NetScaler SDX 13.1

Machine translated content

Disclaimer

Contents

はじめに 4

リリースノート 4

管理サービスのユーザーインターフェイスの使用を開始する 4

データガバナンス 10

NetScaler SDX アプライアンス用 **NetScaler ADM** サービス接続の概要 13

シングルバンドルアップグレード 16

NetScaler インスタンスのアップグレード 18

SDX アプライアンスの管理と監視 21

SDX 管理ドメイン 27

SDX 22000 プラットフォームでの **RAID** ディスク割り当ての管理 29

SDX ライセンスの概要 32

SDX リソースビジュアライザー 35

インターフェースを管理する 36

SDX アプライアンス上のジャンボフレーム 40

SDX アプライアンスでの **SNMP** の設定 52

Syslog 通知の設定 57

メール通知の設定 58

SMS 通知を構成する 59

SDX アプライアンスに構成されたエンティティのステータスをリアルタイムで監視および管理する 60

NetScaler インスタンスで生成されるイベントの監視と管理 65

SDX アプライアンス上の **NetScaler** インスタンスの **Call Home** サポート 72

システムヘルスモニタリング 74

システム通知設定の構成 77

管理サービスの機能を有効または無効にする **78**

管理サービスを構成する **78**

認証と承認の設定を構成する **81**

外部認証サーバの設定 **86**

管理サービスからリンクアグリゲーションを構成する **92**

管理サービスからチャネルを設定する **92**

アクセス制御リスト **94**

NetScaler インスタンスのクラスターをセットアップする **100**

クラスタリンクアグリゲーションの設定 **104**

管理サービスに安全にアクセスするための **SSL** 暗号の設定 **108**

SDX アプライアンスの構成データをバックアップおよび復元する **116**

アプライアンスのリセットを実行する **120**

外部認証サーバのカスケード **123**

ユーザーをロック解除する **125**

NetScaler インスタンスのプロビジョニング **125**

暗号容量の管理 **140**

サードパーティ製仮想マシンのプロビジョニング **146**

SECUREMATRIX GSB **147**

Trend Micro の **InterScan Web Security** **151**

Websense Protector **152**

BlueCat DNS/DHCP **156**

CA アクセスゲートウェイ **160**

パロアルトネットワークス **VM** シリーズ **161**

Citrix SD-WAN VPX インスタンスを **NetScaler SDX** アプライアンスにデプロイします **164**

SDX での帯域幅メータリング **168**

NetScaler インスタンスの構成と管理 **172**

SSL 証明書のインストールと管理 **175**

NetScaler インスタンスで **L2** モードを許可する **179**

インターフェイス上での仮想 **MAC** の設定 **180**

パーティション **MAC** アドレスを生成して、**SDX** アプライアンスの **NetScaler** インスタンスに管理パーティションを構成します **182**

VPX インスタンスの変更管理 **184**

NetScaler インスタンスを監視する **185**

ログを使用して操作とイベントを監視する **189**

NetScaler SDX アプライアンスのユースケース **191**

管理サービスと **NetScaler** インスタンスが同じネットワークにある場合の統合 **192**

管理サービスと **NetScaler** インスタンスが異なるネットワークにある場合の統合 **193**

セキュリティゾーン間での統合 **195**

インスタンスごとに専用のインターフェースで統合 **196**

複数のインスタンスによる物理ポートの共有による統合 **198**

NITRO API **200**

NITRO パッケージの入手 **201**

.NET SDK **201**

REST ウェブサービス **206**

NITRO の仕組み **215**

Java SDK **215**

はじめに

November 23, 2023

NetScaler SDX アプライアンスは、複数の NetScaler 仮想マシン（インスタンス）をプロビジョニングおよび管理できるマルチテナントプラットフォームです。SDX アプライアンスは、単一の管理者がアプライアンスを構成および管理し、各ホストされたインスタンスの管理をテナントに委任できるようにすることで、クラウドコンピューティングおよびマルチテナンシーの要件に対応します。SDX アプライアンスを使用すると、アプライアンス管理者は各テナントに次の利点を提供できます。

- 1 つの完全なインスタンス。各インスタンスには、次の権限があります。
  - 専用の CPU およびメモリリソース
  - エンティティ用の別のスペース
  - リリースを実行し、選択したビルドへの独立性
  - ライフサイクルの独立性
- 完全に隔離されたネットワーク。特定のインスタンスに対するトラフィックは、そのインスタンスにのみ送信されます。

SDX アプライアンスは、アプライアンスに事前プロビジョニングされた管理サービスを提供します。Management Service は、アプライアンス、管理サービス、およびインスタンスを設定、管理、監視するためのユーザーインターフェイス (HTTP および HTTPS モード) と API を提供します。Citrix 自己署名証明書は、HTTPS をサポートするために事前にパッケージ化されています。管理サービスのユーザーインターフェイスにアクセスするには、HTTPS モードを使用することをお勧めします。

リリースノート

November 23, 2023

リリースノートでは、NetScaler ソフトウェアの特定のリリースやビルドで拡張されたり変更されたりした内容、解決された問題、および既知の問題について説明します。NetScaler SDX のリリースノートは、ADC リリースノートの一部として取り上げられています。

SDX 13.1 の拡張機能、既知の問題、およびバグ修正の詳細については、ADCリリースノートを参照してください。

管理サービスのユーザーインターフェイスの使用を開始する

November 23, 2023

アプライアンス、管理サービス、および仮想インスタンスの設定、管理、およびモニタリングを開始するには、ブラウザを使用して管理サービスのユーザーインターフェイスに接続します。その後、アプライアンス上で仮想インスタンスをプロビジョニングします。

Management Service ユーザーインターフェイスには、サポートされている次のブラウザのいずれかを使用して接続できます。

- Internet Explorer
- Google Chrome
- Apple Safari
- Mozilla Firefox

管理サービスのユーザーインターフェイスにログオンします

1. Web ブラウザのアドレスフィールドに、次のいずれかを入力します。

   ```
   http://Management Service IP Address
   ```

   または

   ```
   https://Management Service IP Address
   ```

2. 「ログイン」ページの「ユーザー名」と「パスワード」に、管理サービスのユーザー名とパスワードを入力します。デフォルトのユーザ名は`nsroot`です。デフォルトのパスワードが機能しない場合は、アプライアンスのシリアル番号を入力してみてください。シリアル番号のバーコードは、アプライアンスの背面にあります。デフォルトの認証情報で初めてログインしたら、`nsroot` デフォルトのパスワードを変更する必要があります。admin パスワードの変更については、デフォルトユーザアカウントのパスワードの変更を参照してください。

3. [オプションを表示] をクリックし、次の操作を行います。

   a) [開始場所] ボックスの一覧で、ユーザーインターフェイスにログオンした直後に表示する必要のあるページを選択します。使用可能なオプションは、[ホーム]、[監視]、[構成]、[ドキュメント]、[ダウンロード] たとえば、ログオン時に管理サービスに [構成] ページが表示されるようにするには、[起動] ボックスの一覧の [構成] を選択します。

   b) [タイムアウト] に、セッションの有効期限を分単位、時間単位、または日単位で入力します。タイムアウトの最小値は 15 分です。

   [開始時間] と [タイムアウト] の設定は、セッション間で保持されますこれらのデフォルト値は、キャッシュをクリアした後にのみ復元されます。

4. [ログイン] をクリックして、Management Service ユーザーインターフェイスにログオンします。

初期セットアップウィザード

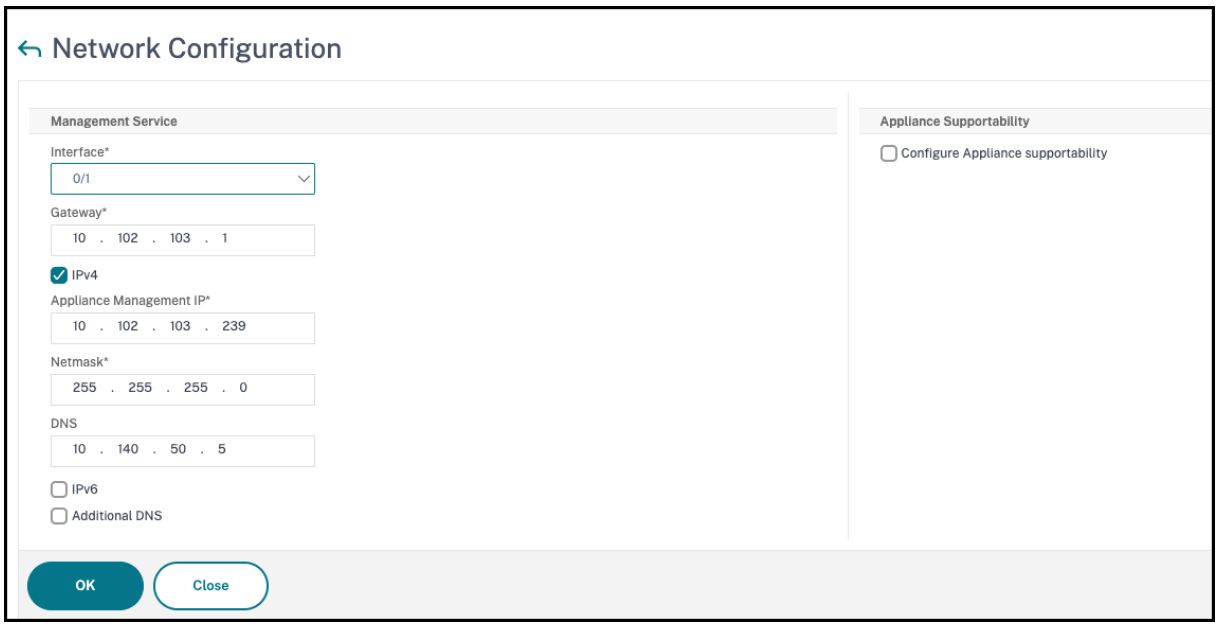
セットアップウィザードを使用すると、すべての初回設定を 1 つのフローで完了できます。

このウィザードを使用して、ネットワーク構成の詳細とシステム設定の構成、デフォルトの管理者パスワードの変更、ライセンスの管理と更新を行うことができます。

このウィザードを使用して、初期構成時に SDX アプライアンスに指定したネットワーク構成の詳細を変更することもできます。

ウィザードにアクセスするには、[構成**] > [**システム] に移動し、[アプライアンスのセットアップ] で [セットアップウィザード] をクリックします。次のパラメータの値を入力します。

- インターフェイス**:** アプライアンスを管理ワークステーションまたはネットワークに接続する管理インターフェイス。可能な値:0/1、0/2。デフォルト:0/1。
- **Gateway:** アプライアンスのサブネットからトラフィックを転送するルーターの IP アドレス。
- 管理サービスに IPv4 アドレスを使用する場合は、[IPv4] チェックボックスをオンにし、次のパラメータの詳細を入力します。
  - アプライアンス管理 **IP:** Web ブラウザを使用して管理サービスにアクセスするために使用される IPv4 アドレス。
  - **Netmask:** SDX アプライアンスが配置されているサブネットマスク。
- **DNS:** プライマリ DNS サーバの IPv4 アドレス。IPv6 アドレスは、プライマリ DNS サーバではサポートされていません。
- 管理サービスに IPv6 アドレスを使用する場合は、IPv6 チェックボックスを選択し、次のパラメータの詳細を入力します。
  - 管理サービスの **IP** アドレス**:** Web ブラウザを使用して管理サービスにアクセスするために使用される IPv6 アドレス。
  - ゲートウェイ **IPv6** アドレス**:** アプライアンスのサブネットからトラフィックを転送するルーターの IPv4 アドレス。
- **DNS** サーバの IP アドレスをプライマリ DNS サーバとは別に追加の DNS サーバとして追加するには、[追加の DNS] を選択します。IP アドレスは、IPv4 または IPv6 のいずれかになります。



> 重要:
>
> セキュリティを強化するために、アプライアンスのサポート機能を無効に Citrix ことをお勧めします。アプライアンスのサポートを無効にするには、[システム] **>** [ネットワーク構成] に移動し、[アプライアンスサポートの構成] チェックボックスをオフにします。

システム設定では、管理サービスと NetScaler インスタンスが安全なチャネル経由でのみ相互に通信するように指定できます。また、Management Service ユーザーインターフェイスへのアクセスを制限することもできます。クライアントは、https を使用しないと管理サービスユーザーインターフェイスにログオンできません。

管理サービスと Citrix Hypervisor のタイムゾーンを変更できます。デフォルトのタイムゾーンは UTC です。管理パスワードを変更するには、[**Change Password**] チェックボックスをオンにして新しいパスワードを入力します。

[ライセンスの管理] では、ライセンスを管理および割り当てることができます。ハードウェアシリアル番号 (HSN) またはライセンスアクセスコードを使用して、ライセンスを割り当てることができます。または、ローカルコンピューターにライセンスが既に存在する場合は、それをアプライアンスにアップロードできます。

アプライアンス上のライセンスを選択し、[**Done**] をクリックして初期設定を完了します。

SDX アプライアンスでのインスタンスのプロビジョニング

管理サービスを使用して、SDX アプライアンス上に 1 つ以上のまたはサードパーティインスタンスをプロビジョニングできます。インストールできるインスタンスの数は、購入したライセンスによって異なります。追加されるインスタンスの数がライセンスで指定された数に等しい場合、Management Service はこれ以上のインスタンスのプロビジョニングを許可しません。

サードパーティ製インスタンスのプロビジョニングについては、「サードパーティ製仮想マシン」を参照してください。

コンソールのアクセス

管理サービスインターフェイスから、NetScaler インスタンス、管理サービス、Citrix Hypervisor、およびサードパーティ仮想マシンのコンソールにアクセスできます。このアクセスは、SDX アプライアンスでホストされているインスタンスのデバッグやトラブルシューティングに役立ちます。

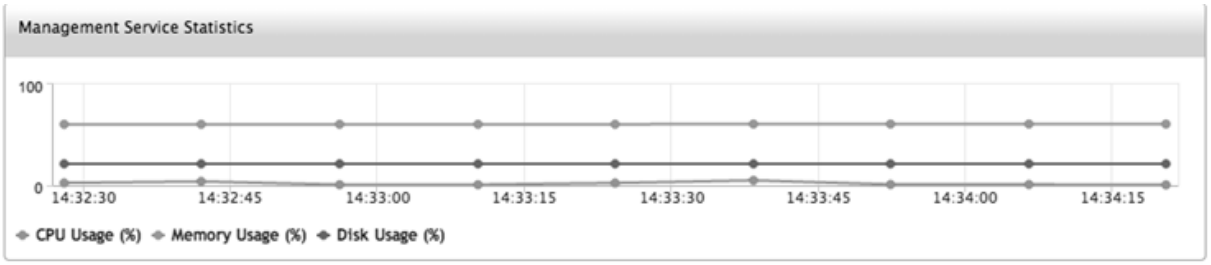
VM のコンソールにアクセスするには、インスタンスのリストに移動し、リストから仮想マシンを選択し、[アクション] リストで [コンソールアクセス] をクリックします。

管理サービスまたは Citrix Hypervisor のコンソールにアクセスするには、［構成］**>**［システム］に移動し、［コンソールアクセス］で［管理サービス］または［**Citrix Hypervisor** ］リンクをクリックします。

注:Internet Explorer ブラウザはコンソールアクセスをサポートしていません。コンソールアクセス機能は、管理サービスの HTTPS セッションでのみ使用することをお勧めします。

管理サービス統計

ダッシュボードには、SDX アプライアンス上の管理サービスによるメモリ、CPU、およびディスクリソースの使用状況を監視するための管理サービス統計が追加されました。



管理サービスと **NetScaler** インスタンスへのシングルサインオン

ユーザー認証情報を使用して Management Service にログオンした後は、インスタンスにログオンするためにユーザー認証情報を再度入力する必要はありません。既定では、[タイムアウト] の値は 30 分に設定され、[構成] タブは新しいブラウザウィンドウで開きます。

[ホーム**]** ページの管理

[Management Service Home] ページには、SDX アプライアンスおよびアプライアンスにプロビジョニングされたインスタンスのパフォーマンスの概要が表示されます。SDX アプライアンスとインスタンスに関する情報は、要件に応じて追加および削除できるガジェットに表示されます。

既定では、[ホーム] ページには次のガジェットが用意されています。

- システムリソース：アプライアンス上の CPU コアの総数、SSL チップの総数、空き SSL チップの数、合計メモリ、および空きメモリを表示します。

** システム CPU	メモリ使用量 (%): アプライアンスの CPU** とメモリの使用率をグラフ形式で表示します。

-

- システム **WAN/LAN** スループット **(Mbps):** 送受信トラフィックに対する SDX アプライアンスの合計スループットを、リアルタイムでプロットされ、定期的に更新されるグラフで表示します。
- **NetScaler** インスタンス**:NetScaler** インスタンスのプロパティを表示します。表示されるプロパティは、名前、VM の状態、インスタンスの状態、IP アドレス、Rx (Mbps)、Tx (Mbps)、HTTP Req/s、CPU 使用率 (%)、メモリ使用量 (%) です。
  注：最初のログオン時には、アプライアンスにインスタンスをプロビジョニングしていないため、ホームページに NetScaler インスタンスに関連するデータは表示されません。
- [ヘルスモニタリングイベント（**Health Monitoring Events**）]：過去 25 件のイベントを、その重大度、メッセージ、イベントが発生した日時とともに表示します

「ホーム」(Home) ページでは、次の操作を実行できます。

- NetScaler インスタンスの詳細を表示または非表示にする

  特定の NetScaler インスタンスの詳細を表示または非表示にするには、名前列のインスタンスの名前をクリックします。
  Expand All をクリックしてすべてのインスタンスノードを展開し、Collapse All をクリックしてすべてのインスタンスノードを折りたたむこともできます。

- ガジェットの追加と削除

  ガジェットを追加して、他のシステム情報を表示することもできます。

  これらのガジェットを追加するには、ホームページの右上隅にある矢印 («) ボタンをクリックし、検索ボックスにキーワードを入力して、[Go] をクリックします。使用できる文字は、a-z、A-Z、0—9、^、$、*、および _ です。検索ボックスに文字を入力せずに [実行] をクリックすると、使用可能なすべてのガジェットが表示されます。ガジェットが表示されたら、[ダッシュボードに追加] をクリックします。

  現在、「ホーム」(Home) ページには次のガジェットを追加できます。

  - ハイパーバイザーの詳細： Hypervisor Details ガジェットには、Citrix Hypervisor の稼働時間、エディション、バージョン、iSCSI 修飾名（IQN）、製品コード、シリアル番号、ビルド日、ビルド番号に関する詳細が表示されます。

- ライセンス**:** Licenses ガジェットには、SDX ハードウェアプラットフォーム、プラットフォームでサポートされるインスタンスの最大数、サポートされる最大スループット (Mbps)、使用可能なスループット (Mbps) の詳細が表示されます。

既定で [ホーム] ページに表示されているガジェットを削除した場合、ガジェットを検索して [ホーム] ページに追加し直すことができます。

ポート

SDX アプライアンスが正常に機能するには、SDX アプライアンス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	着信 HTTP (GUI および NITRO) 要求に使用されます。SDX Management Service インターフェイスにアクセスするための主要なインターフェイスの 1 つ。
TCP	443	着信するセキュア HTTP (GUI および NITRO) 要求に使用されます。SDX Management Service インターフェイスにアクセスするための主要なインターフェイスの 1 つ。
TCP	22	SDX 管理サービスインターフェイスへの SSH および SCP アクセスに使用されます。
UDP	162	SDX 管理サービスインターフェイスは、SDX アプライアンスでホストされている NetScaler インスタンスからの SNMP トラップを受信します。
UDP	161	SDX 管理サービスインターフェイスは SNMP ウォーク/GET リクエストをリッスンします。

データガバナンス

November 23, 2023

NetScaler ADM サービスコネクトとは何ですか?

NetScaler Application Delivery Management（ADM）サービスコネクトは、NetScaler SDX アプライアンスを NetScaler ADM サービスにシームレスにオンボーディングできるようにする機能です。この機能により、NetScaler SDX アプライアンスは自動的に NetScaler ADM サービスに安全に接続し、システム、使用状況、およびテレメトリデータをそのサービスに送信できます。このデータに基づいて、NetScaler ADM サービス上の NetScaler インフラストラクチャに関する洞察と推奨事項が得られます。

NetScaler ADM サービス接続機能を使用して NetScaler SDX アプライアンスを NetScaler ADM サービスにオンボーディングすることで、オンプレミスでもクラウドでも、すべての NetScaler および NetScaler Gateway 資産を管理できます。また、パフォーマンスの問題、高いリソース使用率、重大なエラーなどをすばやく特定するのに役立つ豊富な可視性機能を利用できるというメリットもあります。NetScaler ADM サービスは、NetScaler インスタンスとアプリケーションに幅広い機能を提供します。NetScaler ADM サービスの詳細については、「NetScaler Application Delivery Management サービス」を参照してください。

> 重要
>
> - このドキュメントは NetScaler SDX アプライアンスに関するものです。NetScaler アプライアンスの詳細については、「NetScaler アプライアンス用 NetScaler ADM サービス接続の概要」を参照してください。
> - NetScaler Gateway は、NetScaler ADM サービス接続機能もサポートしています。わかりやすくするために、NetScaler Gateway アプライアンスは連続するセクションでは明示的に呼び出されません。

注:
NetScaler ADM サービス接続機能が NetScaler インスタンスと NetScaler Gateway インスタンス向けにリリースされました。ただし、NetScaler ADM サービスの対応する機能は、今後のリリースで利用できるようになります。この機能の価値は、NetScaler ADM サービスのリリースで間もなく明らかになります。Citrix は、このノートが発生したときに更新されます。
この新機能のメリットは、NetScaler ADM サービスでリリースされた後でも使用できます。

NetScaler ADM サービスとは何ですか?

NetScaler ADM サービスは、NetScaler SDX インスタンスおよびアプリケーションの状態、パフォーマンス、およびセキュリティに関する分析的洞察と機械学習に基づく厳選された推奨事項を提供することにより、NetScaler SDX インスタンスの管理、監視、オーケストレーション、自動化、トラブルシューティングを支援するクラウドベースのソリューションです。詳細については、「NetScaler ADMサービスの概要」を参照してください。

NetScaler ADM サービス接続はどのようにして有効になっていますか

NetScaler SDX をリリース 13.1 にインストールまたはアップグレードすると、NetScaler ADM サービス接続がデフォルトで有効になります。

NetScaler ADM サービス接続を使用してキャプチャされるデータにはどのようなものがありますか**?**

次の詳細は、NetScaler ADM サービス接続を使用してキャプチャされます。

- **NetScaler SDX** の詳細
  - 管理 IP アドレス
  - プラットフォームの説明
  - プラットフォームタイプ
  - ホスト名
  - システム ID
  - エンコードされたシリアル ID
  - バージョン
  - シリアル ID
  - ホスト ID
  - 種類
  - ビルドタイプ
- 主な使用状況メトリック
  - 管理 CPU パーセンテージ
  - メモリ使用率
  - CPU の使用率
  - システム稼働時間
  - システム日時

データはどのように使用されますか

データを収集することで、NetScaler はお使いの NetScaler SDX インストールについて、次のような詳細情報をタイムリーに提供できます。

- 主要な指標。CPU、メモリ、スループット、SSL スループットに関する主要メトリックの詳細と、NetScaler SDX インスタンスでの異常な動作について説明します。
- 重大なエラー。NetScaler インスタンスで発生した可能性のある重大なエラー。
- 導入アドバイザリ。スタンドアロンモードでデプロイされているが、スループットが高く、単一障害点に対して脆弱な NetScaler インスタンスを特定します。

収集されたデータはどのくらいの期間保持されますか

収集されたデータは 13 か月以内に保持されます。

NetScaler ADM サービス接続機能を NetScaler から無効にしてサービスの使用を終了する場合、以前に収集されたデータは 30 日後に削除されます。

データはどこに保存され、どの程度安全ですか

NetScaler ADM Service Connect によって収集されたすべてのデータは、米国、欧州連合、オーストラリアとニュージーランド（ANZ）の 3 つの地域のいずれかに保存されます。詳細については、地理的考慮事項を参照してください。

データは、データベース層で厳密なテナント分離を使用して安全に保存されます。

NetScaler ADM サービス接続を無効にするにはどうすればよいですか?

NetScaler ADM サービス接続によるデータ収集を無効にする場合は、「NetScaler ADM サービス接続を有効または無効にする方法」を参照してください。

NetScaler SDX アプライアンス用 NetScaler ADM サービス接続の概要

November 23, 2023

NetScaler ADM サービスは、NetScaler SDX アプライアンスの管理、監視、オーケストレーション、自動化、トラブルシューティングに役立つクラウドベースのソリューションです。また、アプリケーションの正常性、パフォーマンス、およびセキュリティに関する分析情報と厳選された機械学習ベースの推奨事項も提供します。詳しくは、「NetScaler ADMサービス」を参照してください。

NetScaler Application Delivery Management（ADM）サービス接続は、NetScaler SDX アプライアンスを NetScaler ADM サービスにシームレスにオンボーディングできるようにする機能です。この機能により、NetScaler SDX アプライアンスと NetScaler ADM サービスが総合的なソリューションとして機能し、お客様にさまざまなメリットをもたらします。

NetScaler ADM サービス接続機能により、NetScaler SDX インスタンスは自動的に NetScaler ADM サービスに接続し、システム、使用状況、およびテレメトリデータをそのサービスに送信できます。NetScaler ADM サービスでは、このデータを使用して、パフォーマンスの問題やリソースの使用率が高い場合の迅速な特定など、NetScaler SDX インフラストラクチャに関する洞察や推奨事項を提供します。

NetScaler ADM サービスの機能を活用するには、NetScaler SDX アプライアンスを NetScaler ADM サービスにオンボードすることを選択できます。オンボーディングプロセスでは ADM Service Connect を使用し、シームレスで迅速なエクスペリエンスを実現します。

> 注意事項
>
> - NetScaler ADM サービス接続は、NetScaler MPX、SDX、VPX インスタンス、および NetScaler Gateway アプライアンスで利用できるようになりました。
> - NetScaler ADM サービス接続は、NetScaler ADM サービスではまだ利用できません。

詳しくは、「データガバナンス」を参照してください。

NetScaler ADM サービスはサポートを **NetScaler ADM** サービスに接続する方法を教えてください

NetScaler の NetScaler ADM サービス接続機能が NetScaler ADM サービスとどのように相互作用するかについての大まかなワークフローを次に示します。

1. NetScaler SDX アプライアンスの NetScaler ADM サービス接続機能は、定期的なプローブリクエストを使用して NetScaler ADM サービスに自動接続します。
2. このリクエストにはシステム、使用状況、テレメトリデータが含まれます。NetScaler ADM サービスは、これらを使用して NetScaler ADM サービスから、パフォーマンスの問題や高いリソース使用量の迅速な特定など、NetScaler インフラストラクチャに関する洞察や推奨事項を提供します。
3. 洞察と推奨事項を確認したら、NetScaler SDX アプライアンスを NetScaler ADM サービスにオンボーディングして NetScaler SDX アプライアンスの管理を開始することを決定できます。
4. オンボーディングを決定すると、NetScaler ADM サービス接続機能によりオンボーディングをシームレスに完了できます。

NetScaler ADM サービス接続はどのバージョンの **NetScaler** でサポートされていますか

NetScaler ADM サービス接続は、すべての NetScaler プラットフォームとすべてのアプライアンスモデル（MPX、VPX、および SDX）でサポートされています。NetScaler リリース 13.0 ビルド 64.xx 以降、NetScaler SDX アプライアンスでは NetScaler ADM サービス接続がデフォルトで有効になっています。

NetScaler ADM サービス接続を有効にする方法を教えてください

NetScaler の既存のお客様で、NetScaler リリース 13.0 ビルド 64.xx にアップグレードすると、アップグレードプロセスの一部として NetScaler ADM サービス接続がデフォルトで有効になります。

NetScaler を初めてご利用のお客様は、NetScaler リリース 13.0 ビルド 64.xx をインストールすると、インストールプロセスの一部として NetScaler ADM サービス接続がデフォルトで有効になります。

> 注
>
> 新しい NetScaler アプライアンスとは異なり、既存の NetScaler SDX アプライアンスは Citrix インサイトサービス（CIS）または Call Home を介してルートを検索します。

NetScaler ADM サービス接続を有効または無効にする方法を教えてください

NetScaler ADM サービス接続は、CLI、GUI、または NITRO API メソッドから有効または無効にできます。

CLI での手順

NetScaler ADM サービスを有効にするには、CLI を使用して接続します。

コマンドプロンプトで入力します:

```
set autoreg_setting autoreg=true
```

NetScaler ADM サービスを無効にするには、CLI を使用して接続します。

コマンドプロンプトで入力します:

```
set autoreg_setting autoreg=false
```

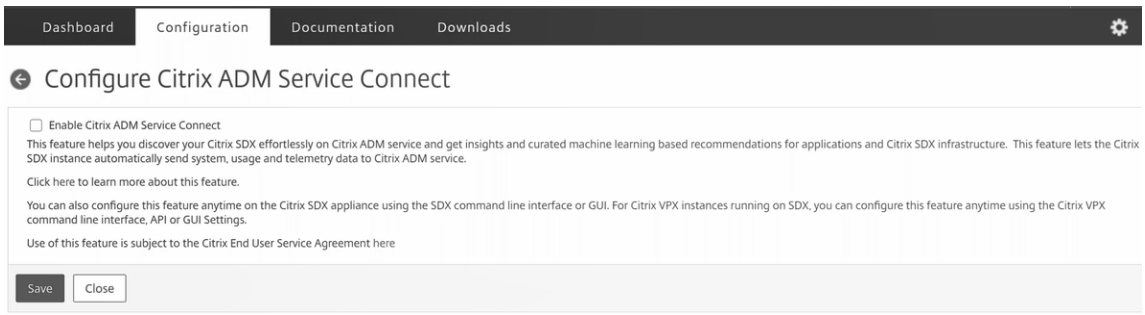
CLI を使用して NetScaler ADM サービスの接続設定を表示するには

```
show autreg_setting

                autoreg: true

     is_banner_displayed: true

Done
```

GUI の使用

NetScaler ADM サービスを無効にするには、NetScaler GUI を使用して接続します。

1. [システム] に移動します。[システム] ページの [システム設定] セクションの [**NetScaler ADM** サービス接続の構成] をクリックします。
2. **ADM** パラメーターの設定ページで、「****NetScaler ADM** サービス接続を有効にする」をオフにして、「OK」をクリックします。**



NITRO API の使用

NetScaler ADM サービス接続を無効にするには、NITRO コマンドを使用します。


```
curl -X PUT -H "Content-Type:application/json"http://192.0.2.10/nitro
/v1/config/sdx_autoreg -d '{ "sdx_autoreg":{ "autoreg":"false" } } '
-u nsroot:Test@1
```

NetScaler ADM ビルトインエージェントの動作

NetScaler リリース 13.0 ビルド 61.xx 以降では、NetScaler SDX インスタンスには ADM サービス接続機能を備えたエージェントが組み込まれています。NetScaler SDX インスタンスで使用可能な NetScaler ADM 組み込みエージェントは、アクティブなデーモンのように起動し、ADM サービスと通信します。ADM サービスとの通信が確立されると、組み込みエージェントは定期的に最新のソフトウェアバージョンに自動的にアップグレードされます。

参照ドキュメント

NetScaler ADM サービス接続の詳細については、以下のトピックを参照してください。

- データガバナンス：データガバナンス。
- NetScaler ADM サービス：NetScaler Application Delivery Management サービス。

シングルバンドルアップグレード

November 23, 2023

注： NetScaler SDX アプライアンスをリリース 13.1 にインストールまたはアップグレードすると、NetScaler ADM サービス接続がデフォルトで有効になります。詳しくは、「データガバナンスと NetScalerADM サービス接続」を参照してください。

11.0 以降のリリースから利用できる単一バンドルアップグレードでは、NetScaler VPX インスタンスイメージと LOM ファームウェアを除くすべてのコンポーネントが 1 つのイメージファイルに統合されます。このファイルを SDX イメージと呼びます。

> （注
>
> ）リリース 12.0 ビルド 57.19 から、ライトアウト管理（LOM）ファームウェアが SBI に追加され、Citrix お客様は LOM を個別にアップグレードする必要はありません。LOM ファームウェアは Citrix によって作成されていません。

このイメージを使用すると、すべてのコンポーネントを 1 回の手順でアップグレードできるため、さまざまなコンポーネント間で非互換性が生じる可能性を排除できます。また、1 つのバンドルをアップグレードするだけで、シトリックスがテストしてサポートしているバージョンをアプライアンスが常に実行できるようになります。すべての SDX

コンポーネントが 1 つのファイルにまとめられているため、SDX イメージファイルは管理サービスイメージファイルよりも大きくなります。

イメージのファイル名は`build-sdx-13.1-<build_number>.tgz`の形式です。管理サービスを SDX 13.1 にアップグレードすると、新しい GUI に Citrix Hypervisor イメージファイル、サプリメンタルパック、または修正プログラムをアップロードするオプションが表示されません。SDX 13.1 では個々のコンポーネントのアップグレードがサポートされていないため、オプションがありません。

注意事項

- シングルバンドルのアップグレードは複数ステップのプロセスで、最大 90 分かかる場合があります。
- まず、管理サービスが提供された新しいバージョンにアップグレードされます。アップグレード中、管理サービスへの接続が失われることがあります。管理サービスに再接続して、アップグレードのステータスを監視します。
- 次に、新しい管理サービスによって Citrix Hypervisor がアップグレードされ、アプライアンスの残りのアップグレードが完了します。リリース 11.0 以降の管理サービスでは、Citrix Hypervisor のフルアップグレードを実行できます。
- Citrix Hypervisor のアップグレード中は、アプライアンスを再起動しないでください。
- Citrix Hypervisor のアップグレードを監視するには、Citrix Hypervisor シリアルコンソール（Citrix Hypervisor LOM コンソール）を使用することをお勧めします。

アプライアンス全体を **13.1** にアップグレードする

注：アップグレードプロセスでは、すべての VPX インスタンスを含む SDX アプライアンス全体が複数回再起動されます。この手順を実行する前に、VPX インスタンスが HA セットアップの場合は、すべてのプライマリ HA ノードをセカンダリノードにフェイルオーバーします。HA を導入していない場合は、それに応じてダウンタイムを計画してください。

アプライアンスをアップグレードするには、次の手順を実行します。

1. 単一バンドルイメージファイルをアップロードし、[設定**] > [**管理サービス**] > [**ソフトウェアイメージ] に移動し、[アップロード] をクリックします。
2. [構成**] > [**システム**] > [**システム管理**]** に移動します。
3. [システム管理] グループで、[アプライアンスのアップグレード] をクリックします。
   アップグレードプロセスには数分かかります。

アップグレードの前に、管理サービスは次の情報を表示します。

- 単一バンドルイメージファイル名。
- アプライアンスで実行されている SDX の現在のバージョン。
- アプライアンスのアップグレード先として選択されているバージョン。
- アプライアンスのアップグレードにかかるおおよその時間。

- その他の情報。

Appliance のアップグレードをクリックする前に、画面に表示されている情報をすべて確認しておいてください。いったん起動したアップグレードプロセスを中止することはできません。

サポートされるアップグレードパス

	11.1	12.0	12.1	13.0	13.1	14.1
10.5 または 11.0	Y	Y	Y	N*	N*	N*
11.1—65.x およびそれ以降	-	非推奨	12.1-56.x およびそれ以降	Y	Y	Y
12.1	-	-	非推奨	Y	Y	Y

* 10.5、11.0、11.1 の古いビルドでは、最初にリリース 11.1 または 12.1 にアップグレードしてから、リリース 13.0、13.1、または 14.1 にアップグレードする必要があります。

関連情報

NetScaler SDX ハードウェアとソフトウェアの互換性マトリックス

NetScaler SDX アプライアンスのアップグレードプロセスの謎を解き明かす

NetScaler インスタンスのアップグレード

November 23, 2023

> メモ
>
> - NetScaler SDX アプライアンスをリリース 13.1 にインストールまたはアップグレードすると、NetScaler ADM サービス接続がデフォルトで有効になります。詳しくは、「データガバナンスと NetScalerADM サービス接続」を参照してください。
> - NetScaler SDX アプライアンスのアップグレードプロセスでは、バージョン 13.1 ビルド 37.x 以降では 2 回再起動するのではなく、1 回の再起動が必要です。

NetScaler インスタンスをアップグレードするプロセスには、ビルドファイルをアップロードしてから NetScaler インスタンスをアップグレードする必要があります。

> 重要
>
> 管理サービスを使用した ADC インスタンスのダウングレードはサポートされていません。インスタンス CLI を使用してダウングレードします。

NetScaler インスタンスをアップグレードする前に、NetScaler SDX アプライアンスに NetScaler ソフトウェアイメージをアップロードします。新しいインスタンスをインストールするには、NetScaler XVA ファイルが必要です。

［ソフトウェアイメージ］ペインでは、次の詳細を表示できます。

- 名前**:** NetScaler インスタンスのソフトウェアイメージファイルの名前。ファイル名にはリリース番号とビルド番号が含まれます。たとえば、build-10-53.5_nc.tgz というファイル名は、リリース 10 ビルド 53.5 を指します。
- 最終更新日**:** ファイルが最後に変更された日付。
- サイズ**:** ファイルのサイズ (MB 単位)。

ソフトウェアイメージをアップロードするには

1. ナビゲーションペインで［NetScaler］を展開し、［ソフトウェアイメージ］をクリックします。
2. ソフトウェアイメージペインで、「アップロード」をクリックします。
3. ［ソフトウェアイメージのアップロード］ダイアログボックスで［参照］をクリックし、アップロードするイメージファイルを選択します。
4. ［アップロード］をクリックします。NetScaler ソフトウェアイメージペインにイメージファイルが表示されます。

ビルドファイルをダウンロードしてバックアップを作成するには

1. ［ソフトウェアイメージ］ペインで、ダウンロードするファイルを選択し、［ダウンロード］をクリックします。
2. メッセージボックスの [保存] リストから [名前を付けて保存] を選択します。
3. [名前を付けて保存] メッセージボックスで、ファイルを保存する場所に移動し、[保存] をクリックします。

XVA ファイルをアップロードするには

1. ナビゲーションペインで［NetScaler］を展開し、［ソフトウェアイメージ］をクリックします。
2. ［ソフトウェアイメージ］ペインの［**XVA** ファイル］タブで、［アップロード］をクリックします。
3. **NetScaler XVA** ファイルのアップロードダイアログボックスで、「ブラウズ」をクリックし、アップロードする NetScaler XVA ファイルを選択します。
4. ［アップロード］をクリックします。XVA ファイルが **XVA** ファイルペインに表示されます。

XVA ファイルをダウンロードしてバックアップを作成するには

1. [XVA ファイル] ペインで、ダウンロードするファイルを選択し、[ダウンロード] をクリックします。
2. メッセージボックスの [保存] リストから [名前を付けて保存] を選択します。
3. [名前を付けて保存] メッセージボックスで、ファイルを保存する場所を参照し、[保存] をクリックします。

NetScaler VPX インスタンスのアップグレード

Management Service を使用して、アプライアンスで実行されている 1 つ以上の VPX 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、SDX アプライアンスに正しいビルドがアップロードされていることを確認してください。

インスタンスのアップグレードを開始する前に、ライセンスフレームワークとライセンスの種類について理解しておく必要があります。ソフトウェアエディションのアップグレード (スタンダードエディションからエンタープライズエディションへ、エンタープライズエディションからプラチナエディションへなど) には、新しいライセンスが必要になる場合があります。また、次の点にも注意してください。

- 設定が失われないように、インスタンスをアップグレードする前に、各インスタンスに設定を保存してください。
- [Instances] ノードから個々のインスタンスをアップグレードすることもできます。そのためには、[Instances] ノードからインスタンスを選択します。詳細ペインでインスタンスを選択し、[アクション] ドロップダウンメニューで [アップグレード] をクリックします。

> 重要
>
> :VPX GUI ではなく SDX Management Service を使用して VPX インスタンスをアップグレードする場合、アップグレードイメージはバックアップファイルの一部であり、インスタンスをスムーズに復元できます。

VPX インスタンスをアップグレードするには

1. ［構成］タブのナビゲーションペインで、［**NetScaler**］をクリックします。
2. 詳細ペインの［**NetScaler** 構成］で、［アップグレード］をクリックします。
3. ［のアップグレード］ダイアログボックスの［ソフトウェアイメージ］で、アップグレードするバージョンのアップグレードビルドファイルを選択します。
4. [**Instance IP Address**] ドロップダウンリストから、アップグレードするインスタンスの IP アドレスを選択します。
5. 「**OK**」をクリックし、「閉じる」をクリックします。

関連情報

NetScaler SDX ハードウェアとソフトウェアの互換性マトリックス

NetScaler SDX アプライアンスのアップグレードプロセスの謎を解き明かす

SDX アプライアンスの管理と監視

February 16, 2024

NetScaler SDX アプライアンスが稼働したら、管理サービスのユーザーインターフェイスからさまざまなタスクを実行してアプライアンスを管理および監視できます。

SDX アプライアンスのネットワーク構成を変更する

SDX アプライアンスに対して指定したネットワーク構成の詳細は、初期構成時に変更できます。

SDX アプライアンスのネットワーク設定を変更するには、[システム] をクリックします。システム・ペインの「セットアップ・アプライアンス」グループで、「ネットワーク構成」をクリックし、ウィザードに詳細を入力します。

> 注：ネットワーク構成で、Citrix Hypervisor へのアクセスを有効にすると、「6 時間後にアクセスが自動的に無効になります」という警告メッセージが表示されます。

既定のユーザーアカウントのパスワードを変更する

デフォルトのユーザーアカウントでは、NetScaler SDX アプライアンスのすべての機能に完全にアクセスできます。セキュリティを維持するために、デフォルトの管理者アカウントは必要な場合にのみ使用してください。フルアクセスを必要とする職務を持つ個人だけが、デフォルトの admin アカウントのパスワードを知っている必要があります。デフォルトの管理者パスワードを頻繁に変更することをお勧めします。パスワードを忘れた場合は、アプライアンスの設定を工場出荷時のデフォルトに戻してパスワードをデフォルトにリセットし、パスワードを変更できます。

デフォルトユーザアカウントのパスワードを変更するには、**[** システム] > [ユーザ管理] > [ユーザ] の順にクリックします。ユーザを選択し、**[**Edit**] をクリックしてパスワードを変更します。

アプライアンスのタイムゾーンを変更する

管理サービスと Citrix Hypervisor のタイムゾーンを変更できます。デフォルトのタイムゾーンは UTC です。

タイムゾーンを変更するには、[システム] をクリックし、[システム設定] グループの [タイムゾーンの変更] をクリックします。

アプライアンスのホスト名を変更する

管理サービスのホスト名を変更するには、[システム] > **[**システム設定**] > [**ホスト名の変更] に移動します。
Citrix Hypervisor のホスト名は、バックアップ/リストア操作中にバックアップおよび復元されます。構成をリセットすると、Citrix Hypervisor のホスト名がデフォルト値の「netscaler-sdx」にリセットされます。

VLAN フィルタリング

VLAN フィルタリングは、物理ポートを共有する VPX インスタンス間でデータを分離します。たとえば、2 つの異なる VLAN に 2 つの VPX インスタンスを構成し、VLAN フィルタリングを有効にした場合、一方のインスタンスはもう一方のインスタンスのトラフィックを表示できません。VLAN フィルタリングが無効の場合、すべてのインスタンスでタグ付きまたはタグなしブロードキャストパケットを参照できますが、パケットはソフトウェアレベルでドロップされます。VLAN フィルタリングが有効の場合、各タグ付きブロードキャストパケットは、対応するタグ付き VLAN に属するインスタンスにのみ到達します。対応するタグ付き VLAN に属するインスタンスがない場合、パケットはハードウェアレベル (NIC) でドロップされます。

インターフェイスで VLAN フィルタリングが有効になっている場合、そのインターフェイスでは限られた数のタグ付き VLAN を使用できます。10 G インターフェイスでは 63 個のタグ付き VLAN、1 G インターフェイスには 32 個のタグ付き VLAN があります。VPX インスタンスは、VLAN ID が設定されたパケットのみを受信します。インターフェイスで VLAN フィルタの状態を DISABLED から ENABLED に変更した場合は、そのインターフェイスに関連付けられている VPX インスタンスを再起動します。

SDX アプライアンスでは、VLAN フィルタリングがデフォルトで有効になっています。インターフェイスで VLAN フィルタリングを無効にすると、そのインターフェイスに最大 4096 個の VLAN を設定できます。

注: VLAN フィルタリングは、Citrix Hypervisor バージョン 6.0 を実行している SDX アプライアンスでのみ無効にできます。

インターフェイスで VLAN フィルタリングを有効にするには、[システム] > [インターフェイス] をクリックします。インターフェイスを選択して [**VLAN Filter**] をクリックし、詳細を入力して VLAN フィルタリングを有効にします。

クロック同期の設定

ネットワークタイムプロトコル (NTP) 同期を有効にすると、管理サービスが再起動されます。SDX アプライアンスのローカルクロックを NTP サーバと同期するように設定できます。その結果、SDX アプライアンスの時計は、ネットワーク上の他のサーバーと同じ日時設定になります。アプライアンスが再起動、アップグレード、またはダウングレードされても、クロック同期の設定は変更されません。ただし、高可用性セットアップでは、構成はセカンダリ NetScaler インスタンスに伝達されません。

NTP サーバを追加したり、認証パラメータを変更したりすると、クロックはただちに同期されます。NTP 同期を明示的に有効または無効にすることもできます。

注：ローカルの NTP サーバーがない場合は、公式 NTP サイト http://www.ntp.orgで公開されているオープンアクセスの NTP サーバーのリストを確認できますパブリック NTP サーバーを使用するように NetScaler を構成する前に、「契約ルール」ページ（すべてのパブリックタイムサーバーページに含まれるリンク）を必ずお読みください。

NTP サーバを設定するには、[システム**] > [NTP** サーバ] をクリックします。

NTP 同期を有効にするには

1. ナビゲーションウィンドウで [システム] を展開し、[**NTP** サーバー] をクリックします。
2. 詳細ウィンドウで、[**NTP** 同期] をクリックします。
3. [**NTP** 同期] ダイアログボックスで、[**NTP** 同期を有効にする] を選択します。
4. 「**OK**」をクリックし、「閉じる」をクリックします。

認証オプションを変更するには

1. ナビゲーションウィンドウで [システム] を展開し、[**NTP** サーバー] をクリックします。
2. 詳細ウィンドウで、[認証パラメーター] をクリックします。
3. [認証オプションの変更] ダイアログボックスで、次のパラメータを設定します。

    - [認証]：NTP 認証を有効にします。可能な値: はい、いいえ。デフォルト: はい。
    - 信頼されるキー **ID**-信頼されるキー ID。NTP サーバを追加するときに、このリストからキー ID を選択します。最小値:1。最大値:65534
    - [**Revoke Interval**]：自動キー方式で使用される特定の暗号化値を 2 の累乗で再ランダム化する間隔（秒単位）。デフォルト値は 17 (2^17=36 時間) です。
    - [**Automax Interval**]：Autokey プロトコルで使用されるセッションキーリストを 2 の累乗で再生成する間隔（秒単位）。デフォルト値は 12 (2^12=1.1 時間) です。

4. 「**OK**」をクリックし、「閉じる」をクリックします。

SDX アプライアンスのプロパティを表示する

[**Configuration**] タブで、CPU コアと SSL チップの数、使用可能なメモリと空きメモリの合計、さまざまな製品の詳細などのシステムプロパティを表示します。

SDX アプライアンスのプロパティを表示するには、［構成］タブをクリックします。

システムリソース、ハイパーバイザー、ライセンス、およびシステムに関する次の情報を表示できます。

システムリソース**:**

- 合計 **CPU** コア：SDX アプライアンス上の CPU コア数。
- **SSL** チップの合計**:** SDX アプライアンス上の SSL チップの総数。

- 無料 **SSL** チップ**:** インスタンスに割り当てられていない SSL チップの総数。
- 合計メモリ **(GB):** アプライアンスの合計メモリ (GB)。
- 空きメモリ **(GB):** アプライアンスの空きメモリ (GB)。

ハイパーバイザー情報**:**

- **Uptime:** アプライアンスが最後に再起動されてからの時間（日数、時間数、分数）。
- エディション： SDX アプライアンスにインストールされている Citrix Hypervisor のエディションです。
- バージョン： SDX アプライアンスにインストールされている Citrix Hypervisor のバージョン。
- **iSCSI IQN:** iSCSI 修飾名。
- 製品コード： Citrix Hypervisor の製品コードです。
- シリアル番号： Citrix Hypervisor のシリアル番号。
- ビルド日： Citrix Hypervisor のビルド日。
- ビルド番号： Citrix Hypervisor のビルド番号。
- サプリメンタルパック： SDX アプライアンスにインストールされているサプリメンタルパックのバージョン。

ライセンス情報**:**

- **Platform:** インストールされているライセンスに基づいた、ハードウェアプラットフォームのモデル番号。
- 最大インスタンス数**:** インストールされているライセンスに基づいて、SDX アプライアンスに設定できるインスタンスの最大数です。
- 使用可能なインスタンス **(**共有**):** まだ使用可能な CPU コアの数に応じて構成できるインスタンスの数。
- 最大スループット **(Mbps):** インストールされているライセンスに基づいて、アプライアンスで達成できる最大スループット。
- 使用可能なスループット **(Mbps):** インストールされているライセンスに基づく使用可能なスループット。

システム情報**:**

- **Platform:** ハードウェアプラットフォームのモデル番号。
- 製品： NetScaler 製品の種類です。
- ビルド： SDX アプライアンス上で実行される NetScaler のリリースおよびビルド。
- **IP** アドレス**:** 管理サービスの IP アドレス。
- ホスト **ID**： Citrix Hypervisor のホスト ID。
- システム **ID**： Citrix Hypervisor のシステム ID。
- シリアル番号：Citrix Hypervisor のシリアル番号。

- システム時刻**:** システム時刻は日月日付時: 分: 秒タイムゾーン年形式で表示されます。
- **Uptime:** 管理サービスが最後に再起動されてからの経過時間 (日数、時間数、分数)。
- **BIOS** バージョン**:** BIOS バージョン。

アプライアンスのスループットをリアルタイムで表示

SDX アプライアンスの送受信トラフィックの合計スループットは、定期的に更新されるグラフにリアルタイムでプロットされます。デフォルトでは、受信トラフィックと送信トラフィックの両方のスループットがグラフにまとめてプロットされます。

SDX アプライアンスのスループットを表示するには、GUI で [ダッシュボード] をクリックし、[システムスループット **(Mbps)**] をオンにします。

CPU とメモリの使用率をリアルタイムで表示

アプライアンスの CPU およびメモリ使用量のグラフを表示できます。グラフはリアルタイムでプロットされ、一定の間隔で更新されます。

SDX アプライアンスの CPU およびメモリ使用率を表示するには、GUI で [ダッシュボード] をクリックし、[管理サービス統計] をオンにします。

すべてのコアの **CPU** 使用率を表示する

SDX アプライアンス上の各 CPU コアの使用状況を表示できます。

[**CPU** コア使用量] ペインには、次の詳細が表示されます。

- コア番号**:** アプライアンスの CPU コア番号。
- 物理 **CPU:** そのコアの物理 CPU 番号。
- ハイパースレッド**:** その CPU コアに関連付けられているハイパースレッド。
- インスタンス**:** その CPU コアを使用しているインスタンス。
- 平均コア使用量**:** 平均コア使用率。パーセンテージで表されます。

SDX アプライアンスのすべてのコアの CPU 使用率を表示するには、GUI で [ダッシュボード] をクリックし、[システム **CPU** 使用率 **(%)**] をオンにします。

SDX アプライアンスに **SSL** 証明書をインストールする

SDX アプライアンスには、デフォルトの SSL 証明書が付属しています。セキュリティ上の理由から、この証明書を独自の SSL 証明書に置き換えることをお勧めします。そのためには、SSL 証明書を Management Service にアップロードしてから、証明書をインストールする必要があります。SSL 証明書をインストールすると、管理サービスとの現在のクライアントセッションがすべて終了します。管理サービスにログオンして、その他の構成タスクを実行してください。

SSL 証明書をインストールするには、[システム] をクリックします。「アプライアンスのセットアップ」グループで、「**SSL** 証明書のインストール」をクリックし、ウィザードに詳細を入力します。

管理サービスで **SSL** 証明書を表示する

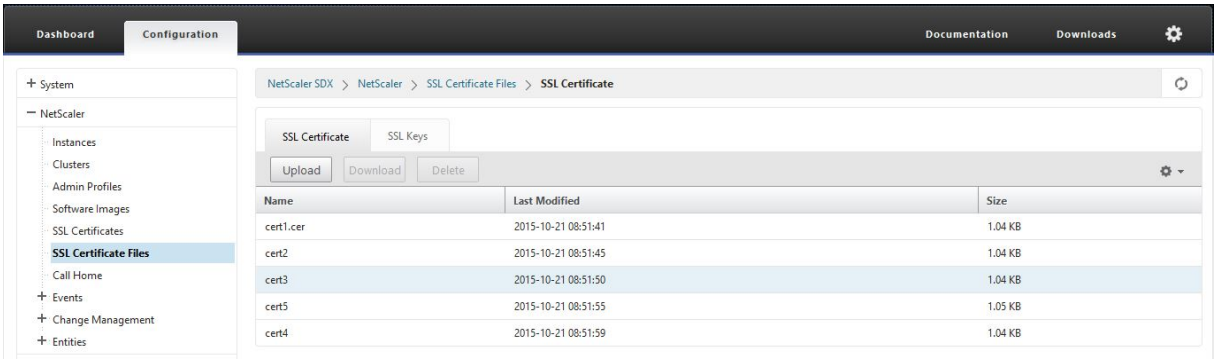
管理サービスは SSL 証明書を使用してクライアント接続をセキュリティで保護します。有効ステータス、発行者、件名、有効期限、有効期間の開始日と終了日、バージョン、シリアル番号など、この証明書の詳細を表示します。

SSL 証明書を表示するには、[システム] をクリックし、[アプライアンスのセットアップ] グループで [**SSL** 証明書の表示] をクリックします。

NetScaler インスタンスの **SSL** 証明書とキー

NetScaler インスタンスの SSL 証明書とキーを個別に表示できるため、操作性が向上します。NetScaler インスタンスにインストールできる SSL 証明書と対応する公開鍵と秘密鍵のペアをアップロードおよび管理するには、新しい管理サービスノードである SSL 証明書ファイルを使用します。

NetScaler インスタンスの SSL 証明書とキーにアクセスするには、[構成**] > [NetScaler] > [SSL** 証明書ファイル] に移動します。



システム設定の変更

セキュリティ上の理由から、Management Service と VPX インスタンスは安全なチャネル経由でのみ相互に通信する必要があることを指定できます。また、Management Service ユーザーインターフェイスへのアクセスを制限

することもできます。クライアントは、https を使用しないと管理サービスユーザーインターフェイスにログオンできません。

システム設定を変更するには、[構成**] > [**システム] をクリックし、[システム設定] グループで [システム設定の変更] をクリックします。

アプライアンスの再起動

管理サービスには、SDX アプライアンスを再起動するオプションがあります。再起動時に、アプライアンスはホストされているすべてのインスタンスをシャットダウンし、Citrix Hypervisor を再起動します。Citrix Hypervisor が再起動すると、ホストされているすべてのインスタンスが管理サービスとともに起動されます。

アプライアンスを再起動するには、[構成**] > [**システム] をクリックし、[システム管理] グループで [アプライアンスの再起動**]** をクリックします。

アプライアンスをシャットダウンする

管理サービスから SDX アプライアンスをシャットダウンできます。

アプライアンスをシャットダウンするには、[構成**] > [**システム] をクリックし、[システム管理] グループで [アプライアンスのシャットダウン] をクリックします。

SDX 管理ドメイン

November 23, 2023

SDX 管理ドメイン機能を使用すると、複数の管理ドメインを作成できます。管理ドメインを使用して、部門ごとにリソースを分けることができます。したがって、管理ドメインはリソースに対する制御を向上させ、リソースをさまざまなドメインに分散して最適に使用することができます。

SDX アプライアンスには、CPU コア、データスループット、メモリ、ディスク容量、SSL チップ、プロビジョニング可能な特定のインスタンス数などの固定リソースが付属しています。作成できるインスタンスの数はライセンスによって異なります。

SDX アプライアンスは、最大 3 つのレベルの管理ドメインをサポートします。アプライアンスが出荷されると、すべてのリソースが所有者に割り当てられます。

作成した管理ドメインはすべて、所有者ドメインのサブドメインです。いずれの場合も、サブドメインのリソースは親ドメインのリソースプールから割り当てられます。管理ドメイン内のユーザーは、そのドメインのリソースにアクセスできます。同じ階層レベルにある他のドメインのリソースや、自分のドメインに割り当てられていない親ドメインのリソースにはアクセスできません。ただし、親ドメインのユーザーは、そのドメインのサブドメインのリソースにアクセスできます。

リソースをサブドメインに割り当てる例

表 1 に、デフォルトルートドメインのリソースを示します。SDX 管理者はこれらのリソースをサブドメインに割り当てることができます。この場合、管理者は最大 10 個の CPU コアと 840 GB のディスク領域を割り当てることができます。

表 1. オーナーリソース

CPU コア	10
スループット (Mbps)	18500
メモリ (MB)	87300
ディスク容量 (GB)	840
SSL チップ	36
インスタンス	36

表 2 に、
Test という名前のサブドメインに割り当てられているリソースを示します。このサブドメインには、親ドメインの 10 個の CPU コアのうち 5 個が割り当てられ、残りの 5 個のコアは Owner の他のサブドメインに割り当てることができます。

表 2. テストドメインのリソース

CPU コア	5
スループット (Mbps)	1024
メモリ (MB)	2048
ディスク容量 (GB)	40
SSL チップ	8
インスタンス	4

サブドメインを作成する場合、*Test* ドメイン管理者は表 2 に示すリソースのみを割り当てることができます。作成できるドメインは 3 つのレベルしかないため、*Test* ドメインにはサブドメインのレベルが 1 つしかありません。

次の図は、表 1 および 2 に示した値とは異なる値を使用した、サブドメイン間でのリソース割り当ての別の例を示しています。

管理ドメインを作成するには、[構成] **>** [システム] **>** [管理ドメイン] に移動し、必要なオプションを選択します。画面の指示に従います。新しいドメインを作成したら、Management Service のログインページを使用してこのドメインにログインし、ドメイン名とユーザー名を入力します。たとえば、NewDomain という名前のドメインをユーザ newUser で作成した場合は、newDomain\ NewUser としてログインします。

ユーザーをドメインに割り当てる

サブドメインが作成されると、管理者グループと読み取り専用グループの 2 つのユーザーグループが自動的に作成されます。デフォルトでは、各ユーザーは管理者グループの一員です。1 人のユーザーを複数のグループに追加できます。

SDX 22000 プラットフォームでの **RAID** ディスク割り当ての管理

November 23, 2023

NetScaler SDX 22040/22060/22080/22100/22120 アプライアンスには、最大 8 台の物理ディスクをサポートできる独立ディスク冗長アレイ（RAID）コントローラーが搭載されるようになりました。複数のディスクを使用することで、パフォーマンスが向上するだけでなく、信頼性が向上します。SDX アプライアンスは多数の仮想マシンをホストし、ディスク障害が複数の仮想マシンに影響を及ぼすため、信頼性は特に重要です。管理サービスの RAID コントローラは、ディスクミラーリングを実装する RAID 1 構成をサポートします。つまり、2 つのディスクで同じデータが保持されます。RAID 1 アレイ内のディスクに障害が発生すると、そのミラーは必要なデータをすべて即座に提供します。

RAID 1 ディスクミラーリングは、2 つの物理ドライブを 1 つの論理ドライブに結合します。論理ドライブの使用可能容量は、論理ドライブの 1 つの物理ドライブの容量に相当します。たとえば、2 台の 1 テラバイトのドライブを組み合わせると、1 つの論理ドライブが作成され、総有効容量は 1 TB になります。このドライブの組み合わせは、アプライアンスでは単一の論理ドライブとして認識されます。

SDX アプライアンスには、論理ドライブ 0 と論理ドライブ 1 を含む構成が同梱されています。論理ドライブ 0 は管理サービスと Citrix Hypervisor に割り当てられ、論理ドライブ 1 はプロビジョニングする NetScaler インスタンスに割り当てられます。より多くの物理ドライブを使用するには、新しい論理ドライブを作成する必要があります。

ドライブのプロパティとオペレーションを表示する

SDX アプライアンスは、最大 8 つの物理ドライブスロット、つまり、アプライアンスの両側に 4 つのスロットのペアをサポートします。物理ドライブをスロットに挿入できます。物理ドライブを使用する前に、その物理ドライブを論理ドライブの一部にする必要があります。

管理サービスの [構成] **>** [システム] **> [RAID**] 画面には、論理ドライブ、物理ドライブ、およびストレージリポジトリのタブが表示されます。

論理ドライブ

[構成] **> [**システム**] > [RAID] > [**論理ドライブ] タブでは、各論理ドライブの名前、状態、サイズ、およびその構成されている物理ドライブに関する情報を表示できます。次の表に、仮想ドライブの状態を示します。

状態	説明
最適	仮想ドライブの動作状態は良好です。構成済みのドライブはすべてオンラインです。
機能低下	仮想ドライブの動作状態が最適ではありません。構成済みのドライブの 1 つに障害が発生しているか、オフラインになっています。
失敗	仮想ドライブに障害が発生しました。
オフライン	RAID コントローラで仮想ドライブを使用できない。

論理ドライブを選択し、[Show Physical Drive] をクリックすると、その論理ドライブに関連付けられている物理ドライブの詳細を表示することもできます。

新しい論理ドライブを作成するには

1. [構成] > [システム] > [**RAID**] に移動し、[論理ドライブ] タブを選択します。
2. [追加] をクリックします。
3. [論理ディスクの作成] ダイアログボックスで、動作可能な物理ドライブを含む 2 つのスロットを選択し、[作成] をクリックします。

物理ドライブ

SDX アプライアンスは、最大 8 つの物理スロット、つまり、アプライアンスの両側に 4 つのスロットのペアをサポートします。[
構成**] > [**システム**] > [RAID] > [**物理ドライブ] タブでは、次の情報を表示できます。

- **Slot:**: 物理ドライブに関連づけられている物理スロット。
- **Size:**: 物理ドライブのサイズ。
- ファームウェアの状態**:**-ファームウェアの状態。指定可能な値:
  - オンライン、スピンアップ: : 物理ドライブは稼働しており、RAID によって制御されています。
  - 未構成 **(**良好**):** 物理ドライブは良好な状態で、論理ドライブペアの一部として追加できます。
  - 未構成 **(**不良**):**—物理ドライブは良好な状態ではなく、論理ドライブの一部として追加できません。
- **Foreign State:**—ディスクが空かどうかを示す。

- 論理ドライブ**:**—関連付けられている論理ドライブ。

[**Physical Drives**] ペインでは、物理ドライブに対して次の操作を実行できます。

- **Initialize:**: ディスクを初期化します。物理ドライブが良好な状態ではなく、論理ドライブペアの一部として追加する必要がある場合は、物理ドライブを初期化できます。
- **Rebuild:**: ドライブのリビルドを開始します。ドライブグループ内のドライブに障害が発生した場合、障害が発生する前にドライブに保存されていたデータを再作成することで、ドライブを再構築できます。RAID コントローラは、ドライブグループ内の他のドライブに保存されているデータを再作成します。
- **Locate:**: アプライアンス上でドライブの位置を特定します。このとき、ドライブに関連付けられているドライブアクティビティ LED が点滅します。
- [**Stop Locate**]: アプライアンスでのドライブの検索を停止します。
-

ストレージリポジトリ

[構成**] > [**システム**] > [RAID] > [**ストレージリポジトリ] タブで、SDX アプライアンス上のストレージリポジトリのステータスを表示できます。接続されていないストレージリポジトリドライブに関する情報を表示することもできます。また、そのドライブを選択して [削除] をクリックすると、そのドライブを削除できます。[ストレージリポジトリ] タブには、各ストレージリポジトリに関する次の情報が表示されます。

- **Name:**: ストレージリポジトリドライブの名前。
- ドライブが接続されていますか**:** ストレージリポジトリが接続されているかどうか。ドライブが接続されていない場合は、[削除] をクリックして削除できます。
- **Size:**: ストレージリポジトリのサイズ。
- **Utilized:**: 使用中のストレージ・リポジトリの容量。

SDX 22000 アプライアンスに論理ドライブを追加する　SDX 22000 プラットフォームに論理ドライブを追加するには、次の手順で行います。

1. 管理サービスにログオンします。
2. [構成**] > [**システム**] > [RAID**] に移動します。
3. SDX 22000 アプライアンスの背面で、2 つの空の SSD をスロット番号 4 と 5 に挿入します。SSD は実行中のシステムに追加できます。
   注： SSD が NetScaler 認定を受けていることを確認してください。
4. 管理サービスで、[構成**] > [**システム**] > [RAID**] に移動し、[物理ドライブ] タブに移動します。追加した SSD が表示されます。
5. [論理ドライブ] タブに移動し、[追加] をクリックします。
6. [論理ディスクの作成] ページで、次の操作を行います。

a) [**First Slot**] ドロップダウンリストで [4] を選択します。

b) [**2** 番目のスロット] ドロップダウンリストで [5] を選択します。

c)［作成］をクリックします。

注**:** 管理サービスでは、スロット番号はゼロから始まります。そのため、管理サービスのスロット番号は、物理アプライアンスのスロット番号とは異なります。

論理ドライブが作成され、[
論理ドライブ**]** タブに一覧表示されます。[Refresh] アイコンをクリックして、論理ドライブの順序を更新します。

SDX 22000 アプライアンスに **2** つ目の論理ドライブを追加する　別の論理ドライブを追加するには、SSD をスロット番号 6 と 7 に挿入します。[
論理ディスクの作成] ページで、[最初のスロット] リストから [6] を選択し、[**2** 番目のスロット] リストから [7] を選択します。

欠陥のある **SSD** ドライブを空の **SSD** ドライブと交換する　欠陥のある SSD ドライブを空の SSD ドライブに交換するには、次の手順に従います。

1. [構成**] > [**システム**] > [RAID**] に移動します。
2. [物理ドライブ] タブで、交換する不良ドライブを選択します。
3. [取り外しの準備] をクリックしてドライブを取り外します。
4. [Refresh] アイコンをクリックして、物理ドライブの一覧を更新します。
5. 欠陥のあるドライブをスロットから物理的に取り外します。
6. 欠陥のある SSD を取り外したスロットに、新しい Citrix 検証済み SSD を挿入します。
7. 管理サービスで、[構成**] > [**システム**] > [RAID**] に移動します。新しい SSD が [物理ドライブ] セクションに表示されます。ドライブのリビルドプロセスが自動的に開始されます。

[Refresh] アイコンをクリックして、再構築プロセスのステータスを確認します。リビルドプロセスが完了すると、[**Firmware State**] 列に [オンライン、スピンアップ] ステータスが表示されます。

SDX ライセンスの概要

February 16, 2024

NetScaler SDX Management Service では、ハードウェアシリアル番号（HSN）またはライセンスアクセスコードを使用してライセンスを割り当てることができます。Management Service ソフトウェアはアプライアンスのシリアル番号を内部的に取得し、ライセンスを購入すると Citrix からライセンスアクセスコードが電子メールで送信されます。

または、ローカルコンピューターにライセンスが既に存在する場合は、それをアプライアンスにアップロードできます。

ライセンスの返却や再割り当てなど、他のすべての機能については、ライセンスポータルを使用する必要があります。オプションで、ライセンスの割り当てにライセンスポータルを引き続き使用できます。詳しくは、「Citrix.com でのライセンスの管理」を参照してください。

SDX ライセンスオプションについては、以下を参照してください。

- 適切なプラットフォームとエディションオプションを選択する
- ライセンスモデル

注：永続ライセンスまたはプールライセンスをインストールする場合、SDX アプライアンスを再起動する必要はありません。

前提条件

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ライセンスを割り当てるには、次の手順を実行します：

1. アプライアンスを介してパブリックドメインにアクセスできる必要があります。たとえば、アプライアンスは www.citrix.comにアクセスできる必要があります。ライセンス割り当てソフトウェアは、ライセンスの Citrix ライセンスポータルに内部的にアクセスします。パブリックドメインにアクセスするには、管理サービスの IP アドレスを構成し、DNS サーバーをセットアップする必要があります。
2. ライセンスはハードウェアにリンクされているか、有効なライセンスアクセスコードを持っている必要があります。

管理サービスを使用してライセンスを割り当てる

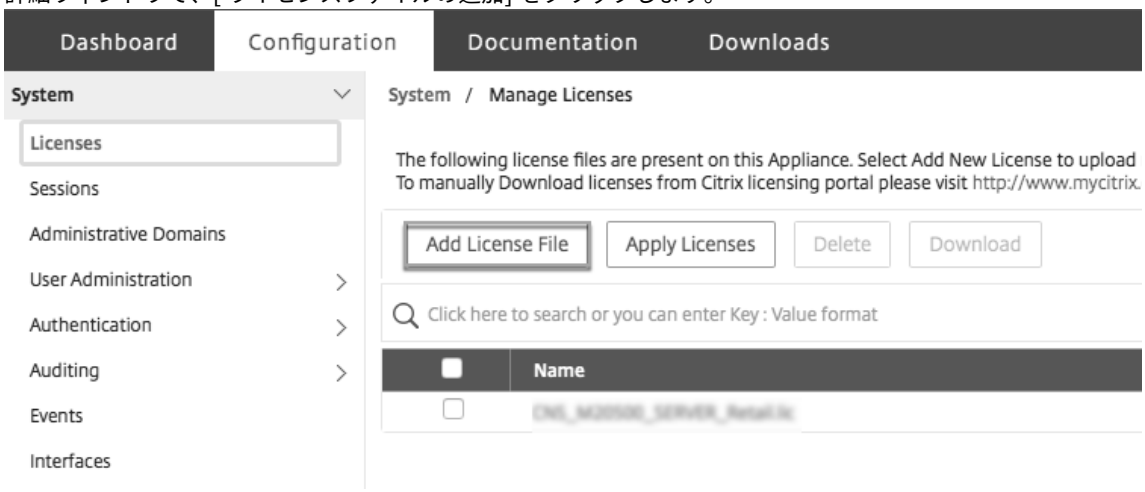
ライセンスがすでにハードウェアにリンクされている場合は、ライセンス割り当てプロセスでハードウェアシリアル番号を使用できます。それ以外の場合は、ライセンスアクセスコードを入力する必要があります。

展開の必要に応じて、ライセンスを部分的に割り当てることができます。たとえば、ライセンスファイルに 10 個のライセンスが含まれていて、現在の要件が 6 つのライセンスだけである場合、ここで 6 つのライセンスを割り当てて、後でさらにライセンスを割り当てることができます。ライセンスファイルに存在するライセンスの合計数を超えるライセンスを割り当てることはできません。

ライセンスを割り当てるには

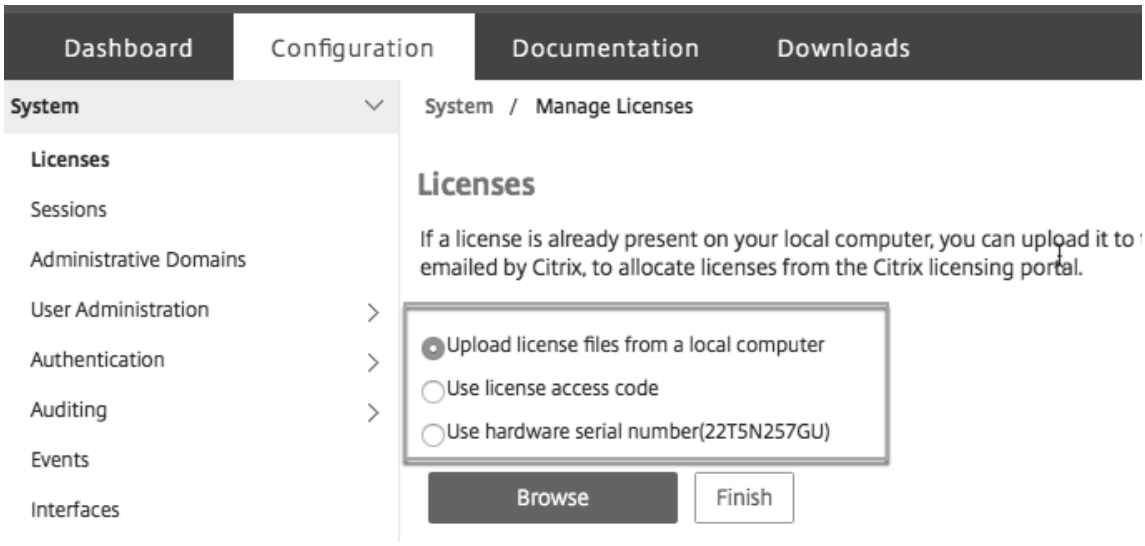
1. Web ブラウザで、SDX アプライアンスの管理サービスの IP アドレス（http://10.102.126.251など）を入力します。
2. ［**User Name**］ボックスと ［**Password**］ボックスに管理者資格情報を入力します。

3. [**Configuration**] タブで、[**System**] **>** [**Licenses**] の順に移動します。
4. 詳細ウィンドウで、[ライセンスファイルの追加] をクリックします。



5. 次に、次のいずれかのオプションを選択します。

   - ローカルコンピュータからライセンスファイルをアップロードする (このオプションはデフォルトで選択されています)
   - ライセンスアクセスコードを使用
   - ハードウェアシリアル番号を使う



- 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: このオプションを選択した場合は、「ブラウズ」をクリックしてローカルマシンからゼロキャパシティライセンスを選択します。その後、[**Finish**] をクリックします。

  1. ゼロキャパシティライセンスが正常に適用されると、** ライセンスページにライセンスモードセクションが表示されます ** 。
  2. ** プールライセンスまたはセルフマネージドプールライセンスのいずれかを選択できます **。

3. [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。
4. 「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。
5. [**Get Licenses**] をクリックします。
6. [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。
7. [**Manage Licenses**] ページでは、ライセンスサーバー、ライセンスエディション、およびプールから割り当てられたインスタンスと帯域幅の詳細を表示できます。

> 注:
>
> NetScaler リリース 13.1 ビルド 30.x 以降、NetScaler SDX アプライアンスはセルフマネージドプールライセンスをサポートしています。このライセンスにより、ライセンスサーバーへのライセンスファイルのアップロードを簡略化および自動化できます。NetScaler ADM を使用して、共通の帯域幅または vCPU とインスタンスプールで構成されるライセンスフレームワークを作成できます。

- – ライセンスの割り当てに使用するライセンスファイルを選択します。
  – [**Allocate**] 列に、割り当てるライセンスの数を入力します。次に、[ダウンロード] をクリックします。

  ライセンスがダウンロードされると、[**License Files**] の下に表示されます。ライセンスファイルを選択し、[**Apply Licenses**] をクリックします。
- ハードウェアシリアル番号を使用: このオプションを選択すると、ソフトウェアはアプライアンスのシリアル番号を内部的に取得し、この番号を使用してライセンスを表示します。

  – [ライセンスの取得] をクリックするか、[プロキシサーバー経由で接続] チェックボックスをオンにして [ライセンスの取得] をクリックします。

  ライセンスファイルをダウンロードしたら、ライセンスファイルを選択し、[**Apply Licenses**] をクリックします。

プールライセンスについて詳しくは、「NetScaler SDX の永久ライセンスを NetScaler プール容量にアップグレードする」を参照してください。

SDX リソースビジュアライザー

February 16, 2024

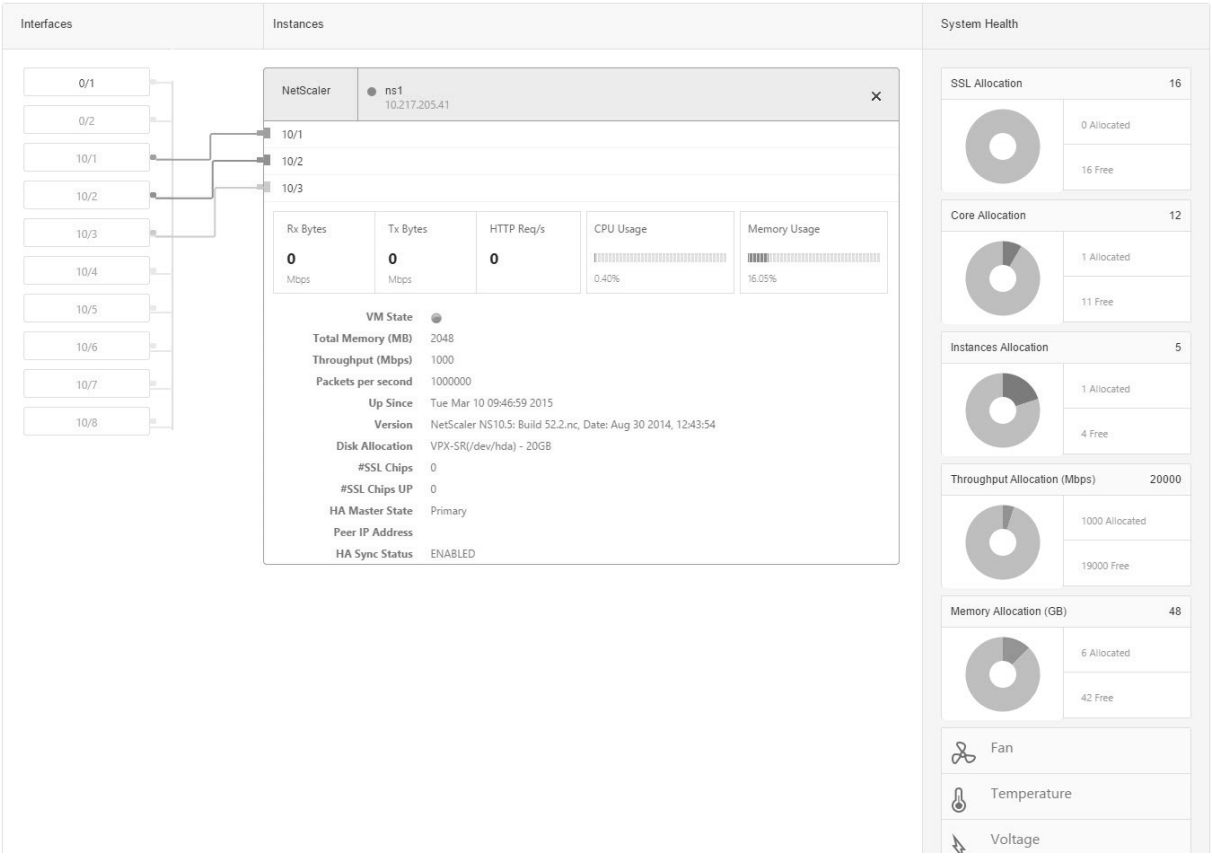
NetScaler SDX アプライアンスで NetScaler インスタンスをプロビジョニングする場合、CPU、スループット、メモリなどのさまざまなリソースをインスタンスに割り当てる必要があります。現在の SDX では、使用可能なさまざまなリソースに関する情報は表示されません。

リソースビジュアライザーを使用すると、インスタンスのプロビジョニングに使用できるすべてのリソースが 1 つのダッシュボードに表示されます。使用可能なリソースと使用中のリソースはすべてグラフ形式で表示されます。リソ

ースビジュアライザーには、割り当て可能なリソースとは別に、電源の状態や温度などの他のパラメータも表示されます。

リソースビジュアライザーには、インスタンスが使用しているさまざまなリソースも表示されます。インスタンスに関連付けられているさまざまなリソースを表示するには、ビジュアライザーでインスタンス名をクリックします。ビジュアライザーの右側には、使用可能なリソースと使用済みのリソースがすべてグラフ形式で表示されます。

次の図は、リソースビジュアライザーでキャプチャされた詳細を示しています。



インターフェースを管理する

November 23, 2023

[**Interfaces**] ペインでは、VPX インスタンス上の仮想インターフェイスの SDX アプライアンスへのマッピングを表示し、インターフェイスに MAC アドレスを割り当てることができます。

注**:** Direct Attach Cable（DAC; 直接接続ケーブル）が接続されているインターフェイスでは、自動ネゴシエーションはサポートされません。

[Interfaces] ペインの [**Interfaces**] リストの [**State**] 列の [UP] は、インターフェイスがトラフィックを正常に受信していることを示します。DOWN は、インターフェイスがトラフィックを送受信できないネットワークの問題

を示します。

重要： 1 GB を超える接続ではフロー制御は推奨されません。

インターフェイスを設定するには

1. [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[インターフェイス] をクリックします。
2. [**Interfaces**] ペインで、設定するインターフェイスをクリックし、[**Edit**] をクリックします。
3. [**Configure Interface**] ウィンドウで、次のパラメータの値を指定します。
   - オートネゴシエーション—オートネゴシエーションを有効にします指定可能な値: オン、オフ。デフォルト: オン。
   - **Speed**：インターフェイスのイーサネット速度（MB/s）。指定できる値は、10、100、1000、および 10000 です。
   - **Duplex**：インターフェイスのデュプレックス動作のタイプ。可能な値: フル、ハーフ、なし。デフォルト: なし。
   - フロー制御オートネゴシエーション：フロー制御パラメータを自動的にネゴシエーションします。指定可能な値: オン、オフ。デフォルト: オン
   - **Rx** フロー制御：Rx フロー制御を有効にします。指定可能な値: オン、オフ。デフォルト: オン
   - **Tx** フロー制御：Tx フロー制御を有効にします。指定可能な値: オン、オフ。デフォルト: オン
4. 「**OK**」をクリックし、「閉じる」をクリックします。

インターフェイスのパラメータをデフォルト値にリセットするには

1. [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[インターフェイス] をクリックします。
2. [**Interfaces**] ペインで、リセットするインターフェイスをクリックし、[**Reset**] をクリックします。

VPX インスタンス上の仮想インターフェースと物理インターフェースのマッピングを表示する

NetScaler VPX インスタンスでは、GUI と CLI に、インスタンスの仮想インターフェイスとアプライアンス上の物理インターフェイスのマッピングが表示されます。

VPX インスタンスにログオンしたら、構成ユーティリティで [ネットワーク] に移動し、[インターフェイス**]** をクリックします。次の図に示すように、インスタンスの仮想インターフェイス番号とアプライアンス上の対応する物理インターフェイス番号が [**Description**] フィールドに表示されます。

CLI で、`show interface` コマンドを入力します。例:

```
> show interface
1) Interface 10/3 (10G VF Interface, PF 10/4) #2
flags=0xe460 <ENABLED, UP, UP, HAMON, 802.1q>
```



```
4   MTU=1500, native vlan=1, MAC=6e:b6:f5:21:5d:db, uptime 43h03m35s
5   Actual: media FIBER, speed 10000, duplex FULL, fctl NONE, throughput
        10000
6   RX: Pkts(2547925) Bytes(287996153) Errs(0) Drops(527183) Stalls(0)
7   TX: Pkts(196) Bytes(8532) Errs(0) Drops(0) Stalls(0)
8   NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
9   Bandwidth thresholds are not set.
10  ...
11 <!--NeedCopy-->
```

MAC アドレスをインターフェイスに割り当てる

SDX アプライアンスで ADC インスタンスをプロビジョニングしている間、Citrix Hypervisor はそのインスタンスに関連付けられた仮想インターフェイスに MAC アドレスを内部的に割り当てます。同じアプライアンスまたは別のアプライアンス上の別のインスタンスに関連付けられた仮想インターフェイスに、同じ MAC アドレスが割り当てられている場合があります。MAC アドレスが重複して割り当てられないように、一意の MAC アドレスを強制できます。

MAC アドレスをインターフェイスに割り当てるには、次の 2 つの方法があります。

1. ベース MAC アドレスと範囲をインターフェイスに割り当てる: 管理サービスは、ベースアドレスと範囲を使用して一意の MAC アドレスを割り当てます。
2. グローバルベース MAC アドレスを割り当てる: グローバルベース MAC アドレスがすべてのインターフェイスに適用されます。その後、管理サービスはすべてのインターフェイスの MAC アドレスを生成します。グローバルベース MAC アドレスを設定すると、1G インターフェイスの範囲は 8 に設定されます。10G インターフェイスの範囲は 64 に設定されています。グローバルベース MAC アドレスが 00:00:00:00:00:00 に設定されている場合のベース MAC アドレスの例については、次の表を参照してください。

物理インターフェイス	ベース MAC アドレス
0/1	00:00:00:00:00:00
0/2	00:00:00:00:00:08
1/1	00:00:00:00:00:10
1/2	00:00:00:00:00:18
1/3	00:00:00:00:00:20
1/4	00:00:00:00:00:28
1/5	00:00:00:00:00:30
1/6	00:00:00:00:00:38
1/7	00:00:00:00:00:40

物理インターフェイス	ベース MAC アドレス
1/8	00:00:00:00:00:48
10/1	00:00:00:00:00:50
10/2	00:00:00:00:00:90

表 1. グローバルベース MAC アドレスから生成されるベース MAC アドレスの例

管理ポートのベース MAC アドレスは参照用です。管理サービスは、ベース MAC アドレスに基づいて、1/x および 10/x ポートに対してのみ MAC アドレスを生成します。

注: ベース MAC アドレスをチャネルに割り当てることはできません。

MAC アドレスでさまざまな操作を実行するには、[システム**] > [**インターフェイス] をクリックします。インターフェイスを選択し、[**Edit**] をクリックします。[インターフェイスの設定（**Configure Interface** ）] ウィンドウで MAC アドレス操作を実行します。

SDX アプライアンスの物理インターフェイスを無効または有効にする

SDX アプライアンスで物理インターフェイスを使用していない場合は、Management Service を使用して物理インターフェイスを無効にできます。このアクションは、セキュリティ上の目的で役立ちます。

注：デフォルトでは、SDX アプライアンス上のすべての物理インターフェイスが有効になっています。また、VPX やチャンネルでインターフェースが使用されている場合、そのインターフェースを無効にすることはできません。

物理インターフェイスを無効にするには、次の手順で行います。

1. [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[インターフェイス] をクリックします。
2. [**Interfaces**] ペインで、無効にするインターフェイスを選択します。
3. [アクション] ドロップダウンリストで、[無効] をクリックします。

無効にした物理インターフェイスを使用する場合は、Management Service を使用してインターフェイスを有効にできます。

無効にした物理インターフェイスを有効にするには、次の手順を実行します。

1. [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[インターフェイス] をクリックします。
2. [**Interfaces**] ペインで、有効にする無効インターフェイスを選択します。
3. [アクション] ドロップダウンリストで [有効] をクリックします。

SDX アプライアンス上のジャンボフレーム

November 23, 2023

NetScaler SDX アプライアンスは、最大 9216 バイトの IP データを含むジャンボフレームの送受信をサポートします。ジャンボフレームでは、標準の IP MTU サイズ（1500 バイト）を使用するよりも効率的に大きなファイルを送信することができます。

NetScaler SDX アプライアンスは、以下の展開シナリオでジャンボフレームを使用できます。

- ジャンボからジャンボ：アプライアンスはデータをジャンボフレームとして受信し、ジャンボフレームとして送信します。
- **Non-Jumbo to Jumbo**：アプライアンスはデータを非ジャンボフレームとして受信し、ジャンボフレームとして送信します。
- ジャンボから非ジャンボ：アプライアンスはデータをジャンボフレームとして受信し、非ジャンボフレームとして送信します。

SDX アプライアンスでプロビジョニングされた NetScaler インスタンスは、次のプロトコルの負荷分散構成のジャンボフレームをサポートします。

- TCP
- TCP 経由のその他のプロトコル
- SIP

ジャンボフレームの詳細については、「ユースケース」を参照してください。

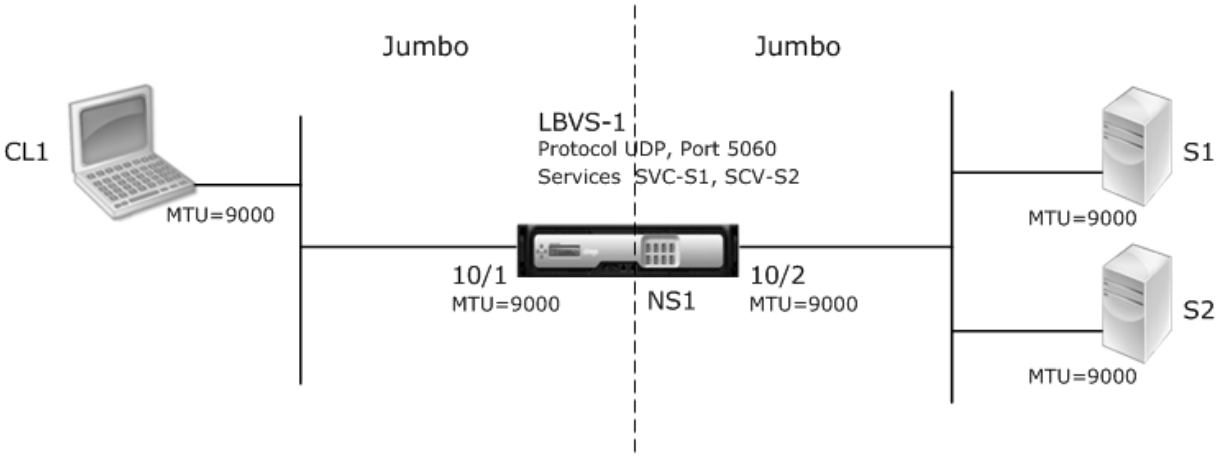
ユースケース**:** ジャンボからジャンボへのセットアップ

ジャンボツージャンボ設定の例を考えてみましょう。NetScaler インスタンス NS1 上に構成された SIP 負荷分散仮想サーバー LBVS-1 を使用して、サーバー S1 と S2 間で SIP トラフィックの負荷分散を行います。クライアント CL1 と NS1 間の接続、および NS1 とサーバ間の接続は、ジャンボフレームをサポートします。

NS1 のインターフェイス 10/1 は、クライアント CL1 との間でトラフィックを送受信します。NS1 のインターフェイス 10/2 は、サーバ S1 または S2 との間でトラフィックを送受信します。NS1 のインターフェイス 10/1 と 10/2 は、それぞれ VLAN 10 と VLAN 20 の一部です。

ジャンボフレームをサポートするために、インターフェイス 10/1、10/2、および VLAN 10、VLAN 20 の MTU は 9216 に設定されます。

このセットアップ例では、CL1、S1、S2 などの他のすべてのネットワークデバイスも、ジャンボフレームをサポートするように設定されています。



次の表は、例で使用される設定の一覧です。

エンティティ	Name	詳細
クライアント CL1 の IP アドレス	CL1	192.0.2.10
サーバの IP アドレス	S1	198.51.100.19
		S2
（管理サービスインターフェイスを使用して）インターフェイスと NS1 上の VLAN（CLI を使用）に指定された MTU。	10/1	9000
		10/2
		VLAN 10
		VLAN 20
NS1 上のサーバを表すサービス	SVC-S1	IP アドレス:198.51.100.19、プロトコル:SIP、ポート:5060
NS1 上のサーバを表すサービス	SVC-S2	IP アドレス:198.51.100.20、プロトコル:SIP、ポート:5060
VLAN 10 上の負荷分散仮想サーバ	LBVS-1	IP アドレス:203.0.113.15、プロトコル:SIP、ポート:5060、SVC-S1、SVC-S2

CL1 から NS1 へのリクエストのトラフィックフローを次に示します。

1. CL1 は LBVS1 に対して 20000 バイトの SIP 要求を作成します。
2. CL1 は、IP フラグメント内の要求データを NS1 の LBVS1 に送信します。各 IP フラグメントのサイズは、CL1 がこれらのフラグメントを NS1 に送信するインターフェイスに設定された MTU（9000）以下になります。

- 最初の IP フラグメントのサイズ = [IP ヘッダー + UDP ヘッダー + SIP データセグメント] = [20 + 8 + 8972] = 9000
- 2 番目の IP フラグメントのサイズ = [IP ヘッダー + SIP データセグメント] = [20 + 8980] = 9000
- 最後の IP フラグメントのサイズ = [IP ヘッダー + SIP データセグメント] = [20 + 2048] = 2068

3. NS1 は、インターフェイス 10/1 で要求 IP フラグメントを受信します。NS1 はこれらのフラグメントを受け入れます。これは、各フラグメントのサイズがインターフェイス 10/1 の MTU（9000）以下であるためです。
4. NS1 はこれらの IP フラグメントを再構成して 27000 バイトの SIP 要求を形成します。NS1 はこの要求を処理します。
5. LBVS-1 の負荷分散アルゴリズムにより、サーバー S1 が選択されます。
6. NS1 は IP フラグメント内の要求データを S1 に送信します。各 IP フラグメントのサイズは、NS1 がこれらのフラグメントを S1 に送信するインターフェイス 10/2 の MTU（9000）と同じかそれ以下です。IP パケットは、NS1 の SNIP アドレスで発信されます。

   - 最初の IP フラグメントのサイズ = [IP ヘッダー + UDP ヘッダー + SIP データセグメント] = [20 + 8 + 8972] = 9000
   - 2 番目の IP フラグメントのサイズ = [IP ヘッダー + SIP データセグメント] = [20 + 8980] = 9000
   - 最後の IP フラグメントのサイズ = [IP ヘッダー + SIP データセグメント] = [20 + 2048] = 2068

この例の CL1 に対する S1 の応答のトラフィックフローを次に示します。

1. サーバ S1 は 30000 バイトの SIP 応答を作成し、NS1 の SNIP アドレスに送信します。
2. S1 は IP フラグメント内の応答データを NS1 に送信します。各 IP フラグメントのサイズは、S1 がこれらのフラグメントを NS1 に送信するインターフェイスに設定されている MTU（9000）以下になります。

   - 最初の IP フラグメントのサイズ = [IP ヘッダー + UDP ヘッダー + SIP データセグメント] = [20 + 8 + 8972] = 9000
   - 2 番目と 3 番目の IP フラグメントのサイズ = [IP ヘッダー + SIP データセグメント] = [20 + 8980] = 9000
   - 最後の IP フラグメントのサイズ = [IP ヘッダー + SIP データセグメント] = [20 + 3068] = 3088

3. NS1 は、インターフェイス 10/2 で応答 IP フラグメントを受信します。NS1 はこれらのフラグメントを受け入れます。これは、各フラグメントのサイズがインターフェイス 10/2 の MTU（9000）以下であるためです。
4. NS1 はこれらの IP フラグメントを再構成し、27000 バイトの SIP 応答を形成します。NS1 はこのレスポンスを処理します。
5. NS1 は IP フラグメント内の応答データを CL1 に送信します。各 IP フラグメントのサイズは、NS1 がこれらのフラグメントを CL1 に送信するインターフェイス 10/1 の MTU（9000）と等しいか、それより小さくなります。IP フラグメントは LBVS-1 の IP アドレスから発信されます。これらの IP パケットは LBVS-1 の IP アドレスから発信され、CL1 の IP アドレスを宛先とします。

   - 最初の IP フラグメントのサイズ = [IP ヘッダー + UDP ヘッダー + SIP データセグメント] = [20 + 8 + 8972] = 9000
   - 2 番目と 3 番目の IP フラグメントのサイズ = [IP ヘッダー + SIP データセグメント] = [20 + 8980] = 9000

最後の IP フラグメントのサイズ = [IP ヘッダー + SIP データセグメント] = [20 + 3068] = 3088

設定タスク:

SDX Management Service で、[構成] **>** [システム] **>** [インターフェイス] ページに移動します。必要なインターフェイスを選択し、[**Edit**] をクリックします。MTU 値を設定し、**OK** をクリックします。

例:

インターフェイス 10/1 の MTU 値を 9000、インターフェイス 10/2 の MTU 値を 9000 に設定します。

NetScaler インスタンスにログオンし、ADC コマンドラインインターフェイスを使用して残りの構成手順を完了します。

次の表は、NetScaler インスタンスで必要な構成を作成するためのタスク、コマンド、および例を示しています。

タスク	ADC コマンド構文	例
VLAN を作成し、ジャンボフレームをサポートする VLAN の MTU を設定します。	`add vlan <id> -mtu <positive_integer>`、`show vlan <id>`	`add vlan 10 -mtu 9000`、`add vlan 20 -mtu 9000`
インターフェイスを VLAN にバインドします。	`bind vlan <id> -ifnum <interface_name>`、`show vlan <id>`	`bind vlan 10 -ifnum 10/1`、`bind vlan 20 -ifnum 10/2`
SNIP アドレスを追加します。	`add ns ip <IPAddress> <netmask> -type SNIP`、`show ns ip`	`add ns ip 198.51.100.18 255.255.255.0 -type SNIP`
SIP サーバを表すサービスを作成します。	`add service <serviceName> <ip> SIP_UDP <port>`、`show service <name>`	サービス追加 SVC-S1 198.51.100.19 SIP_UDP 5060; DD サービス SVC-S2 198.51.100.20 SIP_UDP 5060
SIP 負荷分散仮想サーバを作成し、そのサーバにサービスをバインドする	`add lb vserver <name> SIP_UDP <ip> <port>;bind lb vserver <vserverName> <serviceName>;show lb vserver <name>`	`add lb vserver LBVS-1 SIP_UDP 203.0.113.15 5060;bind lb vserver LBVS-1 SVC-S1;bind lb vserver LBVS-1 SVC-S2`
`bind lb vserver LBVS-1 SVC-S2`	`save ns config`、`show ns config`	

ユースケース**:** 非ジャンボからジャンボへのセットアップ

非ジャンボからジャンボへのセットアップの例を考えてみましょう。NetScaler インスタンス NS1 上に構成された負荷分散仮想サーバー LBVS1 を使用して、サーバー S1 と S2 のトラフィックを負荷分散します。クライアント CL1 と NS1 間の接続は非ジャンボフレームをサポートし、NS1 とサーバ間の接続はジャンボフレームをサポートします。

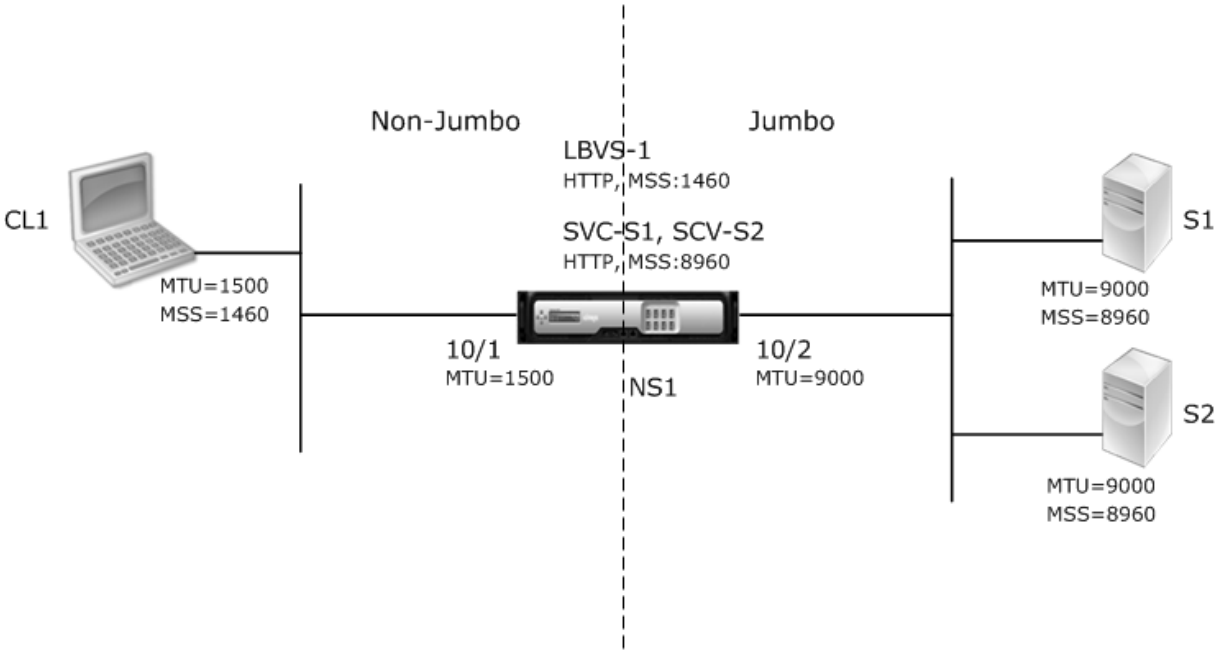
NS1 のインターフェイス 10/1 は、クライアント CL1 との間でトラフィックを送受信します。NS1 のインターフェイス 10/2 は、サーバ S1 または S2 との間でトラフィックを送受信します。

NS1 のインターフェイス 10/1 と 10/2 は、それぞれ VLAN 10 と VLAN 20 の一部です。CL1 と NS1 の間の非ジャンボフレームだけをサポートするために、MTU はインターフェイス 10/1 と VLAN 10 の両方でデフォルト値の 1500 に設定されます。

NS1 とサーバ間のジャンボフレームをサポートするために、インターフェイス 10/2 と VLAN 20 の MTU は 9000 に設定されます。

NS1 とサーバ間のサーバおよびその他すべてのネットワーク・デバイスも、ジャンボ・フレームをサポートするように構成されています。HTTP トラフィックは TCP に基づいているため、ジャンボフレームをサポートするために、各エンドポイントで MSS が適切に設定されます。

- CL1 と NS1 の仮想サーバ LBVS1 の間の接続では、NS1 上の MSS が TCP プロファイルに設定され、それが LBVS1 にバインドされます。
- NS1 と S1 の SNIP アドレス間の接続では、NS1 上の MSS が TCP プロファイルに設定され、NS1 上の S1 を表すサービス (SVC-S1) にバインドされます。



次の表に、この例で使用されている設定の一覧を示します。

エンティティ	Name	詳細
クライアント CL1 の IP アドレス	CL1	192.0.2.10
サーバの IP アドレス	S1	198.51.100.19
		S2
インターフェイス 10/1 の MTU（管理サービスインターフェイスを使用）		1500
インターフェイス 10/2 の MTU セット (管理サービスインターフェイスを使用)。		9000
NS1 上の VLAN 10 の MTU（ADC コマンドラインインターフェイスを使用）		1500
NS1 上の VLAN 20 の MTU セット（ADC コマンドラインインターフェイスを使用)。		9000
NS1 上のサーバを表すサービス	SVC-S1	IP アドレス:198.51.100.19、プロトコル:HTTP、ポート:80、MSS:8960 SVC-S2
VLAN 10 上の負荷分散仮想サーバ	LBVS-1	IP アドレス:203.0.113.15、プロトコル:HTTP、ポート:80。バインドされたサービス:SVC-S1、SVC-S2、MSS: 1460

この例では、CL1 が S1 に要求するトラフィックフローを次に示します。

1. クライアント CL1 は、NS1 の仮想サーバー LBVS-1 に送信する 200 バイトの HTTP 要求を作成します。
2. CL1 は NS1 の LBVS-1 への接続をオープンします。CL1 と NS1 は、接続の確立中にそれぞれの TCP MSS 値を交換します。
3. NS1 の MSS は HTTP 要求よりも大きいため、CL1 は要求データを 1 つの IP パケットで NS1 に送信します。1。

```
<div id="concept_57AEA1C9D3DA47948B6D834341388D29__d978e142">

Size of the request packet = [IP Header + TCP Header + TCP Request
    ] = [20 + 20 + 200] = 240

</div>
```

4. NS1 は、インターフェイス 10/1 で要求パケットを受信し、パケット内の HTTP 要求データを処理します。
5. LBVS-1 の負荷分散アルゴリズムはサーバー S1 を選択し、NS1 はその SNIP アドレスの 1 つと S1 の間の接続を開きます。NS1 と CL1 は、接続の確立中にそれぞれの TCP MSS 値を交換します。
6. S1 の MSS は HTTP 要求よりも大きいので、NS1 は 1 つの IP パケットで要求データを S1 に送信します。

a) 要求パケットのサイズ = [IP ヘッダー + TCP ヘッダー + [TCP 要求] = [20 + 20 + 200] = 240

この例の CL1 に対する S1 の応答のトラフィックフローを次に示します。

1. サーバー S1 は、NS1 の SNIP アドレスに送信する 18000 バイトの HTTP 応答を作成します。
2. S1 は応答データを NS1 の MSS の倍数に分割し、これらのセグメントを IP パケットとして NS1 に送信します。これらの IP パケットは、S1 の IP アドレスから送信され、NS1 の SNIP アドレスを宛先とします。
   - 最初の 2 つのパケットのサイズ = [IP ヘッダー + TCP ヘッダー + (TCP セグメント = NS1 の MSS サイズ)] = [20 + 20 + 8960] = 9000
   - 最後のパケットのサイズ = [IP ヘッダー + TCP ヘッダー + (残りの TCP セグメント)] = [20 + 20 + 2080] = 2120
3. NS1 は、インターフェイス 10/2 で応答パケットを受信します。
4. NS1 は、これらの IP パケットからすべての TCP セグメントを組み立てて、18000 バイトの HTTP 応答データを形成します。NS1 はこのレスポンスを処理します。
5. NS1 は、応答データを CL1 の MSS の倍数にセグメント化し、これらのセグメントを IP パケットとして、インターフェイス 10/1 から CL1 に送信します。これらの IP パケットは LBVS-1 の IP アドレスから発信され、CL1 の IP アドレスを宛先とします。
   - 最後のパケットを除くすべてのパケットのサイズ = [IP ヘッダー + TCP ヘッダー + (TCP ペイロード = CL1 の MSS サイズ)] = [20 + 20 + 1460] = 1500
   - 最後のパケットのサイズ = [IP ヘッダー + TCP ヘッダー + (残りの TCP セグメント)] = [20 + 20 + 480] = 520

設定タスク:

SDX Management Service で、[構成**] > [**システム**] > [**インターフェイス] ページに移動します。必要なインターフェイスを選択し、[**Edit**] をクリックします。MTU 値を設定し、**OK** をクリックします。

例:

次の MTU 値を設定します。

- 10/1 インターフェイスの場合は 1500
- 10/2 インターフェイスの場合は 9000

NetScaler インスタンスにログオンし、ADC コマンドラインインターフェイスを使用して残りの構成手順を完了します。

次の表は、NetScaler インスタンスで必要な構成を作成するためのタスク、コマンド、および例を示しています。

タスク	ADC コマンドライン構文	例
–	–	–
VLAN を作成し、ジャンボフレームをサポートする VLAN の MTU を設定します。	`add vlan <id> -mtu <positive_integer>`、`show vlan <id>`	`add vlan 10 -mtu 1500`、`add vlan 20 -mtu 9000`

インターフェイスを VLAN にバインドします。	bind vlan <id> -ifnum <interface_name>、show vlan <id>	bind vlan 10 -ifnum 10/1、bind vlan 20 -ifnum 10/2
SNIP アドレスを追加します。	add ns ip <IPAddress> <netmask> -type SNIP、show ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP
HTTP サーバを表すサービスを作成する	add service <serviceName> <ip> HTTP <port>、show service <name>	add service SVC-S1 198.51.100.19 http 80、add service SVC-S2 198.51.100.20 http 80
HTTP 負荷分散仮想サーバーを作成し、サービスをバインドします。	add lb vserver <name> HTTP <ip> <port>;bind lb vserver <vserverName> <serviceName>; show lb vserver <name>	add lb vserver LBVS-1 http 203.0.113.15 80、bind lb vserver LBVS-1 SVC-S1
カスタム TCP プロファイルを作成し、ジャンボフレームをサポートするための MSS を設定します。	add tcpProfile <name> -mss <positive_integer>、show tcpProfile <name>	add tcpprofile NS1-SERVERS-JUMBO -mss 8960
カスタム TCP プロファイルを目的のサービスにバインドします。	set service <Name> -tcpProfileName <string>、show service <name>	set service SVC-S1 -tcpProfileName NS1-SERVERS-JUMBO、set service SVC-S2 -tcpProfileName NS1-SERVERS-JUMBO
設定を保存する	save ns config; show ns config

ユースケース：同じインターフェイスセットでのジャンボフローと非ジャンボフローの共存

負荷分散仮想サーバー LBVS1 と LBVS2 が NetScaler インスタンス NS1 上に構成されている例を考えてみましょう。LBVS1 はサーバー S1 と S2 間での HTTP トラフィックの負荷分散に使用され、global はサーバー S3 と S4 間でトラフィックの負荷分散に使用されます。

CL1 は VLAN 10 に、S1 と S2 は VLAN 20 に、CL2 は VLAN 30 に、S3 と S4 は VLAN 40 上にあります。VLAN 10 と VLAN 20 はジャンボフレームをサポートし、VLAN 30 と VLAN 40 は非ジャンボフレームだけをサポートします。

つまり、CL1 と NS1 間の接続、および NS1 とサーバ S1 または S2 の間の接続は、ジャンボフレームをサポートします。CL2 と NS1 間の接続、および NS1 とサーバ S3 または S4 の間の接続では、非ジャンボフレームのみがサポートされます。

NS1 のインターフェイス 10/1 は、クライアントとの間でトラフィックを送受信します。NS1 のインターフェイス 10/2 は、サーバとの間でトラフィックを送受信します。

インターフェイス 10/1 は、タグ付きインターフェイスとして VLAN 10 と VLAN 20 の両方にバインドされます。インターフェイス 10/2 は、タグ付きインターフェイスとして VLAN 30 と VLAN 40 の両方にバインドされます。

ジャンボフレームをサポートするために、インターフェイス 10/1 および 10/2 の MTU は 9216 に設定されます。

NS1 では、ジャンボフレームをサポートするために VLAN 10 と VLAN 30 の MTU が 9000 に設定されています。

VLAN 20 では MTU はデフォルト値の 1500 に設定され、非ジャンボフレームだけをサポートする場合は VLAN 40 に設定されます。

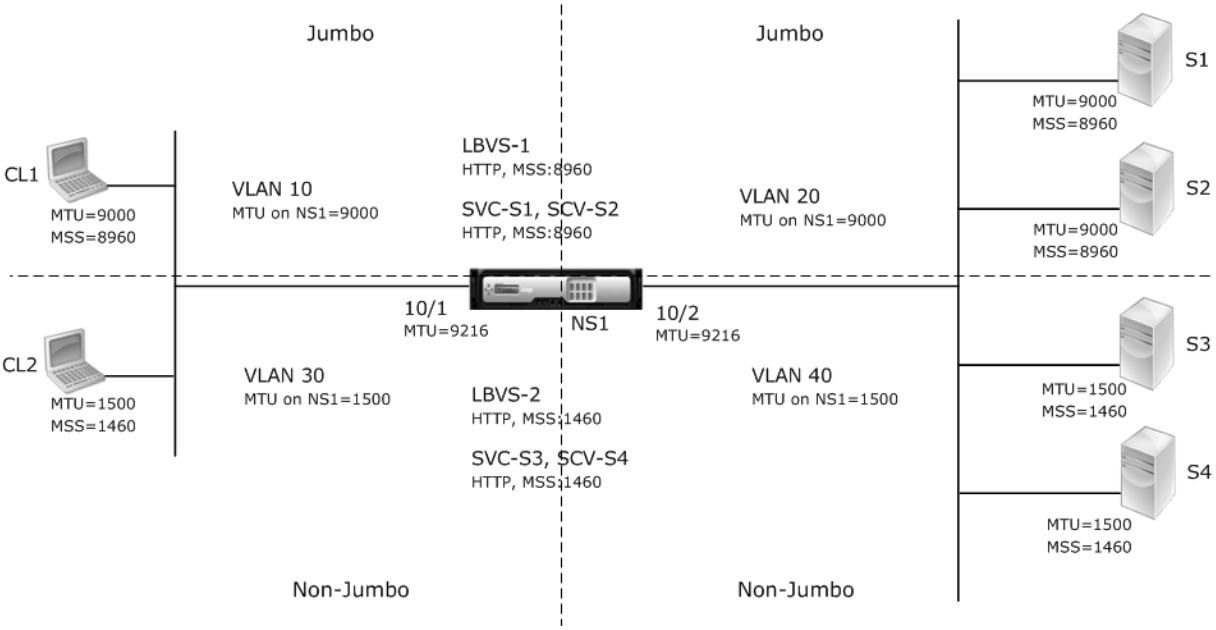
VLAN タグ付きパケットに対する ADC インターフェイスの有効な MTU は、インターフェイスの MTU または VLAN の MTU のいずれか小さい方になります。例:

- インターフェイス 10/1 の MTU は 9216 です。VLAN 10 の MTU は 9000 です。インターフェイス 10/1 では、VLAN 10 タグ付きパケットの MTU は 9000 です。
- インターフェイス 10/2 の MTU は 9216 です。VLAN 20 の MTU は 9000 です。インターフェイス 10/2 では、VLAN 20 タグ付きパケットの MTU は 9000 です。
- インターフェイス 10/1 の MTU は 9216 です。VLAN 30 の MTU は 1500 です。インターフェイス 10/1 では、VLAN 30 のタグ付きパケットの MTU は 1500 です。
- インターフェイス 10/2 の MTU は 9216 です。VLAN 40 の MTU は 1500 です。インターフェイス 10/2 では、VLAN 40 タグ付きパケットの MTU は 9000 です。

CL1、S1、S2、および CL1 と S1 または S2 の間にあるすべてのネットワークデバイスが、ジャンボフレーム用に設定されます。

HTTP トラフィックは TCP に基づいているため、ジャンボフレームをサポートするために、各エンドポイントで MSS が適切に設定されます。

- CL1 と NS1 の仮想サーバー LBVS-1 の間の接続では、NS1 上の MSS が TCP プロファイルに設定され、それが LBVS1 にバインドされます。
- NS1 と S1 の SNIP アドレス間の接続では、NS1 上の MSS が TCP プロファイルに設定され、NS1 上の S1 を表すサービス (SVC-S1) にバインドされます。



次の表に、この例で使用されている設定の一覧を示します。

| エンティティ |Name| 詳細 |
|–|–|–|
| クライアントの IP アドレス |CL1|192.0.2.10
||CL2|192.0.2.20
| サーバの IP アドレス |S1|198.51.100.19
||S2|198.51.100.20
||S3|198.51.101.19
||S4|198.51.101.20
|NS1 の SNIP アドレス ||198.51.100.18; 198.51.101.18
|NS1 のインターフェイスと VLAN に指定された MTU|10/1|9216
||10/2|9216
|VLAN 10|9000
|VLAN 20|9000
|VLAN 30|9000
|VLAN 40|1500
| デフォルト TCP プロファイル |nstcp_default_profile|MSS: 1460
| カスタム TCP プロファイル | すべてジャンボ |MSS: 8960
|NS1 上のサーバを表すサービス |SVC-S1 |IP アドレス:198.51.100.19; プロトコル:HTTP; ポート:80;TCP プロファイル: オールジャンボ (MSS: 8960)
||SVC-S2|IP アドレス:198.51.100.20; プロトコル:HTTP; ポート:80; TCP プロファイル: オールジャンボ (MSS: 8960)
||SVC-S3|IP アドレス:198.51.101.19; プロトコル:HTTP; ポート:80; TCP プロファイル:nstcp_default_profile (MSTCP_default_profile (MSTCP_default_profile) SS: 1460)
||SVC-S4|IP アドレス:198.51.101.20; プロトコル:HTTP; ポート:80; TCP プロファイル:nstcp_default_profile (MSS: 1460)
|NS1 上の負荷分散仮想サーバー |LBVS-1 |IP アドレス = 203.0.113.15; プロトコル:HTTP; ポート:80。バインドされたサービス:SVC-S1、SVC-S2、TCP プロファイル: オールジャンボ (MSS: 8960)
||LBVS-2 |IP アドレス = 203.0.114.15、プロトコル:HTTP、ポート:80。バインドされたサービス:SVC-S3、SVC-S4、TCP プロファイル:nstcp_default_profile (MSS: 1460)

次に、CL1 が S1 に要求した場合のトラフィックフローを示します。

1. クライアント CL1 は、NS1 の仮想サーバ LBVS-1 に送信する 20000 バイトの HTTP 要求を作成します。
2. CL1 は NS1 の LBVS-1 への接続をオープンします。CL1 と NS1 は、接続の確立中に TCP MSS 値を交換します。
3. NS1 の MSS 値は HTTP 要求よりも小さいので、CL1 は要求データを NS1 の MSS の倍数に分割し、VLAN 10 としてタグ付けされた IP パケットでこれらのセグメントを NS1 に送信します。
    - 最初の 2 つのパケットのサイズ = [IP ヘッダー + TCP ヘッダー + (TCP セグメント = NS1 MSS)] = [20 + 20 + 8960] = 9000
    - 最後のパケットのサイズ = [IP ヘッダー + TCP ヘッダー + (残りの TCP セグメント)] = [20 + 20 +

2080] = 2120

4. NS1 は、これらのパケットをインタフェース 10/1 で受信します。NS1 はこれらのパケットを受け入れるのは、これらのパケットのサイズが VLAN 10 タグ付きパケットのインターフェイス 10/1 の実効 MTU（9000）以下であるためです。
5. NS1 は IP パケットからすべての TCP セグメントをアセンブルし、20000 バイトの HTTP 要求を形成します。NS1 はこの要求を処理します。
6. LBVS-1 の負荷分散アルゴリズムはサーバー S1 を選択し、NS1 はその SNIP アドレスの 1 つと S1 の間の接続を開きます。NS1 と CL1 は、接続の確立中にそれぞれの TCP MSS 値を交換します。
7. NS1 は、要求データを S1 の MSS の倍数に分割し、これらのセグメントを VLAN 20 とタグ付けされた IP パケットで S1 に送信します。

    - 最初の 2 つのパケットのサイズ = [IP ヘッダー + TCP ヘッダー + (TCP ペイロード = S1 MSS)] = [20 + 20 + 8960] = 9000
    - 最後のパケットのサイズ = [IP ヘッダー + TCP ヘッダー + (残りの TCP セグメント)] = [20 + 20 + 2080] = 2120

CL1 に対する S1 の応答のトラフィックフローを次に示します。

1. サーバ S1 は 30000 バイトの HTTP 応答を作成し、NS1 の SNIP アドレスに送信します。
2. S1 は応答データを NS1 の MSS の倍数に分割し、これらのセグメントを VLAN 20 としてタグ付けされた IP パケットで NS1 に送信します。これらの IP パケットは、S1 の IP アドレスから送信され、NS1 の SNIP アドレスを宛先とします。

    - 最初の 3 つのパケットのサイズ = [IP ヘッダー + TCP ヘッダー + (TCP セグメント = NS1 の MSS サイズ)] = [20 + 20 + 8960] = 9000
    - 最後のパケットのサイズ = [IP ヘッダー + TCP ヘッダー + (残りの TCP セグメント)] = [20 + 20 + 3120] = 3160

3. NS1 は、インターフェイス 10/2 で応答パケットを受信します。NS1 はこれらのパケットを受け入れます。これは、そのサイズが VLAN 20 タグ付きパケットのインターフェイス 10/2 の実効 MTU 値（9000）以下であるためです。
4. NS1 は、これらの IP パケットからすべての TCP セグメントを組み立てて、30000 バイトの HTTP 応答を形成します。NS1 はこのレスポンスを処理します。
5. NS1 は、応答データを CL1 の MSS の倍数にセグメント化し、これらのセグメントを VLAN 10 としてタグ付けされた IP パケットで、インターフェイス 10/1 から CL1 に送信します。これらの IP パケットは LBVS の IP アドレスから発信され、CL1 の IP アドレスを宛先とします。

    - 最初の 3 つのパケットのサイズ = [IP ヘッダー + TCP ヘッダー + [(TCP ペイロード = CL1 の MSS サイズ)] = [20 + 20 + 8960] = 9000
    - 最後のパケットのサイズ = [IP ヘッダー + TCP ヘッダー + (残りの TCP セグメント)] = [20 + 20 + 3120] = 3160

設定タスク:

SDX Management Service で、[構成] **>** [システム] **>** [インターフェイス] ページに移動します。必要なインターフェイスを選択し、[**Edit**] をクリックします。MTU 値を設定し、**OK** をクリックします。

例:

次の MTU 値を設定します。

- 10/1 インターフェイスの場合は 9216
- 10/2 インターフェイスの場合は 9216

NetScaler インスタンスにログオンし、ADC コマンドラインインターフェイスを使用して残りの構成手順を完了します。

次の表は、NetScaler インスタンスで必要な構成を作成するためのタスク、コマンド、および例を示しています。

タスク	構文	例
–	–	–
VLAN を作成し、ジャンボフレームをサポートする VLAN の MTU を設定します。	add vlan <id> –mtu <positive_integer>、show vlan <id>	add vlan 10 –mtu 9000add vlan 20 –mtu 9000;add vlan 30 –mtu 1500;add vlan 40 –mtu 1500
インターフェイスを VLAN にバインドします。	bind vlan <id> –ifnum <interface_name>、show vlan <id>	bind vlan 10 –ifnum 10/1 –taggedbind vlan 20 –ifnum 10/2 –tagged;bind vlan 30 –ifnum 10/1 –tagged;bind vlan 40 –ifnum 10/2 –tagged
SNIP アドレスを追加します。	add ns ip <IPAddress> <netmask> –type SNIP、show ns ip	add ns ip 198.51.100.18 255.255.255.0 –type SNIP、add ns ip 198.51.101.18 255.255.255.0 –type SNIP
HTTP サーバを表すサービスを作成します。	add service <serviceName> <ip> HTTP <port>、show service <name>	add service SVC-S1 198.51.100.19 http 80add service SVC-S2 198.51.100.20 http 80;add service SVC-S3 198.51.101.19 http 80;add service SVC-S4 198.51.101.20 http 80
HTTP 負荷分散仮想サーバーを作成し、サービスをバインドします。	add lb vserver <name> HTTP <ip> <port>; bind lb vserver <vserverName> <serviceName>;show lb vserver <name>	add lb vserver LBVS-1 http 203.0.113.15 80; bind lb vserver LBVS-1 SVC-S1;bind lb vserver LBVS-1 SVC-S2
		add lb vserver LBVS-2 http 203.0.114.15 80; bind lb vserver LBVS-2 SVC-S3;bind lb vserver LBVS-2 SVC-S4
カスタム TCP プロファイルを作成し、ジャンボフレームをサポートするための MSS を設定します。	add tcpProfile <name> –mss <positive_integer>、show tcpProfile <name>	add tcpprofile ALL-JUMBO –mss 8960
カスタム TCP プロファイルを、必要な負荷分散仮想サーバとサービスにバインドします。	set service <Name> –tcpProfileName <string>、show service <name>	set lb vserver LBVS-1 – tcpProfileName ALL-JUMBO; set service SVC-S1 – tcpProfileName


```
 ALL-JUMBO;set service SVC-S2 - tcpProfileName ALL-JUMBO|
```
| 設定の保存 |ns config の保存、ns config の表示 |

SDX アプライアンスでの SNMP の設定

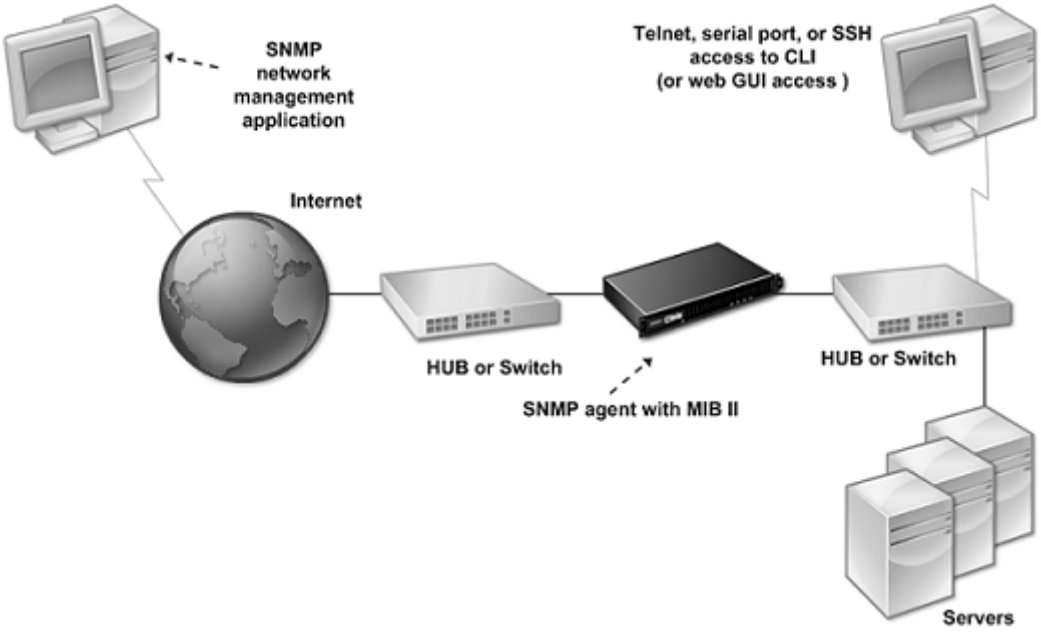
November 23, 2023

NetScaler SDX アプライアンスで SNMP エージェントを構成して、トラップと呼ばれる非同期イベントを生成できます。SDX アプライアンスに異常な状態が発生すると、トラップが生成されます。その後、トラップはトラップリスナーと呼ばれるリモートデバイスに送信され、SDX アプライアンスの異常状態を通知します。

SNMP トラップ先の構成、MIB ファイルのダウンロード、および 1 つ以上の SNMP マネージャーの設定に加えて、NetScaler SDX アプライアンスを SNMPv3 クエリ用に構成できます。

次の図は、SNMP が有効化され構成された SDX アプライアンスを持つネットワークを示しています。この図では、各 SNMP ネットワーク管理アプリケーションが SNMP を使用して SDX アプライアンス上の SNMP エージェントと通信しています。

図 1: *SNMP* をサポートする *SDX* アプライアンス



SDX アプライアンス上の SNMP エージェントは、SNMPv2 にのみ準拠するトラップを生成します。サポートされているトラップは SDX MIB ファイルで確認できます。このファイルは、SDX ユーザーインターフェイスの [ダウンロード] ページからダウンロードできます。

SNMP トラップ送信先を追加するには

1. [構成] タブのナビゲーションウィンドウで、[システム**] > [SNMP**] を展開し、[SNMP トラップの送信先] をクリックします。
2. [SNMP トラップの送信先] ペインで、[追加] をクリックします。
3. [SNMP トラップ送信先の設定] ページで、次のパラメータの値を指定します。
   - 宛先サーバ：SNMP トラップメッセージの送信先となるトラップリスナーの IPv4 アドレス。
   - port：トラップリスナーがトラップメッセージをリッスンする UDP ポート。トラップリスナーの設定と一致する必要があります。一致しない場合、リスナーはメッセージをドロップします。最小値:1。デフォルト:162。
   - [Community]：トラップリスナーがトラップメッセージを認証できるように、トラップメッセージとともに送信されるパスワード（文字列）。英字、数字、ハイフン (-)、ピリオド (.)、ハッシュ (#)、スペース ()、アットマーク (@)、等号 (=)、コロン (:)、アンダースコア (_) を使用できます。
     注: トラップリスナーデバイスで同じコミュニティストリングを指定すると、リスナーはメッセージをドロップします。デフォルト: パブリック。
4. [追加] をクリックし、[閉じる] をクリックします。追加した SNMP トラップの宛先が [SNMP Traps] ペインに表示されます。

   SNMP トラップ送信先のパラメーターの値を変更するには、[SNMP トラップの宛先] ウィンドウで、変更するトラップ送信先を選択し、[変更] をクリックします。[SNMP トラップ送信先の変更] ダイアログボックスで、パラメータを変更します。

   SNMP トラップを削除するには、[SNMP トラップの送信先] ウィンドウで、削除するトラップの送信先を選択し、[削除] をクリックします。[Confirm] メッセージボックスで、SNMP トラップの宛先をクリックして削除します。

MIB ファイルのダウンロード

SDX アプライアンスの監視を開始する前に、次のファイルをダウンロードする必要があります。

SDX-MIB-smiv2.mib. このファイルは SNMPv2 マネージャと SNMPv2 トラップリスナーによって使用されます。

このファイルには、SDX 固有のイベントを提供する NetScaler エンタープライズ MIB が含まれています。

MIB ファイルをダウンロードするには

1. SDX アプライアンスユーザーインターフェイスの [ダウンロード] ページにログオンします。
2. [SNMP ファイル] で、[SNMP v2-MIB オブジェクト定義] をクリックします。このファイルは MIB ブラウザを使用して開くことができます。

SNMP マネージャコミュニティの追加

SDX アプライアンスで SNMP Manager を構成し、アプライアンスおよびアプライアンスでホストされている管理対象デバイスのクエリと監視を行います。また、必要なアプライアンス固有の情報を SNMP Manager に提供する必要があります。IPv4 SNMP マネージャでは、マネージャの IP アドレスの代わりにホスト名を指定できます。その場合は、SNMP マネージャのホスト名を IP アドレスに解決する DNS ネームサーバを追加する必要があります。

SNMP マネージャを少なくとも 1 つ設定します。SNMP マネージャを設定しない場合、アプライアンスはネットワーク上の IP アドレスからの SNMP クエリーを受け入れたり、応答したりしません。1 つ以上の SNMP マネージャを設定すると、アプライアンスはその特定の IP アドレスからの SNMP クエリのみを受け入れ、応答します。

SNMP マネージャを設定するには

1. [構成] タブのナビゲーションウィンドウで、[システム]、[SNMP] の順に展開します。
2. [マネージャー] をクリックします。
3. 詳細ペインで、[Add] をクリックします。
4. [SNMP Manager コミュニティの作成] ページで、次のパラメータを設定します。
    - SNMP マネージャ：SNMP マネージャの IPv4 アドレス。また、IPv4 アドレスの代わりに、SNMP マネージャに割り当てられているホスト名を指定することもできます。その場合は、SNMP マネージャのホスト名を IP アドレスに解決する DNS ネームサーバを追加する必要があります。
    - [Community]：SNMP コミュニティストリング。大文字と小文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、アットマーク (@)、等号 (=)、コロン (:)、アンダースコア (_) を含む 1 ～31 文字で構成できます。
    - ネットマスクを使用して SNMP マネージャを指定するには、[管理ネットワークを有効にする] チェックボックスをオンにします。
    - [**Netmask**] フィールドに、SNMP コミュニティのネットマスクを入力します。
5. [追加] をクリックし、[閉じる] をクリックします。

SNMPv3 クエリ用の **SDX** アプライアンスの設定

SNMPv3 は、SNMPv1 と SNMPv2 の基本構造とアーキテクチャに基づいています。ただし、SNMPv3 では基本アーキテクチャが強化され、認証、アクセスコントロール、データ整合性チェック、データ発信元検証、メッセージの適時性チェック、データ機密性などの管理機能とセキュリティ機能が組み込まれています。

NetScaler SDX アプライアンスは、SNMPv3 のセキュリティ機能を実装できる以下のエンティティをサポートしています。

- SNMP ビュー
- SNMP ユーザ

これらのエンティティは連携して機能し、SNMPv3 セキュリティ機能を実装します。MIB のサブツリーにアクセスできるように、ビューが作成されます。

SNMP マネージャの追加

適切な SNMP マネージャがクエリを実行できるように SDX アプライアンスを設定します。また、必要なアプライアンス固有の情報を SNMP マネージャに提供します。IPv4 SNMP マネージャでは、マネージャの IP アドレスの代わりにホスト名を指定できます。その場合は、SNMP マネージャのホスト名を IP アドレスに解決する DNS ネームサーバを追加する必要があります。

SNMP マネージャを少なくとも 1 つ設定します。SNMP マネージャを設定しない場合、アプライアンスはネットワーク上の IP アドレスからの SNMP クエリーを受け入れたり、応答したりしません。1 つ以上の SNMP マネージャを設定すると、アプライアンスはその特定の IP アドレスからの SNMP クエリのみを受け入れ、応答します。

SNMP マネージャを設定するには、次の手順を実行します。

1. [システム**] > [**構成] ページに移動します。
2. [構成] タブのナビゲーションウィンドウで、[システム]、[SNMP] の順に展開します。
3. [マネージャー] をクリックします。
4. 詳細ペインで、[Add] をクリックします。
5. [SNMP Manager コミュニティの追加] ダイアログボックスで、次のパラメータを設定します。
    - **SNMP** マネージャ：**SNMP** マネージャの IPv4 アドレス。また、IPv4 アドレスの代わりに、SNMP マネージャに割り当てられているホスト名を指定することもできます。その場合は、SNMP マネージャのホスト名を IP アドレスに解決する DNS ネームサーバを追加する必要があります。
    - [**Community**]：SNMP コミュニティストリング。大文字と小文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、アットマーク (@)、等号 (=)、コロン (:)、アンダースコア (_) を含む 1 ～31 文字で構成できます。
6. [追加] をクリックし、[閉じる] をクリックします。

SNMP ビューの構成

SNMP ビューは、ユーザアクセスを MIB の特定の部分に制限します。SNMP ビューはアクセス制御の実装に使用されます。

ビューを設定するには

1. [構成] タブのナビゲーションウィンドウで、[システム]、[SNMP] の順に展開します。
2. [ビュー] をクリックします。
3. 詳細ペインで、[Add] をクリックします。
4. [SNMP View の追加（Add SNMP View）] ダイアログボックスで、次のパラメータを設定します。

- [Name]: SNMPv3 ビューの名前。大文字、小文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、アットマーク (@)、等号 (=)、コロン (:)、アンダースコア (_) を含む 1 ～31 文字で構成されます。SNMPv3 ビューの識別に役立つ名前を選択します。
- [Subtree]: この SNMPv3 ビューに関連付ける MIB ツリーの特定のブランチ（サブツリー）。サブツリーを SNMP OID として指定します。
- [Type]: subtree パラメータで指定されたサブツリーをこのビューに含めるか、このビューから除外します。この設定は、A などのサブツリーを SNMPv3 ビューに含め、B などの A の特定のサブツリーを SNMPv3 ビューから除外する場合に便利です。

SNMP ユーザの設定

SNMP ビューを作成したら、SNMP ユーザを追加します。SNMP ユーザは、SNMP マネージャへのクエリーに必要な MIB にアクセスできます。

ユーザーを構成するには

1. [構成] タブのナビゲーションウィンドウで、[システム]、[SNMP] の順に展開します。
2. [ユーザー] をクリックします。
3. 詳細ペインで、［Add］をクリックします。
4. [SNMP ユーザの作成（Create SNMP User）] ページで、次のパラメータを設定します。

    - [Name]: SNMPv3 ユーザの名前。大文字、小文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、アットマーク (@)、等号 (=)、コロン (:)、アンダースコア (_) を含む 1 ～31 文字で構成されます。
    - [Security Level]: アプライアンスと SNMPv3 ユーザ間の通信に必要なセキュリティレベル。次のいずれかのオプションを選択します:
        - noauthNoPriv: 認証も暗号化も必要ありません。
        - authNoPriv: 認証が必要ですが、暗号化は不要です。
        - authPriv: 認証と暗号化が必要です。
    - 認証プロトコル: アプライアンスと SNMPv3 ユーザ間の通信を認証するために使用する認証アルゴリズム。SNMP マネージャで SNMPv3 ユーザを設定するときに、同じ認証アルゴリズムを指定します。
    - [認証パスワード（Authentication Password）]: 認証アルゴリズムで使用されるパスフレーズ。大文字と小文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等号 (=)、コロン (:)、アンダースコア (_) を含む 1 ～31 文字で構成されます。
    - [Privacy Protocol]: アプライアンスと SNMPv3 ユーザ間の通信を暗号化するために使用する暗号化アルゴリズム。SNMP マネージャで SNMPv3 ユーザを設定するときに、同じ暗号化アルゴリズムを指定します。
    - [View Name]: この SNMPv3 ユーザにバインドする、設定済みの SNMPv3 ビューの名前。SNMPv3 ユーザは、この SNMPv3 ビューに INCLUDED タイプとしてバインドされているサブツリーにアクセスできますが、EXCLUDED タイプのサブツリーにはアクセスできません。

SNMP アラームの設定

アプライアンスには、SNMP アラームと呼ばれる条件エンティティのセットがあらかじめ定義されています。SNMP アラームに設定された条件が満たされると、アプライアンスは SNMP トラップメッセージを生成し、設定されたトラップリスナーに送信されます。たとえば、DeviceAdded アラームが有効な場合、アプライアンスにデバイス（インスタンス）がプロビジョニングされるたびに、トラップメッセージが生成され、トラップリスナーに送信されます。SNMP アラームには重大度を割り当てることができます。その場合、対応するトラップメッセージにその重大度が割り当てられます。

アプライアンスに定義されている重大度レベルを、重大度の降順で示します。

- 重大
  - 重要
- 軽度
- 警告
- 情報 (デフォルト)

たとえば、DeviceAdded という名前の SNMP アラームに Warning 重大度を設定すると、デバイスの追加時に生成されるトラップメッセージには、Warning 重大度が割り当てられます。

SNMP アラームを設定して、そのアラームの条件が満たされたときに生成される対応するトラップメッセージをログに記録することもできます。

定義済みの SNMP アラームを変更するには、[システム**] > [SNMP] > [**アラーム] をクリックします。

Syslog 通知の設定

November 23, 2023

SYSLOG は標準のロギングプロトコルです。NetScaler SDX アプライアンスで実行される SYSLOG 監査モジュールと、リモートシステムで実行できる SYSLOG サーバーの 2 つのコンポーネントで構成されています。SYSLOG はデータ転送に UDP を使用します。

SYSLOG サーバーを実行すると、SDX アプライアンスに接続されます。その後、アプライアンスはすべてのログ情報を SYSLOG サーバに送信し始め、サーバはログエントリをフィルタリングしてからログファイルに保存できます。SYSLOG サーバは複数の SDX アプライアンスからログ情報を受信でき、SDX アプライアンスは複数の SYSLOG サーバにログ情報を送信できます。

SYSLOG サーバが
SDX アプライアンスから収集するログ情報は、メッセージ形式でログファイルに保存されます。通常、これらのメッセージには次の情報が含まれています。

- ログメッセージを生成した SDX アプライアンスの IP アドレス
- タイムスタンプ
- メッセージの種類
- ログレベル (重大、エラー、通知、警告、情報、デバッグ、アラート、緊急)
- メッセージの情報

この情報を使用してアラートの原因を分析したり、必要に応じて修正作業を行ったりすることができます。まず、アプライアンスがログ情報を送信する Syslog サーバを設定し、ログメッセージを記録するためのデータと時刻の形式を指定します。

Syslog サーバを設定する

1. [システム**] > [**通知**] > [syslog** サーバ**]** に移動します。
2. 詳細ペインで、[追加] をクリックします。
3. **[Syslog** サーバの作成] ページで、Syslog サーバパラメータの値を指定します。パラメーターの説明を表示するには、対応するフィールドの上にマウスポインターを置きます。
4. [追加] をクリックし、[閉じる] をクリックします。

Syslog パラメータを設定します

1. [システム**] > [**通知**] > [syslog** サーバ**]** に移動します。
2. 詳細ウィンドウで、[**Syslog** パラメータ] をクリックします。
3. **[Syslog** パラメータの設定] ページで、日付と時刻の形式を指定します。
4. 「**OK**」をクリックし、「閉じる」をクリックします。

メール通知の設定

November 23, 2023

アラートが発生するたびに電子メールメッセージを受信するように SMTP サーバーを構成します。最初に SMTP サーバーを構成し、次にメールプロファイルを構成します。メールプロファイルでは、受信者のアドレスをカンマで区切ります。

SMTP サーバーを構成するには

1. [**System**] > [**Notifications**] > [**Email**] の順に選択します。
2. 詳細ウィンドウで [電子メールサーバー] タブをクリックし、[追加] をクリックします。

3. **[**電子メールサーバの作成] ページで、サーバパラメータの値を指定します。

    - サーバー名**/ IP** アドレス:SMTP メール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: ポート番号を入力します。デフォルト値は 25 です。
    - 認証: メールサーバーへのアクセスを認証するには、このオプションを選択します。
    - セキュア: このオプションを選択すると、安全なメール接続を確立できます。デフォルトでは、TLS 1.2 がメール通信の暗号化に使用されます。

4. ［作成］をクリックします。

メールプロファイルを構成するには

1. ［**System**］**>** ［**Notifications**］**>** ［**Email**］の順に選択します。
2. 詳細ウィンドウで [電子メール] タブをクリックし、[追加] をクリックします。
3. **[**電子メール配布リストの作成] ページで、パラメータの値を指定します。パラメーターの説明を表示するには、対応するフィールドの上にマウスポインターを置きます。
4. ［作成］をクリックします。

SMS 通知を構成する

November 23, 2023

アラートが発生するたびに SMS メッセージを受信するように、ショートメッセージサービス (SMS) サーバーを構成します。最初に SMS サーバーを構成し、次に SMS プロファイルを構成します。SMS プロファイルでは、受信者のアドレスをカンマで区切ります。

SMS サーバーを構成する

1. ［**System**］**>** ［**Notifications**］**>** ［**SMS**］の順に選択します。
2. 詳細ウィンドウで [**SMS** サーバー] をクリックし、[追加] をクリックします。
3. [**SMS** サーバーの作成] ページで、SMS サーバーパラメーターの値を指定します。これらのパラメーターの値はベンダーから提供されます。
4. [作成] をクリックし、[閉じる] をクリックします。

SMS プロファイルを構成する

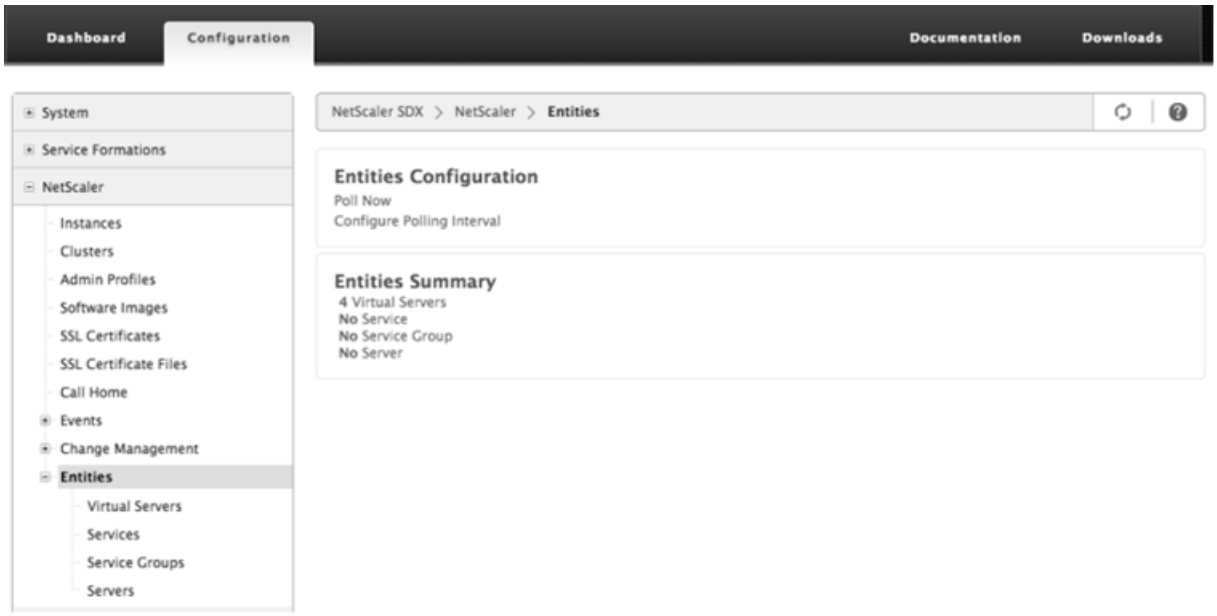
1. ［**System**］**>** ［**Notifications**］**>** ［**SMS**］の順に選択します。
2. 詳細ウィンドウで、[**SMS** 配布リスト] をクリックし、[追加] をクリックします。

3. **[SMS** 配布リストの作成] ページで、メールプロファイルパラメータの値を指定します。パラメーターの説明を表示するには、対応するフィールドの上にマウスポインターを置きます。
4. [作成] をクリックし、[閉じる] をクリックします。

SDX アプライアンスに構成されたエンティティのステータスをリアルタイムで監視および管理する

February 16, 2024

NetScaler SDX アプライアンスは、SDX アプライアンスでホストされている仮想アプライアンス全体の仮想サーバー、サービス、サービスグループ、およびサーバーの状態を監視および管理できます。仮想サーバの状態や、サービスまたはサービスグループの状態が最後に変更されてからの経過時間などの値を監視できます。この監視により、エンティティのステータスをリアルタイムで把握でき、NetScaler インスタンスに多数のエンティティが構成されている場合でもこれらのエンティティを簡単に管理できます。



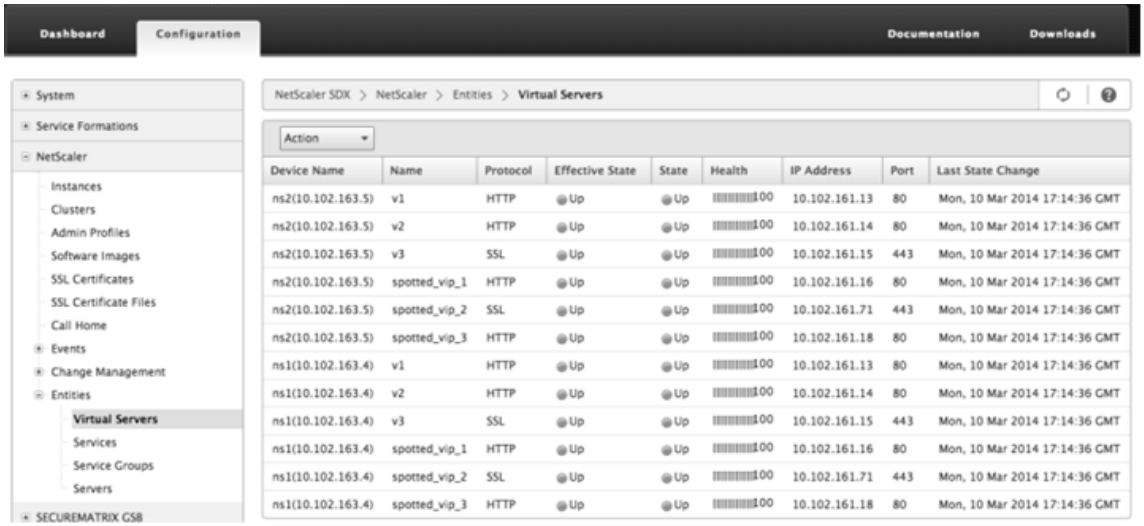
仮想サーバのステータスの表示

仮想サーバの状態と正常性の値をリアルタイムで監視できます。仮想サーバの名前、IP アドレス、タイプなど、仮想サーバの属性を表示することもできます。

- 仮想サーバのステータスを表示するには

    1. ナビゲーションペインの［構成］タブで、［**NetScaler**］**>**［エンティティ］**>**［仮想サーバー］をクリックします。

2. 右ウィンドウ枠の [仮想サーバー] で、次の統計情報を表示します。
   - [デバイス名（Device Name）]：仮想サーバが設定されている VPX の名前。
   - [Name]：仮想サーバの名前。
   - [Protocol]：仮想サーバのサービスタイプ。たとえば、HTTP、TCP、SSL などです。
   - 有効な状態：バックアップ仮想サーバの状態に基づいた、仮想サーバの有効な状態。たとえば、UP、DOWN、OUT OF SERVICE
   - [State]：仮想サーバの現在の状態。たとえば、UP、DOWN、OUT OF SERVICE
   - [Health]：UP 状態にあり、仮想サーバにバインドされているサービスの割合。正常性のパーセンテージの計算には、次の式を使用します。(バインドされた UP サービスの数 * 100)/バインドされたサービスの総数
   - IP アドレス：仮想サーバの IP アドレス。クライアントはこの IP アドレスに接続要求を送信します。
   - [Port]：仮想サーバがクライアント接続をリッスンするポート。
   - [Last State Change]：仮想サーバの状態が最後に変更されてからの経過時間（日、時、分、秒）。つまり、仮想サーバが現在の状態であった期間です。この情報は、NetScaler リリース 9.0 以降で構成された仮想サーバーでのみ使用できます。



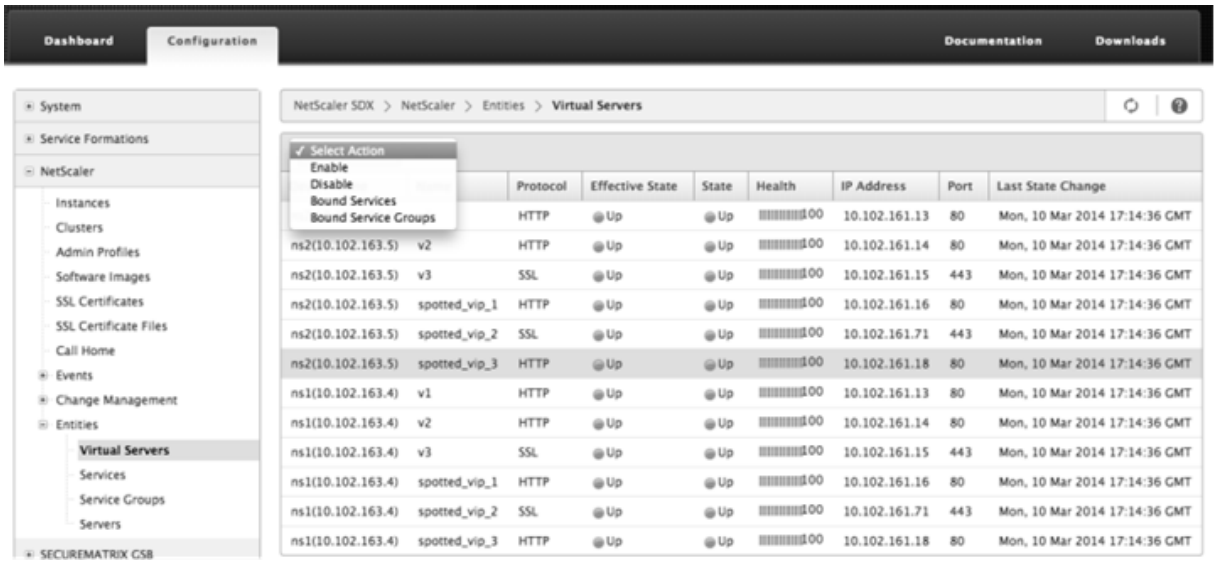
- 仮想サーバにバインドされたサービスおよびサービスグループの表示

  仮想サーバにバインドされたサービスおよびサービスグループのステータスをリアルタイムで監視できます。この監視により、仮想サーバーの正常性のパーセンテージが低くなる原因となる可能性のあるサービスの状態を確認できるため、適切なアクションを実行できます。

  仮想サーバにバインドされたサービスとサービスグループを表示するには

  1. [構成] タブの左側のペインで、[**NetScaler] > [**エンティティ**] > [**仮想サーバー] をクリックします。
  2. 詳細ウィンドウの [仮想サーバー] で、バインドされたサービスとサービスグループを表示する仮想サーバーの名前をクリックし、[アクション] の [バインドされたサービス] または [バインドされたサービスグループ] をクリックします。または、仮想サーバーの名前を右クリックし、[バインドされたサービス]

または [バインドされたサービスグループ] をクリックします。



サービスのステータスの表示

サービスの状態の値と、サービスが現在の状態にあった期間をリアルタイムで監視できます。

仮想サーバのステータスを表示するには

1. ナビゲーションペインの［構成］タブで、［**NetScaler**］**>**［エンティティ］［サービス］をクリックします。
2. 詳細ウィンドウの [サービス] で、次の統計情報を表示します。

    - [Device Name]：サービスが設定されているデバイスの名前。
    - [Name]：サービスの名前。
    - [Protocol]：サービスの動作を決定するサービスタイプ。たとえば、HTTP、TCP、UDP、または SSL などです。
    - State：サービスの現在の状態。たとえば、UP、DOWN、OUT OF SERVICE
    - IP アドレス：サービスの IP アドレス。
    - [Port]：サービスがリッスンするポート。
    - [Last State Change]：サービスの状態が最後に変更されてからの経過時間（日、時、分、秒）。つまり、サービスが現在の状態であった期間です。

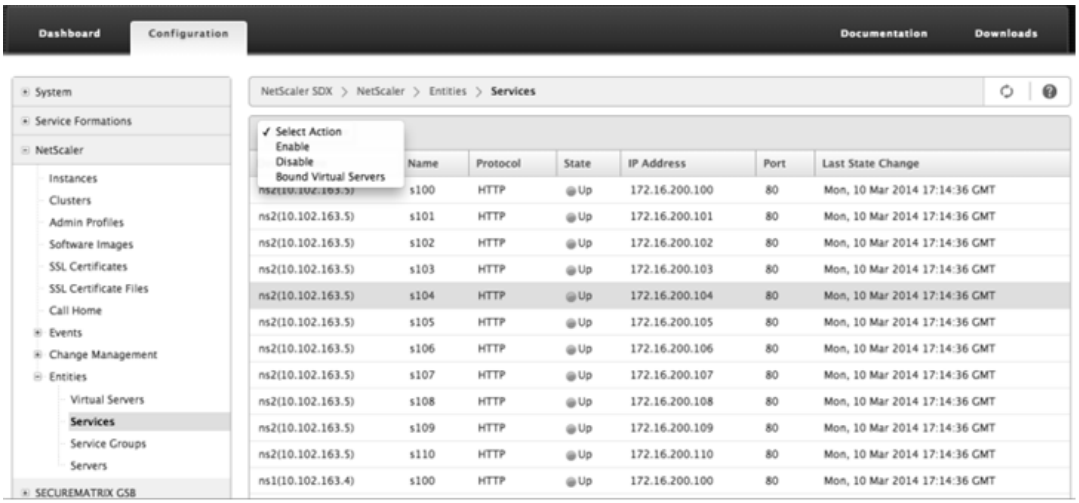
- サービスがバインドされている仮想サーバの表示

  サービスがバインドされている仮想サーバーを表示し、仮想サーバーのステータスをリアルタイムで監視できます。

  サービスがバインドされている仮想サーバーを表示するには

  1. ナビゲーションペインの［構成］タブで、［**NetScaler**］**>**［エンティティ］［サービス］をクリックします。

2. 詳細ウィンドウの [サービス] で、バインドされた仮想サーバーを表示するサービスの名前をクリックします。次に、[操作] メニューの [バインドされた仮想サーバー] を選択します。または、サービスを右クリックし、[バインドされた仮想サーバー] をクリックします。



サービスグループのステータスの表示

SDX インターフェイスから、サービスグループメンバーの状態をリアルタイムで監視できます。

サービスグループのステータスを表示するには

1. ナビゲーションペインの［構成］タブで、［**NetScaler**］**>**［エンティティ］**>**［サービスグループ］をクリックします。
2. 詳細ウィンドウの [サービスグループ] で、次の統計情報を表示します。

   - [Device Name]：サービスグループが設定されているデバイスの名前。
   - [Name]：サービスグループの名前。
   - IP アドレス：サービスグループのメンバーである各サービスの IP アドレス。
   - [Port]：サービスグループメンバーがリッスンするポート。
   - [Protocol]：サービスグループの動作を決定するサービスタイプ。たとえば、HTTP、TCP、UDP、または SSL などです。
   - 有効状態：バックアップ仮想サーバの状態に基づいた、仮想サーバグループの有効状態。たとえば、UP、DOWN、OUT OF Service
   - [State]：サービスグループのメンバーの状態に基づいた、サービスグループの有効な状態。たとえば、UP、DOWN、OUT OF SERVICE
   - [Last State Change]：サービスグループメンバーの状態が最後に変更されてからの経過時間（日、時、分、秒）。つまり、サービスグループメンバーが現在の状態であった期間です。この情報は、NetScaler リリース 9.0 以降で構成されたサービスグループメンバーにのみ表示されます。

- サービスがバインドされている仮想サーバの表示

サービスがバインドされている仮想サーバーを表示し、仮想サーバーのステータスをリアルタイムで監視できます。

サービスがバインドされている仮想サーバーを表示するには

1. [構成] タブの左側のペインで、[**NetScaler] > [エンティティ] **[サーバー] をクリックします。
2. 右ウィンドウの [サーバー] で、リストからサーバーを選択し、[アクション] メニューの [バインドされた仮想サービス] をクリックします。または、サービスを右クリックし、[バインドされた仮想サーバー] をクリックします。

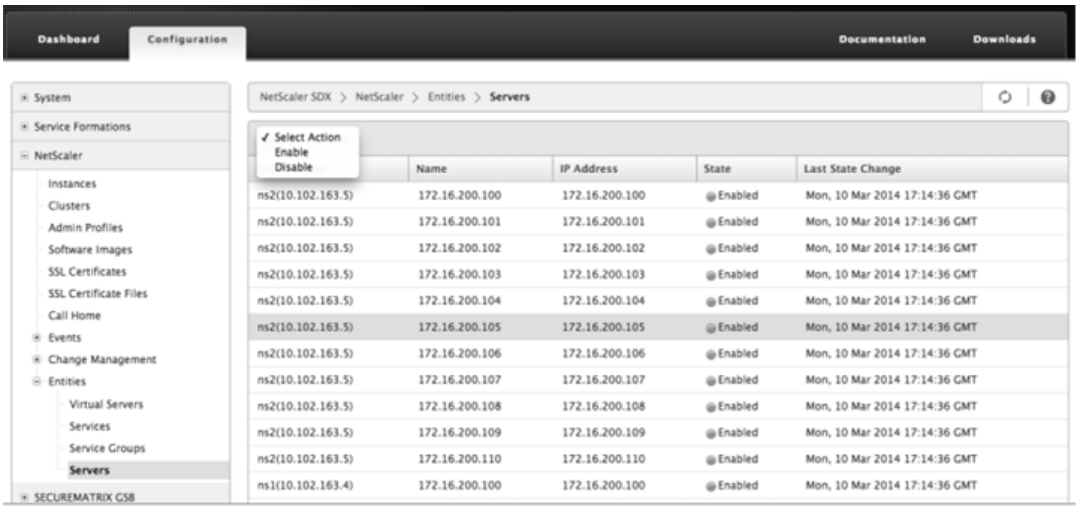
サーバのステータスを表示する

NetScaler インスタンス全体のサーバーの状態を監視および管理できます。この監視により、サーバーの状態をリアルタイムで把握でき、多数のサーバーがある場合でもこれらのサーバーの管理が容易になります。

サーバのステータスを表示するには

1. ナビゲーションペインの［構成］タブで、［**NetScaler**］**>**［エンティティ］［サーバー］をクリックします。
2. 詳細ウィンドウの [サーバー] で、次の統計情報を表示します。

   -
   - State: サーバの現在の状態を指定します。たとえば、アップ、ダウン、アウトオブサービスなどです。
   - [Last State Change]：サーバの状態が最後に変更されてからの経過時間（日、時、分、秒）を指定します。つまり、サーバが現在の状態にある期間です。



ポーリング間隔を構成する

SDX アプライアンスが仮想サーバ、サービス、サービスグループ、およびサーバのリアルタイム値をポーリングする時間間隔を設定できます。デフォルトでは、アプライアンスは 30 分ごとに値をポーリングします。

- 仮想サーバ、サービス、サービスグループ、およびサーバのポーリング間隔を構成します。

  1. [構成] タブで [**NetScaler] > [**エンティティ] をクリックし、右側のペインで [ポーリング間隔の構成] をクリックします。
  2. [ポーリング間隔の構成] ダイアログボックスで、SDX がエンティティ値をポーリングする間隔として設定する分数を入力します。ポーリング間隔の最小値は 30 分です。［OK］をクリックします。

NetScaler インスタンスで生成されるイベントの監視と管理

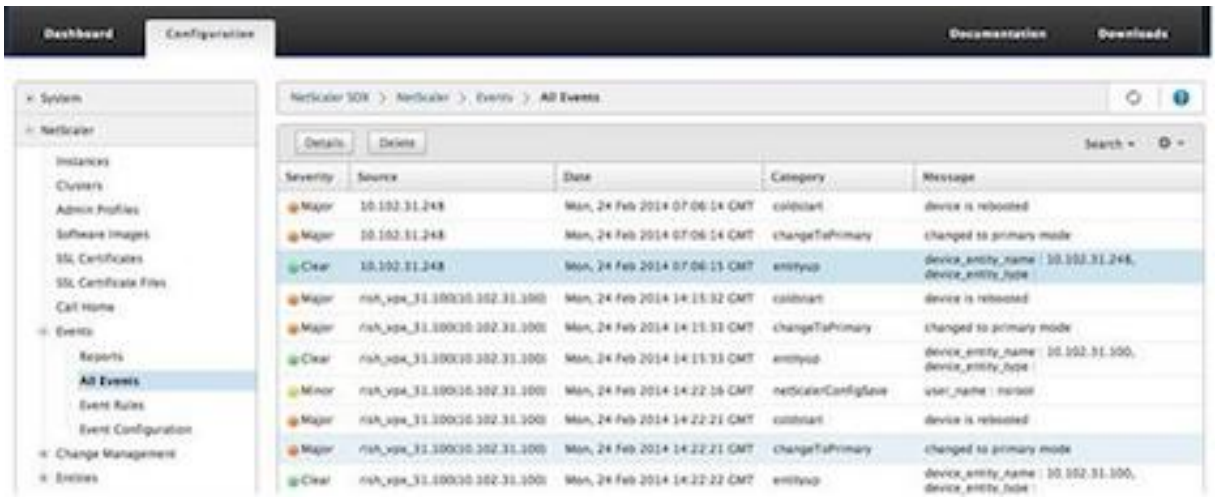
February 16, 2024

イベント機能を使用して、NetScaler インスタンスで生成されたイベントを監視および管理します。管理サービスはイベントをリアルタイムで識別し、問題に即座に対処し、NetScaler インスタンスを効果的に稼働させ続けるのに役立ちます。また、生成されたイベントをフィルタリングし、フィルタリングされたイベントリストに対してアクションを実行するよう通知を受けるようにイベントルールを設定することもできます。

すべてのイベントを表示する

NetScaler SDX アプライアンスにプロビジョニングされた NetScaler インスタンスで生成されたすべてのイベントを表示できます。各イベントの重要度、カテゴリ、日付、ソース、メッセージなどの詳細を表示できます。

イベントを表示するには、[構成**] > [NetScaler] > [**イベント**] > [**すべてのイベント] に移動します。



イベントを選択して [Details] ボタンをクリックすると、イベント履歴とエンティティの詳細を表示できます。特定のイベントを検索したり、このページから削除したりすることもできます。

注: イベントを削除すると、復元できなくなります。

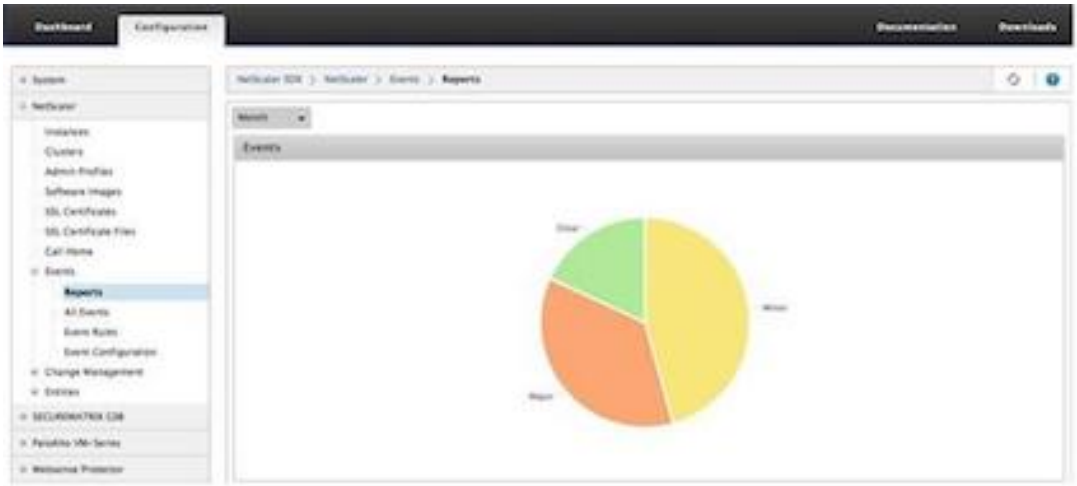
- レポートの表示

  [Reports] ページには、イベントの概要がグラフ形式で表示されます。レポートは、さまざまな時間スケールに基づいて表示できます。デフォルトのタイムスケールは Day です。

  レポートを表示するには、[** 構成] > [NetScaler] > [イベント] **[レポート] に移動します。管理サービスでサポートされるグラフィカルなレポートを次に示します。

  - イベント

    Events レポートは、イベントの数をセグメント化し、重大度に基づいて色分けした円グラフです。

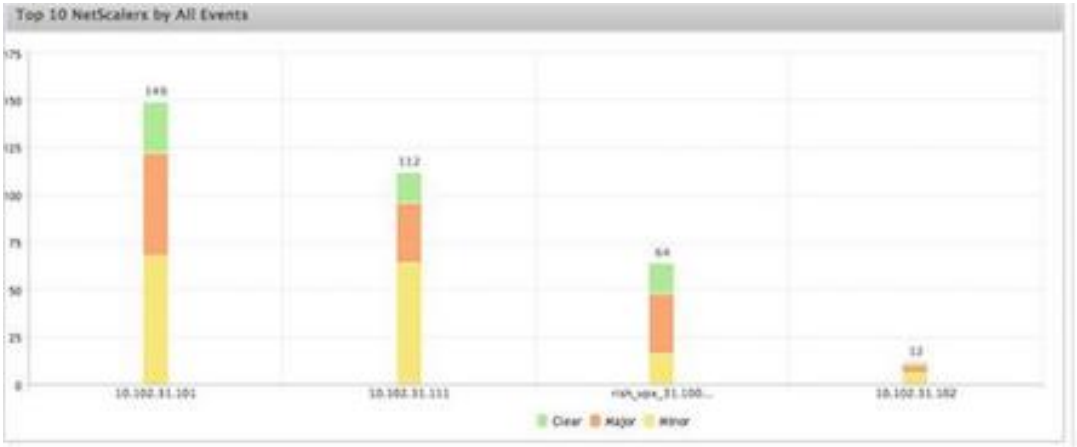
    

    特定の重大度のイベントの詳細を表示するには、円グラフのセグメントをクリックすると、次の詳細を表示できます。

    * Source: イベントが生成されたシステム名、ホスト名、または IP アドレス。
    * Date: アラームが生成された日時。
    * カテゴリ: イベントカテゴリ (`entityup`など)。
    * メッセージ: イベントの説明。

  - 全イベント別の **NetScaler** インスタンスの上位 **10** 件

    このレポートは、選択したタイムスケールのイベント数に応じて上位 10 個の NetScaler インスタンスを表示する棒グラフです。



– エンティティ状態変更イベント別の **NetScaler** インスタンスの上位 **10** 件

このレポートは、選択した期間におけるエンティティ状態の変化の数に応じて、上位 10 個の NetScaler インスタンスを表示する棒グラフです。エンティティの状態の変化は、エンティティのアップ、エンティティの停止、またはアウトオブサービスイベントを反映します。

– しきい値違反イベント別の **NetScaler** インスタンスの上位 **10** 件

このレポートは、選択したタイムスケールのしきい値違反イベントの数に応じて、上位 10 個の NetScaler インスタンスを表示する棒グラフです。しきい値違反イベントには、次のイベントが反映されます。

* cpuUtilization
* memoryUtilization
* diskUsageHigh
* temperatureHigh
* voltageLow
* voltageHigh
* fanSpeedLow
* temperatureCpuHigh

    * interfaceThroughputLow
    * interfaceBWUseHigh
    * aggregateBWUseHigh

- ハードウェア障害イベント別の上位 **10** 個の **NetScaler** インスタンスこのレポートは
  、選択した期間におけるハードウェア障害イベントの数に応じて、上位 10 個の NetScaler インスタンスを表示する棒グラフです。ハードウェア障害イベントには、次のイベントが反映されます。
    * hardDiskDriveErrors
    * compactFlashErrors
    * powerSupplyFailed
    * “sslCardFailed”

- 構成変更イベント別の **NetScaler** インスタンスの上位 **10** 件

  このレポートは、選択した期間における構成変更イベントの数に応じて、上位 10 個の NetScaler インスタンスを反映した棒グラフです。グラフをクリックすると、インスタンスのユーザーベースの設定変更をドリルダウンして表示できます。このグラフをクリックすると、承認ステータスと実行ステータスの詳細をさらに表示できます。

- < 認証失敗イベント別の **NetScaler** インスタンスの上位 **10** 件

  このレポートは、選択した期間における認証失敗イベントの数に応じて、上位 10 個の NetScaler インスタンスを表示する棒グラフです。グラフをクリックすると、インスタンスのユーザーベースの認証失敗をドリルダウンして表示できます。

- イベント規則の設定

  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条件に一致すると、その規則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、デバイス、障害オブジェクト、カテゴリです。

  次のアクションをイベントに割り当てられます。

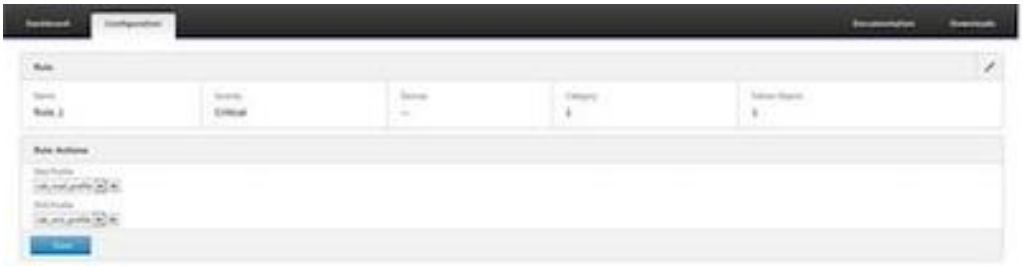
  - **[**電子メールを送信**]** アクションフィルタ条件に一致するイベントを電子メールで送信します。
  - **[SMS** アクションの送信] フィルタ条件に一致するイベントのショートメッセージサービス (SMS) を送信します。

  イベントルールを追加するには

  1. [構成**] > [NetScaler] > [**イベント**] > [**イベントルール] に移動し、[追加] をクリックします。
  2. [Rule] ページで、次のパラメータを設定します。
     - Name - イベント規則の名前です。
     - Enabled - イベント規則を有効にします。
     - Severity - イベント規則に追加するイベントの重要度です。
     - デバイス—イベントルールを定義する NetScaler インスタンスの IP アドレス。
     - Category - NetScaler インスタンスが生成するイベントのカテゴリです。
     - Failure Objects - イベント生成の対象であるエンティティインスタンスまたはカウンターです。

注: このリストには、すべてのしきい値関連イベントのカウンタ名、すべてのエンティティ関連イベントのエンティティ名、および証明書関連イベントの証明書名を含めることができます。

3. ［保存］をクリックします。
4. 「ルールアクション」(Rule Actions) で、イベントに通知アクションを割り当てることができます。
   a) Mail Profile - メールサーバーとメールプロファイルの詳細です。イベントが定義されたフィルター条件を満たすとき、メールがトリガーされます。
   b) SMS Profile - SMS サーバーと SMS プロファイルの詳細です。定義したフィルタ条件にイベントが一致すると、SMS がトリガされます。

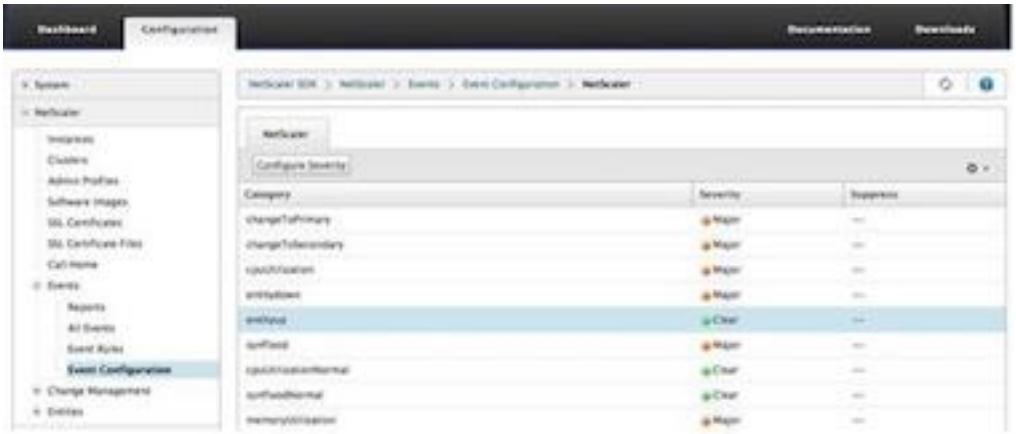


5. ［完了］をクリックします。

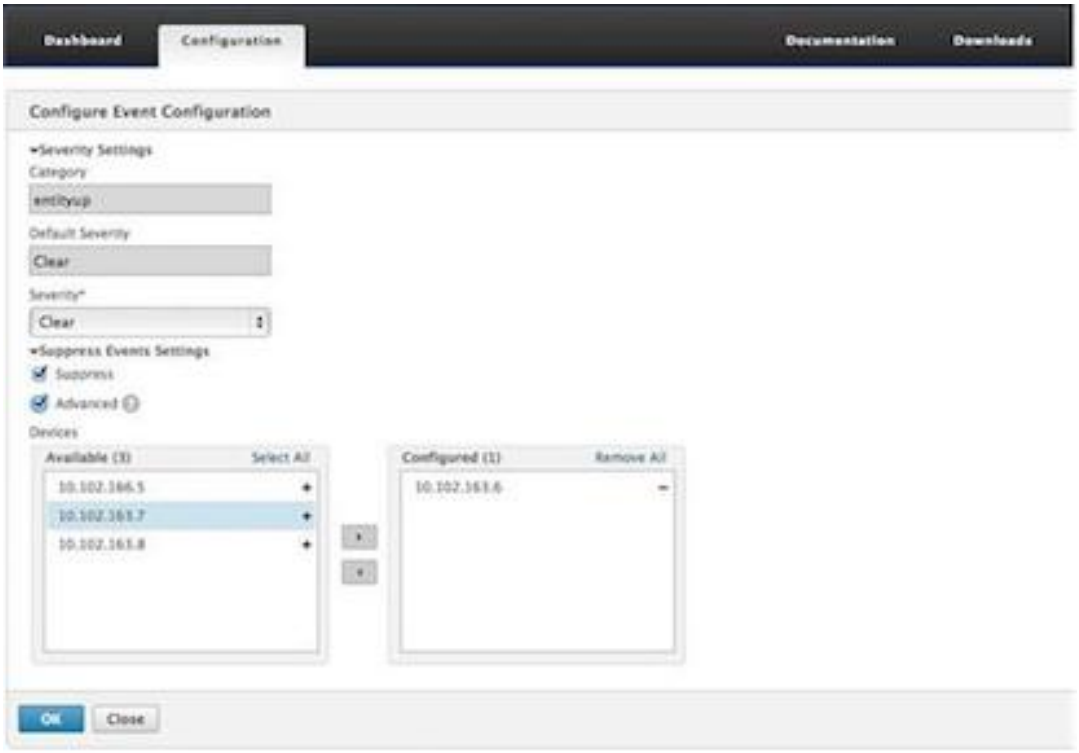
- イベントを設定する

  SDX アプライアンス上の NetScaler インスタンスに対して生成されるイベントに重大度レベルを割り当てることができます。重大、メジャー、マイナー、警告、クリア、情報の重大度レベルを定義できます。また、特定の時間だけイベントを抑止することもできます。
  重要度を設定するには、次の手順に従います。

  1. [構成**] > [NetScaler] > [**イベント**] > [**イベント構成] に移動し、一覧からイベントを選択して、[重要度の設定] をクリックします。

  2. [イベント設定の構成] ページで、ドロップダウンリストから必要な重要度レベルを選択します。
  3. また、「抑制」(Suppress) チェックボックスを選択して、イベントを抑制することもできます。詳細オプションを使用して、このイベントを抑制する NetScaler インスタンスを指定することもできます。



4. ［OK］をクリックします。

SDX アプライアンス上の NetScaler インスタンスの Call Home サポート

February 16, 2024

Call Home 機能は、NetScaler インスタンスの一般的なエラー状態を監視します。NetScaler インスタンスの Call Home 機能を Management Service ユーザーインターフェイスから構成、有効化、または無効化できるようになりました。

注：アプライアンスで事前定義されたエラー状態が発生した場合、Call Home がシステムデータをサーバーにアップロードする前に、NetScaler インスタンスを Citrix テクニカルサポートサーバーに登録する必要があります。NetScaler インスタンスで Call Home 機能を有効にすると、登録プロセスが開始されます。

- NetScaler インスタンスでの Call Home の有効化と無効化

  管理サービスから NetScaler インスタンスの Call Home 機能を有効にできます。Call Home 機能を有効にすると、Call Home プロセスは NetScaler インスタンスを Citrix テクニカルサポートサーバーに登録します。登録が完了するまでに時間がかかります。この間、管理サービスは登録の進捗状況を表示します。

  Call Home 機能を有効にするには、[構成**] > [NetScaler] > [Call Home**] に移動し、NetScaler インスタンスを選択して [有効化] ボタンをクリックします。確認ページで [はい] をクリックします。

Call Home 機能を無効にするには、[構成**] > [NetScaler] > [Call Home**] に移動し、NetScaler インスタンスを選択して [無効] ボタンをクリックします。確認ページで [はい] をクリックします。

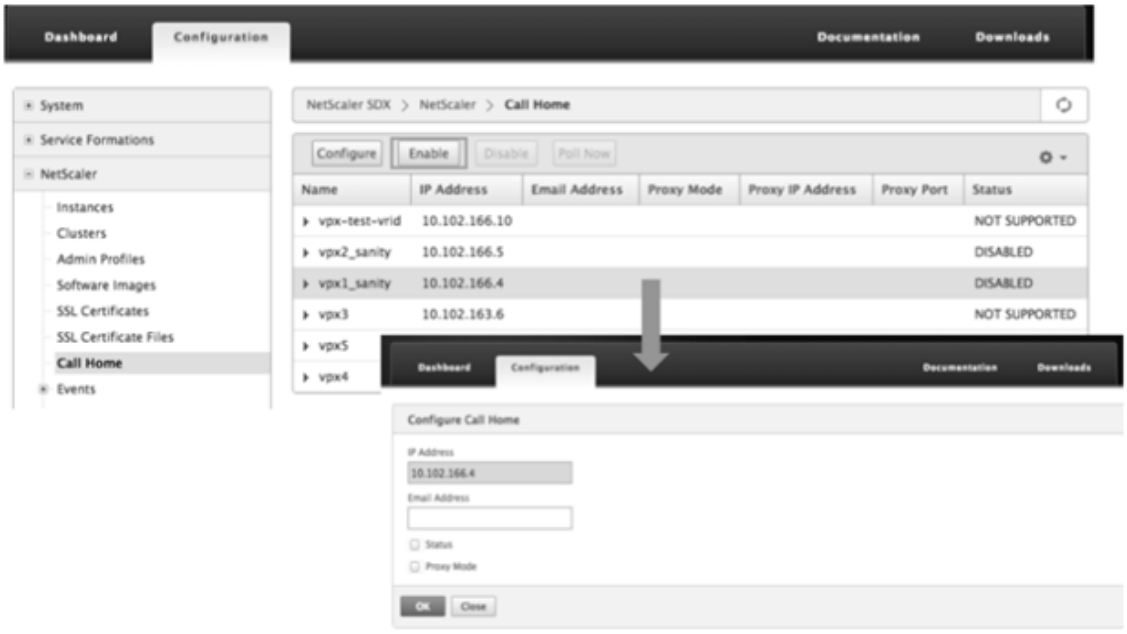
Call Home を有効にすると、次のオプションを設定できます。

1. (オプション) 管理者の電子メールアドレスを指定します。Call Home プロセスは、電子メールアドレスをサポートサーバに送信します。このアドレスは、Call Home に関する今後の対応のために保存されます。
2. (任意) Call Home プロキシモードを有効にします。Call Home は、プロキシサーバーを介して NetScaler インスタンスのデータを Citrix TaaS サーバーにアップロードできます。この機能を使用するには、NetScaler インスタンスでこの機能を有効にし、HTTP プロキシサーバーの IP アドレスとポート番号を指定します。プロキシサーバーから TaaS サーバー (インターネット経由) へのトラフィックはすべて SSL 経由で暗号化されるため、データのセキュリティとプライバシーが侵害されることはありません。

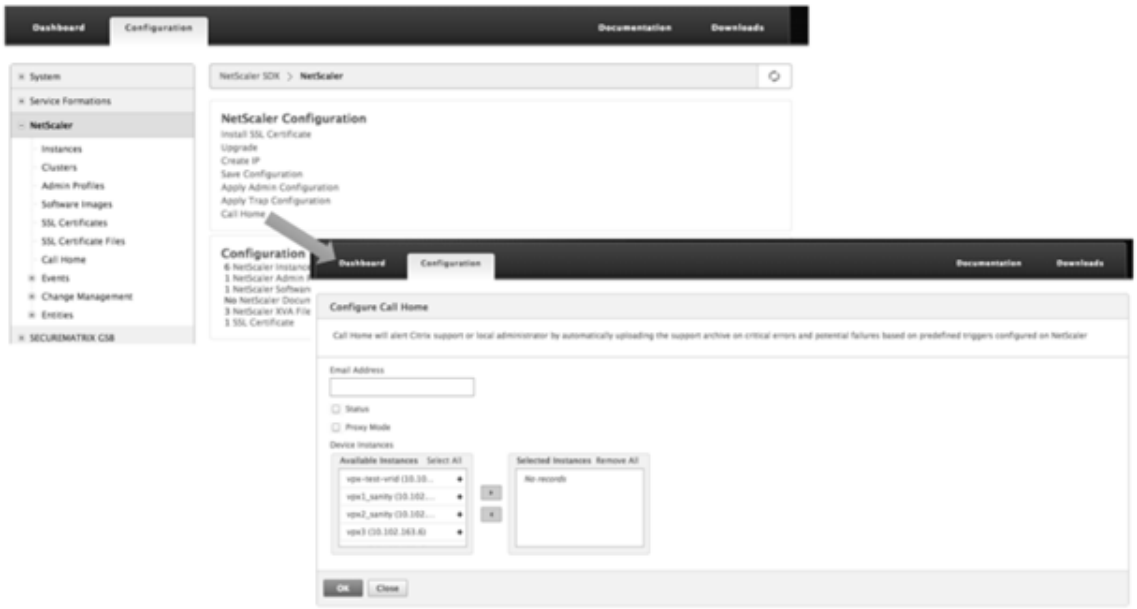
- 管理サービスから NetScaler インスタンスで Call Home を構成するには

  Call Home 機能は、1 つのインスタンスに設定することも、複数のインスタンスに同時に設定することもできます。

  単一の NetScaler インスタンスで Call Home 機能を構成するには、[構成**] > [NetScaler] > [Call Home]** に移動し、**NetScaler** インスタンスを選択して、[構成] ボタンをクリックします。[Call Home の設定] ページで、[OK] をクリックします。



  複数の NetScaler インスタンスで Call Home 機能を構成するには、[** 構成] **[NetScaler] に移動します。右ペインで、[Call Home] をクリックします。「Call Home の構成」ページで、「使用可能なインスタンス」セクションから NetScaler インスタンスを選択し、その他の詳細を指定して、「OK」をクリックします。



– NetScaler インスタンスのポーリング

すべての **NetScaler** インスタンスから **Call Home** 機能をポーリングして現在のステータスを表示するには、**[**** 構成**] > [NetScaler] > [Call Home**] に移動し、[今すぐポーリング] をクリックします。確認ページで **[**** はい] をクリックします。

システムヘルスモニタリング

November 23, 2023

システムヘルスモニタリングでは、監視対象コンポーネントのエラーが検出されるため、障害を回避するための是正措置を講じることができます。NetScaler SDX アプライアンスでは、次のコンポーネントが監視されます。

- ハードウェアとソフトウェアのリソース
- 物理ディスクと仮想ディスク
- < ファン、温度、電圧、電源センサなどのハードウェアセンサ
- インターフェイス

[監視] タブで、[システムヘルス] をクリックします。すべての構成部品のサマリーが表示されます。監視対象コンポーネントの詳細を表示するには、[**System Health**] を展開し、監視するコンポーネントをクリックします。

- SDX アプライアンス上のリソースを監視する

  SDX アプライアンス上のハードウェアおよびソフトウェアコンポーネントを監視し、必要に応じて修正措置を講じることができます。監視対象のコンポーネントを表示するには、[監視] タブで [システムヘルス] を展開し、[リソース] をクリックします。ハードウェアリソースとソフトウェアリソースの詳細が表示されます。す

べてのハードウェアコンポーネントについて、現在の値と期待値が表示されます。BMC ファームウェアのバージョンを除くソフトウェアコンポーネントでは、現在の値と期待値が「該当なし (NA)」と表示されます。

- 名前**:** CPU、メモリ、BMC ファームウェアのバージョンなど、コンポーネントの名前。
- **Status:** コンポーネントの状態 (条件)。
  ハードウェアおよび BMC ファームウェアバージョンの場合、ERROR は予想値からの逸脱を示します。Citrix Hypervisor への呼び出しで、ERROR は、管理サービスが API、HTTP、PING、または SSH 呼び出しを使用して Citrix Hypervisor と通信できないことを示します。ヘルスモニタープラグインの場合
  、ERROR はプラグインが Citrix Hypervisor にインストールされていないことを示します。
- **[**現在の値**]:** コンポーネントの現在の値。通常の状態では、現在の値は期待値と同じです。
- 期待値**:** コンポーネントの期待値。Citrix Hypervisor へのソフトウェアコールには適用されません。

SDX アプライアンス上のストレージリソースを監視する

SDX アプライアンス上のディスクを監視し、必要に応じて修正措置を講じることができます。監視対象のコンポーネントを表示するには、[監視] タブで [システムヘルス] を展開し、[記憶域] をクリックします。物理ディスク、仮想ディスク、または物理ディスクから作成されたパーティションの詳細が表示されます。

ディスク (Disk) の場合、次の詳細が表示されます。

- **[** 名前] 物理ディスクの名前。
- サイズ**:** ディスクのサイズ (GB)。
- **Utilized:** ディスク上のデータ量（GB)。
- トランザクション数**/**秒**:** 1 秒あたりに読み書きされるブロック数。この数値は`iostat`出力から読み込まれます。
- 読み取り回数**/**秒**:** 1 秒あたりに読み取られるブロック数。この値を使用して、ディスクからの出力レートを測定できます。
- 書き込みブロック数**/**秒**:** 1 秒あたりに書き込まれるブロック数。この値を使用して、ディスクへの入力レートを測定できます。
- **Total Blocks Read**：アプライアンスが最後に起動されてから読み取られたブロック数。
- **Total Blocks Writted**：アプライアンスが最後に起動されてから書き込まれたブロック数。

仮想ディスクまたはパーティション (ストレージリポジトリ) の場合、次の詳細が表示されます。

- ドライブベイ**:** ドライブベイ内のドライブの番号。このパラメータでデータをソートできます。
- **Status:** ドライブベイ内のドライブの状態 (状態)。設定可能な値:
  - 良好: ドライブは良好な状態で、使用できる状態です。
  - FAIL: ドライブに障害が発生したため、交換する必要があります。
  - MISSING: ドライブベイにドライブが認識されない。
  - UNKNOWN: ドライブベイに未フォーマットの新しいドライブが存在します。

- **[名前]:** ストレージリポジトリのシステム定義名。
- **Size:** ストレージリポジトリのサイズ (GB 単位)。
- **Utilized:** ストレージリポジトリ内のデータ量（GB)。

SDX アプライアンス上のハードウェアセンサーを監視する

SDX アプライアンス上のハードウェアコンポーネントを監視し、必要に応じて修正措置を講じることができます。[監視] タブで、[システムヘルス] を展開し、[ハードウェアセンサー] をクリックします。監視機能には、さまざまなファンの速度、さまざまなコンポーネントの温度と電圧、および電源の状態に関する詳細が表示されます。

ファン速度については、次の詳細が表示されます。

- 名前**:** ファンの名前。
- **Status:** ファンの状態 (状態)。ERROR は期待値からの偏差を示します。NA はファンがないことを示します。
- 現在の値 **(RPM):** 1 分あたりの現在の回転数。

温度情報には、次の詳細が含まれます。

- 名前**:** CPU やメモリモジュールなどのコンポーネントの名前 (P1-DIMM1A など)。
- **Status:** コンポーネントの状態 (条件)。ERROR は、現在の値が範囲外であることを示します。
- **[**現在の値 **(C)]:** コンポーネントの現在の温度 (度単位)。

電圧情報には、次の詳細が含まれます。

- 名前**:** CPU コアなど、コンポーネントの名前。
- **Status:** コンポーネントの状態 (条件)。ERROR は、現在の値が範囲外であることを示します。
- 電流値 **(**ボルト**):** コンポーネントに存在する電流電圧。

電源装置に関する情報には、次の情報が含まれます。

- 名前**:** コンポーネントの名前。
- **Status:** コンポーネントの状態 (条件)。設定可能な値:
  - エラー:1 つの電源装置だけが接続されているか、動作しています。
  - **OK**: 両方の PSU が接続され、正常に動作しています。

SDX アプライアンス上のインターフェイスを監視する

SDX アプライアンス上のインターフェイスを監視し、必要に応じて修正措置を講じることができます。[監視] タブで [システムヘルス] を展開し、[インターフェイス] をクリックします。モニタリング機能では、各インターフェイスに関する次の情報が詳細に表示されます。

- インターフェイス**:** SDX アプライアンスのインターフェイス番号。
- **Status:** インターフェイスの状態。可能な値:UP、DOWN。

- 割り当てられた **VF** 数**/**合計**:** インターフェイスに割り当てられた仮想機能 (VF) の数と、そのインターフェイスで使用可能な仮想機能の数。プラットフォームが異なれば、サポートする VF の数も異なります。
- **Tx Packets**：アプライアンスが最後に起動されてから送信されたパケット数。
- **Rx Packet:** アプライアンスが最後に起動されてから受信したパケット数。
- **Tx Bytes:** アプライアンスが最後に起動されてから送信されたバイト数。
- **Rx Bytes:** アプライアンスが最後に起動されてから受信したバイト数。
- **Tx Errors:** アプライアンスが最後に起動されてからデータ転送中に発生したエラーの数。
- **Rx Errors:** アプライアンスが最後に起動されてからデータ受信中に発生したエラーの数。

システム通知設定の構成

November 23, 2023

システム関連のさまざまな機能について、選択したユーザーグループと通信するための通知を送信できます。SDX Management Service で通知サーバーを設定して、電子メールおよびショートメッセージサービス (SMS) ゲートウェイサーバーを構成して、電子メールとテキスト (SMS) 通知をユーザーに送信できます。

> 注
>
> SDX Management Service リリース 11.1 にアップグレードすると、すべてのイベントカテゴリに対してシステム通知が有効になり、通知は既存の E メールまたは SMS プロファイルに送信されます。

システム通知設定を構成するには

1. [システム**] > [**通知**] > [**設定**]** に移動し、[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、次の詳細を入力します。
   -カテゴリ-SDX Management Service によって生成されたイベントのカテゴリまたはカテゴリ。
   - 電子メール**-**ドロップダウンメニューから電子メール配布リストを選択します。**+** アイコンをクリックし、該当するフィールドに新しいメールサーバーの詳細を入力して、新しいメール配信リストを作成することもできます。
   - SMS (テキストメッセージ**)**—ドロップダウンメニューから SMS 配信リストを選択します。**+** アイコンをクリックし、
   該当するフィールドに新しい SMS サーバの詳細を入力して、新しい SMS 配布リストを作成することもできます。
3. 「**OK**」をクリックします。

管理サービスの機能を有効または無効にする

November 23, 2023

> 注意:
>
> この機能は、リリース 13.1 ビルド 12.x 以降で使用できます。

NetScaler SDX アプライアンスでは、管理サービスがバックグラウンドで NetScaler インスタンスをポーリングして、SSL 証明書、ネットワーク機能、構成監査などの操作を確認します。要件に応じて、このポーリングを有効または無効にするオプションがあります。このポーリングを無効にすると、管理サービスと ADC インスタンスのパフォーマンスが向上します。

GUI を使用して機能を有効または無効にするには

1. [システム**] > [**システム設定**]** に移動します。
2. [機能の構成] をクリックします。
3. 機能を選択し、[有効] または [****** 無効 ******] をクリックします。

管理サービスを構成する

November 23, 2023

Management Service を使用すると、クライアントセッションを管理し、ユーザーアカウントの作成と管理、要件に応じたバックアップポリシーとプルーニングポリシーの調整などの構成タスクを実行できます。また、管理サービスを再起動して、管理サービスのバージョンをアップグレードすることもできます。さらに、管理サービスと Citrix Hypervisor の tar ファイルを作成し、テクニカルサポートに送信することもできます。

クライアントセッションを管理する

クライアントセッションは、ユーザーが管理サービスにログオンすると作成されます。[Sessions] ペインでは、アプライアンス上のすべてのクライアントセッションを表示できます。

[**Sessions**] ペインでは、次の詳細を表示できます。

- ユーザー名**:** セッションに使用されているユーザーアカウント。
- **IP** アドレス**:** セッションの作成元であるクライアントの IP アドレス。
- **Port:** セッションに使用されているポート。
- ログイン時間： SDX アプライアンスで現在のセッションが作成された時刻。

- 前回のアクティビティ時間**:** セッションでユーザーアクティビティが最後に検出された時刻。
- セッションの有効期限**:** セッションの有効期限が切れるまでの残り時間。

クライアントセッションを表示するには、[構成] タブで [システム**] > [**セッション] に移動します。

クライアントセッションを終了するには、[**Sessions**] ペインで削除するセッションをクリックし、[**End Session**] をクリックします。

セッションを開始したクライアントからセッションを終了することはできません。

ポリシーの構成

記録されたデータのサイズを管理可能な制限内に維持するために、SDX アプライアンスはバックアップポリシーとデータプルーニングポリシーを指定された時刻に自動的に実行します。

プルーニングポリシーは毎日午前 00:00 に実行され、アプライアンスに保持するデータの日数を指定します。デフォルトでは、アプライアンスは 3 日以上経過したデータをプルーニングしますが、保持するデータの日数を指定することもできます。プルーニングされるのは、イベントログ、監査ログ、タスクログだけです。

バックアップポリシーは毎日午前 0 時 30 分に実行され、ログと設定ファイルのバックアップが作成されます。デフォルトでは、このポリシーでは 3 つのバックアップが保持されますが、保持するバックアップの数を指定することもできます。また、バックアップポリシーを使用すると、次のことが可能になります。

- バックアップファイルを暗号化します。
- FTP、SFTP、および SCP を使用してバックアップファイルを外部バックアップサーバに転送するように SDX アプライアンスを設定します。

ログに記録されたデータをプルーニングする日数を指定するには、次の操作を行います。

1. [構成] タブのナビゲーションウィンドウで、[システム] をクリックします。
2. [システム] ペインの [ポリシー管理] で、**[**ポリシーの削除] をクリックします。
3. [プルーニングポリシーの変更] ダイアログボックスの [保持するデータ **(**日数**)**] で、アプライアンスが任意の時点で保持する必要があるデータの日数を指定します。
4. [**OK**] をクリックします。

バックアップポリシーを設定するには、次の手順で行います。

1. [構成] タブのナビゲーションウィンドウで、[システム] をクリックします。
2. [システム] ペインの [ポリシー管理] で、[バックアップポリシー] をクリックします。
3. [バックアップポリシーの変更] ダイアログボックスの [保持する以前のバックアップ] で、アプライアンスが一定時間に保持する必要のあるバックアップの数を指定します。
4. [バックアップファイルを暗号化] を選択して、バックアップファイルを暗号化します。
5. [外部転送] を選択し、次の操作を実行して、バックアップファイルを外部バックアップサーバに転送します。

    a) [**Server**] フィールドに、外部バックアップサーバのホスト名または IP アドレスを入力します。

b) [**User Name**] フィールドと [**Password**] フィールドに、外部バックアップサーバにアクセスするためのユーザ名とパスワードを入力します。
c) [**Port**] フィールドに、ポート番号を入力します。
d) [**Transfer Protocol**] フィールドで、バックアップファイルを外部バックアップサーバに転送するために使用するプロトコルを選択します。
e) [**Directory Path**] フィールドに、バックアップファイルを保存する外部バックアップサーバ内のディレクトリのパスを入力します。

6. 転送後に管理サービスからファイルを削除：バックアップファイルを外部バックアップサーバに転送した後にSDX アプライアンスからバックアップファイルを削除する場合に選択します。
7. [**OK**] をクリックします。

管理サービスの再起動

[システム] ペインから管理サービスを再起動できます。Management Service を再起動しても、インスタンスの動作には影響しません。インスタンスは、Management Service の再起動プロセス中も引き続き機能します。

管理サービスを再起動するには、次の手順で行います。

1. [構成] タブのナビゲーションウィンドウで、[システム] をクリックします。
2. [システム] ウィンドウの [システム管理] で、[管理サービスの再起動] をクリックします。

管理サービスファイルの削除

不要な Management Service ビルドファイルとドキュメントファイルを SDX アプライアンスから削除できます。

管理サービス・ファイルを削除するには、次の手順で行います。

1. [構成] タブのナビゲーションウィンドウで、[管理サービス] を展開し、削除するファイルをクリックします。
2. 詳細ペインでファイル名を選択し、[削除] をクリックします。

テクニカルサポート用に **tar** アーカイブを生成する

[テクニカルサポート] オプションを使用して、Citrix テクニカルサポートに提出するデータと統計情報の tar アーカイブを生成できます。この tar は、管理サービスまたは Citrix Hypervisor、またはその両方に対して同時に生成できます。その後、ファイルをローカルシステムにダウンロードし、Citrix テクニカルサポートに送信できます。

[テクニカルサポート] ウィンドウでは、次の詳細を表示できます。

- 名前**:** tar アーカイブファイルの名前です。ファイル名は、tar が管理サービス用か Citrix Hypervisor サーバー用かを示します。
- 最終更新日**:** このファイルが最後に変更された日付です。

- サイズ**:** tar ファイルのサイズ。

テクニカルサポート用に **tar** アーカイブを生成するには、次の手順を実行します。

1. [構成] タブで、[診断**] > [**テクニカルサポート] に移動します。
2. 詳細ウィンドウの [操作] リストで、[テクニカルサポートファイルの生成] を選択します。
3. [テクニカルサポートファイルを生成] ダイアログボックスの [モード] リストから、適切なオプションを選択します。
4. [**OK**] をクリックします。

テクニカルサポート用に **tar** アーカイブをダウンロードするには、次の手順を実行します。

1. [テクニカルサポート] ウィンドウで、ダウンロードするテクニカルサポートファイルを選択します。
2. [アクション] リストから [ダウンロード] を選択します。ファイルがローカルコンピューターに保存されます。

管理サービスの **CLI** サポート

これで、CLI を使用して管理サービスに対する操作を実行できるようになりました。次の操作がサポートされています。

- [追加]、[設定]、[削除]-リソースを構成します。
- [Do]：システムレベルの操作を実行します。たとえば、管理サービスのアップグレード、シャットダウン、再起動などです。
- [Save]：プロビジョニングに使用されるインターフェイスを追加します。

CLI にアクセスするには、管理サービス IP アドレスに接続された任意のワークステーションから Secure Shell（SSH; セキュアシェル）クライアントを起動します。管理者の資格情報を使用してログオンします。

コマンドの使用法と構文に関する詳細情報には、man ページからアクセスできます。

注**:** CLI はコンソールアクセスではサポートされていません。

認証と承認の設定を構成する

November 23, 2023

NetScaler SDX 管理サービスによる認証は、ローカルでも外部でも可能です。外部認証では、管理サービスは外部サーバーからの応答に基づいてユーザーアクセスを許可します。管理サービスは、次の外部認証プロトコルをサポートしています。

- リモート認証ダイヤルインユーザーサービス (RADIUS)
- ターミナルアクセスコントローラアクセスコントロールシステム (TACACS)
- ライトウェイトディレクトリアクセスプロトコル（LDAP）

管理サービスは SSH からの認証要求もサポートしています。SSH 認証では、キーボード対話型認証要求のみがサポートされます。SSH ユーザの許可は admin 権限のみに制限されます。読み取り専用権限を持つユーザは SSH 経由でログオンできません。

認証を設定するには、認証タイプを指定し、認証サーバを設定します。

管理サービスによる承認はローカルで行われます。管理サービスでは、2 つのレベルの認証がサポートされています。管理者権限を持つユーザは、管理サービスに対してあらゆるアクションを実行できます。読み取り専用権限を持つユーザーは、読み取り操作のみを実行できます。SSH ユーザの許可は admin 権限のみに制限されます。読み取り専用権限を持つユーザは SSH 経由でログオンできません。

RADIUS および LDAP の認可は、グループ抽出によってサポートされています。グループ抽出属性は、管理サービス上の RADIUS または LDAP サーバの設定中に設定できます。抽出されたグループ名は、管理サービス上のグループ名と照合され、ユーザーに付与される権限が決定されます。ユーザーは複数のグループに所属できます。その場合、ユーザーが所属するグループに管理者権限がある場合、そのユーザーには管理者権限が付与されます。デフォルト認証グループ属性は、設定時に設定できます。このグループは、抽出されたグループとともに承認対象として考慮されます。

TACACS 許可では、TACACS サーバ管理者は admin 権限を持つユーザに対して特別なコマンド admin を許可し、読み取り専用権限を持つユーザにはこのコマンドを拒否する必要があります。ユーザーが SDX アプライアンスにログオンすると、Management Service はユーザーがこのコマンドを実行する権限を持っているかどうかを確認します。ユーザに権限がある場合、そのユーザには管理者権限が割り当てられ、それ以外のユーザには読み取り専用権限が割り当てられます。

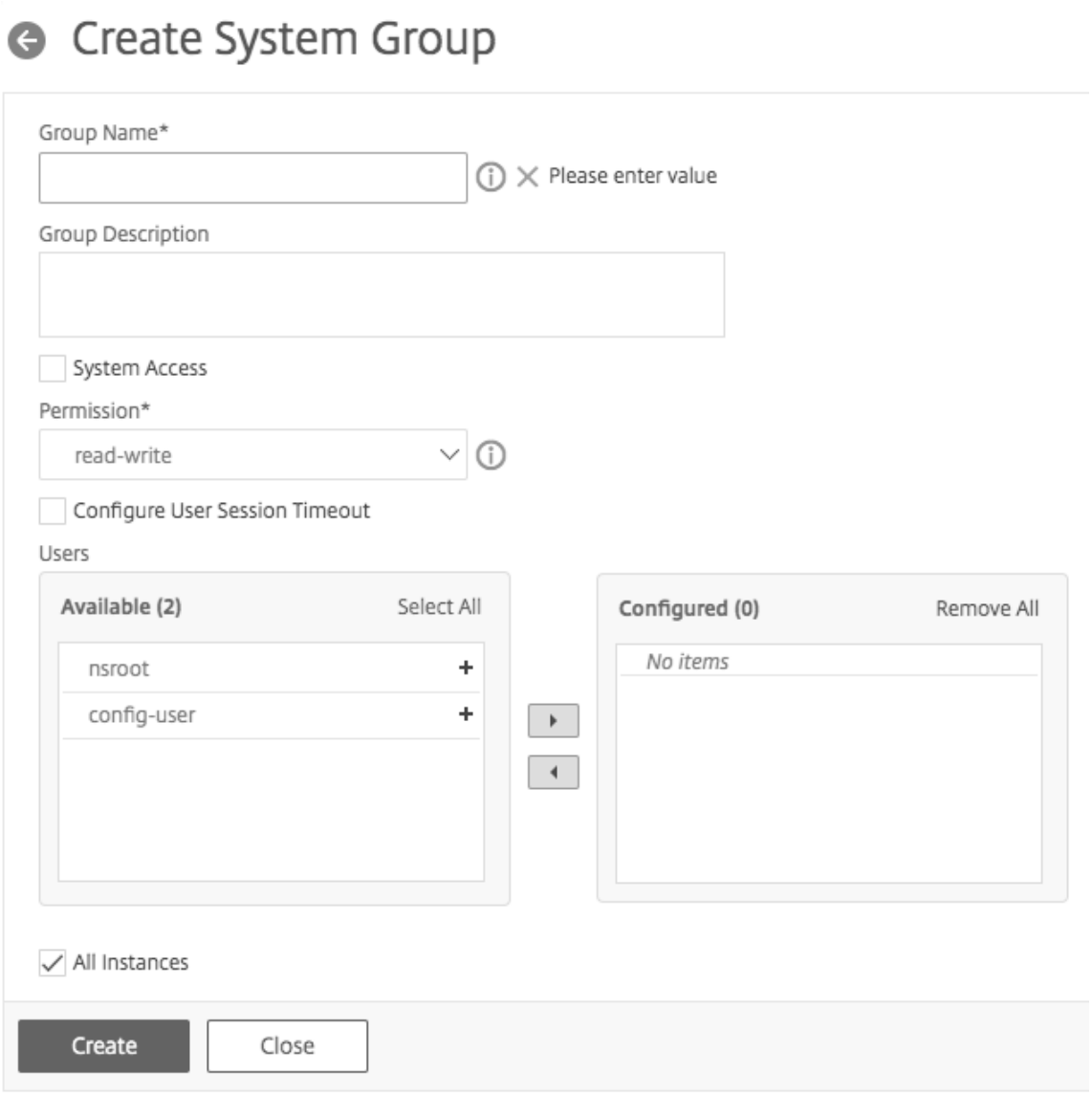
ユーザーグループを追加する

グループは、共通の情報にアクセスしたり、同様の種類のタスクを実行したりする必要のある論理的なユーザーの集合です。ユーザは、一連の一般的な操作によって定義されるグループに編成できます。個々のユーザーではなくグループに特定の権限を付与することで、ユーザーを作成する時間を節約できます。

認証に外部認証サーバーを使用している場合、SDX 内のグループは、認証サーバーで構成されたグループと一致するように構成できます。認証サーバー上のグループと名前が一致するグループに属するユーザーがログオンして認証されると、そのユーザーはそのグループの設定を継承します。

ユーザーグループを追加するには

1. [構成] タブの [システム] で、[ユーザー管理] を展開し、[グループ] をクリックします。
2. 詳細ペインで、[追加] をクリックします。



3. **[**システムグループの作成] ページで、次のパラメータを設定します。

   - グループ名
   - グループ説明

- システムアクセス: このボックスを選択すると、SDX アプライアンス全体と SDX アプライアンスで実行されているインスタンスへのアクセス権が付与されます。または、インスタンスレベルのアクセスでは、**[Instances]** でインスタンスを指定します。

  - 権限
  - ユーザーセッションタイムアウトの設定
  - ユーザ: グループに所属するデータベースユーザ。グループに追加するユーザーを選択します。

1. **[**作成**]** して **[**閉じる**]** をクリックします。

注：バージョン 10.5 からバージョン 11.1 にアップグレードされた SDX アプライアンスに管理者ロールを持つグループを作成するには、[読み取り/書き込み] 権限と [システムアクセス] チェックボックスをオンにします。SDX 10.5 では、このチェックボックスは使用できず、[権限] の値は「admin」と「read-only」になっています。

ユーザーアカウントの構成

ユーザーが SDX アプライアンスにログオンして、アプライアンス管理タスクを実行します。ユーザーがアプライアンスにアクセスできるようにするには、そのユーザーのユーザーアカウントを SDX アプライアンスに作成する必要があります。ユーザーはアプライアンス上でローカルに認証されます。

重要：パスワードは
SDX アプライアンス、管理サービス、および Citrix Hypervisor に適用されます。Citrix Hypervisor で直接パスワードを変更しないでください。

ユーザーアカウントを設定するには

1. [構成] タブの [システム] で、[管理] を展開し、[ユーザー] をクリックします。[Users] ペインには、既存のユーザアカウントとその権限の一覧が表示されます。
2. [**Users**] ペインで、次のいずれかの操作を行います。
   - ユーザアカウントを作成するには、[**Add**] をクリックします。
   - ユーザーアカウントを変更するには、ユーザーを選択し、[**Modify**] をクリックします。
3. [システムユーザの作成] または [システムユーザの変更] ダイアログボックスで、次のパラメータを設定します。
   - [Name*]：アカウントのユーザ名。名前には、a ～z および A ～Z の英字、0 ～9 の数字、ピリオド (.)、スペース、およびアンダースコア (_) を使用できます。最大長:128。この名前は変更できません。
   - [Password*]：アプライアンスにログオンするためのパスワード。最大長:128
   - [パスワードの確認 *]-パスワード。
   - [Permission*]：アプライアンスに対するユーザーの権限。設定可能な値：
     - admin：管理サービスに関連するすべての管理タスクを実行できます。
     - read-only：ユーザはシステムを監視し、アカウントのパスワードを変更することしかできません。デフォルト:admin。
   - [外部認証の有効化]-このユーザの外部認証を有効にします。Management Service は、データベースユーザー認証の前に外部認証を試みます。このパラメータを無効にすると、ユーザは外部認証サーバで認証されません。
     注**:** リモート認証サーバに到達できない場合、ユーザはアプライアンスにアクセスできなくなる可能性があります。このような場合、認証はデフォルトの admin ユーザ (`nsroot`) にフォールバックします。

- [Configure Session Timeout]：ユーザがアクティブなままでいることができる期間を設定できます。次の詳細を指定します。
  - [セッションタイムアウト（Session Timeout）]：ユーザセッションをアクティブにしておくことができる時間
  - [セッションタイムアウト単位]：タイムアウト単位（分または時間）。
- [Groups]：グループをユーザに割り当てます。

* 必須パラメータ

4.「作成」または「OK」をクリックし、「閉じる」をクリックします。作成したユーザーが [Users] ペインに一覧表示されます。

ユーザーアカウントを削除するには

1. [構成] タブのナビゲーションペインで、[システム]、[管理] の順に展開し、[ユーザー] をクリックします。
2. [**Users**] ペインでユーザーアカウントを選択し、[**Delete**] をクリックします。
3.「確認」メッセージ・ボックスで「**OK**」をクリックします。

認証タイプを設定する

Management Service インターフェイスから、ローカル認証または外部認証を指定できます。ローカルユーザーの外部認証はデフォルトで無効になっています。ローカルユーザーを追加するとき、またはユーザーの設定を変更するときに [
外部認証を有効にする] オプションをオンにすることで有効にできます。

重要：外部認証は、RADIUS、LDAP、または TACACS 認証サーバを設定した後にのみサポートされます。

認証タイプを設定するには

1. [構成] タブの [システム] で、[認証] をクリックします。
2. 詳細ウィンドウで、[認証構成] をクリックします。
3. 次のパラメーターを設定します。
   - [Server Type]：ユーザ認証用に設定された認証サーバのタイプ。可能な値:LDAP、RADIUS、TACACS、およびローカル。
   - [Server Name]：管理サービスで構成された認証サーバの名前。このメニューには、選択した認証タイプに対して構成されたすべてのサーバが一覧表示されます。
   - フォールバックローカル認証の有効化：外部認証が失敗した場合に、ローカル認証でユーザを認証するように選択することもできます。このオプションは、デフォルトで有効になっています。
4. [OK] をクリックします。

基本認証を有効または無効にする

基本認証を使用して、管理サービスの NITRO インターフェイスに対して認証できます。デフォルトでは、SDX アプライアンスでは基本認証が有効になっています。管理サービスインターフェイスを使用して基本認証を無効にするには、次の手順を実行します。

ベーシック認証を無効にするには

1. [構成] タブで [システム] をクリックします。
2. [システム設定**]** グループで、[システム設定の変更] をクリックします。
3. [システム設定の構成] ダイアログボックスで、[基本認証を許可する] チェックボックスをオフにします。
4. [**OK**] をクリックします。

外部認証サーバの設定

November 23, 2023

NetScaler SDX Management Service は、ローカルユーザーアカウントまたは外部認証サーバーを使用してユーザーを認証できます。アプライアンスでは、次の認証タイプがサポートされています。

- [Local]：外部認証サーバを参照せずに、パスワードを使用して管理サービスに対して認証します。ユーザーデータは管理サービスにローカルに保存されます。
- RADIUS：外部 RADIUS 認証サーバに対して認証します。
- [LDAP]：外部 LDAP 認証サーバに対して認証します。
- TACACS：外部ターミナルアクセスコントローラアクセスコントロールシステム（TACACS）認証サーバに対して認証します。

外部認証を設定するには、認証タイプを指定し、認証サーバを設定します。

RADIUS サーバの追加

RADIUS 認証を設定するには、認証タイプを RADIUS として指定し、RADIUS 認証サーバを設定します。

管理サービスは、RADIUS 仕様に従って RADIUS チャレンジレスポンス認証をサポートします。RADIUS ユーザは、RADIUS サーバ上でワンタイムパスワードを使用して設定できます。ユーザーが SDX アプライアンスにログオンすると、このワンタイムパスワードを指定するよう求められます。

RADIUS サーバを追加するには

1. [構成] タブの [システム] で、[認証] を展開し、[**Radius**] をクリックします。
2. 詳細ペインで、[追加] をクリックします。
3. [**Radius** サーバーの作成] ダイアログボックスで、パラメーターの値を入力または選択します。

    - [Name*]：サーバの名前。
    - サーバ名/ IP アドレス *-完全修飾ドメイン名 (FQDN) またはサーバ IP アドレス。
      注:DNS は、指定された FQDN を IP アドレスに解決できる必要があり、FQDN の解決にはプライマリ DNS のみが使用されます。プライマリ DNS を手動で設定するには、「FQDN 名前解決用のプライマリ DNS の追加」の項を参照してください。
    - ** ポート *：RADIUS サーバが稼働しているポート。デフォルト値は 1812 です。
    - Timeout*：システムが RADIUS サーバからの応答を待機する秒数。デフォルト値:3。
    - [Secret Key*]：クライアントとサーバ間で共有されるキー。この情報は、システムと RADIUS サーバ間の通信に必要です。
    - NAS IP アドレス抽出の有効化：有効にすると、管理サービス IP アドレスが RADIUS プロトコルに従って`nasip`としてサーバに送信されます。
    - nasid：設定されている場合、このストリングは RADIUS プロトコルに従って`nasid`として RADIUS サーバに送信されます。
    - [Group Prefix]：RADIUS グループ抽出用の RADIUS 属性内でグループ名の前に付けるプレフィ
    - [グループベンダー ID]：RADIUS グループ抽出を使用するベンダー ID。
    - [グループ属性タイプ]：RADIUS グループ抽出用の属性タイプ。
    - [Group Separator]：RADIUS グループ抽出用の RADIUS 属性内のグループ名を区切るグループ区切り文字列。
    - IP アドレスベンダー ID：イントラネット IP を示す RADIUS 内の属性のベンダー ID。値 0 は、属性がベンダーエンコードされていないことを示します。
    - IP アドレス属性タイプ：RADIUS 応答内のリモート IP アドレス属性の属性タイプ。
    - パスワードベンダー ID：RADIUS 応答に含まれるパスワードのベンダー ID。ユーザーパスワードの抽出に使用されます。
    - パスワード属性タイプ：RADIUS 応答に含まれるパスワード属性の属性タイプ。
    - [Password Encoding]：システムから RADIUS サーバに送信される RADIUS パケットでパスワードをエンコードする方法。指定可能な値: パップ、チャップ、mschapv1、および mschapv2。
    - [Default Authentication Group]：抽出されたグループに加えて、認証が成功した場合に選択されるデフォルトグループ。
    - アカウンティング：管理サービスが RADIUS サーバで監査情報を記録できるようにします。

4. [作成] をクリックし、[閉じる] をクリックします。

LDAP 認証サーバの追加

LDAP 認証を設定するには、認証タイプを LDAP として指定し、LDAP 認証サーバを設定します。

LDAP サーバを追加するには

1. [構成] タブの [システム] で、[認証] を展開し、[**LDAP**] をクリックします。
2. 詳細ペインで、[追加] をクリックします。
3. [LDAP サーバの作成] ダイアログボックスで、パラメータの値を入力または選択します。

    - [Name*]：サーバの名前。
    - サーバ名/ IP アドレス *：FQDN またはサーバ IP アドレス。
      注:DNS は、指定された FQDN を IP アドレスに解決できる必要があり、FQDN の解決にはプライマリ DNS のみが使用されます。プライマリ DNS を手動で設定するには、「FQDN 名前解決用のプライマリ DNS の追加」の項を参照してください。
    - **Port*** —LDAP サーバーが稼働しているポート。デフォルト値:389。
    - Timeout*：システムが LDAP サーバからの応答を待機する秒数。
    - [Base DN]：LDAP 検索を開始する必要があるベース、またはノード。
    - [Type]：LDAP サーバのタイプ。有効な値は、Active Directory (AD) と Novell ディレクトリサービス (NDS) です。
    - 管理バインド DN：LDAP サーバにバインドするために使用される完全識別名。
    - 管理パスワード：LDAP サーバにバインドするために使用するパスワード。
    - [LDAP 証明書の検証]：LDAP サーバから受信した証明書を検証するには、このオプションをオンにします。
    - LDAP ホスト名：LDAP サーバのホスト名。validateServerCert パラメーターが有効な場合、このパラメーターは LDAP サーバーからの証明書のホスト名を指定します。ホスト名が一致しないと、接続に失敗します。
    - サーバログオン名属性：外部 LDAP サーバまたは Active Directory を照会するためにシステムによって使用される名前属性。
    - [Search Filter]：デフォルトの LDAP ユーザ検索文字列と組み合わせて値を形成する文字列。たとえば、vpnallowed=true に ldaploginame `samaccount` を指定し、ユーザーが指定したユーザー名 bob を指定すると、LDAP 検索文字列 (& (vpnallowed=true) (samaccount=bob) が返されます。
    - [Group Attribute]：LDAP サーバからグループを抽出するための属性名。
    - [サブ属性名]-LDAP サーバからグループを抽出するためのサブ属性名。
    - [Security Type]：アプライアンスと認証サーバ間の通信に使用される暗号化のタイプ。設定可能な値:
      PLAINTEXT: 暗号化は不要です。
      TLS: TLS プロトコルを使用して通信します。
      SSL: SSL プロトコルを使用した通信
    - [Default Authentication Group]：抽出されたグループに加えて、認証が成功した場合に選択されるデフォルトグループ。

- [Referrals]：LDAP サーバから受信した LDAP 紹介のフォローを有効にします。
- [最大 LDAP リフェラル]：フォローする LDAP リフェラルの最大数。
- [パスワード変更の有効化（Enable Change Password）]：パスワードの有効期限が切れた場合に、ユーザがパスワードパスワードを変更できるのは、[セキュリティタイプ] が [TLS] または [SSL] に設定されている場合のみです。
- ネストされたグループの抽出を有効にする-ネストされたグループの抽出機能を有効にします。
- [最大ネストレベル]-グループを抽出できるレベルの数。
- グループ名識別子：LDAP サーバ内のグループを一意に識別する名前。
- グループサーチ属性：LDAP グループサーチ属性。グループがどのグループに属しているかを判断するのに使用されます。
- グループ検索サブ属性：LDAP グループ検索サブ属性。グループがどのグループに属しているかを判断するのに使用されます。
- [Group Search Filter]：デフォルトの LDAP グループ検索文字列と組み合わせて検索値を構成する文字列。

4. ［Create］をクリックしてから、［Close］をクリックします。

LDAP ユーザに対する **SSH** 公開キー認証のサポート

SDX アプライアンスは、ログオン用の SSH 公開キー認証によって LDAP ユーザーを認証できるようになりました。公開鍵のリストは、LDAP サーバーのユーザーオブジェクトに保存されます。認証中、SSH は LDAP サーバから SSH 公開鍵を抽出します。取得した公開鍵のいずれかが SSH をサポートしていれば、ログオンは成功します。

抽出された公開鍵の同じ属性名が、LDAP サーバーと NetScaler SDX アプライアンスの両方に存在する必要があります。

> 重要
>
> 鍵ベースの認証では、以下の点で、/etc/sshd_configファイル内のAuthorizedkeysfileの値を設定して、公開鍵の場所を指定する必要があります。
>
> ```
> AuthorizedKeysFile .ssh/authorized_keys
> ```

システムユーザー。/etc/sshd_config*‘ファイルにAuthorizedkeysfileの値を設定することで、任意のシステムユーザの公開鍵の場所を指定できます。

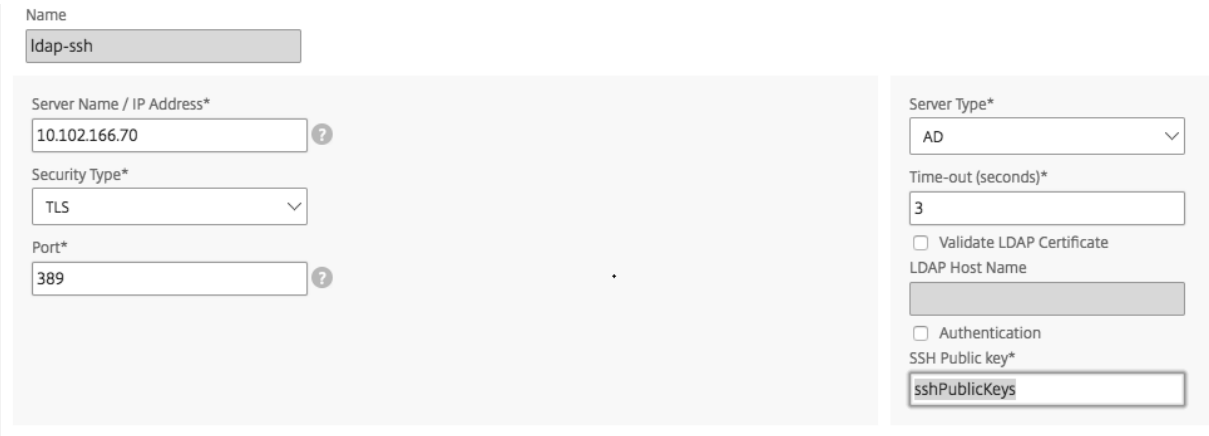
LDAP ユーザ。取得した公開鍵は/var/pubkey/<user_name>/tmp_authorized_keys-<pid>ディレクトリに保存されます。pidは、同じユーザからの同時 SSH 要求を区別するために追加される一意の番号です。この場所は、認証プロセス中に公開鍵を保持するための一時的な場所です。認証が完了すると、公開鍵はシステムから削除されます。

ユーザでログインするには、シェルプロンプトから次のコマンドを実行します。


```
$ ssh -i <private key> <username>@<IPAddress>
```

GUI を使用して **LDAP** サーバを設定するには、次の手順を実行します。

1. [**System**] > [**Authentication**] > [**LDAP**] の順に選択します。
2. [LDAP] ページで、[****** サーバー **] タブをクリックします。
3. 使用可能な LDAP サーバのいずれかをクリックします。
4. [認証 **LDAP** サーバの構成] ページで、[認証] を選択します。



> 注:
>
> LDAP ユーザーの認証に「sshPublicKeys」を使用するには、「認証」チェックボックスをオフにします。

FQDN 名前解決のためのプライマリ **DNS** の追加

IP アドレスの代わりにサーバの FQDN を使用して RADIUS または LDAP サーバを定義する場合は、プライマリ DNS を手動で設定してサーバ名を解決します。GUI または CLI のいずれかを使用できます。

GUI を使用してプライマリ DNS を設定するには、[システム] **> [**ネットワーク構成**] > [DNS]** の順に移動します。

CLI を使用してプライマリ DNS を設定するには、次の手順に従います。

1. セキュアシェル (SSH) コンソールを開きます。
2. 管理者の資格情報を使用して NetScaler SDX アプライアンスにログオンします。
3. `networkconfig`コマンドを実行します。
4. 適切なメニューを選択して DNS IPv4 アドレスを更新し、変更を保存します。

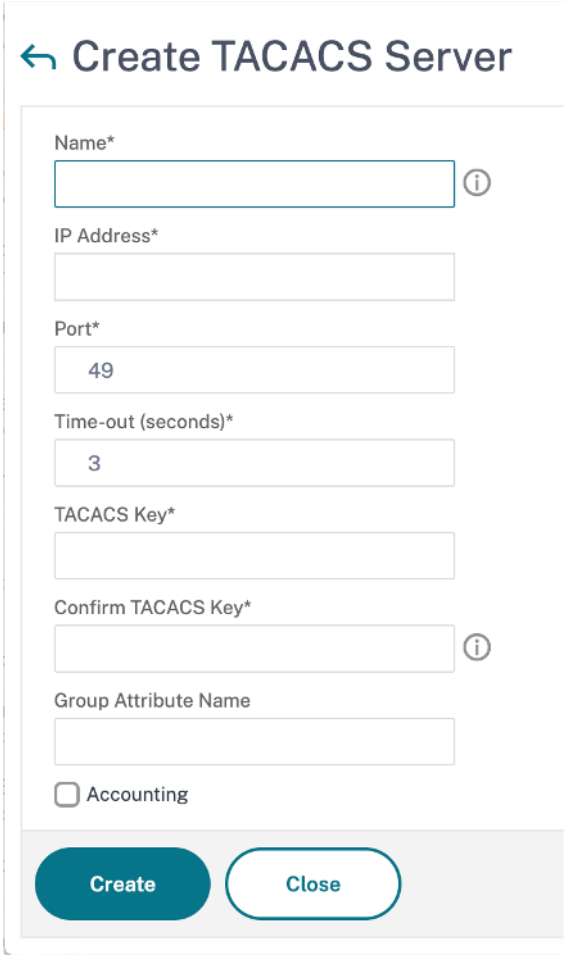
`networkconfig`コマンドをもう一度実行すると、更新された DNS アドレスが表示されます。

TACACS サーバの追加

TACACS 認証を設定するには、認証タイプを TACACS として指定し、TACACS 認証サーバを設定します。

TACACS サーバを追加するには

1. [構成] タブの [システム] で、[認証] を展開し、[**TACACS**] をクリックします。
2. 詳細ペインで、[追加] をクリックします。
3. [Create TACACS Server] ダイアログボックスで、パラメータの値を入力または選択します。
   - [Name]: TACAS サーバの名前
   - IP アドレス: TACACS サーバの IP アドレス
   - [Port]: TACACS サーバが稼働しているポート。デフォルト値:49
   - Timeout: システムが TACACS サーバからの応答を待機する最大秒数。
   - TACACS Key: クライアントとサーバ間で共有されるキー。この情報は、システムが TACACS サーバと通信するために必要です。
   - アカウンティング: 管理サービスが TACACAS サーバに監査情報を記録できるようにします。
   - グループ属性名: TACACS+ サーバに設定されているグループ属性の名前



4. [作成] をクリックし、[閉じる] をクリックします。

管理サービスからリンクアグリゲーションを構成する

November 23, 2023

リンクアグリゲーションは、複数のイーサネットリンクを 1 つの高速リンクに統合します。リンクアグリゲーションを構成すると、NetScaler SDX アプライアンスと他の接続デバイス間の通信チャネルの容量と可用性が向上します。集約されたリンクは「チャネル」とも呼ばれます。

ネットワークインターフェイスをチャネルにバインドした場合、チャネルのパラメーターは、ネットワークインターフェイスのパラメーターよりも優先されます。(つまり、ネットワークインターフェイスパラメータは無視されます)。ネットワークインターフェイスは 1 つのチャネルにのみバインドできます。

ネットワークインターフェイスがチャネルにバインドされると、その VLAN 設定は破棄されます。インターフェイスは元々属していた VLAN から削除され、デフォルト VLAN に追加されます。ただし、チャネルを元の VLAN や新しい VLAN にバインドすることができます。たとえば、ネットワークインターフェイス 1/2 と 1/3 を ID 2 の VLAN (VLAN 2）にバインドし、チャネル LA/1 にバインドすると、ネットワークインターフェイスはデフォルト VLAN に移動されますが、チャネルを VLAN 2 にバインドできます。

注:

- インターフェイスは 1 つのチャネルにのみ属している必要があります。
- チャネルを設定するには、最低 2 つのインターフェイスが必要です。
- NetScaler インスタンスを追加または変更しても、チャネルの一部を形成するインターフェイスはネットワーク設定ビューに表示されません。インターフェイスの代わりに、チャネルが一覧表示されます。

1 つのインスタンスに割り当てられた 3 つのインターフェイスを使用してチャネルを設定し、2 番目のインスタンスがこれらのインターフェイスの一部を使用する場合、Management Service は 2 番目のインスタンスをシャットダウンし、ネットワーク設定を変更して、インスタンスを再起動します。たとえば、Instance1 と Instance2 の 2 つのインスタンスがあるとします。これらのインスタンスがプロビジョニングされると、インターフェイス 10/1、10/2、10/3 が Instance1 に割り当てられ、インターフェイス 10/1 と 10/2 が Instance2 に割り当てられます。インターフェイス 10/1、10/2、および 10/3 で LA チャネルが作成された場合、instance1 は再起動されません。ただし、管理サービスは Instance2 をシャットダウンし、インターフェイス 10/3 を Instance2 に割り当て、Instance2 を再起動します。

LA チャネルからインターフェイスを削除すると、その変更はデータベースに保存され、インスタンスの追加または変更時に [Network Settings] ビューにインターフェイスが表示されます。インターフェイスを削除する前は、そのインターフェイスが属するチャネルだけが一覧表示されます。

管理サービスからチャネルを設定する

November 23, 2023

チャネルは手動で設定することも、リンクアグリゲーション制御プロトコル (LACP) を使用することもできます。LACP を手動で設定したチャネルに適用したり、LACP によって作成されたチャネルを手動で設定したりすることはできません。管理サービスからチャネルを構成します。次に、NetScaler インスタンスのプロビジョニングまたは変更時にチャネルを選択します。

LA チャネルは、リンクの冗長性と帯域幅集約を実現する論理エンティティです。チャネルの一部であるインターフェイスに個別の IP アドレスを割り当てることはできません。

注： NetScaler SDX アプライアンスはリンクアグリゲーションをサポートしていますが、リンク冗長性はサポートしていません。NetScaler リリース 13.1 ビルド 27.x 以降以降、NetScaler SDX アプライアンスでホストされている NetScaler VPX インスタンスでは、リンク冗長構成は明示的にサポートされていません。

管理サービスからチャンネルを構成するには

1. [システム**] > [**チャンネル] に移動します。
2. 詳細ペインで、[追加] をクリックします。
3.「チャンネルを追加 **(Add Channel**)」ダイアログボックスで、次のパラメータを設定します。
    - チャネル ID：作成する LA チャネルの ID。LA チャネルを LA/X 表記で指定します。x の範囲は 1 からインターフェイス数の 2 分の 1 に等しい数です。LA チャネルが作成された後は変更できません。
    - [Type]：チャネルのタイプ。設定可能な値：
        - static：データインターフェイス上でのみ設定されます。
        - active-active：管理インターフェイス 0/x だけで設定されます。
        - active-passive：管理インターフェイス 0/x だけで設定されます。
        - LACP：データインターフェイスと管理インターフェイス 0/x に設定されます。
    - スループット（スタティックチャネルと LACP だけに適用）：LA チャネルのスループットの低しきい値（Mbps 単位）。HA 設定では、LA チャネルで HA MON が有効になっていて、スループットが指定されたしきい値を下回ると、フェールオーバーがトリガーされます。
    - [Bandwidth High]（スタティックチャネルおよび LACP だけに適用）：LA チャネルの帯域幅使用量に対する上限しきい値（Mbps 単位）。LA チャネルの帯域幅使用量が指定された上限しきい値以上になると、アプライアンスは SNMP トラップメッセージを生成します。
    - [Bandwidth Normal]（スタティックチャネルおよび LACP だけに適用）：LA チャネルの帯域幅使用量の標準しきい値（Mbps 単位）。LA チャネルの帯域幅使用量が上限しきい値を超えた後、指定された標準しきい値以下になると、NetScaler SDX アプライアンスは帯域幅使用量が正常に戻ったことを示す SNMP トラップメッセージを生成します。
4. [**Interfaces**] タブで、このチャネルに含めるインターフェイスを追加します。
5. [設定] タブで、次のパラメータを設定します。
    - [Channel State]（スタティックチャネルにのみ適用）：LA チャネルを有効または無効にします。
    - [LACP Time]（LACP にのみ適用）：リンクが LACPDU を受信しない場合に、リンクが集約されなくなるまでの時間。この値は、SDX アプライアンスとパートナーノードのリンクアグリゲーションに参加しているすべてのポートで一致する必要があります。

- HA モニタリング：High Availability（HA; 高可用性）設定では、チャネルに障害イベントがないか HA MON が有効になっている LA チャネルに障害が発生すると、HA フェールオーバーがトリガー
- [Tag All]：このチャネルで送信されるすべてのパケットに 4 バイトの 802.1q タグを追加します。ON 設定では、このチャネルにバインドされているすべての VLAN にタグが適用されます。OFF は、ネイティブ VLAN 以外のすべての VLAN にタグを適用します。
- [Alias Name]：LA チャネルのエイリアス名。読みやすさを向上させるためにのみ使用します。操作を実行するには、LA チャネル ID を指定する必要があります。

6. [作成] をクリックし、[閉じる] をクリックします。

> メモ
>
> - 0/1 と 0/2 の両方のインターフェイスが VPX インスタンスの一部であり、そのインスタンスがクラスタの一部である場合は、管理 LA を作成できません。
> - 管理 LA が VPX インスタンスの一部であり、そのインスタンスがクラスタの一部である場合、管理 LA は削除できません。

アクセス制御リスト

February 16, 2024

Access Control List（ACL; アクセスコントロールリスト）は、IP トラフィックをフィルタリングし、アプライアンスを不正アクセスから保護するためにネットワークアプライアンスに適用できる一連の条件です。

NetScaler SDX 管理サービス GUI で ACL を構成して、アプライアンスへのアクセスを制限および制御できます。

> 注:
>
> SDX アプライアンスの ACL は、リリース 12.0 57.19 以降でサポートされています。

このセクションでは、以下のトピックについて説明します：

- 使用ガイドライン
- ACL の設定方法
- ACL ルールに対するその他のアクション
- トラブルシューティング

使用ガイドライン

アプライアンスで ACL を作成する際は、次の点に注意してください。

- SDX アプライアンスをリリース 11.0 57.19 にアップグレードすると、ACL 機能はデフォルトで無効になります。

- SDX 管理者は、SDX アプライアンスの ACL を通じてインバウンドパケットのみを制御できます。
- NetScaler Application Delivery Management を使用して SDX アプライアンスを管理する場合、MAS と SDX 管理サービス間の通信を許可する適切な ACL ルールを作成する必要があります。
- VPX のプロビジョニングや削除、外部サーバーの追加/削除、SNMP 管理など、SDX アプライアンスのその他の構成では、既存の ACL 設定を変更する必要はありません。これらの事業体とのコミュニケーションは、管理サービスによって行われます。

ACL の設定方法

ACL の設定には、次の手順が含まれます。

- ACL 機能を有効にする
- ACL ルールを作成する
- ACL ルールを有効にする

> 注:
>
> ACL 機能を有効にしなくても ACL ルールを作成できます。ただし、この機能が有効になっていない場合、ACL ルールを作成した後に ACL ルールを有効にすることはできません。

ACL 機能を有効にする

1. ACL 機能を有効にするには、SDX 管理サービス GUI にログオンし、[構成] > [システム**] > [ACL**] の順に移動します。
2. 切り替えボタンを使用して ACL 機能をオンにします。

ACL ルールを作成する

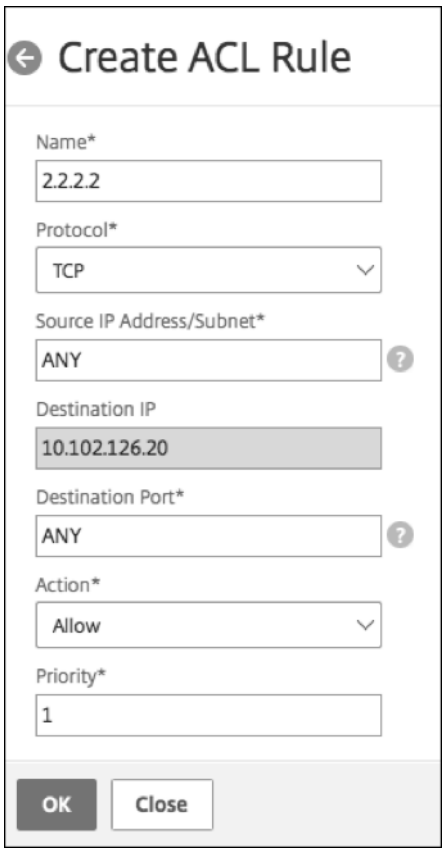
1. [ACL] ページで、[ルールの作成] をクリックします。
2.「規則の作成」ウィンドウが開きます。次の表に示す詳細を追加します。

プロパティ	説明
名前	名前を追加してください。

プロパティ	説明
プロトコル	メニューからプロトコルを選択します。既定では、[TCP] が選択されています。**[ANY]** を選択すると、すべてのプロトコルを許可できます。
送信元 IP アドレス/サブネット	ルールを適用する送信元 IP アドレスまたは送信元サブネットを指定します。ルールをすべての着信トラフィックに適用する必要がある場合は、[**ANY**] を選択します。
接続先 IP	SDX 管理サービス IP アドレスは、宛先 IP として自動入力されます。このフィールドは編集できません。
Destination port	ルールを適用する宛先ポートを指定します。ルールがすべての宛先ポートに適用される場合は、[**ANY**] を選択します。
アクション	ルールに対するアクション ([許可] または [拒否]) を選択します。
優先度	優先度を割り当てて、ルールが評価される順序を指定します。プライオリティ番号によって、ACL ルールが着信パケットと照合される順序が決まります。プライオリティ番号が小さいほどプライオリティが高くなります。たとえば、プライオリティ番号 1 はプライオリティ番号 1 よりもプライオリティが高くなります。どのルールも着信パケットと一致しない場合、そのパケットはブロックされます。

3.「**OK**」をクリックしてルールを作成します。

図: ACL ルールの例



ルールが作成されると、そのルールは無効状態になります。ルールを有効にするには、ルールを有効にする必要があります。

> 注:
>
> ルールを有効にするには、ACL 機能を有効にする必要があります。この機能が無効で ACL ルールを有効にしようとすると、「ACL is not running」というメッセージが表示されます。

ACL ルールを有効にする

1. 有効にするルールの上にマウスポインターを置き、3 つのドットが付いた円をクリックします。
2. メニューから [有効] を選択します。
3. または、その規則のラジオボタンを選択し、[**Enable**] タブをクリックします。
4. プロンプトが表示されたら、[はい] をクリックして確定します。

ACL ルールに対するその他のアクション

ACL ルールには次のアクションを適用できます。

1. ACL ルールを無効にする

2. ACL ルールを編集する
3. ACL ルールを削除する
4. ACL ルールのプライオリティを再番号付けする

ACL ルールを無効にする

1. 無効にするルールの上にマウスポインターを置き、3 つのドットが付いた円を選択します。
2. リストから [無効] をクリックします。
3. または、その規則のラジオボタンを選択し、[**Disable**] タブをクリックします。
4. [はい] をクリックして確定します。

> 注:
>
> ルールを無効にすると、そのルールは着信トラフィックに適用されなくなります。ただし、ルール設定は ACL 設定の下に残ります。

ACL ルールを編集する

1. 編集するルールの上にマウスポインターを置き、3 つのドットが付いた円を選択します。
2. リストから [ルールを編集] をクリックします。**[**規則の変更] ウィンドウが開きます。
3. または、その規則のラジオボタンを選択し、[**Edit Rule**] タブをクリックします。「規則の変更」ウィンドウが開きます。
4. 編集を行い、「**OK**」をクリックします。

> 注:
>
> ルールは、有効状態と無効状態の両方で編集できます。すでに有効になっているルールを編集すると、編集内容がただちに適用されます。無効な状態のルールでは、ルールを有効にすると編集内容が適用されます。

ACL ルールを削除する

1. ルールが無効状態であることを確認します。
2. 削除するルールの上にマウスポインターを置き、3 つのドットが付いた円を選択します。リストから [ルールを削除] をクリックします。
3. または、その規則のラジオボタンを選択し、[**Delete Rule**] タブをクリックします。
4. [はい] をクリックして確定します。

> 注:
>
> 有効状態のルールは削除できません。

ACL ルールのプライオリティの再番号付け

1. 優先順位を再番号付けするルールの上にマウスポインターを置き、3 つのドットが付いた円を選択します。リストから **[**優先度の再番号付け] をクリックします。
2. または、その規則のラジオボタンを選択し、[**Select Action**] タブをクリックします。
3. [優先順位の再番号付け] を選択します。
4. SDX Management Service は、既存のすべてのルールに 10 の倍数になる新しい優先度番号を自動的に割り当てます。
5. ルールを編集して、要件に応じて優先度番号を割り当てます。ルールを編集する方法の詳細については、「ACL ルールを編集するには」section を参照してください。

図。既存の優先度番号の例

	Priority ↑	Name	Source IP Address/Subnet
☐	1	2.2.2.2	ANY
☐	2	test1	1.1.1.1
☐	3	test2	ANY

図。優先順位番号が付け直された後の優先順位番号を 10 の倍数で表した例

	Priority ↑	Name	Source IP Address/Subnet
☐	10	2.2.2.2	ANY
☐	20	test1	1.1.1.1
☐	30	test2	ANY

トラブルシューティング

ACL ルールが正しく設定されていないと、すべてのユーザアカウントがアクセスを拒否される可能性があります。ACL の設定が不適切なために SDX Management Service へのすべてのネットワークアクセスが誤って失われた場合は、次の手順に従ってアクセスを取得してください。

1. SSH と「ルート」アカウントを使用して、Citrix Hypervisor の管理 IP アドレスにログオンします。

2. 管理者権限を使用して、管理サービス VM のコンソールにログオンします。
3. コマンド`pfctl -d`を実行します。
4. GUI を使用して管理サービスにログオンし、それに応じて ACL を再設定します。

NetScaler インスタンスのクラスターをセットアップする

November 23, 2023

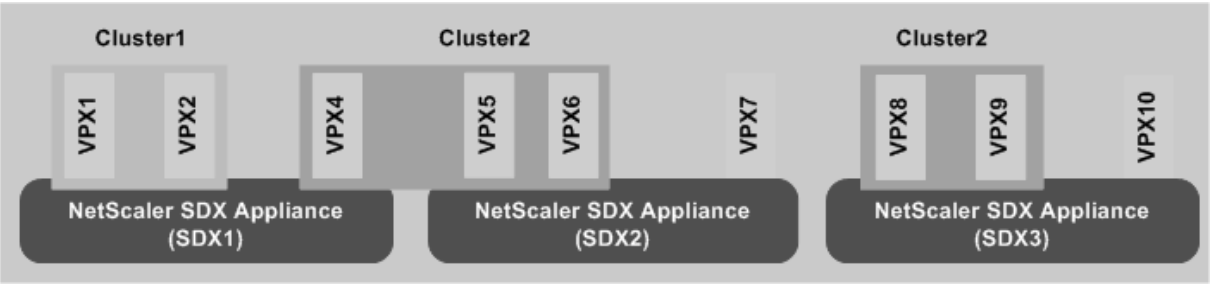
1 つ以上の SDX アプライアンスに NetScaler インスタンスをプロビジョニングすると、NetScaler インスタンスのクラスターを作成できます。

Citrix では、管理サービスからクラスター構成を実行することをお勧めします。VPX インスタンスからクラスター構成を実行すると、管理サービスは 30 分ごとに自動検出中に構成について学習します。最悪の場合、クラスタリング情報は 30 分間検出されません。クラスターは正常に動作するかもしれませんが、クラスターの依存関係に関する必須の検証チェックの一部が欠落しています。Management Service は、ADC インスタンスでクラスタを構成する前に、これらのチェックを実行します。したがって、クラスタ構成はすべて管理サービスから実行する必要があります。

注:

- クラスターをセットアップするには、NetScaler クラスタリングを理解している必要があります。詳細については、「クラスタリング」を参照してください。
- 複数の SDX アプライアンスに NetScaler インスタンスを持つクラスターでは、3 つの SDX アプライアンスの NetScaler インスタンスを使用することをお勧めします。このプロセスにより、最小 (n/2 +1) ノードのクラスタ基準が常に満たされるようになります。

図 1: SDX NetScaler インスタンスのクラスター



上の図は、同じサブネット上にある 3 つの SDX アプライアンス、SDX1、SDX2、SDX3 を示しています。これらのアプライアンス上の NetScaler インスタンスは、Cluster1 と Cluster2 の 2 つのクラスターを形成するために使用されます。

- Cluster1 には SDX1 に 2 つのインスタンスが含まれています。
- Cluster2 には、SDX1 に 1 つのインスタンス、SDX2 に 2 つのインスタンス、SDX3 に別の 2 つのインスタンスが含まれます。

確認事項

- Mellanox インターフェイス (50G および 100G) を使用した CLAG 形成は、SDX プラットフォームではサポートされていません。
- クラスターのノードはすべて同じタイプである必要があります。次の組み合わせではクラスタを形成できません。
  - ハードウェアおよび仮想アプライアンス。
  - NetScaler VPX インスタンスと NetScaler SDX インスタンス。
  - 異なる SDX ハードウェアプラットフォーム上の ADC インスタンス。
- NetScaler インスタンスは同じバージョンでなければならず、バージョン 10.1 以降である必要があります。
- NetScaler インスタンスにはすべて同じ機能ライセンスが必要です。
- クラスターに追加された後は、個々の NetScaler インスタンスの構成を更新することはできません。すべての変更は、クラスタ IP アドレスを使用して実行する必要があります。
- NetScaler インスタンスはすべて同じリソース（メモリ、CPU、インターフェイスなど）を備えている必要があります。
- バックプレーン MTU は、データインターフェイス MTU より 78 バイト大きい必要があります。
- データインターフェイス MTU が 9138 バイト以内であることを確認します。
- リリース 13.0 ビルド 82.x からは、ノードをクラスタに追加するときに SNIP アドレスを追加するよう求められます。ノードの追加時に SNIP アドレスを動的に作成することもできます。この機能は、送信元 IP アドレスの厳密なチェックに関するセキュリティ上の問題に対処するのに役立ちます。
- 重要**:** [クラスターの削除] オプションは注意して使用してください。[**Remove Cluster**] をクリックすると、警告なしにクラスターが削除されます。

SDX アプライアンスでクラスタをセットアップする

1. SDX アプライアンスにログオンします。
2. [構成] タブで、[**NetScaler] > [**クラスター**] > [**クラスターインスタンス] に移動します。
3. クラスターを作成します。
   a) [クラスターの作成] をクリックします。
   b) [**Create Cluster**] ダイアログボックスで、クラスタに必要なパラメータを設定します。パラメータの説明を表示するには、対応するフィールドの上にマウスカーソルを置きます。
   c) [**Next**] をクリックして、構成の概要を表示します。
   d) [**Finish**] をクリックしてクラスターを作成します。
   注：L2 VLAN が構成された NetScaler インスタンスをクラスターに追加すると、
   add VLAN コマンドは
   `sdxvlan`パラメーターを「Yes」に設定して保存されます。このパラメーターは内部引数であり、SDX クラスターの形成中に接続が失われるのを防ぐために使用されます。

4. クラスタにノードを追加します。

   a) [ノードの追加] をクリックします。
   b) [**Add Node**] ダイアログボックスで、クラスタノードの追加に必要なパラメータを設定します。パラメーターの説明を表示するには、対応するフィールドの上にマウスカーソルを合わせます。
   c) [**Next**] をクリックして、構成の概要を表示します。
   d) [**Finish**] をクリックして、ノードをクラスタに追加します。
   e) 手順 1 ～4 を繰り返して、クラスターに別のノードを追加します。

   クラスターを作成したら、クラスター IP アドレスを介してクラスターにアクセスして構成する必要があります。

クラスターインスタンス内のノードが同じ Citx NetScaler SDX アプライアンスに属している場合、NetScaler SDX アプライアンスに障害が発生するとクォーラムが失われる可能性があります。

クラスターノードは以下の方法でデプロイできます。

1. 各 NetScaler SDX アプライアンスから 1 つの VPX インスタンスを使用して複数のクラスターインスタンスを作成します。

例:

SDX1	SDX2	インスタンス ID
VPX1	VPX1	1
VPX2	VPX2	2

1. NetScaler SDX アプライアンスが 3 つ以上ある場合は、`quorumType Majority`のすべてのアプライアンスの VPX インスタンスを使用して 1 つのクラスターインスタンスを作成します。この場合、VPX インスタンスがすべての NetScaler SDX アプライアンスに均等に分散されていることを確認してください。

Example1:

SDX1	SDX2	SDX3	インスタンス ID
VPX1	VPX1	VPX1	1
VPX2	VPX2	VPX2	-
VPX3	VPX3	VPX3	-

Example2:

SDX1	SDX2	SDX3	インスタンス ID
VPX1	VPX1	VPX1	1
VPX2	VPX2	VPX2	-
VPX3	VPX3	VPX3	-
VPX4	-	-	-

1. すべての NetScaler SDX デバイスからのすべての VPX インスタンスを含む単一のクラスターインスタンスを作成します。しかし、`quorum type NONE`を使用してください。これにはいくつかの制限があります。

例:

SDX1	SDX2	インスタンス ID
VPX1	VPX1	1
VPX2	VPX2	2
VPX3	-	-

-quorumTypeパラメータを**NONE**に設定した場合の制限事項:

- 単一障害点によるネットワークの分割を避けるために、トポロジにはクラスタノード間の冗長リンクが必要です。
- ノードの追加や削除などのクラスター操作中にクラスターが不安定になることがあります。

> 注:
>
> 各クラスターに **SDX** アプライアンスの **NetScaler** インスタンスが少なくとも **1** つある **NetScaler** クラスターの最新リストを取得するには、再検出オプションを使用します。

ある **SDX** アプライアンスに存在する **NetScaler** インスタンスを、別の **SDX** アプライアンスで構成されたクラスターに追加します

1. NetScaler インスタンスを追加する SDX アプライアンスにログオンします。
2. **[**** 構成] タブで [**NetScaler**] に移動し、[クラスタ] をクリックします。**
3. [ノードの追加] をクリックします。
4. [**Add Node**] ダイアログボックスで、クラスタノードの追加に必要なパラメータを設定します。パラメーターの説明を表示するには、対応するフィールドの上にマウスカーソルを合わせます。
   注:[
   クラスタ IP アドレス] および [
   クラスタ IP パスワード] パラメータの値が、ノードを追加するクラスタに対応していることを確認します。

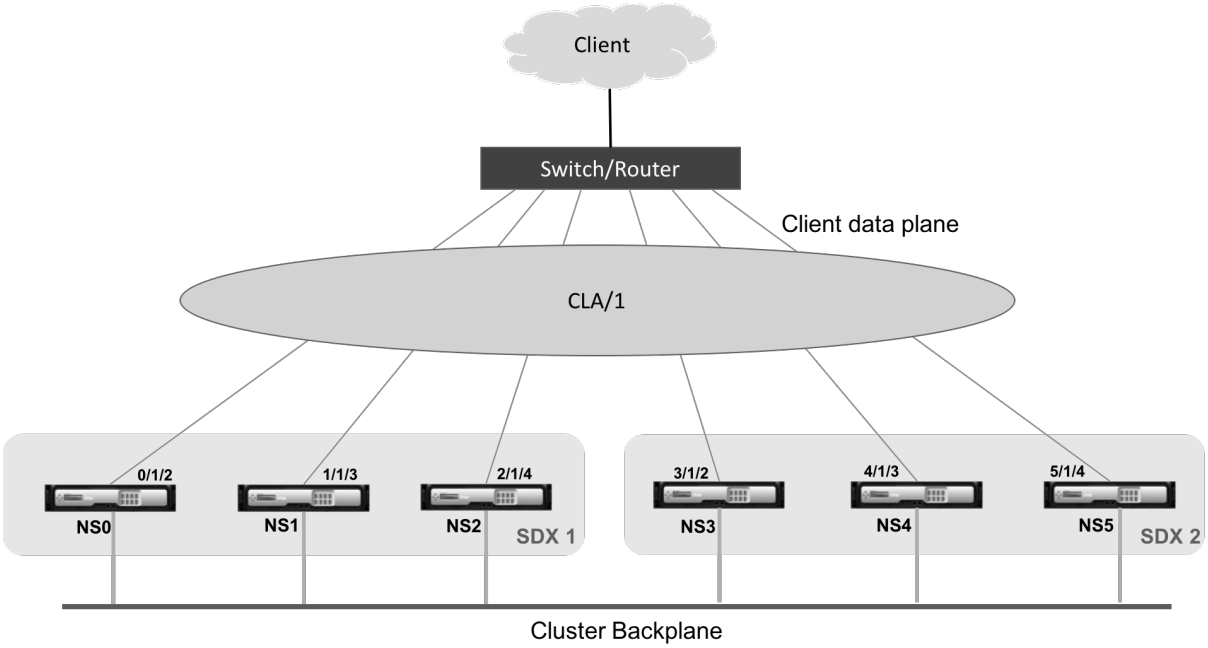
5. [**Next**] をクリックして、構成の概要を表示します。
6. [**Finish**] をクリックして、ノードをクラスタに追加します。

クラスタリンクアグリゲーションの設定

February 16, 2024

クラスタリンクアグリゲーションは、その名前が示すように、クラスタノードインターフェイスのグループをチャネルに結合します。これは NetScaler リンクアグリゲーション（LA）の拡張機能です。唯一の違いは、リンクアグリゲーションではインターフェイスが同じデバイス上にある必要があるのに対し、クラスタリンクアグリゲーションではインターフェイスがクラスタの異なるノード上にあることです。リンクアグリゲーションの詳細については、「リンク集約の設定」を参照してください。

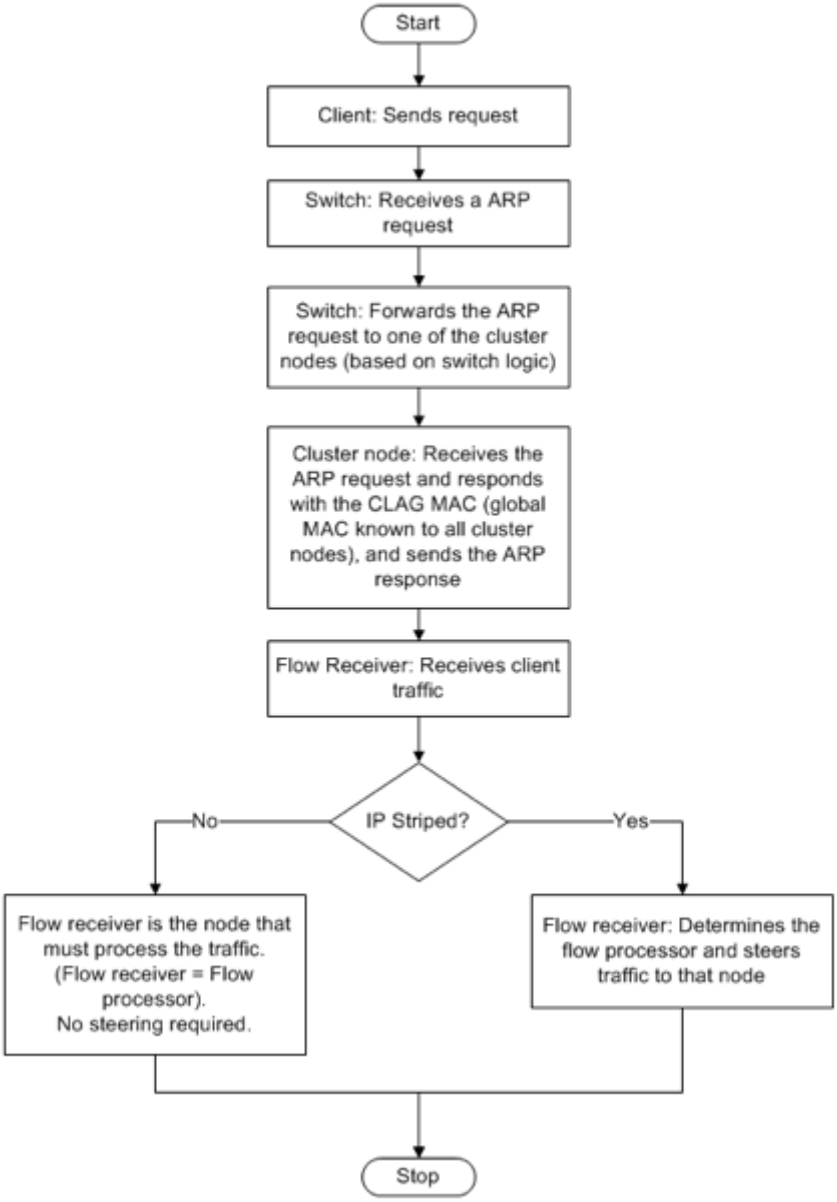
たとえば、2 つの SDX アプライアンスにまたがる 6 ノードクラスタで、6 つのノードすべてがアップストリームスイッチに接続されているとします。クラスタ LA チャネル（CLA/1）は、インターフェイス 0/1/2、1/1/3、2/1/4、3/1/2、4/1/3、および 5/1/4 をバインドすることによって形成されます。



クラスタ LA チャネルには次の属性があります。

- 各チャネルには、クラスタノードによって合意された一意の MAC アドレスがあります。
- チャネルは、ローカルとリモートの両方の SDX ノードのインターフェイスをバインドできます。
- 1 つのクラスタでは、最大 4 つのクラスタ LA チャネルがサポートされます。
- クラスタ LA チャネルごとに最大 16 個のインターフェイスをバインドできます。
- バックプレーンインターフェイスをクラスタ LA チャネルに含めることはできません。

- インターフェイスがクラスタ LA チャネルにバインドされている場合、チャネルパラメータはネットワークインターフェイスパラメータよりも優先されます。
- ネットワークインターフェイスは、1 つのチャネルにのみバインドできます。
- クラスタ LA チャネル（CLA/1 など）またはそのメンバインターフェイス上のクラスタノードには、管理アクセスを設定しないでください。ノードが非アクティブな場合、対応するクラスタ LA インターフェイスは POWER OFF としてマークされ、管理アクセスが失われます。



クラスタ IP アドレスと外部接続デバイスにも同様の設定を実装します。可能であれば、MAC アドレスではなく IP アドレスまたはポートに基づいてトラフィックを分散するようにアップストリームスイッチを設定します。

確認事項:

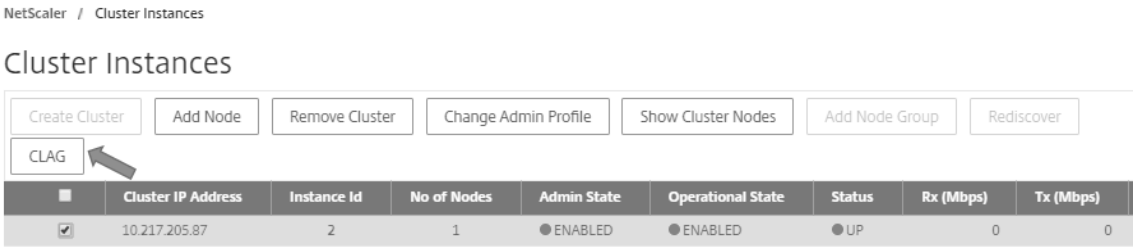
- LACP を有効にします（LACP モードを ACTIVE または PASSIVE に指定します）。
  注： NetScaler クラスターと外部接続デバイスの両方で LACP モードが PASSIVE に設定されていないことを確認してください。
- クラスタ LA チャネルを作成する場合、LACP キーには 5 ～8 の値を指定できます。これらの LACP キーは、CLA/1、CLA/2、CLA/3、および CLA/4 にマッピングされます。
- SDX アプライアンスでは、クラスタリンクアグリゲーショングループ (CLAG) メンバーインターフェイスを他の仮想マシンと共有することはできません。
- アップストリームスイッチで、LACP タイムアウトを「short」に設定して、クラスタノードで長時間トラフィックブラックホールが発生しないようにします。この設定は、LACP タイムアウトが経過するまで CLAG とそのメンバーインターフェイスの電源切断がアップストリームスイッチに通知されない場合に便利です。

前提条件：

NetScaler インスタンスのクラスターを作成します。クラスターのノードは、同じ SDX アプライアンス上の NetScaler インスタンスでも、同じサブネット上で利用可能な他の SDX アプライアンス上の NetScaler インスタンスでもかまいません。

管理サービスを使用してクラスタ **LA** チャネルを構成するには、次の手順を実行します。

1. SDX アプライアンスにログオンします。
2. ［構成］タブで［**NetScaler ADC**］に移動し、［クラスター］をクリックします。
3. [クラスターインスタンス] ページでクラスターを選択し、[**CLAG**] をクリックします。



4. [**CLAG** を作成] ダイアログボックスで、次の操作を行います：
   a) [**Channel ID**] ドロップダウンリストで、クラスタ LA チャネル ID を選択します。
   b)「インタフェース」セクションの「使用可能」選択ボックスからインタフェースを選択し、「**+**」をクリックします。
   c) 選択したインターフェイスが [設定済み] 選択ボックスに表示されます。
5. **[**設定] セクションで、次の操作を行います：
   a) [**Alias**] フィールドに、クラスタ LA チャネルの別名を入力します。
   b) [**LACP Timeout**] フィールドで、次のいずれかの値を選択して、リンクが LACPDU を受信しない場合にリンクが集約されない間隔を定義します。

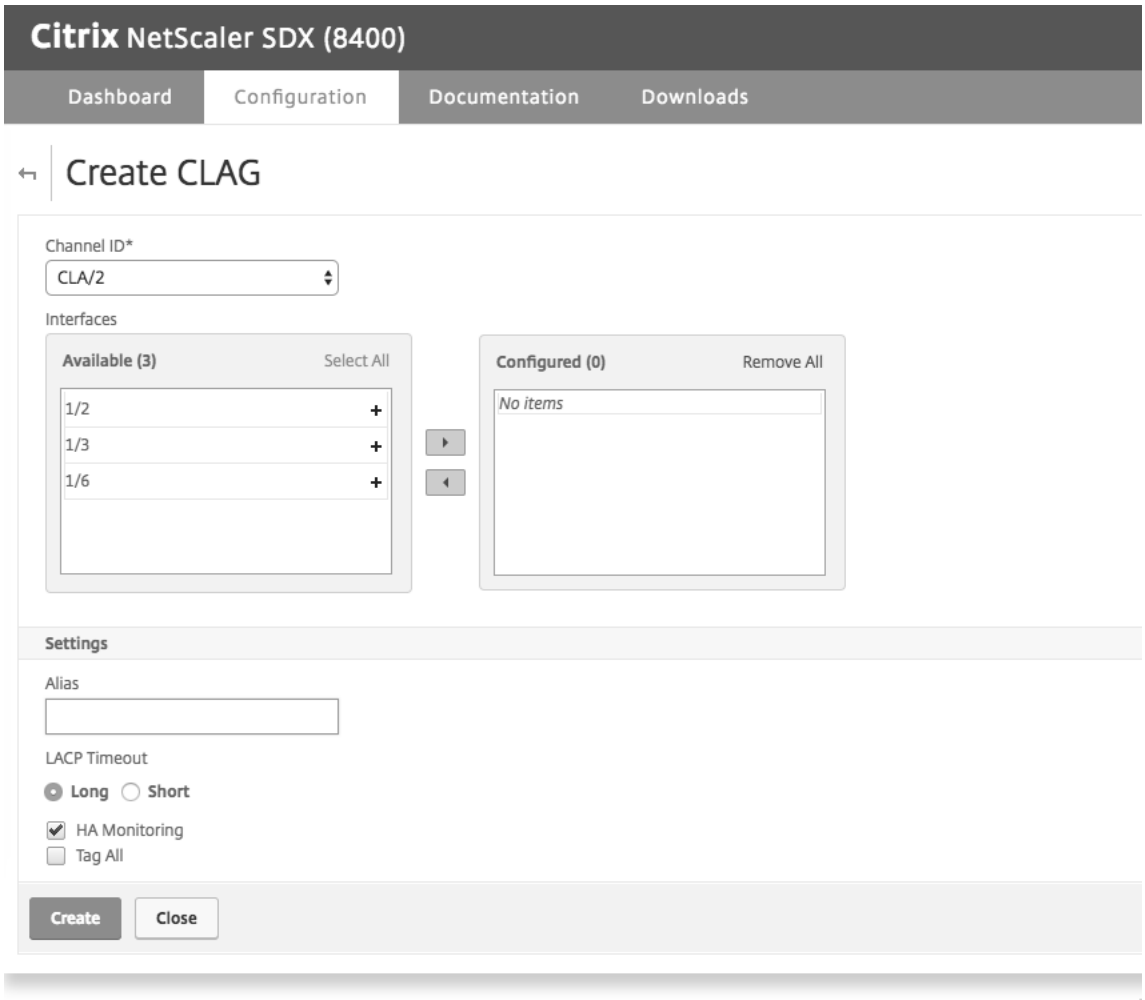
この値は、SDX アプライアンスとパートナーノードのリンクアグリゲーションに参加しているすべてのポートで一致する必要があります:

- ロング—30 秒
- ショート—1 秒

c) 高可用性 (HA) 構成の場合は、[**HA Monitoring**] チェックボックスをオンにして、チャネルに障害イベントがないか監視します。HA MON が有効になっている LA チャネルに障害が発生すると、HA フェールオーバーがトリガー。

d) このチャネルで送信されるすべてのパケットに 4 バイトの 802.1q タグを追加するには、[Tag All] を選択します。**ON** 設定では、このチャネルにバインドされているすべての VLAN にタグが適用されます。OFF は、ネイティブ VLAN 以外のすべての VLAN にタグを適用します。

6.「作成」をクリックして、SDX アプライアンスのいずれかの CLAG を設定します。



7. 確認ダイアログボックスで、「はい」をクリックして他の SDX アプライアンスの CLAG 設定を更新します。

> 注:
>
> - 「いいえ」を選択すると、CLAG は設定されません。
> - 他の SDX アプライアンスの CLAG 設定を手動で更新します。
> - MTU 設定は、両方の SDX アプライアンスで同じにする必要があります。MTU 設定は、いずれかの SDX アプライアンスで手動で変更する必要があります。

8. [**CLAGs**] ダイアログボックスで MTU 設定を変更するには、次の操作を行います:

   a) **CLA/1** を選択し、**[**編集**]** をクリックします。
   b)「CLAG の設定」ダイアログの「**MTU**」フィールドで **MTU** を手動で設定し、「OK」をクリックします。

9. [確認] ダイアログボックスで、[はい] をクリックします。

管理サービスに安全にアクセスするための **SSL** 暗号の設定

February 16, 2024

NetScaler SDX アプライアンスでサポートされている SSL 暗号のリストから SSL 暗号スイートを選択できます。SSL 暗号の任意の組み合わせをバインドして、HTTPS 経由で SDX 管理サービスに安全にアクセスできるようにします。SDX アプライアンスには、類似した暗号の組み合わせである 37 個の定義済み暗号グループが用意されており、サポートされている SSL 暗号のリストからカスタム暗号グループを作成できます。

制限事項

- 鍵交換が「DH」または「ECC-DHE」である暗号のバインドはサポートされていません。
- 認証 =「DSS」による暗号のバインドはサポートされていません。
- サポートされている SSL 暗号リストに含まれていない暗号のバインド、またはこれらの暗号をカスタム暗号グループに含めることはサポートされていません。

サポートされている **SSL** 暗号

次の表に、サポートされている SSL 暗号の一覧を示します。プロトコル列の値は、サポートされている最下位のプロトコルです。たとえば、SSLv3 がリストされている場合、SSLv3/TLSv1/TLSv1.1/TLSv1.2 はすべてサポートされます。

Citrix 暗号名	OpenSSL 暗号名	16 進コード	プロトコル	鍵交換アルゴリズム	認証アルゴリズム	メッセージ認証コード (MAC) アルゴリズム
TLS1-AES-256-CBC-SHA	AES256-SHA	0x0035	SSLv3	RSA	RSA	AES (256)
TLS1-AES-128-CBC-SHA	AES128-SHA	0x002F	SSLv3	RSA	RSA	AES (128)
TLS1.2-AES-256-SHA256	AES256-SHA256	0x003D	TLSv1.2	RSA	RSA	AES (256)
TLS1.2-AES-128-SHA256	AES128-SHA256	0x003C	TLSv1.2	RSA	RSA	AES (128)
TLS1.2-AES256-GCM-SHA384	AES256-GCM-SHA384	0x009D	TLSv1.2	RSA	RSA	AES-GCM(256)
TLS1.2-AES128-GCM-SHA256	AES128-GCM-SHA256	0x009C	TLSv1.2	RSA	RSA	AES-GCM(128)
TLS1-ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA	0xC014	SSLv3	ECC-DHE	RSA	AES (256)
TLS1-ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA	0xC013	SSLv3	ECC-DHE	RSA	AES (128)
TLS1.2-ECDHE-RSA-AES-256-SHA384	ECDHE-RSA-AES256-SHA384	0xC028	TLSv1.2	ECC-DHE	RSA	AES (256)
TLS1.2-ECDHE-RSA-AES-128-SHA256	ECDHE-RSA-AES128-SHA256	0xC027	TLSv1.2	ECC-DHE	RSA	AES (128)

Citrix 暗号名	OpenSSL 暗号名	16 進コード	プロトコル	鍵交換アルゴリズム	認証アルゴリズム	メッセージ認証コード (MAC) アルゴリズム
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA-AES256-GCM-SHA384	0xC030	TLSv1.2	ECC-DHE	RSA	AES-GCM(256)
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA-AES128-GCM-SHA256	0xC02F	TLSv1.2	ECC-DHE	RSA	AES-GCM(128)
TLS1.2-DHE-RSA-AES-256-SHA256	DHE-RSA-AES256-SHA256	0x006B	TLSv1.2	DH	RSA	AES (256)
TLS1.2-DHE-RSA-AES-128-SHA256	DHE-RSA-AES128-SHA256	0x0067	TLSv1.2	DH	RSA	AES (128)
TLS1.2-DHE-RSA-AES256-GCM-SHA384	DHE-RSA-AES256-GCM-SHA384	0x009F	TLSv1.2	DH	RSA	AES-GCM(256)
TLS1.2-DHE-RSA-AES128-GCM-SHA256	DHE-RSA-AES128-GCM-SHA256	0x009E	TLSv1.2	DH	RSA	AES-GCM(128)
TLS1-DHE-RSA-AES-256-CBC-SHA	DHE-RSA-AES256-SHA	0x0039	SSLv3	DH	RSA	AES (256)
TLS1-DHE-RSA-AES-128-CBC-SHA	DHE-RSA-AES128-SHA	0x0033	SSLv3	DH	RSA	AES (128)

Citrix 暗号名	OpenSSL 暗号名	16 進コード	プロトコル	鍵交換アルゴリズム	認証アルゴリズム	メッセージ認証コード (MAC) アルゴリズム
TLS1-DHE-DSS-AES-256-CBC-SHA	DHE-DSS-AES256-SHA	0x0038	SSLv3	DH	DSS	AES (256)
TLS1-DHE-DSS-AES-128-CBC-SHA	DHE-DSS-AES128-SHA	0x0032	SSLv3	DH	DSS	AES (128)
TLS1-ECDHE-RSA-DES-CBC3-SHA	ECDHE-RSA-DES-CBC3-SHA	0xC012	SSLv3	ECC-DHE	RSA	3DES(168)
SSL3-EDH-RSA-DES-CBC3-SHA	EDH-RSA-DES-CBC3-SHA	0x0016	SSLv3	DH	RSA	3DES(168)
SSL3-EDH-DSS-DES-CBC3-SHA	EDH-DSS-DES-CBC3-SHA	0x0013	SSLv3	DH	DSS	3DES(168)
TLS1-ECDHE-RSA-RC4-SHA	ECDHE-RSA-RC4-SHA	0xC011	SSLv3	ECC-DHE	RSA	RC4(128)
SSL3-DES-CBC3-SHA	DES-CBC3-SHA	0x000A	SSLv3	RSA	RSA	3DES(168)
SSL3-RC4-SHA	RC4-SHA	0x0005	SSLv3	RSA	RSA	RC4(128)
SSL3-RC4-MD5	RC4-MD5	0x0004	SSLv3	RSA	RSA	RC4(128)
SSL3-DES-CBC-SHA	DES-CBC-SHA	0x0009	SSLv3	RSA	RSA	DES(56)
SSL3-EXP-RC4-MD5	EXP-RC4-MD5	0x0003	SSLv3	RSA (512)	RSA	RC4(40)
SSL3-EXP-DES-CBC-SHA	EXP-DES-CBC-SHA	0x0008	SSLv3	RSA (512)	RSA	DES(40)

Citrix 暗号名	OpenSSL 暗号名	16 進コード	プロトコル	鍵交換アルゴリズム	認証アルゴリズム	メッセージ認証コード (MAC) アルゴリズム
SSL3-EXP-RC2-CBC-MD5	EXP-RC2-CBC-MD5	0x0006	SSLv3	RSA (512)	RSA	RC2(40)
SSL2-DES-CBC-MD5	DHE-DSS-AES128-SHA256	0x0040	SSLv2	RSA	RSA	DES(56)
SSL3-EDH-DSS-DES-CBC-SHA	EDH-DSS-DES-CBC-SHA	0x0012	SSLv3	DH	DSS	DES(56)
SSL3-EXP-EDH-DSS-DES-CBC-SHA	EXP-EDH-DSS-DES-CBC-SHA	0x0011	SSLv3	DH (512)	DSS	DES(40)
SSL3-EDH-RSA-DES-CBC-SHA	EDH-RSA-DES-CBC-SHA	0x0015	SSLv3	DH	RSA	DES(56)
SSL3-EXP-EDH-RSA-DES-CBC-SHA	EXP-EDH-RSA-DES-CBC-SHA	0x0014	SSLv3	DH (512)	RSA	DES(40)
SSL3-ADH-RC4-MD5	ADH-RC4-MD5	0x0018	SSLv3	DH	なし	RC4(128)
SSL3-ADH-DES-CBC3-SHA	ADH-DES-CBC3-SHA	0x001B	SSLv3	DH	なし	3DES(168)
SSL3-ADH-DES-CBC-SHA	ADH-DES-CBC-SHA	0x001A	SSLv3	DH	なし	DES(56)
TLS1-ADH-AES-128-CBC-SHA	ADH-AES128-SHA	0x0034	SSLv3	DH	なし	AES (128)
TLS1-ADH-AES-256-CBC-SHA	ADH-AES256-SHA	0x003A	SSLv3	DH	なし	AES (256)

Citrix 暗号名	OpenSSL 暗号名	16 進コード	プロトコル	鍵交換アルゴリズム	認証アルゴリズム	メッセージ認証コード (MAC) アルゴリズム
SSL3-EXP-ADH-RC4-MD5	EXP-ADH-RC4-MD5	0x0017	SSLv3	DH (512)	なし	RC4(40)
SSL3-EXP-ADH-DES-CBC-SHA	EXP-ADH-DES-CBC-SHA	0x0019	SSLv3	DH (512)	なし	DES(40)
SSL3-NULL-MD5	NULL-MD5	0x0001	SSLv3	RSA	RSA	なし
SSL3-NULL-SHA	NULL-SHA	0x0002	SSLv3	RSA	RSA	なし

定義済みの暗号グループ

次の表は、SDX アプライアンスによって提供される定義済みの暗号グループの一覧です。

暗号グループ名	説明
ALL	SDX アプライアンスでサポートされるすべての暗号 (NULL 暗号を除く)
DEFAULT	暗号化強度が 128 ビット以上のデフォルトの暗号リスト
kRSA	RSA として Key-EX アルゴを使用した暗号
kEDH	Key-Ex アルゴをエフェメラル-DH とした暗号
DH	Key-Ex アルゴを DH として持つ暗号
EDH	Key-EX/Auth アルゴを DH として持つ暗号
aRSA	認証アルゴを RSA として持つ暗号
aDSS	認証アルゴを DSS として持つ暗号
aNULL	認証アルゴを NULL とした暗号
DSS	認証アルゴを DSS として持つ暗号
DES	Enc アルゴを DES として持つ暗号
3DES	Enc アルゴを 3DES として持つ暗号
RC4	Enc アルゴを RC4 とした暗号

暗号グループ名	説明
RC2	Enc アルゴを RC2 として持つ暗号
NULL	Enc アルゴを NULL とした暗号
MD5	MAC アルゴを MD5 として持つ暗号
SHA1	MAC アルゴを SHA-1 として持つ暗号
SHA	MAC アルゴを SHA として持つ暗号
NULL	Enc アルゴを NULL とした暗号
RSA	RSA としてキー EX/Auth アルゴを使用した暗号
ADH	Key-EX アルゴを DH として、Auth アルゴを NULL とした暗号
SSLv2	SSLv2 プロトコル暗号
SSLv3	SSLv3 プロトコル暗号
TLSv1	SSLv3/TLSv1 プロトコル暗号
TLSv1_ONLY	TLSv1 プロトコル暗号
EXP	暗号のエクスポート
書き出す	暗号のエクスポート
EXPORT40	40 ビット暗号化による暗号のエクスポート
EXPORT56	56 ビット暗号化による暗号のエクスポート
低い	低強度の暗号 (56 ビット暗号化)
中	中強度の暗号 (128 ビット暗号化)
高い	高強度暗号 (168 ビット暗号化)
AES	AES 暗号
FIPS	FIPS 承認済み暗号
ECDHE	楕円曲線エフェメラル DH 暗号
AES-GCM	AES-GCM として Enc アルゴを使用した暗号
SHA2	MAC アルゴを SHA-2 として持つ暗号

定義済みの暗号グループを表示する

定義済みの暗号グループを表示するには、[構成] タブのナビゲーションウィンドウで [管理サービス] を展開し、[暗号グループ] をクリックします。

カスタム暗号グループの作成

サポートされている SSL 暗号のリストから、カスタム暗号グループを作成できます。

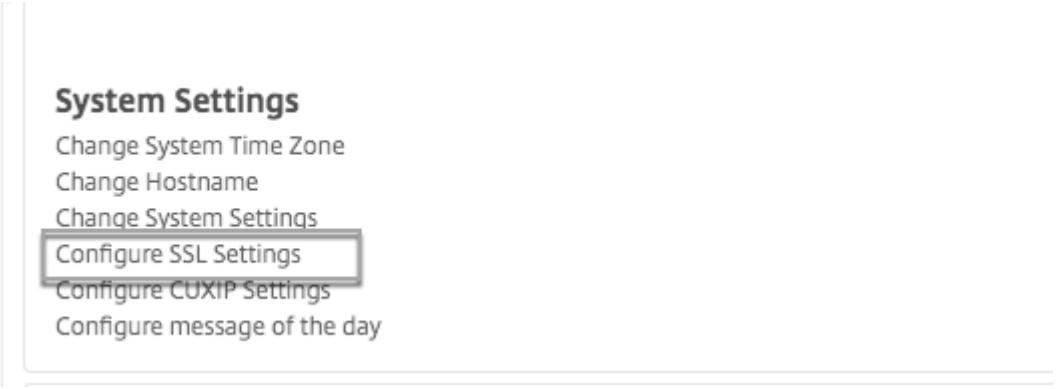
カスタム暗号グループを作成するには:

1. [構成] タブのナビゲーションウィンドウで、[管理サービス] を展開し、[暗号グループ] をクリックします。
2. [暗号グループ] ペインで、[追加] をクリックします。
3. [暗号グループの作成] ダイアログボックスで、次の操作を行います。

    a) [**Group Name**] フィールドに、カスタム暗号グループの名前を入力します。
    b) [**Cipher Group Description**] フィールドに、カスタム暗号グループの簡単な説明を入力します。
    c) [**Cipher Suites**] セクションで、[**Add**] をクリックし、サポートされている SSL 暗号のリストに含める暗号を選択します。
    d) ［作成］ をクリックします。

既存の **SSL** 暗号バインディングの表示

既存の暗号バインドを表示するには、**[**** 構成] タブのナビゲーションウィンドウで [システム] を展開し、[システム設定] の [**SSL** 設定の構成] をクリックします。******



> 注:
>
> 管理サービスの最新バージョンにアップグレードすると、既存の暗号スイートのリストに OpenSSL 名が表示されます。アップグレードされた管理サービスから暗号をバインドすると、表示には Citrix の命名規則が使用されます。

HTTPS サービスに暗号をバインドする

1. [構成] タブのナビゲーションウィンドウで、[システム] をクリックします。
2. [システム] ウィンドウの [システム設定] で、[**SSL** 設定の構成] をクリックします。
3. [設定の編集] ペインで、[暗号スイート] をクリックします。
4. [**Ciphers Suites**] ペインで、次のいずれかの操作を行います。

- 定義済みの暗号グループから暗号グループを選択するには、「Cipher **Groups**」を選択し、「Cipher Groups」リストから暗号グループを選択して、「**OK**」をクリックします。
- サポートされている暗号の一覧から選択するには、［**Cipher Suites** ］チェックボックスをオンにし、［**Add** ］をクリックして暗号を選択し、［**OK**］をクリックします。

SDX アプライアンスの構成データをバックアップおよび復元する

February 16, 2024

NetScaler SDX アプライアンスのバックアッププロセスは、以下を含むバックアップファイルを作成するシングルステップのプロセスです。

- シングルバンドルイメージ:
  - Citrix Hypervisor イメージ
  - Citrix Hypervisor のホットフィックスとサプリメンタルパック
  - マネジメントサービスイメージ
- XVA イメージ
- イメージのアップグレード
- SDX 構成
- 構成

バックアップフォルダは /var/mps/backup/ です。

現在の設定をバックアップする

1. [構成] タブのナビゲーションウィンドウで、[管理サービス] を展開し、[バックアップファイル] をクリックします。
2. [バックアップファイル] ペインで、[バックアップ] をクリックします。
3. [新しいバックアップファイル] ダイアログボックスで、[ファイルのパスワード保護] チェックボックスをオンにして、バックアップファイルを暗号化します。
4. [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、バックアップファイルのパスワードを入力し、確認します。
5. ［続行］をクリックします。

バックアッププロセスにより、バックアップファイルが作成されます。バックアップファイルのファイル名には、管理サービスの現在の IP アドレスと、バックアップが作成されたときのタイムスタンプが含まれます。バックアップファイルに不一致がないかどうかを確認するには、SDX GUI から [構成**] > [**システム**] > [**イベント**/**アラーム] の順に移動します。

予定されたバックアップ

デフォルトでは、SDX はバックアップポリシーを使用して 24 時間ごとにバックアップを作成します。バックアップポリシーを使用して、SDX アプライアンスに保持するバックアップファイルの数を定義できます。また、バックアップファイルのセキュリティを確保するために、パスワードを使用してスケジュールバックアップファイルを暗号化することもできます。

バックアップポリシーを編集する

1. [構成] タブで [システム] をクリックします。
2. [ポリシー管理] ウィンドウで、[バックアップポリシー] をクリックします。
3. [バックアップポリシーの構成] ペインで、次の操作を行います。
   a) [保持する以前のバックアップ] フィールドに、保持するバックアップファイルの数を入力します。
   b) バックアップファイルを暗号化するには、[バックアップファイルを暗号化] チェックボックスをオンにします。
   c) [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、バックアップファイルを暗号化するためのパスワードを入力し、確認します。

バックアップファイルを外部のバックアップサーバに手動で転送する

バックアップファイルを手動で転送する前に、外部バックアップサーバの詳細があることを確認してください。

バックアップファイルを外部バックアップサーバに転送する

1. [構成] タブのナビゲーションウィンドウで、[管理サービス] を展開し、[バックアップファイル] をクリックします。
2. [バックアップファイル] ペインで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. [**Server**] フィールドに、外部バックアップサーバのホスト名または IP アドレスを入力します。
4. [**User Name**] フィールドと [**Password**] フィールドに、外部バックアップサーバにアクセスするためのユーザ名とパスワードを入力します。
5. [**Port**] フィールドにポート番号を入力します。
6. [**Transfer Protocol**] フィールドで、バックアップファイルを外部バックアップサーバに転送するために使用するプロトコルを選択します。
7. [**Directory Path**] フィールドに、バックアップファイルを保存する外部バックアップサーバ内のディレクトリのパスを入力します。
8. バックアップファイルを外部バックアップサーバに転送した後、**SDX** アプライアンスからバックアップファイルを削除するには、**[**管理サービスからファイルを削除] を選択します。
9. [**OK**] をクリックします。

アプライアンスの復元

SDX アプライアンスは、バックアップファイルで使用可能な設定に復元できます。アプライアンスの復元中、現在の設定はすべて削除されます。

注意事項**:**

- 別の SDX アプライアンスのバックアップファイルを使用して SDX アプライアンスを復元する前に、バックアップファイルで使用可能な設定に従って Management Service ネットワーク設定を追加します。
- バックアップが作成されたプラットフォームバリアントが、復元しようとしているプラットフォームバリアントと同じであることを確認します。2 つの異なるプラットフォームバリアント間でのバックアップファイルの復元はサポートされていません。
- SDX バックアップは、ネットワーク構成が設定された後にのみ復元することをお勧めします。SVM には次のネットワーク設定を指定できます。
  - SVM IP アドレス
  - ハイパーバイザ IP アドレス
  - サブネットマスク
  - Gateway
  - DNS サーバー

バックアップファイルからアプライアンスを復元する

1. [構成] タブのナビゲーションウィンドウで、[管理サービス] を展開し、[バックアップファイル] をクリックします。
2. ［バックアップファイル］ペインでバックアップファイルをクリックし、［**OK**］をクリックします。
3. 「リストア」ダイアログ・ボックスで「アプライアンスのリストア」を選択し、「続行」をクリックします。

   アプリケーション復元のさまざまなコンポーネントが表示されます。

   - ライセンス
   - SDX イメージ
   - XVA ファイル
   - NetScaler 構成
   - まとめ

   必要なコンポーネントのいずれかがバックアップファイルにない場合、先に進む前に不足している要素をアップロードするよう求められます。

   現在の SDX Single Bundle Image バージョンでバックアップファイルを復元できるかどうかについては、次の表を参照してください。シングルバンドルイメージの経験則として、それより低いバージョンのバックアップを新しいバージョンに復元することはできません。

SDX シングルバンドルイメージの最新バージョン	バックアップファイルバージョン
11.1	11.1、12.0、12.1、13.0 はサポートされていますが、11.0 はサポートされていません
12.0	12.0、12.1、13.0 はサポートされていますが、11.0 と 11.1 はサポートされていません
12.1	12.1、13.0 はサポートされていますが、11.0、11.1、12.0 はサポートされていません
13.0	13.0 がサポートされています。11.0、11.1、12.0、12.1 はサポートされていません
13.1	13.1 がサポートされています。11.0、11.1、12.0、12.1、13.0 はサポートされていません

4. [ライセンス] ページで、有効なライセンスが存在することを確認し、[次へ] をクリックします。
5. [**SDX** イメージ] ページが表示されます。復元を実行するのに SDX イメージが不要な場合は、[次へ] をクリックします。それ以外の場合は、プロンプトが表示されたら有効な SDX イメージをアップロードし、[次へ] をクリックします。
6. **XVA** ファイル] ページが開きます。すべてのインスタンスの XVA イメージが存在する場合は、[次へ] をクリックします。バックアップファイルにインスタンスの XVA ファイルが存在しない場合は、アップロードするか、このインスタンスの復元をスキップできます。[**Next**] をクリックして次のページに進みます。
7.「NetScaler 構成」ページが開きます。NetScaler 構成ファイルは必須ではありません。構成を復元しなくても、インスタンスをプロビジョニングできます。バックアップファイルに NetScaler 構成ファイルがない場合は、インスタンスのプロビジョニングのみを続行するか、インスタンスの復元をスキップできます。[**Next**] をクリックして次のページに進みます。
8. [Summary] ページが開き、バックアップファイルに存在するすべてのインスタンスに関する次の詳細が表示されます。
   - IP アドレス
   - ホスト名
   - SDX バージョン
   - XVA バージョン
   - バージョンビット
   - 復元: アプライアンスまたはインスタンスが復元の準備ができている場合、チェックマークが表示されます。そうでない場合は、十字マークが表示されます。
   - エラーメッセージ: アプライアンスまたはインスタンスが復元の準備ができていない場合、その理由を説明するエラーメッセージが表示されます。
9. [**Restore**] をクリックして、アプリケーションの復元プロセスを完了します。

NetScaler インスタンスを復元する

SDX アプライアンスの NetScaler インスタンスを、バックアップファイルで使用可能な NetScaler インスタンスに復元できます。

注意点**:** VPX インスタンスは、次の場合に復元に失敗します。

- インスタンスに管理 NIC が割り当てられておらず、
- インスタンスは、LACP 経由でのみ SDX 管理サービスから管理されます。
  SDX Management Service はチャネル構成を自動的に復元できないため、復元は失敗します。この問題を回避するには、チャネル構成を手動で復元し、VPX インスタンスの復元を完了します。

NetScaler インスタンスをバックアップファイルに復元するには:

1. [構成] タブのナビゲーションウィンドウで、[管理サービス] を展開し、[バックアップファイル] をクリックします。
2. [バックアップファイル] ペインでバックアップファイルを選択し、[復元] をクリックします。
3. [リストア] ダイアログボックスで、[インスタンスのリストア] を選択します。
4. 復元する **NetScaler** インスタンスを選択して、**[**続行**]** をクリックします。
5. (オプション) バックアップファイルが暗号化されている場合は、プロンプトが表示されたらパスワードを入力し、**OK** をクリックします。

> 注**:**
>
> 復元するインスタンスを実行する SDX アプライアンスに、適切な XVA、ビルドイメージ、およびチャネル構成が存在することを確認してください。

アプライアンスのリセットを実行する

November 23, 2023

NetScaler SDX アプライアンスでは、次のことが可能になります。

- アプライアンスの設定をリセットします。

  > 注:
  >
  > 構成をリセットしたら、アプライアンスのシリアル番号をパスワードとして使用してログオンする必要があります。

- アプライアンスを工場出荷時のバージョンにリセットします。
- アプライアンスを特定のシングルバンドルイメージバージョンにリセットします。

アプライアンスのリセットを実行する前に、アプライアンスにプロビジョニングされたすべての NetScaler インスタンスの設定を含め、アプライアンスに保存されているすべてのデータをバックアップします。

Citrix では、アプライアンスの外部にファイルを保存することをお勧めします。アプライアンスのリセットを実行すると、管理サービスとの現在のクライアントセッションがすべて終了します。管理サービスにログオンし直して、追加の構成タスクがあるかどうかを確認します。データを復元する準備ができたら、Management Service を使用してバックアップファイルをインポートします。

管理サービスには、アプライアンスをリセットするための次のオプションがあります。

- 設定リセット
- ファクトリリセット
- クリーンインストール

アプライアンスの設定をリセットする

管理サービスには、アプライアンスの設定をリセットするための Config Reset オプションがあります。Config Reset オプションでは、次の処理が実行されます。

- VPX インスタンスを削除します。
- SSL 証明書とキーファイルを削除します。
- ライセンスファイルとテクニカルアーカイブファイルを削除します。
- アプライアンス上の NTP 設定を削除します。
- タイムゾーンを UTC に戻します。
- プルーニングポリシーとバックアップポリシーをデフォルト設定に戻します。
- 管理サービスイメージを削除します。
- NetScaler SDX イメージを削除します。
- アプライアンスで最後にアクセスされたイメージファイルを除くすべての XVA イメージを削除します。
- デフォルトのインターフェイス設定を復元します。
- デフォルトのプロファイル、ユーザ、システム設定など、アプライアンスのデフォルト設定を復元します。
- Citrix Hypervisor と管理サービスのデフォルトパスワードを復元します。
- 管理サービスを再起動します。

アプライアンスの設定をリセットする

1. [構成**] > [**システム**] > [**システム管理グループ] に移動します。
2.「アプライアンスリセット」をクリックします。
3.「アプライアンスのリセット」ダイアログ・ボックスの「****** リセット・タイプ」リストで「構成のリセット ****** 」を選択します
4. [**OK]** をクリックします。

アプライアンスを工場出荷時のバージョンにリセットする

Management Service には、アプライアンスを工場出荷時のバージョンにリセットするための [Factory Reset] オプションがあります。出荷時設定へのリセットオプションは、管理サービスと Citrix Hypervisor の現在の IP アドレスを、管理サービスと Citrix Hypervisor のデフォルトの IP アドレスにリセットします。

アプライアンスにプロビジョニングされたすべての NetScaler インスタンスの設定を含め、アプライアンスに保存されているすべてのデータを必ずバックアップしてください。Citrix では、アプライアンスの外部にファイルを保存することをお勧めします。工場出荷時設定にリセットすると、Management Service との現在のクライアントセッションがすべて終了します。管理サービスにログオンし直して、追加の構成タスクがあるかどうかを確認します。データを復元する準備ができたら、Management Service を使用してバックアップファイルをインポートします。

> 重要
>
> 工場出荷時設定へのリセットを実行する前に、シリアルコンソールケーブルをアプライアンスに接続してください。

アプライアンスを工場出荷時のバージョンにリセットする

1. [構成**] > [**システム**] > [**システム管理**]** に移動します。
2. 「アプライアンスリセット」をクリックします。
3. 「アプライアンスのリセット」ダイアログ・ボックスで、「リセット・タイプ」リストから「出荷時設定」を選択します。
4. [**OK**] をクリックします。

アプライアンスを単一バンドルイメージバージョンにリセットする

管理サービスには、単一バンドルイメージの任意のバージョンをアプライアンスにインストールできる [クリーンインストール（Clean Install）] オプションがあります。これにより、単一バンドルイメージを新しいデフォルトブートイメージとして新規インストールできます。クリーンインストールでは、SDX アプライアンス内のネットワーク設定を除く既存の設定が削除されます。

> 注:
>
> SDX アプライアンスにソフトウェアバージョン 11.0 以前が同梱されていた場合、バージョン 13.1 以降へのクリーンインストールは失敗します。

clean-install オプションは、次の環境でサポートされています。

シングルバンドルイメージバージョン	SDX プラットフォーム
11.0.xx	SDX 14xxx, SDX 25xxx. 注: クリーンインストールオプションは、他の SDX プラットフォームに 10G のファクトリパーティションがある場合、サポートされます。
11.1.xx	SDX 14xxx, SDX 25xxx. 注: クリーンインストールオプションは、他の SDX プラットフォームに 10G のファクトリパーティションがある場合、サポートされます。
11.1.51.x	すべての SDX プラットフォーム。
12.1.xx	すべての SDX プラットフォーム。
13.0.xx	すべての SDX プラットフォーム。
13.1.xx	すべての SDX プラットフォーム。

前提条件

以下の点について確認してください:

- すべてのプライマリ高可用性ノードを別の SDX アプライアンスにフェイルオーバーします。高可用性機能がない場合は、それに応じてダウンタイムを計画してください。
- シングルバンドルイメージをローカルマシンにダウンロードします。

> 重要:
>
> [Clean Install] オプションを使用している間は、アプライアンスの再起動や電源のオフ/オンを行わないようにしてください。
> アプライアンスが複数回再起動される。

アプライアンスを単一バンドルイメージバージョンにリセットする

1. [構成**] > [**システム**] > [**システム管理グループ] に移動します。
2. 「アプライアンスリセット」をクリックします。
3. 「アプライアンスのリセット」ダイアログ・ボックスの「リセット・タイプ **** 」リストで「**** クリーンインストール」を選択します。
4. [**OK**] をクリックします。

外部認証サーバのカスケード

February 16, 2024

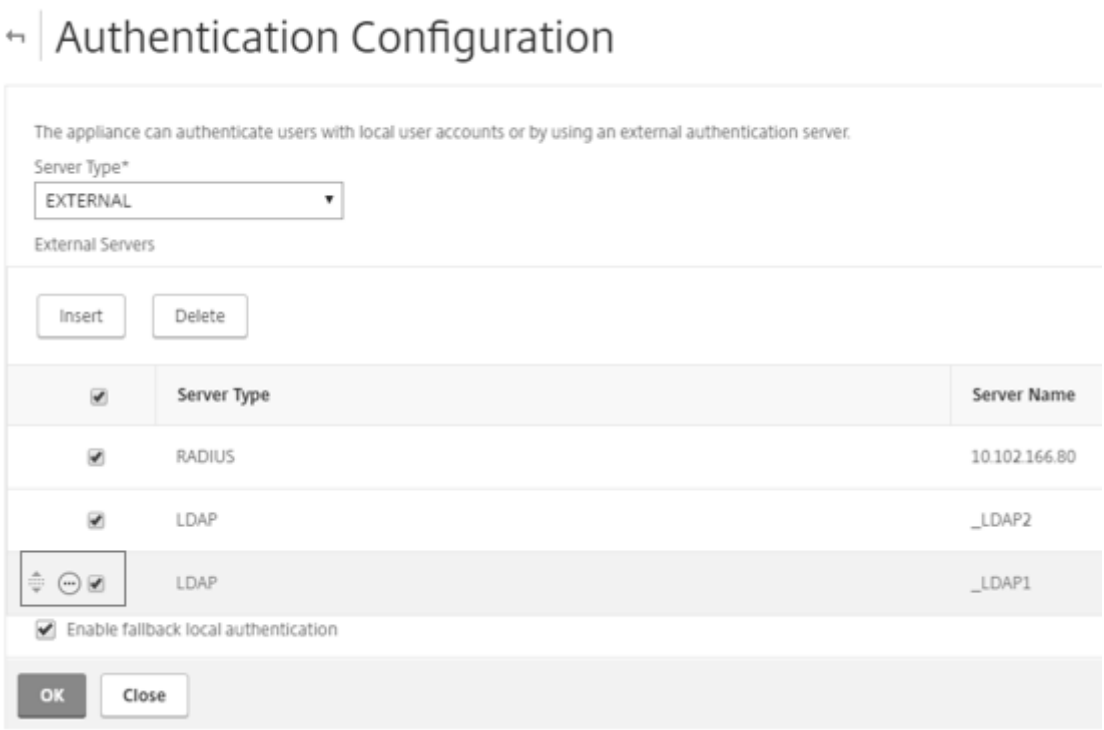
複数の外部認証サーバをカスケード接続すると、外部ユーザの認証と承認のための継続的で信頼性の高いプロセスが提供されます。1 番目の認証サーバーで認証が失敗した場合、管理サービスは 2 番目の外部認証サーバーを使用してユーザーの認証を試みます。

カスケード認証を有効にするには、外部認証サーバーを管理サービスに追加します。詳細については、「外部認証の設定」を参照してください。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 つの外部認証サーバを追加するには、RADIUS、LDAP、および TACACS サーバの任意の組み合わせを追加できます。同じタイプの 4 つのサーバをすべて追加することもできます。NetScaler Application Delivery Management では、最大 32 台の外部認証サーバーを構成できます。

外部認証サーバをカスケード接続する

1. [構成] タブの [システム] で、[認証] を展開します。
2. [認証] ページで、[認証構成] をクリックします。
3. [認証設定] ページで、[サーバタイプ] 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のみです)。
4. [挿入] をクリックし、表示された [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. [**OK**] をクリックします。

次の図に示すように、選択したサーバが [認証サーバ] ページに表示されます。認証の順序を変更するには、サーバ名の横にあるアイコンを使用して、サーバをリスト内で上または下に移動します。



ユーザーをロック解除する

November 23, 2023

NetScaler SDX 管理者は、ロックアウト間隔が切れる前にユーザーのロックを解除できます。ユーザーがコンソール経由で管理サービスにログインする場合、ロックアウトは適用されません。ロックアウト間隔も秒から分に変更されます。最小値 = 1 分。最大値 = 30 分。

GUI を使用したユーザーのロック解除

1. [設定] **>** [システム] **>** [ユーザ管理] **>** [ユーザ] に移動します。
2. ロックを解除するユーザーを選択します。
3. ロック解除] をクリックします。

CLI を使用してユーザーをロック解除する

コマンドプロンプトで入力します:

```
set systemuser id=<ID> unlock=true
```

NetScaler インスタンスのプロビジョニング

November 23, 2023

> 注
>
> NetScaler SDX アプライアンスをリリース 13.1 にインストールまたはアップグレードすると、NetScaler ADM サービス接続がデフォルトで有効になります。詳しくは、「データガバナンスと NetScalerADM サービス接続」を参照してください。

管理サービスを使用して、SDX アプライアンスに 1 つ以上の NetScaler インスタンスをプロビジョニングできます。インストールできるインスタンスの数は、購入したライセンスによって異なります。追加されたインスタンスの数がライセンスで指定された数と等しい場合、管理サービスはそれ以上の NetScaler インスタンスのプロビジョニングを許可しません。

> 注:
>
> 基盤となるハードウェアプラットフォームとは無関係に、ネットワークインターフェイスに最大 20 個の VPX インスタンスを構成できます。

SDX アプライアンスでの NetScaler VPX インスタンスの Provisioning には、次の手順が含まれます。

1. NetScaler インスタンスにアタッチする管理者プロファイルを定義します。このプロファイルは、Management Service が ADC インスタンスをプロビジョニングし、後でインスタンスと通信して構成データを取得するために使用するユーザー資格情報を指定します。デフォルトの管理者プロファイルを使用することもできます。
2. .xva イメージファイルを管理サービスにアップロードします。
3. 管理サービスの NetScaler プロビジョニングウィザードを使用して NetScaler インスタンスを追加します。管理サービスは、NetScaler インスタンスを SDX アプライアンスに暗黙的にデプロイし、インスタンスの構成の詳細をダウンロードします。

> 警告
>
> インスタンスで直接変更を実行するのではなく、Management Service を使用して、プロビジョニングされたネットワークインターフェイスまたは VLAN を変更してください。

管理者プロフィールを作成する

管理者プロファイルは、NetScaler インスタンスをプロビジョニングするときに管理サービスが使用するユーザー認証情報を指定します。これらの認証情報は、後でインスタンスと通信して設定データを取得するときに使用されます。管理者プロファイルに指定されたユーザー資格情報は、クライアントが CLI または GUI を介して NetScaler インスタンスにログオンするときにも使用されます。

管理者プロファイルでは、Management Service と VPX インスタンスがセキュアなチャネルまたは HTTP を使用してのみ相互に通信するように指定することもできます。

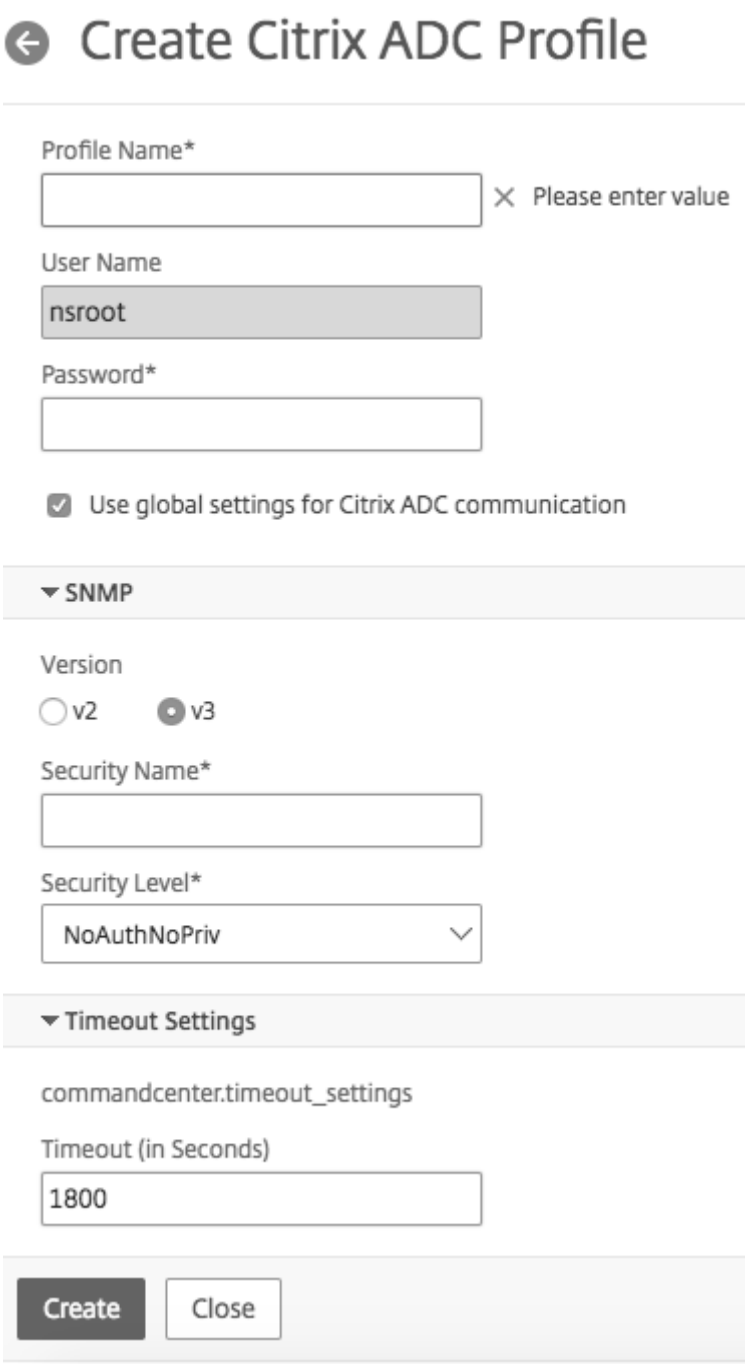
インスタンスのデフォルト管理者プロファイルでは、デフォルトの管理者ユーザ名が指定されます。このプロファイルは変更も削除もできません。ただし、インスタンスのプロビジョニング時に、ユーザー定義の管理者プロファイルを作成してインスタンスにアタッチすることで、デフォルトプロファイルをオーバーライドする必要があります。管理サービス管理者は、NetScaler インスタンスにアタッチされていないユーザー定義の管理者プロファイルを削除できます。

> 重要
>
> VPX インスタンスで直接パスワードを変更しないでください。これを行うと、管理サービスからインスタンスに到達できなくなります。パスワードを変更するには、まず管理者プロファイルを作成し、次に NetScaler インスタンスを変更して、管理者プロファイルリストからこのプロファイルを選択します。

高可用性セットアップで NetScaler インスタンスのパスワードを変更するには、まずセカンダリノードとして指定されたインスタンスのパスワードを変更します。次に、プライマリノードとして指定したインスタンスのパスワードを変更します。パスワードの変更は、管理サービスを使用する場合のみ行ってください。

管理者プロフィールを作成する

1. ナビゲーションペインの［構成］タブで［**NetScaler** 構成］を展開し、［管理者プロファイル］をクリックします。
2. [管理者プロファイル] ペインで、[追加] をクリックします。
3. [管理者プロファイルの作成] ダイアログボックスが表示されます。



次のパラメーターを設定します。

- プロファイル名: 管理者プロファイルの名前。デフォルトのプロファイル名はnsrootです。ユーザ定義のプロファイル名を作成できます。
- パスワード: NetScaler インスタンスへのログオンに使用するパスワード。最大長:31 文字
- SSH ポート:SSH ポートを設定します。デフォルトのポートは 22 です。
- **NetScaler** 通信にグローバル設定を使用する: 管理サービスと NetScaler インスタンス間の通信の設定をシステム設定で定義するかどうかを選択します。このチェックボックスをオフにして、プロトコルを HTTP または HTTPS に変更できます。
  - 管理サービスと **NetScaler** インスタンス間の通信に **HTTP** プロトコルを使用するには、**http** オプションを選択します。
  - 管理サービスと NetScaler インスタンス間の通信に安全なチャネルを使用するには、**https** オプションを選択します。

4. [**SNMP**] で、バージョンを選択します。v2 を選択した場合は、手順 5 に進みます。v3 を選択した場合は、手順 6 に進みます。

5. [SNMP v2] で、SNMP コミュニティ名を追加します。

6. [SNMP v3] で、[セキュリティ名] と [セキュリティレベル] を追加します。

7. [タイムアウト設定] で、値を指定します。

8. [作成] をクリックし、[閉じる] をクリックします。作成した管理者プロファイルが [管理者プロファイル] ペインに表示されます。

[**Default**] 列の値が true の場合、デフォルトのプロファイルは管理者プロファイルになります。値が false の場合、ユーザ定義プロファイルが管理者プロファイルになります。

ユーザー定義の管理者プロファイルを使用しない場合は、Management Service から削除できます。ユーザー定義の管理者プロファイルを削除するには、[**Admin Profiles**] ペインで削除するプロファイルを選択し、[**Delete**] をクリックします。

NetScaler .xva イメージをアップロードする

NetScaler VPX インスタンスを追加するには、.xva ファイルが必要です。

VPX インスタンスをプロビジョニングする前に、NetScaler SDX .xva ファイルを SDX アプライアンスにアップロードします。.xva イメージファイルをバックアップとしてローカルコンピューターにダウンロードすることもできます。.xva イメージファイルフォーマットはNSVPX-XEN-ReleaseNumber-BuildNumber_nc.xva です。

NetScaler XVA ファイルペインでは、次の詳細を表示できます。

- **[名前]:**.xva イメージファイルの名前。ファイル名にはリリースとビルド番号が含まれます。たとえば、ファイル名NSVPX-XEN-12.1-56.22.xva.gzはリリース 12.1 ビルド 56.22 を指します。
- 最終更新日**:**.xva イメージファイルが最後に変更された日付。
- サイズ**:**.xva イメージファイルのサイズ (MB 単位)。

NetScaler.xva ファイルをアップロードするには

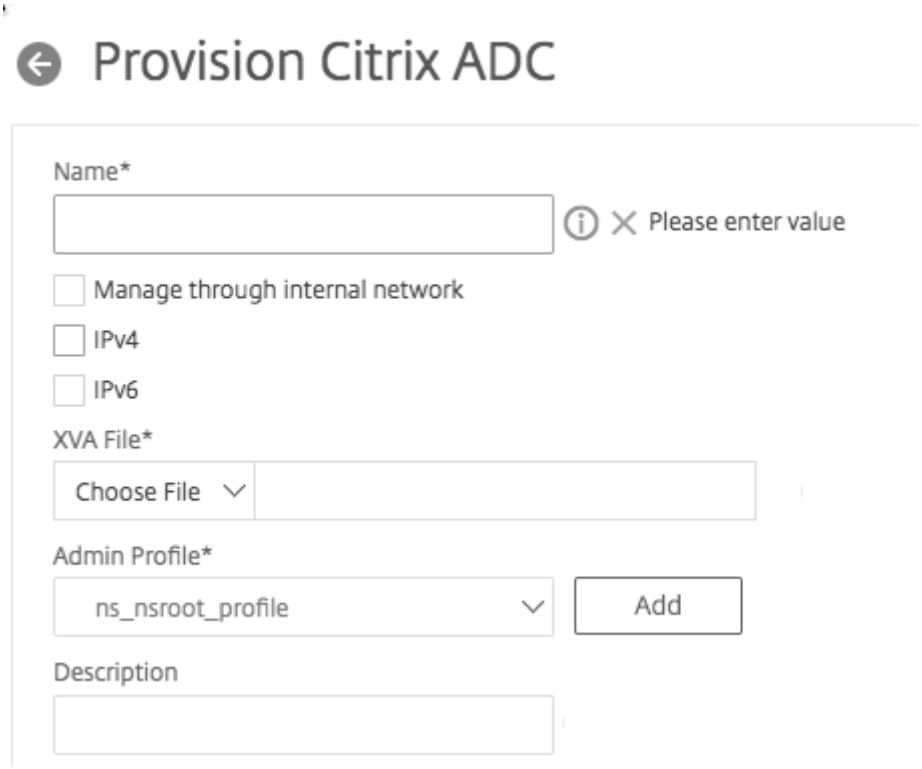
1. ［構成］タブのナビゲーションペインで［**NetScaler** 構成］を展開し、［**XVA** ファイル］をクリックします。
2. **NetScaler XVA** ファイルペインで、［アップロード］をクリックします。
3. ［インスタンス **XVA** のアップロード］ダイアログボックスで［参照］をクリックし、アップロードする XVA イメージファイルを選択します。
4. ［アップロード］をクリックします。XVA イメージファイルは、アップロード後に **NetScaler ADC XVA** ファイルペインに表示されます。

NetScaler .xva ファイルをダウンロードしてバックアップを作成するには

1. ［**NetScaler** ビルドファイル］ペインで、ダウンロードするファイルを選択し、［ダウンロード］をクリックします。
2. [ファイルのダウンロード] メッセージボックスで、[保存] をクリックします。
3. [名前を付けて保存] メッセージボックスで、ファイルを保存する場所を参照し、[保存] をクリックします。

NetScaler インスタンスを追加する

管理サービスから NetScaler インスタンスを追加する場合、一部のパラメーターに値を指定する必要があります。管理サービスは、NetScaler インスタンスでこれらの設定を暗黙的に構成します。



- 名前:NetScaler インスタンスに名前を割り当てます。
- SDX Management Service と VPX インスタンス間の独立した内部常時接続を有効にするには、内部ネットワーク経由で管理を選択します。この機能は、SDX アプライアンスで実行されている 13.0-36.27 以降のバージョンの VPX インスタンスでサポートされています。
- 管理目的で NetScaler VPX インスタンスにアクセスするには、IPv4 アドレスまたは IPv6 アドレス、または IPv4 アドレスと IPv6 アドレスの両方を選択します。NetScaler インスタンスは 1 つの管理 IP（NSIP）のみを持つことができます。NSIP アドレスは削除できません。
- IP アドレスのネットマスク、デフォルトゲートウェイ、ネクストホップを管理サービスに割り当てます。
- VPX がバージョン 13.0—88.9 または 13.1—37.8、およびそれら以降のバージョンでプロビジョニングされている場合、次のいずれかの条件下では、ゲートウェイフィールドと **Nexhopto Management Service** フィールドはオプションです。
  - 内部ネットワーク経由で管理が有効になっている場合。
  - 設定された IPv4 アドレスが管理サービス IP アドレスと同じサブネットにある場合。

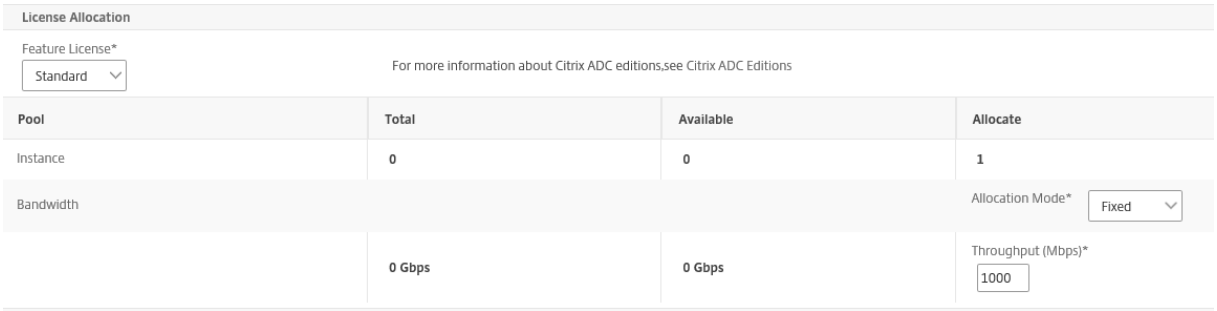
次に、XVA ファイル、管理者プロファイル、およびインスタンスの説明を追加します。

注：高可用性セットアップ（アクティブ/アクティブまたはアクティブ/スタンバイ）では、2 つの NetScaler ADC VPX インスタンスを異なる SDX アプライアンスに構成することをお勧めします。セットアップ内のインスタンスに、CPU、メモリ、インターフェイス、1 秒あたりのパケット数 (PPS)、スループットなどのリソースが同じであることを確認します。

ライセンスの割り当て

このセクションでは、NetScaler 用に取得したライセンスを指定します。ライセンスは、スタンダード、エンタープライズ、プラチナです。

注**:** アスタリスクは必須フィールドを示します。



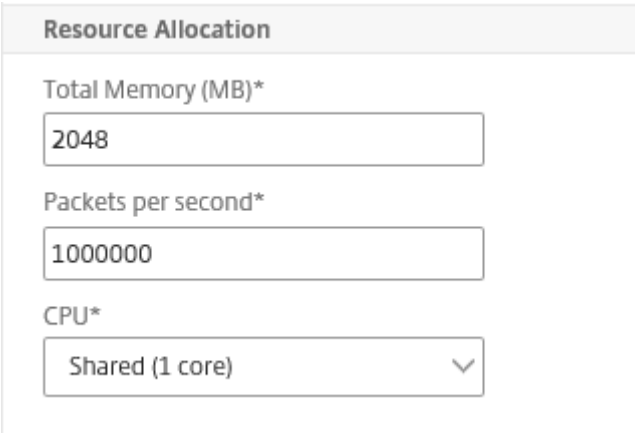
帯域幅のバースト機能が必要な場合は、「割り当てモード」で「バースブル」を選択します。詳しくは、SDX での帯域幅メータリングを参照してください。

暗号配分

リリース 12.1 48.13 から、暗号キャパシティを管理するインターフェイスが変更されました。詳しくは、「暗号容量の管理」を参照してください。

資源配分

[リソース割り当て] で、合計メモリ、1 秒あたりのパケット数、および CPU を割り当てます。



CPU

専用コア (1 つまたは複数) をインスタンスに割り当てるか、インスタンスが他のインスタンスとコアを共有します。[shared] を選択すると、1 つのコアがインスタンスに割り当てられますが、リソースが不足している場合はコアが他のインスタンスと共有されることがあります。CPU コアが再割り当てされた場合、影響を受けるインスタンスを再起動します。パフォーマンスの低下を避けるため、CPU コアが再割り当てされているインスタンスを再起動します。

SDX リリース 11.1.x.x (MR4) から、SDX 25000xx プラットフォームを使用している場合、インスタンスに最大 16 個のコアを割り当てることができます。また、SDX 2500xxx プラットフォームを使用している場合は、インスタンスには最大 11 個のコアを割り当てることができます。

注**:** インスタンスの場合、設定する最大スループットは 180 Gbps です。

次の表に、サポートされている VPX、単一バンドルイメージのバージョン、およびインスタンスに割り当てることができるコアの数を示します。

プラットフォーム名	総コア数	VPX プロビジョニングで使用可能なコアの合計	1 つのインスタンスに割り当て可能な最大コア数
SDX 8015、SDX 8400、SDX 8600	4	3	3
SDX 8900	8	7	7
SDX 11500、SDX 13500、SDX 14500、SDX 16500、SDX 18500、SDX 20500	12	10	5
SDX 11515、SDX 11520、SDX 11530、SDX 11540、SDX 11540、SDX 11542	12	10	5
SDX 17500、SDX 19500、SDX 21500	12	10	5

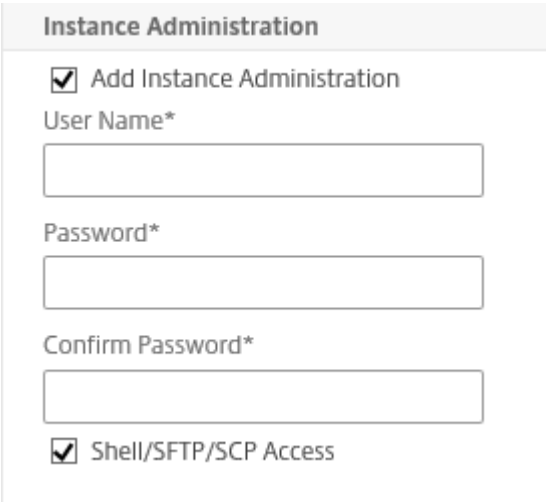
プラットフォーム名	総コア数	VPX プロビジョニングで使用可能なコアの合計	1 つのインスタンスに割り当て可能な最大コア数
SDX 17550、SDX 19550、SDX 20550、SDX 21550	12	10	5
SDX 14020、SDX 14030、SDX 14040、SDX 14060、SDX 14080、SDX 14100	12	10	5
SDX 22040、SDX 22060、SDX 22080、SDX 22100、SDX 22120	16	14	7
SDX 24100 と SDX 24150	16	14	7
SDX 14020 40G, SDX 14030 40G, SDX 14040 40G, SDX 14060 40G, SDX 14080 40G, and SDX 14100 40G	12	10	10
SDX 14020 FIPS, SDX 14030 FIPS, SDX 14040 FIPS, SDX 14060 FIPS, SDX 14080 FIPS, and SDX 14100 FIPS	12	10	5
SDX 14040 40S、SDX 14060 40S、SDX 14080 40S、SDX 14100 40S	12	10	10
SDX 25100A、25160A、25200A	20	18	9
SDX 25100-40G、25160-40G、25200-40G	20	18	16 (バージョンが 11.1-51.x 以上の場合); 9 (バージョンが 11.1-50.x 以下の場合、11.0 および 10.5 のすべてのバージョン)
SDX 26100, 26160, 26200, 26250	28	26	16
SDX 26100-50S, 26160-50S, 26200-50S, 26250-50S	28	26	16

プラットフォーム名	総コア数	VPX プロビジョニングで使用可能なコアの合計	1 つのインスタンスに割り当て可能な最大コア数
SDX 26100-100G, 26160-100G, 26200-100G, 26250-100G	28	26	25
SDX 15000	16	14	14
SDX 15000-50G	16	14	14
SDX 9100	10	9	9
SDX 16000	32	30	16

> 注:
>
> 専用コアは、インスタンスで実行されているパケットエンジンの数に対応します。専用コアで作成された VPX インスタンスには、管理用に追加の CPU が割り当てられます。

インスタンス管理

VPX インスタンスの管理者ユーザーを作成するには、**[**インスタンス管理**]** の **[**** インスタンス管理の追加] を選択します。**



次の詳細を追加します。

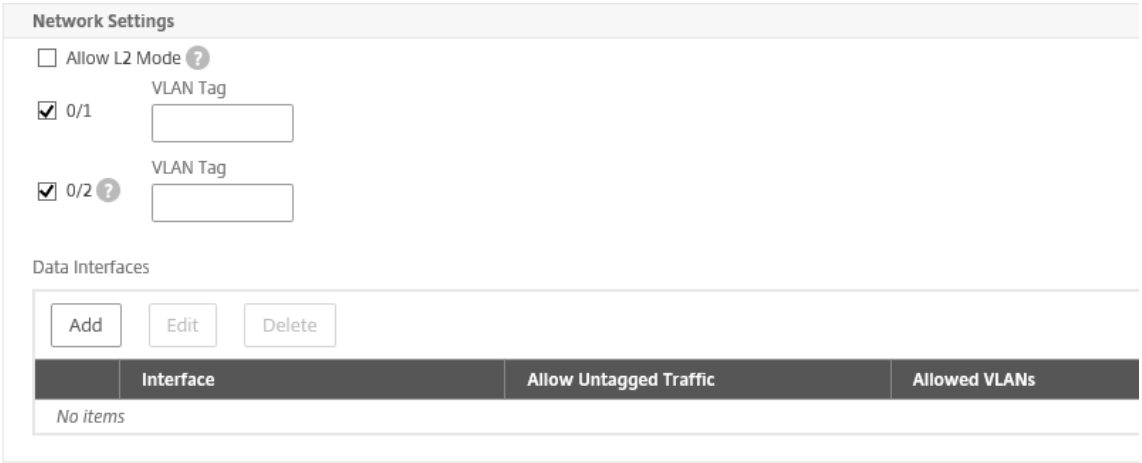
ユーザー名**:** NetScaler インスタンス管理者のユーザー名。このユーザはスーパーユーザアクセスできますが、VLAN およびインターフェイスを設定するためのネットワークコマンドへのアクセス権がありません。

パスワード**:** ユーザー名のパスワード。

シェル/**Sftp/Scp** アクセス:**NetScaler** インスタンス管理者に許可されているアクセスです。このオプションはデフォルトで選択されています。

ネットワーク設定

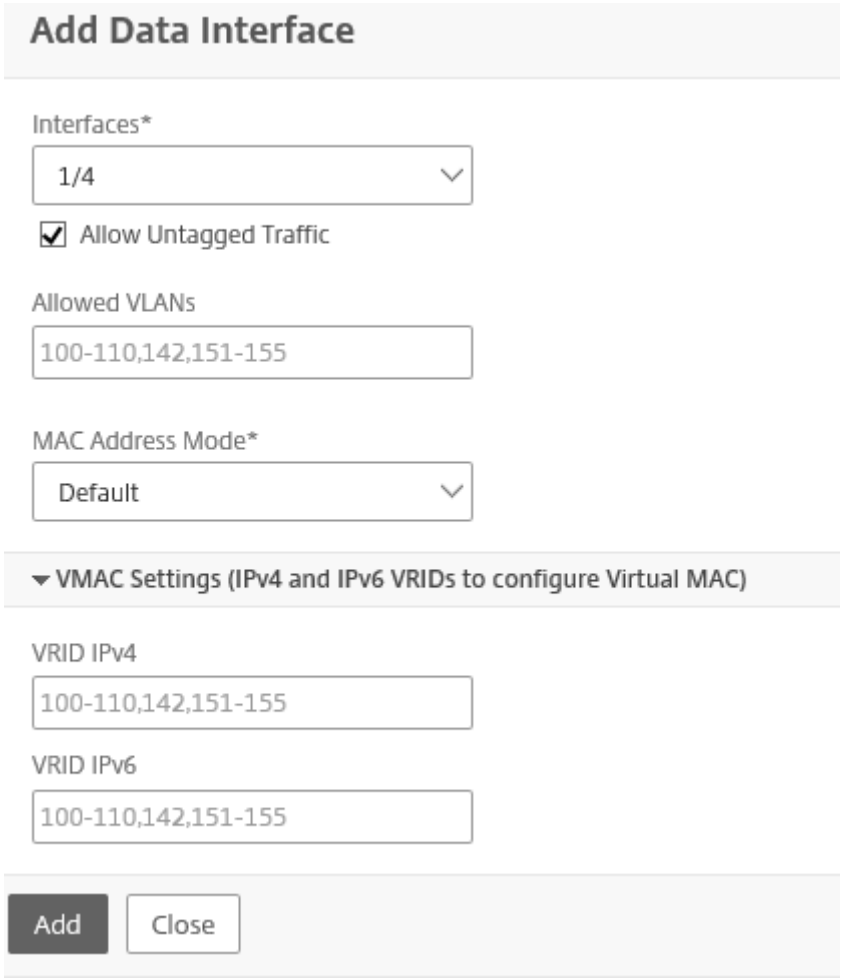
- **L2** モードを許可**:** NetScaler インスタンスで L2 モードを許可できます。[ネットワーク設定] で [**L2** モードを許可] を選択します。インスタンスにログオンし、L2 モードを有効にする前に。詳しくは、「NetScaler インスタンスでの L2 モードの許可」を参照してください。



> 注:
>
> - Management Service からインスタンスの L2 モードを無効にする場合は、インスタンスにログオンし、そのインスタンスから L2 モードを無効にする必要があります。これを行わないと、インスタンスの再起動後に他の NetScaler ADC モードがすべて無効になる場合があります。
> - ADC インスタンスが SDX にプロビジョニングされた後は、ADC インスタンスからインターフェイスまたはチャネルを削除することはできません。ただし、ADC インスタンスにインターフェースまたはチャンネルを追加することはできます。

- インターフェイス **0/1** と **0/2:** デフォルトでは、インターフェイス 0/1 と 0/2 が管理 LA 用に選択されます。
- **VLAN** タグ**:** 管理インターフェイスの VLAN ID を指定します。次に、データインターフェイスを追加します。

> 注意:
>
> インスタンスに追加するインターフェイスのインターフェイス ID は、必ずしも SDX アプライアンスの物理インターフェイス番号と一致するわけではありません。インスタンス 1 に関連付ける最初のインターフェイスがインターフェイス 1/4 の場合、インスタンスのインターフェイス設定を表示すると、インターフェイス 1/1 として表示されます。インスタンス 1 に関連付けた最初のインターフェイスであるため、番号付けが変わります。



- タグなしトラフィックを許可:［タグなしトラフィックを許可］チェックボックスをオンにすると、NetScaler インスタンスがタグなしトラフィックを処理できるようになります。

  > 注:
  >
  > **SDX** アプライアンスのバージョンが **13.1-24.x** 以降で、**NetScaler** インスタンスのバージョンが **13.1**～**24.x** より前の場合、［タグなしトラフィックを許可する］チェックボックスがオフになっていても、**ADC** インスタンスは **Mellanox** インターフェイスでタグなしトラフィックを処理します。

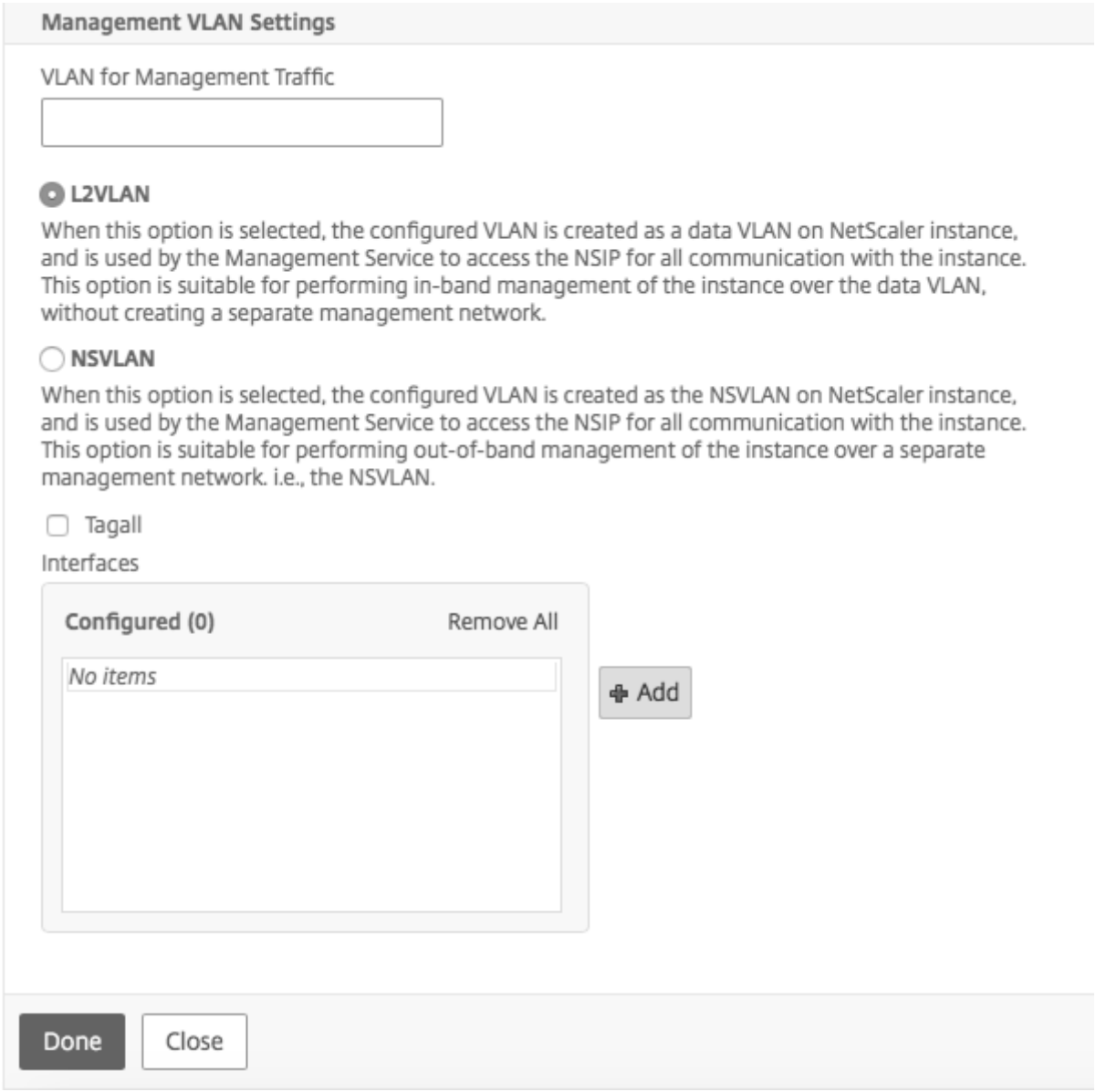
- 許可される **VLAN:** NetScaler インスタンスに関連付けることができる VLAN ID のリストを指定します。
- **MAC** アドレスモード**:** MAC アドレスを割り当てます。次のいずれかのオプションを選択します:
  - デフォルト: Citrix Hypervisor は MAC アドレスを割り当てます。
  - [**Custom**]: 生成された MAC アドレスを上書きする MAC アドレスを指定するには、このモードを選択します。
  - 生成**:** 以前に設定したベース **MAC** アドレスを使用して **MAC** アドレスを生成します。ベース MAC アドレスの設定については、インターフェイスへの MAC アドレスの割り当てを参照してください。
- VMAC 設定（仮想 MAC を設定するための IPv4 および IPv6 VRID）

- **VRID IPv4:** VMAC を識別する IPv4 VRID。可能な値:1 ～255 詳細については、「インターフェイスでの VMC の設定」を参照してください。
- **VRID IPV6:** VMAC を識別する IPv6 VRID。可能な値:1 ～255 詳細については、「インターフェイスでの VMC の設定」を参照してください。

管理 **VLAN** 設定

通常、VPX インスタンスの管理サービスと管理アドレス (NSIP) は同じサブネットワーク内にあり、通信は管理インターフェイスを介して行われます。ただし、管理サービスとインスタンスが異なるサブネットワークにある場合、VPX インスタンスのプロビジョニング時に VLAN ID を指定する必要があります。この ID は、起動時にネットワーク経由でインスタンスに到達できるようにするために必要です。VPX インスタンスのプロビジョニング時に選択したインターフェイスからのみ NSIP にアクセスできるようにする必要がある場合は、NSVLAN オプションを選択します。

NSVLAN オプションを選択した場合、NetScaler インスタンスをプロビジョニングした後にこの設定を変更することはできません。



注:

- HA ハートビートは、NSVLAN の一部であるインターフェイスだけで送信されます。
- NSVLAN は、VPX XVA ビルド 9.3 53.4 以降からのみ設定できます。

重要**:** NSVLAN が選択されていない場合は、VPX インスタンスで「clear config full」コマンドを実行すると、VLAN 構成が削除されます。

[完了] をクリックして、NetScaler VPX アプライアンスをプロビジョニングします。

NetScaler インスタンスを変更する

プロビジョニングされた **ADC** インスタンスのパラメーター値を変更するには、NetScaler インスタンスペインで変更するインスタンスを選択し、「変更」をクリックします。[Modify ADC ウィザード] で、パラメータを変更します。

注意事項**:**

- SSL チップの数、インターフェイス、メモリ、機能ライセンスなどのパラメーターを変更すると、NetScaler インスタンスは暗黙的に停止して再起動し、これらのパラメーターを有効にします。
- [イメージ] パラメータと [ユーザ名] パラメータは変更できません。
- インターフェースやチャンネルを ADC インスタンスから削除することはできません。ただし、新しいインターフェースやチャンネルを ADC インスタンスに追加することはできます。
- **SDX** アプライアンスにプロビジョニングされた **ADC** インスタンスを削除するには、NetScaler インスタンスペインで削除するインスタンスを選択し、「削除」をクリックします。［確認］メッセージボックスで［はい］をクリックして NetScaler ADC インスタンスを削除します。

VLAN を特定の仮想インターフェイスに制限する

SDX アプライアンス管理者は、NetScaler インスタンスに関連付けられた仮想インターフェイスに特定の 802.1Q VLAN を強制できます。この機能は、インスタンス管理者による 802.1Q VLAN の使用を制限する場合に特に役立ちます。2 つの異なる会社に属する 2 つのインスタンスが 1 つの SDX アプライアンスでホストされている場合、2 つの会社が同じ VLAN ID を使用しないように制限できます。そうすることで、ある会社が他方の会社のトラフィックを見ることができなくなります。インスタンス管理者が 802.1Q VLAN にインターフェイスを割り当てようとすると、指定された VLAN ID が許可リストに含まれていることを確認する検証が実行されます。

デフォルトでは、インターフェイス上では任意の VLAN ID を使用できます。インターフェイス上のタグ付き VLAN を制限するには、NetScaler インスタンスのプロビジョニング時にネットワーク設定で VLAN ID を指定します。また、後でインスタンスを変更して指定することもできます。範囲を指定するには、ID をハイフンで区切ります (10 ～ 12 など)。最初にいくつかの VLAN ID を指定し、あとで許可リストから削除した場合、そのインターフェイスでは任意の VLAN ID を使用できます。これで、デフォルト設定が復元されました。

許可 VLAN のリストを作成すると、SDX 管理者は VLAN を作成するためにインスタンスにログオンする必要がなくなります。管理者は、管理サービスから特定のインスタンスの VLAN を追加および削除できます。

重要：L2 モードが有効になっている場合、管理者は異なるインスタンスの VLAN ID が重複しないように注意する必要があります。

許可された **VLAN ID** を指定するには

1. ADC のプロビジョニングウィザードまたは ADC の変更ウィザードの [ネットワーク設定] ページの [許可された **VLAN**] で、このインターフェイスで許可される 1 つ以上の VLAN ID を指定します。範囲を指定するにはハイフンを使用します。たとえば、2 ～4094 と入力します。

2. ウィザードの手順に従って処理を進めます。
3. [完了] をクリックし、[閉じる] をクリックします。

管理サービスからインスタンスの **VLAN** を設定するには

1. [構成] タブで、[NetScaler] > [インスタンス] に移動します。
2. インスタンスを選択し、[**VLAN**] をクリックします。
3. 詳細ペインで、[追加] をクリックします。
4. [**NetScaler VLAN** の作成] ダイアログボックスで、次のパラメーターを指定します。
   - VLAN ID：特定のフレームが属する VLAN を一意に識別する整数。NetScaler 最大 4094 個の VLAN をサポートします。ID 1 はデフォルト VLAN 用に予約されています。
   - IPV6 ダイナミックルーティング：この VLAN 上のすべての IPv6 ダイナミックルーティングプロトコルを有効にします。注: **ENABLED** 設定を機能させるには、インスタンスにログオンし、VTYSH コマンドラインから IPv6 動的ルーティングプロトコルを設定する必要があります。
5. VLAN に含める必要があるインターフェイスを選択します。
6. [作成] をクリックし、[閉じる] をクリックします。

暗号容量の管理

November 23, 2023

リリース 12.1 48.13 から、暗号キャパシティを管理するインターフェイスが変更されました。管理サービスは、NetScaler SDX アプライアンスの SSL 容量を示す非対称暗号ユニット（ACU)、対称暗号ユニット（SCU)、および暗号仮想インターフェイスを提供します。以前の暗号容量は、SSL チップ、SSL コア、および SSL 仮想機能の単位で割り当てられていました。レガシー SSL チップが ACU および SCU ユニットにどのように変換されるかについての詳細は、レガシー SSL チップから ACU および SCU への変換表を参照してください 。

管理サービス GUI を使用すると、暗号容量を ACU と SCU の単位で NetScaler VPX インスタンスに割り当てることができます。

次の表に、ACU、SCU、および暗号仮想インスタンスに関する簡単な説明を示します。

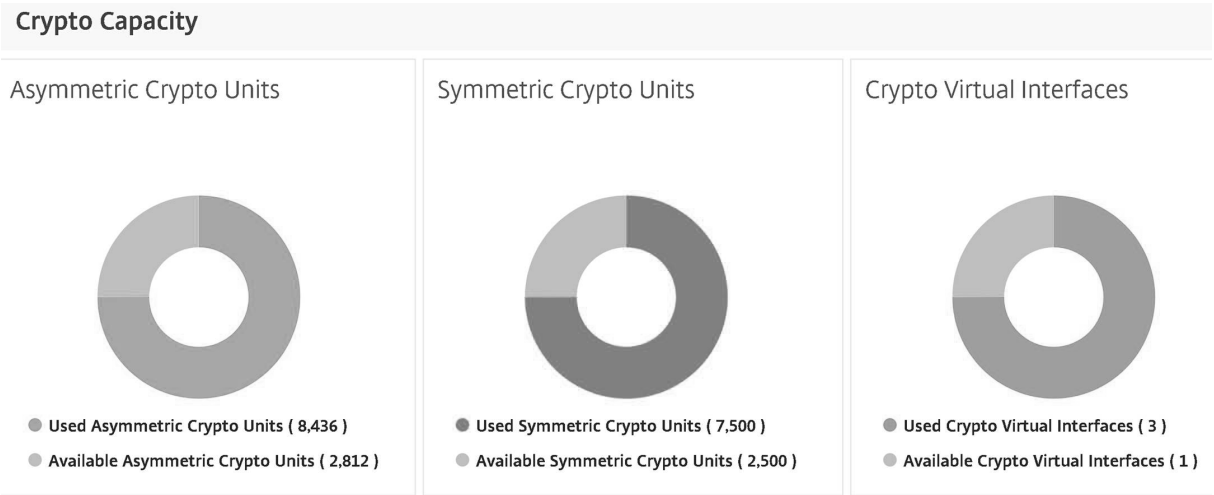
テーブル。単位暗号単位

新しい暗号ユニット	説明
非対称暗号ユニット (ACU)	1 ACU = (RSA) 2 K (2048 ビットキーサイズ) の復号化の 1 秒あたり 1 オペレーション (ops)。詳細については、ACU から PKE へのリソース変換表を参照してください。

新しい暗号ユニット	説明
対称暗号ユニット (SCU)	1 SCU = 1 Mbps の AES-128-CBC + SHA256-HMAC @ 1024B。この定義は、すべての SDX プラットフォームに適用できます。
暗号仮想インターフェイス	仮想関数とも呼ばれる暗号仮想インターフェイスは、SSL ハードウェアの基本単位を表します。これらのインターフェースを使い切ると、SSL ハードウェアを VPX インスタンスに割り当てることができなくなります。暗号仮想インターフェイスは読み取り専用エンティティであり、SDX アプライアンスはこれらのエンティティを自動的に割り当てます。

SDX アプライアンスの暗号容量を表示する

SDX GUI のダッシュボードで SDX アプライアンスの暗号容量を表示できます。ダッシュボードには、SDX アプライアンスで使用されている ACU、SCU、および仮想インターフェイスと使用可能な ACU が表示されます。暗号容量を表示するには、[ダッシュボード**] > [**暗号容量] に移動します。



VPX インスタンスのプロビジョニング中に暗号容量を割り当てる

SDX アプライアンスで **VPX** インスタンスをプロビジョニングする際、**[**暗号割り当て] で、VPX インスタンスに ACU と SCU の数を割り当てることができます。VPX インスタンスをプロビジョニングする手順については、「NetScaler インスタンスの Provisioning」を参照してください。

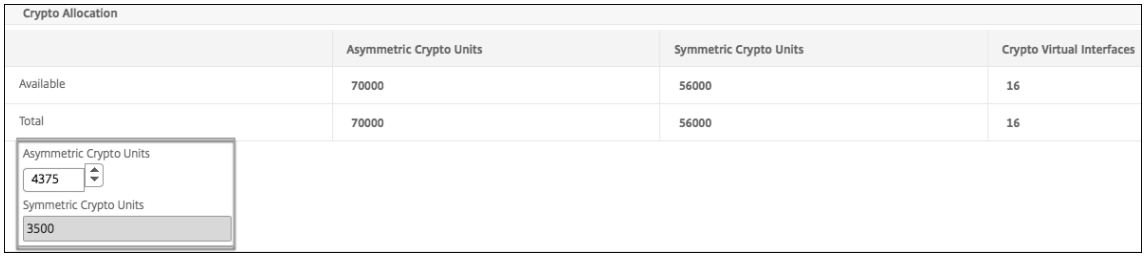
VPX インスタンスのプロビジョニング中に暗号容量を割り当てるには、次の手順に従います。

1. 管理サービスにログオンします。

2. 構成 **> NetScaler >** インスタンスの順に移動し、追加をクリックします。
3. [暗号割り当て（**Crypto Allocation**）] では、使用可能な ACU、SCU、および暗号仮想インターフェイスを表示できます。ACU と SCU の割り当て方法は SDX アプライアンスによって異なります。

   a. さまざまな SDX アプライアンスで使用できる ACU カウンタの最小値にリストされているアプライアンスでは、指定した数の倍数で ACU を割り当てることができます。SCU は自動的に割り当てられ、[SCU 割り当て] フィールドは編集できません。ACU 割り当ては、そのモデルで使用できる最小 ACU の倍数で増やすことができます。たとえば、最小 ACU が 4375 の場合、ACU の増分は 8750、13125 などとなります。

   例。SCU が自動的に割り当てられ、ACU が指定された数の倍数で割り当てられる暗号割り当て。

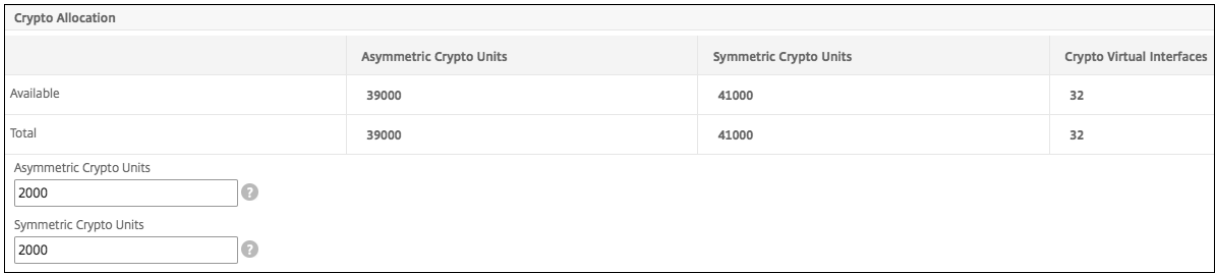


さまざまな **SDX** アプライアンスで使用できる **ACU** カウンタの最小値

SDX プラットフォーム	ACU カウンタの最小値
22040, 22060, 22080, 22100, 22120, 24100, 24150 (36 ポート)	2187
8400, 8600, 8010, 8015	2812
17500, 19500, 21500	2812
17550, 19550, 20550, 21550	2812
11500, 13500, 14500, 16500, 18500, 20500	2812
11515, 11520, 11530, 11540, 11542	4375
14xxx	4375
14xxx 40S	4375
14xxx 40G	4375
14xxx FIPS	4375
25xxx	4375
25xxx	4575

b. 前の表に記載されていないその他の SDX プラットフォームでは、ACU と SCU を自由に割り当てることができます。SDX アプライアンスは、暗号仮想インターフェイスを自動的に割り当てます。

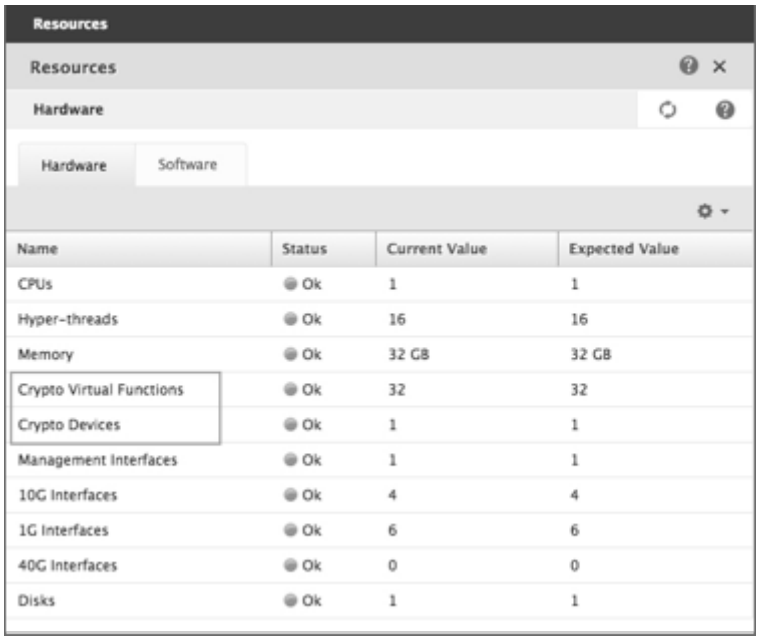
例。ACU と SCU の両方が自由に割り当てられる暗号割り当て



4./ VPX インスタンスのプロビジョニング手順をすべて完了し、[完了] をクリックします。詳しくは、「NetScaler インスタンスの Provisioning」を参照してください。

暗号ハードウェアヘルスの表示

Management Service では、SDX アプライアンスに付属する暗号化ハードウェアの状態を表示できます。暗号化ハードウェアの状態は、暗号化デバイスと暗号仮想関数として表されます。暗号化ハードウェアの状態を表示するには、[ダッシュボード**] > [**リソース] に移動します。



注意事項

SDX アプライアンスを最新バージョンにアップグレードする場合は、次の点に注意してください。

- SDX ユーザーインターフェイスのみがアップグレードされますが、アプライアンスのハードウェア容量は変わりません。
- 暗号の割り当てメカニズムは変わらず、SDX GUI 上の表現だけが変更されます。

- 暗号化インターフェイスには下位互換性があり、NITRO インターフェイスを使用して SDX アプライアンスを管理する既存の自動化メカニズムには影響しません。
- SDX アプライアンスのアップグレード時には、既存の VPX インスタンスに割り当てられている暗号は変更されず、管理サービスでの表示のみが変更されます。

ACU から **PKE** へのリソース変換テーブル

SDX プラットフォーム	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE-ECDSA
22040、22060、22080、22100、22120、24100、24150 (36 ポート)	2187	12497	2187	312	256	190
8400, 8600, 8010, 8015	2812	17000	2812	424	330	-
11515, 11520, 11530, 11540, 11542	4375	25000	4375	625	512	381
22040、22060、22080、22100、22120（24 ポート）	4375	25000	4375	625	512	381
17500, 19500, 21500	2812	17000	2812	424	330	-
17550, 19550, 20550, 21550	2812	17000	2812	424	330	-

SDX プラットフォーム	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE-ECDSA
11500, 13500, 14500, 16500, 18500, 20500	2812	17000	2812	424	330	-
14000, 14000-40G, 25000, 25000A	4375	25000	4375	625	512	381
14000 FIPS	4375	25000	4375	625	512	381
14000-40S	4375	25000	4375	625	512	381
*8900 (8910, 8920, 8930)	1000	4615	1000	136	397	494
*9100 (9110, 9120, 9130)	1000	4615	1000	136	397	494
*26000-100G (26100、26160、26200、26250)	1000	4615	1000	136	397	494
*15000	1000	4615	1000	136	397	494
*15000-50G	1000	4615	1000	136	397	494
*16000	1000	4615	1000	136	397	494
*26000-50S	1000	4615	1000	136	397	494

* これらのプラットフォームでは、PKE 番号は最低保証値です。

ACU から **PKE** へのリソース変換テーブルの読み方

ACU から PKE へのリソース変換テーブルは、次の点に基づいています。

- 管理サービスは、個々の VPX に暗号リソースを割り当てるのに役立ちます。管理サービスでは、パフォーマンスを割り当てたり、約束したりすることはできません。

- 実際のパフォーマンスは、パケットサイズ、使用する暗号/keyex/HMAC (またはそのバリエーション) などによって異なります。

次の例は、ACU を読み取って PKE リソース変換テーブルに適用する方法を理解するのに役立ちます。

例。SDX 22040 プラットフォームの ACU から PKE へのリソース変換

SDX 22040 プラットフォーム上の VPX インスタンスに 2187 個の ACU を割り当てると、256 個の ECDHE-RSA 操作または 2187 個の RSA-2K 操作などに相当する暗号リソースが割り当てられます。

レガシー **SSL** チップから **ACU** および **SCU** への変換テーブル

レガシー SSL チップが ACU および SCU に変換される方法の詳細については、次の表を参照してください。

ACU および SCU 変換テーブル

サードパーティ製仮想マシンのプロビジョニング

November 23, 2023

> 警告:
>
> サードパーティインスタンスのサポートは、バージョン 13.1 ビルド 37.x 以降の NetScaler SDX GUI では廃止されました。それでもサードパーティのインスタンスを使用する場合は、Citrix では以下の操作を行うことをお勧めします。
>
> - 管理サービスシェルにログオンします。
> - `/mpsconfig`ディレクトリにファイル`.thirdPartyVM`を作成します。
> - `svmd restart`コマンドを実行して管理サービスを再起動します。

SDX アプライアンスは、次のサードパーティ製仮想マシン (インスタンス) のプロビジョニングをサポートしています。

- SECUREMATRIX GSB
- InterScan Web Security
- Websense Protector
- BlueCat DNS/DHCP サーバー
- CA アクセスゲートウェイ
- PaloAlto VM シリーズ

SECUREMATRIX GSB は、トークンデバイスを携帯する必要がない、安全性の高いパスワードシステムを提供します。Websense Protector は監視およびブロック機能を提供し、データの損失や機密情報の漏洩を防ぎます。BlueCat DNS/DHCP サーバーは、お客様のネットワークに DNS と DHCP を提供します。NetScaler SDX 上の

PaloAlto VM シリーズを使用すると、高度なセキュリティと ADC 機能を単一のプラットフォームに統合できるため、企業やサービスプロバイダーの顧客によるアプリケーションへの安全で信頼性の高いアクセスが可能になります。NetScaler SDX 上で VM シリーズを組み合わせることで、Citrix Virtual Apps and Desktops の導入環境向けの、完全で検証済みの安全な ADC ソリューションも提供されます。

Management Service から、インスタンスのプロビジョニング、モニタリング、管理、トラブルシューティングを行うことができます。前述のすべてのサードパーティインスタンスは、`SDXTools` デーモンを使用して Management Service と通信します。デーモンはプロビジョニングされたインスタンスにプレインストールされています。新しいバージョンが利用可能になったら、デーモンをアップグレードできます。

サードパーティの仮想マシンを構成すると、チャネルの一部である SR-IOV インターフェイス（1/x および 10/x）はインターフェイスのリストに表示されません。サードパーティの仮想マシンではチャネルがサポートされていないため、インターフェイスがありません。

> 注:
>
> SDX アプライアンスにプロビジョニングできるインスタンスの総数は、アプライアンスにインストールされているライセンスによって異なります。

重要：サードパーティのインスタンスをインストールする前に、Citrix Hypervisor のバージョンを 6.1.0 にアップグレードする必要があります。

SECUREMATRIX GSB

November 23, 2023

SECUREMATRIX は、使いやすくコスト効率に優れた、安全性が高く、トークンレスのワンタイムパスワード (OTP) 認証ソリューションです。マトリクステーブルの位置、シーケンス、イメージパターンの組み合わせを使用して、使い捨てパスワードを生成します。SECUREMATRIX GSB サーバーと SECUREMATRIX 認証サーバーは、VPN/SSL-VPN エンドポイント、クラウドベースのアプリケーションとリソース、デスクトップ/仮想デスクトップログイン、および Web アプリケーション (OTP によるリバースプロキシ) のセキュリティを大幅に強化します。PC、仮想デスクトップ、タブレット、スマートフォンと互換性のあるソリューションを提供します。

ソフトウェアデファインドネットワークで NetScaler SDX マルチテナントプラットフォームアーキテクチャを使用すると、SECUREMATRIX の強力な認証機能を、Web Interface、Citrix Virtual Apps and Desktops、その他認証を必要とする多くのアプリケーションサービスなど、NetScaler を介して提供される他のテナントやクラウドサービスと統合できます。

詳細については、「SECUREMATRIX」を参照してください。

SECUREMATRIX GSB インスタンスをプロビジョニングする

SECUREMATRIX GSB には、SDX アプライアンスの外部で設定する必要がある SECUREMATRIX 認証サーバが必要です。インターフェイスを 1 つだけ選択し、そのインターフェイスにのみネットワーク設定を指定します。

注**:** チャネルの一部である SR-IOV インターフェイス（1/x および 10/x）は、インターフェイスのリストには表示されません。SECUREMATRIX GSB インスタンスではチャネルはサポートされていません。

インスタンスのプロビジョニングを開始する前に、SECUREMATRIX Web サイトから XVA イメージをダウンロードし、SDX アプライアンスにアップロードします。XVA イメージのダウンロードについて詳しくは、SECUREMATRIX Web サイトを参照してください。SDX アプライアンスで管理サービスビルド 118.7 以降を使用していることを確認します。

[構成] タブで、[**SECUREMATRIX GSB] > [**ソフトウェアイメージ] に移動します。

XVA イメージを **SDX** アプライアンスにアップロードするには:

1. 詳細ウィンドウの [**XVA** ファイル**] > [**アクション] で、[アップロード] をクリックします。
2. 表示されるダイアログボックスで「ブラウズ」をクリックし、アップロードする XVA ファイルを選択します。
3. [アップロード] をクリックします。XVA ファイルが XVA ファイルペインに表示されます。

SECUREMATRIX インスタンスをプロビジョニングするには

1. [構成] タブで、[**SECUREMATRIX GSB] > [**インスタンス] に移動します。
2. 詳細ペインで、[追加] をクリックします。
3. **SECUREMATRX GSB** のプロビジョニングウィザードで、画面の指示に従います。
4. [完了] をクリックし、[閉じる] をクリックします。

インスタンスをプロビジョニングしたら、インスタンスにログオンし、詳細設定を実行します。詳細については、SECUREMATRIX の Web サイトを参照してください。

プロビジョニングされた SECUREMATRIX インスタンスの設定を変更するには、[**SECUREMATRIX** インスタンス] ペインで変更するインスタンスを選択し、[変更] をクリックします。SECUREMATRIX GSB の変更ウィザードで、パラメータを変更します。

注**:** インターフェイスパラメータまたはインスタンス名を変更した場合、インスタンスは停止して再起動し、変更を有効にします。

テクニカルサポートに提出する tar アーカイブを生成します。テクニカルサポートファイルの生成については、テクニカルサポート用の Tar アーカイブの生成を参照してください。

SECUREMATRIX GSB インスタンスの設定をバックアップし、後でそのバックアップデータを使用して SDX アプライアンス上のインスタンスの設定を復元します。インスタンスのバックアップと復元の詳細については、「SDX Appliance の設定データのバックアップと復元」を参照してください。

SECUREMATRIX GSB インスタンスを監視する

SDX アプライアンスは、SECUREMATRIX GSB インスタンスのSDXToolsのバージョン、SSH および CRON デーモンの状態、ウェブサーバーの状態などの統計情報を収集します。

SECUREMATRIX GSB インスタンスに関連する統計情報を表示するには、以下を実行します。

1. [**SECUREMATRIX GSB] > [**インスタンス**]** に移動します。
2. 詳細ペインで、インスタンス名の横にある矢印をクリックします。

SECUREMATRIX GSB インスタンスを管理する

SECUREMATRIX GSB インスタンスは、管理サービスから起動、停止、再起動、強制停止、強制再起動できます。

[構成] タブで、[**SECUREMATRIX GSB**] を展開します。

インスタンスを起動、停止、再起動、強制停止、または強制再起動するには**:**

1. インスタンス] をクリックします。
2. 詳細ペインで、操作を実行するインスタンスを選択し、次のいずれかのオプションを選択します。

    - 起動
    - シャットダウン
    - 再起動する
    - 強制シャットダウン
    - 強制再起動

3. 確認メッセージボックスで、「はい」をクリックします。

SECUREMATRIX GSB インスタンス用の **SDX** ツールファイルをアップグレードする

SDXToolsSECUREMATRIX GSB インスタンスで実行されるデーモンは、管理サービスとインスタンス間の通信に使用されます。

SDXToolsのアップグレードでは、ファイルを SDX アプライアンスにアップロードし、インスタンスを選択した後にSDXToolsをアップグレードします。クライアントコンピューターから SDX アプライアンスにSDXToolsファイルをアップロードできます。

SDXTools ファイルをアップロードするには:

1. ナビゲーションペインで、「管理サービス」を展開し、「**SDXTools** ファイル」をクリックします。
2. 詳細ウィンドウの [アクション] リストで、[アップロード] を選択します。
3. **SDXTools** ファイルのアップロードダイアログボックスで、「ブラウズ」をクリックし、ファイルを含むフォルダに移動して、ファイルをダブルクリックします。
4. [アップロード] をクリックします。

SDXTools をアップグレードするには**:**

[構成] タブで、[**SECUREMATRIX GSB**] を展開します。

1. インスタンス] をクリックします。
2. 詳細ペインで、インスタンスを選択します。
3. アクションリストから、「**SDXTools** のアップグレード」を選択します。
4. [**SDxTools** のアップグレード] ダイアログボックスで、ファイルを選択し、[**OK**] をクリックし、[閉じる] をクリックします。

SECUREMATRIX GSB インスタンスをアップグレードおよびダウングレードする

SECUREMATRIX GSB インスタンスのアップグレードプロセスでは、ターゲットビルドのソフトウェアイメージを SDX アプライアンスにアップロードしてから、インスタンスをアップグレードします。ダウングレードすると、以前のバージョンのインスタンスがロードされます。

[構成] タブで、[**SECUREMATRIX GSB**] を展開します。

ソフトウェアイメージをアップロードするには**:**

1. [ソフトウェアイメージ] をクリックします。
2. 詳細ウィンドウの [アクション] リストで、[アップロード] を選択します。
3. ダイアログボックスで [参照] をクリックし、ビルドファイルが格納されているフォルダにナビゲートし、ビルドファイルをダブルクリックします。
4. [アップロード] をクリックします。

インスタンスをアップグレードするには:

1. インスタンス] をクリックします。
2. 詳細ペインで、インスタンスを選択します。
3. [アクション] リストから [アップグレード] を選択します。
4. 表示されたダイアログボックスで、ファイルを選択し、「**OK**」、「閉じる」の順にクリックします。

インスタンスをダウングレードするには:

1. インスタンス] をクリックします。
2. 詳細ペインで、インスタンスを選択します。
3. [アクション] リストから [ダウングレード] を選択します。
4. 確認メッセージボックスで、「はい」をクリックします。

SECUREMATRIX GSB インスタンスのトラブルシューティング

管理サービスから SECUREMATRIX GSB インスタンスに ping を実行して、デバイスが到達可能かどうかを確認します。Management Service からインスタンスへのパケットのルートをトレースして、インスタンスに到達するまでのホップ数を判断できます。

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表示します。再検出中、管理サービスは SDX アプライアンス上で実行されている SECUREMATRIX GSB の構成とバージョンをフェッチします。デフォルトでは、管理サービスは 30 分に 1 回インスタンスの再検出をスケジュールします。

[構成] タブで、[**SECUREMATRIX GSB**] を展開します。

インスタンスに **ping** を実行するには、以下を実行します。

1. インスタンス] をクリックします。
2. 詳細ウィンドウで ping するインスタンスを選択し、[アクション] リストから [**Ping**] をクリックします。Pingmessage ボックスに ping が成功したかどうかが表示されます。

インスタンスのルートをトレースするには:

1. インスタンス] をクリックします。
2. 詳細ウィンドウで、ルートをトレースするインスタンスを選択し、[アクション] リストから [**traceRoute**] をクリックします。Traceroute メッセージボックスには、インスタンスへのルートが表示されます。

インスタンスを再検出するには**:**

1. インスタンス] をクリックします。
2. 詳細ペインで、再検出するインスタンスを選択し、アクションリストから [再検出] をクリックします。
3. 確認メッセージボックスで、「はい」をクリックします。

Trend Micro の InterScan Web Security

November 23, 2023

Trend Micro の InterScan Web Security は、インターネットゲートウェイで従来の脅威や新たな Web 脅威から動的に保護するソフトウェア仮想アプライアンスです。アプリケーション制御、マルウェア対策スキャン、リアルタイム Web レピュテーション、柔軟な URL フィルタリング、高度な脅威対策が統合されています。その結果、ネットワーク上で増え続けるクラウドベースのアプリケーションに対する優れた保護と、より優れた可視性と制御が実現します。リアルタイムのレポート作成と一元管理により、管理者はプロアクティブな意思決定ツールとなり、その場でリスク管理を行うことができます。

InterScan Web Security:

- エンドユーザーのインターネットアクティビティをより詳細に可視化
- 管理を一元化して最大限の管理を実現
- Web の使用を発生時に監視
- オンザスポットでの修復を実現
- アプライアンスの無秩序な増加と電力コストを削減
- データ損失保護とサンドボックス実行分析をオプションで提供

InterScan Web Security インスタンスをプロビジョニングする前に、Trend Micro の Web サイトから XVA イメージをダウンロードする必要があります。XVA イメージをダウンロードしたら、NetScaler SDX アプライアンスにアップロードします。

注**:** チャネルの一部である SR-IOV インターフェイス（1/x および 10/x）は、インターフェイスのリストには表示されません。InterScan Web Security インスタンスでは、チャネルはサポートされていません。

XVA イメージを **SDX** アプライアンスにアップロードするには:

1. [構成] タブで、**Trend Micro IWSVA > [**ソフトウェアイメージ] の順に移動します。
2. 詳細ウィンドウの [**XVA** ファイル] タブで、[アップロード] をクリックします。
3. 表示されるダイアログボックスで「ブラウズ」をクリックし、アップロードする XVA ファイルを選択します。
4. ［アップロード］をクリックします。XVA ファイルが XVA ファイルペインに表示されます。

Trend Micro IWSVA インスタンスをプロビジョニングするには**:**

1. [構成] タブで、**Trend Micro IWSVA > [**インスタンス] に移動します。
2. 詳細ペインで、[追加] をクリックします。
3. **Trend Micro IWSVA** のプロビジョニングウィザードで、画面の指示に従います。
4. 「**OK**」をクリックし、「閉じる」をクリックします。

インスタンスをプロビジョニングしたら、インスタンスにログオンして詳細設定を実行します。

プロビジョニングされたインスタンスのパラメーターの値を変更するには、詳細ペインで変更するインスタンスを選択し、[**Edit**] をクリックします。**Trend Micro IWSVA** の変更ウィザードで、ご使用の環境に適した値にパラメータを設定します。

Websense Protector

November 23, 2023

Websense (現在 Forcepoint と呼ばれる) データセキュリティプロテクタは、アウトバウンド HTTP トラフィック (ポスト) をインターセプトする仮想マシンです。その後、トラフィックを分析して、Web 上でのデータ損失や機密データの漏洩を防ぎます。プロテクタは、DLP ポリシー情報のために専用の Windows サーバと通信し、一致が検出された場合にデータがポストされるのを監視またはブロックできます。コンテンツ分析はボックス上で実行されるため、このプロセス中に機密データが保護装置から送信されることはありません。

プロテクタのデータ損失防止 (DLP) 機能を使用するには、次の操作を行います。

- Websense データセキュリティを購入してインストールする
- データセキュリティマネージャーで Web DLP ポリシーを構成する
- 管理サービスを通じて初期設定を行います。

詳細については、Websense Protector Web サイトを参照してください。

Websense Protector インスタンスをプロビジョニングする

Websense© Protector には、SDX アプライアンスの外部で設定する必要があるデータセキュリティ管理サーバが必要です。1 つの管理インターフェイスと 2 つのデータインターフェイスを選択してください。データインターフェイスでは、[Allow L2 Mode] を選択する必要があります。Websense Protector の管理ネットワークを介してデータセキュリティ管理サーバにアクセスできることを確認します。[ネームサーバー] に、このプロテクターを提供するドメインネームサーバー (DNS) の IP アドレスを入力します。

注**:** チャネルの一部である SR-IOV インターフェイス（1/x および 10/x）は、インターフェイスのリストには表示されません。チャネルは Websense プロテクタインスタンスではサポートされていません。

インスタンスのプロビジョニングを開始する前に、Websense Web サイトからプロテクタイメージをダウンロードして SDX アプライアンスにアップロードします。プロテクターイメージのダウンロードの詳細については、[Websense Web サイト] を参照してください。SDX アプライアンスで管理サービスビルド 118.7 以降を使用していることを確認します。

[構成] タブで、[**Websense Protector] > [**ソフトウェアイメージ] に移動します。

XVA イメージを **SDX** アプライアンスにアップロードするには

1. 詳細ウィンドウの [**XVA** ファイル**] > [**アクション] で、[アップロード] をクリックします。
2. 表示されるダイアログボックスで「ブラウズ」をクリックし、アップロードする XVA ファイルを選択します。
3. ［アップロード］をクリックします。XVA ファイルが XVA ファイルペインに表示されます。

Websense Protector インスタンスをプロビジョニングするには

1. [構成] タブで、[**Websense Protector] > [**インスタンス] に移動します。
2. 詳細ペインで、[追加] をクリックします。
3. **Websense Protector** のプロビジョニングウィザードで、画面の指示に従います。
4. [完了] をクリックし、[閉じる] をクリックします。

インスタンスをプロビジョニングしたら、インスタンスにログオンし、詳細設定を実行します。

プロビジョニングされた Websense Protector インスタンスの設定を変更するには、[Websense Protector インスタンス] ペインで変更するインスタンスを選択し、[変更] をクリックします。[Websense Protector の変更] ウィザードで、パラメータを設定します。Websense インスタンスのプロビジョニング時に選択したインターフェイスは変更しないでください。XVA ファイルは、インスタンスを削除して新しいインスタンスをプロビジョニングした後にのみ変更できます。

テクニカルサポートに提出する tar アーカイブを生成できます。テクニカルサポートファイルの生成については、テクニカルサポート用の Tar アーカイブの生成を参照してください。

Websense Protector インスタンスを監視する

SDX アプライアンスは、SDXToolsのバージョン、Websense© Data Security ポリシーエンジンのステータス、データセキュリティプロキシのステータスなどの統計情報を収集します。

Websense プロテクタインスタンスに関連する統計情報を表示するには、次の手順を実行します。

1. **Websense Protector >** インスタンスに移動します。
2. 詳細ペインで、インスタンス名の横にある矢印をクリックします。

Websense Protector インスタンスを管理する

Websense© protector インスタンスの起動、停止、再起動、強制停止、強制再起動は、管理サービスから実行できます。

[構成] タブで [**Websense Protector**] を展開します。

Websense Protector インスタンスを起動、停止、再起動、強制停止、強制再起動するには

1. インスタンス] をクリックします。
2. 詳細ペインで、操作を実行するインスタンスを選択し、次のいずれかのオプションを選択します。
   - 起動
   - シャットダウン
   - 再起動する
   - 強制シャットダウン
   - 強制再起動
3. 確認メッセージボックスで、「はい」をクリックします。

Websense Protector インスタンスの **SDX** ツールファイルをアップグレードする

SDXToolsは、サードパーティインスタンスで実行されるデーモンで、Management Service とサードパーティインスタンス間の通信に使用されます。

SDXToolsのアップグレードでは、ファイルを SDX アプライアンスにアップロードし、インスタンスを選択した後にSDXToolsをアップグレードします。クライアントコンピューターから SDX アプライアンスにSDXToolsファイルをアップロードできます。

SDX Tools ファイルをアップロードするには

1. ナビゲーションペインで、「管理サービス」を展開し、「**SDXTools** ファイル」をクリックします。

2. 詳細ウィンドウの [アクション] リストで、[アップロード] を選択します。
3. **SDXTools** ファイルのアップロードダイアログボックスで、「ブラウズ」をクリックし、ファイルを含むフォルダに移動して、ファイルをダブルクリックします。
4. [アップロード] をクリックします。

SDX ツールをアップグレードするには

[構成] タブで [
Websense Protector] を展開します。

1. インスタンス] をクリックします。
2. 詳細ペインで、インスタンスを選択します。
3. アクションリストから、「**SDXTools** のアップグレード」を選択します。
4. [**SDxTools** のアップグレード] ダイアログボックスで、ファイルを選択し、[**OK**] をクリックし、[閉じる] をクリックします。

Websense Protector インスタンスを新しいバージョンにアップグレードする

Websense© protector インスタンスのアップグレードプロセスでは、ターゲットビルドのソフトウェアイメージを SDX アプライアンスにアップロードしてから、インスタンスをアップグレードします。

[構成] タブで [**Websense Protector**] を展開します。

ソフトウェアイメージをアップロードするには

1. [ソフトウェアイメージ] をクリックします。
2. 詳細ウィンドウの [アクション] リストで、[アップロード] を選択します。
3. ダイアログボックスで [参照] をクリックし、ビルドファイルが格納されているフォルダにナビゲートし、ビルドファイルをダブルクリックします。
4. [アップロード] をクリックします。

インスタンスをアップグレードするには

1. インスタンス] をクリックします。
2. 詳細ペインで、インスタンスを選択します。
3. [アクション] リストから [アップグレード] を選択します。
4. 表示されたダイアログボックスで、ファイルを選択し、「**OK**」、「閉じる」の順にクリックします。

Websense Protector インスタンスのトラブルシューティング

管理サービスから Websense Protector インスタンスに ping を実行して、デバイスが到達可能かどうかを確認します。Management Service からインスタンスへのパケットのルートをトレースして、インスタンスに到達するまでのホップ数を判断できます。

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表示します。再検出時に、管理サービスは SDX アプライアンスで実行されている Websense Protector の構成とバージョンをフェッチします。デフォルトでは、管理サービスは 30 分に 1 回インスタンスの再検出をスケジュールします。

[構成] タブで [**Websense Protector**] を展開します。

インスタンスに **ping** を実行するには

1. インスタンス] をクリックします。
2. 詳細ウィンドウで ping するインスタンスを選択し、[アクション] リストから [**Ping**] をクリックします。Pingmessage ボックスに ping が成功したかどうかが表示されます。

インスタンスのルートをトレースするには

1. インスタンス] をクリックします。
2. 詳細ウィンドウで、ルートをトレースするインスタンスを選択し、[アクション] リストから [**traceRoute**] をクリックします。Traceroute メッセージボックスには、インスタンスへのルートが表示されます。

インスタンスを再検出するには

1. インスタンス] をクリックします。
2. 詳細ペインで、再検出するインスタンスを選択し、アクションリストから [再検出] をクリックします。
3. 確認メッセージボックスで、「はい」をクリックします。

BlueCat DNS/DHCP

November 23, 2023

BlueCat DNS/DHCP サーバー ™ は、NetScaler SDX アプライアンスによってサポートされているソフトウェアソリューションです。NetScaler SDX プラットフォームでホストされているため、追加の管理コストやデータセンターのスペースを発生させることなく、信頼性が高くスケーラブルで安全な DNS および DHCP コアネットワークサービスを提供できます。重要な DNS サービスは、ハードウェアを追加することなく、1 つのシステム内の複数の DNS ノード間、または複数の SDX アプライアンス間で負荷分散できます。

BlueCat DNS/DHCP Server™ の仮想インスタンスを SDX でホストすることで、モバイルデバイス、アプリケーション、仮想環境、クラウドをよりスマートに接続できます。

BlueCat と Citrix の詳細については、BlueCat の Web サイト（https://citrixready.citrix.com/bluecat-networks.html）を参照してください。

BlueCat をすでにお使いの場合は、https://care.bluecatnetworks.com/の BlueCat サポートポータルからソフトウェアとドキュメントをダウンロードできます。

BlueCat DNS/DHCP インスタンスのプロビジョニング

BlueCat カスタマーケア（https://care.bluecatnetworks.com）から XVA イメージをダウンロードします。XVA イメージをダウンロードしたら、インスタンスのプロビジョニングを開始する前に SDX アプライアンスにアップロードします。SDX アプライアンスで管理サービスビルド 118.7 以降を使用していることを確認します。

BlueCat DNS/DHCP VM では、0/1 および 0/2 インターフェイスにまたがる管理チャネルがサポートされています。詳しくは、「管理サービスからのチャネルの構成」を参照してください。

注: チャネルは BlueCat DNS/DHCP インスタンスでサポートされていないため、チャネルの一部である SR-IOV インターフェイス（1/x および 10/x）はインターフェイスのリストに表示されません。

[構成] タブで、[**BlueCat DNS/DHCP] > [**ソフトウェアイメージ] に移動します。

XVA イメージを **SDX** アプライアンスにアップロードするには:

1. 詳細ウィンドウの [**XVA** ファイル**] > [**アクション] で、[アップロード] をクリックします。
2. 表示されるダイアログボックスで「ブラウズ」をクリックし、アップロードする XVA ファイルを選択します。
3. ［アップロード］をクリックします。XVA ファイルが XVA ファイルペインに表示されます。

BlueCat DNS/DHCP インスタンスをプロビジョニングするには:

1. [構成] タブで、[BlueCat DNS/DHCP] > [インスタンス] に移動します。
2. 詳細ペインで、[Add］をクリックします。BlueCat DNS/DHCP サーバーのプロビジョニング] ページが開きます。
3. BlueCat DNS/DHCP のプロビジョニングウィザードで、画面の指示に従います。

    - [インスタンスの作成] の [名前] フィールドにインスタンスの名前を入力し、[XVA ファイル] ドロップダウンメニューからアップロードしたイメージを選択し、[次へ] をクリックします。必要に応じて、[Domain Name] フィールドにインスタンスのドメイン名を入力します。
      注: 名前にはスペースを含めないでください。
    - [Network Settings] の [Management Interface] ドロップダウンメニューから、インスタンスの管理に使用するインターフェイスを選択し、そのインターフェイスの IP アドレスとゲートウェイを設定します。高可用性とサービスのために、インターフェイスを明示的に割り当てることができます。パラメータを選択し、[次へ] をクリックします。

注: 管理、高可用性、およびサービス用にインターフェイスを割り当てる場合は、サポートされているインターフェイスの組み合わせに基づいてインターフェイスを割り当ててください。

3 つすべてに同じインターフェイスを選択できます。
3 つのインターフェイスすべてに異なるインターフェイスを選択できます。
管理とサービスには同じインターフェイスを選択できますが、高可用性には異なるインターフェイスを選択できます。
[完了] をクリックし、[閉じる] をクリックします。インスタンスが作成され、起動され、選択した IP アドレスで設定されます。

インスタンスをプロビジョニングしたら、SSH を使用してインスタンスにログオンし、設定を完了します。BlueCat DNS/DHCP サーバーの設定方法や BlueCat アドレスマネージャーの管理下に置く方法の詳細については、BlueCat のドキュメント (次の URL を参照) を参照してください。https://care.bluecatnetworks.com

BlueCat DNS/DHCP Server インスタンスの設定を変更するには、[**BlueCat DNS/DHCP** インスタンス] ペインで、変更するインスタンスを選択し、[変更] をクリックします。BlueCat DNS/DHCP の変更ウィザードで、パラメーター設定を変更します。

注: インターフェイスパラメータまたはインスタンス名を変更すると、インスタンスは停止して再起動し、変更を有効にします。

BlueCat DNS/DHCP インスタンスを監視する

SDX アプライアンスは、BlueCat DNS/DHCP インスタンスのインスタンスで実行されているSDXToolsのバージョンなどの統計情報を収集します。

BlueCat DNS/DHCP インスタンスに関連する統計情報を表示するには:

1. BlueCat DNS/DHCP > インスタンスに移動します。
2. 詳細ペインで、インスタンス名の横にある矢印をクリックします。

BlueCat DNS/DHCP インスタンスを管理する

BlueCat DNS/DHCP インスタンスは、管理サービスから起動、停止、再起動、強制停止、強制再起動できます。

「設定」タブで、「**BlueCat DNS/DHCP**」を展開します。

BlueCat DNS/DHCP インスタンスを起動、停止、再起動、強制停止、または強制再起動するには:

1. インスタンス] をクリックします。
2. 詳細ペインで、操作を実行するインスタンスを選択し、次のいずれかのオプションを選択します。
   - 起動
   - シャットダウン
   - 再起動する

- 強制シャットダウン
- 強制再起動

3. 確認メッセージボックスで、「はい」をクリックします。

BlueCat DNS/DHCP SDXTools インスタンスのファイルをアップグレードする

SDXToolsは、サードパーティインスタンスで実行されるデーモンで、Management Service とサードパーティインスタンス間の通信に使用されます。

SDXToolsのアップグレードでは、ファイルを SDX アプライアンスにアップロードし、インスタンスを選択した後にSDXToolsをアップグレードします。クライアントコンピューターから SDX アプライアンスにSDXToolsファイルをアップロードできます。

SDXTools ファイルをアップロードするには:

1. ナビゲーションペインで、「管理サービス」を展開し、「**SDXTools** ファイル」をクリックします。
2. 詳細ウィンドウの [アクション] リストで、[アップロード] を選択します。
3. **SDXTools** ファイルのアップロードダイアログボックスで、「ブラウズ」をクリックし、ファイルを含むフォルダに移動して、ファイルをダブルクリックします。
4. [アップロード] をクリックします。

SDXTools をアップグレードするには:

「設定」タブで、「**BlueCat DNS/DHCP**」を展開します。

1. インスタンス] をクリックします。
2. 詳細ペインで、インスタンスを選択します。
3. アクションリストから、「**SDXTools** のアップグレード」を選択します。
4. [**SDxTools** のアップグレード] ダイアログボックスで、ファイルを選択し、[**OK**] をクリックし、[閉じる] をクリックします。

BlueCat DNS/DHCP インスタンスを再検出する

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表示できます。再検出中、管理サービスは構成をフェッチします。デフォルトでは、Management Service は 30 分に 1 回、すべてのインスタンスを再検出するようにインスタンスをスケジュールします。

「設定」タブで、「**BlueCat DNS/DHCP**」を展開します。

1. インスタンス] をクリックします。
2. 詳細ペインで、再検出するインスタンスを選択し、アクションリストから [再検出] をクリックします。
3. 確認メッセージボックスで、「はい」をクリックします。

CA アクセスゲートウェイ

November 23, 2023

CA Access Gateway は、アクセス制御のためのプロキシベースのソリューションを提供する、拡張性、管理性、拡張性に優れたスタンドアロンサーバです。CA Access Gateway は、企業にネットワークゲートウェイを提供し、従来の Cookie ベースのテクノロジーに依存しない複数のセッションスキームをサポートするプロキシエンジンを採用しています。

組み込み Web エージェントにより、企業全体でシングルサインオン (SSO) が可能になります。CA Access Gateway は、HTTP および HTTPS リクエストと Cookie レス SSO に対するアクセスコントロールを提供します。また、セッション情報はインメモリセッションストアに保存されます。プロキシルールは、CA Access Gateway が企業内の宛先サーバにあるリソースに要求を転送またはリダイレクトする方法を定義します。

CA Access Gateway は、ネットワークリソースに対して単一のゲートウェイを提供することで、企業ネットワークを分離し、アクセス制御を一元化します。

注：CA Access Gateway インスタンスではチャネルがサポートされていないため、チャネルの一部である SR-IOV インターフェイス（1/x および 10/x）はインターフェイスのリストに表示されません。CA Access Gateway の機能の詳細については、その製品のマニュアルを参照してください。

CA Access Gateway インスタンスをプロビジョニングする

CA Access Gateway インスタンスをプロビジョニングする前に、XVA イメージをダウンロードする必要があります。XVA イメージをダウンロードしたら、SDX アプライアンスにアップロードします。SDX アプライアンスで、管理サービスバージョン 10.5 ビルド 52.3.e 以降を使用していることを確認します。CA Access Gateway をプロビジョニングするには、まず XVA イメージを SDX アプライアンスにアップロードしてから、インスタンスをプロビジョニングする必要があります。

XVA イメージを **SDX** アプライアンスにアップロードするには:

1. [構成] タブで、**CA Access Gateway** > [ソフトウェアイメージ] に移動します。
2. 詳細ウィンドウの [**XVA** ファイル] で、[アクション] ドロップダウンリストから [アップロード] をクリックします。
3. 表示されるダイアログボックスで「ブラウズ」をクリックし、アップロードする XVA ファイルを選択します。
4. ［アップロード］をクリックします。XVA ファイルが **XVA** ファイルペインに表示されます。

CA Access Gateway インスタンスをプロビジョニングするには**:**

1. [構成] タブで、**CA Access Gateway**> [インスタンス] に移動します。
2. 詳細ペインで、[追加] をクリックします。
3. CA Access Gateway のプロビジョニングウィザードで、画面の指示に従います。
4. [完了] をクリックし、[閉じる] をクリックします。

インスタンスをプロビジョニングしたら、インスタンスにログオンし、詳細設定を実行します。

プロビジョニングされたインスタンスのパラメーターの値を変更するには、詳細ペインで変更するインスタンスを選択し、**[Modify]** をクリックします。[CA Access Gateway の変更] ウィザードで、パラメータを環境に適した値に設定します。

注:

インターフェイスパラメータまたはインスタンス名を変更すると、インスタンスは停止して再起動され、変更が有効になります。

CA Access Gateway インスタンスを監視する

SDX アプライアンスは、CA Access Gateway `SDXTools` インスタンスのインスタンスで実行されているのバージョンなどの統計情報を収集します。

CA Access Gateway インスタンスに関連する統計情報を表示するには、次の手順を実行します。

1. **CA Access Gateway >** インスタンスに移動します。
2. 詳細ペインで、インスタンス名の横にある矢印をクリックします。

CA Access Gateway インスタンスを管理する

CA Access Gateway インスタンスは、管理サービスから起動、停止、再起動、強制停止、または強制再起動できます。これらのタスクを完了するには、次の手順に従います。

1. [構成] タブで、[**CA Access Gateway **] を展開します。
2. **CA Access Gateway >** インスタンスに移動します。
3. 詳細ペインで、操作を実行するインスタンスを選択し、次のいずれかのオプションを選択します。
    - 起動
    - シャットダウン
    - 再起動する
    - 強制シャットダウン
    - 強制再起動
4. 確認メッセージボックスで、「はい」をクリックします。

パロアルトネットワークス **VM** シリーズ

November 23, 2023

Palo Alto Networks VM シリーズの仮想ファイアウォールは、同社の物理セキュリティアプライアンスで使用できるものと同じ PAN-OS 機能セットを使用し、主要なネットワークセキュリティ機能をすべて提供します。NetScaler SDX 上の VM シリーズでは、高度なセキュリティと ADC 機能を 1 つのプラットフォームに統合して、企業、事業部門、サービスプロバイダーの顧客がアプリケーションに安全かつ信頼性の高い方法でアクセスできるようにします。NetScaler SDX 上の VM シリーズを組み合わせることで、Citrix Virtual Apps and Desktops の導入環境向けの完全で検証済みのセキュリティおよび ADC ソリューションも提供されます。

Management Service から、インスタンスのプロビジョニング、モニタリング、管理、トラブルシューティングを行うことができます。

注意事項**:**

- SDX アプライアンスでプロビジョニングできるインスタンスの総数は、使用可能な SDX ハードウェアリソースによって異なります。
- チャネルの一部である SR-IOV インターフェイス（1/x および 10/x）は、Palo Alto VM シリーズインスタンスではチャネルがサポートされていないため、インターフェイスのリストには表示されません。パロアルトネットワーク VM シリーズの詳細については、パロアルトネットワークのドキュメントを参照してください。

Palo Alto VM シリーズインスタンスのプロビジョニング

パロアルト VM シリーズインスタンスをプロビジョニングする前に、パロアルトネットワークス Web サイトからXVA イメージをダウンロードする必要があります。XVA イメージをダウンロードしたら、SDX アプライアンスにアップロードします。

XVA イメージを **SDX** アプライアンスにアップロードするには:

1. 設定タブで **PaloAltoVM** シリーズ > ソフトウェアイメージに移動します。
2. 詳細ウィンドウの [**XVA** ファイル] で、[アクション] ドロップダウンリストから [アップロード] をクリックします。
3. 表示されるダイアログボックスで「ブラウズ」をクリックし、アップロードする XVA ファイルを選択します。
4. ［アップロード］をクリックします。XVA ファイルが **XVA** ファイルペインに表示されます。

Palo Alto VM シリーズインスタンスをプロビジョニングするには**:**

1. 設定タブで **PaloAltoVM** シリーズ > インスタンスに移動します。
2. 詳細ペインで、[追加] をクリックします。
3. PaloAlto VM シリーズのプロビジョニングウィザードで、画面の指示に従います。
4. [完了] をクリックし、[閉じる] をクリックします。

インスタンスをプロビジョニングしたら、インスタンスにログオンし、詳細設定を実行します。

プロビジョニングされたインスタンスのパラメーターの値を変更するには、詳細ペインで変更するインスタンスを選択し、**[Modify]** をクリックします。[Modify PaloAlto VM シリーズ] ウィザードで、パラメータを環境に適した値に設定します。

注**:** インターフェイスパラメータまたはインスタンス名を変更すると、インスタンスは停止して再起動され、変更が有効になります。

Palo Alto VM シリーズインスタンスを監視する

SDX アプライアンスは、Palo Alto VM シリーズインスタンスの、インスタンスで実行されている`SDXTools`のバージョンなどの統計情報を収集します。

Palo Alto VM シリーズインスタンスに関連する統計を表示するには**:**

1. **PaloAlto VM** シリーズ **>** インスタンスに移動します。
2. 詳細ペインで、インスタンス名の横にある矢印をクリックします。

PaloAlto VM シリーズインスタンスの管理

PaloAlto VM シリーズインスタンスの起動、停止、再起動、強制停止、強制再起動は、管理サービスから実行できます。

「構成」タブで、「**PaloAlto**VM シリーズ」を展開します。

1. **PaloAlto VM** シリーズ **>** インスタンスに移動します。
2. 詳細ペインで、操作を実行するインスタンスを選択し、次のいずれかのオプションを選択します。
   - 起動
   - シャットダウン
   - 再起動する
   - 強制シャットダウン
   - 強制再起動
3. 確認メッセージボックスで、「はい」をクリックします。

PaloAlto VM シリーズインスタンスのトラブルシューティング

管理サービスから PaloAlto VM シリーズインスタンスに ping を実行して、デバイスが到達可能かどうかを確認します。Management Service からインスタンスへのパケットのルートをトレースして、インスタンスに到達するまでのホップ数を判断できます。

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表示します。再検出時に、管理サービスは SDX アプライアンスで実行されている PaloAlto VM シリーズの構成とバージョンをフェッチします。デフォルトでは、管理サービスは 30 分に 1 回インスタンスの再検出をスケジュールします。

「構成」タブで、「**PaloAlto**VM シリーズ」を展開します。

インスタンスに **ping** を実行するには、以下を実行します。

1. インスタンス] をクリックします。
2. 詳細ウィンドウで ping するインスタンスを選択し、[アクション] リストから [**Ping**] をクリックします。**Pingmessage** ボックスに ping が成功したかどうかが表示されます。

インスタンスのルートをトレースするには**:**

1. インスタンス] をクリックします。
2. 詳細ペインで ping するインスタンスを選択し、アクションリストから **TraceRoute** をクリックします。**Traceroute** メッセージボックスには、インスタンスへのルートが表示されます。

インスタンスを再検出するには**:**

1. インスタンス] をクリックします。
2. 詳細ペインで、再検出するインスタンスを選択し、アクションリストから [再検出] をクリックします。
3. 確認メッセージボックスで、「はい」をクリックします。

Citrix SD-WAN VPX インスタンスを **NetScaler SDX** アプライアンスにデプロイします

November 23, 2023

Citrix SD-WAN テクノロジーは、ソフトウェア定義ネットワーク（SDN）の概念を WAN 接続に適用します。このテクノロジーは、トラフィック管理と監視をネットワークハードウェアから抽象化し、個々のアプリケーションに適用します。その結果、地理的に分散した場所でもパフォーマンスが向上し、高品質なユーザーエクスペリエンスが実現し、広域ネットワークとクラウドアクセスネットワークの導入が簡素化されます。詳しくは、「Citrix SD-WAN」を参照してください。

> 注： SD-WAN VPX スタンダードエディションのみがサポートされています。詳細については、SD-WAN VPX エディションを参照してください。

Citrix SD-WAN VPX インスタンスを SDX アプライアンスに展開するには、次のタスクが含まれます。

- ハードウェアのインストール：SDX ハードウェアが正しくインストールされていることを確認します。詳細については、「ハードウェアの取り付け」を参照してください。
- SDX 管理サービスのセットアップと構成。詳細については、「管理サービスユーザーインターフェイスの概要」および「管理サービスの構成」を参照してください。
- SD-WAN VPX インスタンスを SDX アプライアンスにプロビジョニングします。詳しくは、「NetScaler SDX での Citrix SD-WAN VPX インスタンスのプロビジョニング」を参照してください。
- SD-WAN VPX インスタンスの構成。詳細については、「構成ドキュメント 」および「MCN とクライアントサイト間の仮想パスサービスの構成」を参照してください。

前提条件

次のライセンスがあることを確認します。

- Citrix SD-WAN VPX ライセンス
- NetScaler SDX プラットフォームライセンス

Citrix SD-WAN VPX の要件

SDX プラットフォーム上の Citrix SD-WAN VPX は、サイトとしても MCN としても機能できます。MCN は 1 Gb/秒の双方向スループットと 64 のサイトを処理できます。

MCN とサイトでサポートされるスループット

- 250 MB/秒～1 Gb/秒の双方向スループット
- MCN は 64 のサイトをサポート

サポートされるスループットに対するハードウェア要件　サイト

- 4 CPU から 16 CPU
- 4 GB から 16 GB RAM
- 60 GB から 250 GB のディスクストレージ
- 最小 4 つの NIC: 1 つは管理用、残りは 3 つはデータパス用

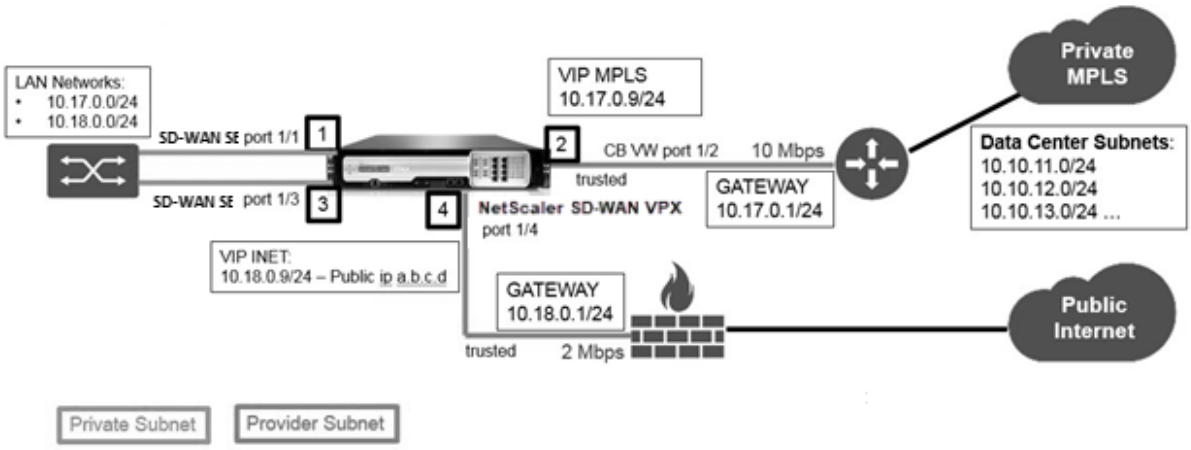
マスターコントロールノード (MCN)

- 4、8、16 CPU
- 16 GB RAM
- 250 GB のディスクストレージ
- 最小 4 つの NIC: 1 つは管理用、残りの 3 つはデータパス用、専用の NIC はデータパス用

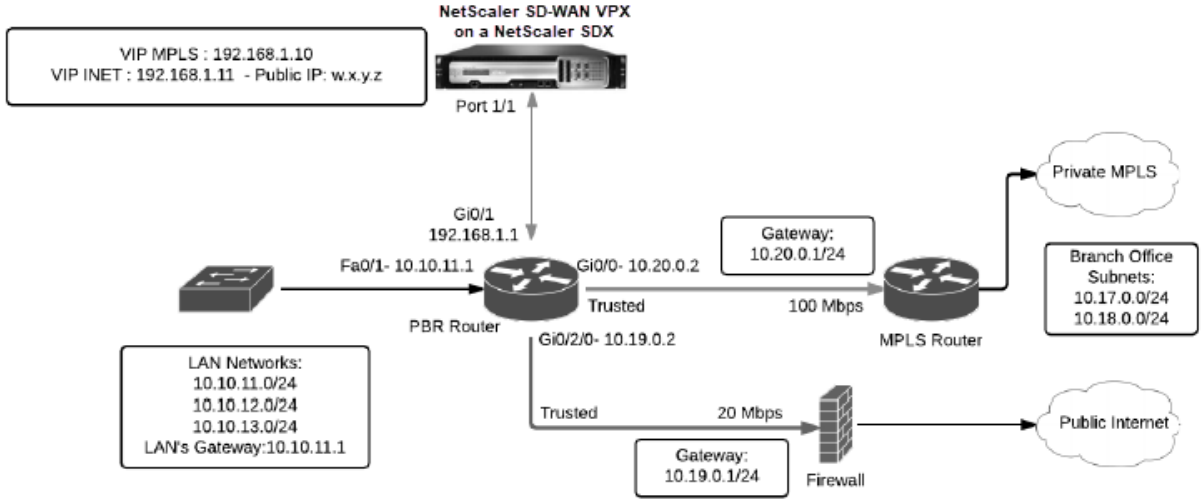
データセンター・トポロジー

Citrix SD-WAN VPX アプライアンスは、ポリシーベースルート（PBR）モードまたはインラインモードで NetScaler SDX に展開できます。これら 2 つのサポートされるモードについては、データセンタートポロジのシナリオ 1 と 2 を参照してください。詳細については、「仮想インラインモードでの SD-WAN の展開」を参照してください。

シナリオ 1: インラインモード



シナリオ 2: PBR モードまたは仮想インラインモード

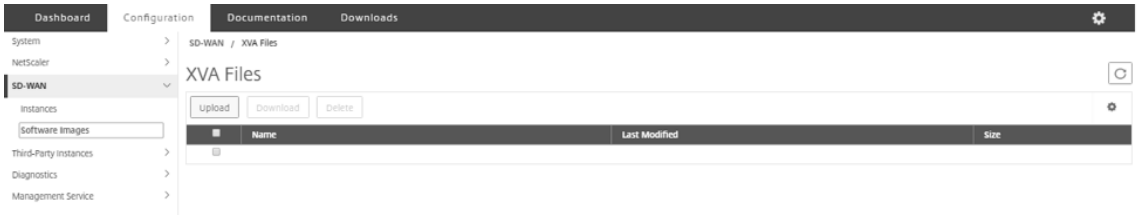


NetScaler SDX に **Citrix SD-WAN VPX** インスタンスをプロビジョニングする

Citrix SD-WAN VPX アプライアンスをプロビジョニングする前に、NetScaler 製品ダウンロードサイトから SD-WAN VPX イメージをダウンロードしてください。
https://www.citrix.com/downloads/netscaler-sd-wan/

Citrix SD-WAN VPX アプライアンスをプロビジョニングするには、次の手順に従います。

1. NetScaler SDX アプライアンスにログオンします。
2. 構成 **> SD-WAN >** インスタンスに移動します。
3. ソフトウェアイメージ **>** アップロードを選択し、SD-WAN XVA ファイルをアップロードします。



4. [インスタンス**] > [**追加] を選択します。[**SD-WAN** インスタンスのプロビジョニング] ページが表示されます。

5. **SD-WAN** インスタンスのプロビジョニングページで、次のように入力します。

   a. Name

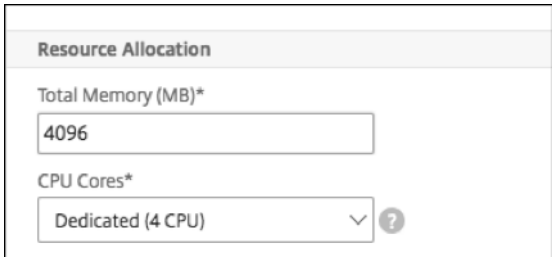
   b. IP アドレス

   c. ネットマスク

   d. ゲートウェイアドレス

   e. XVA ファイルのアップロード

   f. [リソース割り当て] で、リソースを割り当てます。



   g. [ネットワーク設定**]** で、管理インターフェイスをプロビジョニングし、[**OK**] を選択して作成し、SD-WAN VPX インスタンスを SDX アプライアンスにプロビジョニングします。

> 注： SDX Management Service は、インターフェイス名の昇順で VPX インスタンスにインターフェイスをバインドします。たとえば、1/4 と 1/1 を追加すると、Management Service はそれらを 1/1、1/4 として配置します。
> 新しいインターフェイスを追加しても、既存のシーケンスは保持され、新しいシーケンスが作成されます。たとえば、インターフェイス 1/2、10/1、1/3 を追加するとします。新しいシーケンスは 1/1、1/4、1/2、1/3、10/1 になります。

6. SD-WAN VPX インスタンスが [インスタンス] ページの下に表示されます。ここに例があります。

```
1 ![Image](/en-us/sdx/media/sd-wan-vpx-example.png)
```

インスタンスを編集するには、[構成**] > [SD-WAN] > [**インスタンス] に移動します。インスタンスを選択してクリックします。編集が完了したら、「**OK**」をクリックして変更を保存します。

Citrix SD-WAN VPX インスタンスの構成

SDX アプライアンスで SD-WAN インスタンスを作成したら、次の 2 つのタスクを完了して SD-WAN インスタンスを構成します。

1. MCN とサイトアプライアンスの両方に構成を適用します。
2. 仮想パスを設定し、トラフィックを転送します。

詳しくは、次のトピックを参照してください:

- 構成
- MCN サイトとクライアントサイト間の仮想パスサービスの構成

関連情報

Citrix SD-WAN アプライアンスの使用を開始する方法について詳しくは、「Citrix SD-WAN」を参照してください。

NetScaler SDX アプライアンスの詳細については、「NetScaler SDX」を参照してください。

SDX での帯域幅メータリング

February 16, 2024

NetScaler SDX 帯域幅計測は、正確で信頼性が高く、使いやすい計測スキームを提供します。これにより、処理能力を効率的に配分し、帯域幅の使用量を収益化できます。すべてのユーザーが常に割り当てられた帯域幅を取得することを念頭に置いて、さまざまなリソース間で帯域幅を最適に割り当てるには、メータリングスキームが必要です。

帯域幅の割り当ては、次の 2 つのモードで実行できます。

- スループットが固定された専用帯域幅
- 最小限保証されたスループットと帯域幅バースト機能を備えた専用帯域幅

スループットが固定された専用帯域幅

帯域幅割り当て方法では、各 VPX インスタンスに専用の帯域幅が割り当てられます。インスタンスは、設定された上限まで帯域幅を使用できます。専用モードでは、割り当てられる最小帯域幅と最大帯域幅は同じです。VPX インスタンスが一定期間内に割り当てられているよりも多くの帯域幅を必要とする場合、専用モードではインスタンスのスループットを向上させることはできません。VPX インスタンスが重要なリクエストを処理する場合、この問題はマイナス面になることがあります。

また、SDX アプライアンスに VPX インスタンスが少なく、一部のインスタンスが割り当てられた帯域幅を利用していない場合、専用モードで未使用の帯域幅を共有することはできません。これらすべての課題を克服するには、帯域幅を動的に増やすことができる最小保証レートで専用の帯域幅を使用すると便利です。

最小限保証されたスループットと帯域幅バースト機能を備えた専用帯域幅

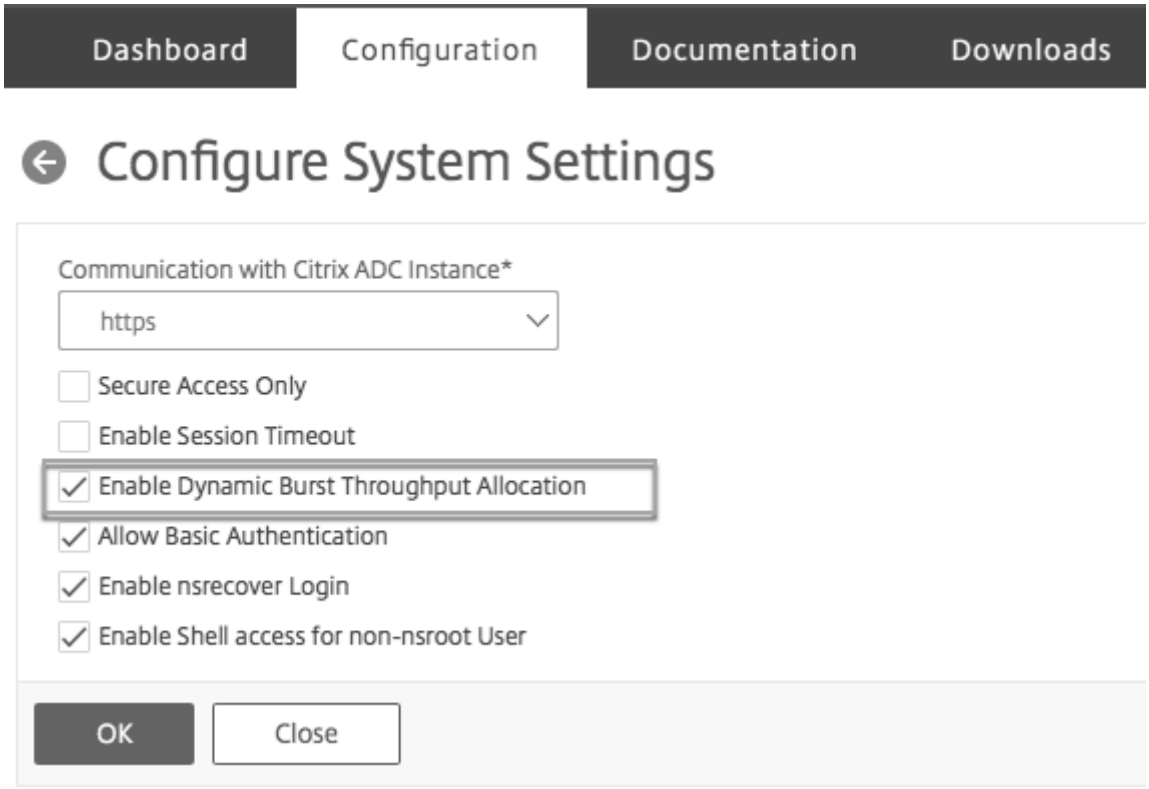
この帯域幅割り当て方法では、VPX には最低保証帯域幅が割り当てられ、帯域幅を事前設定された制限まで柔軟に増やすことができます。VPX が使用できる追加の帯域幅をバーストキャパシティと呼びます。

バーストキャパシティーのメリットは、追加のキャパシティーを持つインスタンスと未使用のキャパシティーを持つ VPX がある場合に見られます。これらの VPX インスタンスの追加容量は、割り当てられた帯域幅を十分に活用し、しばらくの間より多くを必要とする他の VPX インスタンスに割り当てることができます。また、さまざまなサービスプロバイダーが、専用の容量を必要とするさまざまなアドオンサービスを顧客に提供することに関心を持っています。同時に、帯域幅を過剰にプロビジョニングしたくありません。バースタブル帯域幅は、需要の高い時期に帯域幅を増やすオプションを使用して、特定の帯域幅を顧客に保証するような場合に役立ちます。

帯域幅割り当てモードの選択

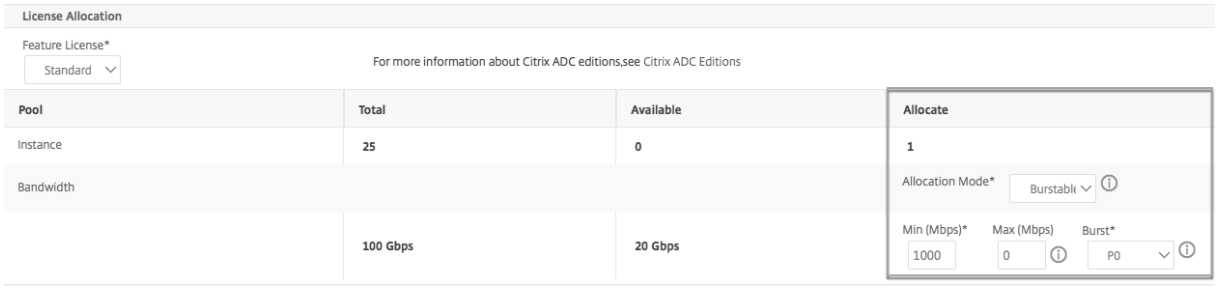
バースタブルスループットを選択する前に、動的バーストスループット割り当てを有効にする必要があります。このオプションを有効にするには、次の手順に従います。

1. SDX 管理コンソールから、[構成**] > [**システム] に移動します。
2. **[**システム設定**]** グループから [システム設定の変更] を選択します。
3. 動的スループットを有効にするには、**[**動的バーストスループット割り当ての有効化] チェックボックスをクリックします。



VPX をプロビジョニングする場合、帯域幅バーストまたは動的スループットから選択できます。

1. **SDX** 管理サービスで、[** 構成] > [NetScaler] > [インスタンス] **[追加] をクリックします。
2. 「**NetScaler** のプロビジョニング」ページが開きます。[ライセンス割り当て] の [割り当てモード] から [バースタブル] を選択します



NetScaler インスタンスをプロビジョニングする方法の詳細については、「NetScaler インスタンスの Provisioning」を参照してください。

固定スループットレートを使用する場合は、[固定] を選択します。デフォルトでは、帯域幅の割り当てには固定モードが設定されています。すべての VPX インスタンスが同じモードで動作している必要はありません。各 VPX インスタンスは異なるモードで構成できます。

注：SDX を 10.5.e 以前のバージョンから移行する場合、デフォルトですべての VPX インスタンスが固定割り当てモードになります。

VPX インスタンスの最大バースト帯域幅の決定

各 VPX がバーストできる範囲は、アルゴリズムによって計算されます。バースト可能な帯域幅を持つ VPX をプロビジョニングする場合、各 VPX に優先度を与える必要があります。バースタブル帯域幅の割り当ては、このバーストプライオリティによって決まります。プライオリティは P0 から P4 までさまざまで、P0 が最高のプライオリティ、P4 が最も低いプライオリティです。

VPX1 と VPX2 の 2 つの VPX がある場合を考えてみましょう。VPX1 と VPX2 に割り当てられる最小帯域幅はそれぞれ 4 Gbps と 2 Gbps で、バースト可能な帯域幅はそれぞれ 2 Gbps と 1 Gbps です。次の表に、パラメータを示します。

VPX 名	パラメーター	Value
VPX1	最小保証帯域幅	4Gbps
-	-	最大バースト可能帯域幅	2 Gbps
-	-	優先度	P0
VPX2	最小保証帯域幅	2 Gbps
-	-	最大バースト可能帯域幅	1 Gbps
-	-	優先度	P1

この場合、ライセンスされた帯域幅の合計が 8 Gbps であると仮定します。両方の VPX インスタンスが最大バースタブル制限までバーストしている場合、次のようになります。

1. VPX1 は最大バースト可能帯域幅、つまり 2 Gbps を使用しており、合計 4+2 = 6 Gbps を使用しています。
2. VPX2 は最大バースト可能帯域幅、つまり 1 Gbps を使用しており、合計 2+1 = 3 Gbps を使用しています

この場合、使用される最大帯域幅は、ライセンスされたキャパシティである 8 Gbps を超えています。そのため、使用量をライセンスされた容量内の帯域幅まで引き下げるには、VPX の 1 つがバースト可能な帯域幅を放棄する必要があります。この場合、VPX2 は VPX1 よりも優先度が低いため、1 Gbps のバースタブル帯域幅を放棄します。VPX1 は VPX2 よりも優先度が高いため、引き続きバーストします。このようなシナリオでは、最低保証帯域幅が常に守られていることが確認されます。

スループットとデータ消費量の統計を確認する

VPX ごとに、スループットとデータ消費量の統計をグラフで確認できます。グラフにアクセスするには、次の手順に従います。

1. SDX 管理サービスから、[構成**] > [NetScaler] > [**インスタンス**]** ページに移動します。
2. VPX インスタンスを選択し、[**Action]** ドロップリストをクリックします。
3. リストから、[スループット統計] または [データ使用統計] のいずれかを選択します。

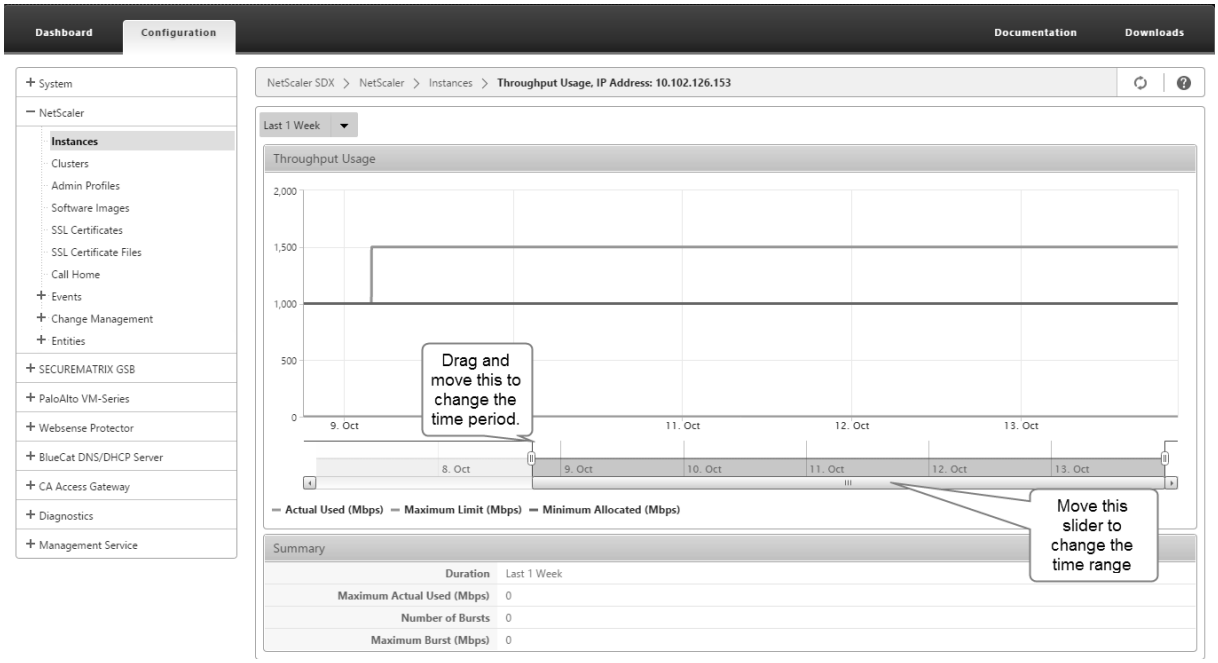
グラフを使用すると、次のようなさまざまな期間のデータ消費量とスループット統計を確認できます。

- 過去 1 時間

- 過去 1 日間
- 過去 1 週間
- 過去 1 か月
- 前月

グラフの下部にあるスライダを調整して、グラフ内の特定の期間を選択することもできます。グラフの線の上にマウスを移動して、特定の時間のデータ消費量またはスループットデータを確認します。

次の図は、1 週間のスループットデータのサンプルグラフを示しています。



NetScaler インスタンスの構成と管理

November 23, 2023

アプライアンスに NetScaler インスタンスをプロビジョニングしたら、インスタンスを構成および管理する準備が整います。まず、サブネット IP (SNIP) アドレスを作成し、設定を保存します。その後、インスタンスに対して基本的な管理タスクを実行できます。管理設定を適用する必要があるかどうかを確認します。

警告**:** インスタンスで直接変更を実行するのではなく、Management Service を使用して、インスタンスにプロビジョニングされたネットワークインターフェイスまたは VLAN を変更してください。

NetScaler インスタンスに SNIP アドレスを作成する

SDX アプライアンスで SNIP アドレスをプロビジョニングした後に、NetScaler インスタンスに割り当てることができます。

SNIP は、接続管理とサーバー監視に使用されます。NetScaler SDX アプライアンスを最初に構成するときに、SNIP を指定する必要はありません。管理サービスから SNIP を NetScaler インスタンスに割り当てることができます。

NetScaler インスタンスに **SNIP** アドレスを追加するには

1. ［構成］タブのナビゲーションペインで、［**NetScaler**］をクリックします。
2. 詳細ペインの［**NetScaler** 構成］で、［**IP** の作成］をクリックします。
3. **NetScaler IP** の作成ダイアログボックスで、次のパラメーターの値を指定します。
   - **IP** アドレス**:** SNIP アドレスとして割り当てられた IP アドレスを指定します。
   - **Netmask:** SNIP アドレスに関連付けられたサブネットマスクを指定します。
   - **[**タイプ**]:** 既定では、値は [SNIP] です。
   - 構成の保存：選択すると、構成が NetScaler に保存されます。デフォルト値は false です。
   - インスタンス **IP** アドレス**:** NetScaler インスタンスの IP アドレスを指定します。
4. [作成] をクリックし、[閉じる] をクリックします。

構成を保存します

管理サービスから NetScaler インスタンスの実行構成を保存できます。

NetScaler インスタンスに構成を保存するには

1. ［構成］タブのナビゲーションペインで、［**NetScaler**］をクリックします。
2. 詳細ペインの［**NetScaler** 構成］で、［構成の保存 **］をクリックします。
3. ［構成の保存］ダイアログボックスの［インスタンス **IP** アドレス］で、構成を保存する NetScaler インスタンスの IP アドレスを選択します。
4. 「**OK**」をクリックし、「閉じる」をクリックします。

NetScaler インスタンスの管理

管理サービスでは、NetScaler インスタンスで次の操作を実行できます。これらの操作は、［構成］タブの **NetScaler** インスタンスペインまたはホームページの **NetScaler** インスタンスガジェットから実行できます。

NetScaler インスタンスの起動**:** 管理サービスのユーザーインターフェイスから任意の NetScaler インスタンスを起動します。管理サービス UI がこの要求を管理サービスに転送すると、NetScaler インスタンスが起動します。

NetScaler インスタンスのシャットダウン**:** 管理サービスのユーザーインターフェイスから任意の NetScaler インスタンスをシャットダウンします。管理サービス UI がこの要求を管理サービスに転送すると、NetScaler インスタンスが停止します。

NetScaler インスタンスの再起動**:NetScaler** インスタンスを再起動します。

NetScaler インスタンスの削除**:** NetScaler インスタンスを使用したくない場合は、管理サービスを使用して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と、
SDX アプライアンスのデータベースからインスタンスとその関連情報が完全に削除されます。

NetScaler インスタンスを起動、停止、削除、または再起動するには

1. ナビゲーションペインの［構成］タブで、［**NetScaler** インスタンス］をクリックします。
2. 操作を実行する **NetScaler** インスタンスを選択し、**[**** 開始**]** または **[**** シャットダウン] または [削除] または [再起動 **] をクリックします。**
3. 確認メッセージボックスで、「はい」をクリックします。

NetScaler インスタンスファイルの削除

XVA、ビルド、ドキュメント、SSL キー、SSL 証明書などの NetScaler インスタンスファイルをアプライアンスから削除できます。

NetScaler インスタンスファイルを削除するには

1. ナビゲーションペインの［構成］タブで［**NetScaler** 構成］を展開し、削除するファイルをクリックします。
2. 詳細ペインでファイル名を選択し、[削除] をクリックします。

管理設定の適用

VPX インスタンスのプロビジョニング時に、管理サービスは VPX インスタンスにいくつかのポリシー、インスタンス管理 (admin) プロファイル、およびその他の設定を作成します。管理サービスが管理設定の適用に失敗した場合は、管理サービスから VPX インスタンスに設定を明示的にプッシュできます。この障害の原因の 1 つは、Management Service と VPX インスタンスが異なるサブネットワーク上にあり、ルーターがダウンしていることが考えられます。もう 1 つの理由は、両方が同じサブネット上にあるが、トラフィックが外部スイッチを通過する必要があり、リンクの 1 つがダウンしている場合です。

NetScaler インスタンスに管理構成を適用するには

1. ［構成］タブのナビゲーションペインで、［**NetScaler**］をクリックします。
2. 詳細ペインの［**NetScaler** 構成］で、［管理者構成の適用 **］をクリックします。
3. [管理者構成の適用] ダイアログボックスの [インスタンス **IP** アドレス] で、管理構成を適用する VPX インスタンスの IP アドレスを選択します。
4. ［**OK**］をクリックします。

SSL 証明書のインストールと管理

November 23, 2023

SSL 証明書をインストールするプロセスでは、まず証明書とキーファイルを NetScaler SDX アプライアンスにアップロードします。次に、NetScaler インスタンスに SSL 証明書をインストールします。SDX アプライアンスに SSL 証明書をインストールまたは更新すると、管理サービスが再起動します。

証明書ファイルを SDX アプライアンスにアップロードします

SSL トランザクションの場合、サーバーには有効な証明書と、対応する秘密鍵と公開鍵のペアが必要です。NetScaler インスタンスに SSL 証明書をインストールする場合、証明書ファイルが SDX アプライアンスに存在している必要があります。SSL 証明書ファイルは、バックアップとしてローカルコンピューターにダウンロードすることもできます。

[**SSL** 証明書] ペインでは、次の詳細を表示できます。

- **Name**

証明書ファイルの名前。

- 最終変更日

証明書ファイルが最後に変更された日付。

- サイズ

証明書ファイルのサイズ (バイト単位)。

SSL 証明書ファイルを SDX アプライアンスにアップロードするには

1. ナビゲーションウィンドウで [管理サービス] を展開し、[SSL 証明書ファイル] をクリックします。
2. [SSL 証明書] ペインで [アップロード] をクリックします。
3. [SSL 証明書のアップロード] ダイアログボックスで [参照] をクリックし、アップロードする証明書ファイルを選択します。
4. [アップロード] をクリックします。証明書ファイルが [SSL 証明書] ペインに表示されます。

SSL 証明書ファイルをダウンロードしてバックアップを作成するには

1. [SSL 証明書] ペインで、ダウンロードするファイルを選択し、[ダウンロード] をクリックします。
2. メッセージボックスの [保存] リストから [名前を付けて保存] を選択します。
3. [名前を付けて保存] メッセージボックスで、ファイルを保存する場所に移動し、[保存] をクリックします。

SDX アプライアンスへの **SSL** キーファイルのアップロード

SSL トランザクションの場合、サーバーには有効な証明書と、対応する秘密鍵と公開鍵のペアが必要です。NetScaler インスタンスに SSL 証明書をインストールする場合、キーファイルが SDX アプライアンスに存在している必要があります。SSL キーファイルは、バックアップとしてローカルコンピューターにダウンロードすることもできます。

[SSL Keys] ペインでは、次の詳細を表示できます。

- **Name**

キーファイルの名前。

- 最終変更日

キーファイルが最後に変更された日付。

- サイズ

キーファイルのサイズ (バイト単位)。

SSL キーファイルを **SDX** アプライアンスにアップロードするには

1. ナビゲーションウィンドウで [管理サービス] を展開し、[SSL 証明書ファイル] をクリックします。
2. [SSL 証明書] ウィンドウの [SSL キー] タブで、[アップロード] をクリックします。
3. [SSL キーファイルのアップロード] ダイアログボックスで [参照] をクリックし、アップロードするキーファイルを選択します。
4. [Upload] をクリックして、キーファイルを SDX アプライアンスにアップロードします。[SSL Keys] ペインにキーファイルが表示されます。

SSL キーファイルをダウンロードしてバックアップを作成するには

1. [SSL 証明書] ウィンドウの [SSL キー] タブで、ダウンロードするファイルを選択し、[ダウンロード] をクリックします。
2. メッセージボックスの [保存] リストから [名前を付けて保存] を選択します。
3. [名前を付けて保存] メッセージボックスで、ファイルを保存する場所に移動し、[保存] をクリックします。

NetScaler インスタンスへの **SSL** 証明書のインストール

管理サービスでは、
SSL 証明書を 1 つ以上の NetScaler インスタンスにインストールできます。SSL 証明書のインストールを開始する前に、SSL 証明書とキーファイルが SDX アプライアンスにアップロードされていることを確認してください。

NetScaler インスタンスに **SSL** 証明書をインストールするには

1. ナビゲーションペインで［NetScaler］をクリックします。
2. 詳細ペインの［NetScaler 構成］で、［SSL 証明書のインストール］をクリックします。
3. [SSL 証明書のインストール] ダイアログボックスで、次のパラメータの値を指定します。(*) は必須フィールドを示します。
   - 証明書ファイル: 有効な証明書のファイル名を指定します。証明書ファイルは SDX アプライアンスに存在する必要があります。
   -
   - 証明書名:NetScaler に追加する証明書とキーのペアの名前を指定します。最大長:31
   - 証明書の形式:NetScaler でサポートされている SSL 証明書の形式を指定します。NetScaler SDX アプライアンスは、SSL 証明書の PEM 形式と DER 形式をサポートしています。
   - パスワード: 秘密鍵の暗号化に使用されたパスフレーズを指定します。このオプションを使用すると、暗号化された秘密鍵をロードできます。最大長:32

     注: パスワードで保護された秘密キーは、PEM 形式でのみサポートされます。
   - 構成の保存: 構成を NetScaler に保存する必要があるかどうかを指定します。デフォルト値は false です。
   - インスタンス IP アドレス:SSL 証明書をインストールする NetScaler インスタンスの IP アドレスを指定します。
4. ［OK］をクリックし、［Close］をクリックします。

NetScaler インスタンスの **SSL** 証明書の更新

NetScaler インスタンスにインストールされている SSL 証明書の証明書ファイル、キーファイル、証明書形式などの一部のパラメーターを更新できます。IP アドレスと証明書名は変更できません。

NetScaler インスタンスの **SSL** 証明書を更新するには

1. ナビゲーションペインで［NetScaler］を展開し、［SSL 証明書］をクリックします。
2. [SSL 証明書] ペインで、[更新] をクリックします。
3. [SSL 証明書の変更] ダイアログボックスで、次のパラメータを設定します。
   - 証明書ファイル: 有効な証明書のファイル名。証明書ファイルは SDX アプライアンスに存在する必要があります。
   - Key File: 証明書の作成に使用された秘密鍵のファイル名。キーファイルは SDX アプライアンス上に存在する必要があります。

- 証明書形式:NetScaler SDX アプライアンスでサポートされている SSL 証明書のフォーマット。アプライアンスは SSL 証明書の PEM および DER 形式をサポートしています。
- Password: 秘密鍵の暗号化に使用されたパスフレーズ。このオプションを使用すると、暗号化された秘密鍵をロードできます。最大長:32 文字。

  注: パスワードで保護された秘密キーは、PEM 形式でのみサポートされます。
- 設定の保存: SDX アプライアンスに設定を保存する必要があるかどうかを指定します。デフォルト値は false です。
- ドメインチェックなし: 証明書の更新中はドメイン名をチェックしません。

4. [OK] をクリックし、[Close] をクリックします。

NetScaler インスタンスでの **SSL** 証明書のポーリング

NetScaler インスタンスにログオンした後で SSL 証明書を直接追加した場合、管理サービスはこの新しい証明書を認識しません。このシナリオを回避するには、管理サービスがすべての NetScaler インスタンスをポーリングして新しい SSL 証明書をチェックするポーリング間隔を指定します。また、管理サービスからいつでもポーリングを実行できます。たとえば、すべての NetScaler インスタンスから SSL 証明書のリストをすぐに取得したい場合です。

ポーリング間隔を構成するには

1. ナビゲーションペインで [NetScaler] を展開し、[SSL 証明書] をクリックします。
2. [SSL 証明書] ウィンドウで、[ポーリング間隔の構成] をクリックします。
3. [ポーリング間隔の構成] ダイアログボックスで、次のパラメータを設定します。
   - ポーリング間隔: 管理サービスが NetScaler インスタンスをポーリングするまでの時間。
   - 間隔単位: 時間の単位。指定可能な値: 時間、分。デフォルト: 時間。
4. [OK] をクリックし、[Close] をクリックします。

即時ポーリングを実行するには

1. ナビゲーションペインで [NetScaler] を展開し、[SSL 証明書] をクリックします。
2. [SSL 証明書] ペインで、[今すぐポーリング] をクリックします。
3. 「確認」ダイアログ・ボックスで、「はい」をクリックします。[SSL 証明書] ペインが更新され、新しい証明書 (存在する場合) がリストに表示されます。

NetScaler インスタンスで L2 モードを許可する

November 23, 2023

レイヤー 2（L2）モードでは、NetScaler インスタンスはラーニングブリッジとして機能し、宛先ではないすべてのパケットを転送します。Citrix CloudBridge などの一部の機能では、NetScaler インスタンスで L2 モードを有効にする必要があります。L2 モードを有効にすると、インスタンスは自身の MAC アドレス以外の MAC アドレスのパケットを受信および転送できます。ただし、NetScaler SDX アプライアンスで実行されている NetScaler インスタンスで L2 モードを有効にするには、管理者はまずそのインスタンスで L2 モードを許可する必要があります。L2 モードを許可する場合は、ブリッジングループを回避するための予防策を講じる必要があります。

注意事項**:**

1. 特定の 1/x インターフェイスでは、タグなしパケットは 1 つのインスタンスでのみ許可される必要があります。同じインターフェイスで有効になっている他のすべてのインスタンスでは、[Tagged] を選択する必要があります。

   注:

   L2 モードのインスタンスに割り当てられたすべてのインターフェイスで［Tagged］を選択 Citrix。タグ付き] を選択すると、そのインターフェイスではタグなしパケットを受信できません。

   インスタンスに割り当てられたインターフェイスに [Tagged] を選択した場合は、そのインスタンスにログオンし、そのインターフェイスでパケットを受信するように 802.1q VLAN を設定します。

2. L2 モードが許可されている NetScaler インスタンスで共有される 1/x および 10/x インターフェイスについては、次の条件が満たされていることを確認してください。

   - VLAN フィルタリングはすべてのインターフェイスで有効になっています。
   - 各インターフェイスは異なる 802.1q VLAN 上にあります。
   - インターフェイス上でタグなしパケットを受信できるインスタンスは 1 つだけです。そのインターフェイスが他のインスタンスに割り当てられている場合は、そのインスタンスに対してそのインターフェイスで [Tagged] を選択する必要があります。

3. L2 モードが許可されているインスタンスの 1/x インターフェイスでタグなしパケットを許可すると、他のインスタンスはそのインターフェイスでタグなしパケットを受信できません。この条件は、他のインスタンスで L2 モードが許可されているか許可されていないかに関係なく適用されます。

4. L2 モードが無効になっているインスタンスの 1/x インターフェイスでタグなしパケットを許可すると、L2 モードが許可されたインスタンスはそのインターフェイスでタグなしパケットを受信できません。

5. L2 モードでプロビジョニングされた instance1 に 0/x インターフェイスが割り当てられ、そのインターフェイスが instance2 にも割り当てられている場合は、instance2 に割り当てられている他のすべてのインターフェイスに対して [Tagged] を選択します。

注**:** 両方の管理インターフェイスが L2 モードのインスタンスに割り当てられている場合、L2 モードが有効な別の ADC インスタンスに割り当てることができるのは、これらのインターフェイスの 1 つだけです。つまり、L2 モードが有効になっている複数の NetScaler インスタンスに両方の管理インターフェイスを関連付けることはできません。

インスタンスで **L2** モードを許可するには

1. ADC のプロビジョニングウィザードまたは ADC の変更ウィザードの [ネットワーク設定] ページで、[**L2** モードを許可] を選択します。
   注**:** インスタンスの [Allow L2 Mode] 設定は、インスタンスをプロビジョニングするとき、またはインスタンスの実行中にアクティブ化できます。
2. ウィザードの手順に従って処理を進めます。
3. [完了] をクリックし、[閉じる] をクリックします。

インターフェイス上での仮想 **MAC** の設定

November 23, 2023

NetScaler インスタンスは、仮想 MAC（VMAC）を使用して高可用性（アクティブ/アクティブまたはアクティブ/スタンバイ）構成を実現します。仮想 MAC アドレス (VMAC) は、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で共有されるフローティングエンティティです。

高可用性設定では、プライマリノードは MIP、SNIP、VIP アドレスなど、すべての Floating IP アドレスを所有します。プライマリノードは、これらの IP アドレスに対するアドレス解決プロトコル (ARP) 要求に自身の MAC アドレスで応答します。その結果、外部デバイス（アップストリームルータなど）の ARP テーブルが Floating IP アドレスとプライマリノードの MAC アドレスで更新されます。

フェイルオーバーが発生すると、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。次に、Gratuitous ARP（GARP）を使用して、プライマリから取得したフローティング IP アドレスをアドバタイズします。ただし、新しいプライマリがアドバタイズする MAC アドレスは、自身のインターフェイスの MAC アドレスです。

一部のデバイス（特に一部のルーター）は、NetScaler SDX アプライアンスによって生成された GARP メッセージを受け入れません。このようなデバイスでは、古いプライマリノードによってアドバタイズされた古い IP と MAC のマッピングが保持され、その結果、サイトがダウンする可能性があります。

この問題は、HA ペアの両方のノードに VMAC を設定することで解決できます。これにより、両方のノードに同じ MAC アドレスが割り当てられます。したがって、フェールオーバーが発生しても、セカンダリノードの MAC アドレスは変更されず、外部デバイスの ARP テーブルを更新する必要はありません。

VMAC の設定には、次の 2 段階のプロセスがあります。

1. SDX 管理サービスで VMAC を設定します。インターフェイスまたは LA チャネルの VRID を追加します。SDX 管理サービスで VMAC を設定します。

2. Citrix インスタンスで VMAC を設定します。詳細については、「チャネルグループでの VMAC の設定 」のサポート記事を参照してください。

SDX 管理サービスで VMAC を構成する

VMAC を設定するには、管理サービスからインターフェイスまたは LA チャネルに IPv4 または IPv6 VRID を追加します。管理サービスは内部で VMAC を生成します。NetScaler インスタンスでアクティブ/アクティブモードを構成するときは、同じ VRID を指定します。このアクティブ/アクティブ構成は、Mellanox インターフェイスではサポートされていません。

次の点に留意してください。

1. 管理サービスから VRID を追加し、NetScaler インスタンスで同じ VRID を指定します。NetScaler インスタンスに直接 VRID を追加した場合、インスタンスは宛先 MAC アドレスとして VMAC アドレスを持つパケットを受信できません。
2. 同じ SDX アプライアンス内で実行されている異なるインスタンスで同じ VRID を使用することはできません。
3. インスタンスの実行中に、インスタンスに割り当てられたインターフェイスの VRID を追加または削除できます。
4. アクティブ/アクティブ構成では、インスタンスに割り当てられたインターフェイスに複数の VRID を指定できます。Mellanox インターフェイスでは、アクティブ/アクティブデプロイはサポートされていません。
5. 10G インターフェイスでは最大 86 個の VMC、1G インターフェイスでは最大 16 個の VMC が許可されます。VMAC フィルタがそれ以上使用できない場合は、別のインスタンスの VRID の数を減らします。

NetScaler VPX インスタンスの追加時に VRID を追加することも、既存の NetScaler インスタンスを変更して VRID を追加することもできます。

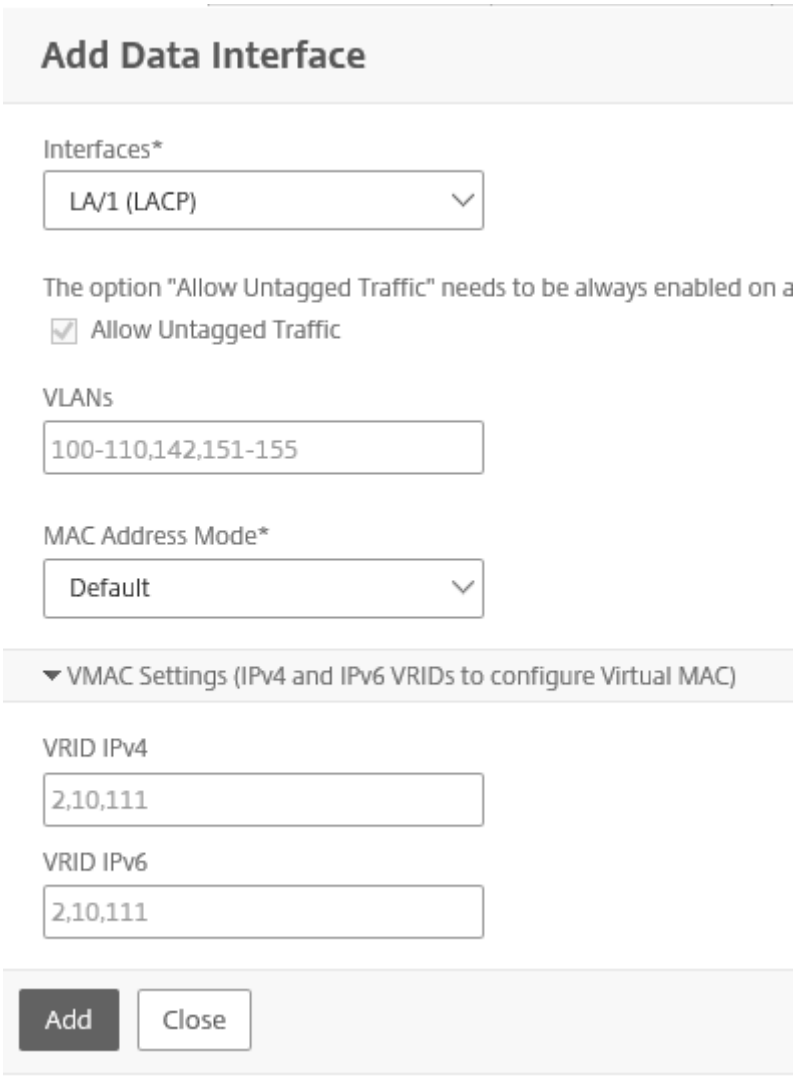
IPv4 または IPv6 VRID をインターフェイスまたは LA チャネルに追加するには

1. SDX に VPX インスタンスを追加するときに、[ネットワーク設定] で [データインターフェイス] を選択します。SDX に VPX インスタンスを追加する方法の詳細については、「NetScaler インスタンスの追加」を参照してください。
2. [**Interfaces**] ドロップダウンメニューから、インターフェイスまたは LA チャネルを選択します。
3. [VMAC 設定] で、次の値の一方または両方を設定します。

   - VRID IPv4: VMAC を識別する IPv4 VRID。可能な値:1 ～255
   - VRID IPv6: VMAC を識別する IPv6 VRID。可能な値:1 ～255

     注: 複数の VRID を区切るにはカンマを使用します。たとえば、12,24 と入力します。

4. [**Add**] をクリックして、**VMAC** 設定をインターフェイスに追加します。
5. [完了] をクリックし、[閉じる] をクリックします。



インスタンスがすでにプロビジョニングされている場合、IPv4 または IPv6 VRID を追加するには、次の手順に従います。

1. SDX 管理サービスから、[構成**] > [NetScaler] > [**インスタンス**]** に移動します。
2. インスタンスを選択して [**Edit**] をクリックします。
3. [データインターフェイス] でインターフェイスを選択し、[編集] をクリックします。
4. [VMAC 設定] で、VRID 値を設定します。[追加] をクリックし、[完了] をクリックします。

パーティション **MAC** アドレスを生成して、**SDX** アプライアンスの **NetScaler** インスタンスに管理パーティションを構成します

November 23, 2023

NetScaler SDX アプライアンス上の NetScaler インスタンスは、管理パーティションと呼ばれる論理エンティティに分割できます。各パーティションは、個別の NetScaler インスタンスとして構成して使用できます。管理パーティションの詳細については、「管理パーティショニング」を参照してください。

共有 VLAN 設定で管理パーティションを使用するには、パーティションごとに仮想 MAC アドレスが必要です。このような仮想 MAC アドレスはパーティション MAC（PMAC）アドレスと呼ばれ、共有 VLAN で受信したトラフィックの分類に使用されます。この PMAC アドレスは、そのパーティションにバインドされたすべての共有 VLAN で使用されます。

管理パーティションを使用する前に、Management Service ユーザーインターフェイスを使用して PMAC アドレスを生成して設定します。管理サービスでは、次の方法によってパーティション MAC アドレスを生成できます。

- ベース MAC アドレスの使用
- カスタム MAC アドレスの指定
- MAC アドレスをランダムに生成する

注:
パーティションの MAC アドレスを生成したら、管理パーティションを構成する前に NetScaler インスタンスを再起動する必要があります。

ベース **MAC** アドレスを使用してパーティション **MAC** アドレスを生成するには、次の手順を実行します。

1. ［構成］タブの左側のペインで［**NetScaler**］を展開し、［インスタンス］をクリックします。
2. インスタンスペインで、パーティション MAC アドレスを生成する NetScaler インスタンスを選択します。
3. [アクション] ドロップダウンリストで、[**MAC** のパーティション] をクリックします。
4. 「**Mac** のパーティション」ペインで、「生成」をクリックします。
5. 「パーティション **MAC** の生成」ダイアログボックスの「生成方法」セクションで、「ベースアドレスの使用」を選択します。
6. [ベース **MAC** アドレス] フィールドに、ベース MAC アドレスを入力します。
7. [**Increment By**] フィールドに、後続の MAC アドレスごとにベース MAC アドレスを増分する値を入力します。
   たとえば、ベース MAC アドレスを 00:A1: C 9:11: C 8:11 と指定し、増分値を 2 に指定した場合、次の MAC アドレスは 00:A1: C 9:11: C 8:13 として生成されます。
8. [**Count**] フィールドに、生成するパーティション MAC アドレスの数を入力します。
9. 生成] をクリックします。

カスタム **MAC** アドレスを指定してパーティション **MAC** アドレスを生成するには、次の手順を実行します。

1. ［構成］タブの左側のペインで［**NetScaler**］を展開し、［インスタンス］をクリックします。
2. インスタンスペインで、パーティション MAC アドレスを生成する NetScaler インスタンスを選択します。
3. [アクション] ドロップダウンリストで、[**MAC** のパーティション] をクリックします。
4. 「**Mac** のパーティション」ペインで、「生成」をクリックします。
5. 「パーティション **MAC** の生成」ダイアログボックスの「生成方法」セクションで、「ユーザー指定」を選択します。

6. [**MAC** アドレス] フィールドに MAC アドレスを入力します。
7. [**+**] アイコンをクリックし、次の MAC アドレスを入力します。さらにカスタム MAC アドレスを指定する場合は、この手順を繰り返します。
8. 生成] をクリックします。

パーティション **MAC** アドレスをランダムに生成するには、次の手順を実行します。

1. ［構成］タブの左側のペインで［**NetScaler**］を展開し、［インスタンス］をクリックします。
2. インスタンスペインで、パーティション MAC アドレスを生成する NetScaler インスタンスを選択します。
3. [アクション] ドロップダウンリストで、[**MAC** のパーティション] をクリックします。
4.「**Mac** のパーティション」ペインで、「生成」をクリックします。
5.「パーティション **MAC** の生成」ダイアログボックスの「生成方法」セクションで、「ランダム」を選択します。
6. [**Count**] フィールドに、生成するパーティション MAC アドレスの数を入力します。
7. 生成] をクリックします。

SDX アプライアンスでパーティション MAC アドレスを生成したら、生成されたパーティション MAC アドレスを使用して NetScaler インスタンスの管理パーティションを構成します。

VPX インスタンスの変更管理

November 23, 2023

管理サービスから NetScaler VPX インスタンスの構成への変更を追跡できます。詳細ウィンドウには、デバイス名と IP アドレス、最終更新日時、日時が表示されます。また、保存されている構成と実行構成との間に違いがあるかどうかも表示されます。デバイスを選択すると、実行構成、保存済み構成、構成変更履歴、およびアップグレード前とアップグレード後の構成の違いが表示されます。VPX インスタンスの構成をローカルコンピューターにダウンロードできます。デフォルトでは、Management Service は 24 時間ごとにすべてのインスタンスをポーリングしますが、この間隔は変更できます。既存の設定ファイルからコマンドをコピーして、監査テンプレートを作成できます。後でこのテンプレートを使用して、インスタンスの設定の変更を検出し、必要に応じて修正措置を講じることができます。

VPX インスタンスの変更管理を表示するには

1. [構成] タブで、[**NetScaler] > [**変更管理] に移動します。
2. [変更管理] ペインで VPX インスタンスを選択し、[アクション] リストから次のいずれかを選択します。

   - [Running Configuration]：選択した VPX インスタンスの実行構成を新しいウィンドウに表示します。
   - 「保存された構成」(Saved Configuration)-選択した VPX インスタンスの保存済み構成を新しいウィンドウに表示します。
   - 保存された対。[Running Diff]：保存した構成、実行構成、修正コマンド（差分）を表示します。
   - 「リビジョン履歴差分」(Revision History Diff)-基本構成ファイルと 2 つ目の構成

- アップグレード前対 [Post Upgrade Diff]：アップグレードの前後の設定の違い、および修正コマンド（違い）を表示します。
- [Template Diff]：保存済みまたは実行中の構成とテンプレートの差分を表示します。この差分はバッチファイルとして保存できます。テンプレートからインスタンスに設定を適用するには、このバッチファイルをインスタンスに適用します。
- [Download]：選択した VPX インスタンスの設定をダウンロードし、ローカルデバイスに保存します。

いずれかの **NetScaler** インスタンスの構成が更新されているかどうかをポーリングするには

1. [構成] タブで、[**NetScaler] > [**変更管理] に移動します。
2.「変更管理」枠の「操作」リストで、次のいずれかを選択します。
   - [Poll Now]：Management Service は、アプライアンスにインストールされている VPX インスタンスの構成（ns.conf）に対する更新について、即時ポーリングを実行します。
   - ポーリング間隔の構成-管理サービスがアプライアンスにインストールされている VPX インスタンスの構成（ns.conf）に対する更新をポーリングするまでの時間。デフォルトのポーリング間隔は 24 時間です。

NetScaler インスタンスの監査テンプレートを構成するには

1. 既存の設定ファイルを開き、そのコマンドのリストをコピーします。
2. [構成] タブで、[**NetScaler] > [**変更管理**] > [**監査テンプレート] に移動します。
3. 詳細ペインで、[追加] をクリックします。
4. [テンプレートの追加] ダイアログボックスで、テンプレートの名前と説明を追加します。
5. [**Command**] テキストボックスに、構成ファイルからコピーしたコマンドのリストを貼り付けます。
6. [作成] をクリックし、[閉じる] をクリックします。

NetScaler インスタンスを監視する

November 23, 2023

Management Service ユーザーインターフェイスの [Monitoring] ページには、アプライアンスおよびアプライアンスにプロビジョニングされた VPX インスタンスのパフォーマンスの概要が表示されます。NetScaler インスタンスをプロビジョニングして構成したら、さまざまなタスクを実行して NetScaler インスタンスを監視できます。

VPX インスタンスのプロパティを表示する

Management Service のユーザーインターフェイスには、SDX アプライアンスにプロビジョニングされたすべての VPX インスタンスのリストと説明が表示されます。**NetScaler** インスタンスペインを使用して、インスタンス名

と IP アドレス、CPU とメモリの使用率、スループット、インスタンスに割り当てられた合計メモリなどの詳細を表示します。

VPX インスタンスの IP アドレスをクリックすると、そのインスタンスの構成ユーティリティ (GUI) が新しいタブまたはブラウザで開きます。

VPX インスタンスのプロパティを表示するには

1. 左側のペインの［構成］タブで［NetScaler 構成］を展開し、［インスタンス］をクリックします。
   注:VPX インスタンスのプロパティは [
   ホーム] タブから表示することもできます。
2. NetScaler インスタンスペインでは、NetScaler インスタンスに関する以下の詳細を表示できます。
   - 名前**:** プロビジョニング中に NetScaler インスタンスに割り当てられるホスト名。
   - **[**仮想マシンの状態**]:** 仮想マシンの状態。
   - **NetScaler** の状態**:** NetScaler インスタンスの状態。
   - **IP** アドレス**:** NetScaler インスタンスの IP アドレスです。IP アドレスをクリックすると、このインスタンスの GUI が新しいタブまたはブラウザで開きます。
   - **Rx (Mbps):** NetScaler インスタンスで受信されたパケット。
   - **Tx (Mbps):** NetScaler インスタンスによって送信されたパケット。
   - **HTTP** 要件**:NetScaler** インスタンスで **1** 秒あたりに受信された **HTTP** リクエストの総数。
   - **CPU** 使用率 **(%):** NetScaler の CPU 使用率のパーセンテージ。
   - メモリ使用量 **(%):** NetScaler のメモリ使用率。
3. NetScaler インスタンスの名前の横にある矢印をクリックすると、そのインスタンスのプロパティが表示されます。「すべて展開」をクリックして、すべての **NetScaler** インスタンスのプロパティを表示することもできます。次のプロパティを表示できます。
   - ネットマスク**:** NetScaler インスタンスのネットマスク IP アドレス。
   - **Gateway:** デフォルトゲートウェイの IP アドレス。インスタンスがインストールされているサブネットの外部にトラフィックを転送するルーターです。
   - **1** 秒あたりのパケット数**:** 1 秒あたりに通過するパケットの総数。
   - **NIC:** NetScaler インスタンスで使用される NIC の名前と、各インターフェイスに割り当てられた仮想機能。
   - バージョン**:** インスタンスで現在実行されている NetScaler ソフトウェアのビルドバージョン、ビルド日時。
   - ホスト名**:** NetScaler インスタンスのホスト名。
   - 合計メモリ **(GB):** NetScaler インスタンスに割り当てられているメモリの合計です。
   - スループット **(Mbps): NetScaler** インスタンスの合計スループット。
   - **Up Since:** インスタンスが継続的に UP 状態になってからの日時。
   - **SSL** チップ**:** インスタンスに割り当てられた SSL チップの総数。

- ピア **IP** アドレス**:** この NetScaler インスタンスが HA セットアップの場合、そのピアの IP アドレス。
- ステータス**:** NetScaler インスタンスで実行されている操作のステータス（インスタンスからのインベントリが完了しているかどうかのステータスなど）。
- **HA** マスター状態**:** デバイスの状態。状態は、インスタンスがスタンドアロンセットアップとプライマリセットアップのどちらで構成されているか、高可用性セットアップの一部であるかを示します。高可用性設定では、状態にはプライマリモードかセカンダリモードかも表示されます。
- **HA** 同期ステータス**:** HA 同期ステータスのモード (有効または無効など)。
- 説明**:** NetScaler インスタンスのプロビジョニング中に入力された説明。

> 注**:**
>
> 認証の失敗により ADC インスタンスがアウトオブサービスになった場合、次の条件が満たされると、インスタンスの状態の色が灰色に変わります。
>
> - ADC インスタンスのパスワードは、インスタンス CLI を使用して直接変更されます。
> - パスワードが、Management Service に保存されているインスタンス管理者プロファイルのパスワードと一致しません。
> - インスタンスを初めて再起動すると、前のセッションは失われます。
>
> 通常、インスタンスがアウトオブサービスになると、インスタンスの状態の色は黄色になります。
>
> インスタンスをリカバリするには、次のいずれかを実行します。
>
> - インスタンス CLI から、インスタンスの管理者プロファイルのパスワードと一致するようにインスタンスのパスワードを変更します。その後、管理サービスからインスタンスを再検出します。
> - ADC インスタンスの現在のパスワードと同じパスワードで admin プロファイルを作成します。次に、ADC インスタンスを新しい管理者プロファイルで更新します。

NetScaler インスタンスの実行中および保存済みの構成を表示する

管理サービスを使用すると、
NetScaler インスタンスの現在実行中の構成を表示できます。NetScaler インスタンスの保存された構成と、構成が保存された時刻を表示することもできます。

NetScaler インスタンスの実行中および保存済みの構成を表示するには

1. 左側のペインの［構成］タブで［NetScaler 構成］を展開し、［インスタンス］をクリックします。
2. NetScaler インスタンスペインで、実行中または保存されている構成を表示したい NetScaler インスタンスをクリックします。
3. 実行構成を表示するには、「実行構成」をクリックし、保存した構成を表示するには「保存済み構成」をクリックします。

4. NetScaler 実行構成ウィンドウまたは NetScaler 保存済み構成ウィンドウでは、NetScaler インスタンスの実行中または保存済みの構成を表示できます。

NetScaler インスタンスに **PING** を送信する

管理サービスから NetScaler インスタンスに ping を送信して、デバイスにアクセスできるかどうかを確認できます。

NetScaler インスタンスに **ping** を送信するには

1. 左側のペインの［構成］タブで［NetScaler 構成］を展開し、［インスタンス］をクリックします。
2. NetScaler インスタンスペインで、ping を送信する NetScaler インスタンスをクリックし、「Ping」をクリックします。Ping メッセージボックスで、ping が成功したかどうかを確認できます。

NetScaler インスタンスのルートをトレースします

管理サービスから NetScaler インスタンスへのパケットのルートは、インスタンスに到達するために使用されたホップ数を特定することで追跡できます。

NetScaler インスタンスのルートをトレースするには

1. 左側のペインの［構成］タブで［NetScaler 構成］を展開し、［インスタンス］をクリックします。
2. NetScaler インスタンスペインで、トレースする NetScaler インスタンスをクリックし、「TraceRoute」をクリックします。Traceroute メッセージボックスでは、NetScaler へのルートを表示できます。

NetScaler インスタンスの再検出

NetScaler インスタンスの最新の状態と構成を確認する必要がある場合は、NetScaler インスタンスを再検出できます。

再検出中、管理サービスは構成をフェッチします。デフォルトでは、管理サービスは 30 分に 1 回、デバイスの再検出をスケジュールします。

NetScaler インスタンスを再検出するには

1. 左側のペインの［構成］タブで［NetScaler 構成］を展開し、［インスタンス］をクリックします。
2. **NetScaler** インスタンスペインで、再検出する **NetScaler** インスタンスをクリックし、「再検出」をクリックします。
3. 確認メッセージボックスで、「はい」をクリックします。

ログを使用して操作とイベントを監視する

November 23, 2023

監査ログとタスクログを使用して、管理サービスと NetScaler SDX インスタンスで実行される操作を監視します。また、イベントログを使用して、管理サービスおよび Citrix Hypervisor で実行されたタスクのすべてのイベントを追跡することもできます。

監査ログを表示する

管理サービスを使用して実行されたすべての操作は、アプライアンスデータベースに記録されます。監査ログを使用して、Management Service ユーザーが実行した操作、日時、各操作の成功または失敗のステータスを表示します。また、該当する列見出しをクリックして、ユーザ、オペレーション、監査時間、ステータスなどで詳細をソートすることもできます。

ページネーションは [Audit Log] ペインでサポートされています。1 ページに表示するレコード数を選択します。既定では、1 ページに 25 件のレコードが表示されます。

監査ログを表示するには、次の手順に従います。

1. ナビゲーションウィンドウで [システム] を展開し、[監査] をクリックします。
2. [Audit Log] ペインでは、次の詳細を表示できます。
    - ユーザー名**:** 操作を実行した管理サービスユーザー。
    - **IP** アドレス**:** 操作が実行されたシステムの IP アドレス。
    - **Port:** 操作の実行時にシステムが稼働していたポート。
    - リソースタイプ**:** xen_vpx_image や login など、操作の実行に使用されるリソースのタイプ。
    - リソース名**:** vpx_image_name やログインに使用したユーザー名など、操作の実行に使用されるリソースの名前。
    -
    - 操作**:** 追加、削除、ログアウトなど、実行されたタスク。
    - **[**ステータス**]:** [成功] や [失敗] など、監査のステータス。
    - メッセージ**:** 操作が失敗した場合は失敗の原因と、操作が成功した場合は「完了」などのタスクのステータスを説明するメッセージです。
3. 特定のフィールドでログを並べ替えるには、列の見出しをクリックします。

タスクログを表示する

タスクログを使用して、Management Service が NetScaler インスタンス上で実行するインスタンスのアップグレードや SSL 証明書のインストールなどのタスクを表示および追跡できます。タスクログでは、タスクが進行中か、失敗したか、成功したかを確認できます。

[タスクログ] ウィンドウ枠ではページ分割がサポートされています。1 ページに表示するレコード数を選択します。既定では、1 ページに 25 件のレコードが表示されます。

タスクログを表示するには、次の手順に従います。

1. ナビゲーションウィンドウで [診断] を展開し、[タスクログ] をクリックします。
2. [Task Log] ペインでは、次の詳細を表示できます。
    - **[**名前**]:** 実行中または既に実行されたタスクの名前。
    - **[**ステータス**]:** [進行中]、[完了]、[失敗] など、タスクのステータス。
    - 実行者**:** 操作を実行した管理サービスユーザー。
    - **[**開始時間**]:** タスクが開始された時刻。
    - 終了時間**:** タスクが終了した時刻。

タスクデバイスログを表示する

タスクデバイスログを使用して、各 SDX インスタンスで実行されているタスクを表示および追跡します。タスクデバイスログでは、タスクが進行中か、失敗したか、成功したかを確認できます。また、タスクが実行されたインスタンスの IP アドレスも表示されます。

タスクデバイスログを表示するには、次の手順に従います。

1. ナビゲーションウィンドウで [診断] を展開し、[タスクログ] をクリックします。
2. [**Task Log**] ペインでタスクをダブルクリックし、タスクデバイスの詳細を表示します。
3. [タスクデバイスログ（Task Device Log）] ペインで、特定のフィールドでログを並べ替えるには、列の見出しをクリックします。

タスクコマンドログを表示する

タスクコマンドログを使用して、NetScaler インスタンスで実行されたタスクの各コマンドのステータスを表示します。タスクコマンドログでは、コマンドが正常に実行されたか、失敗したかを確認できます。また、実行されたコマンドと、コマンドが失敗した理由も表示されます。

タスクコマンドログを表示するには、次の手順に従います。

1. ナビゲーションウィンドウで [診断] を展開し、[タスクログ] をクリックします。
2. [**Task Log**] ペインでタスクをダブルクリックし、タスクデバイスの詳細を表示します。
3. [**Task Device Log**] ペインで、タスクをダブルクリックしてタスクコマンドの詳細を表示します。
4. [タスクコマンドログ（Task Command Log）] ペインで、特定のフィールドでログを並べ替えるには、列の見出しをクリックします。

イベントの表示

管理サービスのユーザーインターフェイスの [イベント] ウィンドウ枠を使用して、管理サービスで実行されるタスクについて管理サービスによって生成されたイベントを監視します。

イベントを表示するには、次の手順に従います。

1. [**System**] **>** [**Events**] の順に選択します。
2. [**Events**] ペインでは、次の詳細を表示できます。
    - 重要度**:** イベントの重要度。重大、メジャー、マイナー、クリア、情報の場合があります。
    - **Source:** イベントが生成される IP アドレス。
    - 日付**:** イベントが生成された日付。
    - カテゴリ**:** PolicyFailed や DeviceConfigChange などのイベントのカテゴリ。
    - **Message:** イベントを説明するメッセージです。
3. 特定のフィールドでイベントを並べ替えるには、列の見出しをクリックします。

NetScaler SDX アプライアンスのユースケース

November 23, 2023

ネットワークコンポーネント (ファイアウォールや Application Delivery Controller など) では、マルチテナンシーのサポートには、従来、1 つのデバイスを複数の論理パーティションに分割する機能が含まれていました。このアプローチにより、多数の個別のデバイスを用意しなくても、テナントごとに異なるポリシーセットを実装できます。しかし、伝統的に、達成される分離の程度に関しては厳しく制限されています。

設計上、SDX アプライアンスには同じ制限はありません。SDX アーキテクチャでは、各インスタンスは専用の NetScaler カーネル、CPU リソース、メモリリソース、アドレス空間、および帯域幅割り当てを備えた個別の仮想マシン（VM）として実行されます。SDX アプライアンスのネットワーク I/O は、総合的なシステムパフォーマンスを維持するだけでなく、各テナントのデータプレーンと管理プレーンのトラフィックを完全に分離することもできます。管理プレーンには 0/x インターフェイスが含まれます。データプレーンには 1/x および 10/x インターフェイスが含まれます。データプレーンは管理プレーンとしても使用できます。

SDX アプライアンスの主な使用例は統合に関するもので、管理の分離を維持しつつ、必要なネットワークの数を削減します。統合の基本的なシナリオを次に示します。

- 管理サービスと NetScaler インスタンスが同じネットワークにある場合の統合。
- Management Service インスタンスと NetScaler インスタンスが異なるネットワークにあるが、すべてのインスタンスが同じネットワークにある場合の統合。
- セキュリティ全体にわたる統合。
- 各インスタンスの専用インターフェイスによる統合。
- 1 つの物理ポートを複数のインスタンスで共有することによる統合。

管理サービスと **NetScaler** インスタンスが同じネットワークにある場合の統合

November 23, 2023

SDX アプライアンスでのシンプルな統合ケースとして、管理サービスと NetScaler インスタンスを同じネットワークの一部として構成する方法があります。このユースケースは、以下の場合に該当します。

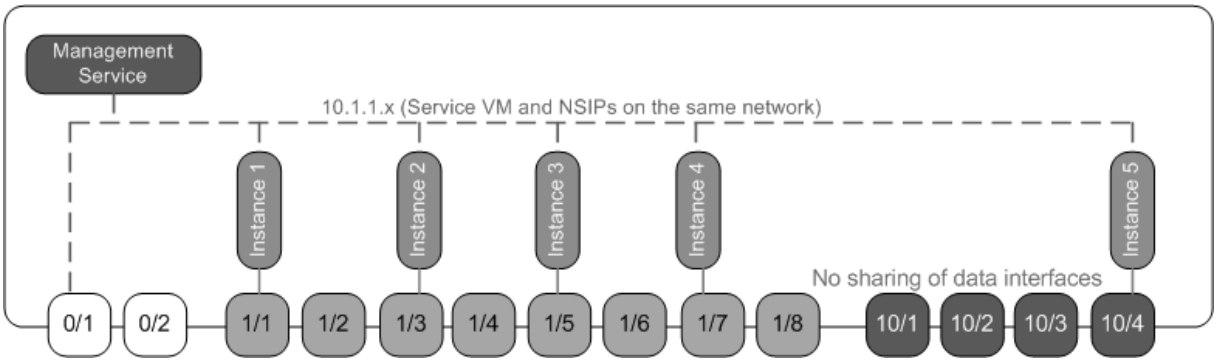
- アプライアンス管理者はインスタンス管理者でもあります。
- 組織のコンプライアンス要件では、Management Service と異なるインスタンスの NSIP アドレスに個別の管理ネットワークが必要と規定されていません。

インスタンスは同じネットワーク (管理トラフィック用) にプロビジョニングできます。VIP アドレスは、異なるネットワーク (データトラフィック用) に設定できるため、異なるセキュリティゾーンに設定できます。

次の例では、管理サービスと NetScaler インスタンスは 10.1.1.x ネットワークの一部です。インターフェイス 0/1 と 0/2 は管理インターフェイス、1/1 ～1/8 は 1G データインターフェイス、10/1 ～10/4 は 10G データインターフェイスです。各インスタンスには専用の物理インターフェイスがあります。したがって、インスタンスの数はアプライアンスで使用できる物理インターフェイスの数に制限されます。デフォルトでは、SDX アプライアンスの各インターフェイスで VLAN フィルタリングが有効になっています。VLAN の数は、1G インターフェイスでは 32、10 G インターフェイスでは 63 に制限されています。VLAN フィルタリングは、インターフェイスごとに有効または無効にできます。各インスタンスのインターフェイスあたり最大 4096 の VLAN を設定するには、VLAN フィルタリングを無効にします。この例では、インスタンスごとに専用のインターフェイスがあるため、VLAN フィルタリングは不要です。VLAN フィルタリングについて詳しくは、SDX アプライアンスの管理と監視の**VLAN** フィルタリングセクションを参照してください。

次の図は、前述のユースケースを示しています。

図 1: 同じネットワーク内のインスタンスに対して Management Service と NSIP を持つ SDX アプライアンスのネットワークトポロジ



次の表は、前述の例で NetScaler インスタンス 1 のプロビジョニングに使用されたパラメーターの名前と値を示しています。

パラメーター名	インスタンス 1 の値
Name	vpx8
IP アドレス	10.1.1.2
ネットマスク	255.255.255.0
Gateway	10.1.1.1
XVA ファイル	NS-VPX-XEN-10.0-51.308.a_nc.xva
機能ライセンス	Platinum
管理者プロフィール	ns_nsroot_profile
ユーザー名	vpx8
パスワード	Sdx1
パスワードの確認	Sdx1
シェル/Sftp/Scp アクセス	True
合計メモリ (MB)	2048
#SSL チップス	1
スループット (Mbps)	1000
1 秒あたりのパケット数	1000000
CPU	共有
インターフェイス	0/1 と 1/1

次の例のように **NetScaler** インスタンス **1** をプロビジョニングします

1. ナビゲーションペインの［構成］タブで［NetScaler 構成］を展開し、［インスタンス］をクリックします。
2. NetScaler インスタンスペインで、「追加」をクリックします。
3. Citrix のプロビジョニングウィザードで、ウィザードの指示に従って、前の表に示したパラメーター値を指定します。
4. ［Create］をクリックしてから、［Close］をクリックします。プロビジョニングした NetScaler インスタンスが NetScaler インスタンスペインに表示されます。

管理サービスと **NetScaler** インスタンスが異なるネットワークにある場合の統合

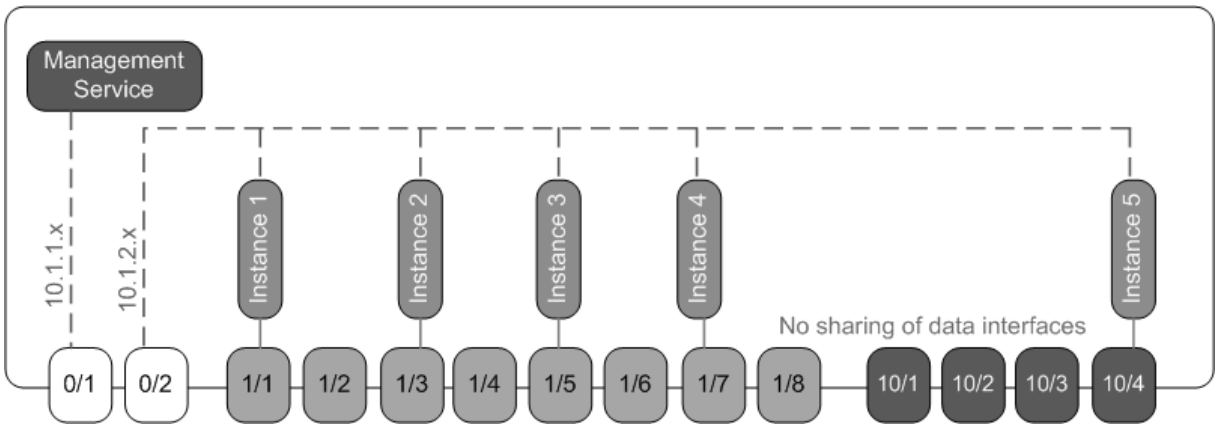
November 23, 2023

場合によっては、アプライアンス管理者が他の管理者に個別のインスタンスに対する管理タスクの実行を許可することがあります。これは、個々のインスタンス管理者にそのインスタンスへのログイン権限を付与することで安全に行えます。ただし、セキュリティ上の理由から、アプライアンス管理者はインスタンスが管理サービスと同じネットワーク上に存在することを許可したくない場合があります。これはサービスプロバイダー環境では一般的なシナリオであり、仮想化やクラウドアーキテクチャを採用する企業ではますます一般的になりつつあります。

次の例では、管理サービスは 10.1.1.x ネットワークにあり、NetScaler インスタンスは 10.1.2.x ネットワークにあります。インターフェイス 0/1 と 0/2 は管理インターフェイス、1/1 ～1/8 は 1G データインターフェイス、10/1 ～10/4 は 10G データインターフェイスです。各インスタンスには、専用の管理者と、専用の物理インターフェイスがあります。したがって、インスタンスの数はアプライアンスで使用できる物理インターフェイスの数に制限されます。各インスタンスには専用のインターフェイスがあるため、VLAN フィルタリングは不要です。必要に応じて、VLAN フィルタリングを無効にして、インターフェイスごとにインスタンスあたり最大 4096 の VLAN を設定します。この例では、インスタンスが物理インターフェイスを共有しておらず、タグ付き VLAN もないため、NSVLAN を設定する必要はありません。NSVLAN について詳しくは、「NetScaler インスタンスの追加」を参照してください。

次の図は、前述のユースケースを示しています。

図 1: 管理サービスと異なるネットワーク内のインスタンス用の NSIP を備えた SDX アプライアンスのネットワークトポロジ



アプライアンス管理者は、管理サービスと SDX アプライアンス上の NSIP アドレス間のトラフィックを維持できます。また、トラフィックを外部ファイアウォールやその他のセキュリティ仲介装置を通過させてアプライアンスに戻す場合などに、トラフィックをデバイスから強制的に送信することもできます。

次の表は、この例で NetScaler インスタンス 1 のプロビジョニングに使用されるパラメーターの名前と値を示しています。

パラメーター名	インスタンス 1 の値
Name	vpx1
IP アドレス	10.1.2.2
ネットマスク	255.255.255.0

パラメーター名	インスタンス 1 の値
Gateway	10.1.2.1
XVA ファイル	NS-VPX-XEN-10.0-51.308.a_nc.xva
機能ライセンス	Platinum
管理者プロフィール	ns_nsroot_profile
ユーザー名	vpx1
パスワード	Sdx1
パスワードの確認	Sdx1
シェル/Sftp/Scp アクセス	True
合計メモリ (MB)	2048
#SSL チップス	1
スループット (Mbps)	1000
1 秒あたりのパケット数	1000000
CPU	共有
インターフェイス	0/2 と 1/1

次の例のように **NetScaler** インスタンス **1** をプロビジョニングするには

1. ［構成］タブのナビゲーションペインで、［NetScaler 構成］を展開し、［インスタンス］をクリックします。
2. **NetScaler** インスタンスペインで、「追加」をクリックします。
3. **NetScaler** のプロビジョニングウィザードで、ウィザードの指示に従って、パラメーターを上記の表に示されている値に設定します。
4. [作成] をクリックし、[閉じる] をクリックします。プロビジョニングした NetScaler インスタンスが NetScaler インスタンスペインに表示されます。

セキュリティゾーン間での統合

November 23, 2023

SDX アプライアンスは、セキュリティゾーン間の統合によく使用されます。攻撃者は DMZ にしかアクセスできないため、DMZ は組織の内部ネットワークにセキュリティを強化します。組織の内部ネットワークにはアクセスできません。コンプライアンスの厳しい環境では、DMZ と内部ネットワークの両方に VIP アドレスを持つ単一の NetScaler

インスタンスは使用できません。SDX では、DMZ で VIP アドレスをホストするインスタンスと、内部ネットワークで VIP アドレスをホストする他のインスタンスをプロビジョニングできます。

場合によっては、セキュリティゾーンごとに個別の管理ネットワークが必要になることがあります。DMZ 内のインスタンスの NSIP アドレスは、1 つのネットワーク内に存在できます。内部ネットワーク内の VIP を持つインスタンスの NSIP アドレスは、別の管理ネットワークに存在できます。また、Management Service とインスタンス間の通信は、ルーターなどの外部デバイスを介してルーティングされる必要がある場合もあります。ファイアウォールポリシーを設定して、ファイアウォールに送信されるトラフィックを制御し、トラフィックをログに記録できます。

SDX アプライアンスには 2 つの管理インターフェイス（0/1 と 0/2）があり、モデルによっては最大 8 個の 1G データポートと 8 個の 10G データポートがあります。データポートを管理ポートとして使用することもできます（管理インターフェイスではタグ付けが許可されていないため、タグ付き VLAN を設定する必要がある場合など）。その場合、管理サービスからのトラフィックはアプライアンスを出て、アプライアンスに戻る必要があります。このトラフィックをルーティングしたり、オプションで、インスタンスに割り当てられたインターフェイスで NSVLAN を指定したりできます。管理インターフェイスがインスタンスと管理サービス間で共通している場合は、2 つのインスタンス間のトラフィックをルーティングする必要はありません。ただし、セットアップで明示的に要求される場合は、トラフィックをルーティングできます。

注：タグ付けは Citrix Hypervisor バージョン 6.0 でサポートされています。

インスタンスごとに専用のインターフェースで統合

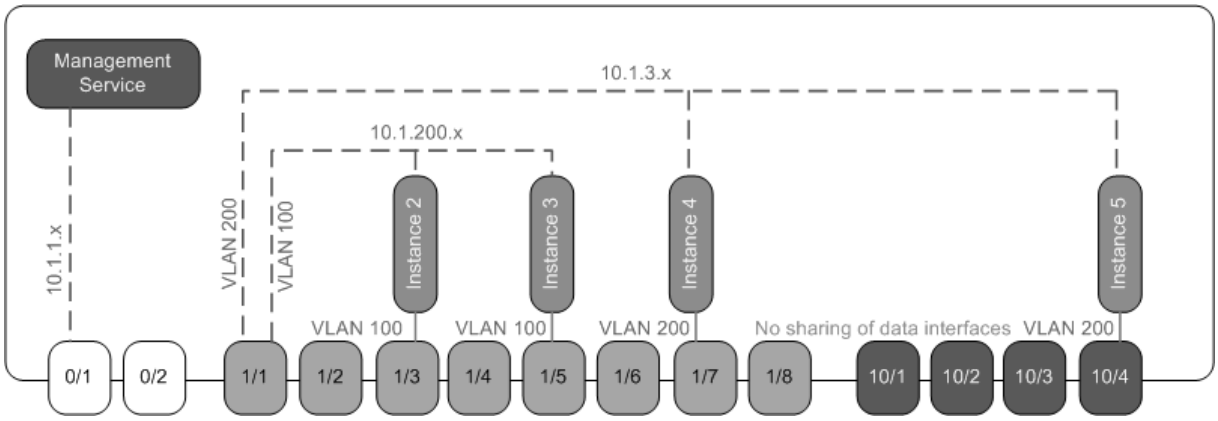
November 23, 2023

次の例では、インスタンスは複数のネットワークの一部です。インターフェイス 0/1 は、内部 10.1.1.x ネットワークの一部である管理サービスに割り当てられます。NetScaler インスタンス 2 と 3 は 10.1.200.x ネットワーク（VLAN 100）の一部です。NetScaler インスタンス 4 と 5 は 10.1.3.x ネットワーク（VLAN 200）の一部です。

オプションで、すべてのインスタンスに NSVLAN を設定できます。

次の図は、前述のユースケースを示しています。

図 1：複数のネットワークに NetScaler インスタンスを持つ SDX アプライアンスのネットワークトポロジー



SDX アプライアンスはスイッチに接続されています。アプライアンスのポート 1/1 が接続されているスイッチポートに VLAN ID 100 および 200 が設定されていることを確認します。

次の表は、この例で NetScaler インスタンス 5 と 3 のプロビジョニングに使用されるパラメーターの名前と値を示しています。

パラメーター名	インスタンス 5 の値	インスタンス 3 の値
Name	vpx5	vpx3
IP アドレス	10.1.3.2	10.1.200.2
ネットマスク	255.255.255.0	255.255.255.240
Gateway	10.1.3.1	10.1.200.1
XVA ファイル	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
機能ライセンス	Platinum	Platinum
管理者プロフィール	ns_nsroot_profile	ns_nsroot_profile
ユーザー名	vpx5	vpx3
パスワード	Sdx1	root
パスワードの確認	Sdx1	root
シェル/Sftp/Scp アクセス	True	True
合計メモリ (MB)	2048	2048
#SSL チップス	1	1
スループット (Mbps)	1000	1000
1 秒あたりのパケット数	1000000	1000000
CPU	共有	共有
インターフェイス	1/1 と 10/4	1/1 と 1/5
NSVLAN	200	100
Add (インタフェース)	1/1	1/1
タグ付きインターフェイス	タグ付きを選択	タグ付きを選択

この例のように **NetScaler** インスタンス **5** と **3** をプロビジョニングするには

1. ［構成］タブのナビゲーションペインで、［NetScaler 構成］を展開し、［インスタンス］をクリックします。
2. **NetScaler** インスタンスペインで、「追加」をクリックします。

3. **NetScaler** のプロビジョニングウィザードで、ウィザードの指示に従って、パラメーターを上記の表に示されている値に設定します。
4. [作成] をクリックし、[閉じる] をクリックします。プロビジョニングした NetScaler インスタンスが NetScaler インスタンスペインに表示されます。

複数のインスタンスによる物理ポートの共有による統合

November 23, 2023

必要に応じて、インターフェイス上で VLAN フィルタリングを有効または無効にできます。たとえば、インスタンスに 100 を超える VLAN を設定するには、そのインスタンスに専用の物理インターフェイスを割り当て、そのインターフェイスで VLAN フィルタリングを無効にします。物理インターフェイスを共有するインスタンスで VLAN フィルタリングを有効にして、1 つのインスタンスが別のインスタンスのトラフィックを認識できないようにします。

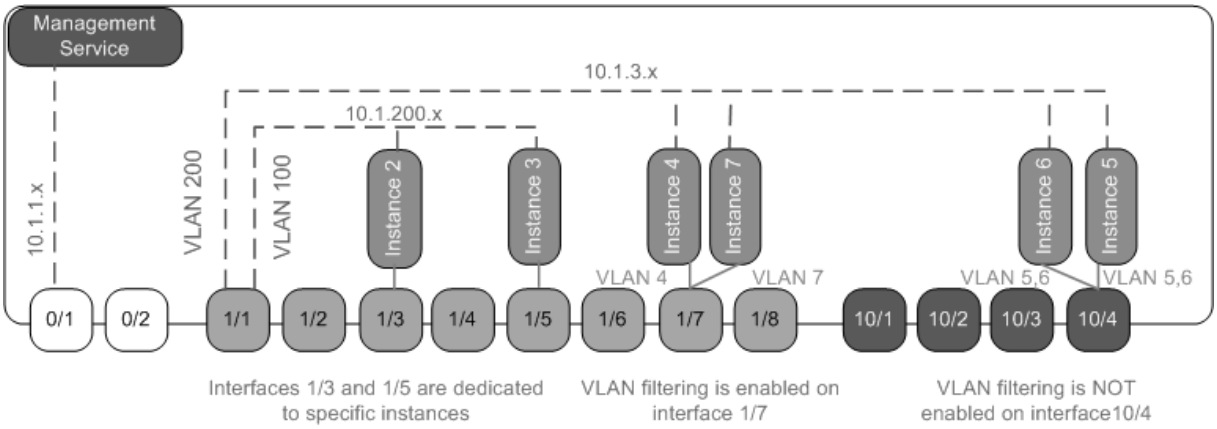
注**:** VLAN フィルタリングはアプライアンスのグローバル設定ではありません。インターフェイスで VLAN フィルタリングを有効または無効にすると、そのインターフェイスに関連付けられているすべてのインスタンスに設定が適用されます。VLAN フィルタリングが無効の場合、最大 4096 個の VLAN を設定できます。VLAN フィルタリングが有効の場合、10 G インターフェイスには最大 63 個のタグ付き VLAN を、1 G インターフェイスには最大 32 個のタグ付き VLAN を設定できます。

次の例では、インスタンスは複数のネットワークの一部です。

- インターフェイス 1/1 は、すべてのインスタンスの管理インターフェイスとして割り当てられます。インターフェイス 0/1 は、内部 10.1.1.x ネットワークの一部である管理サービスに割り当てられます。
- NetScaler インスタンス 2 と 3 は 10.1.200.x ネットワークにあり、インスタンス 4、5、6、7 は 10.1.3.x ネットワークにあります。インスタンス 2 と 3 にはそれぞれ専用の物理インターフェイスがあります。インスタンス 4 と 7 は物理インターフェイス 1/7 を共有し、インスタンス 5 と 6 は物理インターフェイス 10/4 を共有します。
- VLAN フィルタリングはインターフェイス 1/7 で有効になっています。インスタンス 4 のトラフィックは VLAN 4 にタグ付けされ、インスタンス 7 のトラフィックは VLAN 7 のタグが付けられます。その結果、インスタンス 4 のトラフィックはインスタンス 7 からは見えません。逆に、インスタンス 7 のトラフィックはインスタンス 4 からは見えません。インターフェイス 1/7 には最大 32 個の VLAN を設定できます。
- VLAN フィルタリングはインターフェイス 10/4 では無効になっているため、そのインターフェイスには最大 4096 個の VLAN を設定できます。インスタンス 5 に VLAN 500 ～599 を、インスタンス 6 に VLAN 600 ～699 を設定します。インスタンス 5 は VLAN 600 ～699 からのブロードキャストおよびマルチキャストトラフィックを確認できますが、パケットはソフトウェアレベルでドロップされます。同様に、インスタンス 6 は VLAN 500 ～599 からのブロードキャストおよびマルチキャストトラフィックを確認できますが、パケットはソフトウェアレベルでドロップされます。

次の図は、前述のユースケースを示しています。

図 1: 管理サービスインスタンスと NetScaler インスタンスがネットワークに分散された SDX アプライアンスのネットワークトポロジー



次の表は、この例で NetScaler インスタンス 7 と 4 のプロビジョニングに使用されるパラメーターの名前と値を示しています。

パラメーター名	インスタンス 7 の値	インスタンス 4 の値
Name	vpx7	vpx4
IP アドレス	10.1.3.7	10.1.3.4
ネットマスク	255.255.255.0	255.255.255.240
Gateway	10.1.3.1	10.1.3.1
XVA ファイル	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
機能ライセンス	Platinum	Platinum
管理者プロフィール	ns_nsroot_profile	ns_nsroot_profile
ユーザー名	vpx4	vpx4
パスワード	Sdx1	Sdx1
パスワードの確認	Sdx1	Sdx1
シェル/Sftp/Scp アクセス	True	True
合計メモリ (MB)	2048	2048
#SSL チップス	1	1
スループット (Mbps)	1000	1000
1 秒あたりのパケット数	1000000	1000000
CPU	共有	共有
インターフェイス	1/1 と 1/7	1/1 と 1/7

パラメーター名	インスタンス 7 の値	インスタンス 4 の値
NSVLAN	200	200

この例では、**NetScaler** インスタンス **7** と **4** をプロビジョニングするには

1. ナビゲーションペインの［構成］タブで［**NetScaler** 構成］を展開し、［インスタンス］をクリックします。
2. **NetScaler** インスタンスペインで、「追加」をクリックします。
3. Provision NetScaler Wizard で、ウィザードの指示に従ってパラメーターを前述の表の値に設定します。
4. [作成] をクリックし、[閉じる] をクリックします。プロビジョニングした NetScaler インスタンスが NetScaler インスタンスペインに表示されます。

NITRO API

November 23, 2023

NetScaler SDX NITRO プロトコルを使用すると、SDX アプライアンスをプログラムで構成および監視できます。

NITRO では、Representational State Transfer（REST）インターフェイスを介して機能が提供されます。そのため、NITRO アプリケーションはあらゆるプログラミング言語で開発することができます。また、Java、.NET、または Python で開発する必要があるアプリケーションの場合、NITRO プロトコルは関連するライブラリとして公開され、個別のソフトウェア開発キットとしてパッケージ化されます。

注：NITRO を使用する前に、SDX アプライアンスの基本を理解しておく必要があります。

NITRO プロトコルを使用するには、クライアントアプリケーションに次のものが必要です。

- SDX アプライアンスへのアクセス。
- REST インターフェイスを使用するには、SDX アプライアンスへの HTTP または HTTPS リクエスト（JSON 形式のペイロード）を生成するシステムが必要です。任意のプログラミング言語またはツールを使用できます。
- Java クライアントの場合、Java 開発キット (JDK) 1.5 以上のバージョンが利用可能なシステムが必要です。JDK はhttp://www.oracle.com/technetwork/java/javase/downloads/index.htmlからダウンロードできます。
- .NET クライアントの場合は、.NET Framework 3.5 以上のバージョンが使用できるシステムが必要です。.NET フレームワークは http://www.microsoft.com/downloads/en/default.aspxからダウンロードできます。
- Python クライアントの場合、Python 2.7 以上のバージョンと Requests ライブラリ (<NITRO_SDK_HOME>/lib で利用可能) がインストールされているシステムが必要です。

NITRO パッケージの入手

November 23, 2023

NITRO パッケージは、SDX アプライアンスの構成ユーティリティの [ダウンロード] ページで tar ファイルとして入手できます。ファイルをダウンロードし、ローカルシステム上のフォルダに un-tar を実行する必要があります。このフォルダは、<NITRO_SDK_HOME> このドキュメントではと呼びます。

このフォルダには、
lib サブフォルダに NITRO ライブラリが含まれています。NITRO 機能にアクセスするには、ライブラリをクライアントアプリケーションのクラスパスに追加する必要があります。
<NITRO_SDK_HOME> このフォルダーには、NITRO SDK を理解するのに役立つサンプルとドキュメントも用意されています。

注:

- REST パッケージには、REST インターフェイスを使用するためのドキュメントのみが含まれています。
- Python SDK では、ライブラリをクライアントパスにインストールする必要があります。インストール手順については、\/README.txt ファイルをお読みください。

.NET SDK

November 23, 2023

SDX NITRO API は、API の範囲と目的に応じてシステム API と構成 API に分類されます。NITRO 操作のトラブルシューティングも可能です。

システム **API**

NITRO を使用する最初のステップは、SDX アプライアンスとのセッションを確立し、管理者の資格情報を使用してセッションを認証することです。

アプライアンスの IP アドレスとアプライアンスに接続するプロトコル (HTTP または HTTPS) を指定して、nitro_service クラスのオブジェクトを作成します。次に、このオブジェクトを使用し、管理者のユーザー名とパスワードを指定して、アプライアンスにログオンします。

注: そのアプライアンスにはユーザーアカウントが必要です。実行できる構成操作は、アカウントに割り当てられている管理者の役割によって制限されます。

次のサンプルコードは、HTTPS プロトコルを使用して IP アドレス 10.102.31.16 の SDX アプライアンスに接続します。

```
1 //Specify the IP address of the appliance and service type
2 nitro_service nitroservice = new nitro_service ("10.102.31.16", "https"
      );
3
4 //Specify the login credentials
5 nitroservice.login("nsroot", "verysecret");
6 <!--NeedCopy-->
```

注**:**
nitro_service オブジェクトは、アプライアンスでのそれ以降の NITRO 操作すべてで使用します。

アプライアンスから切断するには、次のように logout () メソッドを呼び出します。

```
1 nitroservice.logout();
2 <!--NeedCopy-->
```

設定 **API**

NITRO プロトコルは、SDX アプライアンスのリソースの設定に使用できます。

リソースを構成するための API は、com.citrix.sdx.nitro.resource.config という形式のパッケージまたは名前空間にグループ化されます。. これらのパッケージまたは名前空間にはそれぞれ、リソースを構成するための API を提供します。

たとえば、NetScaler リソースには com.citrix.sdx.nitro.resource.config.ns パッケージまたは名前空間があります。

リソースクラスは、他の操作を実行するための API を提供します。これらの操作には、リソースの作成、リソースとリソースプロパティの取得、リソースの更新、リソースの削除、リソースに対する一括操作の実行などがあります。

リソースを作成する

SDX アプライアンスにリソース（NetScaler インスタンスなど）を作成するには:

1. 対応するプロパティー名を使用して、リソースの必須プロパティーの値を設定します。その結果、リソースに必要な詳細を含むリソースオブジェクトが生成されます。
   注: これらの値はクライアント上でローカルに設定されます。この値は、オブジェクトがアップロードされるまでアプライアンスに反映されません。
2. static add () メソッドを使用して、リソースオブジェクトをアプライアンスにアップロードします。

次のサンプルコードは、SDX アプライアンスに「ns_instance」という名前の NetScaler インスタンスを作成します。


```
ns newns = new ns();

//Set the properties of the NetScaler locally
newns.name = "ns_instance";
newns.ip_address = "10.70.136.5";
newns.netmask = "255.255.255.0";
newns.gateway = "10.70.136.1";
newns.image_name = "nsvpx-9.3.45_nc.xva";
newns.profile_name = "ns_nsroot_profile";
newns.vm_memory_total = 2048;
newns.throughput = 1000;
newns.pps = 1000000;
newns.license = "Standard";
newns.username = "admin";
newns.password = "admin";

int number_of_interfaces = 2;
network_interface[] interface_array = new network_interface[
    number_of_interfaces];

//Adding 10/1
interface_array[0] = new network_interface();
interface_array[0].port_name = "10/1";

//Adding 10/2
interface_array[1] = new network_interface();
interface_array[1].port_name = "10/2";

newns.network_interfaces = interface_array;

//Upload the NetScaler instance
ns result = ns.add(nitroservice, newns);
<!--NeedCopy-->
```

リソース詳細の取得

SDX アプライアンス上のリソースのプロパティを取得するには、次の手順を実行します。

1. get () メソッドを使用して、アプライアンスから設定を取得します。結果はリソースオブジェクトです。
2. 対応するプロパティ名を使用して、必要なプロパティをオブジェクトから抽出します。

次のサンプルコードは、すべての NetScaler リソースの詳細を取得します。

```
//Retrieve the resource object from the SDX appliance
ns[] returned_ns = ns.get(nitroservice);

//Extract the properties of the resource from the object
Console.WriteLine(returned_ns[i].ip_address);
Console.WriteLine(returned_ns[i].netmask);
<!--NeedCopy-->
```


リソース統計情報の取得

SDX アプライアンスは、その機能の使用状況に関する統計を収集します。これらの統計は NITRO を使用して取得できます。

次のサンプルコードは、ID が 123456a の NetScaler インスタンスの統計を取得します。

```
ns obj = new ns();
obj.id = "123456a";
ns stats = ns.get(nitroservice, obj);
Console.WriteLine("CPU Usage:" + stats.ns_cpu_usage);
Console.WriteLine("Memory Usage:" + stats.ns_memory_usage);
Console.WriteLine("Request rate/sec:" +stats.http_req);
<!--NeedCopy-->
```

リソースを更新する

アプライアンス上の既存のリソースのプロパティを更新するには、次の手順を実行します。

1. id プロパティーを、更新するリソースの ID に設定します。
2. 対応するプロパティー名を使用して、リソースの必須プロパティーの値を設定します。結果はリソースオブジェクトです。
   注: これらの値はクライアント上でローカルに設定されます。この値は、オブジェクトがアップロードされるまでアプライアンスに反映されません。
3. update () メソッドを使用して、リソースオブジェクトをアプライアンスにアップロードします。

次のサンプルコードでは、ID が 123456a の NetScaler インスタンスの名前を「ns_instance_new」に更新します。

```
ns update_obj = new ns();

//Set the ID of the NetScaler to be updated
update_obj.id = "123456a";

//Get existing NetScaler details
update_obj = ns.get(nitroservice, update_obj);

//Update the name of the NetScaler to "ns_instance_new" locally
update_obj.name = "ns_instance_new";

//Upload the updated NetScaler details
ns result = ns.update(nitroservice, update_obj);
<!--NeedCopy-->
```


リソースを削除する

既存のリソースを削除するには、削除するリソースの ID を引数として渡して、リソースクラスで静的メソッド delete () を呼び出します。

次のサンプルコードは、ID 1 の NetScaler インスタンスを削除します。

```
ns obj = new ns();
obj.id = "123456a";
ns.delete(nitroservice, obj);
<!--NeedCopy-->
```

一括操作

複数のリソースを同時に照会または変更できるため、ネットワークトラフィックを最小限に抑えることができます。たとえば、同じ操作で複数の NetScaler SDX アプライアンスを追加できます。

各リソースクラスには、リソースの追加、更新、削除のためのリソースの配列を取るメソッドがあります。一括操作を実行するには、各操作の詳細をローカルで指定し、その詳細を一度にサーバーに送信します。

NITRO では、一括操作内の一部の操作が失敗したことを考慮して、次のいずれかの動作を構成できます。

- 出口。最初のエラーが発生すると、実行は停止します。エラー発生前に実行されたコマンドがコミットされます。
- 続ける。一部のコマンドが失敗した場合でも、リスト内のすべてのコマンドが実行されます。

注:
nitro_service () メソッドで
`onerror` param を設定して、アプライアンスとの接続を確立する際に必要な動作を設定します。

次のサンプルコードは、1 回の操作で 2 つの ADC アプライアンスを追加します。

```
ns[] newns = new ns[2];

//Specify details of first NetScaler
newns[0] = new ns();
newns[0].name = "ns_instance1";
newns[0].ip_address = "10.70.136.5";
newns[0].netmask = "255.255.255.0";
newns[0].gateway = "10.70.136.1";
...
...

//Specify details of second NetScaler
newns[1] = new ns();
newns[1].name = "ns_instance2";
newns[1].ip_address = "10.70.136.8";
newns[1].netmask = "255.255.255.0";
newns[1].gateway = "10.70.136.1";
```



```
...
...

//upload the details of the ADC appliances to the NITRO server
ns[] result = ns.add(nitroservice, newns);
<!--NeedCopy-->
```

例外ハンドリング

errorcode フィールドはオペレーションのステータスを示します。

- エラーコード 0 は、操作が成功したことを示します。
- 0 以外のエラーコードは、NITRO 要求の処理中にエラーが発生したことを示します。

エラーメッセージフィールドには、簡単な説明と失敗の性質が表示されます。

com.citrix.sdx.nitro.exception.nitro_exception クラスは、NITRO API の実行におけるすべての例外をキャッチします。例外に関する情報を取得するには、`getErrorCode()` メソッドを使用します。

エラーコードの詳細については、<`NITRO_SDK_HOME`>/`doc`フォルダにある API リファレンスを参照してください。

REST ウェブサービス

November 23, 2023

REST (表現状態転送) は、クライアントとサーバー間の単純な HTTP リクエストとレスポンスに基づくアーキテクチャースタイルです。REST は、サーバー側でオブジェクトの状態を照会または変更するために使用されます。REST では、サーバー側はエンティティのセットとしてモデル化され、各エンティティは一意の URL によって識別されます。

各リソースには、次の操作を実行できる状態もあります。

- 作成。クライアントは「コンテナ」リソース上に新しいサーバー側リソースを作成できます。コンテナリソースはフォルダ、子リソースはファイルまたはサブフォルダと考えることができます。呼び出し側クライアントは、作成されるリソースの状態を提供します。この状態は、XML または JSON 形式を使用してリクエストで指定できます。クライアントは、新しいオブジェクトを識別する一意の URL を指定することもできます。また、サーバーは作成されたオブジェクトを識別する一意の URL を選択して返すこともできます。作成リクエストに使用される HTTP メソッドは POST です。
- 読み取り。クライアントは HTTP GET メソッドで URL を指定することで、リソースの状態を取得できます。レスポンスメッセージには、JSON 形式で表現されたリソースの状態が含まれます。
- **[**更新**]**。PUT HTTP メソッドを使用して、JSON または XML でオブジェクトとその新しい状態を識別する URL を指定することで、既存のリソースの状態を更新できます。

- **[削除]**。サーバー側に存在するリソースを破棄するには、DELETE HTTP メソッドと、削除するリソースを識別する URL を使用します。

この 4 つの CRUD 操作 (作成、読み取り、更新、削除) に加えて、リソースは他の操作やアクションをサポートできます。これらのオペレーションでは HTTP POST メソッドを使用し、JSON のリクエスト本文で、実行するオペレーションとそのオペレーションのパラメータを指定します。

SDX NITRO API は、API の範囲と目的に応じてシステム API と構成 API に分類されます。

システム **API**

NITRO を使用する最初のステップは、SDX アプライアンスとのセッションを確立し、管理者の資格情報を使用してセッションを認証することです。

ログインオブジェクトにユーザ名とパスワードを指定します。作成されるセッション ID は、セッション内のそれ以降のすべての操作のリクエストヘッダーで指定する必要があります。

注: そのアプライアンスにはユーザーアカウントが必要です。実行できる設定は、アカウントに割り当てられている管理者の役割によって制限されます。

HTTPS プロトコルを使用して IP アドレス 10.102.31.16 の SDX アプライアンスに接続するには、次の手順を実行します。

- **URL** `https://10.102.31.16/nitro/v2/config/login/`
- **HTTP** メソッド **POST**
- リクエスト
  - **Header**

```
Content-Type:application/vnd.com.citrix.sdx.login+json
<!--NeedCopy-->
```

注: 以前のバージョンの NITRO でサポートされていた「application/x-www-form-urlencoded」などのコンテンツタイプも使用できます。ペイロードが以前のバージョンで使用されていたものと同じであることを確認します。このドキュメントに記載されているペイロードは、コンテンツタイプが「application/vnd.com.citrix.sdx.login+json」の形式である場合にのみ適用されます。

  - **Payload**

```
{

    "login":
    {

        "username":"nsroot",
        "password":"verysecret"
     }

 }
```



```
11
12   <!--NeedCopy-->
```

- レスポンスペイロード
  - **Header**

```
1   HTTP/1.0 201 Created
2   Set-Cookie:
3   NITRO_AUTH_TOKEN=##87305E9C51B06C848F0942; path=/nitro/v2
4   <!--NeedCopy-->
```

注：アプライアンスでのそれ以降の NITRO 操作では、セッション ID を使用します。

注**:** デフォルトでは、アプライアンスへの接続は 30 分間の非アクティブ状態が続くと期限切れになります。ログインオブジェクトに新しいタイムアウト期間 (秒単位) を指定することで、タイムアウト期間を変更できます。たとえば、タイムアウト時間を 60 分に変更する場合、リクエストペイロードは次のようになります。

```
1  {
2
3      "login":
4      {
5
6          "username":"nsroot",
7          "password":"verysecret",
8          "timeout":3600
9       }
10
11   }
12
13 <!--NeedCopy-->
```

また、操作の要求ヘッダーにユーザー名とパスワードを指定することで、アプライアンスに接続して 1 回の操作を実行することもできます。たとえば、NetScaler インスタンスの作成中にアプライアンスに接続するには、以下を実行します。

- **URL**
- **HTTP** メソッド
- リクエスト
  - **Header**

```
1   X-NITRO-USER:nsroot
2   X-NITRO-PASS:verysecret
3   Content-Type:application/vnd.com.citrix.sdx.ns+json
4   <!--NeedCopy-->
```

  - **Payload**

```
1   {
2
```



```
3       "ns":
4       {
5
6           ...
7        }
8
9    }
10
11   <!--NeedCopy-->
```

- 応答。
  - **Header**

```
1   HTTP/1.0 201 Created
2   <!--NeedCopy-->
```

アプライアンスから切断するには、DELETE メソッドを使用します。

- **URL**
- **HTTP** メソッド削除
- リクエスト
  - **Header**

```
1   Cookie:NITRO_AUTH_TOKEN=tokenvalue
2   Content-Type:application/vnd.com.citrix.sdx.login+json
3   <!--NeedCopy-->
```

設定 **API**

NITRO プロトコルは、SDX アプライアンスのリソースの設定に使用できます。

各 SDX リソースには、実行する操作の種類に応じて一意の URL が関連付けられています。設定操作の URL は次の形式になります。`http://<IP>/nitro/v2/config/<resource_type>`

リソースを作成する

SDX アプライアンスにリソース（NetScaler インスタンスなど）を作成するには、特定のリソースオブジェクトにリソース名とその他の関連引数を指定します。たとえば、vpx1 という名前の NetScaler インスタンスを作成するには、次のようにします。

- **URL**
- **HTTP** メソッド
- リクエスト
  - **Header**


```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
<!--NeedCopy-->
```

- **Payload**

```
{

    "ns":
    {

        "name":"vpx1",
        "ip_address":"192.168.100.2",
        "netmask":"255.255.255.0",
        "gateway":"192.168.100.1",
        "image_name":"nsvpx-9.3-45_nc.xva",
        "vm_memory_total":2048,
        "throughput":1000,
        "pps":1000000,
        "license":"Standard",
        "profile_name":"ns_nsroot_profile",
        "username":"admin",
        "password":"admin",
        "network_interfaces":
        [
            {

                "port_name":"10/1"
             }
,
            {

                "port_name":"10/2"
             }

        ]
     }

 }

<!--NeedCopy-->
```

リソースの詳細と統計情報を取得する

SDX リソースの詳細は、次のようにして取得できます。

- SDX アプライアンス上の特定のリソースの詳細を取得するには、URL でリソースの ID を指定します。
- あるフィルタに基づいてリソースのプロパティを取得するには、URL でフィルタ条件を指定します。

URL の形式は次のとおりです。`http://<IP>/nitro/v2/config/<resource_type>?filter=<property1>:<value>,<property2>:<value>`

- リクエストの結果、アプライアンスから多くのリソースが返される可能性が高い場合は、結果を「ページ」に分割し、ページごとに取得することで、これらの結果をチャンク単位で取得できます。

  たとえば、53 個ある SDX 上の NetScaler インスタンスをすべて取得したいとします。53 件すべてを 1 つの大きな応答で取得する代わりに、結果をそれぞれ 10 個の NetScaler インスタンスのページ（合計 6 ページ）に分割するように構成します。次に、サーバーからページごとに取得します。

  ページサイズクエリ文字列パラメータでページ数を指定し、ページ番号クエリ文字列パラメータを使用して取得するページ番号を指定します。
  URL の形式は次のとおりです。`http://<IP>/nitro/v2/config/<resource_type>?pageno=<value>&pagesize=<value>`

  すべてのページを取得したり、ページを順番に取得したりする必要はありません。各リクエストは独立しており、リクエスト間でページサイズの設定を変更することもできます。

  注**:** リクエストによって返される可能性のあるリソースの数を把握するには、count クエリ文字列パラメーターを使用して、リソースそのものではなく、返されるリソースの数を尋ねることができます。使用可能な NetScaler インスタンスの数を取得するには、URL は次のようになります。
  `http://<IP>/nitro/v2/config/<resource_type>?count=yes`

ID が 123456a のインスタンスの構成情報を取得するには:

- **URL**
- **HTTP** メソッド GET

リソースを更新する

既存の SDX リソースを更新するには、PUT HTTP メソッドを使用します。HTTP リクエストペイロードで、名前と、変更する必要のあるその他の引数を指定します。たとえば、ID が 123456a の NetScaler インスタンスの名前を vpx2 に変更するには、

- **URL**
- **HTTP** メソッド
- ペイロードのリクエスト
  - **Header**

```
1 Cookie:NITRO_AUTH_TOKEN=tokenvalue
2 Content-Type:application/vnd.com.citrix.sdx.ns+json
3 <!--NeedCopy-->
```

  - **Payload**


```
{

    "ns":
    {

        "name":"vpx2",
        "id":"123456a"
     }

 }

<!--NeedCopy-->
```

リソースを削除する

既存のリソースを削除するには、削除するリソースの名前を URL に指定します。たとえば、ID が 123456a の NetScaler ADC インスタンスを削除するには、次のようにします。

- **URL**
- **HTTP** メソッド
- リクエスト
  - **Header**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
<!--NeedCopy-->
```

一括操作

複数のリソースを同時に照会または変更できるため、ネットワークトラフィックを最小限に抑えることができます。たとえば、同じ操作で複数の NetScaler SDX アプライアンスを追加できます。1 つのリクエストで、異なるタイプのリソースを追加することもできます。

NITRO では、一括操作内の一部の操作が失敗したことを考慮して、次のいずれかの動作を構成できます。

- 出口。最初のエラーが発生すると、実行は停止します。エラー発生前に実行されたコマンドがコミットされます。
- 続ける。一部のコマンドが失敗した場合でも、リスト内のすべてのコマンドが実行されます。

注:`X-NITRO-ONERROR` パラメータを使用して、リクエストヘッダーで必要な動作を設定します。

1 回の操作で 2 つの NetScaler ADC リソースを追加し、1 つのコマンドが失敗した場合に続行するには:

- **URL**。
- **HTTP** メソッド。

- ペイロードをリクエストします。

  - **Header**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
X-NITRO-ONERROR:continue
<!--NeedCopy-->
```

  - **Payload**

```
{

    "ns":
    [
        {

            "name":"ns_instance1",
            "ip_address":"10.70.136.5",
            "netmask":"255.255.255.0",
            "gateway":"10.70.136.1"
         }
,
        {

            "name":"ns_instance2",
            "ip_address":"10.70.136.8",
            "netmask":"255.255.255.0",
            "gateway":"10.70.136.1"
         }

    ]
 }

<!--NeedCopy-->
```

1 つの操作で複数のリソース（NetScaler と 2 人の MPS ユーザー）を追加し、1 つのコマンドが失敗しても続行するには:

- **URL**。
- **HTTP** メソッド。POST
- ペイロードをリクエストします。

  - **Header**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
X-NITRO-ONERROR:continue
<!--NeedCopy-->
```

  - **Payload**


```
{

    "ns":
    [
        {

            "name":"ns_instance1",
            "ip_address":"10.70.136.5",
            "netmask":"255.255.255.0",
            "gateway":"10.70.136.1"
         }
,
        {

            "name":"ns_instance2",
            "ip_address":"10.70.136.8",
            "netmask":"255.255.255.0",
            "gateway":"10.70.136.1"
         }

    ],
     "mpsuser":
    [
        {

            "name":"admin",
            "password":"admin",
            "permission":"superuser"
         }
,
        {

            "name":"admin",
            "password":"admin",
            "permission":"superuser"
         }

    ]
 }

<!--NeedCopy-->
```

例外ハンドリング

errorcode フィールドはオペレーションのステータスを示します。

- エラーコード 0 は、操作が成功したことを示します。
- 0 以外のエラーコードは、NITRO 要求の処理中にエラーが発生したことを示します。

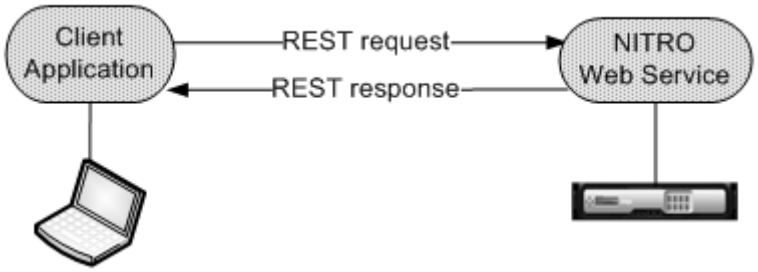
エラーメッセージフィールドには、簡単な説明と失敗の性質が表示されます。

NITRO の仕組み

November 23, 2023

NITRO インフラストラクチャは、NetScaler SDX アプライアンス上で実行されるクライアントアプリケーションと NITRO Web サービスで構成されています。クライアントアプリケーションと NITRO Web サービス間の通信は、HTTP または HTTPS を使用した REST アーキテクチャに基づいています。

図 1: NITRO workflow



ワークフローを詳述する手順

1. クライアントアプリケーションは REST 要求メッセージを NITRO Web サービスに送信します。SDK を使用する場合、API 呼び出しは適切な REST リクエストメッセージに変換されます。
2. Web サービスが REST リクエストメッセージを処理します。
3. NITRO Web サービスは、対応する REST 応答メッセージをクライアントアプリケーションに返します。SDK を使用する場合、REST レスポンスメッセージは API 呼び出しの適切なレスポンスに変換されます。

ネットワーク上のトラフィックを最小限に抑えるには、リソースの状態全体をサーバから取得します。リソースの状態をローカルで修正します。その後、1 回のネットワークトランザクションでサーバーにアップロードし直します。

注: リソースに対するローカル操作 (プロパティの変更) は、オブジェクトの状態が明示的にアップロードされるまでサーバー上の状態には影響しません。

NITRO API は本質的に同期的です。つまり、クライアントアプリケーションは NITRO Web サービスからの応答を待ってから、別の NITRO API を実行します。

Java SDK

November 23, 2023

SDX NITRO API は、API の範囲と目的に応じてシステム API と構成 API に分類されます。NITRO 操作のトラブルシューティングも可能です。

システム **API**

NITRO を使用する最初のステップは、SDX アプライアンスとのセッションを確立し、管理者の資格情報を使用してセッションを認証することです。

アプライアンスの IP アドレスとアプライアンスに接続するプロトコル (HTTP または HTTPS) を指定して、nitro_service クラスのオブジェクトを作成します。次に、このオブジェクトを使用し、管理者のユーザー名とパスワードを指定して、アプライアンスにログオンします。

注: そのアプライアンスにはユーザーアカウントが必要です。実行できる構成操作は、アカウントに割り当てられている管理者の役割によって制限されます。

次のサンプルコードは、HTTPS プロトコルを使用して IP アドレス 10.102.31.16 の SDX アプライアンスに接続します。

```
1 //Specify the IP address of the appliance and service type
2 nitro_service nitroservice = new nitro_service ("10.102.31.16", "https"
      );
3
4 //Specify the login credentials
5 nitroservice.login("nsroot", "verysecret");
6 <!--NeedCopy-->
```

注:
nitro_service オブジェクトは、アプライアンスでのそれ以降の NITRO 操作すべてで使用します。

アプライアンスから切断するには、以下のように`logout()`メソッドを呼び出します。

```
1 nitroservice.logout();
2 <!--NeedCopy-->
```

設定 **API**

NITRO プロトコルは、SDX アプライアンスのリソースの設定に使用できます。

リソースを構成するための API は、com.citrix.sdx.nitro.resource.config という形式のパッケージまたは名前空間にグループ化されます。. これらのパッケージまたは名前空間にはそれぞれ、リソースを構成するための API を提供します。

たとえば、NetScaler リソースには com.citrix.sdx.nitro.resource.config.ns パッケージまたは名前空間があります。

リソースクラスは、その他多くの操作を実行するための API を提供します。これらの操作には、リソースの作成、リソースの詳細と統計の取得、リソースの更新、リソースの削除、リソースに対する一括操作の実行などがあります。

リソースを作成する

SDX アプライアンスにリソース（NetScaler インスタンスなど）を作成するには、次の手順を実行します。

1. 対応するプロパティー名を使用して、リソースの必須プロパティーの値を設定します。その結果、リソースに必要な詳細を含むリソースオブジェクトが生成されます。
   注: これらの値はクライアント上でローカルに設定されます。この値は、オブジェクトがアップロードされるまでアプライアンスに反映されません。
2. static add () メソッドを使用して、リソースオブジェクトをアプライアンスにアップロードします。

次のサンプルコードは、SDX アプライアンスに「ns_instance」という名前の NetScaler インスタンスを作成します。

```
ns newns = new ns();

//Set the properties of the NetScaler locally
newns.set_name("ns_instance");
newns.set_ip_address("10.70.136.5");
newns.set_netmask("255.255.255.0");
newns.set_gateway("10.70.136.1");
newns.set_image_name("nsvpx-9.3.45_nc.xva");
newns.set_profile_name("ns_nsroot_profile");
newns.set_vm_memory_total(new Double(2048));
newns.set_throughput(new Double(1000));
newns.set_pps(new Double(1000000));
newns.set_license("Standard");
newns.set_username("admin");
newns.set_password("admin");

int number_of_interfaces = 2;
network_interface[] interface_array = new network_interface[
    number_of_interfaces];

//Adding 10/1
interface_array[0] = new network_interface();
interface_array[0].set_port_name("10/1");

//Adding 10/2
interface_array[1] = new network_interface();
interface_array[1].set_port_name("10/2");

newns.set_network_interfaces(interface_array);

//Upload the NetScaler instance
ns result = ns.add(nitroservice, newns);
<!--NeedCopy-->
```


リソース詳細の取得

SDX アプライアンス上のリソースのプロパティを取得するには、次の手順を実行します。

1. get () メソッドを使用して、アプライアンスから設定を取得します。結果はリソースオブジェクトです。
2. 対応するプロパティ名を使用して、必要なプロパティをオブジェクトから抽出します。

次のサンプルコードは、すべての NetScaler リソースの詳細を取得します。

```
//Retrieve the resource object from the SDX appliance
ns[] returned_ns = ns.get(nitroservice);

//Extract the properties of the resource from the object
System.out.println(returned_ns[i].get_ip_address());
System.out.println(returned_ns[i].get_netmask());
<!--NeedCopy-->
```

リソース統計の取得

SDX アプライアンスは、その機能の使用状況に関する統計を収集します。これらの統計は NITRO を使用して取得できます。

次のサンプルコードは、ID が 123456a の NetScaler インスタンスの統計を取得します。

```
ns obj = new ns();
obj.set_id("123456a");
ns stats = ns.get(nitroservice, obj);
System.out.println("CPU Usage:" + stats.get_ns_cpu_usage());
System.out.println("Memory Usage:" + stats.get_ns_memory_usage());
System.out.println("Request rate/sec:" +stats.get_http_req());
<!--NeedCopy-->
```

リソースを更新する

アプライアンス上の既存のリソースのプロパティを更新するには、次の手順を実行します。

1. id プロパティーを、更新するリソースの ID に設定します。
2. 対応するプロパティー名を使用して、リソースの必須プロパティーの値を設定します。結果はリソースオブジェクトです。
   注: これらの値はクライアント上でローカルに設定されます。この値は、オブジェクトがアップロードされるまでアプライアンスに反映されません。
3. update () メソッドを使用して、リソースオブジェクトをアプライアンスにアップロードします。

次のサンプルコードでは、ID が 123456a の NetScaler インスタンスの名前を「ns_instance_new」に更新します。


```
ns update_obj = new ns();

//Set the ID of the NetScaler to be updated
update_obj.set_id("123456a");

//Get existing NetScaler details
update_obj = ns.get(nitroservice, update_obj);

//Update the name of the NetScaler to "ns_instance_new" locally
update_obj.set_name("ns_instance_new");

//Upload the updated NetScaler details
ns result = ns.update(nitroservice, update_obj);
<!--NeedCopy-->
```

リソースを削除する

既存のリソースを削除するには、削除するリソースの ID を引数として渡して、リソースクラスで静的メソッド delete () を呼び出します。

次のサンプルコードは、ID 1 の NetScaler インスタンスを削除します。

```
ns obj = new ns();
obj.set_id("123456a");
ns.delete(nitroservice, obj);
<!--NeedCopy-->
```

一括操作

複数のリソースを同時に照会または変更できるため、ネットワークトラフィックを最小限に抑えることができます。たとえば、同じ操作で複数の NetScaler SDX アプライアンスを追加できます。

各リソースクラスには、リソースの追加、更新、削除のためのリソースの配列を取るメソッドがあります。一括操作を実行するには、各操作の詳細をローカルで指定し、その詳細を一度にサーバーに送信します。

NITRO では、一括操作内の一部の操作が失敗したことを考慮して、次のいずれかの動作を構成できます。

- 出口。最初のエラーが発生すると、実行は停止します。エラー発生前に実行されたコマンドがコミットされます。
- 続ける。一部のコマンドが失敗した場合でも、リスト内のすべてのコマンドが実行されます。

注**:**
nitro_service () メソッドで
`onerror` param を設定して、アプライアンスとの接続を確立する際に必要な動作を設定します。

次のサンプルコードは、1 回の操作で 2 つの ADC アプライアンスを追加します。


```
ns[] newns = new ns[2];

//Specify details of first NetScaler
newns[0] = new ns();
newns[0].set_name("ns_instance1");
newns[0].set_ip_address("10.70.136.5");
newns[0].set_netmask("255.255.255.0");
newns[0].set_gateway("10.70.136.1");
...
...
...

//Specify details of second NetScaler
newns[1] = new ns();
newns[1].set_name("ns_instance2");
newns[1].set_ip_address("10.70.136.8");
newns[1].set_netmask("255.255.255.0");
newns[1].set_gateway("10.70.136.1");
...
...

//upload the details of the NetScalers to the NITRO server
ns[] result = ns.add(nitroservice, newns);
<!--NeedCopy-->
```

例外ハンドリング

errorcode フィールドはオペレーションのステータスを示します。

- エラーコード 0 は、操作が成功したことを示します。
- 0 以外のエラーコードは、NITRO 要求の処理中にエラーが発生したことを示します。

エラーメッセージフィールドには、簡単な説明と失敗の性質が表示されます。

com.citrix.sdx.nitro.exception.nitro_exception クラスは、NITRO API の実行中のすべての例外をキャッチします。例外に関する情報を取得するには、`getErrorCode()` メソッドを使用します。

エラーコードの詳細については、`<NITRO_SDK_HOME>/doc`フォルダにある API リファレンスを参照してください。