管理」をクリックし、「ロードバランサー」タブで「仮想サーバー」を選択し、「**+**」アイコンをクリックして仮想サーバーを追加し、次のパラメーターを設定します。

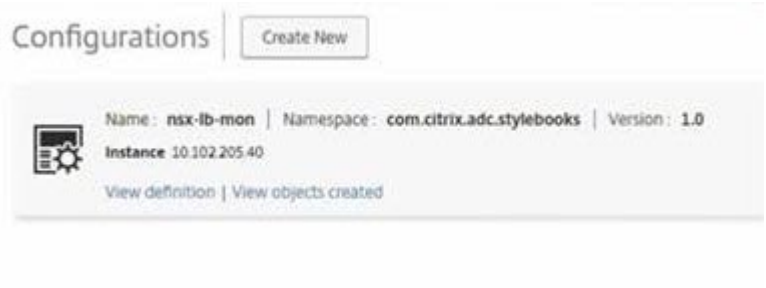
a) アプリケーションプロファイル-デフォルトでは、Citrix ADM で作成したサービスプロファイルが表示されます。

b) Name - 仮想サーバーの名前。

c) IP Address - ［Select］をクリックして既存の IP アドレスのプールを選択するか、新しい IP のプールを作成します。

d) Default pool - ボックスの一覧でデフォルトのプールを選択します。

2. [**OK**] をクリックします。
3. NetScaler ADM で、[オーケストレーション] > [リクエスト] に移動して、選択した 1 つ以上の NetScaler ADC インスタンスでのサービス作成完了の進行状況の詳細を確認します。
4. Citrix ADM で、[アプリケーション] > [構成] に移動し、「nsx-lb-mon」構成パックが作成されていることを確認します。



Citrix ADM GUI で **Citrix ADC VPX** の負荷分散サービスを構成する

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。HA の場合、構成は HA にある両方の Citrix ADC インスタンスにデプロイされます。

StyleBooks を使用して構成パックを作成するには:

1. Citrix ADM で、[アプリケーション] > [構成] > [** 新規作成] に移動し、リストから [HTTP/SSL 負荷分散（モニター付き）] StyleBook** を選択します。StyleBook でユーザーインターフェイスページが表示されます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。
2. すべての必須パラメーターに対して値を指定します。
3. NSX 環境でプロビジョニングされているターゲットの Citrix ADC VPX インスタンスを選択し、「作成」をクリックして、選択したデバイスに構成を適用します。高可用性展開であるため、高可用性モードのインスタンスを選択します。

Citrix ADC VPX インスタンスでの仮想サーバーとサービスグループの作成の検証

Citrix ADC VPX インスタンスにログオンすると、サービスグループと仮想サーバーが作成されていることを確認できます。

サービスグループと仮想サーバを表示するには、次の手順で行います。

1. NetScaler ADC VPX インスタンスにログオンします。高可用性を導入するには、高可用性環境にある両方の Citrix ADC インスタンスにログオンする必要があります。
2. [構成] > [システム] > [ネットワーク] に移動します。右側のペインで、追加された IP アドレスを確認できます。IP アドレスのハイパーリンクをクリックして詳細を表示します。NSX に追加された Web インターフェイスの IP アドレスと同じサブネット IP アドレスが表示されます。

3. 次に、[トラフィック管理] > [負荷分散] > [仮想サーバー] に移動し、仮想サーバーの詳細を表示します。
4. 次に、サービスグループに移動して、サービスグループの詳細を表示します。
5. 最後に、[構成] > [システム] > [ライセンス] に移動し、このインスタンスに適用されているライセンスを表示します。

負荷分散サービスを削除する

NSX Manager にデプロイされた NetScaler ADC VPX インスタンスで負荷分散サービスが不要になった場合は、以前に実行したサービスの挿入を削除できます。

構成とサービス挿入を削除するには:

1. Citrix ADM で、［アプリケーション］>［構成］に移動し、作成したアプリケーション構成を選択し、［X］アイコンをクリックして構成を削除します。
2. NSX Manager で、Citrix ADC VPX インスタンスが接続されているエッジゲートウェイに移動します。**[** 管理] > [ロードバランサー] > [グローバル設定] に移動し、ランタイムエントリを右クリックして [プロビジョニング解除] をクリックします。** 仮想マシンの表示が非稼動状態になります。
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。削除したインスタンスに対する Edge ゲートウェイのマッピングが存在しないことを確認します。

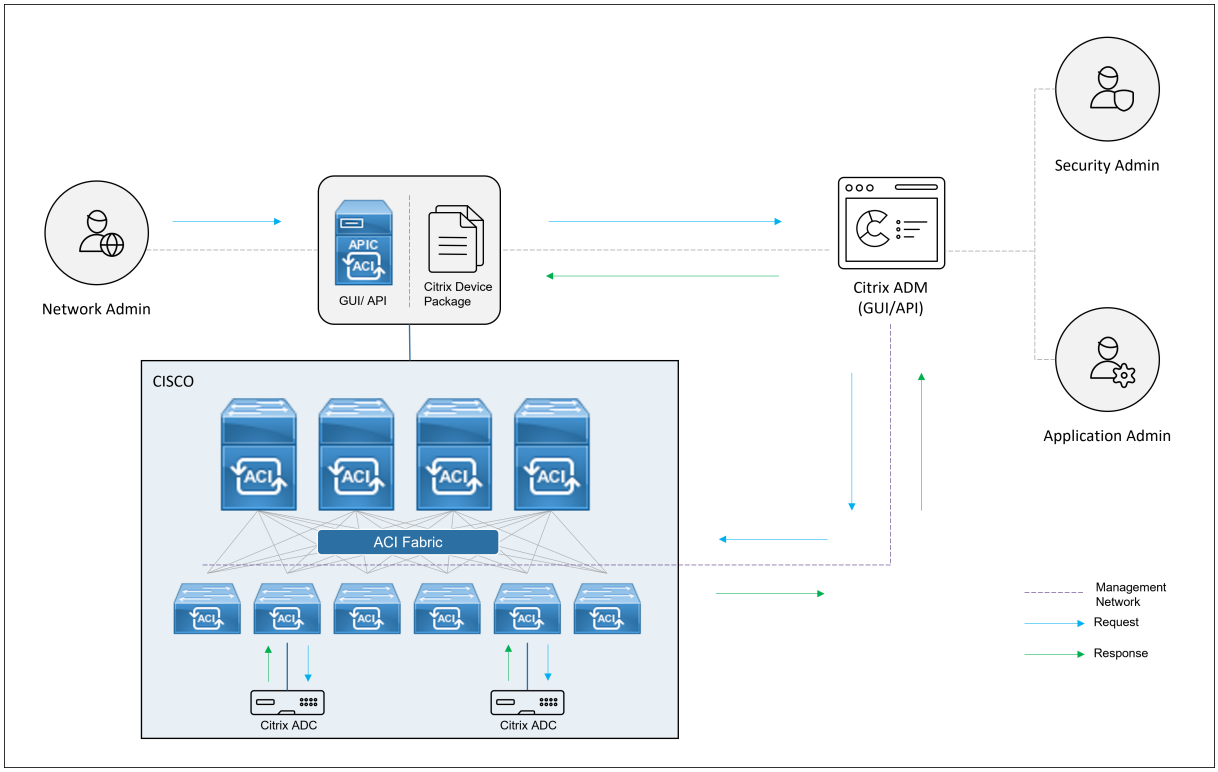
Cisco ACI ハイブリッドモードで **NetScaler ADM** を使用する **NetScaler ADC** オートメーション

February 6, 2024

Cisco ACI では、バージョン 1.3（2f）でハイブリッドモードのサポートが導入されています。ハイブリッドモードでは、アプリケーションポリシーインフラストラクチャコントローラー（APIC）を使用してネットワーク自動化を実行し、L4-L7 構成を APIC のデバイスマネージャーとして機能する Citrix Application Delivery Management（ADM）に委任できます。

Citrix ADC ハイブリッドモードソリューションは、ハイブリッドモードのデバイスパッケージと Citrix ADM でサポートされています。APIC のハイブリッドモードデバイスパッケージをアップロードする必要があります。このパッケージは、Citrix ADC のすべてのネットワーク L2-L3 構成可能なエンティティを提供します。アプリケーションパリティは、StyleBook によって Citrix ADM から APIC にマッピングされます。つまり、StyleBook は、特定のアプリケーションの L2〜L3 構成および L4〜L7 構成間の参照として機能します。APIC for Citrix ADC からネットワークエンティティを設定する際には、StyleBook 名を指定する必要があります。

次の図は、ハイブリッドモードソリューションにおける NetScaler ADC 概要を示しています。

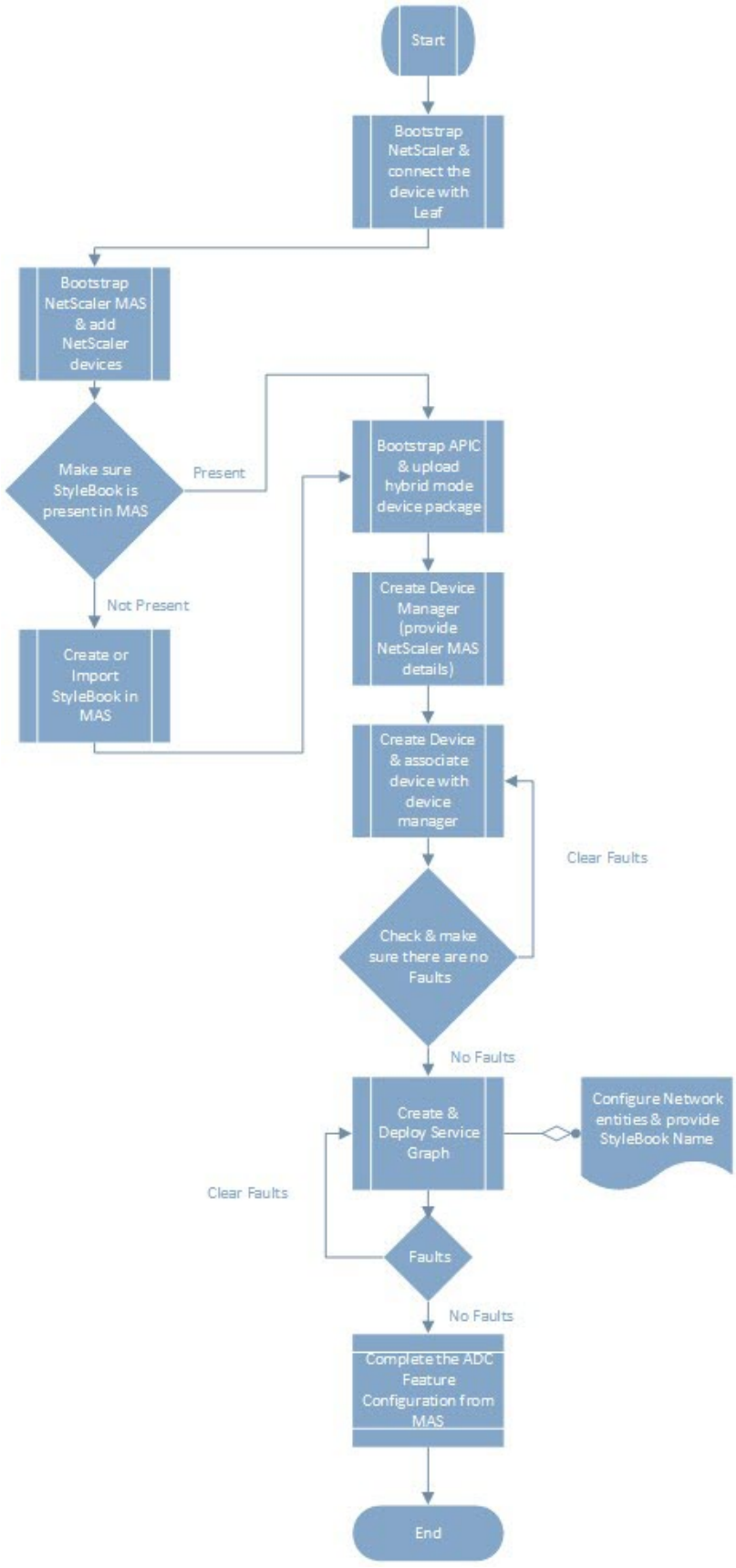


ハイブリッドモードでは、NetScaler ADC 構成は次の 2 つのフェーズで実行されます。

1. Cisco APIC からネットワーク切り替えを実行する。
2. 構成は Citrix ADM から行います

どのアプリケーションの場合も、ネットワーク管理者は、Cisco APIC でサービスグラフを作成および展開するときに、IP アドレス、ポート、VLAN（自動）などの特定の情報を指定する必要があります。これらの構成の詳細は、デバイスパッケージを介して Citrix ADM にプッシュされ、Citrix ADM がそれらを内部で処理して Citrix ADC を構成します。アプリケーション管理者は、Citrix ADM の StyleBook を使用してアプリケーションの ADC 関連の構成を作成し、これらの構成が Citrix ADM から Citrix ADC にプッシュされます。Cisco APIC と Citrix ADM は、管理ネットワークを介して ADC と通信します。

次の図は、ハイブリッドソリューションにおける NetScaler ADC ワークフローを示しています。



前提条件

February 6, 2024

以下の点について確認してください:

- Cisco ACI コンポーネントと NetScaler の概念知識があります。
  - Cisco ACI とそのコンポーネントの詳細については、次の URL にある製品マニュアルを参照してください。http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html
  - NetScaler ADC の詳細については、次の NetScaler ADC 製品ドキュメントを参照してくださいhttp://docs.citrix.com/。
- データセンターの Cisco APIC を含む、Cisco ACI のすべての必須コンポーネントのセットアップと構成が完了している。Cisco ACI とそのコンポーネントの詳細については、次の URL にある製品マニュアルを参照してください。http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html
- Citrix ADC 11.1 以降がインストールされています。
- Cisco ACI で Citrix ADC を設定して、Cisco APIC を使用して管理できるようにしました。
- 環境内に NetScaler Application Delivery Management（ADM）を展開しました。詳しくは、Citrix ADM 12.1を参照してください。
- APIC から NetScaler ADM および ADC への管理接続が確立されます。
- また、次について書き留めておきます。
  - 管理およびデータパス接続に使用される接続インターフェイスと IP アドレス
  - リーフスイッチの詳細：Citrix ADC IP アドレス、ポート、インターフェイスなど。

> 注
>
> このリリースでは、ハイブリッドモードソリューションは単一コンテキストで NetScaler ADC をサポートします。つまり、管理パーティションはサポートされていません。

Cisco APIC および **NetScaler ADM** を使用して **NetScaler ADC** をハイブリッドモードで構成します

February 6, 2024

Cisco APIC と Citrix Application Delivery Management（ADM）を使用してハイブリッドモードで Citrix ADC を設定するには、次のタスクを実行します。

1. ファブリック内の NetScaler ADC インスタンスを NetScaler ADM に追加します。手順については、「NetScaler ADM へのインスタンスの追加」を参照してください。
2. NetScaler ADM を使用して、アプリケーションの StyleBook を作成します。手順については、「NetScaler ADM を使用したアプリケーションの StyleBook の作成」を参照してください。
3. NetScaler ADC ハイブリッドモードデバイスパッケージを Cisco APIC にインポートします。手順については、Citrix ADC ハイブリッドモードデバイスパッケージの Cisco APIC へのインポートを参照してください。
4. Cisco APIC で Device Manager として NetScaler ADM を追加します。手順については、「Cisco APIC で Device Manager として NetScaler ADM を追加する」を参照してください。
5. Cisco APIC を使用して、Cisco ACI に NetScaler ADC デバイスを追加します。手順については、Cisco ACI でデバイスとしての Citrix ADC の追加を参照してください。
6. サービスグラフテンプレートを作成して、展開します。手順については、「サービスグラフの作成とデプロイ」を参照してください。
7. NetScaler ADM で StyleBook を使用して L4-L7 パラメーターを構成します。手順については、「NetScaler ADM の StyleBook を使用した L4-L7 パラメーターの構成」を参照してください。
8. Cisco APIC のエンドポイントイベントが接続または接続解除されます。詳細については、「APIC からのエンドポイントイベントのアタッチまたはデタッチ」を参照してください。

NetScaler ADM を使用したアプリケーションの StyleBook の作成

February 6, 2024

StyleBook は、あらゆるアプリケーションの Citrix ADC 構成を作成および管理するために使用できる構成テンプレートです。StyleBook を作成して、負荷分散、SSL オフロード、コンテンツスイッチなどの特定の Citrix ADC 機能を構成できます。StyleBook を設計することで、Microsoft Exchange や Microsoft Lync などのエンタープライズアプリケーション展開環境を構成できます。詳しくは、「StyleBook」を参照してください。

アプリケーション用に独自の StyleBook を作成することも、NetScaler Application Delivery Management（ADM）に付属の APIC-HTTP-LBStyleBook を変更して使用することもできます。

NetScaler ADM でアプリケーション用に独自の StyleBook を作成するには、「独自の StyleBook を作成する方法」を参照してください。

StyleBook を作成するときには、StyleBook の APIC サービスグラフモデルに従ってください。言い換えると、アプリケーションの APIC サービスグラフは、ADC 機能を介して接続されるコンシューマーモデルとプロバイダーモデルに従います。コンシューマーとプロバイダーは、エンドポイントグループ（EPG）として表され、1 対 1 の関係を

持ちます。StyleBook でも同じモデルに従う必要があります。つまり、プロバイダー EPG はサービスグループとして、各エンドポイントはサービスグループのメンバーとして表す必要があります。ADC 機能ノードは仮想サーバーによって表す必要があり（たとえば、負荷分散仮想サーバー）、仮想サーバーとサービスグループは 1 対 1 の関係である必要があります。

これは基本的にサービスグラフの本質をとらえるもので、これにより APIC に対するイベントの接続または接続解除を処理できます。接続イベントはエンドポイントを対応するサービスグループにバインドし、接続解除イベントはエンドポイントをバインド解除します。ネットワーク L2-L3 から ADC-feature L4-l7 構成へのシームレスな自動化を実現するには、サービスグラフと StyleBook が同等であることを確認する必要があります。

NetScaler ADC ハイブリッドモードデバイスパッケージを **Cisco APIC** にインポート

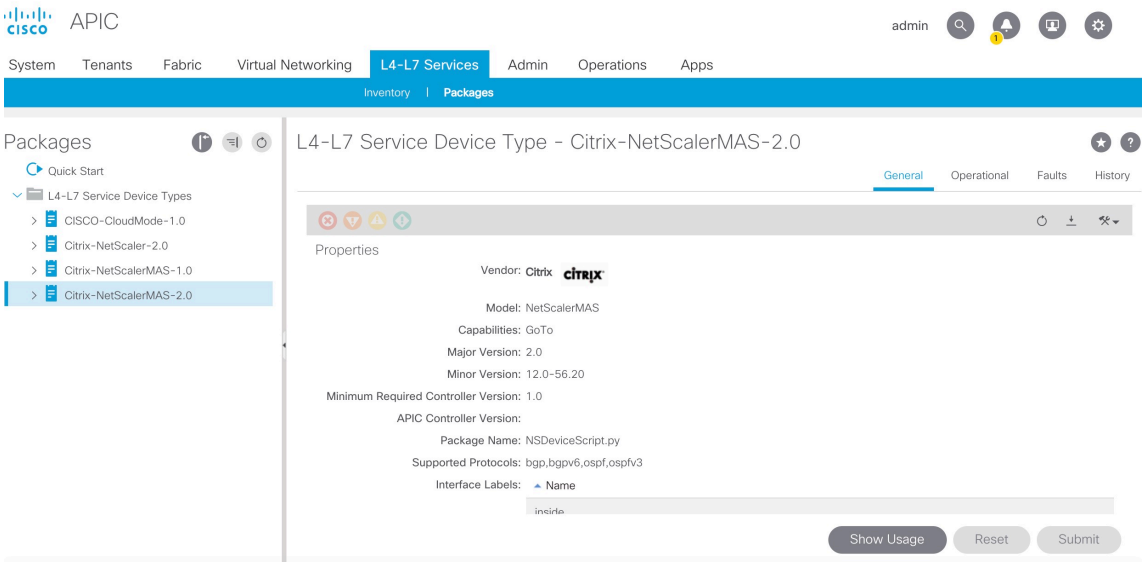
February 6, 2024

ハイブリッドモードのデバイスパッケージは、フルマネージモードと比べると軽量なパッケージです。このデバイスモデルで使用できるのは、L2-L3 ネットワークパラメーターのみです。デバイスモデルには、汎用 ADC 機能が 1 つだけ定義されており、ファブリック内の Citrix ADC の展開に基づく 4 つの機能プロファイル（たとえば、片腕と 2 腕、RHI と同じ）があります。ハイブリッドモードデバイスパッケージ名は、**NetScaler** ハイブリッドモードデバイスパッケージ **12.0** ビルド **56.20** です。Citrix ダウンロードサイトでハイブリッドモードデバイスパッケージを検索してダウンロードし、デバイスパッケージを APIC にインポートします。

> 注
>
> ハイブリッドモードのデバイスパッケージは、フルマネージモードデバイスパッケージと混在させることができます。

APIC GUI を使用してハイブリッドモードのデバイスパッケージを **APIC** にインポートするには**:**

1. メニューバーの L4-L7 サービスタブをクリックし、パッケージパネルを選択します。
2. ナビゲーションペインで、**L4-L7** デバイスタイプを右クリックし、「デバイスパッケージのインポート **」を選択します。
3. ［デバイスパッケージのインポート］ダイアログボックスで、［参照］をクリックして、ダウンロードした Citrix ADC ハイブリッドモードのデバイスパッケージを選択します。
4. ［**Submit**］をクリックします。
   デバイスパッケージが APIC に正常にインポートされたら、ナビゲーションペインでデバイス名をクリックしてデバイスパッケージの詳細を表示できます。



> 重要
>
> デバイスパッケージをインポートしたら、APIC で問題が発生していないことを確認します。障害を表示するには、［Device Types］ウィンドウで［**Faults**］タブをクリックします。

Cisco APIC の **Device Manager** として **NetScaler ADM** を追加します

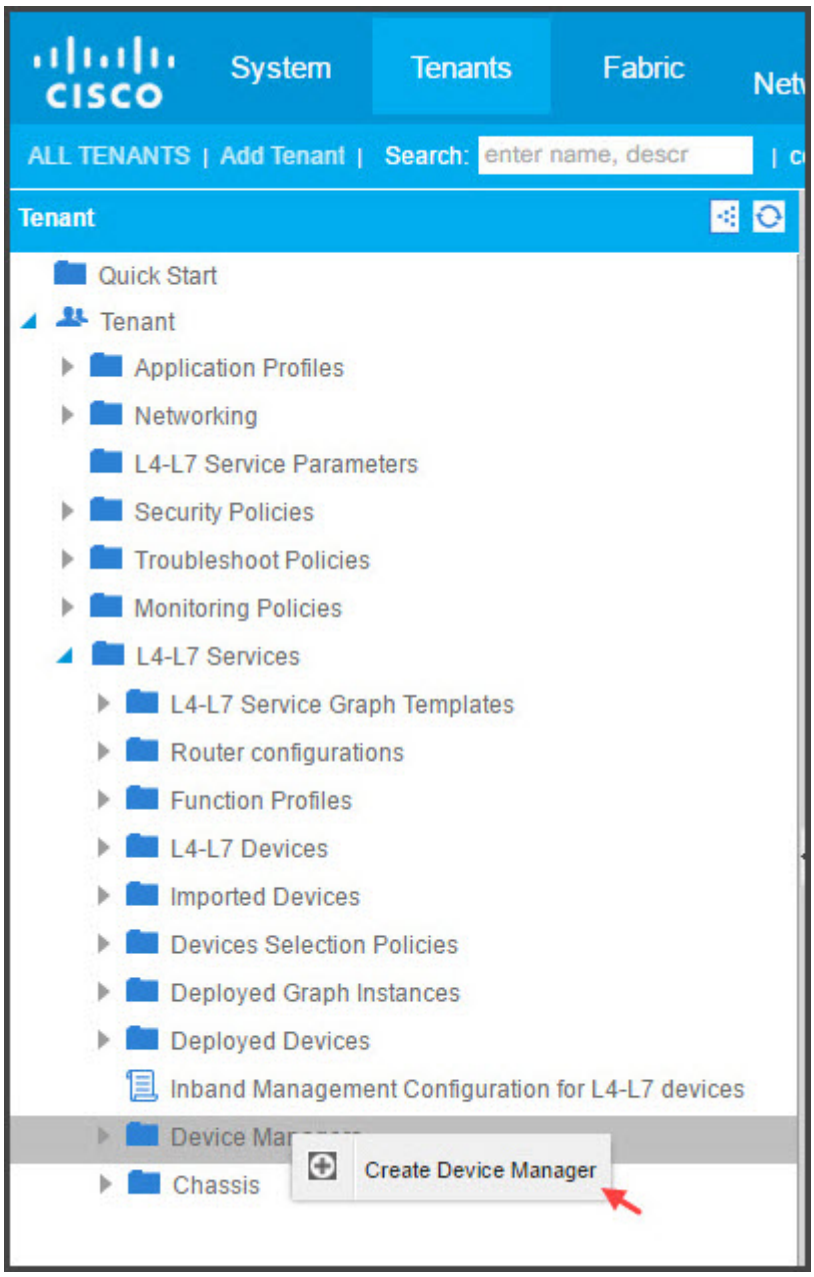
February 6, 2024

2018 年 5 月 24 日

Citrix Application Delivery Management（ADM）は、Cisco ACI に導入された Citrix ADC の一元化されたデバイスマネージャとして機能します。Citrix ADM をデバイスマネージャとして Cisco APIC に追加する必要があります。

APIC GUI を使用して **Citrix ADM** をデバイスマネージャとして **APIC** に追加するには:

1. メニューバーで [テナント] **> [**すべてのテナント] に移動します。
2. 作業ウィンドウで、テナントの名前をダブルクリックします。
3. ナビゲーションペインで、[***** テナント名 ***] > [L4-L7** サービス**]** を選択します。
4. [デバイスマネージャ] を右クリックし、[デバイスマネージャの作成] をクリックします。



5. [デバイスマネージャの作成] ダイアログボックスで、次の操作を行います。

   a)「デバイスマネージャー名」フィールドに、デバイスマネージャーとして登録する Citrix ADM 展開の名前を入力します。

   b)［**Management EPG**］ボックスの一覧で、管理 EPG を選択します。

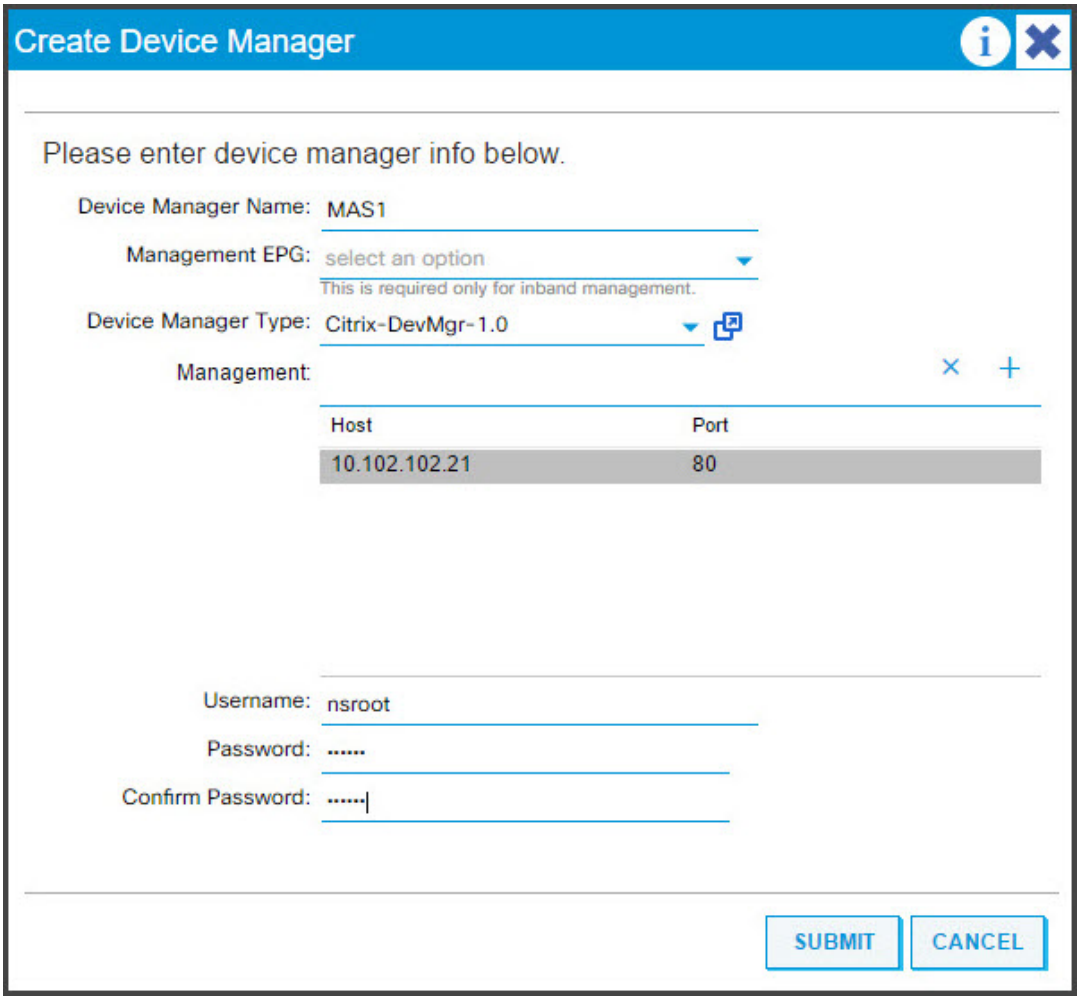
   c)［**Device Manager Type**］ボックスの一覧で、［**Citrix-DevMgr-1.0**］を選択します。

   d)［管理］フィールドで［**+**］をクリックし、Citrix ADM 展開の IP アドレスとポートの詳細を追加します。

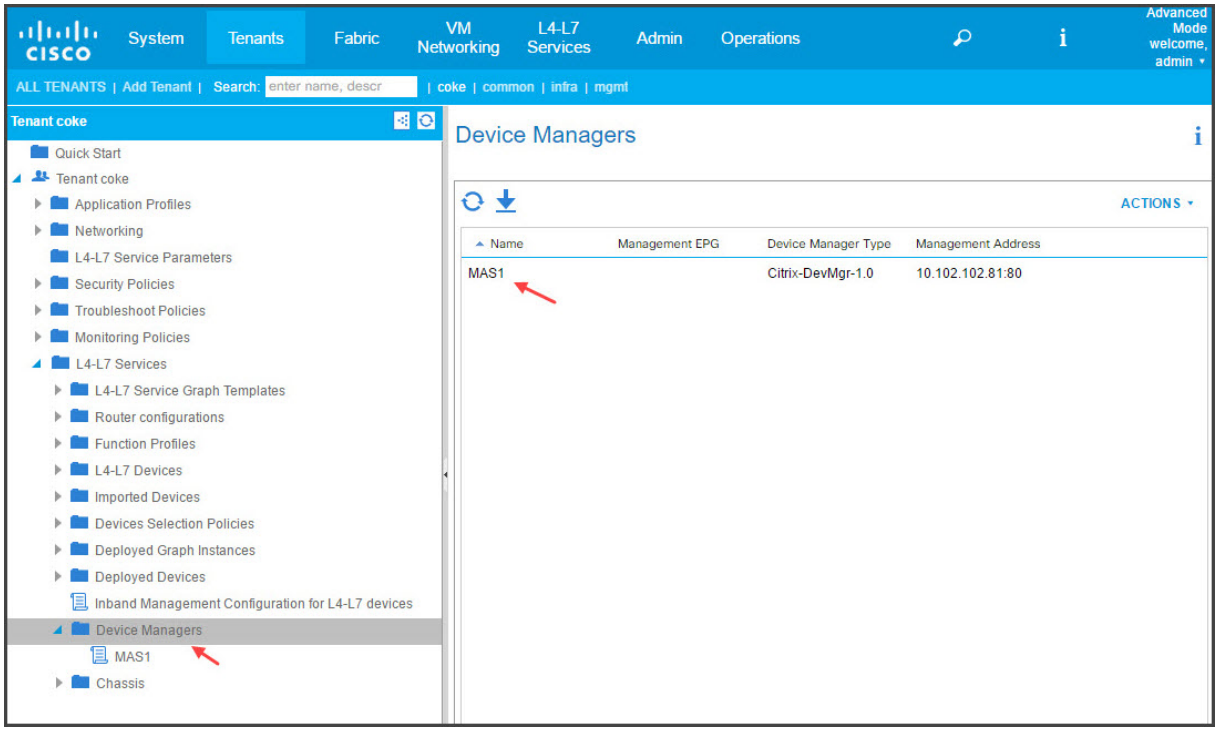
   e)「ユーザー名」フィールドに、Citrix ADM にアクセスするためのユーザー名を入力します。

f) ［パスワード］フィールドと［パスワードの確認］フィールドに、Citrix ADM にアクセスするためのパスワードを入力します。

g) ［**SUBMIT**］をクリックします。



Citrix ADM がデバイスマネージャとして APIC に正常に登録されると、デバイスマネージャが追加され、ナビゲーションペインに表示されます。登録済みのデバイスマネージャを表示するには、ナビゲーションペインで [***tenant_name*] > [L4-L7** サービス] **>** [デバイスマネージャー] に移動します。



> 注
>
> Cisco APIC と Citrix ADM の間に接続上の問題がないことと、Citrix ADM へのアクセスに使用するのと同じ認証情報を入力していることを確認してください。また、アカウントに管理者権限があることも確認します。
>
> 重要
>
> デバイスパッケージをインポートしたら、APIC で問題が発生していないことを確認します。障害を表示するには、[Device Types] ウィンドウで [**Faults**] タブをクリックします。

API を使用して Citrix ADM をデバイスマネージャーとして登録することもできます。次に、API を使用して NetScaler ADM をデバイスマネージャーとして追加する方法を示す XML ペイロードのサンプルを示します。

```
<polUni>
    <fvTenant name="coke">
        <vnsDevMgr name="MAS1">
            <vnsRsDevMgrToMDevMgr tDn="uni/infra/mDevMgr-Citrix-DevMgr-1.0" />
            <vnsCMgmts name="devMgmt" host="10.102.102.81" port="80"/>
            <vnsCCred name="username" value="nsroot"/>
            <vnsCCredSecret name="password" value="*****("/>
        </vnsDevMgr>
    </fvTenant>
</polUni>
```


APIC を使用して Cisco ACI にデバイスとして NetScaler ADC を追加します

February 6, 2024

ネットワークを自動化するには、Citrix ADC を L4-L7 デバイスとして APIC に追加する必要があります。APIC は、デプロイされたサービスグラフに基づいて、リーフと Citrix ADC デバイス間のネットワークステッチを実行します。更新管理 IP アドレス、デバイスマネージャー、資格情報など、デバイス構成の基本設定を行う必要があります。

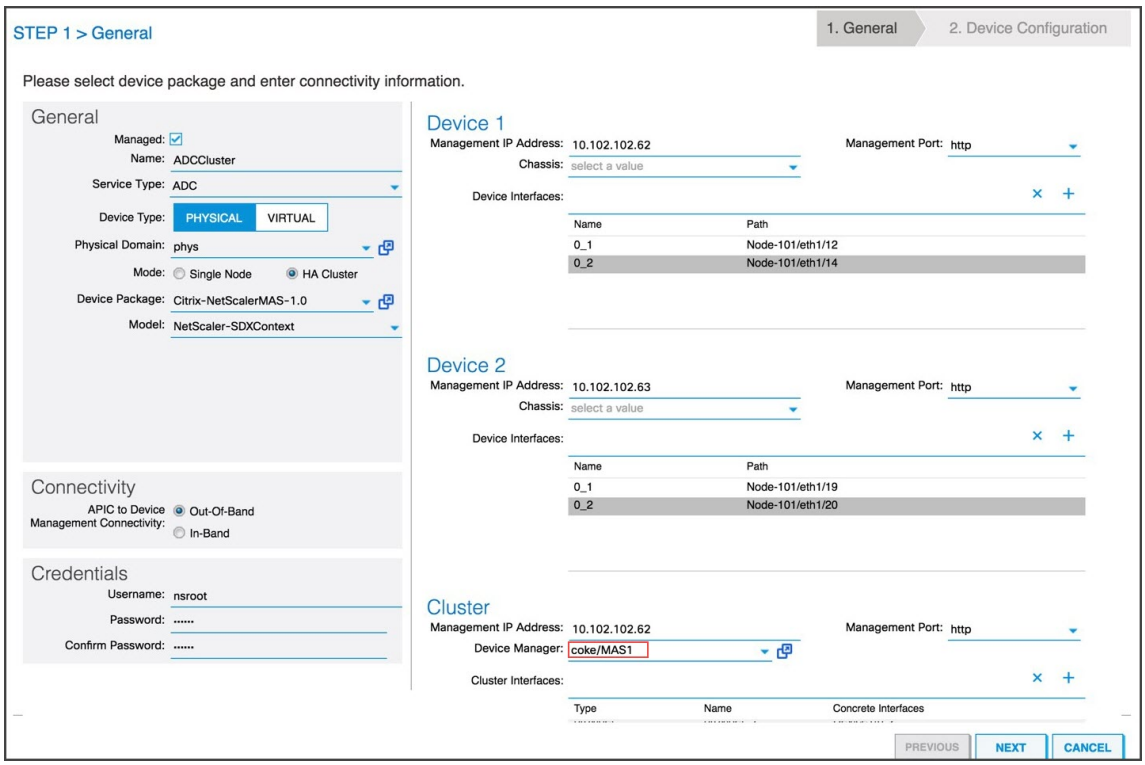
APIC GUI を使用して **Citrix ADC** を **APIC** のデバイスとして登録するには:

1. メニューバーで [テナント] **> [**すべてのテナント] に移動します。
2. 作業ウィンドウで、テナントの名前をダブルクリックします。
3. ナビゲーションペインで、***** テナント名 *** > L4-L7** サービス **> L4-L7** デバイスを選択します。
4. 作業ペインで、［アクション］**>** ［**L4-L7** デバイスの作成］を選択します。
5. **L4-L7** デバイスの作成ダイアログボックスの「一般」セクションで、次の操作を行います。
   a)「管理対象」チェックボックスを選択します。
   b)「名前」フィールドに、デバイスの名前を入力します。
   c)［**Service Type**］ボックスの一覧で、［**ADC**］を選択します。
   d)［**Device Type**］フィールドで、［**Physical**］を選択します。

   > 注**:**
   >
   > VMware ESX の場合は、必ず [仮想] を選択し、それぞれの仮想マシンマネージャ (VMM) ドメインを関連付けてください。

   e)［**Physical Domain**］ボックスの一覧で、物理ドメインを選択します。
   f) [モード] フィールドで、要件に応じて [シングルノード] または [**HA** クラスタ] を選択します。
   g) デバイスパッケージドロップダウンリストで、**Citrix-NetScalerMAS-1.0** を選択します。
   h)「モデル」ドロップダウンリストで、デバイスモデルを選択します。たとえば、Citrix ADC-MPX、または Citrix ADC-VPX。
6. ［接続］セクションの［**APIC** からデバイス管理への接続］フィールドで、Citrix **ADC** がファブリック内でどのように設定されているかに応じて、［アウトオブバンド］または［インバンド］を選択します。
7. 認証情報セクションで、デバイスにアクセスするためのユーザー名とパスワードを指定します。
8.「デバイス **1** 」セクションと「デバイス **2** 」セクションで、それぞれ管理関連の設定を完了します。

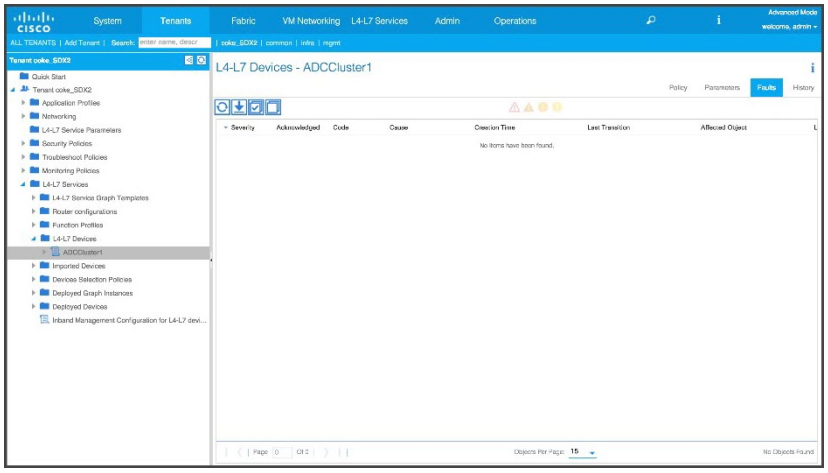
9. [**Cluster**] セクションで、クラスタの管理関連の設定を完了します。[**Device Manager**] ドロップダウンリストで、「Cisco APIC での Device Manager としての NetScaler ADM の追加」で作成したデバイスマネージャを選択していることを確認します。



10. [次へ] をクリックします。[Device Configuration] ページが開きます。ハイブリッドモードデバイスのパッケージには、高可用性、機能とモードの有効化/無効化、NTP、SNMP、SNMP アラームなど、デバイスおよびクラスター固有の詳細な構成は用意されていません。これらの構成は、Citrix ADM を使用して行う必要があります。

11. 「完了」をクリックします。APIC へのデバイスの登録に成功すると、そのデバイスが追加され、ナビゲーションペインに表示されます。登録されたデバイスを表示するには、ナビゲーションペインで [***tenant_name*] > [L4-L7** サービス] **> [L4-L7** デバイス] **> [device_name]** に移動します。

> 重要
>
> デバイスを登録したら、APIC で問題が発生していないことを確認します。障害を確認するには、作業ペインの［障害］タブをクリックします。



API を使用して Citrix ADC デバイスを登録することもできます。以下に、L4-L7 デバイスを追加するための XML ペイロードの例を示します。

```
<polUni>

    <fvTenant name="coke">

    <vnsLDevVipname="ADCCluster1"funcType="GoTo" svcType="ADC">

     <vnsRsMDevAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0" />

     <vnsRsALDevToPhysDomP tDn="uni/phys-phys"/>

     <vnsCMgmt name="devMgmt"host="10.102.102.67"port="80"/>

     <vnsCCred name="username" value="nsroot"/>

     <vnsCCredSecret name="password" value="****"/>

     <vnsRsALDevToDevMgr tnVnsDevMgrName="MAS1"/>

     <vnsCDev name="ADC1" devCtxLbl="C1">

     <vnsCIf name="1_1">

     <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
        /33]"/>

     </vnsCIf>

     <vnsCIf name="1_2">

     <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
        /35]"/>

     </vnsCIf>

     <vnsCMgmt name="devMgmt" host="10.102.102.65" port="80"/>
```



```
34
35        <vnsCCred name="username" value="nsroot"/>
36
37        <vnsCCredSecret name="password" value="****"/>
38
39        </vnsCDev>
40
41        <vnsCDev name="ADC2" devCtxLbl="C1">
42
43        <vnsCIf name="1_1">
44
45        <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
             /34]"/>
46
47        </vnsCIf>
48
49        <vnsCIf name="1_2">
50
51        <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
             /36]"/>
52
53        </vnsCIf>
54
55        <vnsCMgmt name="devMgmt" host="10.102.102.66" port="80"/>
56
57        <vnsCCred name="username" value="nsroot"/>
58
59        <vnsCCredSecret name="password" value="****"/>
60
61        </vnsCDev>
62
63        <vnsLIf name="outside">
64
65        <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
             mIfLbl-outside"/>
66
67        <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
             cIf-1_1"/>
68
69        <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
             cIf-1_1"/>
70
71        </vnsLIf>
72
73        <vnsLIf name="inside">
74
75        <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
             mIfLbl-inside"/>
76
77        <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
             cIf-1_2"/>
78
79        <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
```



```
            cIf-1_2"/>
80
81          </vnsLIf>
82
83          </vnsLDevV
84
85          </fvTenant>
86
87          </polUni>
```

サービスグラフの作成とデプロイ

February 6, 2024

Citrix ADC を作成してデプロイするには、APIC の Cisco APIC サービスグラフテンプレートを使用する必要があります。サービスグラフを作成および展開する場合、必ず ADC 機能プロファイルを使用してください。

APIC でグラフを構成すると、機能定義、デバイスのファブリックへの接続、グラフ展開環境の一部として設定されたエンティティに基づき、APIC により自動的にデバイスが構成されます。VLAN の割り当てとバインドなどのネットワーク構成も、サービスグラフの作成処理の一部として APIC により自動的に行われます。また、APIC からグラフを削除すると、構成も削除されます。

サービスグラフは、間に適切なサービス機能が挿入された 2 つ以上のアプリケーション階層によって表されます。サービスグラフは、契約により、送信元 EPG と送信先 EPG の間に挿入されます。

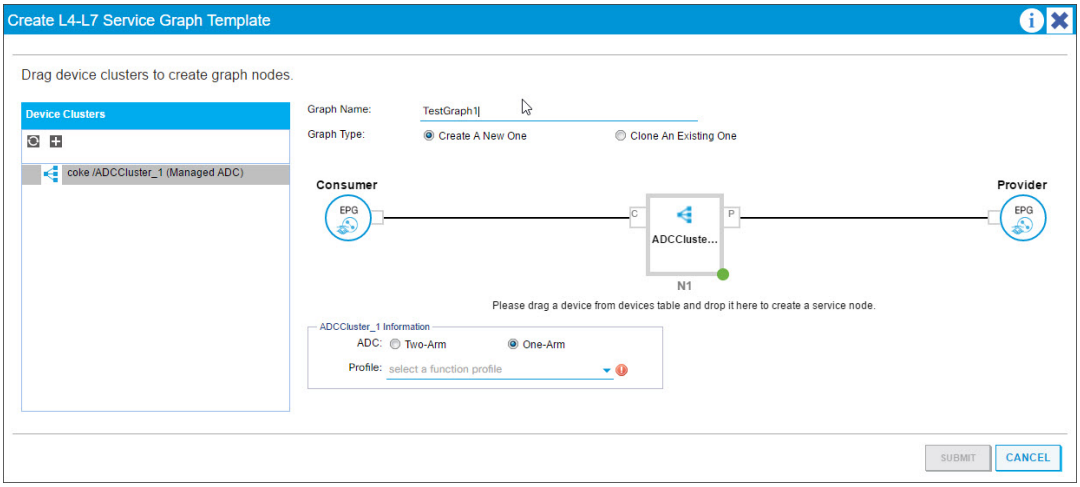
APIC GUI を使用してサービスグラフを作成するには**:**

1. メニューバーで [テナント] **> [**すべてのテナント] に移動します。
2. 作業ウィンドウで、テナントの名前をダブルクリックします。
3. ナビゲーションペインで、***tenant_name* > L4-L7** サービス **> L4-L7** サービスグラフテンプレートを選択します。
4. 作業ペインで、[アクション**] > [L4-L7** サービスグラフテンプレートの作成] を選択します。
5. [**L4-L7** サービスグラフテンプレートの作成] ダイアログボックスの [デバイスクラスタ] セクションで、デバイスクラスタを選択し、次の操作を行います。

   a) [**Graph Name**] ボックスに、サービスグラフテンプレートの名前を入力します。

   b) [**Graph Type**] フィールドで、[**Create A New One**] を選択します。

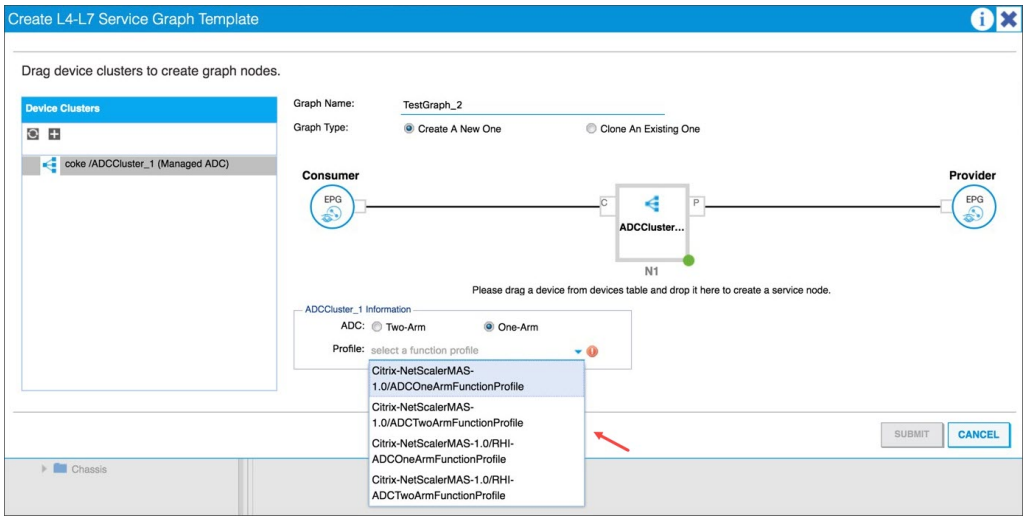
   c) [**Device Cluster**] セクションからデバイスをドラッグし、コンシューマーエンドポイントグループとプロバイダーエンドポイントグループの間にドロップしてサービスノードを作成します。



d) <***L4-L7device_name information***> セクションで、次の手順を実行します。

i. 「**ADC** 」フィールドで、Citrix ADC がファブリックにどのように展開されているかに応じて、「ワンアーム」または「ツーアーム」を選択します。

ii. 「プロファイル」ドロップダウンリストで、デバイスパッケージで提供されている機能プロファイルを選択します。

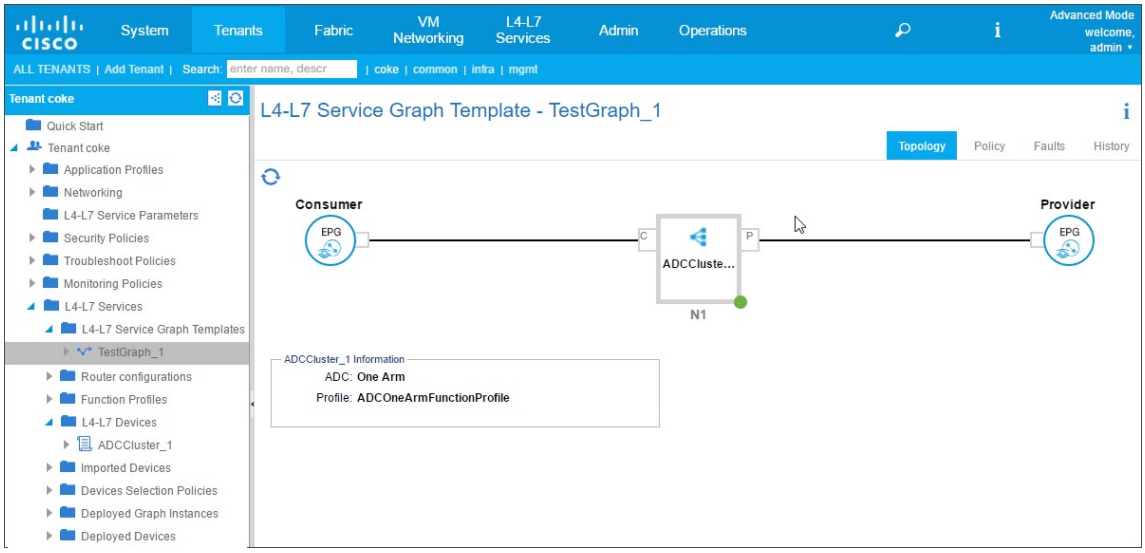


iii. [**SUBMIT**] をクリックします。

6. ナビゲーションペインで、サービスグラフテンプレートをクリックします。画面に、サービスグラフテンプレートのグラフィックトポロジが表示されます。

> 注
>
> Cisco APIC では、コネクタという概念をサポートしており、これらのコネクタは ADC クラスタノードで確認できます。コネクタでネットワークトラフィックの方向とデバイススクリプトを定義します。デバイススクリプトでは、割り当てられた VLAN を、外部接続または内部接続のどちらであるかに応じて、仮想 IP（VIP）アドレスまたはサブネット IP（SNIP）アドレスに動的にバインドします。VLAN は、イ

> ンバウンドトラフィックおよびアウトバウンドトラフィックに使用される個別のインターフェイスにバインドされます。

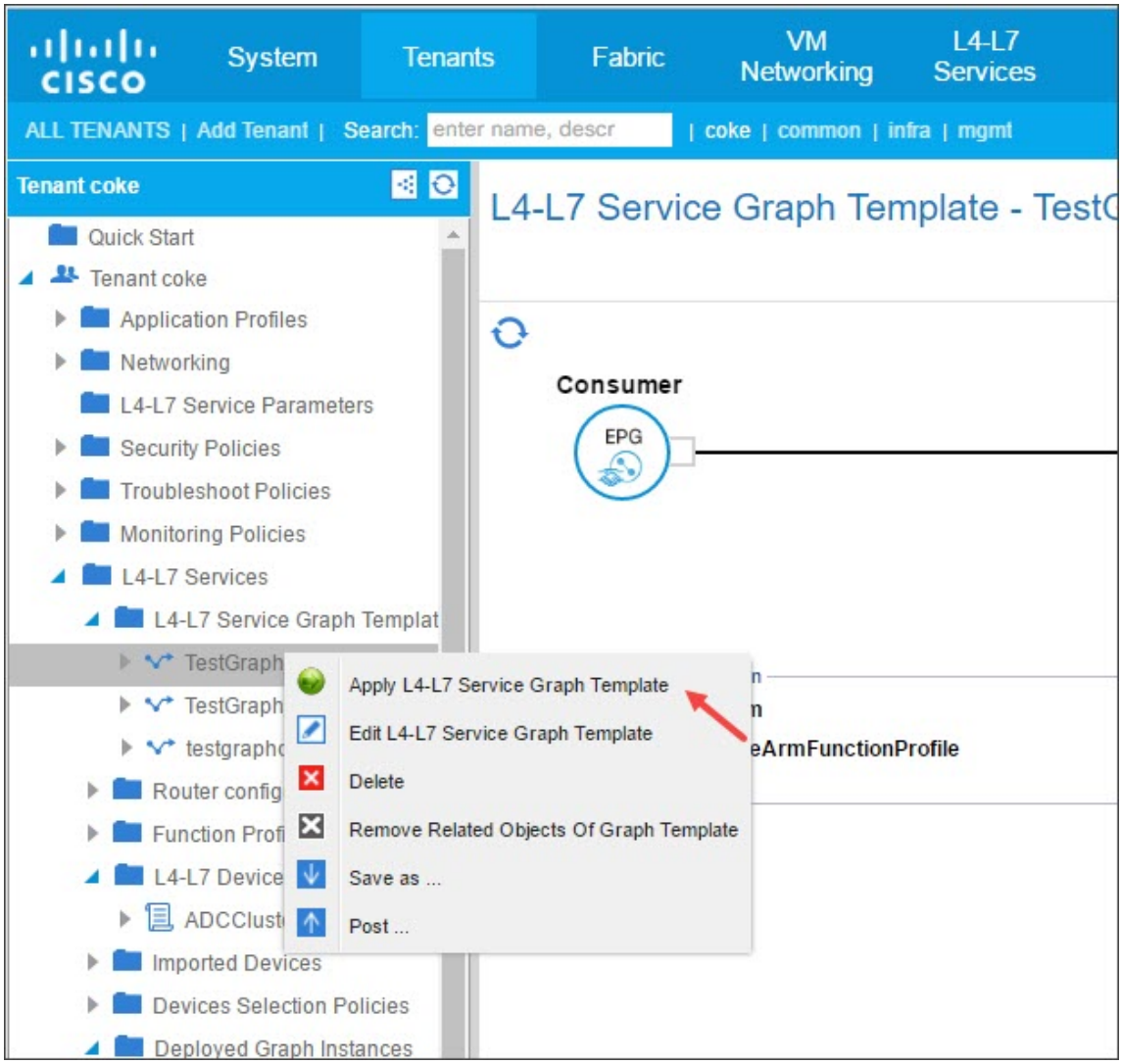


サービスグラフテンプレートのエンドポイントグループへの適用

作成したサービスグラフテンプレートは、APIC GUI を使用して適用する必要があります。

サービスグラフテンプレートを適用するには**:**

1. メニューバーで [テナント] **> [**すべてのテナント] に移動します。
2. 作業ウィンドウで、テナントの名前をダブルクリックします。
3. ナビゲーションペインで、***tenant_name* > L4-L7** サービス **> L4-L7** サービスグラフテンプレートを選択します。
4. ***template_name*** を右クリックして、「**L4-L7** サービスグラフテンプレートを適用」をクリックします。

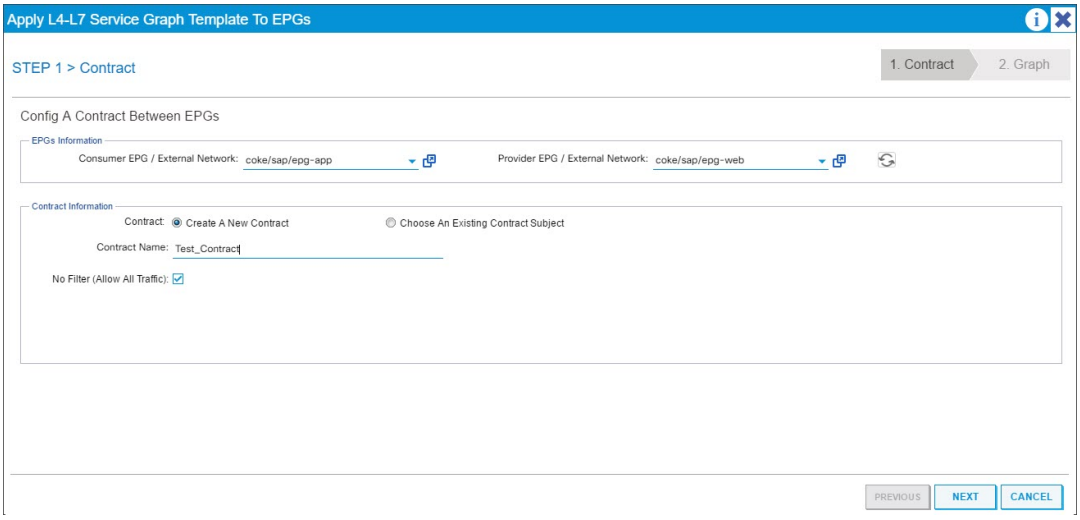


5. 「**L4-L7** サービスグラフテンプレートを **EPG** に適用」ダイアログボックスの「**EPG** 情報」セクションで、次のフィールドに値を入力します。

   a) [**Consumer EPG/External Network**] ボックスの一覧で、コンシューマーエンドポイントグループを選択します。

   b) [**Provider EPG/External Network**] ボックスの一覧で、提供されているエンドポイントグループを選択します。

   c) [**Contract Information**] セクションで、適切なボックスに入力します。契約情報は、Cisco APIC に固有の情報であり、EPG に関連付けられたセキュリティポリシーの一部として構成されます。



d) ［次へ］をクリックします。

e)「グラフテンプレート」ドロップダウンリストで、作成したサービスグラフテンプレートを選択します。

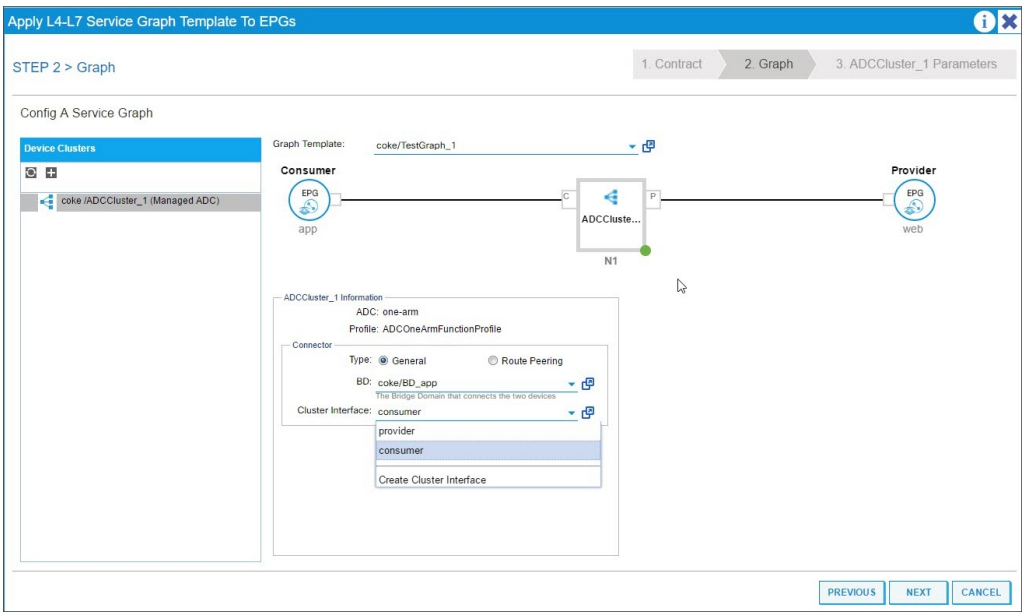
f) コネクタセクションで、次の操作を行います。

i.「タイプ」フィールドで「一般」を選択します。

ii. **BD** ドロップダウンリストで、ブリッジドメインを選択します。コネクタの詳細はブリッジドメインの一部であり、ブリッジドメインは Cisco APIC インフラストラクチャモデルの一部です。

iii. ［**Cluster Interface**］ボックスの一覧で、選択したブリッジドメインの適切なクラスターインターフェイスを選択します。

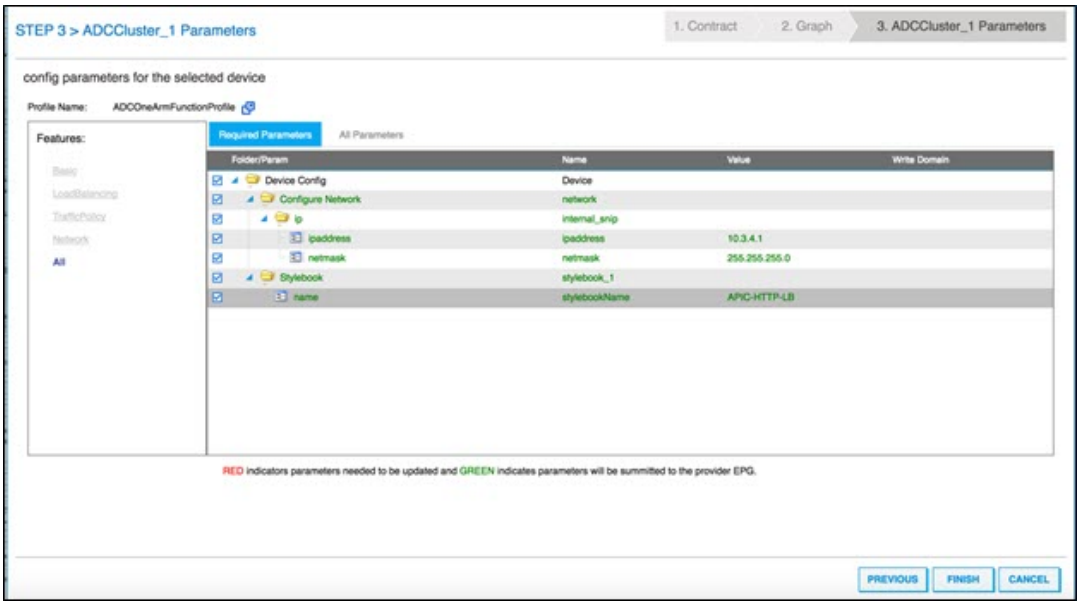
Cisco APIC は、選択したサービスグラフテンプレートの要件に応じて、Citrix ADC デバイスとファブリック間のデータパストラフィックに選択したブリッジドメインを使用します。



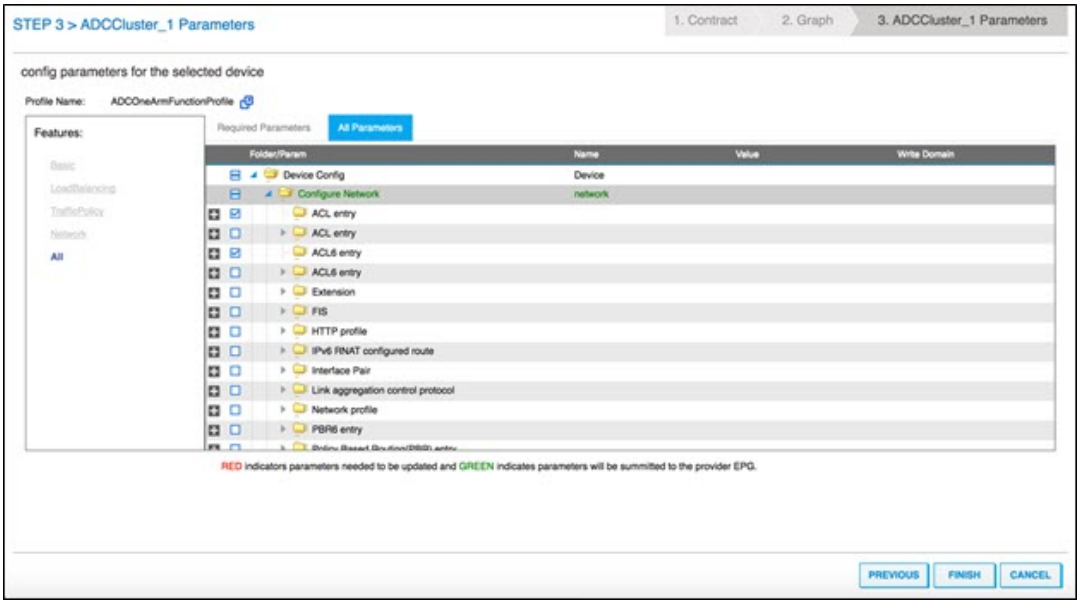
iv. ［次へ］をクリックします。

[パラメータ] 画面の [必須パラメータ] タブに、プロファイルで指定されている IP アドレスなど、L2-L3 固有の詳細を入力します。その他の主要パラメーターとして StyleBook 名があります。NetScaler Application Delivery Management（ADM）で提供される組み込みの StyleBook **APIC-HTTP-LB** 、または NetScaler ADM を使用したアプリケーションの StyleBook の作成で作成した StyleBook の名前を指定できます。

> 注
>
> StyleBook の名前は、サービスグラフの詳細を、特定のアプリケーション用に Citrix ADM で作成された L4-L7 構成にリンクします。



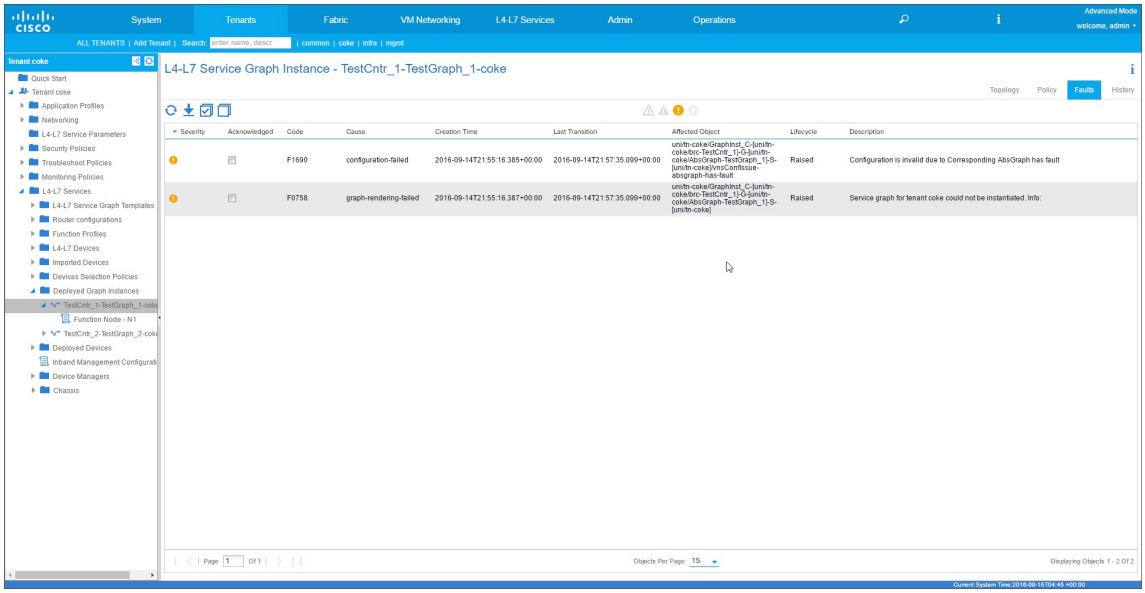
Cisco APIC GUI を使用すると、機能（たとえば、負荷分散）に基づいてパラメーターを絞り込むことができます。すべての必須パラメーターを確認および設定するには［**Required Parameters**］タブを、特定の機能に関連する、その他のすべてのパラメーターを確認および設定するには［**All Parameters**］タブを使用します。



> 注
>
> デフォルトでは、組み込みのワンアームプロファイルで SNIP の詳細（IP アドレスやネットマスクなど）を指定する必要があります。その他のネットワークパラメーターを確認するには、［**All Parameters**］をクリックして、Cisco APIC GUI で［**Configure Network**］ツリーを展開します。これには、Citrix ADC でサポートされているすべてのネットワークパラメーターが一覧表示されます。Cisco APIC GUI から任意のエンティティをインスタンス化して、リスト表示された各属性の値を指定できます。

6. ［完了］をクリックします。

> 重要
>
> サービスグラフテンプレートを適用したら、展開したグラフに問題がないことを確認してください。障害を確認するには、作業ペインの［障害］タブをクリックします。



サービスグラフの導入の一環として、ハイブリッドモードデバイスパッケージは構成の詳細を Cisco APIC から Citrix ADM にプッシュします。Citrix ADM はこれらの構成をそれぞれの Citrix ADC に内部的に処理し、応答を APIC に返します。グラフの展開が成功しても障害は発生せず、Citrix ADC は対応するグラフのファブリックと正常にネットワーク化されます。

APIC では、API を使用してグラフを構成および展開するためのさまざまな方法を用意しています。グラフの展開には、一部の APIC 固有の構造体（テナント、契約、VLAN、名前空間など）に対するさまざまな依存関係が含まれています。

次のアプローチ例は、APIC の API を使用して L4-L7 グラフを作成および展開する方法の 1 つを示しています。この例では、APIC 固有のアーティファクトが APIC 内に既に設定されているものとします。

> 重要
>
> ここに示した XML ペイロードは参考用です。本番環境でこれらのペイロードを使用する場合は、事前に XML を適宜変更するようにしてください。

以下に、API を使用して、サービスグラフを作成および展開する例を示します。

a) AppProfile の作成

b) サービスグラフの詳細部分の作成

c) 契約へのサービスグラフの接続

以下に、AppProfile を作成するための XML ペイロードの例を示します。AppProfile には EPG が含まれ、プロバイダー EPG には Citrix ADC 固有のエンティティ、属性、およびそれらの値が含まれます。次のサンプル XML ペイロードでは、NSIP などの Citrix ADC 固有のネットワークエンティティが、一連の属性と StyleBook 名を使用して作成されます。

```
1  <polUni>
```



```
2       <fvTenant name="coke">
3           <!-- Application Profile -->
4           <fvAp dn="uni/tn-coke/ap-sap" name="sap">
5               <!-- EPG 1  -->
6               <fvAEPg dn="uni/tn-coke/ap-sap/epg-web" name="web">
7                   <fvRsBd tnFvBDName="BD_web" />
8                   <!-- --------- CONFIG PAYLOAD ---------------- -->
9                   <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Network" name=
    "Network">
10                      <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="
    snip1">
11                          <vnsParamInst key="ipaddress" name="ip1"
    value="110.110.110.2"/>
12                          <vnsParamInst key="netmask" name="netmask1
    " value="255.255.255.0"/>
13                          <vnsParamInst key="type" name="tye" value=
    "SNIP"/>
14                          <vnsParamInst key="dynamicrouting" name="
    dynamicrouting" value="DISABLED"/>
15                          <vnsParamInst key="hostroute" name="
    hostroute" value="DISABLED"/>
16                      </vnsFolderInst>
17                      <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="
    snip2">
18                          <vnsParamInst key="ipaddress" name="ip2"
    value="220.220.220.2"/>
19                          <vnsParamInst key="netmask" name="netmask2
    " value="255.255.255.0"/>
20                          <vnsParamInst key="type" name="tye" value=
    "SNIP"/>
21                          <vnsParamInst key="dynamicrouting" name="
    dynamicrouting" value="DISABLED"/>
22                          <vnsParamInst key="hostroute" name="
    hostroute" value="DISABLED"/>
23                      </vnsFolderInst>
24                  </vnsFolderInst>
25                  <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Stylebook"
    name="stylebook_1">
26                      <vnsParamInst name="stylebookName" key="name"
    value="APIC-HTTP-LB"/>
27                  </vnsFolderInst>
28                  <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="
    internal_network" name="internal_network">
29                      <vnsCfgRelInst name="internal_network_key" key
    ="internal_network_key" targetName="Network/snip1"/>
30                  </vnsFolderInst>
31                  <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="
```



```
      external_network" name="external_network">
32                    <vnsCfgRelInst name="external_network_key" key
      ="external_network_key" targetName="Network/snip2"/>
33                </vnsFolderInst>
34                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
      graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="mFCngStylebook
      " name="mFCngStylebook_1">
35                    <vnsCfgRelInst name="Stylebook_key" key="
      Stylebook_key" targetName="stylebook_1"/>
36                </vnsFolderInst>
37                <!-- ------- END CONFIG PAYLOAD -------------- -->
38                <fvSubnet ip="110.110.110.110/24" scope="shared"/>
39                <fvRsProv tnVzBrCPName="Ctrct1"></fvRsProv>
40                <fvRsDomAtt tDn="uni/phys-sepg" />
41                <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
      -[eth1/38]" encap="vlan-3703" instrImedcy="immediate"/>
42            </fvAEPg>
43            <!-- EPG 2 -->
44            <fvAEPg dn="uni/tn-coke/ap-sap/epg-app"  name="app">
45                <fvRsCons tnVzBrCPName="Ctrct1"/>
46                <fvRsBd tnFvBDName="BD_app" />
47                <fvSubnet ip="220.220.220.220/24" scope="shared"/>
48                <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
      -[eth1/37]" encap="vlan-3704" instrImedcy="immediate"/>
49                <fvRsDomAtt tDn="uni/phys-sepg" />
50            </fvAEPg>
51        </fvAp>
52    </fvTenant>
53 </polUni>
54 <!--NeedCopy-->
```

以下に、サービスグラフの詳細を作成するための XML ペイロードの例を示します。

```
1  <polUni>
2      <fvTenant name="coke">
3          <vnsAbsGraph name = "Graph1">
4              <vnsAbsTermNodeProv name = "Input1">
5                  <vnsAbsTermConn name = "C1"></vnsAbsTermConn>
6              </vnsAbsTermNodeProv>
7              <vnsAbsNode name="ADC" funcType="GoTo">
8                  <vnsAbsFuncConn name = "outside" attNotify="true">
9                      <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-
       NetScalerMAS-1.0/mFunc-ADCFunction/mConn-external" />
10                 </vnsAbsFuncConn>
11                 <vnsAbsFuncConn name = "inside" attNotify="true">
12                     <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-
       NetScalerMAS-1.0/mFunc-ADCFunction/mConn-internal" />
13                 </vnsAbsFuncConn>
14                 <vnsRsNodeToMFunc tDn="uni/infra/mDev-Citrix-
       NetScalerMAS-1.0/mFunc-ADCFunction"/>
15                 <vnsRsDefaultScopeToTerm tDn="uni/tn-coke/AbsGraph
       -Graph1/AbsTermNodeProv-Input1/outtmnl"/>
16                 <vnsRsNodeToAbsFuncProf tDn="uni/infra/mDev-Citrix
```



```
    -NetScalerMAS-1.0/absFuncProfContr/absFuncProfGrp-
    ADCOneArmServiceProfileGroup/absFuncProf-A
DCOneArmFunctionProfile"/>
                <vnsRsNodeToLDev tDn="uni/tn-coke/lDevVip-
    ADCCluster1"/>
            </vnsAbsNode>
            <vnsAbsTermNodeCon name = "Output1">
                <vnsAbsTermConn name = "C6"></vnsAbsTermConn>
            </vnsAbsTermNodeCon>
            <vnsAbsConnection name = "CON1">
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsTermNodeCon-Output1/AbsTConn" />
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsNode-ADC/AbsFConn-outside" />
            </vnsAbsConnection>
            <vnsAbsConnection name = "CON2">
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsNode-ADC/AbsFConn-inside" />
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsTermNodeProv-Input1/AbsTConn" />
            </vnsAbsConnection>
        </vnsAbsGraph>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```

以下に、サービスグラフを契約に接続するための XML ペイロードの例を示します。

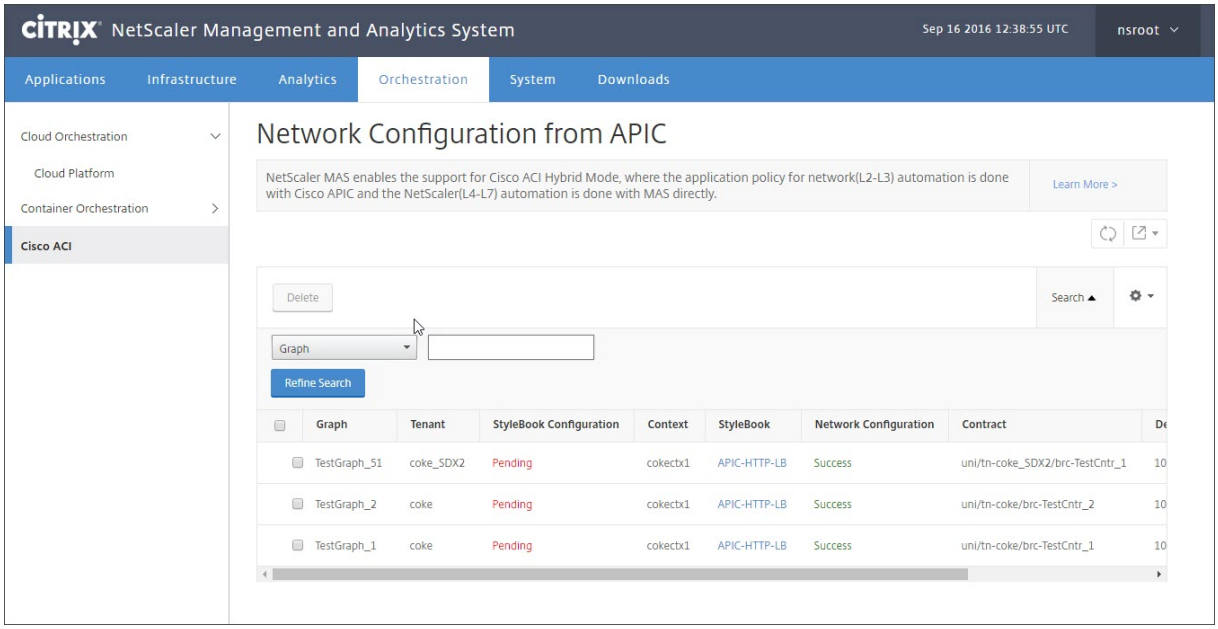
```
<polUni>
    <fvTenant name="coke">
        <vzBrCP name="Ctrct1">
            <vzSubj name="http">
                <vzRsSubjGraphAtt tnVnsAbsGraphName="Graph1"/>
            </vzSubj>
        </vzBrCP>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```

StyleBook を使用して NetScaler ADM から L4-L7 パラメータを構成する

February 6, 2024

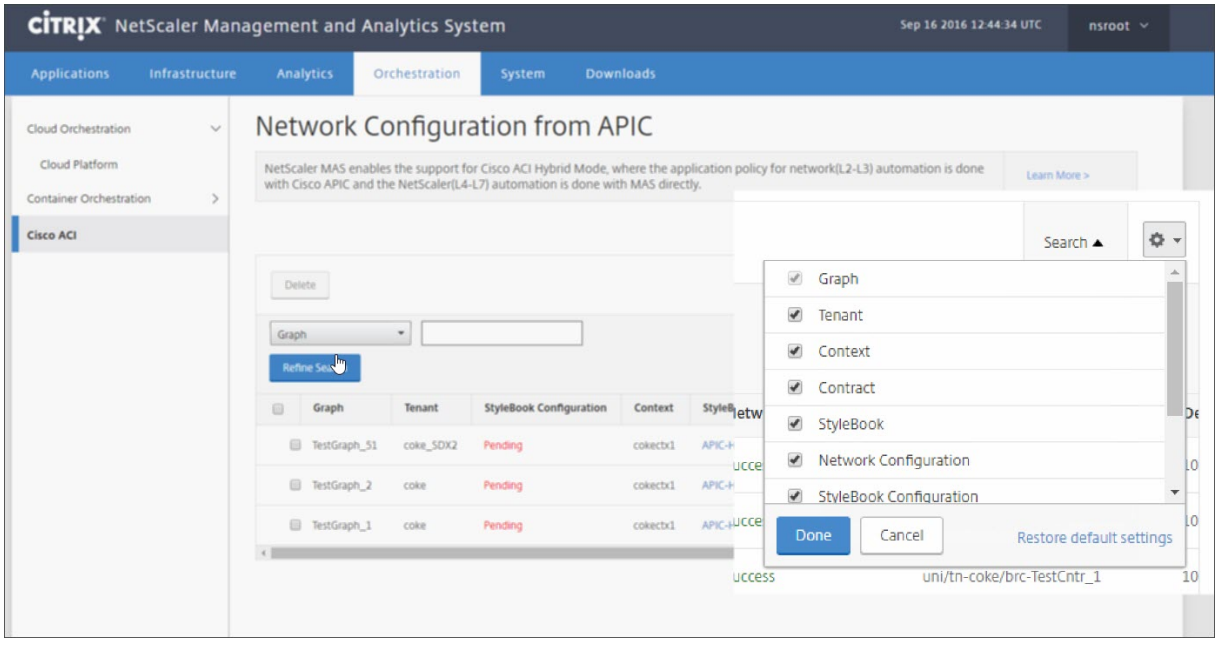
2018 年 5 月 24 日

Citrix Application Delivery Management（ADM）では、展開されたサービスグラフの詳細を **Cisco ACI** の［オーケストレーション］タブで確認できます。表形式ビューに、グラフ名、テナント名、コンテキスト、StyleBook 名、ネットワーク構成の状態などのサービスグラフの詳細が表示されます。



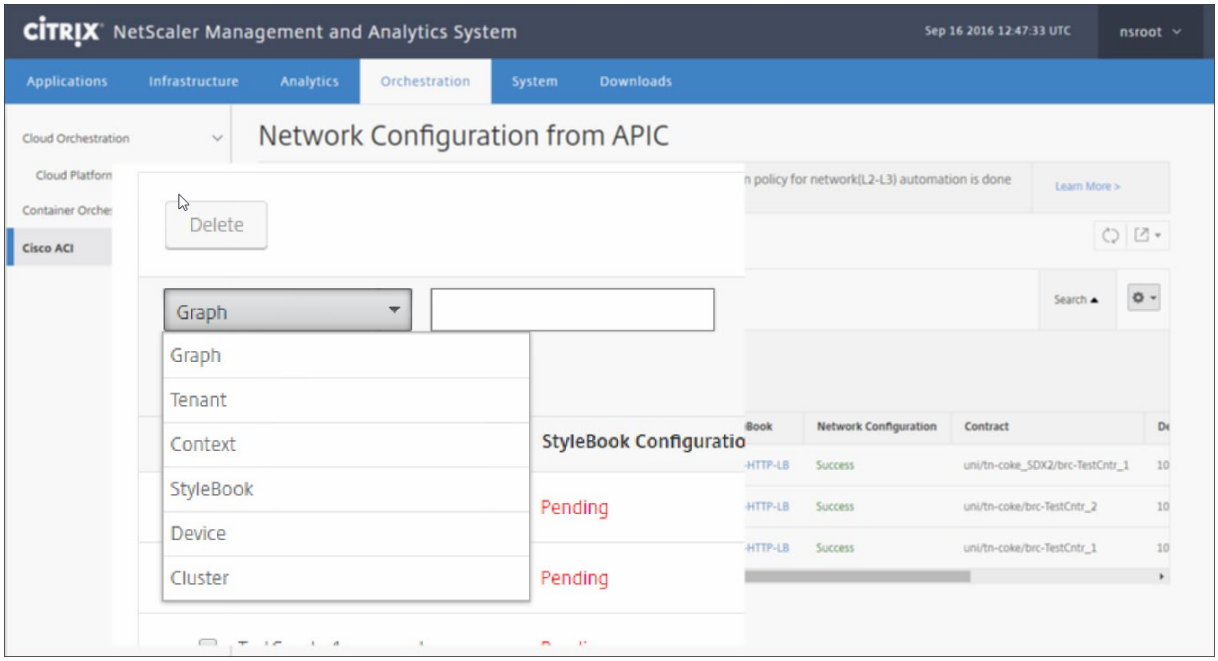
> 注
>
> Cisco APIC からグラフが削除された場合、L4-L7 構成を含む対応する構成が、デバイスから削除されます。

さらに、表形式ビューでは、表の列に合わせて並べ替えを行ったり、[Search] を使用してデータにフィルターを適用したりできます。また、次のように、ボックスで列名のチェックボックスをオンまたはオフにして、列の詳細をカスタマイズできます。



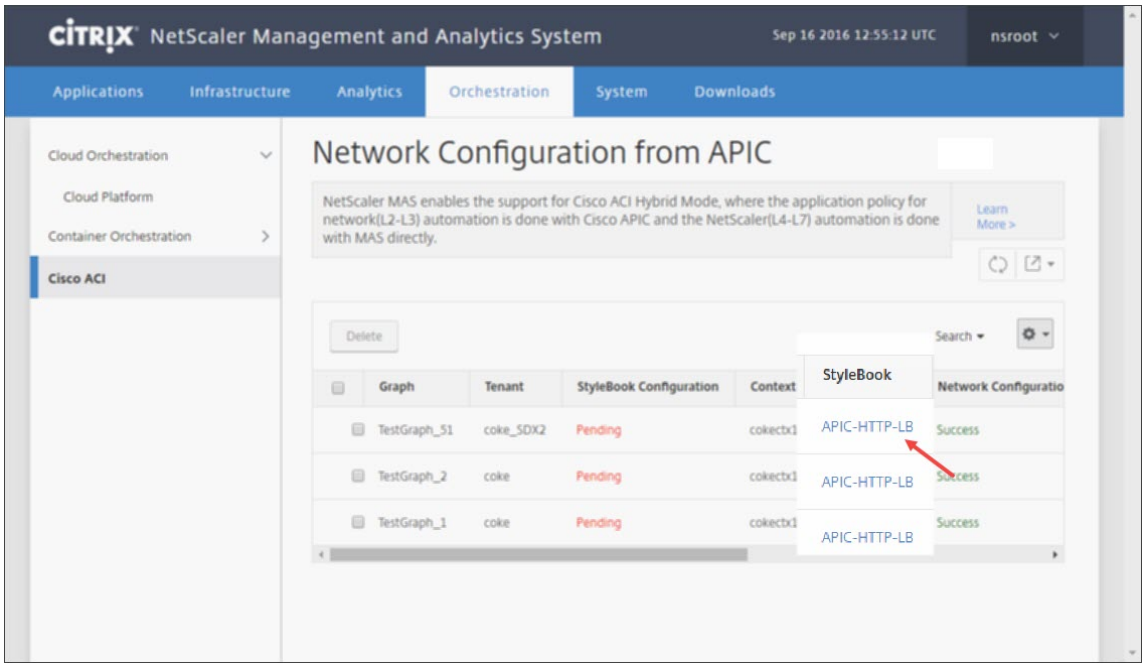
また、[**Search**] をクリックして検索オプションを使用し、データにフィルターを適用できます。ボックスから列を選択して、対応する値を入力すると、表のデータにフィルターを適用できます。

> 注
>
> 検索機能では大文字と小文字が区別されるので、正確な検索条件を入力してください。

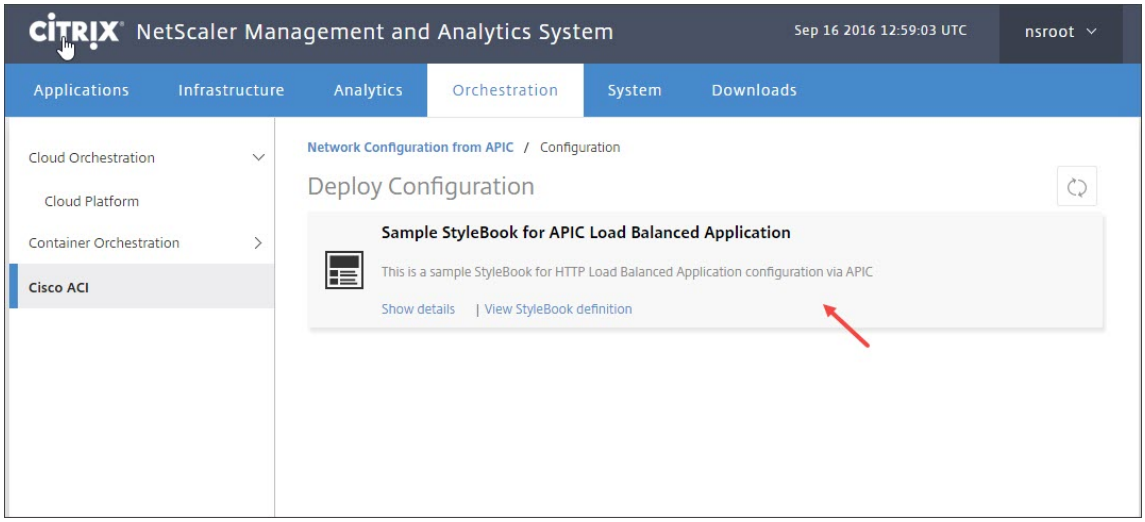


Citrix ADM で StyleBook を使用して L4-L7 構成を展開するには:

1. 表形式ビューで URL として表示されている StyleBook の名前をクリックします。



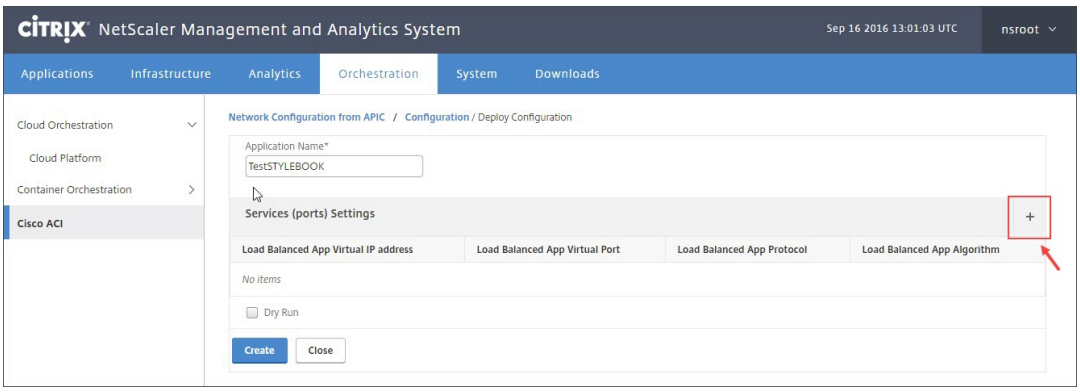
2. 設定ウィンドウで **StyleBook** をダブルクリックします。



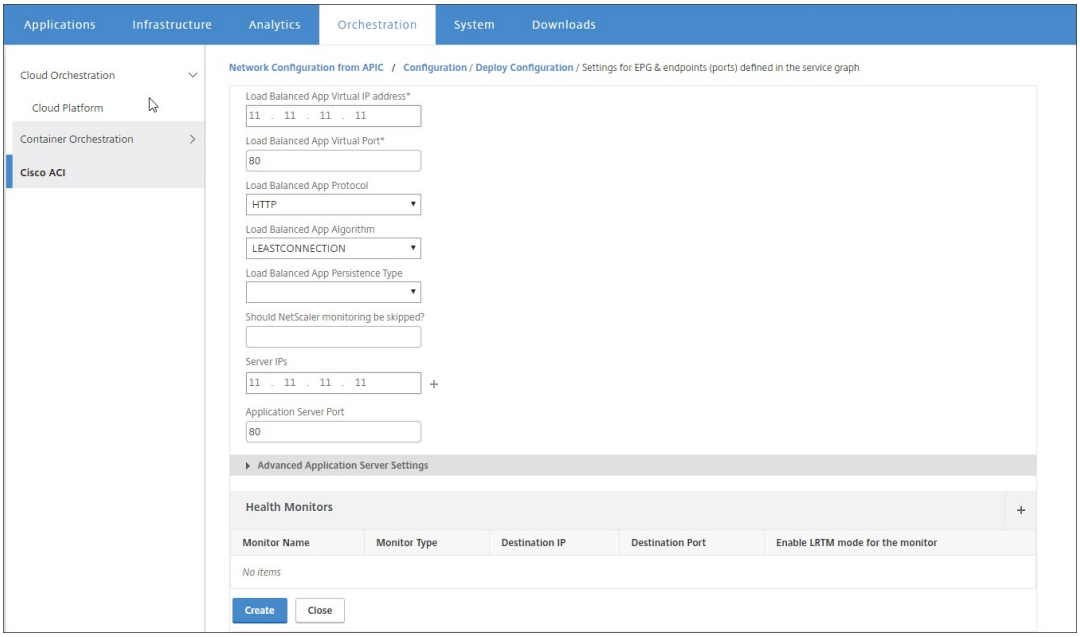
3. [Deploy Configuration] ウィンドウで次の操作を行います。

   a) APIC のアプリケーションのサービスグラフに対応する ADC の機能構成の名前を［**Application Name**］フィールドに入力します。

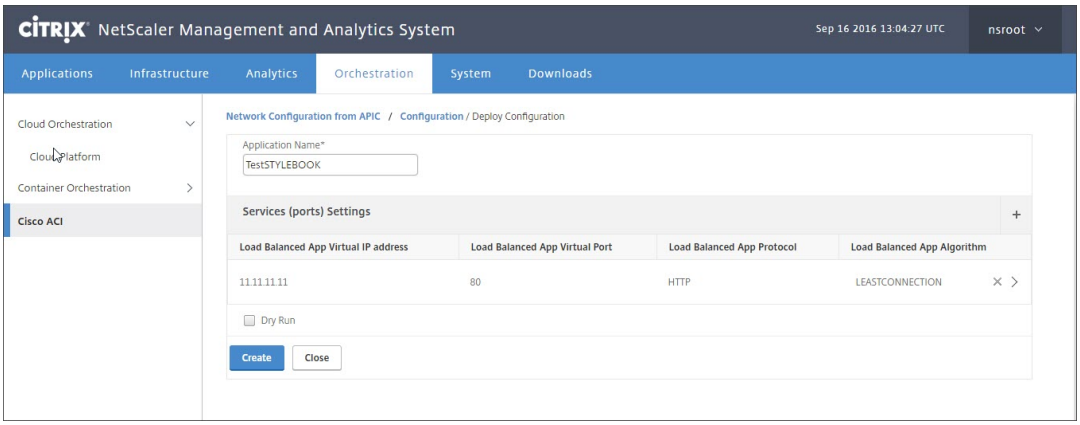
   b) [Service (ports) Settings] セクションで［**+**］をクリックします。



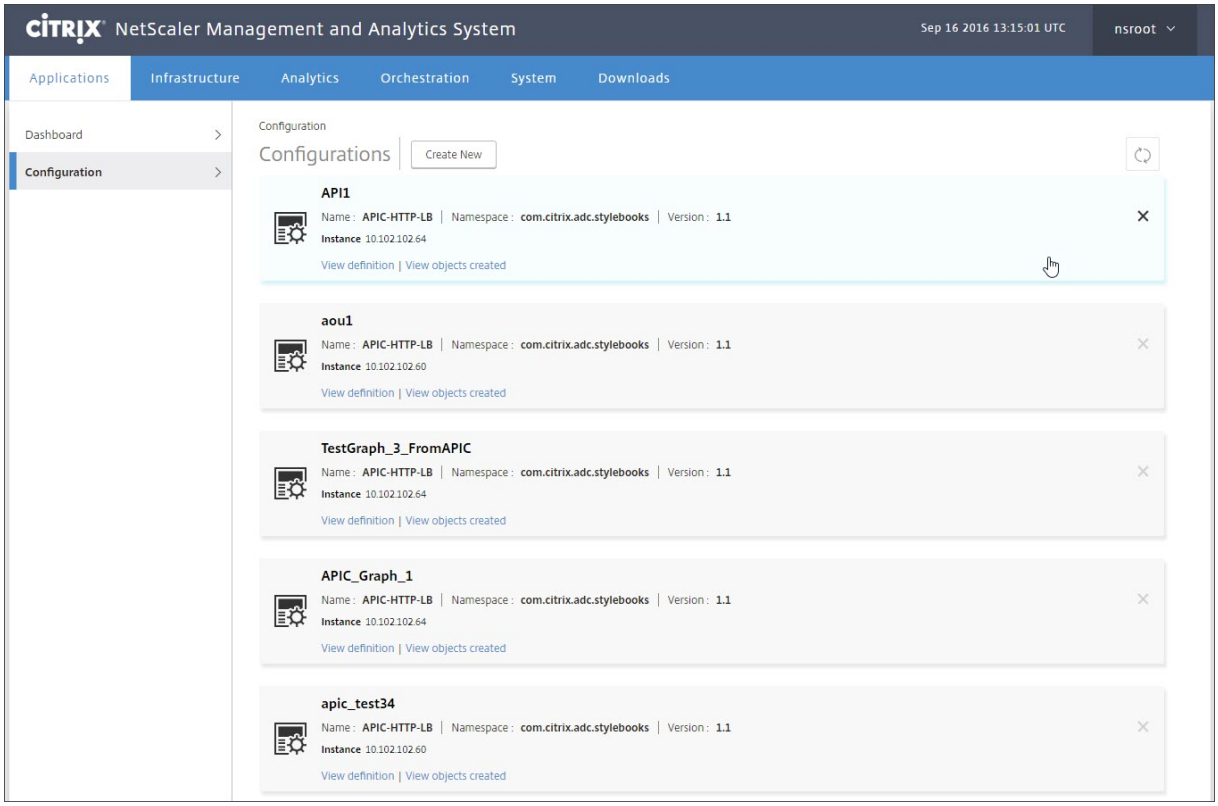
   c) サービスグラフウィンドウで定義されている **EPG** とエンドポイント（ポート）の設定で、**StyleBook** から入力されたパラメータの値を入力し、「作成」をクリックします。



d) [作成] をクリックします。



StyleBook で指定されている L4-L7 構成が Citrix ADM にデプロイされます。StyleBoook 構成を表示するには、[**Application**] タブで [**Application**] > [**Configuration**] の順に選択します。



APIC からのエンドポイントイベントのアタッチとデタッチ

February 6, 2024

ハイブリッドモードソリューションでは、Cisco APIC からの接続/接続解除エンドポイントイベントを暗黙的に処理します。Cisco APIC がエンドポイント接続イベントをトリガーすると、Citrix Application Delivery Management（ADM）の StyleBook によって servicegroup_servicegroupmember_binding が自動的にトリガーされ、エンドポイントのデタッチイベント中にエンドポイントのバインドが解除されます。

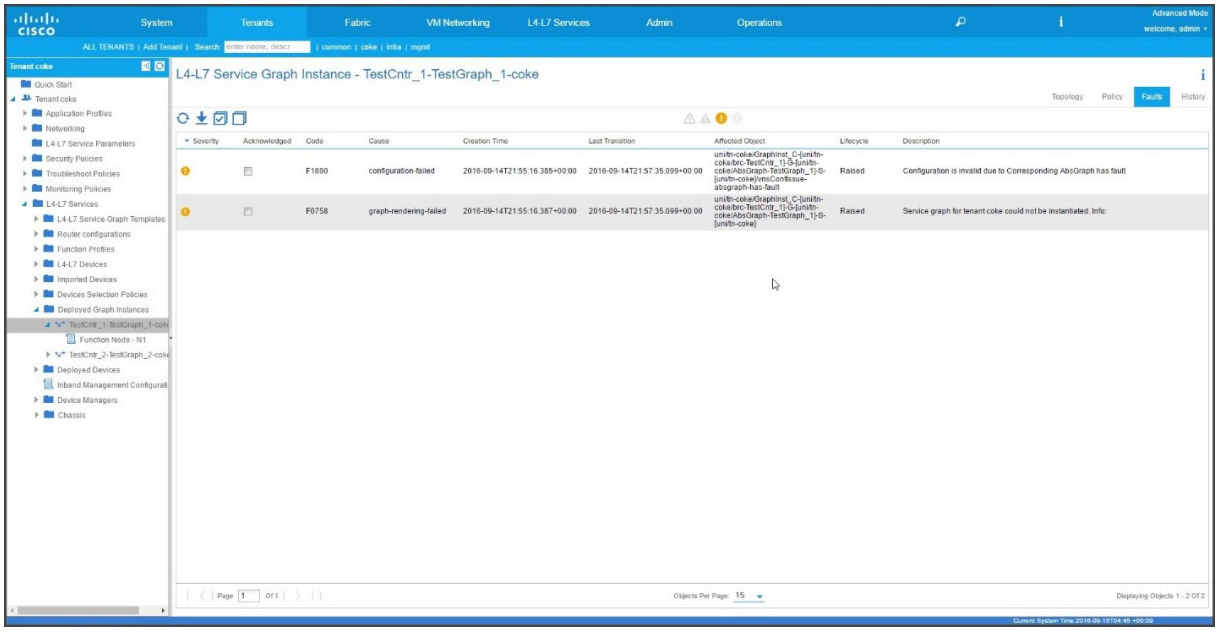
さらに、Cisco APIC でエンドポイントの接続または切断イベントがトリガーされる前に Citrix ADM に L4-L7 構成を展開していない場合、ソリューションは接続 IP アドレスをデータベースに保持します。これらの IP アドレスは、StyleBook 経由でサービスグループが作成された後、対応するサービスグループにバインドされます。

APIC 障害レポート

February 6, 2024

Citrix ADC デバイスパッケージを Cisco ACI にデプロイすると、Cisco APIC はすべての障害を報告します。障害レポートは、APIC のどのレベルのものでも表示できます（例：デバイス、テナント、EPG、サービスグラフ）。次のスクリーンショットは、デバイスレベルの障害レポートを示しています。障害の詳細については、http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/faults/guide/b_APIC_Faults_Errors/b_IFC_Faults_Errors_chapter_01.htmlを参照してください。

いずれかの APIC エンティティを選択して、[**Faults**] タブをクリックすると、そのエンティティについて APIC が報告した障害が表示されます。



NetScaler ADM によって生成されたログ

February 6, 2024

CitrixApplication Delivery Management（ADM）は、問題のトラブルシューティングに役立つ広範なログを提供します。生成されたログ（**admin.log**）は、**/var/controlcenter/log/**に格納されます。

Citrix ADM にログオンし、シェルを使用して Citrix ADM ディレクトリ構造に移動できます。次に、APIC のグラフ展開用の NetScaler ADM ログのサンプルスニペットを示します。

```
    2016-06-29 10:58:33,816 DEBUG APIC Config  = {
(0, '', 5230): {
'dn': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-cokectx1', 'state': 1, 'transaction': 0, 'ackedstate': 0, 'tenant': 'coke_SDX2', 'ctxName': 'cokectx1', 'value': {
(10, '', 'ADCHybridMode_1_Consumer_1'): {
'state': 1, 'transaction': 0, 'cifs': {
```



```
6   'ADCHybridMode_1_Device_1': '1_1' }
7   , 'ackedstate': 0 }
8   , (7, '', '2129920_32778'): {
9   'state': 1, 'tag': 273, 'type': 1, 'ackedstate': 0, 'transaction': 0 }
10  , (1, '', 5790): {
11  'transaction': 0, 'ackedstate': 0, 'value': {
12  (3, 'ADCFunction', 'N1'): {
13  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
14  (4, 'mFCngNetwork', 'mFCngnetwork'): {
15  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
16  (6, 'Network_key', 'network_key'): {
17  'state': 1, 'transaction': 0, 'target': 'network', 'ackedstate': 0 }
18   }
19   }
20  , (4, 'internal_network', 'internal_network'): {
21  'connector': 'provider', 'state': 1, 'transaction': 0, 'ackedstate':
       0, 'value': {
22  (6, 'internal_network_key', 'internal_network_key'): {
23  'state': 1, 'transaction': 0, 'target': 'network/internal_snip', '
       ackedstate': 0 }
24   }
25   }
26  , (2, 'external', 'consumer'): {
27  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
28  (9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
29  'state': 1, 'transaction': 0, 'target': '
       ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
30   }
31   }
32  , (4, 'mFCngStylebook', 'mFCngStylebook'): {
33  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
34  (6, 'Stylebook_key', 'Stylebook_key'): {
35  'state': 1, 'transaction': 0, 'target': 'stylebook_1', 'ackedstate': 0
        }
36   }
37   }
38  , (2, 'internal', 'provider'): {
39  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
40  (9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
41  'state': 1, 'transaction': 0, 'target': '
       ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
42   }
43   }
44   }
45   }
46   }
47  , 'state': 1, 'absGraph': 'HybridModeGraph_1', 'rn': u'vGrp-[uni/tn-
       coke_SDX2/GraphInst_C-[uni/tn-coke_SDX2/brc-TestCntr_3]-G-[uni/tn-
       coke_SDX2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
48  , (4, 'Network', 'network'): {
49  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
50  (4, 'nsip', 'internal_snip'): {
51  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
```



```
(5, 'type', 'type'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'SNIP' }
, (5, 'hostroute', 'hostroute'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'DISABLED' }
, (5, 'ipaddress', 'ipaddress'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '10.1.1.1' }
, (5, 'dynamicrouting', 'dynamicRouting'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'ENABLED' }
, (5, 'netmask', 'netmask'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '255.255.255.0
    ' }
 }
 }
 }
 }
, (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'state': 1, 'transaction': 0, 'vif': 'ADCHybridMode_1_Consumer_1', '
    ackedstate': 0, 'encap': '2129920_32778' }
, (4, 'Stylebook', 'stylebook_1'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(5, 'name', 'stylebookName'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'
     }
 }
 }
 }
, 'txid': 10000 }
 }

   2016-06-29 10:58:33,816 DEBUG get Graph Return details = {
'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[
    uni/tn-coke_SDX2]-ctx-cokectx1', (1, '', 5790): {
'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-
    coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-
    HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
, 'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB', '
    graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', '
    graphInstanceId': 5790 }

   2016-06-29 10:58:33,827 DEBUG SUCCESS created track 2.0
   2016-06-29 10:58:33,833 DEBUG SUCCESS updated track with new task 2
   2016-06-29 10:58:33,851 DEBUG SUCCESS updated track with new task 1
   2016-06-29 10:58:33,867 DEBUG fn_wrapper:long_operation_thread_id:<
       eventlet.greenthread.GreenThread object at 0x80aa5c7d0>
   2016-06-29 10:58:33,867 DEBUG +++++++ Service Audit Call for Device
        Details  = 10.102.102.62 ++++++++++++++++++
   2016-06-29 10:58:33,867 DEBUG Inside APIC Cred Col If = 2
   2016-06-29 10:58:33,867 DEBUG Host name from device =
       ADCHybridMode_1
   "InProgress","message":null,"replication_status":"","target":"
       10.102.102.81","operation":"POST","entity_type":"apic","
       entity_id":null }
 }
```



```
92
93      2016-06-29 10:58:44,141 DEBUG  Save config  Response = {
94    "errorcode": 0, "message": "Done", "severity": "NONE"  }
95
96      2016-06-29 10:58:44,141 DEBUG +++++++++ getContextAwareFlag = True
97      2016-06-29 10:58:44,141 DEBUG +++++ get context tenant name from
           Config ++++++
98      2016-06-29 10:58:44,141 DEBUG +++++ getContextTenantName = {
99    'state': 1, 'ctxName': 'cokectx1', 'tenant': 'coke_SDX2', 'vdev': 5230
         }
100   ++++++
101     2016-06-29 10:58:44,142 DEBUG Service health details = {
102   }
103   collection length = 0
104     2016-06-29 10:58:44,142 DEBUG Count details Total = 0 Up = 0 Down =
           0
105     2016-06-29 10:58:44,142 DEBUG Health Score details Up = 0
106     2016-06-29 10:58:44,142 DEBUG Service HEALTH final collection  = {
107   ((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')): {
108   'faults': [], 'state': 0, 'health': ([(0, '', 5230), (1, '', 5790),
        (3, 'ADCFunction', 'N1')], 0) }
109   }
110
111     2016-06-29 10:58:44,142 DEBUG ++++++getServiceHealth Fault List =
           []
112     2016-06-29 10:58:44,142 DEBUG Service HEALTH final response  = {
113   'devs': 'ADCHybridMode_1_Device_1', 'faults': [], 'state': 0, 'health'
        : [([(0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')], 0)] }
114
115     2016-06-29 10:58:44,236 DEBUG RESPONSE from NSLOGOUT = {
116   "errorcode": 0, "message": "Done", "severity": "NONE"  }
117   , sessionId = ##
        D2EAFA7CFCD73119E6C5E78D8BCB2E842829C971C1DC7E99850949DAE0029F2191B5E7EDF2764

118     2016-06-29 10:58:44,237 DEBUG +++++ Faults respCol   = {
119   '10.102.102.62': {
120   '10.102.102.62': {
121   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
         u'NONE', 'operation_name': 'add_op' }
122   }
123   , (7, '', '2129920_32778'): {
124   'vlan': {
125   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
         u'NONE', 'operation_name': 'add_op' }
126   }
127   , (((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1'), (2, '
        internal', 'provider')), 'nsip'): {
128   'vlan_nsip_binding': {
129   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
         u'NONE', 'operation_name': 'bind_op' }
130   }
131   , (((0, '', 5230), (4, 'Network', 'network')), (4, 'nsip', '
        internal_snip')): {
```



```
'nsip': {
u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity': u'NONE', 'operation_name': 'add_op' }
 }
, (): {
 }
, (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'vlan_interface_binding': {
u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity': u'NONE', 'operation_name': 'bind_op' }
 }
 }

   2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg = Done, statusCode = add_op
   2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg = Done, statusCode = add_op
   2016-06-29 10:58:44,237 DEBUG Fault details oprName = bind_op, erMsg = Done, statusCode = bind_op
   2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg = Done, statusCode = add_op
   2016-06-29 10:58:44,238 DEBUG Fault details oprName = bind_op, erMsg = Done, statusCode = bind_op
   2016-06-29 10:58:44,238 DEBUG +++++++++++++ ServiceAudit response = {
'faults': [], 'state': 0, 'health': [] }

   2016-06-29 10:58:44,238 DEBUG APIC Graph Details = {
'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-cokectx1', (1, '', 5790): {
'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
, 'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB', 'graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', 'graphInstanceId': 5790 }

   2016-06-29 10:58:44,242 DEBUG Journal Processing: Database task: create apic_graph
   2016-06-29 10:58:44,264 DEBUG SUCCESS created task 2
   2016-06-29 10:58:44,269 DEBUG SUCCESS updated track with new task 2
   2016-06-29 10:58:44,308 DEBUG +++++++ get IP and Connector collection from Config with type 22 for attach & detach event ++++++
   2016-06-29 10:58:44,308 DEBUG ----- connector with IP List = {
0: [], 1: [], 3: [] }

   2016-06-29 10:58:44,308 DEBUG ----- attachIpList = [] dettachIpList = []
   2016-06-29 10:58:44,308 DEBUG ----- In _attachDettachIps attachIpList = [] dettachIpList = []
   2016-06-29 10:58:44,312 DEBUG ----- In _attachDettachIps row = {
'deviceIP': u'10.102.102.62', 'responseToAPIC': None, 'graphDN': u'uni
```



```
        /vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-
        coke_SDX2]-ctx-cokectx1', 'apicGraphState': None, 'serviceGroupName
        ': None, 'configPackId': None, 'tenantName': u'coke_SDX2', '
        styleBookName': u'APIC-HTTP-LB', 'graphInstanceName': u'
        HybridModeGraph_1', 'context': u'cokectx1', 'serviceGroupPort':
        None, 'graphInstanceId': 5790, 'createDate': None, 'serviceGroupIP'
        : None }
167
168 <!--NeedCopy-->
```

ハイブリッドモードデバイスパッケージによって生成されるログ

February 6, 2024

Citrix ADC ハイブリッドモードデバイスパッケージは、構成関連のログと監視関連のログを生成します。生成されたログは、**/data/devicescript/ Citrix.NetScalerMAS.1.0/logs** にあります。

Cisco APIC の **debug.log** のスニペットの例を次に示します。

```
1      2016-06-28 03:06:53.879767 DEBUG Thread-20 18723 [10.102.102.62,
          24063] Device manager details ip = 10.102.102.81, port = 80
2      2016-06-28 03:06:53.879856 DEBUG Thread-20 18724 [10.102.102.62,
          24063] +++++++++++++++ serviceAudit  request ++++++++++++++++++
3      2016-06-28 03:06:53.879929 DEBUG Thread-20 18725 [10.102.102.62,
          24063] ++++++++++ getStyleBookObjects ++++++++++++
4      2016-06-28 03:06:53.879995 DEBUG Thread-20 18726 [10.102.102.62,
          24063] NMAS collection A3 = (4, 'Stylebook', 'stylebook_1') B3 =
           {
5   'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
6   (5, 'name', 'stylebookName'): {
7   'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'
        }
8    }
9    }
10
11     2016-06-28 03:06:53.880045 DEBUG Thread-20 18727 [10.102.102.62,
          24063] NMAS collection styleBookName= APIC-HTTP-LB
12     2016-06-28 03:06:53.880093 DEBUG Thread-20 18728 [10.102.102.62,
          24063] NMAS collection retCol= {
13  'Stylebook': 'APIC-HTTP-LB', 'tuple': ((0, '', 5230), (4, 'Stylebook',
        'stylebook_1')) }
14
15     2016-06-28 03:06:53.880140 DEBUG Thread-20 18729 [10.102.102.62,
          24063]  ++++ devMgrStyleBookUrl = http://10.102.102.81/stylebook
          /nitro/v1/config/stylebooks/com.citrix.adc.stylebooks/1.1/APIC-
          HTTP-LB
16     2016-06-28 03:06:54.135240 DEBUG Thread-20 18730 [10.102.102.62,
          24063]  ++++ Response from styleBookresCode serviceAudit = {
17  u'stylebook': {
```



```
18  u'uses_builtin_namespaces': {
19  u'netscaler.nitro.config': u'10.5' }
20  , u'name': u'APIC-HTTP-LB', u'used_by_stylebooks': [], u'namespace': u
       'com.citrix.adc.stylebooks', u'source': u'---\nname: APIC-HTTP-LB\
       nnamespace: com.citrix.adc.stylebooks\nversion: "1.1"\ndisplay-name
       : "Sample StyleBook for APIC Load Balanced Application"\
       ndescription: "This is a sample StyleBook for HTTP Load Balanced
       Application configuration via APIC"\nschema-version: "1.0"\nimport-
       stylebooks: \n  - \n    namespace: netscaler.nitro.config\n
       prefix: ns\n    version: "10.5"\n  - \n    namespace: "com.citrix.
       adc.stylebooks"\n    prefix: "stlb"\n    version: "1.1"\nparameters
       -default-sources:\n  - stlb::APIC-ROOT\nsubstitutions:\n  lb-name(
       appname, port): $appname + "-" + str($port) + "-lb"\n  sg-name(
       appname, port): $appname + "-" + str($port) + "-sg"\n
       healthmonitor[]:\n    true: "NO"\n    false: "YES"\ncomponents: \n
        - \n    name: lbvserver\n    type: ns::lbvserver\n    repeat:
       $parameters.app-services\n    repeat-item: app\n    properties: \
       n      name: $substitutions.lb-name($parameters.appname, $app.
       virtual-port)\n      ipv46: $app.virtual-ip\n      port: $app.
       virtual-port\n      servicetype: $app.protocol\n      lbmethod?:
       $app.algorithm\n      persistencetype?: $app.persistence\n  - \n
        name: svcgrp\n    type: ns::servicegroup\n    repeat: $parameters.
       app-services\n    repeat-item: app\n    properties: \n      name:
       $substitutions.sg-name($parameters.appname, $app.virtual-port)\
       n      servicetype: $app.protocol\n      useproxyport?: $app.sg-
       advanced.useproxyport\n      usip?: $app.sg-advanced.usip\n
       cip?: $app.sg-advanced.cip\n      cipheader?: $app.sg-advanced.
       cipheader\n      healthmonitor?: $substitutions.healthmonitor($app.
       skip_healthmonitor)\n    components: \n      -\n        name:
       lbvserver-svg-binding\n        type: ns::
       lbvserver_servicegroup_binding\n        properties: \n
       name: $substitutions.lb-name($parameters.appname, $app.virtual-port
       )\n          servicegroupname: $parent.properties.name\n      - \
       n        name: svg-members\n        type: ns::
       servicegroup_servicegroupmember_binding\n        condition: $app.
       server-ips\n        repeat: $app.server-ips\n        repeat-item:
       serverip\n        properties: \n          ip: $serverip\n
       port: $app.server-port\n          servicegroupname: $parent.
       properties.name\noutputs: \n  - \n    name: lbvservers\n    value:
       $components.lbvserver\n  - \n    name: servicegroups\n    value:
       $components.svcgrp', u'version': u'1.1', u'uses_stylebooks': [{
21  u'version': u'1.1', u'namespace': u'com.citrix.adc.stylebooks', u'name
       ': u'APIC-ROOT' }
22  ] }
23   }
24
25     2016-06-28 03:06:54.359142 DEBUG Thread-20 18731 [10.102.102.62,
          24063]  ++++ Dev Mgr request details devMgrUrl = http://
          10.102.102.81/admin/v1/apic
26     2016-06-28 03:06:54.359221 DEBUG Thread-20 18732 [10.102.102.62,
          24063]  ++++ Response from Device Mgr serviceAudit = {
27  "APIC":[] }
28
```



```
29      2016-06-28 03:06:54.359266 DEBUG Thread-20 18733 [10.102.102.62,
           24063] ++++++++++++++ serviceAudit response = {
30   "APIC":[] }
31
32      2016-06-28 03:06:54.359306 DEBUG Thread-20 18734 [10.102.102.62,
           24063] ++++++++++++++ serviceAudit response headers content type
           = application/json; charset=utf-8
33      2016-06-28 03:06:54.359394 DEBUG Thread-20 18735 [10.102.102.62,
           24063] ++++++++++++++ serviceAudit response headers = {
34   'content-length': '11', 'job_id': 'ctxt-f4db2883-e42c-4262-a35f-04628
        c4ad5ea', 'x-content-type-options': 'nosniff', 'transfer-encoding':
         'chunked', 'connection': 'close', 'date': 'Wed, 29 Jun 2016
        10:58:33 GMT', 'x-frame-options': 'SAMEORIGIN', 'content-type': '
        application/json; charset=utf-8' }
35
36      2016-06-28 03:06:54.359480 DEBUG Thread-20 18736 [10.102.102.62,
           24063] ++++++++++++++ pollingURL = http://10.102.102.81/admin/v1
           /journalcontexts/ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea
37      2016-06-28 03:06:54.359713 DEBUG Thread-20 18737 [10.102.102.62,
           24063] ++++++++++++++ pollingStatus = True, pollingTime = 0
38      2016-06-28 03:06:54.483228 DEBUG Thread-20 18738 [10.102.102.62,
           24063] ++++++++++++++ pollingResponse json = {
39   u'journalcontext': {
40   u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name':
         u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
        service_name': u'admin', u'start_time': u'2016-06-29T10
        :58:33.760565', u'is_default': u'false', u'end_time': None, u'
        target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883
        -e42c-4262-a35f-04628c4ad5ea', u'replication_status': u'' }
41    }
42
43      2016-06-28 03:07:04.493074 DEBUG Thread-20 18739 [10.102.102.62,
           24063] ++++++++++++++ pollingStatus = True, pollingTime = 1
44      2016-06-28 03:07:04.587595 DEBUG Thread-20 18767 [10.102.102.62,
           24063] ++++++++++++++ pollingResponse json = {
45   u'journalcontext': {
46   u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name':
         u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
        service_name': u'admin', u'start_time': u'2016-06-29T10
        :58:33.760565', u'is_default': u'false', u'end_time': None, u'
        target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883
        -e42c-4262-a35f-04628c4ad5ea', u'replication_status': u'' }
47    }
48
49      2016-06-28 03:07:14.597812 DEBUG Thread-20 18790 [10.102.102.62,
           24063] ++++++++++++++ pollingStatus = True, pollingTime = 2
50      2016-06-28 03:07:14.692590 DEBUG Thread-20 18791 [10.102.102.62,
           24063] ++++++++++++++ pollingResponse json = {
51   u'journalcontext': {
52   u'status': u'Finished', u'scopes': [], u'entity_id': None, u'name': u'
        Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
        service_name': u'admin', u'start_time': u'2016-06-29T10
        :58:33.760565', u'is_default': u'false', u'end_time': u'2016-06-29
```



```
        T10:58:44.486919', u'target': u'10.102.102.81', u'message': u'Done'
        , u'id': u'ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea', u'
        replication_status': u'' }
    }

      2016-06-28 03:07:14.692932 DEBUG Thread-20 18793 [10.102.102.62,
         24063] Attempts 1
      2016-06-28 03:07:14.693031 DEBUG Thread-20 18794 [10.102.102.62,
         24063] Cluster (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1', (0,
          '', 5230)), transaction: 0
      2016-06-28 03:07:14.693147 DEBUG Thread-20 18795 [10.102.102.62,
         24063] Attempts for {
  'name': 'ADCHybridMode_1', 'host': '10.102.102.62', 'virtual': False,
      'devs': {
  'ADCHybridMode_1_Device_1': {
  'state': 0, 'virtual': False, 'manager': {
  'hosts': {
  '10.102.102.81': {
  'port': 80 }
   }
  , 'name': 'NMAS_1', 'creds': {
  'username': 'nsroot', 'password': '<hidden>' }
   }
  , 'version': '11.0', 'host': '10.102.102.62', 'port': 80, 'creds': {
  'username': 'nsroot', 'password': '<hidden>' }
   }
   }
  , 'manager': {
  'hosts': {
  '10.102.102.81': {
  'port': 80 }
   }
  , 'name': 'NMAS_1', 'creds': {
  'username': 'nsroot', 'password': '<hidden>' }
   }
  , 'contextaware': True, 'port': 80, 'creds': {
  'username': 'nsroot', 'password': '<hidden>' }
   }
   is 0
      2016-06-28 03:07:14.693339 DEBUG Thread-20 18796 [10.102.102.62,
         24063] Deleting (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1',
         (0, '', 5230))
      2016-06-28 03:07:14.693379 DEBUG Thread-20 18797 [10.102.102.62,
         24063] pending: False, delete: False, txId: None
      2016-06-28 03:07:14.693517 DEBUG Thread-20 18798 [10.102.102.62,
         24063] Faults: []
      2016-06-28 03:07:14.693558 DEBUG Thread-20 18799 [10.102.102.62,
         24063] Health: []
      2016-06-28 03:07:14.693914 DEBUG Thread-20 18800 [10.102.102.62,
         24063] Send num: 761, type: 220, len: 382
<!--NeedCopy-->
```


Cisco ACI のクラウドオーケストレータモードの **NetScaler ADC** デバイスパッケージ

February 6, 2024

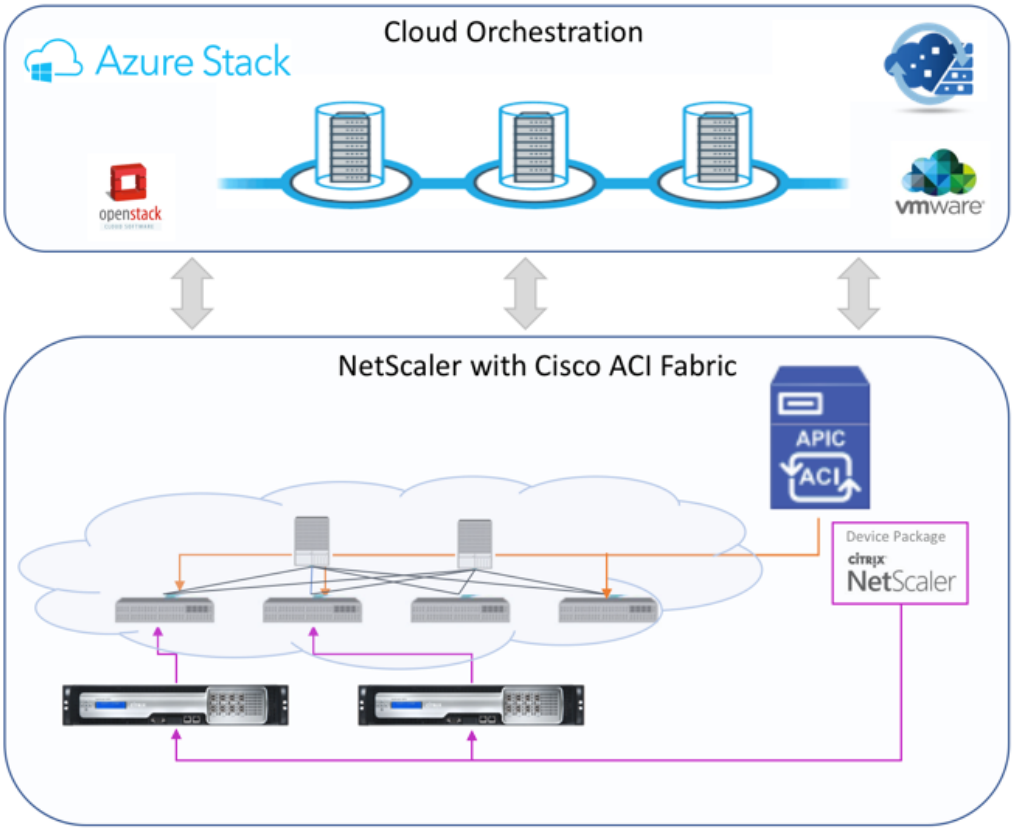
アプリケーションポリシーインフラストラクチャコントローラ（APIC）バージョン 3.1 により、Citrix ADC と Cisco ACI は共同統合ポートフォリオを拡大し、お客様のニーズに対応する新しいソリューションを提供します。新しい統合モードである ACI Cloud Orchestrator Mode* は、標準化されたパラメーターによって構成の複雑さを抽象化することで、L4-L7 の統合を簡素化します。このソリューションはシームレスに動作し、L4-L7 サービスを自動化し、アジャイルなアプリケーション展開、運用の柔軟性、シンプルさという目標を達成します。

NetScaler ADC ソリューションを使用した Cisco ACI クラウドオーケストレータモードには、次の利点があります。

- L4-L7 サービスの自動化により、ヒューマンエラーが減少します。
- 事前に構築された Cisco ACI ソリューションの統合により、導入時間を短縮し、Web アプリケーション、仮想マシン、SQL などのアプリケーションのパフォーマンスを向上させることができます。
- 物理ネットワークコンポーネントと仮想ネットワークコンポーネント全体で、Web アプリケーション、仮想マシン、SQL などのアプリケーションの健全性を完全に統合して可視化します。

ACI クラウドオーケストレータモードでは、新しい簡略化された APIC GUI を直接使用するか、Cisco Cloud Center、Windows Azure Pack、OpenStack、vRealize などの任意のクラウドオーケストレータを好みに応じて選択して、より多くの選択肢が提供されます。この新しい変更は、一連の ADC 属性を ADC スキーマとして公開することで実現されます。これらの属性は、デバイスパッケージの機能プロファイルにマッピングされます。クラウドオーケストレータ（Cisco Cloud Center またはワイヤレスアプリケーションプロトコル（WAP））による ADC サービスのプロビジョニング中に、これらの属性の値を指定できます。

次の図に、クラウドオーケストレーションソリューションにおける NetScaler ADC 概要を示します。

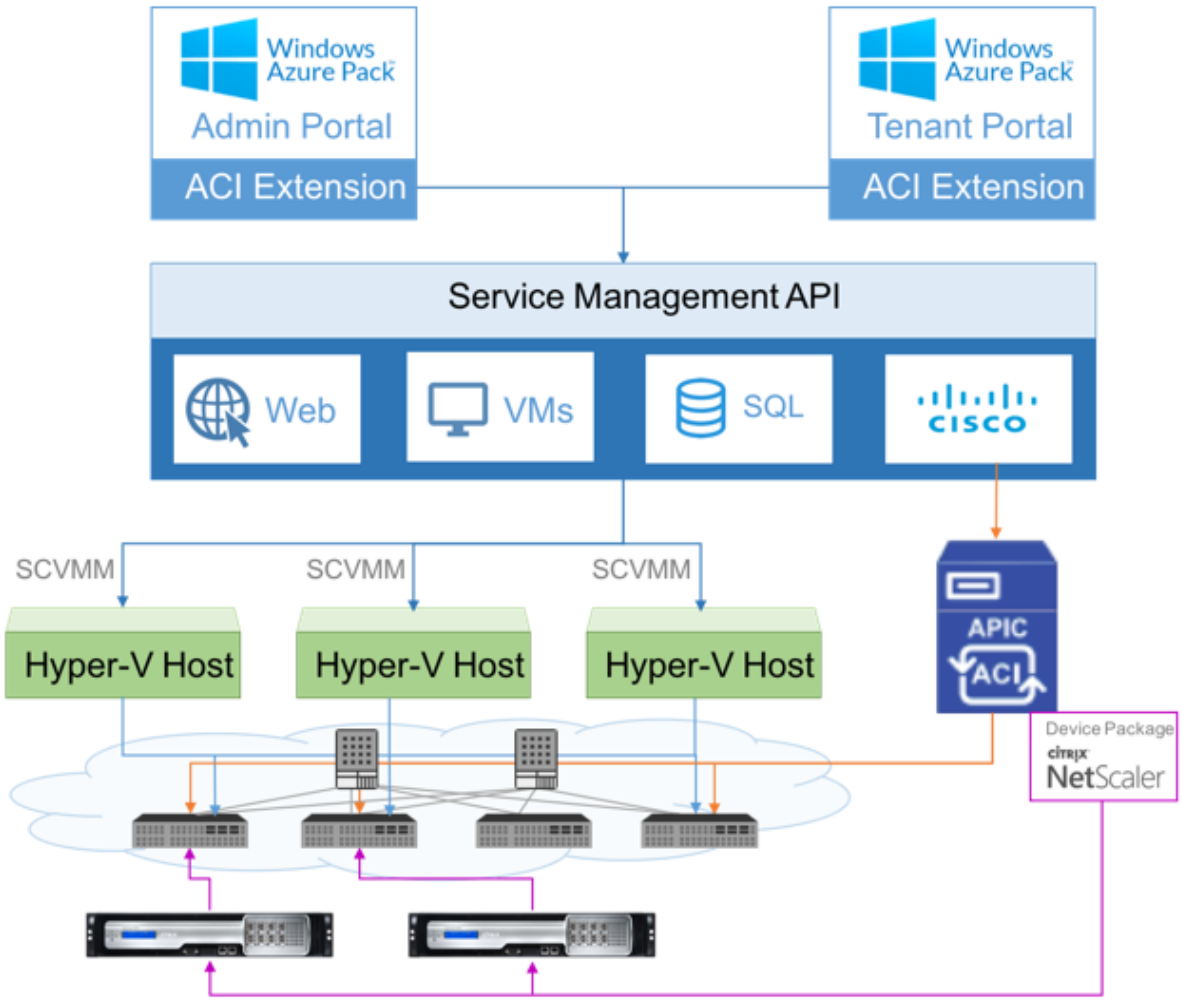


Microsoft Azure パックを使用するクラウドオーケストレーターモードソリューションには、Azure Pack から Cisco APIC、Cisco APIC からシステムセントラルのバーチャルマシンマネージャー (SCVMM)、Cisco APIC から NetScaler ADC への統合など、多くのポイントが含まれます。プライベートクラウドのテナントとして、NAT の有効化、ネットワークサービスのプロビジョニング、ロードバランサーの追加を行うことができます。

Azure Pack はテナントポータルと管理者ポータルをサポートし、それぞれに実行可能な独自の操作セットがあります。

- 管理者は、ACI 登録、VIP 範囲、NetScaler ADC デバイスと仮想マシンクラウドとの関連付け、テナントユーザーアカウントの作成などの管理タスクを実行できます。
- テナントは、Azure Pack テナントポータルへのログオンや、ネットワーク、ブリッジドメイン、仮想ルーティングおよび転送（VRF）の構成などのタスクを実行でき、NetScaler ADC 負荷分散および RNAT 機能を使用できます。

次の図は、クラウドモードソリューションにおける Azure Pack の概要を示しています。



重要

- クラウド管理者は APIC でサポートされている L4-L7 スキーマを使用でき、追加の変更は APIC 管理者が直接 APIC で実行できます。これにより、サポートされている機能セットと同等の NetScaler ADC を構成および展開できます。
- テナントは、同じネットワークに対して異なるポートを持つ複数の VIP アドレスを展開できます。IP とポートの組み合わせが一意であることを確認する必要があります。
- NetScaler ADC デバイスパッケージは、単一コンテキスト展開のみをサポートします。各テナントは専用の NetScaler ADC インスタンスを取得します。
- ワイヤレスアプリケーションプロトコル（WAP）は、NetScaler ADC MPX アプライアンスおよび NetScaler ADC VPX アプライアンス（NetScaler ADC SDX プラットフォームにデプロイされた NetScaler ADC VPX インスタンスを含む）をサポートします。

クラウドオーケストレータモードのデバイスパッケージは、完全マネージドモードとサービスマネージャモードの両

方をサポートしています。完全マネージドモードパッケージは、単純な負荷分散、コンテンツスイッチング、SSL オフロード、その他のプロファイルなど、さまざまな機能プロファイルをサポートします。これらの関数プロファイルは、NetScaler ADC の完全な機能セットと展開モードをカバーします。同様に、サービスマネージャモードのデバイスパッケージでは、APIC を使用した NetScaler ADC のワンアームおよびツ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 ADC のプロビジョニング中）の値を提供します。オーケストレータは APIC の API と通信し、特定の機能プロファイルのペイロードの一部として ADC 固有の詳細を渡します。内部的に、APIC は値を抽出し、NetScaler ADC を内部的に構成するデバイスパッケージに渡します。

Cisco APIC でサポートされている ADC スキーマの完全なリストについては、『Cisco APIC レイヤ 4 ～レイヤ 7 サービス導入ガイド、リリース 3.x 以前』を参照してください。

フルマネージドモードデバイスパッケージは、次の機能プロファイルをサポートします。

1. LB-HTTP-One-Arm-ProfileCM
2. LB-HTTP-Two-Arm-ProfileCM
3. LB-HTTP-Two-Arm-ServiceBackendProfileCM
4. CS-HTTP-LB-Service-ProfileCM
5. CS-SSL-LB-Service-ProfileCM
6. LB-SSL-ProfileCM
7. SSLVServerProfileInlineModeCM
8. WebVServerProfileWithRHICM
9. WebInlineVServerProfileWithRHICM
10. WebAnywhereVServerProfileWithRHIC
11. SSLVServerProfileForAnywhereModeCM
12. SSLAnywhereServerProfileCM
13. WebVServerProfileCM
14. WebInlineVServerProfileCM
15. WebAnywhereVServerProfileCM

16. CSLBServerProfileCM
17. GSLBServerProfileCM
18. CMPServerProfileCM
19. CRServerProfileC
20. DNSServerProfileCM
21. DSServerProfileCM
22. ICServerProfileCM
23. SSLVPNServerProfileCM
24. AppFWServerProfileCM
25. AAAServerProfileCM
26. AAASyslogServerProfileCM
27. IPv6WebInlineVServerProfileCM

サービス管理モードのデバイスパッケージでは、次のクラウドモード機能プロファイルがサポートされています。

1. ADCOneArmFunctionProfileCM
2. AADCTwoArmFunctionProfileCM
3. RHI-ADCOneArmFunctionProfileCM
4. RHI-ADCTwoArmFunctionProfileCM

NetScaler ADC は上記の機能プロファイルをサポートしています。APIC では、ADC スキーマでこれらのパラメータのサブセットがサポートされています。Cisco ACI でサポートされていない属性が機能プロファイルに存在する場合は、クラウドオーケストレータモードの機能プロファイルのクローンを作成し、APIC でサポートされていないすべての属性の値を指定し、その属性を保存する必要があります。その後、オーケストレータは新しくクローンされた機能プロファイルを使用できます。

Citrix Cloud モードデバイスパッケージは NetScaler ADC 12.0 をサポートし、サービスマネージャーモードでは NetScaler ADM 12.0 も使用されます。デバイスパッケージのモデルバージョンが 1.0 から 2.0 に変更され、新規インストールとして使用できるようになりました。Cloud Orchestrator モードデバイスパッケージは、モデルバージョンが変更されたため、以前のデバイスパッケージバージョンからアップグレードできません。

Cloud Orchestrator モードのデバイスパッケージは、通常の展開でも使用できます。このパッケージでは、クラウドオーケストレータを介して NetScaler ADC をプロビジョニングすることをユーザーに義務付けるものではありません。デバイスパッケージは APIC と APIC とクラウドオーケストレータとのみ互換性があります。

NetScaler ADC プール容量

February 6, 2024

NetScaler ADC プール容量により、異なる ADC フォームファクタ間で帯域幅またはインスタンスライセンスを共有できます。仮想 CPU サブスクリプションベースのインスタンスの場合、仮想 CPU ライセンスをインスタンス間で共有できます。このプールされたキャパシティーは、データセンターまたはパブリッククラウドにあるインスタンスに使用します。インスタンスがリソースを必要としなくなると、割り当てられたキャパシティーを共通プールにチェックインし直します。解放された容量を、リソースを必要とする他の ADC インスタンスに再利用します。

プールされたライセンスを使用して、必要な帯域幅をインスタンスに割り当てて、必要量を超えないようにすることで、帯域幅の使用率を最大化できます。トラフィックに影響を与えずに、実行時にインスタンスに割り当てられる帯域幅を増減します。プール容量ライセンスを使用すると、インスタンスの Provisioning を自動化できます。

NetScaler ADC プール容量ライセンスの仕組み

NetScaler ADC プール容量には、次のコンポーネントがあります。

- NetScaler ADC インスタンス。次のものに分類できます。
  - ゼロキャパシティハードウェア
  - スタンドアロンの VPX インスタンスまたは CPX インスタンス
- 帯域幅プール
- インスタンスプール
- Citrix ADM がライセンスサーバーとして構成されている

ゼロキャパシティハードウェア

NetScaler ADC プール容量を使用して管理する場合、MPX および SDX インスタンスは「容量ゼロハードウェア」と呼ばれます。これは、これらのインスタンスは、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。そのため、これらのプラットフォームは MPX-Z アプライアンスや 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。ただし、NetScaler ADC プール容量を別の NetScaler ADC ハードウェアインスタンスに使用することはできません。

プラットフォームライセンスを管理およびインストールします。プラットフォームライセンスは、ハードウェアシリアル番号またはライセンスアクセスコードを使用して手動でインストールする必要があります。プラットフォームライセンスがインストールされると、そのライセンスはハードウェアにロックされ、NetScaler ADC ハードウェア

インスタンス間でオンデマンドで共有できなくなります。ただし、プラットフォームライセンスを別の NetScaler ADC ハードウェアインスタンスに手動で移動することはできます。

ADC ソフトウェアリリース 11.1 ビルド 54.14 以降を実行する ADC MPX インスタンスと 11.1 ビルド 58.13 以降を実行する ADC SDX インスタンスは、ADC プールされた容量をサポートします。詳細については、表 **1** を参照してください。**MPX** および **SDX** インスタンスのプール容量をサポートしました。

スタンドアロン **NetScaler ADC VPX** インスタンス

次のハイパーバイザーで NetScaler ADC ソフトウェアリリース 11.1 Build 54.14 以降を実行している NetScaler ADC VPX インスタンスは、プール容量をサポートします。

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

Citrix ADC ソフトウェアリリース 12.0 Build 51.24 以降を実行する Citrix ADC VPX インスタンスは、以下のハイパーバイザーとクラウドプラットフォーム上でプールキャパシティをサポートします。

- Microsoft Hyper-V
- AWS
- Microsoft Azure

> 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 Citrix ADC VPX インスタンスを Citrix ADM に追加する」を参照してください。
> ゼロキャパシティハードウェアとは異なり、VPX にプラットフォームライセンスは必要ありません。VPX では、トラフィック処理のためにプールから帯域幅とインスタンスライセンスをチェックアウトする必要があります。

スタンドアロン **NetScaler ADC CPX** インスタンス

Docker er ホストにデプロイされた NetScaler ADC CPX インスタンスは、プール容量をサポートします。ゼロキャパシティハードウェアとは異なり、CPX にプラットフォームライセンスは必要ありません。CPX では、トラフィック処理のためにプールからインスタンスライセンスをチェックアウトする必要があります。

帯域幅プール

帯域幅プールは、NetScaler ADC インスタンス（物理および仮想の両方）で共有できる合計帯域幅です。帯域幅プールは、ソフトウェアエディション（Standard、Enterprise、Platinum）別のプールで構成されます。特定の

NetScaler ADC インスタンスでは、異なるプールの帯域幅を同時にチェックアウトすることはできません。インスタンスが帯域幅をチェックアウトできる帯域幅プールは、ライセンスが割り当てられているソフトウェアエディションによって決まります。

インスタンスプール

インスタンスプールは、NetScaler ADC プール容量を介して管理できる VPX インスタンスまたは CPX インスタンスの数、または SDX-Z インスタンス内の VPX インスタンスの数を定義します。

ライセンスがプールからチェックアウトされると、ライセンスにより MPX-Z、SDX-Z、VPX、CPX の各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、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

Citrix ADC 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 Citrix ADM ソフトウェアを使用して、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。Citrix ADM を使用すると、ADM ライセンスなしで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 ADC フォームファクタとハードウェアモデル番号によって、

- NetScaler ADC インスタンスが機能する前にチェックアウトする必要のある最小帯域幅とインスタンス数。
- NetScaler ADC がチェックアウトできる最大帯域幅とインスタンス数。
- 帯域幅チェックアウトごとの最小帯域幅単位。最小帯域幅単位は、NetScaler ADC がプールからチェックアウトする必要がある最小帯域幅単位です。チェックアウトは、最小帯域幅単位の整数倍で行う必要があります。たとえば、NetScaler ADC 最小帯域幅単位が 1Gbps の場合、100Gbps をチェックアウトできますが、200Mbps または 150.5Gbps はチェックアウトできません。最小帯域幅単位は、最小帯域幅要件とは別のものです。NetScaler ADC インスタンスは、少なくとも最小帯域幅でライセンスされた後にのみ動作します。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 は、サポートされているすべての NetScaler インスタンスの最大帯域幅/インスタンス、最小帯域幅/インスタンス、および最小帯域幅単位をまとめたものです。表 4 は、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。サポートされているすべての Citrix ADC インスタンスの場合:

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
MPX 8005Z	15	5	-	-	1Gbps
MPX 8900Z	33	5	-	-	1Gbps
MPX-14000Z シリーズ	100	20	-	-	1Gbps
MPX-15000Z シリーズ	100	20	-	-	1Gbps
MPX-25000Z-40G	200	100	-	-	1Gbps
MPX-24000Z シリーズ	150	100	40	80	1Gbps
SDX 8015Z	15	2	1	5	1Gbps
SDX 89XX シリーズ	33	10	2	7	1Gbps
SDX-115XX シリーズ	42	7	2	20	1Gbps
SDX-14000Z シリーズ	100	10	2	25	1Gbps
SDX 15000Z-50G	100	10 (注:12.1 54.x より前のバージョンでは 20 Gbps)	2 (注:12.1 54.x より前のバージョンでは 5 インスタンス)	55	1Gbps
セックス**-1500Z**	100	10 (注:12.1 54.x より前のバージョンでは 20 Gbps)	2 (注:12.1 54.x より前のバージョンでは 5 インスタンス)	55	1Gbps
SDX-22XXX シリーズ	120	20	10	80	1Gbps
SDX-25000Z-40G	200	50	10	115	1Gbps
SDX 26000Z-100G	200	50	10	115	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
SDX 26000Z	200	50	10	115	1Gbps
SX 26000Z-50S	200	50	10	115	1Gbps
SDX 8005Z	15	2	1	2	1Gbps
SDX-24000Z シリーズ	150	50	10	80	1Gbps

> 注
>
> : 最小帯域幅とインスタンス数は、11.1 64.x、12.0 63.x、12.1 54.x 以降のリリースを実行している SDX インスタンスに適用されます。
>
> 最小購入数量は、最小システム要件とは異なります。

表 **2. CPX** インスタンスでサポートされるプール容量

	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
CPX	10	1	1	1	10Mbps

表 **3.** ハイパーバイザーとクラウドサービス上の **VPX** インスタンスでサポートされるプール容量

ハイパーバイザ/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	5Gbps	10Mbps	1	1	10Mbps

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
Azure	3Gbps	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。

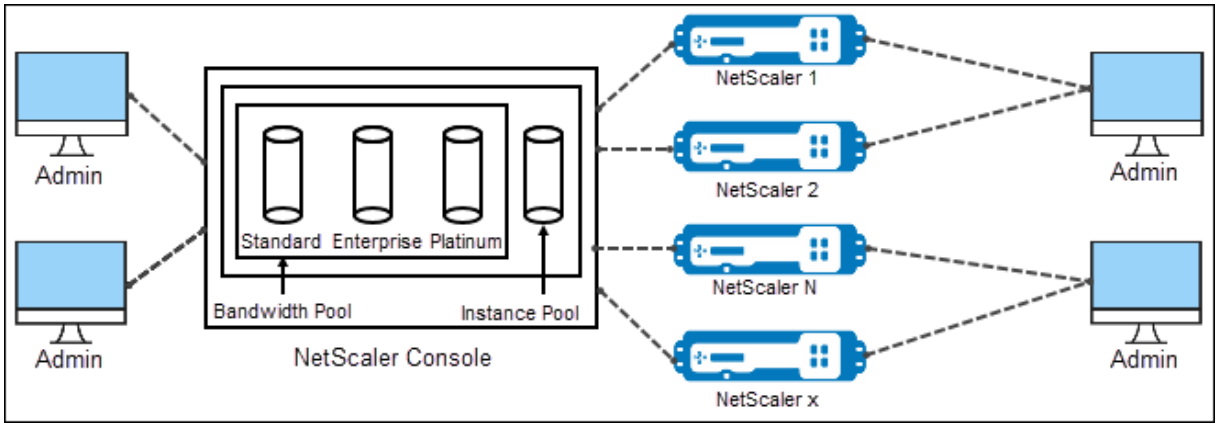
表 **4.** さまざまなフォームファクタのライセンス要件

製品ライン	ゼロキャパシティハードウェアの購入	帯域幅およびエディションのサブスクリプション	インスタンスのサブスクリプション
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

NetScaler ADC プール容量を構成する

February 6, 2024

Citrix Application Delivery Management（ADM）は、ADM に追加されたすべての Citrix ADC インスタンスのライセンスサーバーです。ライセンスサーバーには、プールキャパシティライセンスファイル（帯域幅プールまたはインスタンスプール）をアップロードできます。ライセンスプール内のライセンスは、必要に応じて Citrix ADC インスタンスに割り当てることができます。Citrix ADM からライセンスを割り当てることも、インスタンスの最小容量と最大容量に応じて Citrix ADC インスタンス（MPX-Z /SDX-Z/VPX/CPX）からライセンスをチェックアウトすることもできます。



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

NetScaler ADC ソフトウェアのバージョン	Citrix ADC MPX ゼロキャパシティハードウェア	Citrix ADC SDX ゼロキャパシティハードウェア	Citrix ADC VPX でサポートされているハイパーバイザー
11.1 ビルド 54.14 およびそれ以降 12.0 ビルド 51.24 以降	MPX-14000Z、 MPX-14000Z-40G、 MPX-14000Z-40G	SDX-14000Z, SDX-14000Z-40G, SDX-25000Z-40G	VMware ESX 6.0、Citrix Hypervisor、Linux KVM Microsoft Hyper-V、Amazon AWS、Microsoft Azure

Citrix ADM をライセンスサーバーとして構成する

Citrix ADM を Citrix ADC プールキャパシティのライセンスサーバーとして構成できます。Citrix ADC インスタンスが帯域幅またはインスタンスライセンス、あるいはその両方を取得する方法は 2 つあります。

- Citrix ADC インスタンスは、Citrix ADM へのチェックアウトリクエストを開始して、帯域幅やインスタンスライセンスを取得できます。
- ライセンスは、Citrix ADM を介して Citrix ADC インスタンスに割り当てることができます。

> 注
>
> プールされたキャパシティは、プールされたライセンスが Citrix ADM に追加された場合にのみ Citrix ADM に表示されます。

Citrix ADC プールキャパシティを使用している Citrix ADC インスタンスの動作モードは次のとおりです。

- 最適—インスタンスは適切なライセンス容量で実行されています。

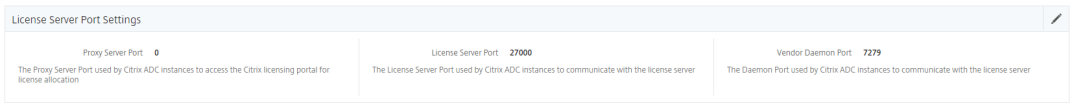
- 容量の不一致—インスタンスは、ユーザーが設定した容量よりも少ない容量で実行されています。
- **Grace**-インスタンスはグレースライセンスで実行されています。
- 猶予と不一致—インスタンスは猶予状態で実行されていますが、容量がユーザー設定よりも少なくなっています。
- 使用不可—インスタンスが管理用に Citrix ADM に登録されていないか、Citrix ADM からインスタンスへの Nitro 通信が機能していません。
- 未割り当て—ライセンスはインスタンスに割り当てられません。

NetScaler ADM にライセンスファイルをインストールするには:

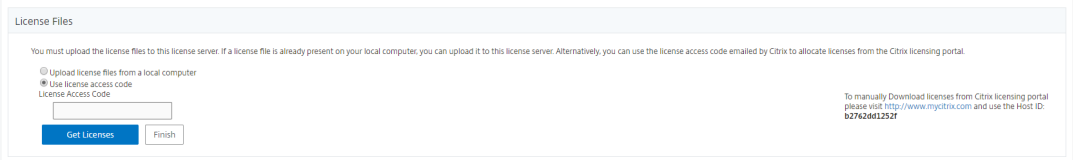
1. Web ブラウザで、**Citrix ADM** の IP アドレス（たとえば、http://192.168.100.1）を入力します。
2. [**User Name**] と [**Password**] に管理者の資格情報を入力します。
3. [ネットワーク **] > [**ライセンス] に移動します。
4. 「ライセンスファイル」セクションで、次のオプションのいずれかを選択します。

    - ローカルコンピュータからのライセンスファイルのアップロード**-**ローカルコンピュータに ライセンスファイルがすでに存在する場合は、NetScaler ADM にアップロードできます。ライセンスファイルを追加するには、[**Browse**] をクリックし、追加するライセンスファイル (.lic) を選択します。次に、[完了] をクリックします。

        > 注
        >
        > アップロードされたライセンスファイルによって Citrix ADC Pooled キャパシティにライセンスが追加されない場合は、ライセンスファイルを選択して [**Apply Licenses**] をクリック してライセンスをプールに追加できます。

    - 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（LAC）が電子メールで送信されます。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 LAC を入力し、[**Get Licenses**] をクリックします。

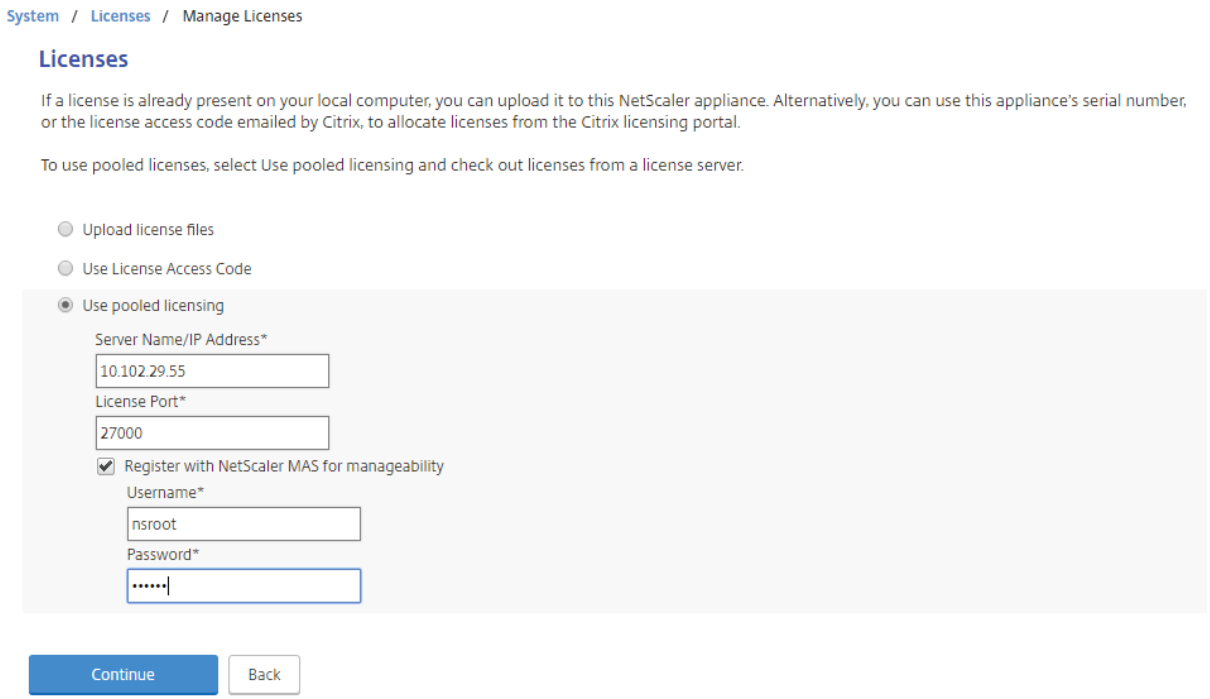
        > 注
        >
        > いつでも、ライセンス設定から Citrix ADM にライセンスを追加できます。

Citrix ADC プールキャパシティライセンスを **Citrix ADM** から割り当てるには:

> 注
>
> Citrix ADC インスタンスを Citrix ADM に登録していない場合は、Citrix ADM からライセンスをチェックアウトできますが、Citrix ADM から Citrix ADC プールキャパシティ対応インスタンスに割り当てることはできません。

プールキャパシティライセンスを ADC インスタンスに割り当てる前に、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。

> 前提
>
> 条件 Citrix ADM を使用してインスタンスのプールライセンスを管理する前に、Citrix ADC インスタンスを Citrix ADM に登録する必要があります。Citrix ADC GUI で、Citrix ADM IP を追加するときに、[システム] > [ライセンス] > [ライセンスの管理] に移動し、[**Citrix ADM** に登録して管理しやすくする] チェックボックスを選択します。

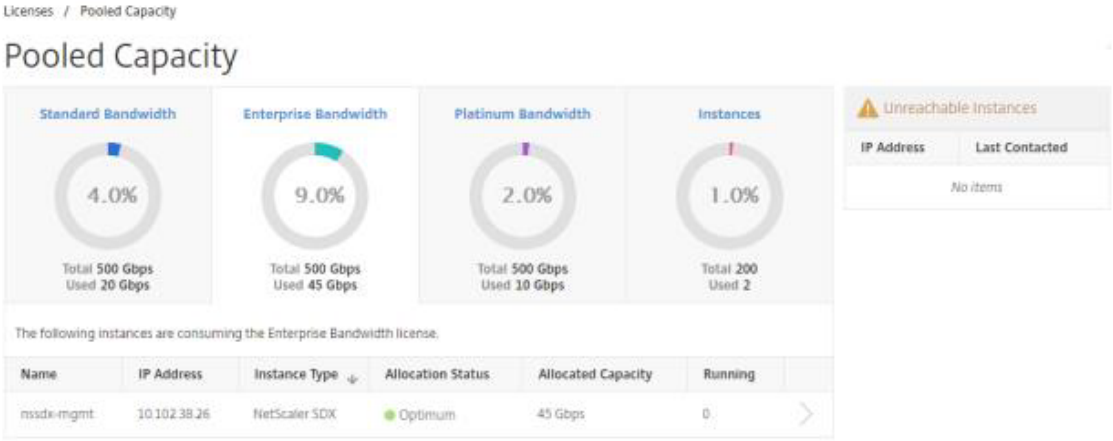


> 注
>
> 上の画面の［ユーザー名］フィールドと［パスワード］フィールドに、Citrix ADM 資格情報を入力します。

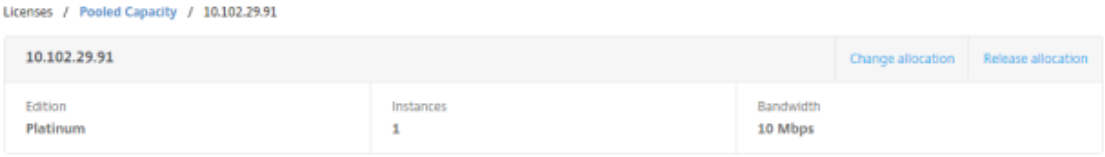
ライセンスサーバーへのインスタンスの登録後、以下の手順でライセンスを割り当てます。

1. Web ブラウザで、**Citrix 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. [構成] タブで、[ネットワーク **] > [**ライセンス**] >** [プールキャパシティ] に移動します。

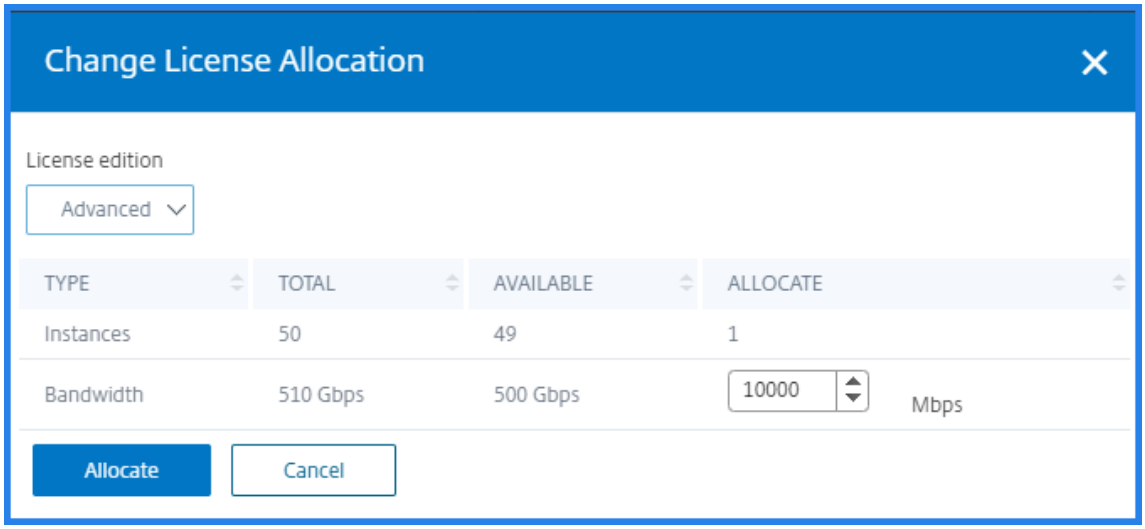
4. 管理するライセンスプールをクリックします。
5. **>** ボタンをクリックして、使用可能なインスタンス のリストから Citrix ADC インスタンスを選択します。



6. ライセンスの割り当てを変更またはリリースする場合は、[割り当ての変更] または **[割り当て ** の解除] をクリックします。



7. [割り当てを変更] をクリックすると、ライセンスサーバーで使用可能なライセンスを含むポップアップウィンドウが表示されます。



8. Citrix ADC インスタンスへの帯域幅またはインスタンスの割り当ては、「割り当て」ドロップダウンオプションを設定することで選択できます。選択後、[割り当て] をクリックします。
9. 「ライセンス割り当ての変更」ウィンドウのドロップダウンオプションから、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。

MPX-Z での **Citrix ADC** プールキャパシティの構成

MPX-Z は、Citrix ADC プールキャパシティ対応の Citrix ADC MPX アプライアンスです。MPX-Z では、Platinum、Enterprise m、Standard の各エディションのライセンスの帯域幅プールがサポートされます。

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、ローカルコンピューターからライセンスファイルをアップロードするか、インスタンスのハードウェアシリアル番号を使用するか、Citrix ADC インスタンスの GUI の [システム] > [ライセンス] セクションからライセンスアクセスコードを使用してインストールできます。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化され、チェックアウト済みのライセンスはすべてライセンスサーバーにチェックインされます。

MPX-Z インスタンスの帯域幅は、再起動することなく動的に変更できます。再起動が必要になるのは、ライセンスエディションを変更する場合のみです。

> 注
>
> インスタンスを再起動すると、構成済みのキャパシティに必要なプールされているライセンスをインスタンスが自動でチェックアウトします。

Citrix ADC VPX インスタンスでの **Citrix ADC** プールキャパシティの構成

プールキャパシティ対応の Citrix ADC VPX インスタンスは、帯域幅プール（プラチナ/エンタープライズ/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。Citrix ADC GUI を使用して、ライセンスサーバーからライセンスをチェックアウトできます。

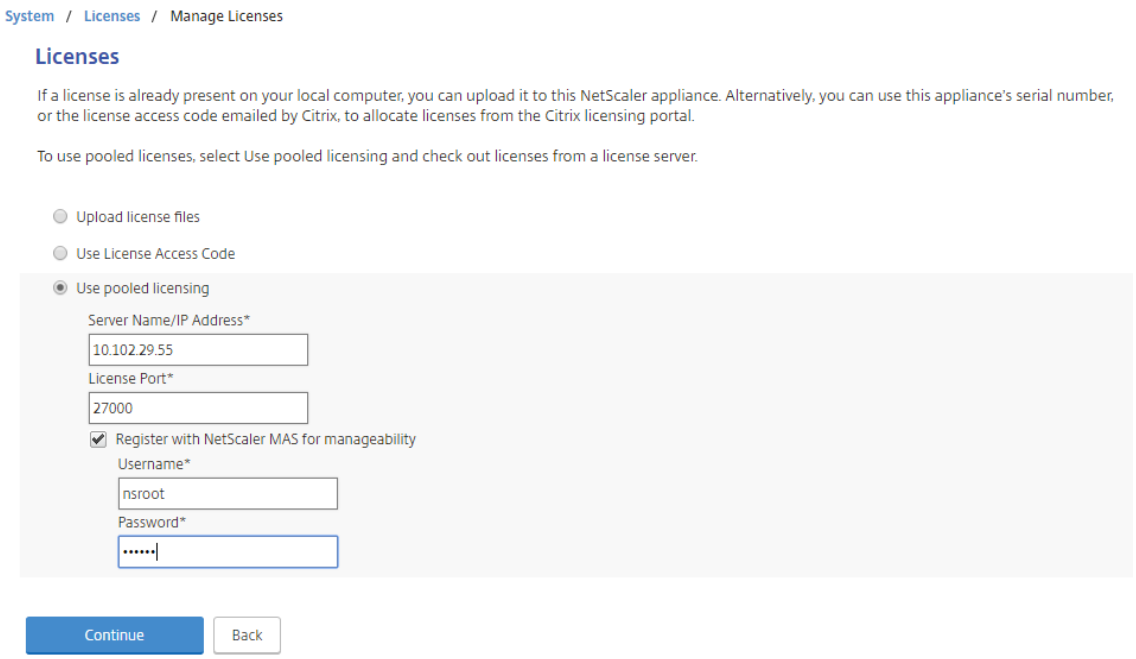
VPX インスタンスの帯域幅は、再起動することなく動的に変更できます。再起動が必要になるのは、ライセンスエディションを変更する場合のみです。

> 注
>
> インスタンスを再起動すると、構成済みのキャパシティに必要なプールされているライセンスをインスタンスが自動でチェックアウトします。

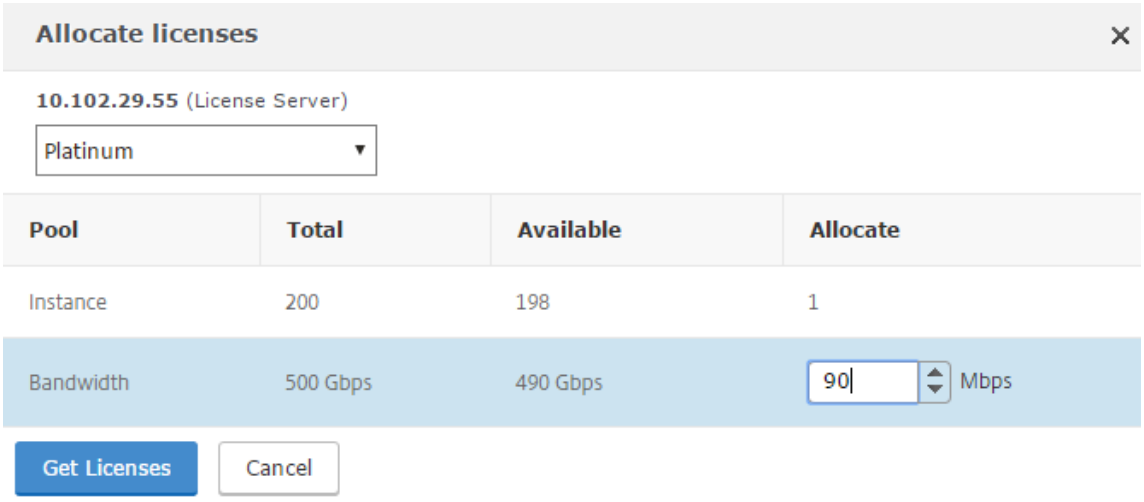
Citrix ADC MPX-Z または **Citrix ADC VPX** インスタンスへのプールライセンスの割り当て

ライセンスを割り当てるには:

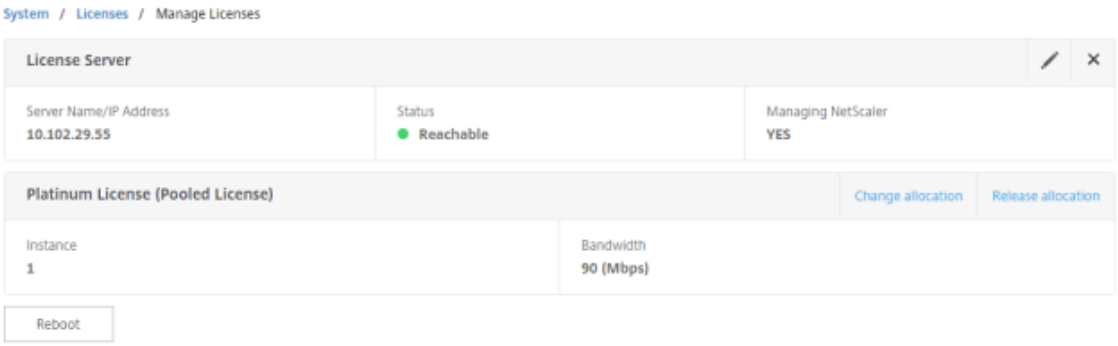
1. Web ブラウザで、NetScaler ADC インスタンスの IP アドレス（例: http://192.168.100.1）を入力します。
2. ［**User Name**］と ［**Password**］の各フィールドに管理者の資格情報を入力します。
3. [構成] タブで、[システム**] > [**ライセンス**] > [**ライセンスの管理**]** に移動し、**[**** 新しいライセンスを追加] をクリックして [プールライセンスを使用 **] を選択します。



4. **[**サーバ ー名**/IP** アドレス**]** フィールドにライセンスサーバーの詳細を入力します。
5. Citrix ADM を使用してインスタンスのプールライセンスを管理する場合は、[管理しやすくするために **Citrix ADM** に登録する] チェックボックスを選択し、ADM 認証情報を入力します。
6. ライセンスエディションと必要な帯域幅を選択し、[**Get Licenses**] をクリックします。



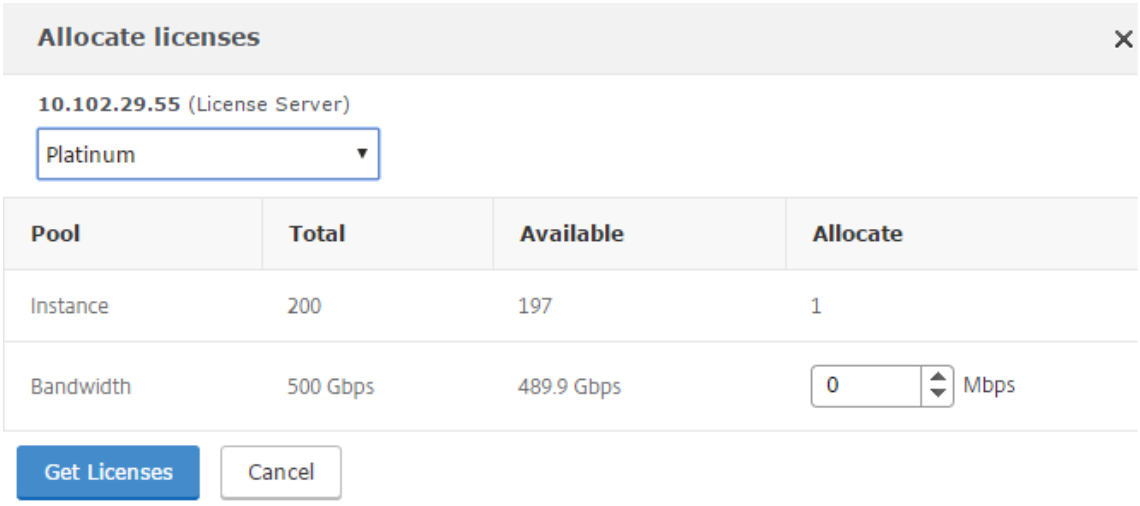
7. [割り当ての変更] または [割り当ての解除] を選択すると、** ライセンスの割り当てを変更または解除できます **。



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。



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

    帯域幅の割当量は、最小帯域幅単位の倍数にする必要があります。

SDX-Z での Citrix ADC プールキャパシティの構成

SDX-Z インスタンスは、Citrix ADC SDX のプールキャパシティ対応インスタンスです。SDX-Z では、Platinum、Enterprise m、Standard の各エディションの帯域幅プール、およびインスタンスプールがサポートされます。

SDX-Z プラットフォームライセンスを適用すると、Management Service は、ライセンスをライセンスサーバーからチェック
アウトしたり、ライセンスサーバーに戻したり、SDX-Z プラットフォーム上で実行されている Citrix ADC インスタンスに帯域幅容量を割り当てたりするためのオプションを提供します。

> 注
>
> SDX-Z 上で実行されている NetScaler ADC VPX インスタンスは、ライセンスサーバーから直接ライセンスをチェックアウトしたり、ライセンスサーバーへチェックインしたりすることはできません。この操作は、SDX の管理サービスで行います。

SDX-Z プラットフォームライセンスは、ローカルコンピューターでからライセンスファイルをアップロードするか、インスタンスの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することでインストールできます。

SDX-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化され、すべて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。

> 注
>
> インスタンスを再起動すると、構成済みのキャパシティに必要なプールされているライセンスをインスタンスがチェックアウトします。

Citrix ADC SDX のプール容量

インスタンスプール:

SDX アプライアンスでは、その SDX アプライアンスのインスタンスプールで利用可能な分と同じ数のインスタンスをプロビジョニングできます。

帯域幅プール:

NetScaler ADC インスタンスの Provisioning 中に、帯域幅がインスタンスに割り当てられます。仮想 Citrix ADC インスタンスをプロビジョニングするためのエディションと必要な帯域幅を選択できます。管理サービスでは、指定したエディションで必要な分の帯域幅がインスタンスにある場合のみプロビジョニングが許可されます。帯域幅が不足している場合は通知されます。

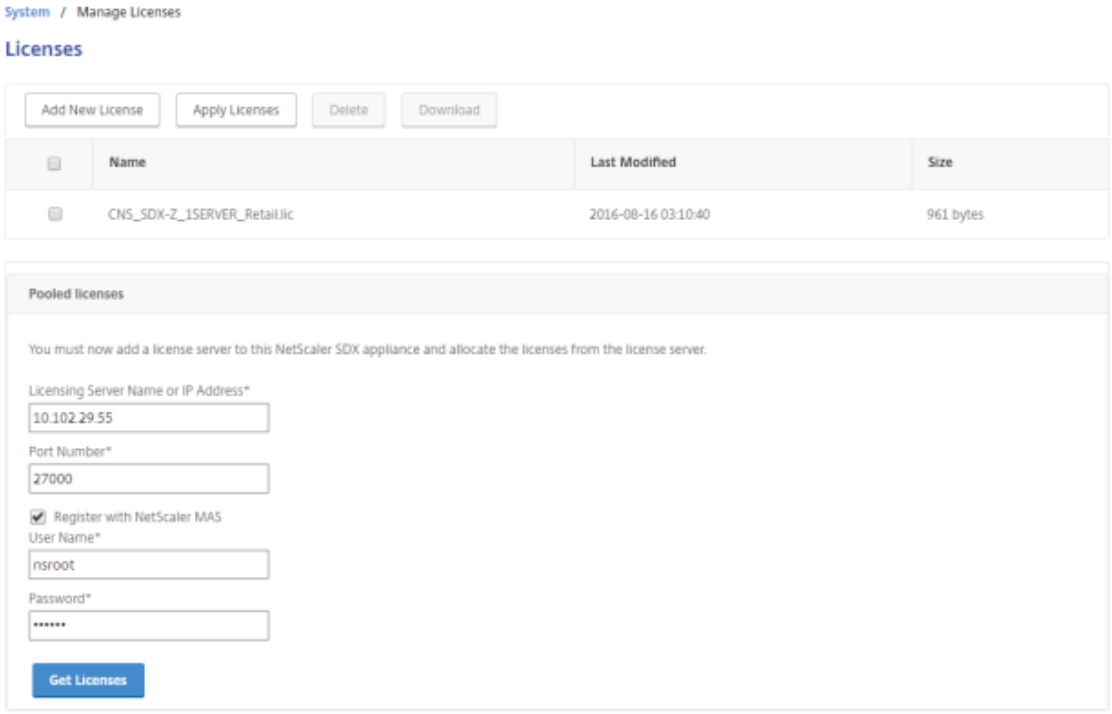
> 注
>
> 帯域幅を変更する場合インスタンスを再起動する必要はありません。

Citrix ADC SDX-Z インスタンスへのプールライセンスの割り当て

ライセンスを割り当てるには:

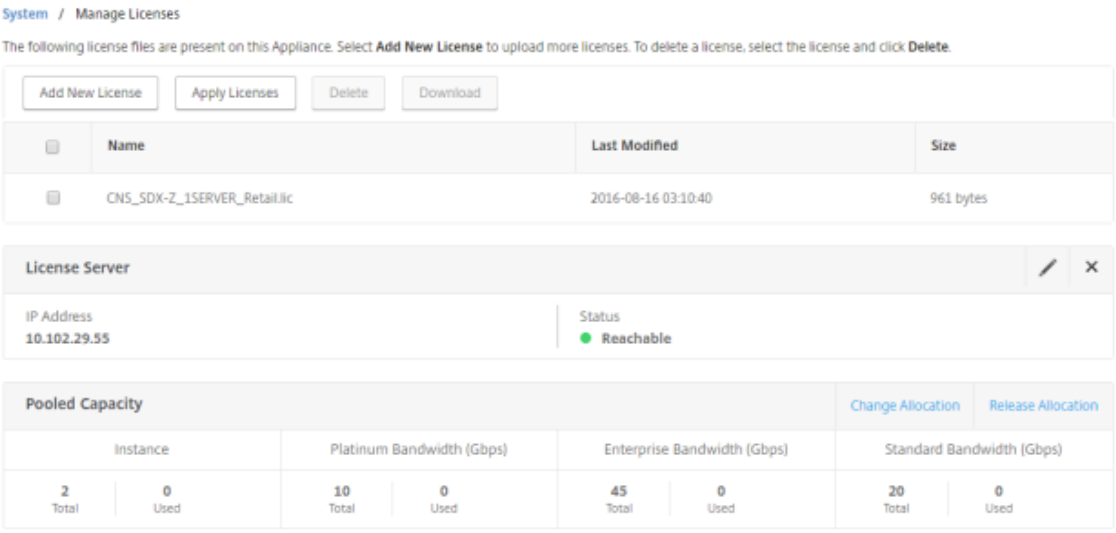
1. ウェブブラウザで、Citrix ADC SDX-Z インスタンスの IP アドレス（たとえば、http://192.168.100.1）を入力します。

2. ［**User Name**］と ［**Password**］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**]** に移動し、[プールキャパシティ] に移動します。

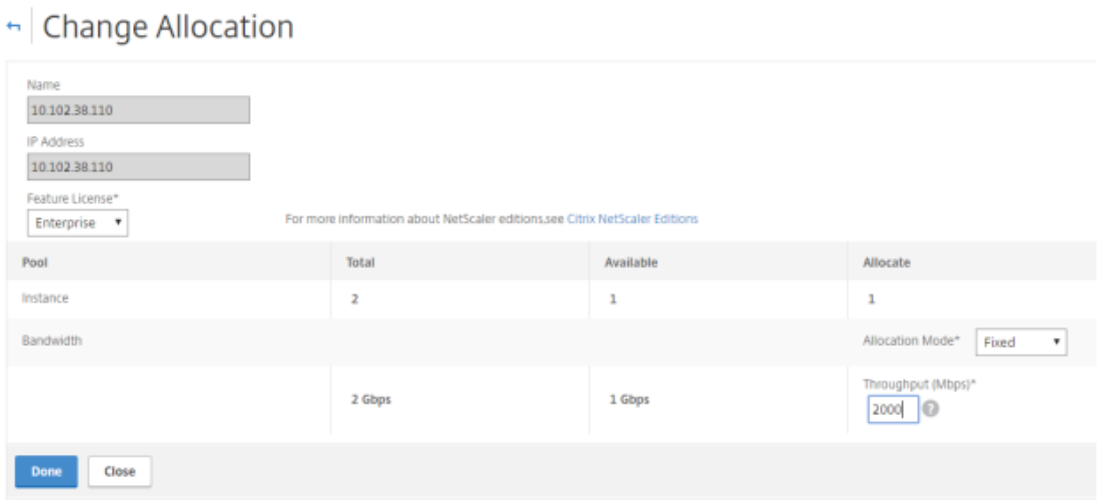


4. **[**サーバ ー名**/IP** アドレス**]** フィールドにライセンスサーバーの詳細を入力します。
5. NetScaler ADM を使用してインスタンスのプールライセンスを管理する場合は、NetScaler ADM に登録する］チェックボックスをオンにして、ADM 認証情報を入力します。
6. [割り当ての変更] または [割り当ての解除] を選択すると、**** ライセンスの割り当てを変更または解除できます ****。

> 注
>
> チェックアウトされたライセンスは、ADM によって別のプールに保存されます。



7. SDX-Z インスタンス内の特定の VPX インスタンスのライセンス割り当てを変更するには、[インスタンス] セクションからインスタンスを選択し、[割り当ての変更] をクリックします。新しいウィンドウに、使用可能なライセンスが表示されます。



8. **Feature License** ドロップダウンリストからインスタンスの帯域幅エディションを変更し、必要な帯域幅を [スループット **(mbps)**] フィールドで変更できます。完了したら ［**Done**］をクリックします。

> 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。

Citrix ADC CPX インスタンスでの **Citrix ADC** プールキャパシティの構成

Citrix ADC CPX インスタンスをプロビジョニングするときに、Citrix ADC プールキャパシティを使用するように Citrix ADC CPX インスタンスを構成できます。***docker*** run コマンドでは、Citrix ADC ライセンスサーバーの詳細

を指定する必要があります。Citrix ADC CPX インスタンスは、インスタンスプールからライセンスをチェックアウトします。

> 注
>
> デフォルトでは、Citrix ADC CPX インスタンスはインスタンスプールからインスタンスライセンスをチェックアウトし、スループットは自動的に 1000 Mbps に設定されます。インスタンスに割り当てられるこの 1000Mbps の帯域幅は変更できます。

NetScaler ADC CPX は、Docker アプリストアからダウンロードできます。Docker ホストで、NetScaler ADC CPX をダウンロードするには、次のコマンドを実行します。

```
docker pull store/citrix/netscalercpx: <version>

<!--NeedCopy-->
```

Citrix ADC CPX インスタンスのプロビジョニング中に **Citrix ADC** プールキャパシティを設定するには:

Citrix ADC CPX インスタンスをプロビジョニングするときに、以下のように ***docker*** run コマンドで Citrix 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 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> --name
    <container_name> --ulimit core=-1 -e EULA=yes -v <host_dir>:/cpx --
    cap-add=NET_ADMIN <REPOSITORY>:<TAG>

<!--NeedCopy-->
```

各項目の意味は次のとおりです:

- <LS_IPADDRESS> は、Citrix ライセンスサーバーの IP アドレスです。
- <LS_PORT> は Citrix 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。

Citrix ADC MPX の永久ライセンスから **Citrix ADC** プールキャパシティへのアップグレード

February 6, 2024

永続ライセンスを持つ NetScaler ADC MPX アプライアンスは、NetScaler ADC プール容量ライセンスにアップグレードできます。NetScaler ADC プール容量ライセンスにアップグレードすると、ライセンスプールから NetScaler ADC アプライアンスにライセンスをオンデマンドで割り当てることができます。高可用性モードで構成された NetScaler ADC インスタンスの NetScaler ADC プールキャパシティーライセンスを構成することもできます。Citrix ADC MPX インスタンスの Citrix ADC 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、「Citrix ADCMPX 高可用性ペアの永続ライセンスを Citrix ADC プールキャパシティにアップグレードする」を参照してください。

> 重要
>
> Citrix ADC MPX アプライアンスを Citrix ADC プール容量ライセンスにアップグレードするには、MPX-Z ライセンスをアプライアンスにアップロードする必要があります。

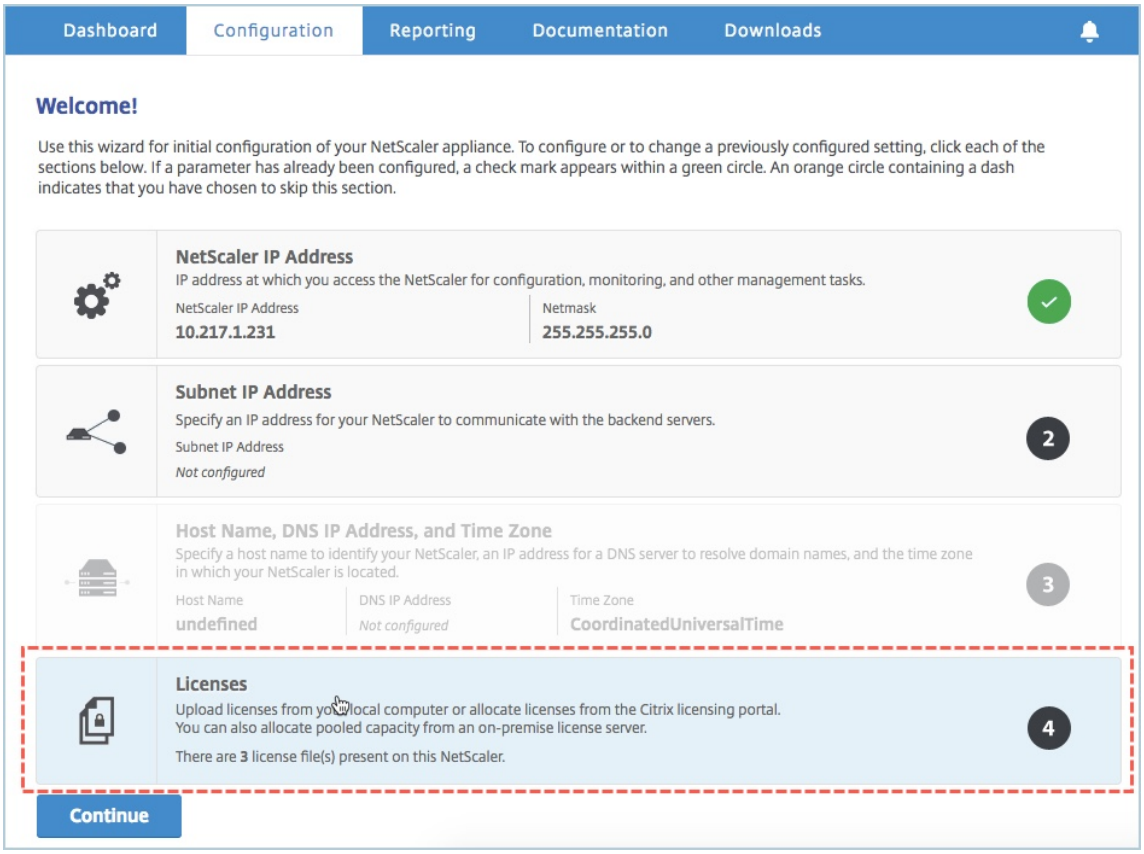
Citrix ADC プールキャパシティにアップグレードするには:

1. Web ブラウザーで、NetScaler ADC アプライアンスの IP アドレス（http://192.168.100.1など）を入力します。
2. [ユーザー名] フィールドと [パスワード] フィールドに、管理者の資格情報を入力します。
3. [ようこそ] ページで、[続行] をクリックします。
4. ゼロキャパシティライセンス (MPX-Z ライセンス) をアップロードします。[構成] タブで、[システム] > [ライセンス] に移動します。
5. 詳細ペインで、[ライセンスの管理**]** をクリックし、**[**** 新しいライセンス ** の追加] をクリックします。
6. [ライセンス] ページで、[ライセンスファイルのアップロード] を選択し、[参照] をクリックして、ローカルマシンからゼロキャパシティライセンスを選択します。
7. ライセンスがアップロードされたら、[**Reboot**] をクリックしてアプライアンスを再起動します。

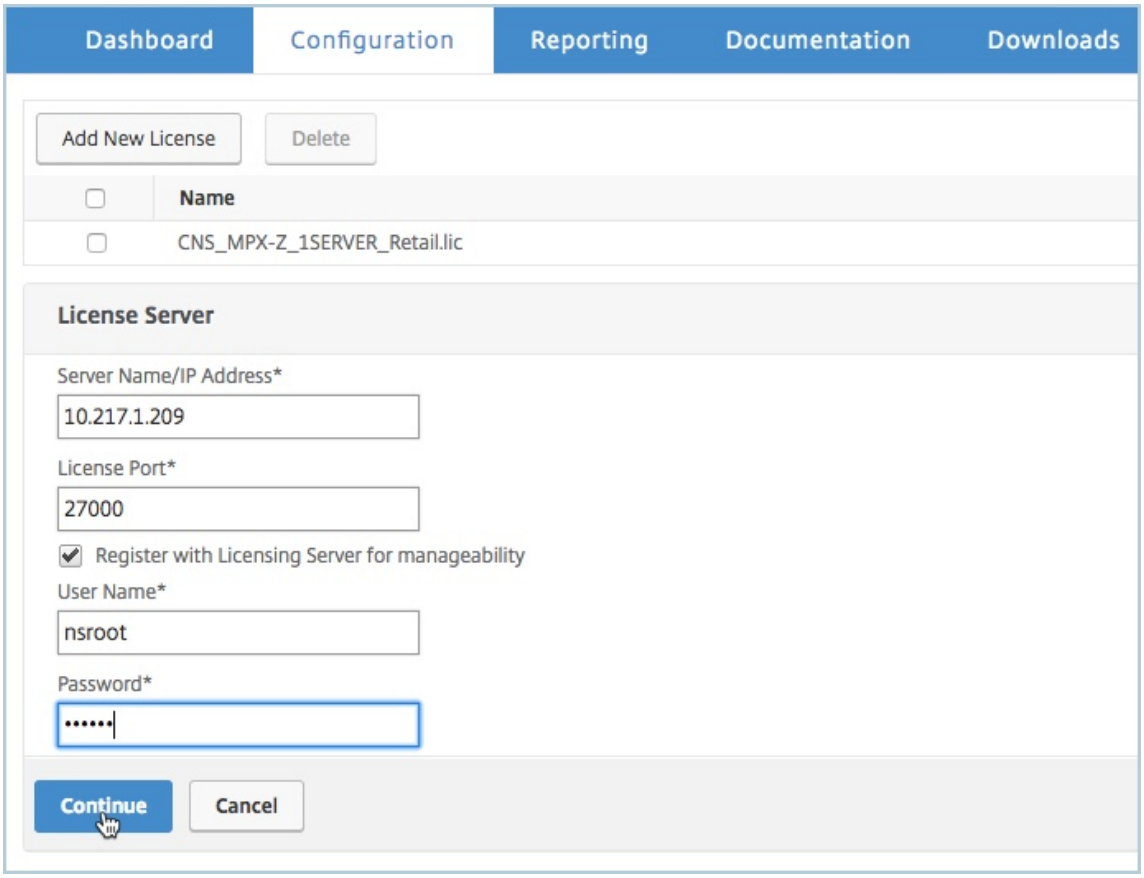
   アプライアンスを再起動する前に、設定が保存されていないことを確認してください。

   > 警告
   >
   > MPX-Z ライセンスを適用すると、アプライアンスの SSL オフロードを含む機能のライセンスが解除されます。アプライアンスは HTTPS 要求の処理を停止します。
   >
   > アップグレード前にアプライアンスで「セキュアアクセスのみ」オプションが有効になっている場合、HTTPS を使用して NetScaler ADM GUI 経由でアプライアンスに接続することはできません。

8. 「確認」ページで、「はい」をクリックします。
9. アプライアンスが再起動したら、アプライアンスにログオンします。
10. 「ようこそ」ページで、「ライセンス」セクションをクリックします。



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。

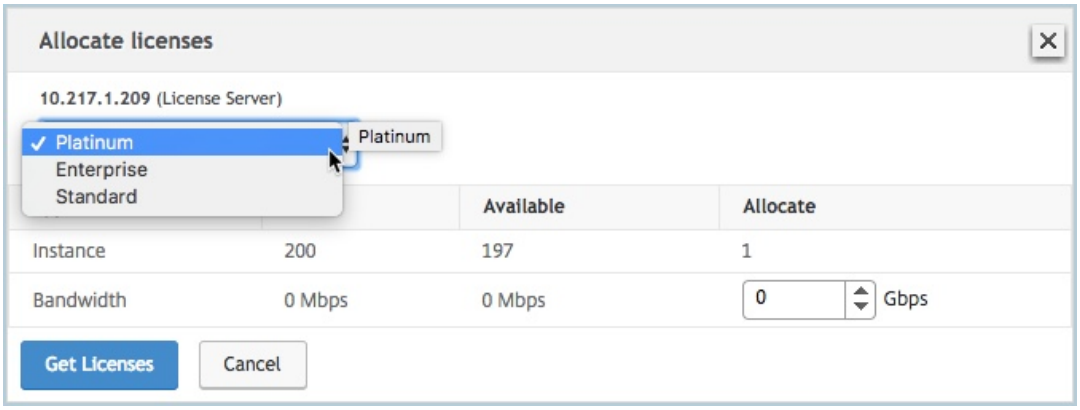
b)「ライセンスポート」フィールドに、ライセンスサーバーのポートを入力します。デフォルト値：27000。

c) Citrix ADM を使用してインスタンスのプールライセンスを管理する場合は、［管理しやすいようにライセンスサーバーに登録する］チェックボックスを選択し、ADM 認証情報を入力します。

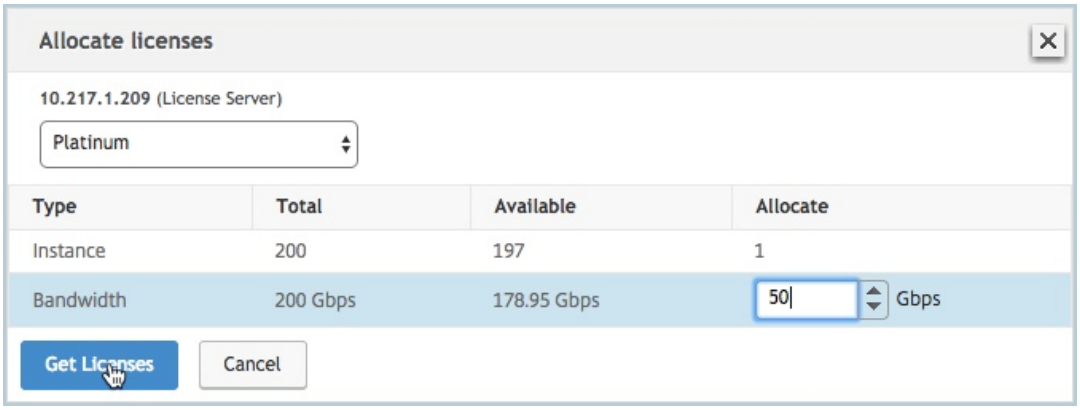
d)［続行］をクリックします。

12. [ライセンスの割り当て] ウィンドウで、次の操作を行います。

a) ドロップダウンリストからライセンスエディションを選択します。



b) ［割り当て］メニューから NetScaler ADC アプライアンスに帯域幅 を割り当て て、［ライセンスの取得］をクリックします。



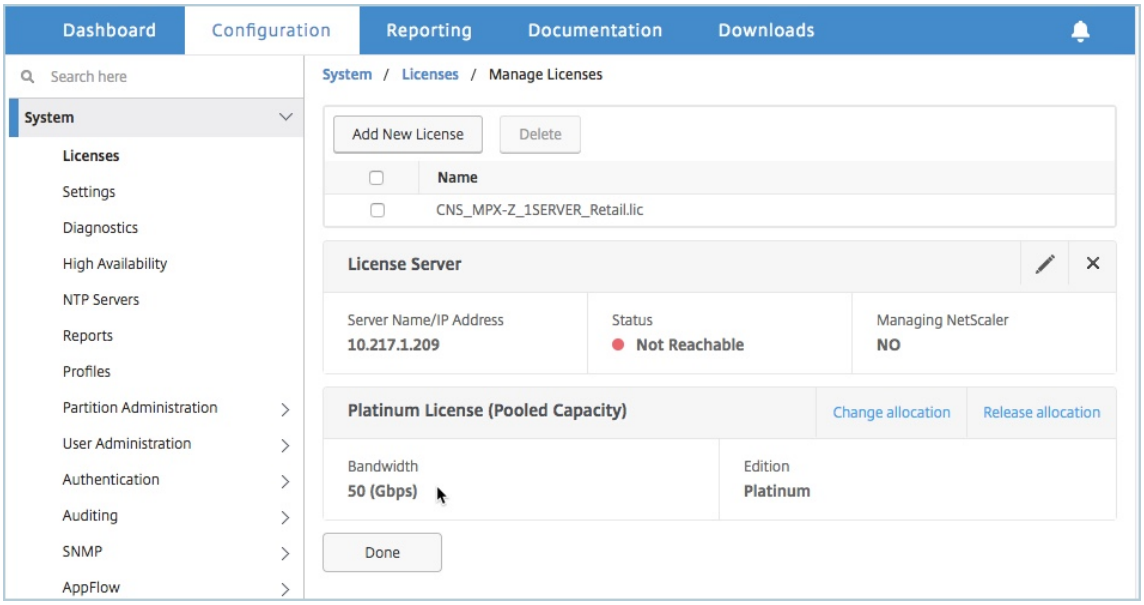
c) プロンプトが表示されたら、[**Reboot**] をクリックしてアプライアンスを再起動します。

13. NetScaler ADC MPX アプライアンスが再起動したら、NetScaler ADC MPX アプライアンスにログオンします。[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。



Citrix ADC MPX 高可用性ペアの永久ライセンスを **Citrix ADC** プールキャパシティにアップグレードする

高可用性モードで構成された NetScaler ADC MPX アプライアンスの場合、高可用性ペアのプライマリおよびセカンダリ NetScaler ADC インスタンスの両方で NetScaler ADC プール容量を構成する必要があります。同じ容量のライセンスを高可用性ペアのプライマリおよびセカンダリ NetScaler ADC インスタンスの両方に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 Gbps の容量を割り当てる必要があります。これにより、HA ペアのプライマリおよびセカンダリ NetScaler ADC インスタンスにそれぞれ 1 Gbps の容量を割り当てることができます。

> 重要
>
> NetScaler ADC MPX アプライアンスをアップグレードして NetScaler ADC プールキャパシティライセンスを使用するには、MPX-Z をアプライアンスにアップロードする必要があります。

前提条件

MPX-Z ライセンスを HA ペアのプライマリインスタンスとセカンダリインスタンスの両方にアップロードしてください。

MPX-Z ライセンスを **HA** ペアの **NetScaler ADC MPX** インスタンスにアップロードするには:

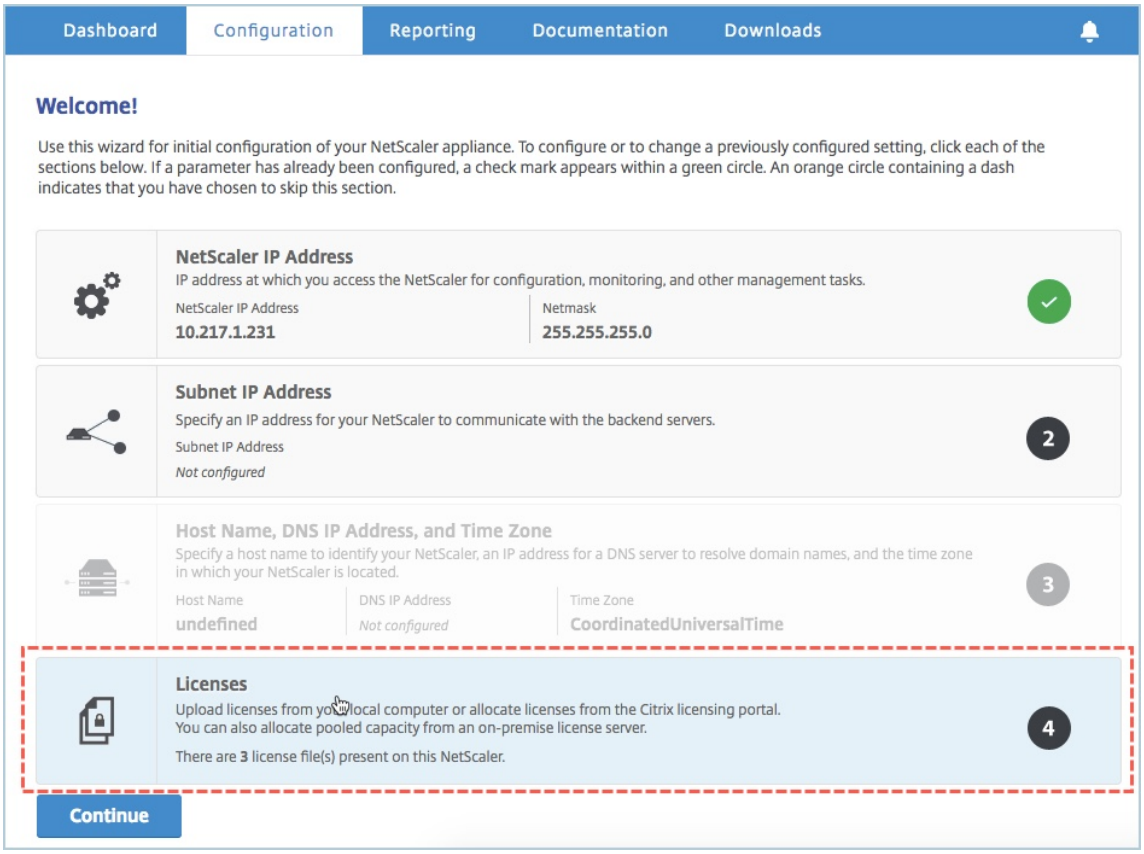
1. Web ブラウザで、アプライアンスの IP アドレス（http://192.168.100.1など）を入力します。
2. [ユーザー名] フィールドと [パスワード] フィールドに、管理者の資格情報を入力します。
3. [ようこそ] ページで、[続行] をクリックします。
4. ゼロキャパシティライセンス (MPX-Z ライセンス) をアップロードします。［**Configuration**］タブで、［**System**］**>**［**Licenses**］の順に移動します。
5. 詳細ウィンドウで、[ライセンスの管理**]** をクリックし、**[**新しいライセンスの追加] をクリックします。
6. [ライセンス] ページで、[ライセンスファイルのアップロード] を選択し、[参照] をクリックして、ローカルマシンからゼロキャパシティライセンスを選択します。

   ライセンスがアップロードされると、アプライアンスを再起動するように求められます。
7. [**Reboot**] をクリックして、アプライアンスを再起動します。
8. 「確認」ページで、「はい」をクリックします。

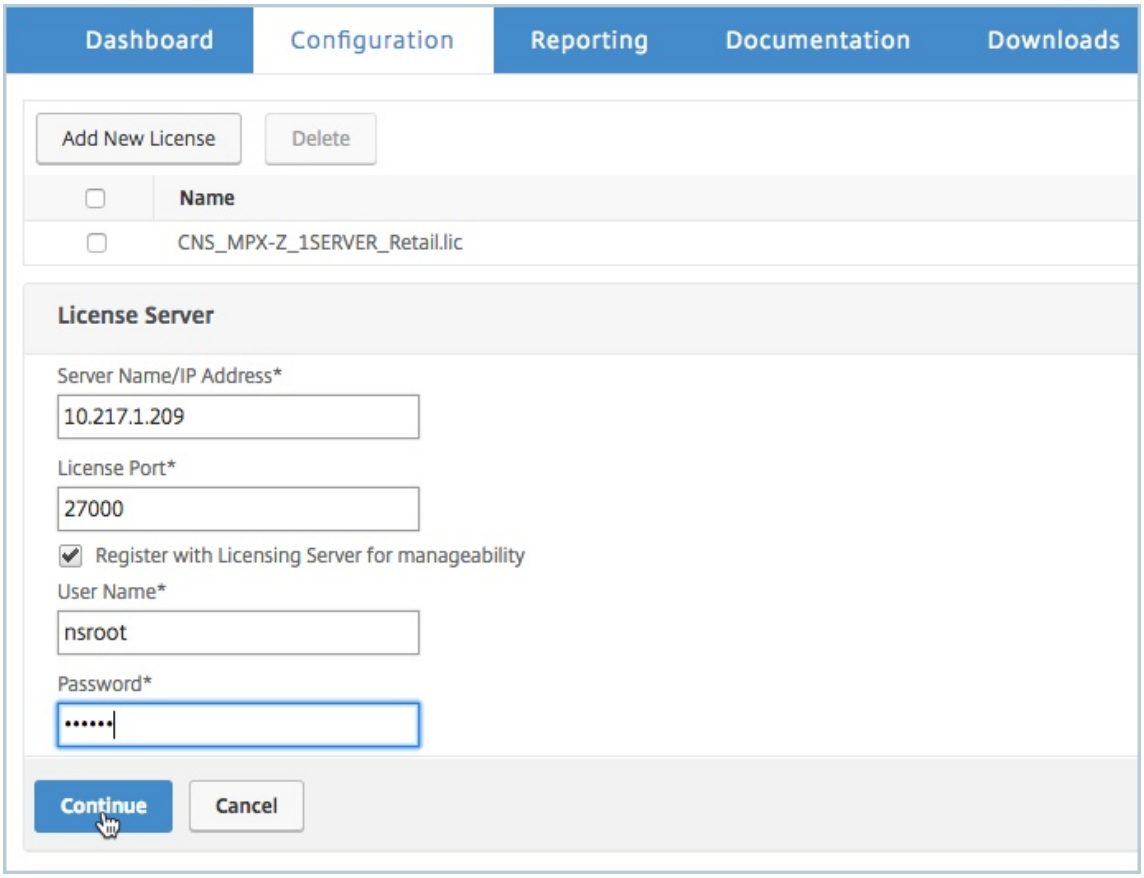
既存の高可用性セットアップを **NetScaler ADC** プール容量にアップグレードするには:

1. セカンダリ NetScaler ADC MPX インスタンスにログオンします。Web ブラウザーで、NetScaler ADC アプライアンスの IP アドレス（http://192.168.100.1など）を入力します。
2. [ユーザー名] フィールドと [パスワード] フィールドに、管理者の資格情報を入力します。

3. 「ようこそ」ページで、「ライセンス」セクションをクリックします。



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。

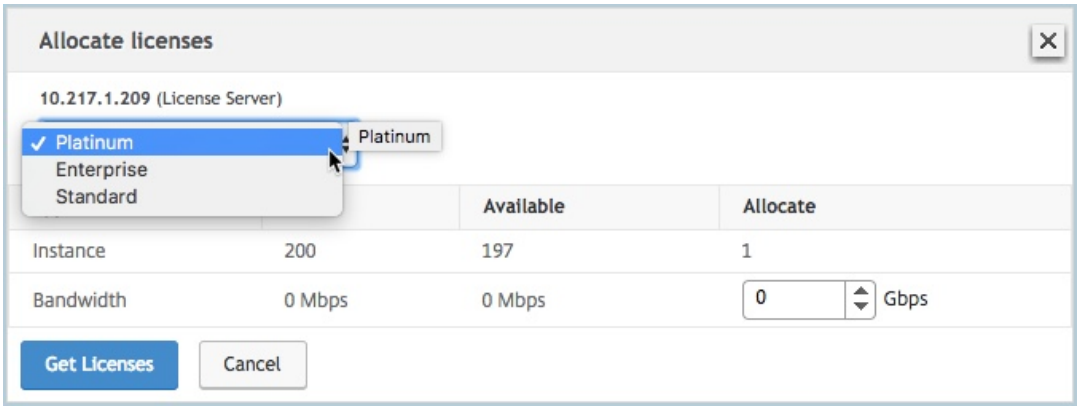
b)「ライセンスポート」フィールドに、ライセンスサーバーのポートを入力します。デフォルト値：27000。

c) Citrix ADM を使用してインスタンスのプールライセンスを管理する場合は、［管理しやすいようにライセンスサーバーに登録する］チェックボックスを選択し、ADM 認証情報を入力します。

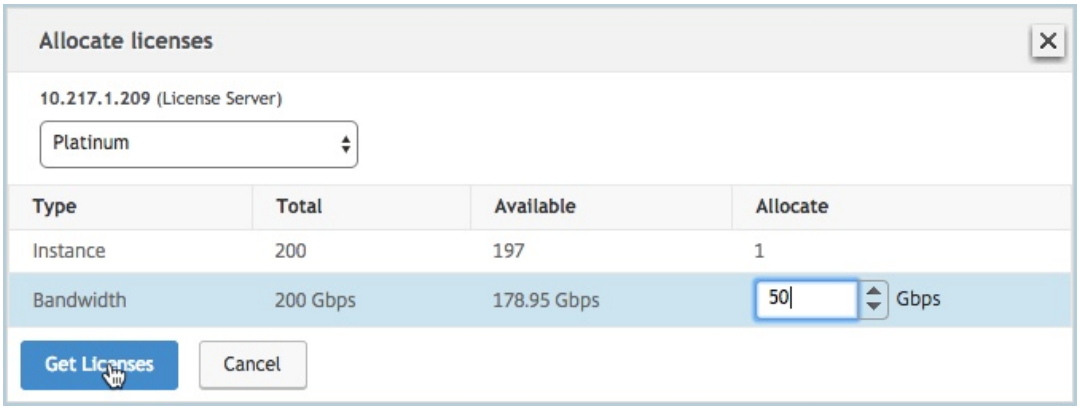
d)［続行］をクリックします。

5. [ライセンスの割り当て] ウィンドウで、次の操作を行います。

a) ドロップダウンリストからライセンスエディションを選択します。



b) ［割り当て］メニューから NetScaler ADC アプライアンスに帯域幅 を割り当て て、［ライセンスの取得］をクリックします。



c) プロンプトが表示されたら、[**Reboot**] をクリックしてアプライアンスを再起動します。

セカンダリ NetScaler ADC MPX アプライアンスが再起動すると、HA ペアのプライマリ NetScaler ADC MPX アプライアンスになります。

6. 既存のプライマリ Citrix ADC MPX アプライアンスにログオンし、アプライアンスを再起動します。以下の手順に従います:

a) Web ブラウザーで、NetScaler ADC アプライアンスの IP アドレス（http://192.168.100.1など）を入力します。

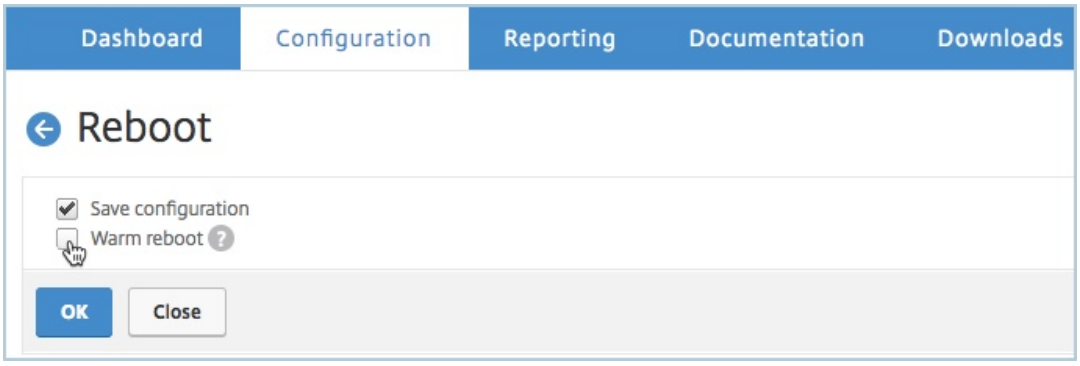
b) [ユーザー名] フィールドと [パスワード] フィールドに、管理者の資格情報を入力します。

c) [ようこそ] ページで、[続行] をクリックします。

d) [構成] タブで [システム] をクリックします。

e) [システム] ページで、[再起動] をクリックします。

f) [再起動] ページで、[ウォーム再起動] を選択し、[**OK**] をクリックします。



プライマリ NetScaler ADC MPX アプライアンスが再起動すると、HA ペアのセカンダリ NetScaler ADC MPX アプライアンスになります。必要に応じて、HA ペアの任意のインスタンスで次のコマンドを使用して、HA ペアのプライマリおよびセカンダリインスタンスを元の HA ペア設定に変更できます。


```
> force ha failover
<!--NeedCopy-->
```

NetScaler ADC SDX で永続ライセンスを NetScaler ADC プール容量にアップグレードする

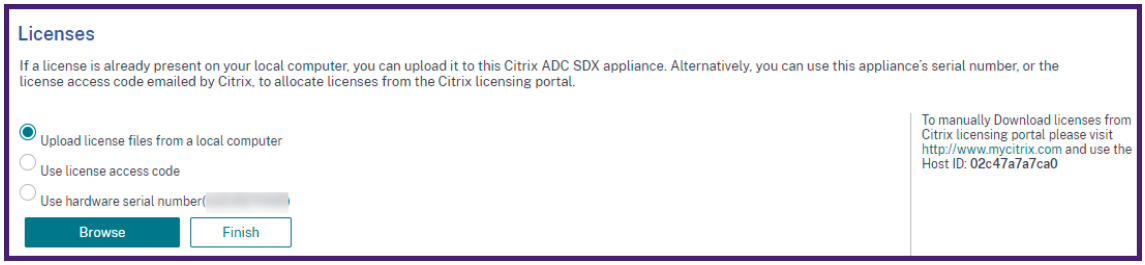
February 6, 2024

永続ライセンスを持つ NetScaler ADC SDX アプライアンスは、NetScaler ADC プール容量ライセンスにアップグレードできます。Citrix ADC プールキャパシティライセンスにアップグレードすると、ライセンスプールから Citrix ADC アプライアンスにライセンスをオンデマンドで割り当てることができます。高可用性モードで構成された NetScaler ADC インスタンスの NetScaler ADC プールキャパシティーライセンスを構成することもできます。

> 重要
>
> SDX アプライアンスを Citrix ADC プールキャパシティライセンスにアップグレードするには、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。

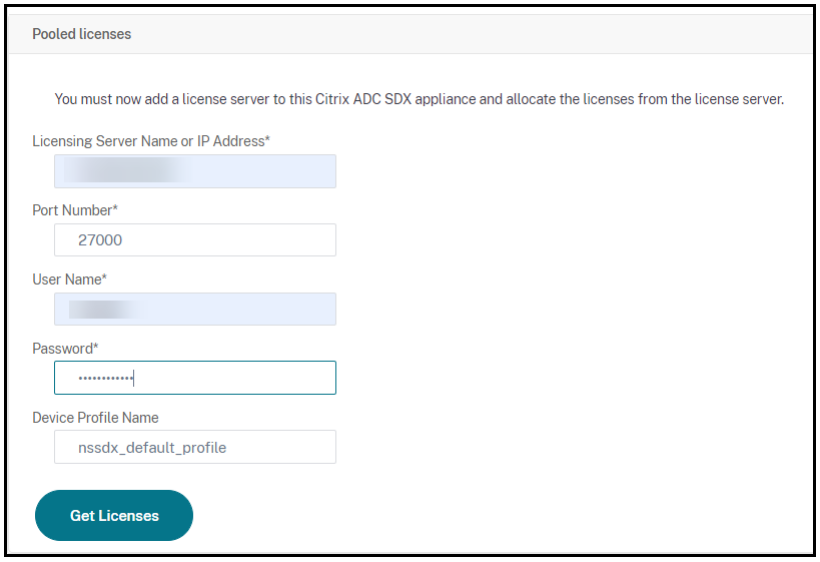
NetScaler ADC プール容量にアップグレードするには:

1. Web ブラウザで、SDX ADC アプライアンスの IP アドレス（など）を入力しますhttp://192.168.100.1。
2. [ユーザー名] フィールドと [パスワード] フィールドに、管理者の資格情報を入力します。
3. [ようこそ] ページで、[続行] をクリックします。
4. ゼロキャパシティライセンスをアップロードします。[構成] タブで、[システム] > [ライセンス] に移動します。
5. [システム] > [ライセンス] に移動します。
6. ライセンスページで、「ライセンスを管理」をクリックし、「新しいライセンスを追加」をクリックします。
7. 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キャパシティゼロライセンスを選択します。その後、[**Finish**] をクリックします。



容量ゼロのライセンスが正常に適用されると、[ライセンス] ページに [プールライセンス] セクションが表示されます。

8. ［プールライセンス］セクションで、次の操作を行います。



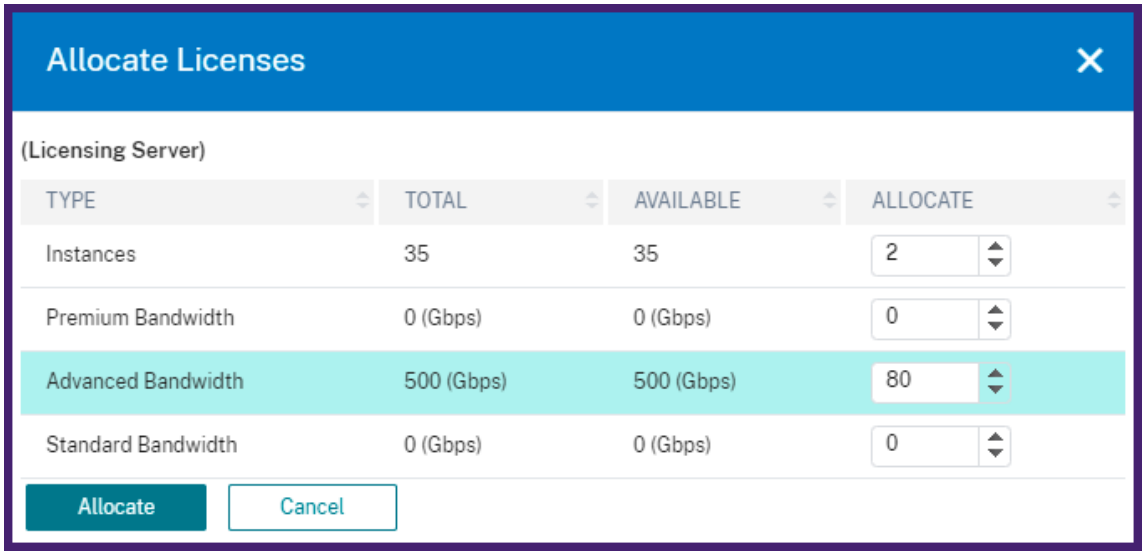
   a) ［ライセンスサーバ名**]** または **[IP** アドレス］フィールドに、ライセンスサーバの詳細を入力します。

   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。

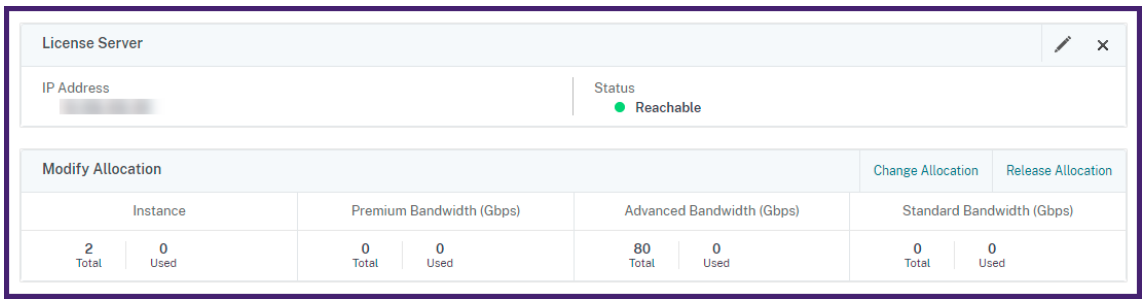
   c) NetScaler ADM を使用してインスタンスのプールライセンスを管理する場合は、NetScaler ADM に登録する］チェックボックスをオンにして、ADM 認証情報を入力します。

   d) ［**Get Licenses**］をクリックします。

9. ［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、プールから割り当てられたインスタンスおよび帯域幅の詳細を表示できます。



クラスターモードの **NetScaler ADC** インスタンス上の **NetScaler ADC** プール容量

February 6, 2024

クラスターとして構成された NetScaler ADC インスタンスで、NetScaler ADC プール容量を構成できます。Citrix ADC 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、プールキャパシティライセンスモードで個別に実行しクラスターを形成している必要があります。
- インスタンスはすべて、同じ帯域幅で実行されている必要があります。
- すべてのインスタンスは、同じ CitrixApplication Delivery Management（ADM）からプールされた容量をチェックアウトする必要があります。
- 容量と NetScaler ADM 構成がクラスター内の既存のインスタンスの構成と同じでない限り、新しいインスタンスを既存の NetScaler ADC クラスターに追加することはできません。

Citrix ADC クラスターから容量をチェックアウトすると、すべてのクラスターノードに同じ容量が割り当てられ、チェックアウト帯域幅 = 提供された帯域幅 x ノードの数になります。

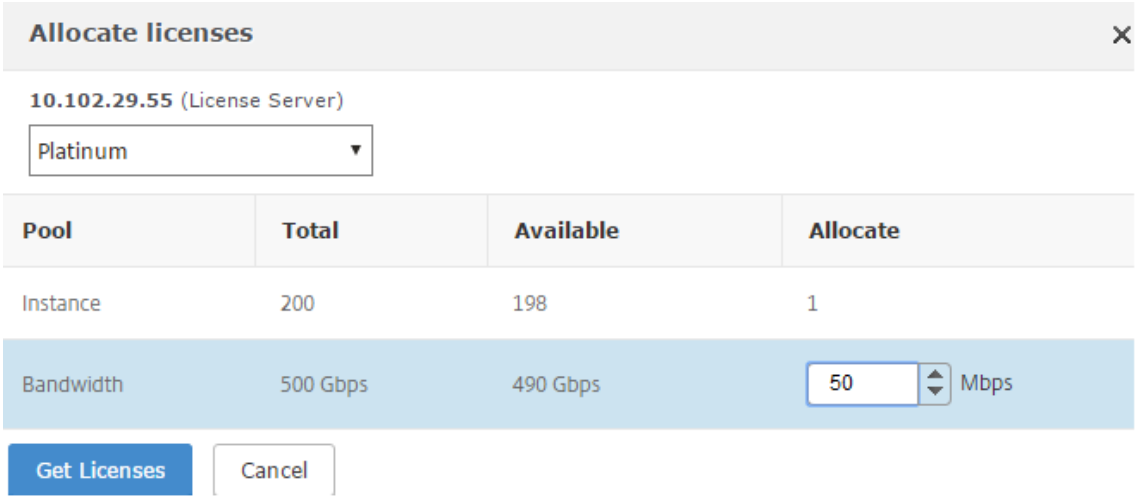
たとえば、Citrix ADC クラスターから 50 Mbps の帯域幅をチェックアウトし、クラスターに 12 個のインスタンスが含まれている場合、各インスタンスは自動的に 50 Mbps を受け取り、600 Mbps がプールからチェックアウトされます。

> 注
>
> クラスター内の 1 つ以上のインスタンスが応答しなくなった場合、クラスターは残りのインスタンスのキャパシティで動作を継続します。

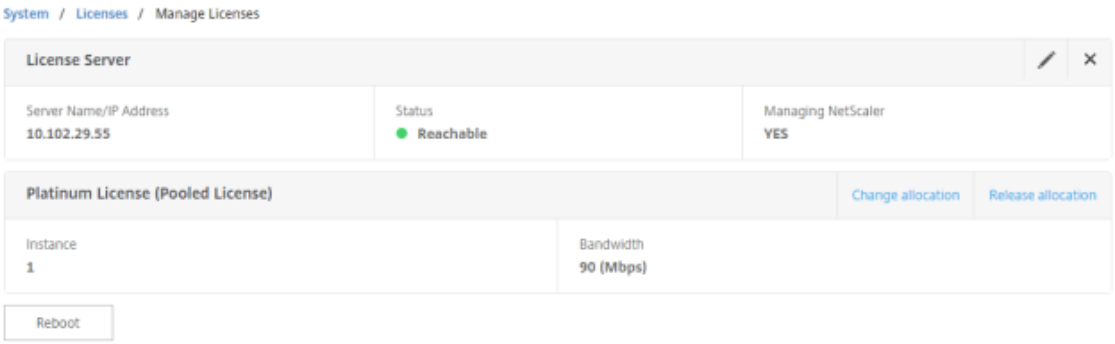
Citrix ADC プール容量をクラスターモードで **Citrix ADC** インスタンスに割り当てるには:

1. Web ブラウザで、クラスタ **IP (CLIP)** アドレスの **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. [設定] タブで、[システム**] > [**ライセンス**] > [**ライセンスの管理] に移動し、[新しいライセンスを追加**]** をクリックして、[プールライセンスを使用する] を選択します。

4. 「サーバー名/**IP** アドレス」フィールドにライセンスサーバーの名前またはアドレスを入力します。
5. Citrix ADM を使用してインスタンスのプールライセンスを管理する場合は、［管理しやすくするために **Citrix ADM** に登録する］チェックボックスを選択し、ADM 認証情報を入力します。
6. ライセンスエディションと必要な帯域幅を選択し、[**Get Lic**enses] をクリックします。

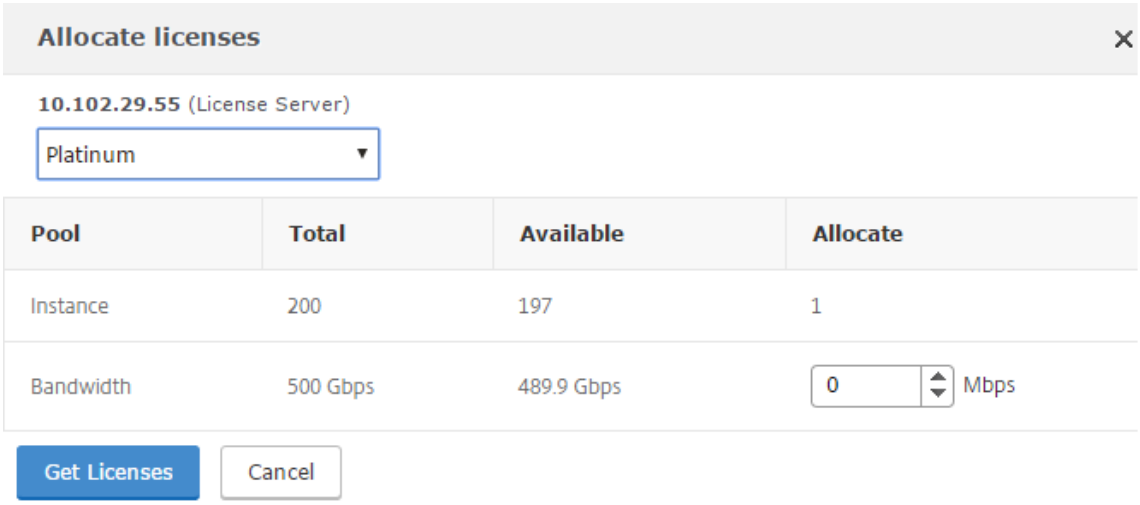


7. [割り当ての変更] または [割り当ての解除] を選択すると、**** ライセンスの割り当てを変更または解除できます ****。



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。

サーバーヘルス監視

February 6, 2024

ライセンスサーバーは、Citrix ADC プールキャパシティ対応インスタンスの状態を継続的に監視します。そのインスタンスは定期的なメッセージングによってライセンスサーバーと通信しています。連続してメッセージが受信されなければ、ライセンスサーバーは接続が切れたとレポートします。

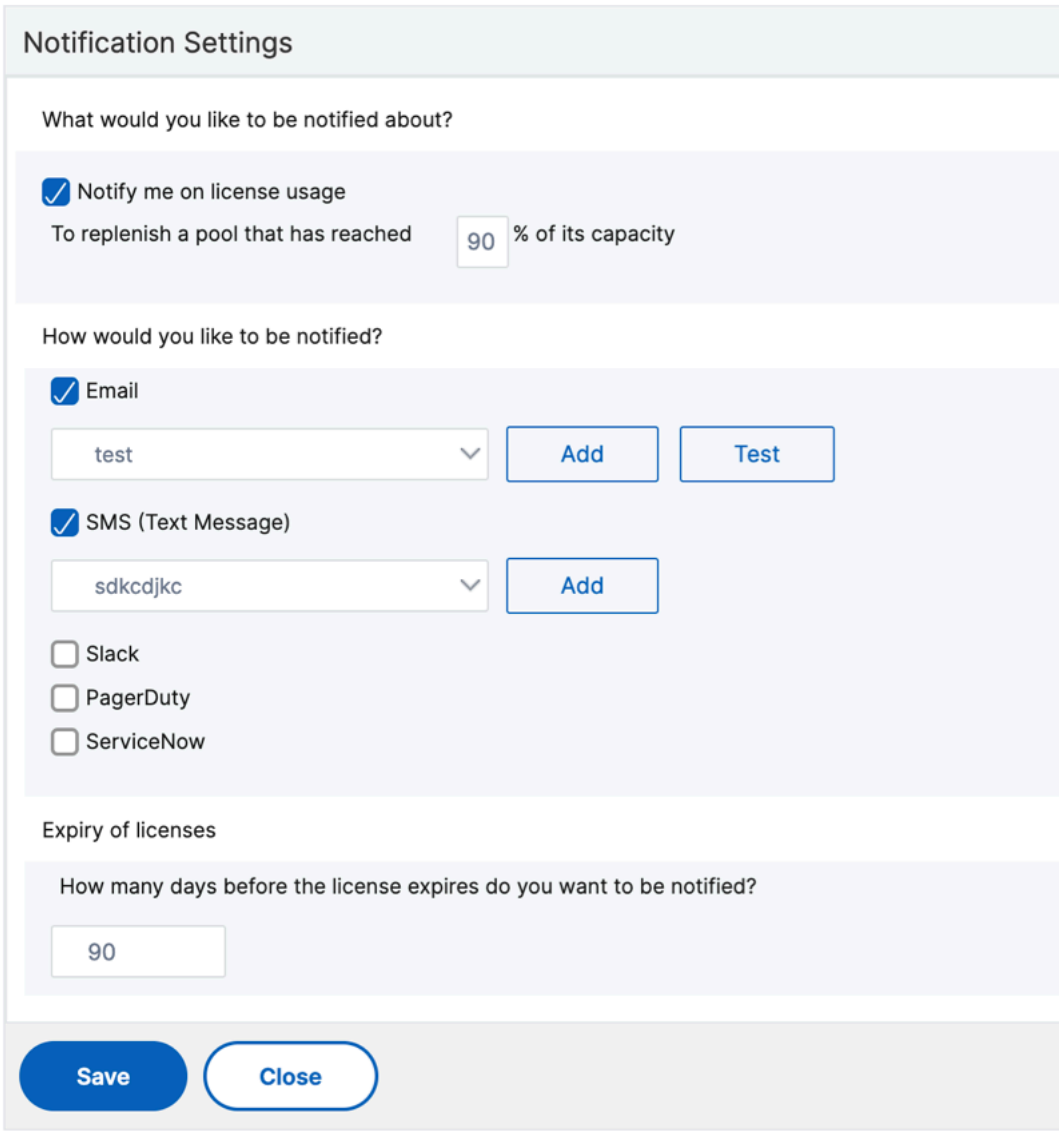
デフォルトのアラームを補足するカスタムの通知を作成することができます。

猶予期間

Citrix ADC プールキャパシティ対応インスタンスが正常な状態にあり、ライセンスサーバーが応答を停止しても、インスタンスは現在の容量で 30 日間動作し続けます。30 日後もライセンスサーバーへの接続が回復していない場合、インスタンスはキャパシティを失ってトラフィック処理を停止します。

通知とアラーム

インスタンスで実行されるすべてのアクションについて、Citrix Application Delivery Management（ADM）から通知を有効にできます。カスタム通知設定とは別に、デフォルトで構成されているアラームもあります。たとえば、容量の一定割合が枯渇したプールを補充するためのアラームを設定するには、[インフラストラクチャ] > [ライセンス] > [設定] > [通知 ** 設定 **] の順に選択し、[編集] ボタンをクリックします。



問題が発生したときに予想される動作

February 6, 2024

説明されている問題が発生した場合に、ライセンスサーバーと Citrix ADC インスタンスで予想される動作は次のとおりです。

ライセンスサーバーの応答停止

> 警告
>
> ライセンスサーバーが応答していません。Citrix ADC は、現在のキャパシティで 30 日間引き続き運用されます。30 日後にライセンスサーバーへの接続が復元されない場合、Citrix ADC は現在の容量を失い、トラフィックの処理を停止します。

ライセンスサーバーが応答しなくなった場合、NetScaler ADC インスタンスは接続が回復するまで猶予期間に入ります。

Citrix ADC プールキャパシティ対応インスタンスが応答を停止する

NetScaler ADC プールキャパシティ対応インスタンスが応答を停止し、ライセンスサーバーが正常な状態にある場合、ライセンスサーバーは 10 分後にすべての NetScaler ADC インスタンスのライセンスをチェックインします。インスタンスは再起動すると要求を送信し、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します。

ライセンスサーバーと **NetScaler ADC** プール容量が有効なインスタンスの両方が応答を停止する

ライセンスサーバーと Citrix ADC プールキャパシティ対応インスタンスの両方が再起動して接続を再確立すると、ライセンスサーバーは 10 分後にすべてのライセンスをチェックインし、Citrix ADC プールキャパシティ対応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 ADC プールキャパシティが有効なインスタンスは正常にシャットダウンする

正常なシャットダウンの際には、このシャットダウンの前に割り当てられていたライセンスをチェックインするか保持するかを選択できます。ライセンスをチェックインすることを選択した場合、Citrix ADC プールキャパシティ対応インスタンスは再起動後にライセンス解除されます。ライセンスを保持する場合、インスタンスのシャットダウン時にそれらのライセンスがライセンスサーバーにチェックインされます。インスタンスは再起動後にライセンスサーバーとの接続を再確立し、保存済みの構成での指定されているとおりにライセンスをチェックアウトします。

システムが再起動し、プールに空き容量がないためにチェックアウトが失敗した場合、Citrix ADC は Citrix Application Delivery Management（ADM）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アウトします。Citrix ADC が構成どおりにフル稼働していない場合、SNMP アラームが発生してこの状態をユーザーに通知します。帯域幅プールに利用可能なキャパシティがない場合、プールキャパシティ対応インスタンスのライセンスは解除されます。

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 ADC プールキャパシティ対応インスタンスが正常な状態にあるものの、ネットワーク接続が失われた場合、インスタンスは現在の容量で 30 日間稼働し続けます。30 日後もライセンスサーバーへの接続が回復していない場合、インスタンスはキャパシティを失ってトラフィック処理を停止し、ライセンスサーバーはライセンスすべてをチェックインします。ライセンスサーバーが NetScaler ADC インスタンスとの接続を再確立した後、インスタンスはライセンスを再度チェックアウトします。

プール容量ライセンスの有効期限チェックの構成

February 6, 2024

NetScaler ADC プールキャパシティライセンスのライセンス有効期限のしきい値を設定できるようになりました。しきい値を設定することで、CitrixApplication Delivery Management（ADM）は、ライセンスの有効期限が切れるときに電子メールまたは SMS で通知を送信します。NetScaler ADM でライセンスの有効期限が切れた場合も、SNMP トラップと通知が送信されます。

ライセンス有効期限の通知が送信されると、イベントが生成され、このイベントは NetScaler ADM で表示できます。

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. [ネットワーク] > [ライセンス] に 移動します。
2. [ライセンス設定**]** ページの [ライセンスの有効期限情報] セクションに、有効期限が切れるライセンスの詳細が表示されます。
    - 機能：有効期限が切れる予定のライセンスのタイプ。
    - **Count**: 影響を受ける仮想サーバーまたはインスタンスの数。
    - 有効期限までの日数: ライセンスの有効期限までの日数。
3. [通知設定] セクションで、[編集] アイコンをクリックし、アラートのしきい値を指定します。プールされたライセンス容量の割合を設定して、管理者に通知することができます。
4. 適切なチェックボックスを選択して、送信する通知の種類を選択します。通知の種類を次に示します。
    a) メールプロファイル: メールサーバーとプロファイルの詳細を指定します。ライセンスの有効期限が近づくと、メールがトリガーされます。
    b) **SMS** プロファイル: ショートメッセージサービス (SMS) サーバーとプロファイルの詳細を指定します。ライセンスの有効期限が近づくと、SMS メッセージがトリガーされます。

5. 次に、ライセンスの有効期限が切れるまでの日数で通知を送信するタイミングを指定します。
6. ［保存］をクリックします。

> 注
>
> プールに新しいライセンスを追加すると、NetScaler ADC インスタンスは既存のライセンスの有効期限が切れた時点で新しいライセンスを使用します。

NetScaler ADC VPX チェックインとチェックアウトのライセンス

February 6, 2024

NetScaler Application Delivery Management（ADM）からオンデマンドで NetScaler ADC VPX インスタンスに VPX ライセンスを割り当てることができます。ライセンスは、拡張性と自動化されたライセンスプロビジョニングを提供するライセンスフレームワークを備えた NetScaler ADM によって保存および管理されます。NetScaler ADC VPX インスタンスは、NetScaler ADC VPX インスタンスがプロビジョニングされたときに NetScaler ADM からライセンスをチェックアウトしたり、インスタンスが削除または破棄されたときに NetScaler ADM にライセンスをチェックインし直すことができます。

前提条件

次の前提条件が満たされていることを確認してください。

- ソフトウェアバージョン 12.0 を実行している Citrix ADC VPX イメージを使用しています。
  例：NSVPX-ESX-12.0-xx.xx_nc.zip
- バージョン 12.0 を実行している Citrix ADM をインストールしました。
  例:MAS-ESX-12.0-xx.xx.zip

> 注
>
> Citrix ADM で既存の VPX ライセンスを管理するには、ライセンスを Citrix ADM に再ホストする必要があります。

Citrix ADM へのライセンスのインストール

> 注
>
> ：ソフトウェアのエディションまたは帯域幅を変更した場合は、ライセンスをインストールする前に、Citrix ADM 仮想アプライアンスを再起動してください。

NetScaler ADM にライセンスファイルをインストールするには：

1. Web ブラウザで、Citrix ADM IP アドレス（例：http://192.168.100.1）を入力します。
2. ［User Name］と［Password］に管理者の資格情報を入力します。
3. [ネットワーク] > [ライセンス] に移動します。
4.「ライセンスファイル」セクションで、次のオプションのいずれかを選択します。

   - ローカルコンピュータからのライセンスファイルのアップロード-ローカルコンピュータに ライセンスファイルがすでに存在する場合は、NetScaler ADM にアップロードできます。
     ライセンスファイルを追加するには、[**Browse**] をクリックし、追加するライセンスファイル (.lic) を選択します。次に、[完了] をクリックします。
   - ライセンスアクセスコードを使用する -購入したライセンスのライセンスアクセスコード（LAC）が電子メールで送信されます。
     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 LAC を入力し、[**Get Licenses**] をクリックします。

   > 注
   >
   > :LAC コードを使用してライセンスをインストールする前に、インターネットに接続していることを確認してください。

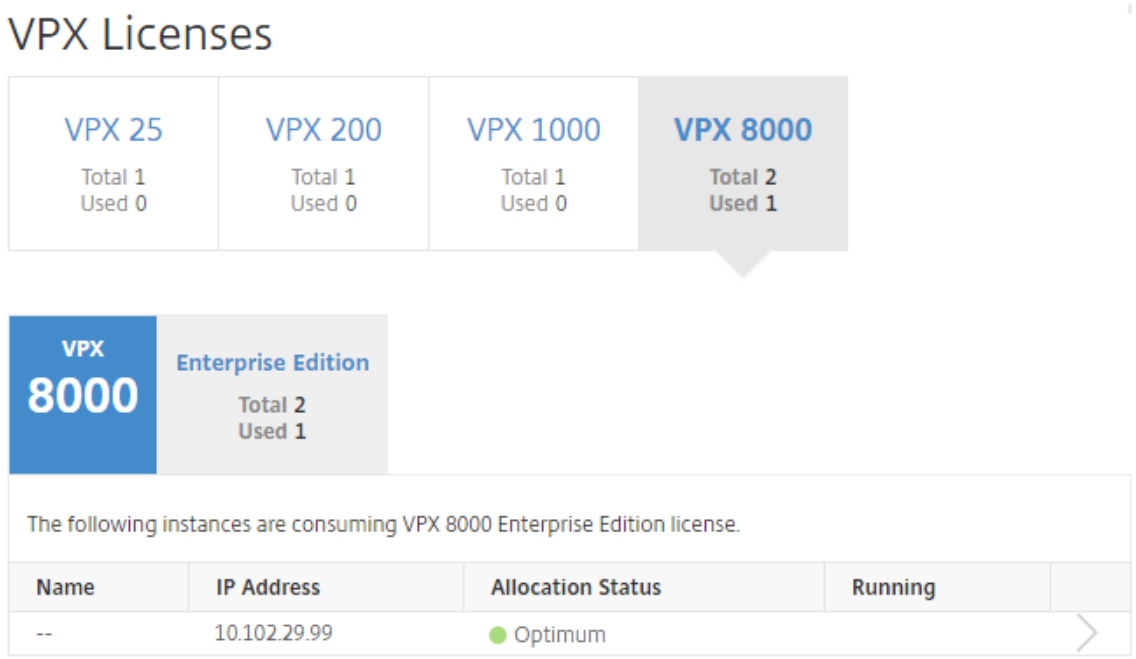
［ライセンス設定］からいつでも NetScaler ADM にライセンスを追加できます。

確認

Citrix ADM GUI で、使用可能なライセンスと割り当てられたライセンスを表示できます。

ライセンスを表示するには**:**

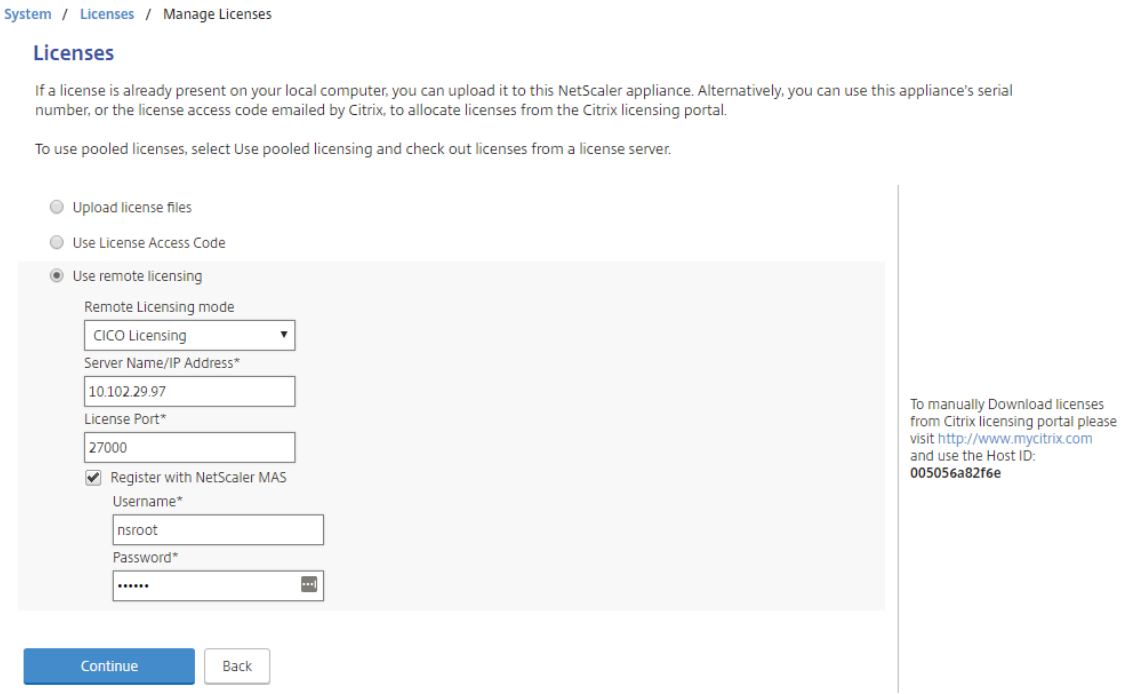
1. Web ブラウザで、Citrix ADM IP アドレス（例：http://192.168.100.1）を入力します。
2. ［**User Name**］と ［**Password**］に管理者の資格情報を入力します。
3. ［構成］タブで、［ネットワーク］>［ライセンス］>［**VPX** ライセンス］に移動します。



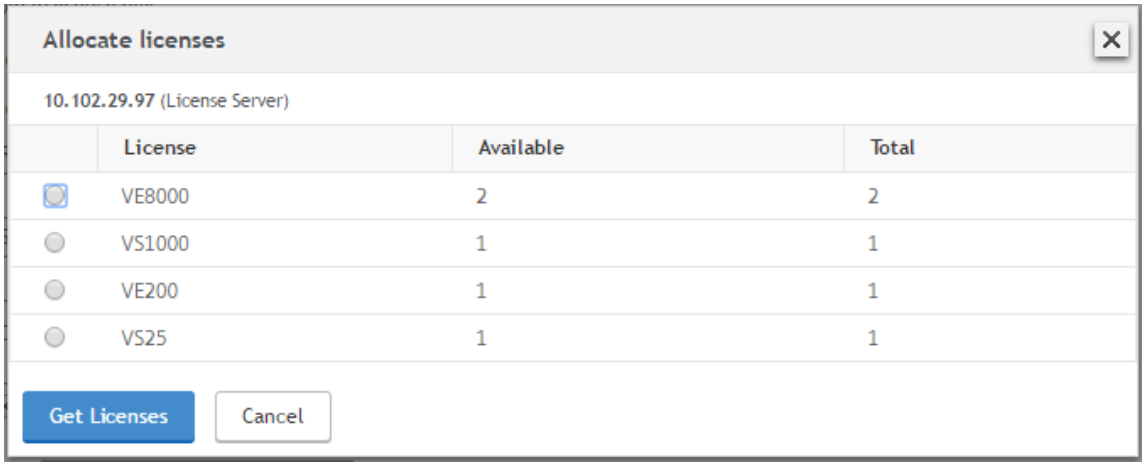
4. 割り当て済みのライセンスは、利用可能なライセンスのセクションの下の表で表示できます。

Citrix ADC GUI を使用して **Citrix ADC VPX** インスタンスに **VPX** ライセンスを割り当てる

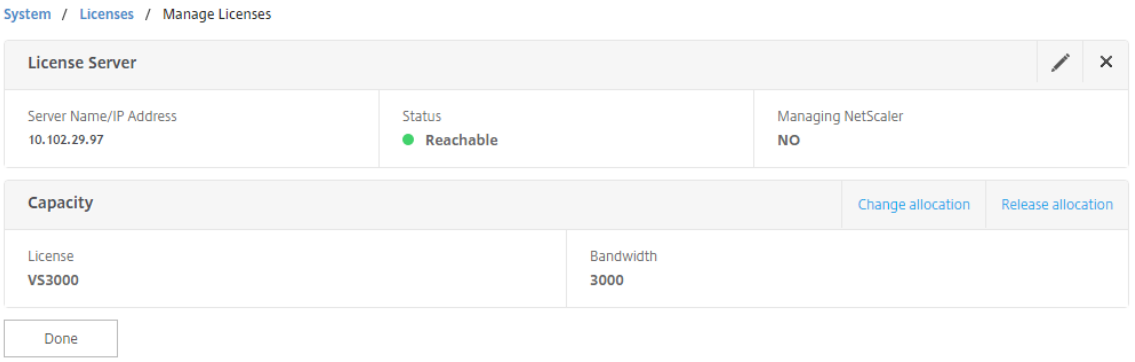
1. Web ブラウザで、NetScaler ADC インスタンスの IP アドレス（例: http://192.168.100.1）を入力します。
2. [**User Name**] と [**Password**] の各フィールドに管理者の資格情報を入力します。
3. [構成] タブで、[システム] > [ライセンス] > [ライセンスの管理**]** に移動し、**[**** 新しいライセンスを追加] をクリックして [リモートライセンスを使用 ** する] を選択します。
4. ライセンスサーバーの詳細を [サーバー名/**IP** アドレス**]** フィールドに入力します。
5. インスタンスの VPX ライセンス（Citrix ADM）を管理する場合は、[Citrix ADM に登録する] チェックボックスを選択し、**Citrix ADM** 認証情報を入力します。



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、Citrix ADC VPX 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 ADC CLI を使用した NetScaler ADC VPX インスタンスへの VPX ライセンスの割り当て

1. SSH クライアントで、Citrix ADC インスタンスの IP アドレスを入力し、管理者の資格情報を使用してログオンします。
2. ライセンスサーバーを追加するには、次のコマンドを入力します。

```
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 ADC VPX アプライアンスにライセンスを割り当てるには、次のコマンドを入力します。

```
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
```

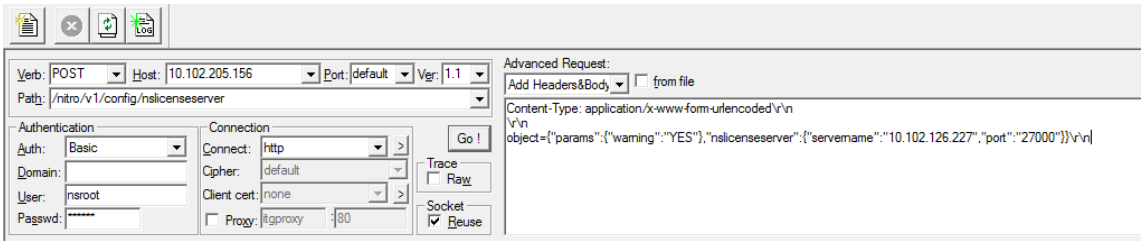
API を使用した NetScaler ADC VPX インスタンスへの VPX ライセンスの割り当て

Web ブラウザまたは API クライアントで、管理者の資格情報を使用して Citrix ADC VPX 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” :” <Citrix ADM IP>” ,  “port” :” 27000”  }
  }
 \r\n
<!--NeedCopy-->
```

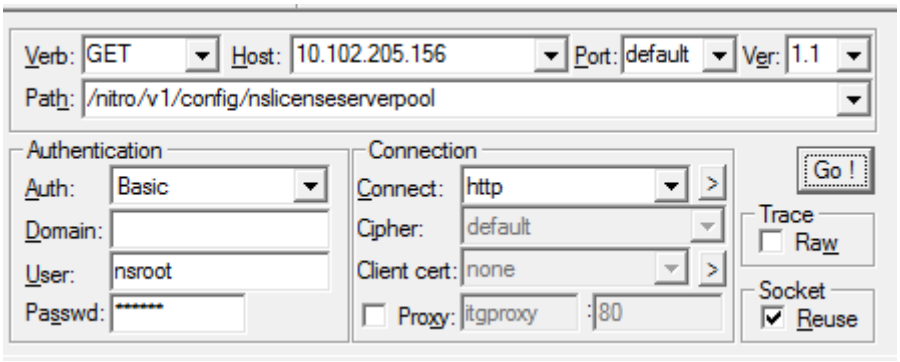



NetScaler ADM は要求に応答します。次のサンプル応答は、成功を示しています。

```
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。



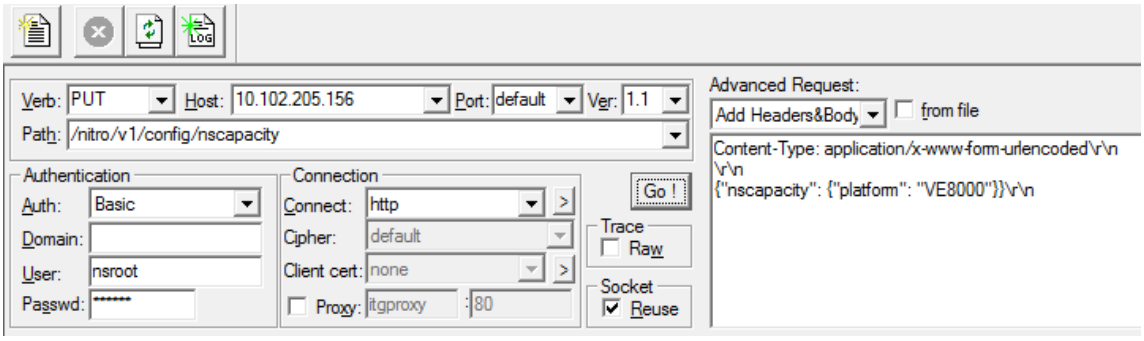
NetScaler ADM は要求に応答します。次のサンプル応答は成功と、ライセンスサーバーで利用可能なライセンスの一覧を示しています。

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.

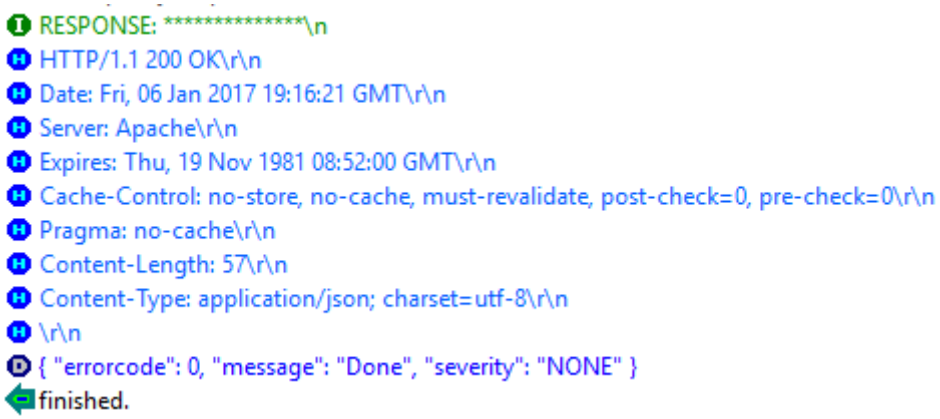
NetScaler ADC VPX アプライアンスにライセンスを割り当てるには:

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。



NetScaler ADC VPX チェックイン/チェックアウトライセンスの有効期限チェックを構成する

NetScaler ADC VPX 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た場合も、SNMP トラップと通知が送信されます。

ライセンス有効期限の通知が送信されると、イベントが生成され、このイベントは NetScaler ADM で表示できます。

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. [ネットワーク] > [ライセンス] に 移動します。
2. ライセンス設定 ページの 「ライセンス 有効期限情報 」セクションで、有効期限が切れるライセンスの詳細を確認できます。
    - 機能: 有効期限が切れる予定のライセンスのタイプ。
    - 数: 影響を受ける仮想サーバーまたはインスタンスの数。
    - 有効期限までの日数: ライセンスの有効期限までの日数。
3. [通知設定] セクションで、[編集] アイコンをクリックし、アラートのしきい値を指定します。プールされたライセンス容量の割合を設定して、管理者に通知することができます。
4. 適切なチェックボックスを選択して、送信する通知の種類を選択します。通知の種類を次に示します。
    a) メールプロファイル: メールサーバーとプロファイルの詳細を指定します。ライセンスの有効期限が近づくと、メールがトリガーされます。
    b) **SMS** プロファイル: ショートメッセージサービス (SMS) サーバーとプロファイルの詳細を指定します。ライセンスの有効期限が近づくと、SMS メッセージがトリガーされます。
5. 次に、ライセンスの有効期限が切れるまでの日数で通知を送信するタイミングを指定します。
6. ［保存］をクリックします。

NetScaler ADC 仮想 CPU ライセンス

February 6, 2024

皆さんのようなデータセンターの管理者は、ネットワーク機能を簡素化すると同時に、コスト削減と拡張性の向上を実現する新しいテクノロジーに移行しています。新しいデータセンターのアーキテクチャには、少なくとも次の機能が含まれている必要があります。

- ソフトウェア定義ネットワーク (SDN)
- ネットワーク機能仮想化 (NFV)
- ネットワーク仮想化（NV）
- マイクロサービス

このような動きにより、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、かつアジャイルであることが必要になります。ライセンスは、使用状況を完全に把握できる中央管理ツールによって管理されることも期待されています。

Citrix ADC VPX の仮想 CPU ライセンス

以前は、NetScaler ADC VPX ライセンスは、インスタンスによる帯域幅消費に基づいて割り当てられていました。NetScaler ADC VPX は、バインドされているライセンスエディションに基づいて、特定の帯域幅やその他のパフォーマンスメトリックを使用するように制限されています。使用可能な帯域幅を増やすには、より多くの帯域幅を提供するライセンスエディションにアップグレードする必要があります。特定のシナリオでは、帯域幅要件は小さくても、SSL TPS、圧縮スループットなど、他の L7 パフォーマンスの要件はより高くなる場合があります。このような場合、NetScaler ADC VPX ライセンスのアップグレードは適切ではない可能性があります。ただし、CPU 負荷の高い処理に必要なシステムリソースのロックを解除するには、帯域幅が大きいライセンスを購入する必要があります。NetScaler ADM は、仮想 CPU 要件に基づく NetScaler ADC インスタンスへのライセンスの割り当てをサポートするようになりました。

仮想 CPU 使用量ベースのライセンス機能では、特定の NetScaler ADC VPX が資格を持つ CPU の数がライセンスに指定されます。そのため、Citrix ADC VPX は、その上で実行されている仮想 CPU の数のみをライセンスサーバーからチェックアウトできます。NetScaler ADC VPX は、システムで実行されている CPU の数に応じてライセンスをチェックアウトします。NetScaler ADC VPX は、ライセンスのチェックアウト中にアイドル状態の CPU を考慮しません。

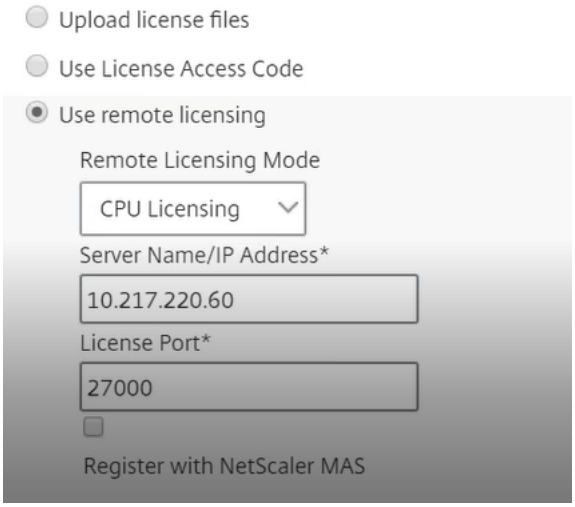
プールされたライセンス容量と CICO ライセンス機能と同様に、NetScaler ADM ライセンスサーバーは個別の仮想 CPU ライセンスを管理します。ここでも、仮想 CPU ライセンス用に管理されているエディションは、スタンダード、エンタープライズ、プラチナの 3 つです。これらのエディションは、帯域幅ライセンスのエディションでロック解除された機能と同じ機能のセットをロック解除します。

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ら、Citrix ADC VPX を再起動する必要があります。

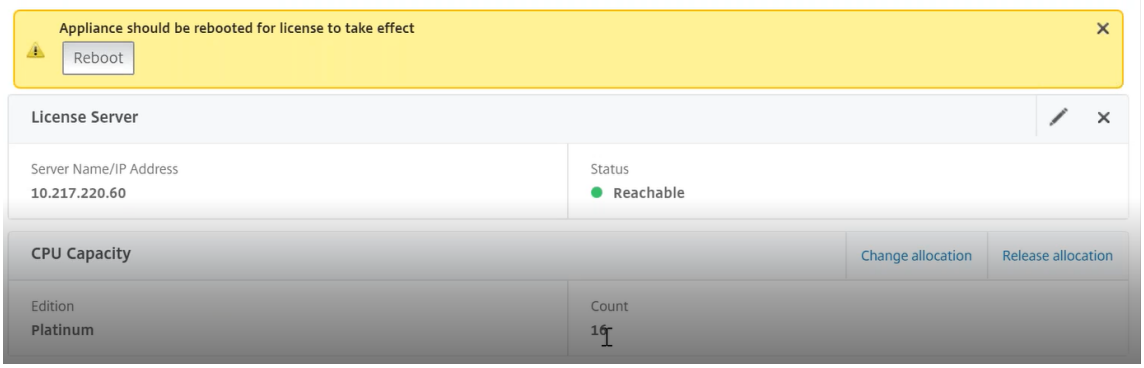
GUI を使用して **NetScaler ADC VPX** でライセンスサーバーを構成するには:

1. NetScaler ADC VPX で、［システム］>［ライセンス］に移動し、［ライセンスの管理］をクリックします。
2. ライセンスページで、「新規ライセンスを追加」をクリックします。
3. ライセンスページで、「リモートライセンスを使用する **」オプションを選択します。
4. ** リモートライセンスモードリストから CPU** ライセンスを選択します。
5. ライセンスサーバーの IP アドレスとポート番号を入力します。
6. ［続行］をクリックします。



> 注:
>
> NetScaler ADC VPX インスタンスは常に NetScaler ADM に登録する必要があります。まだ行っていない場合は、［**NetScaler ADM** に登録］を有効にして、NetScaler ADM のログイン資格情報を入力します。

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 [**Reboot**] 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 Standard Edition ライセンスをすでに実行しているとします。そのライセンスをリリースして、Enterprise エディションからチェックアウトできます。

CLI を使用した NetScaler ADC VPX ライセンスでのライセンスサーバーの構成

NetScaler ADC VPX コンソールで、次のコマンドを入力して次の 2 つのタスクを実行します。

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:

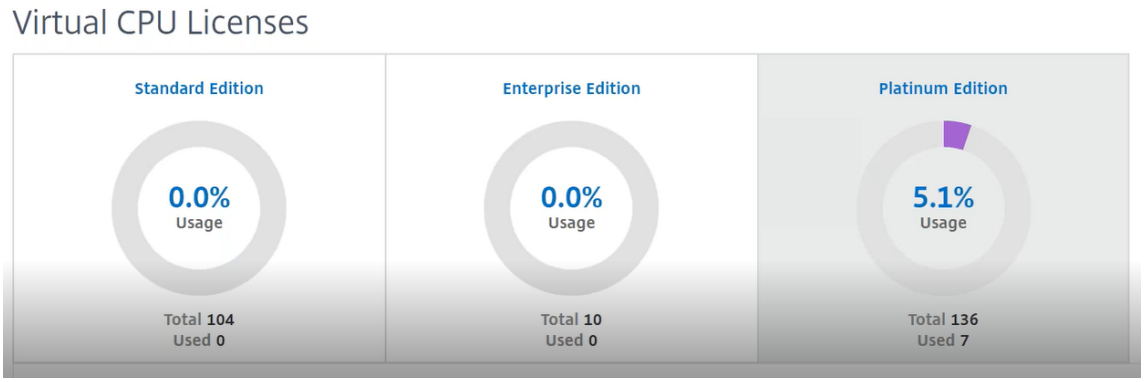
```
set capacity -vcpu - edition platinum
<!--NeedCopy-->
```

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-->
```

NetScaler ADM での仮想 CPU ライセンスの管理

1. Citrix ADM で、［ネットワーク］>［ライセンス］>［仮想 **CPU** ライセンス］に移動します。
2. このページには、各ライセンスエディションに割り当てられたライセンスが表示されます。
3. 各ドーナツ内の番号をクリックすると、このライセンスを使用している Citrix ADC インスタンスが表示されます。



NetScaler ADC CPX 用の仮想 CPU ライセンス

NetScaler ADC CPX インスタンスをプロビジョニングするときに、インスタンスの CPU 使用率に応じて、ライセンスサーバーからライセンスをチェックアウトするように NetScaler ADC CPX インスタンスを構成できます。

NetScaler ADC CPX は、NetScaler ADM 上で稼働するライセンスサーバーを利用してライセンスを管理します。NetScaler ADC CPX は、起動時にライセンスサーバーからライセンスをチェックアウトします。NetScaler ADC CPX がシャットダウンすると、ライセンスはライセンスサーバーにチェックインされます。

NetScaler ADC CPX は、Docker アプリストアからダウンロードできます。Docker ホストで、NetScaler ADC CPX をダウンロードするには、次のコマンドを実行します。

```
1 docker pull store/citrix/netscalercpx:<version>
2 <!--NeedCopy-->
```

CPX ライセンスには、次の 3 つのライセンスタイプがあります。

1. CPX と VPX でサポートされる仮想 CPU サブスクリプションライセンス
2. プールキャパシティライセンス
3. CPX のみの単一または複数の vCPU をサポートする CP1000 ライセンス

NetScaler ADC CPX インスタンスの **Provisioning** 中に **vCPU** サブスクリプションライセンスを構成するには:

Citrix ADC CPX インスタンスが使用する vCPU ライセンスの数を指定する必要があります。

- この値は、Docker、Kubernetes、または Mesos/Marathon を通じて環境変数として入力されます。
- ターゲット変数は「CPX_CORES」です。CPX は 1 ～7 コアをサポートできます。

2 つのコアを指定するには、次のように docker run コマンドを実行します。

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2
2 <!--NeedCopy-->
```

NetScaler ADC CPX インスタンスをプロビジョニングする際には、次に示すように、**docker run** コマンドで **Citrix** ADC ライセンスサーバーを環境変数として定義します。

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
     LS_PORT> cpx:11.1
2 <!--NeedCopy-->
```

各項目の意味は次のとおりです。

- *<LS_IP_ADDRESS>* は NetScaler ADC ライセンスサーバーの IP アドレスです。
- *<LS_PORT>* は Citrix ADC ライセンスサーバーのポートです。デフォルトのポートは 27000 です。

> 注:
>
> デフォルトでは、NetScaler ADC CPX インスタンスは vCPU サブスクリプションプールからライセンスをチェックアウトします。インスタンスが「n」の CPU で実行されている場合、CPX インスタンスは「n」のライセンス数をチェックアウトします。

NetScaler ADC CPX インスタンスの **Provisioning** 時に **NetScaler ADC** プールキャパシティまたは **CP1000** ライセンスを構成するには:

プールライセンス（帯域幅ベース）または CPX プライベートプール（CP1000 またはプライベートプールベース）を使用して CPX インスタンスのライセンスをチェックアウトする場合は、それに応じて環境変数を指定する必要があります。

例:

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
     LS_PORT> -e PLATFORM=CP1000 cpx:11.1
2 <!--NeedCopy-->
```

CP1000. このコマンドは、CP1000 プール（CPX プライベートプール）からのチェックアウトをトリガーします。次に、NetScaler ADC CPX インスタンスは、CPX_CORES に指定された「n」個のコアに対して「n」個のインスタンスを取得します。最も一般的な使用例は、1 つのインスタンスのチェックアウトに n = 1 を指定することです。マルチコア CPX のユースケースでは、「n」個の vCPU (「n」は 1 ～7) をチェックします。

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
     LS_PORT> -e BANDWIDTH=2000 cpx:11.1
2 <!--NeedCopy-->
```

プールされた容量。このコマンドは、インスタンスプールから 1 つのライセンスをチェックアウトし、プラチナ帯域幅プールから 1000 Mbps の帯域幅を消費しますが、CPX は最大 2000 Mbps で実行できます。プールライセンスでは、最初の 1000 Mbps は課金されません。

> 注
>
> : 次の表に示すように、帯域幅プールからチェックアウトするときに、目的のターゲット帯域幅に対応する vCPU の数を指定します。

コア数 (vCPU)	最大帯域幅
1	1000Mbps
2	2000 Mbps
3	3500 メガビット/秒
4	5000Mbps

5	6500 メガビット/秒
6	8000Mbps
7	9300 メガビット/秒

Citrix SD-WAN インスタンスの管理

February 6, 2024

Citrix ADM を使用すると、ネットワーク内の Citrix SD-WAN アプライアンスの分析を監視、管理、および表示できます。次の相互運用性表は、Citrix SD-WAN プラットフォームの各エディションで現在サポートされている Citrix ADM の機能に関する情報を示しています。

Citrix SD-WAN プラットフォームエディションと NetScaler ADM 機能の操作性マトリックス

プラットフォーム版	検出中	構成	監視	レポート (ネットワークレポート)	イベント管理	HDX Insight	WAN Insight
Citrix SD-WAN WANOP	はい	はい	はい	はい	はい	はい	はい
Citrix SD-WAN SE	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
Citrix SD-WAN PE	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ

Citrix ADM がサポートする Citrix SD-WAN バージョン

プラットフォーム版	Citrix SD-WAN バージョン	Citrix ADM バージョン
Citrix SD-WAN WANOP	Citrix CloudBridge 7.4 以降	Citrix ADM 11.0 以降
Citrix SD-WAN SE	Citrix SD-WAN 9.3.0 以降のバージョンでは、	NetScaler ADM 12.0.53.8 以降

プラットフォーム版	Citrix SD-WAN バージョン	Citrix ADM バージョン
Citrix SD-WAN PE	Citrix SD-WAN 9.3.0 以降のバージョンでは、	NetScaler ADM 12.0.53.8 以降

Citrix SD-WAN WANOP アプライアンスを管理インスタンスとして NetScaler ADM に追加できます。詳しくは、「NetScaler ADM へのインスタンスの追加」を参照してください。Citrix SD-WAN WANOP インスタンスの WAN Insight、HDX Insight、ネットワークレポート、イベントレポートを表示できます。

NetScaler ADM では、Citrix SD-WAN スタンダードエディション（SE）およびエンタープライズエディション（EE）アプライアンスが自身を NetScaler ADM で管理対象インスタンスとして登録できます。

Citrix SD-WAN SE/PE/AE アプライアンスを NetScaler ADM に追加するには、Citrix SD-WAN SE/PE/AE アプライアンスで NetScaler ADM を AppFlow コレクタとして構成します。Citrix SD-WAN SE/PE/AE アプライアンスは、それ自身を NetScaler ADM 上で管理対象インスタンスとして追加します。SD-WAN SE/PE/AE アプライアンスは、分析データを NetScaler ADM に送信します。

NetScaler ADM は、各 SD-WAN SE/PE/AE デバイスの AppFlow コレクタとして個別に設定することも、Citrix SD-WAN Center を使用して構成を管理アプライアンスにエクスポートすることもできます。

詳細については、「NetScaler ADM での Citrix SD-WAN SE/PE/AE インスタンスの追加」を参照してください。

Citrix SD-WAN PE アプライアンスの場合、AppFlow の構成に応じて、HDX データレコードまたはマルチホップデータを表示できます。Citrix SD-WAN SE アプライアンスは、マルチホップデータのみを提供します。詳しくは、HDX [Insight のレポートとメトリクスの表示およびマルチホップ展開用の Analytics データの表示を参照してください](/ja-jp/netscaler-application-delivery-management-software/12-1/manage-sd-wan-wo-instances/view-sd-wan-analytics-data-multi-hop-deployment.html)。

このページでは、NetScaler ADM をセットアップし、NetScaler ADM を使用して SD-WAN WANOP アプライアンスを管理するために参照できるトピックへのクイックアクセスリンクを提供します。

Citrix ADM の概要

Citrix ADM について

アーキテクチャ

Citrix ADM がインスタンスを検出する方法

Citrix ADM が管理対象インスタンスと通信する方法

Citrix ADM デプロイメント

Citrix Hypervisor で Citrix ADM をデプロイする

Microsoft Hyper-V を使用して NetScaler ADM を展開する

VMware ESXi で Citrix ADM をデプロイする

Linux KVM サーバーを使用した NetScaler ADM デプロイ

Citrix ADM を高可用性モードでデプロイする

NetScaler Insight Center から NetScaler ADM への移行

Citrix ADM を Director と統合

インスタンス管理

Citrix ADM にインスタンスを追加する方法

Citrix ADM でインスタンスグループを作成する方法

Citrix ADM を使用してインスタンスをバックアップおよび復元する方法

構成管理

Citrix ADM の修正コマンドから構成ジョブを作成する方法

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

Citrix ADM の組み込みテンプレートを使用して構成されたジョブを再スケジュールする方法

実行済みの構成ジョブを再使用する方法

分析

WAN Insight

HDX Insight

Citrix SD-WAN WANOP インスタンスのネットワークレポートを表示する方法

アダプティブしきい値を構成する方法

分析用のデータベースの概要を構成する方法

Citrix ADM を使用してしきい値とアラートを作成する方法

イベント管理

Citrix ADM でイベントのイベント経過時間を設定する方法

Citrix ADM を使用してイベントフィルターをスケジュールする方法

Citrix ADM からのイベントに繰り返し電子メール通知を設定する方法

Citrix ADM を使用してイベントを抑制する方法

Citrix SD-WAN WANOP インスタンスのイベントレポートを表示する方法

NetScaler インスタンスで発生イベントの報告重要度を変更する方法

NetScaler ADM でイベントの概要を表示する方法

Citrix ADM のインフラストラクチャダッシュボードに SNMP トラップのイベントの重大度とスキューを表示する方法

認証

外部認証サーバーをカスケードする方法

RADIUS 認証サーバーを追加する方法

LDAP 認証サーバーを追加する方法

TACACS 認証サーバーを追加する方法

Citrix ADM で認証サーバーグループを抽出する方法

ローカル認証のフォールバックを有効にする方法

NetScaler ADM システム

Citrix ADM システムの管理

Citrix ADM をアップグレードする方法

Citrix ADM のテクニカルサポートファイルを生成する方法

単一サーバー展開で Citrix ADM サーバーをバックアップおよび復元する方法

高可用性ペアの Citrix ADM 構成をバックアップおよび復元する方法

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

Citrix ADM で NTP サーバーを構成する方法

Citrix ADM の SSL 設定を構成する方法

Citrix ADM のシスログ消去間隔を構成する方法

NetScaler ADM 監査情報を表示する方法

NetScaler ADM システム通知設定を構成する方法

Citrix ADM の CPU、メモリ、およびディスクの使用状況を監視する方法

Citrix ADM の暗号グループを構成する方法

Citrix ADM で SNMP トラップ、マネージャー、およびユーザーを作成する方法

Citrix ADM サーバーにホスト名を割り当てる方法

Citrix ADM のシステムプルーニング設定を構成する方法

Citrix ADM を使用してシステムバックアップ設定を構成する方法

NetScaler ADM でシステムアラームを構成および表示する方法

Citrix SD-WAN インスタンスの追加

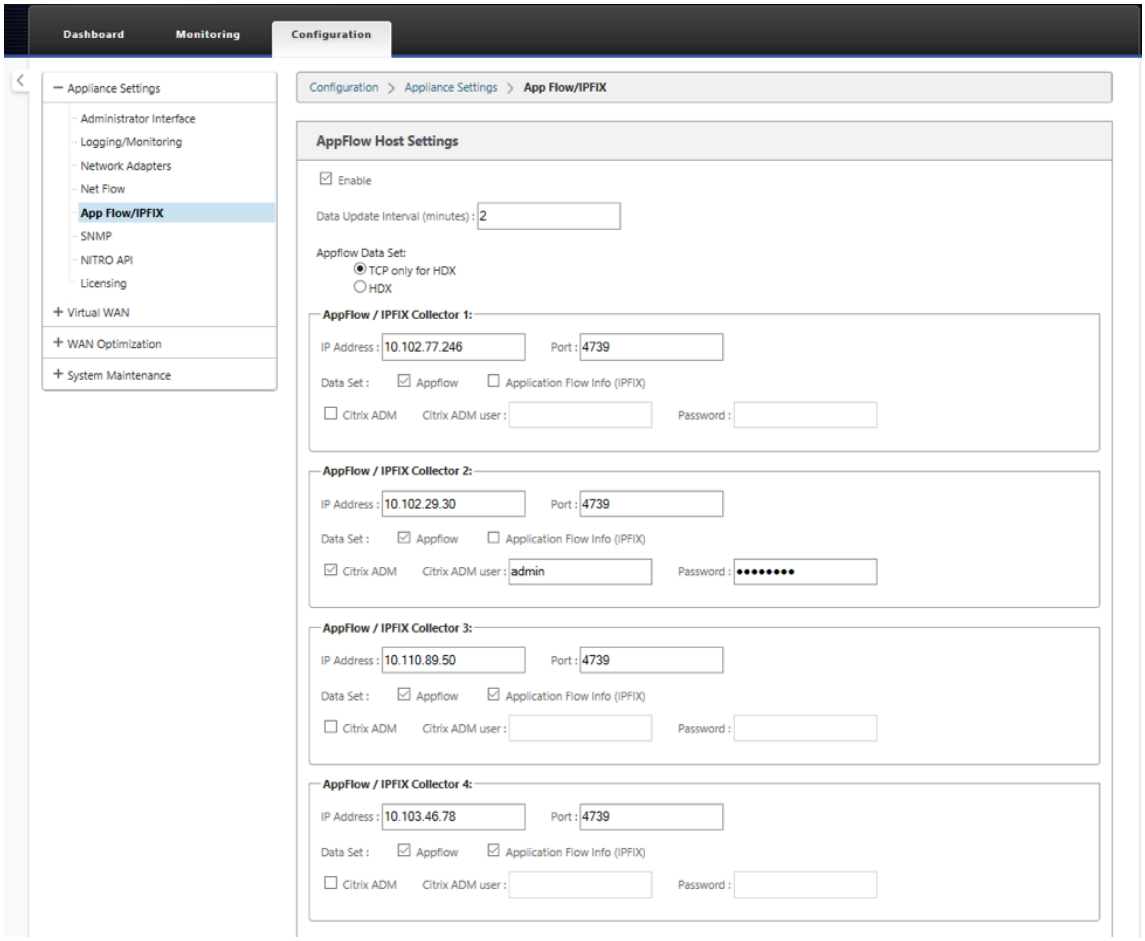
February 6, 2024

NetScaler ADM にこれらのインスタンスを追加するには、Citrix SD-WAN SE/PE アプライアンスの AppFlow コレクターとして NetScaler ADM を構成します。Citrix SD-WAN SE/PE アプライアンスは Citrix ADM にマネージドインスタンスとして登録され、その AppFlow レコードが収集されます。**Citrix SD-WAN PE** アプライアンスの場合、**HDX** テンプレートのみの TCP または HDX テンプレートのいずれかを有効にできます。 **HDX** 専用 **TCP** テンプレートはマルチホップデータを提供します。**HDX** テンプレートは HDX データを提供します。データセンターアプライアンスでのみ有効にしてください。

NetScaler ADM は、個々の SD-WAN SE/PE/AE アプライアンス上で AppFlow コレクタとして構成できます。または、SD-WAN Center を使用して NetScaler ADM を AppFlow コレクタとして構成し、その構成を管理しているアプライアンスにエクスポートできます。

Citrix SD-WAN SE/PE/AE アプライアンスで、**NetScaler ADM** を **AppFlow ow** コレクタとして構成するには:

1. SD-WAN SE/PE/AE Web インターフェイスで、[設定] > [**AppFlow/IPFIX**] に移動します。
2. [有効] を選択します。



3. 「データ更新間隔」フィールドで、AppFlow レポートが AppFlow コレクターにエクスポートされる時間間隔を分単位で指定します。

> 注
>
> Citrix ADM が AppFlow コレクターの場合、データ更新間隔は 1 分である必要があります。

4. 次のいずれかを行います：

   - **HDX** を選択して、HDX インサイトデータを AppFlow コレクターに送信します。これは、ブランチアプライアンスで有効にする必要があります。
   - マルチホップデータを AppFlow コレクターに送信するには 、**HDX** 用の **TCP** のみを選択します。

> 注
>
> **HDX** テンプレートオプションは Citrix SD-WAN PE アプライアンスでのみ使用でき、データセンターアプライアンスで有効にする必要があります

5. 「**IP** アドレス」フィールドに、外部 AppFlow コレクターシステム（Citrix ADM サーバー）の IP アドレスを入力します。

6. 「ポート 」フィールドに、外部 AppFlow コレクターシステムがリスンするポート番号を入力します。デフォルト値は 4739 です。
7. **Citrix ADM** チェックボックスを選択して、Citrix ADM が AppFlow コレクターであることを指定します。

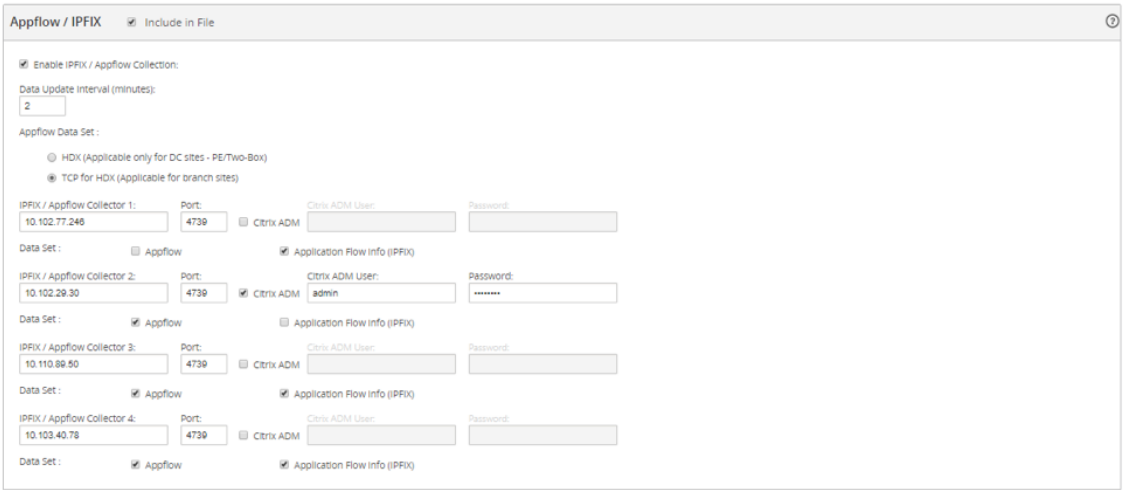
   > 注
   >
   > - NetScaler ADM は現在、IPFIX 収集をサポートしていません。
   > - 最大 4 つの AppFlow コレクターを追加できます。Citrix ADM または IPFIX プロトコルをサポートする任意の AppFlow コレクターのいずれか。

8. Citrix ADM サーバーの認証情報を入力します。
9. [設定の適用] をクリックします。

Citrix SD-WAN SE/PE アプライアンスが検出され、Citrix ADM に一覧表示されます。Citrix SD-WAN SE/PE アプライアンスは、分析データを NetScaler ADM に送信します。詳細については、「AppFlow と IPFIX」を参照してください。

Citrix SD-WAN センターを使用して **NetScaler ADM** を **AppFlow** コレクターとして構成するには:

1. Citrix SD-WAN Center 管理 UI で、[構成] > **[** アプライアンス設定] に移動します。
2. **AppFlow/IPFIX** セクションに移動し、「ファイルに含める」を選択 します。
3. [**IPFIX /AppFlow** 収集を有効にする] を選択します。



4. 「データ更新 間隔」フィールドで、AppFlow レポートが AppFlow コレクターにエクスポートされる間隔を分単位で指定します。

   > 注
   >
   > Citrix ADM が AppFlow コレクターの場合、データ更新間隔は 1 分である必要があります。

5. 次のいずれかを行います:

- **HDX** を選択して、HDX インサイトデータを AppFlow コレクターに送信します。
- マルチホップインサイトデータを **AppFlow** コレクターに送信するには、**HDX** 用の **TCP** を選択します。これは、ブランチアプライアンスで有効にする必要があります。

> 注
>
> **HDX** テンプレートオプションは Citrix SD-WAN PE アプライアンスでのみ使用でき、データセンターアプライアンスで有効にする必要があります。

6. **IPFIX/AppFlow Collector** フィールドに、外部の AppFlow コレクターシステム (Citrix ADM サーバー) の IP アドレスを入力します。
7. 「ポート」フィールドに、外部 AppFlow コレクターシステムがリスンするポート番号を入力します。デフォルト値は 4739 です。
8. **Citrix ADM** チェックボックスを選択して、Citrix ADM が AppFlow コレクターであることを指定します。
9. Citrix ADM サーバーの認証情報を入力します。

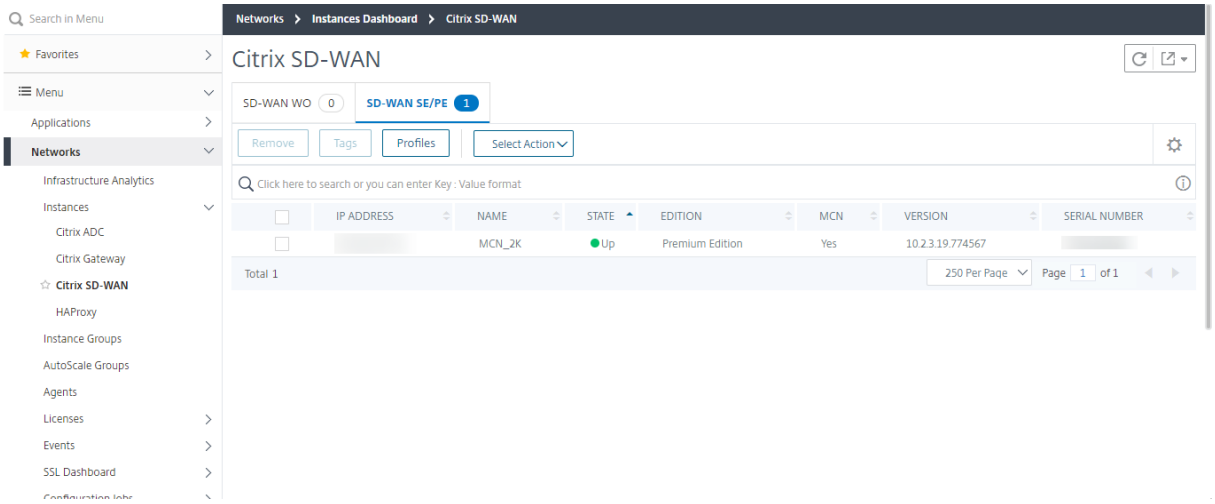
> 注
>
> 最大 4 つの AppFlow コレクターを追加できます。Citrix ADM または IPFIX プロトコルをサポートする任意の AppFlow コレクターのいずれか。

10. 構成を保存して、管理対象アプライアンスにエクスポートします。

    詳細については、「アプライアンス設定を構成して管理アプライアンスにエクスポートする方法」を参照してください。

Citrix SD-WAN センター、AppFlow、および IPFIX を使用して NetScaler ADM を AppFlow コレクタとして構成する方法の詳細については。

Citrix SD-WAN SE/PE アプライアンスが検出され、NetScaler ADM によってリストされます。Citrix SD-WAN SE/PE アプライアンスが検出され、NetScaler ADM に表示されます。検出された Citrix SD-WAN SE/PE アプライアンスを表示するには、NetScaler ADM Web インターフェイスで［ネットワーク］>［インスタンス］**>**［**Citrix SD-WAN**］の順に選択し、［**SD-WAN SE/PE/AE**］を選択します。



検出されたアプライアンスの IP アドレス、名前、現在の状態、ソフトウェアエディション、およびバージョンを確認できます。アプライアンスがマスターコントローラーノード（MCN）かどうかも確認できます。

次の操作を実行できます。

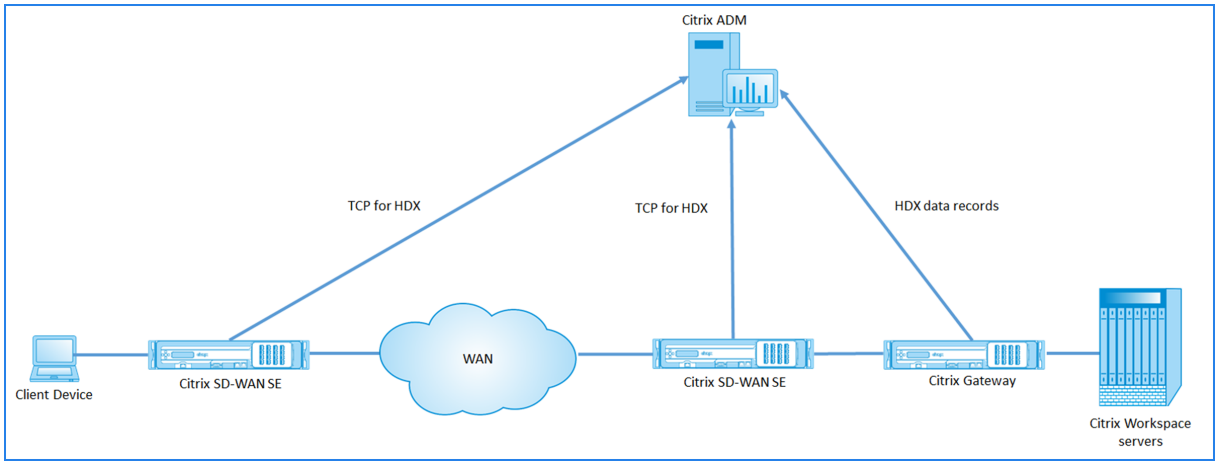
- インスタンスプロファイルの表示と削除。
- Citrix ADM からインスタンスを削除します。
- インスタンスの再検出。

Citrix SD-WAN PE アプライアンスの場合、AppFlow の構成に応じて、HDX データレコードまたはマルチホップデータを表示できます。Citrix SD-WAN SE アプライアンスは、マルチホップデータのみを提供します。詳しくは、「HDX Insight レポートとメトリックの表示」および 「マルチホップ展開用の Citrix SD-WAN Analytics データの表示」を参照してください。

マルチホップ展開のための **Citrix SD-WAN** 分析データの表示

February 6, 2024

マルチホップネットワーク展開では、次の図で示すように、クライアントとサーバー間にデバイスが複数存在します。このタイプの展開では、Citrix SD-WAN SE アプライアンスと Citrix ゲートウェイが Citrix ADM に追加され、AppFlow が有効になります。



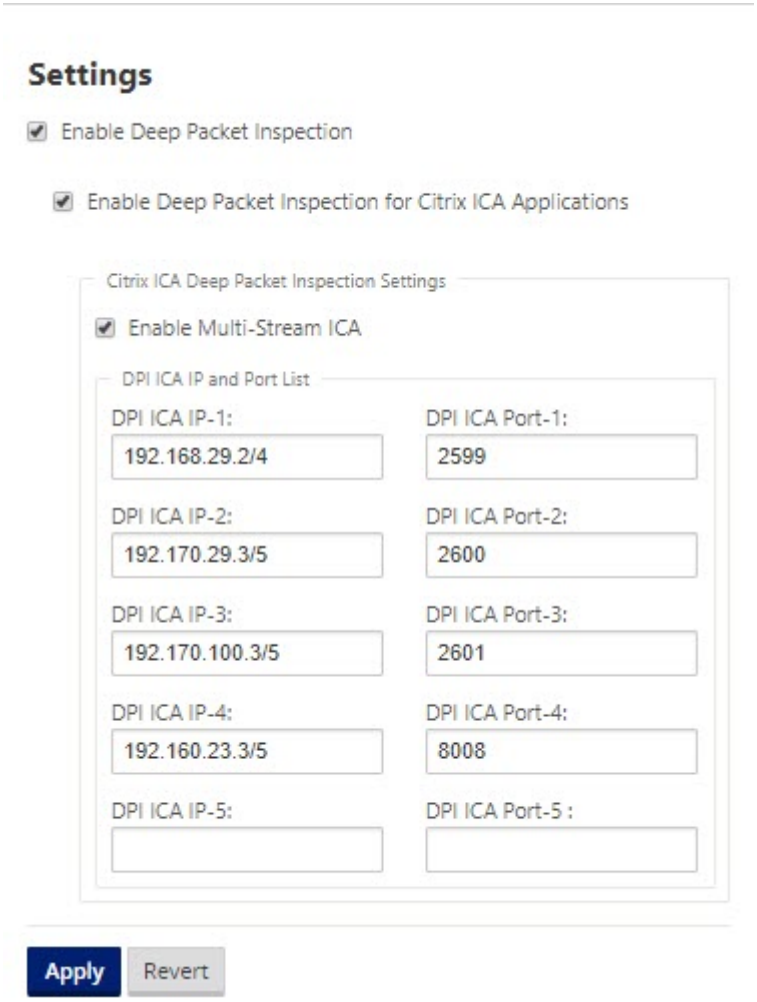
Citrix ADM は、ホップカウントと接続チェーン ID に基づいて、データを受信するアプライアンスを識別します。ホップ数は、トラフィックがクライアントからサーバーへ流れるときに通過するアプライアンスの数を表します。接続チェーン ID は、クライアントとサーバー間のエンドツーエンド接続を表します。

Citrix ADM は、ホップカウントと接続チェーン ID を使用してアプライアンスからのデータを関連付けて、レポートを生成します。

Citrix SD-WAN SE アプライアンスが分析データを Citrix ADM に送信するには、Citrix Gateway の仮想 IP アドレスを DPI ICA IP として構成し、DPI ICA のポート番号を 443 に設定する必要があります。

ICA DPI の設定を構成するには次の手順を実行します。

1. **Citrix SD-WAN SE** アプライアンスの **UI** で、[構成エディタ] **>** [詳細設定] **>** [グローバル] **>** [アプリケーション] **>** [設定] に移動します。
2. [ディープパケットインスペクションを有効にする] > [**Citrix ICA** アプリケーションのディープパケットインスペクションを有効にする] **>** [マルチストリーム ICA を有効にする **] を選択します



3. 「**DPI ICA IP-1** 」フィールドに、Citrix Gateway の仮想 IP アドレスとプレフィックスを入力します。
4. **DPI ICA** ポート**-1** フィールドに、ポート番号 443 を入力します。
5. 「適用」をクリックし、変更管理プロセスを使用して構成をアプライアンスにエクスポートします。

Citrix ADM では、アクティブな ICA セッションごとに、HDX Insight でセッション図を表示できます。セッションダイアグラムには、接続パスにあるデバイスの詳細が表示されます。また、ネットワークデバイスと直近のホップ間におけるクライアント側/サーバー側の遅延も詳細に確認できます。こうした情報により、遅延の根本原因を特定し、パフォーマンスの問題を解決することができます。

Citrix SD-WAN SE は HDX データレコードを送信しません。NetScaler SD-WAN SE で提供されるのは、HDX 情報の TCP のみです。HDX Insight データは、ネットワーク内の HDX Insight 対応デバイス（NetScaler ADC や NetScaler Gateway など）によって提供されます。

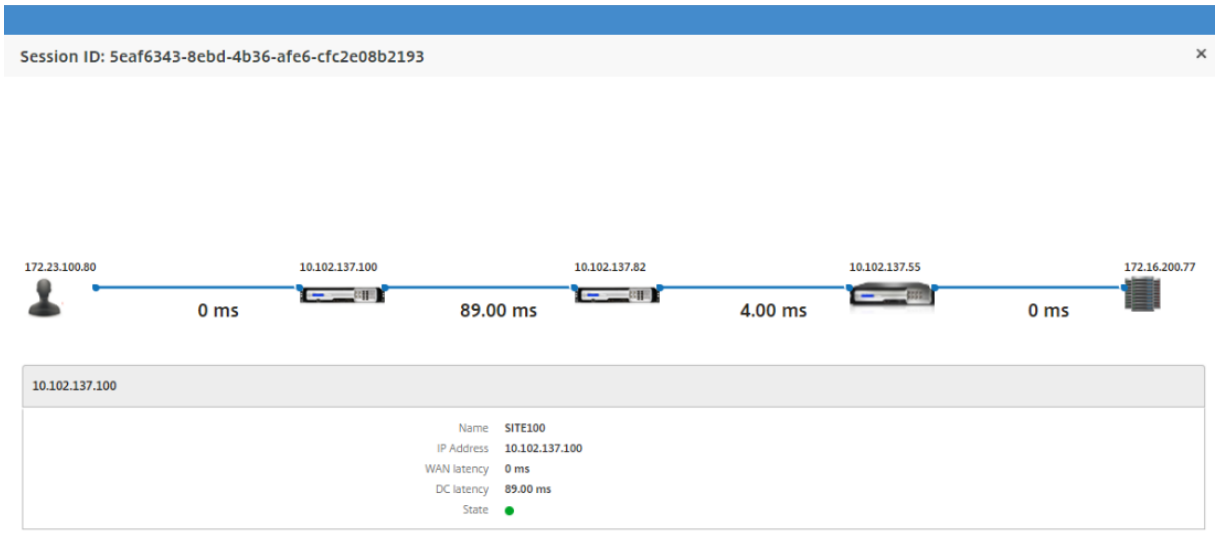
Citrix SD-WAN PE アプライアンスは、アプライアンスの AppFlow 構成に応じて、HDX データまたは HDX Insight データの TCP を送信できます。データセンターアプライアンスでは HDX テンプレートを有効にする必要があります。

> 注
>
> マルチホップ展開では、ネットワークデバイスのうち 1 つのみから HDX Insight データが送信されるようにしてください。残りのネットワークデバイスでは、HDX データの TCP を送信できます。

マルチホップデータを表示するには**:**

Citrix ADM Web インターフェイスで、[HDX Insight] **>** [ユーザー] **>** [現在のセッション] または [HDX Insight] **>** [アプリケーション] **>** [現在のセッション] に移動し、[図] アイコンをクリックします。

ネットワークトポロジダイアグラムが表示されます。



ネットワーク要素をクリックすると、詳細が表示されます。

> 注
>
> 表示される情報は、選択したネットワーク要素によって異なります。

Citrix アプライアンスには次のパラメータが表示されます。

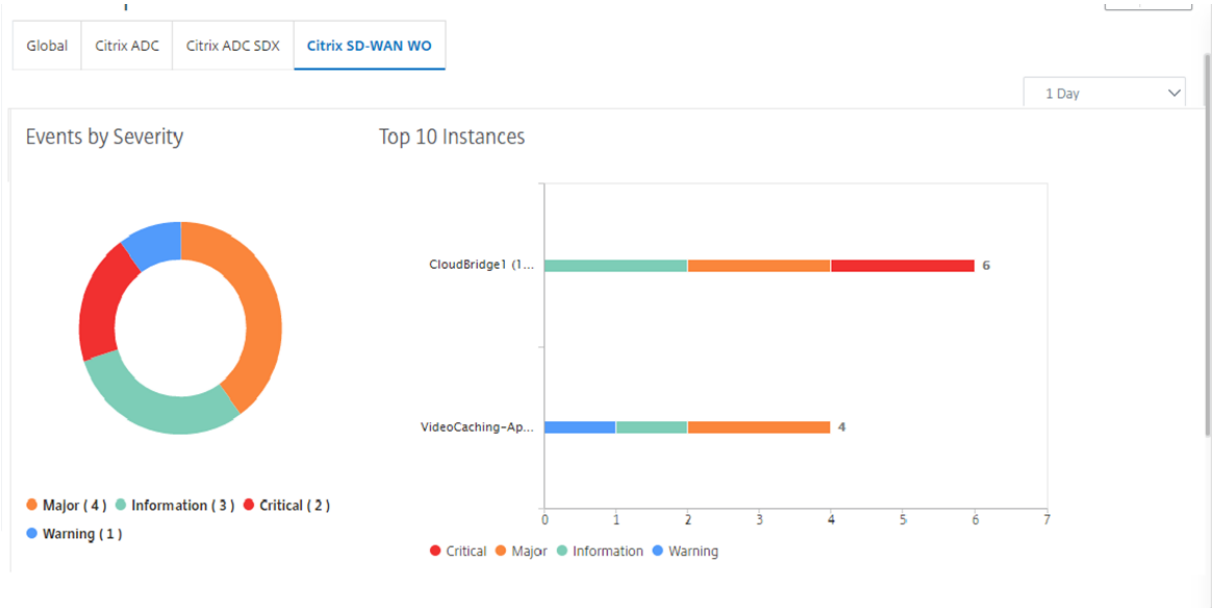
- 名前:Citrix アプライアンスの名前。
- **IP** アドレス: アプライアンスの IP アドレス。
- **WAN** 遅延: ネットワークのクライアント側による遅延。つまり、Citrix アプライアンスからエンドユーザーまで。
- **DC** 遅延: ネットワークのサーバー側による遅延。つまり、Citrix アプライアンスからバックエンドサーバーまでです。
- 状態: デバイスの到達可能性ステータス。

Citrix SD-WAN WANOP インスタンスのイベントレポートを表示する

February 6, 2024

[ネットワーク] > [イベント] > [レポート] に移動し、[**Citrix SD-WAN WO]** を選択すると、上位 **10** の **SD-WAN**WANOP インスタンスのイベントをグラフィカルに表示できます。

インスタンスごとにイベントが重要度に応じて表示され、各イベントをクリックするとイベント数、発生時期、イベントのカテゴリに関する詳細を確認できます。



Citrix SD-WAN WANOP インスタンスのネットワークレポートの表示

February 6, 2024

Citrix ADM で WAN 最適化ネットワーク関連のレポートを表示できます。このデータを使用して、ネットワークの問題のトラブルシューティングや、Citrix SD-WAN WANOP デバイスの動作の分析を行うことができます。WAN 最適

化デバイスについて、過去 1 時間、過去 1 日、過去 1 週間、または過去 1 ヵ月のネットワーク統計情報に関するレポートを表示できます。

次のレポートを表示できます。

レポート	説明
アクセラレーション	このレポートを使用して、高速トラフィックのパターン（サービスクラス別の KBPS）と、WAN 最適化アプライアンスを通過する高速 TCP 接続の数を分析します。これには、WAN 最適化デバイスを通過してアクセラレーションが行われる TCP 接続の数、アクセラレーション対象として選択されたオープン接続 とハーフクローズ接続の数、アクセラレーションの対象となるハーフオープン接続 の数が含まれます。
パススルー接続	このレポートでは、WAN 最適化デバイスの非アクセラレーション対象接続を確認できます。
サービスクラス	このレポートを使用すると、WAN 最適化デバイスに定義されているサービスクラスタイプ に基づく送受信帯域幅の削減量を確認できます。
アプリケーション	このレポートを使用して、WAN 最適化デバイスで実行されているアプリケーション の送受信データ量をビット/秒単位で表示します。
CPU 使用率	このレポートでは、WAN 最適化デバイスの CPU 使用率（%）を確認できます。
増加容量	このレポートでは、WAN 最適化デバイスの累積送信圧縮率を確認できます。
データ削減率	このレポートでは、送受信帯域幅の節約率（%）を確認できます。また、WAN 最適化デバイスの 送信帯域幅と受信帯域幅の節約値を個別に分析することもできます。
リンク使用率	このレポートを使用して、WAN 最適化の送信リンク使用率と受信リンク使用率をパーセンテージで表示します。
プラグイン使用状況	このレポートでは、WAN 最適化デバイスに接続されているプラグインの数を確認できます。
パケット損失	このレポートを使用して、WAN 最適化デバイスで定義されているリンクについて、リンクがドロップした送信パケットとリンク ドロップされた受信パケットを表示します。
スループット	このレポートを使用して、WAN 最適化デバイスのリンク送信量とリンク受信量をビット/秒単位で 表示します。

レポート	説明
QoS	このレポートを使用して、WAN 最適化デバイスの QoS 送信量 と QoS 受信量（ビット/秒）を 表示します。

Citrix SD-WAN WANOP ネットワークレポートを表示するには：

1. Citrix ADM で、[ネットワーク] > [ネットワークレポート] > [**Citrix SD-WAN WO**] に移動します。
2. [レポート名] ドロップダウンリストから、表示するレポートを選択します。
3. インスタンスドロップダウンリストから 、レポートを表示する Citrix SD-WAN WANOP インスタンスを選択します。
4. 「期間」ドロップダウンリストから、時間間隔を選択します。
5. ［実行］をクリックします。

Citrix SD-WAN WANOP インスタンスのバックアップ

February 6, 2024

インスタンスの現在の状態をバックアップし、後でバックアップしたファイルを使用してインスタンスを同じ状態に復元できます。インスタンスをアップグレードする前または予防上の理由から、インスタンスをバックアップすることをお勧めします。安定したシステムをバックアップしておくと、システムが不安定になった場合にシステムを安定した状態に復元できます。Citrix SD-WAN WANOP インスタンスでバックアップと復元を実行する方法は複数あります。GUI、CLI を使用してインスタンスを手動でバックアップおよび復元するか、Citrix ADM を使用してバックアップを実行できます。Citrix ADM は、NITRO コール、Secure Shell（SSH）プロトコル、およびセキュアコピー（SCP）プロトコルを使用して、管理対象 Citrix SD-WAN WANOP インスタンスの現在の状態をバックアップします。

インスタンスバックアップ設定の構成

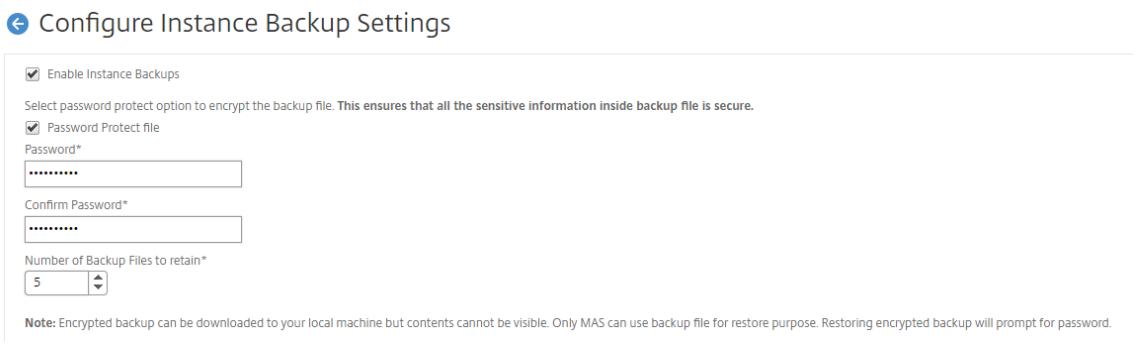
Citrix ADM で Citrix SD-WAN WANOP インスタンスのバックアップを作成する前に、Citrix ADM でインスタンスのバックアップ設定を構成する必要があります。

インスタンスのバックアップ設定を構成するには**:**

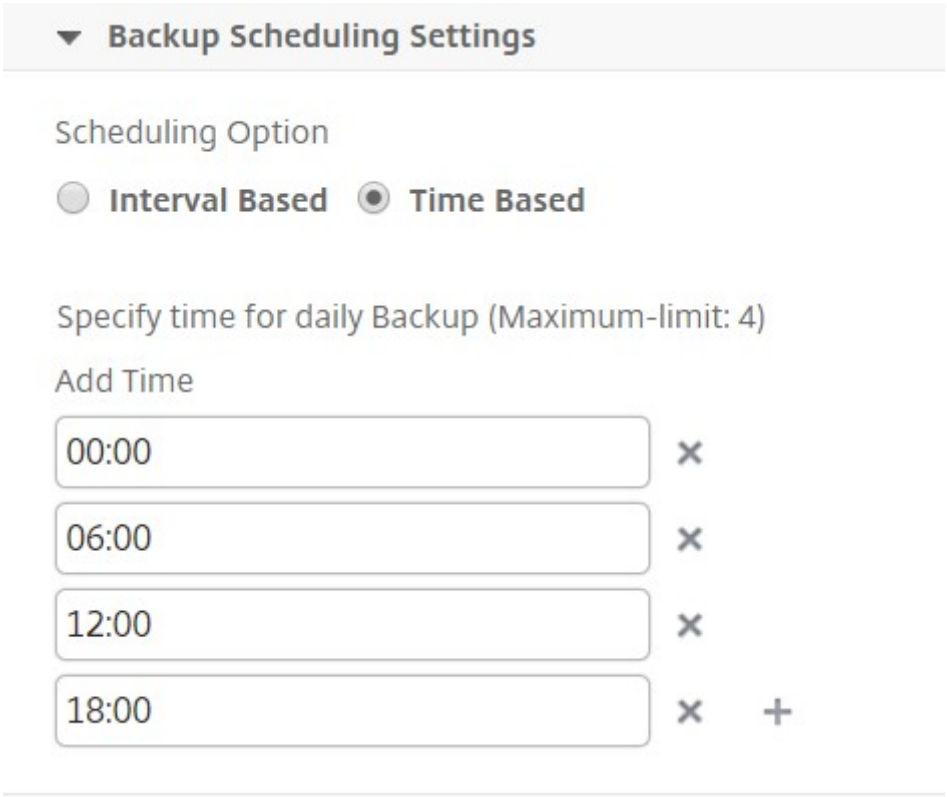
1. NetScaler ADM で、［システム］ > ［システム管理］ に移動します。右側のペインの [バックアップ設定] で、[インスタンスバックアップ設定] を選択します。
2. [インスタンスバックアップを有効にする] を選択します。このオプションは、デフォルトで有効になっています。

3. バックアップファイルを暗号化するには、「パスワード保護ファイル」を選択します。バックアップファイルを暗号化することで、バックアップファイル内の機密情報の安全性が確保されます。
4. [保持するバックアップファイルの数] フィールドで、Citrix ADM に保持するバックアップファイルの数を指定します。最大 50 個のバックアップファイルを保持できます。

> 注
>
> 各バックアップファイルには、ある程度のストレージ要件が必要です。Citrix ADM には、要件に応じて最適な数のバックアップファイルを保存することをお勧めします。



5. バックアップスケジュール設定を設定します。ここでは、次のいずれかオプションを選択できます:
   - 間隔ベース -指定した間隔が経過すると、NetScaler ADM でバックアップファイルが作成されます。デフォルトのバックアップ間隔は 12 時間です。
   - 時間ベース-バックアップを実行する時間を「時間: 分」形式で指定できます。Citrix ADM では、インスタンスで毎日最大 4 回のバックアップを実行できます。

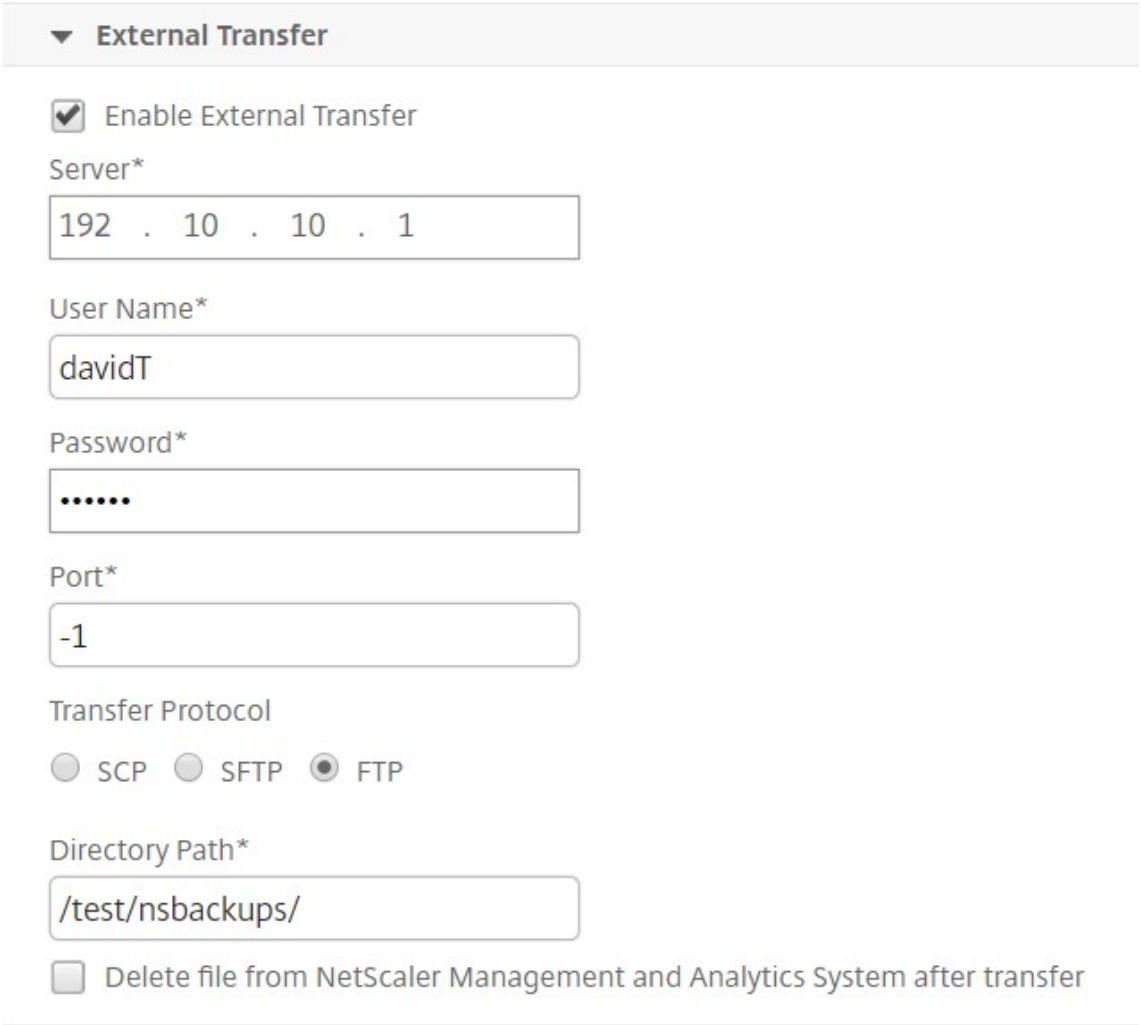


> 注
>
> **Citrix ADC** 設定セクションは無視してください。これらの設定は Citrix SD-WAN WANOP インスタンスには適用されません。

6. [外部転送を有効にする] を選択して、インスタンスのバックアップファイルを外部の場所に転送します。次のフィールドに値を入力します。

   - サーバー: 外部サーバーの IP アドレス。
   - ユーザー名: 外部サーバーのユーザー名
   - パスワード: 外部サーバーのパスワード。
   - ポート: 外部サーバーとの通信に使用されるポート番号。
   - 転送プロトコル: Citrix ADM から外部サーバーにバックアップファイルを転送するために使用されるプロトコル。

   バックアップファイルを外部サーバーに転送した後、Citrix ADM から削除することもできます。



7. [**OK**] をクリックします。

> 注
>
> Citrix ADM は、選択した Citrix SD-WAN WANOP インスタンスのいずれかでバックアップが失敗すると、SNMP トラップまたは Syslog 通知をそれ自体に送信します。

Citrix SD-WAN WANOP インスタンスのバックアップの作成

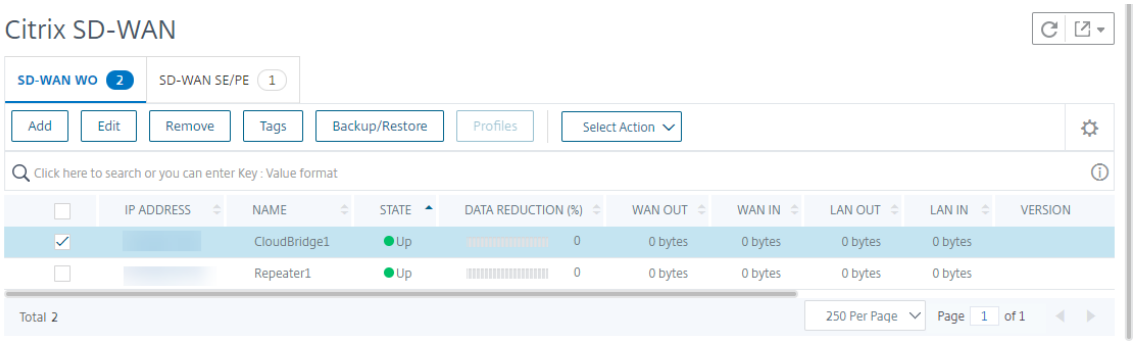
Citrix SD-WAN WANOP インスタンスのバックアップを作成する手順は、デフォルトの nsroot プロファイルを使用して管理者ユーザーにも適用できます。

カスタムユーザーが Citrix SD-WAN WANOP インスタンスのバックアップを作成する方法については、このトピックの「カスタムユーザー用の Citrix SD-WAN WANOP インスタンスのバックアップを作成する」を参照してください。

Citrix SD-WAN WANOP インスタンスが NetScaler ADM に追加されていることを確認します。詳細については、「NetScaler ADM へのインスタンスの追加」を参照してください。

Citrix SD-WAN WANOP インスタンスのバックアップを作成するには:

1. Citrix ADM で、[ネットワーク] > [インスタンス] > **[**Citrix SD-WAN**] に移動し ます。
2. [**SD-WAN WO**] で、バックアップする Citrix SD-WAN OP インスタンスを選択し、[バックアップと復元] をクリックします。



3. 「バックアップファイル」ページで 、「バックアップ」をクリック します。
4. 以下のオプションのいずれかを使用してバックアップファイルを暗号化します。

   - [パスワードで保護されたファイル] を選択し、パスワードを入力してバックアップファイルを暗号化します。
   - インスタンスバックアップ設定ページで指定したグローバルパスワードを使用するには、「グローバルパスワード を使用」を選択します。

5. 「バックアップを作成」を
   クリックします

カスタムユーザー向けの **Citrix SD-WAN WANOP** インスタンスのバックアップの作成

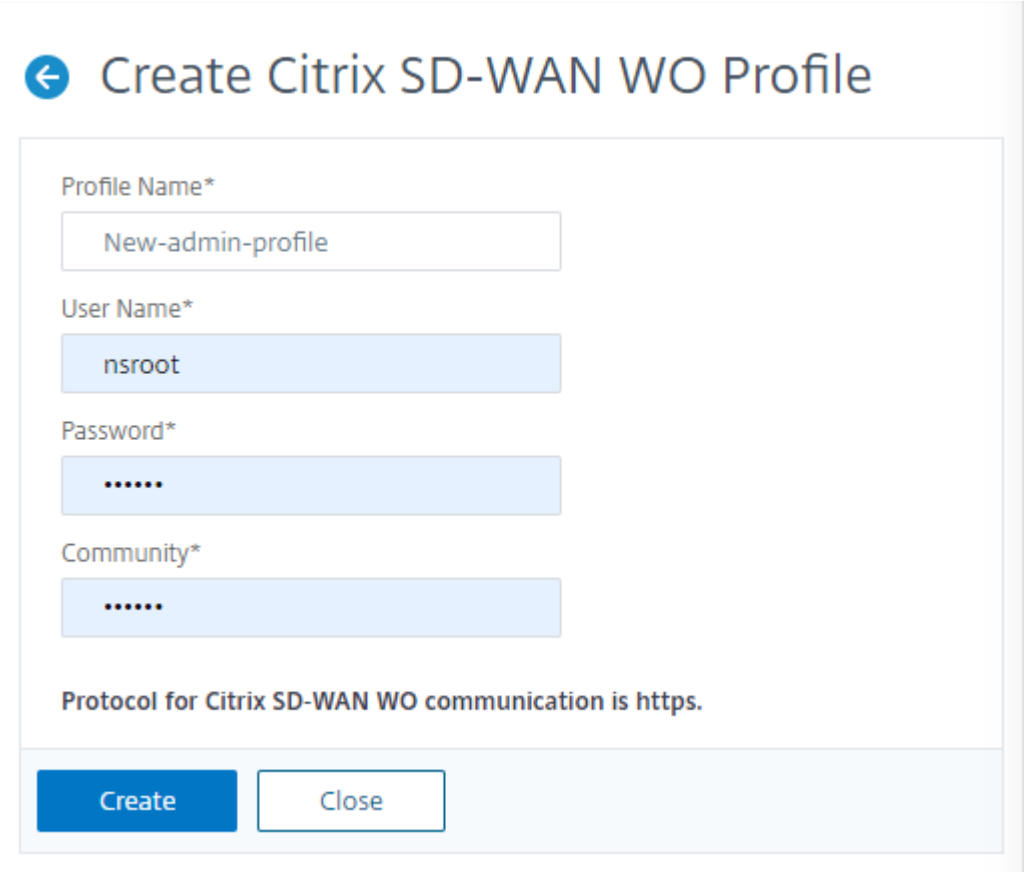
Citrix SD-WAN WANOP インスタンスで管理者権限を持つカスタムユーザーを作成した場合は、次の手順を使用してインスタンスを追加し、Citrix ADM を使用してそのインスタンスをバックアップします。

カスタムユーザーによるバックアップ操作は、400/800/1000WS/2000WS/3000/4000/5000/4100/5100 SD-WAN WANOP プラットフォームではサポートされていません。

> 注
>
> Citrix ADM で Citrix SD-WAN アドバンストプラットフォームのバックアップを作成する際には、デフォルトの nsroot プロファイルを使用することをお勧めします。

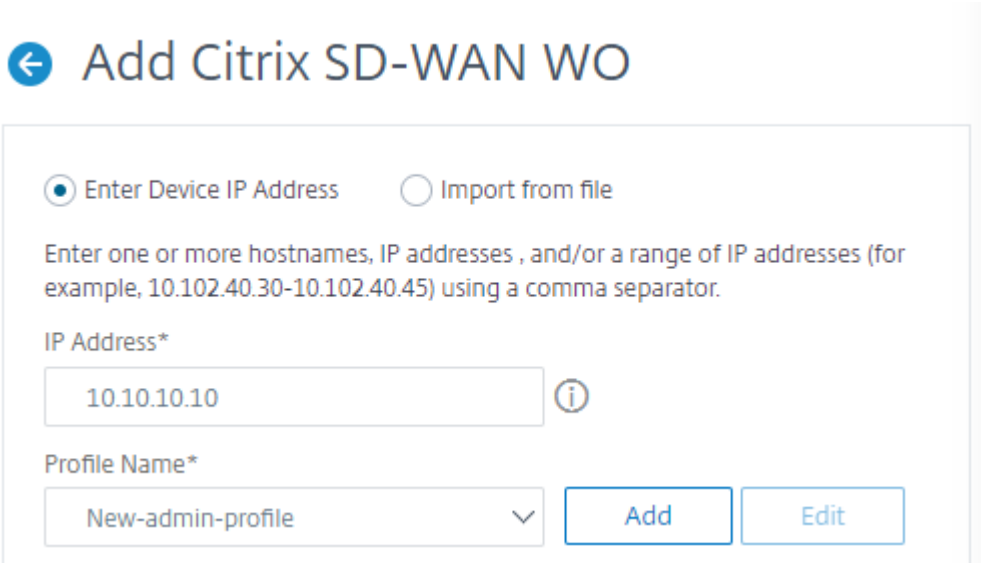
Citrix SD-WAN WANOP インスタンスを追加し、カスタムユーザーのバックアップを作成するには:

1. Citrix ADM で、[ネットワーク] > [インスタンス] > **[****Citrix SD-WAN] に移動し、[**SD WAN** WO**] を選択します。
2. [追加] をクリックします。
3. 「**IP** アドレス」フィールドに、Citrix SD-WAN WANOP インスタンスの IP アドレスを入力します。
4. 「プロファイル名」フィールドの横にある「追加」をクリックして、新しいプロファイルを作成します。[**Citrix SD-WAN WO** プロファイルの作成] ウィンドウが表示されます。



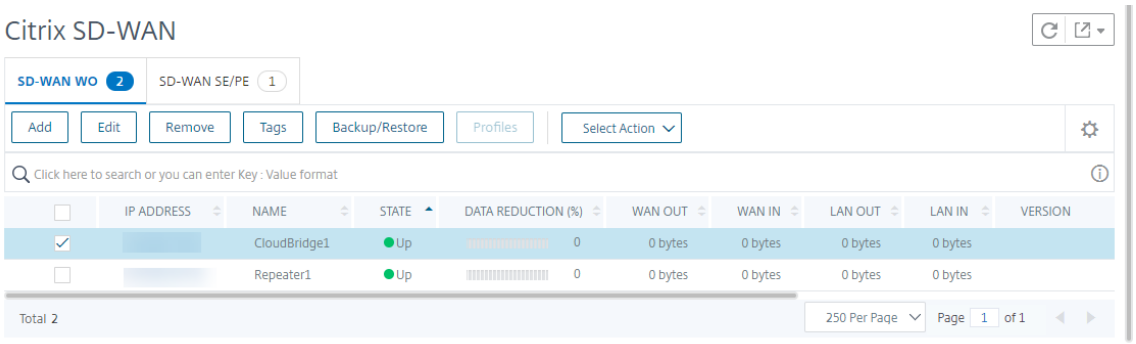
5. 「プロファイル名」フィールドに、プロファイルの名前を入力します。
6. [ユーザー名] フィールドに、SD-WAN WANOP インスタンスで作成したカスタムユーザーのユーザー名を入力します。
7. [パスワード] フィールドに、SD-WAN WANOP インスタンスでカスタムユーザーに設定したパスワードを入力します。
8. コミュニティフィールドに、SD-WAN WANOP アプライアンスで構成されている SNMP 通信文字列を入力します。(例: パブリック)
9. [作成] をクリックします。

10. 「プロファイル名」フィールドで、新しく作成したプロファイルを選択して「**OK**」をクリックします。



11. [ネットワーク] > [インスタンス] > **[**Citrix SD-WAN**] に 移動します。

12. **SD-WAN WO** で、追加した Citrix SD-WAN OP インスタンスを選択し、[バックアップと復元] をクリックします。



13. 「バックアップファイル」ページで 、「バックアップ」をクリック します。

14. 以下のオプションのいずれかを使用してバックアップファイルを暗号化します。

    - [パスワードで保護されたファイル] を選択し、パスワードを入力してバックアップファイルを暗号化します。
    - インスタンスバックアップ設定ページで指定したグローバルパスワードを使用するには、「グローバルパスワードを使用」を選択します。

注

暗号化されたバックアップファイルをローカルマシンにダウンロードすることはできますが、その内容を表示することはできません。これらのバックアップファイルを復元目的で使用できるのは Citrix ADM だけです。暗号化されたバックアップを復元すると、パスワードの入力を求められます。

15.「バックアップを作成」をクリックします。

重要

```
1. Citrix SD-WAN WANOP VPX アプライアンスの場合、Citrix ADM は CB ブローカー構成ファイルのみをバックアップします。
```

a) 高度な Citrix SD-WAN WANOP プラットフォームの場合、Citrix ADM は次の ものをバックアップします。·

- CB ブローカー設定ファイル
- NTP 設定ファイル
- DNS
- SNMPD コンフィギュレーションファイル
- シスログ設定ファイル
- SSL 証明書、キー、ポリシー
- SVM データベースファイル
- コンポーネント (XML 形式)
- リソース (XML フォーマット)

各フォルダーでバックアップされるファイルは、以下の表に一覧表示されています。フォルダー名に「*」が続いている場合は、そのフォルダーのすべてのファイルがバックアップされることに注意してください。

ディレクトリ	サブディレクトリまたはファイル
/br_broker/	CB-6BBB660A/ ws.conf
/など/	resolv.conf
/mps/	mps_devices.xml
/mpsconfig/	ssl/*、ntp.conf、snmpd.conf、syslog.conf
/mpsdb/	mpsdb_dump.sql
/ns/	ns-6cbb660a/*
/var/	mps/policy/, *mps/ssl_certs/ sdx_default_ssl_cert, mps/ssl_keys/ sdx_default_ssl_key, mps/tenants/*

HAProxy インスタンスの管理

February 6, 2024

HAProxy、すべての TCP サービスおよび HTTP サービスの負荷を分散させることができるオープンソースのロードバランサーです。HAProxy の詳細については、を参照してください http://www.haproxy.org/。

Application Delivery Management（Citrix ADM）は HAProxy バージョン 1.4.24 以降をサポートしています。HAProxy インスタンスをプロビジョニングしたホストを Citrix ADM に追加すると、Citrix ADM はホスト上の HAProxy インスタンスを検出し、それらを監視できるようにします。NetScaler MAS には、各インスタンスの HAProxy 構成について以下の種類の情報が表示されます。

- Frontend –バックエンドへの要求の転送方法
- Backend –転送された要求を受信するサーバー
- Servers –HAProxy によりトラフィックの負荷分散が行われるサーバー

詳しくは、http://www.haproxy.org/download/1.7/doc/configuration.txtを参照してください。

また、NetScaler ADM には、フロントエンドをリアルタイムで監視できる HAProxy アプリダッシュボードが用意されています。詳細については、HAProxy アプリダッシュボードを参照してください。

HAProxy インスタンスを NetScaler ADM に追加する

February 6, 2024

Citrix Application Delivery Management（Citrix ADM）では、HAProxy インスタンスをプロビジョニングしたホストの詳細を手動で追加する必要があります。これらの詳細を追加すると、NetScaler ADM はホストでプロビジョニングされた HAProxy インスタンスを自動的に検出し、NetScaler ADM インベントリに追加します。また、HAProxy インスタンスに構成されているすべてのフロントエンド、バックエンド、およびサーバーを検出し、フロントエンドを検出されたアプリケーションとして認識します。

前提条件

以下の点について確認してください。

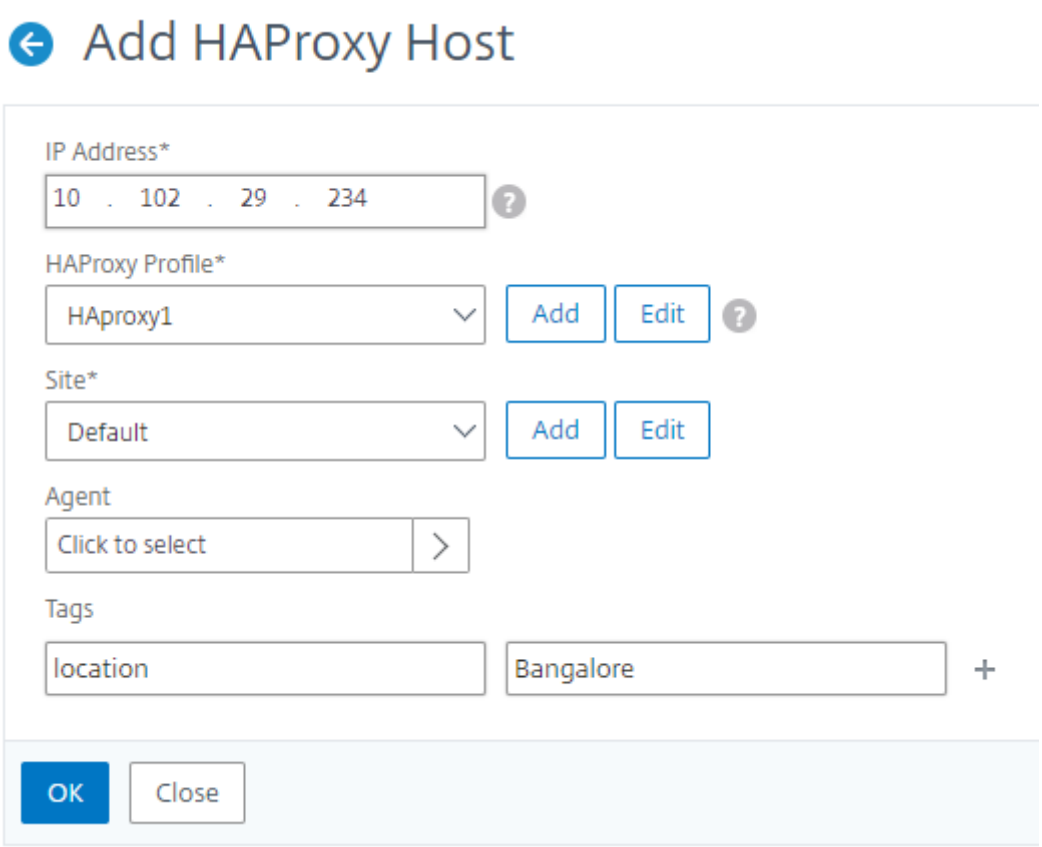
- 展開環境に HAProxy インスタンスを展開済みであること。詳しくは、http://www.haproxy.org/#docsを参照してください。
- HAProxy App ダッシュボードに表示するアプリケーションの統計情報について、フロントエンドの数が確定していること。デフォルトでは、検出された 30 アプリケーションの統計情報が HAProxy App ダッシュボードに表示されます。HAProxy アプリダッシュボードの詳細については、HAProxy アプリダッシュボードを参

照してください。検出されたアプリケーションの統計情報を 30 を超えて表示する場合は、ライセンスを別途購入する必要があります。詳しくは、「サードパーティライセンス」を参照してください。

> 重要
>
> Citrix ADM では、ホスト内の HAProxy インスタンスを検出するためにホストにアクセスする必要があります。NetScaler ADM へのアクセスを提供するには、ホストの SSH キーペアを指定するか、ホストのパスワードを使用します。SSH キーペアを使用してアクセスを提供する場合は、秘密キーと公開キーの SSH キーペアをホストで生成して、公開キーをホスト上で承認されたキーに追加するようにします。また、SSH ユーザーアカウントにはスーパーユーザー権限が必要です。

HAProxy インスタンスを **NetScaler ADM** に追加するには:

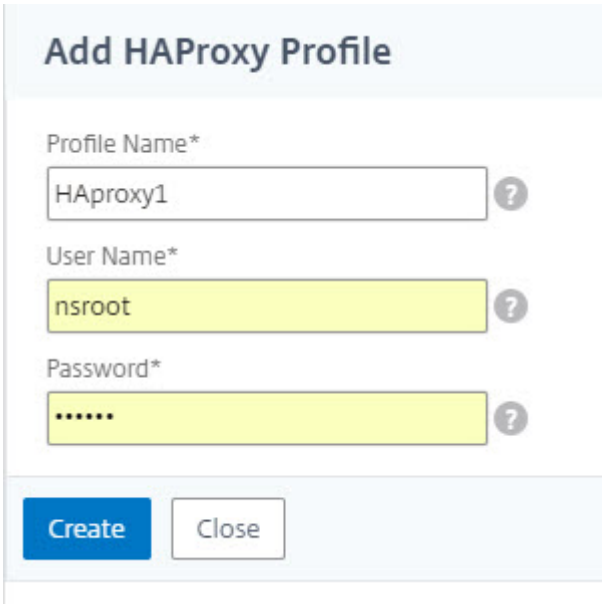
1. Web ブラウザで、**CitrixApplication Delivery Management** の IP アドレス(例:http://192.168.100.1)を入力します。
2. 「ユーザー名」フィールドと「パスワード」フィールドに、管理 者の資格情報を入力します。デフォルトの管理者認証情報は「nsroot」と「nsroot」です。
3. [ネットワーク] > [インスタンス] に移動します。「インスタンス」で「**HAProxy** 」を選択し、「追加」をクリックします。
4. [**HAProxy** ホストの追加] ダイアログボックスで、次の操作を行います。



1. [**IP Address**] フィールドに、HAProxy インスタンスをプロビジョニングしたホストの IP アドレスを入力します。

   a) **HAProxy** プロファイルメニューで、既存の HAProxy プロファイルを選択するか、新しい HAProxy プロファイルを作成して選択します。HAProxy プロファイルを作成するには、「追加」をクリックします。

      i. [**HAProxy** プロファイルの追加] ダイアログボックスで、次の操作を行います。



      i. [プロファイル名] フィールドに、プロファイル名を入力します。

      ii.「ユーザー名」フィールドと「パスワード」フィールドに、ホストのユーザー認証情報を入力します。

      iii.［作成］をクリックします。

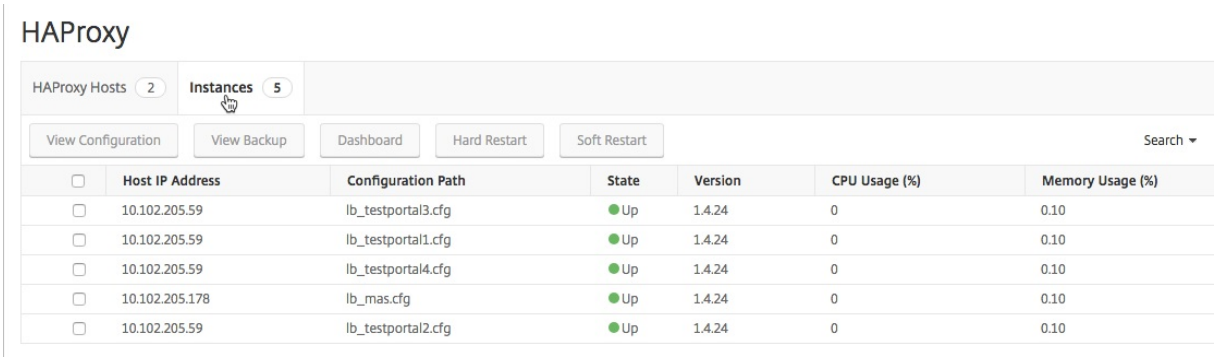
2.「サイト」メニューから、HAProxy サイトを選択します。新しいサイトを作成してメニューに追加するには、「追加」をクリックします。

3. [エージェント] メニューから [エージェント] を選択します。

4.「タグ」フィールドに、適切な値を入力します。

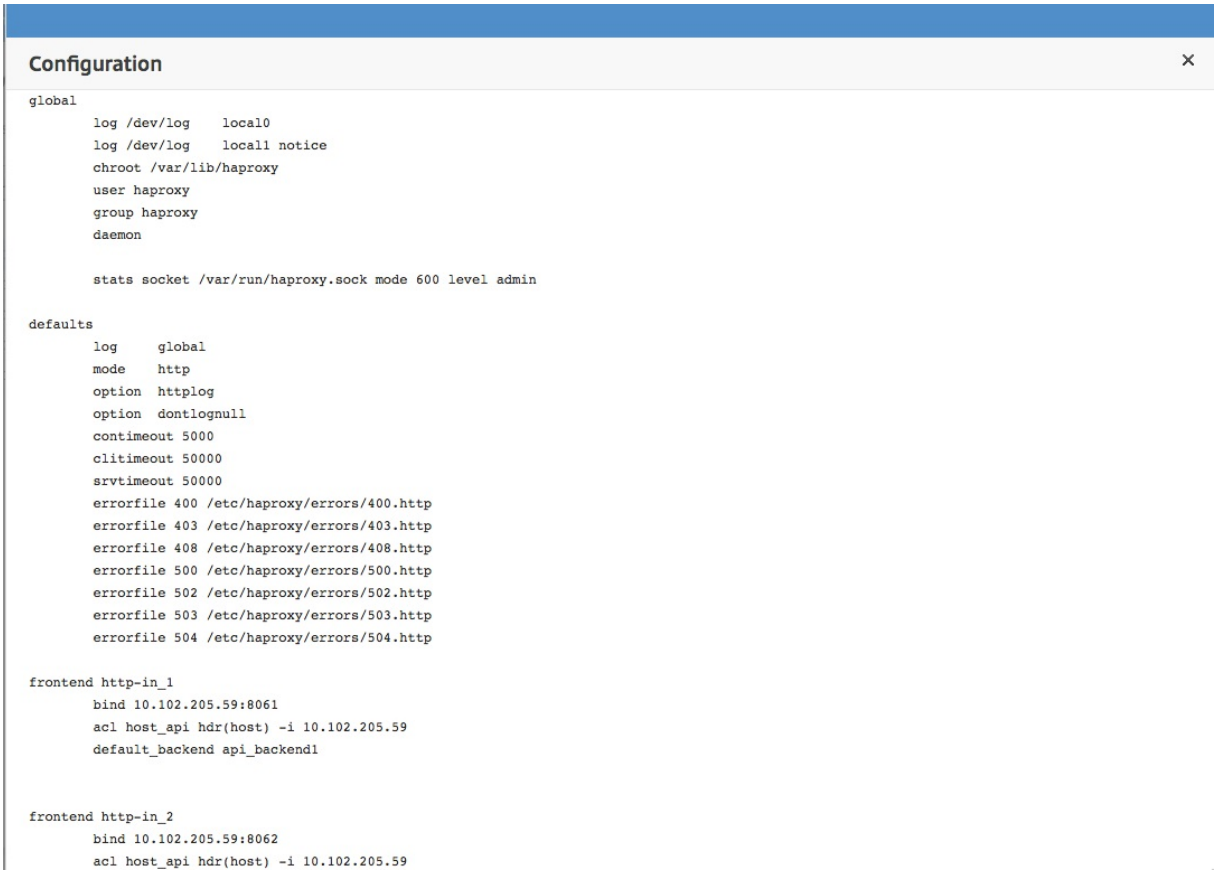
5.［**OK**］をクリックします。

NetScaler ADM は、ホスト上でプロビジョニングされた HAProxy インスタンスを検出し、［インスタンス］タブですべての HAProxy インスタンスを 表示できます。



HAProxy インスタンスの設定の表示

NetScaler ADM で HAProxy インスタンスの構成を表示するには、[ネットワーク] > [インスタンス] > [**HAProxy**] に移動し、[インスタンス] タブで HAProxy インスタンスを選択し、[構成の表示] をクリックします。



HAProxy アプリのダッシュボード

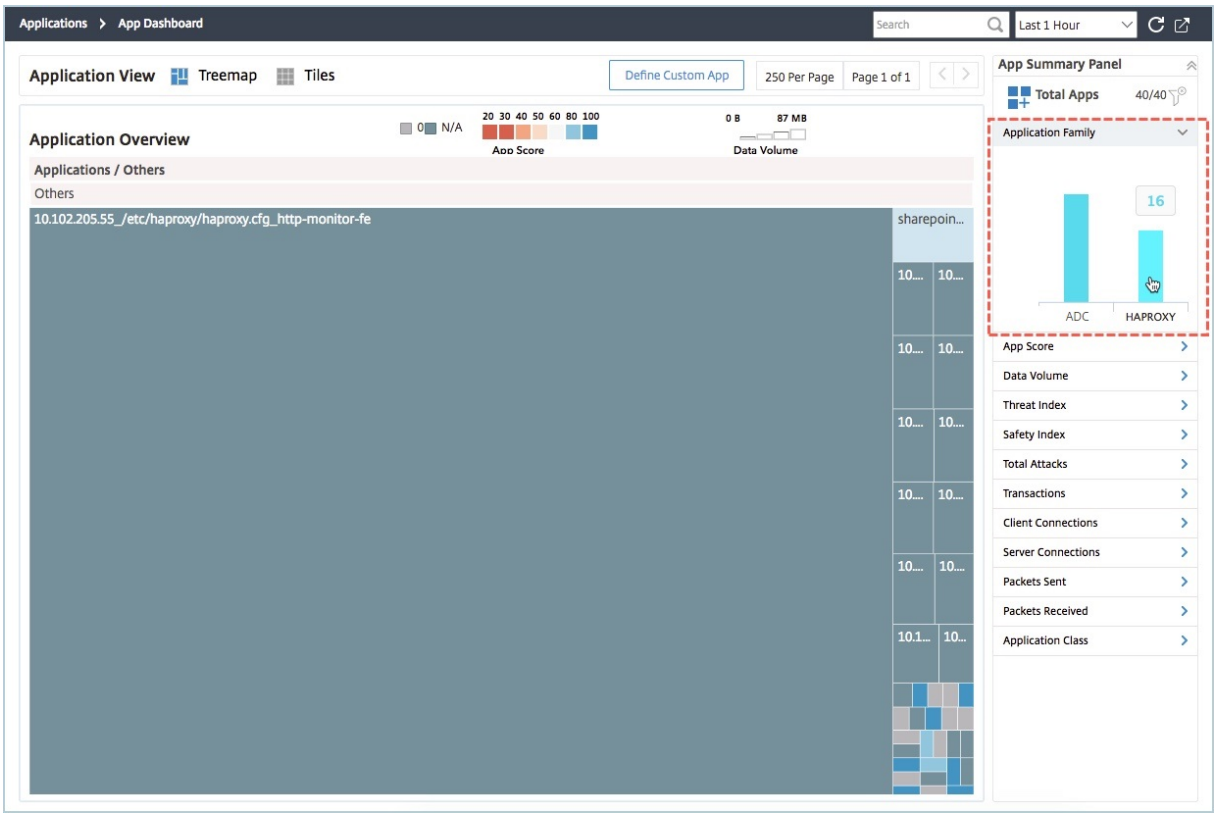
February 6, 2024

アプリケーションダッシュボードには、Citrix Application Delivery Management（Citrix ADM）によって監視されるすべての HAProxy フロントエンドのリアルタイム統計が表示されます。フロントエンドを個別のアプリケーションとして一覧表示して、アプリケーションのトランザクション、スループット、およびセッションの情報を提供します。

> 重要
>
> 必ず HAProxy インスタンス設定ファイルで **stats** を有効にしてください。統計情報を有効にするには、HAProxy 設定ファイルを編集し、default セクションの後に、次のサンプルのようなエントリを追加します。

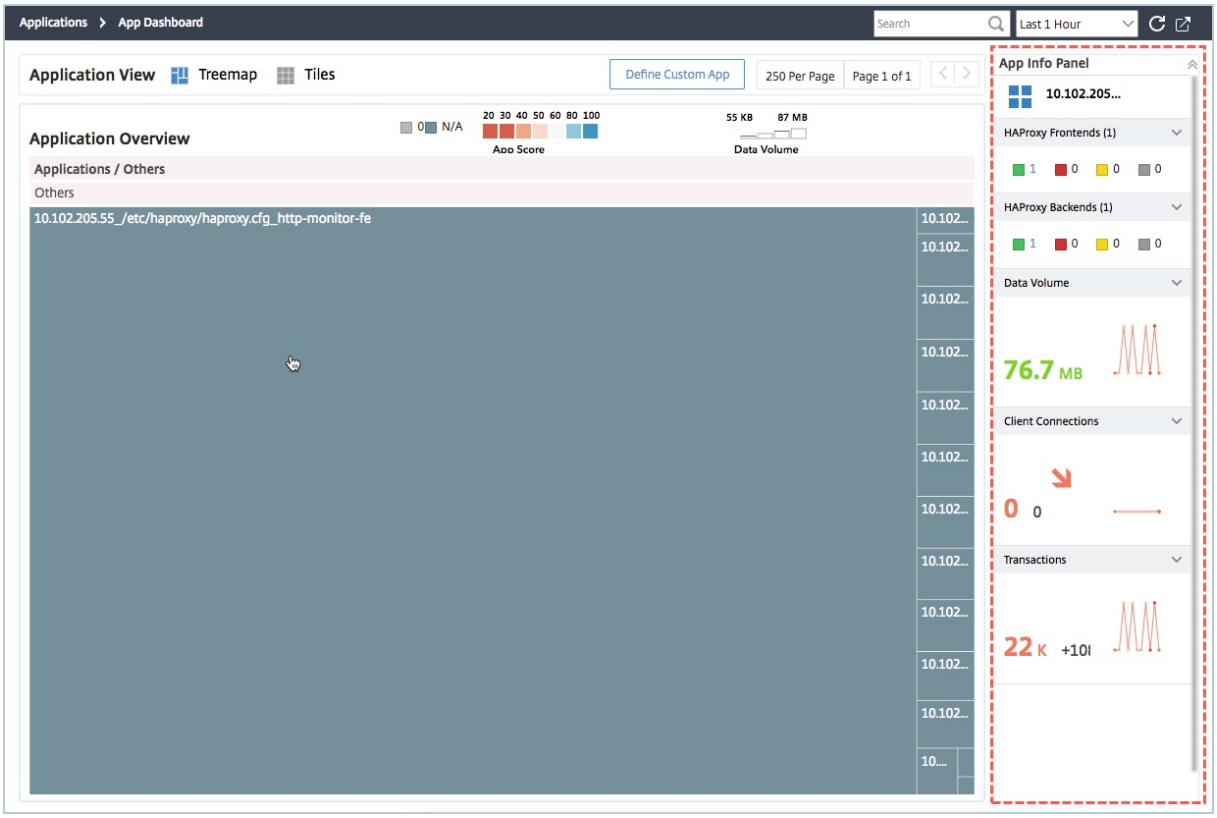
```
    listen stats :9000  # Listen on localhost:9000
    mode http
    stats enable  # Enable stats page
    stats hide-version  # Hide HAProxy version
    stats realm Haproxy\ Statistics  # Title text for popup window
    stats uri /haproxy_stats  # Stats URI
    stats auth Username:Password  # Authentication credentials
<!--NeedCopy-->
```

Citrix ADM のアプリケーションダッシュボードで HAProxy アプリケーションにアクセスするには、HAProxy インスタンスを Citrix ADM に追加した後、[アプリケーション] > [ダッシュボード] に移動します。HAProxy アプリケーションのみを表示するようにダッシュボードをフィルタリングできます。ダッシュボードをフィルタリングするには、「App Summary Info」パネルの「アプリケーションファミリー」セクションに表示される「**HAPPROXY**」を選択します。



HAProxy アプリケーションの主要なメトリックの表示

アプリケーション情報パネルは、HAProxy アプリケーションをドリルダウンするときの最初のレベルです。アプリケーションの状態とともに、主要な測定基準とコンポーネントが表示されます。たとえば、選択した HAProxy アプリケーションについて、アプリ情報パネルには HAProxy フロントエンドの総数、HAProxy バックエンドの総数、データ量、クライアント接続の傾向、およびトランザクションが表示されます。HAProxy アプリケーションの主要なメトリクスを表示するには、アプリケーションダッシュボードの HAProxy アプリケーションタイルをクリックします。[App Summary Panel] が [App Info Panel] に置き換わります。

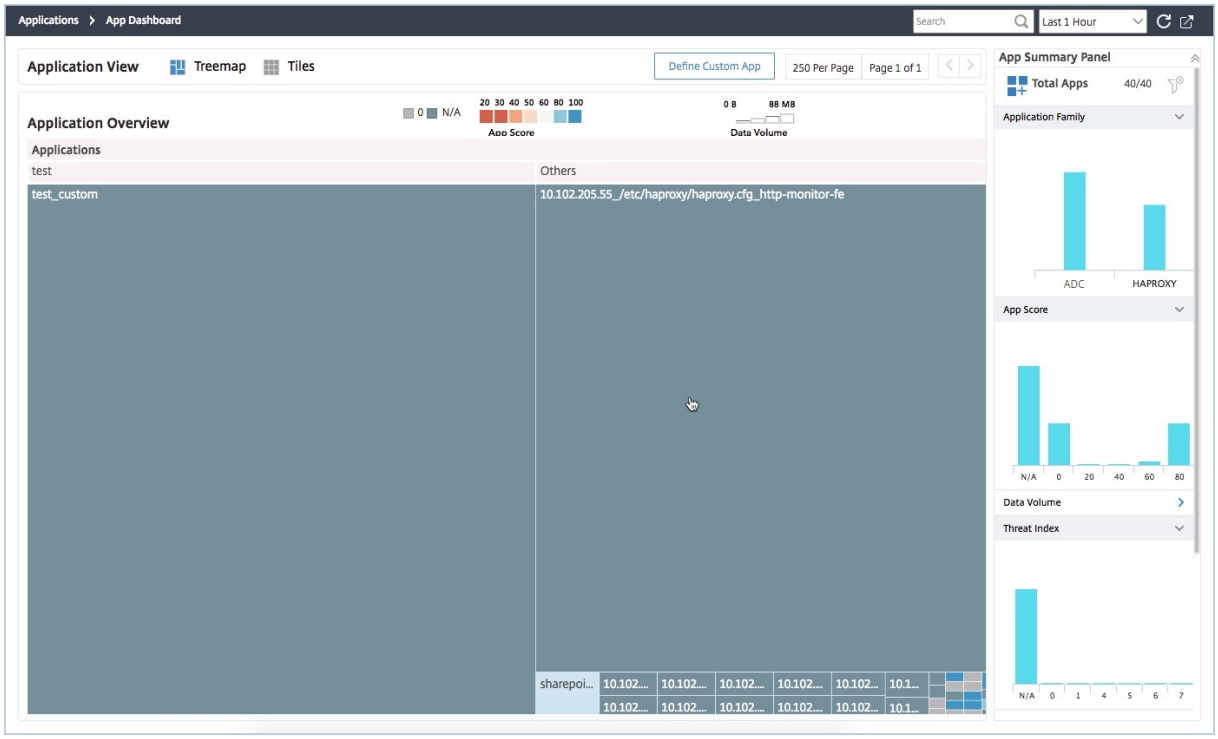


HAProxy アプリケーションのリアルタイムパフォーマンスを表示

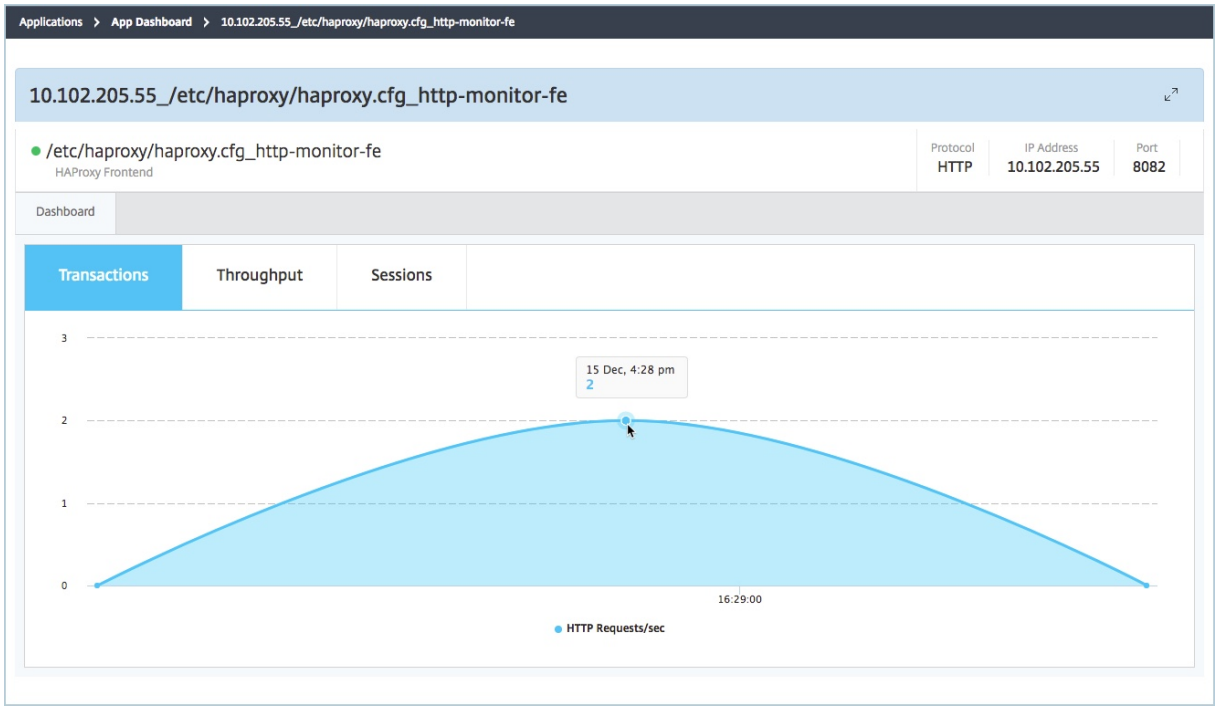
Citrix ADM では、HAProxy アプリケーションのパフォーマンスをリアルタイムで表示できます。選択した HAProxy アプリケーションの以下の詳細がリアルタイムで表示されます。

- 取引。アプリケーションが実行したトランザクション。
- スループット。アプリケーションのスループット。
- セッション。アプリケーションによって確立されたセッションの数。

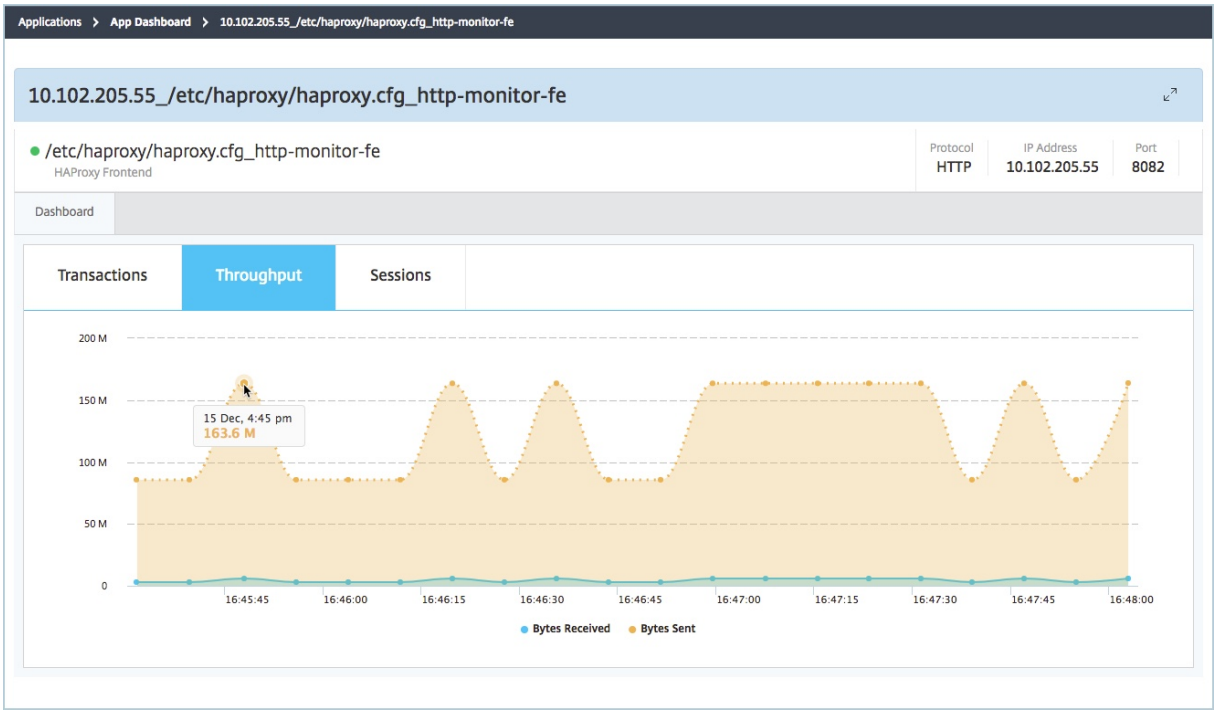
HAProxy アプリケーションのリアルタイムパフォーマンスを表示するには、アプリケーションダッシュボードで HAProxy アプリケーションタイルをダブルクリックします。



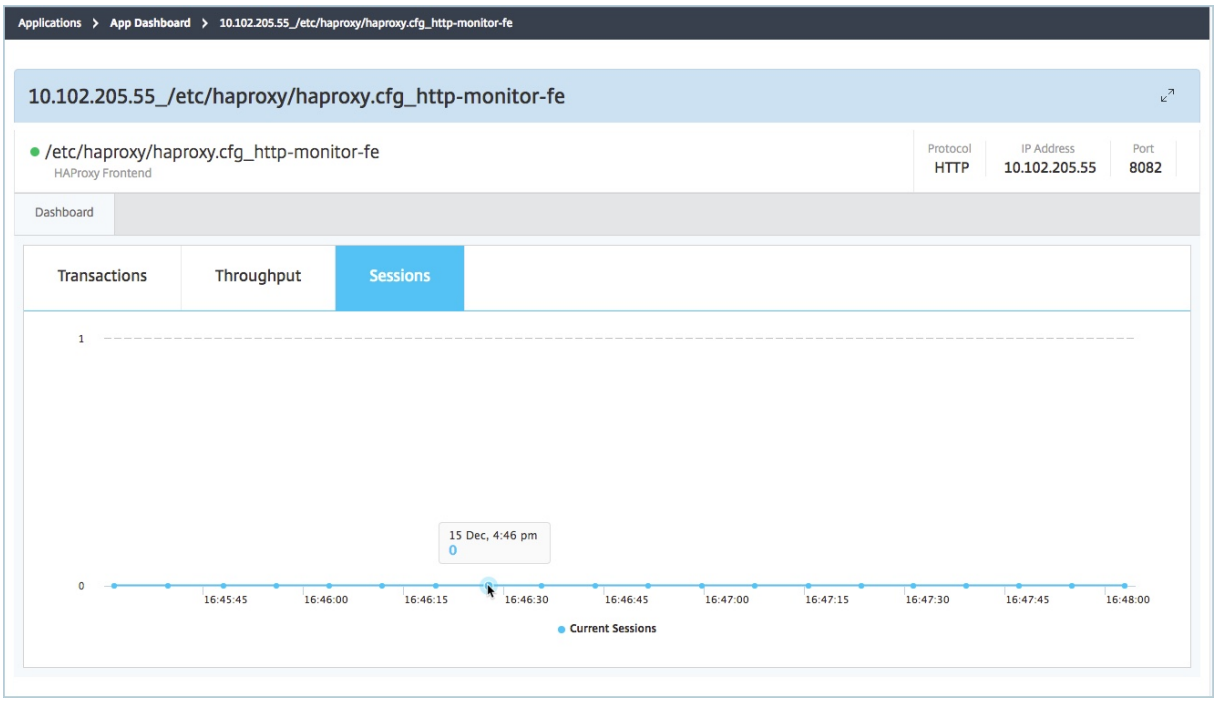
デフォルトでは、「トランザクション」タブが選択され、アプリケーションによって実行されたリアルタイムのトランザクションが表示されます。



アプリケーションのリアルタイムスループットを表示するには、[スループット] タブをクリックします。



[**Sessions**] タブをクリックすると、アプリケーションによって確立されたセッション数をリアルタイムで表示できます。

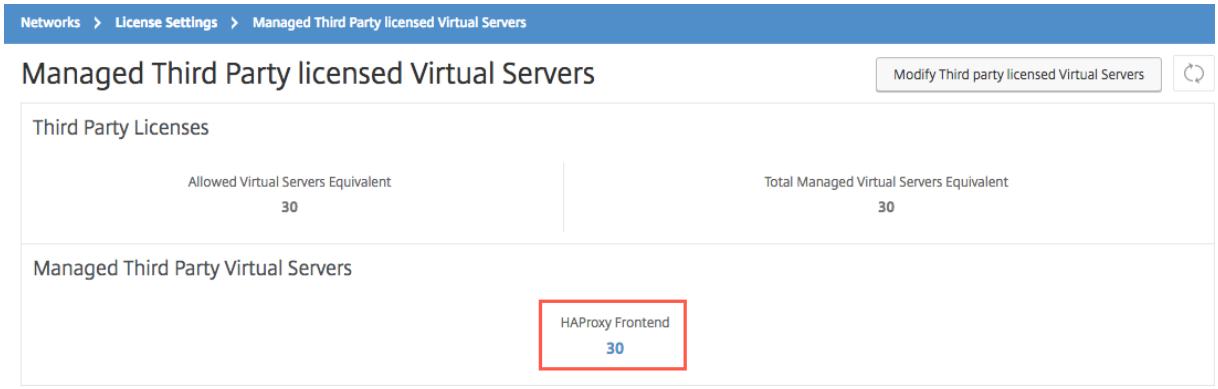


サードパーティライセンス

February 6, 2024

ホストを NetScaler Application Delivery Management（NetScaler ADM）に追加すると、NetScaler ADM はホスト上でプロビジョニングされた HAProxy インスタンスを自動的に検出し、NetScaler ADM インベントリに追加します。また、HAProxy インスタンスに構成されているすべてのフロントエンド、バックエンド、およびサーバーを検出し、フロントエンドを検出されたアプリケーションとみなします。

検出されたすべてのアプリケーションを管理、監視できますが、デフォルトでは、HAProxy App ダッシュボードには検出された 30 のアプリケーションのアプリケーション統計が表示されます。HAProxy App ダッシュボードについて詳しくは、「HAProxy App ダッシュボード」を参照してください。検出されたアプリケーションのアプリケーション統計を 30 を超えて表示する場合は、ライセンスを別途購入する必要があります。



追加のフロントエンド用ライセンスは、100 の仮想サーバーパックで使用できます。有効なライセンスを取得し、NetScaler ADM GUI を使用してライセンスをインストールできます。

サードパーティライセンスのインストール

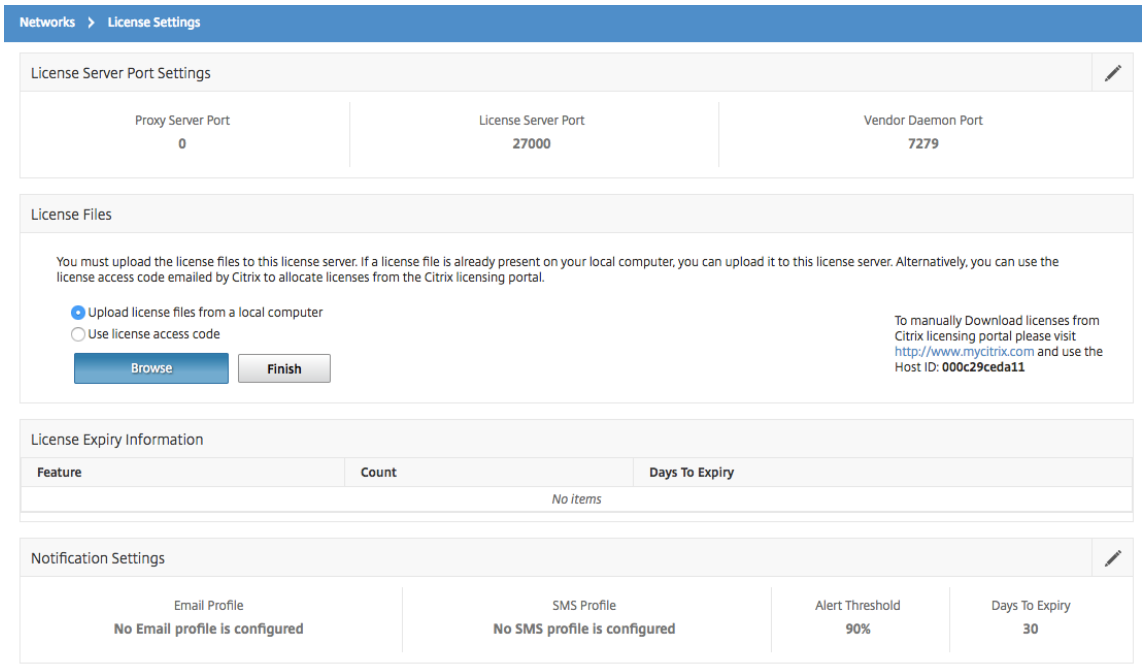
NetScaler ADM にライセンスをインストールすると、検出された 30 を超えるアプリケーションのアプリケーション統計を表示できます。

ライセンスをインストールするには以下を行います。

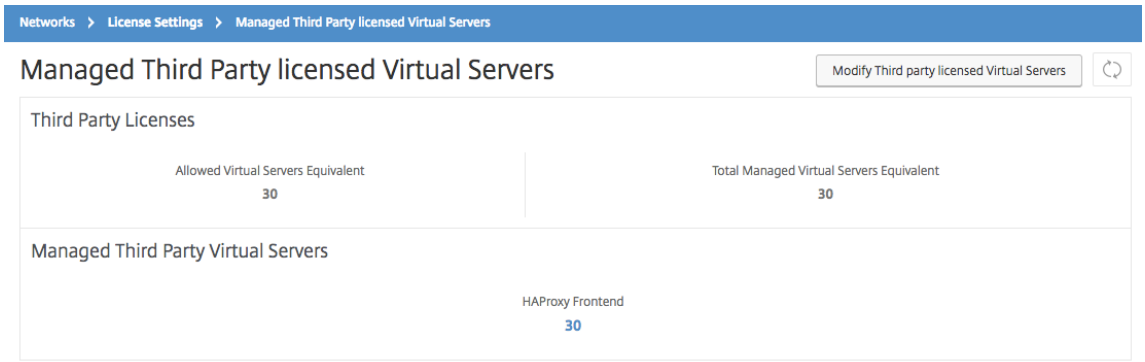
1. Web ブラウザーに **NetScaler Management and Analytics System** の IP アドレスを入力します（例: http://192.168.100.1）。
2. [**User Name**] と [**Password**] に管理者の資格情報を入力します。
3. [ネットワーク] > [ライセンス] に移動します。
4. 「ライセンスファイル」セクションで、次のオプションのいずれかを選択します。

- ローカルコンピューターからライセンスファイルをアップロードします。ライセンスが既にローカルコンピューターに存在する場合は、［Browse］をクリックし、ライセンスの割り当てに使用するライセンスファイル（.lic）を選択します。［完了］をクリックします。
- **Use License Activation Code** - 購入したライセンスのアクティブ化コード（LAC：License Activation Code）を、Citrix からメールで受け取ります。テキストボックスに LAC 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 Management and Analytics System がインターネットに接続されているか、またはプロキシサーバーが使用可能でなければなりません。



NetScaler ADM にインストールされているライセンスを確認するには、［ネットワーク］>［ライセンス］>［サードパーティライセンス **］の順に選択します。

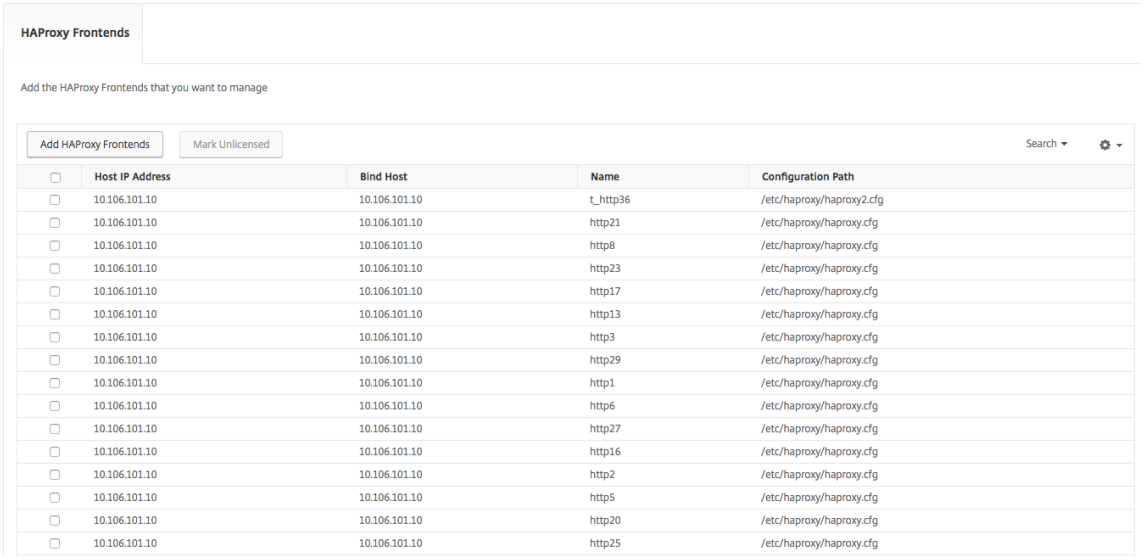


サードパーティライセンスの管理

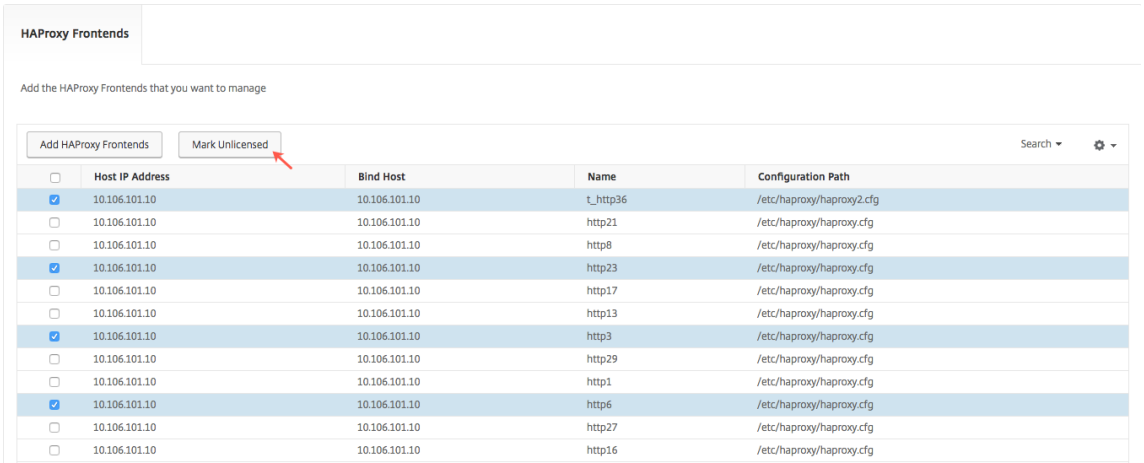
NetScaler ADM は、HAProxy インスタンスで検出されたアプリケーションをランダムに選択し、自動的にライセンスを取得します。選択された検出済みアプリケーションを変更する場合は、手動で、ライセンス許可された検出済みアプリケーションのライセンスを取り消してから、ライセンス許可する検出済みアプリケーションにライセンスを割り当てる必要があります。

サードパーティライセンスを管理するには、以下を行います。

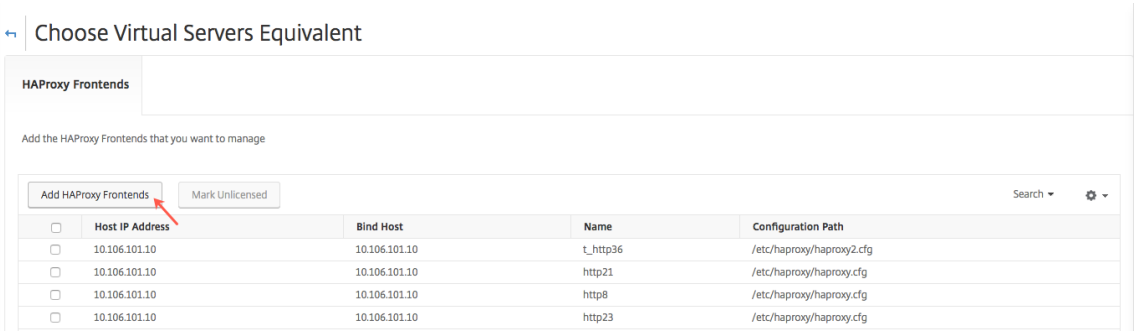
1. [ネットワーク] > [ライセンス] > [サードパーティライセンス] に移動し、[サードパーティライセンス仮想サーバーの変更] をクリックします。ダッシュボードに管理対象のフロントエンドが表示されます。



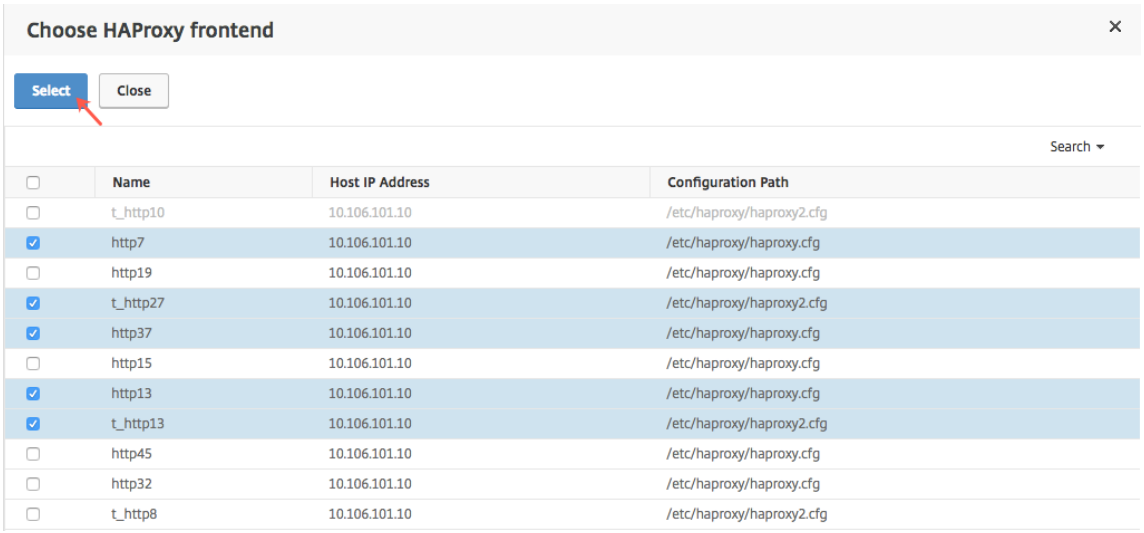
2. リストからフロントエンドを選択し、「ライセンスなしにする」を選択し、「完了」をクリックしてライセンスを解放します。



3. ライセンスを解放した後、または使用可能なライセンスをすでに持っている場合は、「**HAProxy** フロントエンドを追加」をクリックします。



4. 「**HAProxy** フロントエンドを選択」ダイアログで、ライセンスされていないフロントエンドをリストから選択し、「選択」をクリックします。



5. [今すぐ終了] をクリックします。

HAProxy インスタンスのロールベースのアクセス制御

February 6, 2024

Citrix Application Delivery Management（Citrix ADM）は、きめ細かなロールベースのアクセス制御（RBAC）を使用して構成オブジェクトへのアクセスを制御します。たとえば、ユーザーを作成して特定の HAProxy インスタンスへのアクセスを与えることができます。また［HAProxy App］ダッシュボードの表示/読み取り専用権限を指定できます。詳しくは、「NetScaler ADM の役割ベースのアクセス制御」を参照してください。

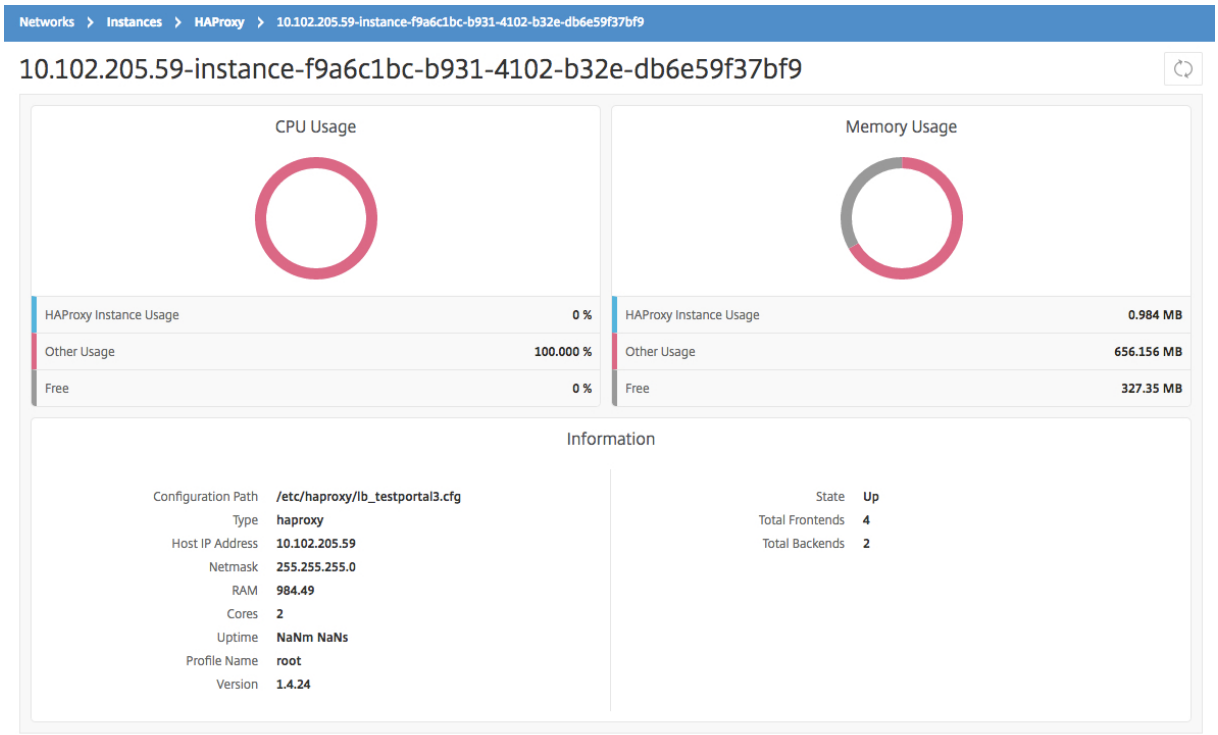
HAProxy インスタンスの監視

February 6, 2024

Citrix Application Delivery Management（Citrix ADM）の HAProxy ダッシュボードには、HAProxy インスタンスの CPU とメモリの使用状況を追跡するのに役立つグラフが表示されます。このダッシュボードには、次の内容を示すグラフも表示されます。

- ホスト上の HAProxy インスタンスによって使用されている CPU の割合
- ホスト上の他のエンティティによって使用されている CPU の割合
- ホスト上の残りの CPU の割合
- ホスト上の HAProxy インスタンスによって使用されているメモリの割合
- ホスト上の他のエンティティによって使用されているメモリの割合
- ホスト上の残りのメモリの割合

NetScaler ADM で HAProxy インスタンスを監視するには、［ネットワーク］>［インスタンス］>［**HAProxy** ］>［インスタンス］タブに移動し、HAProxy インスタンスを選択し、［ダッシュボード］をクリックします。



HAProxy インスタンスに設定されたフロントエンドの詳細を表示する

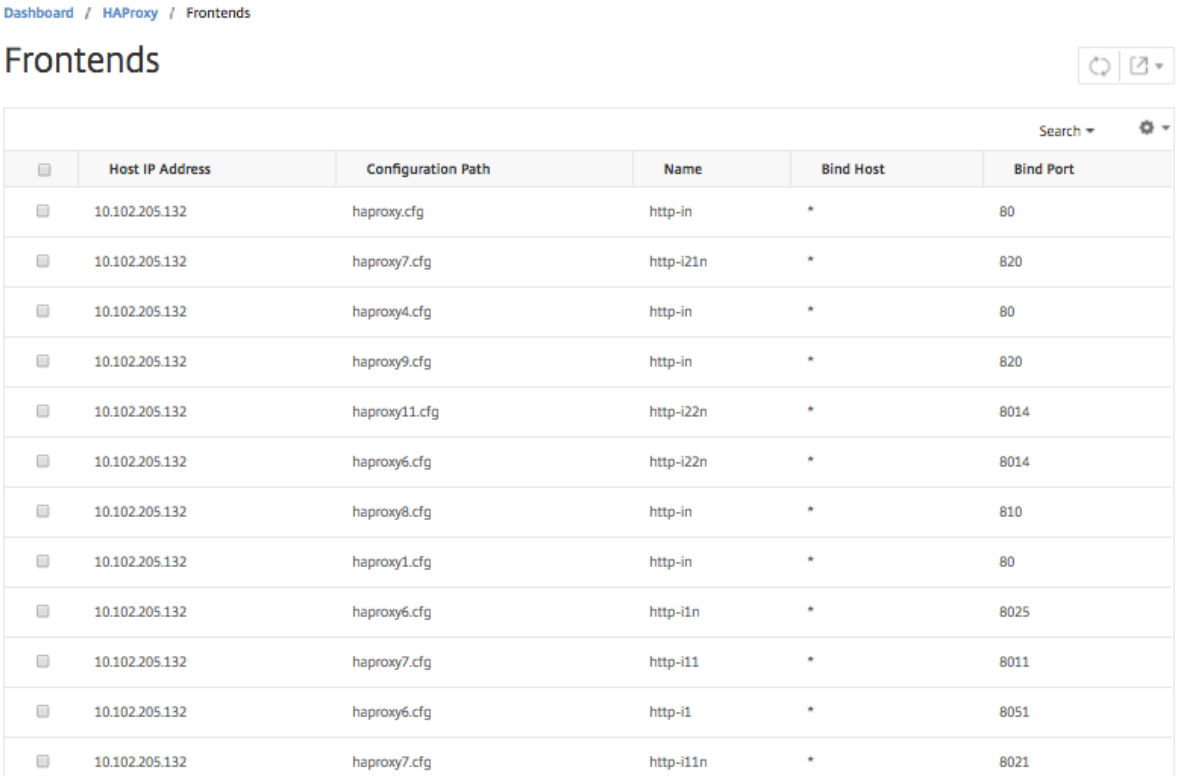
February 6, 2024

Citrix Application Delivery Management（Citrix ADM）は、HAProxy インスタンス上に構成されたフロントエンドに関する以下の詳細を報告します。

- ホストの **IP** アドレス。ホストの IP アドレス
- 設定パス。ホスト上の HAProxy インスタンスの絶対設定パス。
- 名前。受信トラフィックを処理するフロントエンドの名前。
- **[** ホストのバインド**]**。フロントエンドのバインド先の IP アドレス。
- バインドポート。フロントエンドのバインド先のポート。

HAProxy インスタンス上で構成されているフロントエンドを表示するには、次の手順に従います。

NetScaler ADM で、［ネットワーク］>［ネットワーク機能］**>**［**HAProxy**］**>**［フロントエンド］に移動します。



HAProxy インスタンスに設定されたバックエンドの詳細を表示する

February 6, 2024

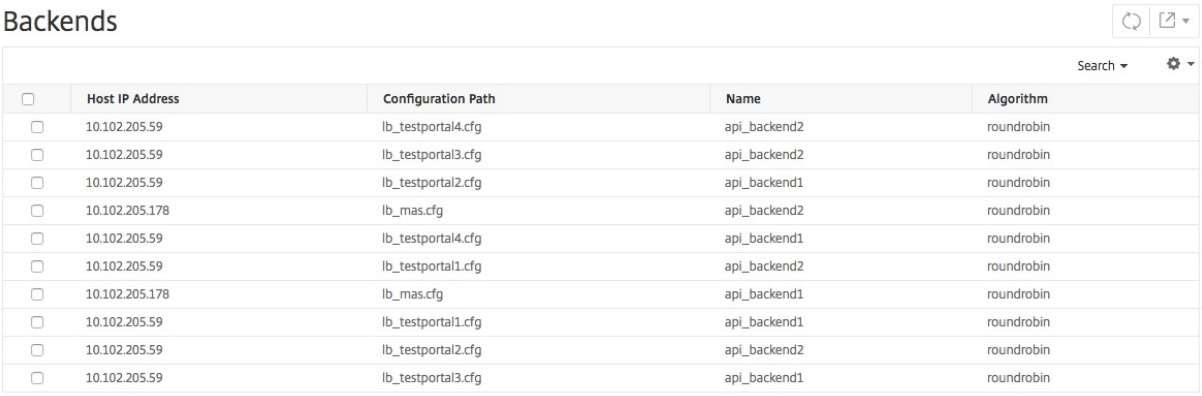
Citrix Application Delivery Management（Citrix ADM）は、HAProxy インスタンス上に構成されたバックエンドアプリケーションの次の詳細を報告します。

- ホストの **IP** アドレス。ホストの IP アドレス。
- 設定パス。ホスト上の HAProxy インスタンスパス。

- 名前。トラフィックの転送先のバックエンドの名前。
- アルゴリズム。トラフィックを分散させるために使用する負荷分散アルゴリズムです。

HAProxy インスタンス上で構成されているバックエンドを表示するには、次の手順に従います。

NetScaler ADM で、［ネットワーク］>［ネットワーク機能］>［**HAProxy**］>［バックエンド］に移動します。



HAProxy インスタンスで設定されたサーバーの詳細の表示

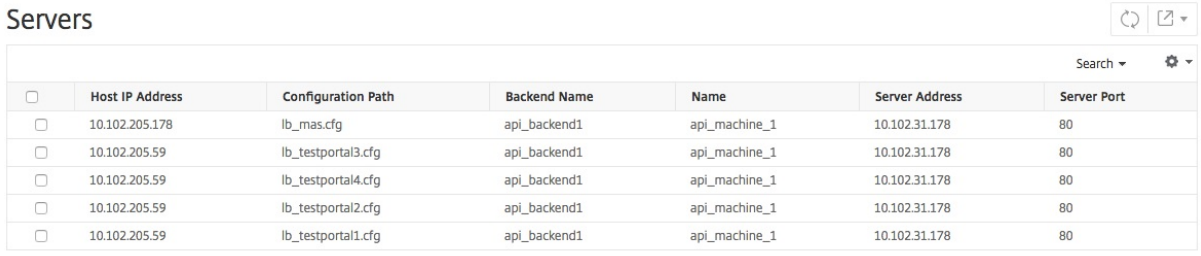
February 6, 2024

Citrix Application Delivery Management（Citrix ADM）は、HAProxy インスタンス上に構成されたサーバーに関する以下の詳細を報告します。

- ホストの **IP** アドレス。ホストの名前です。
- 設定パス。ホスト上の HAProxy インスタンス構成ファイルの絶対パスです。
- バックエンド名。HAProxy 構成内のバックエンドの名前です。
- 名前。HAProxy 構成内のサーバーの名前です。
- サーバーアドレス。サーバーの IP アドレスです。
- サーバーポート。サーバーによって使用されるポートです。

HAProxy インスタンス上で構成されているサーバーを表示するには、次の手順に従います。

NetScaler ADM で、[ネットワーク**] > [**** ネットワーク 機能 **] > [**HAProxy**] > [サーバー] に移動します。

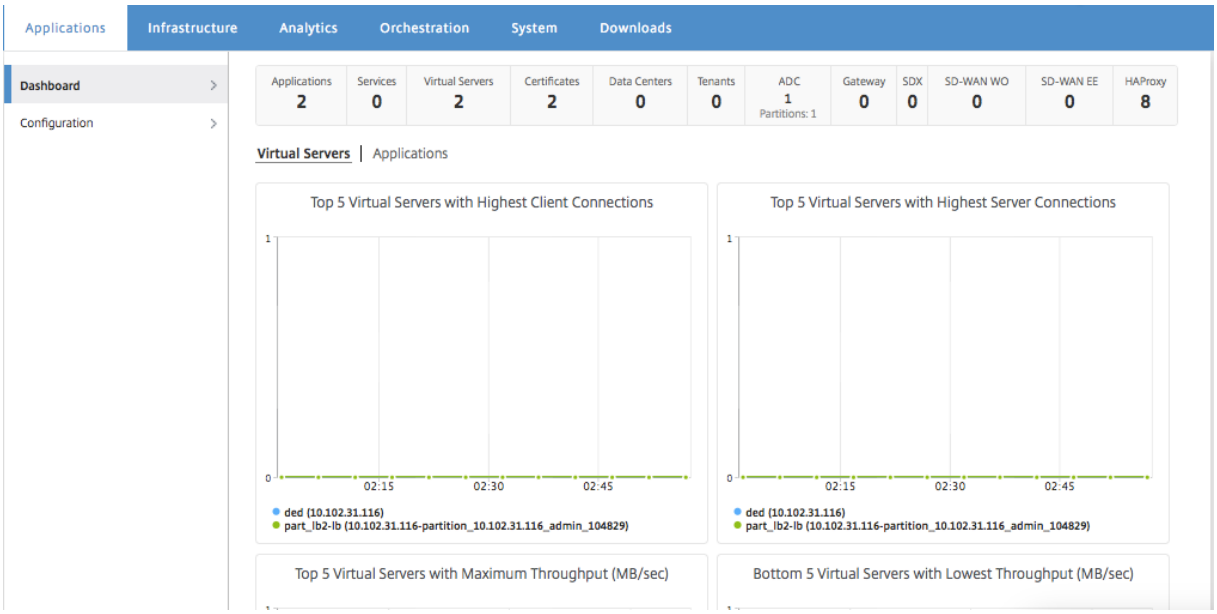


フロントエンドまたはサーバーの数が最も多い **HAProxy** インスタンスを表示する

February 6, 2024

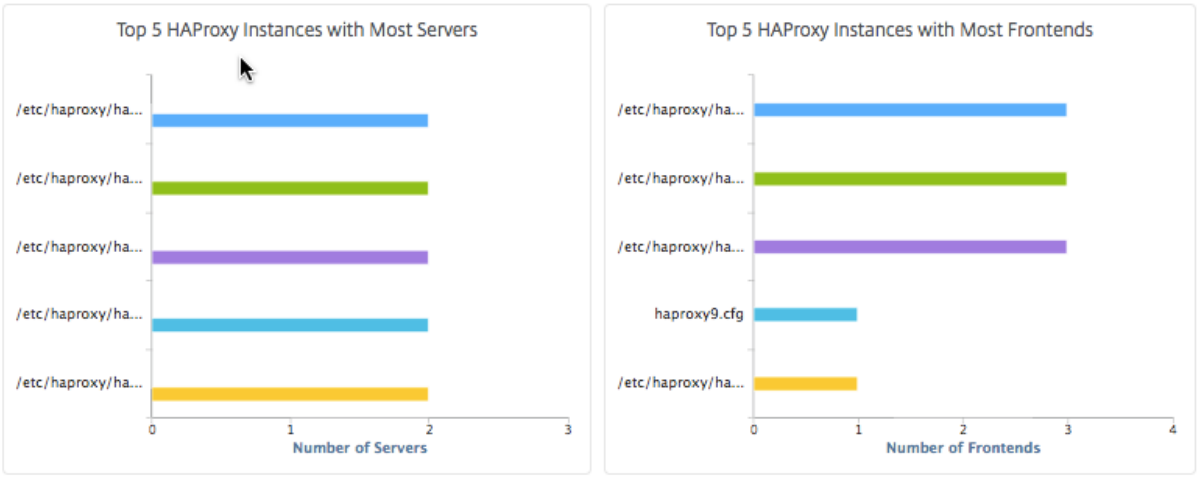
アプリケーションダッシュボードには、Citrix Application Delivery Management（Citrix ADM）は、検出した HAProxy インスタンスの数を表示し、フロントエンドまたはサーバーの数が最も多い上位 5 つの HAProxy インスタンスを一覧表示します。

アプリケーションダッシュボードを表示するには、Citrix ADM で［アプリケーション］>［ダッシュボード］に移動します。



Citrix ADM によって検出された HAProxy インスタンスの数は、以下のように一番上の行に表示されます。

最も多くのフロントエンドまたは最も多くのサーバーで構成されている HAProxy インスタンスの上位 5 台の一覧を表示するには、ダッシュボードを下方向にスクロールします。



HAProxy インスタンスを再起動する

February 6, 2024

Citrix Application Delivery Management（Citrix ADM）GUI から HAProxy インスタンスを再起動するには、ハードリスタートまたはソフトリスタートを選択できます。

ハードリスタート

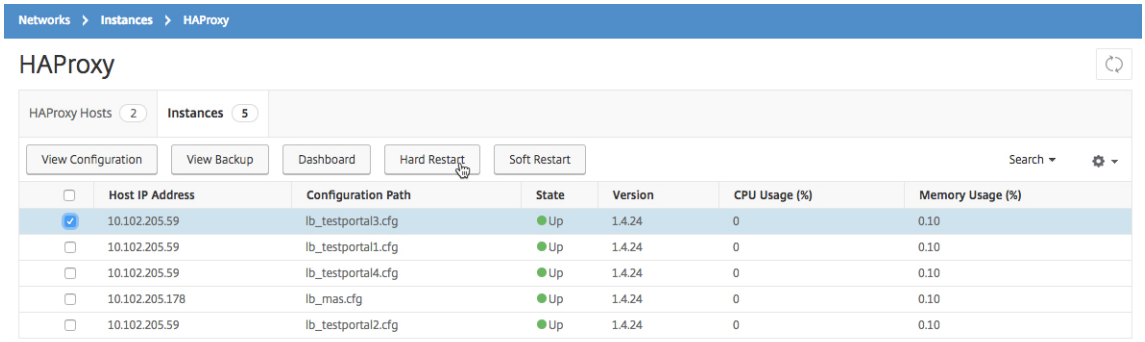
ハード再起動では、インスタンス上の HAProxy プロセスが終了され、確立されている接続がすべて閉じられます。再起動後、新しい HAProxy プロセスが作成され、後続の新しい接続は、その新しい HAProxy プロセスによって処理されます。

ソフト再起動

ソフト再起動では、HAProxy プロセスがリスナーポートからバインド解除されますが、既存の接続は、閉じられるまで HAProxy プロセスによって引き続き処理されます。新しい接続を処理するために新しい HAProxy プロセスが作成されます。

HAProxy インスタンスを再起動するには、次の手順に従います。

1. [ネットワーク] > [インスタンス] > **[**HAProxy**]** に移動し、[インスタンス] タブをクリックします。
2. [インスタンス] タブで、再起動する HAProxy インスタンスを選択します。
3. 「ハード再起動」をクリックして HAProxy インスタンスをハード再起動するか、「ソフト再起動」をクリックして HAProxy インスタンスをソフト再起動します。



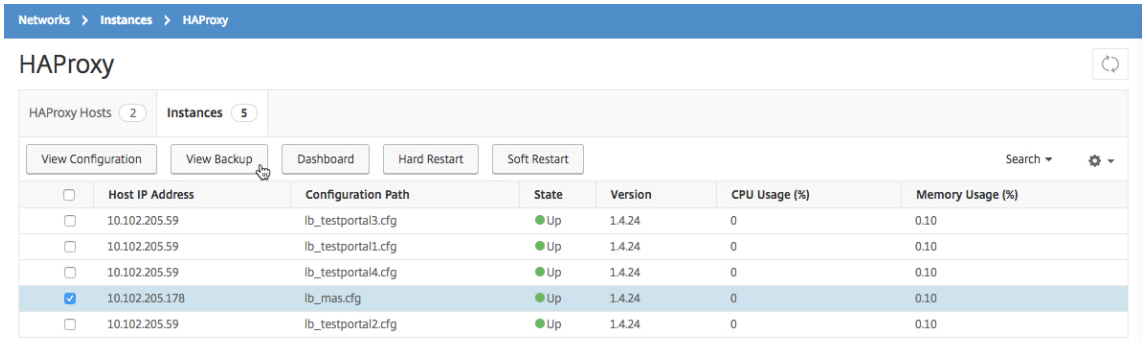
HAProxy インスタンスのバックアップと復元

February 6, 2024

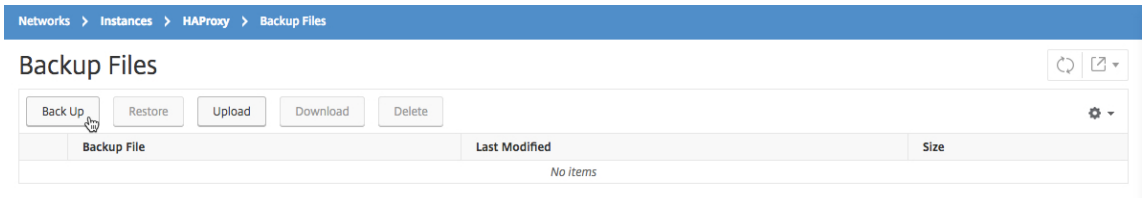
HAProxy 構成ファイルの HAProxy インスタンスの現在の状態をバックアップすることができます。インスタンスが不安定になった場合は、バックアップファイルを使用して、インスタンスを安定な状態に戻すことができます。

NetScaler ADM を使用して **HAProxy** インスタンスをバックアップするには:

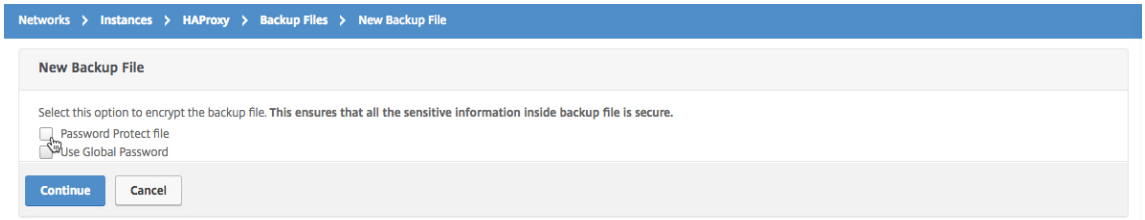
1. Citrix Application Delivery Management（Citrix ADM）で、[ネットワーク] **>** **[**インスタンス**]** **>** **[HAProxy**] に移動します。
2. **HAProxy** ページで、「インスタンス」タブをクリックします。
3. バックアップする HAProxy インスタンスを選択し、[バックアップの表示] をクリックします。



4.「バックアップファイル」ページで、「バックアップ」をクリックします。



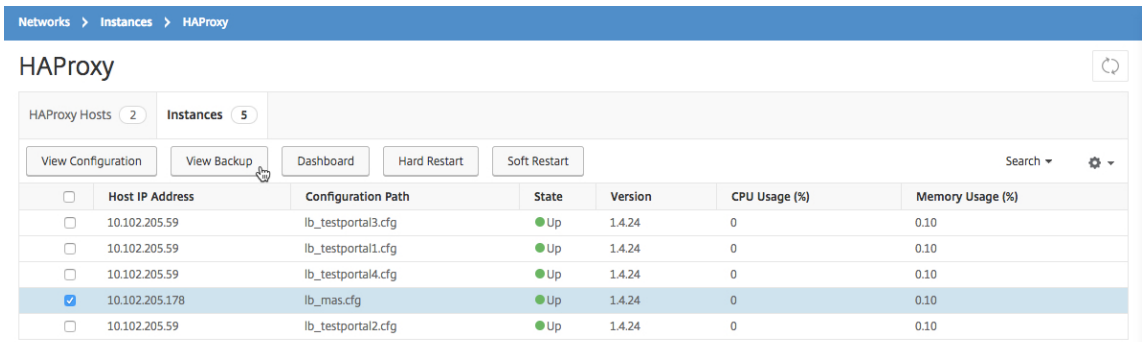
5. バックアップファイルの暗号化を選択して、セキュリティを高めることもできます。



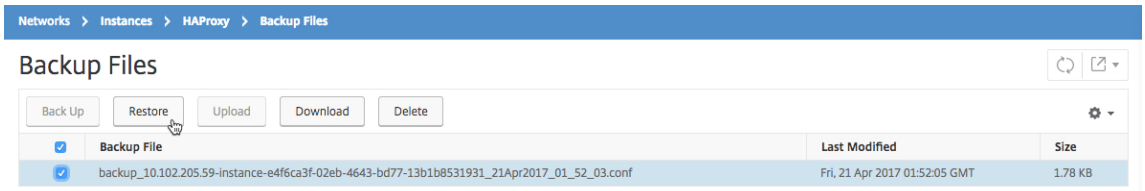
6. [続行] をクリックします。

NetScaler ADM を使用してインスタンスを復元するには:

1. [ネットワーク] > [インスタンス] > **[****HAProxy**] に移動します。
2. **HAProxy** ページで、「インスタンス」タブをクリックします。
3. 復元するインスタンスを選択し、[**View Backup**] をクリックします。



4. [**Backup Files**] ページで、復元するバックアップファイルを選択し、[**Restore**] をクリックします。



> 注
>
> インスタンスを復元すると、NetScaler ADM ソフトは HAProxy インスタンスを再起動します。

HAProxy 設定ファイルを編集します

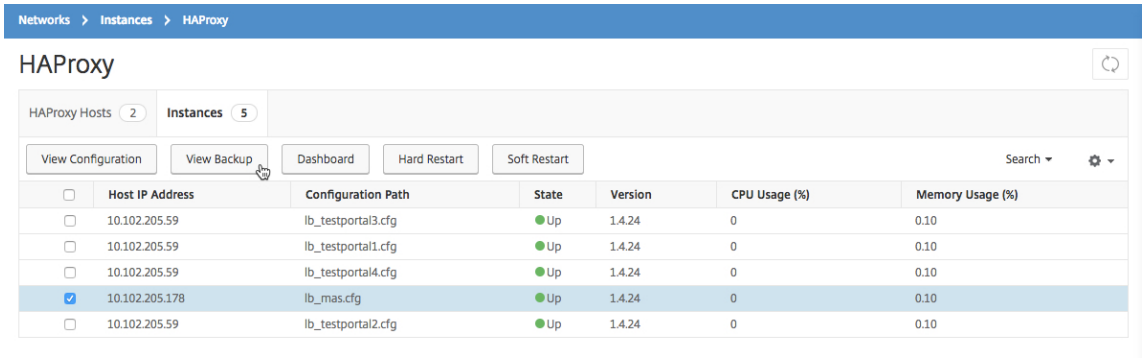
February 6, 2024

既存の HAProxy 構成ファイル内のフロントエンド設定、バックエンド設定、サーバー設定、およびその他の設定を更新できます。HAProxy 構成ファイルを編集するには、次の手順に従います。

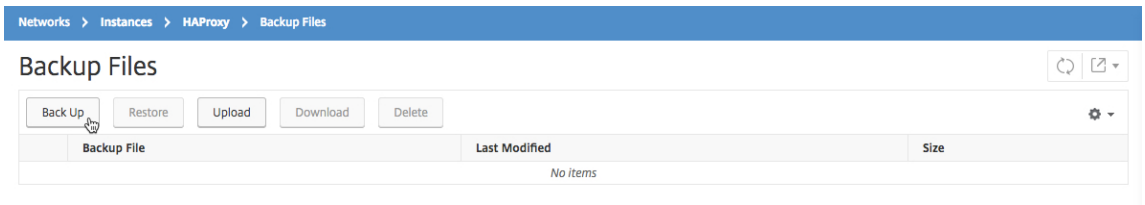
- HAProxy 構成ファイルをバックアップします。
- バックアップの HAProxy 構成ファイルをダウンロードし、オフラインで編集します。
- 更新された HAProxy 構成ファイルを Citrix Application Delivery Management (Citrix ADM) にアップロードします
- 更新したバックアップファイルを使用して HAProxy インスタンスを復元します。

NetScaler ADM を使用して **HAProxy** 構成ファイルを編集するには:

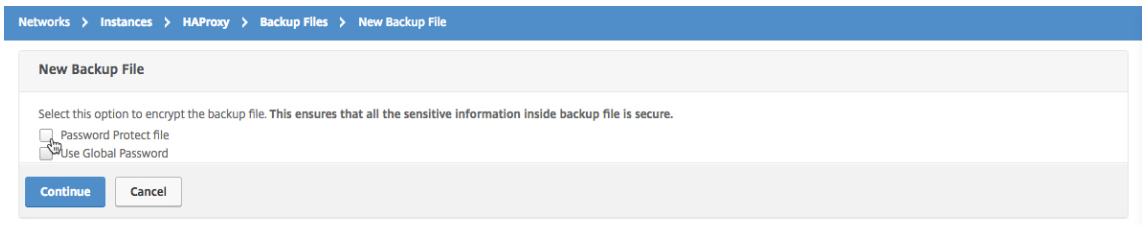
1. Citrix ADM で、[ネットワーク] > [インスタンス] > **[****HAProxy**] に移動します。
2. **HAProxy** ページで、「インスタンス」タブをクリックします。
3. バックアップする HAProxy インスタンスを選択し、[バックアップの表示] をクリックします。



4. [**Backup Files**] ページで [**Back Up**] をクリックします。

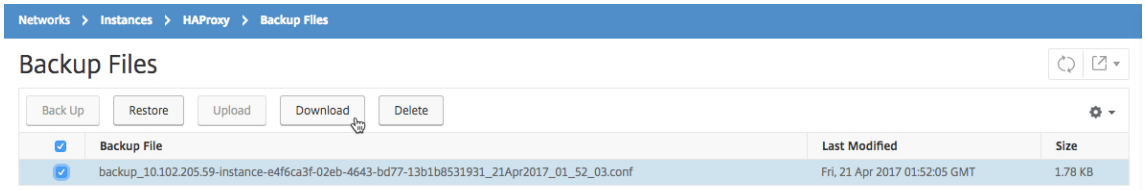


5. [続行] をクリックします。

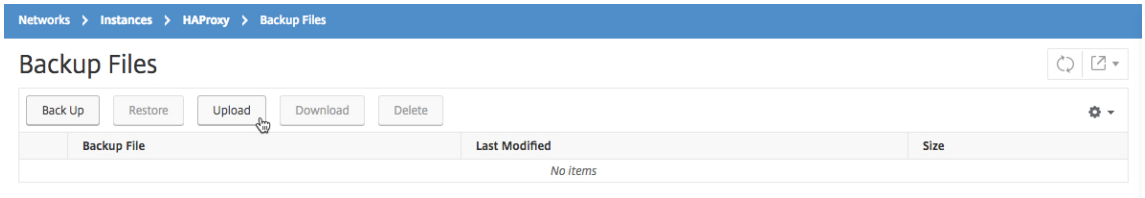


> 注
>
> バックアップファイルを暗号化しないでください。

6. [バックアップファイル] ページで、バックアップファイルを選択し、[ダウンロード] をクリックします。



7. テキストエディターを使用して、HAProxy 構成ファイルを編集します。
8. 「バックアップファイル」ページで「アップロード」をクリックして、更新された HAProxy 設定ファイルを参照して選択します。



   更新された HAProxy 設定ファイルがアップロードされると、[バックアップファイル] ページに表示されます。

9. 更新された HAProxy 設定ファイルを選択し、「復元」をクリックします。

システム設定の管理

February 6, 2024

次の表では、Citrix ADM のシステム設定を構成する方法について説明します。

あなたがしたいなら…	これを…
今日のメッセージの設定	Citrix ADM でウェルカムメッセージを作成できるようになりました。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。[システム] > [** システム **** 設定 **] に移動し、[** 今日のメッセージの設定 **] をクリックします。「** 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、「**OK**」をクリックします。
Citrix ADM をシャットダウンする	** [System] **>** [System Administrations] ** の順に選択します。「Citrix ADM を ** シャットダウン」をクリックすると、Citrix ADM** を完全にシャットダウンできます。** 注 **: Citrix ADM をシャットダウンすると、Citrix ADM をインストールしたハイパーバイザーからのみ再起動できます。
セットアップウィザード設定の構成	** [System] **>** [System Administrations] ** の順に選択します。「**Citrix ADM セットアップ」で **、「セットアップウィザード ** 設定 **」を選択します。**Citrix ADM ネットワーク ** オプションを選択して、Citrix ADM の IP アドレスやパスワードなどのネットワーク設定を変更できます。** システム設定 ** をクリックして、ホスト名、インスタンスとの通信モード、またはローカルタイムゾーンを変更できます。

ネットワーク設定を構成する	**［System］**>**［System Administrations］** の順に選択します。「**Citrix ADM のセットアップ」で **、「** ネットワーク ** 構成」を選択します。GUI には、Citrix ADM にインストールされている SSL 証明書とキーが表示されます。
SSL 証明書の表示	**［System］**>**［System Administrations］** の順に選択します。「**Citrix ADM のセットアップ」で **、「**SSL 証明書を表示 **」を選択します。GUI には、Citrix ADM にインストールされている SSL 証明書とキーが表示されます。
タイムゾーンの変更	[システム] > **[** システム **** 管理] に移動します。[** システム設定 **] で、[タイム ** ゾーンの変更] を ** 選択します。タイムゾーンドロップダウンリストから **、Citrix ADM アプライアンスの ** 時計のタイムゾーンを選択します。
ホスト名の変更	**［System］**>**［System Administrations］** の順に選択します。** ［System Settings］** の **［Change Hostname］** を選択します。Citrix ADM Gateway のユニバーサルライセンスを生成するときに、そのホスト名がライセンスに表示されるように、Citrix ADM 識別に使用するホスト名を入力します。
システム設定の変更	[システム] > **[** システム **** 管理] に移動します。[** システム設定 **] で、[システム設定の ** 変更 **] を選択します。次に、チェックボックスをオンまたはオフにして、次の機能を 有効または無効にします。[セキュアアクセスのみ]、[セッションタイムアウトを有効にする]、[基本認証を許可]、[nsrecover ログインを有効にする]、[証明書のダウンロードを有効にする]、[nsroot 以外のユーザーのシェルアクセスを有効にする]、[インスタンスログイン用のユーザー認証情報の入力を促す]
SSL 設定の構成	**［System］**>**［System Administrations］** の順に選択します。[** システム設定 **] で [**SSL 設定 ** の構成] を選択すると、現在のプロトコル設定と適用されている暗号スイートが表示されます。いずれかの設定を変更する場合は、[設定の ** 編集] で [** プロトコル ** 設定 **] または [** 暗号スイート **] を選択します。
ユーザーエクスペリエンス向上設定機能を有効にする	**［System］**>**［System Administrations］** の順に選択します。[** システム設定 **] で、[** ユーザエクスペリエンス向上設定 ** の構成] を選択し、[**CUXIP を有効にする **] チェックボックスを選択します。このチェックボックスを選択すると、グラフィカルユーザーインターフェイス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。
NetScaler ADM アップグレード	**［System］**>**［System Administrations］** の順に選択します。「** システム ** 管理」小見出しで、「**Citrix ADM のアップグレード **」を選択し、新しいイメージファイルを選択します。Citrix ADM 仮想 アプライアンスにすでに存在するファイルを選択するか、ローカルコンピューターからファイルをアップロードできます。
Citrix ADM を再起動する	**［System］**>**［System Administrations］** の順に選択します。「** システム ** 管理」サブ見出しで、「**Citrix ADM の再起動 **」を選択します。アクションの確認を求めるダイアログボックスが開きます。**［はい］** をクリックします。
システムプルーニングの設定 (古いデータのプルーニング用)	**［System］**>**［System Administrations］** の順に選択します。** プルーニング設定 ** で、システムプルーニング設定を選択 ** します **。［Data to keep (days)］フィールドに、システムでデータを保持する日数を入力します。
システムバックアップ設定の構成	**［System］**>**［System Administrations］** の順に選択します。「** バックアップ設定 **」で、「** システムバックアップ設定 **」を選択し、Citrix ADM アプライアンスに保持するシステムバックアップ の数を入力します。また、バックアップファイルを暗号化することや、バックアップファイルの

転送先となる外部の場所を指定することもできます。転送されたバックアップファイルはシステムで保持できます。また、システムから削除できます。|

| インスタンスバックアップ設定の構成 | ** ［System］**>** ［System Administrations］** の順に選択します。「** バックアップ設定 **」で、「インスタンス ** バックアップ設定 **」を選択し、Citrix ADM によって管理されるすべてのインスタンスをバックアップするバックアップファイルを作成する時間間隔（時間単位）を 入力します。保持するバックアップファイルの数と、パスワードがないとアクセスできないように暗号 化するかどうかを指定できます。|

| システム統計の表示 | [** システム **] > [** 統計 **] に移動します。CPU、メモリ、ディスクの使用状況など、情報の折れ線グラフが表示されます。|

| セッションの表示と管理 | [** システム **] > [** セッション **] に移動します。すべてのアクティブセッションを詳細と共に確認できます。セッションを終了するには、そのチェックボックスを選択して、「** セッションをキャンセル **」をクリックします。|

| テナントの追加または変更 | [** システム **] > [** テナント **] に移動し、新しいテナントを追加するか、既存のテナントの設定を編集します。テナントの組織単位名や部署、URL などの追加情報を設定できます。|

| ユーザーロックアウトポリシーの変更 | [** システム **] > [** ユーザー ** 管理] に移動します。「** ユーザー構成 **」で、「** ユーザー・ロックアウト ** 構成」を選択し、「ユーザー・** ロックアウトを有効にする ** 」チェック・ボックスを選択します。アカウントが無効になるまでにユーザーが実行できる無効 な試行の回数と、ユーザーロックアウトポリシーが有効な期間を指定できます。|

| パスワードの複雑さに関する変更 | [** システム **] > [** ユーザー ** 管理] に移動します。「** ユーザーの構成 **」で「** パスワードポリシー **」を選択し、「パスワードの ** 複雑さを有効にする ** 」チェックボックスを選択します。[** パスワードの最小文字数 ** ］フィールドに、Citrix ADM のパスワードに必要 な最小文字数を入力します。|

| ユーザーの追加または変更 | [** システム **] > [ユーザー管理] > [** ユーザー **] に移動します。「ユーザー」で、新しいユーザーを追加するか、既存のユーザーの設定を編集します。ユーザーを追加するときに、外部 認証、セッションタイムアウト、特定のグループへのユーザーの割り当てなどのオプションを有効にできます。|

| ユーザーグループの追加または変更 | [** システム **] > [** ユーザー管理 **] > [** グループ **] に移動します。[** グループ **] で、新しいグループを追加するか、既存のグループの設定を編集します。グループを追加するときに、グループへの権限の割り当て、セッションタイムアウトの構成、グループへのユーザーの割り当て、Citrix ADM 上の特定またはすべてのアプリケーションへのアクセスの 許可などのオプションを有効にできます。|

| 認証構成の変更 | [** システム **] > [認証] > [** 認証 **] ** に ** 移動します。[** 認証 **] で [** 認証設定 **] を選択し、認証サーバーの種類を選択します。|

| RADIUS サーバーの追加または変更 | [** システム **] > [** 認証 **] > [**RADIUS**] に移動します。[**RADIUS**] で、新しい RADIUS サーバを追加するか、ネットワークパラメータを 入力または変更して既存の RADIUS サーバの設定を編集します。|

| LDAP サーバーの追加または変更 | ［System］> ［Authentication］> ［LDAP］の順に選択します。LDAP で、新しい LDAP サーバーを追加するか、ネットワークパラメーターを入力 または変更して既存の LDAP サーバーの設定を編集します。|

| TACACS サーバを追加または変更する | [** システム **] > [認証] > **[****TACACS**] に移動します。**TACACS** で、新しい TACACS サーバを追加するか、ネットワークパラメータを入力 または変更して既存の TACACS サーバの設定を編集します。|

Syslog サーバーの追加または変更	[** システム **] > [** 監査 **] > [**Syslog サーバー **] に移動します。[**Syslog Servers**] で、新しい Syslog サーバーを追加するか、ネットワーク パラメーターを入力または変更して既存の Syslog サーバーの設定を編集します。監視するログレベルの種類を選択すると、追加情報を設定できます。
Syslog メッセージの確認	[** システム **] > [** 監査 **] に移動します。** ［Audit Messages］** の ** [Syslog Messages］** を選択します。すべてのシステムログファイルの概要が Syslog Viewer 上に表示されます。「ファイル」ドロップダウンオプションから、表示したい syslog ファイルを選択できます。さらに、syslog ファイル は、モジュール、イベントタイプ、および重要度でさらにフィルタリングできます。
Syslog のパージ設定の構成	[** システム **] > [** 監査 **] に移動します。「** 設定 **」で「**Syslog 消去設定 **」を選択し、Citrix ADM から削除さ れるまでに Syslog データを保持する日数を入力します。
システムイベントの表示	[** システム **] > [** イベント **] に移動します。現在の全イベントを詳細と共に確認できます。
NTP サーバーの追加または変更	** ［System］**>** ［NTP Servers］** の順に選択します。新しい NTP サーバーを追加するか、既存の NTP サーバーの設定を編集します。
NTP パラメーターの構成	** ［System］**>** ［NTP Servers］** の順に選択します。** ［NTP Parameters］** をクリックして、表示されているフィールドにサーバー構成の詳細を入力します。
NTP 同期の有効化	** ［System］**>** ［NTP Servers］** の順に選択します。NTP サーバーに表示される時刻をローカルクロックと同期するには、「NTP ** 同期を有効にする ** 」チェックボックスを選択します。
暗号グループの追加または変更	[** システム **] > [** 暗号グループ **] に移動して、新しい暗号グループを追加するか、既存の暗号グループの設定 を編集します。暗号グループについての説明を入力して、暗号の組み合わせに割り当ててください。
通知設定の構成	「** システム ** 」>「** 通知 **」に移動します。** ［Settings］** で ** ［Change Notification Settings］** を選択します。通知を送信するアクションを選択し、[電子メール]、[**SMS**]、またはその両方を選択 ** し ** ます。
イベントダイジェスト設定の構成	「** システム ** 」>「** 通知 **」に移動します。** ［Settings］** で ** [Configure Event Digest Settings］** を選択します。「** イベントダイジェストを無効 ** にする」チェックボックスをオフにすると、繰り返し期間を設定したり、イベントダイジェスト通知を送信するメール配布リストを選択したりできます。
メールサーバーの追加または変更	[** システム **] > [通知] > [電子 ** メール **] ** に ** 移動します。「電子 ** メール **」で「電子 ** メールサーバー ** 」タブを選択 し、新しい電子メールサーバーを追加するか、既存の電子メールサーバーの設定を編集します。追加のチェックを有効にして、電子メールサーバーへのアクセス に認証が必要であることを確認したり、電子メールサーバーが SSL 認証をサポートすることを指定したりできます。
メール配布リストの追加または削除	[** システム **] > [通知] > [電子 ** メール **] ** に ** 移動します。[電子 ** メール **] で [電子 ** メール配布リスト **] タブを選択し、新しい 電子メール配布リストを追加するか、既存の電子メール配布リストの設定を編集します。
SMS サーバーの追加または変更	[** システム **] > [** 通知 **] > [**SMS**] に移動します。[**SMS**] で [**SMS サーバ **] タブを選択し、新しい SMS サーバーを追加するか、既存の SMS サーバーの設定を編集 します。
SMS 配布リストの追加または削除	[** システム **] > [** 通知 **] > [**SMS**] に移動します。[**SMS**] で [**SMS 配布リスト **] タブを選択し、新しい SMS 配布リストを追加する か、既存の SMS 配布リストの設定を編集します。

SNMP エンジン ID の構成	[** システム **] > [**SNMP**] に移動します。[** 設定 **] で [** エンジン ID の設定 **] を選択し、エンジン ID を指定します。
SNMP MIB の構成	[** システム **] > [**SNMP**] に移動します。[** 設定 **] で [**SNMP MIB の設定 **] を選択し、SNMP MIB の詳細を入力します。
SNMP トラップの構成	**［System］**>**［SNMP］**>**［Trap Destinations］** の順に選択します。[**SNMP トラップ **] で、新しい SNMP トラップ送信先を追加するか、既存の SNMP トラップ送信先の設定を編集します。
SNMP マネージャーの追加または変更	**［System］**>**［SNMP］**>**［Managers］** の順に選択します。**SNMP マネージャー ** で、新しい SNMP マネージャーを追加するか、既存の SNMP マネージャーの設定を編集します。
SNMP ユーザーの追加または変更	**［System］**>**［SNMP］**>**［Users］** の順に選択します。**［SNMP User］** で新しい SNMP ユーザーを追加するか、既存の SNMP ユーザーの設定を編集します。
SNMP ビューの追加または変更	[** システム **] > [**SNMP**] > [** ビュー **] に移動します。**［SNMP Views］** で新しい SNMP ビューを追加するか、既存の SNMP ビューの設定を編集します。
アラームの変更	[** システム **] > [** アラーム **] に移動し、設定を変更するアラームを選択します。アラームは、Citrix ADM サーバーの状態を監視するのに役立ちます。
タスクログの表示	[** システム **] > [** 診断 **] > [** タスクログ **] に移動します。その後、すべてのタスクログを詳細とともに表示できます。タスクログを選択し、そのデバイスログを表示することで追加情報 を表示し、選択したデバイスログのコマンドログを表示できます。
テクニカルサポートファイルの生成	[** システム **] > [** 診断 **] > [** テクニカルサポート **] に移動します。「** テクニカルサポート **」で「テクニカルサポートファイルの ** 生成 ** 」をクリックし て、Citrix ADM データと統計のアーカイブ（TAR ファイル）を生成します。このアーカイブは、Citrix サポートに送信して 問題のデバッグを支援してもらうことができます。
ダッシュボード レポートのタイムゾーン設定	[** システム **] > [** アナリティクス設定 **] に移動します。[**Analytics 設定 **] で [** ダッシュボード レポートのタイムゾーン設定の ** 構成] を選択し、ダッシュボードに表示されるレポートのデフォルトとして ローカルタイムまたは GMT ゾーンを設定します。
ICA セッションタイムアウトの構成	[** システム **] > [** アナリティクス設定 **] に移動します。「**Analytics 設定 **」で、「**ICA セッションタイムアウトの設定 ** 」を選択し、ICA セッションが終了するまでアイドル状態のままでい られる時間を入力します。
分析機能の構成	[** システム **] > [** アナリティクス設定 **] に移動します。「**Analytics 設定 **」で「** 機能 ** の構成」を選択し、マルチホップ設定と適応型しきい値設定を有効にします。「マルチホップを有効に ** する ** 」チェックボックスを選択すると、Citrix ADM は、クライアントとサーバー間で複数の Citrix ADC インスタンスでデプロイさ れたすべてのアプライアンスから AppFlow レコードを収集して関連付けます。「** 適応型しきい値を有効にする ** 」チェックボックスを選択すると、URL のヒット数がしきい値を上回るたびに Syslog メッセージが Syslog サーバーに送信 されます。
データベース設定の構成	[** システム **] > [** アナリティクス設定 **] に移動します。[**Analytics 設定 **] で [** 機能 ** の構成] を選択して、データベースインデックス設定とデータベースクリーンアップ設定を有効にします。「** データベースインデックスを有効にする ** 」チェックボックスを選択すると、Citrix ADM データベースの効率 的なクエリが容易になります。[** データベースクリーンアップを有効にする ** ］チェックボックスをオンにす

ると、Citrix ADM の負荷が高いために定期的にスケジュールされた時間にクリーンアップが妨げられると、データベース のクリーンアップが繰り返されます。|
データベースキャッシュ設定の構成	[** システム **] > [** アナリティクス設定 **] に移動します。[**Analytics 設定 **] で [** データベースキャッシュ設定 ** の 構成] を選択し、データベースコンテンツをキャッシュにローカルに保存します。これにより、データベースサーバーに アクセスしなくてもこのコンテンツを表示できます。
データレコード設定の構成	**Analytics 設定 ** で、** データレコード設定の設定 ** を選択します。データレコードログ設定、データ期間永続 性設定、Web インサイトレポート設定、Web Insight SLA データ収集設定、Web Insight URL データ収集設定、Web Insight URL データ収集設定、URL パラメータ 設定の各設定で機能を有効にできます。
特定の Citrix ADC IP アドレスの SLA 管理を 設定する	[** システム **] > [**Analytics 設定]** > [**SLA 管理 **] に移動します。表示されたリストから、サーバーの応答時間、ヒット数/秒、および帯域幅使用量に関する SLA を管理するアプライアンスの Citrix ADC IP アドレス を選択します。
Insight 要約レベルごとにデータベース レコードを保持する期間を設定します。	[** システム **] > [**Analytics 設定]** > [** データベースの概要 **] に移動します。Citrix ADM でインサイトデータを 保持する期間を指定します。このデータの保存については、1 時間ごと、1 日ごと、または 1 分ごとに 1 回を選択できます。
アダプティブしきい値の追加または変更	[** システム **] > [** アナリティクス設定 **] > [** 適応しきい値 **] に移動します。[** 適応しきい値 **] で、新しい適応しきい値を追加するか、既存の適応しきい値の設定を編集します。適応型しきい値機能は、各 URL の最大 ヒット数のしきい値を設定します。URL の最大ヒット数が URL に設定されて いるしきい値を上回ると、Syslog メッセージが外部の Syslog サーバに送信 されます。しきい値の間隔は、日単位または週単位で設定できます。
しきい値とアラートの追加または変更	[** システム **] > [**Analytics 設定]** > [** しきい値 **] に移動します。[しきい ** 値 **] で、新しい制限を追加するか、既存のしきい値の設定を編集します。しきい値を作成または変更する際に、しきい値の 有効化、電子メールまたは SMS による通知の送信、しきい値のルールの設定など、追加 のアクション項目を指定できます。
SSL 証明書ファイルと SSL キーのアップロード	[** システム **] > [詳細 ** 設定 **] > [**SSL 証明書ファイル **] に移動します。[**SSL 証明書ファイル **] で [**SSL** 証明書] タブを選択し、新しい SSL 証明書をアップロードします。同様に、[**SSL 証明書ファイル **] で [**SSL キー **] タブを選択し、新しい SSL キーをアップロードします。
レポートエクスポートのスケジュール表示または編集	[** システム **] > [詳細 ** 設定 **] > [** スケジュールのエクスポート **] に移動します。すべてのエクスポートのスケジュールを詳細と共に確認できます。ここに表示されているリストから、任意のエクスポートスケジュールを編集できます。
レポートエクスポートのスケジュール指定	[** システム **] > [詳細 ** 設定 **] > [** スケジュールのエクスポート **] に移動します。新しいスケジュールを追加するには、右端のボタンをクリックし、[** スケジュールのエクスポート **] タブを選択 します。詳細を指定し、** ［Schedule］** をクリックします。
バックアップと復元機能の使用	[** システム **] > [詳細 ** 設定 **] > [** バックアップファイル **] に 移動して、Citrix ADM の現在の設定のバックアップを作成します。後でこれら のバックアップファイルを使用して、Citrix ADM をバックアップした状態に復元できます。Citrix では、アップグレードを実行する前に、また一般的には予防措置 としてこの機能を使用することをお勧めします。
SSL 証明書のインストール	** ［System］**>** ［System Administrations］** の順に選択します。「**Citrix

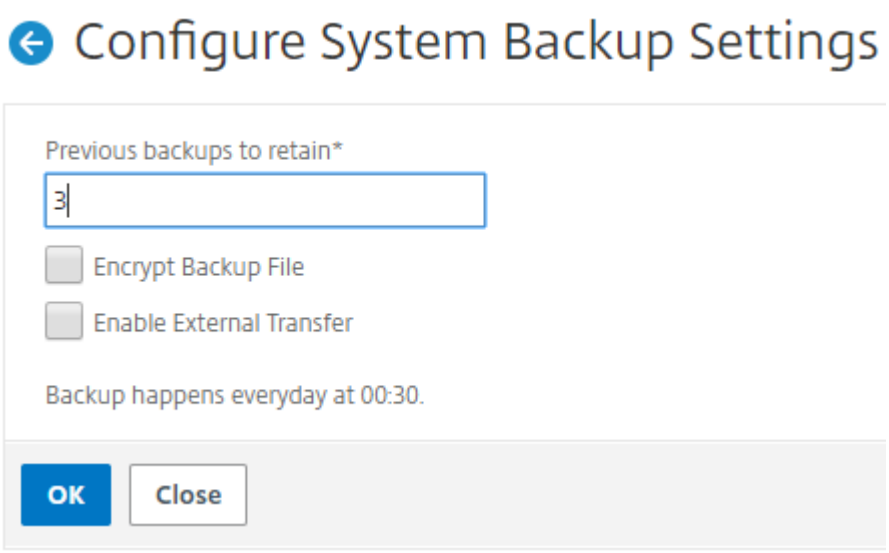
ADM の設定」で **、「**SSL 証明書のインストール **」を選択します。Citrix ADM 仮想アプライアンスに既にある証明書ファイルと SSL キーファイルを選択するか、ローカルコンピューターからファイルを アップロードできます。SSL 証明書を正常にインストールするには、［パスワード］フィールドに Citrix ADM パスワードを入力する必要があります。|
| インスタンスへのログインでの資格情報の要求 | [システム] > [** システム **** 設定の変更 **] に移動します。Citrix ADC インスタンスの任意の構成操作 ** でユーザー にインスタンス認証情報の入力を求めるには、「インスタンスログイン ** の認証情報を確認する」を有効にします。|
| 自動データパージの有効化 | **［System］**>**［System Administrations］** の順に選択します。** プルーニング設定 ** で、システムプルーニング設定を選択 ** します **。ディスク ** 使用量が設定 ** されたしきい値に達したときに Citrix ADM が データを消去できるようにするには、「自動データ消去を有効にする」チェックボックスを選択します。この機能を有効にすると、Citrix ADM は、ディスク使用量 が 設定されたしきい値を下回るまで、イベント、Syslog、パフォーマンスレポート、および分析に関連するデータを消去します。編集アイコンをクリックして、ディスク使用量の しきい値を変更します。|
|

システムバックアップの設定を構成する

February 6, 2024

Citrix 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する必要があります。

1. [システム] > [システム管理] に移動します。[バックアップ設定] で、[システムバックアップ設定] をクリックします。
2. 「システムバックアップ設定の構成」ページで、次の項目を指定します。
   - 保持するバックアップの数。最大 10 バックアップまで保持できます。
   - バックアップファイルの暗号化。
   - 外部転送の有効化。通常の予防措置として、バックアップファイルのコピーのコピーを他のシステムに転送することができます。構成を復元する場合は、まずファイルを Citrix ADM サーバーにアップロードしてから、復元操作を実行する必要があります。サーバー、ユーザー名とパスワード、ポート、使用する転送プロトコル、およびディレクトリパスを指定します。外部転送について詳しくは、「 Citrix 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。

Citrix ADM で **NTP** サーバーを構成するには:

1. ［**System**］>［**NTP Servers**］の順に選択して、［**Add**］をクリックします。
2. ［**Create NTP Server**］ページで、次の詳細情報を入力します。
   - **Server Name/IP Address** –NTP サーバーのドメイン名と IP アドレスを入力します。ここで入力したドメイン名と IP アドレスは、NTP サーバーを追加した後は変更できません。
   - **Minimum Poll Interval** –NTP メッセージの送信間隔の最小値を秒数（2 のべき乗）で指定します。たとえば、最小ポーリング間隔を 64 秒にする場合、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。

> 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 ADM アップグレード

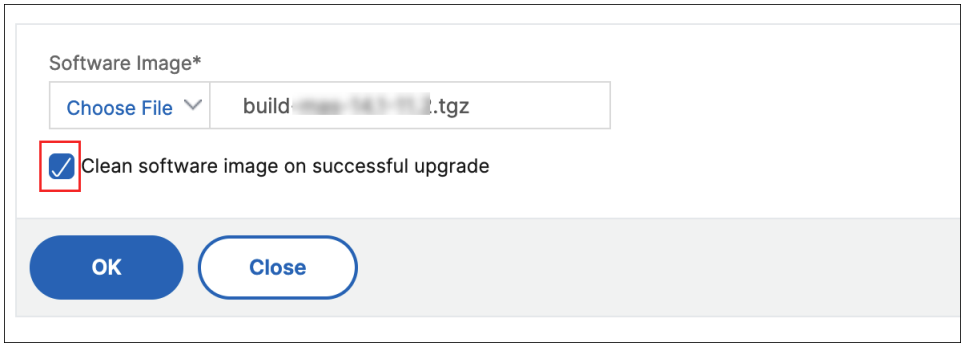
February 6, 2024

CitrixApplication Delivery Management（ADM）の各リリースでは、機能が強化された新機能や更新機能が提供されています。機能拡張についてはすべて、リリース発表に付属のリリースノートに記載されています。ソフトウェアをアップグレードする前に、リリースノートをご一読ください。アップグレードする前に、ライセンスフレームワークとライセンスの種類について理解することが重要です。

Citrix ADM をアップグレードするには:

1. ［**System**］>［**System Administrations**］の順に選択します。「システム管理」サブ見出しで、「**Citrix ADM** のアップグレード」をクリックします。

2. [Citrix ADM のアップグレード] ページで、[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 Citrix ADM 仮想アプライアンスに存在する必要があります）を選択して、新しいイメージファイルをアップロードします。
   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。



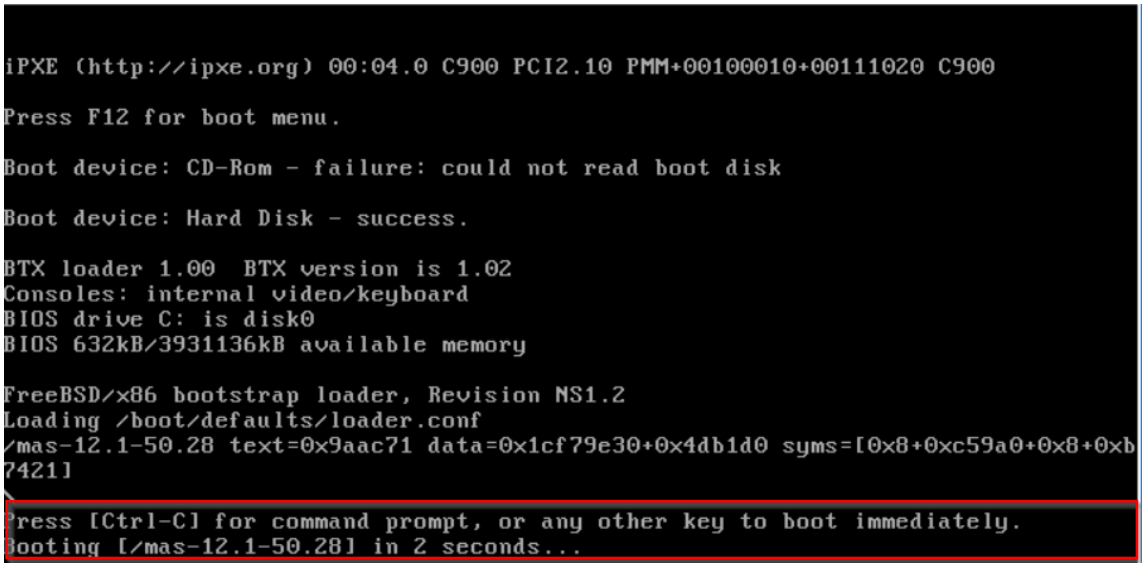
NetScaler ADM パスワードをリセットする方法

February 6, 2024

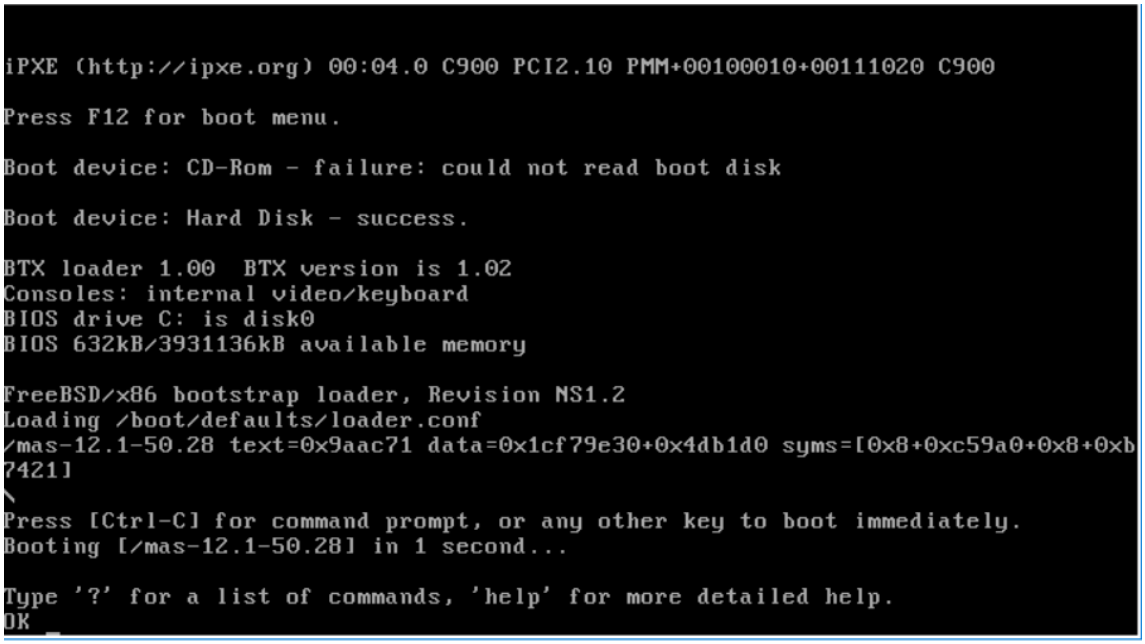
NetScaler ADM のパスワードをリセットする手順は、ホストされているハイパーバイザーによって異なる場合があります。デフォルトのパスワードを変更し、デフォルトのパスワードにリセットしたい場合は、NetScaler ADM ノードを再起動してパスワードをリセットできます。

XenCenter を使用する **Citrix Hypervisor**:

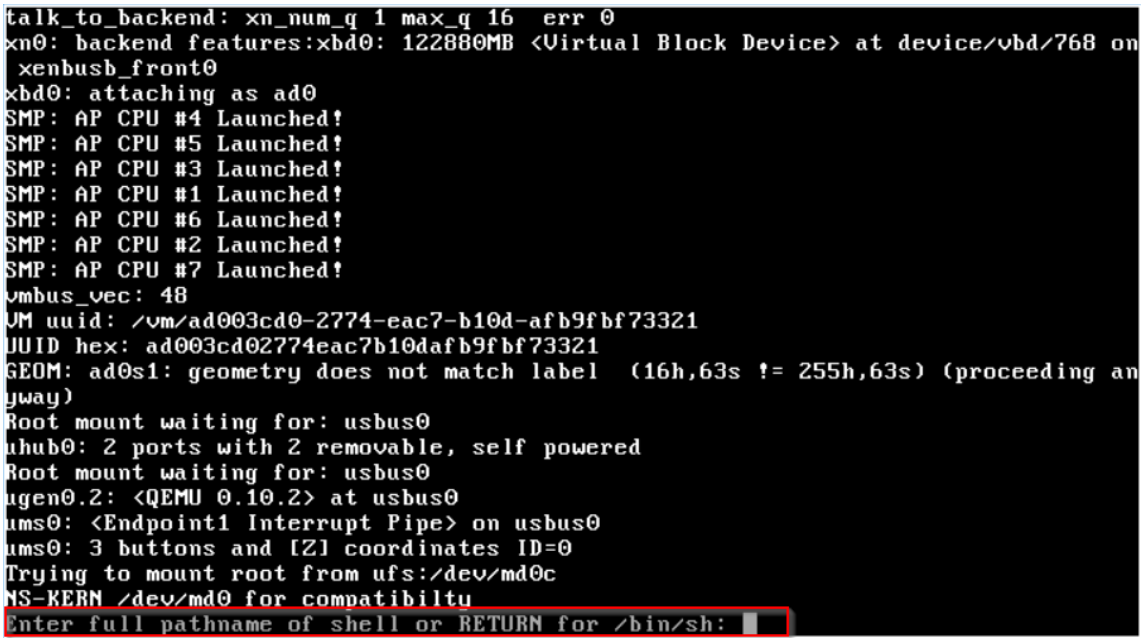
1. XenCenter を使用して Citrix Hypervisor にログオンします。
2. NetScaler ADM ノードを選択して右クリックし、「再起動」を選択します。
3. ** コンソールタブで **CTL+C** を押してブートシーケンスを中断します ** 。



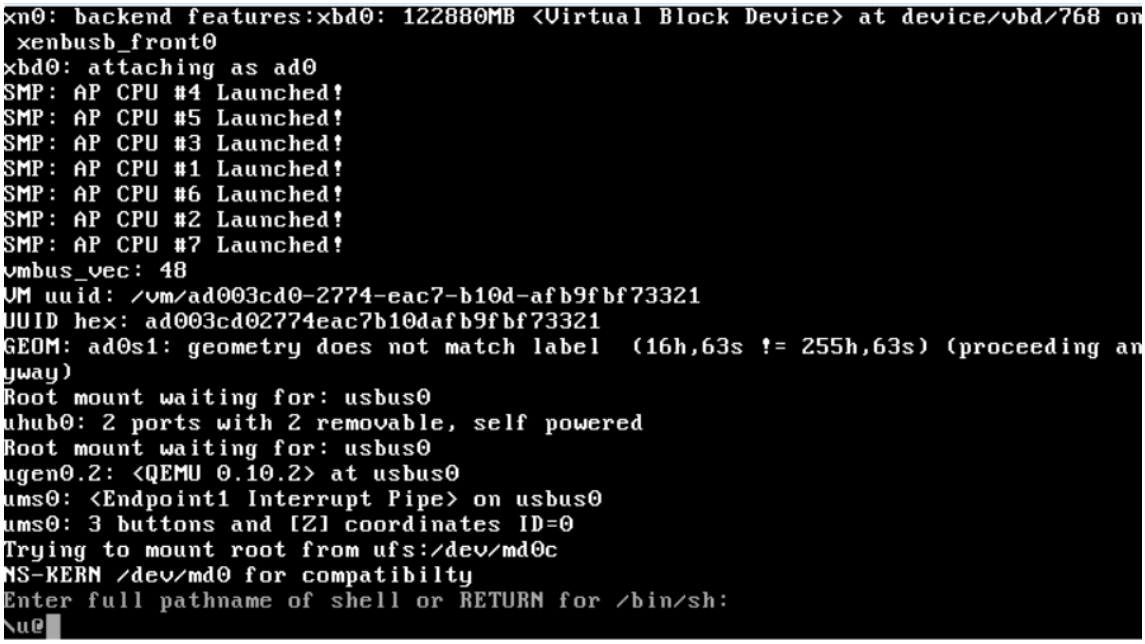
4. OK プロンプトで **boot-s** コマンドを実行します。



NetScaler ADM が再起動し、次のメッセージが表示されます。

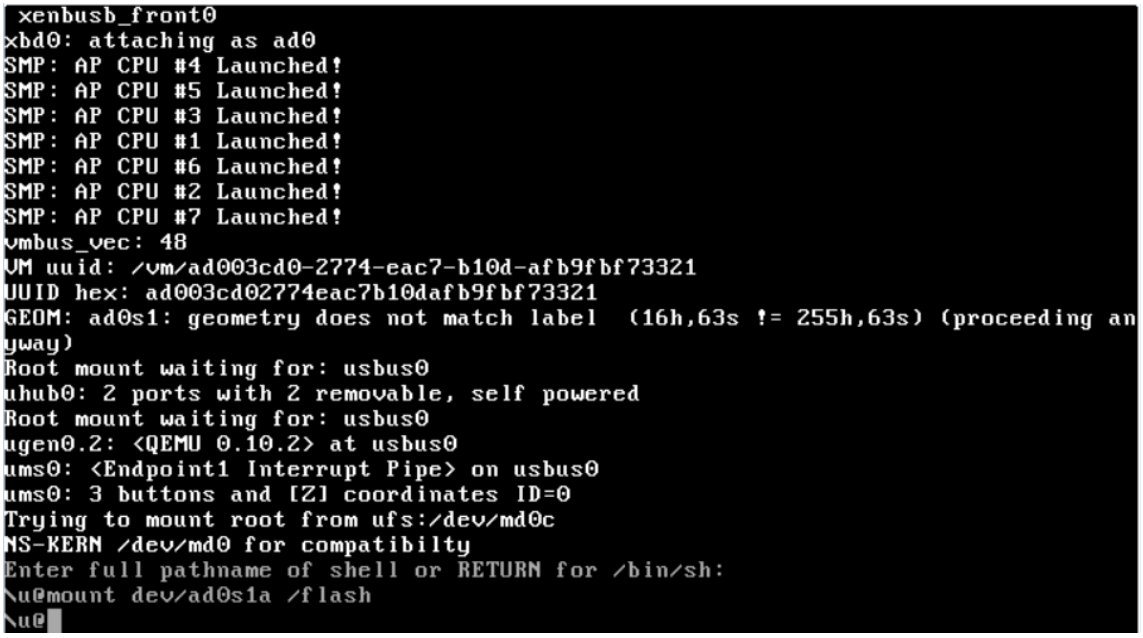


5. **Enter** キーを押して /u @ プロンプトを表示します。



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/ad0s1a /flash
```

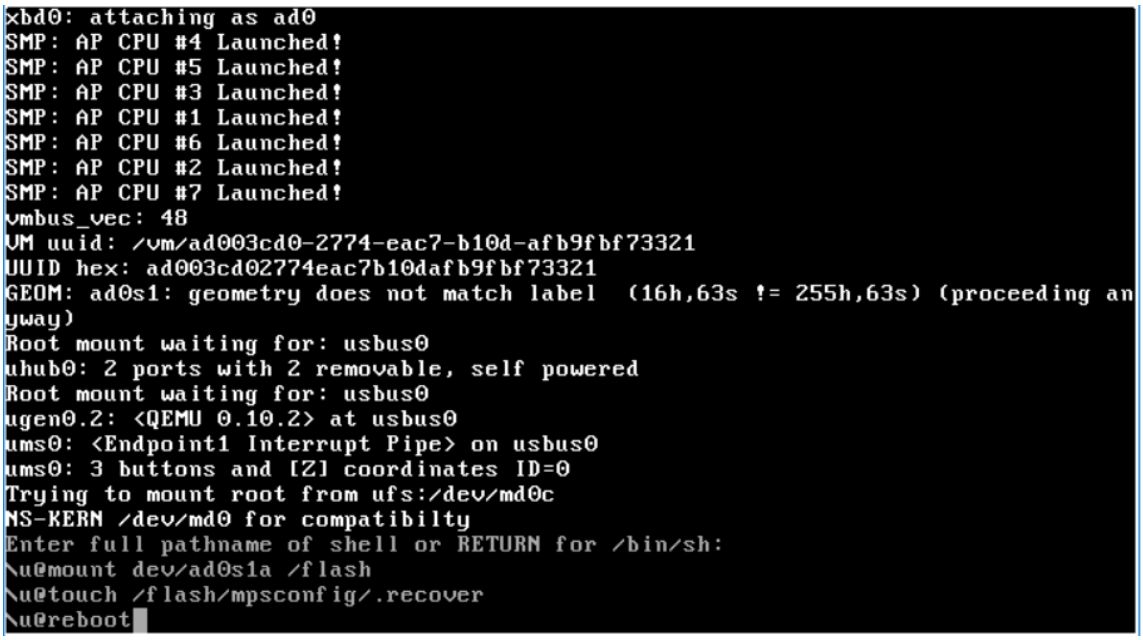



7. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm -rf /etc/passwd`
9. 次のコマンドを使用してファイルを作成します。

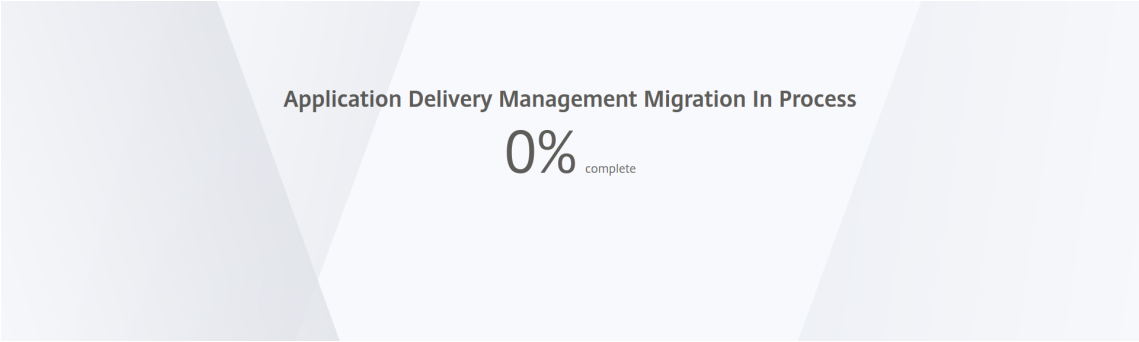
   `touch /flash/mpsconfig/.recover`

   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。

10. 再起動コマンドを実行して **Citrix** ADM を再起動します。



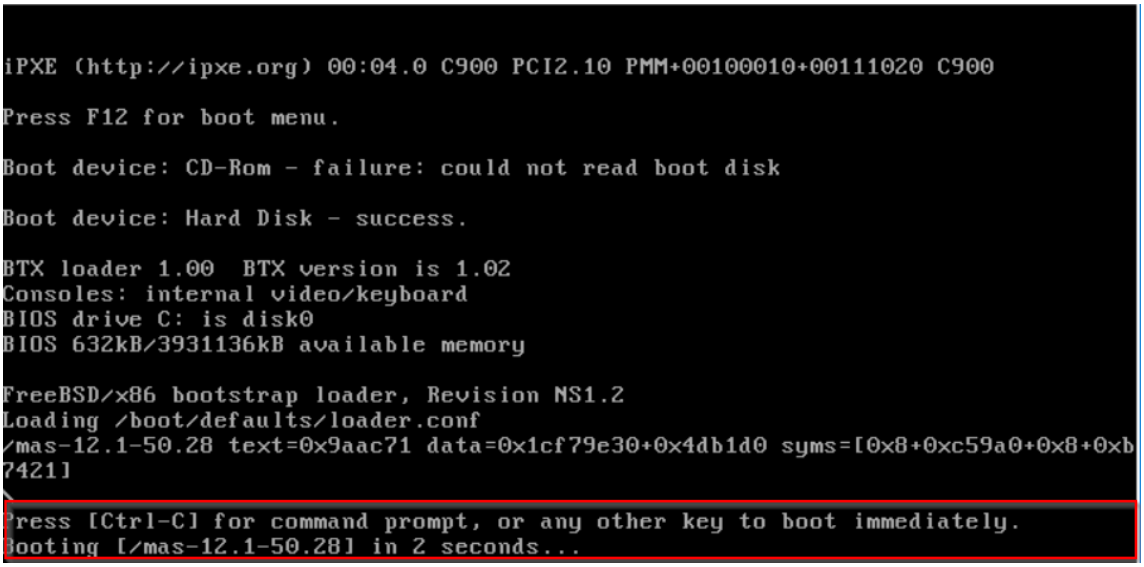
11. NetScaler ADM GUI にアクセスし、再起動が完了するまで待ちます。



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。

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。

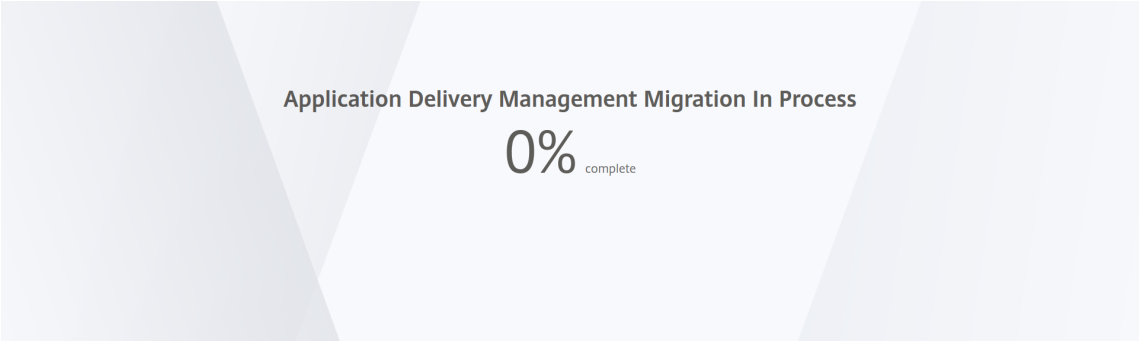
   ```
   mount dev/da0s1a /flash
   ```
7. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm -rf /etc/passwd`

9. 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。

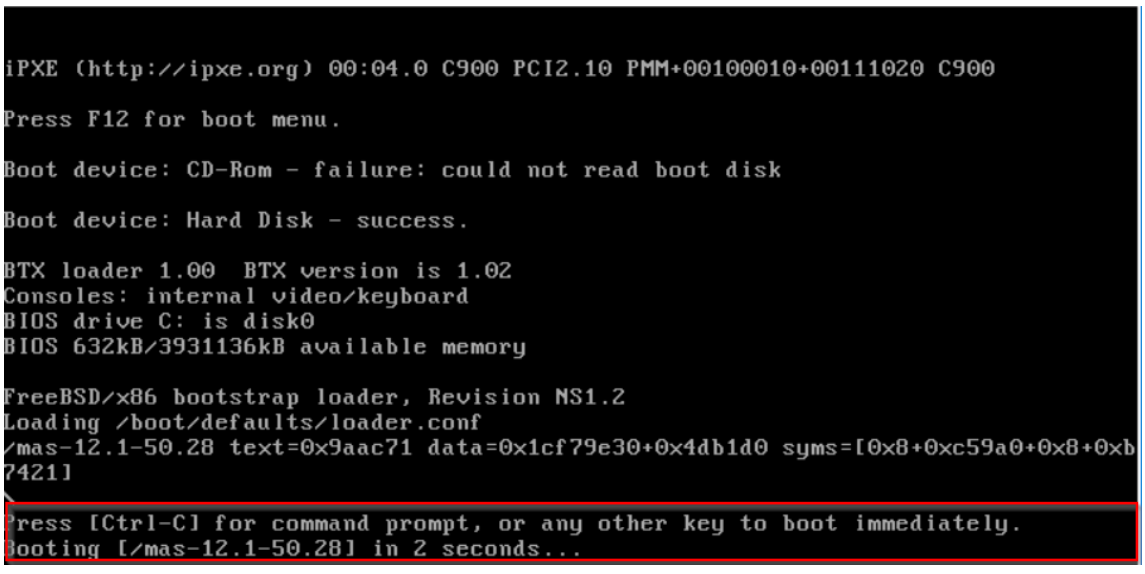
10. 再起動コマンドを実行して **Citrix** ADM を再起動します。
11. NetScaler ADM GUI にアクセスし、再起動が完了するまで待ちます。



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。

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。

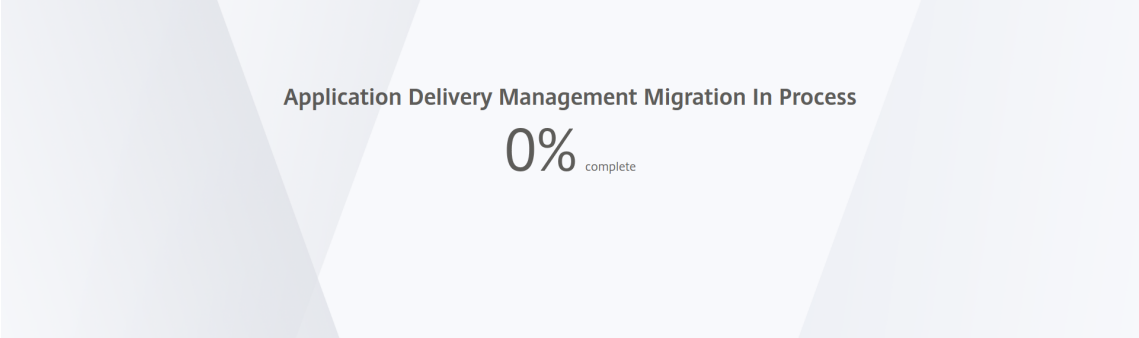
6. 次のコマンドを使用して、フラッシュパーティションをマウントします。

   ```
   mount dev/ad0s1a /flash
   ```

7. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm -rf /etc/passwd`
9. 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。
10. 再起動コマンドを実行して **Citrix** ADM を再起動します。
11. 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。

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。

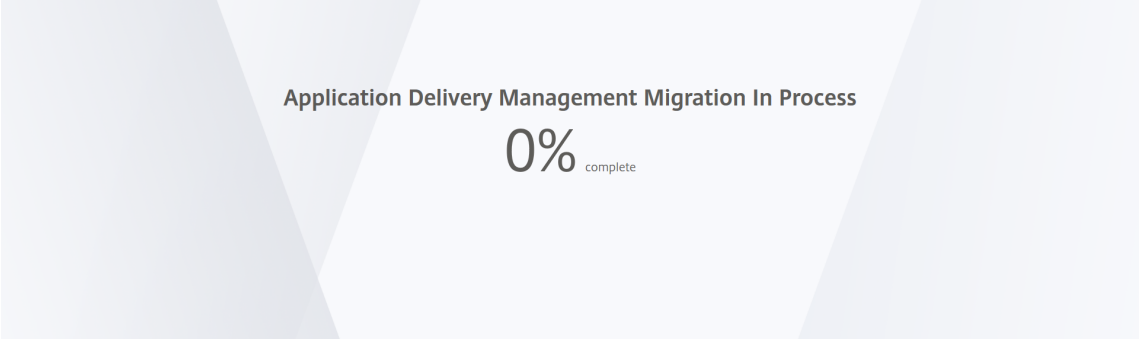
   ```
   mount dev/vtbd0s1a /flash
   ```

8. `Delete /flash/mpsconfig/master.passwd`

9. `Delete rm -rf /etc/passwd`
10. 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。
11. 再起動コマンドを実行して **Citrix** ADM を再起動します。
12. 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。

syslog パージ間隔の設定

February 6, 2024

Syslog は、ログ記録用の標準プロトコルです。これには、Citrix Application Delivery Controller （ADC）インスタンスで実行される Syslog 監査モジュールと、Citrix ADC インスタンスの基盤となる FreeBSD オペレーティングシステム（OS）またはリモートシステムのいずれかで実行できる Syslog サーバーの 2 つのコンポーネントがあります。Syslog は、データ転送に UDP（User Datagram Protocol：ユーザーデータグラムプロトコル）を使用します。

Syslog によって、情報を生成するシステムと、情報を保存するシステムを分離できます。ログ情報を統合して、集められたデータから詳細な情報を得られます。Syslog を構成して、さまざまな種類のイベントをログ記録することもできます。

データベースに保存される Syslog データの量を制限するために、Syslog データをパージする間隔を指定できます。次の syslog データが NetScaler Application Delivery Management（ADM）から削除されるまでの日数を指定できます。

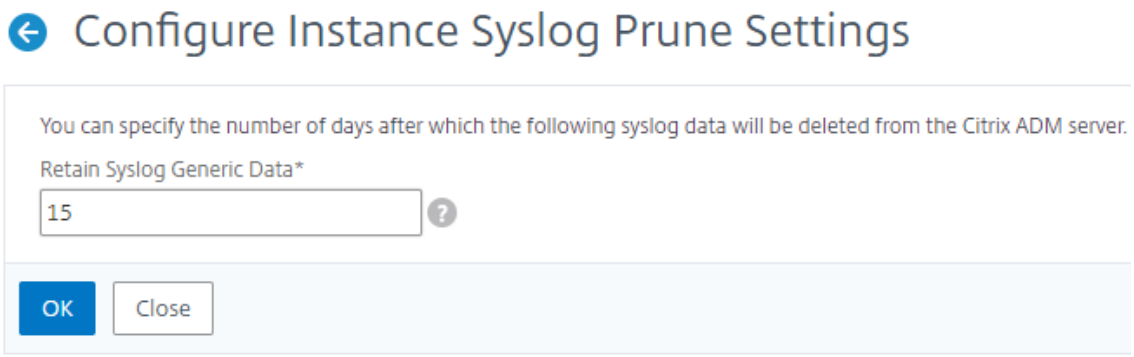
- 汎用 Syslog データ
- AppFirewall データ

- NetScaler Gateway データ

Citrix Gateway のパージ間隔を syslog タイプごとに構成することもできます。このパージ間隔は、Citrix Gateway データを保持するように構成されたパージ間隔よりも優先されます。

Citrix ADM の **syslog** パージ間隔を設定するには:

1. [**System**] > [**System Administrations**] の順に選択します。「プルーニング設定」で、「インスタンス **Syslog** プルーニング設定」をクリックします。
2. インスタンスの **Syslog** 消去設定の構成ページで、「**Syslog** 汎用データを保持」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。



システム削除設定の構成

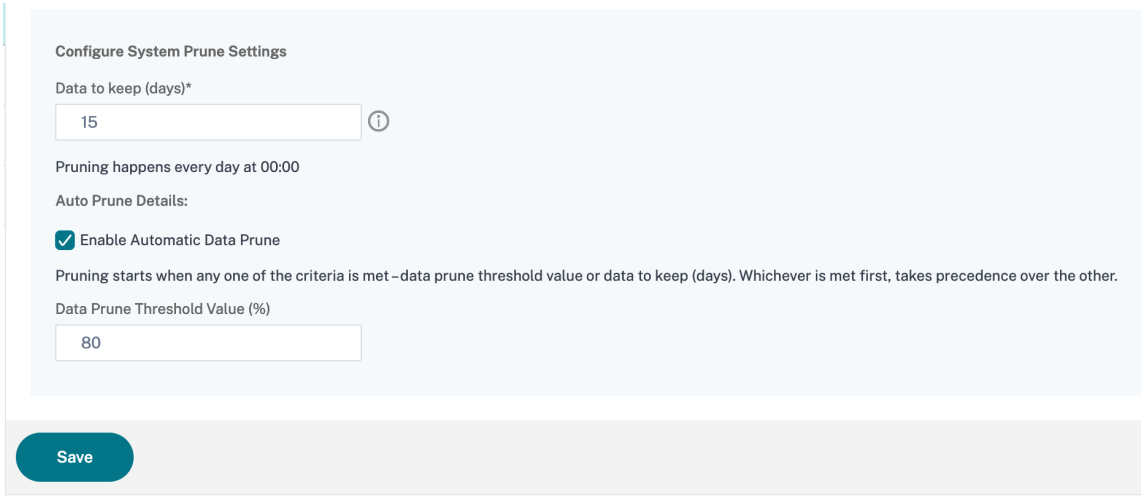
February 6, 2024

Citrix Application Delivery Management（ADM）ソフトウェア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、データベースを削除できます。NetScaler ADM でネットワークレポートデータ、イベント、監査ログ、タスクログを保持する間隔を指定できます。デフォルトでは、これらのデータは 24 時間ごとに（00:00 の時刻に）削除されます。

> 注
>
> 指定する値は 30 日を超えることも、15 日未満にすることもできません。

NetScaler ADM を使用してパフォーマンスレポートのシステム削除設定を構成するには:

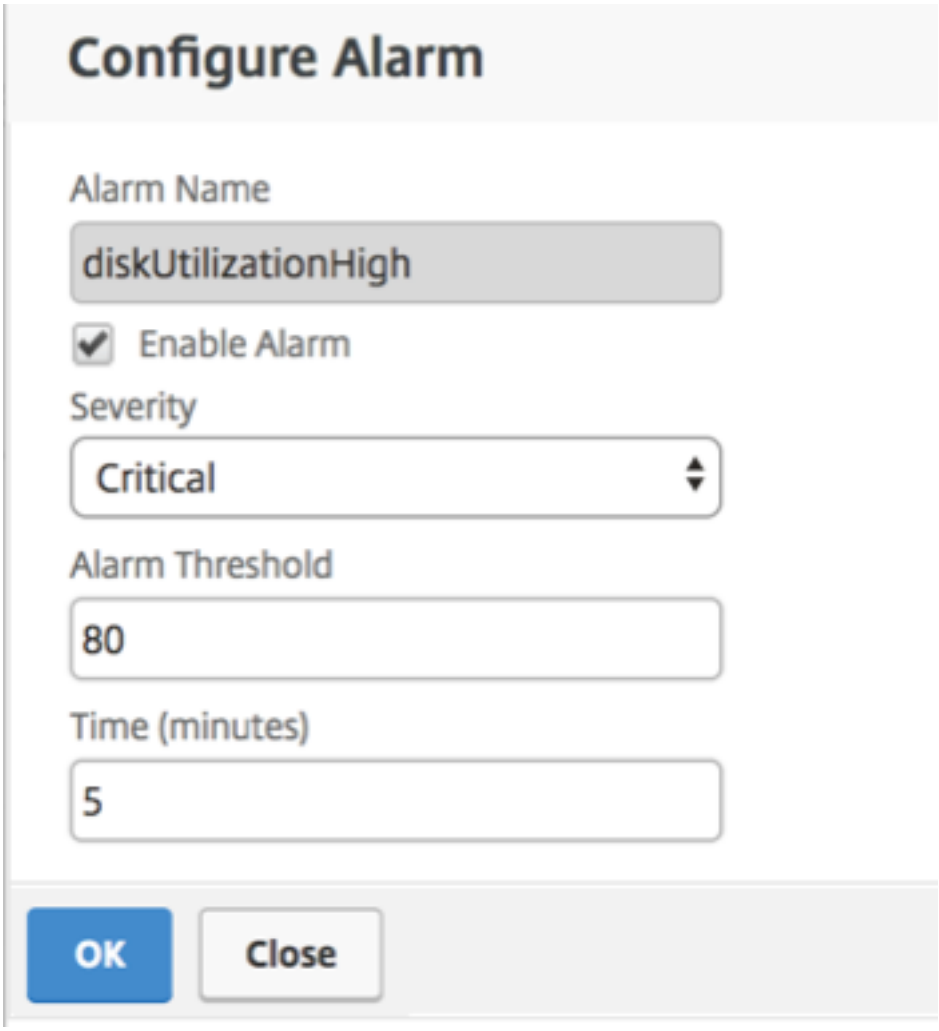
1. [システム] > [システム管理] に移動します。「 プルーニング設定」で、「システムプルーニング設定」をクリック します。
2. [システム削除設定の構成] ページで、データを保持する日数を指定し、[**OK**] をクリックします。



自動消去を有効にするには、「自動データ消去を有効に 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消去しきい値を超えると 、アラームがトリガーされます。

diskutIlizationHigh アラームを設定および有効にし（デフォルト）、次の項目を指定できます。

- 重要度 **(** 「緊急」など)
- アラームしきい値。イベントの重要度を計算する基準となる値を入力します。
- 時間。アラームをトリガーするまでの時間（分単位）。



デフォルト以外のユーザーのシェルアクセスを有効にする

February 6, 2024

Citrix Application Delivery Management（ADM）では、デフォルト以外のユーザーのシェルアクセスを有効にできます。この機能を使用し、インスタンスとの通信モードを有効にして、セットアップできます。

> 注
>
> 特に指定しない限り、デフォルト以外のユーザーに対してシェルアクセスは無効になっています。

Citrix ADM でデフォルト以外のユーザーのシェルアクセスを有効にするには：

1. NetScaler ADM で、［システム］>［システム管理］に移動します。
2. ［**System Settings**］の［**Change System Settings**］をクリックします。

3. [**Modify System Settings**] ページで次のパラメーターを構成します。
   - **Communication with instances** - 通信プロトコルを選択します。
   - 安全なアクセス-Citrix ADM の安全なアクセスを有効にします。
   - **Enable Session Timeout** - 非アクティブなセッションを保持する期間を指定します。
   - **Allow Basic Authentication** - 基本認証プロトコルを使用して提供された資格情報を管理サービスが受け入れられるようにします。
   - **Enable nsrecover Login** - 管理サービスで nsrecover ログインを有効にします。
   - 証明書のダウンロードを有効にする -追加した NetScaler ADC から証明書をダウンロードできます。
   - **nsroot** 以外のユーザーのシェルアクセスを有効にする-Citrix ADM のデフォルト以外のユーザーのシェルアクセスを有効にします。
   - インスタンスログインのユーザー資格情報を要求する -Citrix ADM からインスタンスにログオンするときに、ユーザーがユーザー資格情報を入力できるようにします。
4. [**OK**] をクリックします。

アクセスできない **NetScaler ADM** サーバーをリカバリする

February 6, 2024

Citrix Application Delivery Management（ADM）には、システムデータベースのクリーンアップを実行するデータベースメンテナンスツールが提供されるようになりました。これで、Citrix ADM ユーティリティツールを起動してファイルシステムに接続し、いくつかのコンポーネントを削除して、データベースにアクセスできるようになります。Citrix ADM リカバリスクリプトは、古いデータベーステーブルや未使用のデータベーステーブルやファイルを消去することで、ファイルシステム内のスペースを回復するのに役立つツールです。このツールを使用すると、データベーステーブルやファイル間を連続してナビゲートでき、ファイルシステム上で現在占められているスペースが各項目ごとに表示されます。削除するデータベーステーブルとファイルを選択すると、ツールは確認後にそれらをファイルシステムから削除します。

Citrix ADM スタンドアロン展開で **Citrix ADM** データベース回復スクリプトを使用する方法

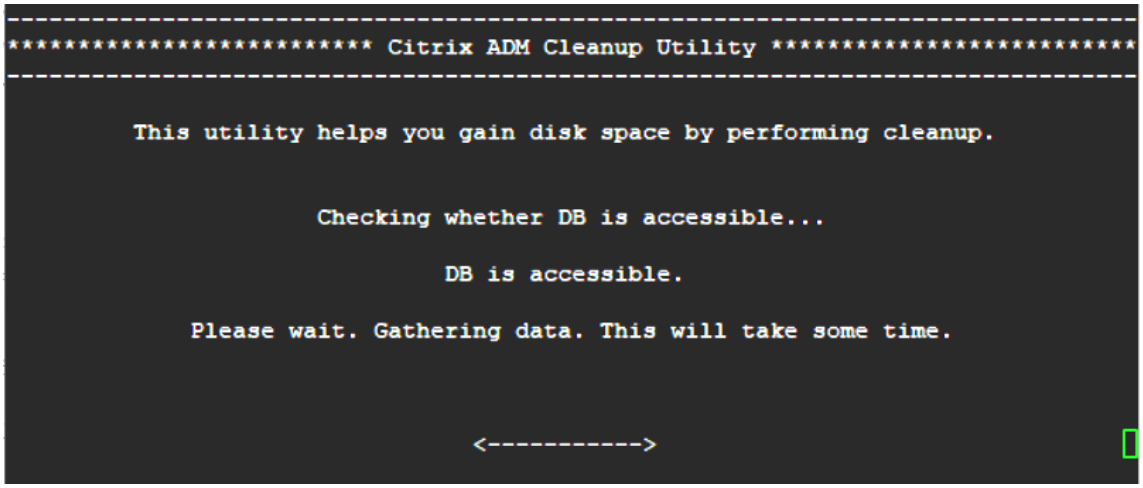
単一サーバーの NetScaler ADM 展開環境で次の手順を使用して、ファイルシステムに接続し、いくつかのコンポーネントを削除し、データベースにアクセスできるようにしてから、リカバリ操作を実行します。

1. SSH クライアントまたはハイパーバイザーのコンソールを使用して Citrix ADM にログオンし、次のコマンドを入力します。

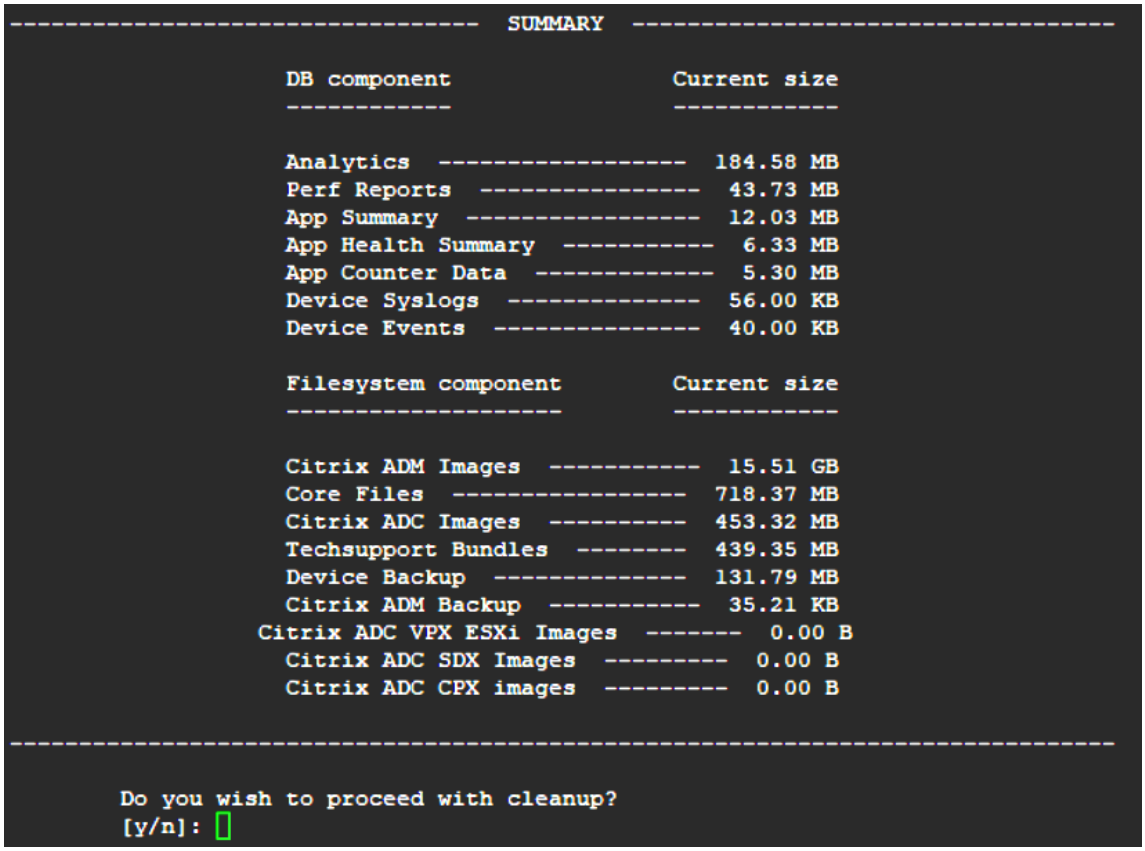
```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

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。

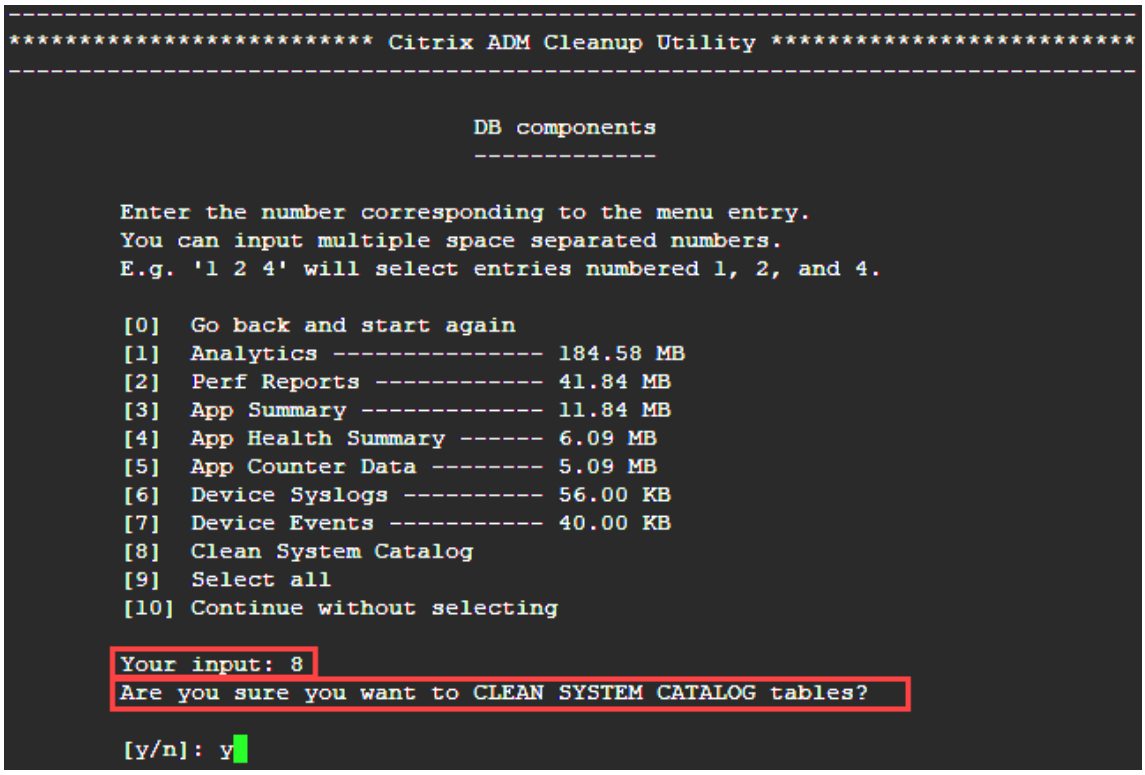


4. クリーニングが必要な特定のデータベースコンポーネントを選択し、対応する番号を入力できます。**Enter** キーを押します。

   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。

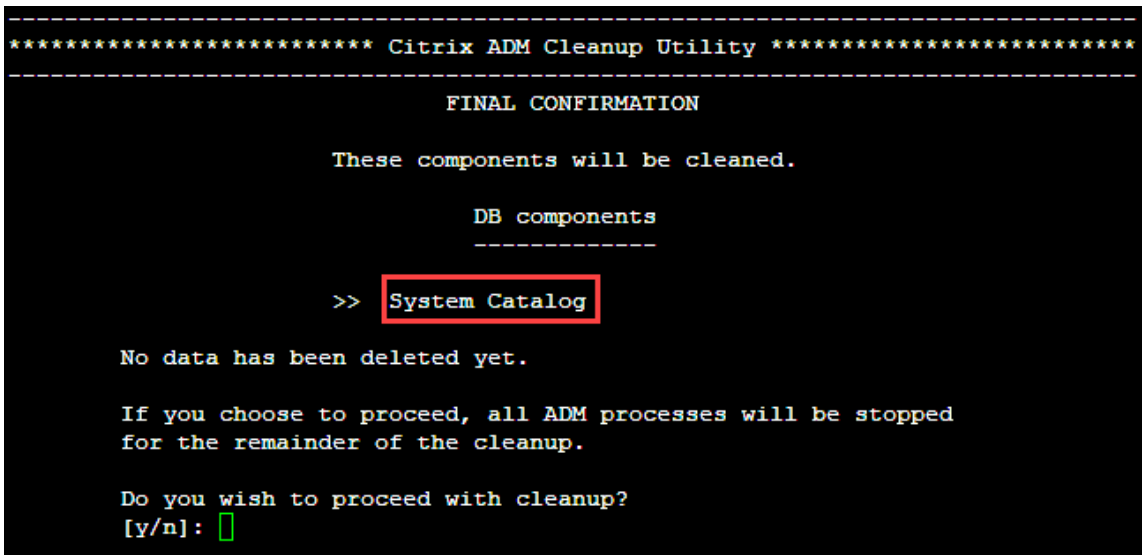
> 注
>
> : Citrix ADM には、システムカタログと呼ばれるユーザーテーブルが含まれています。システムカタログは、Citrix ADM データベース内の場所であり、リレーショナルデータベース管理システムは、テーブルや列、内部レコードに関する情報などのスキーマメタデータを格納します。システムカタログのテーブルは通常のテーブルに似ており、時間が経つにつれて膨張した行や使用されなくなった行が蓄積されることがあるため、最適なパフォーマンスを得るには定期的なクリーンアップが必要です。これらのテーブルは定期的に管理することをお勧めします。このアクティビティにより、ディスク容量が解放されるだけでなく、データベース全体、ひいては Citrix ADM のパフォーマンスも向上します。



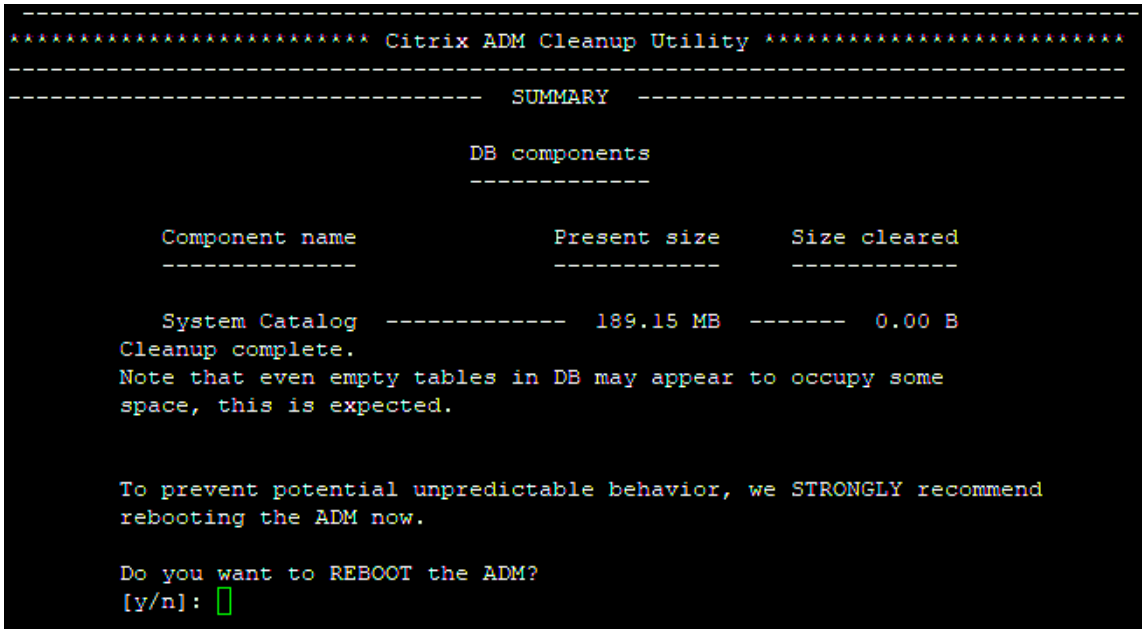
クリーンアップユーティリティには、データベースコンポーネントとファイルコンポーネントをクリーンアップするオプションがあります。「1」から「9」までの数字を入力して任意のファイルコンポーネントを選択するか、「11」と入力して Enter キーを押してデータベースコンポーネントをクリーンアップできます。

> 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、**Enter** キーを押して Citrix ADM を再起動します。

   システムのクリーンアップ後は、必ず Citrix ADM を再起動してください。NetScaler ADM が再起動した後、内部データベース操作が完了するまで約 30 分間待ちます。その後、Citrix ADM データベースに接続できる必要があります。そうでない場合は、回復スクリプトを再度実行して空き領域を増やします。Citrix ADM が起動して実行されると、期待どおりに動作する必要があります。

   > 注:
   >
   > システムカタログテーブルの現在のサイズは、クリーンアップ後ゼロに等しくなることはありません。これは、テーブルから空の行だけが削除され、クリーンアップされた後でもテーブルに有効なエントリがある可能性があるためです。

Citrix ADM 高可用性展開で **Citrix ADM** データベースリカバリスクリプトを使用する方法

高可用性環境の Citrix ADM サーバーのデータベースシステムは、連続同期モードになっています。新しいデータベース回復ツールを使用している間は、両方の Citrix ADM サーバーで手順を複製する必要はありません。

1. SSH クライアントまたはハイパーバイザーのコンソールを使用して、プライマリノードにログオンします。
2. 次のコマンドを実行します:

   ```
   /mps/mas_recovery/mas_recovery.py
   ```

3. NetScaler ADM スタンドアロン展開回復スクリプトで利用可能な手順 2 の手順に従います。

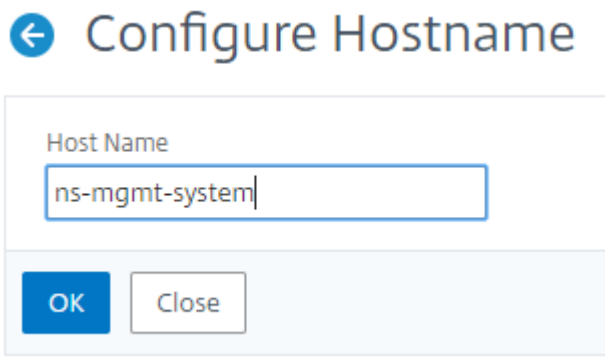
NetScaler ADM サーバーへのホスト名の割り当て

February 6, 2024

NetScaler Application Delivery Management（ADM）サーバーを識別するために、サーバーにホスト名を割り当てることができます。ホスト名は、NetScaler ADM のユニバーサルライセンスに表示されます。

NetScaler ADM サーバーにホスト名を割り当てるには:

1. NetScaler ADM で、［システム］>［システム管理］に移動します。
2. ［**System Settings**］の［**Change Hostname**］をクリックします。
3. [ホスト名の構成**]** ページで、ホスト名 を入力し、[**OK**] をクリックします。



NetScaler ADM サーバーのバックアップと復元

February 6, 2024

Citrix ADM サーバーの定期的なバックアップを作成できます。設定ファイル、インスタンスの詳細、システムデータなどをバックアップおよび復元できます。アップグレードする前に、予防的な理由により ADM サーバの構成ファイルをバックアップしてください。

バックアップには次のコンポーネントが含まれます。

- Citrix ADM 設定ファイル:
  - SNMP
  - Syslog サーバー構成ファイル
  - NTP ファイル
  - SSL 証明書

  - Control Center ファイル

- Citrix ADM サーバーが管理する Citrix ADC インスタンスのバックアップ。
- 構成監査テンプレート
- データベースに格納されているシステムデータ:
  - 作成されたテナントとユーザーの一覧
  - 外部認証サーバーの構成（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:
  - 追加および管理された Citrix ADC インスタンスからのデータ。
  - インスタンスプロファイルの詳細、バージョンの詳細、インスタンスグループの詳細など
  - 管理者が作成した静的アプリケーション（仮想サーバーのグループ）
- SNMP の設定

> 注
>
> :Analytics データ、イベント、および Syslog メッセージはバックアップから除外されます。

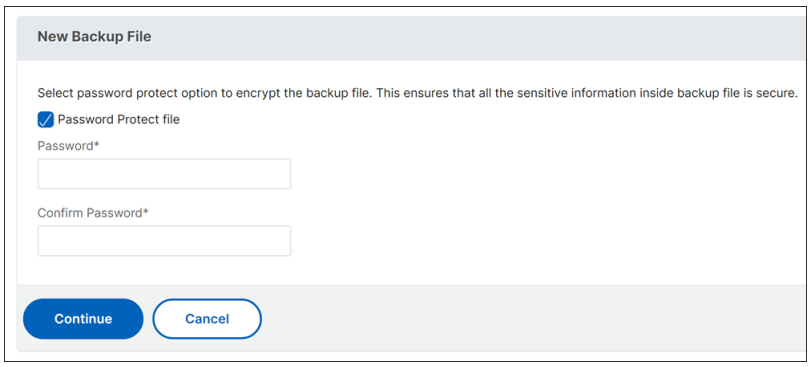
NetScaler ADM 構成のバックアップ

デフォルトでは、Citrix ADM サーバーは 24 時間ごと（00 時 30 分）に構成をバックアップします。バックアップの時間をスケジュールして選択することもできます。さらに、バックアップしたファイルのコピーを別のシステムに移動できます。

バックアップは暗号化もできる圧縮 TAR ファイルとして格納されます。デフォルトでは、3 つのバックアップファイルがサーバーに保持されます。ディスク容量不足の問題を回避するには、NetScaler ADM サーバー上に最大 10 個のバックアップファイルを保存できます。ただし、予防策として、バックアップファイルのコピーをサーバーに保存するか、別のシステムに転送することをお勧めします 。

NetScaler ADM 構成をバックアップするには:

1. [**System**] > [**Advanced Settings**] > [**Backup Files**] の順に選択して、[**Back Up**] を選択します。
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。



> 注
>
> バックアップファイルを暗号化するように設定するには、[システム] > [システムバックアップ設定] に移動し、[バックアップファイルの暗号化] を選択します。

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。

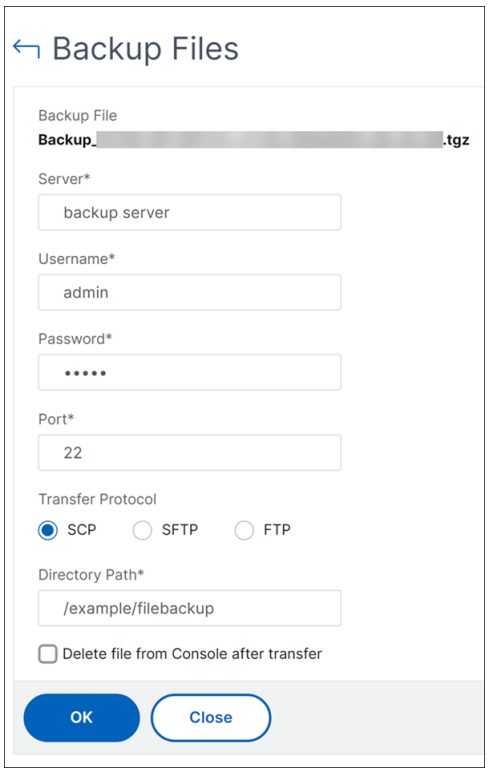
Citrix ADM バックアップファイルを転送するには:

1. [システム] > [詳細設定] > [バックアップファイル] に移動し ます。
2. 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。

    または、[システム] > [システムバックアップ設定] に移動して、外部
    ** システムの詳細を設定 ** することもできます。

4. 転送後に NetScaler ADM からバックアップファイルを削除するには、[転送後に アプリケーション配信管理からファイルを削除 する] チェックボックスをオンにします。
5. 「**OK**」をクリックして転送を行います。



> 注
>
> バックアップファイルのコピーをローカルシステムに保存するには、[システム] **> [詳細設定 **]> [** 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。

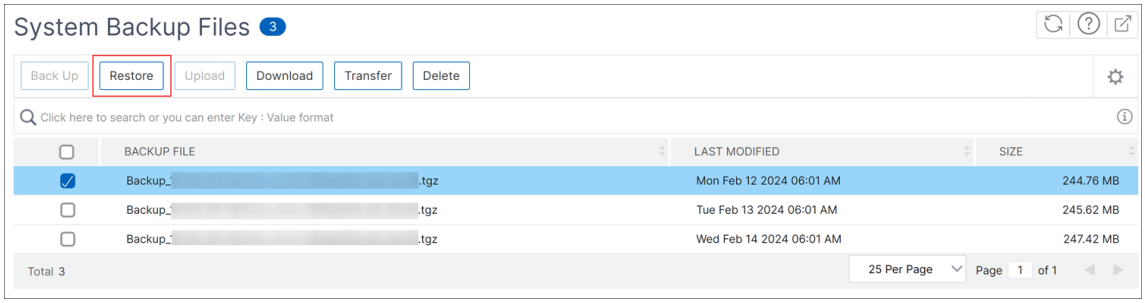
バックアップファイルから **NetScaler ADM** 構成を復元する

以前にバックアップしたファイルから Citrix ADM 構成を復元すると、復元操作によってバックアップファイルが解凍され、構成が復元されます。復元操作は既存の構成を削除し、バックアップファイルの構成で置き換えます。

> 注
>
> バックアップファイルの名前が変更されたり、バックアップファイルの内容が変更されたりすると、復元操作は失敗します。

バックアップファイルから **NetScaler ADM** 構成を復元するには:

1. [**System**] > [**Advanced Settings**] > [**Backup Files**] の順に選択します。
2. 復元するバックアッププロファイルを選択して、[**Restore**] をクリックします。
3. 確認ダイアログボックスで、[**Yes**] をクリックします。



> 注
>
> 外部システムに格納されているバックアップファイルから設定を復元するには、復元操作を実行する前に、バックアップファイルを ADM サーバにアップロードします。ファイルをアップロードするには、[システム] > [詳細設定] > [ファイルのバックアップ] に移動し、[アップロード] をクリックします。

監査情報の表示

January 29, 2024

Syslog は、ログ記録用の標準プロトコルです。これには、Citrix Application Delivery Controller （ADC）インスタンスで実行される Syslog 監査モジュールと、Citrix ADC インスタンスの基盤となる FreeBSD オペレーティングシステム（OS）またはリモートシステムのいずれかで実行できる Syslog サーバーの 2 つのコンポーネントがあります。Syslog は、データ転送に UDP（User Datagram Protocol：ユーザーデータグラムプロトコル）を使用します。

Syslog によって、情報を生成するシステムと、情報を保存するシステムを分離できます。ログ情報を統合して、集められたデータから詳細な情報を得られます。Syslog を構成して、さまざまな種類のイベントをログ記録することもできます。

Syslog メッセージを Citrix Application Delivery Management（ADM）にリダイレクトするようにデバイスを構成すると、Citrix ADC デバイスが生成する syslog メッセージを監視できます。Citrix ADM の組み込みテンプレート機能を使用して、さまざまな種類の Syslog データを生成する Syslog サーバーを作成するジョブをスケジュールできます。

まず、インスタンスがログ情報を送信する対象の Syslog サーバーを構成します。次に、ログメッセージを記録する日時形式を指定します。

Citrix ADM でシスログサーバーを構成するには：

1. [システム] > [監査] に移動します。「構成の概要」で、「**Syslog** サーバー」を選択します。または、[システム] > [監査] > [**Syslog** サーバー] に移動することもできます。
2. 「**Syslog** サーバー」ページで、「追加」をクリックします。
3. [**Create Syslog Server**] ページで、次の値を入力します。

- **Name** - Syslog サーバーの名前
- **IP Address** - Syslog サーバーの IP アドレス
- **Port** - Syslog サーバーのポート

4. ログレベルを選択します（All、None、または Custom）。それに応じて重要度レベルを選択します。
5. [**Create**] をクリックします。

Citrix ADM でシスログの日付と時刻の形式を設定するには：

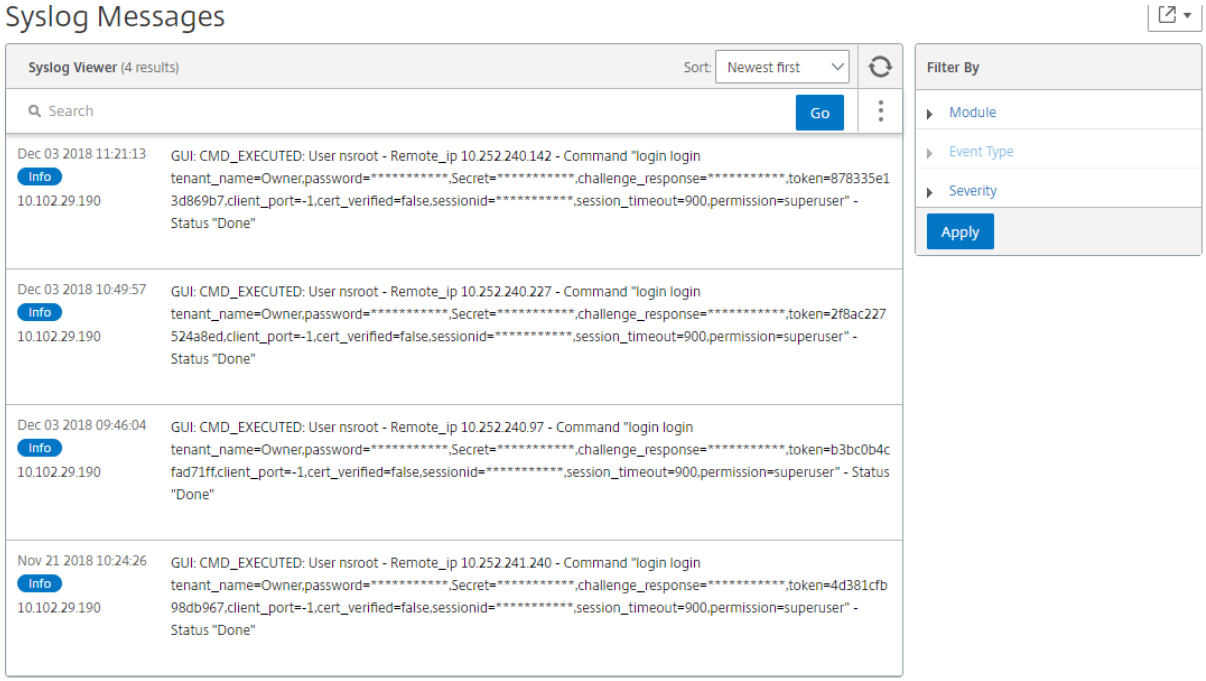
1. [システム] > [監査] に移動します。「構成の概要」で、「**Syslog** サーバー」を選択します。
2. 「**Syslog** サーバー」ページで、Syslog サーバーを選択し、「**Syslog** パラメータ」をクリックします。
3. [**Configure Syslog Parameters**] ページで日時形式を指定します。
4. [**OK**] をクリックします。

Citrix ADM でシステムログメッセージを表示するには：

Syslog メッセージを Citrix ADM サーバーにリダイレクトするようにインスタンスを構成している場合は、管理対象 Citrix ADC インスタンスで生成されたすべての syslog メッセージを表示できるようになりました。Syslog メッセージは Citrix ADM サーバーのデータベースに一元的に保存され、監査目的で Syslog ビューアで利用できるようになります。こうしたログ情報を統合し、集められたデータからレポートを作成できます。

これらの情報は、モジュール、イベントタイプ、および重要度でフィルタリングできます。Syslog を構成して、さまざまな種類のイベントをログ記録することもできます。

Syslog ビューアを表示するには、[システム] > [監査] に移動します。「監査」ページの「監査メッセージ」で、「Syslog メッセージ」を選択します。適切なフィルターを選択して、システムのログメッセージを表示します。



SSL 設定の構成

February 6, 2024

SSL（Secure Socket layer）と TLS（Transport Layer Security）は、ユーザーとサーバー間の暗号化通信を実現する、広く使用されているセキュリティネットワークプロトコルです。Citrix Application Delivery Management（ADM）で SSL 設定を構成し、システムに接続するクライアントの種類を指定できます。

Citrix ADM の **SSL** 設定を構成するには：

1. ［**System**］> ［**System Administrations**］の順に選択します。［**System Settings**］で［**Configure SSL Settings**］を選択します。
2. **SSL** 設定ページで、現在のプロトコル設定とシステムに適用されている暗号スイートを確認します。
3. プロトコル設定を変更するには、［**Edit Settings**］> ［**Protocol Settings**］の順に選択して、必要な変更を行います。
4. 適用されている暗号の組み合わせを変更するには、［**Edit Settings**］> ［**Cipher Suites**］の順に選択して、必要な変更を行います。
5. 「**OK**」をクリックし、「閉じる」をクリックします。

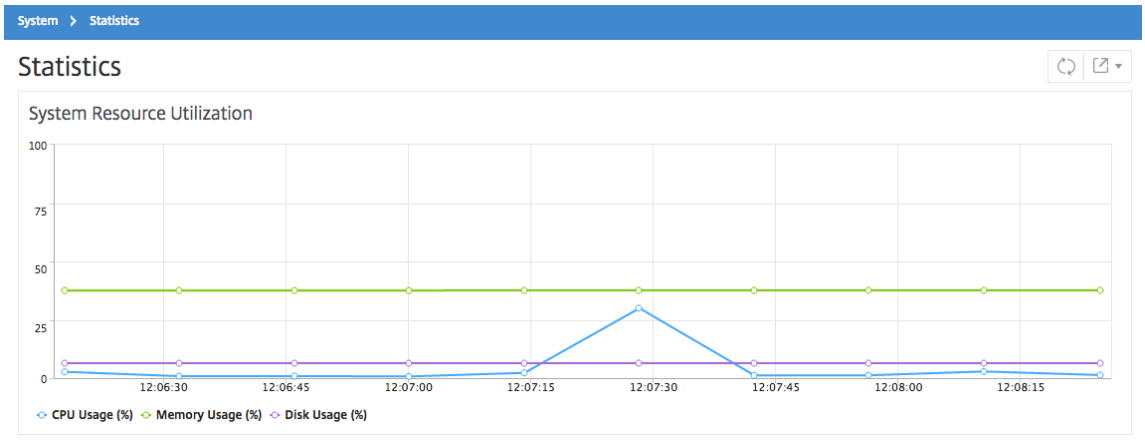
CPU、メモリ、ディスク使用率の監視

January 29, 2024

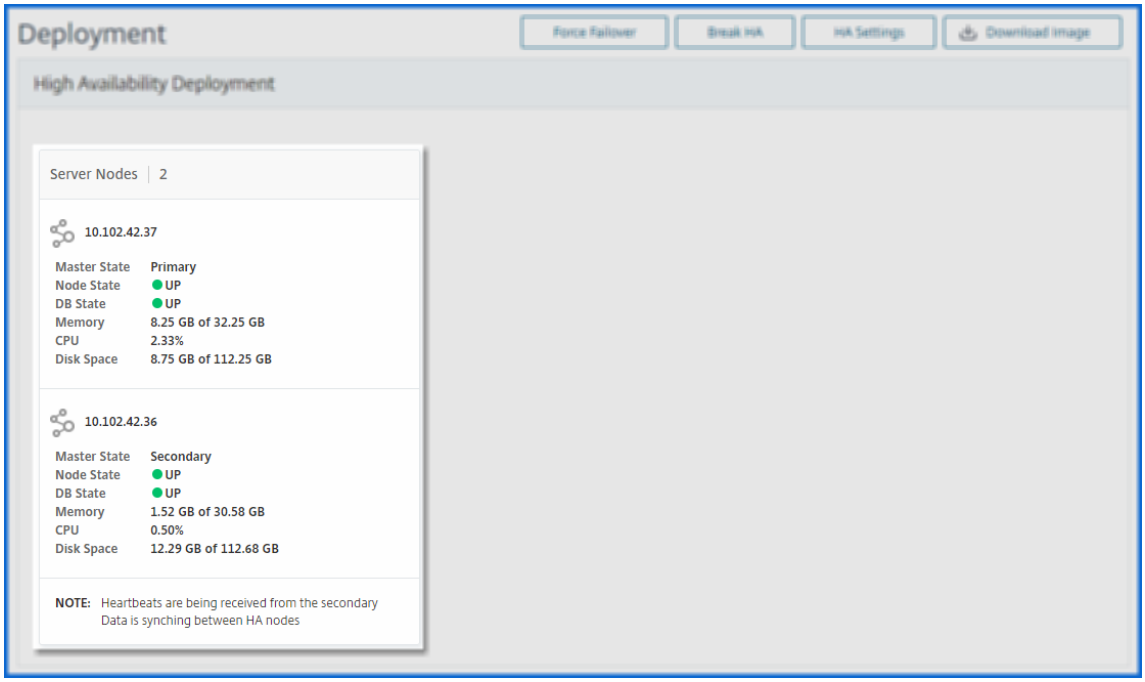
ログと統計に保持されている情報を使用できます。この情報は、Citrix Application Delivery Management（ADM）の構成と保守に役立つレポートにも表示されます。

CPU、メモリ、ディスクの使用状況を監視するには、

- スタンドアロンデプロイメント。[システム] > [統計] に移動します。CPU、メモリ、ディスク使用率のグラフをリアルタイムで表示できます。



- 高可用性導入。[システム] > [展開] に移動します。メモリ、CPU、ディスク領域、および管理対象インスタンスの統計は、次の図のように数値で表示されます:



システム通知設定の構成

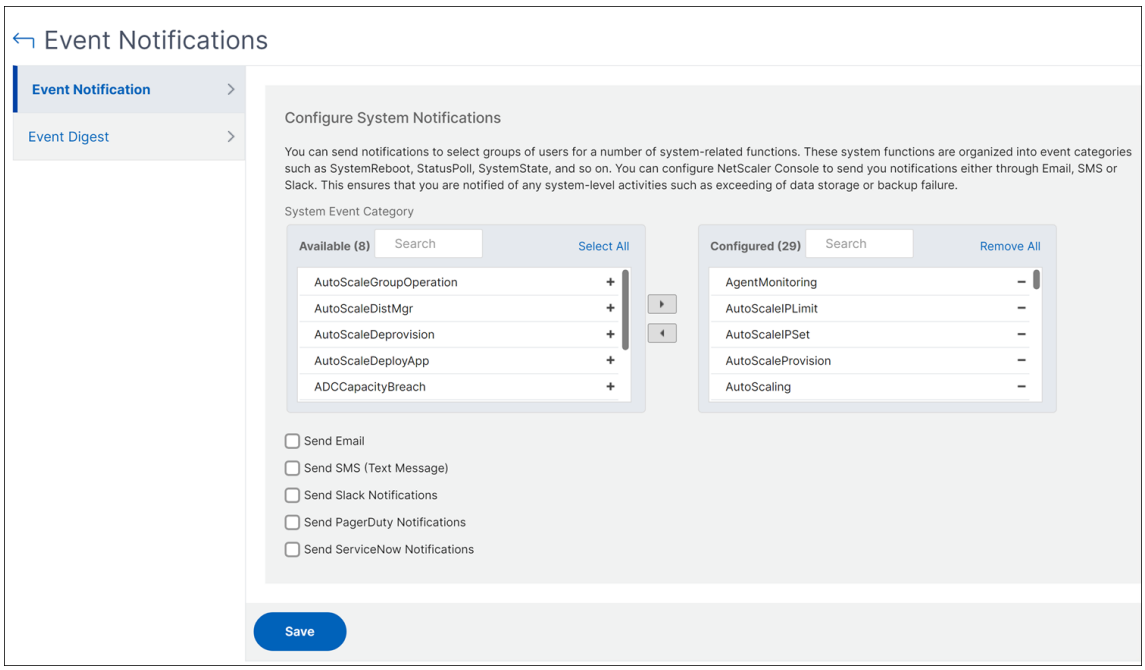
February 6, 2024

多くのシステム関連機能に関して、選択したグループのユーザー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）を構成して、電子メールまたは SMS で通知を送信できます。メールや電子メールやテキスト通知をユーザーに送信するには、電子メールサーバーおよびショートメッセージサービス（SMS）ゲートウェイサーバーの両方またはいずれかを構成する必要があります。これによりユーザーログオンやシステムの再起動などの、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。

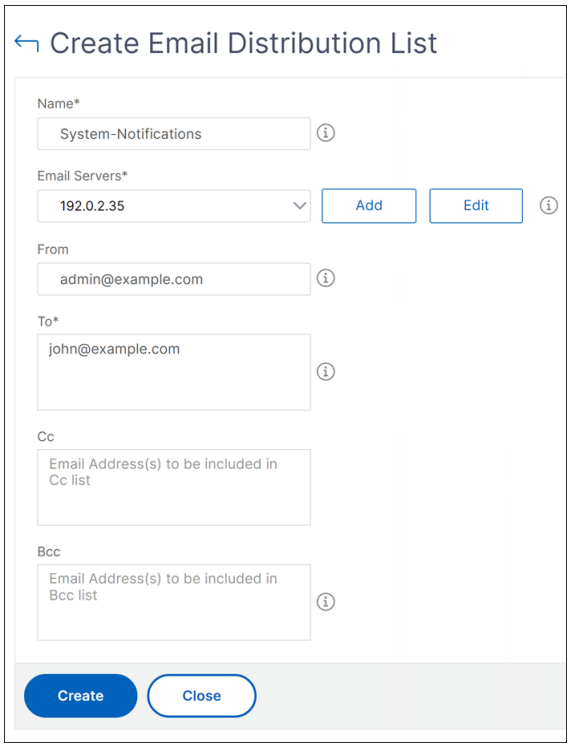
たとえば、誰かが CLI を使用して Citrix ADM にログオンしようとして失敗したときに、2 人のユーザーに電子メール通知を送信したい場合があります。［UserLogin］カテゴリを選択して、通知を送るのに電子メール通知サーバーを作成するか、既存の電子メール配布リストを選択するかのいずれかを実行して、システム通知設定を構成する必要があります。

Citrix ADM でシステム通知設定を構成するには:

1. 「システム」>「通知」に移動します。[設定] で、[通知設定の変更] をクリックします。
2. [システム通知設定の構成**]** ページの [カテゴリ] で、[**UserLogin**] などのカテゴリを選択します。

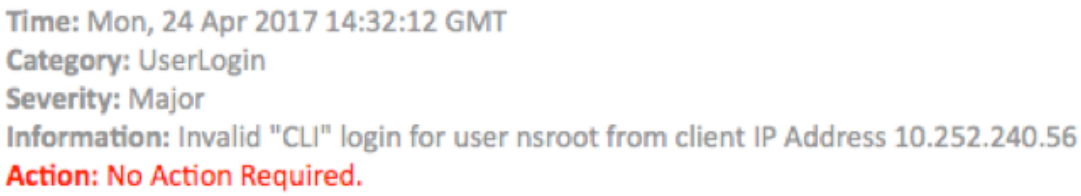


3. 「メールを送信」を選択し、ドロップダウンリストからメール配信を選択するか、「**+**」アイコンをクリックして下図のように新しいメール配信リストを作成します。テキスト通知を送信する場合は、「**SMS**（テキストメッセージ）を送信」を選択し、「**+**」アイコンをクリックして SMS サーバーの詳細を指定して SMS 配布リストを作成します。



特定のイベントのカテゴリに通知が設定されると、そのカテゴリについてのイベントが発生した場合に、電子メールか SMS で設定された宛先に通知が送られます。この例では、CLI を使用してユーザーが Citrix ADM

へのログオンに失敗した場合の電子メール通知を確認できます。



システム通知は、次のイベントに対して送信されます。

カテゴリ	原因
バックアップ失敗	システムバックアップが失敗する
DataStorageExceeded	データベースストレージがライセンスで指定された制限を超えています
DeviceBackupFailure	インスタンスのバックアップが失敗する
ハモニター	システムの HA フェールオーバーが発生し、ピアノードからのハートビートが発生せず、データベース同期が失敗する
HealthMontoring	CPU、RAM、またはディスクの使用率がしきい値を超えています
ライセンスプール	ライセンスプールがしきい値を超えています
ライセンス	ライセンスを適用すると失敗する
パスワードリカバリ	パスワード回復の失敗または成功
パフォーマンスカウンタしきい値高	パフォーマンスカウンタの値が制限を超えています
パフォーマンスカウンタしきい値標準	パフォーマンスカウンタの値は正常
ポリシー失敗	システムポリシーのいずれかが失敗する
リモートデバイスバックアップの失敗	リモートインスタンスのバックアップが失敗する
リモートシステムバックアップの失敗	リモートシステムのバックアップが失敗する
リモートシステムバックアップ標準	リモートシステムのバックアップは成功します
SSL 証明書のしきい値	証明書の基準値を超えている
ステータス投票	インスタンスの状態におけるあらゆる変化
SubSystemState	サブシステムの状態のすべての変化
SystemReboot	システムが再起動されます。
システムステート	システムの状態に変更があった場合

カテゴリ	原因
トラップ設定の失敗	インスタンスに SNMP トラップを追加すると障害が発生する
ユーザーログイン	ユーザー認証が失敗する

テクニカルサポートファイルを生成する

February 6, 2024

Citrix は、問題をデバッグするためにテクニカルサポートに連絡する前に、NetScaler Application Delivery Management（ADM）のデータと統計のアーカイブを生成することをお勧めします。テクニカルサポートチームに送信できるアーカイブは、TAR ファイルです。

> 注
>
> 高可用性モードの Citrix ADM サーバーでは、どちらのサーバーからでも テクニカルサポートファイルを生成できます。Citrix では、テクニカルサポートファイルを生成する場合に負荷分散仮想サーバーの IP アドレスを使用しないことをお勧めしています。

NetScaler ADM からテクニカルサポートファイルを構成して送信するには:

1. [システム] > [診断] > [テクニカルサポート] に移動し、[テクニカルサポートファイルの生成] をクリックします。
2. [サポートファイルを生成] ページで、次のオプションを選択します。

- **Collect Debug Logs** - このオプションは、afdecoder ログを収集する場合に選択します。
- **Duration** - デバッグログを収集する期間を入力します。このオプションは、[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 CIS にアップロードできます。

b) ADM コンソールでスクリプトを実行して、テクニカルサポートファイルを Citrix Insight Services（CIS）Web サイトにアップロードすることもできます。

i. SSH を使用して、ADM コンソールにログオンします。

ii. シェルプロンプトに切り替えて、次のように入力します。

/mps/collector_upload.pl

コマンド全体を、指定する必要がある属性とともに以下に示します。

```
/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できます。

CIS のアカウントを持っていることを確認してください。Citrix アカウントの認証情報を使用して CIS にファイルをアップロードできます。

プロキシサーバーがない場合はどうなりますか? それとも、SSL フォワードプロキシで何らかの問題に直面している場合はどうでしょうか? (これは、Perl スクリプトがプロキシサーバーのルート証明書を信頼していない場合に発生する可能性があります)
。ADM シェルから CIS にファイルを直接アップロードすることは引き続き可能です。

> 注:
>
> ADM がコンソールから CIS にファイルをアップロードできない場合でも、ファイルをダウンロードして Citrix テクニカルサポートチームに電子メールで送信できます。または、ADM からローカルストレージにファイルをダウンロードし、Web ブラウザを使用して CIS にアップロードすることもできます。

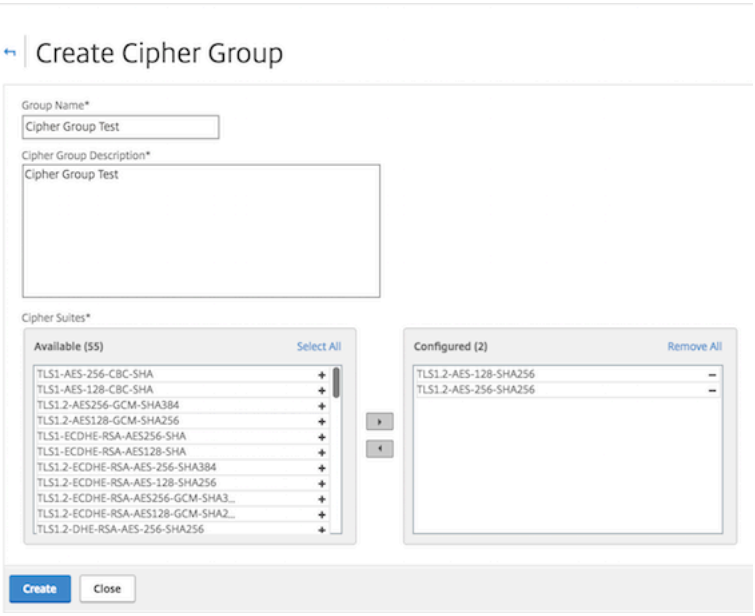
暗号グループの構成

January 29, 2024

暗号グループは、Citrix Application Delivery Controller（ADC）インスタンス上の SSL 仮想サーバー、サービス、またはサービスグループにバインドする暗号スイートのセットです。暗号の組み合わせは、プロトコル、キー交換（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、メッセージ認証コード（Mac）アルゴリズムから構成されます。

NetScaler ADM で暗号グループを追加するには:

1. [**System**] > [**Cipher Groups**] の順に選択して、[**Add**] をクリックします。
2. [**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。
3. [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

Citrix ADM で異常な状態が発生するたびに、SNMP トラップが生成されます。次に、トラップは、トラップ宛先サーバーまたは *SNMP* トラップ宛先と呼ばれるリモートデバイスに送信されます。SNMP マネージャと呼ばれるリモートデバイスから、システム固有の情報について *SNMP* エージェントに問い合わせることができます。エージェントは、要求されたデータを MIB（Management Information Base：管理情報ベース）で検索して、データを SNMP マネージャーに送信します。

Citrix ADM で **SNMP** トラップの送信先を作成するには:

1. [**System**] > [**SNMP**] > [**Trap Destinations**] の順に選択します。
2. 「**SNMP** トラップ」で、「追加」をクリックして SNMP トラップを作成し、次の詳細を指定します。

- バージョン。使用する SNMP バージョンを選択します。
- 送信先サーバー。トラップ宛先の名前または IP アドレス。
- ポート。トラップ先のポートを入力します。デフォルトでは、ポートは 162 に設定されています。
- コミュニティ。トラップリスナーにトラップを送信するときに使用するコミュニティストリングを指定します。

3. ［作成］をクリックします。

> 注
>
> SNMP v3 トラップの宛先を作成する場合は、トラップをバインドする SNMP ユーザー認証情報を指定します。SNMP ユーザー認証情報を追加するには、「挿入」をクリックし、利用可能な SNMP ユーザーのリストからユーザーを追加します。

SNMP マネージャーコミュニティを作成するには**:**

1. ［**System**］> ［**SNMP**］> ［**Managers**］の順に選択します。
2. 「**SNMP** マネージャー」で、「追加」をクリックして SNMP マネージャーコミュニティを作成し、次の詳細を指定します。
   - **SNMP** マネージャ。SNMP マネージャーの名前または IP アドレスを入力します。
   - コミュニティ。トラップリスナーにトラップを送信するときに使用するコミュニティストリングを指定します。
3. オプションで、「管理ネットワークを有効にする」チェックボックスを選択して、**SNMP** マネージャーネットワークのサブネットマスクであるネットマスクを指定できます。
4. ［作成］をクリックします。

SNMP ユーザーを作成するには**:**

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。システムのアラームを構成して、システム上の重大な問題や重要な問題を確実に把握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、Major などの重大度を割り当てることができます。NetScaler ADM がシステムファイルのバックアップを試行し、失敗するとアラームがトリガーされます。Citrix ADM でメッセージを表示したり、電子メールや SMS で通知を受け取ったりできます。

アラームを設定するには、BackupFailed アラームを選択し、重大度レベルを Major として指定する必要があります。このアラームはデフォルトで有効化されています。

NetScaler ADM を使用してシステムアラームを構成および表示するには：

1. [システム] > [アラーム] に移動します。

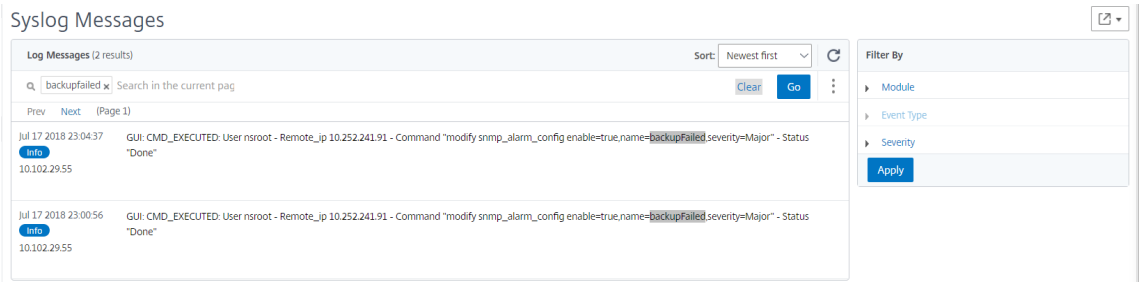
2. 設定するアラーム（BackupFailed など）を選択し、[**Edit**] をクリックして設定を変更します。
3. このアラームはデフォルトで有効化されています。重要度レベル (例: メジャー) を割り当て、「**OK**」をクリックします。

> 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。

Citrix ADM を使用してバックアップ失敗アラームによって生成されたイベントを表示するには：

1. [システム] > [監査] に移動します。

2. 「監査」ページの「監査メッセージ」で、「Syslog メッセージ」を選択します。
3. 検索フィールドに、アラームの名前を入力します。
   この例では、失敗したバックアップ試行に対してイベントが生成されていることがわかります。



   アラームが発生したときに、電子メールか SMS（Short Message Service）テキストのいずれかを送る通知を設定することもできます。システム通知の構成方法については、「NetScaler ADM のシステム通知設定を構成する方法」を参照してください。

API プロキシサーバーとしての NetScaler ADM

February 6, 2024

Application Delivery Management（Citrix ADM）は、独自の管理および分析機能に対する NITRO REST API リクエストを受信できるだけでなく、マネージドインスタンスの REST API プロキシサーバーとしても機能します。REST API クライアントは、API リクエストを管理対象インスタンスに直接送信する代わりに、API リクエストを Citrix ADM に送信できます。Citrix ADM は、応答する必要のある API リクエストと、変更されずにマネージドインスタンスに転送する必要がある API リクエストを区別できます。

API プロキシサーバーとして、Citrix ADM には次の利点があります。

- **API** 要求の検証：Citrix ADM は、すべての API リクエストを、構成済みのセキュリティおよびロールベースのアクセス制御（RBAC）ポリシーと照合して検証します。Citrix ADM はテナント対応でもあり、API アクティビティがテナントの境界を越えないようにします。
- 集中監査：Citrix ADM は、管理対象インスタンスに関連するすべての API アクティビティの監査ログを保持します。
- セッション管理：NetScaler ADM は、API クライアントを管理対象インスタンスとのセッションを維持するタスクから解放します。

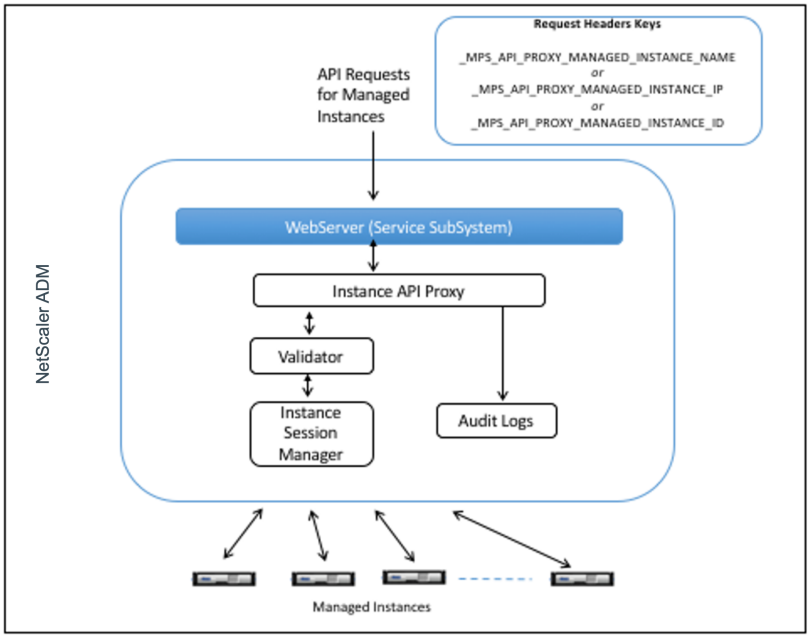
Citrix ADM が API プロキシサーバーとして機能する仕組み

NetScaler ADM で管理対象インスタンスにリクエストを転送する場合は、API リクエストに次の HTTP ヘッダーのいずれかを含めるように API クライアントを構成します。

- _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。

これらの HTTP ヘッダーが存在すると、NetScaler ADM は API リクエストを管理対象インスタンスに転送する必要がある API リクエストとして識別するのに役立ちます。ヘッダーの値は、Citrix ADM がリクエストを転送する必要がある管理対象インスタンスを識別するのに役立ちます。

次の図はこのフローを示しています。



上記の図に示すように、これらの HTTP ヘッダーの 1 つが要求に表示されると、NetScaler ADM は要求を次のように処理します。

1. Citrix ADM は、リクエストを変更せずに、リクエストをインスタンス API プロキシエンジンに転送します。
2. インスタンス API プロキシエンジンは API 要求を検証ツールに転送し、API 要求の詳細を監査ログに記録します。
3. 検証ツールは、要求が構成されているセキュリティポリシー、RBAC ポリシー、テナント境界などに違反がないことを確認します。管理対象インスタンスが利用可能かどうかを判断するチェックなど、追加のチェックを実行します。

API リクエストが有効でマネージドインスタンスに転送できる場合、Citrix ADM はインスタンスセッションマネージャーによって維持されているセッションを識別し、リクエストを管理対象インスタンスに送信します。

NetScaler ADM を API プロキシサーバーとして使用する方法

次の例は、API クライアントが IP アドレス 192.0.2.5 の Citrix ADM サーバーに送信する REST API リクエストを示しています。Citrix ADM は、リクエストを変更せずに IP アドレス 192.0.2.10 の管理対象インスタンスに転送する必要があります。すべての例で _MPS_API_PROXY_MANAGED_INSTANCE_IP ヘッダーを使用します。

Citrix ADM に API リクエストを送信する前に、API クライアントは次のことを行う必要があります。

- Citrix ADM にログインする
- セッション ID を取得
- 後続の API リクエストにはセッション ID を含めてください。

ログオン API 要求の形式は次のとおりです。

```
    POST /nitro/v2/config/login HTTP/1.1
    Host: 192.0.2.5
    Content-Type: application/json
    Accept: application/json
    Cache-Control: no-cache

    {

        "login":
        {

            "username":"******",
            "password":"*******"
         }

     }

<!--NeedCopy-->
```

Citrix ADM は、セッション ID を含む応答でログオン要求に応答します。次のサンプル応答本文は、セッション ID を示しています。

```
{


  "errorcode": 0,
  "message": "Done",
  "operation": "add",
  "resourceType": "login",
  "username": "**********",
  "tenant_name": "Owner",
  "resourceName": "******",
  "login": [
    {

      "tenant_name": "Owner",
      "permission": "superuser",
```



```
16         "session_timeout": "36000",
17         "challenge_token": "",
18         "username": "",
19         "login_type": "",
20         "challenge": "",
21         "client_ip": "",
22         "client_port": "-1",
23         "cert_verified": "false",
24         "sessionid": "##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",
25         "token": "b2f3f935e93db6a"
26        }
27
28     ]
29
30    }
31
32  <!--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 HTTP/1.1
2       Host: 192.0.2.5
3       _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4       Cookie: SESSID=##
           D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5       Accept: application/json
6       Cache-Control: no-cache
7   <!--NeedCopy-->
```

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 HTTP/1.1
2       Host: 192.0.2.5
3       _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4       Cookie: SESSID=##
           D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5       Content-Type: application/json
6       Accept: application/json
7       Cache-Control: no-cache
8
9       {
10    "lbvserver":{
11    "name":"sample_lbvserver","servicetype":"HTTP","ipv46":"10.102.1.11","
          port":"80" }
```



```
12    }
13
14  <!--NeedCopy-->
```

例 **3:** 負荷分散仮想サーバーの変更

クライアントは、NetScaler ADM に次の形式の API 要求を送信する必要があります。

```
1      PUT /nitro/v1/config/lbvserver HTTP/1.1
2      Host: 192.0.2.5
3      SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
4      _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5      Content-Type: application/json
6      Accept: application/json
7      Cache-Control: no-cache
8
9      {
10   "lbvserver":{
11   "name":"sample_lbvserver","appflowlog":"DISABLED" }
12    }
13
14  <!--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、Citrix ADM に次の形式の API 要求を送信する必要があります。

```
1      DELETE /nitro/v1/config/lbvserver/sample_lbvserver HTTP/1.1
2      Host: 192.0.2.5
3      Cookie: SESSID=##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
4      _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5      Cache-Control: no-cache
6
7   <!--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デプロイされた **Citrix Gateway** インスタンスで **EUEM** 仮想チャネルを有効にすることはできますか**?**

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] に移動し、分析を有効にする Citrix アプリケーション Delivery Controller (Citrix ADC) インスタンスを選択します。
2. 「アクション」ドロップダウンリストから「**Insight** を有効化**/**無効化」を選択します。
3. 表示された［**Configure Insight**］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て、［**Enable AppFlow**］をクリックします。詳しくは、「インスタンスの分析を有効にする方法」を参照してください。

> 注
>
> 11.0 リリース、65.30 ビルド以降の NetScaler ADC インスタンスの場合、NetScaler ADM では Security Insight を明示的に有効にするオプションはありません。NetScaler ADC インスタンスで AppFlow パラメータを構成して、NetScaler ADM が Web Insight トラフィックとともに Security Insight トラフィックの受信を開始するようにします。NetScaler ADC インスタンスで AppFlow パラメーターを設定する方法について詳しくは、「構成ユーティリティを使用して AppFlow パラメーターを設定するには」を参照してください。

NetScaler ADC インスタンスを追加すると、**NetScaler ADM** は自動的に分析情報の収集を開始しますか**?**

いいえ。まず、Citrix ADM によって管理されている Citrix 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する必要があります。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 **Citrix ADC** アプライアンスにアクセスする必要がありますか**?**

いいえ。すべての構成は、特定の NetScaler ADC インスタンスでホストされている仮想サーバーを一覧表示する NetScaler ADM ユーザーインターフェイスから行います。 詳細については、「インスタンスで アナリティクスを有効にする方法」を参照してください。

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

現在、NetScaler ADM ユーザーインターフェイスには、分析を有効にするための次の仮想サーバーが一覧表示されます。

- 負荷分散仮想サーバー
- コンテンツスイッチ仮想サーバー
- VPN 仮想サーバー
- キャッシュリダイレクト仮想サーバー

Citrix ADM に追加のディスクを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. Hypervisor で、必要なディスクサイズの追加のディスクを NetScaler ADM 仮想マシンに接続します。

   たとえば、120GB の NetScaler ADM 仮想マシンで 200GB にディスク容量を増やすことを考えてみましょう。このシナリオでは、80 GB ではなく 200 GB のディスク容量を接続する必要があります。新しく接続された 200 GB のディスク容量は、データベースデータ、NetScaler ADM ログファイルの保存に使用されます。既存の 120 GB のディスク容量は、コアファイル、オペレーティングシステムログファイルなどの保存に使用されます。
3. NetScaler ADM 仮想マシンを起動します。

NetScaler ADC 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 ADC アプライアンスによって生成された AppFlow レコードを受信します。

AppFlow 機能が有効になっている場合、NetScaler ADM は NetScaler ADC インスタンスから Security Insight サイトと Web インサイトのトラフィックを受信します。NetScaler ADC インスタンスで AppFlow 機能を有効にする場合は、AppFlow レコードの送信先となるコレクターを少なくとも 1 つ指定する必要があります。NetScaler ADC インスタンスでコレクターが構成されていない場合、NetScaler ADM はインスタンスからのトラフィックを受信しません。

たとえば、5 つの NetScaler ADC インスタンスが NetScaler ADM に追加されます。コレクタが 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。

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

多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場合があります。たとえば、外部サーバーにアクセスできなくなったり、新しいユーザーの資格情報がどの外部認証サーバーにも入力されなかったりする可能性があります。このような状況でユーザーがロックアウトされないようにするには、ローカル認証のフォールバックを有効にします。詳しくは、「ローカル認証のフォールバックを有効にする方法」を参照してください。

ローカル認証のフォールバックとは何ですか

ローカル認証のフォールバックとは、外部認証に失敗したときにユーザーをローカルで認証するオプションです。外部認証に失敗すると、NetScaler ADM はローカルユーザーデータベースにアクセスしてユーザーを認証します。

Citrix ADM で、[システム] > [認証] > [認証構成] に移動します。このページでは、複数の外部認証サーバーをカスケードに追加したり、［**Enable fallback local authentication**］をオンにできます。

外部ユーザーグループの抽出とは何ですか

ユーザーを認証するために外部サーバーを追加した場合は、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。Citrix ADM にログインし、Citrix ADM で同じグループ情報を手動で作成し、それらのグループに権限を割り当てます。ユーザーおよびユーザーグループの権限は、外部サーバーではなく、NetScaler ADM で管理されます。ユーザーは、外部サーバーでさまざまな役割ベースのアクセス権限を持っています。NetScaler ADM のユーザーにも同じ権限を構成します。権限をユーザーごとに個別に構成するのではなく、グループレベルの権限を構成できます。これにより、ユーザーグループのメンバーが負荷分散された仮想サーバー上の特定のサービスにアクセスできるようになります。割り当てることができる一般的な権限は、NetScaler ADC インスタンス、Citrix SDX インスタンス、仮想サーバーなどを管理する権限です。これにより、そのグループのユーザーはそれらのインスタンスまたは仮想サーバーのみを管理できます。ユーザーにグループレベルで付与した権限は、後で編集できます。1 つ以上のユーザーグループを削除することもできますが、他のグループユーザーは引き続き NetScaler ADM で機能します。

構成管理

NetScaler ADM を使用して、複数の **NetScaler ADC** インスタンスにまたがって構成を同時に実行できますか

はい。構成ジョブを使用して、複数の NetScaler ADC インスタンスにわたって構成を実行できます。

NetScaler ADM の構成ジョブは何ですか**?**

ジョブとは、管理対象インスタンスに対して作成および実行できる構成コマンドのセットです。ジョブを作成してインスタンス間で構成を変更したり、ネットワーク上の複数のインスタンスに構成を複製したり、NetScaler ADM GUI を使用して構成タスクを記録して再生したりできます。記録したタスクを CLI コマンドに変換することもできます。

NetScaler ADM 構成ジョブ機能を使用して、構成ジョブの作成、電子メール通知の送信、および作成されたジョブの実行ログの確認を行うことができます。

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

はい！組み込みテンプレートオプションを使用して、ジョブにスケジュールを指定できます。ジョブとは、管理対象インスタンスで実行できる一連の構成コマンドのことです。たとえば、組み込みテンプレートオプションを使用して、Syslog サーバーを構成するジョブにスケジュールを指定できます。ジョブをすぐに実行するか、後で実行するようにジョブをスケジュールするかを選択できます。

作成済みのジョブの構成を保存して、コマンド、パラメーター、構成ソース、ターゲットインスタンスを変更してから、そのジョブを再実行できます。これは、同じ一連のコマンドを別のインスタンスで実行する必要がある場合や、ジョブでエラーが発生してそれ以降の実行を停止する場合に便利です。

証明書管理

Citrix ADM から **SSL** 証明書を削除すると、**Citrix ADC** インスタンスからの証明書も削除されますか**?**

いいえ

展開

デフォルトのユーザー名とパスワードは何ですか**?**

- 初期ネットワーク構成が完了したら、デフォルトのユーザー名とパスワード（nsrecover/nsroot）を使用して、ハイパーバイザーまたは SSH コンソールから NetScaler ADM にログオンできます。
- GUI からログオンするデフォルトのユーザー名とパスワードは、*nsroot/nsroot* です。

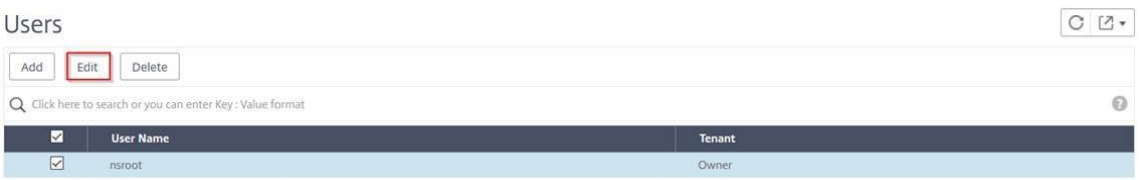
デフォルトパスワードを変更するにはどうすればいいですか

パスワードを変更するには、次の手順に従います。

1. NetScaler ADM で、［システム］>［ユーザー管理］>［ユーザー］に移動します。

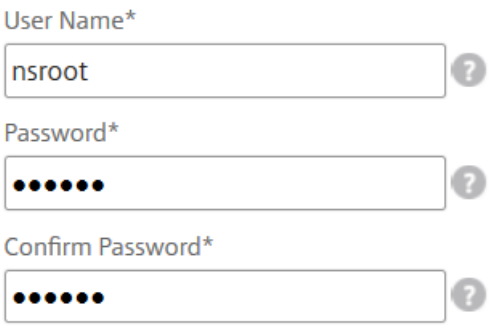
   「ユーザー」ページが表示されます。

2. ユーザー名 **nsroot** を選択し、［編集］をクリックします。



   [システムユーザーの構成] ページが表示されます。

3. [パスワードの変更] を選択し、任意のパスワードを作成します。



4. [**OK**] をクリックします。

これで、新しいパスワードを使用して GUI、ハイパーバイザー、または SSH コンソールからログオンできます。

> 注
>
> ユーザー名は変更できません。

パスワードをリセットするには**?**

このドキュメントを参照して 、パスワードをリセットできます。

HA ペアで、プライマリノードでパスワードを変更し、後で **[Break HA pair]** オプションを選択した場合、どのような動作になりますか

新しいパスワードを使用して、両方のスタンドアロンノードにログオンできます。

2 台のスタンドアロンサーバーでパスワードが異なる場合、これら **2** 台のサーバーを **HA** ペアで展開するとどのような影響がありますか

2 台のスタンドアロンサーバーを HA ペアに展開する場合は、両方のサーバーにデフォルトパスワードを設定することをお勧めします。

高可用性構成は完了しましたが、プライマリノードの **GUI** にはアクセスできません。理由は何でしょうか**?**

設定が有効になるまでに数分かかります。数分後にもう一度アクセスしてみることができます。

HA 設定は完了しましたが、フローティング **IP** アドレス **GUI** にはアクセスできません。理由は何でしょうか**?**

HA の設定が完了したら、まずプライマリノードの GUI にアクセスし、展開を完了する必要があります。詳細については、「プライマリノードとセカンダリノードを高可用性ペアとしてデプロイする」を参照してください。展開が完了すると、サーバは再起動し、高可用性展開の準備が整います。その後、フローティング IP アドレス GUI にアクセスできます。

NetScaler ADM スタンドアロンと **NetScaler ADM HA** ではどのデータベースがサポートされていますか**?**

NetScaler ADM スタンドアロンと NetScaler ADM HA はどちらも PostgreSQL をサポートしています。

セカンダリノードへの潜在的なデータ損失は何ですか**?**

セカンダリノードは、プライマリノードが NetScaler ADM データベースを介して送信するハートビートメッセージをリッスンします。セカンダリノードが 180 秒を超えてハートビートを受信しない場合、セカンダリノードはプライマリノードで SSH ベースのチェックを実行します。ハートビートと SSH ベースのチェックが失敗した場合、プライマリノードはダウンしていると見なされます。

このシナリオでは、セカンダリノードがプライマリノードを引き継ぎ、180 秒の時間枠は、セカンダリノードへのデータ損失の可能性と見なすことができます。

プライマリノードがダウンした場合はどうなりますか

セカンダリノードが引き継ぎ、プライマリノードになります。

障害が発生したノードを再インストールするにはどうすればいいですか

新しい VM ビルドをインストールすることが推奨されます。再インストールするには:

1. HA ペアを解除します。[システム] > [展開] に移動します

   配置ページが表示されます。**HA** ブレークをクリックします
2. Hypervisor から障害が発生したノードを削除します。
3. .xva イメージファイルをハイパーバイザーにインポートします。
4. [コンソール] タブで、NetScaler ADM を初期ネットワーク構成で構成します。詳細については、「1 番目のサーバー (1 次ノード) の登録と展開」および「2 番目のサーバー (2 次ノード) の登録と展開」を参照してください。
5. HA ペアを再展開します。

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

NetScaler ADM VHD をローカルストレージでホストすることをお勧めします。SAN 内のストレージデバイスでホストされている場合、NetScaler ADM が期待どおりに動作しないことがあります。

NetScaler ADM は追加のディスクをサポートしていますか**?**

はい。NetScaler ADM HA ペアの新規インストールでは、デフォルトで 120 GB のストレージが割り当てられます。120 GB を超えるストレージの場合は、ディスクを 1 つ追加して最大 3 TB のストレージにすることができます。複数のディスクを追加すること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 アドレスにはアクセスできなくなるため、高可用性ペアを再デプロイする必要があります。

再デプロイ中に別のフローティング **IP** アドレスを指定できますか**?**

はい。新しい Floating IP アドレスを設定できます。

セカンダリノードの **GUI** にアクセスできないのはなぜですか**?**

セカンダリノードは読み取りレプリカサーバーであり、何らかの理由でプライマリノードがダウンした場合にのみプライマリノードとして機能します。プライマリノード GUI またはフローティング IP アドレス GUI にアクセスすることをお勧めします。

プライマリノードが長時間ダウンしている場合でも、フローティング **IP** アドレス **GUI** を使用して設定を行うことはできますか

はい。引き続き設定を行うことができ、設定はセカンダリノードに保存されます。プライマリノードが復帰すると、すべての構成が同期されます。

将来、プライマリノードの **IP** アドレス、セカンダリノード **IP** アドレス、または **Floating IP** アドレスを変更する必要がある場合 **(**たとえば、**IPv6** に変更するなど**)**、推奨される解決策は何ですか

HA ペアの IP アドレスの変更は、HA ペアを壊さない限りサポートされません。

プライマリノードまたはセカンダリノードの IP アドレスを更新するには、次の手順を実行します。

1. HA ペアを解除します。[システム] > [展開] に移動します。

   「配置」ページが表示されます。**HA** ブレークをクリックします

   a) SSH クライアントを使用するか、ハイパーバイザーからプライマリノードにログオンします。

   b) `nsrecover` をユーザー名として使用し、設定したパスワードを入力します。

   c) **networkconfig** と入力します。最初のサーバ (プライマリノード) の登録と展開にあるステップ**3** の手順を実行します。

      初期ネットワーク構成では、別の IP アドレスを指定できます。

   d) セカンダリノードについても同じ手順を実行し、2 番目のサーバ（セカンダリノード）の登録と展開にあるステップ**3** の手順に進みます。

フローティング IP アドレスを更新するには:

1. [システム] > [展開] に移動します。

   「配置」ページが表示されます。

   a) **HA** 設定をクリックします。

   b) [高可用性モードの **Floating IP** アドレスの設定] をクリックします。

   c) フローティング IP アドレスを入力し、[**OK**] をクリックします。

ADM は **AMD** プロセッサーをサポートしていますか

いいえ。ADM は AMD プロセッサをサポートしていません

導入（災害復旧）

プライマリサイトとディザスタリカバリサイトの間でレプリケーションが行われる頻度はどれくらいですか

プライマリサイトとディザスタリカバリサイト間のレプリケーションはリアルタイムです。

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

いいえ。これで、DR サイトがプライマリサイトになります。

[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 ADC** インスタンスで生成されたすべてのイベントを追跡するにはどうすればよいですか

ネットワーク管理者は、NetScaler ADC インスタンスの構成変更、ログオン条件、ハードウェア障害、しきい値違反、エンティティ状態の変化などの詳細を、特定のインスタンスでのイベントとその重大度とともに表示できます。NetScaler ADM イベントダッシュボードを使用して、すべての NetScaler ADC インスタンスに関する重大なイベントの重大度の詳細について生成されたレポートを表示できます。

イベント規則とは何ですか

NetScaler ADM を使用して、特定のイベントを監視するルールを構成できます。イベントルールを使用すると、Citrix ADM インフラストラクチャ全体で生成される多数のイベントを簡単に監視できます。

特定の条件で規則を構成し、規則にアクションを割り当てることで、一連のイベントにフィルターを適用できます。生成されたイベントがルール内のフィルタ条件を満たすと、そのルールに関連付けられたアクションが実行されます。

フィルタを作成できる条件は、重大度、NetScaler ADC インスタンス、カテゴリ、および障害オブジェクトです。イベントに割り当てることができるアクションは、電子メール通知の送信、管理対象 NetScaler ADC インスタンスから NetScaler ADM への SNMP トラップの転送、SMS 通知の送信です。

インスタンス管理

NetScaler ADM のデータセンターとは何ですか**?**

NetScaler ADM データセンターは、特定の地理的場所にある NetScaler ADC インスタンスの論理グループです。各サーバーは、データセンター内の複数の NetScaler ADC インスタンスを監視および管理できます。Citrix ADM サーバーを使用して、管理対象インスタンスからの Syslog、アプリケーショントラフィックフロー、SNMP トラップなどのデータを管理できます。データセンターの構成の詳細については、「Citrix ADM でジオマップ用にデータセンターを構成する方法」を参照してください。

NetScaler ADM でサポートされているさまざまな **Citrix** アプライアンスは何ですか**?**

インスタンスは、NetScaler ADM から検出、管理、監視する Citrix アプライアンスまたは仮想アプライアンスです。これらのインスタンスは NetScaler ADM サーバーに追加する必要があります。以下の Citrix アプライアンスと仮想アプライアンスを NetScaler ADM に追加できます。

- Citrix MPX
- Citrix VPX
- Citrix SDX
- Citrix CPX
- NetScaler Gateway
- Citrix SD-WAN WO
- Citrix SD-WAN PE

インスタンスは、Citrix ADM サーバーを初めて設定するときに追加することも、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、Citrix ADM が特定の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 に無制限の **SD-WAN** インスタンスを追加できますか? **NetScaler ADM** は、**SD-WAN** のすべてのスカラーおよびベクトルカウンターを処理できますか

現在、NetScaler ADM に追加できる SD-WAN インスタンスにはライセンス制限はありません。NetScaler ADM には、スカラーカウンターとベクトルカウンターの両方を内部的にポーリングする一連の組み込みレポートがあります。

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

はい。NetScaler ADM で複数の Citrix **VPX** インスタンスを再検出して、インスタンスの最新の状態と構成を確認することができます。

[ネットワーク] > **[**** インスタンス**] > [**NetScaler VPX]** に移動し、再検出するインスタンスを選択して、[アクション] ドロップダウンリストで [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 **Citrix** の **SDX** にインストールすることはできますか**?**

いいえ

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、その構成はインスタンスには適用されず、すでに適用されている構成は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

Citrix ADC サーバーにホスト名を割り当てることはできますか**?**

はい。ホスト名を割り当てて、NetScaler ADM サーバーを識別できます。ホスト名を割り当てるには、［**System**］>［**System Administration**］>［**System Settings**］の順に選択し、［**Change Hostname**］をクリックします。

ホスト名は、NetScaler ADM のユニバーサルライセンスに表示されます。詳しくは、「NetScaler ADM サーバーにホスト名を割り当てる方法」を参照してください。

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

はい。構成ファイル（NTP ファイルと SSL 証明書）、システムデータ、インフラストラクチャとアプリケーションのデータ、およびすべての SNMP 設定をバックアップできます。NetScaler ADM が不安定になった場合は、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。

Citrix ADM の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、「Citrix 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、および Citrix Gateway データが Citrix ADM から削除されるまでの日数を指定できます。

NetScaler ADM で **NTP** サーバーを構成できますか**?**

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

NTP サーバーを設定するには 、[システム] > [**NTP** サーバー] に移動し、[追加] をクリック します。詳しくは、「NetScaler ADM で NTP サーバーを構成する方法」を参照してください。

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

NetScaler ADM アクティブ/パッシブ HA 展開モードは、NetScaler ADM バージョン 12.0 ビルド 51.24 からサポートされています。

NetScaler ADM アクティブ**-**アクティブ **HA** セットアップを行い、統合 **GUI** アクセス用に負荷分散仮想サーバーを備えた **NetScaler ADC** アプライアンスを構成しました。この構成をどうすればアップグレードできますか

NetScaler ADM HA ペアをアクティブ/パッシブモードにアップグレードした後、NetScaler ADC アプライアンスで次のコマンドを実行して、負荷分散構成を更新する必要があります。

lb モニターを追加 MAS_Monitor **TCP-ECV-**送信「**GET /mas_health HTTP/1.1\ r\ n** 受け入れエンコーディング**:** アイデンティティ**\ r\ n** ユーザーエージェント**:NetScaler-Monitor\ r\ n** 接続**:** 閉じる**\ r\ n\ n** “」**-recv**「**{\”** ステータスコード**\」: 0,** “**is_passive\」: 0}」-LRTM DISABLED**

ポート **443** を使用して **NetScaler ADC** インスタンスで **NetScaler ADM HA** ペアの負荷分散を構成できますか

いいえ。ポート 443 を使用して NetScaler ADC インスタンス上で NetScaler ADM HA ペアの負荷分散を構成することはできません。

NetScaler ADC で`http-ecv`および`https-ecv`モニタを構成すると、NetScaler ADM HA ノードが正しく監視されません。

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

はい

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

はい。Citrix ADM バックアップファイルをダウンロードし、別の Citrix ADC インスタンスのバックアップリポジトリにアップロードして、そのインスタンスを復元します。ネットワーク情報と認証情報が競合しないようにしてください。たとえば、IP アドレスやポートの競合、パスワードプロファイルの不一致をチェックします。また、復元された VPX インスタンスに、バックアップされた NSIP アドレスと NetScaler ADC ライセンスが同じであることを確認してください。

高可用性ペアのインスタンスを復元する前に、バックアップファイルに保存されている IP アドレスと状態 (プライマリまたはセカンダリ) が元の HA 構成の IP アドレスと状態 (プライマリまたはセカンダリ) と一致していることを確認してください。また、新しいプライマリとセカンダリに同じ種類の NetScaler ADC ライセンスがあることも確認します。

Citrix ADM サーバーの **NSIP** アドレスを使用する代わりに、**Citrix ADM** に **SNIP** アドレスを使用して **Citrix ADC** インスタンスと通信するように強制することはできますか**?**

はい。NetScaler ADCCitrix ADC インスタンスと通信するために、NetScaler ADM に SNIP アドレス（管理が有効になっている場合）を追加できます。

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

NetScaler ADM による NetScaler ADC インスタンスのバックアップは完全バックアップです。

NetScaler ADM のトラブルシューティングガイドはありますか

はい。https://support.citrix.com/article/CTX224502を参照してください。

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

ハートビートと SSH ベースのチェックが失敗した場合、プライマリノードはダウンしていると見なされ、セカンダリノードがプライマリノードとして引き継ぎます。デフォルトでは、すべての NetScaler ADC インスタンスは、SNMP トラップ宛先として最新のプライマリノードの詳細で更新されます。

新しいプライマリ（アクティブ）Citrix ADM ノードは、以前にアクティブだったノードが AppFlow コレクターまたは Syslog サーバーとして構成されているかどうかを確認します。構成されている場合、新しいプライマリは、インスタンスに送信される情報に AppFlow コレクターまたは Syslog サーバーの詳細を追加します。

syslog の場合、古いサーバの詳細が置き換えられます。

ダウンした **NetScaler ADM HA** ノードが復旧するとどうなりますか

サービスに戻った後、アクティブノードがフェイルオーバーしない限り、NetScaler ADM ノードはパッシブなままです

NetScaler ADC インスタンスは、**NetScaler ADM HA** ノード間でどのように分散されていますか

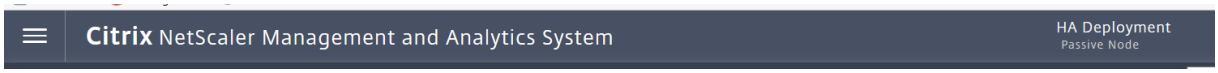
すべての NetScaler ADC インスタンスは、プライマリ NetScaler ADM ノードによって管理されます。

NetScaler ADM HA フェイルオーバーの場合、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。ライセンスは、猶予期間の終了までに新しいプライマリに再適用する必要があります。別の方法については、Citrix サポートにお問い合わせください。

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

いいえ。ただし、ロードバランサーがない場合は、NetScaler ADM ノードには独自の IP アドレスを使用してアクセスする必要があります。パッシブノードには「パッシブ」というタグが付いています。パッシブノードには構成を作成しないことをお勧めします。



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

いいえ

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

はい

NetScaler ADM HA ノード間で同期されるデータは何ですか

NetScaler ADM データベース全体が同期され、次のフォルダーが同期されます。

- /var/mps/テナント/ルート/
- /var/mps/ns_images/
- /var/mps/sdx_images/
- /var/mps/xen_nsvpx_images/
- /var/mps/cbwanopt_images/
- /var/mps/sdwanvw_images/
- /var/mps/mps_images/
- /var/mps/ssl_certs/

- /var/mps/ssl_keys/
- /mpsconfig/ssl/
- /var/mps/backup/
- /var/mps/esx_nsvpx_images/
- /var/mps/locdb/