オンプレミス向け Citrix SD-WAN Orchestrator 14.4

Contents

SD-WAN Orchestrator for On-Premises 14.4 リリースのリリース ノート

December 10, 2024

このリリース ノート ドキュメントでは、Citrix SD-WAN Orchestrator for On-Premises リリース ビルド 14.4 の機能強化と変更、修正された問題と既知の問題について説明します。

注記

このリリース ノート ドキュメントには、セキュリティ関連の修正は含まれていません。セキュリティ関連の修正とアドバイザリの一覧については、Citrix セキュリティ速報を参照してください。

既知の問題

リリース 14.4 に存在する問題。

Citrix SD-WAN Orchestrator for On-Premises で SD-WAN ソフトウェアを公開すると、次のエラーが発生して失敗する場合があります。

```
Failed to fetch software details from Citrix cloud.
```

回避策: Citrix SD-WAN Orchestrator for On-Premises 経由で Citrix Cloud からログアウトして再度ログインし、SD-WAN ソフトウェアを公開します。

[SDW-24980]

オンプレミス用 **SD-WAN Orchestrator** のリリースノート **14.3**

October 26, 2022

このリリースノートドキュメントでは、オンプレミスリリースビルド 14.3 用の Citrix SD-WAN Orchestrator の機能強化と変更、修正された問題と既知の問題について説明します。

注

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

新機能

ビルド 14.3 で利用できる機能強化と変更点。

構成と管理

QoS ポリシー

QoS ポリシーページは、ユーザーエクスペリエンスを向上させるために刷新されました。カスタムアプリケーションルール、アプリケーションルール、HDX ルール、アプリケーショングループルール、IP ルール、デフォルト IP プロトコルルールなどのオプションが、新しいルックアンドフィールで強化されました。

[SDW-11029]

プラットフォームとシステム

管理 **IP/**帯域内 **IP** の強化:

**** 次の **UI** 画面の管理 **IP** 列とデバイスアクセス列が拡張され ** 、デバイスがオンプレミス向け Citrix SD-WAN Orchestrator との通信に使用している IP アドレスの種類に基づいて、帯域内 IP アドレスまたは管理 IP アドレスのいずれかが表示されるようになりました。

- プロバイダー > レポート > インベントリ > 詳細
- 顧客 > 設定 > ネットワークホーム > アクション > 詳細を表示
- 顧客 > レポート > インベントリ > 詳細
- サイト > ダッシュボード > デバイス

[SDW-23353]

レポートを CSV としてエクスポート

CSV 形式でエクスポート機能を使用すると、任意の時系列 (時間単位、週単位など) のパスグラフポイント (仮想パス/メンバーパス) を Excel のカンマ区切り値 (CSV) ファイルとしてダウンロードし、特定のサイトレポートのすべての異なるデータポイントをプロットできます。

[SDW-20988]

証明書の認証

オンプレミス向け Citrix SD-WAN Orchestrator は、追加のセキュリティ機能として公開鍵基盤（PKI）を使用して、静的および動的仮想パスのアプライアンス認証をサポートします。この機能を有効にすると、アプライアンスが交換を開始することによって PKI 証明書をデータパス上に配布することにより、既存の仮想パス認証メカニズムが拡張されます。PKI 拡張では、侵害された証明書を一元的に失効するための証明書失効リスト (CRL) 管理もサポートしています。

[SDW-19295]

SD-WAN Orchestrator

構成を表示 (プレビュー)

オンプレミス向け Citrix SD-WAN Orchestrator では、サイトレベルで「構成を表示」ページが導入されています。このページには、複数のサブシステムにわたるサイトの構成の詳細な概要が表示されます。

[SDW-22284]

ネットワークレベルのリアルタイム統計、サイトレベルのリアルタイム統計

これで、** ファイアウォール接続の名前がファイアウォール統計に変更されました **。NAT ポリシーとフィルタポリシーが統計タイプドロップダウンリストに新しく追加されました。また、リアルタイム統計オプションが再構成され、次のカテゴリに分類されました。

- ネットワーク統計
- アプリケーション統計
- ルート統計情報

[SDW-20966]

モバイルブロードバンド設定とモバイルブロードバンドステータス

これで、ブロードバンドインターネット接続を使用して、Citrix SD-WAN アプライアンスをサイトからネットワークに接続できます。このモバイルブロードバンドのステータスと設定のサポートは、内蔵モデムで利用できます。また、デバイスとアクティブな SIM のブロードバンド設定のステータスを表示することもできます。

[SDW-10907]

解決された問題

ビルド 14.3 で対処されている問題。

構成と管理

PKI 証明書は、オンプレミス UI 用 Citrix SD-WAN Orchestrator に表示されませんでした。この問題は、PKI 証明書の組織単位フィールドが必須だったために発生しました。

[SDW-23726]

その他

一部のサイトは、オンプレミス UI 用 Citrix SD-WAN Orchestrator に接続できません。

[SDWANHELP-2601]

既知の問題

リリース 14.3 に存在する問題。

Citrix SD-WAN Orchestrator for On-Premises UI の［レポート］>［使用状況］>［アプリケーション］ページでは、アプリケーションおよびアプリケーションカテゴリのグラフは空です。

[SDW-23817]

UI の［展開］**>**［設定］**>**［部分的なサイトのアップグレード］>［ソフトウェアバージョン］ページで以前に選択したソフトウェアバージョンは、ユーザーがこのページに戻っても保持されません。

回避策:[展開] > [サイトの選択] に移動して、サイトごとにサイトの一部アップグレードソフトウェアバージョンを手動で選択します。

[SDW-22374]

管理インターフェイス設定の構成を実行した後に、UI にエラーが表示されることがあります。ただし、構成は成功しており、更新された設定を UI に表示するには更新が必要です。

[SDW-22139]

プロバイダー管理の設定では、プロバイダー管理者が追加したアナウンスがログイン時に顧客に表示されません。

[SDW-18491]

オンプレミス用 **SD-WAN Orchestrator** のリリースノート **13.2.1** リリース

October 26, 2022

このリリースノートドキュメントでは、Citrix SD-WAN Orchestrator for On-Premises リリースビルド 13.2.1 の機能強化と変更、修正された問題と既知の問題について説明します。

注

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

解決された問題

ビルド 13.2.1 で対処されている問題。

プラットフォームとシステム

オンプレミス向け Citrix SD-WAN Orchestrator は、TCP 同期パケットを AWS エンドポイントに送信します。

[SDW-23477]

既知の問題

リリース 13.2.1 に存在する問題。

その他

一部のサイトは、オンプレミス UI 用 Citrix SD-WAN Orchestrator に接続できません。

回避策:172.17.x.x サブネット以外の別のサブネットを使用してください。

[SDWANHELP-2601]

一部のシナリオでは、サイトに Cloud Direct をデプロイして構成をプッシュした後（ステージングとアクティベーション）、Cloud Direct サービスが起動しません。

回避策：サイトごとに Cloud Direct サービスを手動で有効にします。

[SDW-22493]

UI の［展開］**>**［設定］**>**［部分的なサイトのアップグレード］>［ソフトウェアバージョン］ページで以前に選択したソフトウェアバージョンは、ユーザーがこのページに戻っても保持されません。

回避策:[展開] > [サイトの選択] に移動して、サイトごとにサイトの一部アップグレードソフトウェアバージョンを手動で選択します。

[SDW-22374]

管理インターフェイス設定の構成を実行した後に、UI にエラーが表示されることがあります。ただし、構成は成功しており、更新された設定を UI に表示するには更新が必要です。

[SDW-22139]

プロバイダー管理の設定では、プロバイダー管理者が追加したアナウンスがログイン時に顧客に表示されません。

[SDW-18491]

プラットフォームとシステム

ネットワーク統計プロバイダーがセッションを再利用しているため、Citrix SD-WAN アプライアンスの UI にアクセスできません。これにより、HTTPD プロセスが不適切に動作しました（まれに）。

[SDW-23392]

Citrix SD-WAN 210 アプライアンスでは、SE アドオンライセンスを削除すると、サービスが無効になります。

回避策：SE アドオンライセンスを削除する（または）AE から SE ライセンスに移行する前に、セキュリティプロファイルを含むファイアウォールポリシーを削除し、アプライアンスを帯域外管理として設定し（帯域内管理が設定されている場合）、ステージングとアクティベーションプロセスを進めて、次の段階に進んでください。アプライアンスを Standard Edition に変換します。

[SDW-18031]

オンプレミス用 **SD-WAN Orchestrator** のリリースノート **13.2**

October 26, 2022

このリリースノートドキュメントでは、オンプレミスリリースビルド 13.2 用の Citrix SD-WAN Orchestrator の機能強化と変更、修正された問題と既知の問題について説明します。

注

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

新機能

ビルド 13.2 で利用できる機能強化と変更点。

構成と管理

以前のバージョンを復元

オンプレミス向け Citrix SD-WAN Orchestrator には、以前のバージョンの復元機能が導入されています。[以前のバージョンを復元する] オプションを選択すると、Citrix SD-WAN Orchestrator for On-Premises は以前の構成のネットワーク全体のアクティブ化を開始し、ネットワーク上で以前にアクティブ化された構成（/ソフトウェア）を復元します。

[SDW-22042]

ライセンスの強化

ライセンスを取得して実稼働環境にアップグレードすると、[**Upgrade to** Production] ボタンのラベルが [**Upgraded to Production**] に変わり、ライセンスのアップグレードが既に完了していることを示します。

[SDW-20674]

API-サイトアドレス解決:

API を使用してサイトを作成すると、サイトアドレスは Google Maps API を使用してサイト作成の一部として渡される緯度と経度の値を使用して自動的に取得されます。

[SDW-20654]

ネットワークメニューの再構築

Citrix SD-WAN Orchestrator for On-Premises グローバル構成メニューは、Citrix SD-WAN の主要な機能をより適切に分類して見つけやすくするために再構築されました。また、各配信サービスは、配信チャネルとすべての主要機能ページの両方で利用できるようになり、グローバルまたは機能ごとのコンテキストから管理者設定に対応できるようになりました。たとえば、管理者は 0 日目に配信チャネルで Citrix SIA サービスをグローバルに設定し、クラウドセキュリティサービスのセキュリティで N 日目の機能を実行して変更を加えることもできます。

ネットワークレベルの設定ページは次のように拡張されました。

- ****** ネットワーク構成ホームの名前がネットワークホームに変更されました **。
- [設定] **>** [配信チャネル] の **[**配信サービス ****]** の名前が **[**** サービス定義] に変更されました。
- [構成] **>** [セキュリティ] で、[ネットワーク暗号化] ページの名前が [ネットワークセキュリティ] に変更されました。
- [設定] **>** [セキュリティ] の下のページは、簡単に見つけられるように次のように論理的にグループ化されています。

グループ	メニューオプション
SD-WAN オーバーレイセキュリティ	Network Security
	仮想パス IPsec
ベースファイアウォール	ファイアウォールゾーン
	ファイアウォールのデフォルト
	ファイアウォールポリシー
IPsec と GRE	証明書
	IPsec 暗号化プロファイル
	IPsec サービス
	GRE サービス
Wi-Fi セキュリティ	RADIUS プロファイル
	SSID プロファイル

- 次のサービスは、［設定］>［配信チャネル］**>**［サービス定義］または ［設定］**>**［セキュリティ］から設定できます。

  - IPsec
  - GRE

- **ECMP** グループページは [構成] **>** [ルーティング] に移動されました。
- **BGP**、**OSPF**、マルチキャストグループ、**VRRP** は、[設定] **>** [ルーティング] でネットワークレベルで設定できます。サイトを選択して [**Go**] をクリックできます。サイトレベルの特定の設定ページが表示されます。以前は、これらの構成はサイトレベルでしか使用できませんでした。
- Cloud Direct サービスは、[設定] **>** [配信チャネル] **>** [サービス定義] から、または **[**設定] **>** [ルーティング] **> [SaaS & Cloud On Ramp**
- [アプリケーションと **DNS** 設定] ページの名前が [アプリの設定とグループ] に変更されました。
- 以前は [構成] **>** [アプリと **DNS** の設定] **>** [アプリケーション設定] にあった **DPI** 関連の設定は、[構成] **>** [アプリ設定とグループ] **>** [**DPI** 設定] に移動されました。
- [設定] **>** [配信サービス] にある [ネットワークロケーションサービス ******] ページは、**[**** 設定] の直下にあります。

[SDW-14698]

エラー発生時のロールバック

ネットワーク展開（アクティベーション）中に、オンプレミス用 Citrix SD-WAN Orchestrator に接続できなかったサイトは以前のバージョンにロールバックされ、接続の復元が試みられます。このようなサイトでのロールバックは、特定の時間（現在は 30 分）オフラインになった後に開始されます。

ネットワーク内のいずれかのサイトがロールバックしようとすると、ポップアップボックスが開き、ネットワーク全体をロールバックするか、それらのサイトを無視してデプロイを終了するかの 2 つのオプションがあります。

ネットワーク展開を開始する前に、Rollback on Error 機能を有効にする必要があります。

[SDW-11153]

その他

IP ルール

「**IP** ルール」**>**「仮想パストラフィックポリシー」セクションに「オーバーライドサービス」オプションが追加されました。****** トラフィックポリシーがオーバーライドサービスとして選択されている場合 ******、仮想パスサービスがオーバーライドするサービスタイプを [イントラネット]、[インターネット]、[パススルー]、または [破棄] から選択できます。

[SDW-22213]

設定の違い

ネットワークレベルの **Configuration Diff 機能が新たに追加されました。**Config Diff 機能を使用すると、任意の 2 つのバージョンの設定チェックポイントの違いを確認できます。グローバルレベルとサイトレベルの両方で構成を表示することもできます。

[SDW-4563]

アプライアンスの設定

オンプレミス向け Citrix SD-WAN Orchestrator には、管理ネットワークの優先順位を設定するオプションが導入されています。ネットワークの管理インターフェイスとして [インバンド] または [アウトオブバンド] を選択できます。このオプションは、SD-WAN アプライアンスが 11.4.2 以降のソフトウェアバージョンを実行している場合にのみ使用できます。

[NSSDW-35774]

プラットフォームとシステム

証明書の認証

オンプレミス向け Citrix SD-WAN Orchestrator は、追加のセキュリティ機能として公開鍵インフラストラクチャ（PKI）を使用して、静的および動的仮想パスのアプライアンス認証をサポートしています。この機能を有効にすると、アプライアンスが交換を開始することによって PKI 証明書をデータパス上に配布することにより、既存の仮想パス認証メカニズムが拡張されます。PKI 拡張では、侵害された証明書を一元的に失効するための証明書失効リスト (CRL) 管理もサポートしています。

[SDW-19295]

[プロバイダー監査ログとネットワーク監査ログの強化](/ja-jp/citrix-sd-wan-orchestrator-on-premises/troubleshooting/network-log.html)

** プロバイダー監査ログとネットワーク監査ログページは ** 、次のオプションで拡張されました。

- **Source IP** -このフィールドには、SD-WAN 機能が設定されているエンドポイントの IP アドレスが表示されます。このフィールドは、「監査ログ」ページと「監査情報」ページに表示されます。
- **CSV** としてエクスポート -このオプションでは、監査ログを CSV 形式にエクスポートできます。
- 変更内容 -このセクションには、UI を通じて機能に加えられたすべての変更のログが表示されます。ログペイロード切り替えボタンを有効にすると、監査情報ページにこのセクションが表示されます。現在、このセクションはネットワーク監査情報ページにあります。

[SDW-19219]

ドメイン名ベースのアプリケーションのカスタムポート、プロトコル構成

ドメイン名ベースのアプリケーションは、オンプレミス向け Citrix SD-WAN Orchestrator で構成可能なポートとプロトコルをサポートするようになりました。[**Configure Port**] チェックボックスをオンにすると、必要に応じて任意のポートまたはポート範囲を編集、追加、または削除できます。また、プロトコルを [TCP]、[UDP]、または [任

意] に変更または選択できます。以前は (また、[ポートを設定] チェックボックスがオフの場合)、アプリケーションの下にグループ化されたドメインでは、ポート 80 と 443、およびプロトコル **Any** のみがサポートされていました。

[NSSDW-29930]

解決された問題

ビルド 13.2 で対処されている問題。

その他

オンプレミス UI 用 Citrix SD-WAN Orchestrator にアクセスできません。この問題は、{page.productname}} で実行されているサービスがハートビート要求に応答せず、再起動の制限を超えた場合に発生します。

[SDWANHELP-2544]

オンプレミス用 Citrix SD-WAN Orchestrator では、ソフトウェアアップグレードパッケージのアップロードが失敗します。この問題は、ソフトウェアパッケージのアップロード中にユーザーがアップロードページから移動したときに発生します。

[SDWANHELP-2495]

プラットフォームとシステム

ソフトウェアバージョン 11.4.1 を実行している SD-WAN アプライアンスは、オンプレミス向け Citrix SD-WAN Orchestrator からアプライアンスにライセンスが割り当てられると、グレースモードになります。

[SDW-23171]

既知の問題

リリース 13.2 に存在する問題。

構成と管理

新しくインポートされた Citrix SD-WAN Orchestrator for On-Premises インスタンスで、ステージングがパッケージ準備中の状態で止まる。この問題は、新しい仮想マシンを作成した直後にステージングプロセスが開始された場合に発生します。

回避策: ステージングプロセスを再試行します。

[SDW-20863]

その他

ソフトウェアバージョン 11.4.2 を実行している SD-WAN アプライアンスのサービス状態が、オンプレミス UI 用の Citrix SD-WAN **Orchestrator** で **BAD** と表示されます。表示されるエラーメッセージは「**Orchestrator** の **URL** からの応答なし」です。この問題は、オンプレミス用 Citrix SD-WAN Orchestrator でカスタムドメインが構成されている場合に発生します。

回避策：SD-WAN アプライアンスを再起動します。

[SDW-2332]

部分的なサイトアップグレードリストが変更され、ネットワーク上で変更管理 （ステージングおよびアクティベーション）が実行されると、**PSU** 内のサイトの **Activation Failed**（**ER101** ）エラーメッセージが表示され、以前のバージョンへの復元操作が失敗します。

回避策:「前のバージョンを復元」アクションを適用する前に、変更管理をもう一度実行してください。

[SDW-23227]

一部のシナリオでは、サイトに Cloud Direct をデプロイして構成をプッシュした後（ステージングしてアクティブ化）、Cloud Direct サービスが起動しません。

回避策：サイトごとに Cloud Direct サービスを手動で有効にします。

[SDW-22493]

UI の［展開］**>**［設定］**>**［部分的なサイトのアップグレード］>［ソフトウェアバージョン］ページで以前に選択したソフトウェアバージョンは、ユーザーがこのページに戻っても保持されません。

回避策:[展開] > [サイトの選択] に移動して、サイトごとにサイトの一部アップグレードソフトウェアバージョンを手動で選択します。

[SDW-22374]

管理インターフェイス設定の構成を実行した後に、UI にエラーが表示されることがあります。ただし、構成は成功しており、更新された設定を UI に表示するには更新が必要です。

[SDW-22139]

プロバイダー管理の設定では、プロバイダー管理者が追加したアナウンスがログイン時に顧客に表示されません。

[SDW-18491]

プラットフォームとシステム

お客様は自分の HTTP サーバにプッシュ通知を送信できません。

[SDW-23134]

オンプレミス **12.3** リリース用 **SD-WAN Orchestrator** のリリースノート

July 19, 2023

このリリースノートドキュメントでは、オンプレミスリリースビルド 12.3 用の Citrix SD-WAN Orchestrator の機能強化と変更、修正された問題と既知の問題について説明します。

注

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

新機能

ビルド 12.3 で利用できる機能強化と変更点。

その他

消去設定

オンプレミス向け Citrix SD-WAN Orchestrator を使用すると、統計情報の消去間隔の日数（デフォルトでは 30 日）よりも古い履歴データを消去できます。データが消去されると、選択した日数より古い履歴データは削除され、使用できなくなります。消去処理は、SD-WAN アプライアンスに設定されているタイムゾーンに基づいて、毎日午前 12:48 頃に行われます。

[SDW-20402]

ゼロタッチ導入インターフェース

オンプレミス向け Citrix SD-WAN Orchestrator でゼロタッチ展開（ZTD）インターフェイスを有効にできます。双方向認証によって保護された ZTD インターフェイスは、SD-WAN アプライアンスと Citrix SD-WAN Orchestrator for オンプレミス用の安全な通信インターフェイスを提供します。

[SDW-19152]

リンクの仮想パス設定

WAN リンクに関連する仮想パスと動的仮想パスの帯域幅をカスタマイズできます。この機能は、一部のサイトで帯域幅の問題によりパフォーマンスが低下する兆候が見られる場合に役立ちます。

[SDW-9760]

SD-WAN Orchestrator

Syslog サーバー設定

オンプレミス向け Citrix SD-WAN Orchestrator は、SD-WAN アプライアンスの Syslog サーバー設定の構成をサポートします。Syslog 設定を有効にすると、SD-WAN アプライアンスのシステムアラートとイベント詳細を外部 Syslog サーバーに送信できます。

[SDW-13990]

解決された問題

ビルド 12.3 で対処されている問題。

その他

特定の条件下では、帯域内管理が有効で帯域外管理が接続されていると、SD-WAN アプライアンスが帯域内管理経由で Citrix SD-WAN Orchestrator と通信できません。

[SDWANHELP-2368]

動的仮想パスの値が 8 以上に設定されている場合、最大許容制限は 32 ですが、UI に誤ってエラーが表示されます。この問題は VPXL および 4100 SE アプライアンスで発生します。

[SDWANHELP-2354]

部分的なサイトアップグレード設定の [ソフトウェアバージョン] ドロップダウンリストには、[インフラストラクチャ] > [**Orchestrator** 管理] > [ソフトウェアイメージ**]** で公開されているバージョンのみではなく、サポートされているすべてのソフトウェアバージョンが表示されます。アプライアンス。

サイトの一部アップグレードに記載されているソフトウェアバージョンが [インフラストラクチャ] > [**Orchestrator** 管理] > [ソフトウェアイメージ] > [アプライアンス] で公開できない場合、そのリリースでは部分的なサイトアップグレードを実行できません。

[SDW-20992]

既知の問題

リリース 12.3 に存在する問題。

構成と管理

新しくインポートされた Citrix SD-WAN Orchestrator for On-Premises インスタンスで、ステージングがパッケージ準備中の状態で止まる。この問題は、新しい仮想マシンを作成した直後にステージングプロセスが開始された場合に発生します。

回避策: ステージングプロセスを再試行します。

[SDW-20863]

その他

VMware ESXi 13 を実行しているオンプレミス用 Citrix SD-WAN Orchestrator が再起動に失敗し、不良状態になります。

回避策：VMware ESXi バージョン 9 を使用してください。

[SDWANHELP-2182]

一部のシナリオでは、サイトに Cloud Direct をデプロイして構成をプッシュした後（ステージングしてアクティブ化）、Cloud Direct サービスが起動しません。

回避策：サイトごとに Cloud Direct サービスを手動で有効にします。

[SDW-22493]

ユーザーがサイトの一部アップグレードを実行すると、ステージングプロセスが断続的に失敗します。UI には、「例外によるステージング失敗」というエラーメッセージが表示されます。

回避策: ステージングプロセスを再試行します。

[SDW-22398]

UI の［展開］**>**［設定］**>**［部分的なサイトのアップグレード］>［ソフトウェアバージョン］ページで以前に選択したソフトウェアバージョンは、ユーザーがこのページに戻っても保持されません。

回避策:[展開] > [サイトの選択] に移動して、サイトごとにサイトの一部アップグレードソフトウェアバージョンを手動で選択します。

[SDW-22374]

管理インターフェイス設定の構成を実行した後に、UI にエラーが表示されることがあります。ただし、構成は成功しており、更新された設定を UI に表示するには更新が必要です。

[SDW-22139]

ユーザーは、UI の [インフラストラクチャ] > [**Orchestrator** 管理**] > [**ソフトウェアイメージ**]** ページにアップロードされた **Citrix SD-WAN Orchestratorfor On-Premises **tar.gz** イメージファイルを削除できません ** 。表示されるエラーメッセージは、「ソフトウェアパッケージの削除中にエラーが発生しました」です。

回避策: 新しいソフトウェアパッケージをアップロードします。以前にアップロードされたファイルは自動的に削除されます。

[SDW-22137]

UI の [構成] > [****** ネットワーク構成のホーム **] ページでは、構成ファイルがアップロードされた直後に、セカンダリ SD-WAN アプライアンスの Orchestrator 接続ステータスがオンラインで表示されます。ただし、サイトの構成を保存すると、正しいステータスが表示されます。

[SDW-20913]

プロバイダー管理の設定では、プロバイダー管理者が追加したアナウンスがログイン時に顧客に表示されません。

[SDW-18491]

アプライアンスのデータベースバックアップを、同じリリースのオンプレミス用 Citrix SD-WAN Orchestrator を搭載した別のアプライアンスに復元しても、ユーザーの詳細は復元されません。復元されたアプライアンスで、バックアップされたデータベースと同じユーザー名でユーザーを作成すると、次のエラーが表示されます。

`User has a role already assigned`。

回避策: バックアップしたデータベースに存在しなかった別のユーザー名でユーザーを作成します。

[SDW-15984]

プラットフォームとシステム

Citrix SD-WAN 210 アプライアンスでは、アドオンライセンスを削除すると、サービスが無効になります。

回避策：セキュリティプロファイルを含むファイアウォールポリシーを削除してステージングし、変更を有効にしてアプライアンスを標準エディションに変換します。

[SDW-18031]

オンプレミス用 **SD-WAN Orchestrator** のリリースノート **11.4.0a** リリース

July 19, 2023

このリリースノートドキュメントでは、Citrix SD-WAN Orchestrator for オンプレミスリリースビルド 11.4.0a の機能強化と変更、修正された問題と既知の問題について説明します。

注

- オンプレミス用 Citrix SD-WAN Orchestrator 11.4.0a は、SDWANHELP-2317 で説明されている問題に対処し、リリース 11.4 に代わるものです。
- このリリースノートには、セキュリティ関連の修正は含まれていません。セキュリティに関する修正とアドバイスの一覧については、Citrix セキュリティ情報を参照してください。

新機能

ビルド 11.4.0a で利用できる機能強化と変更。

構成と管理

HTTP プロキシ

オンプレミス用 Citrix SD-WAN Orchestrator で HTTP プロキシ設定を構成できます。この機能により、Citrix Cloud に送信されるすべての要求を一元管理できます。管理者は、オンプレミス用 Citrix SD-WAN Orchestrator からの送信要求を HTTP プロキシサーバー経由で Citrix Cloud にルーティングできます。

[SDW-20247]

クラウドダイレクトサービス

オンプレミス向け Citrix SD-WAN Orchestrator は、クラウドダイレクトサービスをサポートしています。

Cloud Direct サービスは、ホスト環境 (データセンター、クラウド、インターネット) に関係なく、インターネットに向かうすべてのトラフィックを信頼性が高く安全に配信することにより、SD-WAN 機能をクラウドサービスとして提供します。

Cloud Direct サービスは、ネットワークの可視性と管理を向上させます。パートナーは、ビジネスクリティカルな SaaS アプリケーション向けのマネージド SD-WAN サービスをエンドカスタマーに提供できます。

[SDW-16396]

ストレージ管理-一般可用性

ストレージ管理機能が一般可用性をサポートするようになりました。

オンプレミス向け Citrix SD-WAN Orchestrator は、構成とデータをあるディスクから別のディスクに移行することをサポートしています。ディスクマイグレーションは、ディスク容量を増やすため、または障害回復のために実行できます。

- 新しいディスクの追加: Citrix SD-WAN Orchestrator for On-Premises が使用している現在のデータの少なくとも 2 倍のストレージサイズの新しいディスクを追加できます。
- 障害回復: 障害が発生した場合、オンプレミス用 Citrix SD-WAN Orchestrator 構成とデータを含むディスクを、オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator の新しいインスタンスに接続できます。

[SDW-21316]

クラウド仲介型ゼロタッチ導入-一般公開

クラウドブローカーのゼロタッチデプロイ機能が一般公開をサポートするようになりました。

クラウド仲介型ゼロタッチ展開は、オンプレミス向け Citrix SD-WAN Orchestrator と Citrix SD-WAN アプライアンス間の接続を確立するためのブローカーとしてオンプレミス向け Citrix SD-WAN Orchestrator を含む自動プロセスです。

[SDW-21312]

Citrix SD-WAN 11.4.1 リリース

Citrix SD-WAN 11.4.1 リリースは、オンプレミス 11.4 用の Citrix SD-WAN Orchestrator でサポートされています。

[SDW-21082]

プラットフォームとシステム

ICMP プロービング

オンプレミス用 Citrix SD-WAN Orchestrator は ICMP プローブをサポートしています。これにより、管理者は SD-WAN アプライアンスと宛先ホストとの間でインターネットにアクセスできるかどうかを判断できます。UI には次の ICMP サービスが導入されています。

- ICMP プローブを使用して、リンクからインターネットにアクセスできるかどうかを調べる
- IPv4 ICMP エンドポイントアドレス
- プローブ間隔 (秒単位)
- 再試行

[SDW-19292]

グローバルトランジットノード設定をオーバー

グローバルトランジットノード設定を上書きして、選択したコントロールトランジットノードでのみスポークツースポーク転送とルートエクスポートを有効または無効にできるようになりました。

[SDW-19276]

メンバーパス統計 **API (**プレビュー**)**:

メンバーパス統計 API は、API クライアントが関心のあるフィールドを指定できるように変更されました。指定されたフィールドがレスポンスペイロードで返されます。

[SDW-18903]

サイトレポート:VRRP

VRRP レポートは、設定された VRRP グループのリアルタイムレポートを提供します。

[SDW-12082]

サイトレポート:IGMP

IGMP レポートテーブルには、IGMP 統計情報と IGMP プロキシグループのリアルタイムレポートが表示されます。

[SDW-12077]

サイトレポート:IPsec

IPsec レポートは、ネットワーク上の IPsec トンネル構成のリアルタイムレポートを提供します。

[SDW-12076]

サイトレポート: ルーティングプロトコル

ルーティングプロトコルレポートには、ルーティングプロトコルに関連するパラメータの詳細が表示されます。必要に応じて、「表示」ドロップダウンリストからプロトコルを選択し、「ルーティングドメイン」ドロップダウンリストからルーティングドメインを選択できます。現在のデータを表示するには、「最新データを取得」をクリックします。

[SDW-12075]

プロバイダー監査ログ、 ネットワーク監査ログ

プロバイダーレベルとネットワークレベルの監査ログページが次の機能で強化されました。

- 検索: キーワードに基づいて監査アクティビティを検索できます。
- フィルタリング: ユーザー、機能、および時間範囲に基づいてフィルタリングすることにより、監査ログ検索を実行します。ネットワークレベルのログについては、サイトで絞り込むこともできます。
- 監査情報:「アクション」列の情報アイコンを選択し、「監査情報」セクションに移動します。このセクションでは、次の内容について説明します:
- メソッド: 呼び出された API の HTTP リクエストメソッド。
- ステータス:API リクエストの結果。API リクエストが失敗すると、エラーメッセージが表示されます。
- ペイロードメッセージ:API を介して送信されたリクエストメッセージの本文。
- **URL**: 取り消された API の HTTP URL。
- ログペイロード: デフォルトでは、このオプションは無効になっています。有効にすると、API メッセージのリクエスト本文が **Audit Info** セクションに表示されます。

[SDW-18937]

サイト選択コンポーネント

次の構成でのサイト選択コンポーネントの使いやすさが向上しました。

1. サイトの一部アップグレード
2. ネットワークロケーションサービス
3. ルーティングポリシー
4. QoS ポリシー
5. ルートフィルターのインポート
6. ルートフィルターのエクスポート
7. プロキシ自動設定
8. 侵入防止
9. ファイアウォールポリシー
10. アプリケーション設定

[SDW-16895]

解決された問題

ビルド 11.4 で対処されている問題。

その他

クラウドブローカー ZTD 機能が動作するためには SD-WAN Orchestrator サービスに依存しています。これは、今後予定されている SD-WAN Orchestrator リリースで対処される予定です。ただし、お客様はオンプレミス向けの Citrix SD-WAN Orchestrator をアップグレードする必要はありません。

[SDW-20307]

クラウド ZTD がプライマリサイトですでに設定されている場合、SD-WAN クラウド ZTD 構成は HA サイトでは機能しません。

[SDW-20208]

SD-WAN アプライアンスがオンプレミス用 Citrix SD-WAN **Orchestrator** に接続されているにもかかわらず、オンプレミス用 **Citrix SD-WAN Orchestrator** のステータスが **[**未接続] と表示されます。

[SDW-18280]

既知の問題

リリース 11.4 に存在する問題。

構成と管理

新しくインポートされた Citrix SD-WAN Orchestrator for On-Premises インスタンスで、ステージングがパッケージ準備中の状態で止まる。この問題は、新しい仮想マシンを作成した直後にステージングプロセスが開始された場合に発生します。

回避策: ステージングプロセスを再試行します。

[SDW-20863]

その他

オンプレミス 11.4 用の Citrix SD-WAN Orchestrator を実行しているユーザーが Citrix SD-WAN アプライアンスを 11.4.1 バージョンにアップグレードすると、ステージングプロセスが失敗します。UI には、ステータスが「ステージング失敗 **(**スクリプトファイルのダウンロードに失敗しました**)**」と表示されます。この問題は、Citrix SD-WAN アプライアンスとオンプレミス用 Citrix SD-WAN Orchestrator の間の帯域幅が少ない場合に発生します。

[SDWANHELP-2317]

VMware ESXi 13 を実行しているオンプレミス用 Citrix SD-WAN Orchestrator が再起動に失敗し、不良状態になります。

回避策: VMware ESXi バージョン 9 を使用してください。

[SDWANHELP-2182]

UI の **[**構成**] > [**** ネットワーク構成ホーム] および [構成] > [展開] ページに、正しくない SD-WAN アプライアンスソフトウェアのバージョンが表示される。** この問題は、ユーザーが変更管理を実行する前に、新しくインストールされた Citrix SD-WAN Orchestrator for オンプレミスインスタンスで発生します。

[SDW-21018]

Cloud Direct サイトの操作が失敗すると、UI にエラーメッセージが表示されません。

[SDW-21009]

部分的なサイトアップグレード設定の [ソフトウェアバージョン] ドロップダウンリストには、[インフラストラクチャ] > [**Orchestrator** 管理] > [ソフトウェアイメージ**]** で公開されているバージョンのみではなく、サポートされているすべてのソフトウェアバージョンが表示されます。アプライアンス。

サイトの一部アップグレードに記載されているソフトウェアバージョンが [インフラストラクチャ] > [**Orchestrator** 管理] > [ソフトウェアイメージ] > [アプライアンス] で公開できない場合、そのリリースでは部分的なサイトアップグレードを実行できません。

[SDW-20992]

UI の [構成] > [****** ネットワーク構成のホーム **] ページでは、構成ファイルがアップロードされた直後に、セカンダリ SD-WAN アプライアンスの Orchestrator 接続ステータスがオンラインで表示されます。ただし、サイトの構成を保存すると、正しいステータスが表示されます。

[SDW-20913]

プロバイダー管理の設定では、プロバイダー管理者が追加したアナウンスがログイン時に顧客に表示されません。

[SDW-18491]

アプライアンスのデータベースバックアップを、同じリリースのオンプレミス用 Citrix SD-WAN Orchestrator を搭載した別のアプライアンスに復元しても、ユーザーの詳細は復元されません。復元されたアプライアンスで、バックアップされたデータベースと同じユーザー名でユーザーを作成すると、次のエラーが表示されます。

```
User has a role already assigned
```

回避策: バックアップしたデータベースに存在しなかった別のユーザー名でユーザーを作成します。

[SDW-15984]

オンプレミス用 **Citrix SD-WAN Orchestrator 11.1** リリースに関するリリースノート

July 19, 2023

このリリースノートドキュメントでは、オンプレミスリリース 11.1 向け Citrix SD-WAN Orchestrator の機能強化と変更、修正された問題と既知の問題について説明します。

注

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

新機能

リリース 11.1 で使用可能な機能強化と変更。

Citrix SD-WAN 11.4.0a リリース

Citrix SD-WAN 11.4.0a リリースは、オンプレミス用 Citrix SD-WAN Orchestrator でサポートされています。

[SDW-19785]

Citrix SD-WAN 11.3.2 リリース

Citrix SD-WAN 11.3.2 リリースは、オンプレミス用 Citrix SD-WAN Orchestrator でサポートされています。

[SDW-19038]

ルート集約

オンプレミス向け Citrix SD-WAN Orchestrator では、ルート集約機能が強化されています。この機能拡張により、ゲートウェイの IP アドレスを指定せずにサマリールートを追加できます。

[SDW-19404]

ECMP 負荷分散

Equal Cost Multi-Path（ECMP; 等価コストマルチパス）グループを使用すると、同じコスト、宛先、サービスタイプを持つ複数のルートをグループ化できます。ECMP 負荷分散により、次のことが保証されます

- 複数の等価コスト接続でのトラフィックの分散。
- 利用可能な帯域幅の最適な使用。
- ルートが到達不能になった場合、他の ECMP メンバルートへのトラフィックのダイナミック転送。
- ECMP グループは、仮想パスおよびイントラネットサービス経由で形成できます。

[SDW-17452]

ストレージ管理 (プレビュー)

オンプレミス向け Citrix SD-WAN Orchestrator は、構成とデータをあるディスクから別のディスクに移行することをサポートしています。ディスクマイグレーションは、ディスク容量を増やすため、または障害回復のために実行できます。

- 新しいディスクの追加: Citrix SD-WAN Orchestrator for On-Premises が使用している現在のデータの少なくとも 2 倍のストレージサイズの新しいディスクを追加できます。
- 障害回復: 障害が発生した場合、オンプレミス用 Citrix SD-WAN Orchestrator 構成とデータを含むディスクを、オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator の新しいインスタンスに接続できます。

[SDW-16404]

クラウド仲介によるゼロタッチ導入 (プレビュー)

クラウド仲介型ゼロタッチ展開は、オンプレミス向け Citrix SD-WAN Orchestrator と Citrix SD-WAN アプライアンス間の接続を確立するためのブローカーとしてオンプレミス向け Citrix SD-WAN Orchestrator を含む自動プロセスです。

[SDW-11614]

トランジットノードの強化

グローバル設定の一部としてハブアンドスポーク通信を有効にすると、すべてのサイトで、サイト間通信で制御ノードを中継ノードとして使用できます。仮想オーバーレイトランジットノードのサイト固有の環境設定を使用すると、ネットワーク内のすべてのサイトのグローバル仮想オーバーレイトランジットノード設定を上書きできます。非制御ノードを、サイトのプライマリ中継ノードとして選択することもできます。

[SDW-12443]

IPv6 データプレーンのサポート

オンプレミス用 Citrix SD-WAN Orchestrator は、Citrix SD-WAN ソフトウェアバージョン 11.3.1 以上で、次の Citrix SD-WAN アプライアンス構成の IPv6 アドレスをサポートします。

- DNS サーバー
- フロー
- ファイアウォール接続
- IP グループ
- 領域
- DHCP クライアント
- IP ルールとアプリケーションルール
- ネットワークアドレス変換
- GRE サービス
- インターフェイス

- インターネットサービス
- 近傍探索プロトコル
- プレフィックス委任グループ
- IPSec サービス
- HA 設定
- IP ルート
- 帯域内管理
- DNS 設定
- DHCP サーバー、DHCP リレー、DHCP オプションセット

[SDW-19194]

解決された問題

リリース 11.1 で解決された問題。

11.2.0 より前の SD-WAN アプライアンスバージョンは、11.1 より前のオンプレミスバージョンの Citrix SD-WAN Orchestrator に接続できません。ユーザーが 11.2.0 より前のソフトウェアバージョンを実行している SD-WAN アプライアンスを接続する場合は、Citrix SD-WAN Orchestrator for On-Premises 11.1 が推奨バージョンです。

[SDW-20220]

お客様のアカウントを本番環境にアップグレードする際に障害が発生した場合、UI には失敗メッセージが表示されません。

[SDW-19574]

永久ライセンスのみを持つプリペイド顧客の場合、オンプレミス向け Citrix SD-WAN Orchestrator で本番環境へのアップグレードが失敗します。

[SDW-19558]

オンプレミス用 Citrix SD-WAN Orchestrator では、サイトに永続ライセンスを割り当てると失敗します。

[SDW-19556]

ライセンスの割り当てに失敗した場合、**UI** の **[**** 管理] > [ライセンス] には失敗メッセージが表示されません。**

[SDW-19238]

顧客管理者にリモート認証サーバを削除するアクセス権がない場合でも、UI には削除アイコンが表示されます。ただし、顧客管理者が削除操作を実行しようとすると、次のエラーが表示されます。

```
User is not authorized to perform this operation。
```

[SDW-18945]

プロバイダーレベルの [管理] > [お知らせ] ページから、上部のメニューバーから顧客を選択すると、見出しとしてネットワーク管理を含む空白のページが表示されます。

[SDW-18944]

有効なプロダクションエンタイトルメントをインポートすると、ライセンスをアプライアンスに割り当てる前でも、「ライセンス」で「プロダクションにアップグレード」オプションが使用可能になります。

[SDW-18721]

既知の問題

リリース 11.1 に存在する問題。

クラウドブローカー ZTD 機能が動作するためには SD-WAN Orchestrator サービスに依存しています。これは、今後予定されている SD-WAN Orchestrator サービスリリースで対処される予定です。ただし、お客様はオンプレミス向けの Citrix SD-WAN Orchestrator をアップグレードする必要はありません。

[SDW-20307]

Citrix SD-WAN Orchestrator for On-Premises を 11.1 バージョンにアップグレードすると、以前のリリースで収集された監査ログには **sdwan-onprem-sp** がユーザーとして表示され、UI のログペイロード切り替えボタンが有効になります。これらのログは 92 日後に消去されます。

[SDW-20305]

クラウド ZTD がプライマリサイトですでに設定されている場合、SD-WAN クラウド ZTD 構成は HA サイトでは機能しません。

回避方法:

1. [管理] > [ZTD 設定**] > [**クラウド仲介 **ZTD]** に移動して、プライマリサイトクラウド **ZTD** 設定を削除します。
2. プライマリサイトとセカンダリサイトの両方のクラウド ZTD サイトを同時に再構成します。

[SDW-20208]

ライセンス機能は、オンプレミス用 Citrix SD-WAN Orchestrator のプロバイダー管理セットアップではサポートされていません。プロバイダーはトライアルライセンスを継続できます。60 日間の猶予期間があります。

[SDW-18831]

アプライアンスがオンプレミス用 Citrix SD-WAN Orchestrator への接続を 20 分以上失い、再登録フェーズに入ると、登録要求に誤ったシリアル番号が送信されます。

回避策:アプライアンスを再起動します。

[SDW-18781]

プロバイダー管理の設定では、プロバイダー管理者が追加したアナウンスがログイン時に顧客に表示されません。

[SDW-18491]

SD-WAN アプライアンスがオンプレミス用 Citrix SD-WAN **Orchestrator** に接続されているにもかかわらず、オンプレミス用 **Citrix SD-WAN Orchestrator** のステータスが **[**未接続] と表示されます。

回避策：［構成］>［** ネットワーク構成ホーム ** ］に移動し、Citrix SD-WAN Orchestrator for On-Premises UI でアプライアンスの接続ステータスを確認します。

[SDW-18280]

アプライアンスのデータベースバックアップを、同じリリースのオンプレミス用 Citrix SD-WAN Orchestrator を搭載した別のアプライアンスに復元しても、ユーザーの詳細は復元されません。復元されたアプライアンスで、バックアップされたデータベースと同じユーザー名でユーザーを作成すると、次のエラーが表示されます。

```
User has a role already assigned
```

回避策: バックアップしたデータベースに存在しなかった別のユーザー名でユーザーを作成します。

[SDW-15984]

VMware ESXi 13 を実行しているオンプレミス用 Citrix SD-WAN Orchestrator が再起動に失敗し、不良状態になります。

回避策：VMware ESXi バージョン 9 を使用してください。

[SDWANHELP-2182]

オンプレミス用 **Citrix SD-WAN Orchestrator 10.3** リリースに関するリリースノート

October 26, 2022

このリリースノートドキュメントでは、オンプレミスリリース 10.3 用の Citrix SD-WAN Orchestrator の機能強化と変更、修正された問題と既知の問題について説明します。

注

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

新機能

リリース 10.3 で使用可能な機能強化と変更。

構成と管理

動的ルーティング

Citrix SD-WAN 11.3.1 リリース以降では、プロトコル全体に 1 つのルーター ID を構成でき、ルーティングドメインごとに 1 つのルーター ID を構成することもできます。この拡張により、ルーター ID が異なる複数のインスタンスにわたる安定した動的ルーティングが可能になり、安定した方法で収束できるようになります。

[SDW-17097]

ステージングを再試行

ステージングプロセスが失敗したサイトでステージングを再開するために、ステージングを再試行するオプションが使用できるようになりました。

[SDW-16538]

カスタムアプリケーション

IP プロトコルベースのカスタムアプリケーションに [レポートを有効にする] チェックボックスが新しく追加されました。また、[レポート**] **[** 使用状況] ページで IP プロトコルとドメイン名ベースのカスタムアプリケーション定義トラフィックを表示できるようになりました。カスタムアプリケーションオプションもアプリケーション品質設定ページにタイプとして追加されます。

[SDW-10862]

その他

フォールバック構成

フォールバック設定により、リンク障害、設定の不一致、またはソフトウェアの不一致が発生した場合でも、アプライアンスはゼロタッチ展開サービスに接続したままになります。フォールバック構成は、デフォルト構成プロファイルを持つアプライアンスではデフォルトで有効になっています。フォールバック構成がサイトで無効になっている場合は、オンプレミス用 Citrix SD-WAN Orchestrator を使用してフォールバック構成を有効にできます。

[SDW-13978]

フロー

これで、アプライアンス設定のフローセクションを使用して次のアクションを実行できるようになりました。

- Citrix 仮想 WAN サービスの有効化/無効化
- 動的ルーティングを再起動
- 仮想パスの有効化/無効化
- WAN リンクの有効化/無効化

[SDW-13977]

ネットワーク管理者とセキュリティ管理者の役割 (プレビュー)

オンプレミス向け Citrix SD-WAN Orchestrator は次の役割をサポートします。

- **Provide-Network-Admin**: ネットワーク関連情報の表示と編集のみができる管理者。

- **Provider-Security-Admin**: セキュリティ関連情報の表示と編集のみができる管理者。
- 顧客ネットワーク管理者: ネットワーク関連情報のみを表示および編集できる顧客管理者。
- **Customer-Security-Admin**: セキュリティ関連情報のみを表示および編集できる顧客管理者。

[SDW-13845]

アプライアンスの設定

オンプレミス向け Citrix SD-WAN Orchestrator を使用して、サイトレベルで日付と時刻を構成できるようになりました。日付と時刻は手動で設定することも、NTP サーバーを使用してタイムゾーンを設定することもできます。

[SDW-13321]

プロバイダーレベルのサポート

オンプレミス用 Citrix SD-WAN Orchestrator はマルチテナントをサポートします。マルチテナント機能を使用すると、オンプレミス用の単一の Citrix SD-WAN Orchestrator インスタンスを使用して複数の顧客アカウントを管理できます。次のいずれかのタイプのセットアップを使用できます。

- プロバイダー管理セットアップ：お客様は、マルチテナント機能を使用して、Citrix パートナーが提供するマネージド Citrix SD-WAN Orchestrator for On-Premises サービスを利用します。
- 顧客管理のセットアップ：お客様は、オンプレミス向け Citrix SD-WAN Orchestrator を企業向けの自己管理サービスとして管理します。

プロバイダー管理セットアップサポートの一環として、次の機能が導入されました。

- 役割: 以下のプロバイダーレベルの役割が追加されました。
  - プロバイダー-マスター-管理者-すべて
  - プロバイダー-マスター-管理者-テナント
  - Provider-master-readonly-all
- ダッシュボード: プロバイダーが管理しているすべての SD-WAN 顧客を大まかに見ることができる新しい UI ページが追加されました。
- **SD-WAN** アプライアンスとの接続：プロバイダーが管理するセットアップでは、認証タイプを有効にして Citrix SD-WAN Orchestrator for On-Premises 証明書を再生成できるのはプロバイダーのみです。お客様はアプライアンス証明書をアップロードできます。
- サイトプロファイルテンプレートと **WAN** リンクテンプレート: テンプレートを使用すると、顧客レベルでサイトプロファイルと **WAN** リンクプロファイルを作成できます。
- ソフトウェアの公開：オンプレミス向け Citrix SD-WAN Orchestrator を使用すると、プロバイダー管理者はネットワーク内のすべてのアプライアンスに必要な Citrix SD-WAN アプライアンスソフトウェアバージョンをダウンロードできます。プロバイダーは、ダウンロードしたソフトウェアバージョンを公開できます。公開されたソフトウェアは、オンプレミス向け Citrix SD-WAN Orchestrator にダウンロードされ、保存されます。顧客管理者は、公開されたソフトウェアを Citrix SD-WAN Orchestrator for On-Premises によって管理されるすべてのアプライアンスに展開できます。

- 管理: プロバイダー管理者は、管理 IP、DNS、NTP サーバー、およびリモート認証サーバーを設定できます。
- お知らせ: プロバイダーは [お知らせ] オプションを使用して、顧客に通知または通知を送信できます。
- レポート: プロバイダーレポートは、プロバイダーが管理するすべての顧客を対象に集計されたアラート、使用量の傾向、インベントリを可視化します。

[SDW-12589]

ゼロタッチ導入-バッチサイト

CSV ファイルをインポートして、ゼロタッチデプロイメント用に複数のサイトを同時に追加できるようになりました。ダウンロード可能なサンプルテンプレートが UI にあります。ダウンロードしてサイトの詳細をすべて入力してください。

[SDW-12249]

プラットフォームとシステム

サイトレポート:WAN リンクメータリング

WAN リンクメータリングレポートには、従量制課金の WAN リンクの使用状況に関する詳細が表示されます。レポートを表示して、従量制課金 WAN リンクのデータ消費に関する洞察を得ることができます。

[SDW-8892]

既知の問題

リリース 10.3 に存在する問題。

構成と管理

帯域内 HA の場合、GUI にはサービスタイプが Any の宛先ルールの方向を選択するオプションがないため、アウトバウンドルールが失敗します。エラーメッセージ [EC818] At Site site-name: サービスタイプ‘any’は、方向がアウトバウンドの場合には使用できません。

[SDW-16968]

その他

カスタマー管理者にリモート認証サーバを削除するアクセス権がない場合でも、GUI には削除アイコンが表示されます。ただし、削除操作を実行しようとすると、次のエラーが表示されます。

```
User is not authorized to perform this operation
```

[SDW-18945]

プロバイダーレベルの [管理**] > [**お知らせ] ページから、上部のメニューバーから顧客を選択すると、見出しとしてネットワーク管理を含む空白のページが表示されます。

[SDW-18944]

プロバイダー管理セットアップで作成されたデータベースバックアップをカスタマー管理セットアップに復元することはできません。同様に、顧客管理設定で作成したデータベースバックアップをプロバイダー管理セットアップに復元することはできません。

[SDW-18904]

サイト設定への読み取り専用アクセス権を持つ customer-security-admin ロールが設定を編集しようとすると、不正アクセスではなくエラーメッセージを含む赤いバナーが表示されます。

[SDW-18840]

ライセンス機能は、オンプレミス用 Citrix SD-WAN Orchestrator のプロバイダー管理セットアップではサポートされていません。プロバイダーはトライアルライセンスを継続できます。60 日間の猶予期間が提供されます。

[SDW-18831]

アプライアンスがオンプレミス用 Citrix SD-WAN Orchestrator への接続を 20 分以上失い、再登録フェーズに入ると、登録要求に誤ったシリアル番号が送信されます。

回避策：アプライアンスを再起動します。

[SDW-18781]

有効なプロダクションエンタイトルメントをインポートすると、ライセンスをアプライアンスに割り当てる前でも、「ライセンス」で「プロダクションにアップグレード」オプションが使用できるようになります。

回避策：ライセンスがアプライアンスに割り当てられた後にのみ、「実稼働環境にアップグレード」をクリックします。

[SDW-18721]

オンプレミス用 Citrix SD-WAN Orchestrator とアプライアンスの間では、ネットワークアドレス変換（NAT）はサポートされていません。

[SDW-18703]

プロバイダー管理の設定では、プロバイダー管理者が追加したアナウンスがログイン時に顧客に表示されません。

[SDW-18491]

CLI では、ユーザは許可されている 8 ～128 の範囲外のパスワードを作成できますが、パスワードの長さが許容範囲外の場合、GUI ログインは失敗します。

回避策:GUI にログインすると、ユーザーはパスワードの長さを許可された範囲に変更する必要があります。

[SDW-16068]

ユーザーがログインしようとすると、ログインページが表示される前の数秒間、ページの上部に赤いバナーが表示されることがあります。

[SDW-16024]

アプライアンスのデータベースバックアップを、同じリリースのオンプレミス用 Citrix SD-WAN Orchestrator を搭載した別のアプライアンスに復元しても、ユーザーの詳細は復元されません。復元されたアプライアンスで、バックアップされたデータベースと同じユーザー名でユーザーを作成すると、次のエラーが表示されます。

```
User has a role already assigned
```

回避策: バックアップしたデータベースに存在しなかった別のユーザー名でユーザーを作成します。

[SDW-15984]

オンプレミス向け **Citrix SD-WAN Orchestrator** リリースノート **9.6**

July 19, 2023

このリリースノートドキュメントでは、オンプレミスリリース 9.6 向け Citrix SD-WAN Orchestrator の機能強化と変更、修正された問題と既知の問題について説明します。

> 注:
>
> このリリースノートドキュメントには、セキュリティ関連の修正は含まれていません。セキュリティに関する修正とアドバイスの一覧については、Citrix セキュリティ情報を参照してください。

新機能

リリース 9.6 で使用可能な機能強化と変更。

構成と管理

動的ルーティング

Citrix SD-WAN 11.3.1 リリース以降では、プロトコル全体に 1 つのルーター ID を構成でき、ルーティングドメインごとに 1 つのルーター ID を構成することもできます。この拡張により、ルーター ID が異なる複数のインスタンスにわたる安定した動的ルーティングが可能になり、安定した方法で収束できるようになります。

[SDW-17097]

その他

HTTPS 証明書

オンプレミス用 Citrix SD-WAN Orchestrator への安全な管理 HTTPS 接続を確立するには、HTTPS 証明書が必要です。Citrix SD-WAN Orchestrator for オンプレミス GUI で使用できるデフォルトの証明書を使用するか、

OpenSSL などの他のフレームワークから生成されたカスタム HTTPS 証明書をアップロードできます。カスタム HTTPS 証明書を使用すると、証明書に関連するセキュリティやその他のサブジェクトパラメータを制御できます。

[SDW-16359]

インターフェイス

Citrix SD-WAN 11.3.1 リリース以降では、［有効］チェックボックスを使用して仮想インターフェイスを有効または無効にできます。

[SDW-15993]

解決された問題

リリース 9.6 で解決された問題。

構成と管理

Citrix SD-WAN 6100 SE アプライアンスの場合、UI に [構成**] > [**詳細設定**]** の [**LAG**] ページが表示されません。

[SDWANHELP-1895]

その他

Citrix SD-WAN Orchestrator for オンプレミス GUI では、GUI が継続的に使用されていてアイドル状態になっていない場合でも、1 時間ごとにログインするように求められます。

[SDWANHELP-1902]

既存のサイトを複製してサイトを作成すると、[構成**/**ソフトウェアの導入**] > [**構成の検証**]** が失敗します。

[SDW-16103]

既知の問題

リリース 9.6 に存在する問題。

その他

認証トークンの更新中に Citrix SD-WAN Orchestrator for On-Premises GUI を新しいタブで開くと、ブラウザ内の既存のセッションはすべてログアウトされます。

[SDW-17719]

ディスクのサイズが 1.8 TB を超える場合、ディスクのサイズ変更は行われません。

[SDW-16404]

CLI では、ユーザーは許可されている 8〜128 文字の範囲外のパスワードを作成できます。ただし、パスワードの長さが許容範囲外の場合、GUI ログインは失敗します。

回避策:GUI にログインすると、ユーザーはパスワードの長さを許可された範囲に変更する必要があります。

[SDW-16068]

ユーザーがログインしようとすると、ログインページが表示される前の数秒間、ページの上部に赤いバナーが表示されることがあります。

[SDW-16024]

アプライアンスのデータベースバックアップを、同じリリースのオンプレミス用 Citrix SD-WAN Orchestrator を搭載した別のアプライアンスに復元しても、ユーザーの詳細は復元されません。復元されたアプライアンスで、バックアップされたデータベースと同じユーザー名でユーザーを作成すると、次のエラーが表示されます。

```
User has a role already assigned
```

回避策: バックアップしたデータベースに存在しなかった別のユーザー名でユーザーを作成します。

[SDW-15984]

オンプレミス用 **Citrix SD-WAN Orchestrator 1.0** リリースに関するリリースノート

October 26, 2022

オンプレミス向け Citrix SD-WAN Orchestrator は、顧客ごとに個別のインスタンスとして利用できるセルフホスト型の管理サービスです。このプラットフォームは、SD-WAN ネットワーク上のすべての SD-WAN アプライアンスを構成、監視、分析できる単一ペインの管理プラットフォームを提供します。

オンプレミス向け Citrix SD-WAN Orchestrator は、データの主権とデータプライバシーに関する強力な規制要件を持つお客様にお勧めします。

主な機能の一部を次に示します。

- 認証: ローカル認証と RADIUS/TACACS+ 認証をサポートします。
- 一元的な構成: ガイド付きのワークフロー、ビジュアルエイド、プロファイルを備えた SD-WAN ネットワークの一元的な構成。
- ゼロタッチプロビジョニング: ネットワークと接続をシームレスに起動します。
- アプリケーション中心のポリシー: アプリケーションベースのトラフィックステアリング、Quality of Service（QoS）、およびファイアウォールポリシーを、グローバルまたはサイトごとに構成できます。
- ヘルスの階層的要約: ネットワーク全体の状態、使用状況、品質、パフォーマンスを一元的に監視でき、個々のサイトや関連する接続にドリルダウンできます。
- トラブルシューティング: デバイスと監査ログ、Ping、Traceroute、ネットワーク接続の問題をトラブルシューティングするためのパケットキャプチャなどの診断ユーティリティ。

前提条件

- アプライアンス: 最低 2 つのアプライアンス。各 SD-WAN アプライアンスまたは仮想インスタンスには IP アドレスが設定されている必要があります。
- **Citrix SD-WAN Orchestrator** サービスアカウント: オンプレミス用 Citrix SD-WAN Orchestrator を使用するには、Citrix SD-WAN Orchestrator サービスにアカウントが必要です。詳しくは、「Citrix SD-WAN Orchestrator サービスのオンボーディング」を参照してください。

オンプレミス用 **Citrix SD-WAN Orchestrator 1.0.1**

解決された問題

- **SDW-16456**: オンプレミス用 Citrix SD-WAN Orchestrator では、任意からすべてのルーティングドメインはサポートされていません。
- **SDW-16063**: ネットワークレベルでは、Wi-Fi の概要レポートが使用できない。
- **SDW-16054**: Citrix SD-WAN Orchestrator サービスの米国地域外で顧客アカウントを作成すると、Citrix Cloud の ID と管理 (IDAM) ページで取得した API トークンが機能しない。オンプレミス向け Citrix SD-WAN Orchestrator へのお客様のログインが失敗し、「顧客 ID、クライアント ID、またはクライアントシークレットが無効です」というエラーメッセージが表示されます。

  オンプレミス用 Citrix SD-WAN Orchestrator を初めて起動するときに、クラウドアカウントがオンボードされた **POP** を選択できるようになりました。

既知の問題

- **SDW-16068**: CLI では、ユーザは許可されている 8 ～128 の長さの範囲外のパスワードを作成できるが、パスワードの長さが許可されている範囲外の場合、GUI ログインが失敗する。
  - 回避策:GUI にログインすると、ユーザーはパスワードの長さを許可された範囲に変更する必要があります。
- **SDW-16024**: ユーザーが UI にログインすると、ログインページが表示される前に、ページの上部に数秒間、赤いバナーが表示されることがあります。
- **SDW-15984**: アプライアンスのデータベースバックアップが、同じリリースのオンプレミス向け Citrix SD-WAN Orchestrator を搭載した別のアプライアンスに復元されると、ユーザーの詳細が復元されない。復元されたアプライアンスで、バックアップされたデータベースと同じユーザー名でユーザーを作成すると、次のエラーが表示されます。

  ユーザーにはすでに役割が割り当てられています

  - 回避策: バックアップしたデータベースに存在しなかった別のユーザー名でユーザーを作成します。

- **SDW-16103**: 既存のサイトを複製してサイトを作成すると、[構成/ソフトウェアの展開] > [構成の検証] が失敗する。
  - 回避策: 既存のサイトを複製してサイトを作成しないでください。
- **SDW-16404**: ディスクのサイズを 1.8 TB 以上に変更すると、ディスクのサイズが変更されない。

システム要件とインストール

October 26, 2022

Citrix SD-WAN Orchestrator for On-Premises を仮想マシン（VM）にインストールする前に、ハードウェアとソフトウェアの要件を理解し、前提条件を満たしていることを確認してください。

> 注:
>
> システム要件は、単一地域ネットワークと多地域ネットワークの両方に共通です。

ハードウェア要件

以下は、オンプレミス向け Citrix SD-WAN Orchestrator が平均して 1 か月分のデータまたは 2 つの WAN リンクの統計情報を保存するためのハードウェア要件です。

サイト数	プロセッサ	RAM	ストレージ
2000	256 vCPU 3 GHz 以上	512GB	2 TB
1000	128 vCPU 3 GHz 以上	256 GB	1TB
500	64 仮想 CPU 3 GHz 以上	128GB	500GB
256	32 vCPU 3 GHz 以上	64GB	256 GB
128	8 vCPU 3 GHz 以上	16GB	256 GB

ソフトウェア

オンプレミス VPX 用 Citrix SD-WAN Orchestrator は、次のプラットフォームで構成できます。

ハイパーバイザー

- VMware ESXi 7.0 アップデート 1.
- VMware ESXi サーバ、バージョン 6.5。
- Citrix XenServer 6.5 以降。

ブラウザーで Cookie を有効にし、JavaScript をインストールして有効にする必要があります。

Citrix SD-WAN Orchestrator for オンプレミス Web インターフェイスは、次のブラウザでサポートされています。

- Google Chrome 40.0+
- Microsoft Internet Explorer 11+
- Mozilla Firefox 41.0+

前提条件

オンプレミス用 Citrix SD-WAN Orchestrator をインストールして展開するための前提条件は次のとおりです。

- SD-WAN マスターコントロールノード（MCN）と既存のクライアントノードは、最新の Citrix SD-WAN ソフトウェアバージョンにアップグレードする必要があります。
- SD-WAN ネットワークに DHCP サーバーを用意して構成することをお勧めします。
- オンプレミス用の Citrix SD-WAN Orchestrator インストールファイルが必要です。

> 注
>
> オンプレミス用 Citrix SD-WAN Orchestrator では、サードパーティのソフトウェアをカスタマイズしたりインストールしたりすることはできません。ただし、vCPU、メモリ、およびストレージの設定は変更できます。

オンプレミス向け **Citrix SD-WAN Orchestrator** ソフトウェアをダウンロード

必要なリリースとプラットフォーム用の Citrix SD-WAN Orchestrator for On-Premises 管理コンソールソフトウェアのインストールファイルを、ダウンロードページからダウンロードします 。

Citrix SD-WAN Orchestrator for オンプレミスインストールファイルでは、次の命名規則を使用します。

- ctx-sdw-onprem-build.extension
- ctx-onprem-build.extension
- ctx-onprem-build.extension

プラットフォーム	拡張子
Citrix XenServer	xva
VMware ESXi	-vmware.ova

インストールと構成のチェックリスト

このセクションでは、オンプレミス向け Citrix SD-WAN Orchestrator のインストールと展開を完了するために必要な情報のチェックリストを提供します。

次の情報を収集または決定してください。

- オンプレミス仮想マシン (VM) 用 Citrix SD-WAN Orchestrator をホストする ESXi サーバと XenServer の IP アドレス。
- オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator に割り当てる一意の名前。
- オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator に割り当てるメモリ量。
- 仮想マシンの仮想ディスクに割り当てるディスク容量。
- オンプレミス向け Citrix SD-WAN Orchestrator が外部ネットワークとの通信に使用するゲートウェイ IP アドレス。
- オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator がインストールされているネットワークのサブネットマスク。

> 注
>
> Citrix では、仮想マシンと SD-WAN 構成のスナップショットを定期的に作成することを推奨しています。

オンプレミス用 **SD-WAN Orchestrator** と **Citrix SD-WAN Orchestrator** サービスの違い

October 26, 2022

機能

機能	Citrix SD-WAN Orchestrator サービス	オンプレミス向け Citrix SD-WAN Orchestrator
Advanced Edition プラットフォーム	はい	いいえ
Premium Edition プラットフォーム	はい	いいえ
Zscaler サービス	はい	いいえ
Azure Virtual WAN サービス	はい	いいえ
Citrix Secure Internet Access サービス	はい	いいえ
ホストファイアウォール	はい	いいえ
プリセット DPI アプリとカスタムアプリ (FQDN または IP ベース) でのアプリケーションルーティング	はい	はい

機能	Citrix SD-WAN Orchestrator サービス	オンプレミス向け Citrix SD-WAN Orchestrator
動的な署名更新を必要とするアプリ（Office 365、Citrix Cloud、新しくサポートされるアプリなど）でのアプリケーションルーティング。	はい	いいえ
Orchestrator-高可用性	はい	いいえ

要件

要件	Citrix SD-WAN Orchestrator サービス	オンプレミス用 SD-WAN Orchestrator
SD-WAN ファクトリイメージが必要です	すべて (工場出荷リリース)	Citrix SD-WAN 10.2.7、11.1.1、11.2.0、11.2.2、11.3.0 以降。*
ネットワークに導入されたアプライアンス	すべて	Citrix SD-WAN 11.2.2、11.3.0 以降。*
SD-WAN アプライアンスのインターネット接続	必須	必要ない
ファイアウォールのポートを開く予定	443	443、22、ICMP
ライセンス	ポストペイドモデルとプリペイドモデル	プリペイドモデルのみ

- サポートされている Citrix SD-WAN ソフトウェアバージョンは、オンプレミス用 SD-WAN Orchestrator ソフトウェアバージョンによって異なります。

ESXi Server にオンプレミス用 **SD-WAN Orchestrator** をインストールして構成する

October 26, 2022

VMware vSphere クライアントのインストール

以下は、オンプレミス仮想マシン（VM）用 Citrix SD-WAN Orchestrator の作成と展開に使用する VMware vSphere クライアントをダウンロードしてインストールするための基本的な手順です。

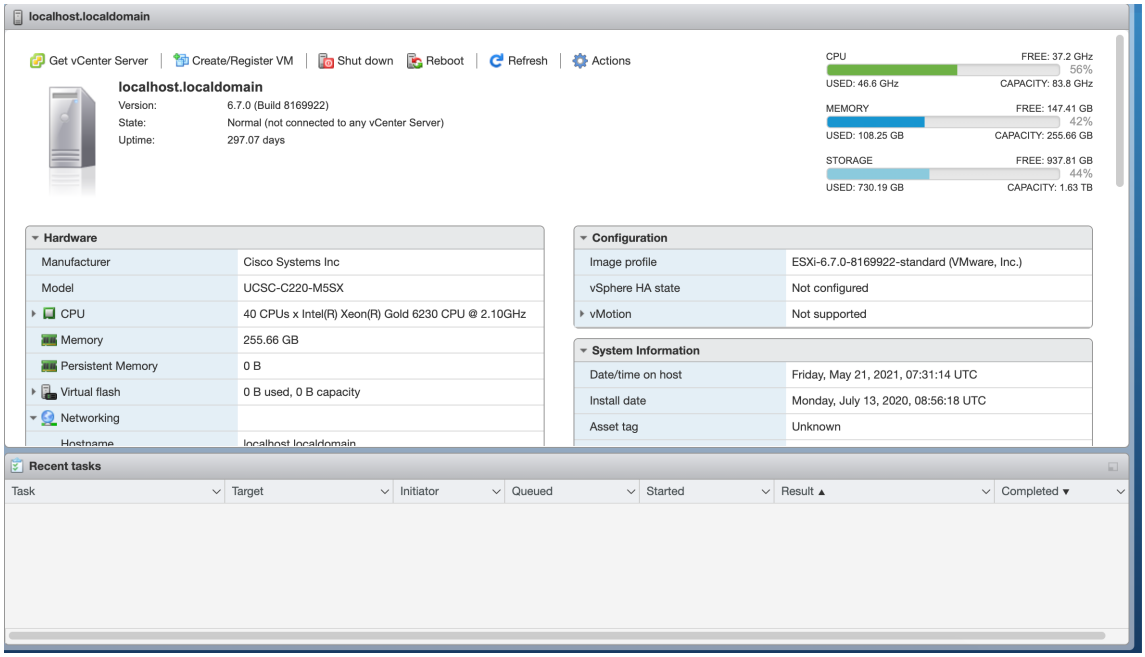
VMware vSphere クライアントをダウンロードしてインストールするには、次の操作を行います。

1. ブラウザを開き、vSphere Client と Citrix SD-WAN Orchestrator for オンプレミス仮想マシンインスタンスをホストする ESXi サーバに移動します。VMware ESXi のウェルカムページが表示されます。
2. **vSphere Client** のダウンロードリンクをクリックして、vSphere Client のインストールファイルをダウンロードします。
3. vSphere Client をインストールします。

   ダウンロードした vSphere Client インストーラファイルを実行し、プロンプトが表示されたら各デフォルトオプションを受け入れます。
4. インストールが完了したら、vSphere Client プログラムを起動します。

   VMware vSphere Client のログインページが表示され、ESXi サーバのログイン認証情報の入力を求められます。
5. ESXi サーバのログイン認証情報を入力します。

   - **IP** アドレス/名前:Citrix SD-WAN Orchestrator for オンプレミス仮想マシンインスタンスをホストする ESXi サーバーの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
   - ユーザー名: サーバー管理者のアカウント名を入力します。デフォルトは［root］です。
   - パスワード: この管理者アカウントに関連付けられているパスワードを入力します。
6. [ログイン] をクリックします。
   vSphere クライアントのメインページが表示されます。



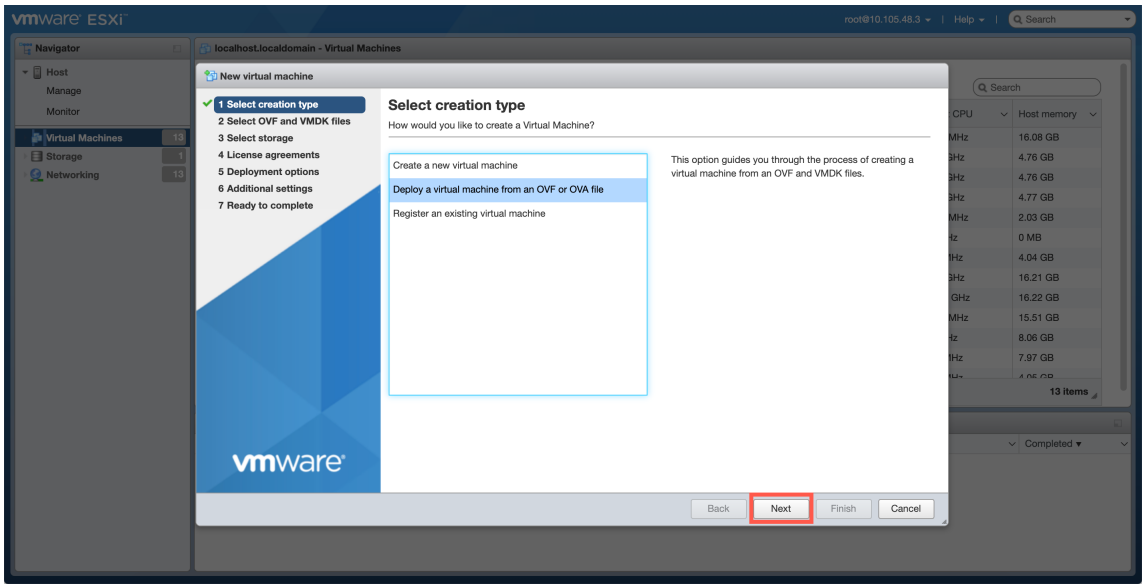
OVF テンプレートを使用したオンプレミス仮想マシン用 **Citrix SD-WAN Orchestrator** の作成

VMware vSphere クライアントをインストールしたら、オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator を作成します。

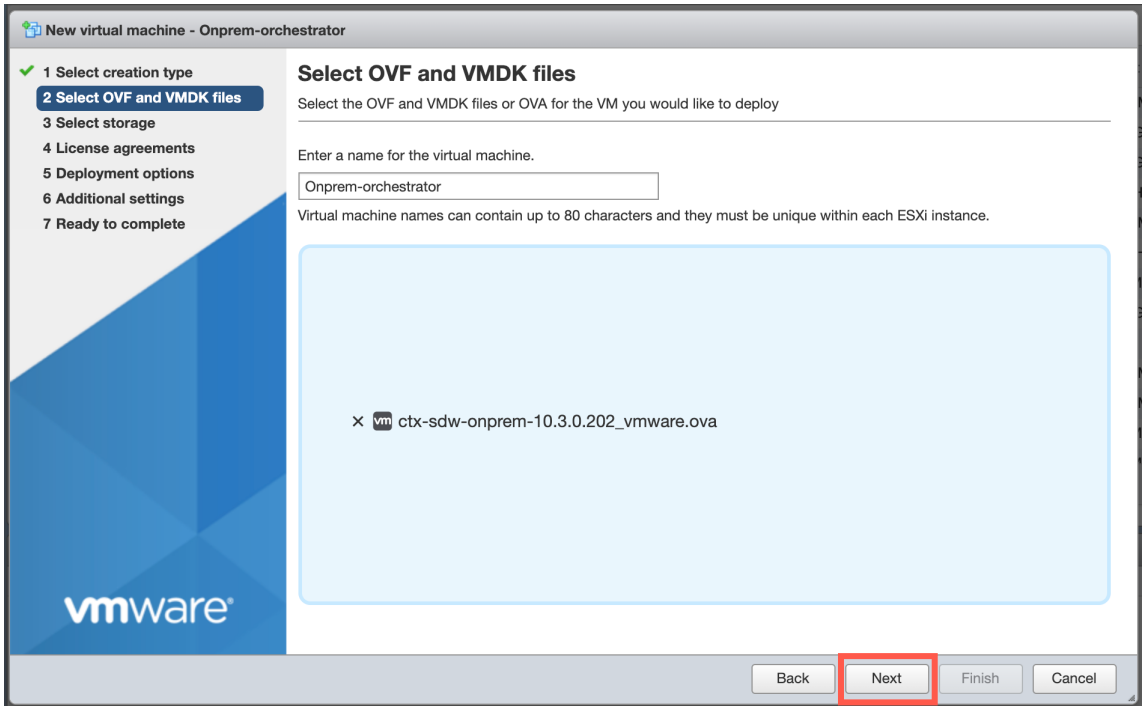
1. まだダウンロードしていない場合は、Citrix SD-WAN Orchestrator for オンプレミス OVF テンプレートファイル（.ova ファイル）をローカル PC にダウンロードします。

   詳しくは、「システム要件とインストール」を参照してください。

2. vSphere Client で [仮想マシンの作成/登録] をクリックし、リストから **[OVF** または **OVA** ファイルから仮想マシンをデプロイ] を選択します。[次へ] をクリックします。



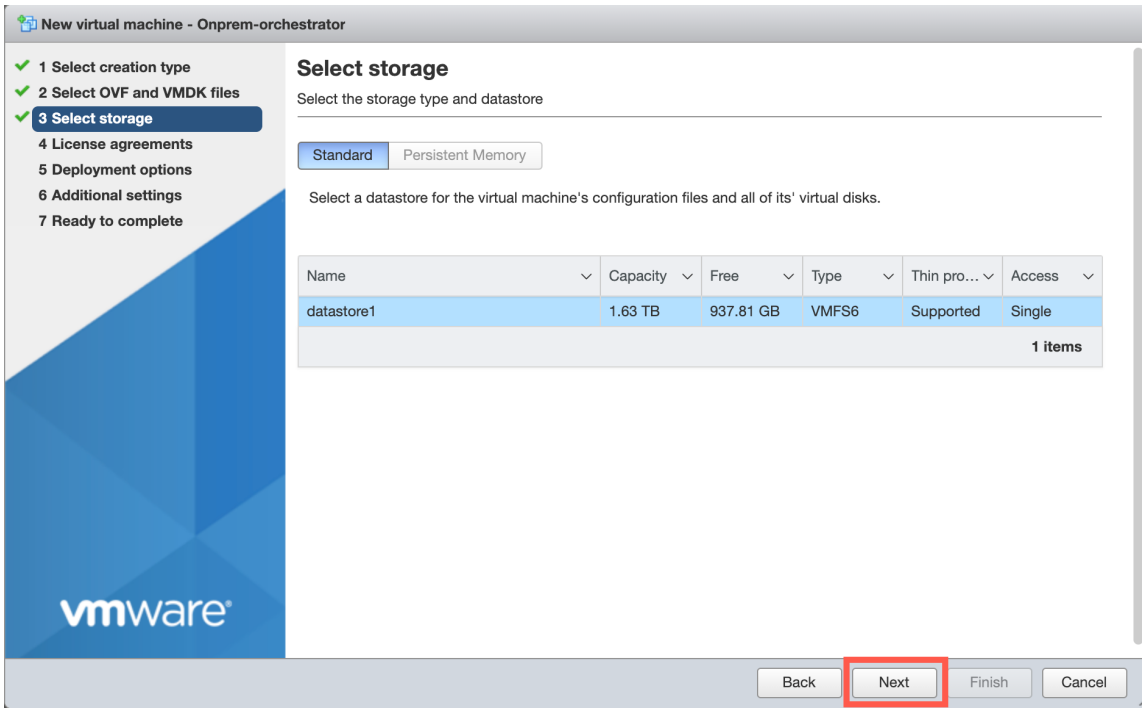
3. 新しい仮想マシンの一意の名前を入力します。
4. ボックスの内側をクリックし、インストールする Citrix SD-WAN Orchestrator for On-Premises OVF テンプレート（.ova ファイル）を選択するか、ファイルをボックス内にドラッグします。
5. [次へ] をクリックします。



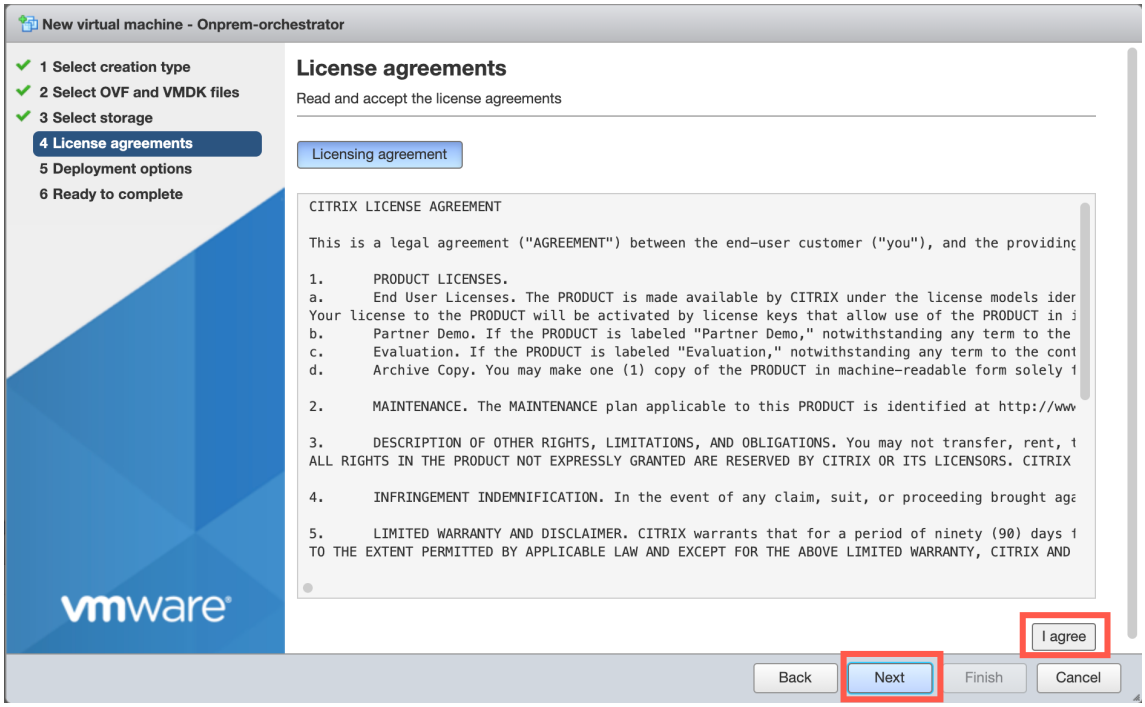
6. [次へ] をクリックします。

   [ストレージ] ページが表示されます。

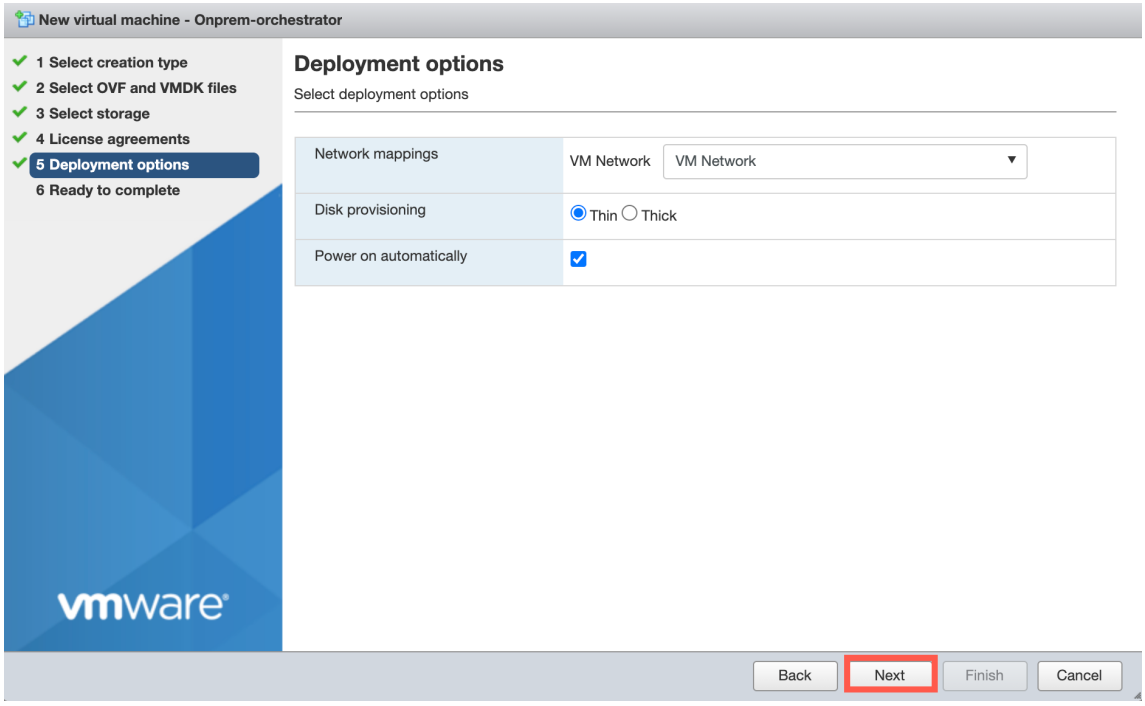
7. [次へ] をクリックして、デフォルトのストレージリソースをそのまま使用します。



8. EULA ページで [同意する] をクリックし、[次へ] をクリックします。

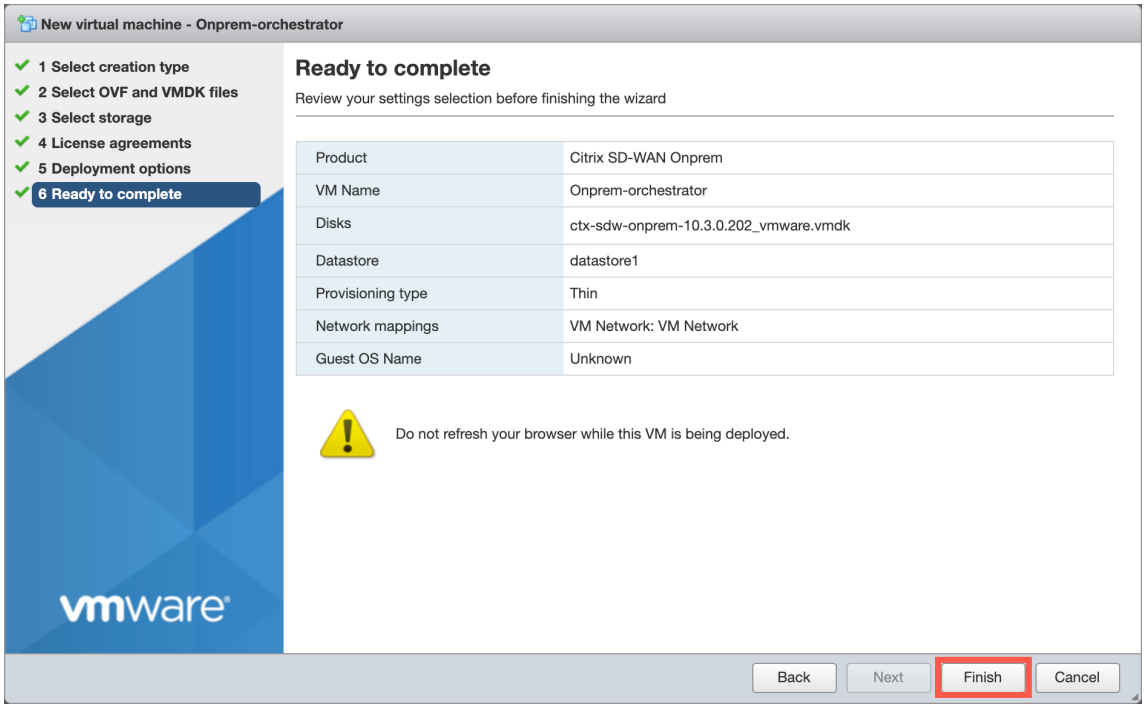


9. デプロイオプションページで、ドロップダウンリストから VM ネットワークを選択し、他のフィールドはデフォルト設定のままにします。[次へ] をクリックします。



10. [設定の確認] ページで、[完了] をクリックして仮想マシンを作成します。

> 注:
>
> ディスクイメージをサーバーに解凍するには、数分かかることがあります。

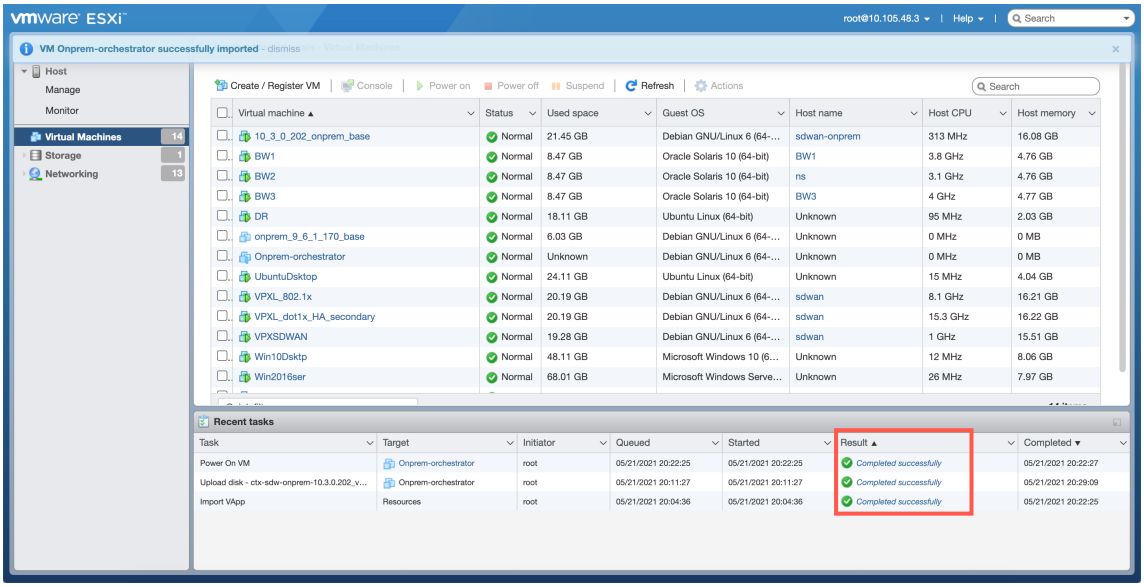


ESXi サーバ上の管理 IP アドレスを表示して記録します

管理 IP アドレスは、オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator の IP アドレスです。この IP アドレスを使用して、オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator にログインします。

管理 IP アドレスを表示するには、次の操作を行います。

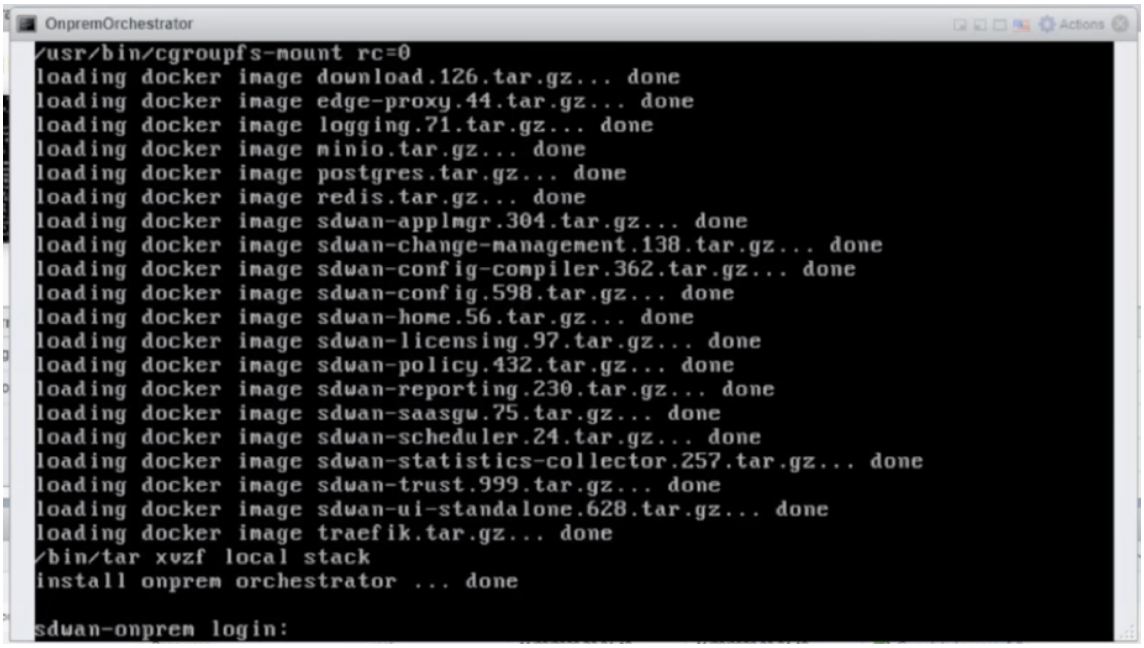
1. vSphere クライアントのインベントリページで、オンプレミス仮想マシン用の新しい Citrix SD-WAN Orchestrator を選択します。
2. オンプレミス用 Citrix SD-WAN Orchestrator ページの [最近のタスク] で、結果が [完了] と表示されるのを待ちます。



3. コンソールタブを選択し、コンソール領域内の任意の場所をクリックしてコンソールモードに入ります。

> 注
>
> カーソルのコンソールコントロールを解除するには、<Ctrl>キーと<Alt>キーを同時に押します。

4. **Enter** キー を押して、コンソールログインプロンプトを表示します。



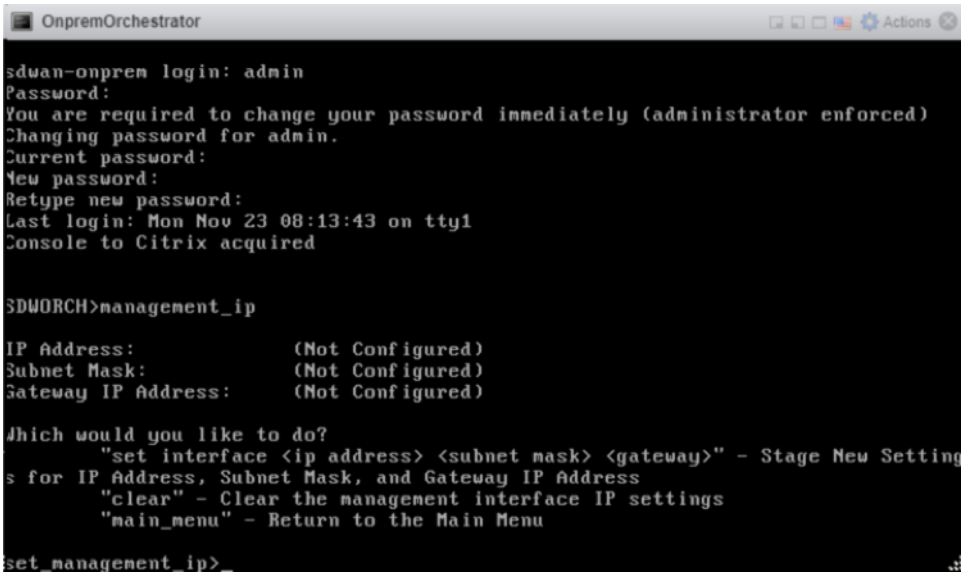
5. 仮想マシンのコンソールにログインします。

   オンプレミス仮想マシンの新しい Citrix SD-WAN Orchestrator のデフォルトのログイン認証情報は次のとおりです。

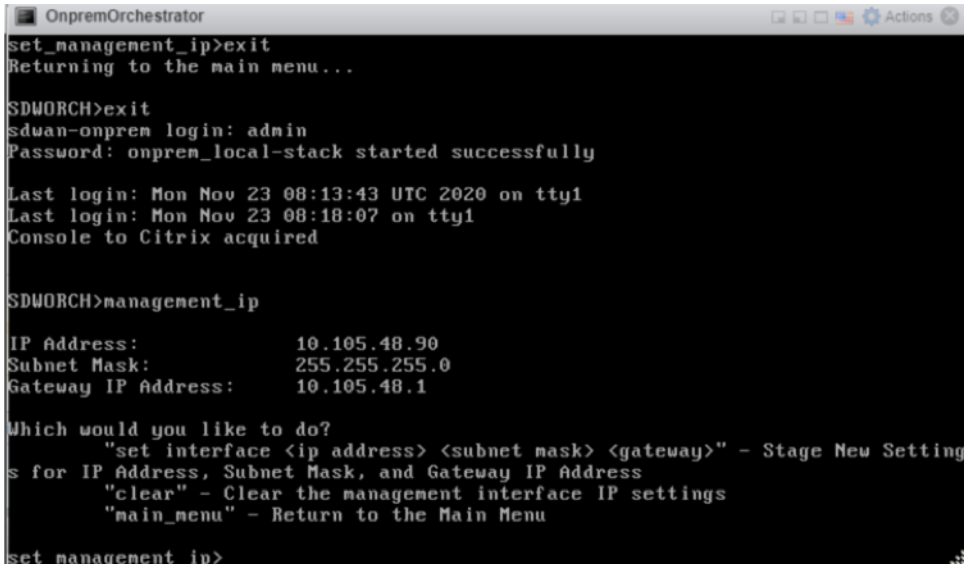
   - ログイン:admin

- **Password**: password

> 注
>
> 初回ログオン時には、デフォルトの管理者ユーザーアカウントのパスワードを変更する必要があります。この変更は、CLI と UI の両方を使用して適用されます。



6. オンプレミス仮想マシンの Citrix SD-WAN Orchestrator の管理 IP アドレスを記録します。これは、ログオン時に表示されるウェルカムメッセージにホスト IP アドレスとして表示されます。



> 注
>
> - DHCP サーバーが SD-WAN ネットワークに存在し、利用可能である必要があります。そうしないと、この手順を完了できません。

> - コンソールで CLI コマンド`set_dns`を入力して現在の DNS サーバー設定を確認し、既存の DNS サーバーが DNS サービスを提供できない場合は DNS サーバーを再構成します。`set_dns` コマンドの使用方法について詳しくは、「Citrix SD-WAN Orchestrator for オンプレミスログイン」を参照してください。

DHCP サーバーが SD-WAN ネットワークで構成されていない場合は、静的 IP アドレスを手動で入力する必要があります。

静的 IP アドレスを管理 IP アドレスとして設定するには:

1. 仮想マシンが起動したら、コンソールタブをクリックします。
2. 仮想マシンにログインします。オンプレミス仮想マシンの新しい Citrix SD-WAN Orchestrator のデフォルトのログイン認証情報は次のとおりです。
   - ログイン:admin
   - **Password**: password
3. コンソールで CLI コマンド`management_ip`を入力します。
4. コマンド`set interface <ipaddress> <subnetmask> <gateway>`を入力して、管理 IP を設定します。
5. 管理インターフェイスの IP 設定を変更してもよろしいですか?

   アプライアンスへの接続が失われる可能性があります。<y/n>?

   「y」を押して IP を変更し、約 6〜7 分後に設定した新しい管理 IP にアクセスします。

XenServer にオンプレミス用 SD-WAN Orchestrator をインストールして構成する

October 26, 2022

オンプレミス用 Citrix SD-WAN Orchestrator を XenServer インストールする前に、「インストールと構成のチェックリスト」の説明に従って必要な情報を収集します。

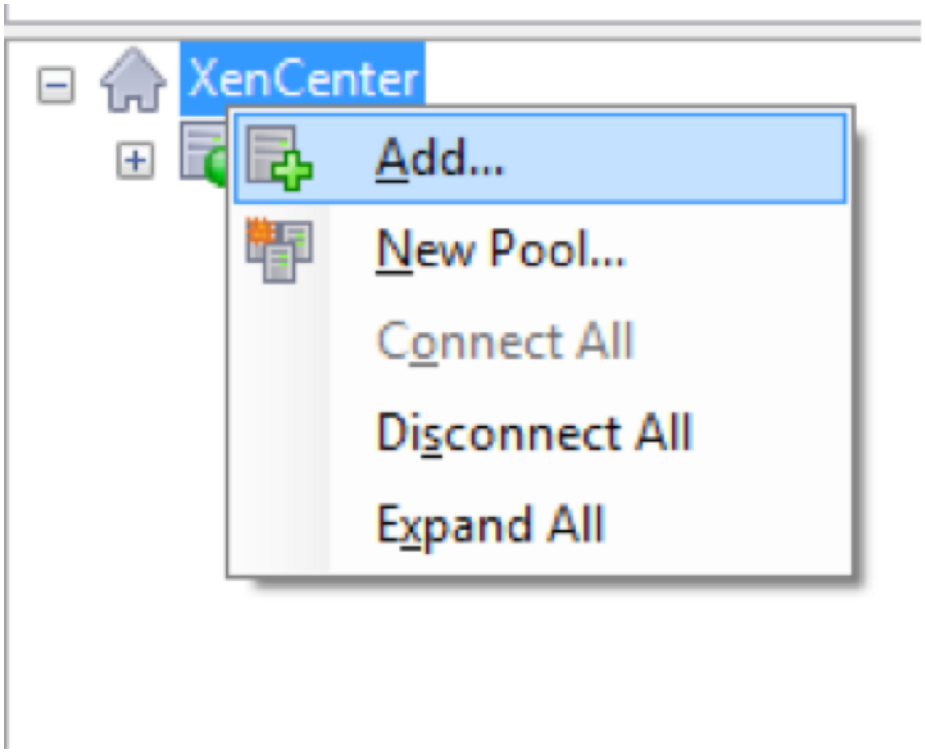
XenServer サーバーのインストール

オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator を展開する Citrix XenServer サーバーをインストールするには、コンピューターに XenCenter をインストールする必要があります。XenCenter をまだダウンロードしていない場合は、ダウンロードしてインストールしてください。

XenServer をインストールするには:

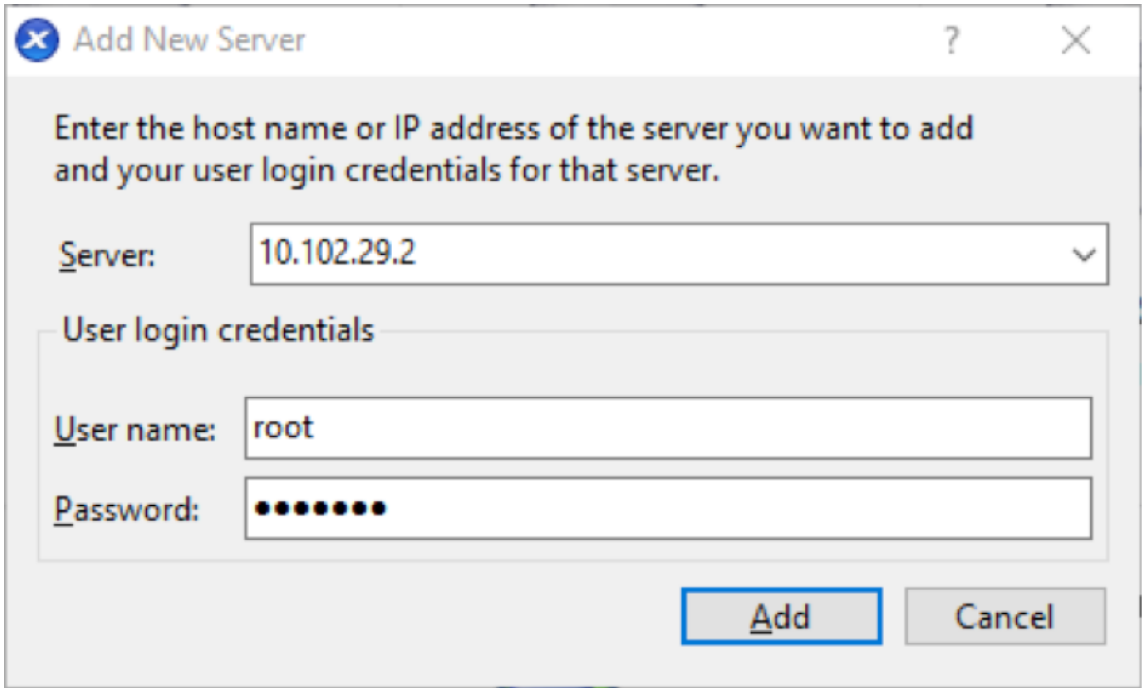
1. パソコンで XenCenter アプリケーションを開きます。

2. 左側のツリーペインで、**XenCenter** を右クリックして［追加］を選択します。



3.「新規サーバーの追加」ウィンドウで、次のフィールドに必要な情報を入力します。

- サーバー: Citrix SD-WAN Orchestrator for オンプレミス仮想マシンインスタンスをホストする XenServer サーバーの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。
- ユーザー名: サーバー管理者のアカウント名を入力します。デフォルトは［root］です。
- パスワード: この管理者アカウントに関連付けられているパスワードを入力します。



4. ［追加］をクリックします。

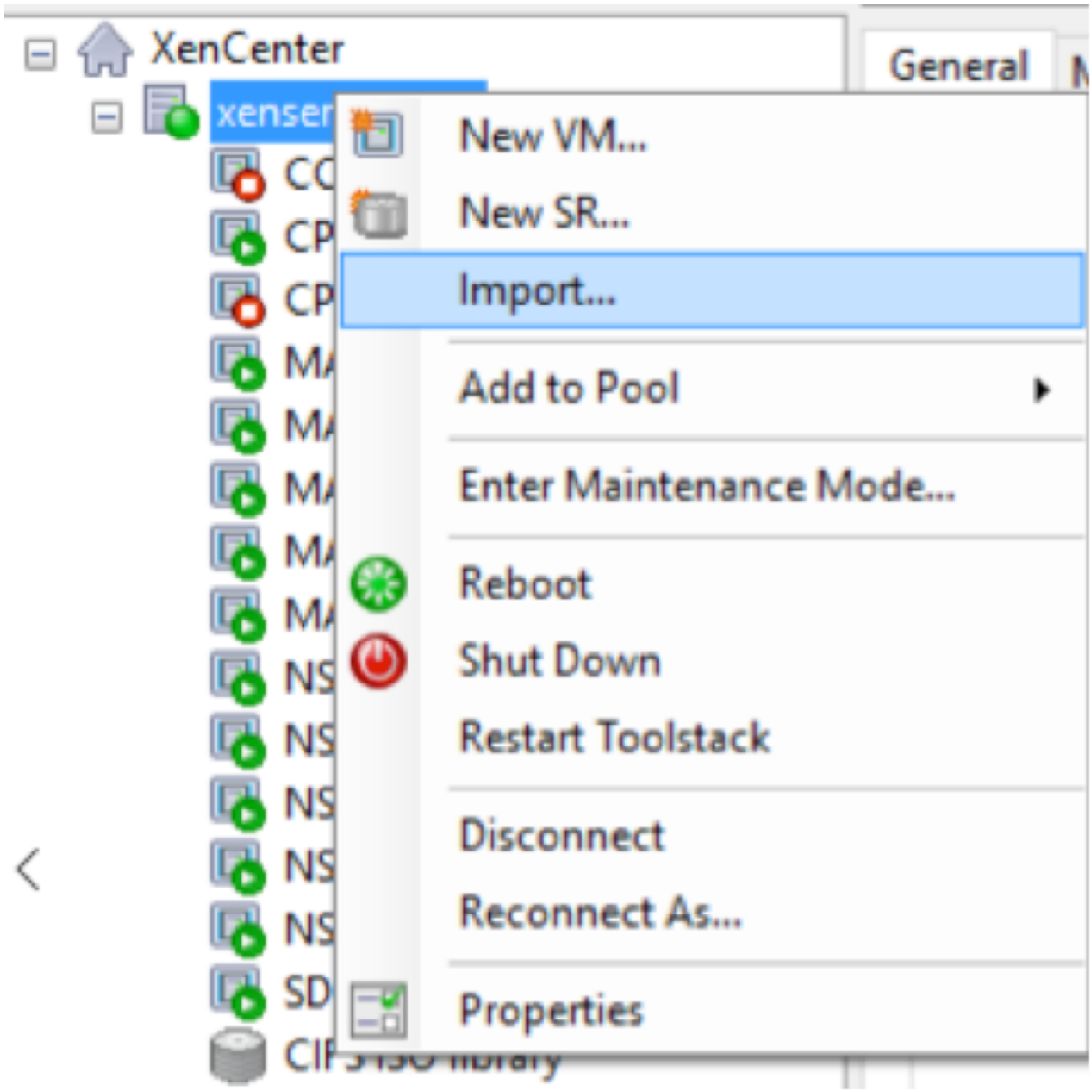
新しいサーバーの IP アドレスが左側のペインに表示されます。

XVA ファイルを使用して、オンプレミス仮想マシン用 **Citrix SD-WAN Orchestrator** を作成します

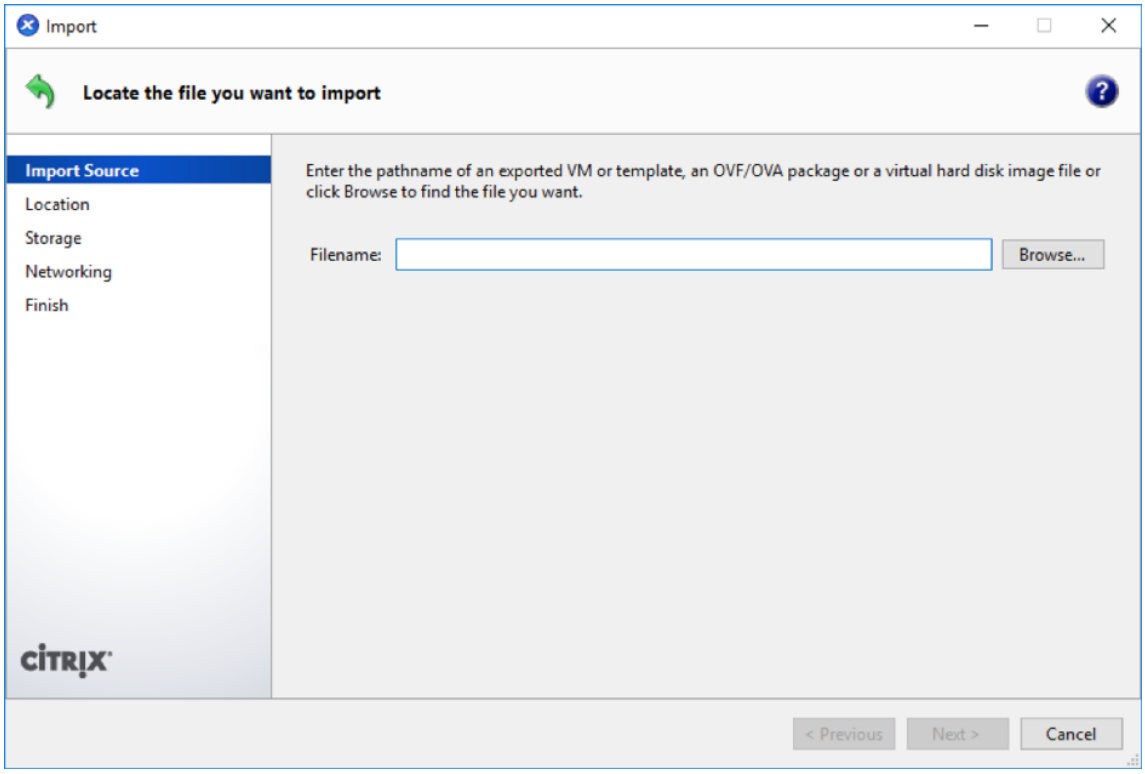
オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator ソフトウェアは、XVA ファイルとして配布されます。まだ行っていない場合は、.xva ファイルをダウンロードします。詳しくは、「システム要件とインストール」を参照してください。

オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator を作成するには:

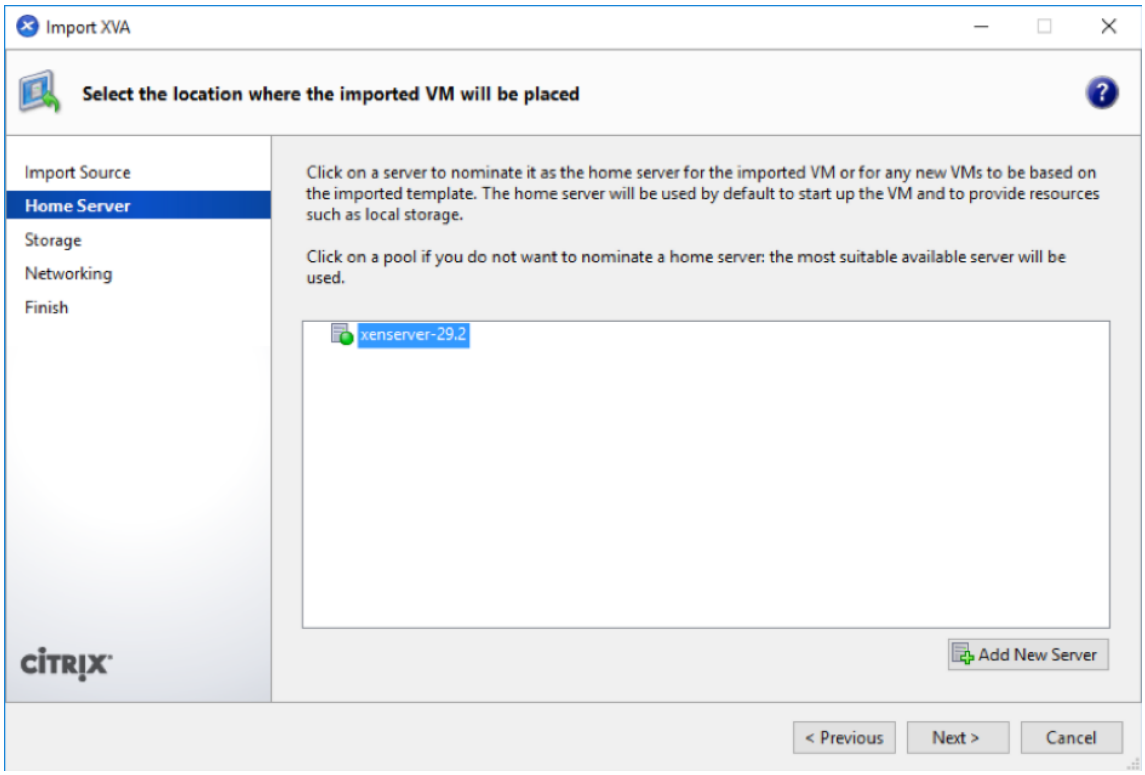
1. XenCenter で、［**XenServer** ］を右クリックして［インポート］をクリックします。



2. ダウンロードした.xva ファイルを参照して選択し、[次へ] をクリックします。

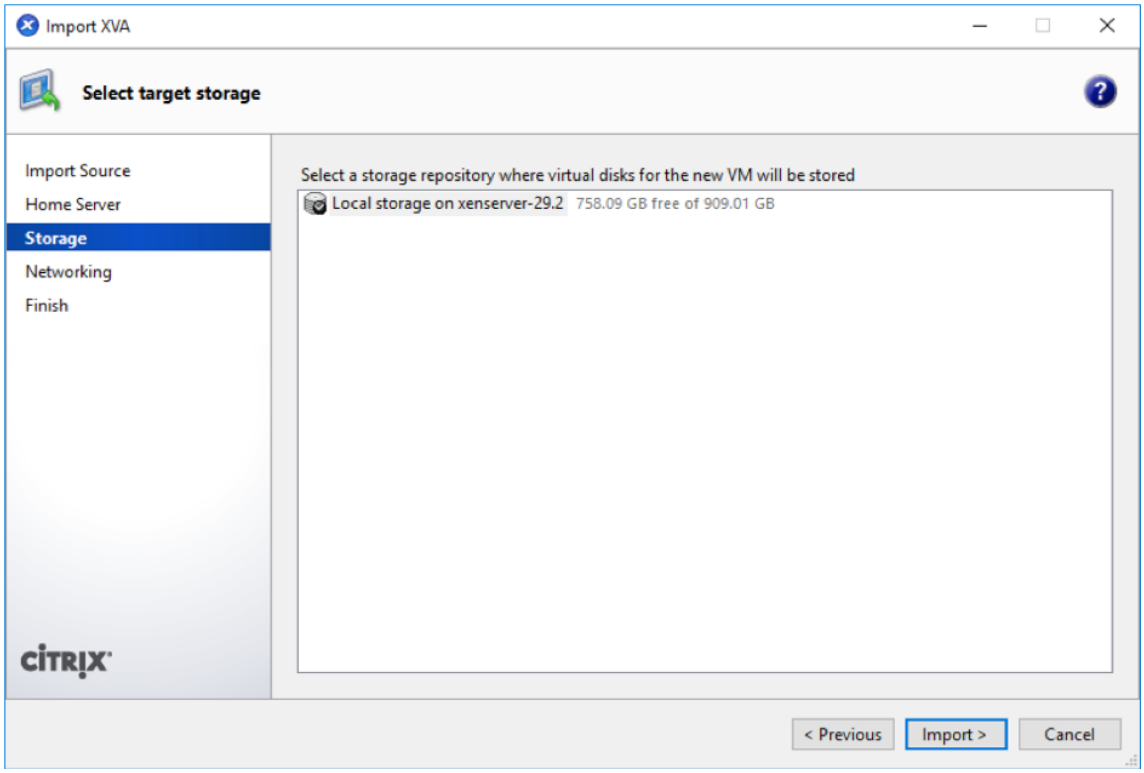


3. 仮想マシンをインポートする場所として以前に作成した XenServer を選択し、［次へ］をクリックします。



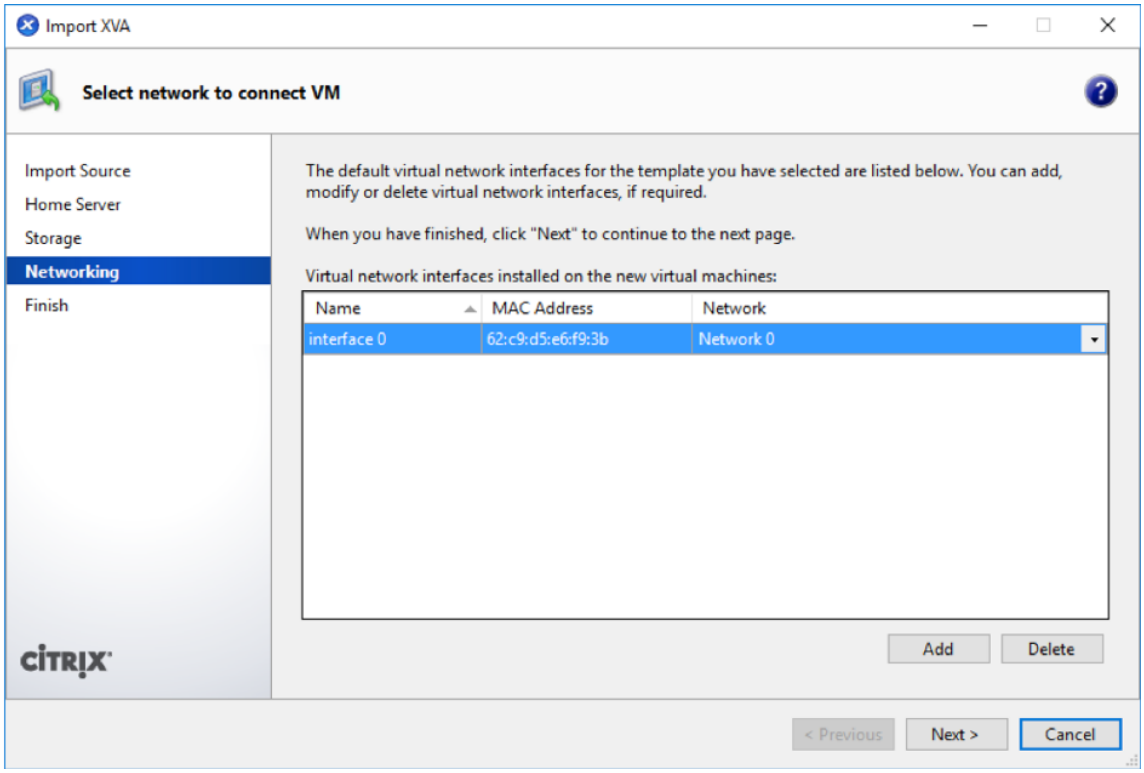
4. 新しい仮想マシンの仮想ディスクが保存されているストレージリポジトリを選択し、[インポート] をクリックします。

今のところ、デフォルトのストレージリソースをそのまま使用できます。または、データストアを設定することもできます。



インポートされたオンプレミス仮想マシン用 Citrix SD-WAN Orchestrator が左側のペインに表示されます。

5. 仮想マシンを接続するネットワークを選択し、[次へ] をクリックします。



6. [完了] をクリックします。

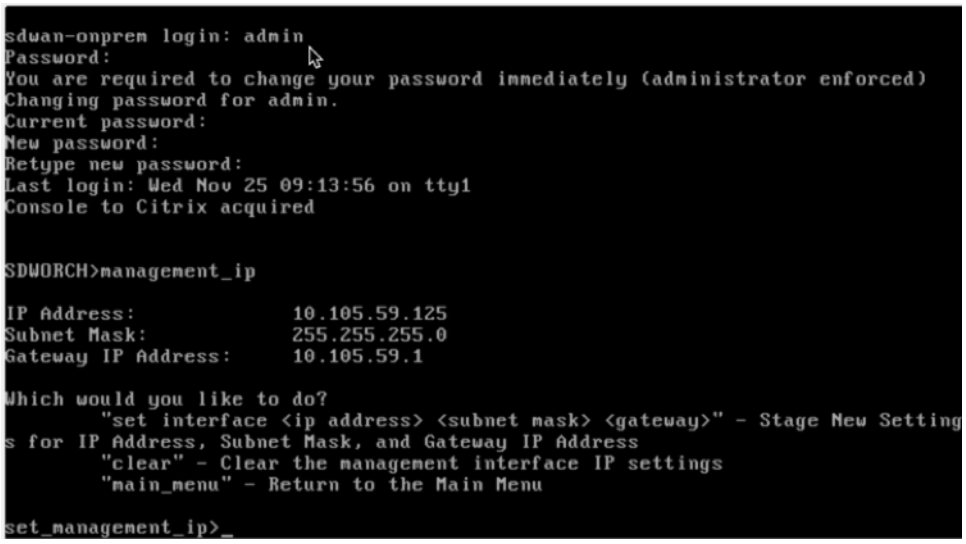
XenServer の管理 IP アドレスを表示および記録します

管理 IP アドレスは、オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator の IP アドレスです。この IP アドレスを使用して、オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator にログインします。

> 注:
>
> DHCP サーバーが SD-WAN ネットワークに存在し、利用可能である必要があります。

管理 IP アドレスを表示するには:

1. XenCenter インターフェイスの左側のペインで、オンプレミス仮想マシン用の新しい Citrix SD-WAN Orchestrator を右クリックして、「開始」を選択します。
2. 仮想マシンが起動したら、コンソールタブをクリックします。



3. 管理 IP アドレスを書き留めておきます。

   > 注:
   >
   > DHCP サーバーが SD-WAN ネットワークに存在し、利用可能でない場合、この手順を完了できません。

4. 仮想マシンにログインします。オンプレミス仮想マシンの新しい Citrix SD-WAN Orchestrator のデフォルトのログイン認証情報は次のとおりです。

   ログイン:admin

   Password: password

   > 注:
   >
   > 初回ログオン時には、デフォルトの管理者ユーザーアカウントのパスワードを変更する必要があります。この変更は、CLI と UI の両方を使用して適用されます。

   DHCP サーバーが Citrix SD-WAN ネットワークで構成されていない場合は、静的 IP アドレスを手動で入力する必要があります。

静的 IP アドレスを管理 IP アドレスとして設定するには:

1. 仮想マシンが起動したら、コンソールタブをクリックします。
2. 仮想マシンにログインします。オンプレミス仮想マシンの新しい Citrix SD-WAN Orchestrator のデフォルトのログイン認証情報は次のとおりです。

   ログイン:admin

   Password: password

3. コンソールで CLI コマンド`management_ip`を入力します。

4. コマンド`set interface <ipaddress> <subnetmask> <gateway>`を入力して、管理 IP を設定します。
5. 管理インターフェイスの IP 設定を変更してもよろしいですか?

   アプライアンスへの接続が失われる可能性があります。<y/n>?

   「y」を押して IP を変更し、約 6〜7 分後に設定した管理 IP にアクセスします。

オンプレミス用 **SD-WAN Orchestrator** のオンボーディング

October 26, 2022

オンプレミス向け Citrix SD-WAN Orchestrator のオンボーディングプロセスの概要は次のとおりです。

- オンボーディングプロバイダーとテナント：お客様は、マルチテナントの Citrix SD-WAN Orchestrator サービスによって可能な、Citrix パートナーのマネージド SD-WAN サービスを利用できます。
- 「Do It Yourself」（DIY）企業のオンボーディング：Citrix SD-WAN Orchestrator サービスは、企業向けの自己管理サービスとしても利用できます。

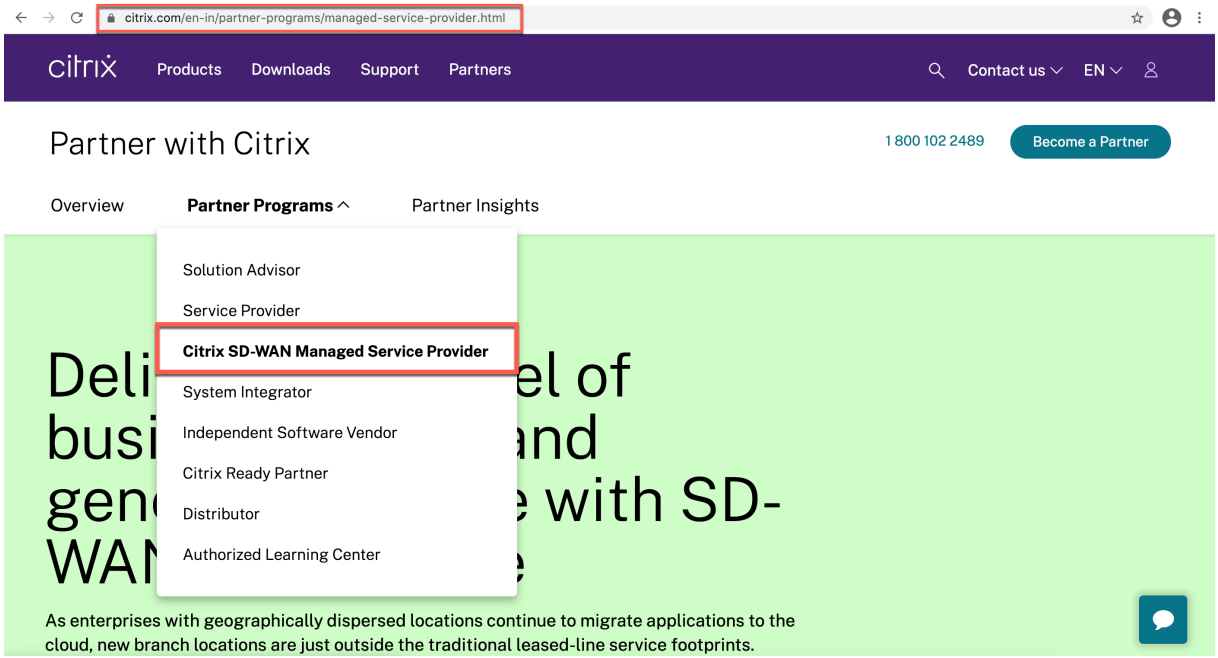
オンボーディングプロバイダーとテナント

このセクションでは、Citrix パートナーとそのテナントのオンボーディングプロセスについて説明します。
ここでは、初期登録プロセスの概要を示します。

1. パートナー候補者は Citrix Partner として登録します。
2. Citrix Partner は、Citrix SD-WAN リセラーとして登録します。

パートナーが **Citrix** パートナーシッププログラムにサインアップする

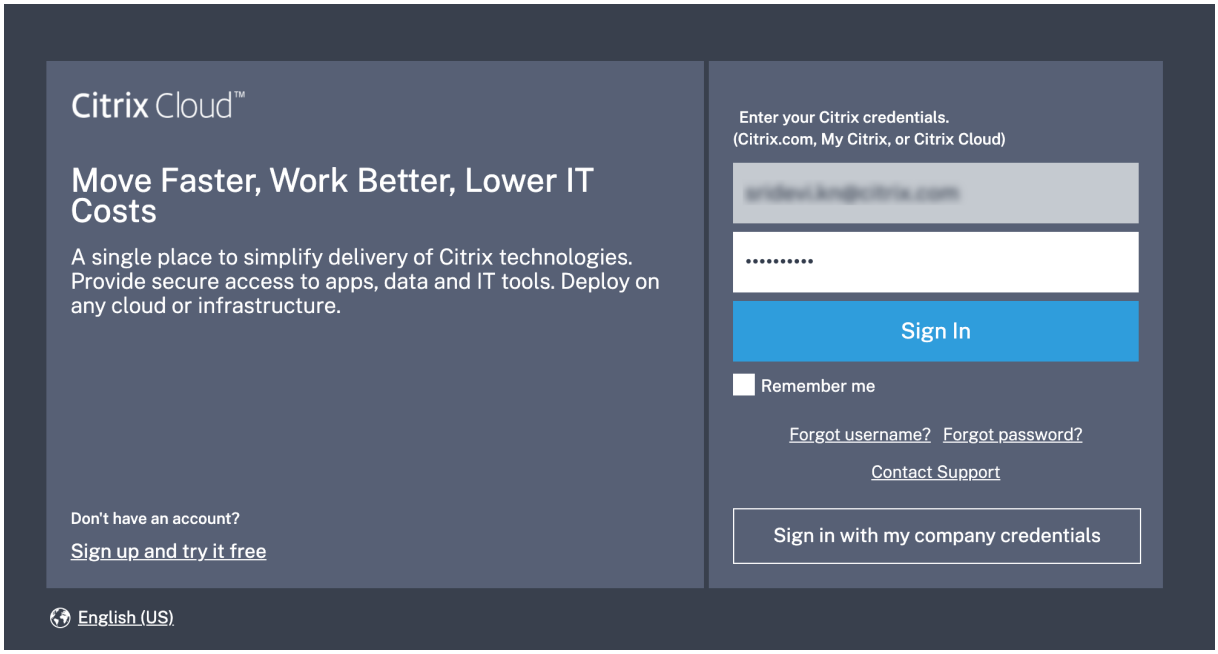
パートナー候補者は、Citrix Service Provider プログラム（CSP）- CSP のサインアップにサインアップする必要があります。
パートナーは、Citrix SD-WAN パートナー向けに特別に作成された Citrix SD-WAN マネージドサービスプロバイダープログラム（SD-WAN MSP Sign Up）にサインアップすることもできます。



登録プロセスの一環として、パートナー用の Citrix Cloud（CC）アカウントが作成されます。詳しくは、「Citrix Cloud へのサインアップ」を参照してください。

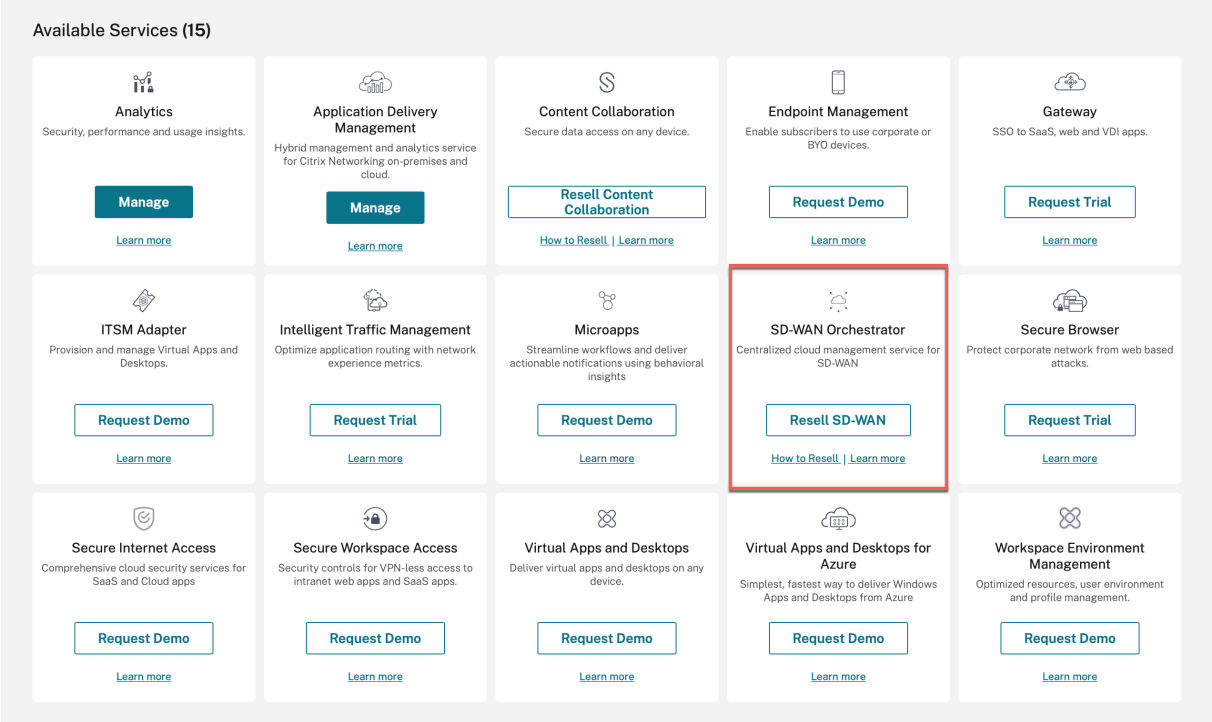
パートナーが **Citrix SD-WAN** リセラーとして登録する

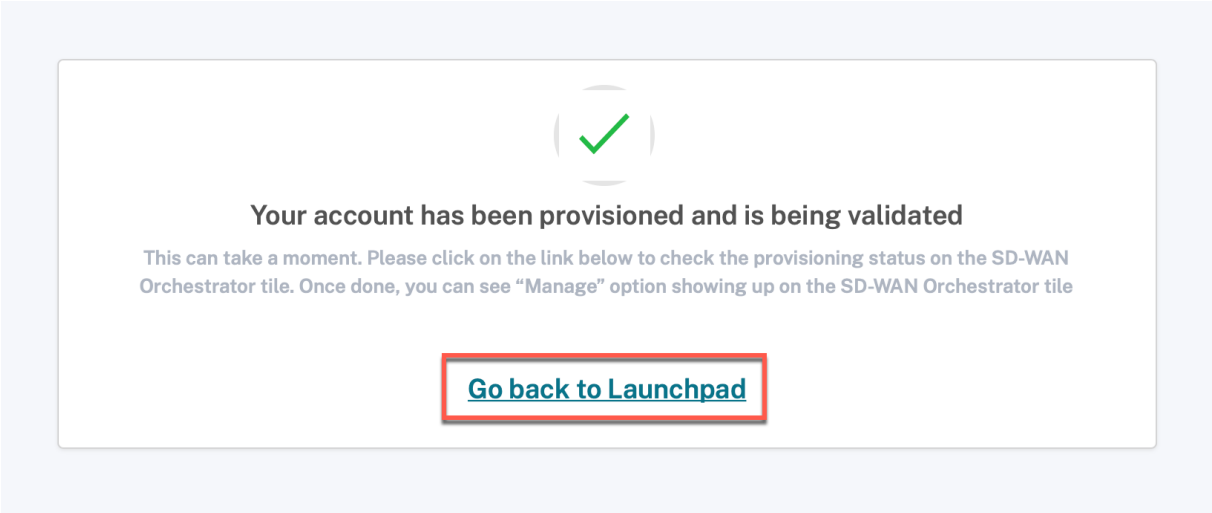
パートナーは Citrix Cloud アカウントにログインします。



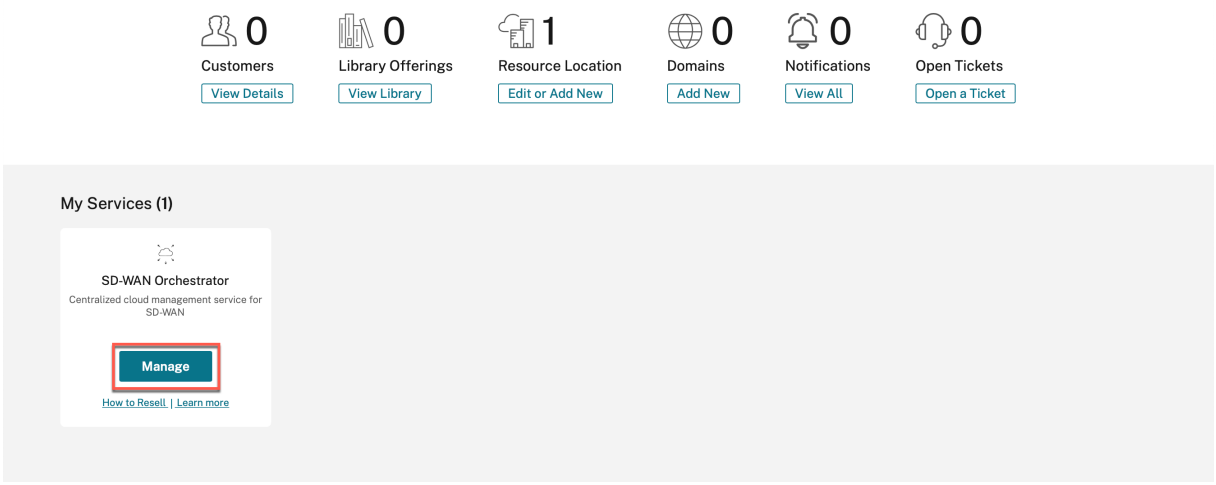
Citrix Cloud で利用可能なすべてのサービスのメニューがホームページに表示されます。**Citrix SD-WAN Orchestrator** サービスタイルは、「利用可能なサービス」セクションにあります。パートナーは、タイルの

「**SD-WAN** を再販する」をクリックして、Citrix SD-WAN 再販業者またはサービスプロバイダーとして登録します。





Citrix SD-WAN Orchestrator サービスタイルが [マイサービス] の下に表示されるようになりました。

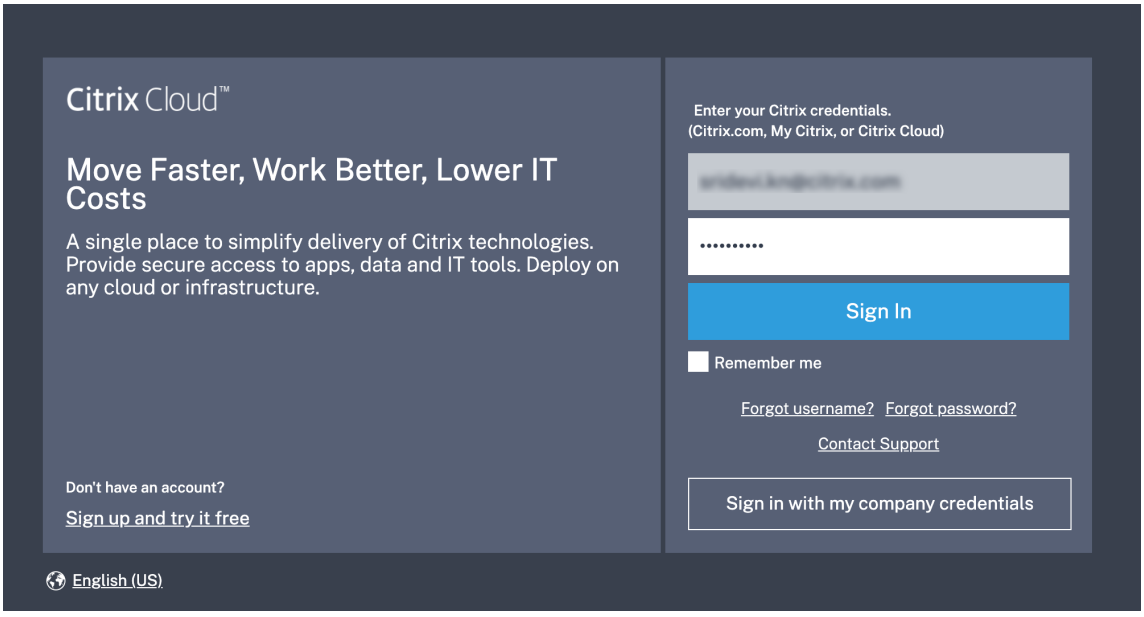


DIY エンタープライズ顧客のオンボーディング

このセクションでは、DIY エンタープライズカスタマーをオンボードするプロセスと、SD-WAN ネットワークを管理するように管理者に招待する手順について説明します。

DIY カスタマーのオンボーディング

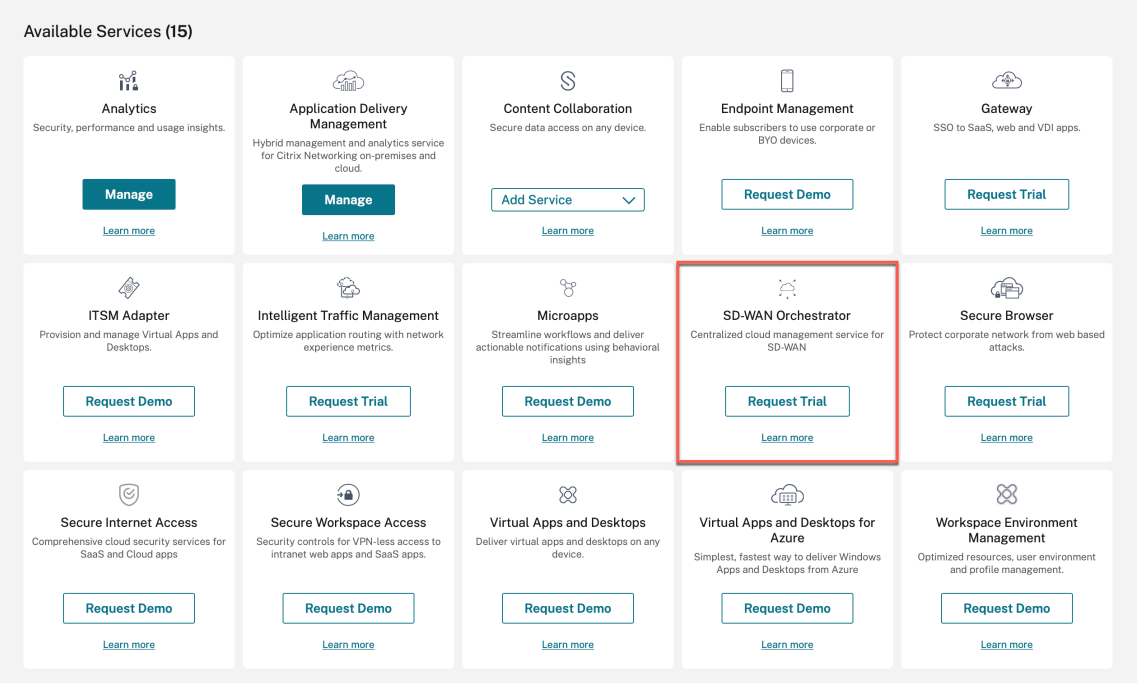
1. お客様は Citrix Cloud アカウントにログインします。



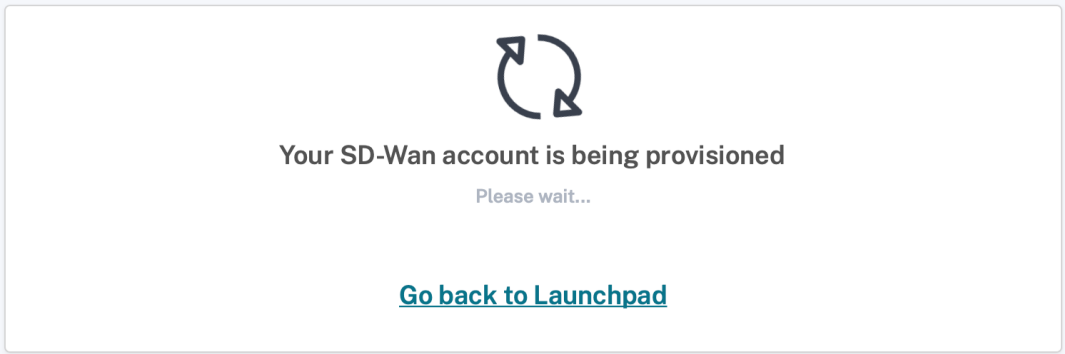
   Citrix Cloud で利用可能なすべてのサービスのメニューがホームページに表示されます。**Citrix SD-WAN Orchestrator** サービスタイルは、「利用可能なサービス」セクションにあります。

> 注
>
> Citrix Cloud にサインアップする場合は、1 つの公式アカウントのみを使用してください。使用する会社名と電子メール ID は、1 つの Citrix Cloud アカウントにのみ関連付ける必要があります。

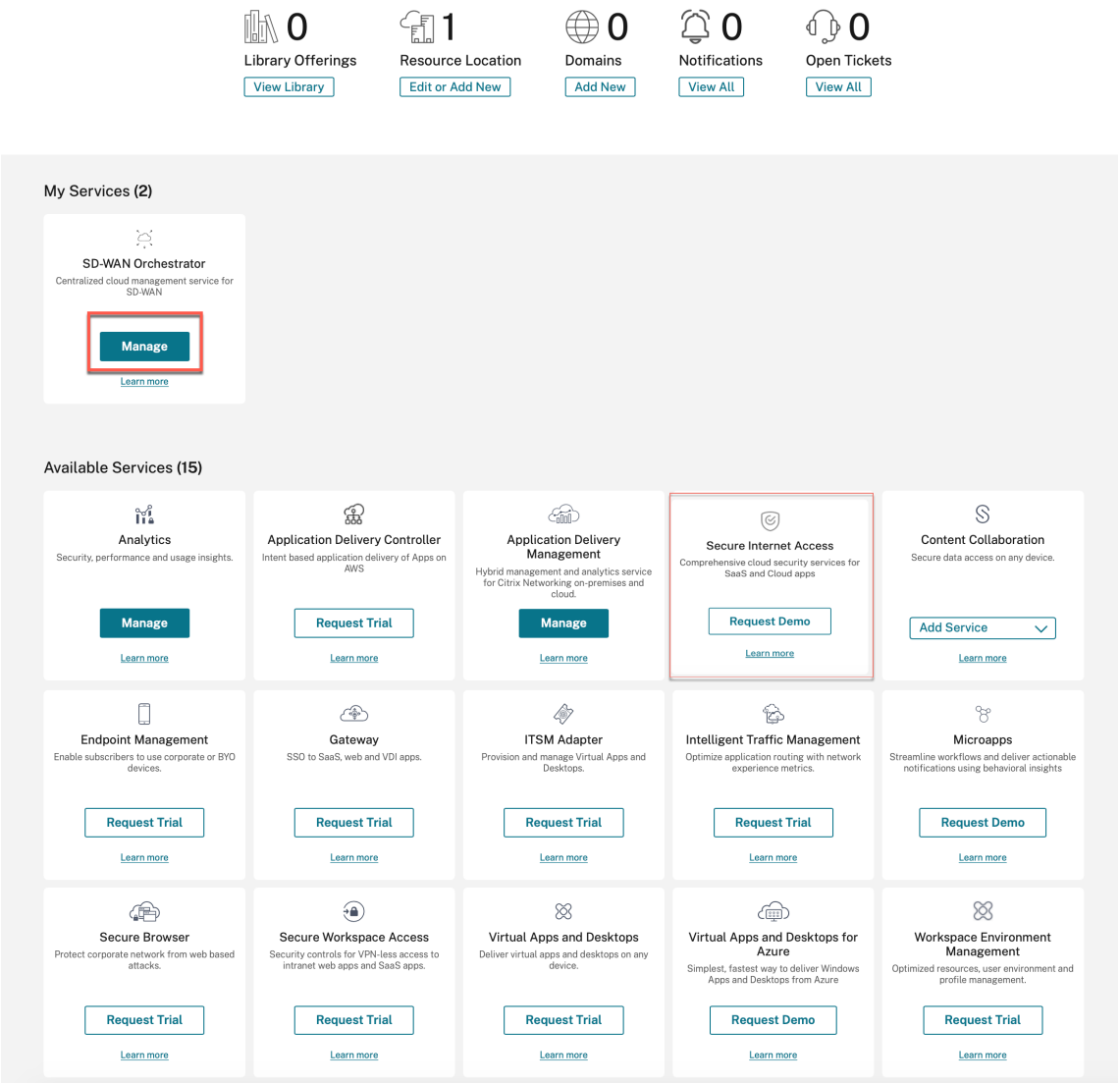
2. お客様は [トライアルをリクエスト] をクリックします。



カスタマーの SD-WAN アカウントがプロビジョニングされます。



3. **Citrix SD-WAN Orchestrator** サービスタイルが [マイサービス] の下に表示されるようになりました。



オンプレミスログイン用 **Citrix SD-WAN Orchestrator**

July 19, 2023

この記事では、お客様がオンプレミス向け Citrix SD-WAN Orchestrator に初めてログインする方法について説明します。

オンプレミス向け Citrix SD-WAN Orchestrator にログインする前に必要な前提条件は次のとおりです。

- Citrix Cloud アカウントが必要です。詳細については、「お客様が SD-WAN Orchestrator にアクセスする」を参照してください。

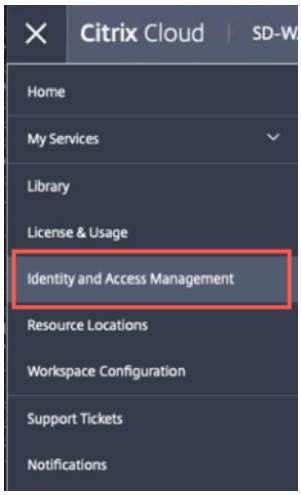
- Citrix SD-WAN Orchestrator をオンプレミスで使用するには、Citrix SD-WAN Orchestrator サービスのアカウントが必要です。詳しくは、「Citrix SD-WAN Orchestrator サービスのオンボーディング」を参照してください。
- カスタム権限を持つ管理者を作成します。
- API Access ページからクライアントを作成して、顧客 ID、ID、および秘密の詳細を取得します。これらの詳細は、オンプレミス用 Citrix SD-WAN Orchestrator のログイン時に必要です

> 注:
>
> Cloud ログインがないと、ローカルログインに進むことはできません。

管理者を作成

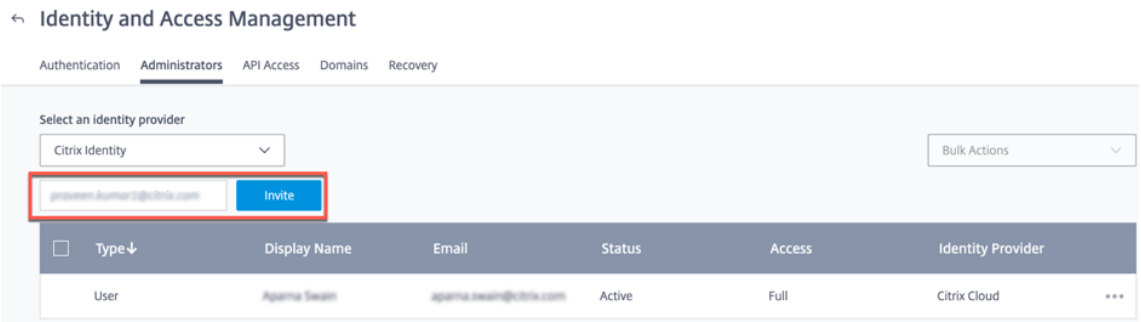
プロバイダーまたは企業のお客様は、管理者を招待して SD-WAN ネットワークを管理することができます。管理者を招待するには、以下の手順を実行します。

1. Citrix Cloud にログインし、[**ID** およびアクセス管理] に移動します。

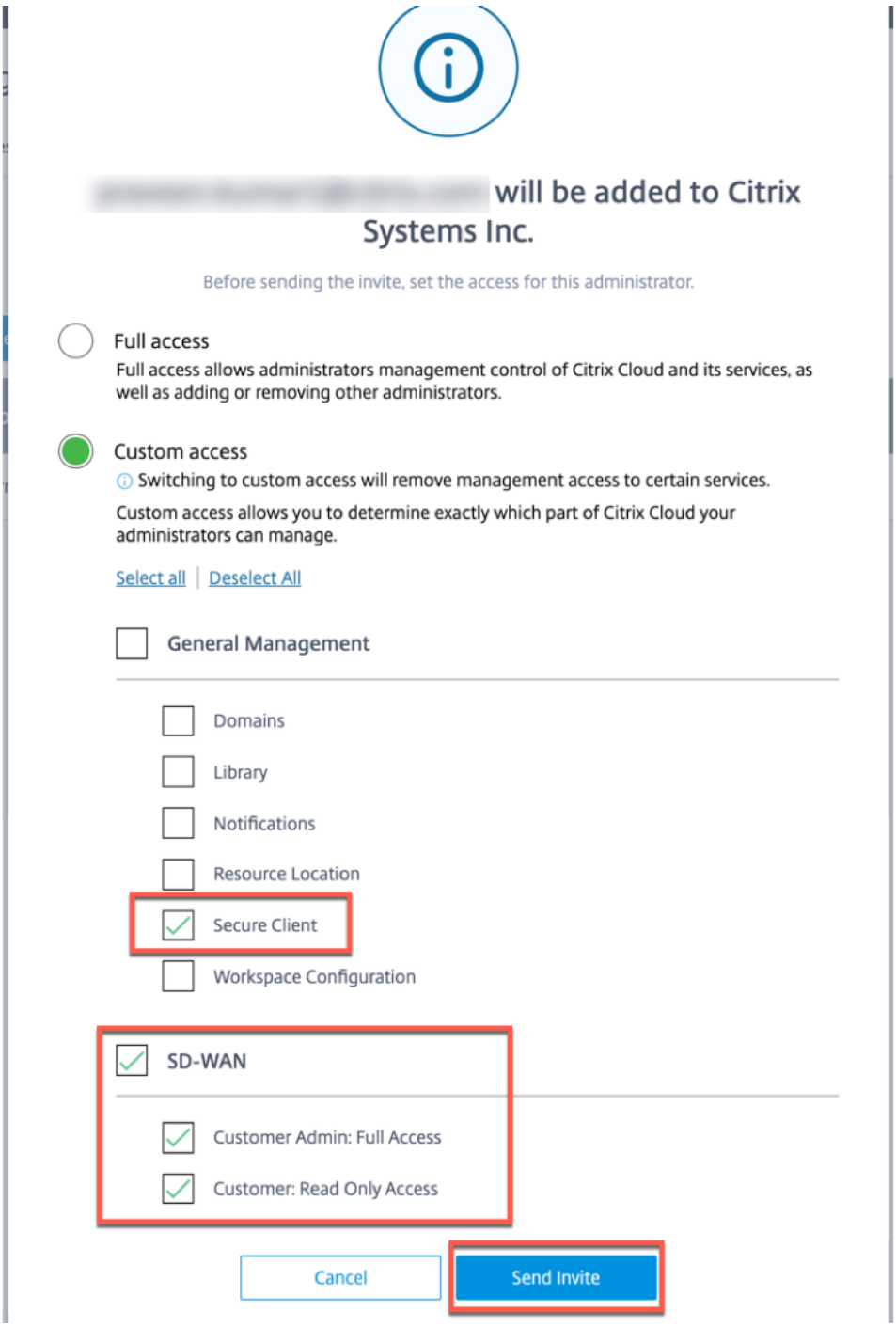


2. 管理者ページに移動し、**ID** プロバイダーのドロップダウンリストから「**Citrix** Identity」を選択します。

3. 新しい管理者の電子メール ID を入力し、[招待] をクリックします。



4. [フルアクセス] または **[**** カスタムアクセス] を選択できます。**SD-WAN** サービスのみを管理する管理者には、カスタムアクセスを設定することをお勧めします。**[**** カスタムアクセス] ラジオボタンを選択した場合は、[一般管理] セクションの [セキュアクライアント] チェックボックスと [**SD-WAN**] チェックボックスも選択する必要があります。



5. ［招待を送信する］をクリックします。

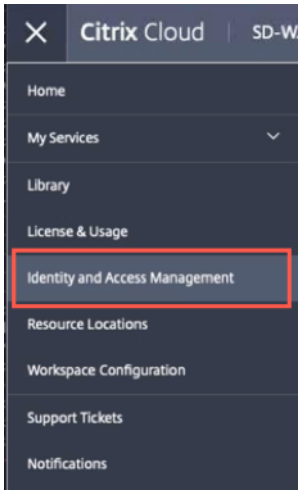
管理者アカウントを作成したら、管理者アカウントからログインして **API** キーを生成します。

> 注:
>
> カスタム管理者ロールが既にある場合は、そのロールを使用して API トークンを作成できます。

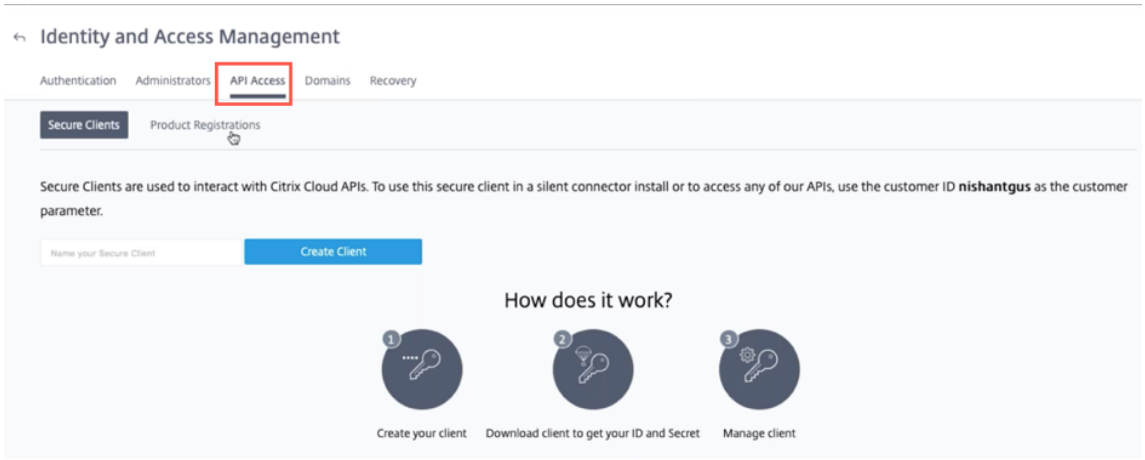
API トークンを生成

次の手順を実行して、オンプレミス用 Citrix SD-WAN Orchestrator にログインします。

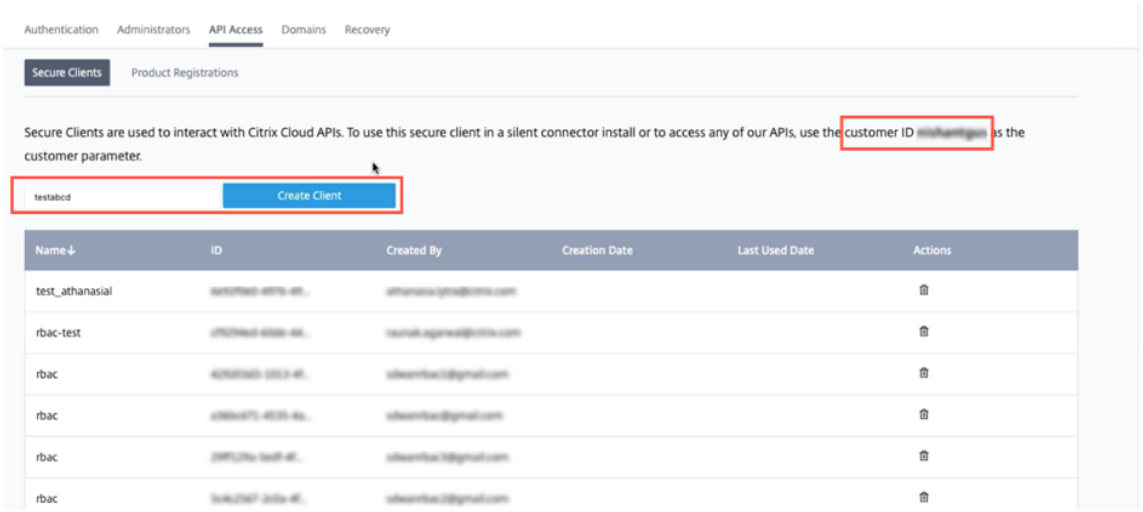
1. Citrix Cloud にログインし、[**ID** およびアクセス管理] に移動します。



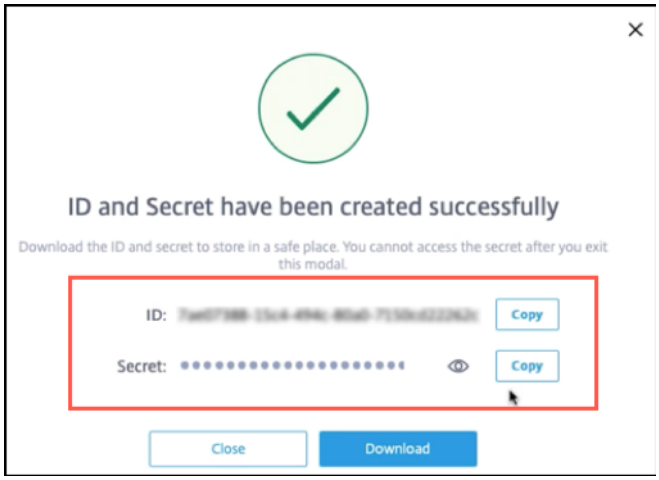
2. **API** アクセスページに移動します。



3. クライアントを作成します。後でオンプレミス用 Citrix SD-WAN Orchestrator にログインするときに必要になる顧客 **ID** を書き留めておきます。



4. **Create Client** をクリックすると、コピーして保存したり、ダウンロードしたりできる **ID** とシークレットキーが表示されます。



5. Citrix Hypervisor（XenServer/VMware）に移動し、オンプレミス用 Citrix SD-WAN Orchestrator を起動します。
6. オンプレミス用 Citrix SD-WAN Orchestrator を起動したら、デフォルトのユーザー名（admin）とパスワード（パスワード）を入力します。

   > 注:
   >
   > 初回ログオン時には、デフォルトの管理者ユーザーアカウントのパスワードを変更する必要があります。この変更は、CLI と UI の両方を使用して適用されます。

7. DHCP サーバーが SD-WAN ネットワークで構成されていない場合は、静的 IP アドレスを手動で入力する必要があります。静的 IP アドレスを管理 IP アドレスとして設定するには:

   - コンソールで CLI コマンド`management_ip`を入力します。
   - コマンド`set interface <ipaddress> <subnetmask> <gateway>`を入力します。

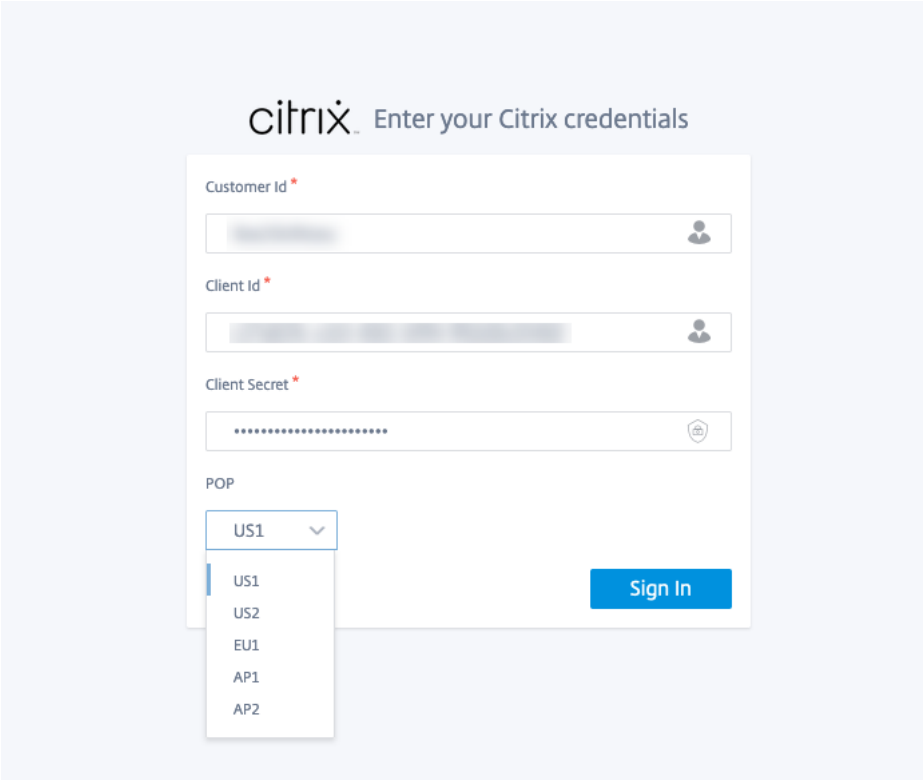
> 注
>
> - 管理 IP アドレスは、オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator の IP アドレスです。この IP アドレスを使用して、オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator にログインします。
> - 管理インターフェイスは、CLI と DHCP の 2 つの方法で設定できます。

8. オンプレミス向け Citrix SD-WAN Orchestrator が起動すると、デフォルトでは DNS サーバー 9.9.9.9 と 149.112.112.112 をそれぞれプライマリとセカンダリとして構成されます。必要に応じて、次のコマンドを使用して DNS サーバーの IP アドレスを変更できます。

   - コンソールで CLI コマンド`set_dns`を入力します。
   - コマンド`set primary <ipaddress>`を入力してから`y`を入力して変更を確認します。
   - コマンド`set secondary <ipaddress>`を入力し、`y`と入力して変更を確認します。

```
SDWORCH>set_dns

Primary :               nameserver 9.9.9.9
Seconday :              nameserver 149.112.112.112

Which would you like to do?
        "set primary <ip address>" - Stage New Primary DNS IP Address
        "set secondary <ip address>" - Stage New Primary DNS IP Address
        "clear" - Clear all DNS IP Address
        "main_menu" - Return to the Main Menu

set_dns>set primary 8.8.8.8

Are you sure you want to change your Domain Name Server IP settings? <y/n>?
y

Primary :               nameserver 8.8.8.8
Seconday :              nameserver 149.112.112.112

Which would you like to do?
        "set primary <ip address>" - Stage New Primary DNS IP Address
        "set secondary <ip address>" - Stage New Primary DNS IP Address
        "clear" - Clear all DNS IP Address
        "main_menu" - Return to the Main Menu

set_dns>set secondary 9.9.9.9

Are you sure you want to change your Domain Name Server IP settings? <y/n>?
y

Primary :               nameserver 8.8.8.8
Seconday :              nameserver 9.9.9.9

Which would you like to do?
        "set primary <ip address>" - Stage New Primary DNS IP Address
        "set secondary <ip address>" - Stage New Primary DNS IP Address
        "clear" - Clear all DNS IP Address
        "main_menu" - Return to the Main Menu
```

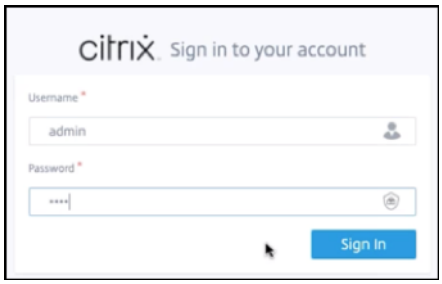
9. 管理 IP を使用して新しいブラウザを開きます。次の画面が表示されます。



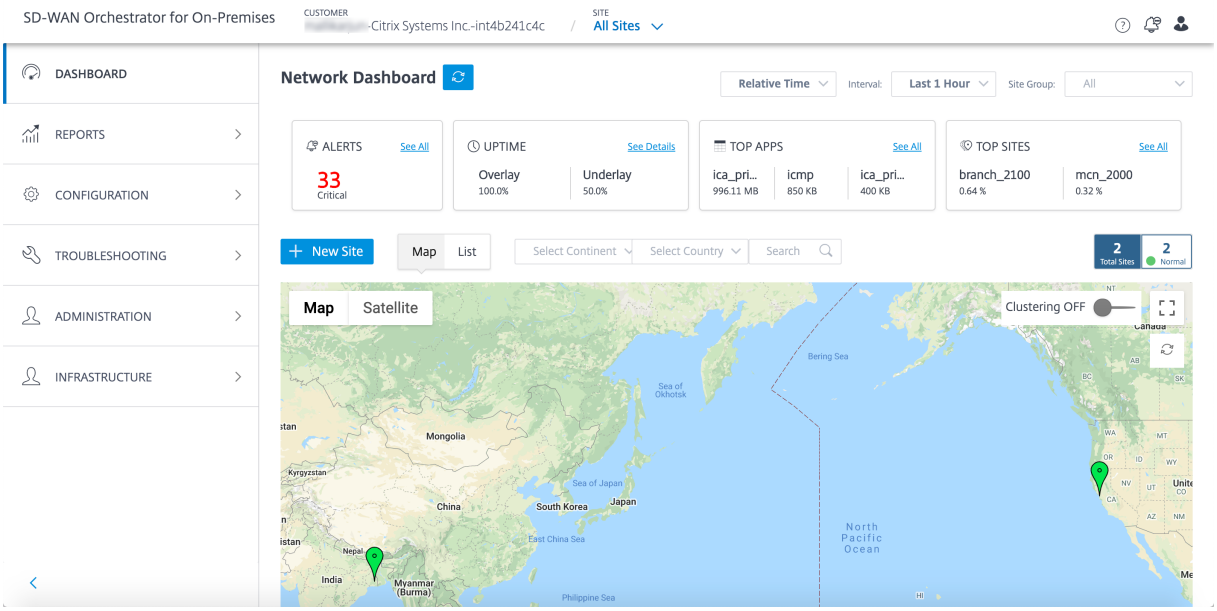
10. クラウド **Orchestrator** からクライアントを作成する際に以前に保存またはダウンロードした顧客 **ID**、クライアント ID、およびクライアントシークレットを指定します。クラウドアカウントが登録されていた POP を選択します。ログインに成功したら POP を変更することはできません。

    > 注:
    >
    > この画面は 15 日に 1 回表示されます。それ以降のログオン/ログアウトでは、ローカルログインページのみが表示されます。

11. ローカルログインページにデフォルトのユーザー名とパスワードを入力します。



オンプレミスダッシュボード用 Citrix SD-WAN Orchestrator ページが表示されます。



オンプレミスライセンス用 **Citrix SD-WAN Orchestrator**

October 26, 2022

Citrix SD-WAN Orchestrator for オンプレミスライセンスは、Do It Yourself（DIY）のお客様、つまり直接の企業のお客様に適用されます。

オンプレミス向け Citrix SD-WAN Orchestrator ライセンスの前提条件として、Citrix Cloud にログインしていることを確認してください。詳しくは、「オンプレミスログイン用 Citrix SD-WAN Orchestrator」を参照してください。

オンプレミス展開用 Citrix SD-WAN Orchestrator は無料で利用できますが、管理サーバーのインフラストラクチャとメンテナンスの費用はお客様が負担する必要があります。

トライアルモード

お客様のオンプレミス用 Citrix SD-WAN Orchestrator アカウントは試用モードでプロビジョニングされます。試用モードはデフォルトで 60 日間継続されます。

試用期間が終了すると、お客様のデータパスは停止します。有効なライセンスがアップロードされるまで、追加の変更は展開できません。オンプレミス向け Citrix SD-WAN Orchestrator のお客様の Citrix Cloud 資格は、最初の有効なライセンスがホストされると、試用版から実稼働版に変更されます。アップロードされたライセンスの数とタイプに基づいて、同等の数のサイトに、適切な帯域幅エンタイトルメントを使用できます。体験版の有効期限が切れたという永続的なメッセージ 。ネットワーク機能を復元して使用を続けるには、**Orchestrator** で少なくとも **1** つの

有効なライセンス資格を取得して実稼働環境にアップグレードします。プリペイドをご利用のお客様には表示されます。詳細については、「前払い請求モデルの資格の取得と割り当て」を参照してください。

プリペイド課金モデル

オンプレミスのお客様向けの Citrix SD-WAN Orchestrator には、プリペイド請求モデルが提供されています。次の 3 種類のプリペイド課金モデルを使用できます。

- プリペイド年間サブスクリプション: プリペイドサブスクリプションには、1 年プランと 3 年プランがあります。サブスクリプションの有効期限が切れます。お客様のネットワーク内のすべてのアプライアンスには、前払いの年間サブスクリプションがあります。メンテナンスライセンスはサブスクリプションパッケージに含まれており、アプライアンスを新しいソフトウェアバージョンにアップグレードできます。
- プリペイドパーペチュアル: プリペイドパーペチュアルでは、ライセンスには時間制限、制限期間、有効期限はありません。ただし、ハードウェアメンテナンスライセンスは有料のアドオンとして提供され、別途購入する必要があります。カスタマーネットワーク内のすべてのアプライアンスには、前払いの永久サブスクリプションがあります。

オンプレミス向け Citrix SD-WAN Orchestrator の請求モデルを表示するには、ネットワークレベルで [管理] > [ライセンス] **>** [請求モデルの選択] に移動します。請求モデルは「前払い」、「年払い」と「無期限」と表示されます。

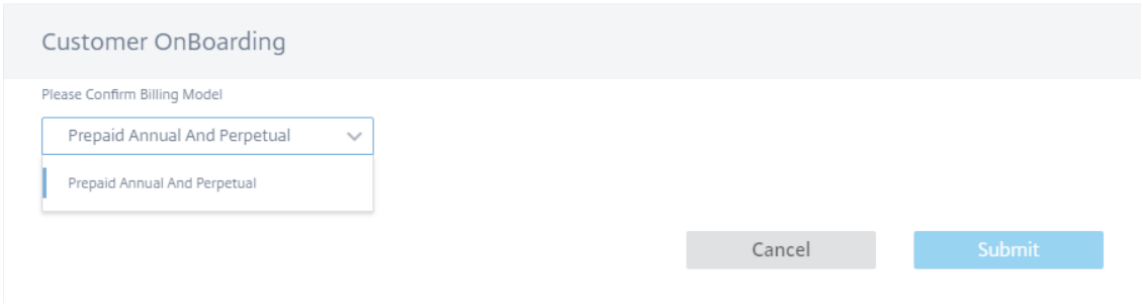
ライセンスをすべての顧客サイトにアップロードします。詳細については、「前払い請求モデルの資格の取得と割り当て」を参照してください。

前払い請求モデルのエンタイトルメントを取得して割り当てる

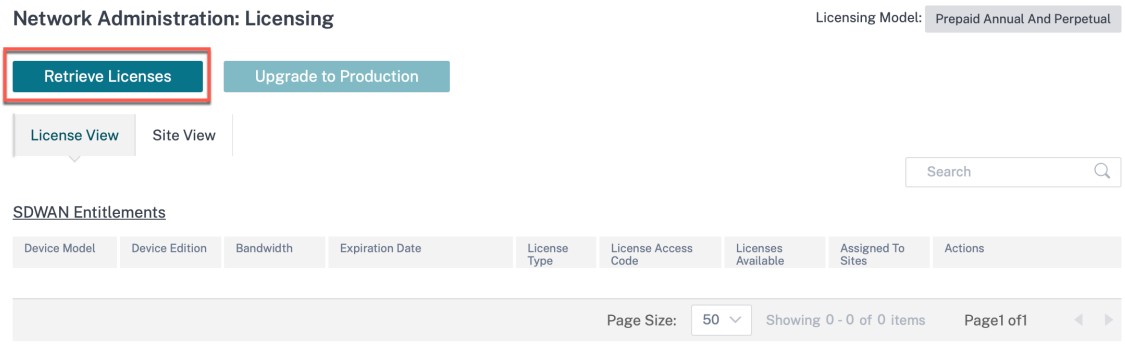
Citrix から電子メールで提供されたアクセスコードを使用して、ライセンス資格を取得できます。または、お客様は Citrix Cloud 内のライセンス管理ポータルでアクセスコードを確認することもできます 。お客様は、** ネットワーク内でプリペイドパーペチュアルまたはプリペイド年間サブスクリプションのいずれかの請求モデルを使用できます ** 。

前提条件：ライセンス管理ポータルにログインして、オンプレミス向け Citrix SD-WAN Orchestrator ライセンスが割り当てられていないことを確認します。ライセンスが割り当てられている場合は、Citrix SD-WAN Orchestrator for On-Premises 製品のライセンスアクセスコードを使用する前に、ライセンスを解放/割り当て解除します。

1. オンプレミス向け Citrix SD-WAN Orchestrator UI で、[管理] > [ライセンス] に移動し、[請求モデルの選択] をクリックします。請求モデルを選択し、[送信] をクリックします。

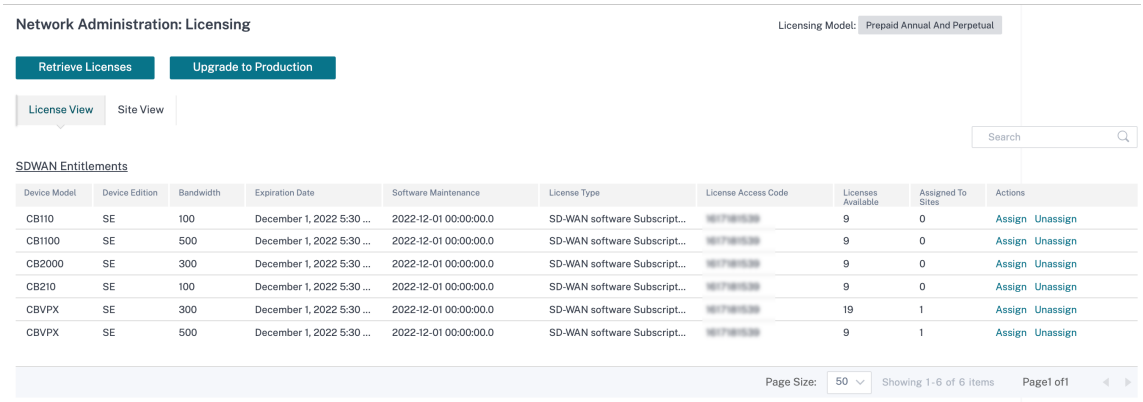


2. 「ライセンスを取得」をクリックします。

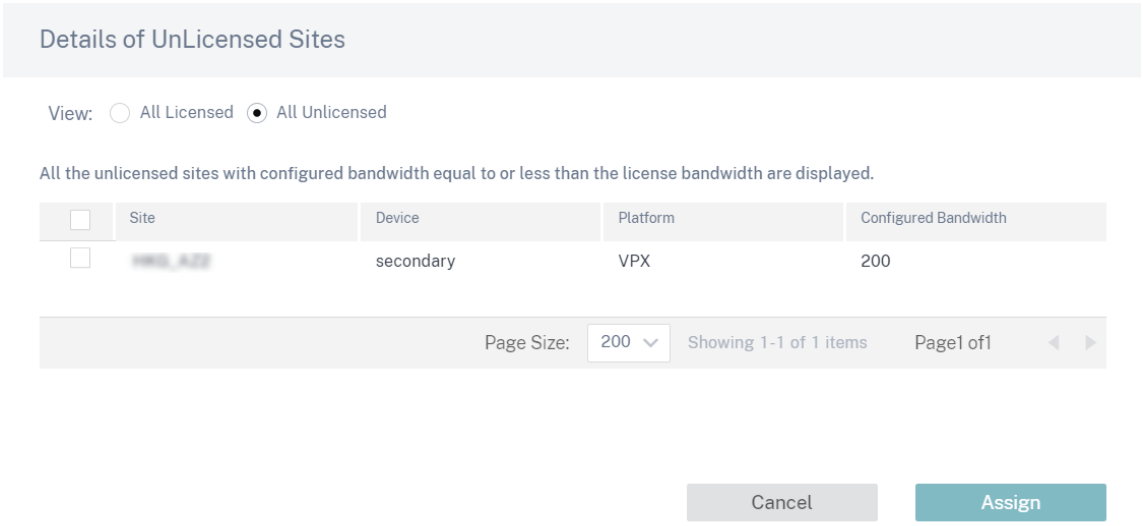


3. 「**+ License Access Code**」をクリックし、必要な数のアクセスコードを入力して資格を取得し、「**Submit**」をクリックします。

オンプレミス向け Citrix SD-WAN Orchestrator が資格を取得し、ライセンステーブルに入力します。

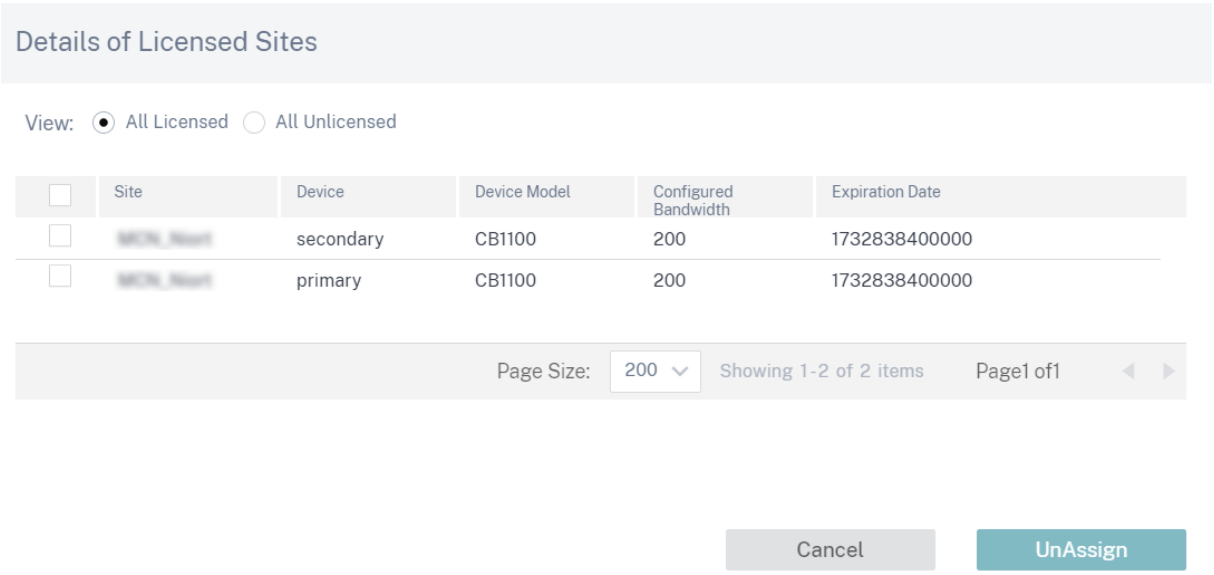


4. [割り当て/割り当て解除] をクリックし、[すべて非ライセンス] を選択します。設定された帯域幅がライセンス帯域幅以下であるライセンスされていないサイトがすべて表示されます。



5. サイトを選択して [割り当て] をクリックし、次に [実稼働環境にアップグレード] をクリックします。

すべてのライセンスビューに、ライセンスされたサイトのリストが表示されます。ライセンスの割り当てを解除し、プールに解放することができます。



サイトビューでは、設定された帯域幅とライセンス帯域幅に基づいてサイトが自動的にライセンスと照合されるため、ライセンスをすばやく割り当てることができます。

> 注
>
> アプライアンスにライセンスを割り当てるには、アプライアンスに検証済みのシリアル番号が必要です。

ライセンスの有効期限

ライセンスの有効期限が切れると、30 日間の猶予期間が付与されます。パートナー/お客様は、この期間中にライセンスを更新する必要があります。猶予期間が終了すると、お客様のネットワークデータパスは停止し、ライセンスが更新されるまで追加の変更を導入することはできません。

Citrix SD-WAN アプライアンスとの接続

October 26, 2022

オンプレミス用 Citrix SD-WAN Orchestrator でサイトを構成したら、オンプレミス用 Citrix SD-WAN Orchestrator があるサイト上の Citrix SD-WAN アプライアンス間の接続を確立します。接続は次のいずれかの方法で確立できます。

- 一方向認証：SD-WAN アプライアンスは、オンプレミス用の Citrix SD-WAN Orchestrator を認証します。一方向認証を有効にする場合は、オンプレミス用 Citrix SD-WAN Orchestrator 証明書をダウンロードし、SD-WAN アプライアンスにアップロードする必要があります。
- 双方向認証:SD-WAN は、交換された証明書を使用して相互に認証します。双方向認証を有効にする場合は、SD-WAN アプライアンス証明書をオンプレミス用 Citrix SD-WAN Orchestrator にアップロードし、SD-WAN アプライアンスの Citrix SD-WAN Orchestrator 証明書もアップロードする必要があります。
- 認証なし：オンプレミス向け Citrix SD-WAN Orchestrator と SD-WAN アプライアンス間の接続は、認証なしで確立されます。オンプレミス証明書には SD-WAN アプライアンスや Citrix SD-WAN Orchestrator を使用する必要はありません。MPLS などの安全なネットワークがある場合は、[認証なし] を使用できます。

> 注**:**
>
> 一方向認証または双方向認証のみを使用することをお勧めします。認証がない場合は、安全な DNS サーバーを選択する必要があります。

各サイトとの接続を手動で設定することも、自動ゼロタッチ展開を使用することもできます。

> 注
>
> Citrix SD-WAN 11.3.0 は、アプライアンスをオンプレミス向け Citrix SD-WAN Orchestrator に接続するために必要な最低限のソフトウェアバージョンです。

ゼロタッチ展開

ゼロタッチデプロイメントは、アプライアンスとオンプレミス向け Citrix SD-WAN Orchestrator 間の接続を自動構成するプロセスです。クラウド以外のゼロタッチデプロイメントまたはクラウド仲介ゼロタッチデプロイメント設定を使用して、接続を自動的に確立できます。

クラウド以外のゼロタッチ導入

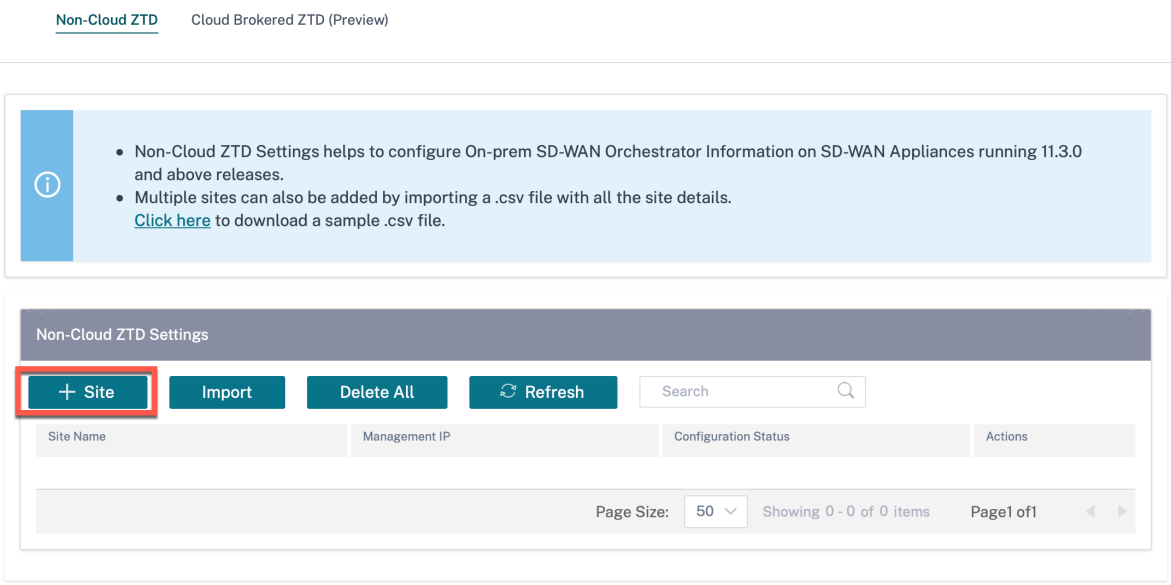
クラウド以外のゼロタッチ展開設定により、SD-WAN アプライアンス上のオンプレミス情報用に Citrix SD-WAN Orchestrator を構成できます。バックエンドで実行される NITRO API は、証明書のダウンロードとアップロードを処理します。オンプレミス用 Citrix SD-WAN Orchestrator から証明書をダウンロードし、SD-WAN アプライアンスにログインして、証明書をアップロードします。また、SD-WAN アプライアンス証明書をダウンロードして、オンプレミス用 Citrix SD-WAN Orchestrator にアップロードします。

> 注:
>
> クラウド以外のゼロタッチデプロイメントは、11.3.0 リリース以降で実行されている SD-WAN アプライアンスでサポートされています。

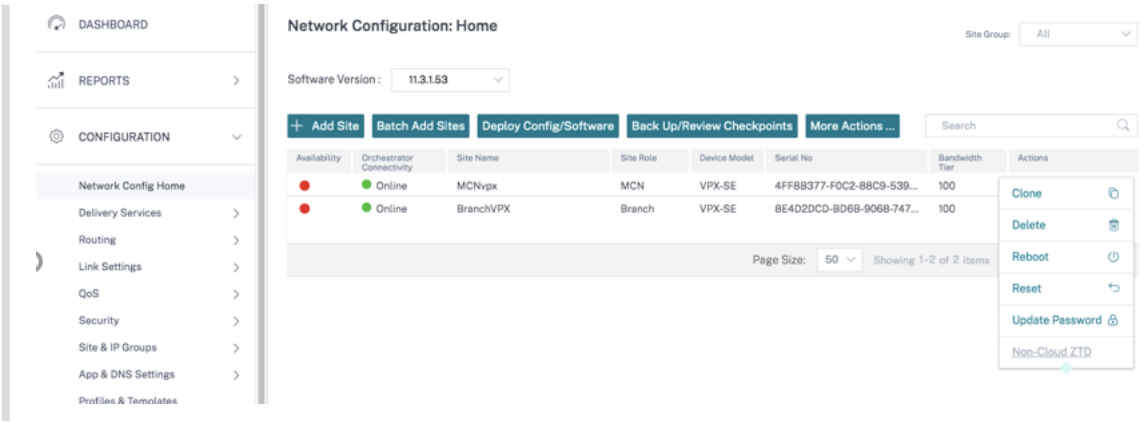
ゼロタッチ導入では、** 一方向認証と双方向認証のみがサポートされます。認証はサポートされていません ** 。管理 > ** 証明書認証ページで認証タイプを有効にすると ** 、双方向認証が確立されます。認証タイプが無効になっている場合、一方向の認証が確立されます。

サイトを手動で追加することも、CSV ファイルをインポートして複数のサイトを同時に追加することもできます。

クラウド以外のゼロタッチデプロイメント設定を行うには、[管理] > [**ZTD** 設定] > [非クラウド **ZTD**] に移動し、[**+** サイト] をクリックします。



> 注
>
> また、ネットワーク設定のホームページから、各サイトのクラウド以外のゼロタッチデプロイメント設定にアクセスすることもできます。サイトのアクションアイコンをクリックし、**noncloud ZTD** を選択します。



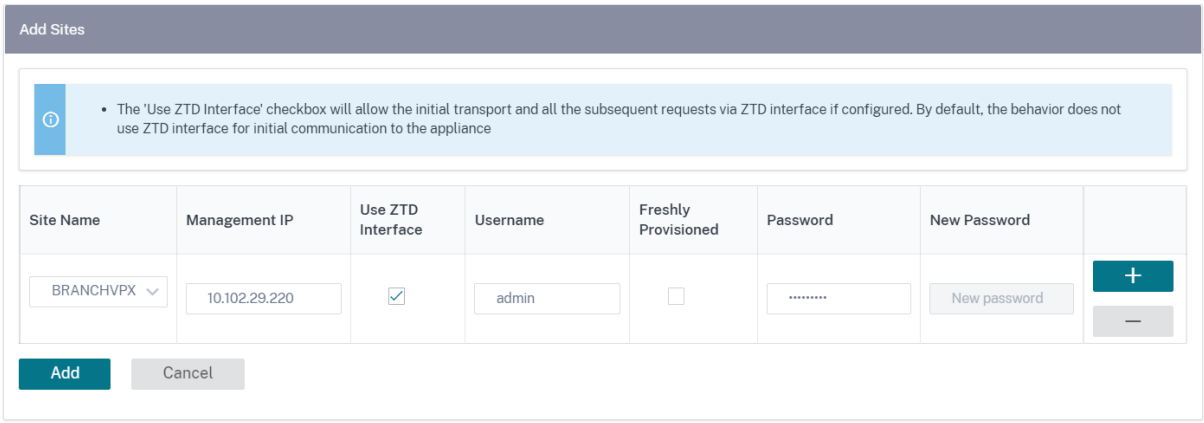
サイト名ドロップダウンリストからサイトを選択し、Citrix SD-WAN アプライアンスの管理 **IP** アドレスを入力します。

ZTD インターフェイスを使用するオプションを有効にすると、ZTD インターフェイスがオンプレミス用 SD-WAN Orchestrator で有効になっている場合、ZTD インターフェイスが非クラウド ZTD に確実に使用されます。

> 注
>
> - オンプレミス用 SD-WAN Orchestrator で ZTD インターフェイスが有効になっていない場合は、「ZTD インターフェイスを使用」オプションを無視してください。
> - SD-WAN アプライアンスが **ZTD** インターフェイスの **IP** アドレスにはアクセスできるが管理 **IP** アドレスにはアクセスできない場合は、「**ZTD** インターフェイスを使用」オプションを有効にします。
> - **ZTD** インターフェイスを有効にした後に [**ZTD** インターフェイスを使用] オプションを選択しなくても、SD-WAN アプライアンスとオンプレミス用 SD-WAN Orchestrator 間の通信に管理インターフェイスの IP アドレスが使用されるわけではありません。「**ZTD** インターフェイスを使用」オプションは、Non-Cloud ZTD を使用するアプライアンスの初期設定にのみ使用されます。

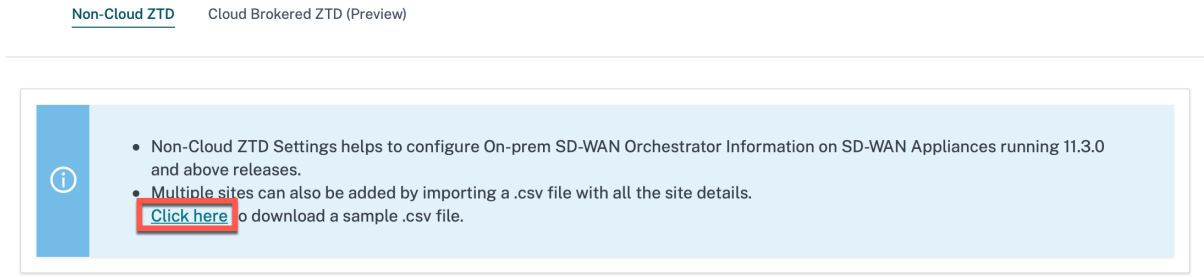
アプライアンスのユーザー名とパスワードを入力します。デフォルトのパスワードが変更されていない新しくプロビジョニングされたサイトを追加する場合は、「**Freshly** Provisioned」チェックボックスを選択します。新しいパスワードを入力します。デフォルトのパスワードは、このゼロタッチ導入プロセス中に新しいパスワードに変更されます。

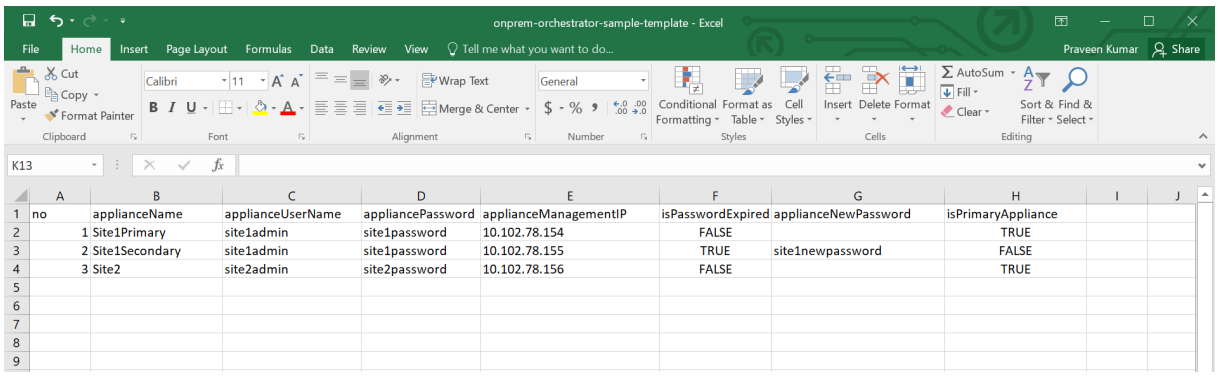
> 注
>
> 新しくプロビジョニングされたサイトでは、初回ログイン時にデフォルトパスワードを変更する必要があります。



サイトをさらに追加するには、[**+**] をクリックします。

CSV ファイルをインポートして、複数のサイトを同時に追加することもできます。ダウンロード可能なサンプルテンプレートが UI にあります。それをダウンロードして、サイトの詳細を提供してください。

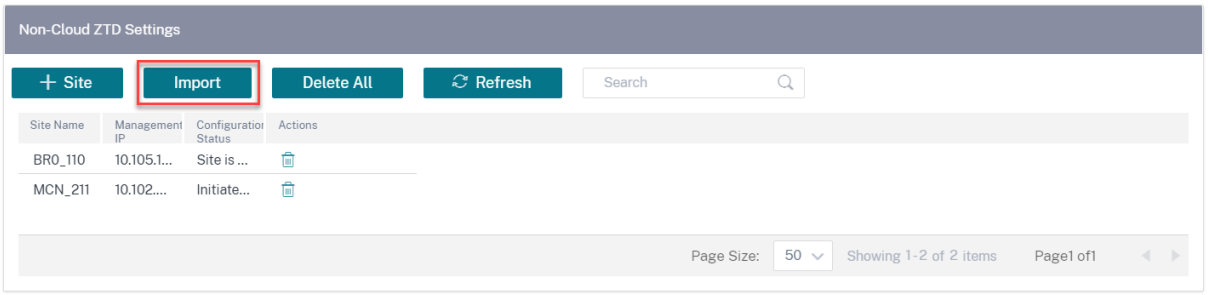


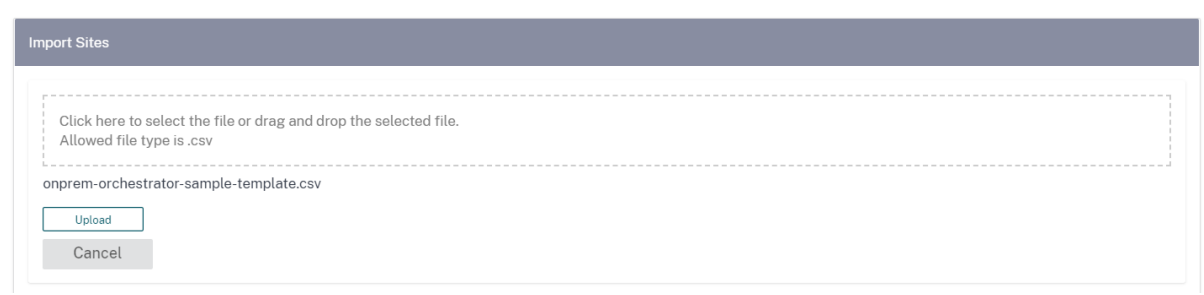


- アプライアンス名: サイト構成中に構成されたサイト名。詳細については、「サイト構成」を参照してください。
- アプライアンスユーザー名: サイトアプライアンスで設定されているユーザー名。
- アプライアンスパスワード: サイトアプライアンスに対応するパスワード。
- パスワードの有効期限が切れているかどうか: アプライアンスが新しくプロビジョニングされたかどうかを判断します。値が **True** の場合は、アプライアンスの新しいパスワードを入力します。
- アプライアンスの新しいパスワード: 新しくプロビジョニングされたアプライアンスのパスワード。パスワードの有効期限が切れているかどうかの値が **True** の場合は、アプライアンスの新しいパスワードを入力します。
- プライマリアプライアンスですか: 高可用性 (HA) が設定されている場合、アクティブアプライアンスの値は True、スタンバイアプライアンスの値は False でなければなりません。HA が設定されていない場合、値は

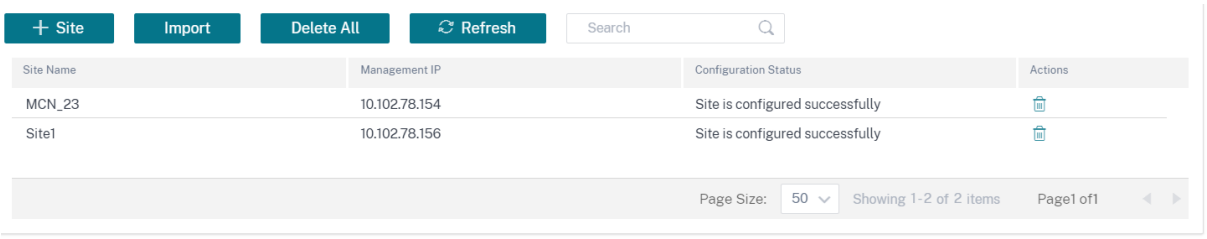
True でなければなりません。

[インポート] をクリックし、CSV ファイルを選択して [アップロード] をクリックします。





サイトの構成ステータスが表示されます。サイトを個別に削除するか、サイトがゼロタッチ展開に必要ない場合は [すべて削除] を選択できます。



クラウド仲介によるゼロタッチ導入

クラウド仲介型ゼロタッチ展開では、オンプレミス向け Citrix SD-WAN Orchestrator と Citrix SD-WAN アプライアンスの間のブローカーとして Citrix SD-WAN Orchestrator サービスを使用します。オンプレミス向け Citrix SD-WAN Orchestrator は、クラウドゼロタッチ展開構成パッケージを Citrix SD-WAN Orchestrator サービスに送信します。クラウドゼロタッチデプロイメント設定パッケージは、次の情報で構成されています。

- オンプレミスの ID 情報
- 認証の種類
- オンプレミス証明書
- アプライアンスの詳細 (シリアル番号のリスト)

Citrix SD-WAN Orchestrator サービスは、Citrix SD-WAN Orchestrator から受信した情報をオンプレミス用に保存します。アプライアンスがシリアル番号を使用して Citrix SD-WAN Orchestrator サービスに接続すると、

Citrix SD-WAN Orchestrator サービスの取得したインテリジェンスによって、アプライアンスはオンプレミス用 Citrix SD-WAN Orchestrator によって管理される必要があると判断されます。Citrix SD-WAN Orchestrator サービスは、オンプレミスの詳細について Citrix SD-WAN Orchestrator をアプライアンスに渡します。Citrix SD-WAN アプライアンスは証明書を Orchestrator サービスに送信します。Citrix SD-WAN Orchestrator サービスは、アプライアンス証明書を受信して保存します。

オンプレミス用 Citrix SD-WAN Orchestrator は、Citrix SD-WAN Orchestrator サービスからアプライアンス証明書を定期的に取得します。オンプレミス用 Citrix SD-WAN Orchestrator とアプライアンスとの間に安全な接続が確立されると、オンプレミス用 Citrix SD-WAN Orchestrator は構成と関連ファイルをアプライアンスにプッシュします。

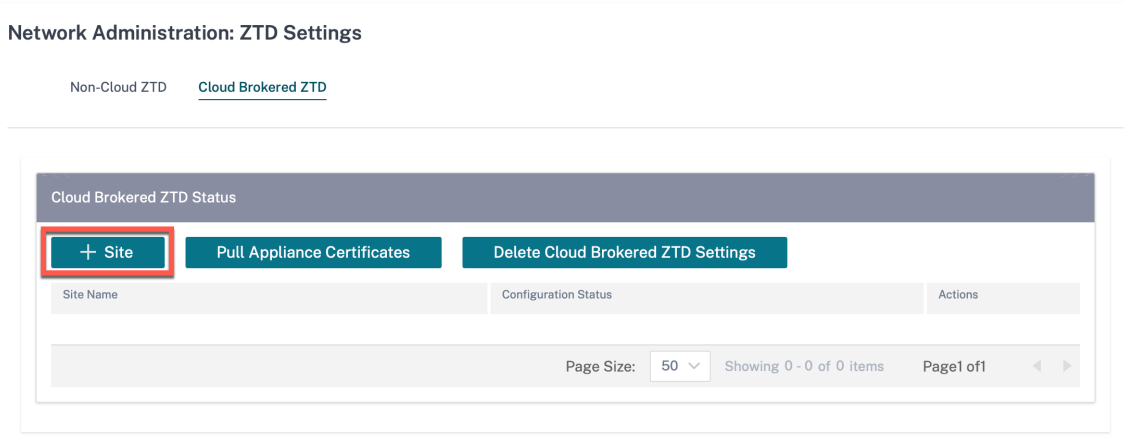
クラウド仲介型のゼロタッチ導入設定は、顧客管理型セットアップのお客様のみが使用できます。プロバイダー管理セットアップは、クラウドブローカーのゼロタッチデプロイ設定をサポートしていません。

前提条件

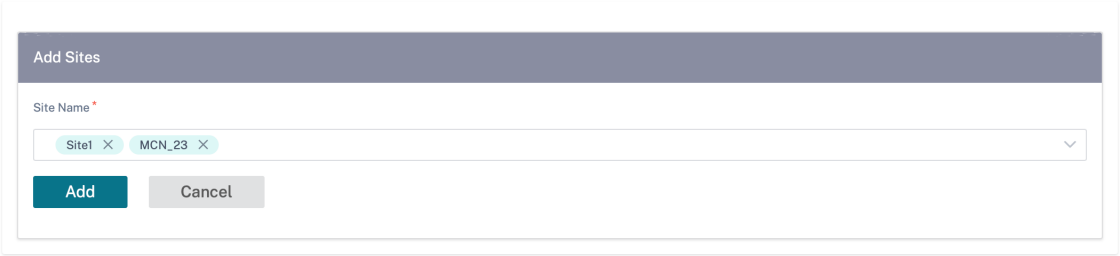
- Citrix SD-WAN Orchestrator サービスとの接続を確立するには、アプライアンスが次のドメイン名にアクセスする必要があります。
  - sdwanzt.citrixnetworkapi.net
  - download.citrixnetworkapi.net
  - trust.citrixnetworkapi.net
  - sdwan-home.citrixnetworkapi.net
- オンプレミス用 Citrix SD-WAN Orchestrator が常に Citrix SD-WAN Orchestrator サービスに接続して SD-WAN アプライアンスをオンボーディングするようにしてください。
- 最初のオンボーディングプロセス中、および SD-WAN アプライアンスで工場出荷時設定へのリセットが行われた場合は、Citrix SD-WAN アプライアンスが SD-WAN Orchestrator サービスに接続できることを確認します。

クラウドブローカーのゼロタッチデプロイメント設定を構成するには:

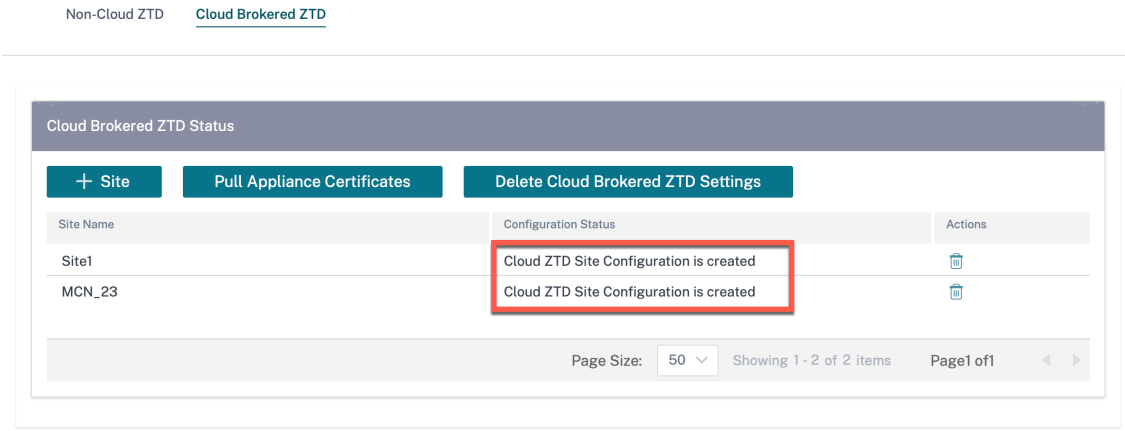
1. オンプレミス向け Citrix SD-WAN Orchestrator では、ガイド付きワークフローを使用してサイトを作成および定義します。詳しくは、「サイト構成」を参照してください。
2. デプロイメントトラッカーを使用して設定を検証し、コンパイルします。詳細については、「ネットワーク設定」トピックの「Deployment Tracker」セクションを参照してください。
3. [管理] **> [ZTD** 設定] **> [**クラウドブローカー **ZTD**] に移動し、[**+** サイト] をクリックします。



4. ドロップダウンリストからサイト名を選択し、[追加] をクリックします。サイトは構成に基づいて一覧表示されます。1 つのサイトまたは複数のサイトを選択できます。



5. クラウドゼロタッチ展開構成が作成され、Citrix SD-WAN Orchestrator サービスに送信されます。



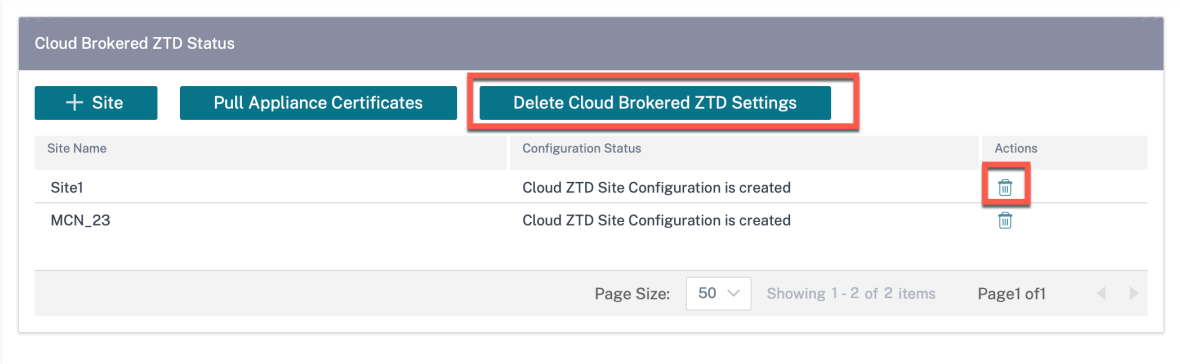
6. データセンターとブランチサイトの SD-WAN アプライアンスをケーブルで接続し、電源を入れます。
7. アプライアンスは、シリアル番号を使用して Citrix SD-WAN Orchestrator サービスに連絡します。
8. Citrix SD-WAN Orchestrator サービスは、オンプレミス用 Citrix SD-WAN Orchestrator とアプライアンスの間の仲介役として機能します。これにより、証明書の交換が可能になり、Citrix SD-WAN アプライアンスはオンプレミス用 Citrix SD-WAN Orchestrator との安全な接続を確立します。ゼロタッチ展開が成功す

ると、構成されたサイトがオンラインになり、[構成] **>** [ネットワーク構成ホーム] の [**Orchestrator** 接続] 列に表示されます。

9. ** 構成をアクティブ化してステージングし ** 、構成とソフトウェアをアプライアンスにプッシュします。
10. 構成/ソフトウェアが適用されると、仮想パスが確立され、[構成] **> [**ネットワーク構成ホーム] の [可用性] 列が適切な仮想パスのステータスに更新されます。

> 注:
>
> オンプレミス用 Citrix SD-WAN Orchestrator がアプライアンス証明書を取得してアプライアンスを完全にオンボーディングするまでに約 30 分かかります。アプライアンス証明書をすぐに（30 分待たずに）プルするには、「アプライアンス証明書をプル配信」をクリックします。

必要に応じて、「**Cloud Brokered ZTD** 設定の削除」をクリックすることもできます。すべてのサイトに関連する情報を削除します。特定のサイト情報を削除する必要がある場合は、そのサイトに対応する削除アイコンをクリックします。



制限事項

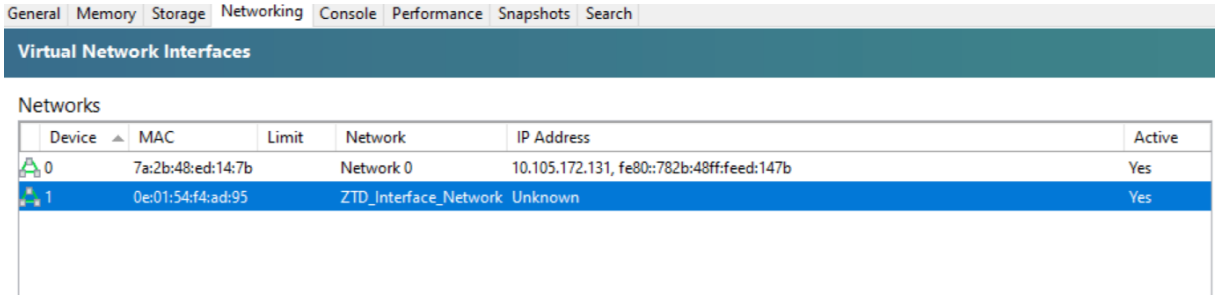
- SD-WAN アプライアンスは、クラウドログイン認証情報を共有するオンプレミス用 Citrix SD-WAN Orchestrator の複数のインスタンスに接続することはできません。たとえば、SD-WAN アプライアンスは、初めて構成されたオンプレミス用 Citrix SD-WAN Orchestrator に接続されたままになります。次に構成されるオンプレミス用 Citrix SD-WAN Orchestrator の詳細は、SD-WAN アプライアンスにプッシュされません。
- LTE 経由で接続された SD-WAN アプライアンスは、プライベートネットワークでホストされているオンプレミス向け Citrix SD-WAN Orchestrator との接続を確立できません。

ZTD インターフェイス設定

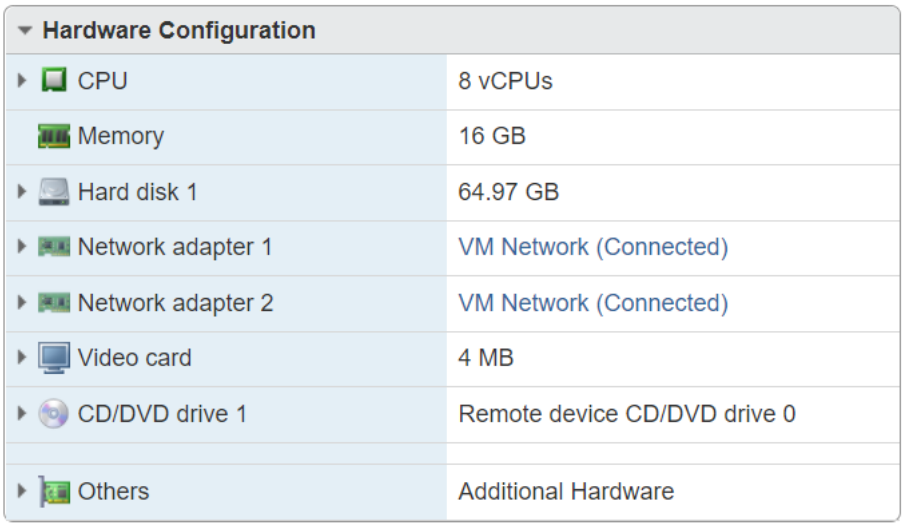
オンプレミス用 SD-WAN Orchestrator でゼロタッチデプロイ (ZTD) インターフェイスを有効にできます。双方向認証によって保護された ZTD インターフェイスは、SD-WAN アプライアンスとオンプレミスの SD-WAN Orchestrator に安全な通信インターフェイスを提供します。

ZTD インターフェイスを有効にすると、非クラウド ZTD およびクラウドブローカー ZTD を介してデプロイされた新しい D-WAN アプライアンスは、ZTD インターフェイス IP アドレスを使用してオンプレミス用 SD-WAN Orchestrator と通信します。

前提条件として、オンプレミス仮想マシン用 SD-WAN Orchestrator に、管理インターフェイスとは別に追加のインターフェイスがあることを確認します。



> 注
>
> VMware ESXi 仮想マシンの場合は、ZTD 用のインターフェイスを追加した後に仮想マシンを再起動してください。

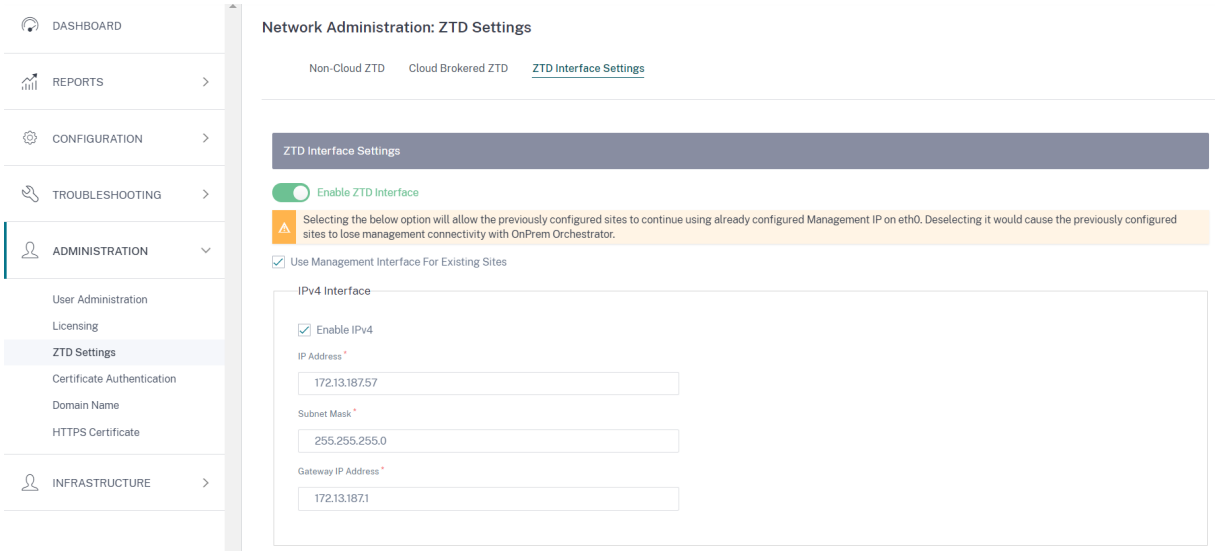


ZTD インターフェイスの有効化

オンプレミス GUI 用 SD-WAN Orchestrator で、[管理] > [**ZTD** 設定] に移動し、[**ZTD** インターフェイスを有効にする] を選択して ZTD インターフェイスを有効にします。ZTD インターフェイスの IP アドレス、サブネットマスク、およびゲートウェイ IP アドレスを指定します。

非クラウド ZTD または Cloud Brokered-ZTD を介して既にデプロイされている SD-WAN アプライアンスが、管理インターフェイス **IP** アドレスを使用してオンプレミス用 **SD-WAN Orchestrator** に引き続き接続できるようにするには、**[**既存のサイトに管理インターフェイスを使用] を選択します。

> 警告
>
> [既存のサイトに管理インターフェイスを使用] が選択されていない場合、非クラウド ZTD または Cloud Brokered-ZTD を介して既にデプロイされている SD-WAN アプライアンスは、オンプレミス用 SD-WAN Orchestrator への接続を失います。



ZTD インターフェイスを使用した非クラウド **ZTD** の設定　「既存のサイトに管理インターフェイスを使用」オプションが選択されている場合、Non-Cloud ZTD を使用してすでにデプロイされているアプライアンスは、引き続き管理インターフェイスの IP アドレスを使用してオンプレミス用 SD-WAN Orchestrator に接続します。アプライアンスで非クラウド ZTD を起動し、ZTD インターフェイス IP アドレスを使用してオンプレミス用 SD-WAN Orchestrator との接続を確立します。

> 注
>
> すべての SD-WAN アプライアンスが ZTD インターフェイス IP アドレスを介してオンプレミス用 SD-WAN Orchestrator との接続を確立したら、[既存のサイトの管理インターフェイスを使用] オプションを無効にできます。

[既存のサイトに管理インターフェイスを使用] オプションが選択されていない場合、非クラウド ZTD を使用して既にデプロイされている SD-WAN アプライアンスは、オンプレミス用 SD-WAN Orchestrator への接続を失います。SD-WAN アプライアンスで非クラウド ZTD を起動し、ZTD インターフェイス IP アドレスを使用してオンプレミス用 SD-WAN Orchestrator との接続を復元します。

ZTD インターフェイスを使用したクラウドブローカー **ZTD** の設定　「既存のサイトに管理インターフェイスを使用」オプションを選択すると、Cloud Brokered ZTD を使用してすでにデプロイされているアプライアンスは、引き続き管理インターフェイスの IP アドレスを使用してオンプレミス用 SD-WAN Orchestrator に接続します。ZTD

インターフェイスの IP アドレスを使用してオンプレミス用 SD-WAN Orchestrator との接続を確立するには、次のいずれかを実行します。

- SD-WAN アプライアンスで、オンプレミス用 SD-WAN Orchestrator の IP アドレスと証明書を更新します。

  > 注
  >
  > 証明書が手動で再生成された場合にのみ証明書を更新してください。アプライアンスにすでに証明書がある場合は、証明書を更新する必要はありません。

- 工場出荷時の状態にリセットし、アプライアンスで Cloud Brokered-ZTD を起動し、ZTD インターフェイス IP アドレスを使用してオンプレミス用 SD-WAN Orchestrator との接続を確立します。

> 注
>
> すべての SD-WAN アプライアンスが ZTD インターフェイス **IP** アドレスを介してオンプレミス用 **SD-WAN Orchestrator** との接続を確立したら、**[**既存のサイトの管理インターフェイスを使用] オプションを無効にできます。

[既存のサイトに管理インターフェイスを使用] オプションが選択されていない場合、クラウドブローカー ZTD を使用して既にデプロイされている SD-WAN アプライアンスは、オンプレミス用 SD-WAN Orchestrator への接続を失います。ZTD インターフェイスの IP アドレスを使用してオンプレミス用 SD-WAN Orchestrator との接続を復元するには、次のいずれかを実行します。

- SD-WAN アプライアンスで、オンプレミス用 SD-WAN Orchestrator の IP アドレスと証明書を更新します。
- 工場出荷時の状態にリセットし、アプライアンスで Cloud Brokered-ZTD を起動し、ZTD インターフェイス IP アドレスを使用してオンプレミス用 SD-WAN Orchestrator との接続を確立します。

手動接続設定

接続を手動で設定するときは、Citrix SD-WAN Orchestrator for On-Premises 証明書をダウンロードして、ネットワーク内の各アプライアンスにアップロードする必要があります。証明書をアップロードするには、各アプライアンスに手動でログインする必要があります。

接続を手動で設定するには-

1. [管理**] > [**証明書認証] に移動し、[認証タイプ**]** を有効にします。

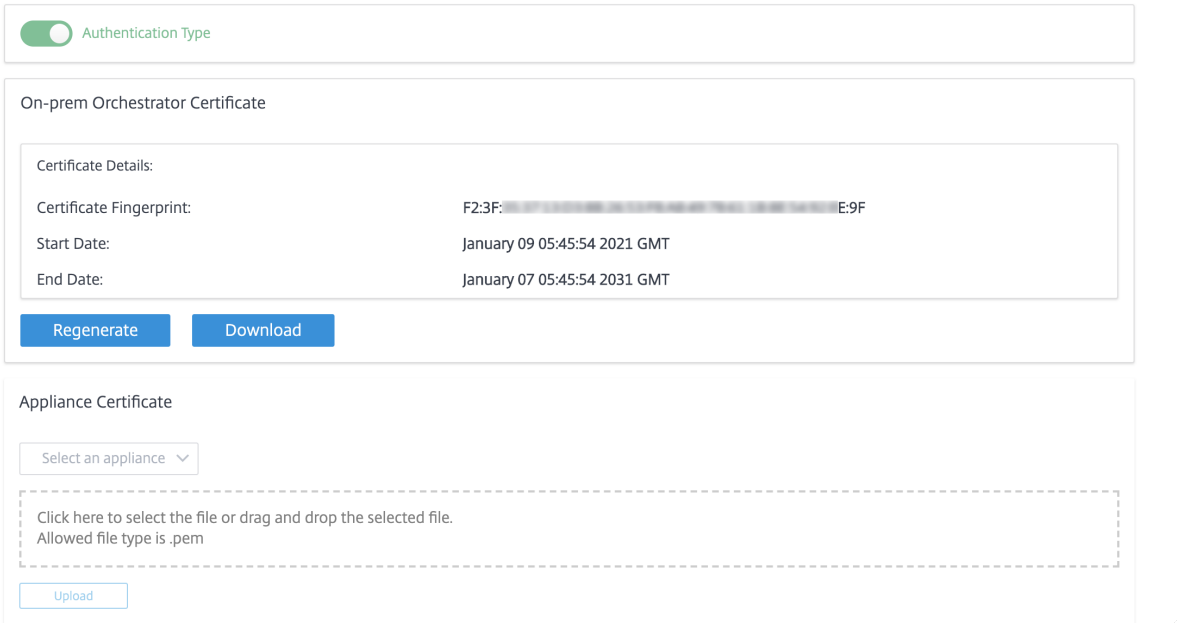
   認証タイプが有効になっている場合、SD-WAN アプライアンスは双方向認証を介してのみオンプレミス用の Citrix SD-WAN Orchestrator に接続できます。認証タイプが無効になっている場合、SD-WAN アプライアンスは、認証なし、一方向認証、または双方向認証のいずれかを使用して、オンプレミス用 Citrix SD-WAN Orchestrator に接続できます。

> 注:
>
> プロバイダーが管理するセットアップでは、認証タイプを有効にして Citrix SD-WAN Orchestrator for On-Premises 証明書を再生成できるのはプロバイダーのみです。

2. 「オンプレミス用 Citrix SD-WAN Orchestrator ** 証明書を再生成してダウンロードする ** 」をクリックします。
3. アプライアンス証明書セクションからアプライアンスを選択し、SD-WAN アプライアンスからダウンロードした対応する証明書をアップロードします。アプライアンス証明書のダウンロードについて詳しくは、「SD-WAN アプライアンス上の Citrix SD-WAN Orchestrator オンプレミス構成」を参照してください。

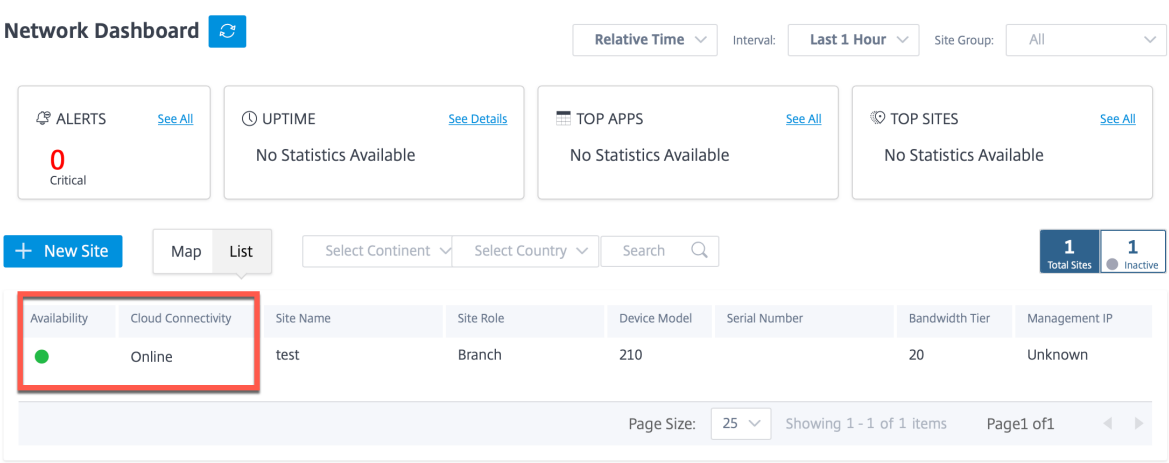
   > 注
   >
   > - .pem ファイルタイプのみがサポートされています。
   > - アプライアンス証明書をアップロードできるのは顧客管理者だけです。

4. SD-WAN アプライアンス UI にログオンし、[構成] **>** [仮想 **WAN] >** [オンプレミス **SD-WAN Orchestrator**] に移動します。オンプレミス用 Citrix SD-WAN Orchestrator からダウンロードした証明書をアップロードします。詳細については、「SD-WAN アプライアンスでのオンプレミス構成用 Citrix SD-WAN Orchestrator」を参照してください。



接続を確認

アプライアンスの接続ステータスを確認するには、[構成] > [ネットワーク構成] **>** [ホーム] に移動し、サイトに対応する [クラウド接続] 列を確認します。

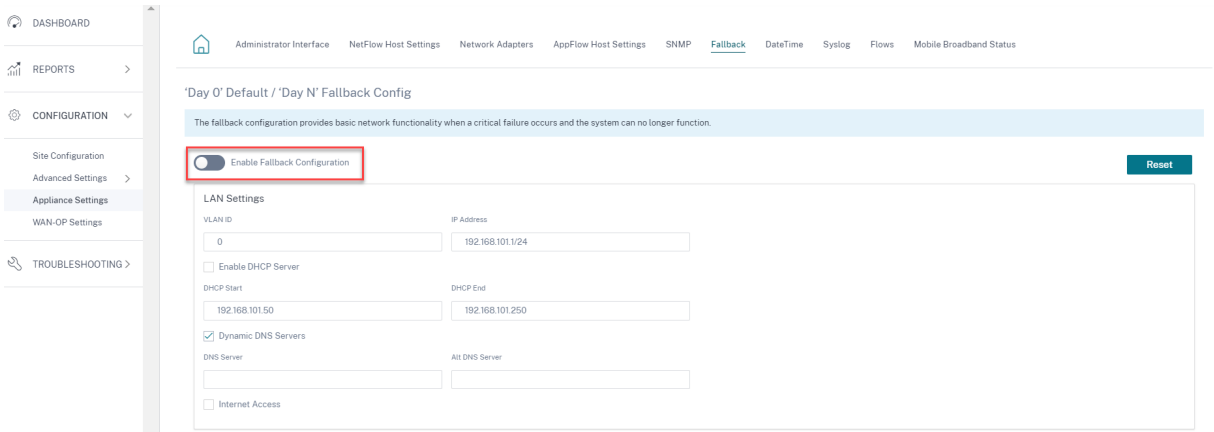


> 注:
>
> [インフラストラクチャ] > [**Orchestrator** 管理] > [ソフトウェアイメージ] > [アプライアンス] で、必要なソフトウェアを公開してアプライアンスをアップグレードできます。詳しくは、「ソフトウェアの公開」を参照してください。

フォールバック構成

フォールバック構成により、Citrix SD-WAN アプライアンスとの間で確立した Citrix SD-WAN Orchestrator for On-Premises 接続が、アプライアンスの帯域内管理 IP を介して確実に保持されます。

Citrix SD-WAN Orchestrator for On-Premises のフォールバック構成をサイトレベルで有効にするには、[構成] > [アプライアンス設定] > [フォールバック] に移動し、[フォールバック構成を有効にする] をクリックします。

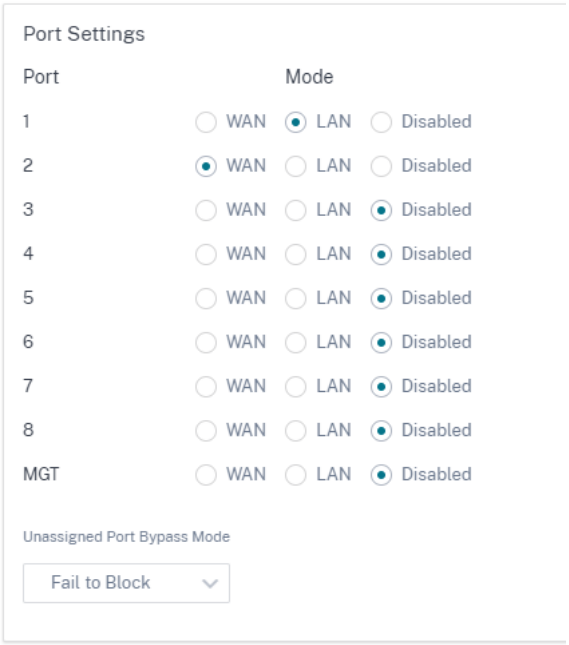


フォールバック構成の詳細については、「帯域内管理」を参照してください。

> 注:
>
> Citrix SD-WAN 110 SE 以外のアプライアンスを使用している場合は、デフォルトのフォールバック構成を有効にするには、SD-WAN 11.2 以降のバージョンを実行していることを確認してください。

次の表に、異なるプラットフォームでのフォールバック構成用に事前に指定された WAN ポートおよび LAN ポートの詳細を示します。

プラットフォーム	WAN ポート	LAN ポート
110	1/2	1/1
110-LTE	1/2、LTE-1	1/1
210	1/4, 1/5	1/3
210-LTE	1/4, 1/5, LTE-1	1/3
VPX	2	1
410	1/4, 1/5, 1/6	1/3 (FTB)
1100	1/4, 1/5, 1/6	1/3 (FTB)



プロバイダーレベルの構成

November 30, 2020

プロファイル

プロファイルは、** ライブ構成テンプレートです。通常のテンプレートは、新しいエンティティの作成を支援するためのものです。ただし、テンプレートが作成されると、それ以降のテンプレートの変更は、ベーステンプレートを使用して作成された新しいエンティティには適用されません。プロファイルはライブの中央マスターエンティティとして機能し、すべての子エンティティは作成中だけでなく、プロファイルの存続期間中も継承します。プロファイルに関連付けられているすべての子エンティティは、プロファイルに加えられた変更を自動的に継承します。

たとえば、管理者は、** 小規模小売店と呼ばれるサイト構成プロファイルを作成し、会社が所有するすべての小規模小売店に適用します。これで、小規模小売店舗のプロファイルに対して行った変更は、このプロファイルを継承するすべての店舗に自動的に適用されます。すべてのエンティティで共通するものとそうでないものに基づいて、プロファイル設定の特定のパラメーターは設定しないままにすることができます。このようなパラメータはカスタマイズ可能で、同じプロファイルを継承するエンティティ間で異なる場合があります。

サービスプロバイダ用のプロファイルテンプレート

パートナーはプロファイルテンプレートを作成できます。プロファイルテンプレートは、顧客がプロファイルの作成時に使用できます。

たとえば、プロバイダーは 4 つのサイトプロファイルテンプレート (小支店、中支店、大支店、データセンターなど) を作成できます。これらのテンプレートは、パートナーに関連付けられている顧客アカウントで自動的に利用できるようになります。お客様は、プロファイルの作成時にこれらのテンプレートを使用できます。

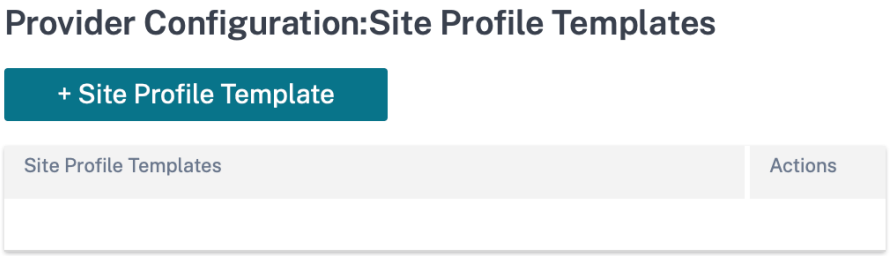
たとえば、顧客が小規模なブランチ構成用のプロファイルを作成するとします。お客様は、パートナーが共有するテンプレートの 1 つを選択できます。テンプレートは、プロファイル設定の一部としてドロップダウンリストから利用できます。お客様は、プロファイルを保存する前に、ネットワークのニーズに合わせてカスタマイズできます。縦断テンプレートはライブエンティティではありません。これは、顧客レベルでのプロファイルの作成を支援するだけです。プロファイルは顧客レベルでのみ作成でき、マスター構成レコードとして機能するライブエンティティであることを意図しています。

プロバイダーは、必要に応じて一部またはすべての顧客と共有できる設定プロファイルを作成できます。サイトプロファイルと WAN プロファイルは、現在サポートされています。

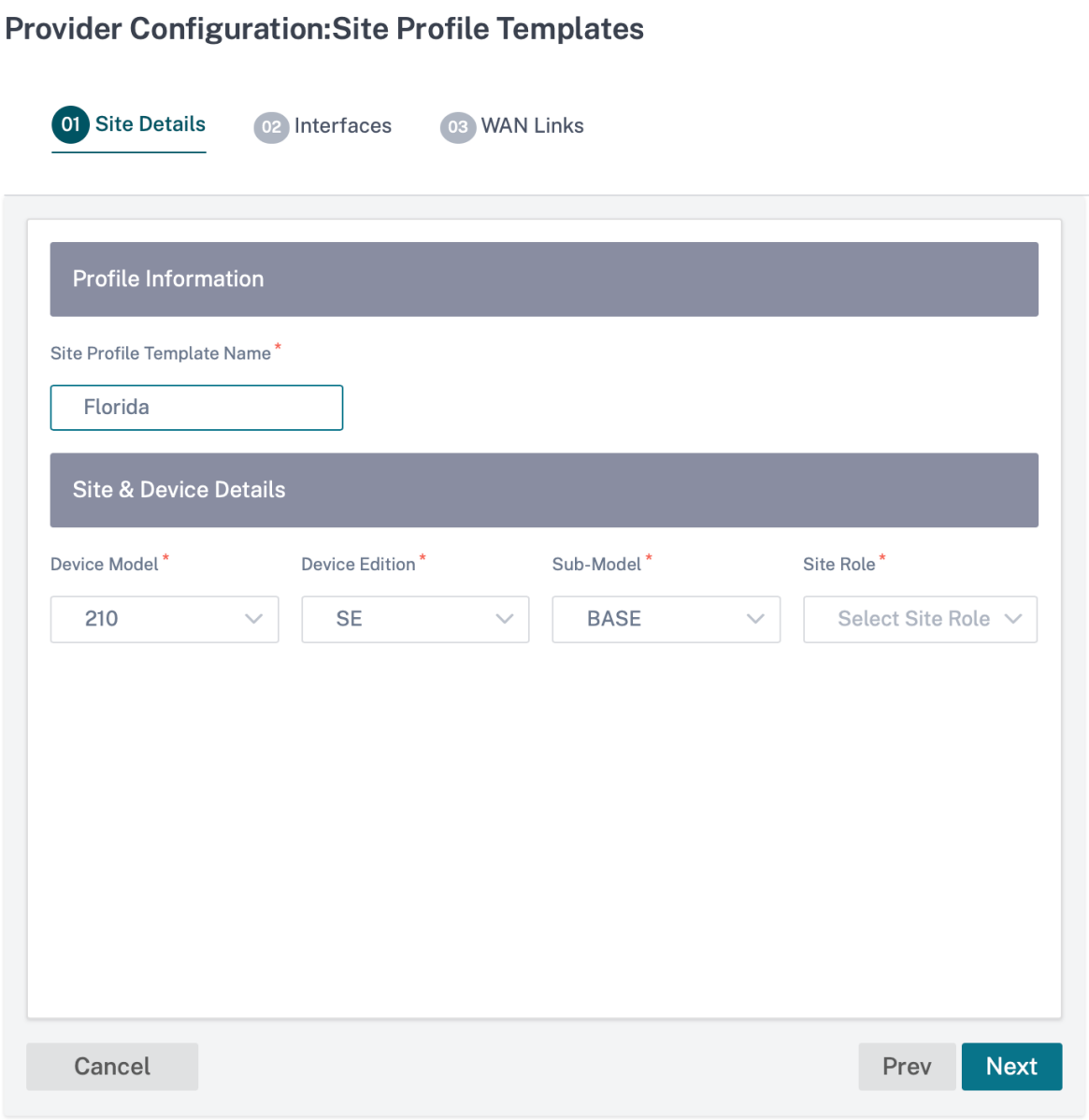
サイトプロファイルテンプレート

サイトプロファイルテンプレートは、顧客レベルでサイトプロファイルの作成を可能にするために、サービスプロバイダーによって作成されるサイト構成テンプレートです。

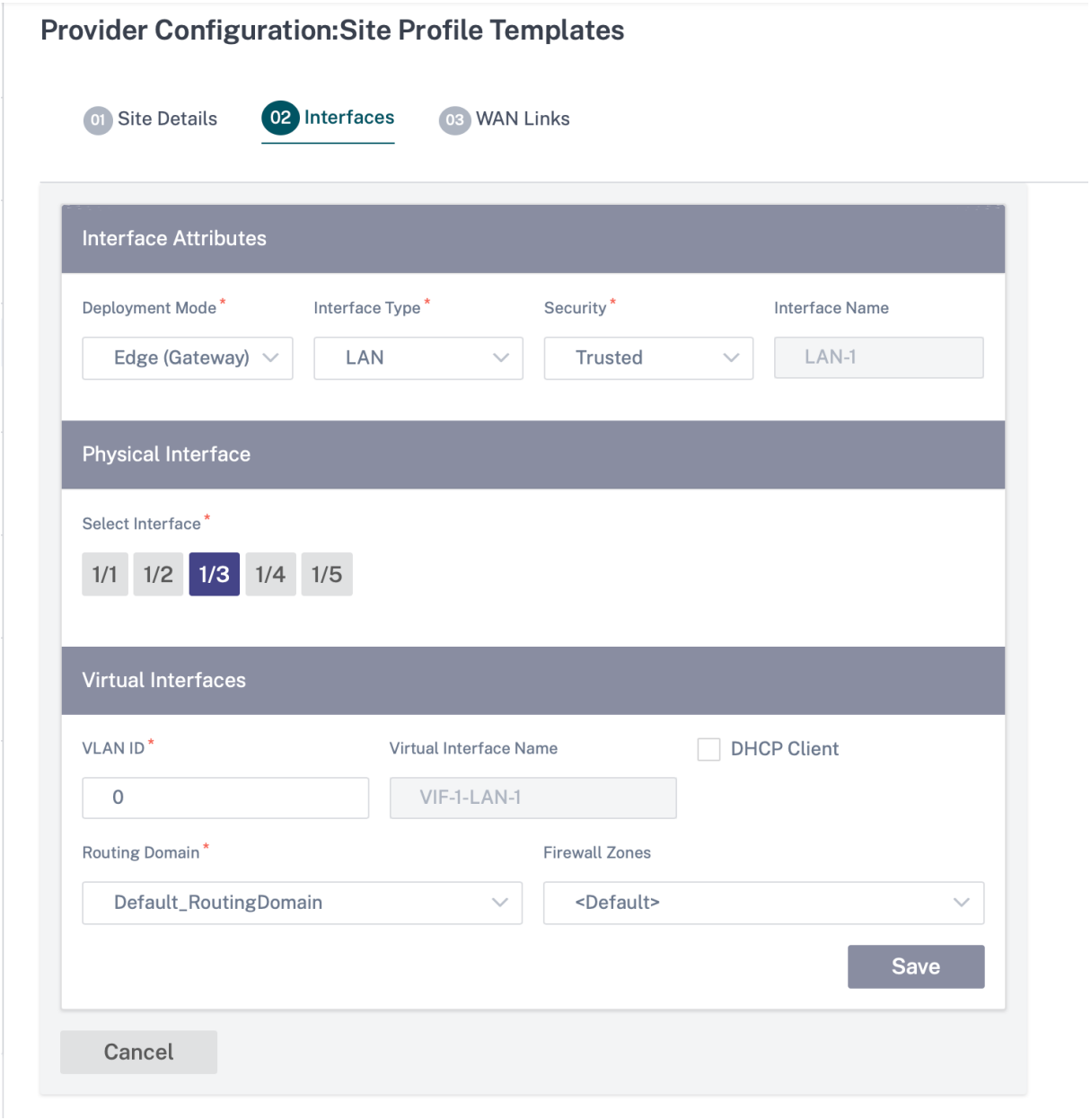
プロファイルテンプレートを作成するには、[構成]> [サイトプロファイルテンプレート] に移動し、[+ サイトプロファイルテンプレート] をクリックします。



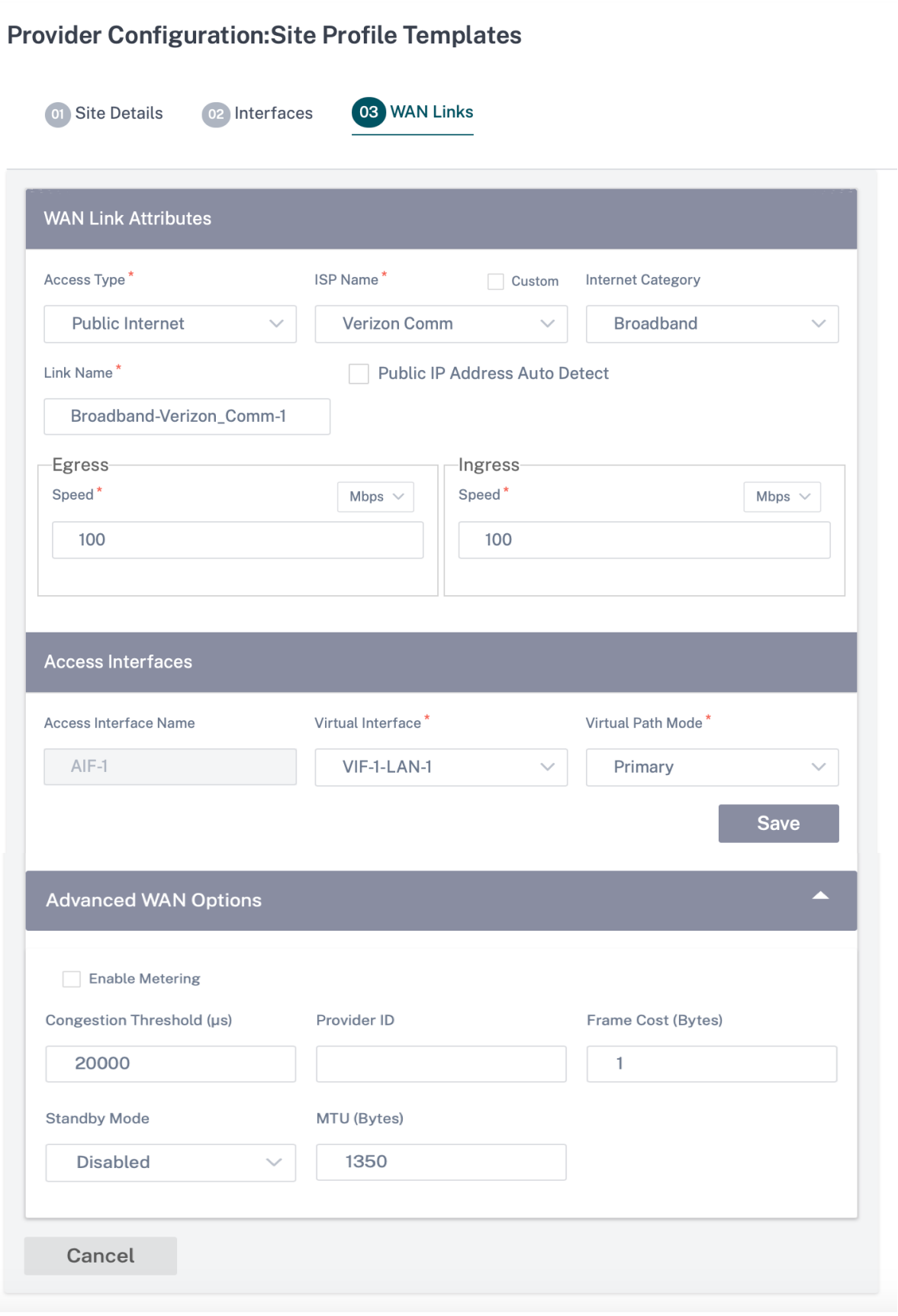
サイトプロファイルテンプレートを作成するには、サイトの詳細、インターフェイス、および **WAN** リンクを構成する必要があります。サイトの構成の詳細については、「サイトの詳細」を参照してください。



[**+ Interface**] オプションをクリックして、サイトのインターフェイスを割り当てます。インターフェイスを追加するには、[インターフェイス属性]、[物理インターフェイス]、および［仮想インターフェイス］フィールドに入力する必要があります。インターフェイスの設定の詳細については、「インターフェイス」を参照してください。



WAN リンク属性、アクセスインターフェイス、****** およびサービスの詳細オプションを提供します ******。WAN リンクの設定の詳細については、「WAN リンク」を参照してください。



WAN リンクテンプレート

WAN プロファイルテンプレートは、サービスプロバイダーによって作成される WANリンク設定テンプレートで、顧客レベルで WANリンクプロファイルの作成を可能にします。

WAN リンクテンプレートを作成するには、[**+ WAN** リンクテンプレート] をクリックします。プロファイル名、アクセスタイプ、インターネットカテゴリ、**LAN** 対 **WAN** レート（**Mbps**）などの WAN リンク情報を入力して、WAN プロファイルを作成します。WAN リンクの設定の詳細については、「WAN リンク」を参照してください。

ネットワークホーム

October 26, 2022

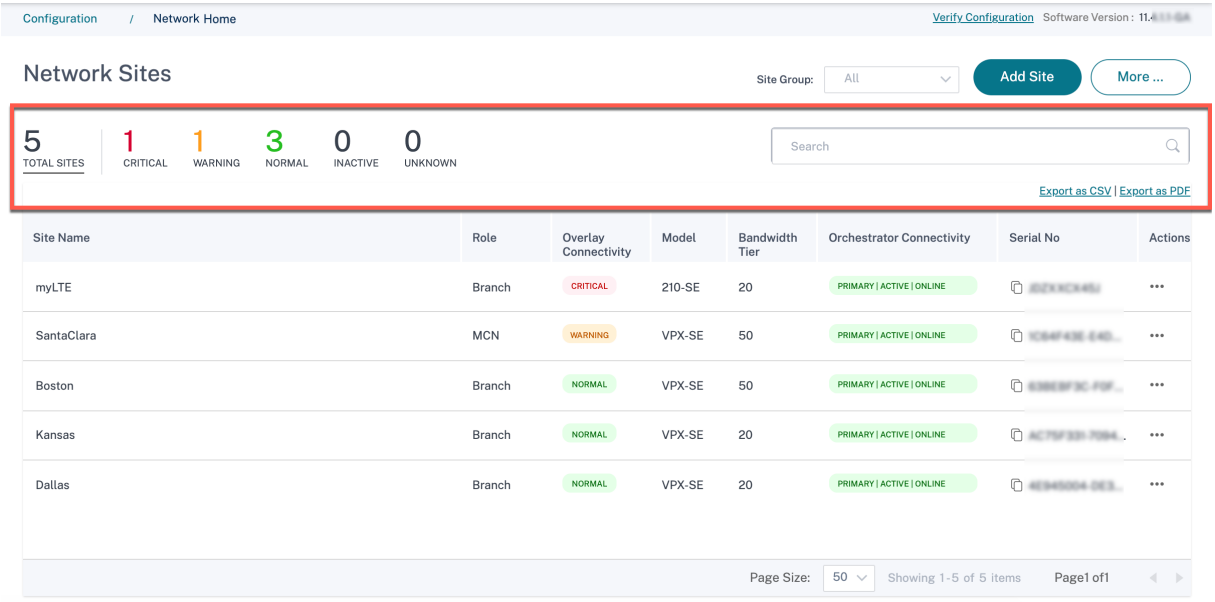
ネットワークホームページは、ネットワーク構成のアンカーとして機能し、エンタープライズネットワークレベルの設定機能を提供し、企業の SD-WAN ネットワークを設定するための出発点として機能します。

ネットワークホームページには、ネットワーク内のサイトの総数が表示され、接続状態に基づいてサイトが分類されます。番号付きのリンクを選択すると、次のステータスカテゴリに基づいてサイトが表示されます。

- 重要—関連する仮想パスがすべてダウンしているサイト。
- 警告 -少なくとも 1 つの仮想パスがダウンしているサイト。
- 標準 -サイトのすべての仮想パスと関連するメンバーパスが稼働しています。
- 非アクティブ -サイトは未展開で非アクティブな状態です。
- 不明 -サイトのステータスは不明です。

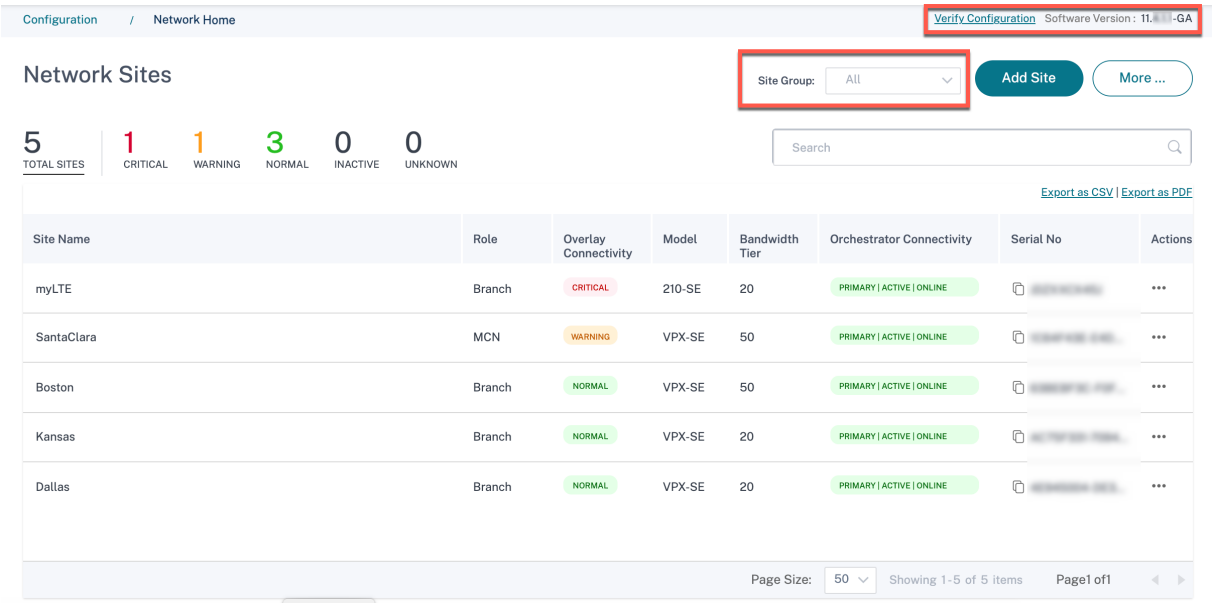
ステータスをクリックすると、ステータスに基づいてサイトがフィルタリングされ、詳細が表示されます。検索バーを使用して、サイト名、役割、オーバーレイ接続、モデル、帯域幅層、およびシリアル番号パラメータに基づいてサイトの詳細を表示することもできます。

[CSV としてエクスポート] オプションと [PDF としてエクスポート] オプションを使用して、フィルタリングした結果を **CSV** または **PDF** ファイルにエクスポートできます。CSV および PDF ファイル名の先頭には **SiteList** が付き、その後にファイルがエクスポートされた日付と時刻が続きます。



画面の右上隅には、現在のソフトウェアバージョンが表示されます。監査エラーを確認するには、「構成を確認」をクリックします。詳細については、「構成の検証」を参照してください。

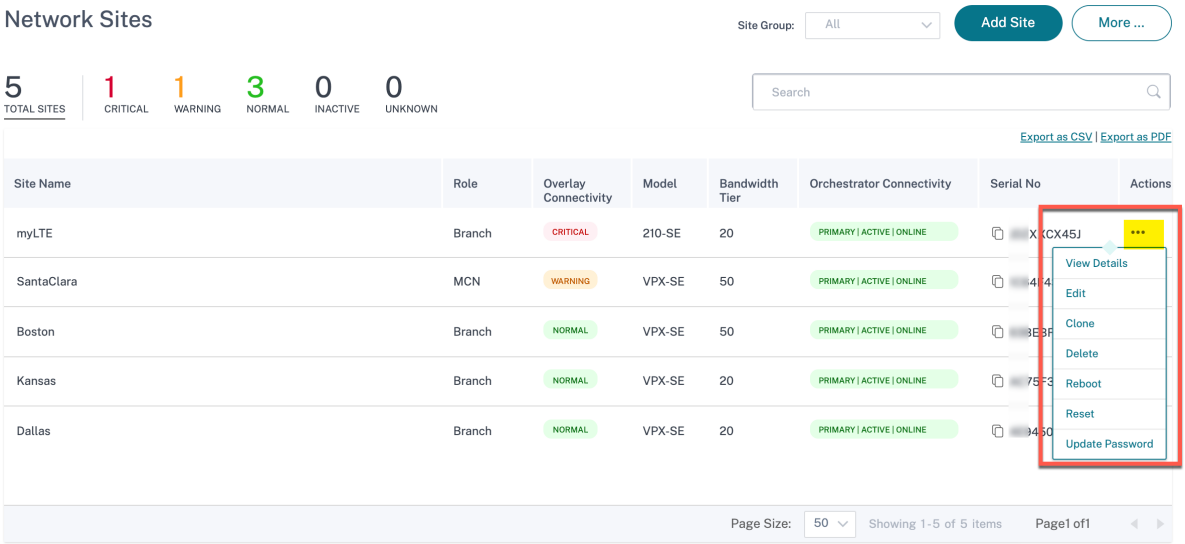
サイトグループドロップダウンリストを使用して、サイトが属するグループ/地域に基づいてサイトをフィルタリングできます。



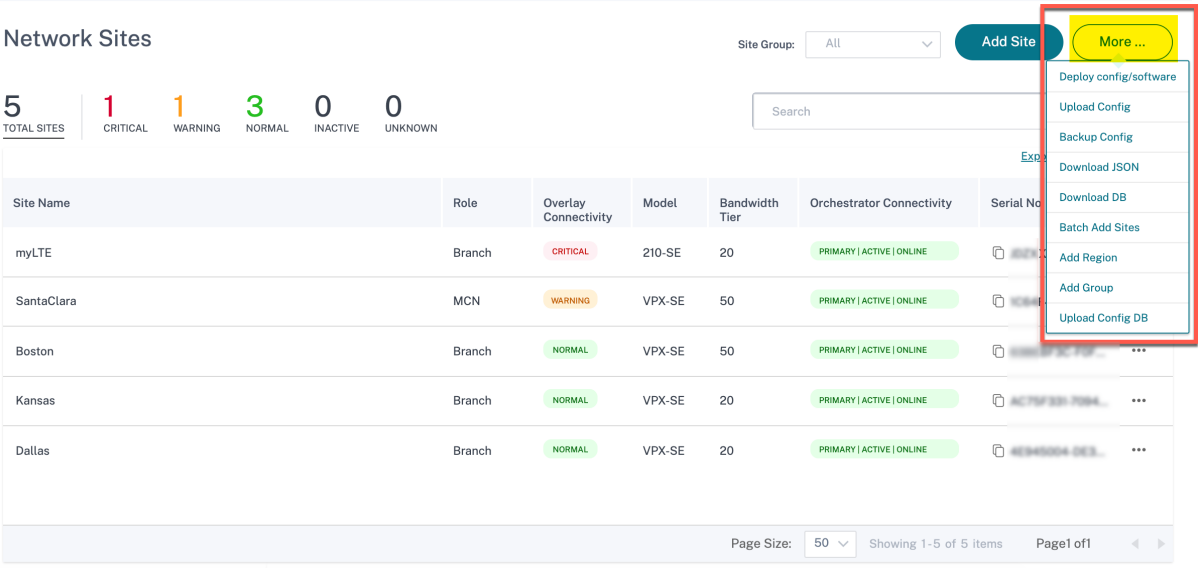
フィルタリングされた結果のサイト名をクリックすると、サイト構成画面が表示されます。サイトが高可用性設定になっている場合、**Orchestrator Connectivity** 列にはプライマリアプライアンスとセカンダリアプライアンスの両方のステータスが表示されます。シリアル番号列には、アプライアンスのシリアル番号が表示されます。高可用性セットアップでは、プライマリアプライアンスとセカンダリアプライアンスの両方のシリアル番号が表示されます。コピーアイコンを使用してアプライアンスのシリアル番号をコピーできます。

アクション列を使用して、サイトの詳細を表示したり、サイトのパスワードを編集、複製、削除、リセット、更新した

りできます。サイトに関連付けられたデバイスを再起動することもできます。



More…オプションを使用して、設定のアップロード、サイトのバッチ追加、JSON のダウンロードなど、その他のアクションを実行できます。



サイトの追加

[**+** サイトの追加] オプションを使用して、新しいサイトを追加します。サイト設定ワークフローの詳細については、「サイト設定」を参照してください。

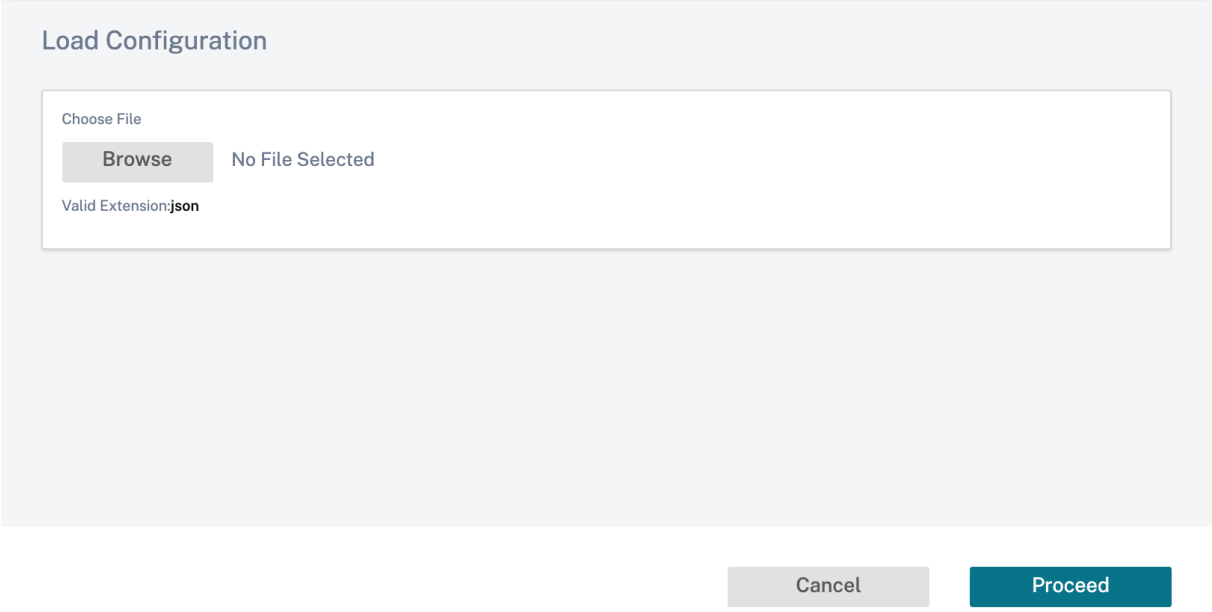
構成とソフトウェアの導入

[詳細] **>** [設定/ソフトウェアのデプロイ] オプションを選択すると、ネットワーク全体で構成の検証、ステージング、

アクティブ化に役立つデプロイメントセクションが表示されます。構成とソフトウェアの展開について詳しくは、「展開」を参照してください。

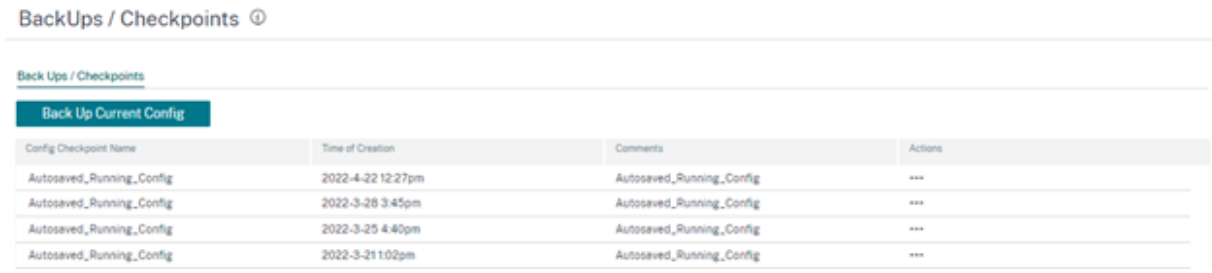
設定をアップロード

[詳細] **>** **[**設定のアップロード] オプションでは、以前に保存した設定のいずれかを参照してアップロードできます。新しくアップロードされた構成は、ネットワークのアクティブな構成として機能します。



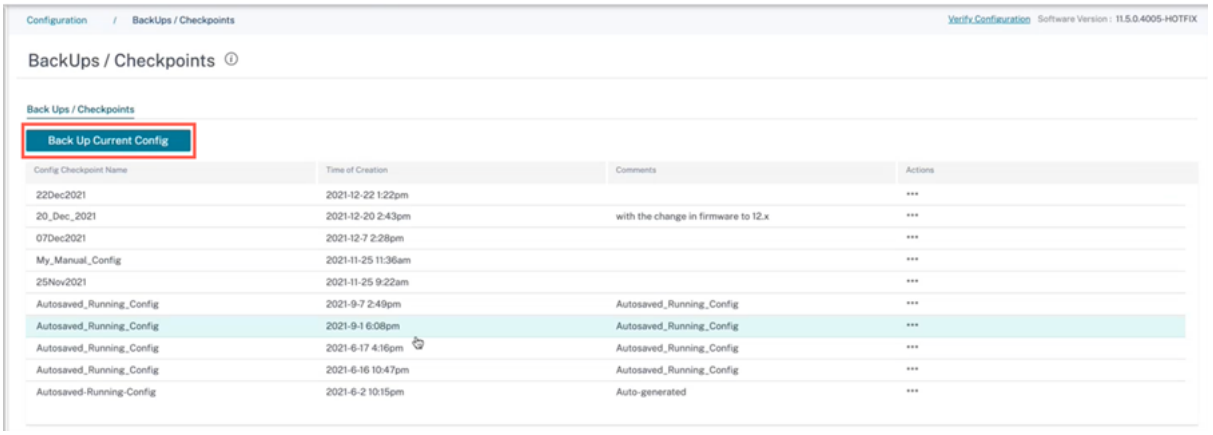
バックアップ/チェックポイント

[詳細] **>** **[**構成のバックアップ] オプションを選択すると、[バックアップ/チェックポイント] ページが表示され、構成のバックアップと復元、または保存されているチェックポイントの確認を行うことができます。

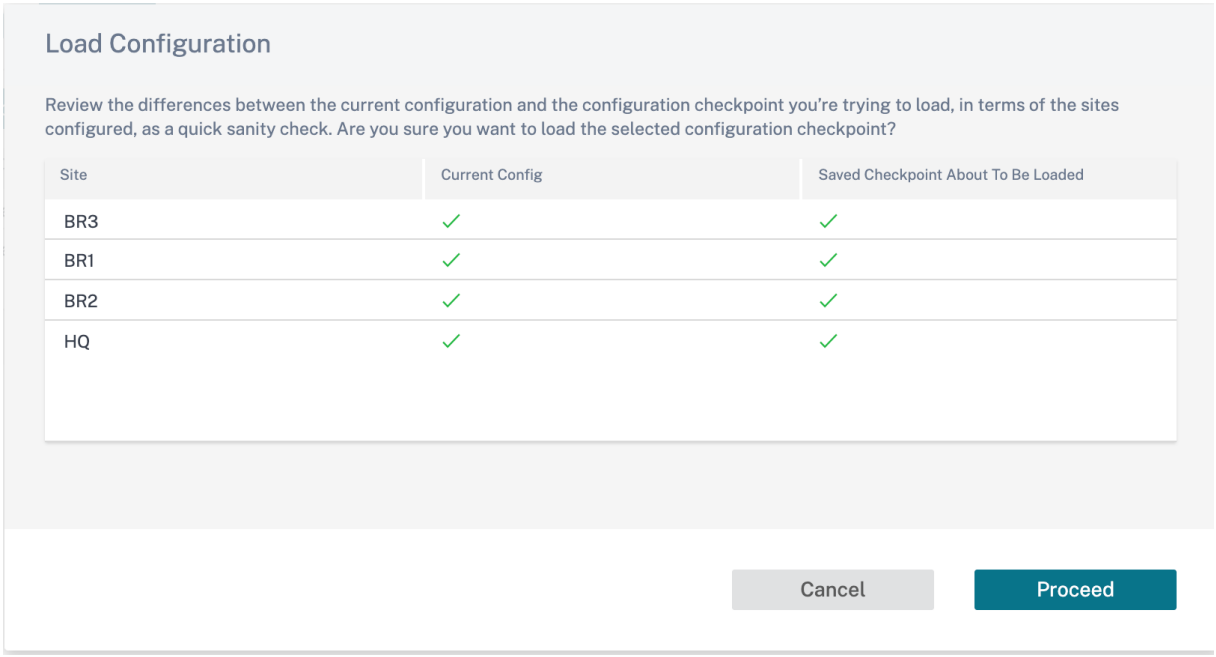


監査エラーを確認するには、「構成を確認」をクリックします。

「現在の構成をバックアップ」をクリックして、現在の構成を今後の使用に備えてチェックポイントとしてバックアップします。



[アクションの下] の [設定の読み込み] をクリックして、保存した構成をロードします。[続行] をクリックします。



[アクション] の下の [コピー] をクリックして、既存の設定の同様のコピーを作成します。保存された設定チェックポイントをダウンロード、編集、削除することもできます。これらの操作はアクションの下にあります。

JSON をダウンロード

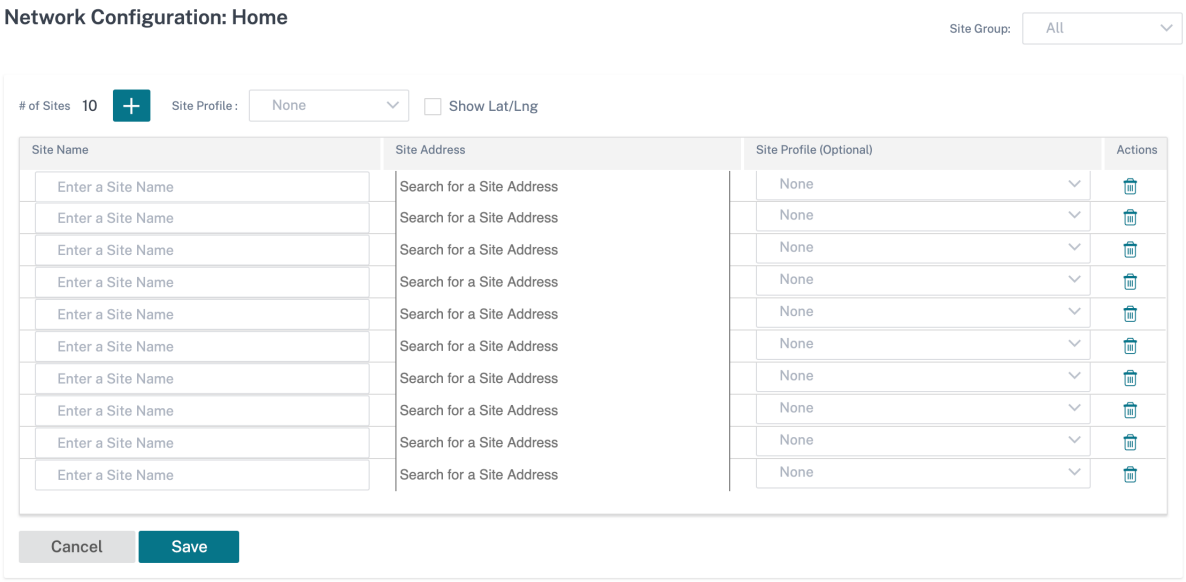
[詳細] **> [JSON** のダウンロード] オプションを使用すると、現在の設定を JSON 形式でダウンロードしてエクスポートし、オフラインで確認できます。

データベースをダウンロード

More > Download DB オプションでは、現在の設定を DB 形式でダウンロードしてエクスポートできます。

サイトを一括で追加

[その他] **>** [サイトの一括追加] オプションを使用すると、複数のサイトをバッチですばやく追加できます。また、各サイトで使用するサイトプロファイルを選択することもできます。ただし、IP アドレスなどの固有のパラメーターは、サイトごとに構成されたままです。



リージョンの追加

[その他] **>** [リージョンの追加] オプションを選択すると、リージョンを作成して [サイトと **IP** グループ] **>** [リージョン] ページに移動します。詳細については、「リージョン」を参照してください。

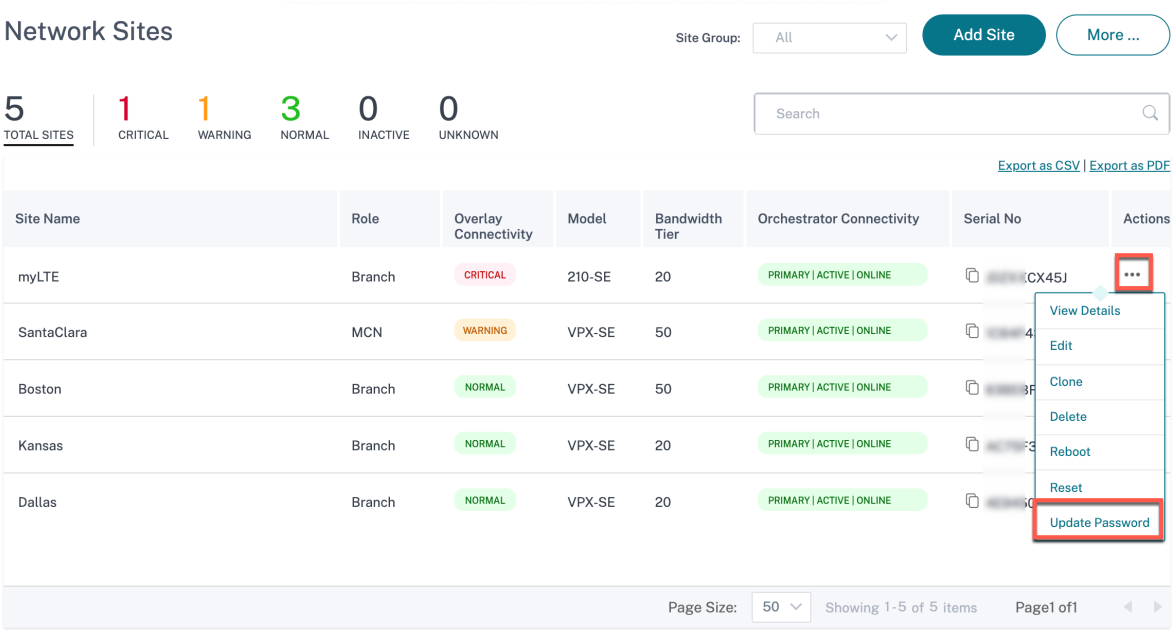
[グループを追加]

[その他] **>** [グループの追加] オプションを選択すると、[サイトと **IP** グループ] **>** [カスタムグループ] ページが開き、そこでリージョンを作成できます。詳細については、「カスタムグループ」を参照してください。

パスワードの更新

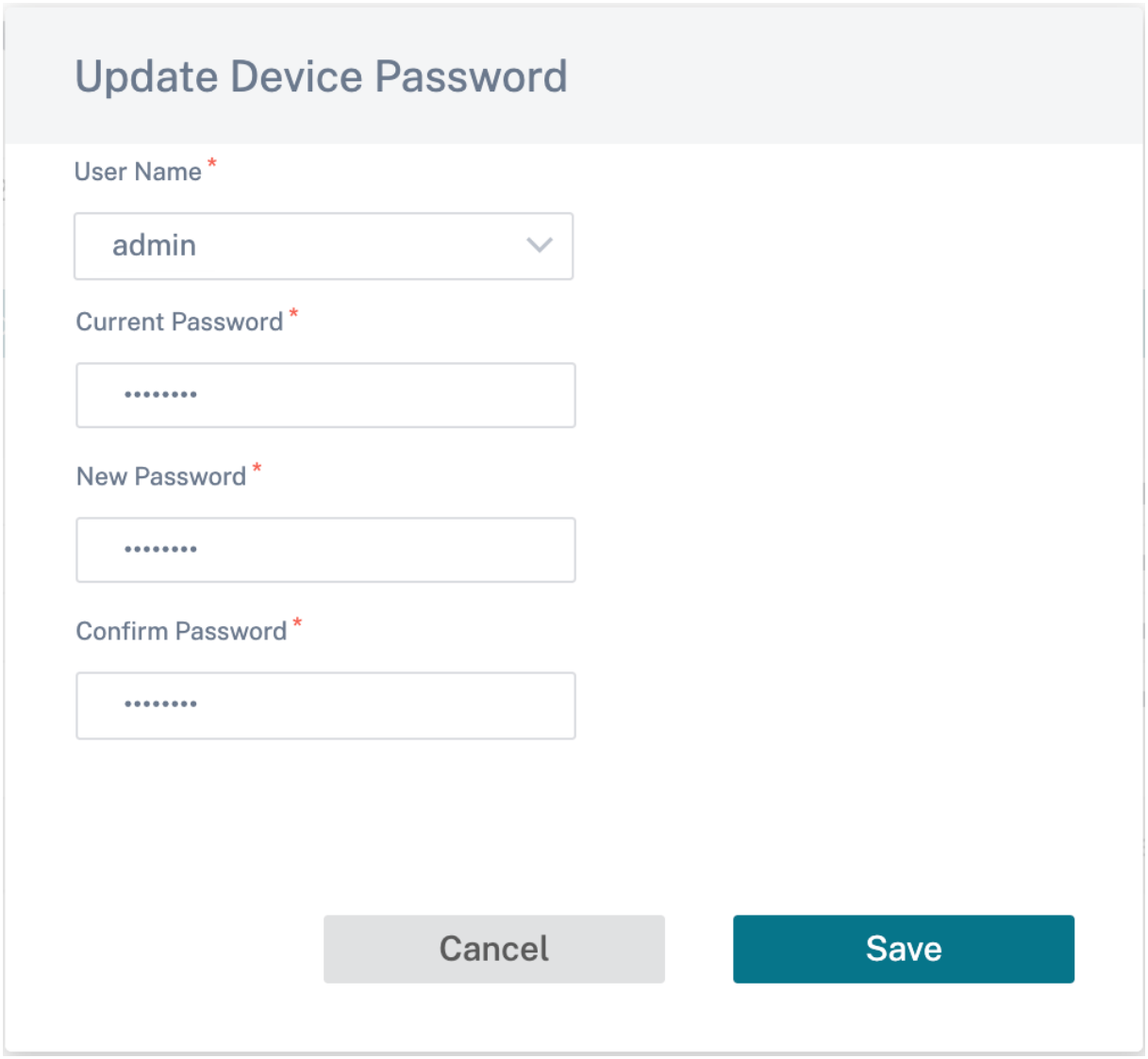
オンプレミス向け Citrix SD-WAN Orchestrator を使用して、ネットワーク上のさまざまなサイトで SD-WAN アプライアンスのパスワードを変更できます。

パスワードを変更するには、オンラインのアプライアンスの詳細アイコンをクリックし、「パスワードの更新」を選択します。



次のフィールドに値を入力します。

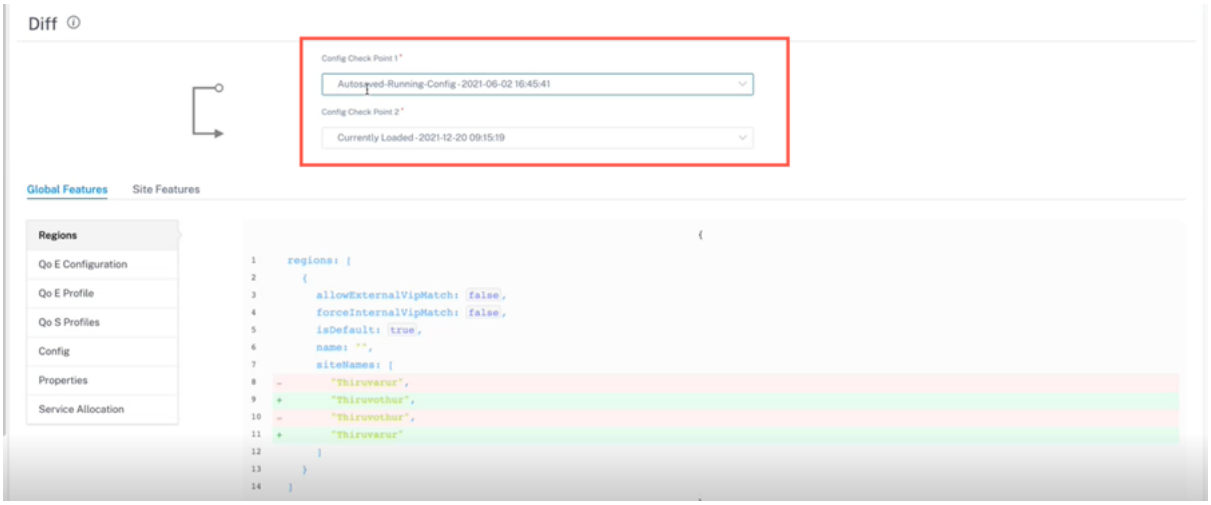
- ユーザー名: サイトで構成されているユーザーのリストから、パスワードを変更するユーザー名を選択します。
- 現在のパスワード: 現在のパスワードを入力します。管理者ユーザの場合、このフィールドはオプションです。
- 新しいパスワード: お好きな新しいパスワードを入力します。
- パスワードの確認: 確認のため、パスワードを再入力します。



構成の違い

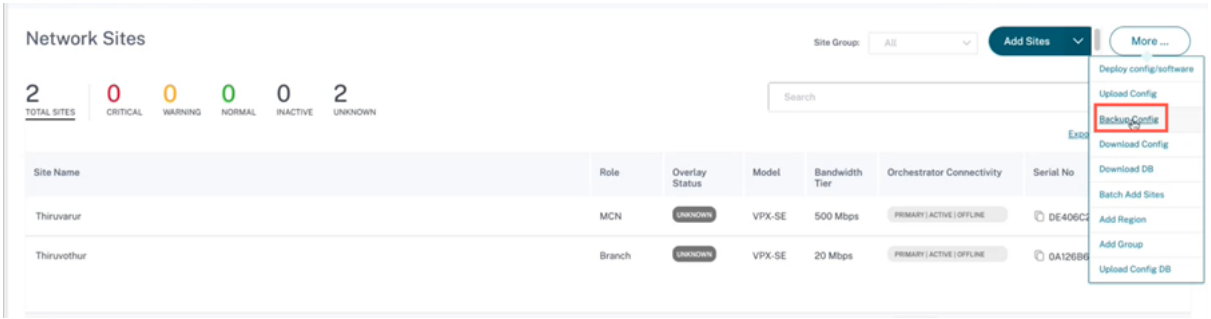
October 26, 2022

Config Diff 機能を使用すると、任意の 2 つのバージョンの設定チェックポイントの違いを確認できます。**Config Diff** オプションは、ネットワークレベルの [構成] > [**Config Diff**] の下にあります。

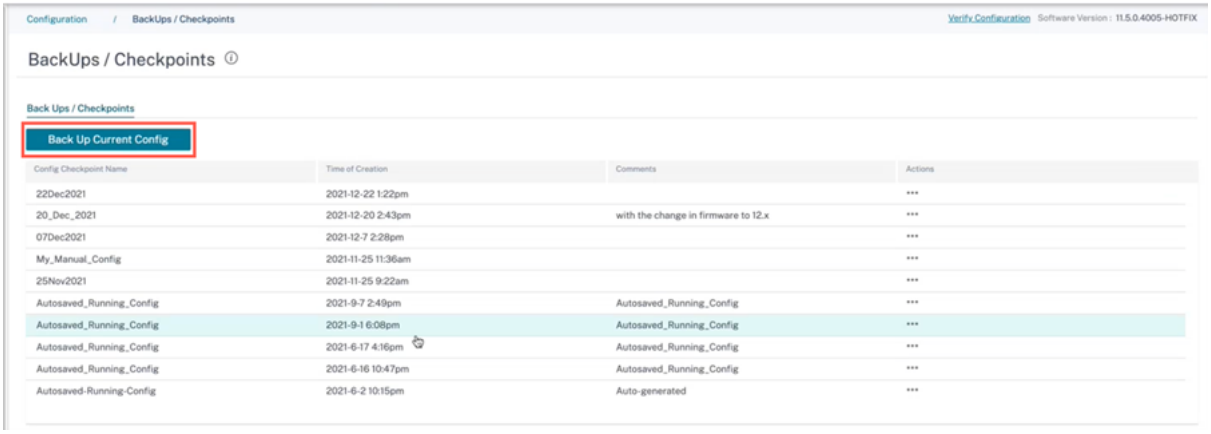


デプロイ中に、構成を適切な名前で保存できます。保存された構成はチェックポイントと呼ばれます。2 つの構成の違いを比較する際には、**Config Check Point 1/2** ドロップダウンリストから必要な構成を選択する必要があります。

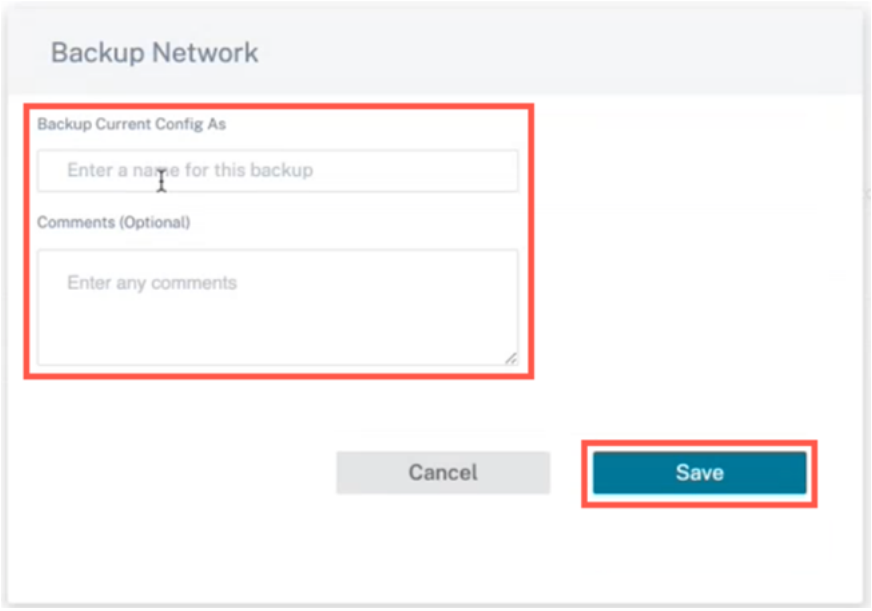
保存されている設定のバックアップ/チェックポイントのリストは、[構成] > [ネットワークホーム] で確認できます。[詳細] ドロップダウンリストから [****** 構成のバックアップ ******] を選択します。



デプロイが行われると、設定は毎回自動的にバックアップされます。現在の設定を手動でバックアップすることもできます。そのためには、「現在の構成をバックアップ」オプションをクリックします。



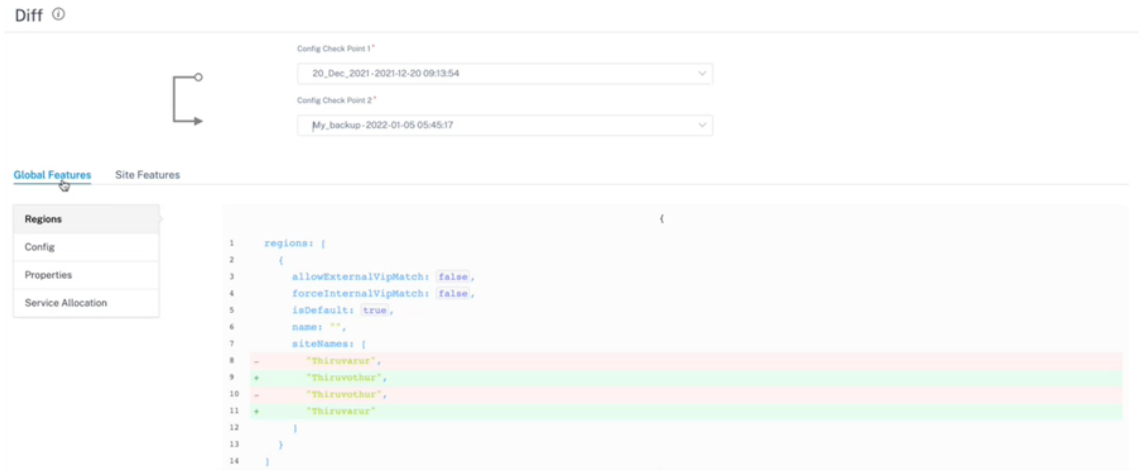
設定を保存する名前をコメントと共に入力します (オプション)。[保存] をクリックします。



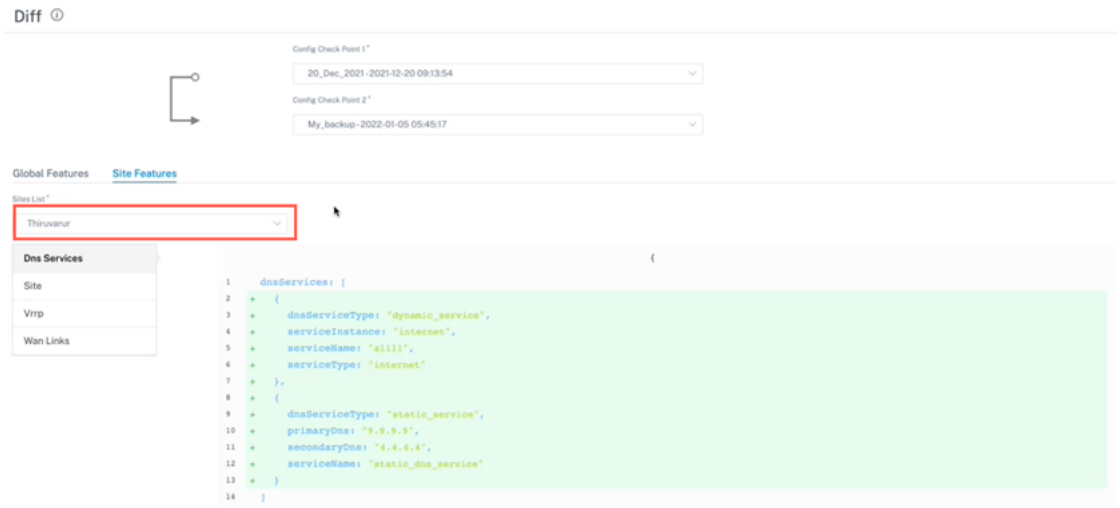
> 注:
>
> 構成バックアップは最大 5 つまで保存/作成できます。新しいバックアップを作成すると、最も古いバックアップ構成が自動的に削除されます。

次の 2 種類の構成を使用できます。

- グローバルレベル: グローバルカテゴリでは、リージョン、プロパティ、設定など、更新されたグローバル機能のリストを表示できます。



- サイトレベル: サイトカテゴリで、ドロップダウンリストからサイトを選択し、サイト、WAN リンク、DNS サービスなどの変更された詳細を表示できます。



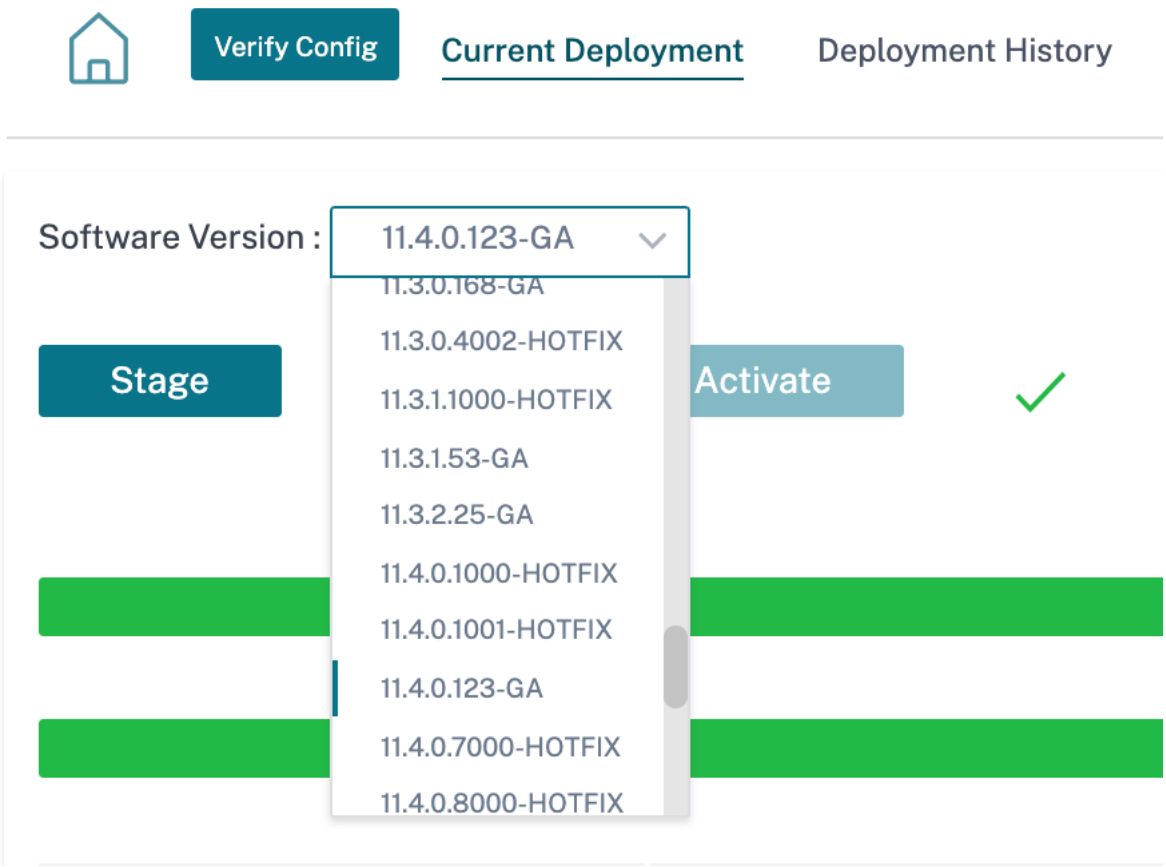
削除された値は、マイナス記号付きの赤い背景に表示され、更新/追加された値は、プラス記号付きの緑色の背景に表示されます。

展開

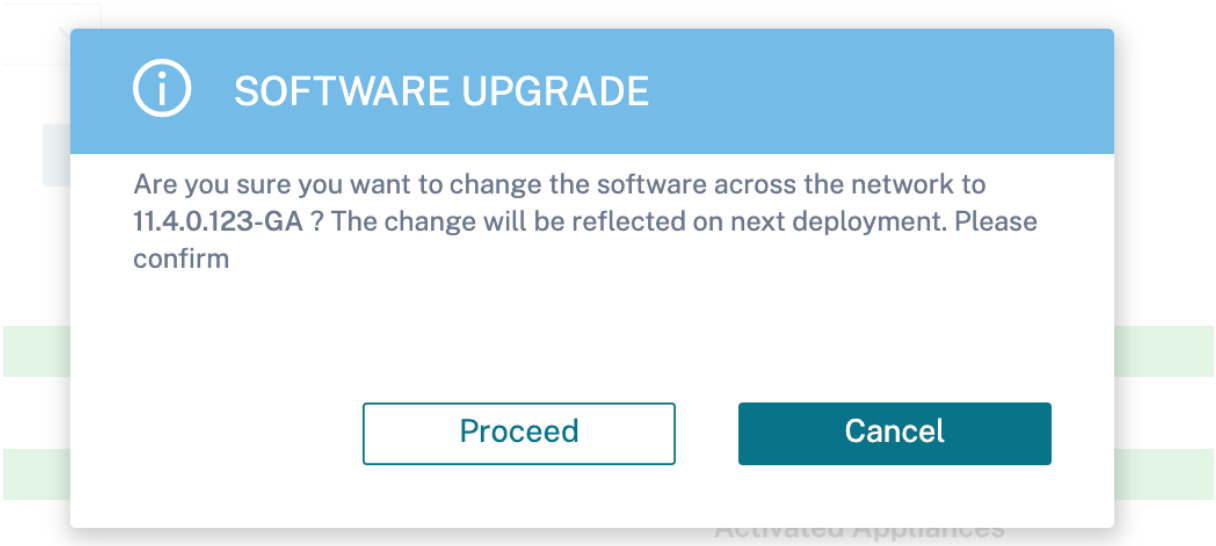
October 26, 2022

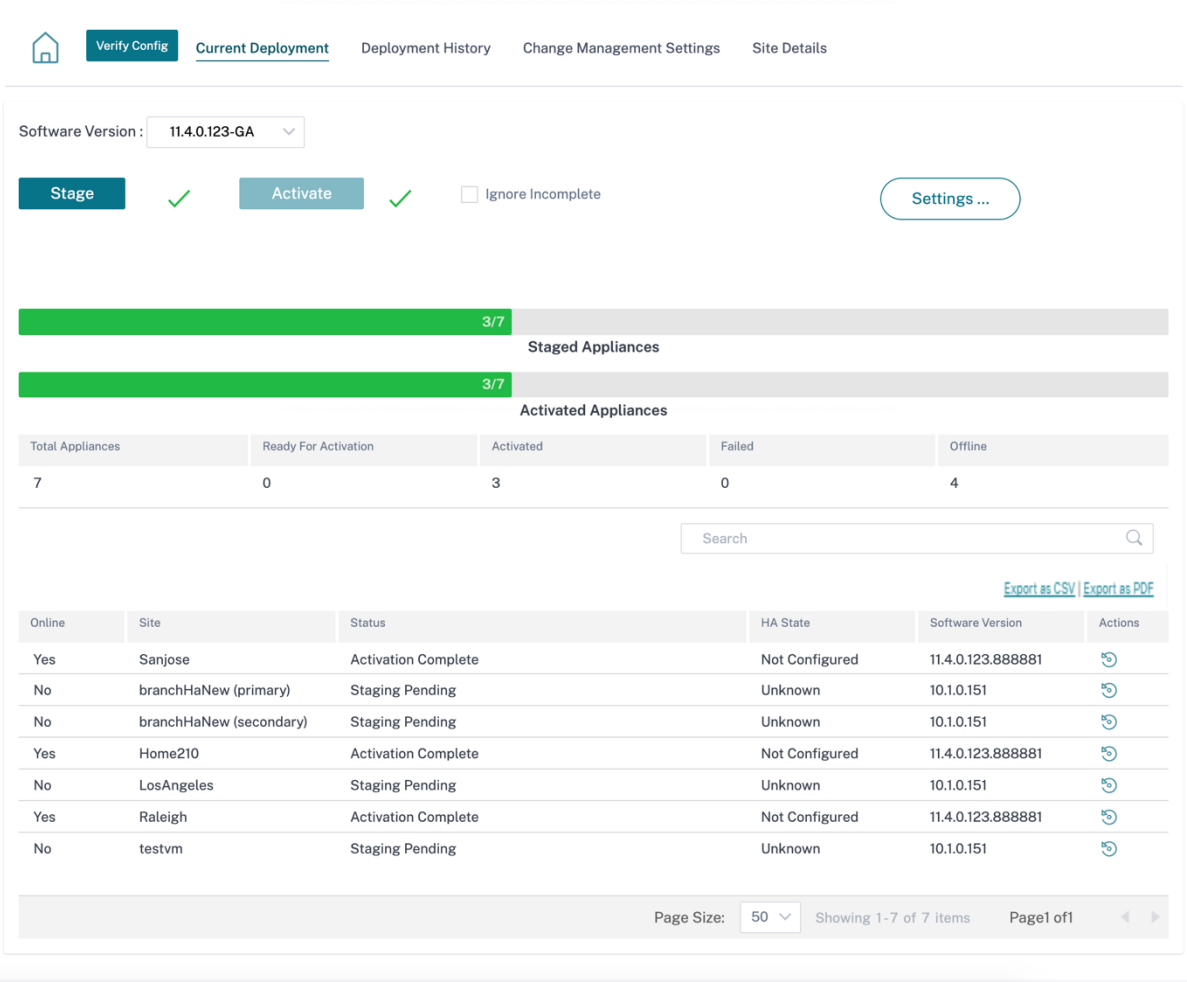
サイトを設定したら、**Deployment** ページを使用してソフトウェアバージョンを変更し、ネットワーク全体にその設定をステージングしてデプロイできます。

Software Version フィールドでアプライアンスソフトウェアバージョンを選択すると、ネットワーク上のすべてのアプライアンスの SD-WAN ソフトウェアをアップグレードできます。



確認のメッセージが表示されます。[続行] をクリックします。





エラー発生時のロールバック

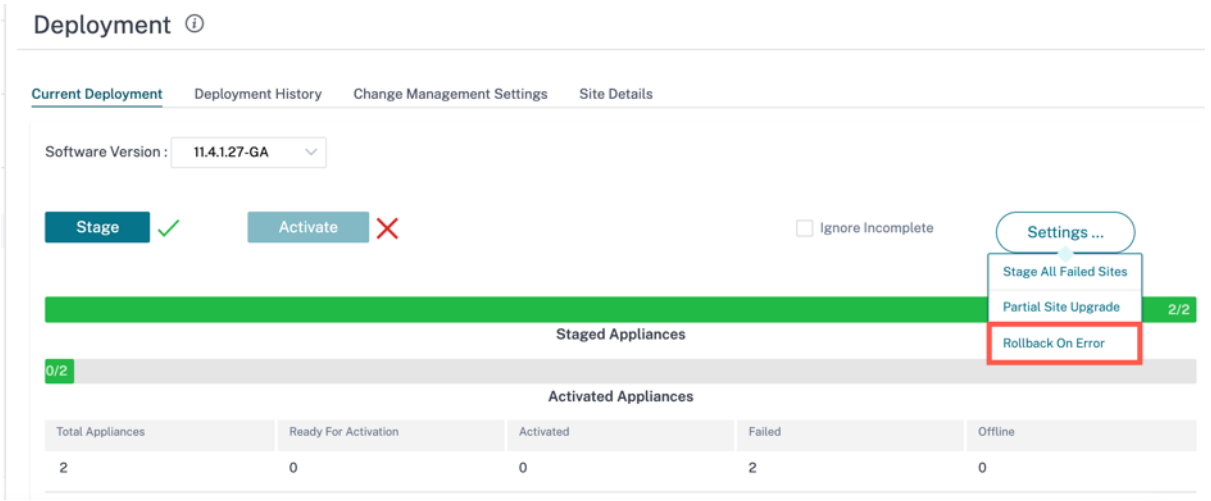
エラー時のロールバック機能を有効にすると、（展開の一部として）ネットワークアクティベーションを実行した後に Citrix SD-WAN Orchestrator サービスに接続できなかったサイトは、以前のバージョン（最後にステージングされたパッケージ）への自動ロールバックをトリガーして接続の復元を試みます。

> 注:
> 自動ロールバックは、Citrix SD-WAN Orchestrator サービスへの接続に失敗したサイトのみを対象としており、ネットワーク全体には適用されません。

ロールバックは、アプライアンスが Citrix SD-WAN Orchestrator サービスの接続を失った場合にのみトリガーされ、仮想パスのステータスがダウンするなど他のシナリオではトリガーされません。

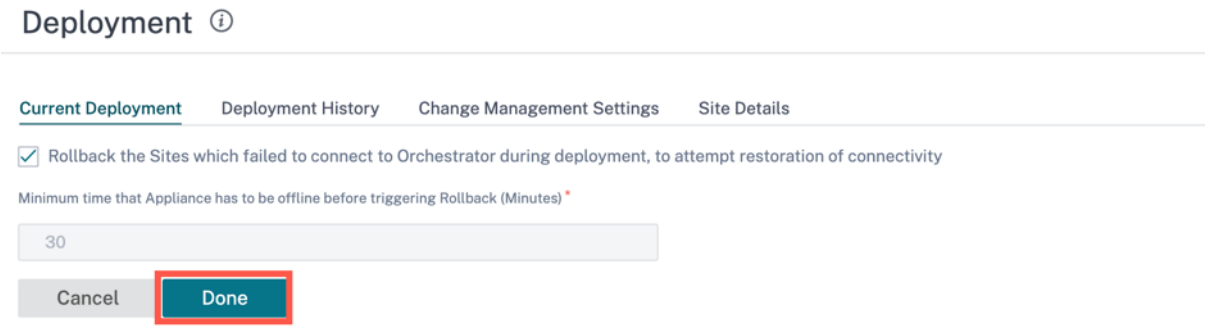
ネットワーク内の少なくとも 1 つのサイトがロールバックを開始すると、警告メッセージが表示され、ロールバックしようとしているサイトのリストと、すべてのオンラインサイトのネットワーク全体のロールバックを開始するオプションが表示されます。これらのサイトの進捗状況を確認し、適切なアクションを選択できます。

エラー時ロールバック機能を有効にするには、[構成] **>** [デプロイ] **>** [設定] **>** [エラー時ロールバック] に移動します。



「エラー時にロールバック」チェックボックスを選択すると、アクティベーション後に Citrix SD-WAN Orchestrator サービスに接続できなかったサイトの自動ロールバックを有効にできます。**Rollback on Error** 機能を有効にするには、デプロイを開始する前に Rollback on Error 機能を有効にする必要があります。

サイトが自動ロールバックをトリガーするには、アクティベーション後、少なくとも 30 分間（現在は変更不可）オフラインのままにする必要があります。サイトが 30 分以内に Citrix SD-WAN Orchestrator サービスに接続できる場合、ロールバックはトリガーされません。

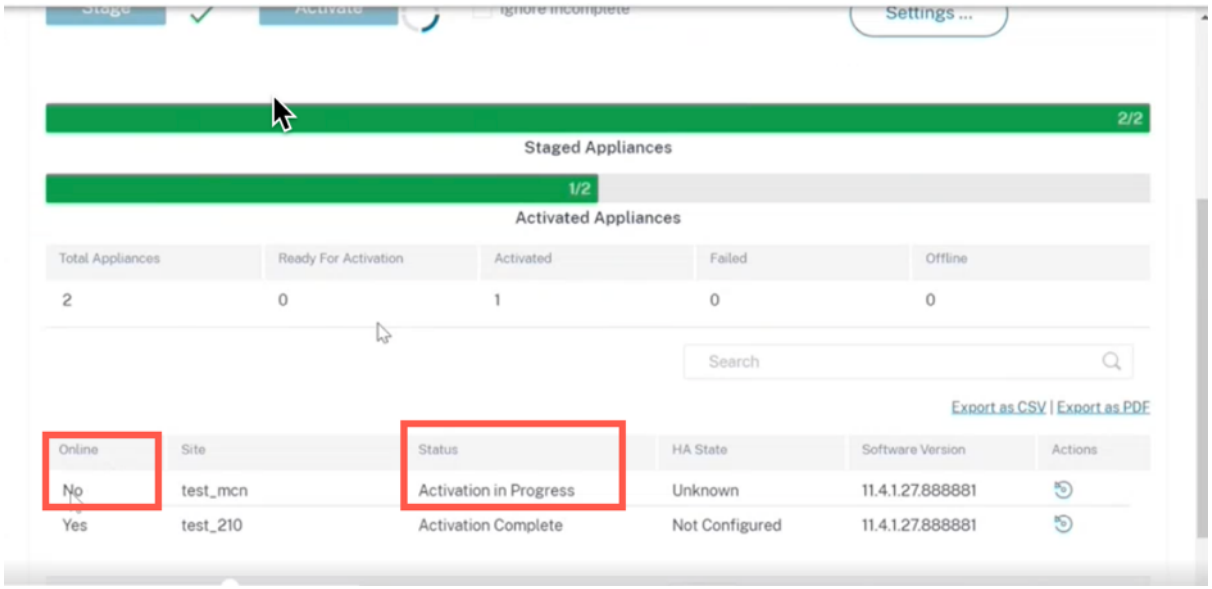


> 注:
> サイトのロールバックは、アクティブ化後にサイトが接続を失った場合にのみ実行されます。サイトがオンラインで、アクティベーションが失敗した場合、ロールバックはトリガーされません。

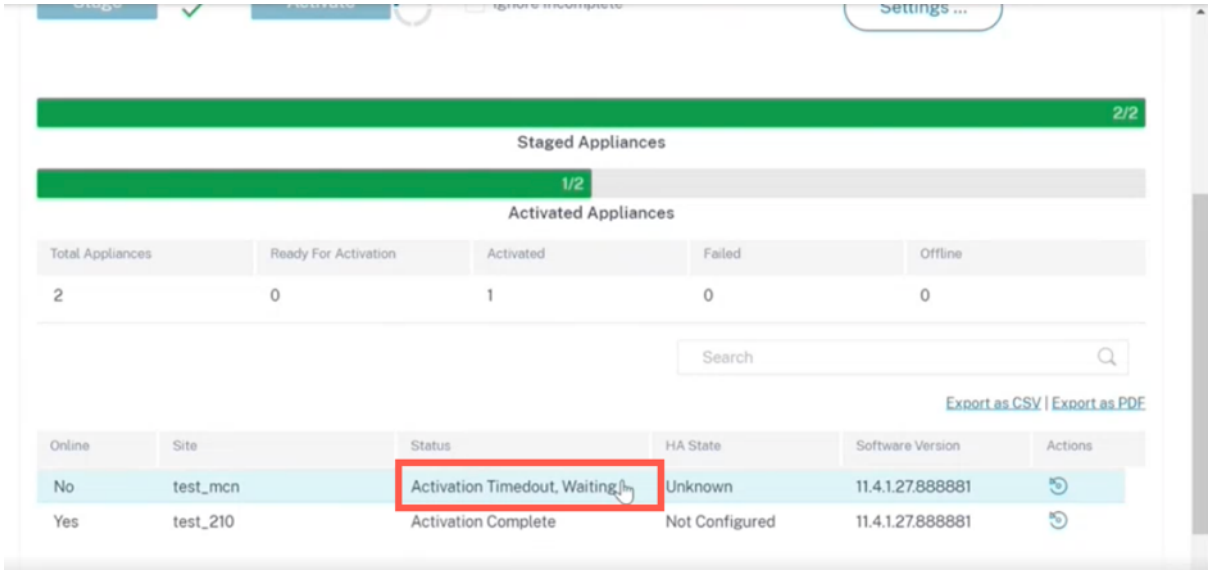
「エラー時のロールバック」を有効にしたら、「完了」をクリックします。

ユースケース **1:** ヒットレスアップグレード

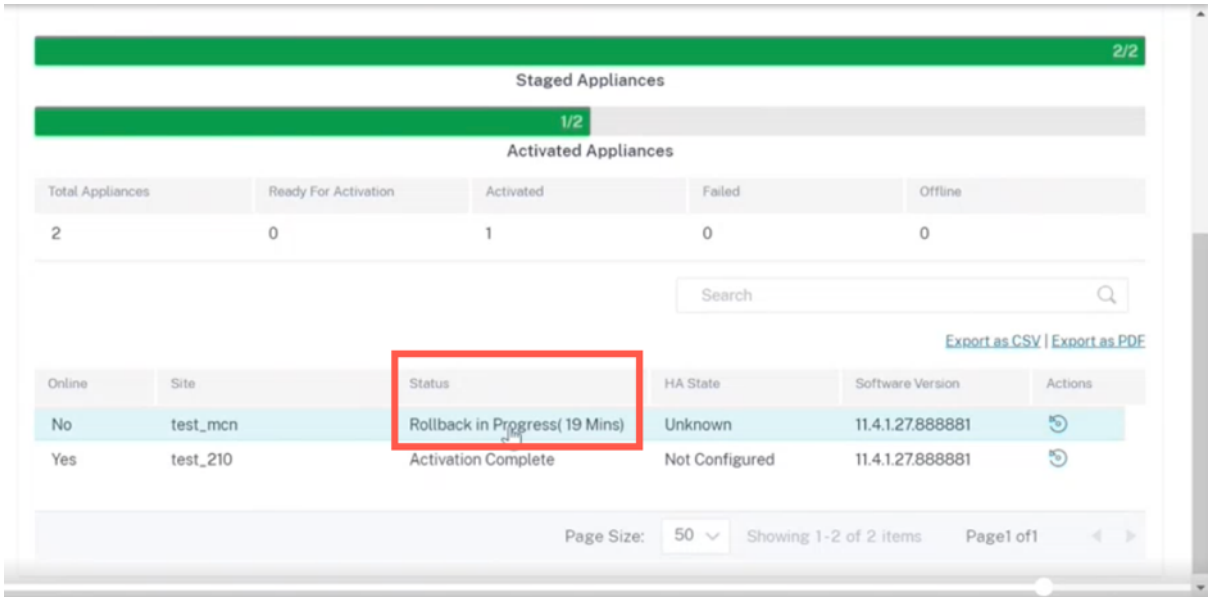
サイトは、ステータスが [アクティベーション中] の状態で指定された時間アクティベーションが完了するのを待ちます。



そのタイムアウトを過ぎると、サイトがまだオフラインの場合は、Citrix SD-WAN Orchestrator サービスはさらに 30 分（ロールバック開始タイムアウト）待ってサイトに接続し直す機会を与えます。この段階では、ステータスには [アクティベーションタイムアウト]、[ロールバック開始待ち] (残り時間 (分)) と表示されます。

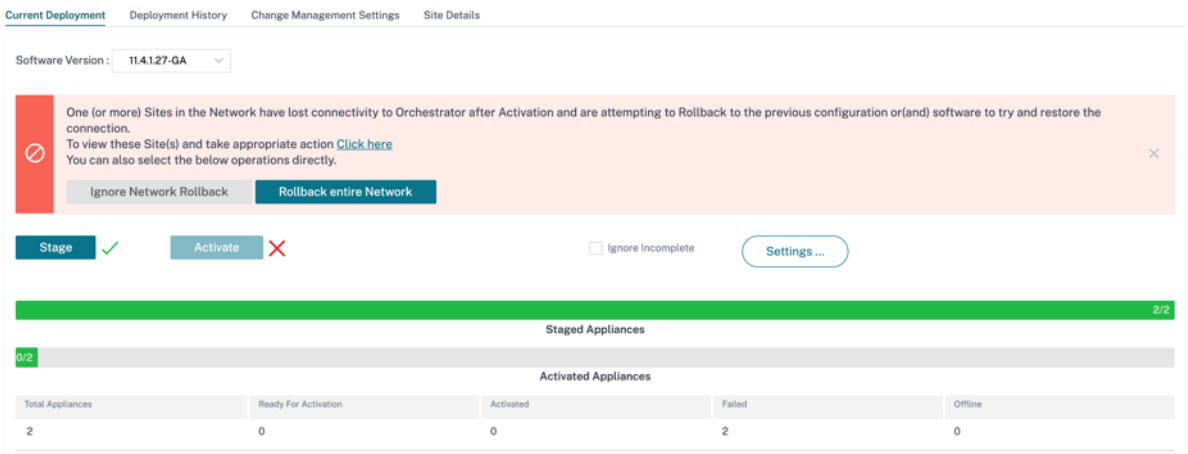


30 分の待機期間を過ぎると、アプライアンスは以前の構成または（および）ソフトウェアへの自動ロールバックをトリガーして、Citrix SD-WAN Orchestrator サービスの接続を復元しようとします。Citrix SD-WAN Orchestrator サービスは、アプライアンスが Citrix SD-WAN Orchestrator サービスに接続するまで 20 分（設定不可）待ちます。この間、ステータスには「ロールバック中」（残り時間（分単位）と表示されます。



アプライアンスが接続に失敗した場合、この 20 分以内に、Citrix SD-WAN Orchestrator サービスはロールバック操作を失敗とマークし、ステータスには「デバイスロールバック失敗」と表示されます。

ネットワークでは、少なくとも 1 つのデバイスが自動ロールバックを開始すると、次のようなバナーがユーザーに表示されます。



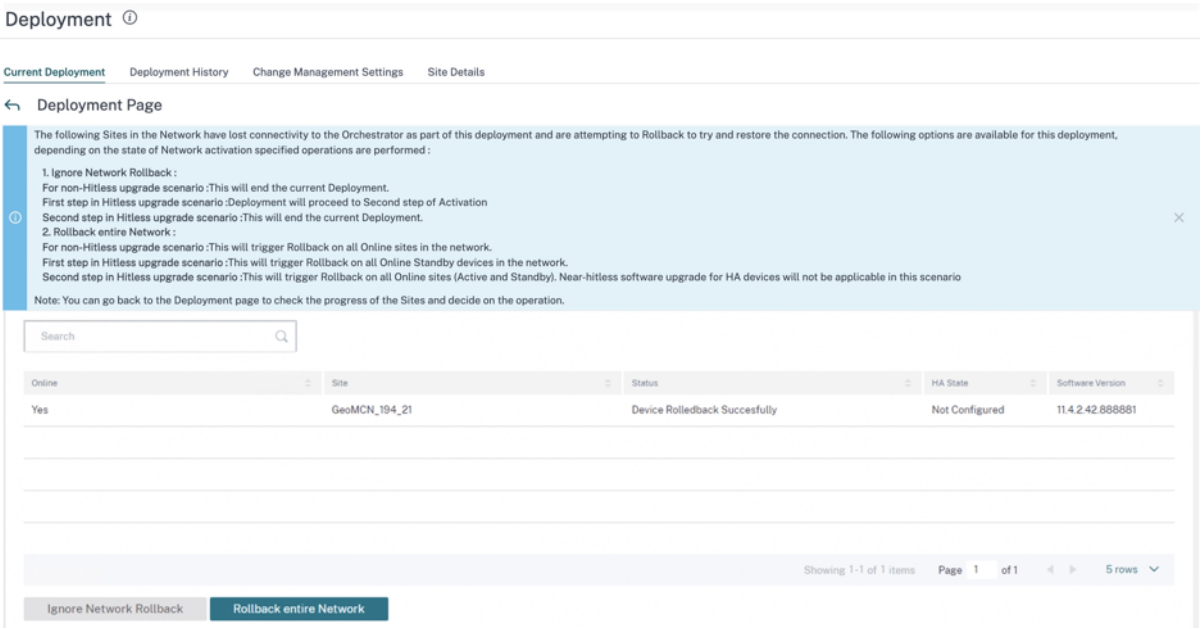
ネットワークアクティベーションの段階に基づいて、表示されたオプションは次の操作を実行します。

- ネットワークロールバックを無視:
  - ヒットレスアップグレードシナリオの場合: 現在のデプロイを終了します。
  - ヒットレスアップグレードシナリオの最初のステップ: デプロイはアクティベーションの 2 番目のステップに進みます。
  - ヒットレスアップグレードシナリオの **2** 番目のステップ: 現在のデプロイを終了します。
- ネットワーク全体のロールバック:

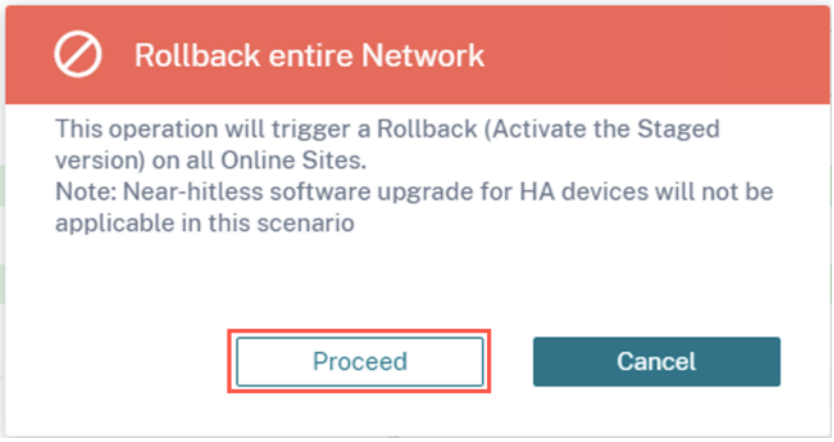
- ヒットレスアップグレードシナリオの場合: ネットワーク内のすべてのオンラインサイトでロールバックをトリガーします。
- ヒットレスアップグレードシナリオの最初のステップ: ネットワーク内のすべてのオンラインスタンバイデバイスでロールバックをトリガーします。
- ヒットレスアップグレードシナリオの **2** 番目のステップ: すべてのオンラインサイト (アクティブおよびスタンバイ) でロールバックをトリガーします。このシナリオでは、高可用性デバイスのほぼヒットレスなソフトウェアアップグレードは適用されません。

さらに「Click **Here**」ハイパーリンクをクリックすると、ロールバックが進行中または完了しているサイトのリストを表示し、そのページに対して上記のアクションを実行できます。

また、ロールバックをトリガーしたサイトが成功または失敗するまで待ってから、ネットワーク全体のロールバックをトリガーするかどうかを決定することもできます。



「ネットワーク全体をロールバック」オプションを選択すると、次のポップアップボックスが表示されます。



> 注:
> このシナリオでは、高可用性アプライアンスのニアヒットレスソフトウェアアップグレードは適用されません。つまり、ネットワークに高可用性サイトがある場合、ネットワーク全体のロールバックをトリガーすると、そのサイトの両方の高可用性アプライアンスが同時にアクティブになり、一部の原因となる可能性があります。ネットワークのダウンタイム。

[続行] をクリックすると、すべてのオンラインサイトでネットワーク全体のロールバックが開始されます。

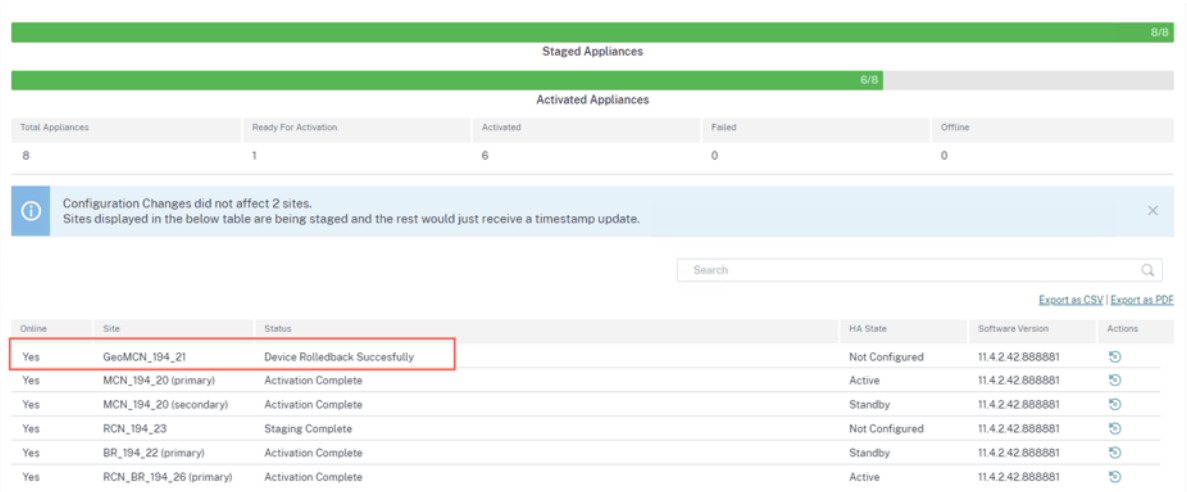
ユースケース **2:** ヒットレスアップグレード

ヒットレスアップグレードの場合、スタンバイアプライアンスが最初にアクティブ化され、次にアクティブで非高可用性アプライアンスがアクティブ化されます。アクティベーション後にスタンバイアプライアンスがオフラインになり、ロールバックを開始する場合の最初のステップの一部として、次のオプションを使用できます。

- ネットワークロールバックを無視: オフラインのスタンバイアプライアンスを無視して、アクティブなアプライアンスのアクティベーションを続行します。
- ネットワーク全体のロールバック: アクティベーションを完了したオンラインスタンバイアプライアンスをすべてロールバックし、進行中のデプロイを終了します。この場合、アクティブで非高可用性アプライアンスのアクティベーションは行われません。

ヒットレスアップグレードの次のステップは、アクティブで非高可用性アプライアンスのアクティベーションです。前述の「ヒットレスアップグレード 」セクションで説明したように、エラー発生時のロールバックワークフローと同じです。このシナリオでは、「ネットワーク全体をロールバック」を選択すると、すべての（アクティブおよびスタンバイの）アプライアンスでロールバックがトリガーされます。

サイトがロールバックを完了し、Citrix SD-WAN Orchestrator サービスに接続し直すと、そのサイトのステータスに「デバイスロールバック成功」と表示され、サイトはオンラインになります。



制限事項

ロールバックまたはロールバックされたアプライアンスとネットワークの自動修正はサポートされていません。

> 注**:**
> サイトの自動ロールバックは、失われた接続を Citrix SD-WAN Orchestrator サービスに復元するためのバックアップメカニズムにすぎません。それでもアプライアンスが Citrix SD-WAN Orchestrator サービスに接続できない場合は、このアプライアンスのネットワーク構成を確認してください。

[CSV としてエクスポート] オプションと [PDF としてエクスポート**]** オプションを使用して、フィルタリングした結果を **CSV** または **PDF** ファイルにエクスポートできます。CSV および PDF ファイル名の先頭には「展開サイトリスト」が付き、その後にファイルがエクスポートされた日付と時刻が続きます。

- ステージ: 設定の検証が成功したら、「ステージ」をクリックして、ネットワーク内のすべてのアプライアンスに設定ファイルを配布します。デフォルトでは、Citrix SD-WAN Orchestrator サービスは、すべての制御ノード（MCN、RCN、Geo MCN、Geo RCN）とオンラインブランチアプライアンスがステージングされるのを待ってから、ユーザーがアクティブ化できるようにします。

  いずれかのサイトでステージングプロセスが失敗した場合は、「アクション」列の「ステージングを再試行」オプションを使用してステージングプロセスを再開します。

- 有効化:「有効化」をクリックして、ネットワーク上のすべてのサイトで段階的構成を有効にします。
- 未完了を無視: 選択すると、すべてのオンライン制御ノード (MCN、RCN、Geo MCN、Geo RCN) がステージングされた後にのみ、アクティブ化チェックボックスが有効になります。オンラインブランチアプライアンスの一部がステージングされていない場合でも、アクティベーションを選択できます。ステージングに失敗したオンラインブランチアプライアンスは無視されます。
- サイトの一部アップグレード設定: 選択したサイトを別のバージョンでアップグレードまたはダウングレードするための、サイトの一部アップグレードオプションが追加されました。部分的なサイトアップグレード機能により、ネットワーク全体に導入する前に新しいバージョンをテストできます。

サイトの一部アップグレード機能を使用すると、アップグレードをずらして行うことができるため、営業時間中のソフトウェアアップグレードの影響を軽減できます。

> 注
>
> サイトの一部アップグレードは、ネットワーク内のすべてのサイトで Citrix SD-WAN ソフトウェアバージョン 11.2.2 以降が実行されている場合にのみ実行できます。

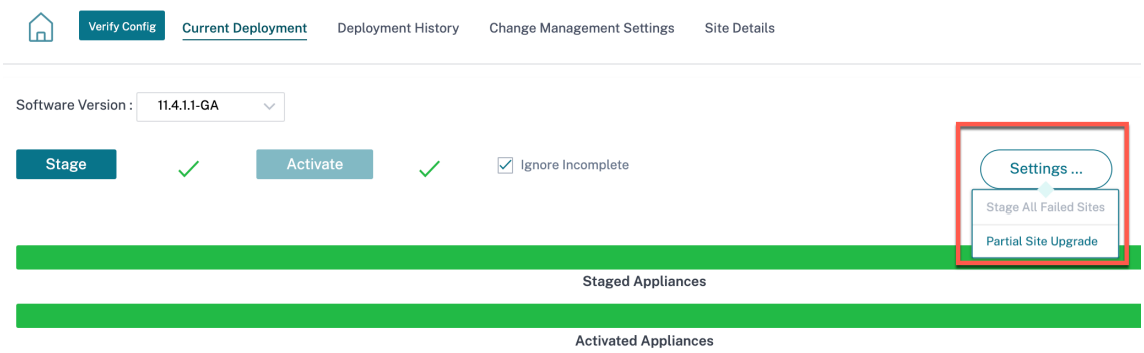
部分的なサイトアップグレードの構成変更は、変更を有効にするために変更管理が必要です。部分的なサイトアップグレードでは、下位バージョンが選択され、同じバージョンの設定が生成されます。ネットワークが部分的なサイトアップグレードモードの間は、新しい機能をテストできません。

部分的なサイトアップグレードを使用して新しいバージョンから古いバージョンにダウングレードする場合、新しいバージョンでのみサポートされている機能（新しいバージョンと古いバージョンの両方で同様の設定が存在する）の

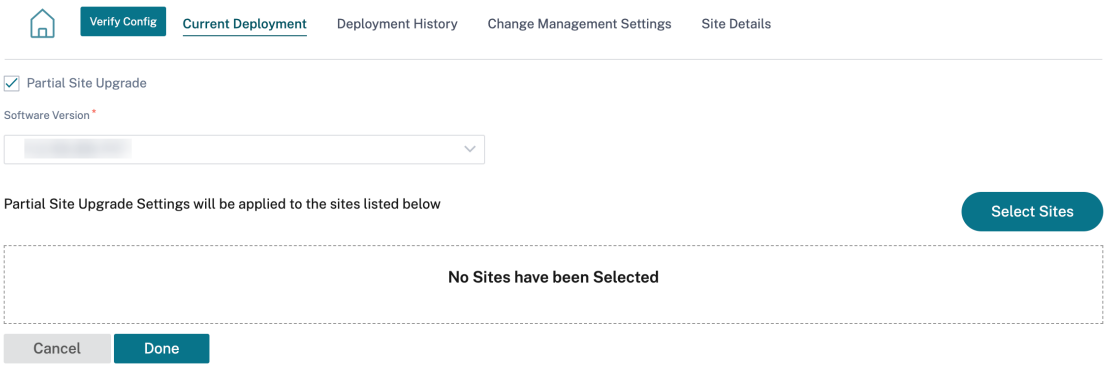
場合、監査エラーが発生します。たとえば、新しいバージョンでのみサポートされている新しいプラットフォームを選択すると、監査エラーが発生します。

サイトの一部アップグレードを実行するには:

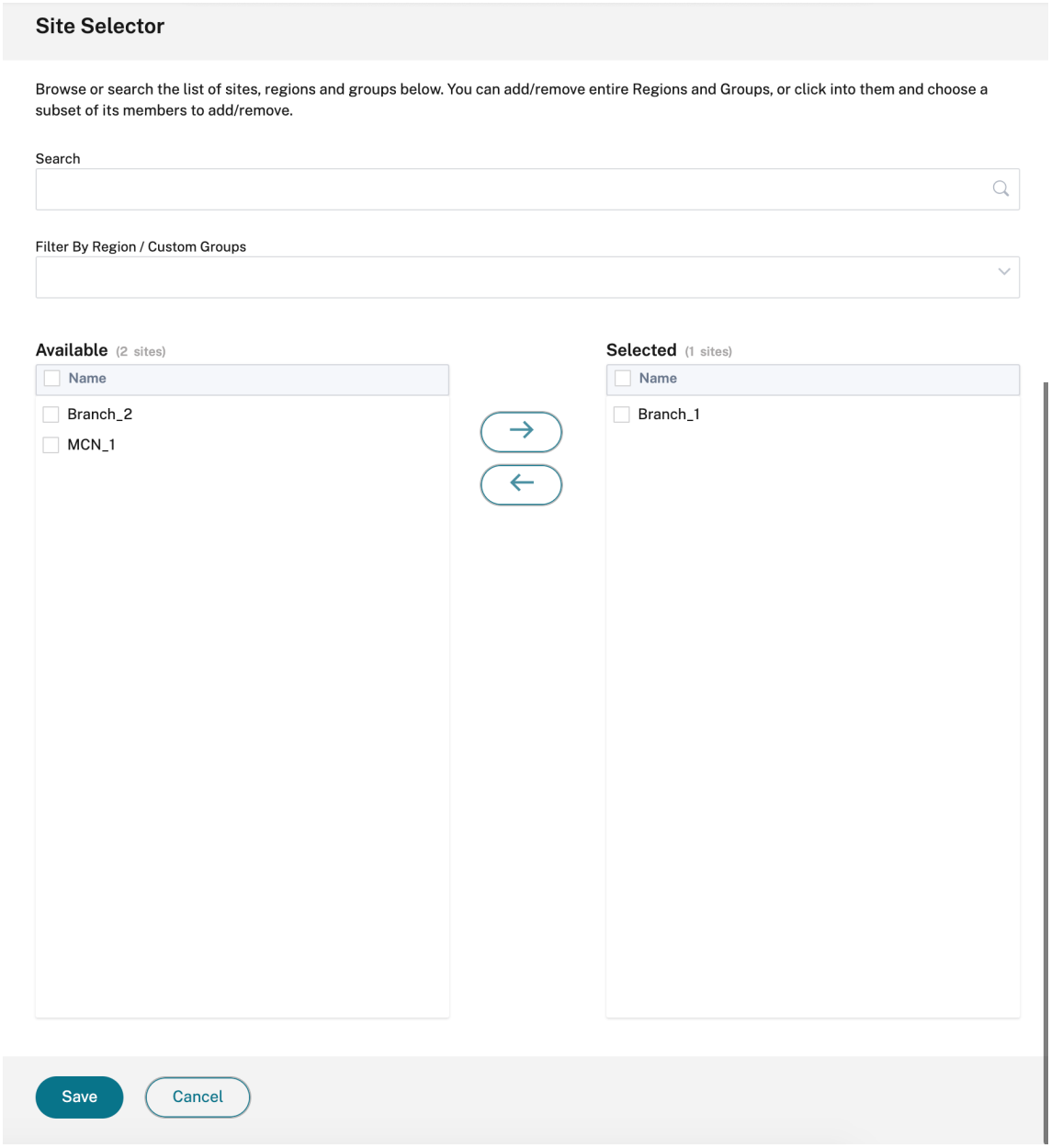
1. [設定…] をクリックします。アイコンをクリックし、「サイトの一部アップグレード」オプションを選択します。

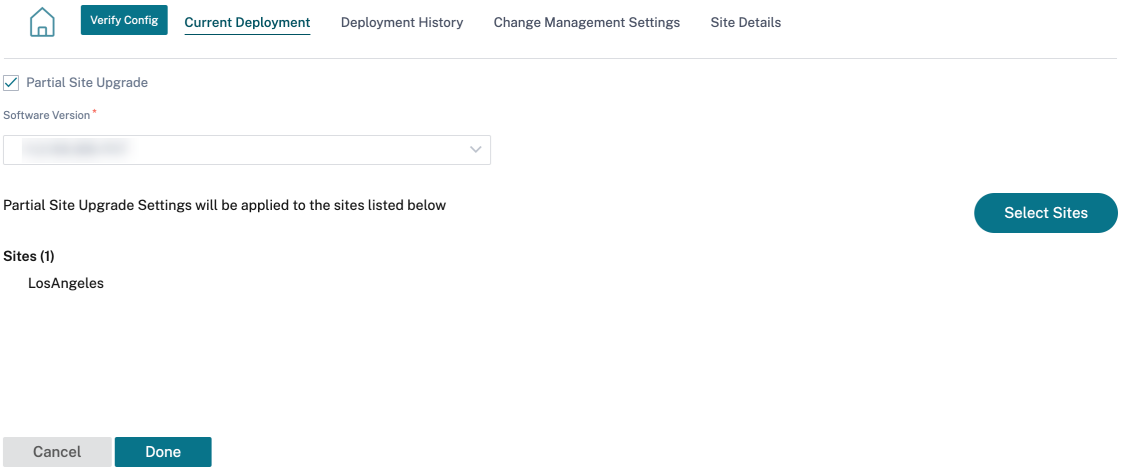


2. 「サイトの一部アップグレード」チェックボックスを選択し、ソフトウェアバージョンを選択し、「サイトを選択」をクリックして新しいサイトを追加します。



3. サイトを選択し、[保存] をクリックします。

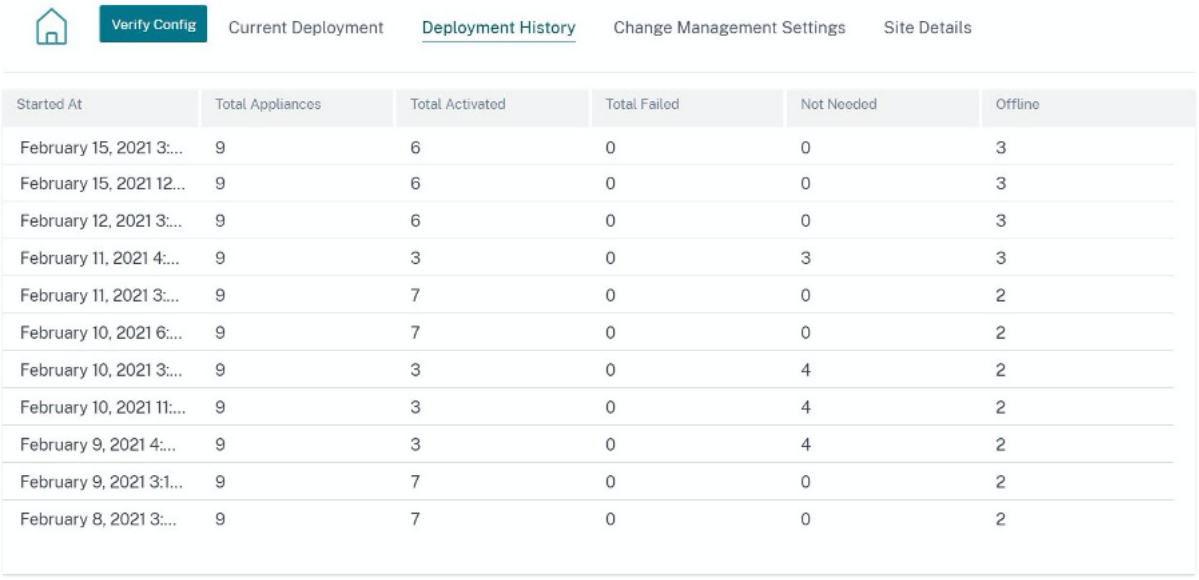




構成のみの更新の場合、構成が変更されたサイトのみがステージングされ、アクティブ化されます。残りのサイトでは、タイムスタンプが更新され、処理されます。

ソフトウェアバージョンを変更する場合、構成とソフトウェアパッケージの両方がネットワーク内のすべてのサイトでステージングされ、アクティブ化されます。

「デプロイ履歴」セクションでは、以前のデプロイ操作と結果を確認できます。



Started At	Total Appliances	Total Activated	Total Failed	Not Needed	Offline
February 15, 2021 3:...	9	6	0	0	3
February 15, 2021 12...	9	6	0	0	3
February 12, 2021 3:...	9	6	0	0	3
February 11, 2021 4:...	9	3	0	3	3
February 11, 2021 3:...	9	7	0	0	2
February 10, 2021 6:...	9	7	0	0	2
February 10, 2021 3:...	9	3	0	4	2
February 10, 2021 11:...	9	3	0	4	2
February 9, 2021 4:...	9	3	0	4	2
February 9, 2021 3:1...	9	7	0	0	2
February 8, 2021 3:...	9	7	0	0	2

HA ほぼヒットレスなソフトウェアアップグレード

ソフトウェアアップグレード（11.0.x 以前のバージョン）では、ネットワーク内のすべてのアプライアンスのステージングとアクティベーションが同時に行われます。これには高可用性 (HA) ペアが含まれ、ネットワークのダウンタイムにつながります。Citrix SD-WAN Orchestrator サービスでは、HA のほぼヒットレスなソフトウェアアップグ

レード機能により、ソフトウェアアップグレード（11.1.x 以上）プロセス中のダウンタイムが HA 切り替えの時間を超えないようにします。

> 注
>
> HA ほぼヒットレスソフトウェアのアップグレードは、次の場合に適用されます。
>
> - 高可用性 (HA) モードで展開されているサイト。HA 以外のサイトには適用されません。
> - Citrix SD-WAN Orchestrator サービスベースの展開のみで、SD-WAN Center または MCN を使用して管理されるネットワークには適用されません。
> - ソフトウェアのアップグレードのみであり、設定の更新は行われません。アップグレードの一環としてソフトウェアとともに構成が変更された場合、Citrix SD-WAN Orchestrator サービスは HA ニアヒットレスソフトウェアアップグレードを実行せず、以前の方法（シングルステップアップグレード）でアップグレードを続行します。

アップグレードシーケンスの概要は次のとおりです。

1. Citrix SD-WAN Orchestrator サービスは、ネットワーク内のすべてのアプライアンスの HA 状態をチェックします。
2. スタンバイ状態のすべてのセカンダリアプライアンスをアップグレードします。
3. HA スイッチオーバーがトリガーされ、**** アクティブアプライアンスとスタンバイアプライアンスの状態が切り替わります ** 。
4. 現在スタンバイ状態になっているプライマリアプライアンスをアップグレードします。

HA ほぼヒットレスソフトウェアアップグレードは、次の 2 段階のアップグレードプロセスです。

ステップ **1**: ソフトウェアアップグレード中、11.1 リリース後、Citrix SD-WAN Orchestrator サービスは、ネットワーク全体でスタンバイ状態にあるすべてのアプライアンスで最初にソフトウェアアップグレードを実行します。ネットワークは、アクティブアプライアンスを配置した状態でまだ稼働しています。

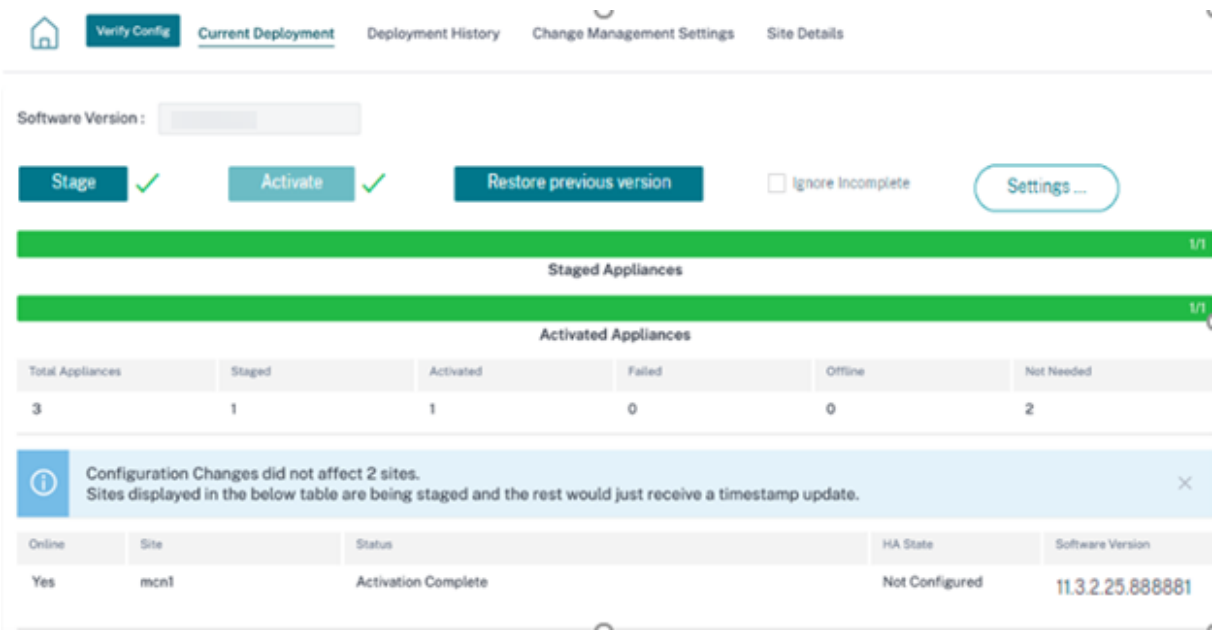
すべてのスタンバイアプライアンスが最新のソフトウェアにアップグレードされると、ネットワーク全体で HA スイッチオーバーがトリガーされます。スタンバイアプライアンス（最新のソフトウェアがインストールされている）がアクティブになります。

ステップ**-2**: 古いソフトウェアバージョンを使用している現在のスタンバイアプライアンスは最新のソフトウェアにアップグレードされ、引き続きスタンバイモードで動作します。

このソフトウェアのアップグレードプロセスでは、他のすべての非 HA サイトも最新のソフトウェアでアクティブ化されます。

詳細については、FAQを参照してください。

アップグレードの状況を確認するには、**Deployment Tracker** > 現在のデプロイに移動してください。



- ステージ:「ステージ」をクリックして、ネットワーク内のすべてのアプライアンスに設定ファイルを配布します。デフォルトでは、Citrix SD-WAN Orchestrator サービスは、すべての制御ノード（MCN、RCN、Geo MCN、Geo RCN）とオンラインブランチアプライアンスがステージングされるのを待ってから、ユーザーがアクティブ化できるようにします。
- 有効化:「有効化」をクリックして、ネットワーク上のすべてのサイトで段階的構成を有効にします。
- 以前のバージョンを復元**:**「以前のバージョンを復元」をクリックすると、ネットワーク上で以前にアクティブ化された構成に戻ります。HA ニアヒットレスソフトウェアアップグレードは、以前にアクティブだったバージョンが単なるソフトウェアバージョン変更であり、設定の変更ではない場合、以前のバージョンを復元するときに適用されます。この機能の詳細については、「以前のバージョンを復元する」を参照してください。
- 未完了を無視: 選択すると、すべてのオンライン制御ノード (MCN、RCN、Geo MCN、Geo RCN) がステージングされた後にのみ、アクティブ化チェックボックスが有効になります。オンラインブランチアプライアンスの一部がステージングされていない場合でも、アクティベーションを選択できます。ステージングに失敗したオンラインブランチアプライアンスは無視されます。

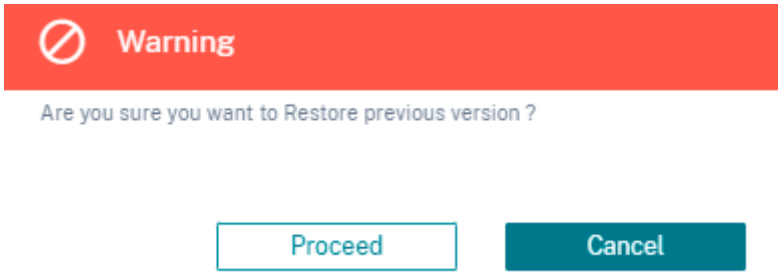
構成のみの更新の場合、構成が変更されたサイトのみがステージングされ、アクティブ化されます。残りのサイトでは、タイムスタンプが更新され、処理されます。「不要」列には、構成の変更がないサイトの数が表示されます。

ソフトウェアバージョンを変更する場合、構成とソフトウェアパッケージの両方がネットワーク内のすべてのサイトでステージングされ、アクティブ化されます。

以前のバージョンを復元

以前のバージョンの復元機能では、Citrix SD-WAN Orchestrator サービスが以前の構成のネットワーク全体のアクティブ化を開始し、ネットワーク上で以前にアクティブ化された構成（および/またはソフトウェア）を復元します。

[以前のバージョンを復元] オプションを選択すると、次の確認メッセージが表示されます。



> 注:
>
> ネットワークがステージングされていない状態でも、以前のバージョンを復元するアクションを実行できます。このオプションはステージングされたネットワークでは無効です。

構成とソフトウェアのアップグレードの自動修正

Citrix SD-WAN Orchestrator サービスでは、変更管理ワークフローに自動修正機能が実装されています。

1 つのサイトでステージングが失敗し、ステージングに失敗したサイトがコントロールノードの場合は、ステージングの失敗メッセージを取得した後に再ステージングする必要があります。コントロールノードのステージングが失敗した場合、「**Activate** 」ボタンは有効になりません。ステージングに失敗したサイトがブランチノードの場合でも、アクティベーションを進めることができます。しかし、そのブランチをネットワークと同期させるには、別の変更管理を実行します。

> 注
>
> - 自動修正チェックは、[アクティブ化] ボタンがクリックされた後にのみ開始され、Citrix SD-WAN Orchestrator サービス UI から次の段階が発行されると停止します。
> - メンテナンスモード機能は、自動修正機能にのみ適用されます。** ステージングとアクティベーションを開始すると **、メンテナンスモードが有効になっているアプライアンスもソフトウェアと構成の変更を反映して更新されます。

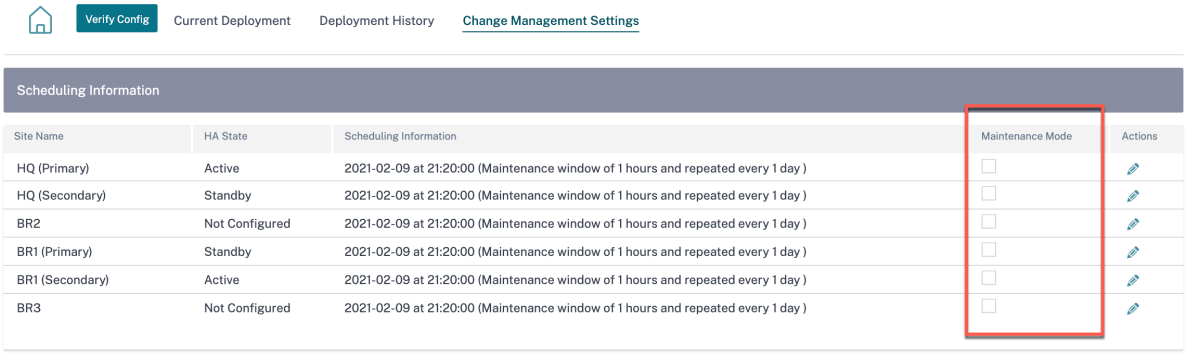
自動修正機能の拡張により、ステージング障害が発生すると、自動修正メカニズムは、予想されるソフトウェアおよび設定バージョンを障害が発生したブランチにプッシュし、現在のネットワークと同期して起動しようとします。自動修正機能は、ブランチノードでのステージングの失敗および任意のノードでのアクティブ化の失敗に適用されます。

自動補正の開始時の 2 つのトリガーポイントは次のとおりです。

- Citrix SD-WAN Orchestrator サービスデプロイメントトラッカー UI では、「ステージング失敗」または「アクティベーション失敗」メッセージが表示されると、自動修正がバックグラウンドで実行を開始します。アクティベーションが完了すると、自動修正チェックが開始されます。
- ソフトウェアと構成が一致せず、アプライアンスが期待どおりのソフトウェアと構成バージョンを作成しなかった場合、Citrix SD-WAN Orchestrator サービスは実際に必要なソフトウェアと構成のコピーをアプライ

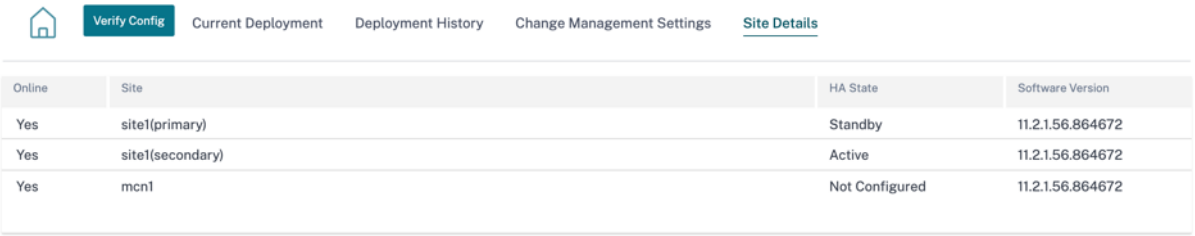
アンスにプッシュしてアクティベーションを開始します。

アプライアンスを手動でトラブルシューティングするには、変更管理設定の下のメンテナンスモードチェックボックスを有効にします。このチェックボックスは、デバイスを自動修正のためにチェックする必要があるかどうかを制御するために使用されます。メンテナンスモードのチェックボックスをオフにすると、自動修正により、アプライアンスはネットワークソフトウェアおよび構成バージョンと同期します。



サイトの詳細

Deployment Tracker の下の [サイトの詳細] タブには、ネットワーク内のすべてのデバイスに関する情報が表示されます。この表には、アプライアンス名、Citrix SD-WAN Orchestrator サービスの接続、高可用性（HA）の状態、および現在実行中のソフトウェアバージョンが含まれています。



構成を確認する

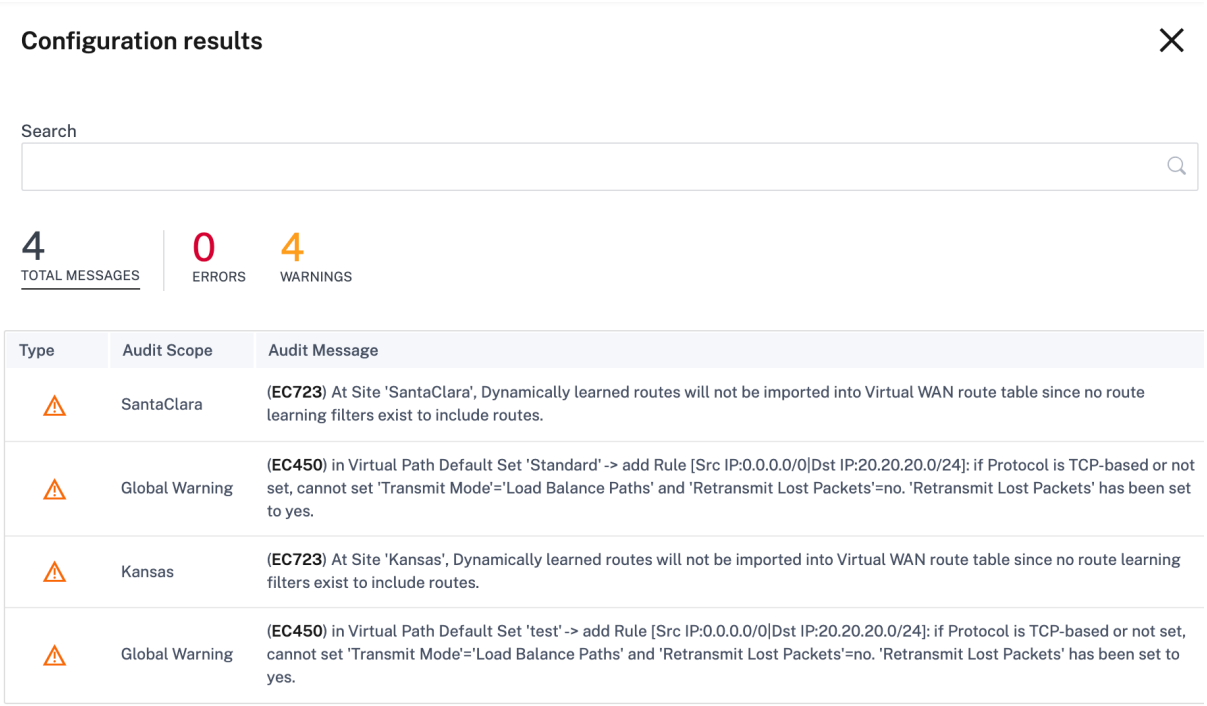
「**Verify Config** 」をクリックすると、ネットワーク構成を検証し、監査エラーや警告がないかどうかを確認できます。「構成を確認」をクリックすると、構成結果ページが表示されます。このページには、監査エラーと警告の詳細が含まれています。

構成結果には、監査エラーと警告の総数が表示されます。また、結果は監査タイプ (エラーまたは警告) に基づいてフィルタリングされ、さまざまなカラーコードで表示されます。数字のリンクをクリックすると、フィルタリングされた結果が表示されます。

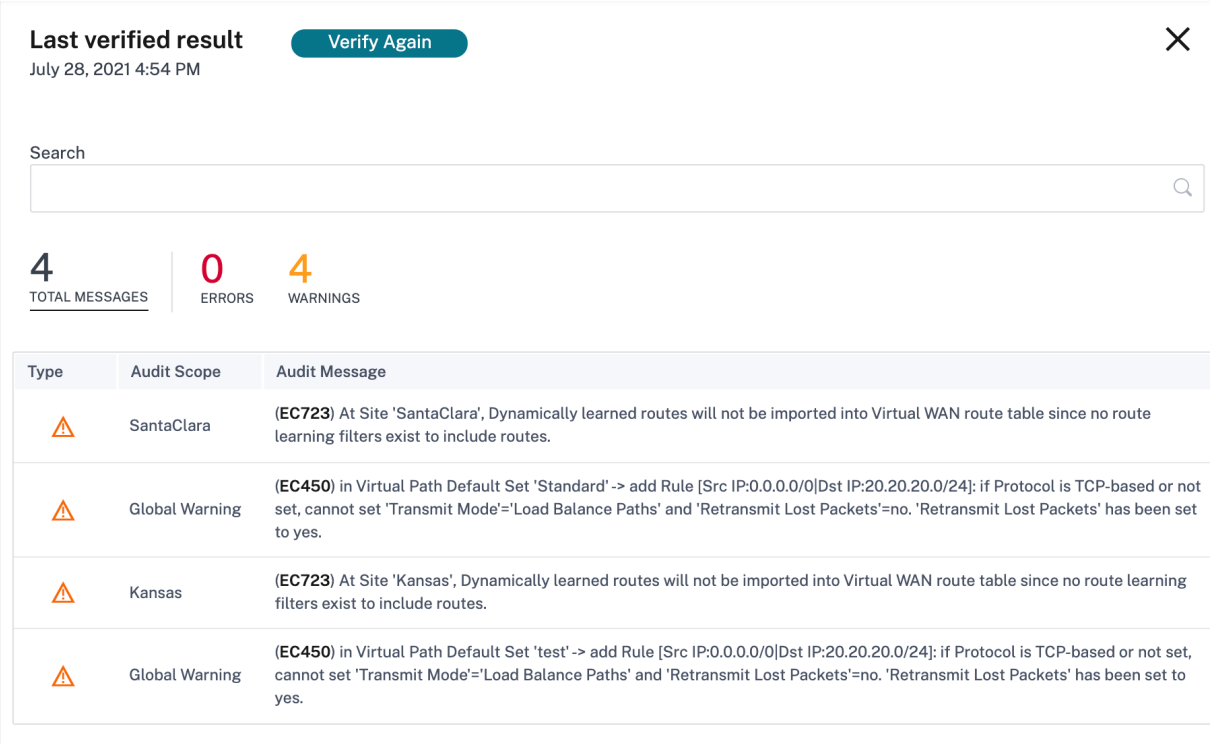
タイプ列には、エラーか警告かを示すアイコンが表示されます。「監査範囲」列では、エラーまたは警告がサイトに関するものか、ネットワークレベルのものかを指定します。エラーまたは警告がサイトに固有のものである場合は、サ

イトの名前が表示されます。エラーまたは警告がグローバルレベルの場合、** グローバルエラーまたはグローバル警告がそれぞれ表示されます ** 。監査メッセージ列には、エラーコードとエラーメッセージが含まれます。

検索バーを使用して、タイプ、エラーコード、サイト名、またはエラーメッセージに基づいて特定のエラーまたは警告を検索できます。



[構成を確認] をもう一度クリックすると、構成の結果ページが開き、構成が最後に検証されたときと同じ結果と日付とタイムスタンプが表示されます。必要に応じて、[再検証] をクリックして検証を再実行できます。



サービス定義

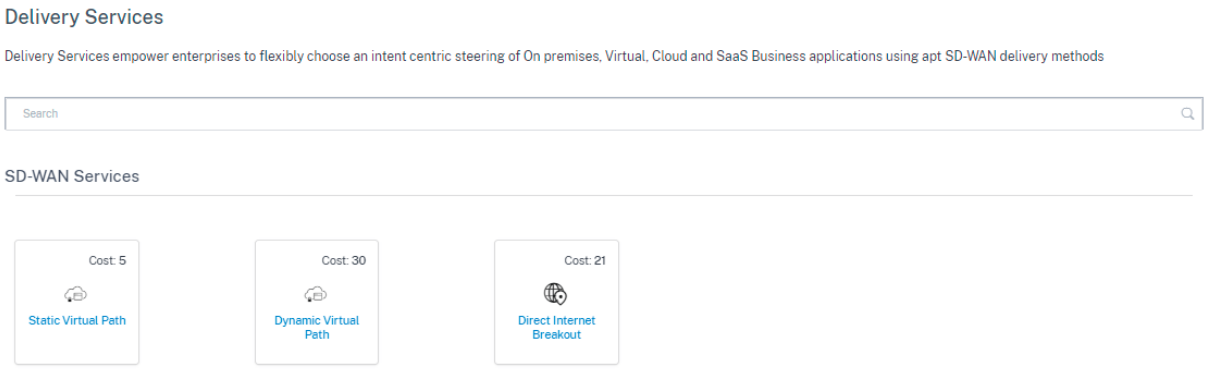
October 26, 2022

配信チャネルは、サービス定義と帯域幅割り当てに大きく分類されます。

配信サービスは、Citrix SD-WAN で利用できる配信メカニズムであり、ビジネスの目的に応じて適切な配信方法を使用してさまざまなアプリケーションやトラフィックプロファイルを制御します。インターネット、イントラネット、仮想パス、IPsec、LAN GRE などの配信サービスを構成できます。配信サービスはグローバルに定義され、必要に応じて個々のサイトの WAN リンクに適用されます。

各 WAN リンクは、関連するサービスのすべてまたはサブセットを適用し、すべての配信サービス間で帯域幅の相対共有（%）を設定できます。

仮想パスサービスは、デフォルトですべてのリンクで使用できます。その他のサービスは、必要に応じて追加できます。
デリバリーサービスを設定するには、顧客レベルで [設定] > [配信チャネル] > [サービス定義] に移動します。

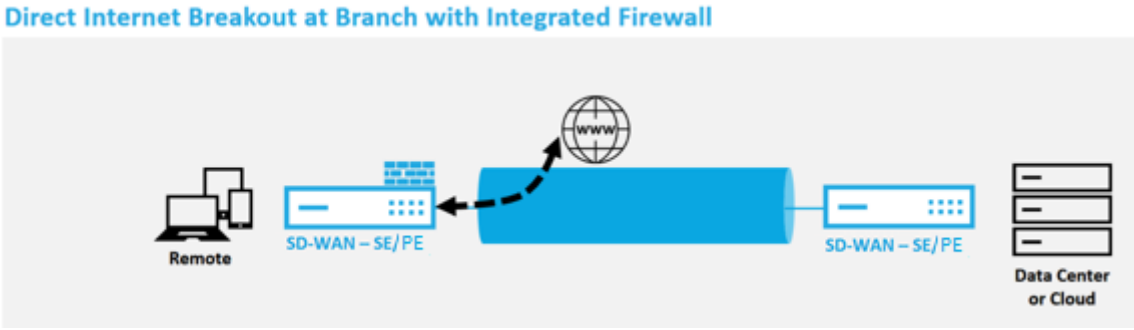


デリバリーサービスは、大きく次のように分類できます。

- 仮想パスサービス:SD-WAN アプライアンスまたは仮想インスタンスをホストする 2 つのサイト間で、安全で信頼性が高く、高品質の接続を提供するデュアルエンドオーバーレイ SD-WAN トンネルです。各仮想パスの最小予約帯域幅を Kbps 単位で設定します。この設定は、ネットワーク内のすべてのサイトのすべての WAN リンクに適用されます。
- インターネットサービス:SD-WAN サイトとパブリックインターネット間の直接チャネル。SD-WAN カプセル化は必要ありません。Citrix SD-WAN は、複数のインターネットリンクにわたるインターネットバウンドトラフィックのセッション負荷分散機能をサポートしています。
- イントラネットサービス:SD-WAN サイトから任意の非 SD-WAN サイトへのリンクベースの接続をアンダーレイします。トラフィックはカプセル化されていないか、IPSec、GRE などの非仮想パスカプセル化を使用できます。複数のイントラネットサービスを設定できます。

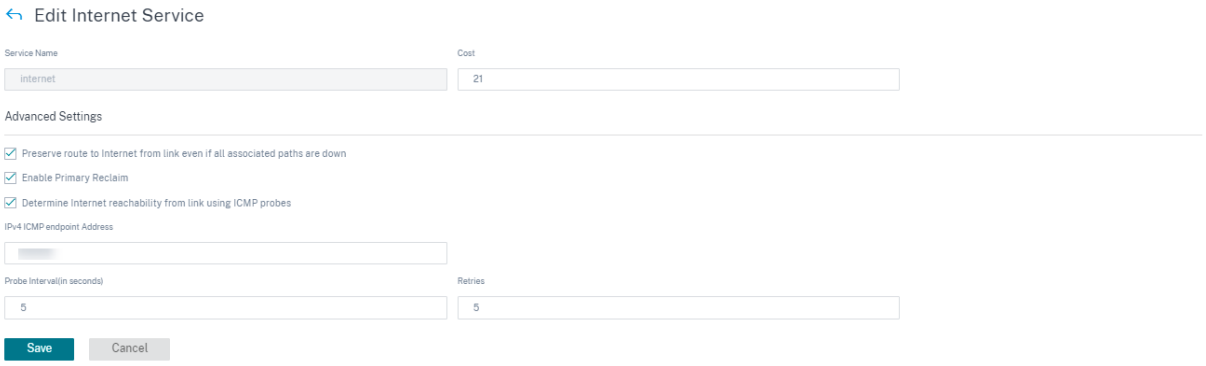
インターネットサービス

インターネットサービスは、配信サービスの一部としてデフォルトで利用できます。インターネットサービスを設定するには、顧客レベルから [設定] > [配信チャネル] > [サービス定義] に移動します。**SD-WAN** サービスセクションで、ダイレクトインターネットブレイクアウトタイルを選択し、[追加] をクリックします。



次のインターネットサービスを構成できます。

- 関連するすべてのパスがダウンしても、リンクからインターネットへのルートを保存: インターネットサービスのルートコストを他の配信サービスと比較して設定できます。このサービスを使用すると、関連するすべてのパスがダウンしても、リンクからインターネットへのルートを維持できます。WAN リンクに関連付けられているパスがすべて停止した場合、SD-WAN アプライアンスはこのルートを使用してインターネットトラフィックを送受信します。
- **ICMP** プローブを使用して、リンクからインターネットへの到達可能性を判断する: インターネット上の明示的なサーバーへの特定のインターネット WAN リンクの ICMP プローブを有効にできます。ICMP プローブ設定を使用すると、SD-WAN アプライアンスは、リンクのメンバーパスが稼働しているか、サーバーから ICMP プローブ応答を受信したときに、インターネットリンクを起動中として扱います。
- **IPv4 ICMP** エンドポイントアドレス: 宛先 IPv4 アドレスまたはサーバーアドレス。
- プローブ間隔 **(**秒単位**)**: SD-WAN アプライアンスがインターネットに設定された WAN リンク上でプローブを送信する間隔。デフォルトでは、SD-WAN アプライアンスは 5 秒ごとに設定された WAN リンクにプローブを送信します。
- 再試行:WAN リンクが稼働しているかどうかを判断する前に試行できる再試行の回数。プローブが 3 回連続して失敗すると、WAN リンクは停止していると見なされます。最大リトライ回数は 10 回です。



サポートされている展開モード

インターネットサービスは、次の展開モードで利用できます。

- インライン展開モード（SD-WAN オーバーレイ）

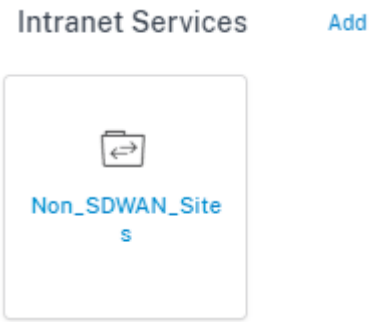
Citrix SD-WAN は、どのネットワークでもオーバーレイソリューションとして導入できます。オーバーレイソリューションとして、SD-WAN は通常、既存の Edge ルータやファイアウォールの背後に展開されます。SD-WAN がネットワークファイアウォールの背後に展開されている場合、インターフェイスを信頼できるものとして構成し、インターネットトラフィックをインターネットゲートウェイとしてファイアウォールに配信できます。

- Edge モードまたは Gateway モード

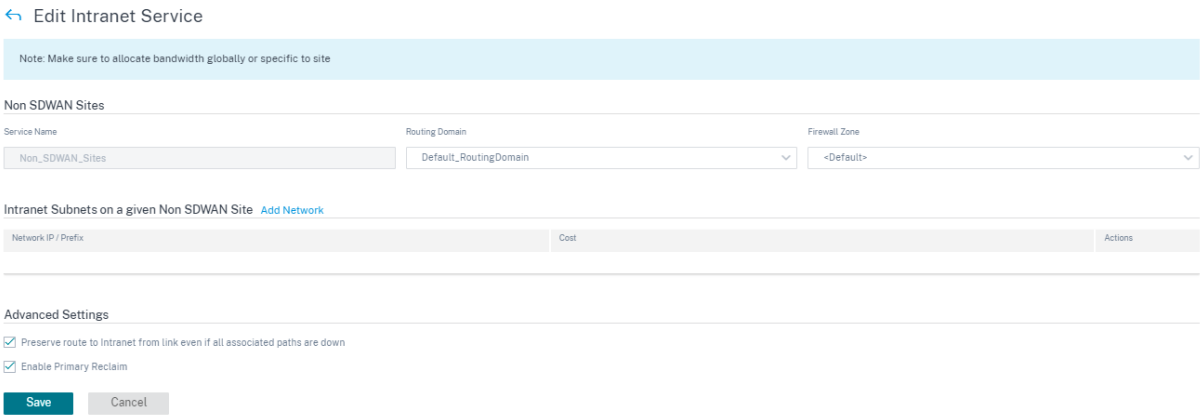
Citrix SD-WAN を Edge デバイスとして展開し、既存の Edge ルーターやファイアウォールデバイスを置き換えることができます。オンボードファイアウォール機能により、SD-WAN は直接インターネット接続からネットワークを保護できます。このモードでは、パブリックインターネットリンクに接続されているインターフェイスが信頼できないように設定され、暗号化が強制的に有効になり、ファイアウォールとダイナミック NAT 機能が有効になり、ネットワークを保護します。

イントラネットサービス

複数のイントラネットサービスを作成できます。イントラネットサービスを追加するには、顧客レベルから [構成] > [配信チャネル] > [サービス定義] に移動します。[イントラネットサービス] セクションで、[追加] をクリックします。



イントラネットサービスをグローバルレベルで作成したら、WAN リンクレベルで参照できます。サービス名を入力し、** 目的のルーティングドメインとファイアウォールゾーンを選択します **。ネットワーク上のすべてのイントラネット IP アドレスを追加します。このアドレスは、ネットワーク内の他のサイトが相互作用する可能性があります。関連するすべてのパスがダウンしている場合でも、リンクからイントラネットへのルートを保持することもできます。

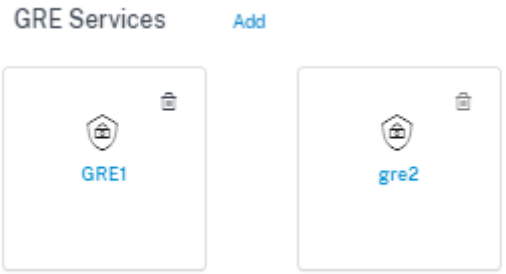


GRE サービス

LAN 上の GRE トンネルを終了するように SD-WAN アプライアンスを設定できます。

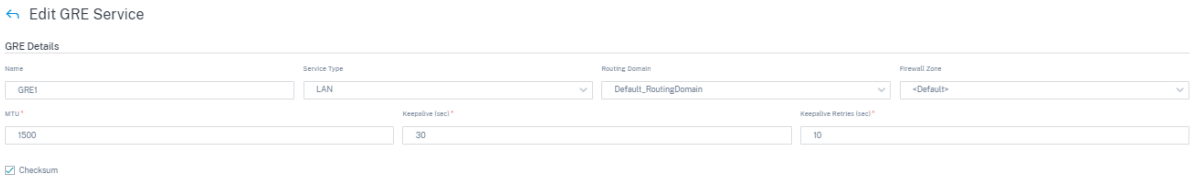
GRE サービスを追加するには、顧客レベルから [設定] > [配信チャネル] > [サービス定義] に移動します。また、設定 **>** セキュリティから GRE サービス設定ページに移動することもできます **。

「**IPsec** と **GRE** 」セクションで、「**IPsec** サービス」に移動し、「追加」をクリックします。



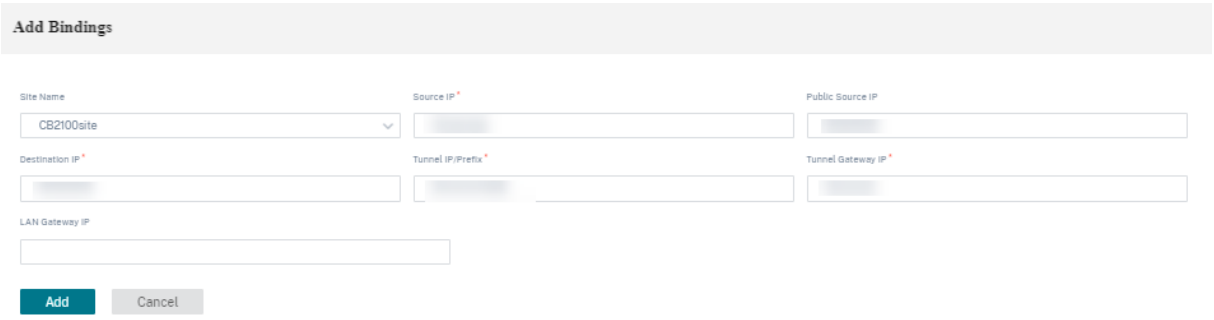
GRE の詳細:

- サービスタイプ:GRE トンネルが使用するサービスを選択します。
- 名前:LAN GRE サービスの名前。
- ルーティングドメイン:GRE トンネルのルーティングドメイン。
- ファイアウォールゾーン: トンネル用に選択されたファイアウォールゾーン。デフォルトでは、トンネルは Default_LAN_Zone に配置されます。
- **MTU**: 最大伝送単位—特定のリンクを介して転送できる最大 IP データグラムのサイズ。指定できる範囲は 576 ～1500 です。デフォルト値は 1500 です。
- キープアライブ: キープアライブメッセージを送信する間隔。0 に設定すると、キープアライブパケットは送信されませんが、トンネルはアップ状態のままです。
- キープアライブ再試行: Citrix SD-WAN アプライアンスがトンネルをダウンさせる前に応答なしでキープアライブパケットを送信する回数。
- チェックサム: トンネルの GRE ヘッダーのチェックサムを有効または無効にします。



サイトバインディング:

- サイト名:GRE トンネルをマッピングするサイト。
- 送信元 **IP**: トンネルの送信元 IP アドレス。これは、このサイトで構成されている仮想インターフェイスの 1 つです。選択したルーティングドメインによって、使用可能な送信元 IP アドレスが決まります。
- パブリックソース **IP**: トンネルトラフィックが NAT を通過する場合の送信元 IP。
- 宛先 **IP**: トンネルの宛先 IP アドレス。
- トンネル **IP/**プレフィックス:GRE トンネルの IP アドレスとプレフィックス。
- トンネルゲートウェイ **IP**: トンネルトラフィックをルーティングするネクストホップ IP アドレス。
- **LAN** ゲートウェイ **IP**: LAN トラフィックをルーティングするネクストホップ IP アドレス。



IPSec サービス

Citrix SD-WAN アプライアンスは、LAN または WAN 側のサードパーティのピアと固定 IPSec トンネルをネゴシエートできます。トンネルのエンドポイントを定義し、サイトをトンネルエンドポイントにマッピングできます。

セキュリティプロトコルと IPsec 設定を定義する IPsec セキュリティプロファイルを選択して適用することもできます。

仮想パス IPsec 設定を構成するには、次の手順を実行します。

- FIPS 準拠が必要なすべての仮想パスに対して、仮想パス IPSec トンネルを有効にします。
- IPsec モードを AH または ESP+ 認証に変更してメッセージ認証を構成し、FIPS 承認ハッシュ機能を使用します。SHA1 は FIPS によって受け入れられますが、SHA256 を強く推奨します。
- IPsec ライフタイムは、8 時間（28,800 秒）以下に設定する必要があります。

Citrix SD-WAN は、事前共有キーを備えた IKE バージョン 2 を使用して、次の設定を使用して仮想パスを介した IPSec トンネルをネゴシエートします。

- DH グループ 19: キーネゴシエーションのための ECP256 (256 ビット楕円曲線)
- 256 ビット AES-CBC 暗号化
- メッセージ認証のための SHA256 ハッシュ
- メッセージの整合性のための SHA256 ハッシュ
- DH Group 2: MODP-1024 Perfect Forward Secrecy

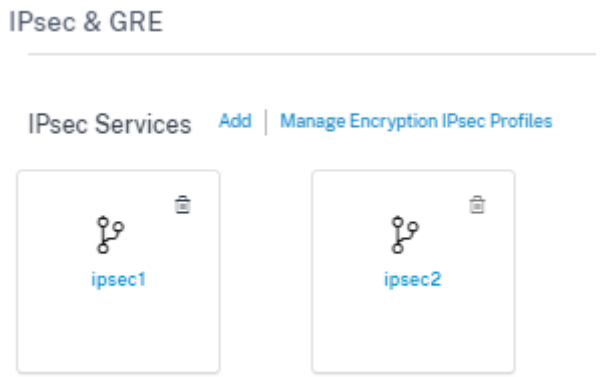
サードパーティの IPsec トンネルを設定するには:

- FIPS 承認済みの DH グループを構成します。グループ 2 と 5 は FIPS では許可されますが、グループ 14 以降を強く推奨します。
- FIPS 承認ハッシュ関数を設定します。SHA1 は FIPS によって受け入れられますが、SHA256 を強くお勧めします。
- IKEv2 を使用する場合は、FIPS 承認の整合性機能を設定します。SHA1 は FIPS によって受け入れられますが、SHA256 を強くお勧めします。
- IKE ライフタイムおよび最大ライフタイムを 24 時間（86,400 秒）以下に設定します。
- IPSec モードを AH または ESP+ 認証に変更して IPSec メッセージ認証を構成し、FIPS 承認ハッシュ機能を使用します。SHA1 は FIPS によって受け入れられますが、SHA256 を強く推奨します。
- IPSec ライフタイムおよび最大ライフタイムを 8 時間（28,800 秒）以内に設定します。

IPsec トンネルの設定

顧客レベルから、[設定] > [配信チャネル] > [サービス定義] に移動します。[構成**] > [**セキュリティ] から [**IPsec** サービス] ページに移動することもできます。

[**IPsec & GRE**] > [**IPsec** サービス] セクションで、[追加] をクリックします。「**IPsec** サービスの編集」ページが表示されます。



1. サービスの詳細を指定します。
    - サービス名:IPsec サービスの名前。
    - サービスタイプ:IPsec トンネルが使用するサービスを選択します。

- ルーティングドメイン:LAN 上の IPsec トンネルの場合は、ルーティングドメインを選択します。IPsec トンネルがイントラネットサービスを使用する場合、イントラネットサービスはルーティングドメインを決定します。
- ファイアウォールゾーン: トンネルのファイアウォールゾーン。デフォルトでは、トンネルは Default_LAN_Zone に配置されます。
- **ECMP** を有効にする:「**ECMP** を有効にする」チェック・ボックスを選択すると、IPsec トンネルの ECMP 負荷分散が有効になります。
- **ECMP** タイプ: 必要に応じて ECMP 負荷分散メカニズムのタイプを選択します。ECMP タイプの詳細については、「ECMP 負荷分散」を参照してください。

2. トンネルエンドポイントを追加します。

   - 名前: サービスタイプがイントラネットの場合は、トンネルが保護するイントラネットサービスを選択します。それ以外の場合は、サービスの名前を入力します。
   - ピア **IP**: リモートピアの IP アドレス。
   - **IPsec** プロファイル: セキュリティプロトコルと IPsec 設定を定義する IPsec セキュリティプロファイル。
   - 事前共有キー: IKE 認証に使用される事前共有キー。
   - ピア事前共有キー： IKEv2 認証に使用される事前共有キー。
   - **ID** データ: 手動 ID またはユーザー FQDN タイプを使用する場合に、ローカル ID として使用されるデータ。
   - ピア **ID** データ: 手動 ID またはユーザ FQDN タイプを使用している場合に、ピア ID として使用されるデータ。
   - 証明書： IKE 認証として [証明書（Certificate）] を選択した場合は、設定された証明書から選択します。

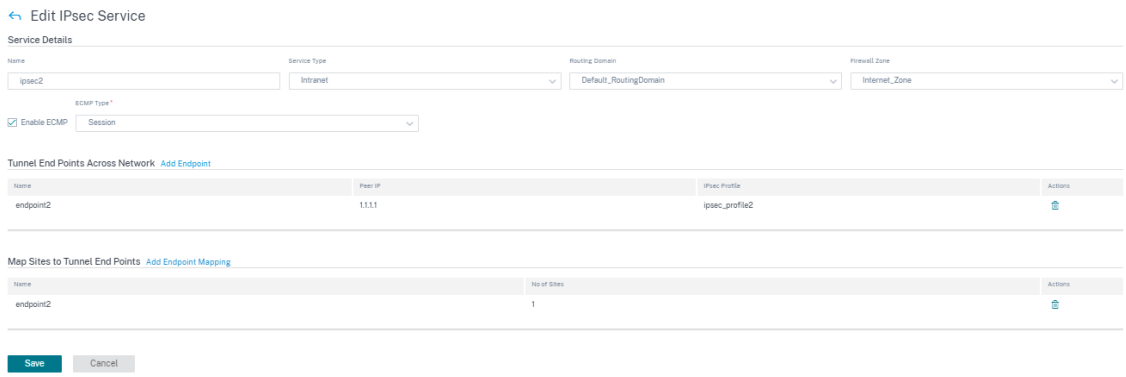
3. サイトをトンネルエンドポイントにマッピングします。

   - エンドポイントの選択: サイトにマッピングされるエンドポイント。
   - サイト名: エンドポイントにマップされるサイト。
   - 仮想インターフェイス名： エンドポイントとして使用されるサイトの仮想インターフェイス。
   - ローカル **IP**: ローカルトンネルエンドポイントとして使用するローカル仮想 IP アドレス。
   - ゲートウェイ **IP**: ネクストホップの IP アドレス。

4. 保護されたネットワークを作成します。

   - 送信元ネットワーク **IP/Prefix**: IPsec トンネルが保護するネットワークトラフィックの送信元 IP アドレスとプレフィックス。
   - 宛先ネットワーク **IP/**プレフィックス:IPsec トンネルが保護するネットワークトラフィックの宛先 IP アドレスとプレフィックス。

5. IPsec 構成がピアアプライアンスにミラーリングされていることを確認します。



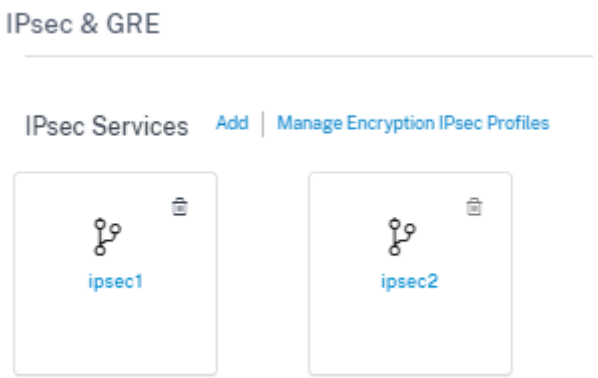
FIPS コンプライアンスの詳細については、「ネットワークセキュリティ」を参照してください。

> 注
>
> オンプレミス向け Citrix SD-WAN Orchestrator は、IPsec を介した Oracle クラウドインフラストラクチャ（OCI）への接続をサポートします。

IPSec 暗号化プロファイル

IPsec 暗号化プロファイルを追加するには、顧客レベルで [設定] > [配信チャネル] > [サービス定義] に移動します。[構成] **>** **[**セキュリティ**]** から IPsec 暗号化プロファイルの設定ページに移動することもできます **。

「**IPsec & GRE** 」セクションで、「暗号化 **IPsec** プロファイルの管理」を選択します。



IPsec は安全なトンネルを提供します。Citrix SD-WAN は IPsec 仮想パスをサポートし、サードパーティデバイスが Citrix SD-WAN WAN アプライアンスの LAN 側または WAN 側で IPsec VPN トンネルを終了できるようにします。140-2 レベル 1 FIPS 認定の IPSec 暗号化バイナリを使用して、SD-WAN アプライアンスで終端するサイト間の IPSec トンネルを保護できます。

また、Citrix SD-WAN は、差別化された仮想パストンネリングメカニズムを使用した耐障害性 IPSec トンネリングもサポートします。

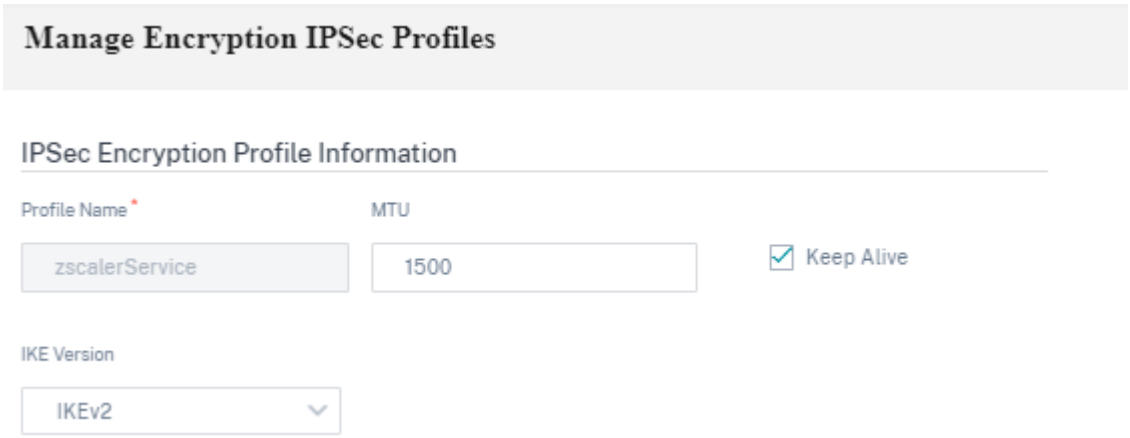
IPsec プロファイルは、IPsec サービスを配信サービスセットとして構成するときに使用されます。IPsec セキュリティプロファイルページで、次の IPsec 暗号化プロファイル、**IKE** 設定、および **IPsec** 設定に必要な値を入力しま

す。

監査エラーを確認するには、「構成を確認」をクリックします。

IPSec 暗号化プロファイル情報:

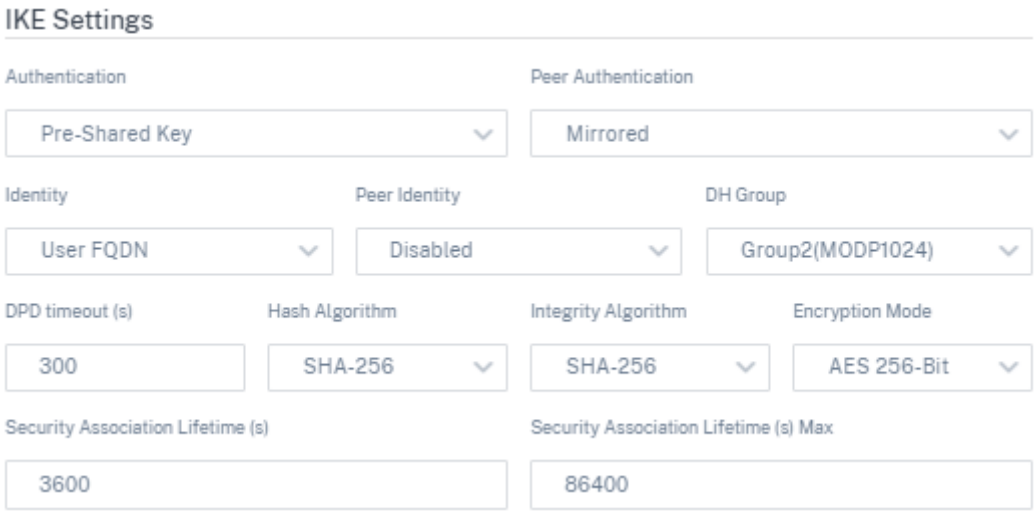
- プロファイル名: プロファイル名を入力します。
- **MTU**: IKE または IPsec の最大パケットサイズをバイト単位で入力します。
- **Keep Alive**: チェックボックスを選択してトンネルをアクティブに保ち、ルートの適格性を有効にします。
- **IKE** バージョン: ドロップダウンリストから IKE プロトコルバージョンを選択します。



IKE 設定

- モード:IKE フェーズ 1 ネゴシエーションモードのドロップダウンリストから [メインモード] または [アグレッシブモード] を選択します。
  - メイン: ネゴシエーション中に潜在的な攻撃者に情報が公開されることはありませんが、アグレッシブモードよりも遅くなります。メインモードは FIPS に準拠しています。
  - **Aggressive**: ネゴシエーション中に一部の情報（ネゴシエーションピアのアイデンティティなど）が潜在的な攻撃者に公開されますが、メインモードよりも高速です。アグレッシブモードは FIPS に準拠していません。
- 認証: ドロップダウンメニューから [証明書] または [事前共有キー] として認証タイプを選択します。
- ピア認証: ドロップダウンリストからピア認証タイプを選択します。
- **ID**: ドロップダウンリストから識別方法を選択します。
- ピアアイデンティティ: ドロップダウンリストからピアアイデンティティの方法を選択します。
- **DH** グループ:IKE キー生成に使用できる Diffie-Hellman (DH) グループを選択します。
- **DPD** タイムアウト:VPN 接続のデッドピア検出タイムアウト (秒単位) を入力します。
- ハッシュアルゴリズム: ドロップダウンリストからハッシュアルゴリズムを選択し、IKE メッセージを認証します。

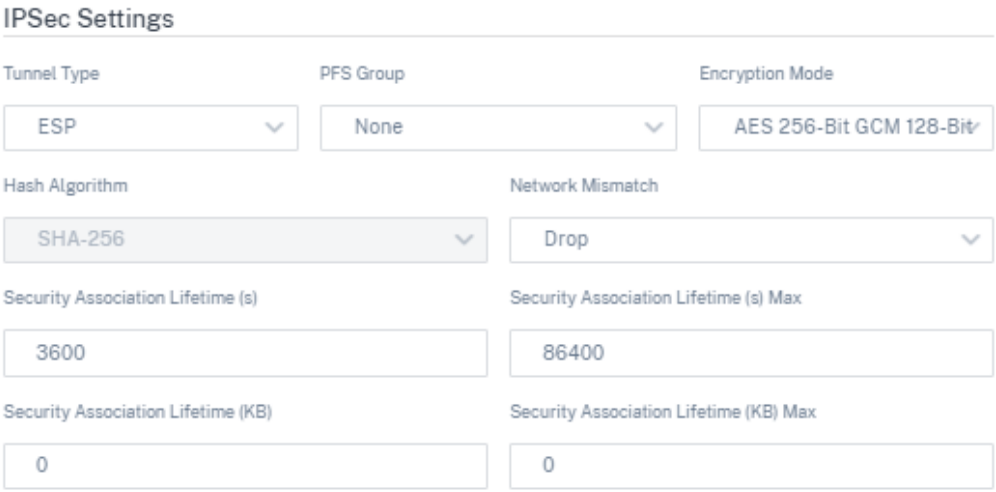
- 整合性アルゴリズム:HMAC 検証に使用する IKEv2 ハッシュアルゴリズムを選択します。
- 暗号化モード: ドロップダウンリストから IKE メッセージの暗号化モードを選択します。
- セキュリティアソシエーションの有効期間:IKE セキュリティアソシエーションが存在するまでの時間を秒単位で入力します。
- セキュリティアソシエーションの最大有効期間:IKE セキュリティアソシエーションが存続できる最大時間を秒単位で入力します。



IPSec の設定

- トンネルタイプ: ドロップダウンリストからトンネルのカプセル化タイプとして **ESP**、**ESP+Auth**、**ESP+NULL**、または **AH** を選択します。これらは、FIPS 準拠と非 FIPS 準拠のカテゴリの下にグループ化されています。
  - **ESP**: ユーザーデータのみを暗号化します
  - **ESP+Auth**: ユーザーデータを暗号化し、HMAC を含めます
  - **ESP+NULL**: パケットは認証されるが暗号化されていない
  - **AH**: HMAC のみが含まれています
- **PFS** グループ: パーフェクトフォワードシークレットキー生成に使用する Diffie-Hellman グループをドロップダウンメニューから選択します。
- 暗号化モード: ドロップダウンメニューから IPsec メッセージの暗号化モードを選択します。
- ハッシュアルゴリズム:MD5、SHA1、および SHA-256 ハッシュアルゴリズムは、HMAC 検証に使用できます。
- ネットワークの不一致: パケットが IPsec トンネルの保護対象ネットワークと一致しない場合に実行するアクションをドロップダウンメニューから選択します。

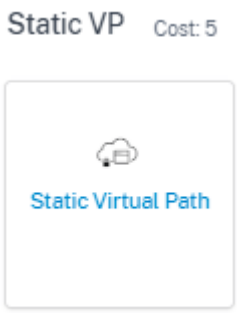
- セキュリティアソシエーションの有効期間:IPsec セキュリティアソシエーションが存在するまでの時間 (秒単位) を入力します。
- セキュリティアソシエーションの最大有効期間:IPsec セキュリティアソシエーションが存在できる最大時間 (秒単位) を入力します。
- セキュリティアソシエーションの有効期間 **(KB)**: IPsec セキュリティアソシエーションが存在するデータ量 (KB 単位) を入力します。
- セキュリティアソシエーションの最大有効期間 **(KB)**: IPsec セキュリティアソシエーションが存在できる最大データ量 (KB 単位) を入力します。



静的仮想パス

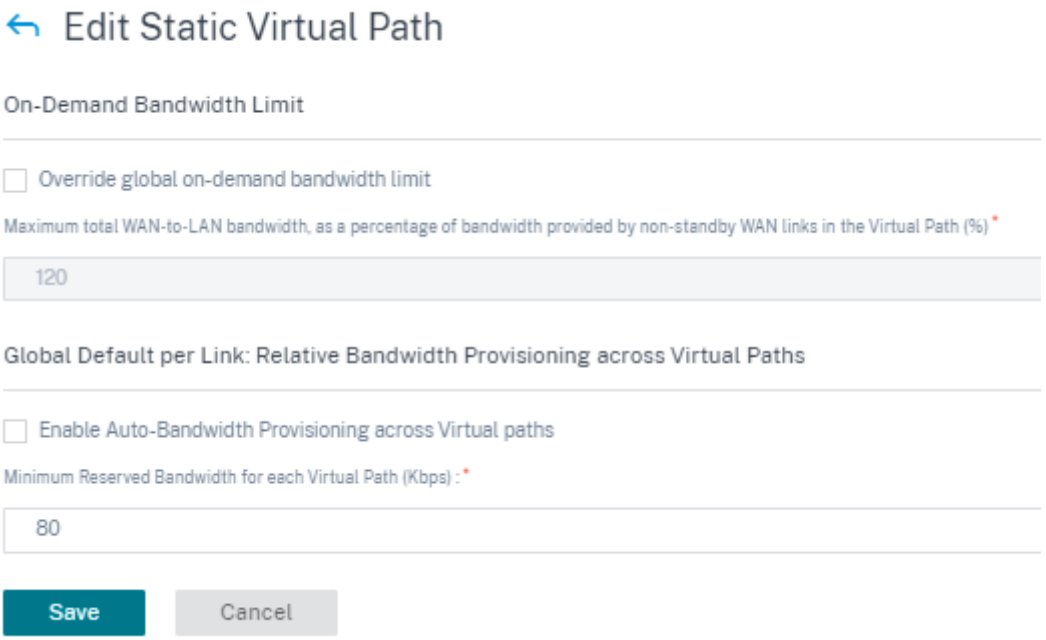
仮想パスの設定は、グローバルな WAN リンク自動パス設定から継承されます。これらの構成を上書きし、メンバーパスを追加または削除できます。サイトおよび適用された QoS プロファイルに基づいて、仮想パスをフィルタリングすることもできます。WAN リンクの状態を判断するために ping を送信できる WAN リンクのトラッキング IP アドレスを指定します。逆方向パスの状態を特定するために ping を実行できるリバースパスのリバーストラッキング IP を指定することもできます。

静的仮想パスを設定するには、顧客レベルで [構成] > [配信チャネル] に移動し、[静的仮想パス] タイルをクリックします。



サポートされている設定の一部を次に示します。

- オンデマンド帯域幅リスト:
  - グローバルオンデマンド帯域幅制限の上書き: 有効にすると、グローバル帯域幅制限値がサイト固有の値に置き換えられます。
  - 仮想パス内の非スタンバイ **WAN** リンクが提供する帯域幅のパーセンテージで表した **WAN-to-LAN** の最大帯域幅 **(%)**: 最大帯域幅制限を% で更新します。
- リンクごとのグローバルデフォルト**:** 仮想パス間の相対帯域幅 **Provisioning**:
  - 仮想パス全体にわたる自動帯域幅 **Provisioning** を有効にする: 有効にすると、リモートサイトで消費される帯域幅の大きさに応じて、すべてのサービスの帯域幅が自動的に計算され、適用されます。
  - 各仮想パスの最小予約帯域幅 **(Kbps)**: すべての WAN リンク上の各サービス専用に予約される最大帯域幅。

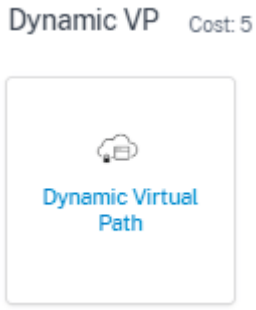


動的仮想パスの設定

グローバル動的仮想パス設定を使用すると、管理者はネットワーク全体で動的仮想パスのデフォルトを構成できます。

動的仮想パスは、2 つのサイト間で動的にインスタンス化され、中間 SD-WAN ノードホップなしで直接通信が可能になります。同様に、動的仮想パス接続も動的に削除されます。動的仮想パスの作成と削除は、帯域幅のしきい値と時間設定に基づいてトリガーされます。

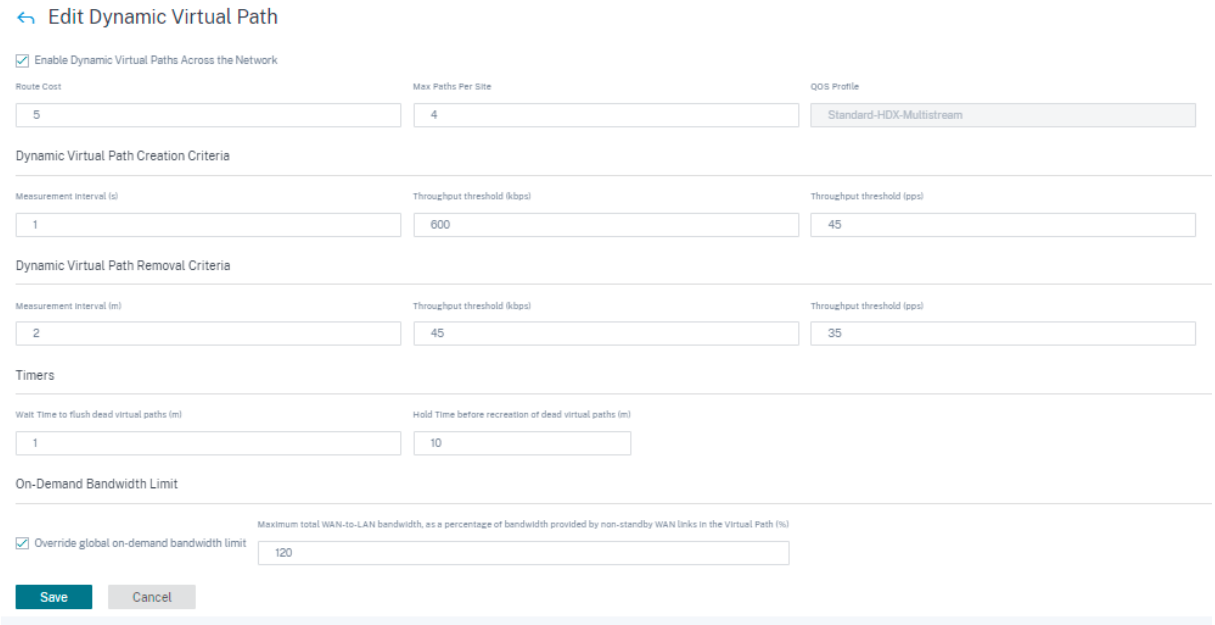
動的仮想パスを設定するには、顧客レベルから [設定] > [配信チャネル] > [サービス定義] に移動し、[動的仮想パス] タイルをクリックします。



サポートされている設定の一部を次に示します。

- ネットワーク経由の動的仮想パスを有効または無効にするためのプロビジョニング
- 動的仮想パスのルートコスト
- 使用する QoS プロファイル—デフォルトでは標準。
- 動的仮想パス作成基準:
  - 測定間隔 **(秒)**: 2 つのサイト間 (この場合は特定のブランチとコントロールノードの間) に動的仮想パスを作成する必要があるかどうかを判断するために、パケット数と帯域幅を測定する時間です。
  - スループットしきい値 **(kbps)**: 動的仮想パスがトリガーされる測定間隔で測定された、2 つのサイト間の合計スループットのしきい値。この場合、しきい値はコントロールノードに適用されます。
  - スループットしきい値 **(pps)** - 動的仮想パスがトリガーされる測定間隔で測定された、2 つのサイト間の合計スループットのしきい値。
- 動的仮想パス削除基準:
  - 測定間隔（分）: 2 つのサイト間（この場合は特定のブランチとコントロールノードの間）で動的仮想パスを削除する必要があるかどうかを判断するために、パケット数と帯域幅を測定する時間。
  - スループットしきい値 **(kbps)** - 測定間隔で測定された 2 つのサイト間の合計スループットのしきい値。このしきい値に達すると、動的仮想パスは削除されます。
  - スループットしきい値 **(pps)** - 測定間隔で測定された 2 つのサイト間の合計スループットのしきい値。このしきい値に達すると、動的仮想パスは削除されます。

- タイマー
  - 使用されていない仮想パスをフラッシュするまでの待機時間 **(m)**: 使用していない動的仮想パスが削除されるまでの時間。
  - 使用されていない仮想パスを再作成するまでの待機時間 **(m):** 使用停止状態になったために削除された動的仮想パスを再作成できるようになるまでの時間。
- オンデマンド帯域幅リスト
  - グローバルオンデマンド帯域幅制限の上書き: 有効にすると、グローバル帯域幅制限値がサイト固有の値に置き換えられます。
  - 仮想パス内の非スタンバイ **WAN** リンクが提供する帯域幅のパーセンテージで表した **WAN-to-LAN** の最大帯域幅 **(%)**: 最大帯域幅制限を% で更新します。



監査エラーを確認するには、「構成を確認」をクリックします。

ルーティング

October 26, 2022

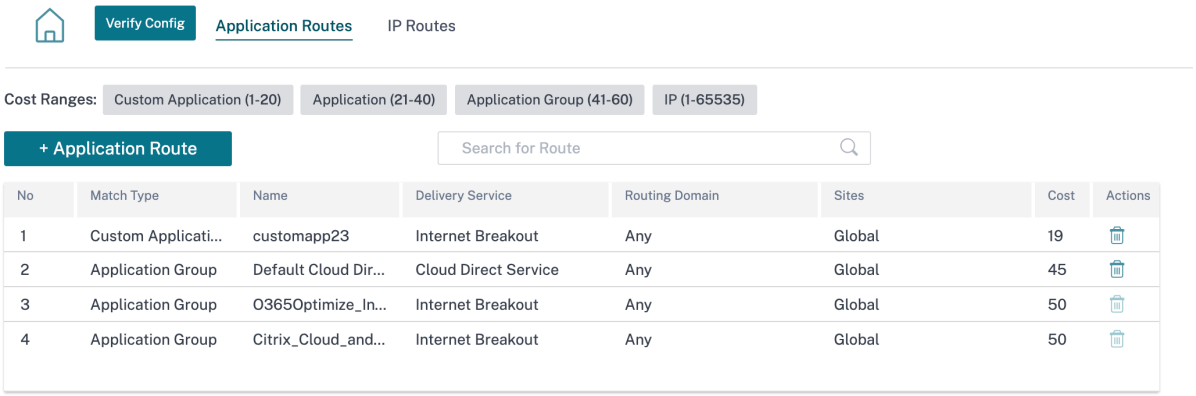
ルーティングセクションには次のオプションがあります。

- ルーティングポリシー
- ルート集約
- ルーティングドメイン
- ルートプロファイルのインポート

- ルートプロファイルのエクスポート
- トランジットノード

ルーティングポリシー

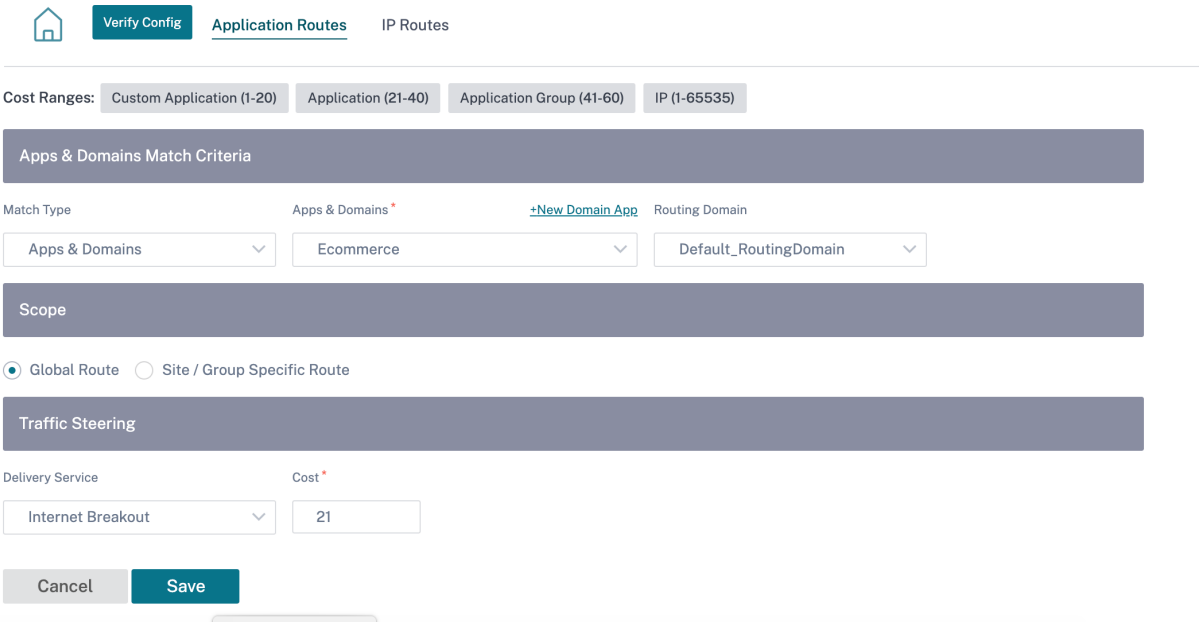
ルーティングポリシーは、トラフィックステアリングを有効にするのに役立ちます。選択（アプリケーションルートと IP ルート）に基づいて、さまざまな方法でトラフィックを誘導できます。



アプリケーションルート

[**+** アプリケーションルート] をクリックして、アプリケーションルートを作成します。

- カスタムアプリケーション一致基準:
  - マッチタイプ: ドロップダウンリストからアプリケーション/カスタムアプリケーション/アプリケーショングループとしてマッチタイプを選択します。
  - アプリケーション: リストからアプリケーションを 1 つ選択します。
  - ルーティングドメイン: ルーティングドメインを選択します。
- スコープ: グローバルレベルまたはサイトおよびグループ固有のレベルでアプリケーションルートをスコープできます。
- トラフィックステアリング;
  - 配送サービス: 一覧から配送サービスを 1 つ選択します。
  - コスト: 各ルートの相対的な優先順位を反映します。コストを低くすると、優先順位が高くなります。
- パスに基づく資格:
  - パスを追加: サイトと WAN リンクを選択します。選択したパスがダウンした場合、アプリケーションルートはトラフィックを受信しません。

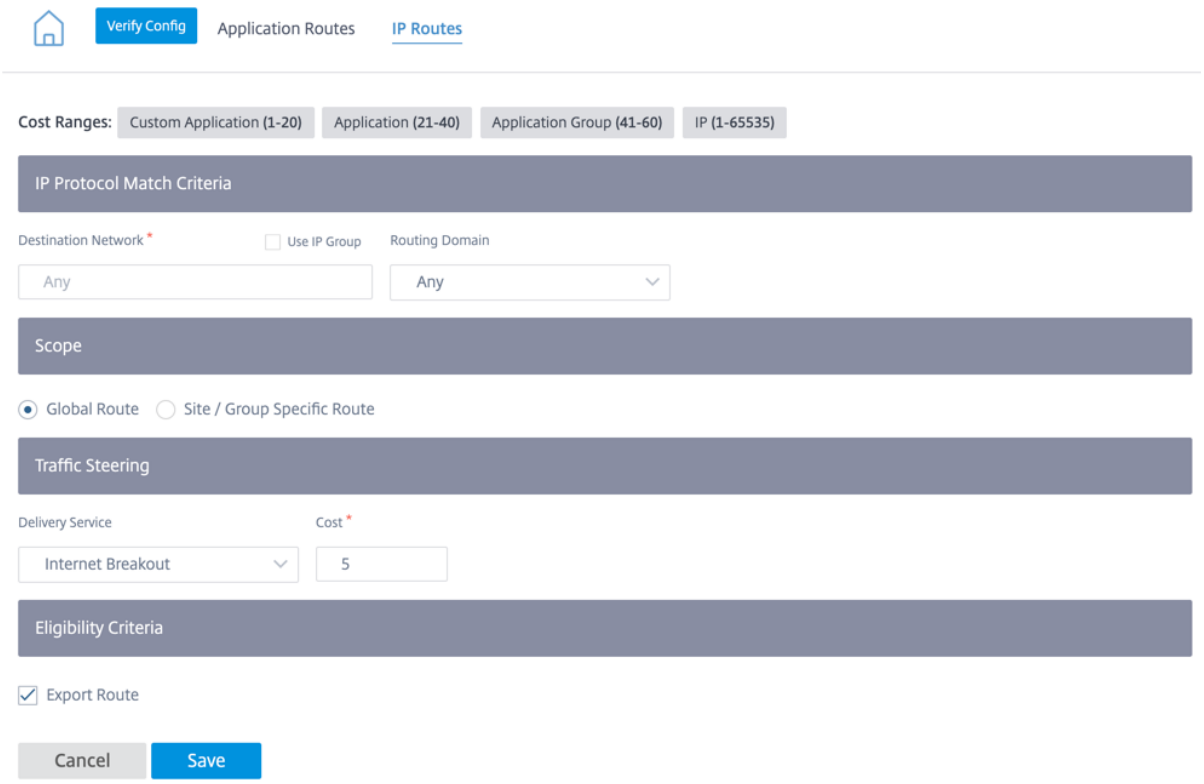


新しいアプリケーションルートが追加された場合、ルートコストは次の範囲内にある必要があります。

- カスタムアプリケーション:1 ～20
- アプリケーション:21—40
- アプリケーショングループ:41—60

IP ルート

[**IP** ルート] タブに移動し、[**+ IP Route** to IP Route] ポリシーをクリックしてトラフィックを誘導します。



- **IP** プロトコル一致基準:
  - 宛先ネットワーク: パケットの転送に役立つ宛先ネットワークを追加します。
  - **IP** グループを使用する: 宛先ネットワークを追加するか、[**IP** グループを使用] チェックボックスをオンにしてドロップダウンリストから任意の IP グループを選択できます。
  - ルーティングドメイン: ドロップダウンリストからルーティングドメインを選択します。
- スコープ: グローバルレベルまたはサイトおよびグループ固有のレベルで IP ルートをスコープできます。
- トラフィックステアリング:
  - 配信サービス: ドロップダウンリストから配信サービスを 1 つ選択します。
  - コスト: 各ルートの相対的な優先順位を反映します。コストを低くすると、優先順位が高くなります。

  新しい IP ルートを追加する場合、ルートコストは 1 ～20 の範囲でなければなりません。
- 適格基準:
  - ルートのエクスポート:「ルートのエクスポート」チェックボックスが選択されていて、ルートがローカルルートの場合、ルートはデフォルトでエクスポートできます。ルートがイントラネット/インターネットベースのルートの場合、エクスポートが機能するには、WAN から WAN への転送を有効にする必要があります。**Export Route** チェックボックスがオフになっている場合、ローカルルートは他の SD-WAN へのエクスポートに適さず、ローカルな意味を持ちます。
- パスに基づく資格:

- パスを追加: サイトと WAN リンクを選択します。追加されたパスがダウンした場合、IP ルートはトラフィックを受信しません。

監査エラーを確認するには、「構成を確認」をクリックします。

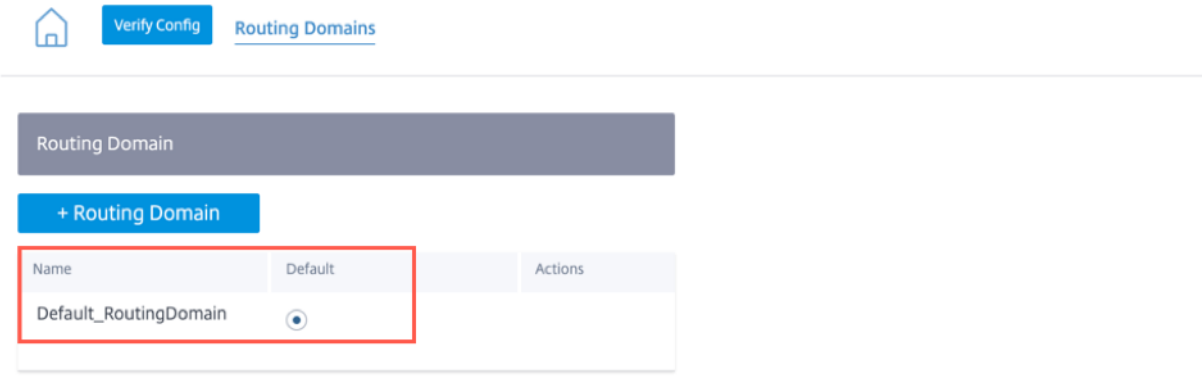
ルート集約

ルート集約により、ルータが維持する必要のあるルートの数が減少します。サマリールートは、複数のルートを表すために使用される 1 つのルートです。1 つのルートアドバタイズメントを送信することで帯域幅を節約し、ルータ間のリンク数を削減します。1 つのルートアドレスだけが維持されるため、メモリを節約できます。CPU リソースは、再帰的なルックアップを避けることによって、より効率的に使用されます。ゲートウェイの IP アドレスを指定せずにサマリールートを追加できます。

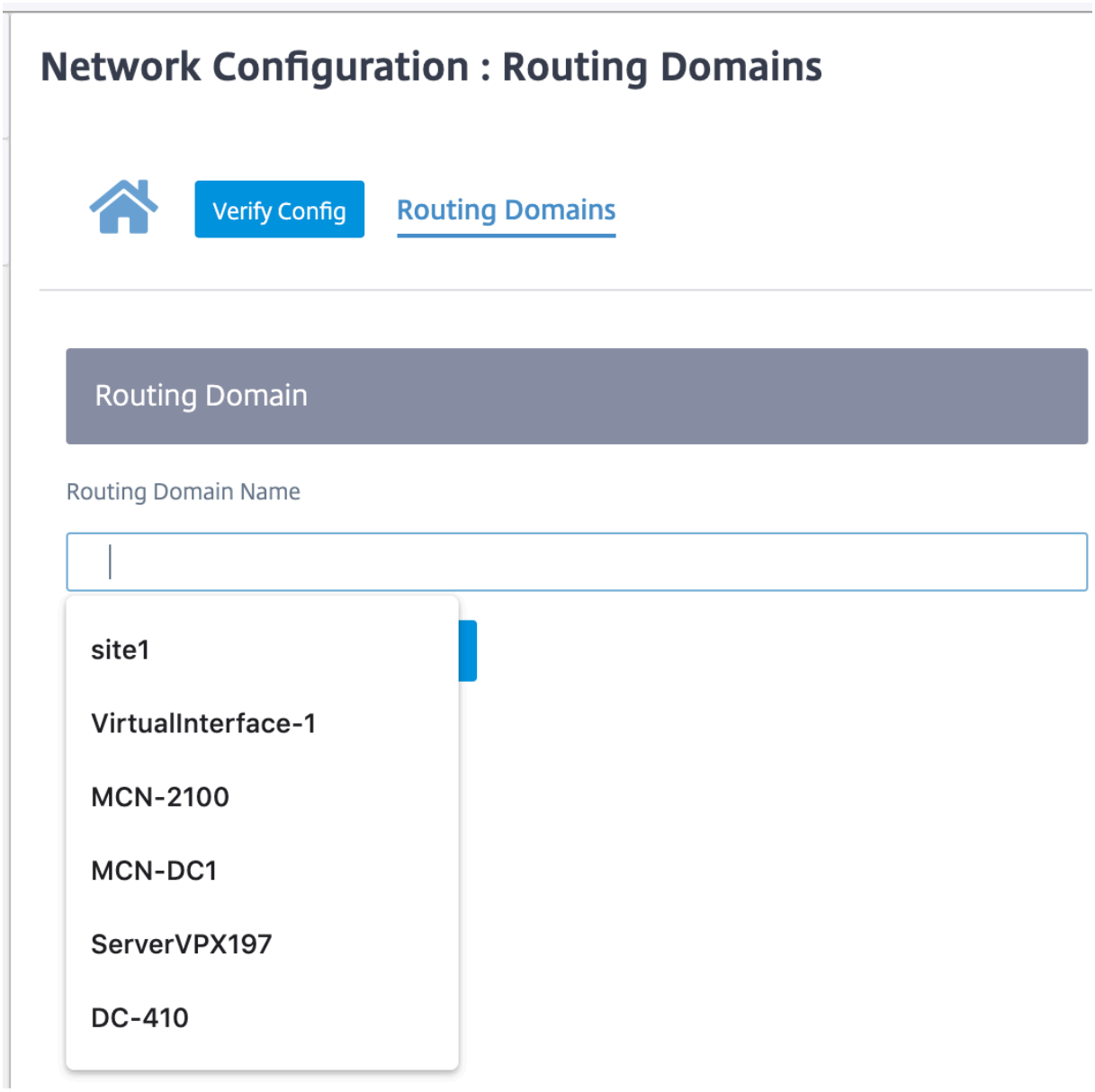
ルーティングドメイン

ルーティングドメインは、VLAN を介してトラフィックを分離するために使用されます。ルーティングドメインを作成したら、グローバルレベル (イントラネットサービスの場合) またはインターフェイスレベルで参照できます。

すべてのサイトに適用されるデフォルトのルーティングドメインを選択することもできます。



特定のルーティングドメインからのルートを照合するには、「**+ Routing Domain** 」をクリックし、ドロップダウンリストから設定されているルーティングドメインのいずれかを選択します。［保存］をクリックします。



監査エラーを確認するには、「構成を確認」をクリックします。

詳細については、「ルーティングドメイン」を参照してください。

ルーティング間ドメインサービス

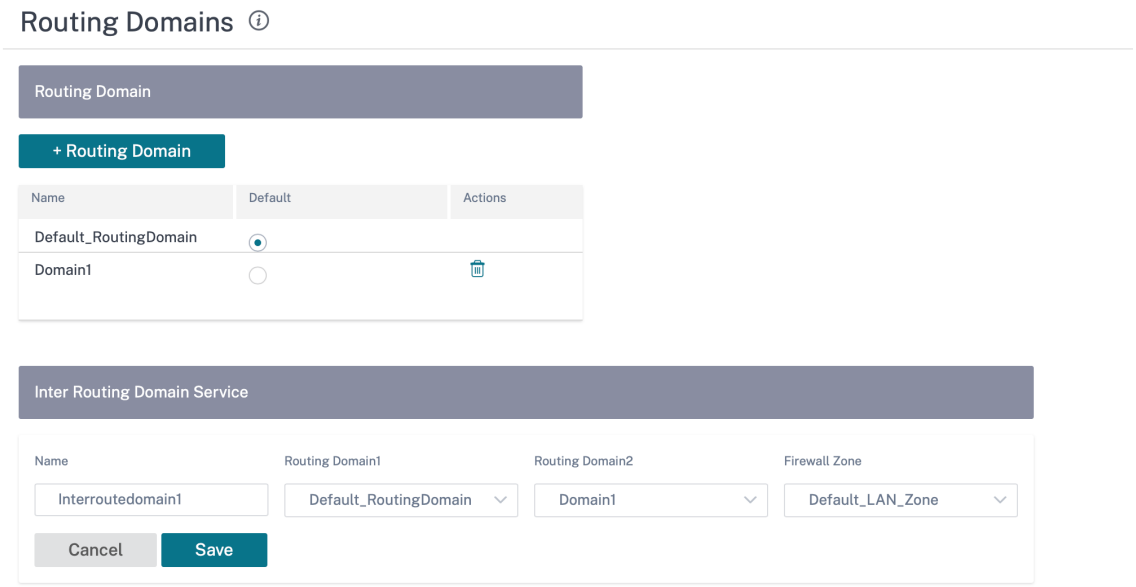
オンプレミス向け Citrix SD-WAN Orchestrator は、静的ルーティングドメイン間サービスを提供し、サイト内のルーティングドメイン間または異なるサイト間のルートリークを可能にします。これにより、Edge ルータがルートリークを処理する必要がなくなります。さらに、Inter-VRF ルーティングサービスを使用して、ルート、ファイアウォールポリシー、および NAT 規則を設定できます。

詳細については、「インタールーティングドメインサービス」を参照してください。

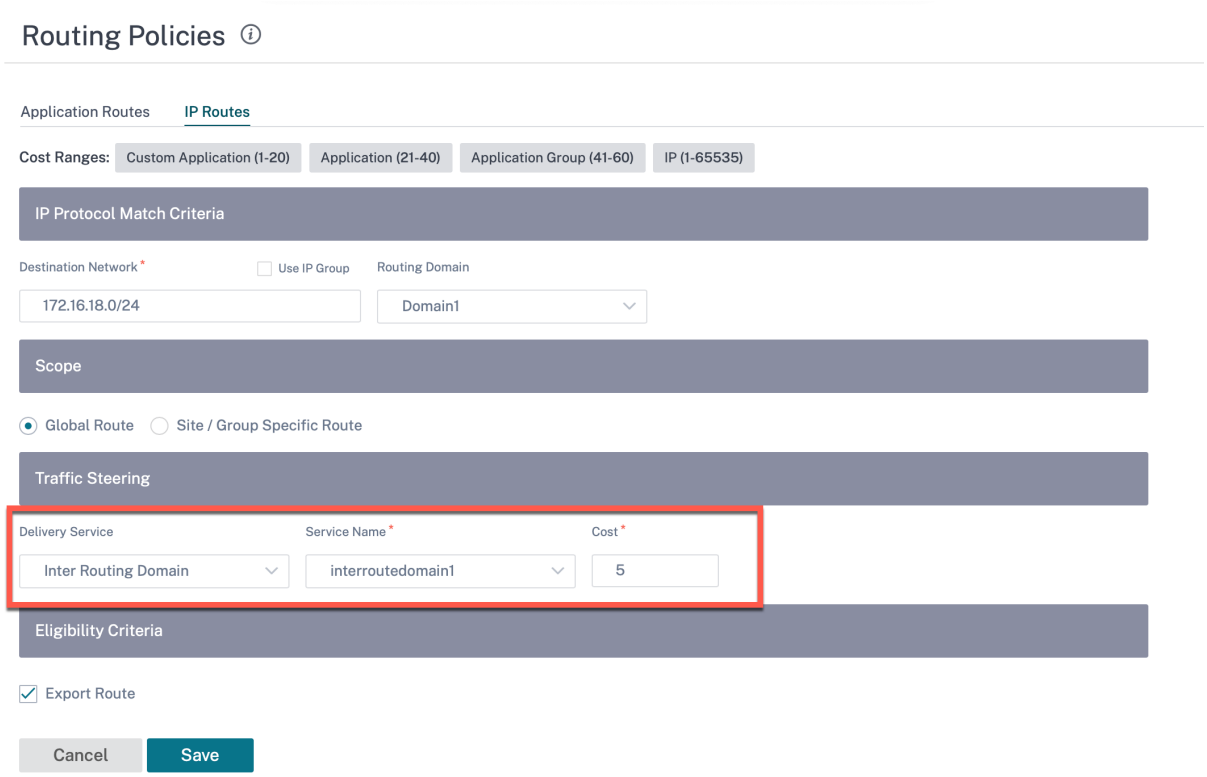
オンプレミス用 Citrix SD-WAN Orchestrator を介してルーティング間ドメインサービスを構成するには:

1. ネットワークレベルで、[構成] > [ルーティング] > [ルーティングドメイン] > [ルーティングドメイン間サービス] に移動します。
2. **+ Inter-Routing Domain** をクリックし、次のパラメータの値を入力します。

- 名前: ルーティング間ドメインサービスの名前。
- ルーティングドメイン **1**: ペアの最初のルーティングドメイン。
- ルーティングドメイン **2**: ペアの 2 番目のルーティングドメイン。
- ファイアウォールゾーン: サービスのファイアウォールゾーン。
  - デフォルト: **Inter_Routing_Domain_Zone** ファイアウォールゾーンが割り当てられます。
  - なし: サービスはゾーンがなく、パケットの元のゾーンを維持するコンジットのように動作します。
  - ネットワーク内で構成されているすべてのゾーンが選択されることがあります。

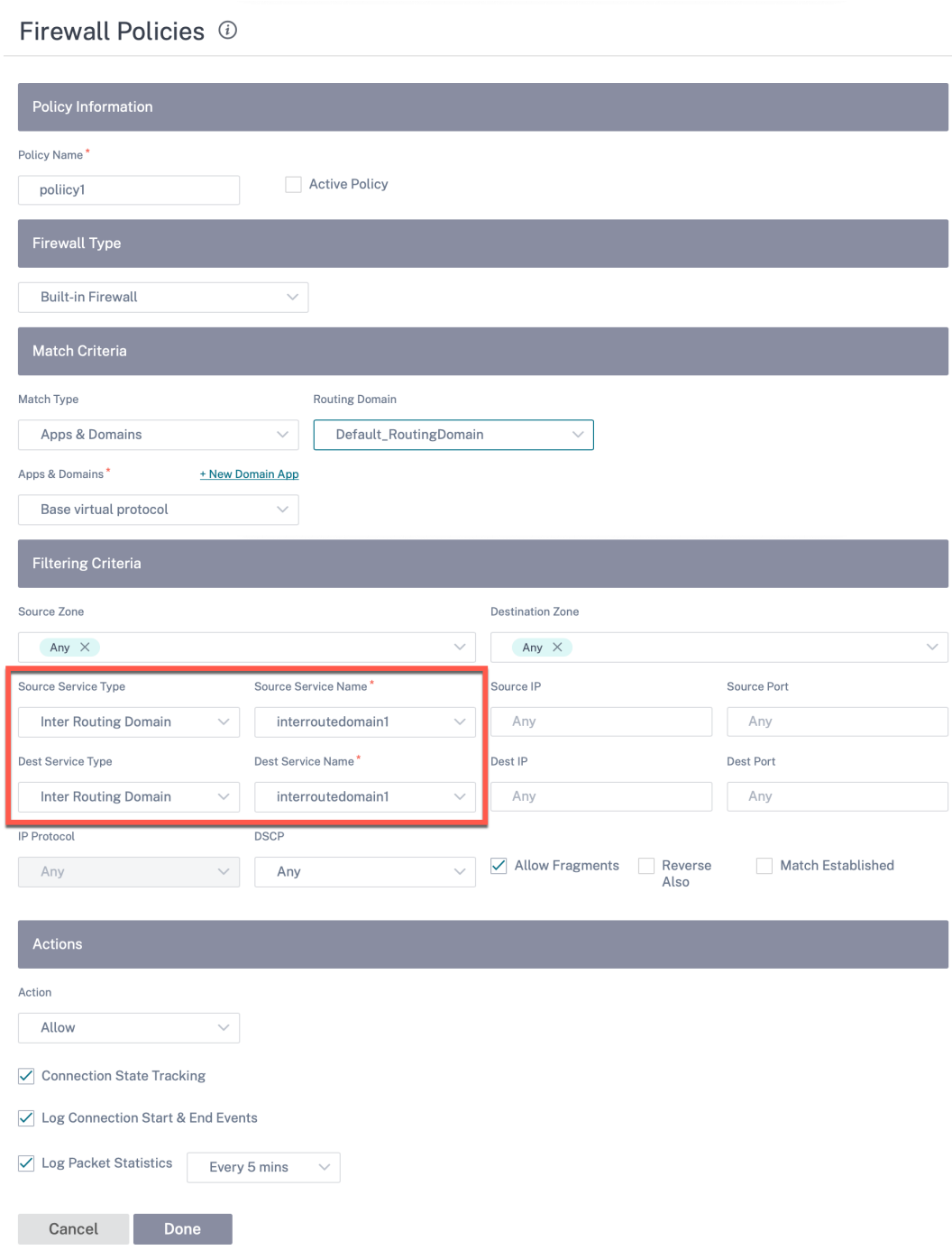


インタールーティングドメインサービスを使用してルートを作成するには、サービスタイプを [インタールーティングドメインサービス] としてルートを作成し、ルーティング間ドメインサービスを選択します。ルートの設定について詳しくは、「ルーティングポリシー」を参照してください。



また、他の Routing Domain ペアからルートを追加して、2 つのルーティングドメイン間の接続を確立します。

ファイアウォールポリシーを構成して、ルーティングドメイン間のトラフィックフローを制御することもできます。ファイアウォールポリシーで、送信元および宛先サービスに対して [Inter-Routing ドメインサービス] を選択し、必要なファイアウォールアクションを選択します。ファイアウォールポリシーの設定については、「ファイアウォールポリシー」を参照してください。

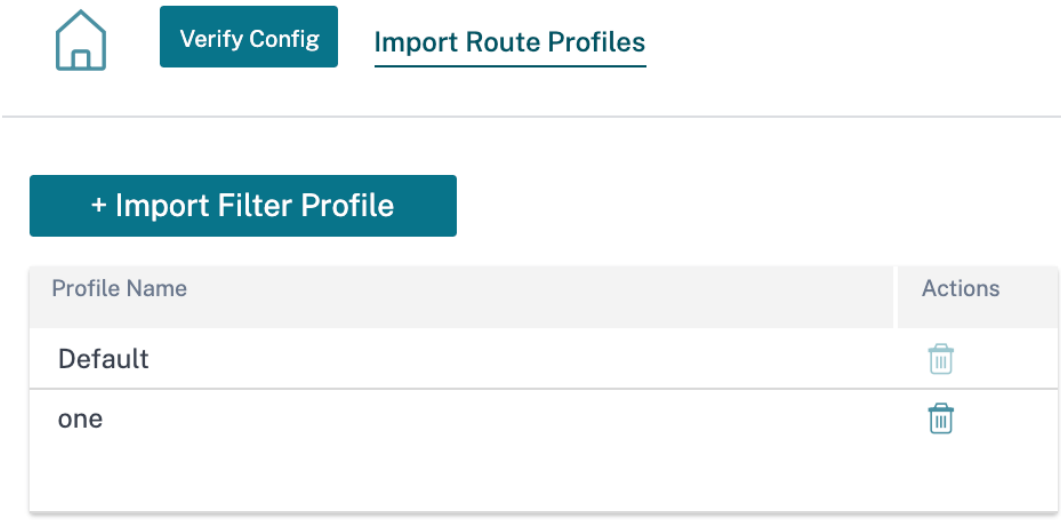


また、イントラネットサービスの種類を選択して、スタティック NAT ポリシーとダイナミック NAT ポリシーを構成することもできます。NAT ポリシーの設定の詳細については、「ネットワークアドレス変換」を参照してください。

ルートプロファイルのインポート

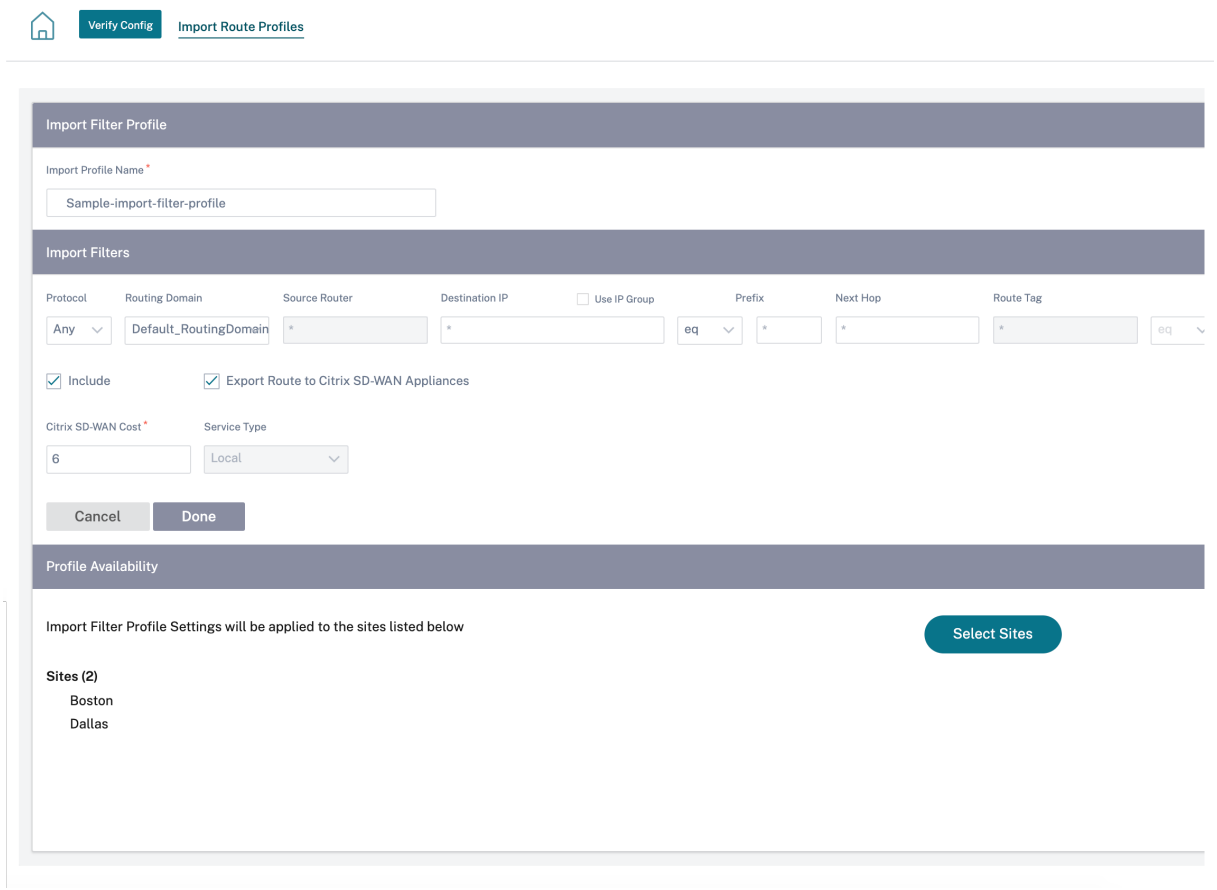
フィルタを設定して、ルートラーニングがどのように行われるかを微調整できます。

インポートフィルタルールは、SD-WAN ルートデータベースにダイナミックルートをインポートする前に満たす必要があるルールです。デフォルトでは、ルートはインポートされません。



インポート・プロファイル名、プロファイルの可用性、インポート・フィルタとともに、次のフィールドを含むインポート・フィルタ・プロファイルを追加します。

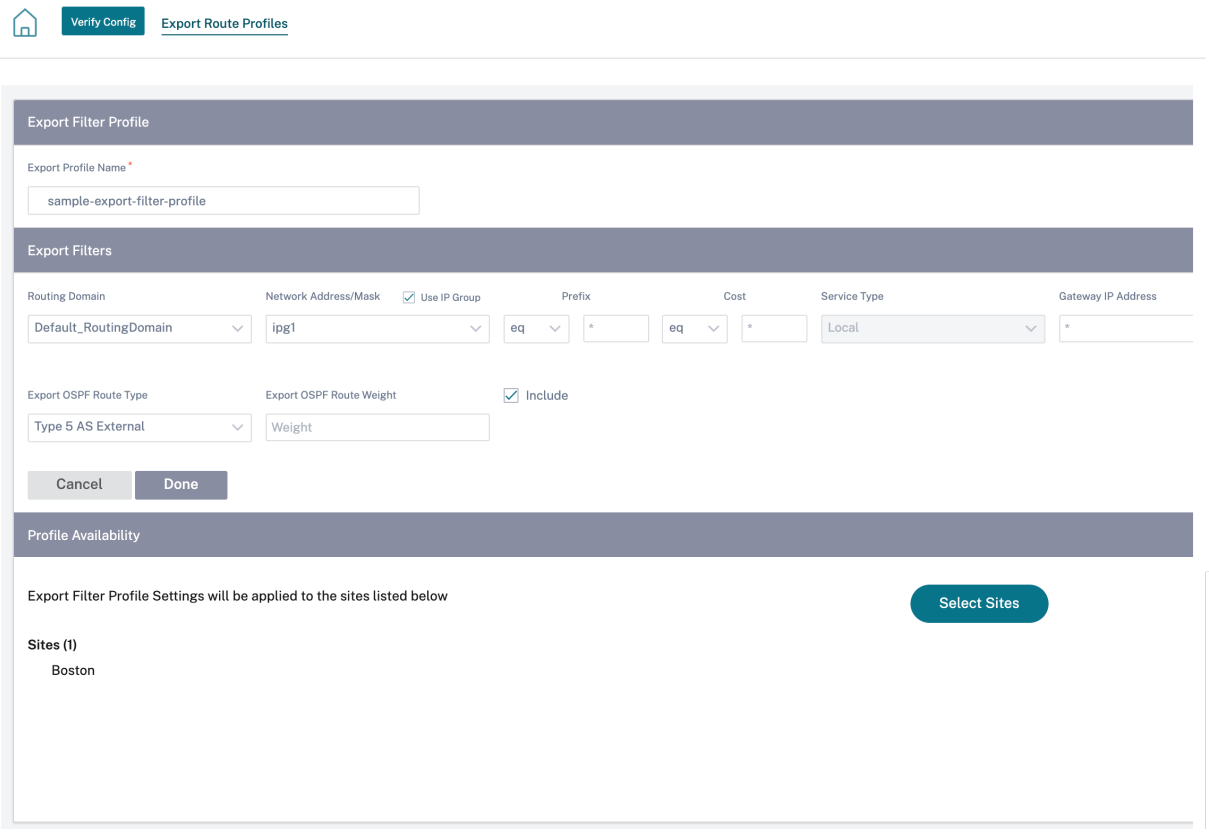
- プロトコル -リストからプロトコルを選択します。
- ルーティングドメイン -特定のルーティングドメインからのルートを照合するには、設定済みのルーティングドメインをリストから選択します。
- ソースルーター-ルートのネットワークを説明する設定済みのネットワークオブジェクトの IP アドレスとネットマスクを入力します。
- 宛先 **IP** -宛先 IP アドレスを入力します。
- プレフィックス -ルートをプレフィックスで照合するには、リストから一致する述語を選択し、隣接するフィールドにルートプレフィックスを入力します。
- ネクストホップ-ネクストホップの宛先を入力します。
- ルートタグ -ルートタグを入力します。
- コスト -エクスポートされるルートの選択を絞り込むために使用される方法（述語）と SD-WAN ルートコスト。



監査エラーを確認するには、「構成を確認」をクリックします。

ルートプロファイルのエクスポート

ダイナミックルーティングプロトコルで SD-WAN ルートをアドバタイズするときに満たす必要があるルールを定義します。デフォルトでは、すべてのルートがピアにアドバタイズされます。



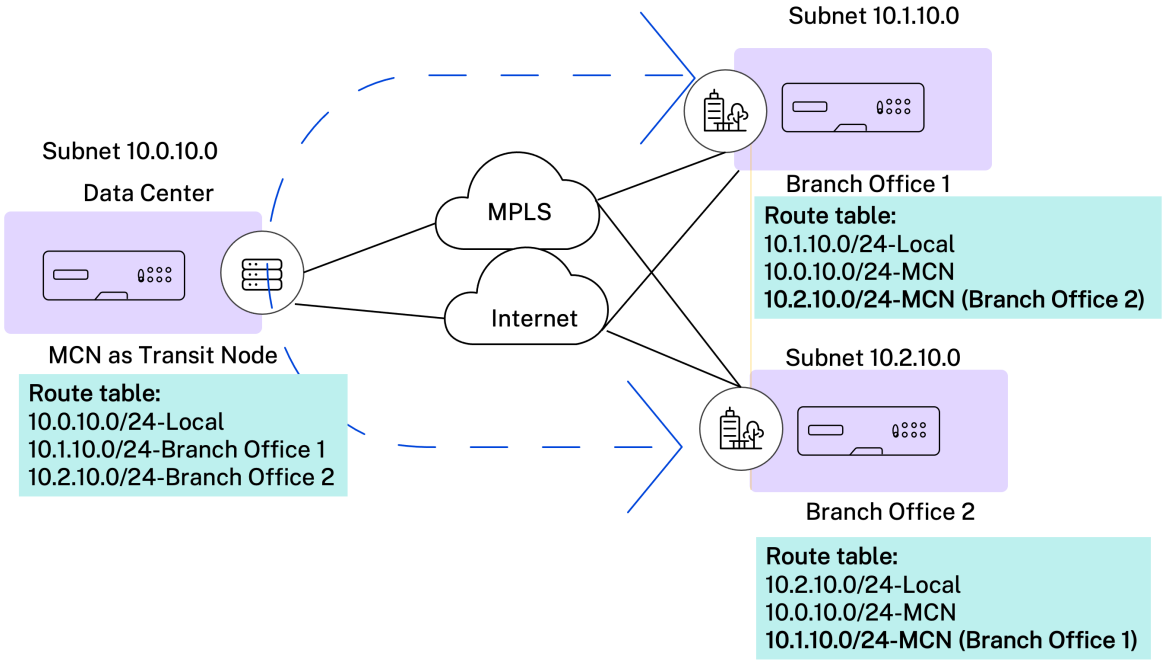
監査エラーを確認するには、「構成を確認」をクリックします。

トランジットノード

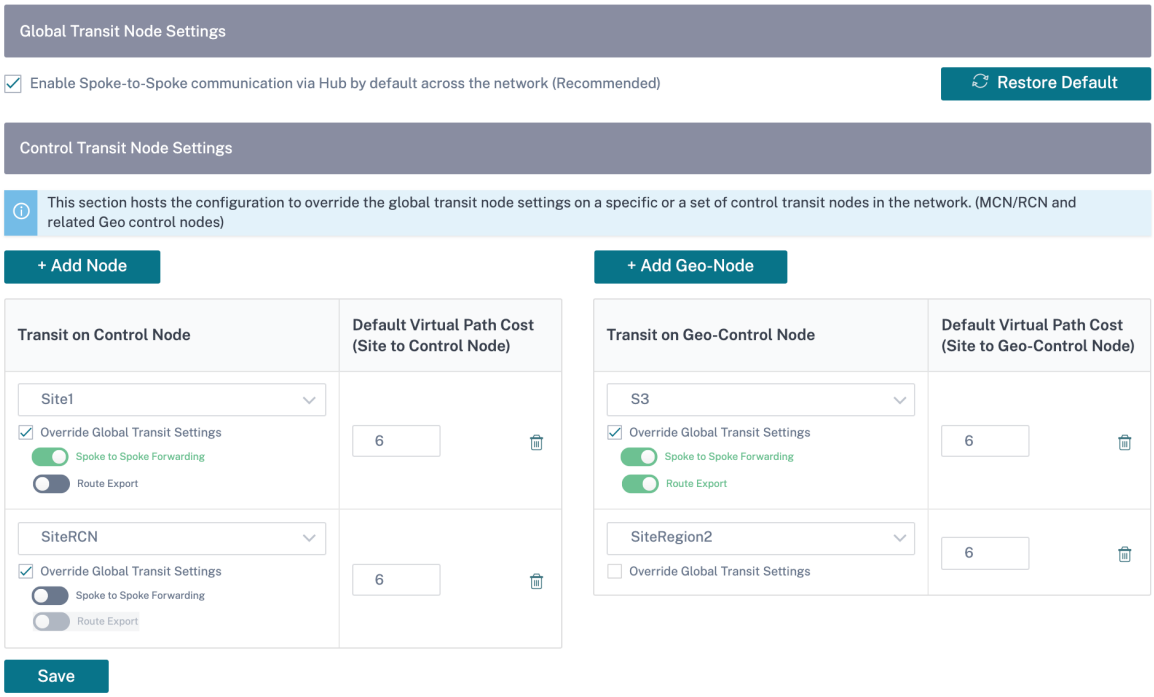
仮想オーバーレイトランジットノード

トランジットノードは、リージョン内の 1 つ以上の支店間でトラフィックを転送できるサイトです。

ルートコストを調整することで、2 つのノード間のトラフィックに影響を与え、中継ノードを中間ホップとして選択することができます。トランジットノードは、隣接していないノードにデータをルーティングするために使用されます。たとえば、3 つのノードが直列 A-B-C で接続されている場合、A から C へのデータを B 経由でルーティングできます。Citrix SD-WAN Orchestrator サービスでは、トランジットノードとトランジットノードを介してルーティングされるサイトを指定できます。仮想パスは、コストの昇順で選択されます。コストを低くし、優先順位を高めます。



デフォルトのグローバル仮想オーバーレイトランジットノード　制御ノード (MCN/RCN) と地理制御ノード (Geo-MCN/RCN) を指定して、ネットワーク内のデフォルトのグローバル仮想オーバーレイ中継ノードとして機能させることができます。グローバル設定の一部としてハブを介したスポークアンドスポーク通信を有効にすると、すべてのサイトが、設定済みのコントロールノードをデフォルトでサイト間通信の中継ノードとして使用できるようになります。



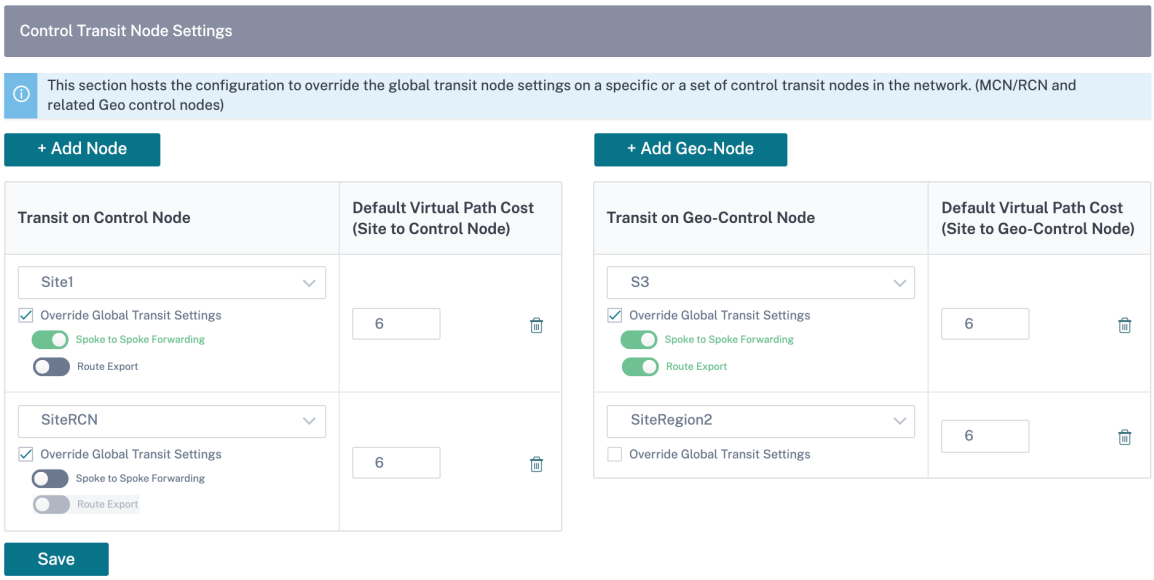
仮想オーバーレイトランジットノードとして使用する制御ノードと geo コントロールノードを追加し、仮想パスコストを指定します。制御ノードと地理制御ノードには、それぞれのデフォルト仮想パスコストとして 6 と 7 があります。ネットワーク要件に応じて、仮想パスコストを変更できます。「デフォルトに戻す」をクリックすると、デフォルトの中継ノードの仮想パスコストがデフォルトに戻ります。

> 注
>
> トランジットノードとして、最大 3 つのコントロールノードと 3 つのジオコントロールノードを追加できます。

デフォルトでは、WAN-to-WAN 転送は、選択したコントロールノードと geo コントロールノードに関連付けられたすべてのパスで有効になります。WAN 間転送を使用すると、サイトは、サイト間、インターネット、またはイントラネットトラフィックに対して、隣接する 2 つのサイト間の中間ホップとして機能し、動的仮想パスのメディエータとして機能できます。

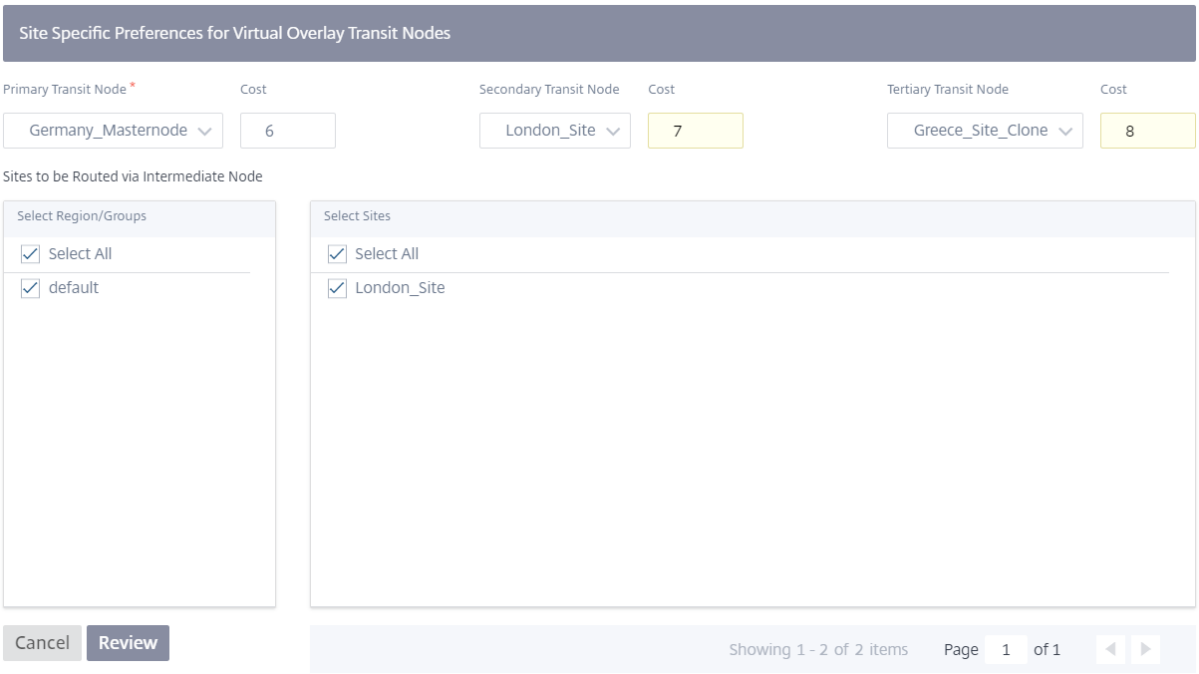
グローバルトランジットノード設定を上書きして、選択したコントロールトランジットノードでのみスポークツースポーク転送を有効または無効にすることができます。スポークツースポーク転送を有効にすると、中継制御ノードは接続されているサイト間のルートをエクスポートします。サイト間通信とトランジットノードのみに接続されたサイト間の動的仮想パスが有効になります。

ルートエクスポートを有効にすると、すべてのサイトパスで仮想パスから仮想パスへの転送とルートのエクスポート (WAN-to-WAN 転送) が可能になります。トグルボタンを無効にすると、仮想パスから仮想パスへの転送のみが有効になり、すべてのサイトパスでルートのエクスポートが無効になります。ルートエクスポートは、スポークツースポーク転送が有効になっている場合にのみ有効にできます。



仮想オーバーレイトランジットノードのサイト固有の環境設定　仮想オーバーレイトランジットノードのサイト固有の環境設定を使用すると、ネットワーク内のすべてのサイトのグローバル仮想オーバーレイトランジットノード設定を上書きできます。非制御ノードを、サイトのプライマリ中継ノードとして選択することもできます。2 番目と 3 次トランジットノードとして、コントロールノードまたは geo コントロールノードを選択します。プライマリ中継ノー

ドがダウンしている場合、サイトはセカンダリトランジットノードを使用します。プライマリトランジットノードとセカンダリ中継ノードの両方がダウンしている場合、サイトは第 3 中継ノードを使用します。トランジットノードのコストを指定し、サイト固有の仮想オーバーレイトランジットノード設定を適用するサイトを選択します。



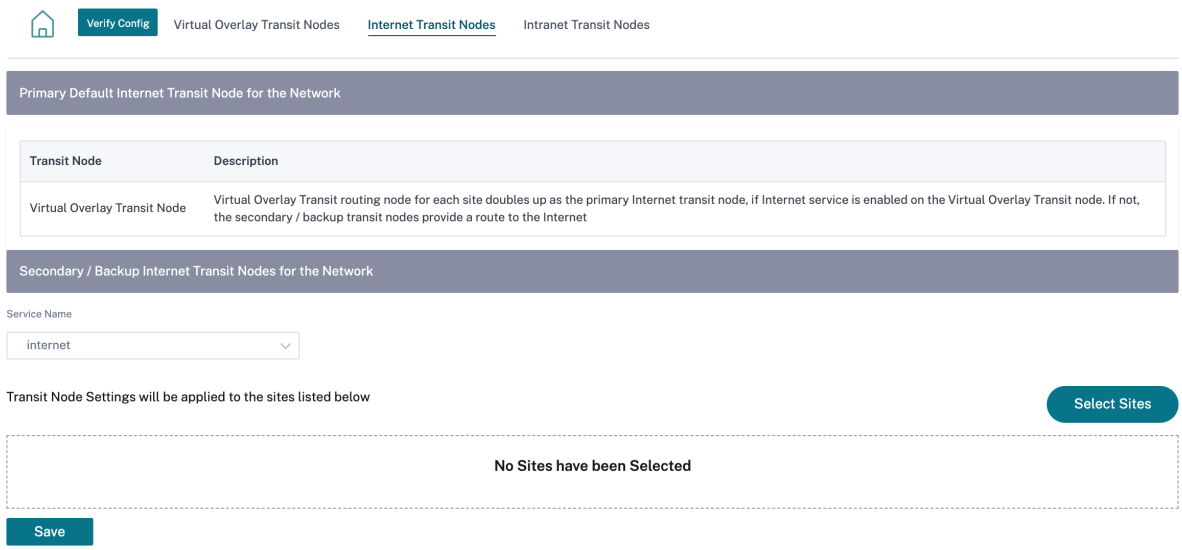
インターネットトランジットノード

サイトをインターネット中継サイトとして追加して、サイトへのインターネットアクセスを有効にすることができます。直接インターネット接続が必要なサイトでは、インターネットサービスを有効にしたリンクが少なくとも 1 つ必要です。つまり、少なくとも 1 つのリンクが 0 以外の帯域幅共有% に設定されます。

各トランジットサイトには、ルートコストを割り当てることができます。インターネットサービスの利用可能なサイトは、直接ルートが最もコストの低いルーティングパスになるので、インターネットに直接アクセスします。インターネットサービスのないサイトは、設定されたトランジットサイトを通じてインターネットにルーティングできます。インターネットトランジットサイトが構成されると、これらのトランジットサイトを経由してインターネットへのルートが自動的にすべてのサイトにプッシュされます。インターネットトランジットサイトとは、インターネットサービスが有効なサイトです。

たとえば、サンフランシスコとニューヨークがインターネット中継サイトとして構成されている場合などです。サンフランシスコとニューヨーク経由でインターネットへのルートは、自動的にすべてのサイトにプッシュされます。

インターネットサービスが有効な仮想オーバーレイトランジットノードは、プライマリインターネット中継ノードとして機能します。仮想オーバーレイトランジットノードでインターネットサービスが有効になっていない場合、セカンダリ/バックアップインターネット中継ノードはインターネットへのルートを提供します。

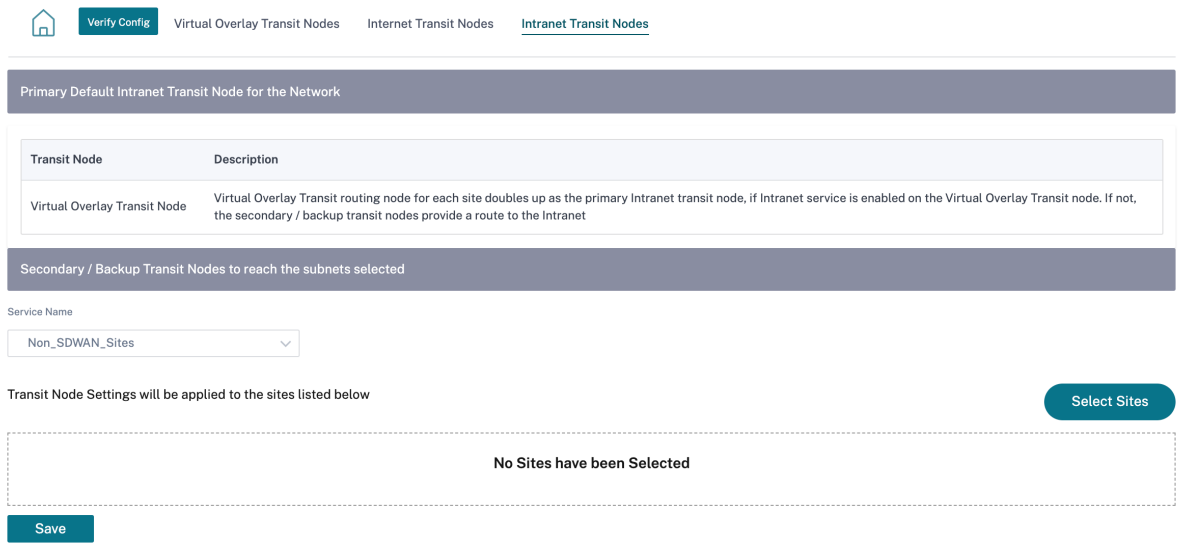


イントラネットトランジットノード

イントラネット中継ノードを使用すると、すべての非イントラネットサイトが、構成されたイントラネットネットワークにアクセスできます。各トランジットサイトには、ルートコストを割り当てることができます。イントラネットサービスを利用できるサイトでは、直接ルートが最もコストの低いルーティングパスになるため、イントラネットネットワークに直接アクセスします。イントラネットサービスのないサイトは、構成された中継サイトを通じてイントラネットネットワークにルーティングできます。トランジットサイトが構成されると、これらの中継サイトを経由してイントラネットネットワークへのルートが自動的にすべてのサイトにプッシュされます。

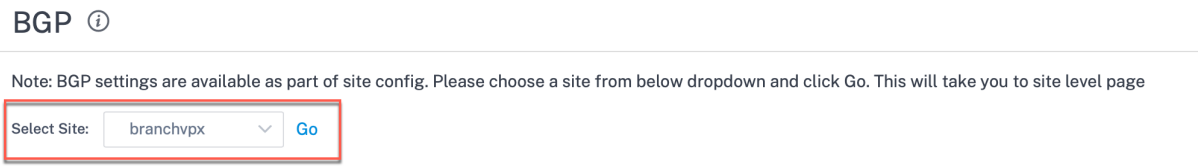
たとえば、10.2.1.0/24 がイントラネットネットワークで、オースティンとダラスが中継サイトを構成しているとします。オースティンとダラスを経由するネットワークアドレスへのルートは、自動的にすべてのサイトにプッシュされます。

イントラネットサービスが有効な仮想オーバーレイトランジットノードは、プライマリイントラネット中継ノードとして機能します。仮想オーバーレイトランジットノードでイントラネットサービスが有効になっていない場合、セカンダリ/バックアップイントラネット中継ノードは、イントラネットへのルートを提供します。



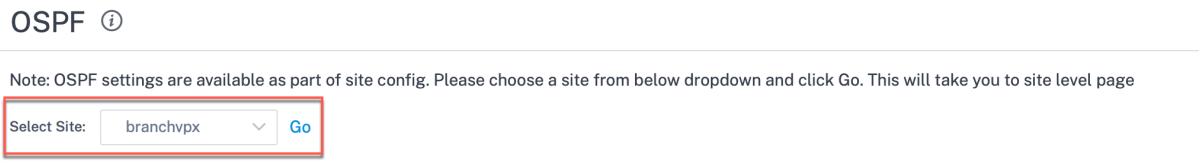
BGP

ドロップダウンリストから必要なサイトを選択し、「**GO**」をクリックすると、サイトの BGP 設定を構成できます。これにより、サイトレベルの BGP 設定ページが表示されます。BGP の設定について詳しくは、「BGP」を参照してください。



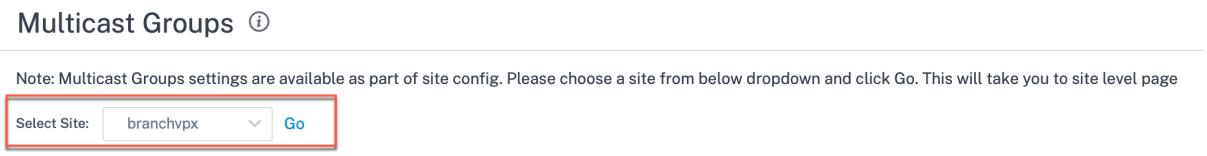
OSPF

ドロップダウンリストから必要なサイトを選択し、[**GO**] をクリックすると、サイトの OSPF 設定を構成できます。これにより、サイトレベルの OSPF 設定ページが表示されます。OSPF の設定の詳細については、「OSPF」を参照してください。



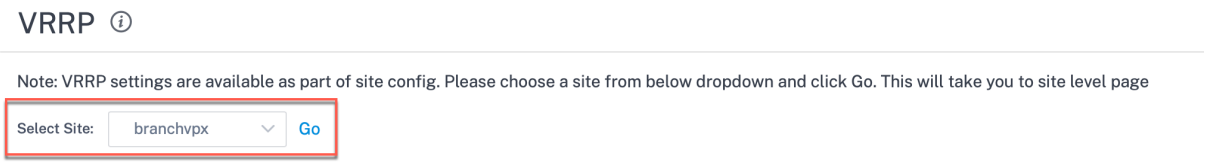
マルチキャストグループ

ドロップダウンリストから必要なサイトを選択し、「実行」をクリックすると、サイトのマルチキャストルーティングを設定できます。これにより、サイトレベルのマルチキャストグループ設定ページが表示されます。マルチキャストルーティングの設定について詳しくは、「マルチキャストグループ」を参照してください。



VRRP

ドロップダウンリストから必要なサイトを選択し、[**GO**] をクリックすると、サイトの仮想ルーター冗長プロトコル (VRRP) を設定できます。これにより、サイトレベルの VRRP 設定ページが表示されます。マルチキャストルーティングの設定の詳細については、VRRPを参照してください。



リンク間通信

October 26, 2022

リンク間通信設定は、互換性のある WAN リンク間の自動パス作成に使用されます。これらの設定は [サイトの構成] と [仮想パス] でオーバーライドできます。ここでは、特定の仮想パスの個々のメンバーパスを選択または選択解除できます。

現在、次の 2 つの設定を使用できます。

- 互換性のある WAN リンク間のパスの作成を自動化するためのルール。
- 動的仮想パスのグローバルデフォルト

これらの設定は、カスタマーネットワーク内のすべての WAN リンクに継承されます。

監査エラーを確認するには、「構成を確認」をクリックします。

デフォルトのリンク間通信グループ

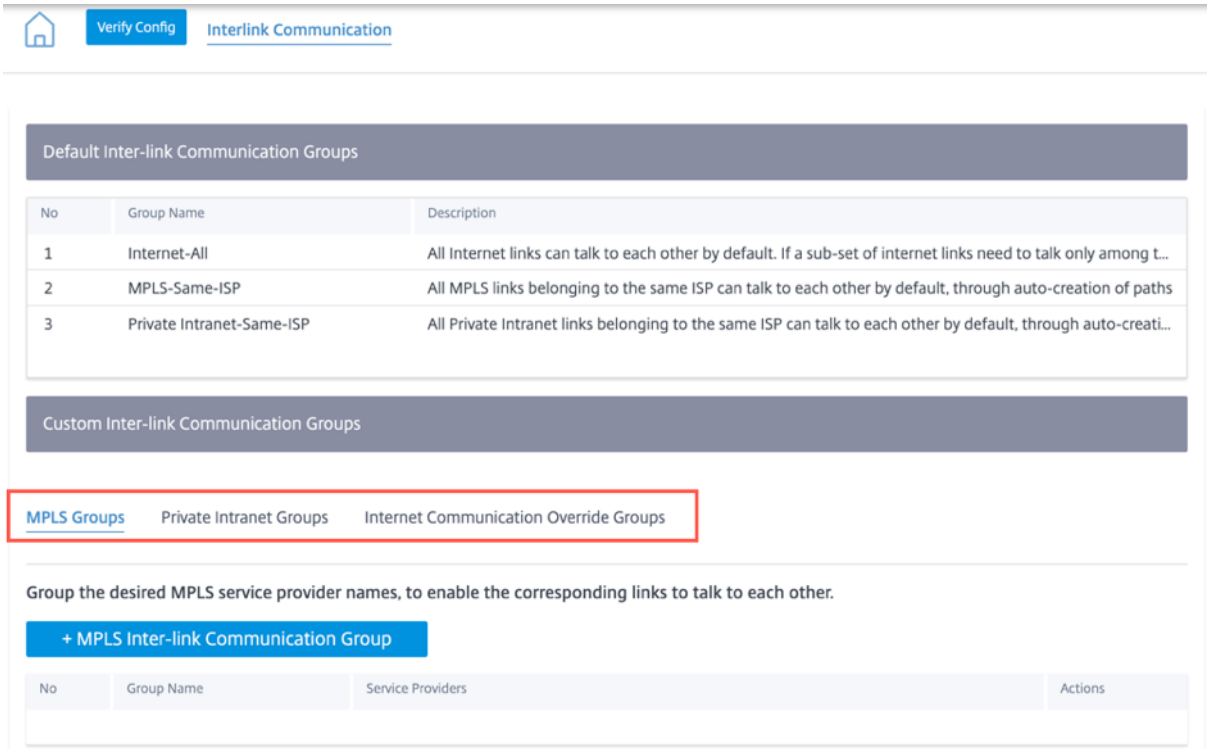
デフォルトのリンク間通信グループは、次の間のパスの作成を自動化することを目的としています。

- 任意の 2 つのインターネットリンク
- サービスプロバイダーを共有する任意の 2 つの MPLS リンク
- サービスプロバイダーを共有する任意の 2 つのプライベートイントラネットリンク

カスタムリンク間通信グループ

カスタムリンク間通信グループを使用すると、プライベートイントラネット、パブリックインターネット、または MPLS リンクを使用して、さまざまなサービスプロバイダー間で他のプライベートイントラネット、パブリックインターネット、または MPLS リンクとのパスを自動的に作成できます。

たとえば、このシナリオを考えてみましょう-同社は米国とインドにオフィスを持っています。米国のオフィスでは AT&T MPLS リンクを使用し、インドのオフィスでは Airtel MPLS リンクを使用します。AT&T と Airtel の MPLS リンクが DSCP タグと関連パラメータの点で互換性があり、相互にパスを作成できるとしましょう。カスタムリンク間通信ルールを使用すると、ISP ペア（この場合は ATT —Airtel など）を選択し、これらの ISP に属するリンク間のパスの自動作成を有効にできます。

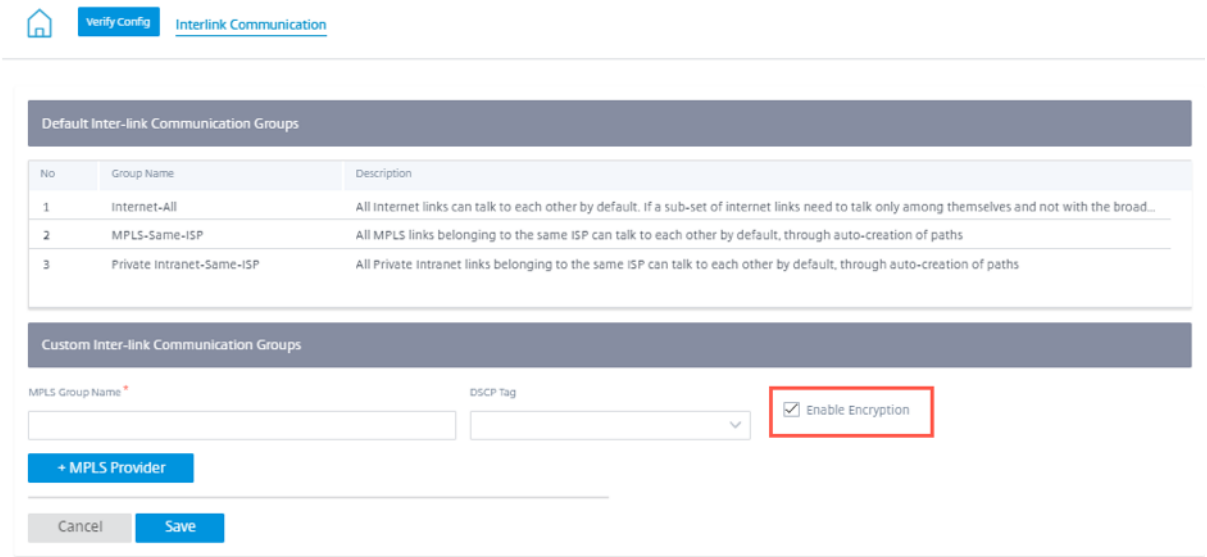


- **MPLS** グループ: 必要な MPLS サービスプロバイダー名をグループ化して、対応するリンクが相互に通信できるようにします。**+ MPLS** インターリンクコミュニケーショングループをクリックし、MPLS グループ名を入力します。ドロップダウンリストから DSCP タグを選択します。ドロップダウンリストから ISP 名を選択し

て、MPLS プロバイダーを追加することもできます。**Enable Encryption** チェックボックスは、すべてのカスタム MPLS リンク間通信グループの暗号化を有効にするのに役立ちます。まれに、暗号化のオーバーヘッドをなくすために、このオプションを無効にしてもかまいません。

- プライベートイントラネットグループ: 必要なイントラネットサービスプロバイダ名をグループ化して、対応するリンクが相互に通信できるようにすることができます。[**+** プライベートイントラネットインターリンクコミュニケーショングループ] をクリックし、プライベートイントラネットグループ名を指定します。ドロップダウンリストから DSCP タグを選択します。ドロップダウンリストから ISP 名を選択して、プライベートイントラネットプロバイダを追加することもできます。[暗号化を有効にする] チェックボックスは、すべてのカスタムプライベートイントラネットリンク間通信グループの暗号化を有効または無効にするのに役立ちます。
- インターネット通信オーバーライドグループ: インターネットリンクのサブセット同士でのみ通信し、他のインターネットリンクとは通信しないようにする必要がある場合は、対応する ISP 名をグループ化して、デフォルトグループからの除外を有効にすることができます。

残りのインターネットリンクは引き続き相互に通信できます。[**+** パブリックインターネットインターリンクコミュニケーショングループ] をクリックし、パブリックインターネットグループ名を指定します。ドロップダウンリストから DSCP タグを選択します。ドロップダウンリストから ISP 名を選択して、パブリックインターネットプロバイダーを追加することもできます。**Enable Encryption** オプションにより、仮想パス上で送信されるリンク間通信グループのパケットが確実に暗号化されます。



セキュリティ

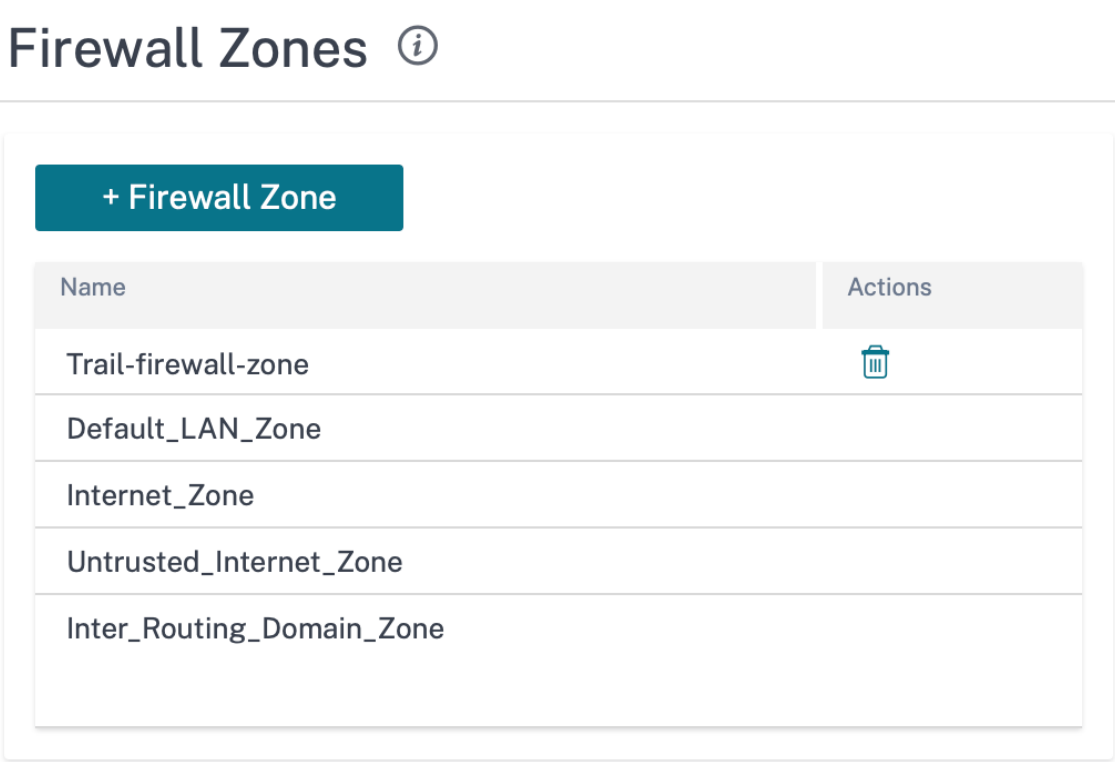
October 26, 2022

ネットワークセキュリティ、仮想パス IPsec、ファイアウォール、ネットワーク上のすべてのアプライアンスに適用される証明書などのセキュリティ設定を構成できます。

ファイアウォールゾーン

ネットワーク内にゾーンを設定し、トラフィックがゾーンに出入りする方法を制御するポリシーを定義できます。デフォルトでは、次のゾーンを使用できます。

- **Default_LAN_Zone:** ゾーンが設定されていない、設定可能なゾーンのあるオブジェクトで送受信されるトラフィックに適用されます。
- **Internet_Zone**: 信頼できるインターフェイスを使用するインターネットサービスとの間で送受信されるトラフィックに適用されます。
- **Untrusted_Internet_Zone**: 信頼できないインターフェイスを使用するインターネットサービスとの間で送受信されるトラフィックに適用されます。



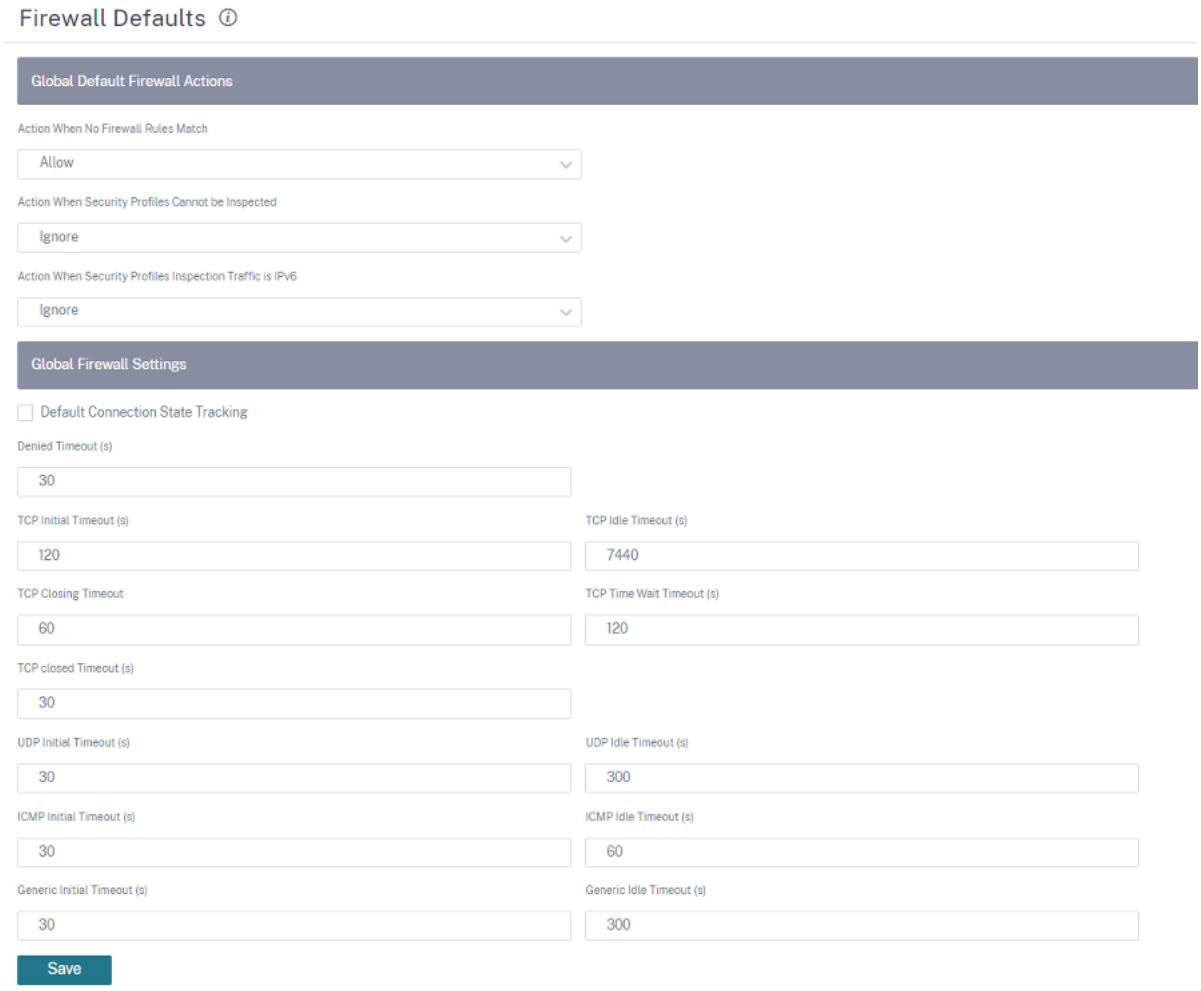
独自のゾーンを作成して、次のタイプのオブジェクトに割り当てることもできます。

- 仮想ネットワーク インターフェイス
- イントラネットサービス
- GRE トンネル
- LAN IPsec トンネル

監査エラーを確認するには、「構成を確認」をクリックします。

ファイアウォールのデフォルト

SD-WAN ネットワーク内のすべてのアプライアンスに適用できるグローバルなデフォルトのファイアウォールアクションとグローバルファイアウォール設定を構成できます。この設定は、グローバル設定よりも優先されるサイトレベルで定義することもできます。



- ファイアウォールルールが一致しない場合のアクション: ファイアウォールポリシーと一致しないパケットに対するアクション ([許可] または [ドロップ]) をリストから選択します。
- セキュリティプロファイルを検査できない場合のアクション: ファイアウォールルールに一致し、セキュリティプロファイルを適用するが、一時的に Edge Security サブシステムで検査できないパケットのアクション ([無視] または [ドロップ]) を選択します。[無視] を選択すると、関連するファイアウォールルールは一致しないものとして処理され、次のファイアウォール規則が順番に評価されます。[**Drop**] を選択すると、関連するファイアウォールルールに一致するパケットがドロップされます。
- デフォルトのファイアウォールアクション: ポリシーと一致しないパケットのアクション (許可/ドロップ) をリストから選択します。

- デフォルト接続状態トラッキング: フィルタポリシーまたは NAT ルールと一致しない TCP、UDP、および ICMP フローの方向接続状態追跡を有効にします。

  > 注
  >
  > デフォルト接続状態追跡が有効になっていると、ファイアウォールポリシーが定義されていない場合でも、非対称フローはブロックされます。サイトで非対称フローが発生する可能性がある場合、グローバルではなく、サイトまたはポリシーレベルで有効にすることが推奨されます。

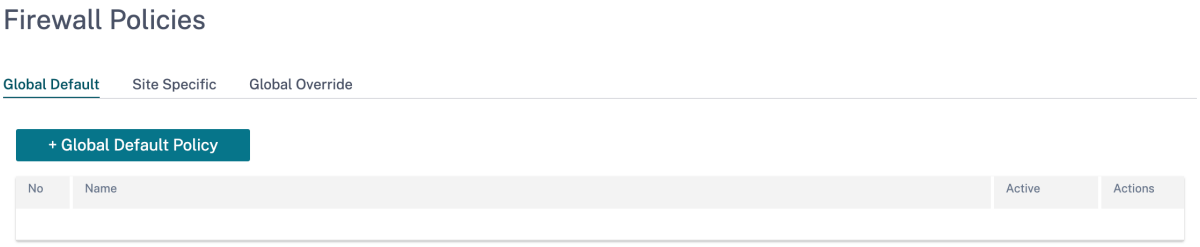
- 拒否タイムアウト **(s)**: 拒否された接続を閉じる前に新しいパケットを待つ時間 (秒単位)。
- **TCP** 初期タイムアウト **(s)**: 不完全な TCP セッションを閉じる前に新しいパケットを待つ時間 (秒単位)。
- **TCP** アイドルタイムアウト **(s)**: アクティブな TCP セッションを閉じる前に新しいパケットを待つ時間 (秒単位)。
- **TCP** 終了タイムアウト: 終了要求後に TCP セッションを閉じる前に新しいパケットを待つ時間 (秒単位)。
- **TCP Time Wait Timeouts (s)**: 終了した TCP セッションを閉じる前に新しいパケットを待つ時間 (秒単位)。
- **TCP Closed Timeout (s)**: 中止された TCP セッションを閉じる前に新しいパケットを待つ時間 (秒単位)。
- **UDP** 初期タイムアウト **(**秒**)**: 両方向のトラフィックが見られなかった UDP セッションを閉じる前に、新しいパケットを待つ時間 (秒単位)。
- **UDP** アイドルタイムアウト **(**秒**)**: アクティブな UDP セッションを閉じる前に新しいパケットを待つ時間 (秒単位)。
- **ICMP** 初期タイムアウト **(s)**: 両方向のトラフィックが見られなかった ICMP セッションを閉じる前に、新しいパケットを待つ時間 (秒単位)
- **ICMP** アイドルタイムアウト **(s)**: アクティブな ICMP セッションを閉じる前に新しいパケットを待つ時間 (秒単位)。
- **Generic Initial Timeout (s)**: 両方向のトラフィックが見られなかった汎用セッションを閉じる前に、新しいパケットを待つ時間 (秒単位)。
- 汎用アイドルタイムアウト **(**秒**)**: アクティブな汎用セッションを閉じる前に新しいパケットを待つ時間 (秒単位)。

監査エラーを確認するには、「構成を確認」をクリックします。

ファイアウォールポリシー

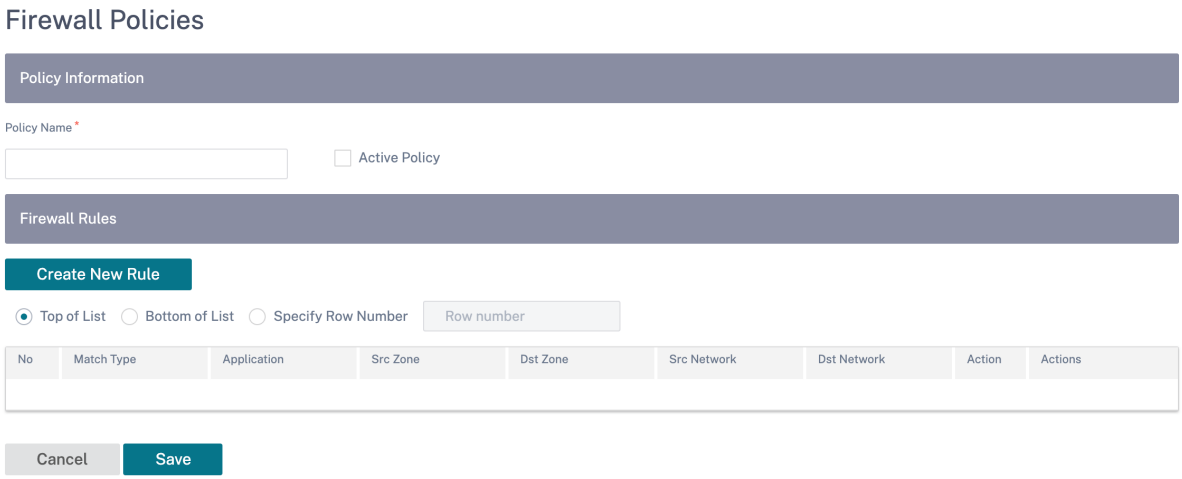
ファイアウォールプロファイルは、一致基準に応じてネットワークトラフィックが特定のファイアウォールルールにのみ制限されるようにし、特定のアクションを適用することにより、セキュリティを提供します。ファイアウォールポリシーには 3 つのセクションがあります。

- グローバルデフォルト—グローバルデフォルトポリシーは、いくつかのファイアウォールルールをまとめたものです。グローバルデフォルトセクションで作成したポリシーは、ネットワーク内のすべてのサイトに適用されます。
- サイト固有—定義済みのファイアウォールルールを特定のサイトに適用できます。
- グローバルオーバーライド—グローバルオーバーライドポリシーを使用して、グローバルポリシーとサイト固有のポリシーの両方を上書きできます。

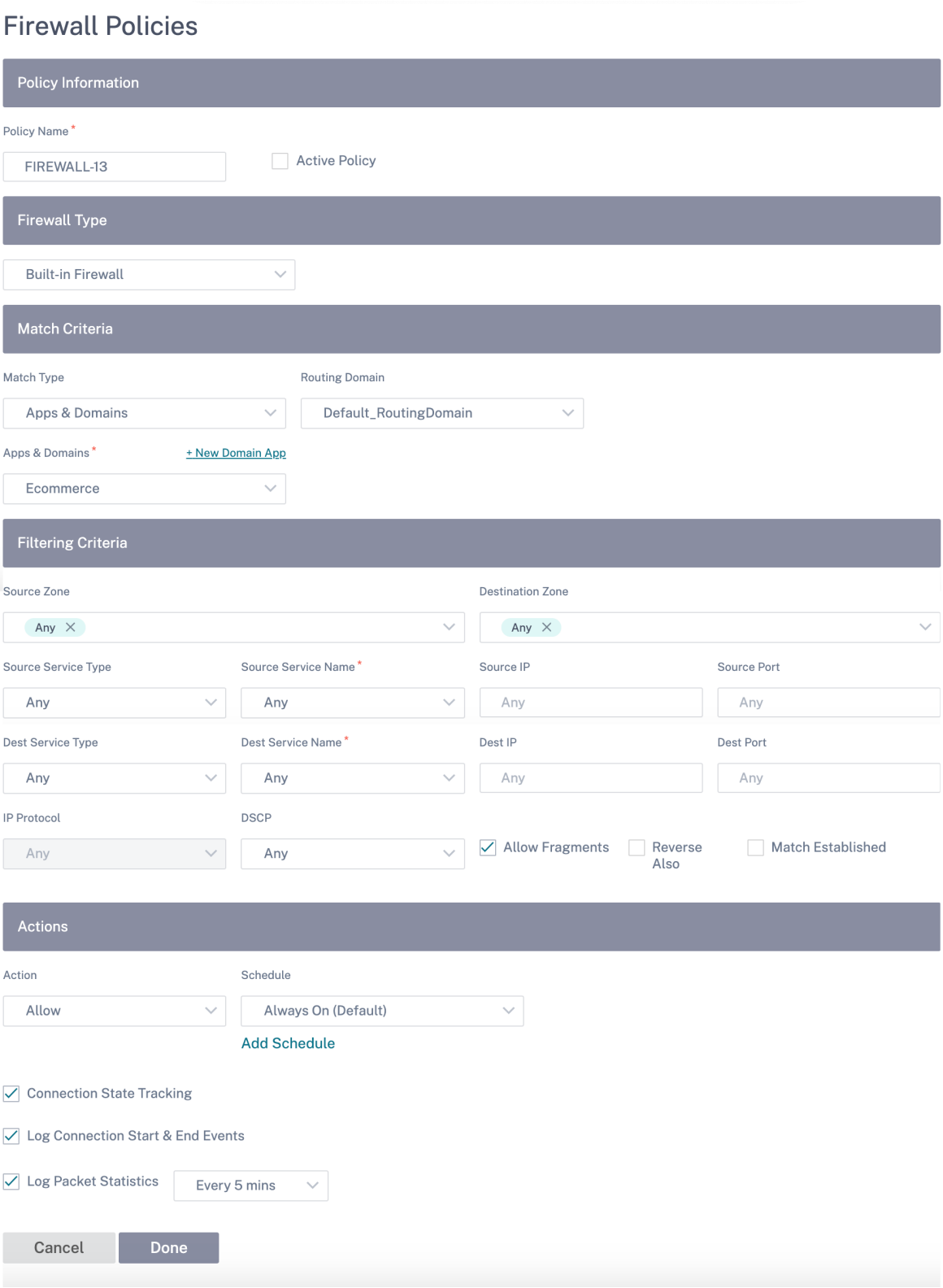


ファイアウォールルールを定義し、優先順位に基づいて配置できます。優先順位は、リストの上、リストの下部、または特定の行から開始するように選択できます。

アプリケーションまたはサブアプリケーションに対してより具体的なルールを上部に配置し、さらに広いトラフィックを表すルールについてはあまり具体的でないルールを設定することをお勧めします。



ファイアウォールルールを作成するには、[新しいルールを作成] をクリックします。



- すべてのファイアウォールルールを適用する場合は、ポリシー名を入力し、アクティブポリシーチェックボックスを選択します。

- 一致基準は、アプリケーション、カスタム定義アプリケーション、アプリケーショングループ、アプリケーションファミリ、IP プロトコルベースなど、ルールのトラフィックを定義します。
- フィルタ条件:
  - ソースゾーン: ソースファイアウォールゾーン。
  - 宛先ゾーン: 宛先ファイアウォールゾーン。
  - ソースサービスタイプ: ソース SD-WAN サービスタイプ（ローカル、仮想パス、イントラネット、IP ホスト、またはインターネット）はサービスタイプの例です。
  - ソースサービス名: サービスタイプに関連するサービスの名前。たとえば、ソースサービスの種類に仮想パスが選択されている場合は、特定の仮想パスの名前になります。これは必ずしも必要ではなく、選択したサービスタイプによって異なります。
  - ソース **IP**: ルールが照合に使用する IP アドレスとサブネットマスク。
  - ソースポート: 特定のアプリケーションが使用するソースポート。
  - **Dest** サービスタイプ: ターゲット SD-WAN サービスタイプ (ローカル、仮想パス、イントラネット、IP ホスト、インターネット) は、サービスタイプの例です。
  - **Dest** サービス名: サービスタイプに関連するサービスの名前。これは必ずしも必要ではなく、選択したサービスタイプによって異なります。
  - **Dest IP**: フィルターが照合に使用する IP アドレスとサブネットマスク。
  - 宛先ポート: 特定のアプリケーションが使用する宛先ポート (つまり、TCP プロトコルの HTTP 宛先ポート 80)。
  - **IP** プロトコル: このマッチタイプを選択した場合は、ルールと一致する IP プロトコルを選択します。オプションには、任意、TCP、UDP ICMP などがあります。
  - **DSCP**: ユーザーが DSCP タグの設定を照合できるようにします。
  - フラグメントを許可: このルールに一致する IP フラグメントを許可します。
  - 逆方向: ソースと宛先の設定を逆にした状態で、このフィルターポリシーのコピーを自動的に追加します。
  - **Match**Established: 受信パケットを、送信パケットが許可されている接続と照合します。
- 一致したフローに対して、次のアクションを実行できます。
  - 許可: ファイアウォールを通過するフローを許可します。
  - ドロップ**:** パケットをドロップして、ファイアウォールを通過するフローを拒否します。
  - 拒否: ファイアウォールを通過するフローを拒否し、プロトコル固有の応答を送信します。TCP はリセットを送信し、ICMP はエラーメッセージを送信します。

- **Count and Continue**: このフローのパケット数とバイト数をカウントしてから、ポリシーリストの下位に進みます。

実行するアクションを定義する以外に、キャプチャするログを選択することもできます。

ネットワークセキュリティ

ネットワーク全体で使用する暗号化メカニズムを選択します。SD-WAN ネットワーク全体をセキュリティで保護するグローバルセキュリティ設定を構成できます。

ネットワーク暗号化モードは、SD-WAN ネットワーク内のすべての暗号化パスに使用されるアルゴリズムを定義します。暗号化されていないパスには適用されません。暗号化は、AES-128 または AES-256 に設定できます。

FIPS コンプライアンス

FIPS モードでは、ユーザーは IPSec トンネルの FIPS 準拠設定と仮想パスの IPSec 設定を構成する必要があります。

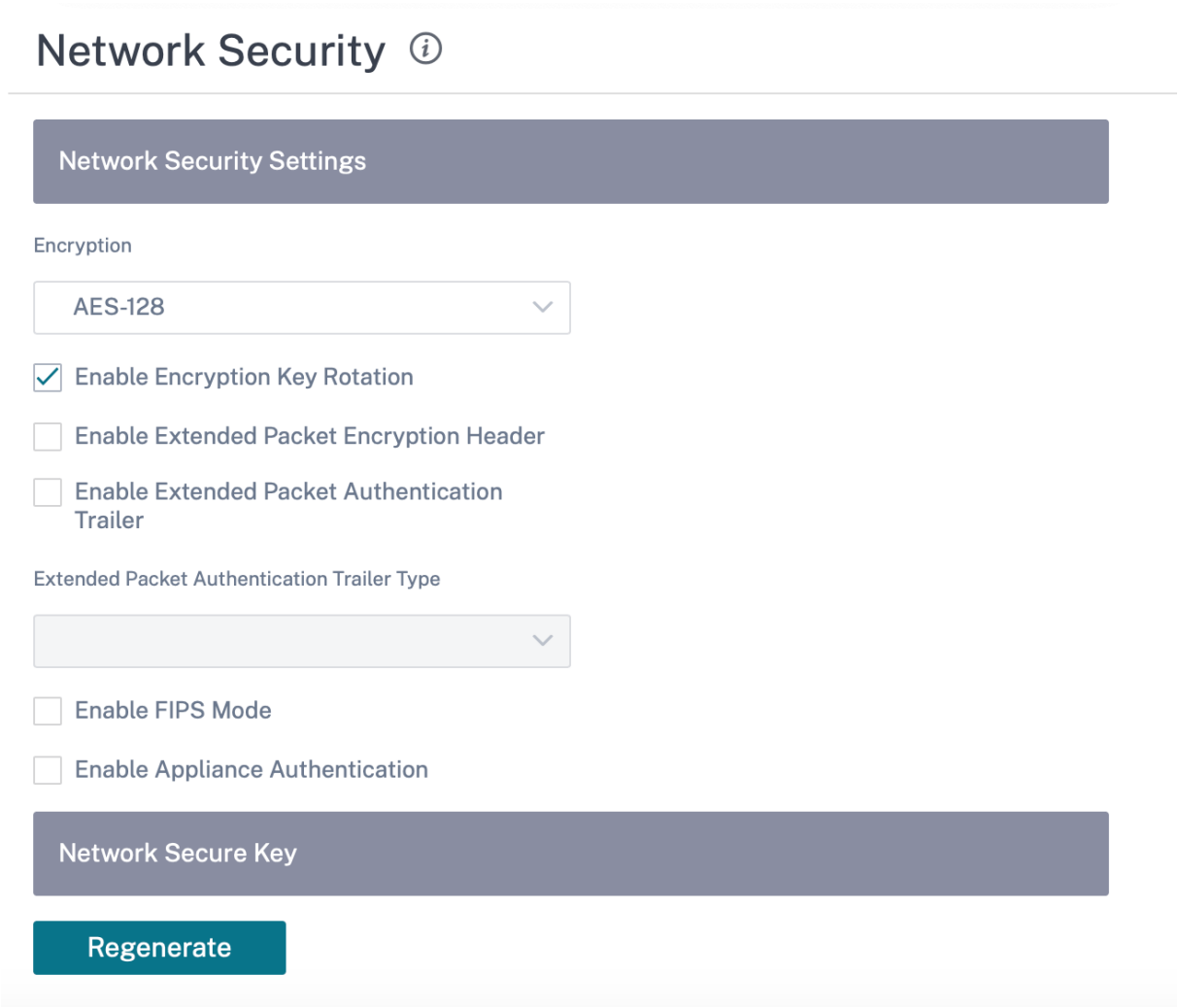
FIPS モードを有効にすると、次の機能が提供されます。

- FIPS 準拠の IKE モードを表示します。
- FIPS 準拠の IKE DH グループを表示します。このグループから、アプライアンスを FIPS 準拠モード（2,5,14～21）に設定するために必要なパラメータを選択できます。
- 仮想パスの IPSec 設定で FIPS 準拠の IPSec トンネルの種類を表示します
- IKE ハッシュおよび（IKEv2）整合性モード、IPsec 認証モード。
- FIPS ベースのライフタイム設定の監査エラーを実行します。

Citrix SD-WAN Orchestrator サービスで FIPS コンプライアンスを有効にするには:

1. [設定] > [セキュリティ] > [ネットワークセキュリティ] に移動します。
2. 「ネットワークセキュリティ設定」セクションで、「**FIPS** モードを有効にする」チェックボックスをクリックします。

FIPS モードを有効にすると、設定中にチェックが実行され、IPSec 関連のすべての設定パラメータが FIPS 標準に準拠しているかどうかが確認されます。監査エラーと警告によって、IPsec を設定するためのプロンプトが表示されます。



IPSec 構成が有効になっているときに FIPS 標準に準拠していない場合、監査エラーが発生する可能性があります。オンプレミス用 Citrix SD-WAN Orchestrator UI で [構成の検証] をクリックしたときに表示される監査エラーの種類は次のとおりです。

- FIPS モードが有効で、非 FIPS 準拠オプションが選択されている場合。
- FIPS モードが有効で、誤ったライフタイム値が入力された場合。
- FIPS モードが有効で、仮想パスのデフォルトセットの IPsec 設定も有効になっていて、正しくないトンネルモードが選択されている場合 (ESP vs ESP_Auth/AH)。
- FIPS モードを有効にすると、仮想パスのデフォルトセットの IPsec 設定も有効になり、誤ったライフタイム値が入力されます。

暗号化キーのローテーションを有効にする：有効にすると、暗号化キーは 10 ～15 分間隔でローテーションされます。

Enable Extended Packet Encryption Header：有効にすると、16 バイトの暗号化カウンタが暗号化トラフィックの先頭に追加され、初期化ベクトルとして機能し、パケット暗号化がランダム化されます。

拡張パケット認証トレーラを有効にする：有効にすると、暗号化トラフィックのコンテンツに認証コードが追加され、メッセージが改変されずに配信されることが検証されます。

拡張パケット認証トレーラータイプ：これは、パケットの内容を検証するために使用されるトレーラーのタイプです。ドロップダウンメニューから [**32** ビットチェックサム] または [**SHA-256**] のいずれかを選択します。

SSL インスペクション

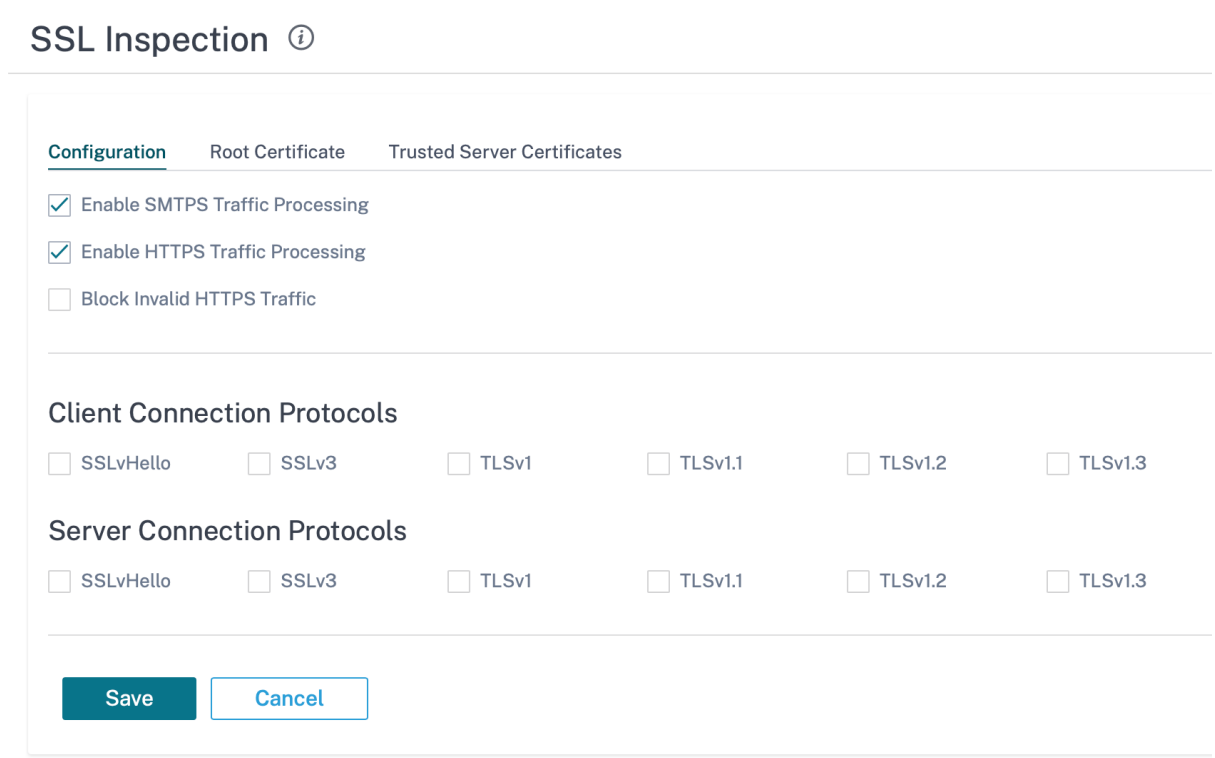
Secure Sockets Layer (SSL) インスペクションは、HTTPS トラフィックとセキュア SMTP トラフィックを傍受、復号化、スキャンして悪意のあるコンテンツがないか調べるプロセスです。SSL インスペクションは、組織との間で送受信されるトラフィックをセキュリティで保護します。組織のルート CA 証明書を生成してアップロードし、トラフィックの中間者検査を実行できます。

> 注**:**
>
> SSL インスペクションは、Citrix SD-WAN 11.3.0 リリース以降でサポートされています。

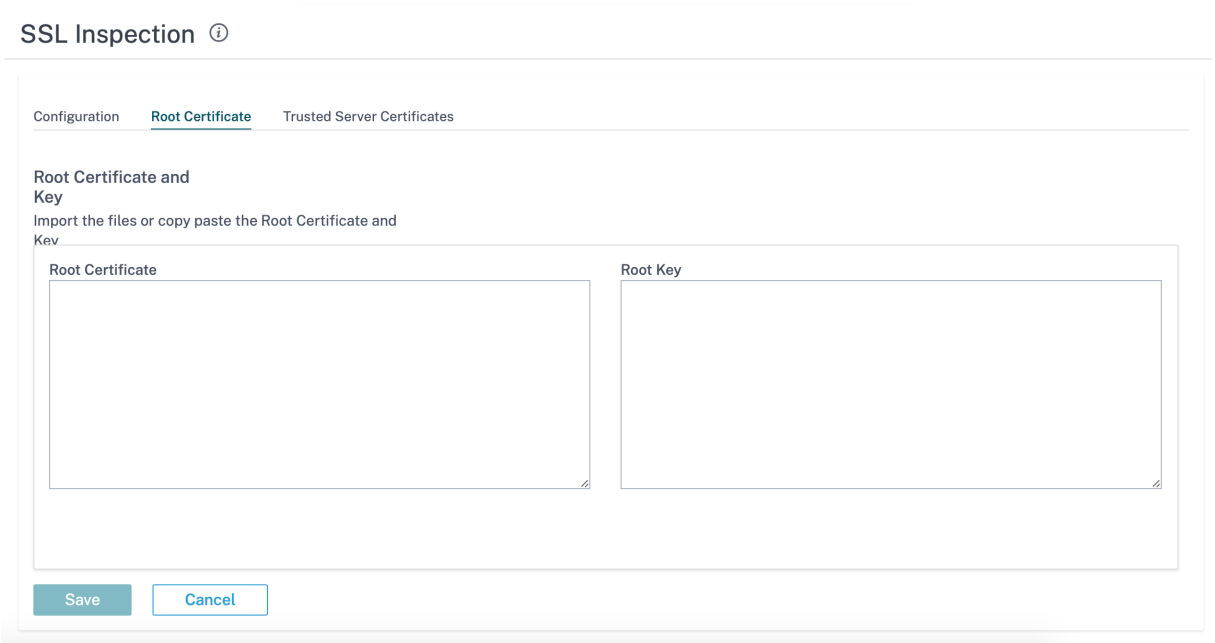
SSL インスペクションをネットワークレベルで有効にするには、[** 設定] > [セキュリティ] > [SSL インスペクション] ** [設定] に移動し、次の SSL 設定を定義します。

- **SMTPS** トラフィック処理を有効にする: 安全な SMTP トラフィックは SSL 検査を受けます。
- **HTTPS** トラフィック処理を有効にする:HTTPS トラフィックは SSL インスペクションを受けます。
- 無効な **HTTPS** トラフィックをブロック: デフォルトでは、無効な **HTTPS** トラフィックをブロックするチェックボックスがオフになっている場合、ポート 443 の HTTPS 以外のトラフィックは無視され、妨げられることなくフローが許可されます。無効な **HTTPS** トラフィックをブロックを選択すると、HTTPS 以外のトラフィックは SSL インスペクションの対象としてブロックされます。このオプションを有効にすると、正規のトラフィック、つまりポート 443 の HTTP トラフィックや、証明書の有効期限が切れたサイトからの HTTPS トラフィックがブロックされる可能性があります。
- クライアント接続プロトコル: 必要なクライアントプロトコルを選択します。使用可能なプロトコルは、SSLvHello、SSLv3、TLSv1、TSlv1.1、TLSv1.2、および TLSv1.3 です。
- サーバー接続プロトコル: 必要なサーバープロトコルを選択します。使用可能なプロトコルは、SSLvHello、SSLv3、TLSv1、TSlv1.1、TLSv1.2、および TLSv1.3 です。

> 注**:**
>
> TLSv1.2 より古いバージョンは脆弱とみなされるため、下位互換性が重要でない限り有効にしないでください。

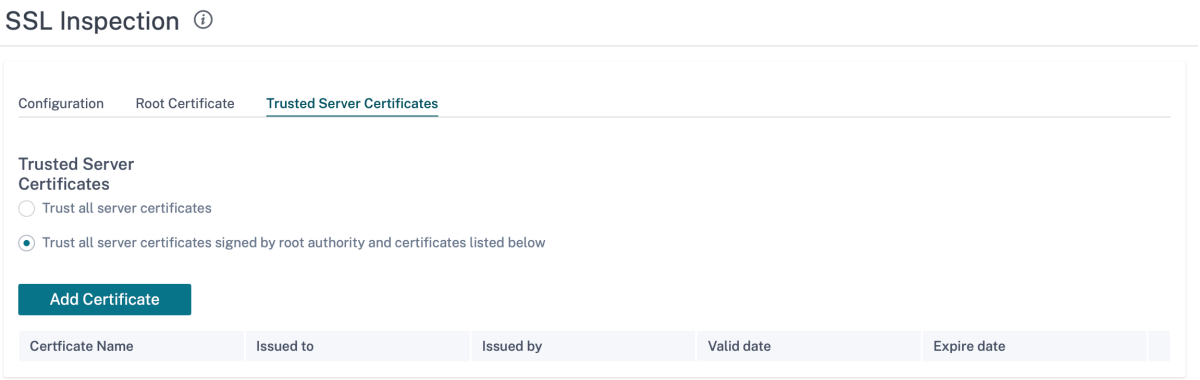


[ルート証明書] タブで、組織のルート認証局 (CA) のルート証明書とキーをコピーして貼り付けます。SSL インスペクションを実行できるように、ルート CA を使用して元のサイトの証明書の偽造コピーを作成して署名します。ルート CA 証明書は、トラフィックの SSL 検査が可能なすべてのクライアントワークステーションとデバイスにインストールされていると暗黙的に想定されています。



デフォルトの [ルート認証局によって署名されたすべてのサーバー証明書と以下にリストされている証明書を信頼す

る] オプションを選択すると、SD-WAN はすべてのサーバー証明書を、以前に構成されたルート CA およびルート CA の標準リストと照合して検証します。また、証明書が無効なサーバーも破棄されます。この動作を無効にするには、内部サーバーの **SSL** 自己署名証明書を信頼できるサーバー証明書タブにアップロードします。[証明書を追加] をクリックして名前を指定し、証明書を参照してアップロードします。または、「すべてのサーバー証明書を信頼する」を選択すると、証明書の検証状況に関係なく、すべてのサーバーが Citrix SD-WAN によって信頼できると見なされます。



セキュリティプロファイルの一部として、SSL ルールを作成し、SSL インスペクションを有効にすることができます。セキュリティプロファイルの SSL ルール作成の詳細については、「Edge セキュリティ」を参照してください。

侵入防止

侵入防止システム (IPS) は、悪意のあるアクティビティを検出し、ネットワークへの侵入を防ぎます。IPS はネットワークトラフィックを検査し、すべての受信トラフィックフローに対して自動アクションを実行します。34,000 件を超えるシグネチャ検出とポートスキャン用のヒューリスティックシグネチャのデータベースが含まれているため、最も疑わしいリクエストを効果的に監視してブロックできます。

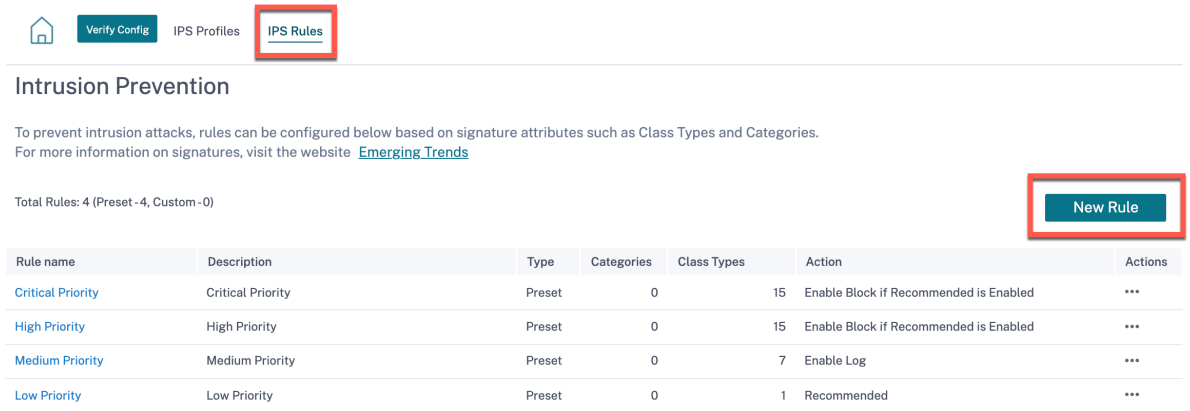
IPS はシグニチャベースの検出を使用します。この検出は、着信パケットを一意に識別可能なエクスプロイトおよび攻撃パターンのデータベースと照合します。シグニチャデータベースは、毎日自動的に更新されます。何千ものシグニチャが存在するため、シグニチャは [カテゴリ] と [クラス] タイプにグループ化されます。

IPS ルールを作成して、ネットワークに必要なシグニチャカテゴリまたはクラスタイプのみを有効にできます。侵入防止は計算上の影響を受けやすいプロセスであるため、ネットワークに関連する最小限のシグニチャカテゴリまたはクラスタイプのみを使用してください。

IPS プロファイルを作成して、IPS ルールの組み合わせを有効にできます。これらの IPS プロファイルは、ネットワーク全体にグローバルに関連付けることも、特定のサイトのみに関連付けることもできます。

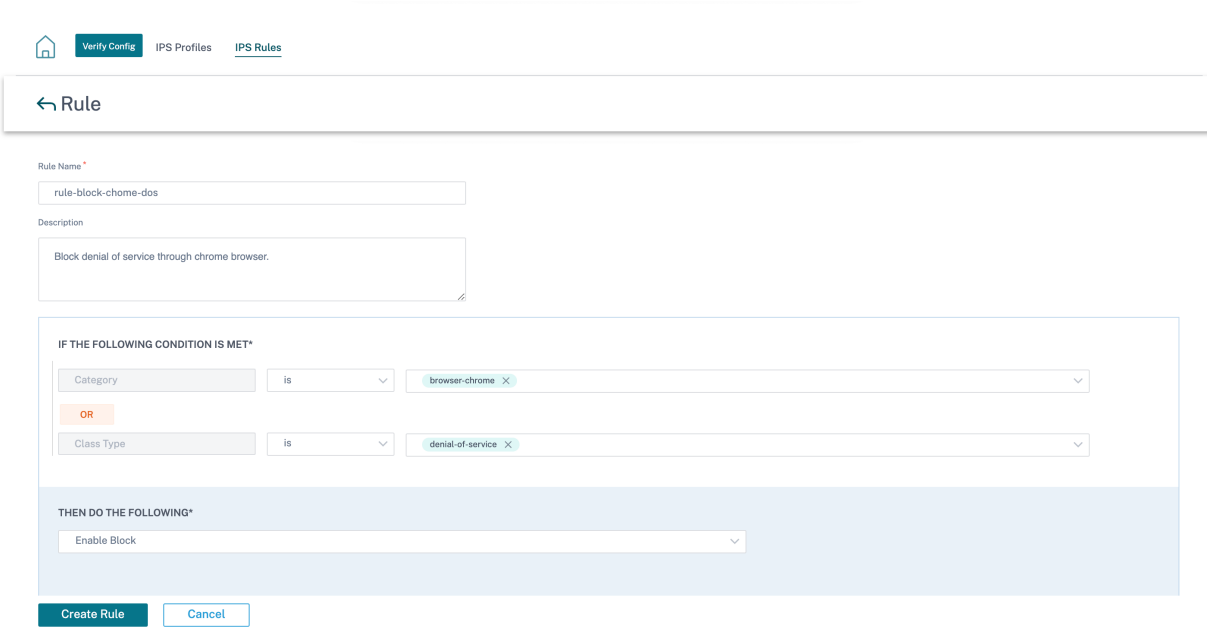
各ルールは複数の IPS プロファイルに関連付けることができ、各 IPS プロファイルは複数のサイトに関連付けることができます。IPS プロファイルを有効にすると、IPS プロファイルが関連付けられているサイトのネットワークトラフィックと、そのプロファイル内で有効になっている IPS ルールが検査されます。

IPS ルールを作成するには、ネットワークレベルで [設定] **>** [セキュリティ] **>** [侵入防止] **>** [**IPS** ルール] に移動し、[新しいルール] をクリックします。



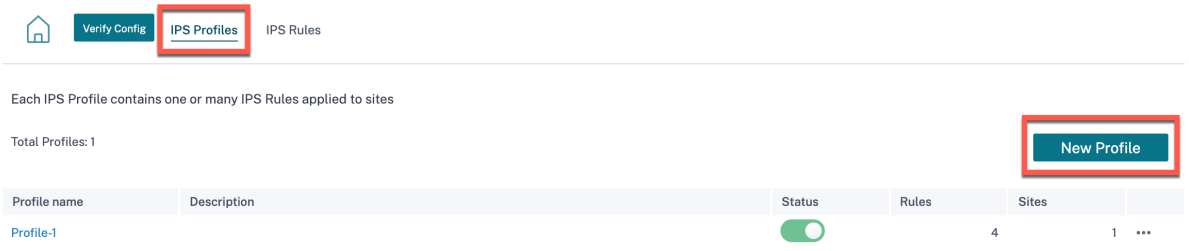
ルールの名前と説明を入力します。マッチカテゴリまたはクラスタイプのシグニチャ属性を選択し、ルールのアクションを選択して有効にします。次のルールアクションから選択できます。

ルールアクション	機能
推奨	シグニチャごとに推奨されるアクションが定義されています。シグニチャに対して推奨されるアクションを実行します。
ログを有効にする	ルール内のいずれかのシグニチャに一致するトラフィックを許可し、ログに記録します。
[推奨] が有効な場合はブロックを有効にする	ルールアクションが **Recommended** で、シグニチャの推奨アクションが **Enable Log** の場合は、ルール内のシグニチャのいずれかに一致するトラフィックをドロップします。
ブロックを有効にする	ルール内のシグニチャのいずれかに一致するトラフィックをドロップします。

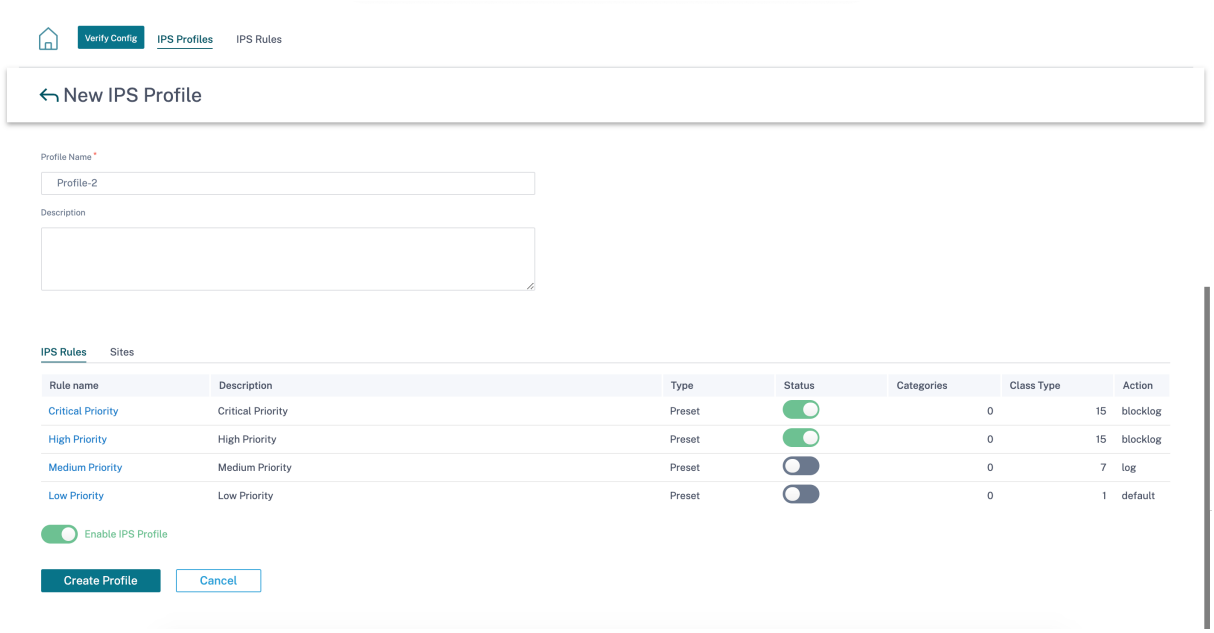


> 注
>
> - 侵入防止は処理に影響されやすいプロセスであるため、Edge セキュリティの導入に関連する最小限の署名カテゴリのみを使用してください。
> - SD-WAN ファイアウォールは、ポート転送されず、IPS エンジンに表示されないすべての WAN L4 ポート上のトラフィックをドロップします。これにより、些細な DOS 攻撃やスキャン攻撃に対する追加のセキュリティレイヤーが提供されます。

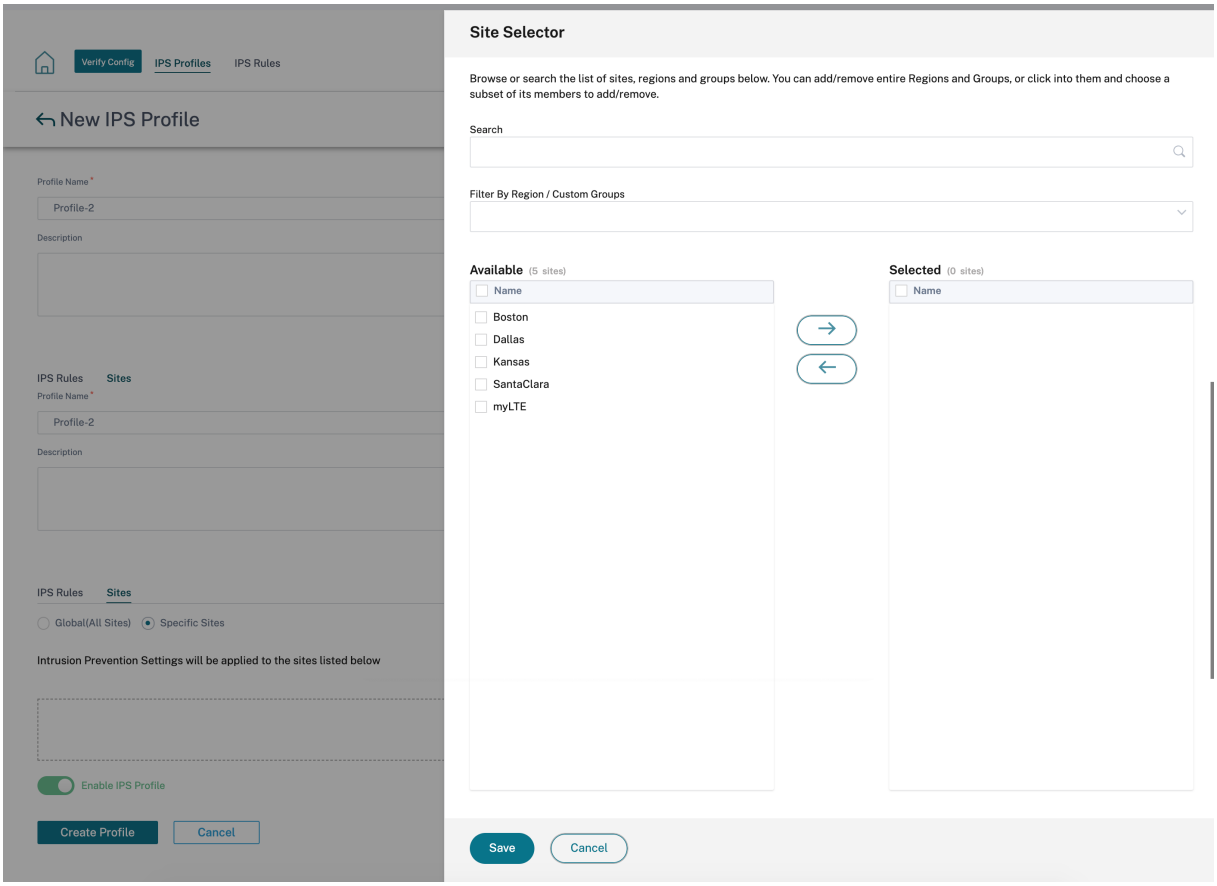
IPS プロファイルを作成するには、ネットワークレベルで [設定] **>** [セキュリティ] **>** [侵入防止] **>** [**IPS** プロファイル] に移動し、[新しいプロファイル] をクリックします。



IPS プロファイルの名前と説明を入力します。[**IPS** ルール] タブで必要な **IPS** ルールを有効にし、[**IPS** プロファイルを有効にする] をオンにします。



「サイト」タブで、「サイトを選択」をクリックします。サイトを選択し、[保存] をクリックします。[プロフィールを作成] をクリックします。



セキュリティプロファイルの作成中に、これらの IPS プロファイルを有効または無効にできます。セキュリティプロ

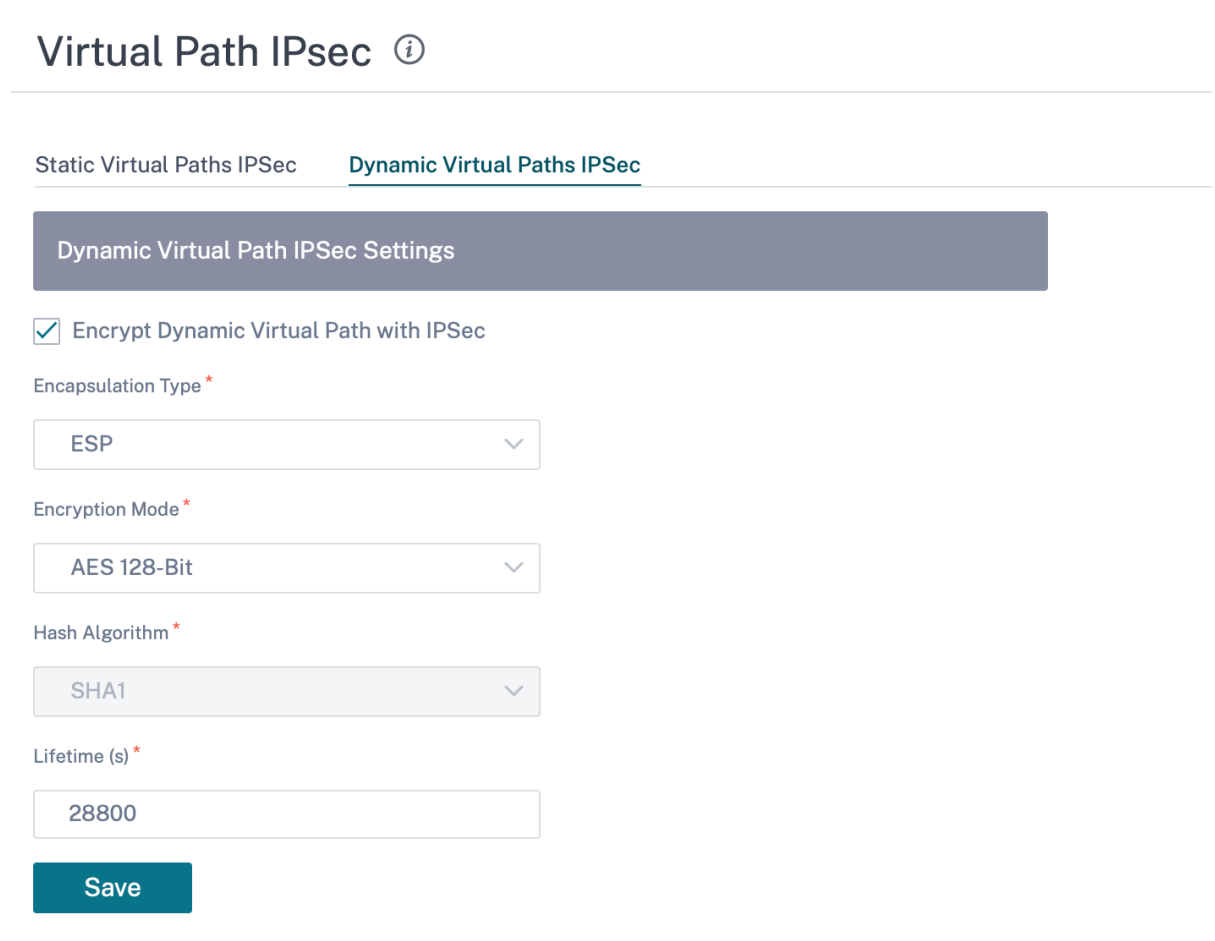
ファイルは、ファイアウォールルールを作成するために使用されます。詳細については、「セキュリティプロファイル—侵入防止」を参照してください。

仮想パス **IPsec**

仮想パス **IPsec** は、静的仮想パスと動的仮想パスを介してデータを安全に転送するための IPsec トンネル設定を定義します。IPsec トンネル設定を定義するには、[静的仮想パス **IPsec]** タブまたは **[**動的仮想パス IPsec] タブを選択します。

- カプセル化タイプ: 次のセキュリティタイプのいずれかを選択します。
  - **ESP**: データはカプセル化され、暗号化されます。
  - **ESP+Auth**: データは HMAC でカプセル化、暗号化、検証されます。
  - **AH**: データは HMAC で検証されます。
- 暗号化モード:ESP が有効な場合に使用される暗号化アルゴリズム。
- ハッシュアルゴリズム:HMAC の生成に使用されるハッシュアルゴリズム。
- 有効期間**:IPsec** セキュリティアソシエーションが存在するまでの推奨期間 **(**秒単位**)**。無制限の場合は 0 を入力します。

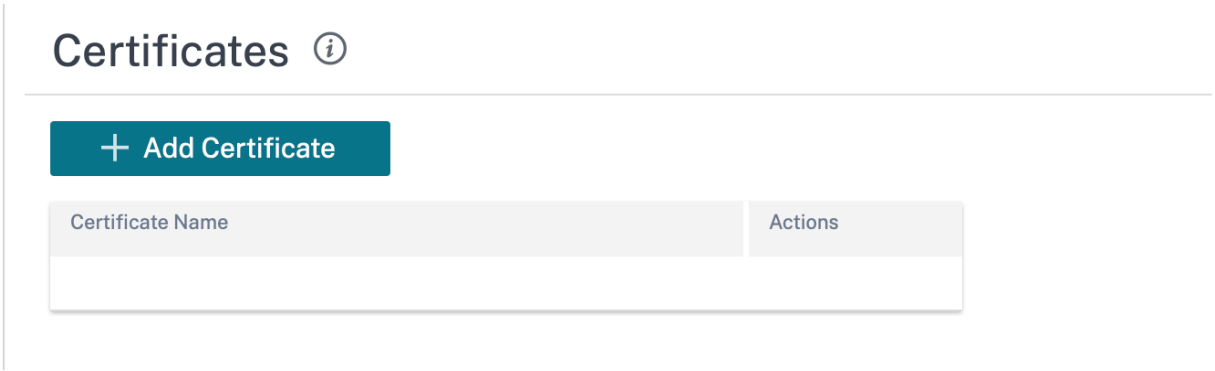
IPsec サービスの構成については、「IPsec サービス」を参照してください。



監査エラーを確認するには、「構成を確認」をクリックします

証明書

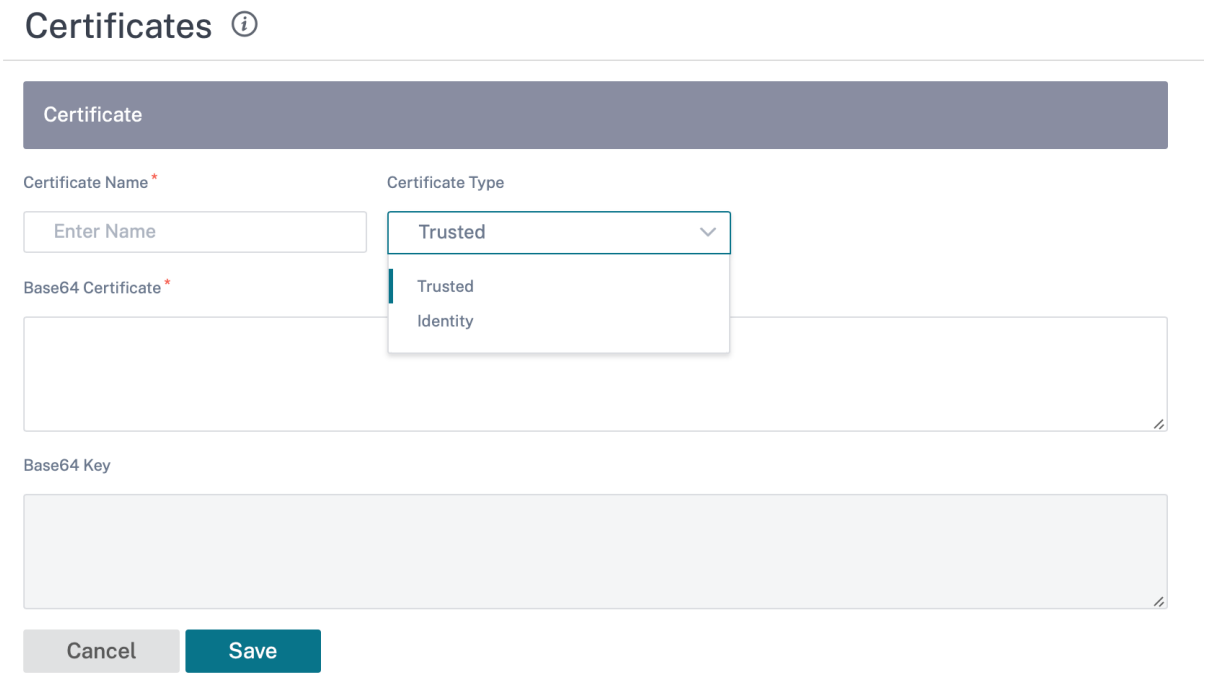
証明書には、「アイデンティティ」と「信頼済み」の 2 種類があります。ID 証明書は、メッセージの内容と送信者の身元を検証するために、データの署名または暗号化に使用されます。信頼された証明書は、メッセージ署名の検証に使用されます。Citrix SD-WAN アプライアンスは、ID 証明書と信頼された証明書の両方を受け入れます。管理者は、構成エディタで証明書を管理できます。



監査エラーを確認するには、「構成を確認」をクリックします

証明書を追加するには、「証明書を追加」をクリックします。

- 証明書名: 証明書の名前を入力します。
- 証明書の種類: ドロップダウンリストから証明書の種類を選択します。
  - **ID** 証明書:ID 証明書では、署名者が証明書の秘密鍵を利用できるようにする必要があります。ID 送信者の内容と ID を検証するためにピアによって信頼される証明書またはその証明書チェーン。構成されたアイデンティティ証明書とそれぞれのフィンガープリントが、構成エディタに表示されます。
  - 信頼できる証明書: 信頼できる証明書は、ピアの身元を検証するために使用される自己署名の中間認証局 (CA) 証明書またはルート CA 証明書です。信頼された証明書には秘密キーは必要ありません。構成された信頼された証明書とそれぞれのフィンガープリントがここに表示されます。

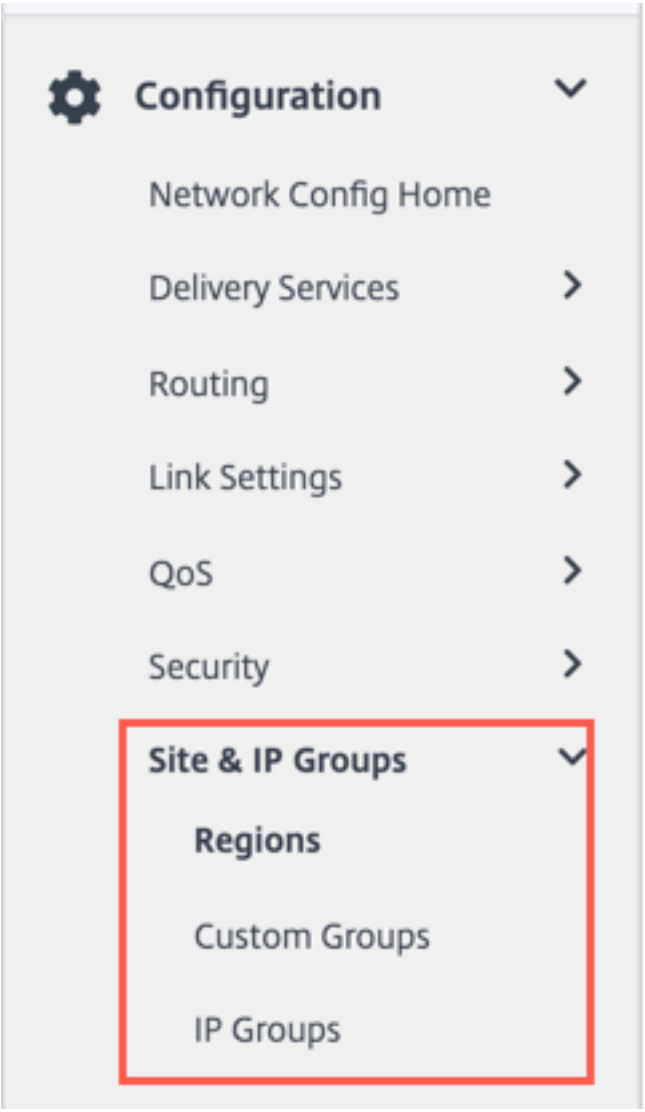


サイトおよび **IP** グループ

October 26, 2022

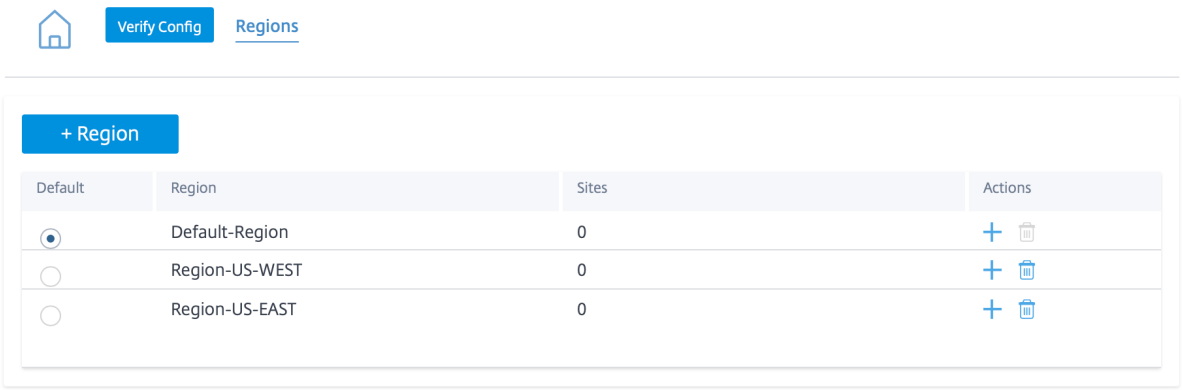
管理者は、サイトまたは IP アドレスをグループ化して、複数のサイトまたはネットワークアドレスで共通のアプリケーションポリシーを簡素化し、レポートのフィルタとしても使用できます。

リージョン、サイト、IP グループを表示するには、[設定] > [サイト **& IP** グループ] に移動します。



リージョン

リージョンは、数百から数千のサイトにまたがる大規模なネットワーク内に管理境界を作成するのに役立ちます。組織に複数の管理（または地理的）境界にまたがる大規模なネットワークがある場合は、ネットワークをセグメント化するリージョンの作成を検討できます。



現在、リージョンごとに最大 1000 のサイトがサポートされています。各リージョンには、リージョンのハブおよび Controller として機能するリージョナルコントロールノード (RCN) が必要です。そのため、ネットワークに 500 を超えるサイトがある場合は、通常、マルチリージョン展開を検討します。デフォルトでは、すべてのネットワークは単一リージョンネットワークであり、マスターコントロールノード（MCN）はすべてのサイトのハブおよびコントロールノードとして機能します。1 つ以上のリージョンを追加すると、ネットワークはマルチリージョンネットワークになります。MCN に関連する地域はデフォルト地域と呼ばれます。

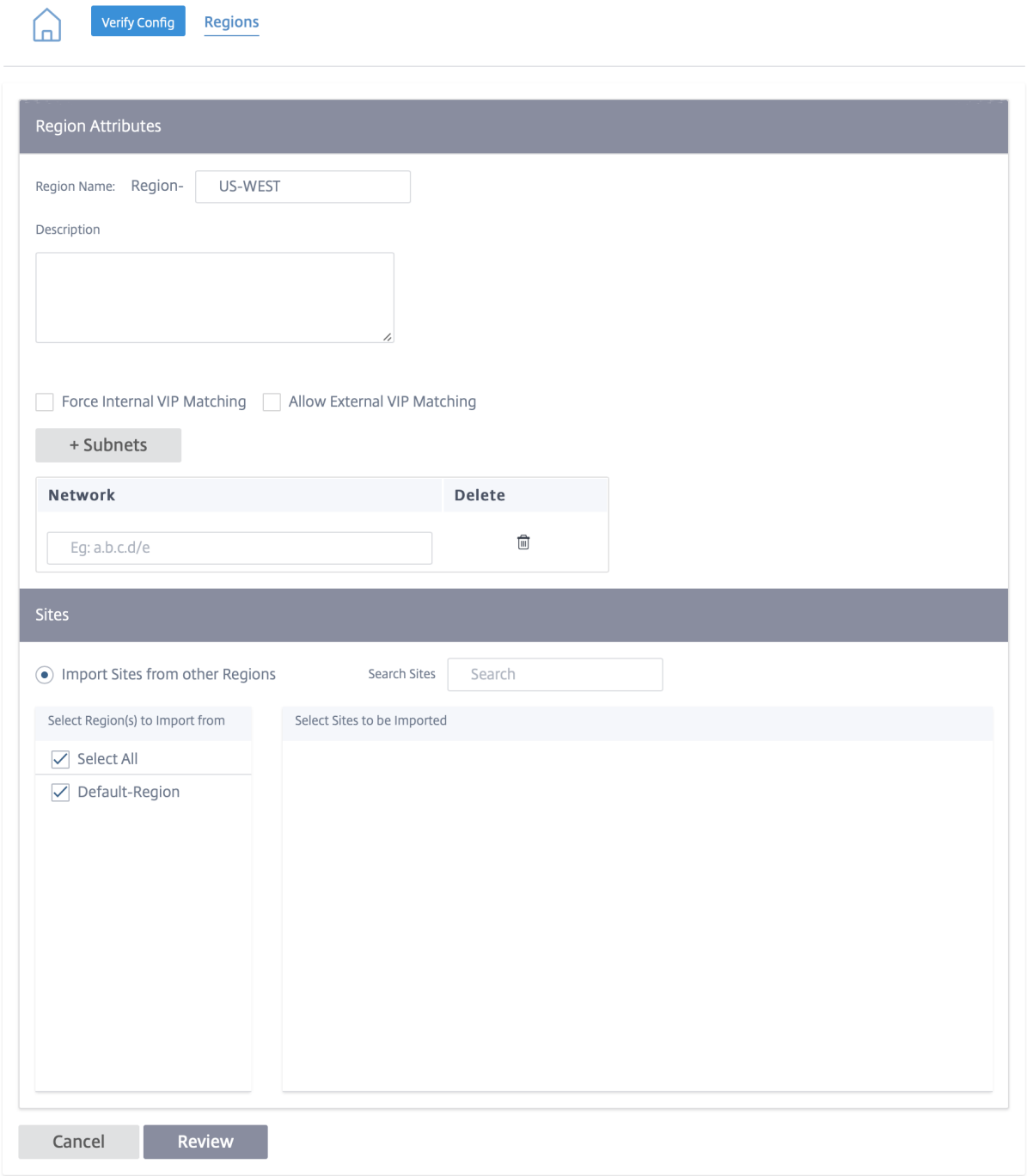
マルチリージョンネットワークは、MCN が複数の RCN を制御する階層アーキテクチャをサポートします。各 RCN は、複数のブランチサイトを制御します。マルチリージョン展開でも、MCN をサイトのサブセットのダイレクトハブノードとしてダブルアップし、残りのサイトでそれぞれの RCN をハブノードとして使用することができます。

MCN によって直接管理されているサイト、つまり RCN と MCN によって直接管理されているその他のサイトは、デフォルトリージョンにあると言われます。デフォルトのリージョンは、他のリージョンが追加される前のネットワークの唯一のリージョンになります。他のリージョンを追加したら、「デフォルト」オプションを選択して、目的のリージョンをデフォルトリージョンとして使用できます。

リージョンを作成する手順は、次のとおりです。

1. [**+** 地域] をクリックします。リージョン名と説明を入力します。
2. [強制内部 **VIP** マッチング**]** または **[**外部 **VIP** マッチングを許可**]** のどちらを使用するかに基づいて、インターバル **VIP** マッチングを有効にします。
    - 強制内部 VIP 照合：有効にすると、リージョン内のすべての非プライベート仮想 IP アドレスが、設定されたサブネットに一致するように強制されます。
    -
3. [**+** サブネット] をクリックしてサブネットを追加します。ネットワーク アドレスを入力します。ネットワークアドレスは、サブネットの IP アドレスとマスクです。
4. サイトを選択します。
5. [レビュー] をクリックし、[保存] をクリックします。新しく作成されたリージョンが、既存のリージョンのリストに追加されます。

> 注:
>
> お客様が持つことができるのは、リージョン内の静的仮想パスまたは動的仮想パスのみです。



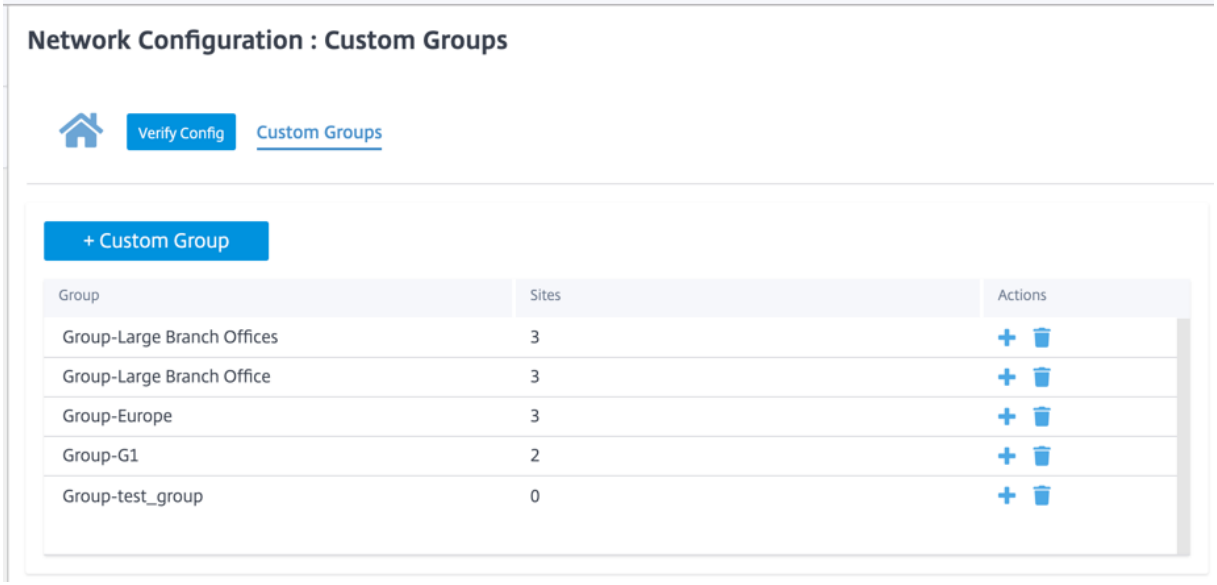
リージョンが正常に作成されると、その領域の下にサイトを配置できます。

> 注:
>
> 異なるリージョンのブランチ間で動的仮想パスを確立することはできません。

監査エラーを確認するには、「構成を確認」をクリックします。

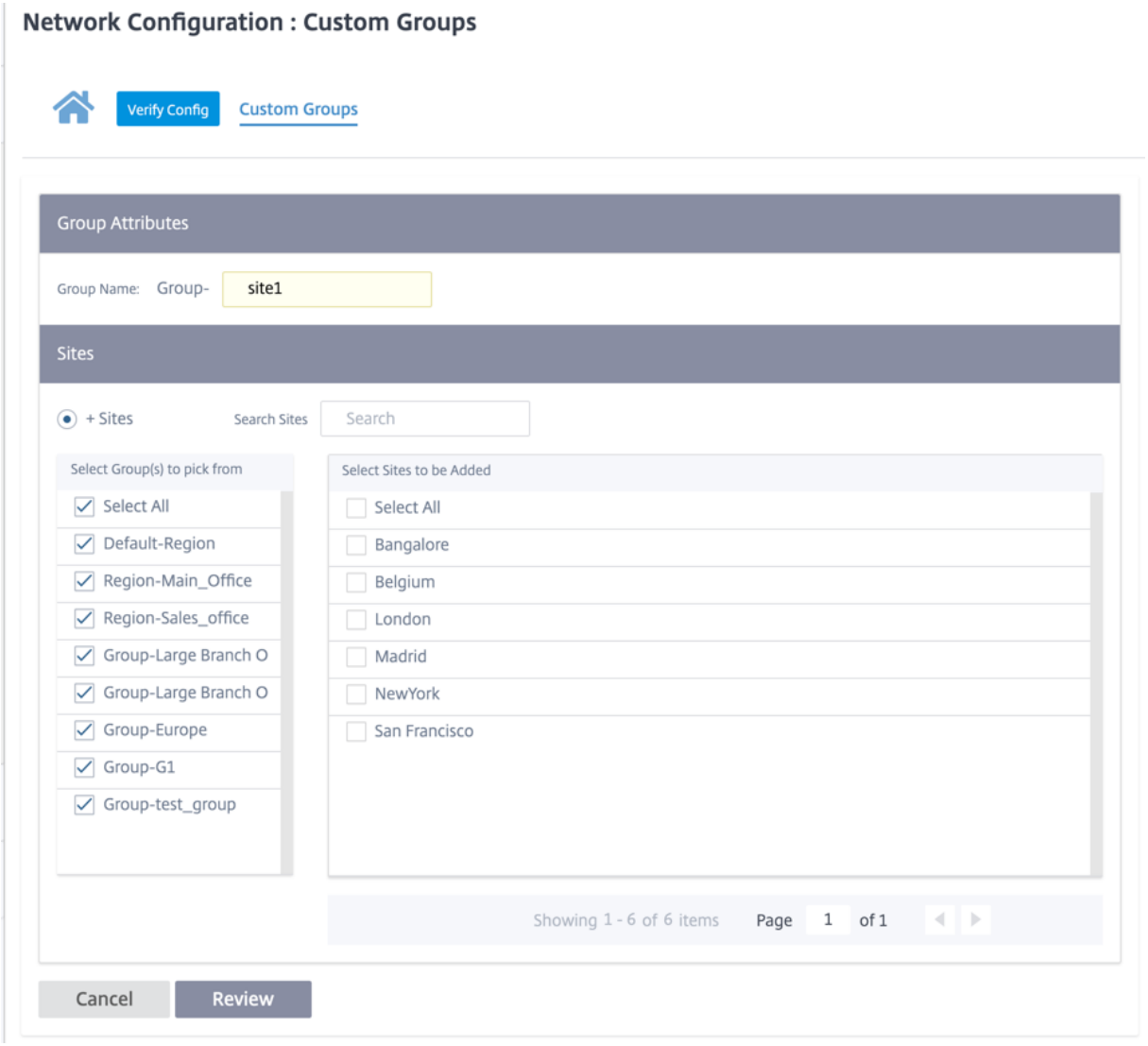
カスタムグループ

カスタムグループを使用すると、ユーザーは必要に応じてサイトを柔軟にグループ化できます。ユーザーは、各サイトを個別に処理しなくても、一度にサイトのグループにポリシーを適用できます。グループは、ダッシュボード、レポート、またはネットワーク構成のフィルターとしても使用できます。リージョンとは異なり、グループはサイトに関して重複する可能性があります。つまり、同じサイトを複数のグループに含めることができます。



たとえば、ユーザーは **Business Critical Sites** という名前のグループを作成して、すべてのビジネスクリティカルサイトに共通のポリシーを設定できます。また、ユーザーは、各自の正常性とパフォーマンスをグループとして個別に監視することもできます。たとえば、これらのサイトの中には、大規模支店グループの一部である場合もあります。

カスタムサイトグループは、レポート目的でサイトを論理的にグループ化する方法を提供します。カスタムグループを作成し、各カスタムグループにサイトを追加できます。カスタムグループを作成するには、**+ Custom Group** をクリックします。グループ名を入力し、サイトを選択または追加します。[レビュー] をクリックし、[保存] をクリックします。

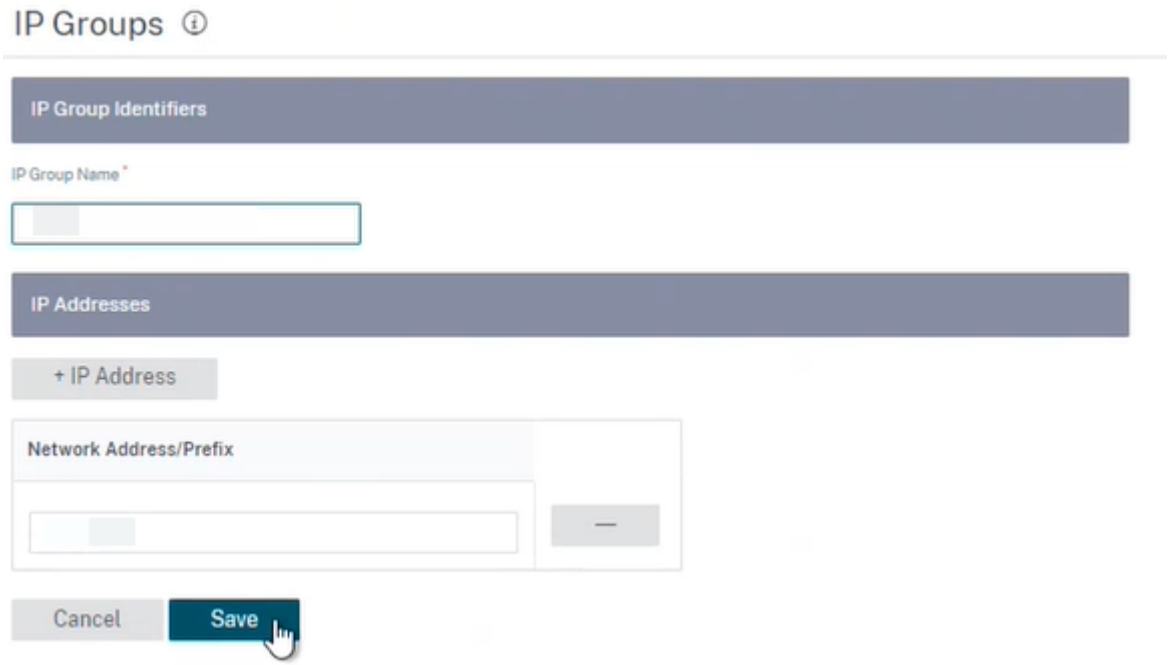


監査エラーを確認するには、「構成を確認」をクリックします。

IP グループ

Citrix SD-WAN Orchestrator サービスでは、IP グループ（ネットワークオブジェクト）を追加するオプションが導入されています。このオプションを使用すると、サブネットごとにフィルターを作成するのではなく、ルートフィルターを定義する際に **IP** グループを使用して **IP** アドレスとネットワークアドレスをグループ化できます。これらのグループは、必要に応じて設定およびポリシーで使用できます。毎回個々の IP アドレスをキー入力する必要はありません。

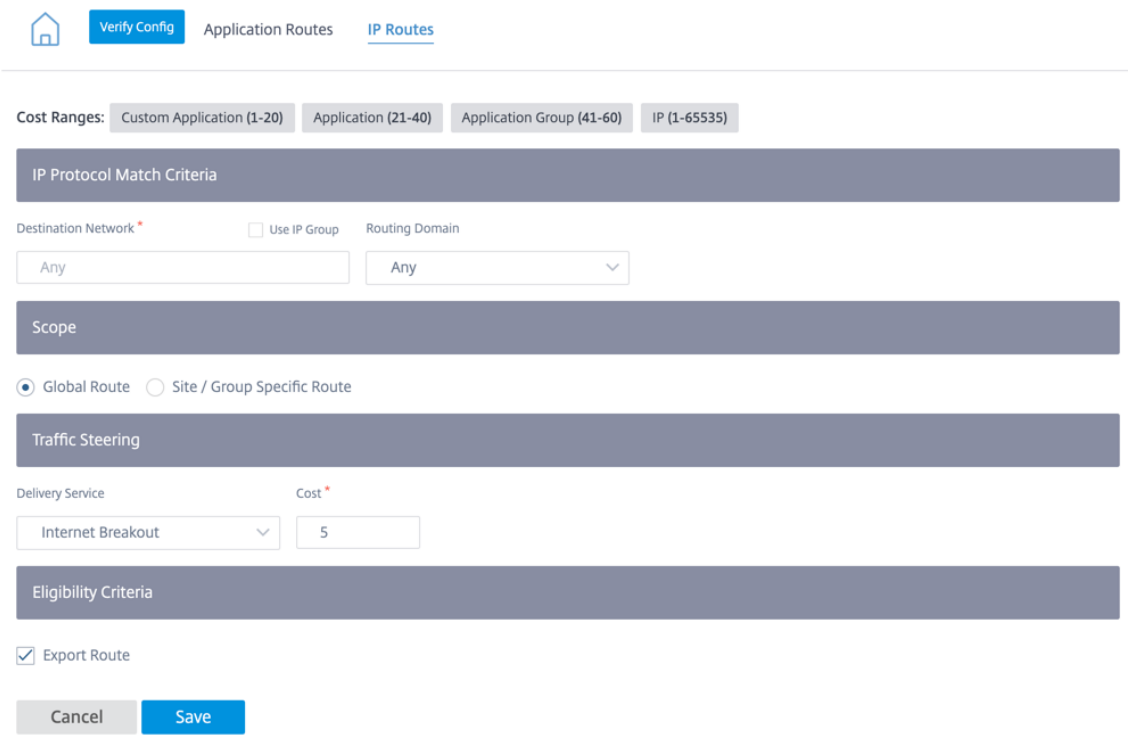
IP グループを作成し、ネットワークアドレスとプレフィックスを追加できます。**IP** グループを作成するには、**IP** グループを選択し、+ IP グループをクリックします。グループ名を指定します。[**+ IP** アドレス] をクリックし、**IP** グループに追加する IP アドレスを入力します。



監査エラーを確認するには、「構成を確認」をクリックします

次の機能は IP グループを利用します。

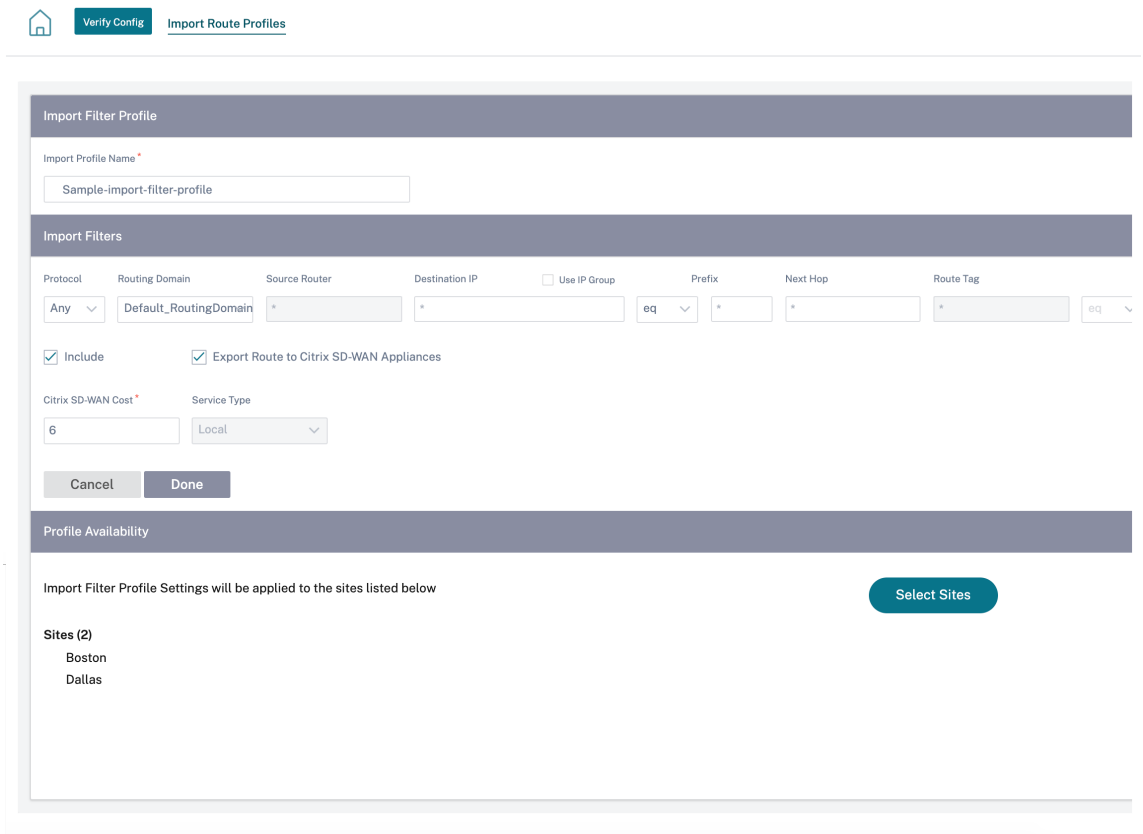
- **IP** ルートの作成: 宛先ネットワークを追加するか、[**IP** グループを使用] チェックボックスをオンにして既存の IP グループを選択できます。詳細については、「IP グループ」を参照してください。



- ルートプロファイルのインポート: インポートフィルタプロファイルの作成時に、ネットワーク上で使用可能な IP グループのリストから選択できます。

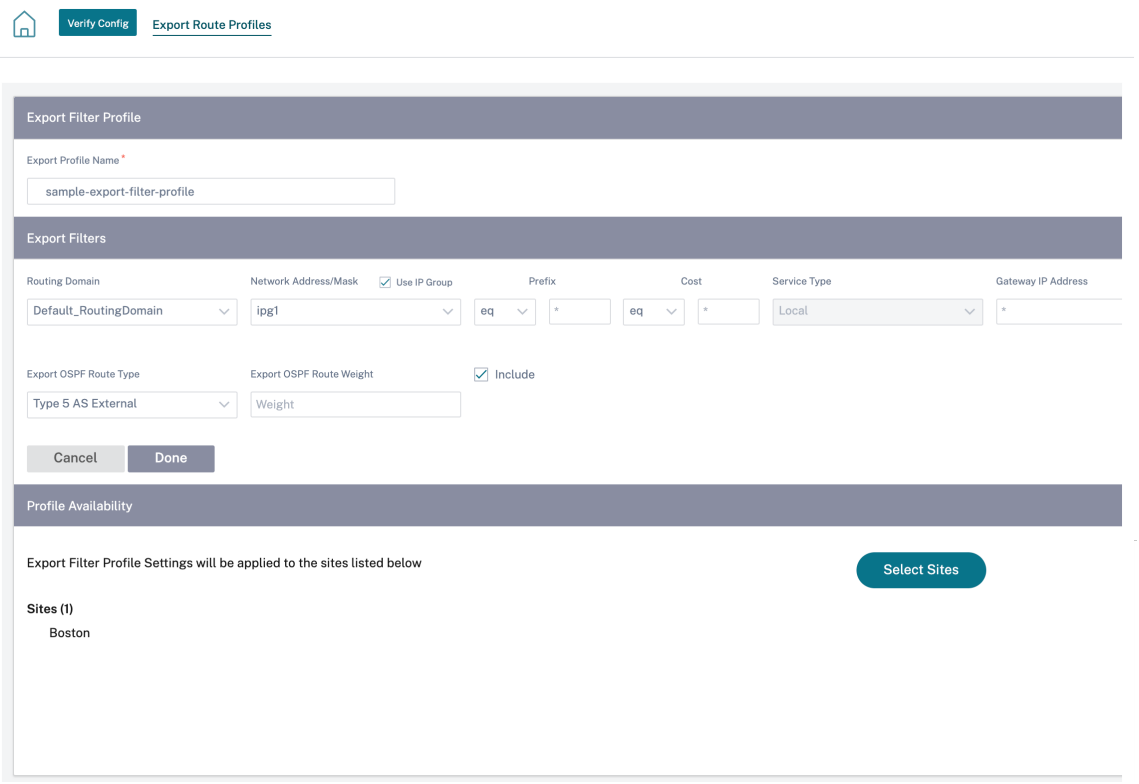
  宛先ネットワークを追加するか、[**Use IP Group**] チェックボックスをオンにして既存の IP グループを選択できます。

  詳細については、「ルートプロファイルのインポート」を参照してください。



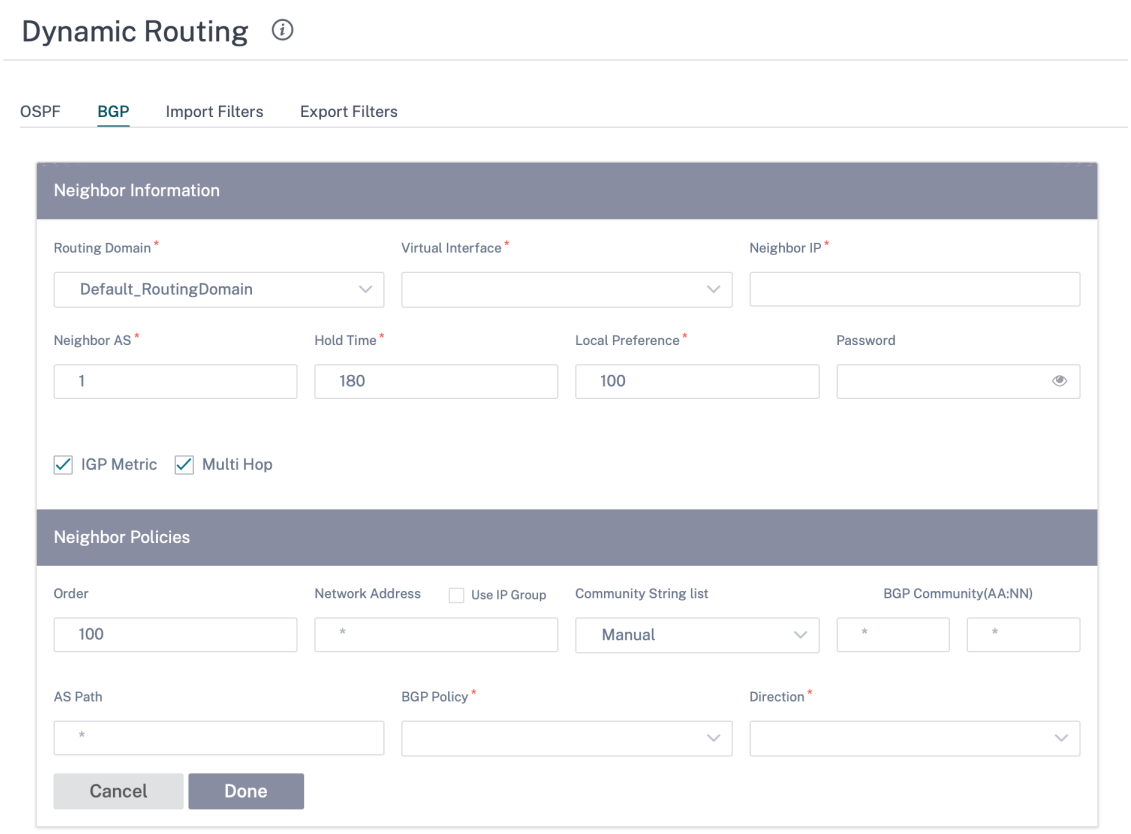
- ルートプロファイルのエクスポート: エクスポートフィルタプロファイルの作成時に、ネットワークアドレスマスクを追加するか、[**Use IP Group**] チェックボックスをオンにして既存の IP グループを選択できます。

  詳細については、「ルートプロファイルのエクスポート」を参照してください。



- **BGP** ネイバーポリシー: ネイバールータ用に設定済みの BGP ポリシーを追加するときに、ネットワークアドレスを追加するか、[**Use IP Group**] チェックボックスをオンにして既存の IP グループを選択できます。

  詳細については、「BGP」を参照してください。



アプリケーション設定とグループ

October 26, 2022

このセクションでは、アプリケーションをカスタム定義し、ポリシーで使用するアプリケーションのグループ化、QoS プロファイル、および DNS 設定を行うことができます。

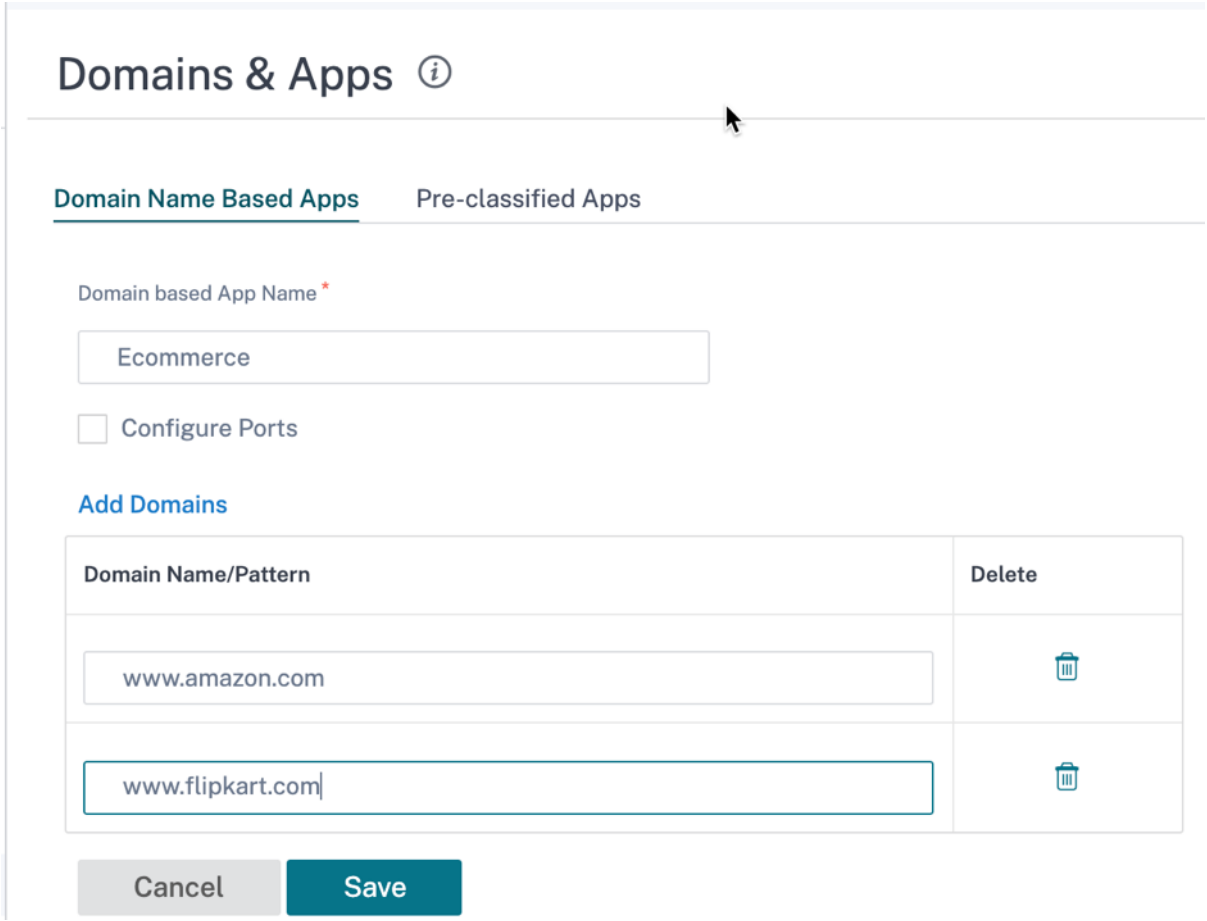
アプリケーショングループは、定義済みアプリケーションとカスタムアプリケーションの両方に対して定義できます。アプリケーショングループには、セキュリティポリシーを定義する際に同様の処理が必要なアプリケーションが含まれます。

アプリケーションステアリングやファイアウォールルールなどのポリシーを定義するときに、アプリケーショングループを頻繁に再利用できます。これにより、個々のアプリケーションに対して複数のエントリを作成する必要がなくなります。同様に、アプリケーションサービスを使用している間、アプリケーショングループは、単純で一貫した再利用のために、一意の名前を持つ共通アプリケーションをサポートします。

アプリケーショングループを表示するには、［構成］**>**［アプリ設定とグループ］に移動します。

ドメインとアプリケーション

ドメインとアプリページの公開アプリケーションのリストにないドメイン名に基づいて内部アプリケーションを作成できます。ドメイン名に基づいてアプリケーションを作成するには、ネットワークレベルで [アプリの設定とグループ] **>** [ドメインとアプリ] **>** [ドメイン名ベースのアプリ] タブに移動し、[新しいドメイン名ベースのアプリケーション] をクリックします。アプリケーション名を入力し、ドメイン名またはパターンを追加します。完全なドメイン名を入力することも、先頭にワイルドカードを使用することもできます。



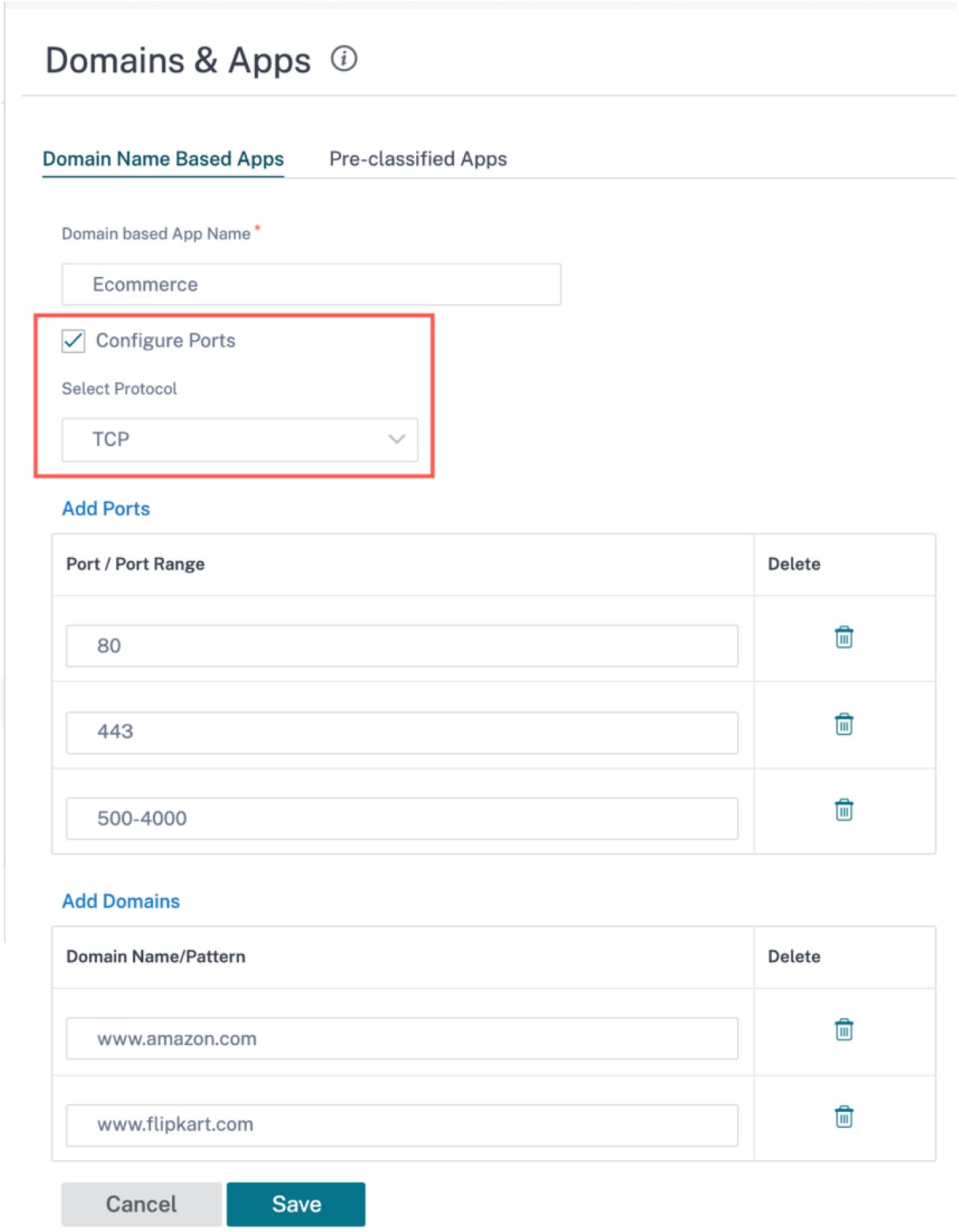
ドメイン名ベースのアプリケーションはすべて、アプリケーションルーティング、アプリケーションルール、およびファイアウォールポリシーに表示されます。

Citrix SD-WAN 11.4.2 リリース以降では、「ドメイン名ベースのアプリケーション」で「ポートの構成」チェックボックスオプションが使用できるようになりました。**Configure Ports** チェックボックスを有効にすると、ドメインベースのアプリケーション用に複数のポート、ポート範囲、プロトコル (TCP/UDP/任意) のグループを柔軟に設定できます。

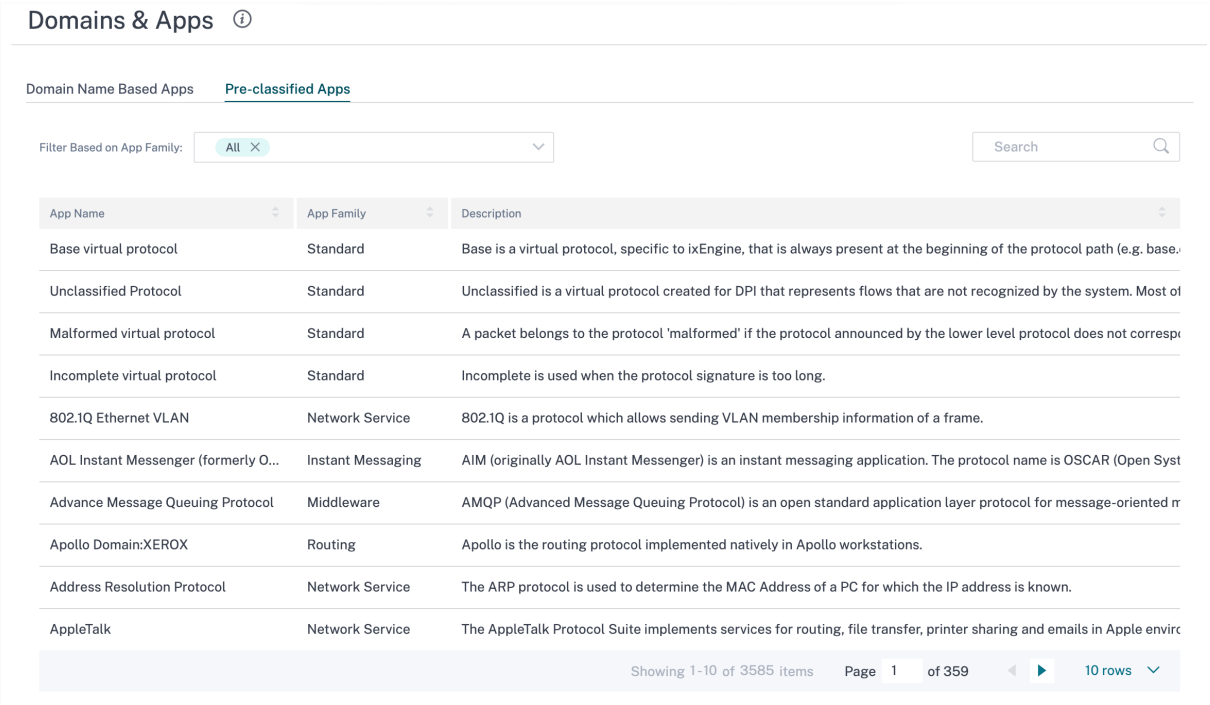
以前は、****** ポート **80** と **443**、****** およびプロトコル **Any** は、アプリケーションにグループ化されたドメインでサポートされていました。**Configure Ports** チェックボックスをオフにしても、同じ動作になります。デフォルトでは、ポートの設定チェックボックスは無効になっています。

Configure Port チェックボックスを選択すると、TCP、UDP、Any などのプロトコル選択に加えて、必要に応じ

て任意のポートまたはポート範囲を編集、追加、削除できます。デフォルトでは、プロトコル値は **Any** に設定され、ポートは **80** と **443** に設定されます。



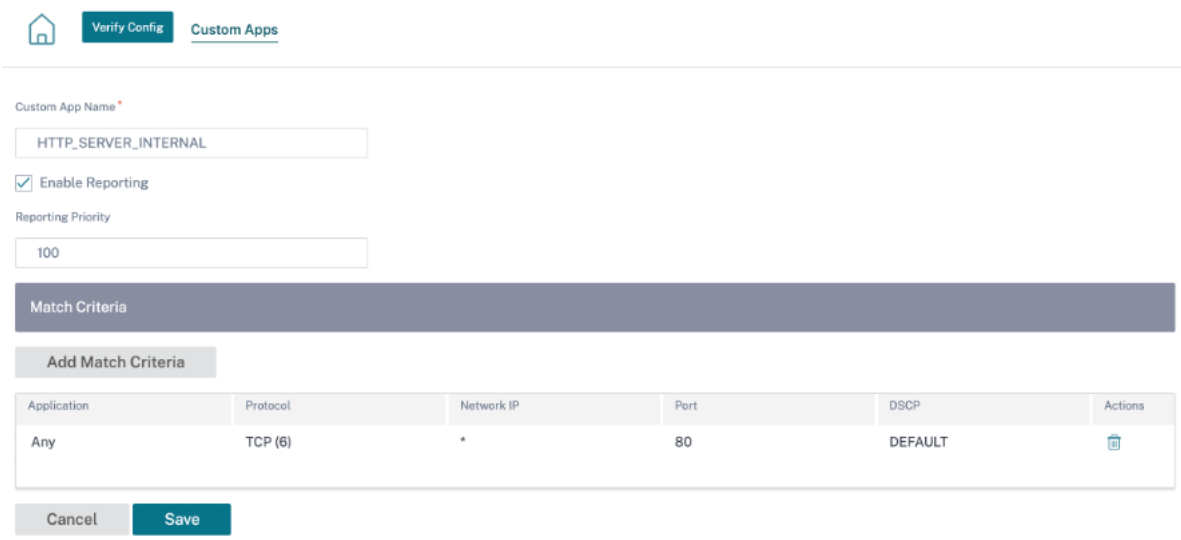
事前分類済みアプリタブでは、事前定義済みのアプリケーションのリストを表示することもできます。検索バーを使用して特定のアプリケーションを検索したり、アプリケーションファミリに基づいてリストをフィルタリングしたりできます。



カスタムアプリケーション

カスタムアプリケーションは、公開アプリケーションのリストにない内部アプリケーションまたは IP ポートの組み合わせを作成するために使用されます。管理者は、IP アドレスやポート番号の詳細を毎回参照することなく、必要に応じて複数のポリシーで使用できる IP プロトコルに基づいてカスタムアプリケーションを定義する必要があります。

カスタムアプリケーションを作成するには、ネットワークレベルで [アプリの設定とグループ**] > [**カスタムアプリ] に移動し、[**+** カスタムアプリケーション] をクリックしてカスタムアプリケーションの名前を指定します。IP プロトコル、ネットワーク IP アドレス、ポート番号、DSCP タグなどの一致基準を指定します。この条件に一致するデータフローは、カスタムアプリケーションとしてグループ化されます。

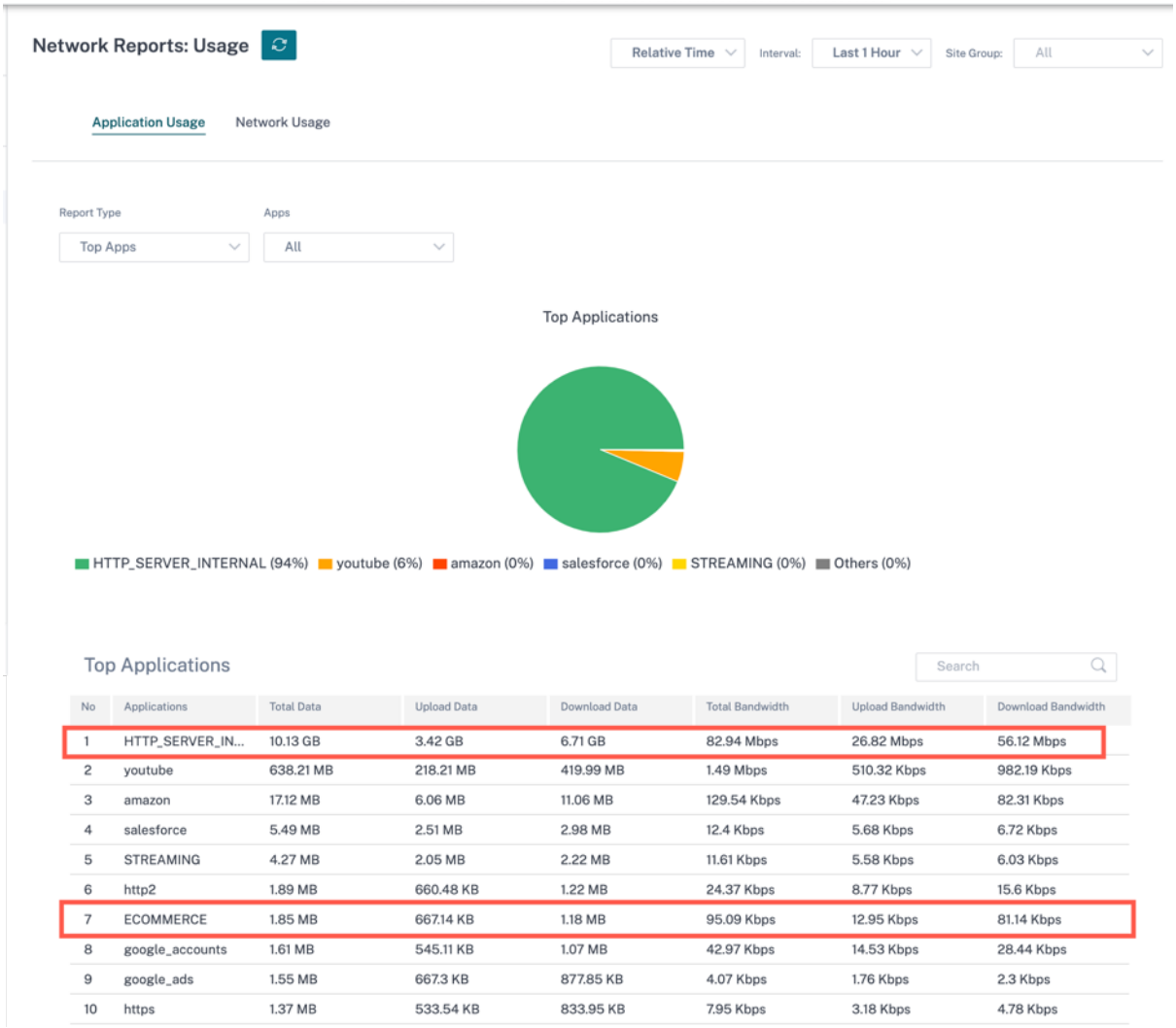


保存すると、カスタムアプリケーションがリストに表示され、必要に応じて編集または削除できます。

IP プロトコルベースのカスタムアプリケーションとアプリケーショングループに [レポートを有効にする] チェックボックスが追加されました。「レポートを有効にする」チェックボックスを選択して、レポートの優先順位を指定する必要があります。

[レポートを有効にする] チェックボックスを選択すると、[レポート] > [使用状況] に IP カスタムアプリケーショントラフィックが表示されます。

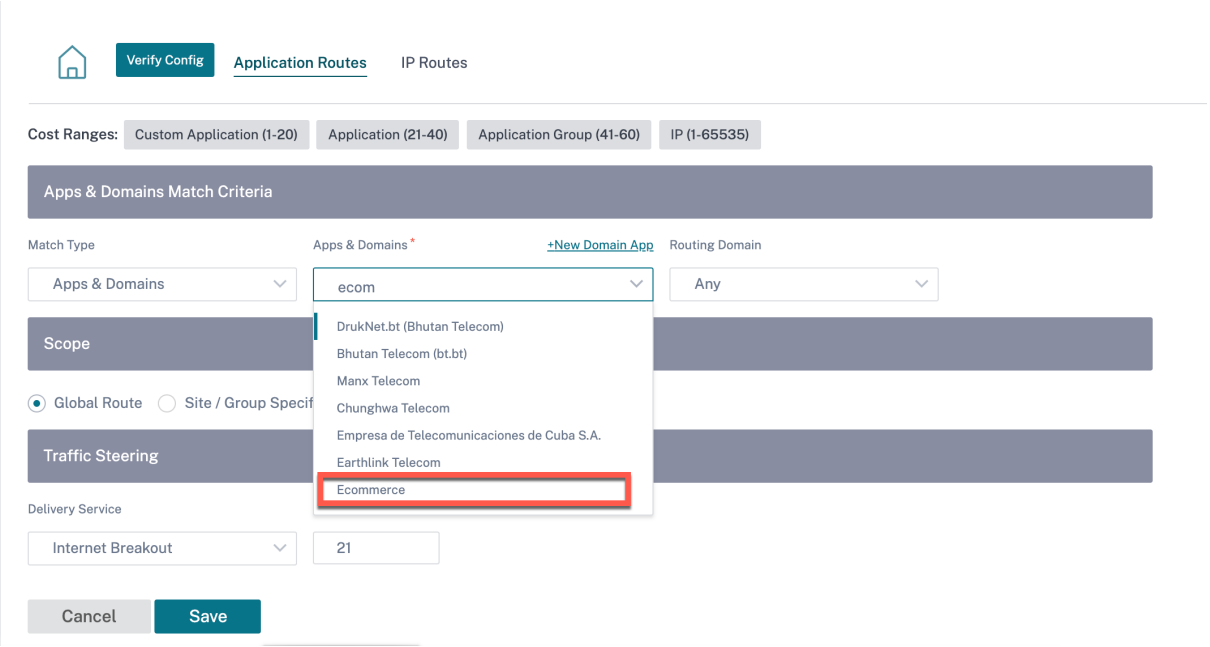
レポート優先度は、IP プロトコルベースのカスタムアプリケーションまたはアプリケーショングループがレポート対象として選択される順序です。レポートを有効にして一致するものが複数ある場合は、優先度の高いカスタムアプリケーションまたはレポート作成用のアプリケーショングループを選択すると便利です。たとえば、カスタムアプリケーションのレポート優先度が 1 に設定されている場合、カスタムアプリケーションのレポート優先度が最も高くなります。一方、レポートの優先度が 100 に設定されている場合、カスタムアプリケーションのレポート優先順位はずっと低くなります。



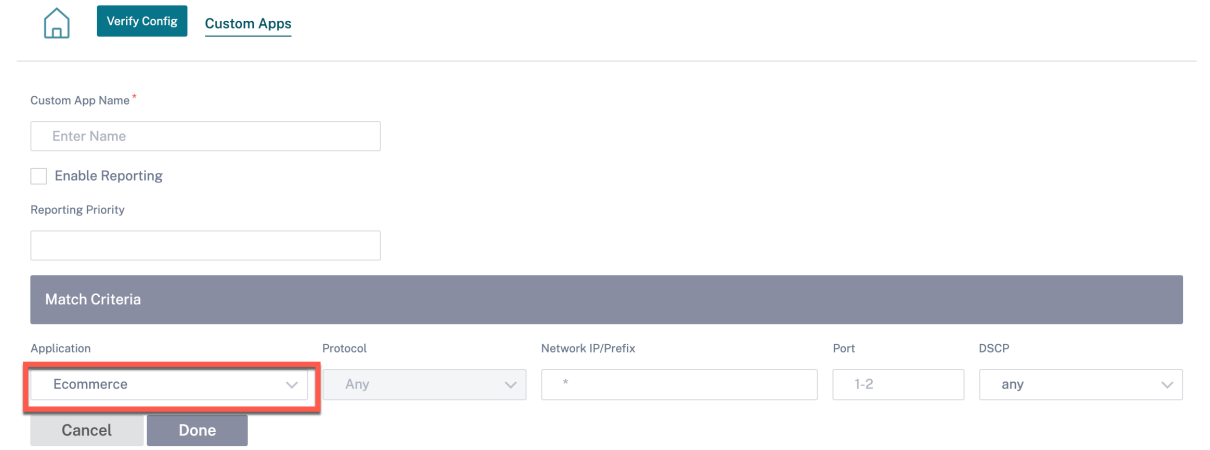
注

- ドメイン名ベースのアプリケーションを使用するには、アプリケーションルート、QoS ポリシー、およびファイアウォールポリシーを作成する際に、アプリとドメインを一致条件としてリストする必要があります。
- カスタムアプリケーションを使用するには、アプリケーションルート、QoS ポリシー、およびファイアウォールポリシーを作成する際に、一致基準としてカスタムアプリケーションを指定する必要があります。

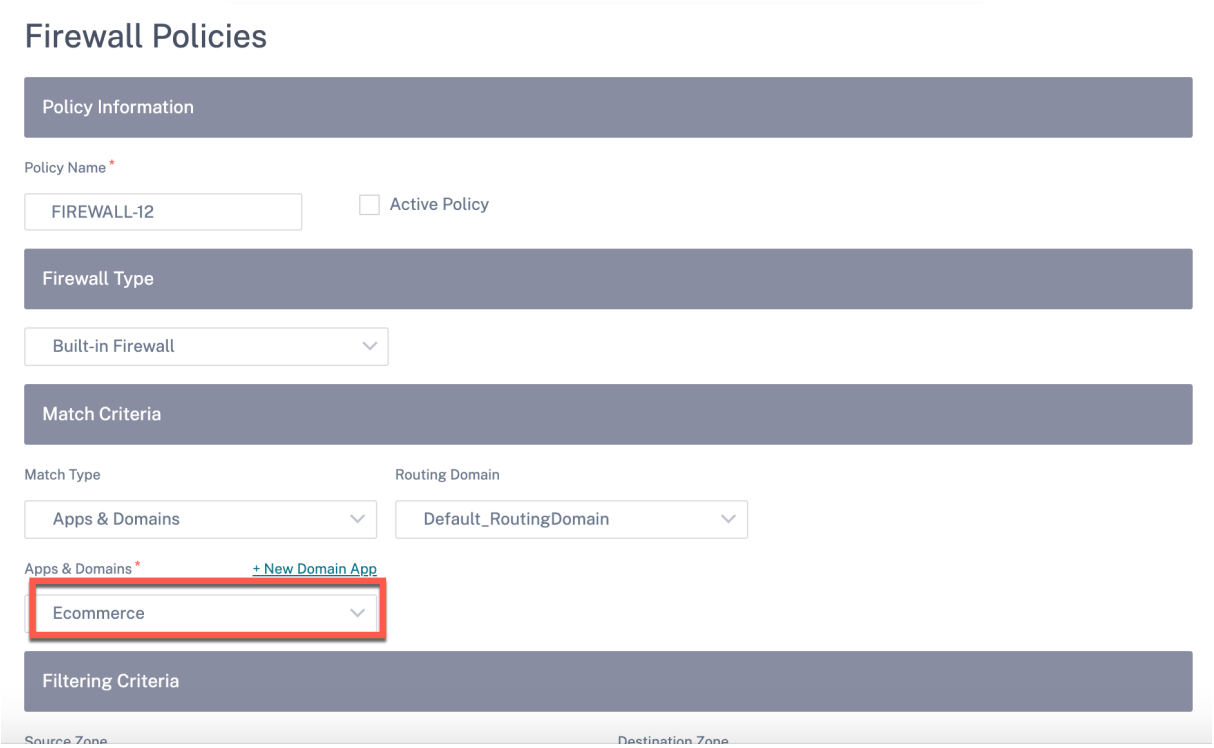
カスタムアプリケーションを作成したら、アプリケーションルーティングを実行するには、[ルーティング] > [ルーティングポリシー] **> [+** アプリケーションルート] に移動し、[マッチタイプ] ドロップダウンリストから [カスタムアプリケーション] を選択します。同様に、ドメイン名ベースのアプリケーションの場合は、「マッチタイプ」ドロップダウンリストから「アプリとドメイン」を選択します。



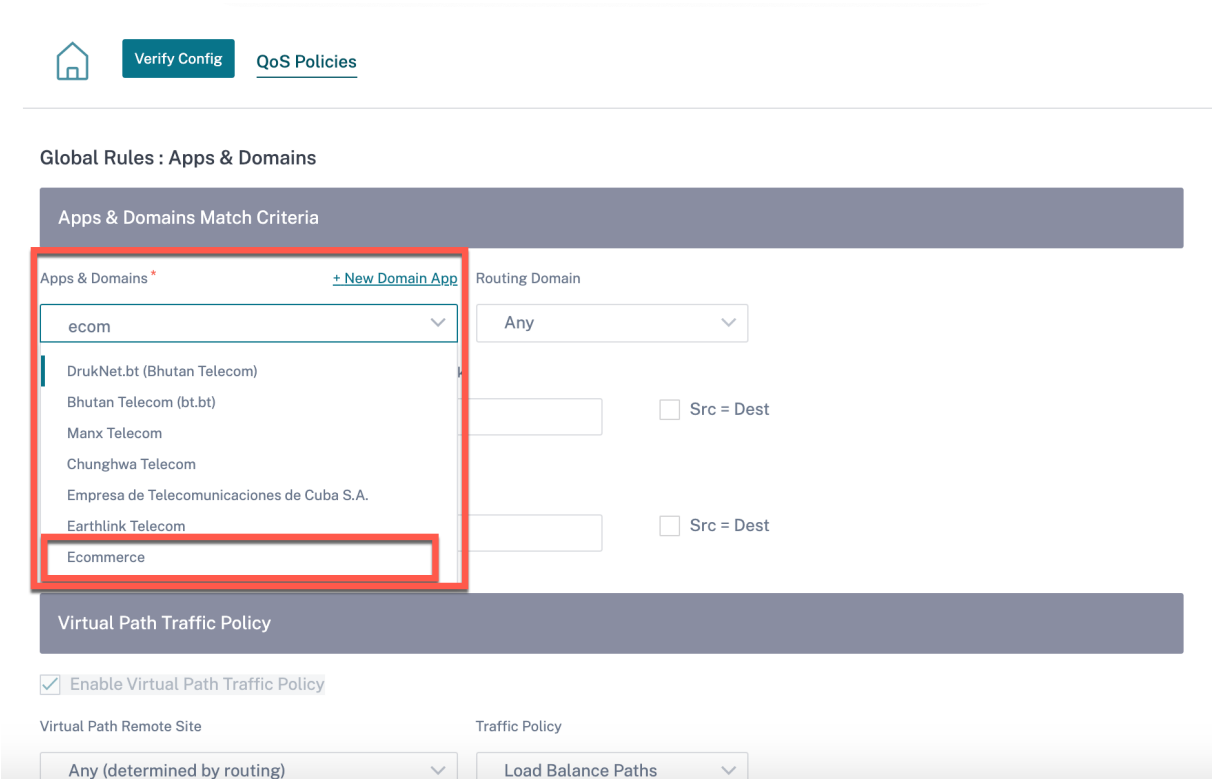
IP プロトコルカスタムアプリケーションを作成するときに、一致基準に基づいてドメイン名ベースのアプリケーションを選択することもできます。



同様に、ファイアウォールポリシーの下にカスタムアプリケーションを表示するには、[セキュリティ**] > [**ファイアウォールポリシー] に移動します。このアプリケーションは、どのタイプのポリシー（グローバルオーバーライド/サイト固有/グローバルポリシー）にも使用できます。「新規ルールを作成」をクリックし、「一致基準」で、「一致タイプ」ドロップダウンリストから「カスタムアプリケーション」を選択します。ドメイン名ベースのアプリケーションを表示するには、マッチタイプドロップダウンリストから「アプリとドメイン」を選択します。



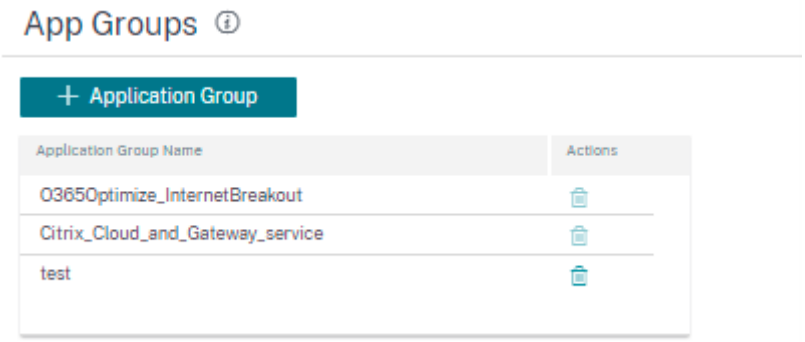
ドメイン名ベースのカスタムアプリケーションは、グローバルルールまたはサイト/グループ固有ルールの両方で表示できます。ドメイン名ベースのアプリケーションを表示するには、[QoS] **> [QoS** ポリシー**] > [**グローバルルール**] > [**アプリケーションルール**] > [+** アプリケーションルール] に移動し、[アプリケーションとドメイン] ドロップダウンリストから必要なドメイン名ベースのアプリケーションを選択します。カスタムアプリケーションを表示するには、[**QoS] > [QoS** ポリシー**] > [**グローバルルール**] > [**カスタムアプリケーションルール**] > [+** カスタムアプリケーションルール] に移動し、[カスタムアプリケーション] ドロップダウンリストから必要なカスタムアプリケーションを選択します。



監査エラーを確認するには、「構成を確認」をクリックします。

アプリケーショングループ

アプリケーショングループを使用すると、管理者は類似のアプリケーションをグループ化して共通のポリシーで使用できます。必ずしも個々のアプリケーションごとにポリシーを作成する必要はありません。

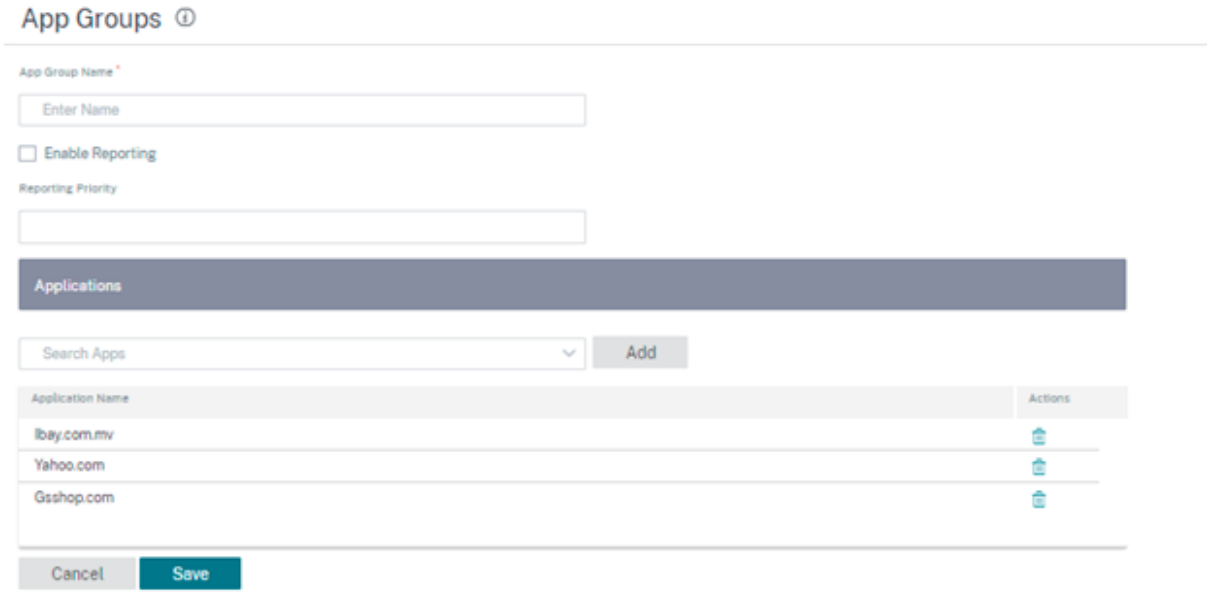


アプリケーショングループは、「アプリケーショングループの追加 ** 」オプションを使用して作成できます。アプリケーションロールごとにポリシーを作成する際に、同じアプリケーショングループを参照できます。特定のグループに対して定義されたポリシーは、特定のカテゴリに一致する各アプリケーションに適用されます。

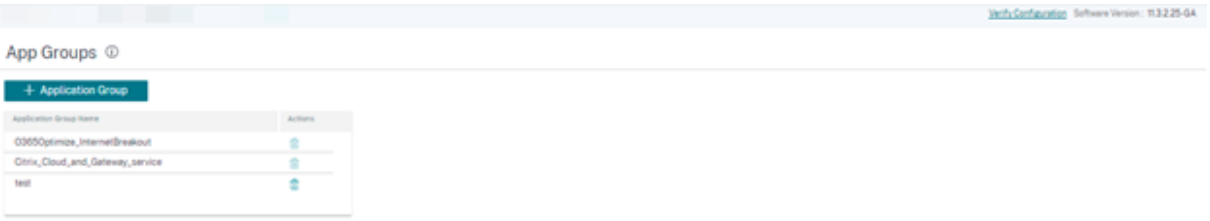
たとえば、** ソーシャルネットワーキングとしてアプリケーショングループを作成し ** 、Facebook、LinkedIn、Twitter などのソーシャルネットワークをそのグループに追加して、ソーシャルネットワーキングアプリケーション

の特定のポリシーを定義できます。

アプリケーショングループを作成するには、グループ名を指定し、アプリケーションリストからアプリを検索して追加します。
必要に応じて、いつでも戻って設定を編集したり、アプリケーショングループを削除したりできます。

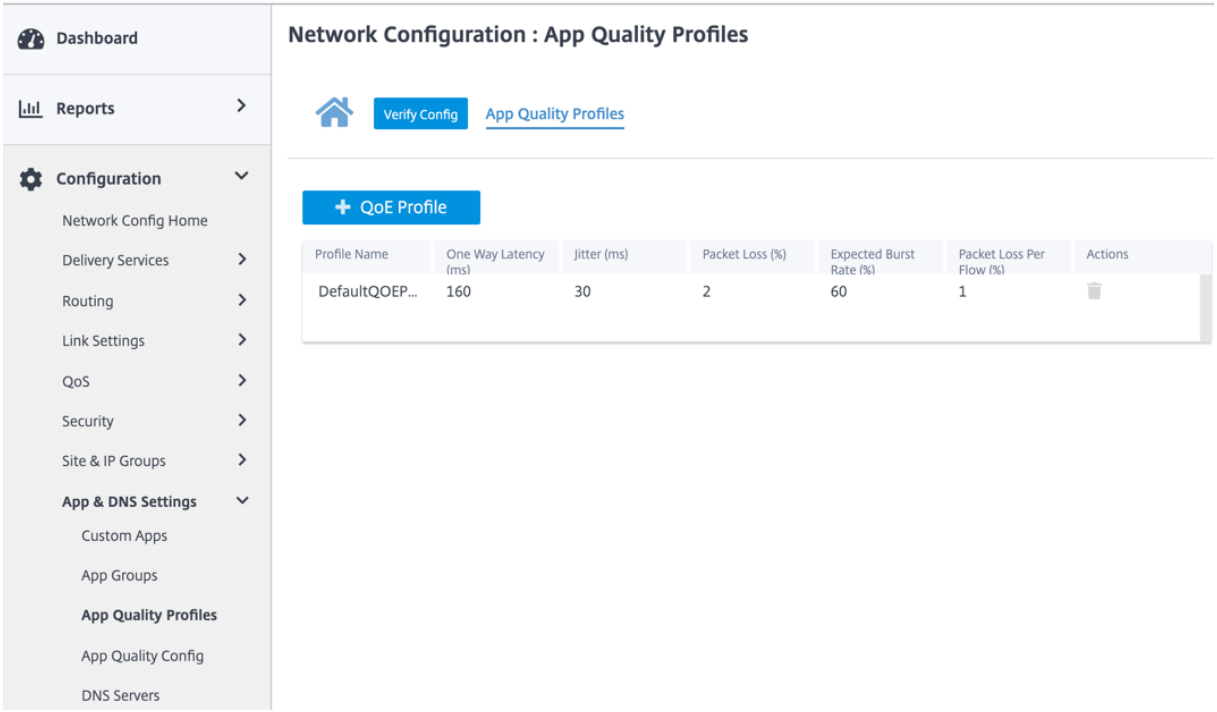


［構成］>［アプリ設定およびグループ］**>**［アプリグループ］ページで［構成の検証］をクリックして、監査エラーを確認します。



アプリケーション品質プロファイル

このセクションでは、アプリケーション品質プロファイルを表示および作成できます。



アプリケーション **QoE** は、SD-WAN ネットワーク内のアプリケーションのエクスペリエンス品質の尺度です。2 つの SD-WAN アプライアンス間の仮想パスを通過するアプリケーションの品質を測定します。

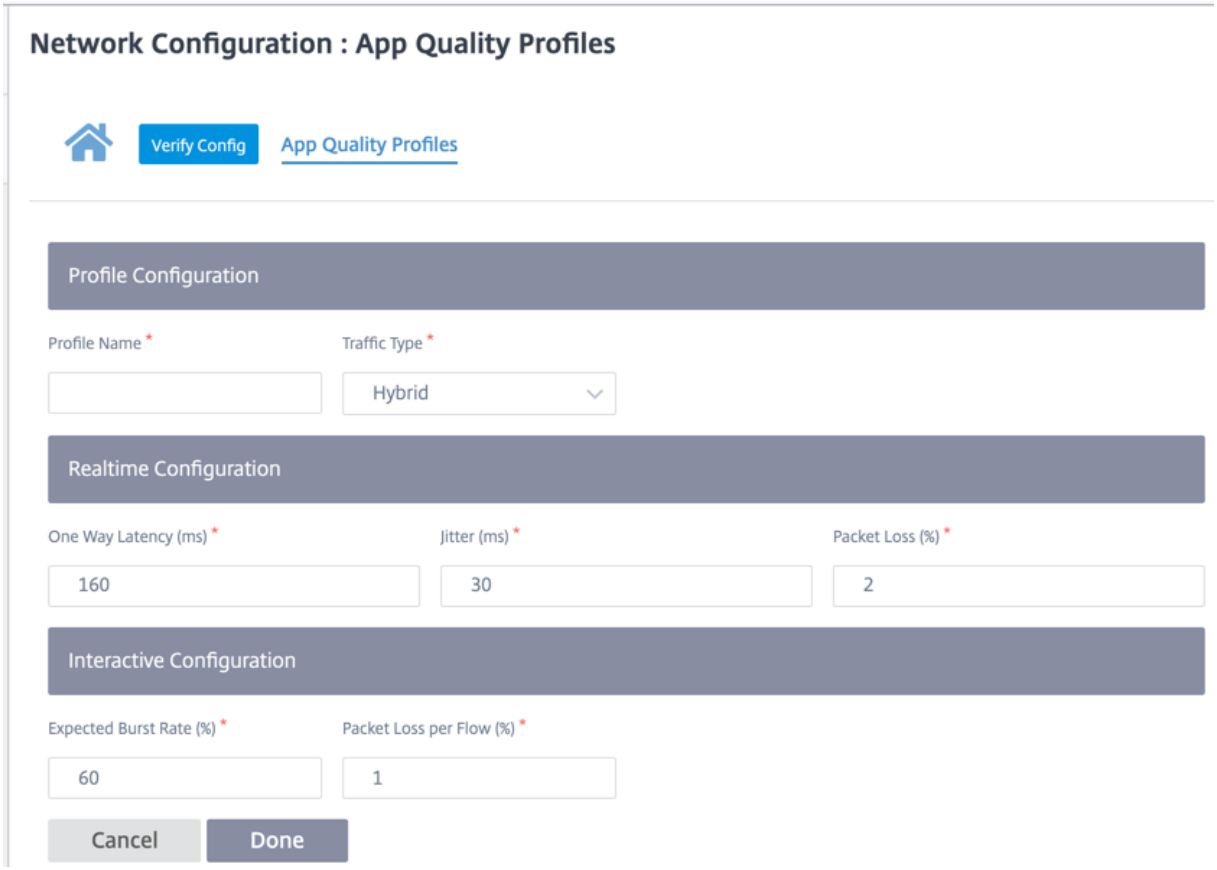
アプリケーション QoE スコアは 0 ～10 の値です。該当するスコア範囲によって、アプリケーションの品質が決まります。

品質	範囲
高	8–10
標準	4–8
低	0–4

アプリケーション QoE スコアは、アプリケーションの品質を測定し、問題のある傾向を特定するために使用することができます。

プロファイルの設定

+ QoE Profile をクリックして QoE プロファイルを作成し、プロファイル名を指定して、ドロップダウンリストからトラフィックタイプを選択します。



リアルタイム構成

QoE プロファイルを使用して、リアルタイムおよび対話型アプライアンスの品質しきい値を定義し、これらのプロファイルをアプリケーションまたはアプリケーションオブジェクトにマッピングできます。

リアルタイムアプリケーションのアプリケーション QoE 計算では、MOS スコアから派生した Citrix の革新的な手法が使用されます。

デフォルトのしきい値は次のとおりです。

- 遅延しきい値（ミリ秒）：160
- ジッタしきい値 (ミリ秒): 30
- パケット損失しきい値（%）：2

遅延、損失、およびジッタに関するしきい値を満たすリアルタイムアプリケーションのフローは、品質が良いと見なされます。

リアルタイムアプリケーションの QoE は、しきい値を満たすフローの割合をフローサンプルの合計数で割った値から決定されます。

リアルタイムの QoE =（しきい値を満たすフローサンプル数/フローサンプルの合計数）* 100

これは、0 から 10 の範囲の QoE スコアとして表されます。

対話型の構成

対話型アプリケーションのアプリケーション QoE では、パケット損失とバーストレートのしきい値に基づいて Citrix の革新的な技術を使用しています。

対話型アプリケーションは、パケット損失とスループットに影響されます。したがって、フロー内のパケット損失率、および入出力トラフィックのバーストレートを測定します。

設定可能なしきい値は、次のとおりです。

- パケット損失率。
- 入力バーストレートと比較して、予想される出力バーストレートのパーセンテージ。

デフォルトのしきい値は次のとおりです。

- パケット損失しきい値:1%
- バーストレート:60%

次の条件が満たされている場合、フローの品質は良好です。

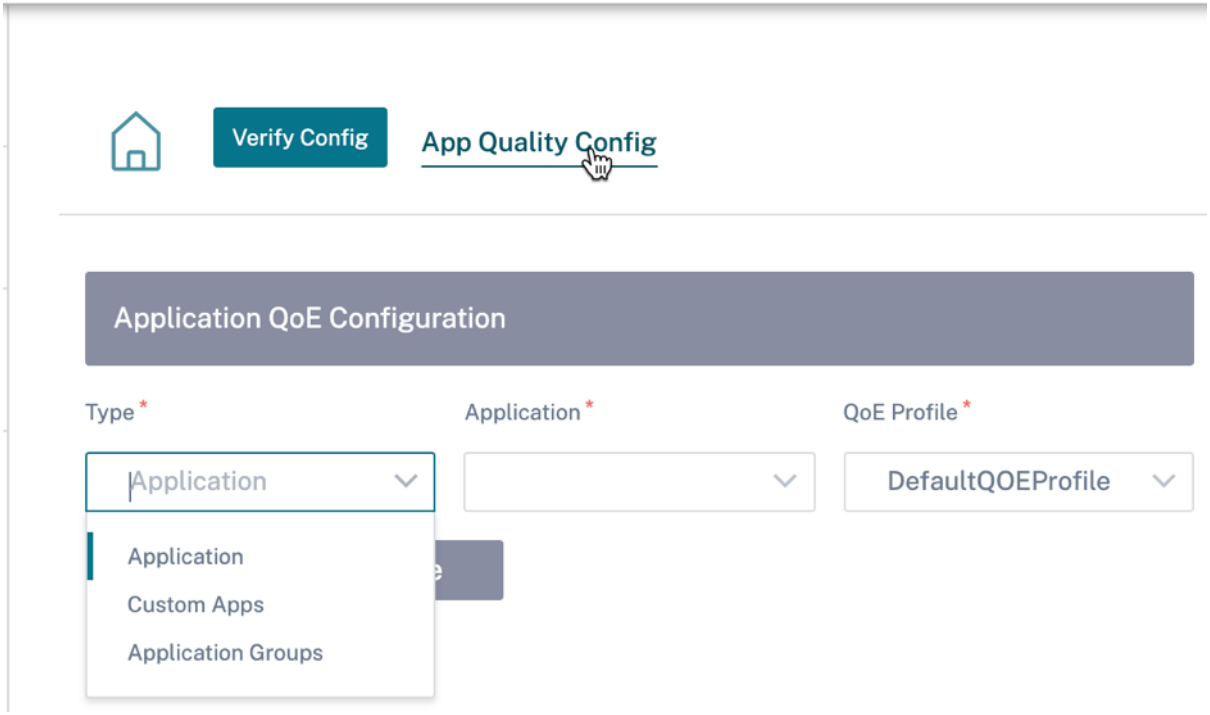
- フローの損失の割合は、設定されたしきい値より小さくなります。
- 出力バーストレートは、少なくとも入力バーストレートに設定されたパーセンテージです。

アプリケーション品質の設定

アプリケーションまたはアプリケーションオブジェクトをデフォルトまたはカスタム QoE プロファイルにマッピングします。リアルタイムおよび対話型トラフィック用のカスタム QoE プロファイルを作成できます。

+QoE 設定をクリックして、カスタム QoE プロファイルを作成します。

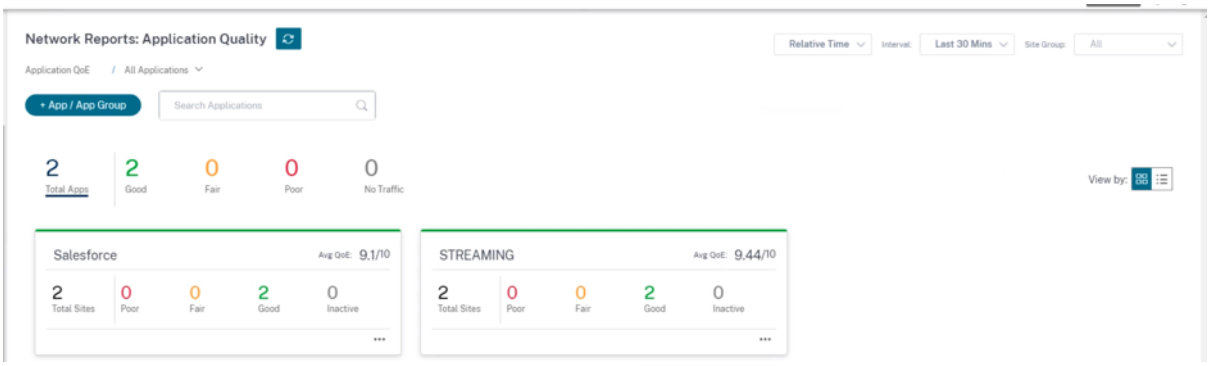
- タイプ:DPI アプリケーションまたはアプリケーションオブジェクト (アプリケーション、カスタムアプリ、アプリケーショングループ) を選択します。
- アプリケーション: 選択したタイプに基づいて、アプリケーションまたはアプリケーションオブジェクトを検索して選択します。
- **QoE** プロファイル: アプリケーションまたはアプリケーションオブジェクトにマッピングする QoE プロファイルを選択します。



[完了] をクリックします。

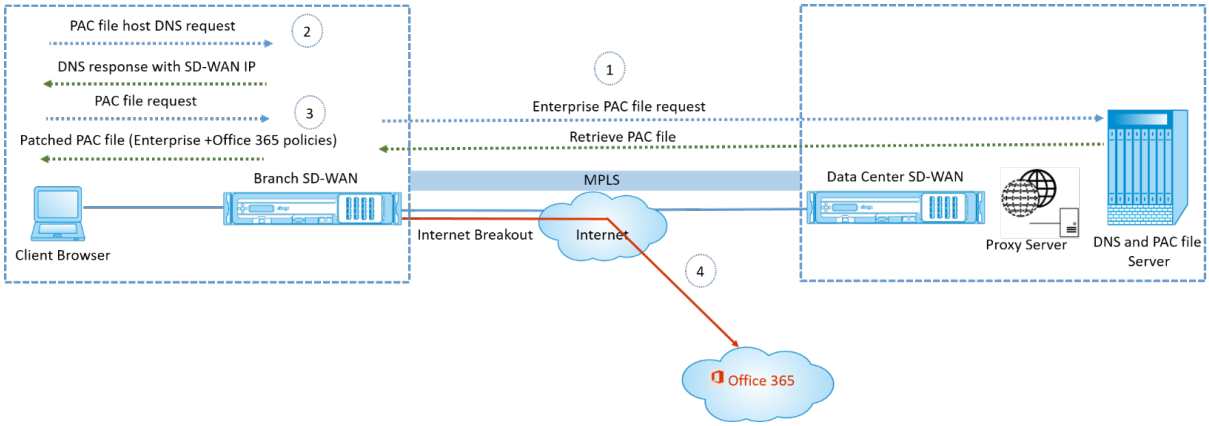
監査エラーを確認するには、「構成を確認」をクリックします。

カスタムアプリケーションタイプを使用してアプリケーション QoE を設定すると、関連するアプリケーションレポートタイルが [レポート] **>** **[**アプリケーション品質] の下に自動生成されます。選択したアプリケーションと一致するトラフィックはすべて、カスタムアプリケーションの仮想パスを経由します。



PAC ファイルのカスタマイズの仕組み

理想的には、内部 Web サーバー上のエンタープライズネットワークホスト PAC ファイル、これらのプロキシ設定はグループポリシーを介して配布されます。クライアントブラウザは、エンタープライズ Web サーバから PAC ファイルを要求します。Citrix SD-WAN アプライアンスは、Office 365 ブレークアウトが有効なサイト用にカスタマイズされた PAC ファイルを提供します。



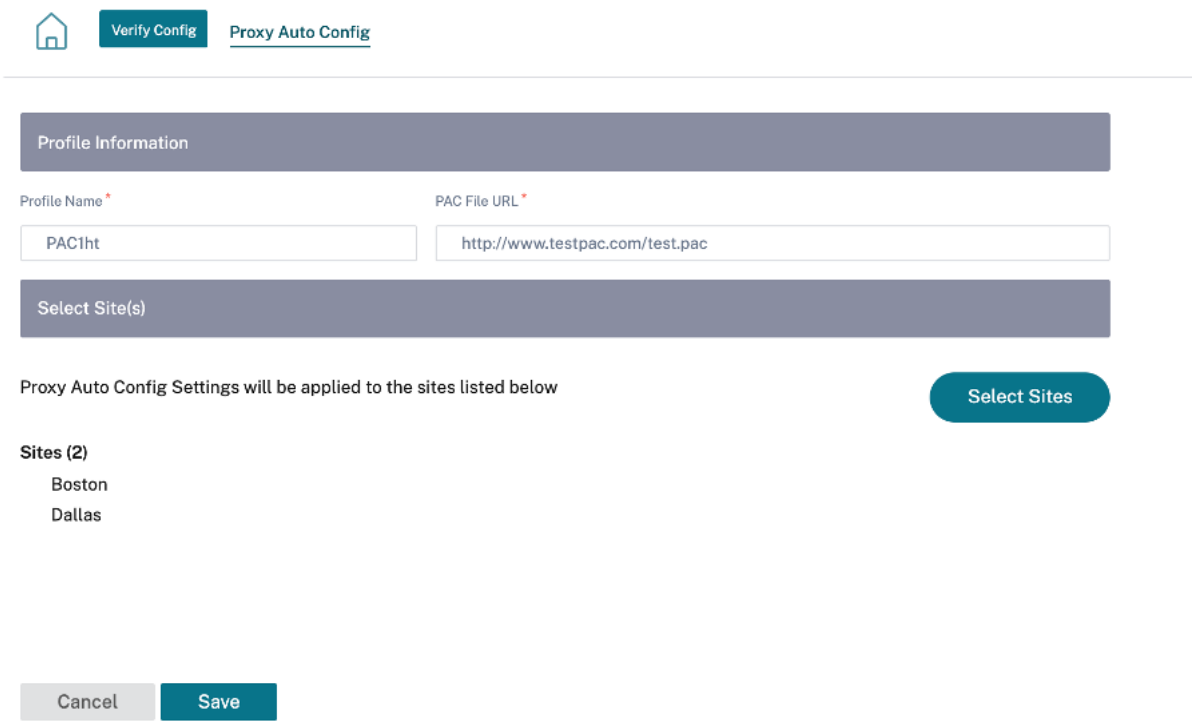
1. Citrix SD-WAN は、エンタープライズ Web サーバーからエンタープライズ PAC ファイルの最新のコピーを定期的に要求し、取得します。Citrix SD-WAN アプライアンスは、オフィス 365 の URL をエンタープライズ PAC ファイルにパッチします。エンタープライズ PAC ファイルには、Office 365 の URL にシームレスにパッチが適用されるプレースホルダ (SD-WAN 固有のタグ) が必要です。
2. クライアントブラウザーは、エンタープライズ PAC ファイルホストの DNS 要求を生成します。Citrix SD-WAN は、プロキシ構成ファイル FQDN に対する要求を代行受信し、Citrix SD-WAN VIP に応答します。
3. クライアントブラウザが PAC ファイルを要求します。Citrix SD-WAN アプライアンスは、パッチが適用された PAC ファイルをローカルで提供します。PAC ファイルには、エンタープライズプロキシ構成と Office 365 の URL 除外ポリシーが含まれています。
4. Office 365 アプリケーションに対する要求を受信すると、Citrix SD-WAN アプライアンスは直接インターネットブレークアウトを実行します。

前提条件

1. 企業は PAC ファイルをホストする必要があります。
2. PAC ファイルには、プレースホルダー *SDWAN_TAG* か、Office 365 の URL にパッチを適用する`findproxyforurl`関数が 1 つ存在する必要があります。
3. PAC ファイルの URL は、IP ベースではなく、ドメインベースである必要があります。
4. PAC ファイルは、信頼されたアイデンティティ VIP を介してのみ提供されます。
5. Citrix SD-WAN アプライアンスは、管理インターフェイス経由でエンタープライズ PAC ファイルをダウンロードできる必要があります。

プロキシ自動設定の構成

SD-WAN Orchestartor UI のネットワークレベルで、[構成] > [アプリ設定とグループ] > [プロキシ自動構成] に移動し、[**+ PAC** ファイルプロファイル] をクリックします。



PAC ファイルプロファイルの名前を入力し、エンタープライズ PAC ファイルサーバの URL を指定します。Office 365 ブレークアウトルールは、エンタープライズ PAC ファイルに動的に修正されます。

PAC ファイルプロファイルを適用するサイトを選択します。サイトごとに異なる URL がある場合は、サイトごとに異なるプロファイルを作成します。

制限事項

- HTTPS PAC ファイルサーバー要求はサポートされていません。
- ルーティングドメインまたはセキュリティゾーンの PAC ファイルなど、ネットワーク内の複数の PAC ファイルはサポートされません。
- Citrix SD-WAN での PAC ファイルのゼロからの生成はサポートされていません。
- DHCP 経由の WPAD はサポートされていません。

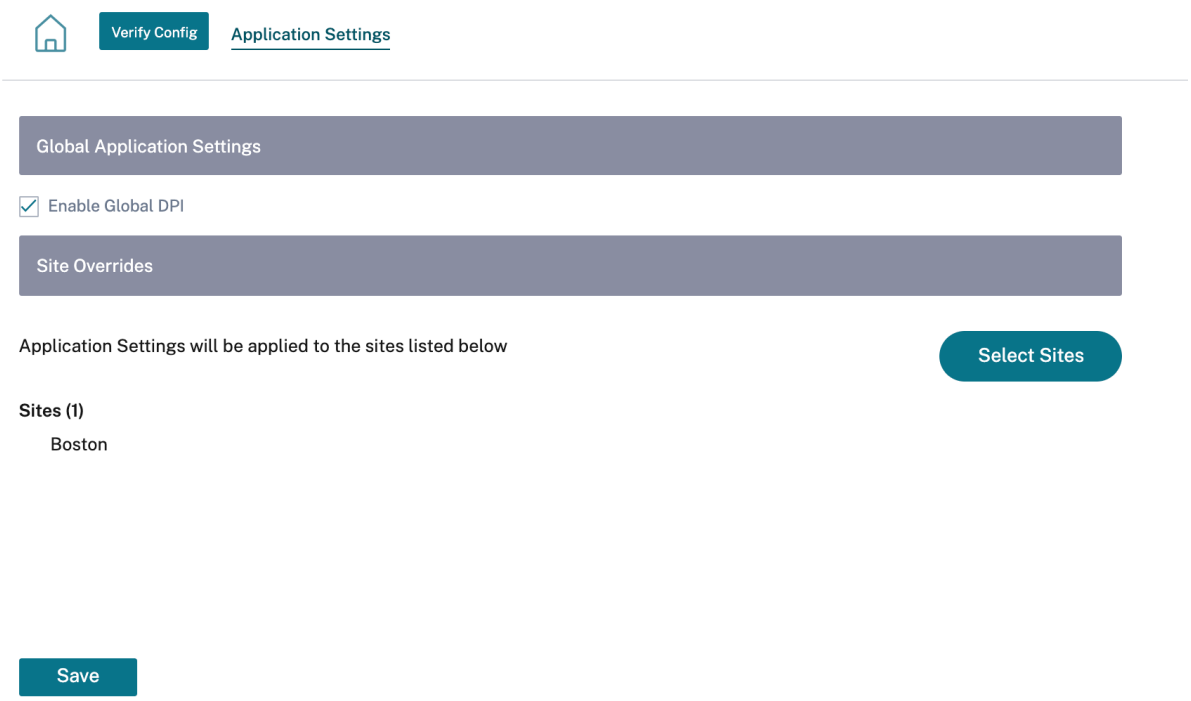
DPI 設定

Citrix SD-WAN アプライアンスは、ディープパケットインスペクション（DPI）を実行して、アプリケーションを識別して分類します。DPI ライブラリは、何千もの商用アプリケーションを認識します。これにより、アプリケーションのリアルタイムの検出とクラス分けが可能になります。SD-WAN アプライアンスは DPI テクノロジーを使用して、

着信パケットを分析し、トラフィックを特定のアプリケーションまたはアプリケーションファミリに属するものとして分類します。

DPI は、ネットワーク内のすべてのサイトで、既定でグローバルに有効になっています。DPI を無効にすると、アプライアンスの DPI 分類機能が停止します。DPI 分類アプリケーション/アプリケーションカテゴリを使用して、ファイアウォール、QoS、およびルーティングポリシーを設定できなくなりました。また、上位アプリケーションおよびアプリケーションカテゴリレポートも表示できません。

グローバル DPI を無効にするには、ネットワークレベルで、［構成］**>**［アプリ設定とグループ］**>**［**DPI** 設定］に移動し、［グローバル **DPI** を有効にする］チェックボックスをオフにします。



グローバルな DPI 設定をオーバーライドして、特定のサイトの DPI を無効にするように選択することもできます。選択したサイトの DPI を無効にするには、サイトオーバーライドリストにサイトを追加します。

プロファイルとテンプレート

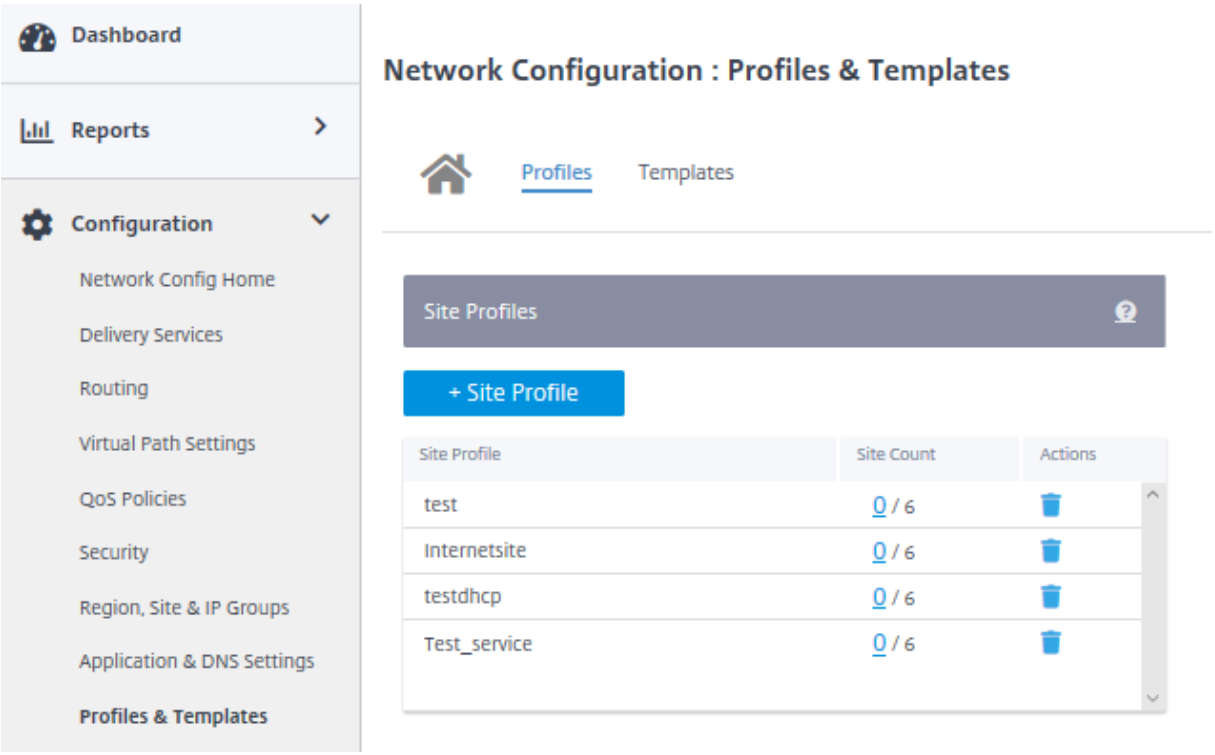
October 26, 2022

プロファイルは、ライブ構成テンプレートです。通常のテンプレートは、新しいエンティティの作成に役立ちます。ただし、テンプレートが作成されると、その後にテンプレートに加えられた変更は、基本テンプレートを使用して作成された既存のエンティティには適用されません。縦断は、ライブの中央マスターエンティティとして機能します。すべての子エンティティは、作成中だけでなく、プロファイルの存続期間中も、プロファイルから継承されます。プロファイルに関連付けられているすべての子エンティティは、プロファイルに加えられた変更を自動的に継承します。

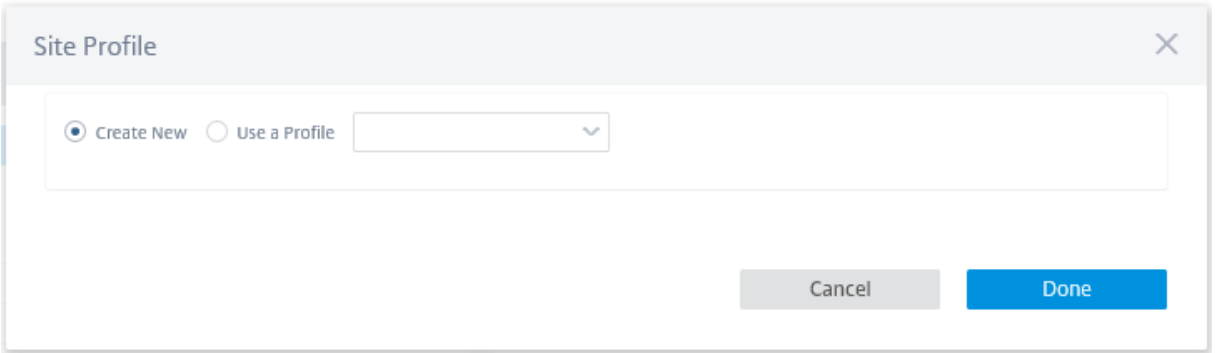
たとえば、管理者は、小規模小売店と呼ばれるサイト構成プロファイルを作成し、会社が所有するすべての小規模小売店に適用します。これで、小規模小売店舗のプロファイルに対して行った変更は、このプロファイルを継承するすべての店舗に自動的に適用されます。すべてのエンティティで共通するものとそうでないものに基づいて、プロファイル設定の特定のパラメーターは設定しないままにすることができます。このようなパラメータはカスタマイズ可能で、同じプロファイルを継承するエンティティ間で異なる場合があります。

サイトプロファイル

サイトプロファイルを使用すると、サイトを簡単かつ迅速に構成できます。サイトプロファイルは 1 回作成して、サイトの作成中に複数回再利用することができます。

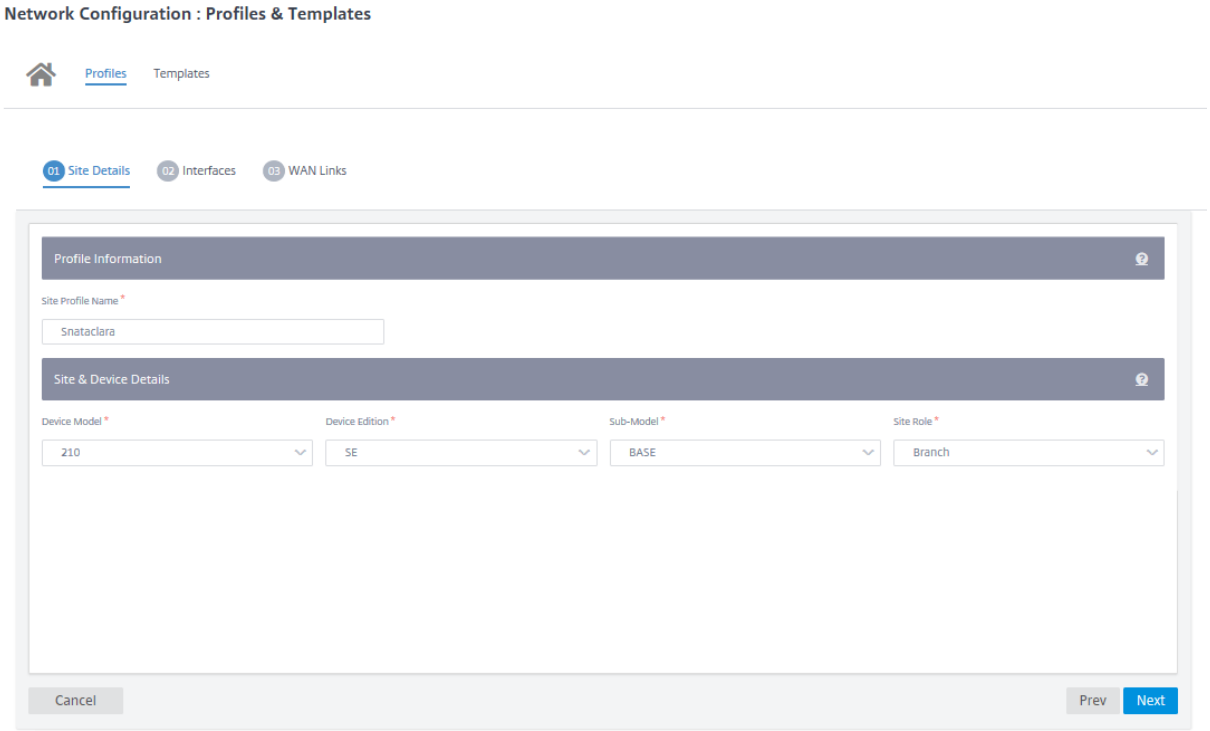


サイトプロファイルを作成するには、[**+** サイトプロファイル] をクリックします。プロファイルを最初から作成することも、既存のサイトプロファイルを編集して新しいプロファイルとして保存することもできます。

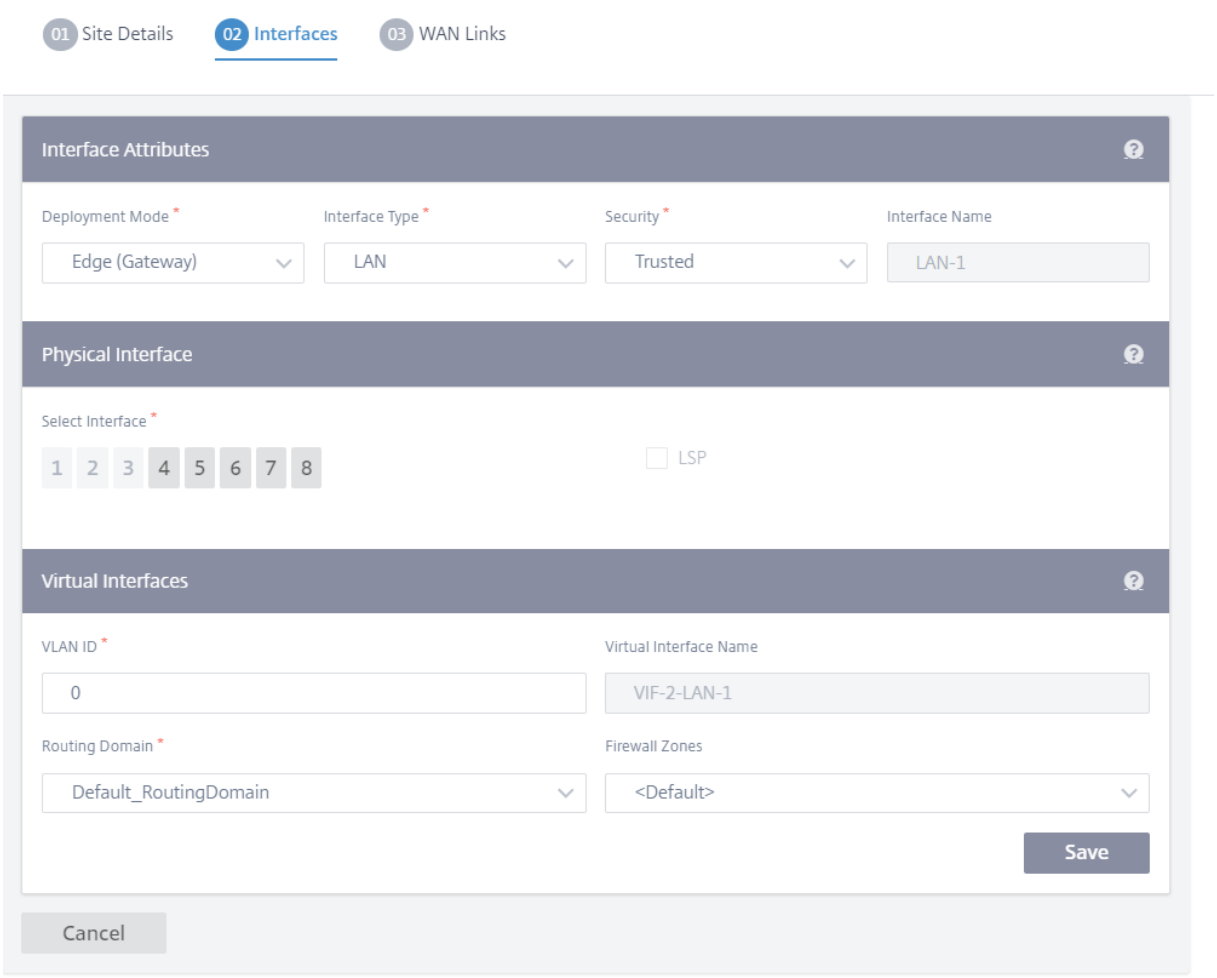


サイトプロファイルを作成するには、サイトの詳細、インターフェイス、および **WAN** リンクを設定する必要があります。サイト構成の詳細な説明については、「サイトの詳細」を参照してください。

デバイスの詳細を入力します。

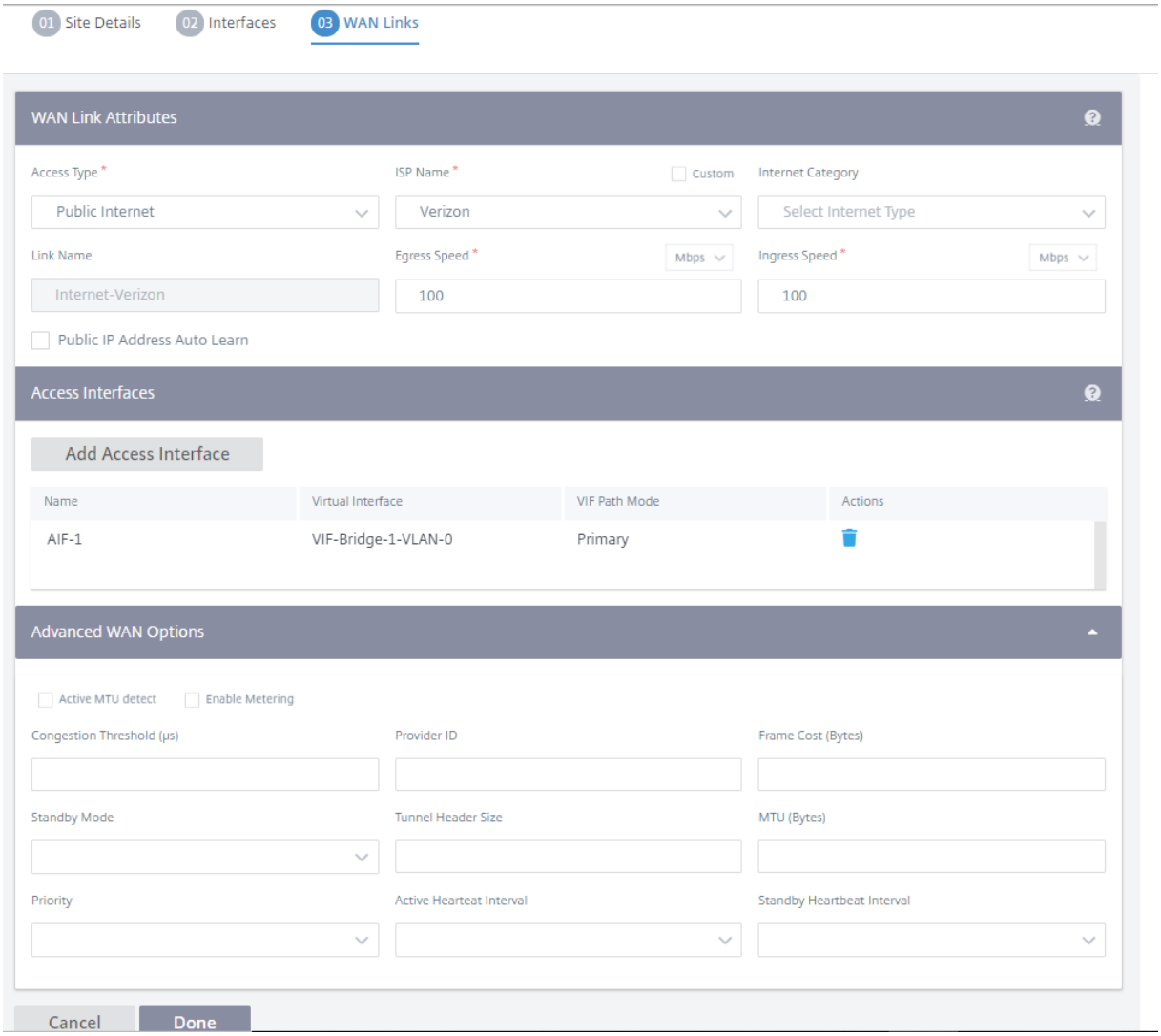


[**+** インターフェイス**]** オプションをクリックして、サイトのインターフェイスを割り当てます。インターフェイスを追加するには、[インターフェイス属性**]**、**[**物理インターフェイス**]**、**[**** 仮想インターフェイス ******] の各フィールドを入力する必要があります。インターフェイス設定の詳細な説明については、「インターフェイス」を参照してください。



WAN リンク属性、アクセスインターフェイス、**** サービスに詳細オプションを入力します ****。

WAN リンクの設定の詳細については、WAN リンクを参照してください。



テンプレート

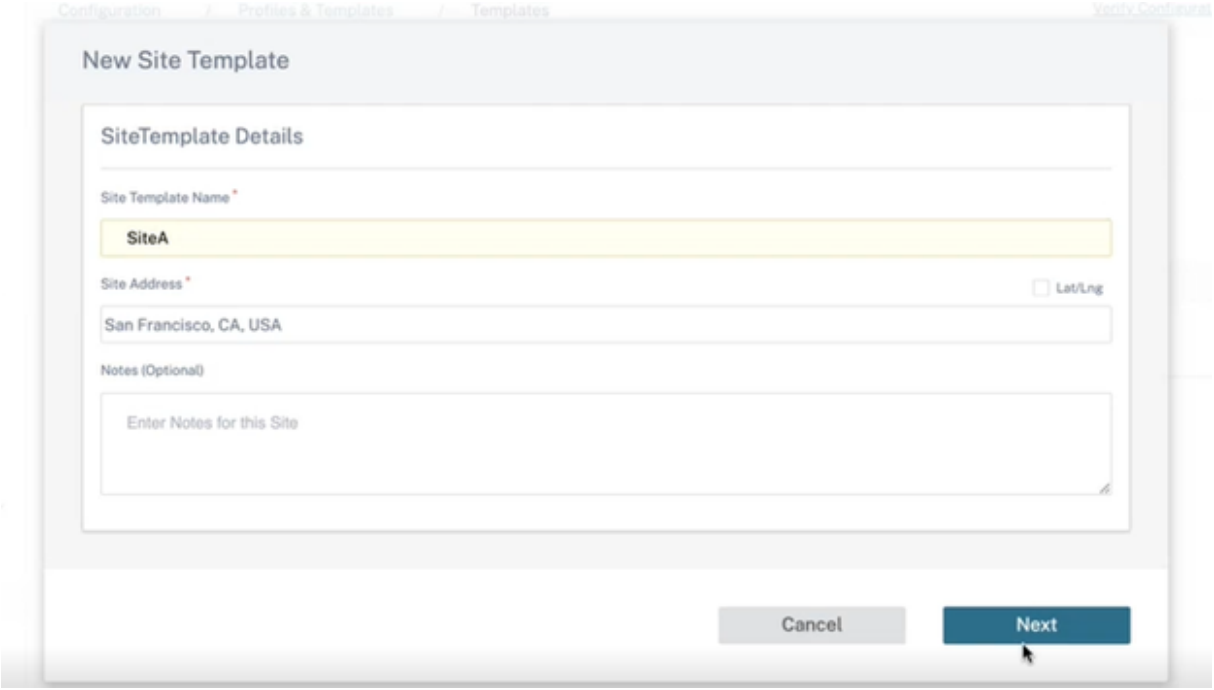
Citrix SD-WAN Orchestrator サービスを使用すると、テンプレートを事前定義済みのフィールドセットとして使用して、新しいサイトまたは WAN リンクを設定できます。

サイトテンプレート

サイトテンプレートは、サイトの作成に使用される定義済みのテンプレートです。定義済みのサイトテンプレートを使用してサイトを設定するには、顧客レベルで **[**** 設定] > [プロファイルとテンプレート**] > [**テンプレート] に移動します。**[**** サイトテンプレート] セクションで、[サイトテンプレートの追加] をクリックします。

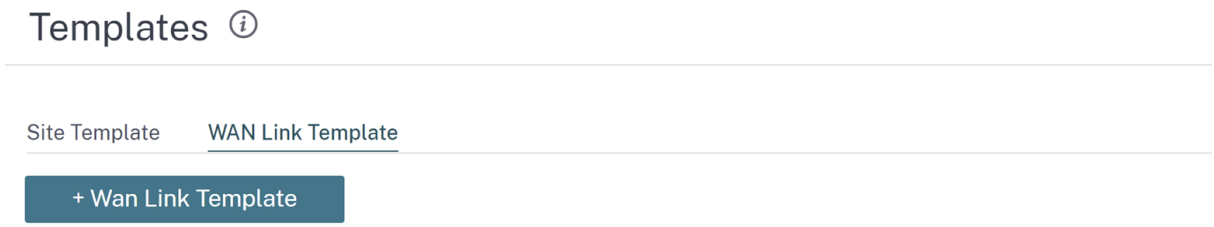
表示される [新しいサイトテンプレート] 画面で、必要に応じて詳細を入力し、[次へ] をクリックします。

> 注
>
> サイトのクローンを作成するか、サイトテンプレートを使用してサイトを作成し、ソースに Wi-Fi が設定されている場合、Wi-Fi 設定は新しいサイトにコピーされません。

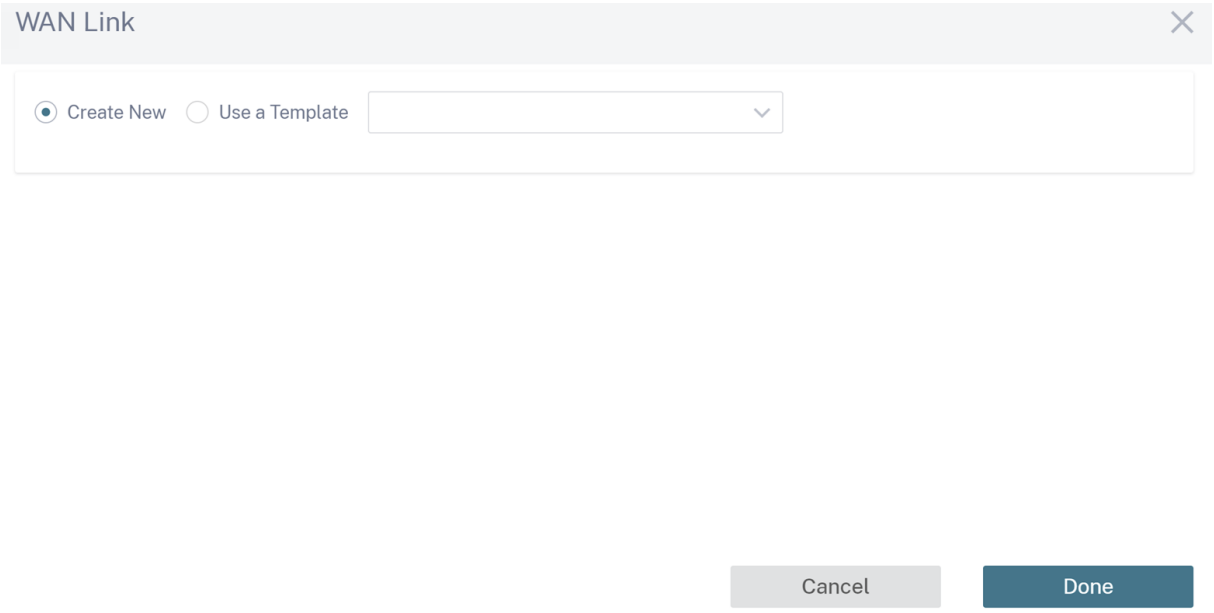


WAN リンクテンプレート

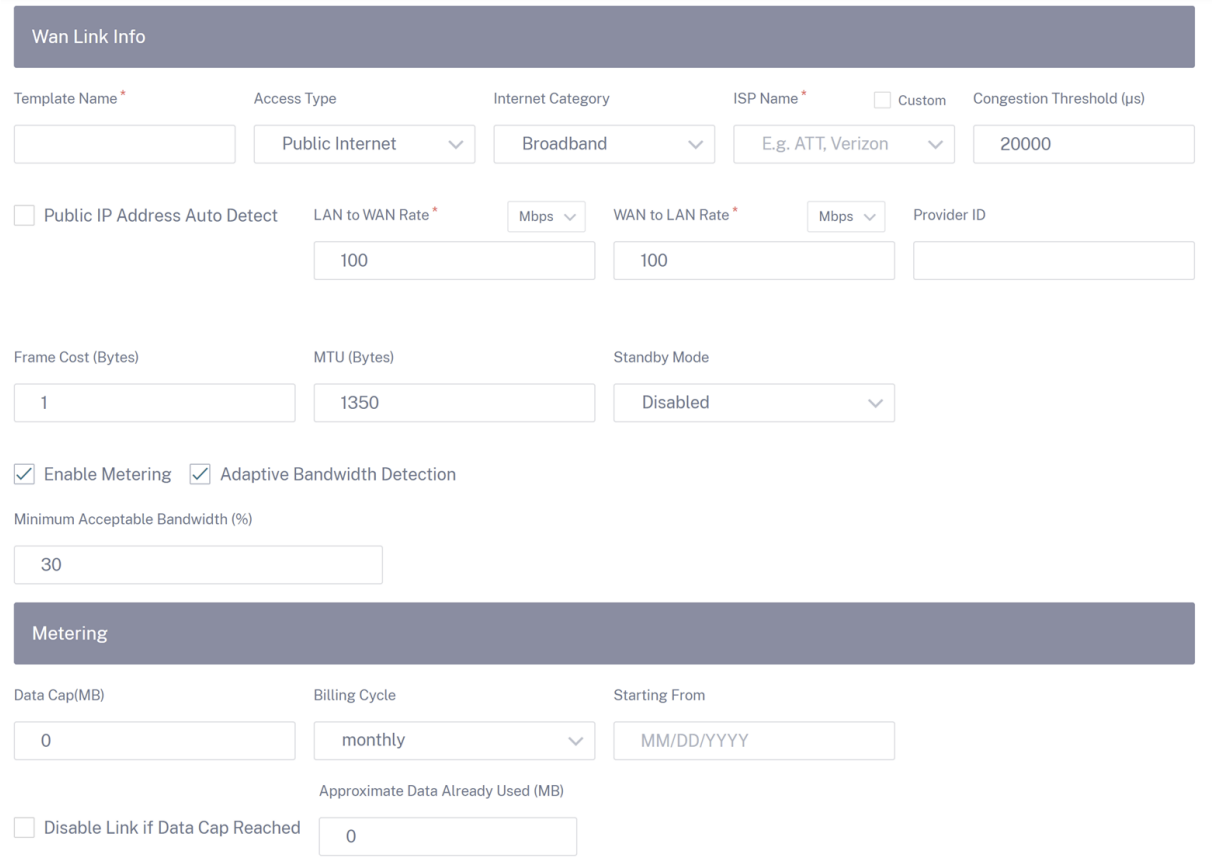
WAN リンクテンプレートを使用すると、WAN リンクを簡単かつ迅速に設定できます。WAN リンクテンプレートを 1 回作成し、WAN リンクを設定するときに複数回再利用することができます。変更した WAN リンクテンプレート構成を、WAN リンクテンプレートを使用して作成されたサイトの WAN リンク構成にコピーすることもできます。



WAN リンクテンプレートを作成するには、[**+ WAN** リンクテンプレート] をクリックします。テンプレートを最初から作成することも、既存の WAN リンクテンプレートを編集して新しいテンプレートとして保存することもできます。



プロファイル名、アクセスタイプ、インターネットカテゴリ、**LAN-to-WAN** レート **(Mbps)** などの **WAN** リンク情報を指定して WAN プロファイルを作成します。WAN リンクの設定の詳細については、WAN リンクを参照してください。

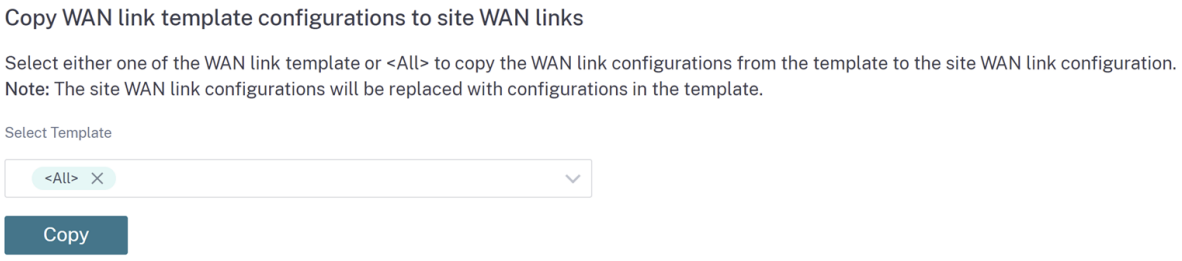


以前は、変更した WAN リンクテンプレート構成をサイト WAN リンク構成にコピーするオプションは使用できませ

んでした。たとえば、ユーザーが既に WAN リンクテンプレートを使用して複数のサイト WAN リンクを作成していて、特定の構成（輻輳閾値の設定など）を変更する必要がある場合、ユーザーはすべてのサイトの WAN リンクで個別に変更する必要がありました。これ以降、ユーザーは WAN リンクテンプレートを新しい輻輳閾値設定で更新し、最新の WAN リンクテンプレート構成を WAN リンクテンプレートを使用して作成されたすべてのサイト WAN リンクにコピーできます。

1 つ以上の WAN リンクテンプレートを選択して [コピー] をクリックすると、WAN リンクテンプレートで行った更新が、選択したテンプレートを使用して作成されたサイトの WAN リンク構成にコピーされます。

> 注:
>
> サイトプロファイル機能を使用して作成された WAN リンクサイト構成は更新されません。



ネットワークロケーションサービス

July 10, 2024

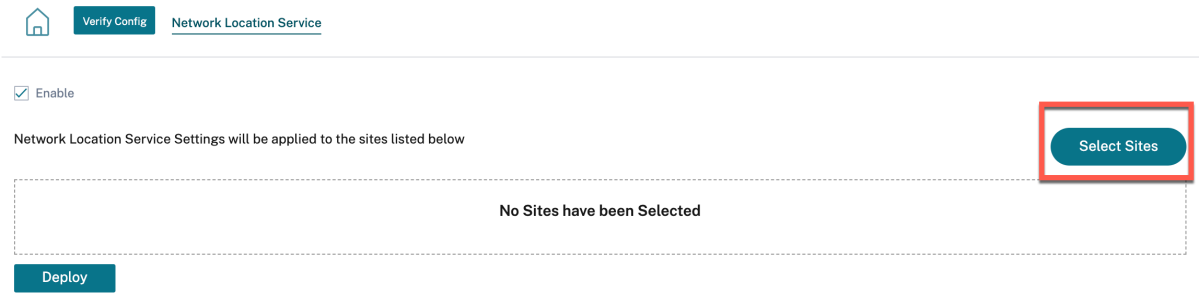
> 重要な更新:
>
> この機能は、Citrix SD-WAN Orchestrator サービスの展開では廃止されました。ただし、Citrix Cloud を使用して NLS を有効にすることは引き続き可能です。詳しくは、「直接ワークロード接続でワークスペースへの接続を最適化する」を参照してください。

ネットワークロケーションサービス（NLS）は、Citrix Virtual Apps and Desktops に接続しているユーザーが内部ネットワークから接続しているかどうかを判断する Citrix Cloud サービスです。NLS を使用すると、PowerShell スクリプトを使用して Citrix SD-WAN にデプロイされた場所の IP アドレスを手動で構成する必要がなくなります。NLS について詳しくは、「Citrix Workspace ネットワークロケーションサービス」を参照してください。

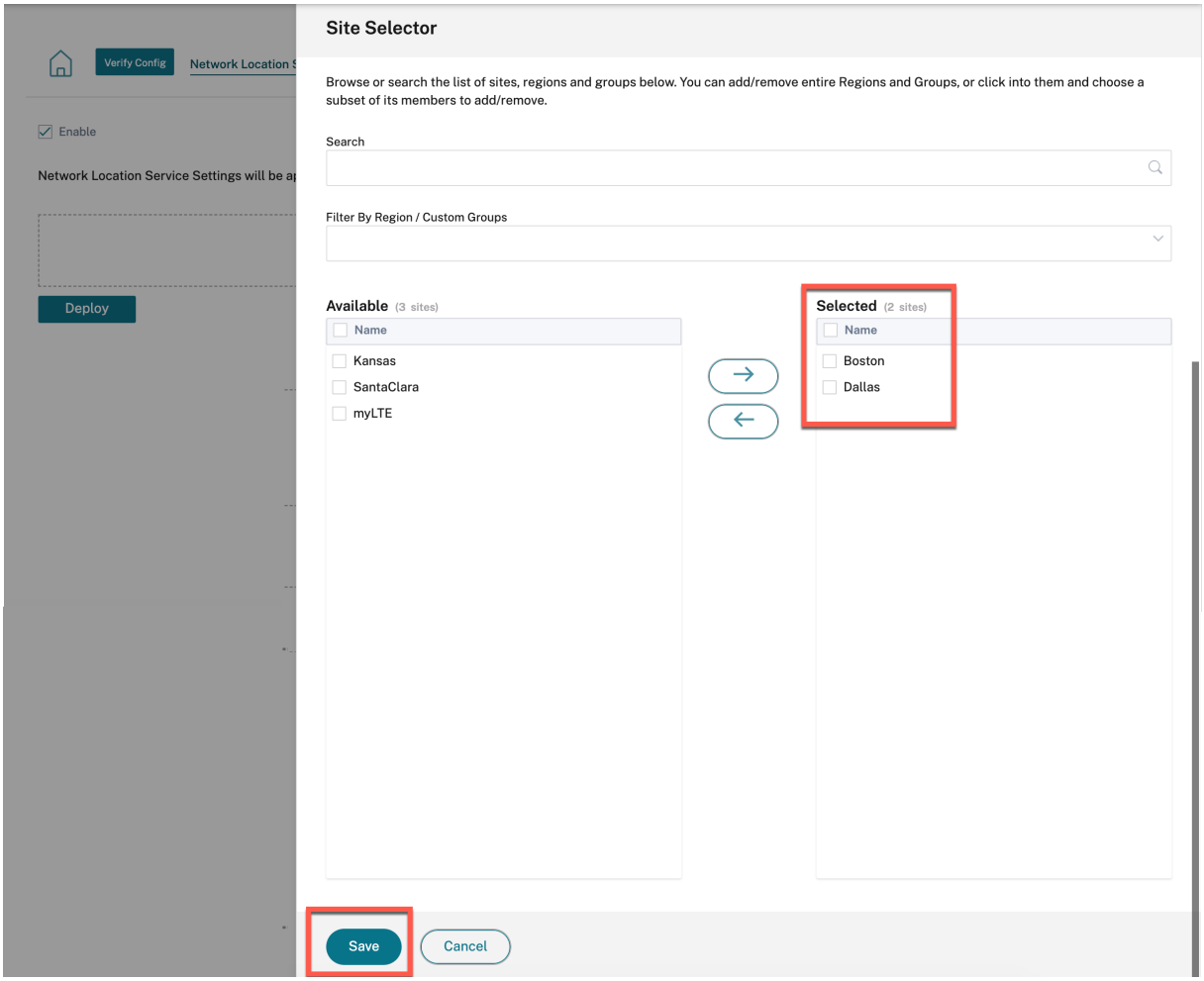
ネットワーク内のすべてのサイトまたは特定のサイトで NLS を有効にできます。NLS に対応したサイトは、すべてのインターネット WAN リンクのパブリック IP アドレスを、地理的位置やタイムゾーンなどの他のサイト詳細とともに NLS データベースと共有します。これらの詳細に基づいて、ネットワークロケーションサービスは、Citrix Virtual Apps and Desktops に接続しているユーザーが Citrix SD-WAN によって終了したネットワークフロントエンドにいるかどうかを判断します。

ユーザーリクエストが Citrix SD-WAN によって終了されたネットワークフロントから送信されている場合、ユーザーは NetScaler Gateway サービスをバイパスして Citrix Virtual Apps and Desktops の VDA に直接接続されます。

NLS を有効にするには、カスタマーレベルで [構成] **>** **[**ネットワークロケーションサービス] に移動します。



ネットワーク内のすべてのサイトで **NLS** を有効にする場合は、**[**有効にする**]** を選択します。特定のサイトの NLS を有効にするには、「サイトを選択」をクリックします。地域を選択し、それに応じてサイトを選択します。[保存] をクリックし、[展開] をクリックします



ECMP 負荷分散

October 26, 2022

ECMP（等コストマルチパス）グループを使用すると、同じコスト、宛先、サービスで複数のパスをグループ化できます。接続またはセッション・データは、ECMP グループのタイプに応じて、ECMP グループ内のすべてのパスでロード・バランシングされます。たとえば、同じルートコストを持つブランチとデータセンターの間に 2 つの WAN リンクを持つネットワークがあるとします。従来、WAN リンクの 1 つはアクティブで、もう 1 つはフォールバックリンクとして機能している状態のままでした。ECMP グループを使用すると、これらの WAN リンクをグループ化して、両方の WAN リンクを通じてトラフィックの負荷分散を行うことができます。ECMP 負荷分散により、次のことが保証されます

- 複数の等価コストパスへのトラフィックの分散
- 利用可能な帯域幅の最適な使用。
- ルートが到達不能になった場合、トラフィックを他の ECMP メンバーパスに動的に転送します。

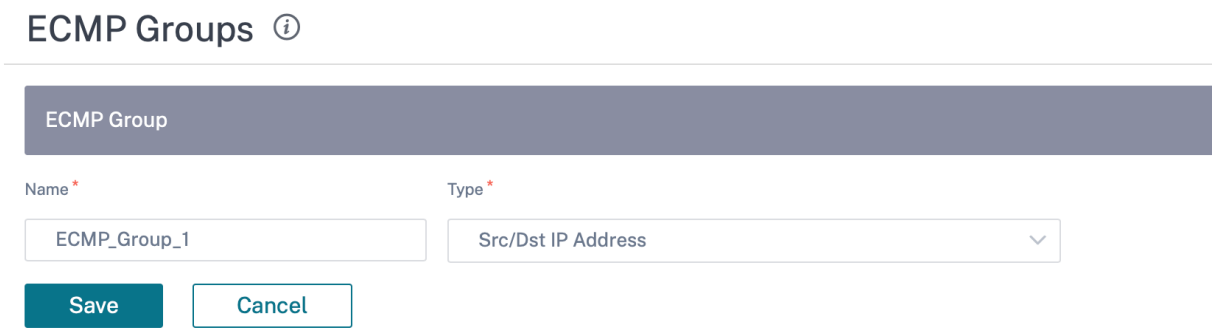
ECMP 負荷分散は次のサービスでサポートされています。

- 仮想パス
- Citrix Secure Internet Access
- Zscaler
- IPsec
- GRE

ネットワークには、最大 254 の ECMP グループを定義できます。ECMP グループ内の ECMP 適格ルートの最大数は、アプライアンスとライセンスタイプによって異なります。Citrix SD-WAN では、次の 2 種類の ECMP グループがサポートされています。

- 送信元/宛先 IP アドレス: 複数のクライアントが同じ宛先に接続しようとするネットワークでは、同じコストの WAN リンク間で接続の負荷分散が行われます。
- セッション: 単一のクライアントが宛先に接続され、複数のセッションが生成されるネットワーク。セッションデータは、等コストの WAN リンク間で負荷分散されます。

ECMP グループを設定するには、ネットワークレベルで [構成**] > [**ルーティング**] > [ECMP** グループ] に移動します。ECMP グループの名前を入力し、必要に応じて [**Src/Dest IP** アドレス] または [セッション] としてタイプを選択します。

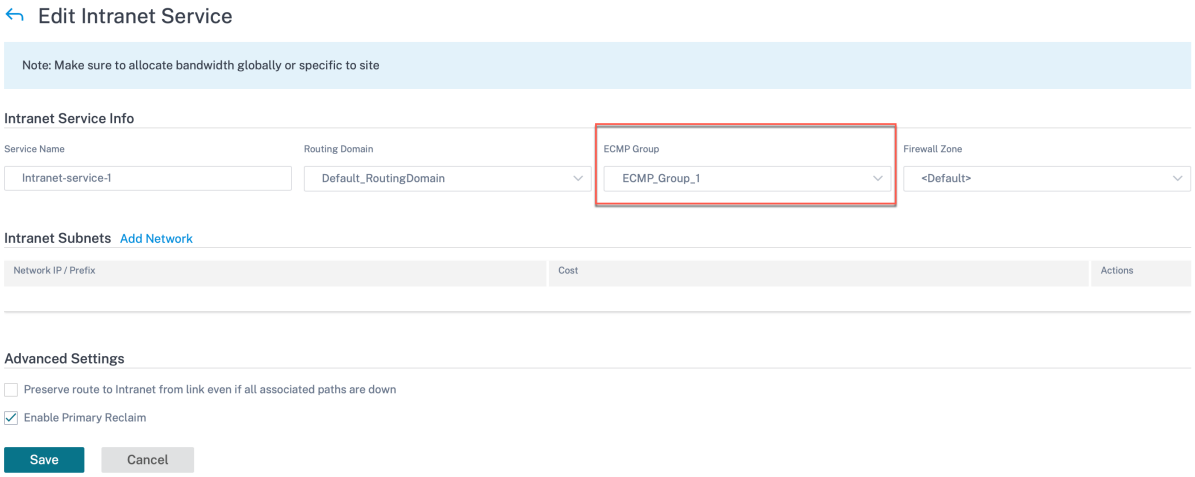


ECMP グループを次のサービスに関連付けることができます。

- 仮想パス (サイトレベル)
- Citrix Secure Internet Access
- Zscaler
- IPsec
- GRE

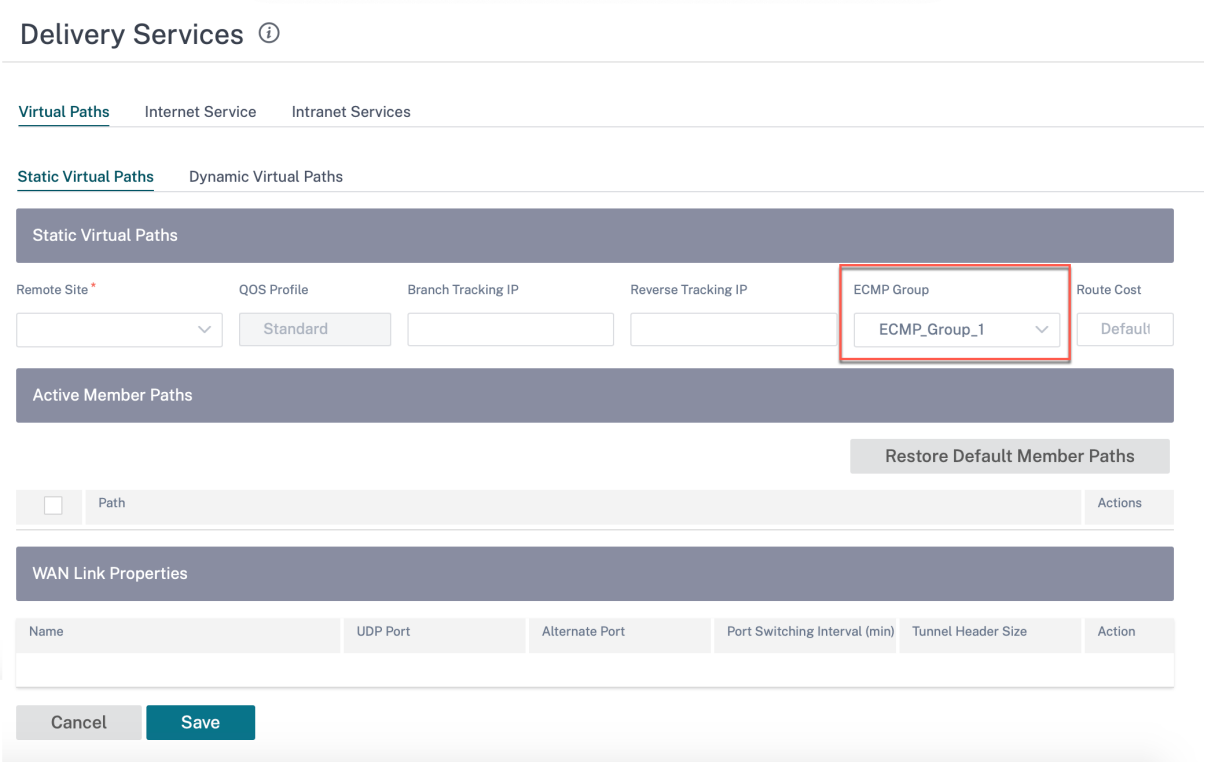
イントラネットサービスで ECMP 構成を有効にするには、ネットワーク * レベルで、[構成] **>** [配信チャネル] **>** [帯域幅割り当て] **>** [イントラネット **+** サービス] に移動し、[サービスの種類] として [イントラネット] を選択します。イントラネットサービスの設定時に ECMP グループを選択します。

> 注
>
> [なし] を選択しても、サービスの ECMP 構成は有効になりません。



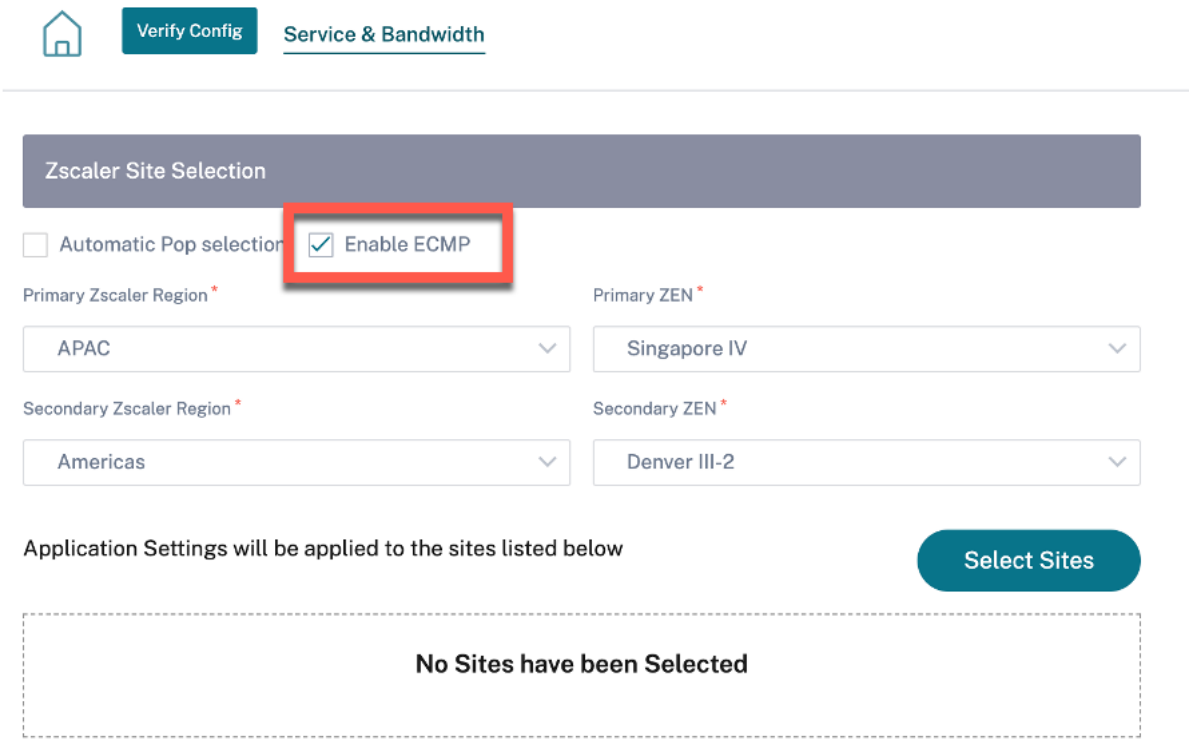
仮想パスの ECMP 構成を有効にするには、サイトレベルで、［構成］> ［詳細設定］**>** ［デリバリーサービス］**>** ［仮想パス］> ［静的仮想パス］> ［**+** 仮想パス］に移動します。静的仮想パスを設定するときに ECMP グループを選択します。

> 注
>
> [なし] を選択しても、サービスの ECMP 構成は有効になりません。



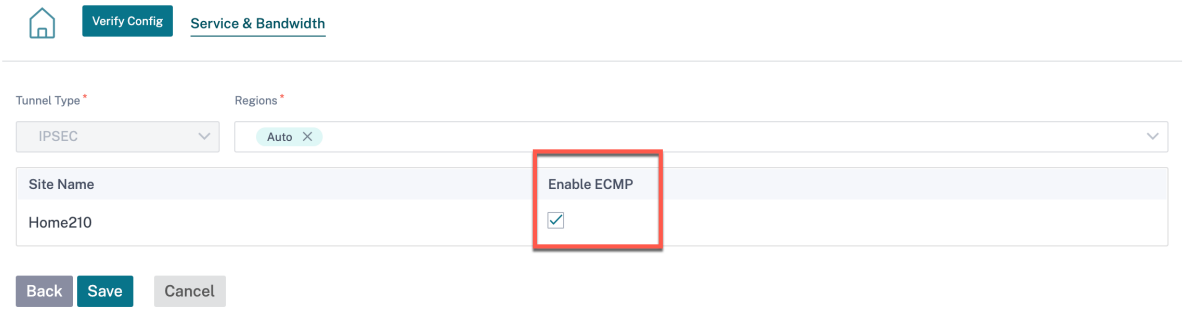
Zscaler サービスで ECMP 構成を有効にするには、ネットワークレベルで [構成] **>** [サービスと帯域幅] に移動します。「デリバリーサービス」列の下にリストされている Zscaler の横にある「設定」アイコンをクリックします。認証して [**+ Site**] をクリックします。サイトを追加するときに、「**ECMP** を有効にする」チェックボックスを選択します。

> 注:
>
> Zscaler サービスはセッションベースの ECMP 負荷分散のみをサポートします。

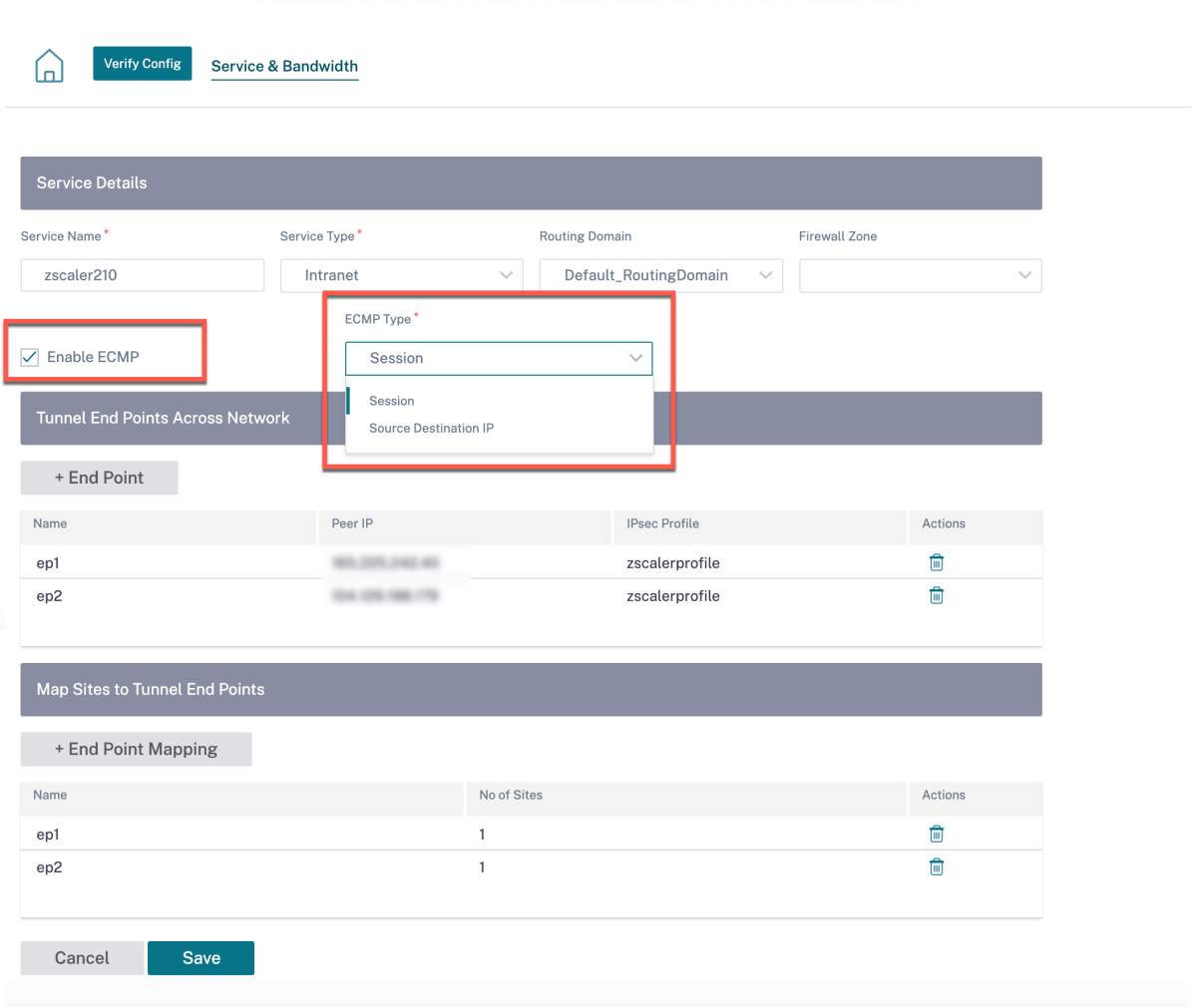


Citrix Secure Internet Access サービスの ECMP 構成を有効にするには、ネットワークレベルで［構成］**>**［サービスと帯域幅］に移動します。****Secure Internet Access** サービスの横にある設定アイコンをクリックし ** 、**+** サイトをクリックします。サイトを選択したら、「**ECMP** を有効にする」チェックボックスを選択します。

> 注:
>
> Citrix Secure Internet Access サービスは、セッションベースの ECMP 負荷分散のみをサポートします。



LAN または WAN 側のサードパーティピアとの固定 IPsec トンネルで ECMP 構成を有効にするには、[構成**] > [**サービスと帯域幅**] > [** イントラネット **+** サービス] に移動し、[サービスタイプとして **IPsec**] を選択します。「**ECMP** を有効にする」チェックボックスを選択し、「**ECMP** タイプ」ドロップダウンリストからタイプを選択します。



アプリケーションルール

October 26, 2022

アプリケーションルールにより、Citrix SD-WAN アプライアンスは受信トラフィックを解析し、特定のアプリケーションまたはアプリケーショングループに属するものとして分類できます。この分類は、アプリケーションルールを作成して適用することにより、個々のアプリケーションまたはアプリケーションファミリのサービス品質（QoS）を向上させます。

アプリケーション、アプリケーショングループ、またはアプリケーションオブジェクトの一致タイプに基づいてトラフィックフローをフィルタリングし、それらにアプリケーションルールを適用できます。アプリケーションルールはインターネットプロトコル (IP) ルールに似ています。IP ルールについては、「IP ルール」を参照してください。

アプリケーションルールごとに、トラフィックポリシーを指定できます。利用可能なトラフィックポリシーは次のとおりです。

- **Load Balance Path**: フローのアプリケーショントラフィックは、複数のパスにまたがって分散されます。トラフィックは、そのパスが使用されるまで、最適パスを介して送信されます。残りのパケットは、次の最適パスを介して送信されます。
- 永続パス: アプリケーショントラフィックは、パスが使用できなくなるまで同じパス上に残ります。
- 重複パス: アプリケーショントラフィックは複数のパス間で重複するため、信頼性が向上します。
  アプリケーションルールはクラスに関連付けられています。

アプリケーションルールの適用方法

SD-WAN ネットワークでは、着信パケットが SD-WAN アプライアンスに到達すると、最初の少数のパケットが DPI 分類を受けません。この時点で、クラス、TCP 終端などの IP 規則属性がパケットに適用されます。DPI 分類後、クラス、トラフィックポリシーなどのアプリケーションルール属性は IP ルール属性よりも優先されます。

IP ルールは、アプリケーションルールと比較して、属性のより多くの数を持っています。アプリケーションルールは、いくつかの IP ルール属性のみをオーバーライドします。残りの IP ルール属性は、パケット上で処理されたままになります。

たとえば、SMTP プロトコルを使用する Google Mail などのウェブメールアプリケーションのアプリケーションルールを指定したとします。SMTP プロトコルに設定された IP ルールは、DPI 分類の前に最初に適用されます。パケットを解析して Google Mail アプリケーションに属するものとして分類すると、Google Mail アプリケーションに指定されているアプリケーションルールが適用されます。

アプリケーションルールの作成

アプリケーションルールを作成するには、[設定**] > [QoS] > [QoS** ポリシー] > [アプリケーションルール] に移動します。グローバルレベルでアプリケーションルールを作成するには [グローバルルール] タブを選択し、サイトレベルでルールを作成するには **[**サイト**/**グループ固有のルール] を選択します。

「アプリケーションルール」セクションの「新規アプリケーションルール ** 」をクリックします。

- アプリとドメインの一致基準
  - アプリとドメイン: ドロップダウンリストからアプリケーションまたはドメインを選択します。**+ New Domain App** をクリックしてドメインアプリを作成することもできます。名前を入力してドメインを追加します。
  - ルーティングドメイン: ルーティングドメインを選択します。デフォルトのルーティングドメインを選択することも、[**Any**] を選択することもできます。
  - 送信元ネットワーク: トラフィックと照合する送信元 IP アドレスとサブネットマスク。
  - 宛先ネットワーク: トラフィックと照合する宛先 IP アドレスとサブネットマスク。
  - 送信元ポート: トラフィックと照合する送信元ポート番号またはポート範囲。
  - 宛先ポート: トラフィックと照合する宛先ポート番号またはポート範囲。
  - **Src = Dest**: 選択すると、送信元ポートが宛先ポートとしても使用されます。

- 仮想パストラフィックポリシー

  「仮想パストラフィックポリシーを有効にする」チェックボックスを選択します。

  - 仮想パスリモートサイト: リモートサイトの仮想パスを選択します。
  - トラフィックポリシー: 必要に応じて、次のトラフィックポリシーのいずれかを選択します。
    - 負荷分散パス: フローのアプリケーショントラフィックは複数のパスに分散されます。トラフィックは、そのパスが使用されるまで、最適パスを介して送信されます。残りのパケットは、次の最適パスを介して送信されます。
    - 永続パス: アプリケーショントラフィックは、パスが使用できなくなるまで同じパス上に残ります。次のパーシスタンスポリシーのいずれかを選択します。
      - 発信元リンクで維持: アプリケーショントラフィックは、パスが使用できなくなるまで発信元リンクにとどまります。
      - 使用可能な場合は **MPLS** リンク上に存続し、それ以外の場合は発信元リンクに存続します。アプリケーショントラフィックは MPLS リンク上に残ります。MPLS リンクが使用できない場合、トラフィックは発信元のリンクに残ります。
      - 利用可能な場合はインターネットリンクを維持し、それ以外の場合は元のリンクで維持する: アプリケーショントラフィックはインターネットリンク上に残ります。インターネットリンクが利用できない場合、トラフィックは元のリンクに残ります。
      - 使用可能な場合はプライベートイントラネットリンクに保持し、それ以外の場合は元のリンクに保持する: アプリケーショントラフィックはプライベートイントラネットリンクに残ります。プライベートイントラネットリンクが使用できない場合、トラフィックは元のリンクに残ります。

      パーシステンスインピーダンスは、アプリケーショントラフィックがリンク上に留まるまでの時間（ミリ秒単位）です。
    - 重複パス: アプリケーショントラフィックは複数のパスにわたって重複するため、信頼性が向上します。

- QoS 設定 (QoS クラス)

  - 転送タイプ: 次の転送タイプのいずれかを選択します。
    - リアルタイム: 低遅延、低帯域幅、時間に敏感なトラフィックに使用されます。リアルタイムアプリケーションは時間に敏感ですが、実際には高い帯域幅（Voice over IP など）は必要ありません。リアルタイムアプリケーションはレイテンシーとジッターに敏感ですが、ある程度の損失は許容できます。
    - **Interactive**：低～中レイテンシーおよび低～中帯域幅要件の対話型トラフィックに使用されます。通常、対話はクライアントとサーバーの間で行われます。通信は、高帯域幅を必要としない場合がありますが、損失や遅延に敏感です。
    - バルク: 高帯域幅トラフィックおよび高遅延に耐えるアプリケーションに使用されます。ファイル転送を処理し、高帯域幅を必要とするアプリケーションは、バルククラスとして分類されます。こ

れらのアプリケーションは、人間の干渉をほとんど伴わず、ほとんどシステム自体によって処理されます。

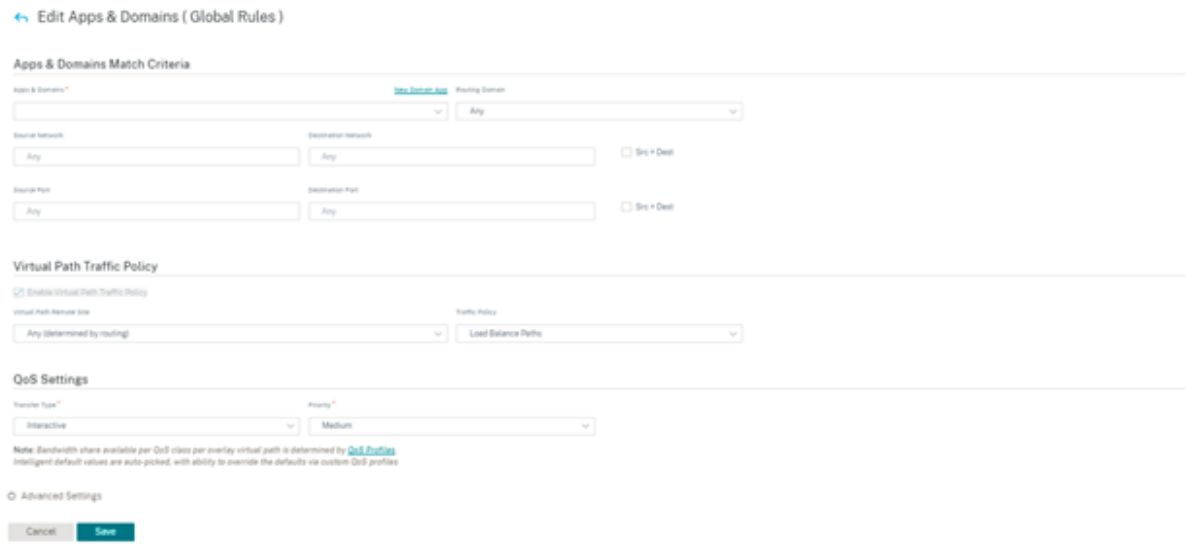
- 優先度: 選択した転送タイプの優先度を選択します。

詳細設定

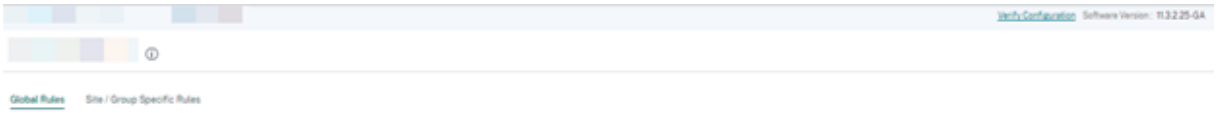
- WAN ジェネラル
  - 失われたパケットの再送信: このルールに一致するトラフィックを信頼できるサービスを介してリモートアプライアンスに送信し、失われたパケットを再送信します。
  - パケットアグリゲーションを有効にする: 小さなパケットを大きなパケットに集約します。
- LAN から WAN
  - ドロップ深度 **(**バイト**)**: パケットがドロップされるまでのキュー深度のしきい値。
  - ドロップ制限: クラススケジューラで待機しているパケットがドロップされるまでの時間。バルククラスには適用されません。
  - **ENABLE RED**: ランダム早期検出（RED）は、輻輳が発生したときにパケットを廃棄することにより、クラスリソースの公平な共有を保証します。
  - 重複パケット無効化レベル **(**バイト**)**: クラススケジューラのキュー深度。この時点で重複パケットは生成されません。
  - 重複パケット無効制限: 重複パケットが帯域幅を消費するのを防ぐために、重複パケットを無効にできる時間。
- WAN から LAN へ
  - **DSCP** タグ: このルールに一致するパケットを LAN に送信する前に WAN/LAN 上で適用される DSCP タグ。
  - パケットの再順序付けを有効にする: ルールに一致するトラフィックフローにシーケンス順序のタグが付けられ、パケットは WAN-to-LAN アプライアンスで（必要に応じて）並べ替えられます。
  - **Hold Time**: パケットが再シーケンシングのために保持される時間間隔。この時間が経過すると、パケットは LAN に送信されます。タイマーが切れると、パケットは前提条件のシーケンス番号を待たずに LAN に送信されます。

    ルールに重複パスとしてのトラフィックポリシーがある場合、デフォルトのホールドタイムは 80 ミリ秒です。それ以外の場合、デフォルトは TCP ルールでは 900 ミリ秒、TCP 以外のルールでは 250 ミリ秒です。
  - 遅延再シーケンスパケットの破棄: 再シーケンス処理に必要なパケットが LAN に送信された後に到着した順序どおりでないパケットを廃棄します。

[保存] をクリックして構成設定を保存します。



[設定] **> [QoS] > [**QoS** ポリシー] ページの [設定の検証 **] をクリックして、監査エラーを検証します。監査エラーを検証します。

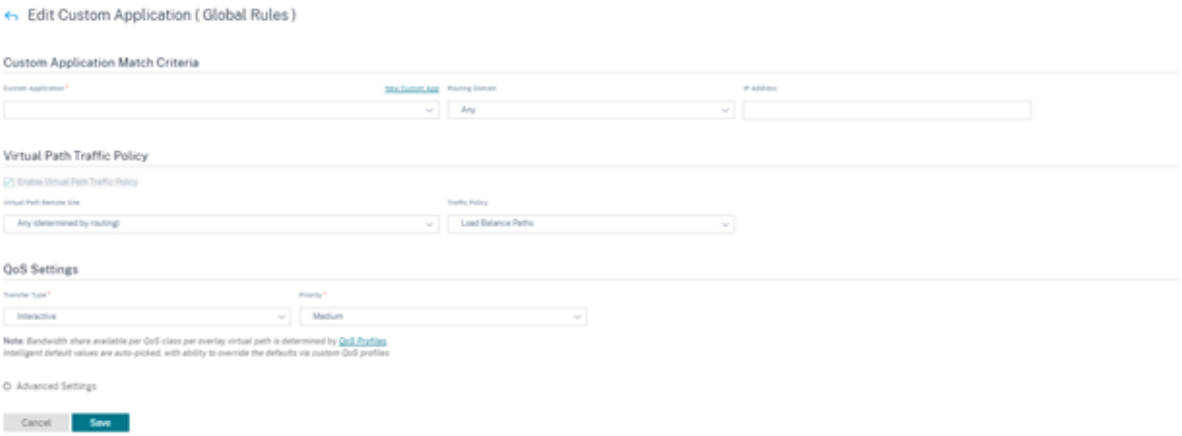


カスタムアプリケーションルールの作成

カスタムアプリケーションルールを作成することもできます。カスタムアプリケーションルールを作成するには、[設定] **> [QoS] > [QoS** ポリシー] > [カスタムアプリケーションルール] に移動します。グローバルレベルでカスタムアプリケーションルールを作成するには [グローバルルール] タブを選択し、サイトレベルでルールを作成するには **[**サイト**/**グループ固有のルール] を選択します。

「カスタムアプリケーションルール」セクションの「新規カスタムアプリケーションルール **** 」をクリックします。**[**** カスタムアプリケーション**]** フィールド名の横にある **[**** 新規カスタムアプリケーション **] をクリックします。カスタムアプリケーションの名前を入力します。**Match Criteria** セクションで、アプリケーション、プロトコル、DSCP タグを選択し、ネットワーク IP とポート番号を入力します。［保存］をクリックします。

必要に応じて、他のフィールドに詳細を入力します。フィールドの説明については、「アプリケーションルールの作成」を参照してください。

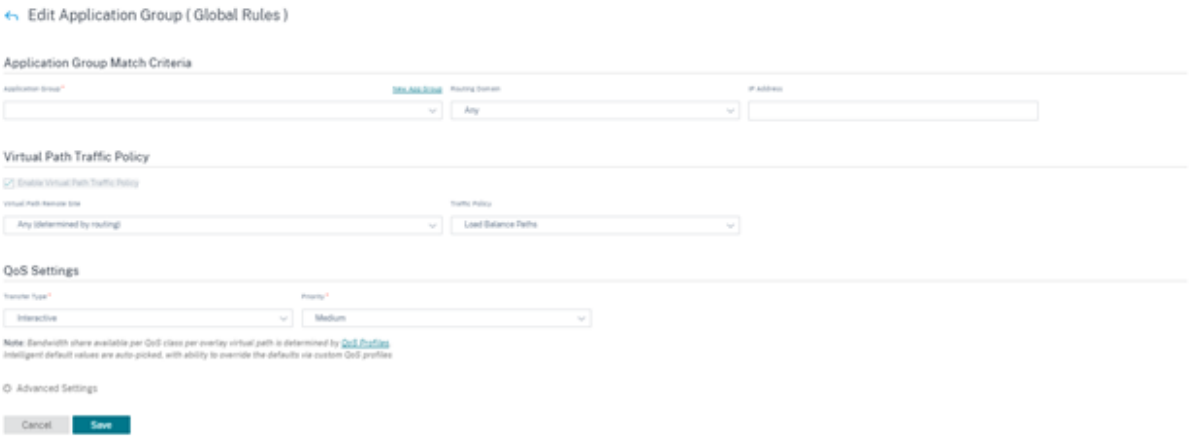


アプリケーショングループルールの作成

アプリケーショングループのルールを作成できます。アプリケーショングループルールを作成するには、[構成**] > [QoS** ポリシー**] **[**** アプリケーショングループルール] に移動します。グローバルレベルでアプリケーショングループルールを作成するには「グローバルルール」タブを選択し、サイトレベルでルールを作成するには「サイト**/**グループ固有のルール」を選択します。

アプリケーショングループルールセクションの「新規アプリケーショングループルール ****** 」をクリックします。****** アプリケーショングループフィールド名の横にある「****** 新規アプリグループ ** 」をクリックします。アプリケーショングループの名前を入力します。必要に応じてアプリケーションを検索して追加します。［保存］をクリックします。

必要に応じて、他のフィールドに詳細を入力します。フィールドの説明については、「アプリケーションルールの作成」を参照してください。



アプリケーションルールを検証

アプリケーションルールを確認するには、[レポート] **>** [リアルタイム] **>** [フロー] に移動します。フロー情報と表示するフローの数を表示するサイトを選択します。「列をカスタマイズ」をクリックし、表示したいフロー情報に対応するチェックボックスを選択します。フロー情報が設定された規則に従っているかどうかを確認します。

[レポート] **>** [リアルタイム] **>** [統計] に移動し、[ルール] を選択します。サイトを選択し、[最新データを取得] をクリックします。設定したルールを確認します。

レポートの詳細については、「フロー」を参照してください。

HDX QoE

October 26, 2022

レイテンシー、ジッタ、パケットドロップなどのネットワークパラメーターは、HDX ユーザーのユーザーエクスペリエンスに影響します。体感品質（QoE）は、ユーザーが ICA 体験の質を理解して確認するのに役立ちます。QoE は計算されたインデックスで、ICA トラフィックのパフォーマンスを示します。ユーザーは、QoE を向上させるために、ルールとポリシーを調整できます。

QoE は 0 ～100 の数値で、値が大きいほどユーザーエクスペリエンスが向上します。

QoE の計算に使用されるパラメータは、クライアント側とサーバー側にある 2 つの Citrix SD-WAN アプライアンス間で測定され、クライアントまたはサーバーアプライアンス自体の間で測定されるものではありません。遅延、ジッタ、およびパケットドロップはフローレベルで測定され、リンクレベルの統計情報とは異なる場合があります。エンドホスト（クライアントまたはサーバ）アプリケーションは、WAN でパケット損失があることを認識しません。再送信が成功すると、フローレベルのパケット損失レートはリンクレベルの損失よりも低くなります。ただし、その結果、レイテンシーとジッタが少し増加する可能性があります。

オンプレミス向け Citrix SD-WAN Orchestrator の HDX ダッシュボードでは、HDX アプリケーションの全体的な品質をグラフィカルに表示できます。HDX アプリケーションは、次の 3 つの品質カテゴリに分類されます。

品質	QoE 範囲
高	71-100
標準	51-70
低	0-50

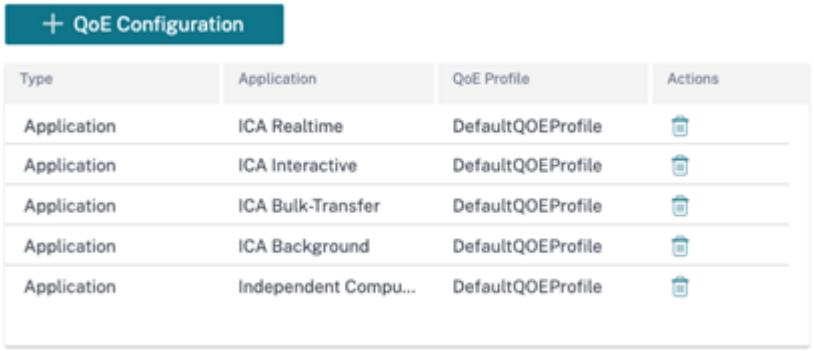
選択した UI ページに応じて、下位（QoE が最低）の 5 つのサイト、5 人のユーザー、5 つのセッション、またはそれらすべてのリストが HDX ダッシュボードに表示されます。

異なる時間間隔での QoE のグラフィック表示により、各サイトで HDX アプリケーションのパフォーマンスを監視できます。

HDX QoE の設定

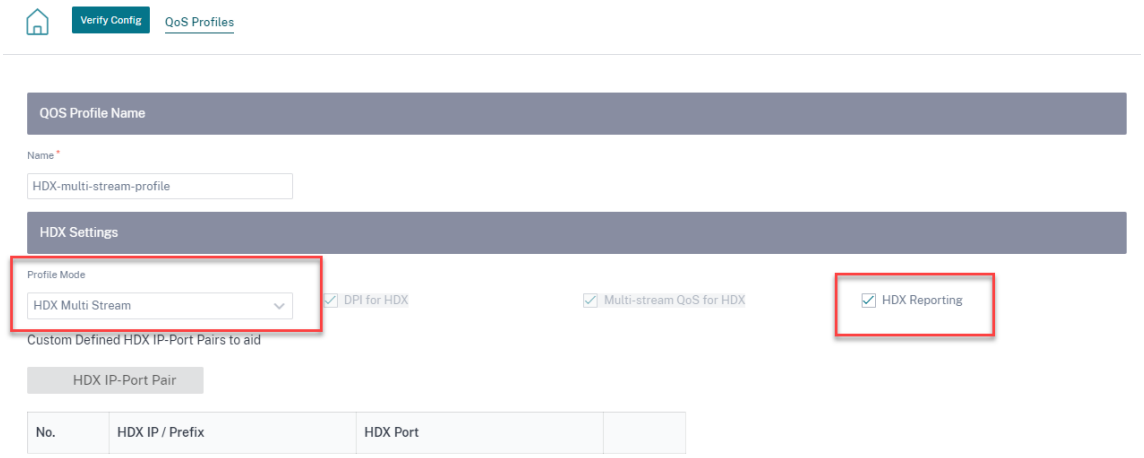
1. ネットワークレベルで、[構成] **>** [アプリ設定とグループ] **>** [アプリ品質設定] に移動し、[**+ QoE** 設定] をクリックします。HDX 動作の計算に使用する QoE プロファイルを使用して、次のアプリケーションを追加します。

   - ICA リアルタイム (ica_priority_0)
   - ICA インタラクティブ (ica_priority_1)
   - ICA 一括転送 (ica_priority_2)
   - ICA の背景 (ica_priority_3)
   - 独立コンピューティングアーキテクチャ（Citrix）(ICA)

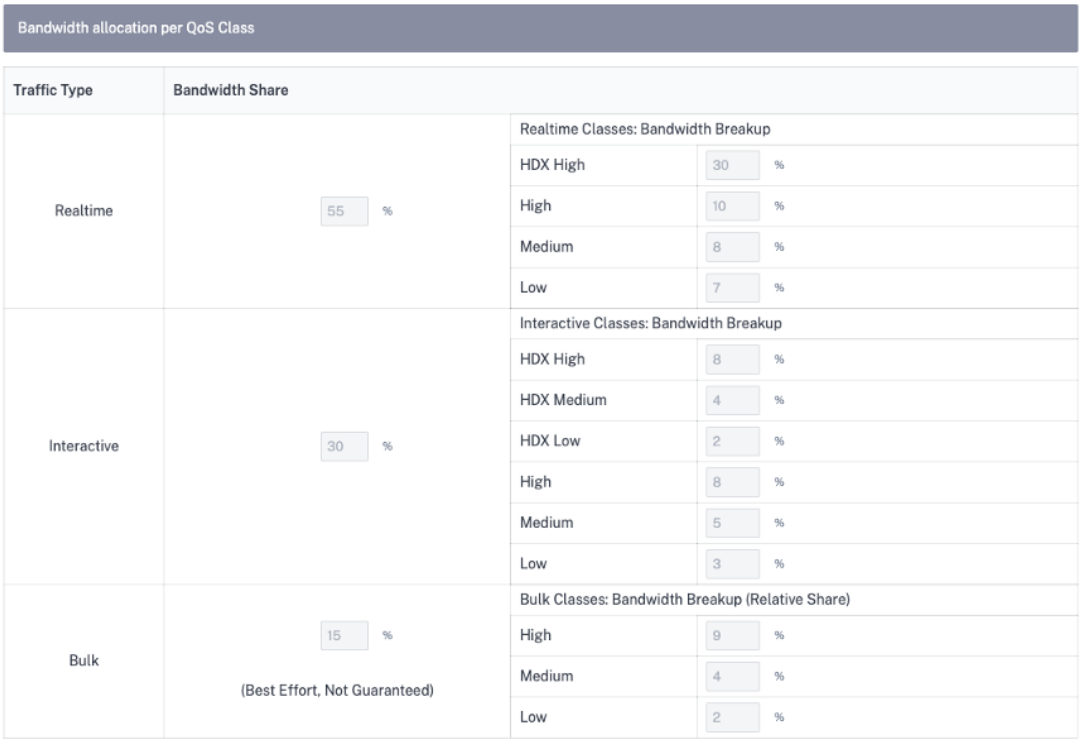


   これらの構成は、プロファイルを通じて HDX レポートで使用される HDX パフォーマンスを測定するためのパラメータを提供します。HDX マルチストリーム（MSI）接続には ICA リアルタイム、ICA インタラクティブ、ICA 一括転送、ICA バックグラウンドの設定が必要です。シングルストリーム（SSI）接続には独立コンピューティングアーキテクチャ（Citrix）が必要です。

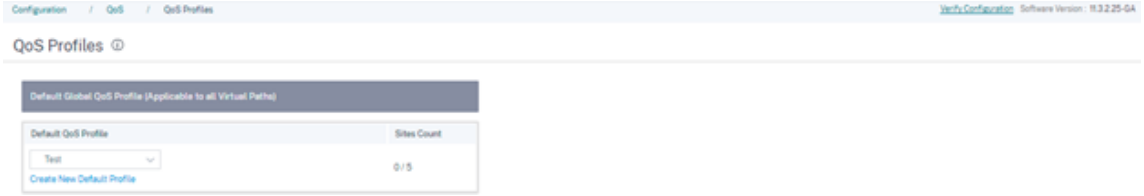
2. 設定 **> QoS > QoS** プロファイルに移動します。デフォルトの QoS プロファイルとして「標準**-HDX-**マルチストリーム」を選択し、「**HDX** レポート」チェックボックスを選択します。**HDX** レポートが不要な場合は、HDX レポートをクリアしてください。



各 QoS プロファイルには、クラスごとに事前に定義された帯域幅パーセンテージがあります。これらは、HDX トラフィックが使用しているクラスに割り当てられる帯域幅を調整するように構成できます。

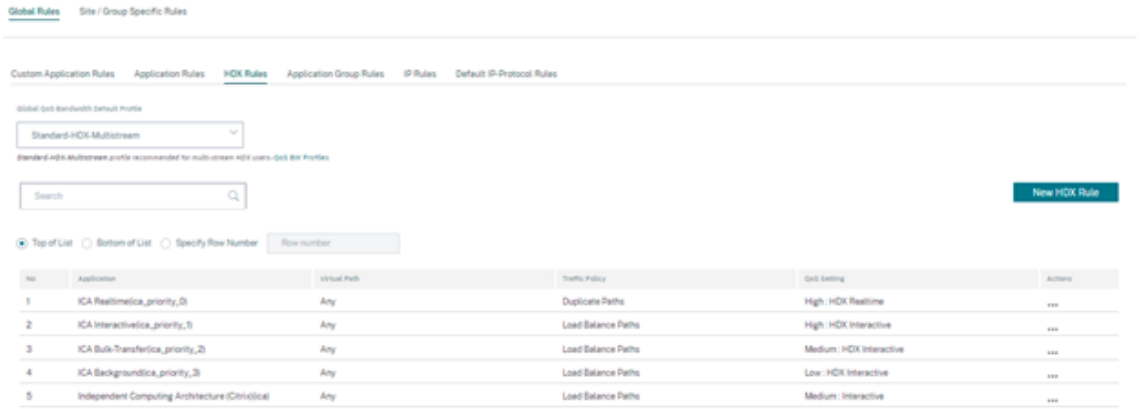


3. サイト数インジケータをチェックして、新しい QoS プロファイルがアクティブに使用されていることを確認します。



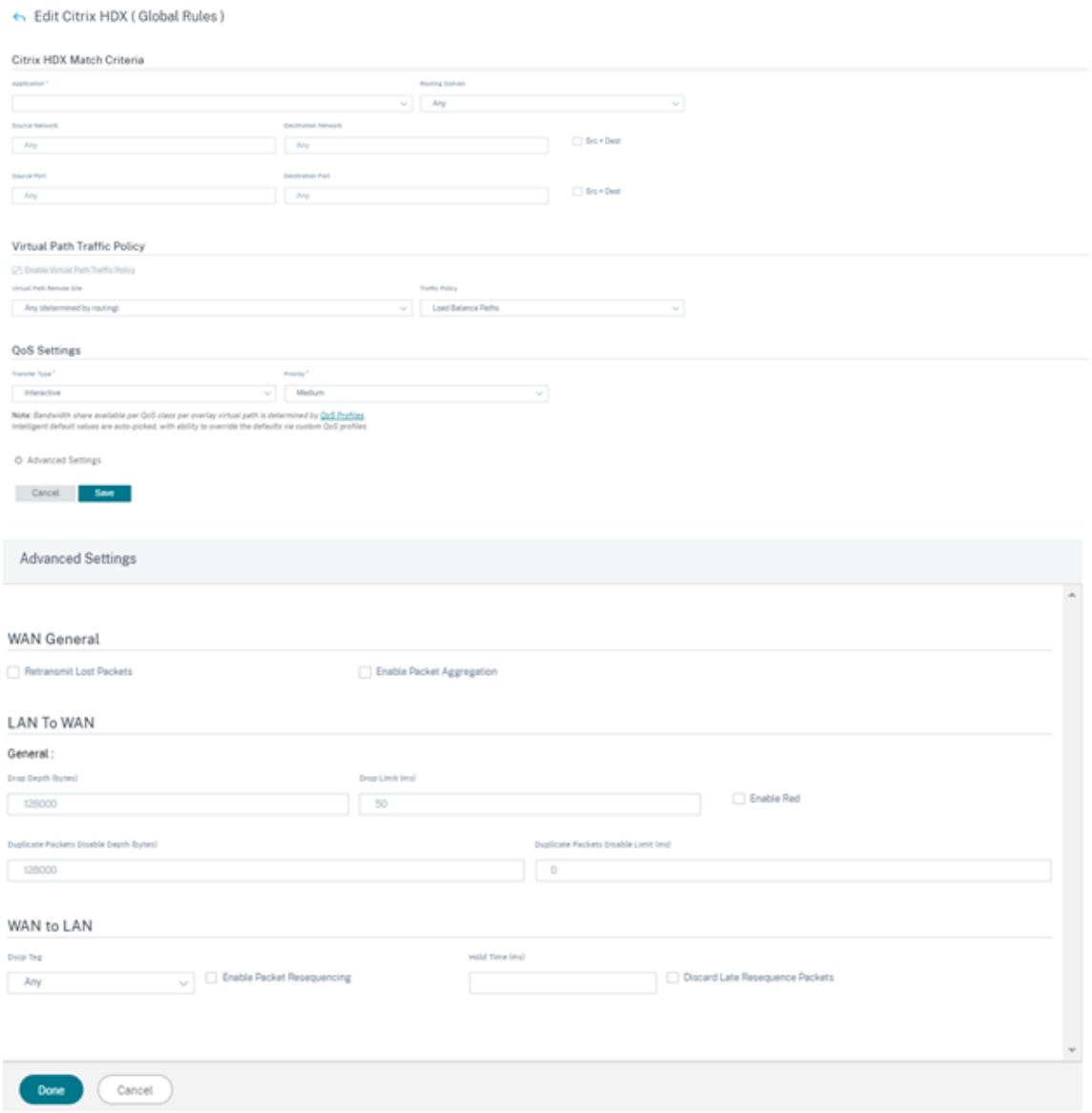
4. ［構成］**>** ［**QoS** ポリシー］> ［**HDX** ルール］に移動し、有効な **HDX** レポートを含む新しい **QoS** プロファイルをグローバル **QoS** 帯域幅デフォルトプロファイルとして設定します。

5. HDX ルールを追加します。これらの構成により、HDX 接続に適切な QoS 設定が割り当てられます。ルールの詳細を確認したり、ルールを編集したりするには、**HDX** ルールページの下部セクションに移動します。「ルール」テーブルで、「アクション」列に移動して「編集」を選択します。デフォルトルールの設定を変更するには、[クローン] をクリックして必要な変更を加えます。



次の構成は変更できます。

- QoS クラス: リアルタイム、インタラクティブ、バルク
- 交通政策:
  - 重複パス: 信頼性を高めるため、トラフィックは複数のパスにわたって複製されます。
  - パーシステントパス: フローのトラフィックは、パスが使用できなくならない限り、同じパスにとどまります。
  - 負荷分散パス: フローのトラフィックは複数のパスに分散されます。
  - 詳細設定: 再送信、RED、遅延パケットのポリシーを設定します。



HDX ダッシュボードとレポート

オンプレミス向け Citrix SD-WAN Orchestrator は、サイト、ユーザー、およびセッションごとに、ネットワーク全体の Citrix 仮想アプリケーションおよびデスクトップのユーザーエクスペリエンスを最新の詳細に測定するための HDX ダッシュボードを提供します。

HDX セッションには、シングルストリームとマルチストリームの 2 種類があります。シングルストリームセッションは、セッション内の接続は 1 つだけですが、マルチストリームセッションには 4 つの接続があります。マルチストリームセッションにより、より高度な QoS が可能になります。マルチストリーム HDX セッションの最優先接続は、リアルタイムクラスとインタラクティブクラスに他の 3 つのデフォルトながら、シングルストリーム HDX セッションでの接続は、インタラクティブクラスにデフォルトで、インタラクティブクラスにデフォルトです。これは構成可能です。

エクスペリエンス品質 (QoE) スコアは、0 ～100 の間の数値です。値が高いほど、ユーザーエクスペリエンスは向上します。リアルタイムクラストラフィック QoE は、ジッタ、遅延、および損失率に基づいて計算されます。対話型クラス QoE は、バーストレートと損失率に基づいて計算されます。セッションの QoE は、セッション内のすべての接続の平均です。ユーザーの QoE は、そのユーザーが起動したすべてのセッションの平均値です。サイトの QoE は、そのサイト上のすべてのセッションの平均です。

すべての統計はメトリックスです。

- そのサイトの HDX トラフィックの場合
- そのユーザーが経験した
- そのセッション内のすべての接続のうち

他のタイプのトラフィックのメトリックは含まれません。メトリックは、選択した期間の平均か、選択した期間の合計のいずれかです。

> 注:
>
> HDX レポート作成には最低限のソフトウェアバージョンが必要です。
>
> - Citrix Virtual Apps and Desktops 7—1912 LTSR（または現在のリリース）
> - Windows 19.12 LTSR（または現在のリリース）向け Citrix Workspace アプリ
> - SD-WAN 11.2.0 (または現在のバージョン)

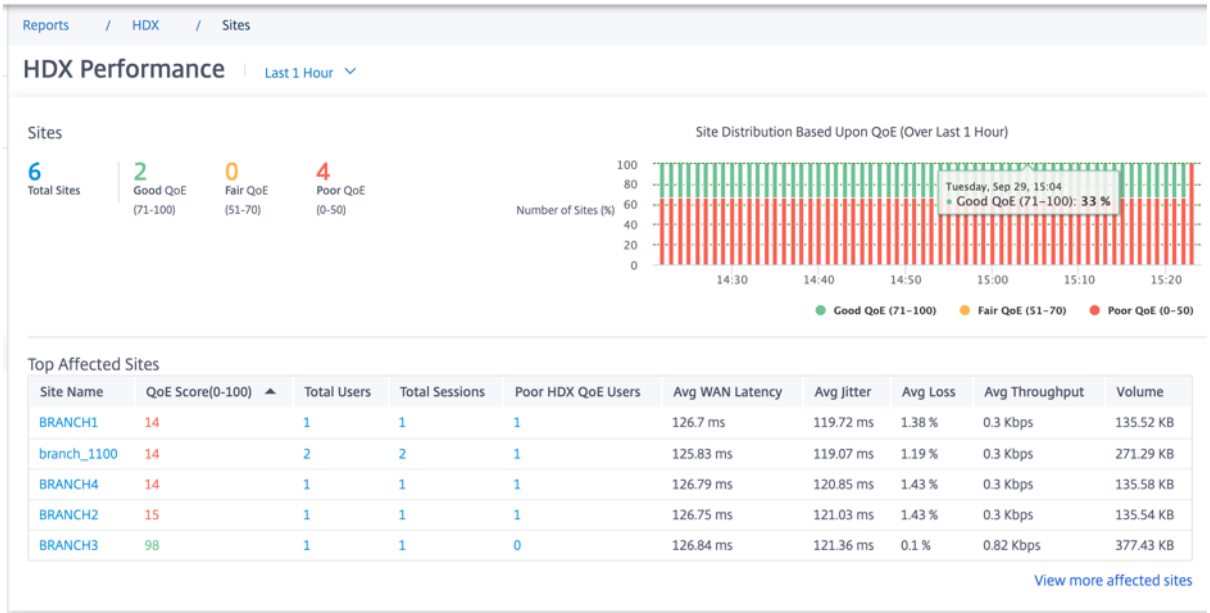
Citrix は、常に最新のソフトウェアバージョンを使用して、最新のバグ修正と拡張機能を取得することを推奨しています。たとえば、SD-WAN では、Citrix Virtual Apps and Desktops LTSR の新しいバージョンで導入された新しい EDT コマンドをサポートするには、リリース 11.2.3 または 11.3.1 が必要です。

Mac クライアントと Linux クライアントは、Citrix SD-WAN を介したマルチストリーム ICA および HDX レポートを完全にはサポートしていません。たとえば、Linux クライアントはマルチストリームをサポートしていますが、往復時間や遅延などの詳細はありません。CWA 機能マトリックスでは、どのオペレーティングシステムが NSAP VC 機能を備えたマルチポート **ICA** および **HDX Insight** 機能をサポートしているかがわかります。

ユーザーは、StoreFront に直接アクセスするか、ビーコンポイントまたはネットワークロケーションサービスを使用して、Citrix Gateway 暗号化の外部で HDX にアクセスする必要があります。

サイト

この HDX レポートは、サイトごとの詳細な HDX データを提供します。サイトの統計情報を表示するには、［レポート］>［**HDX**］>［サイト］に移動します。



ダッシュボードは、選択した時間間隔（たとえば、過去 5 分、過去 30 分、過去 1 日、過去 1 か月など）に HDX トラフィックが実行されているサイトでレポートされます。サイトのパフォーマンスは、サイトの HDX トラフィックの QoE に基づいて、良い (71-100)、公正 (51-70)、または低下 (0-50) に分類されます。概要セクションと上位影響を受けたサイトの表の **QoE** 値は、選択した期間の平均値です。時系列グラフィックレポートには、経過とともに詳細な履歴が表示されます。各バーは、その時点での良好な QoE サイト、公正サイト、不良サイトの割合を示します。

また、「**QoE** に基づくサイト分布」グラフでは、その時点で **QoE** が良い、公平な、悪いサイトの数をパーセンテージで表示できます。カラーバーにマウスを置くと、良い/フェア/貧弱な状態のサイトの割合が表示されます。

> 注
>
> - 統計情報は、リモート側から現在のサイトまで、一方向に収集されます。たとえば、サイト A とサイト B 間のセッションの場合、サイト A のレポートは、サイト-B からサイト A へのトラフィックで収集され、一方、サイト-B のレポートは、サイト A からサイト-B へのトラフィックについて収集されます。したがって、サイト A とサイト B の同じセッションの統計は異なる場合があります。
> - 上位影響を受けたサイトの表には、最も影響を受けた上位 5 つのサイトのみが反映されています。デフォルトでは、QoE スコアが最も低い 5 つのサイトが表示されます。しかし、各列はソート可能、昇順、または降順であり、クエリ条件として使用されます。たとえば、平均ジッター列のタイトルをクリックすると、平均ジッターが最も低い 5 つのサイトと平均ジッターが最も高い 5 つのサイトの表示が切り替わります。他の列でも同じです。選択した期間に HDX トラフィックがあったすべてのサイトの詳細を確認するには、「影響を受けたサイトをさらに表示」をクリックします。

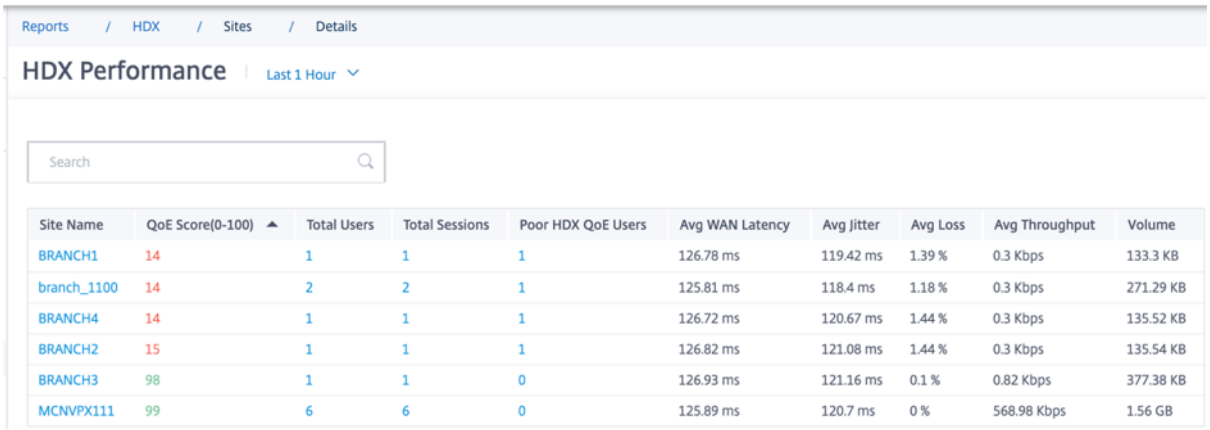
各サイトの詳細は次のとおりです。

- サイト名: サイト名。
- **QoE** スコア **(0-100)**: このサイトの平均 QoE スコア。
- 総ユーザー数: 選択した期間中にサイトで閲覧されたアクティブな HDX ユーザーの総数です。

- 合計セッション数：選択した期間中にサイトで閲覧された HDX セッションの総数。シングルストリームセッションとマルチストリームセッションの両方が含まれます。
- 貧弱な **HDX QoE** ユーザー：QoE が低い（50 人未満）に苦しんでいる HDX ユーザーの数。
- 平均 **WAN** 遅延: リモートサイトからこのサイトまでの WAN 経由の平均遅延。
- 平均ジッター: 選択した期間の平均ジッター値。
- 平均損失: 選択した期間の平均パケット損失率値。
- 平均スループット: 選択した期間の平均データスループット値。
- ボリューム: このサイトで見られた総トラフィック量。Citrix SD-WAN Orchestrator for オンプレミス GUI は、数値の値に基づいてユニットを調整および変更する場合があります。

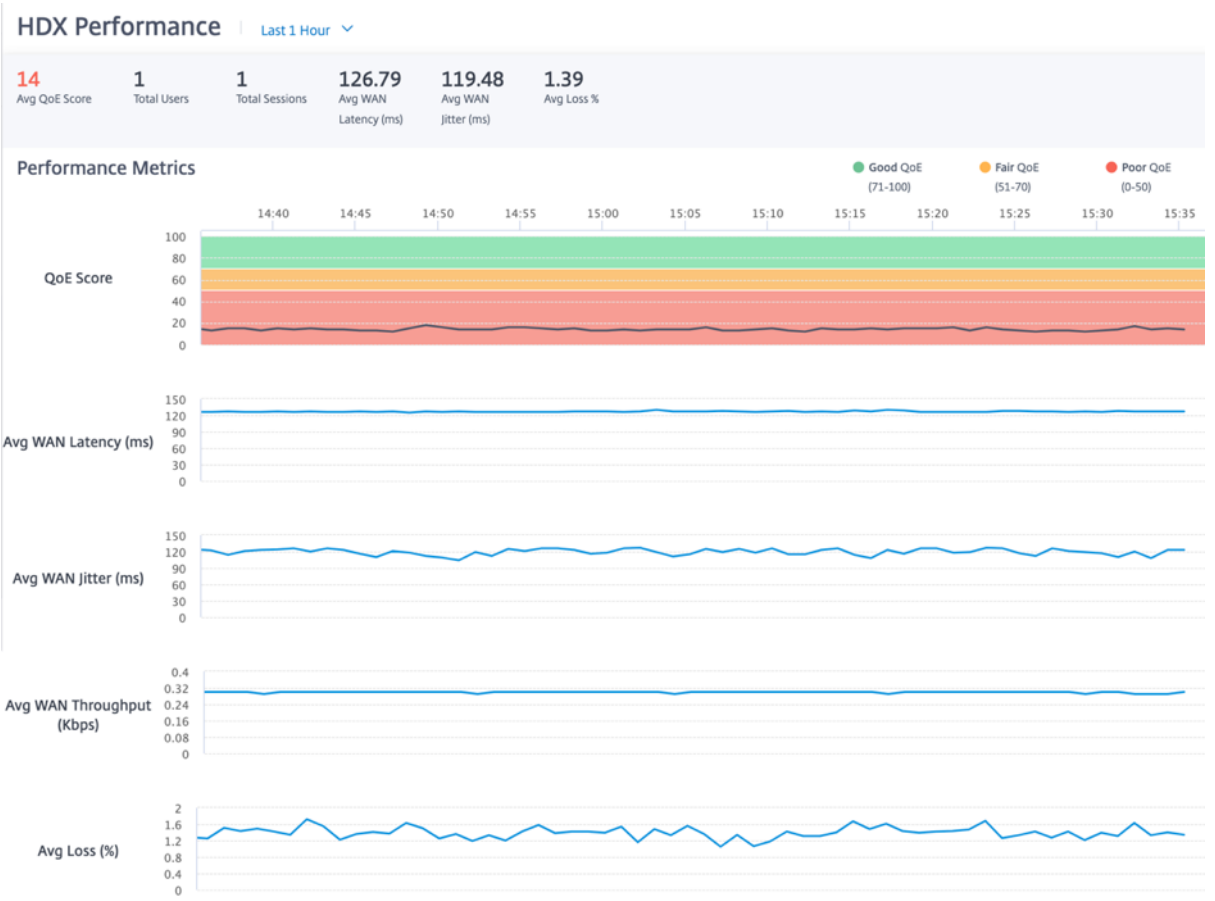
列タイトルをクリックすると、その列でソートされたレポートが表示されます。すべてのサイトのレポートを表示するには、[影響を受けるサイトをさらに表示] をクリックします。1 つの行をクリックすると、そのサイトの詳細レポートが表示されます。

次のスクリーンショットの表は、すべてのサイトを示すレポート表の例です。この列には、上位影響を受けたサイトの表と同じ列があります。



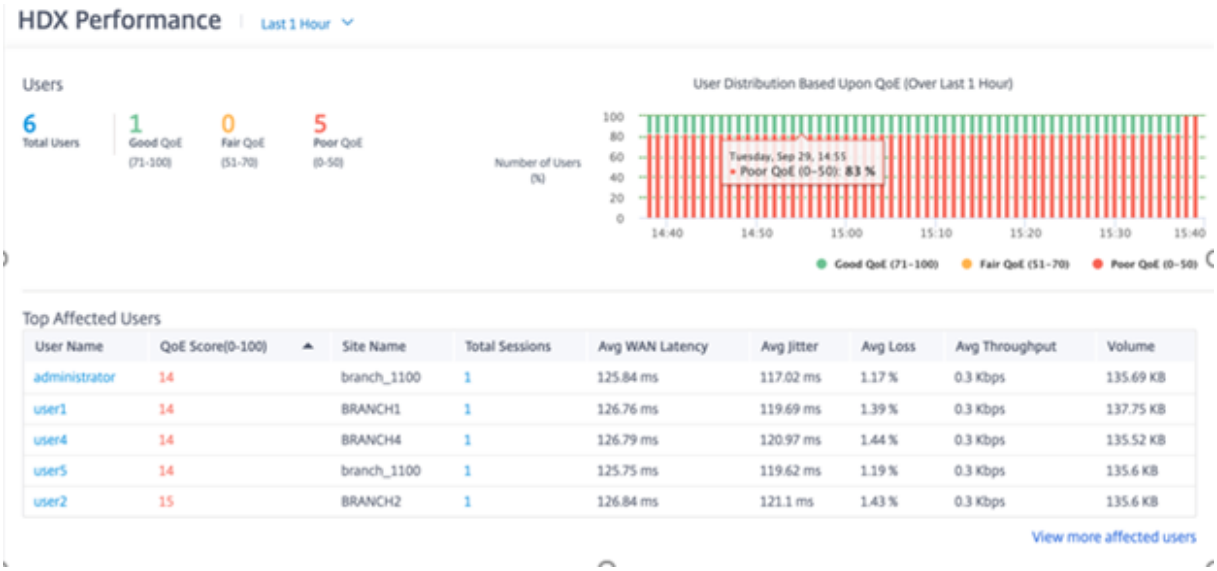
Site Name	QoE Score(0-100)	Total Users	Total Sessions	Poor HDX QoE Users	Avg WAN Latency	Avg Jitter	Avg Loss	Avg Throughput	Volume
BRANCH1	14	1	1	1	126.78 ms	119.42 ms	1.39 %	0.3 Kbps	133.3 KB
branch_1100	14	2	2	1	125.81 ms	118.4 ms	1.18 %	0.3 Kbps	271.29 KB
BRANCH4	14	1	1	1	126.72 ms	120.67 ms	1.44 %	0.3 Kbps	135.52 KB
BRANCH2	15	1	1	1	126.82 ms	121.08 ms	1.44 %	0.3 Kbps	135.54 KB
BRANCH3	98	1	1	0	126.93 ms	121.16 ms	0.1 %	0.82 Kbps	377.38 KB
MCNVPX111	99	6	6	0	125.89 ms	120.7 ms	0 %	568.98 Kbps	1.56 GB

個々のサイトの行をクリックすると、パフォーマンスメトリックがグラフィカルに表示されます。グラフィックの上にマウスを置くと、詳細が表示されます。



Users

HDX ユーザーレポートを表示するには、［レポート］>［**HDX**］**>**［ユーザー］に移動します。



ユーザーレポートには、選択した期間（過去 5 分間、過去 30 分間、過去 1 日、過去 1 か月など）に各ユーザーが経

験したパフォーマンスが表示されます。選択した期間中にユーザーが複数のサイトにアクセスしている場合、そのユーザーが最後にログインしたサイトがレポートに表示されます。ユーザーエクスペリエンスは、HDX トラフィックの QoE スコアに基づいて、良い（71-100）、公平（51-70）、または貧しい（0-50）に分類されます。概要セクションと上位影響を受けるユーザー表の **QoE** 値は、選択した期間の平均値です。時系列グラフィックレポートには、経過とともに詳細な履歴が表示されます。各バーは、その時点での QoE が良好で公正で貧弱なユーザーの割合を示します。

また、「**QoE** に基づくユーザー分布」グラフでは、その時点での **QoE** が良い、公平な、悪いユーザー数をパーセンテージで表示できます。カラーバーにマウスを置くと、良い/フェア/貧弱な状態のユーザー数の割合が表示されます。

個人を特定できる情報　現在、HDX QoE レポートには次の 2 つの個人識別情報（PII）フィールドがあります。

- ユーザー名: ユーザー名を表示します。
- **IP** アドレス: クライアントの IP アドレスが表示されます。

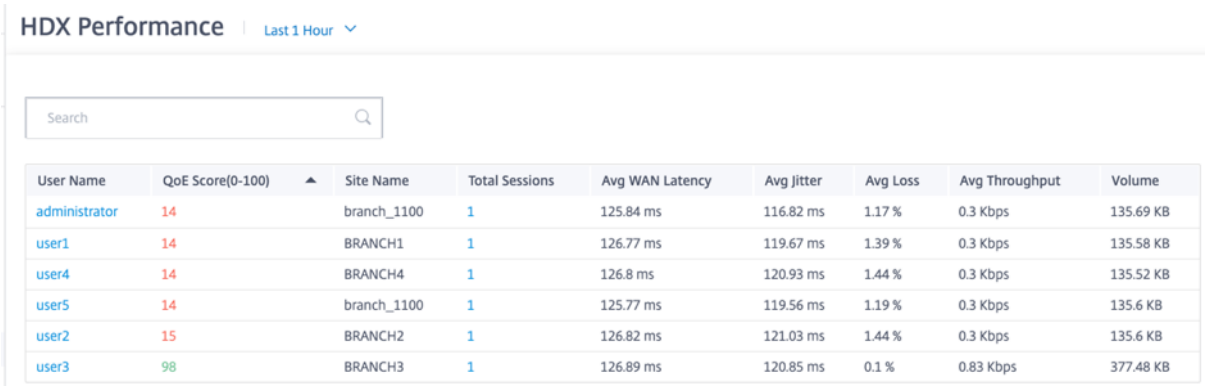
> 注
>
> - ユーザー名が使用できない場合、IP アドレスが [ユーザー名] フィールドに表示されます。
> - HDX ユーザー・レポートは、Virtual Delivery Agent （VDA）側の SD-WAN ではなく、クライアント側の SD-WAN からの統計に基づいています。これは、エンドユーザーの HDX エクスペリエンスを反映しています。
> - 上位影響を受けたユーザーの表には、最も影響を受けた上位 5 人のユーザーのみが反映されています。デフォルトでは、QoE が最も低い上位 5 人のユーザーが表示されます。しかし、各列はソート可能、昇順、または降順であり、クエリ条件として使用されます。たとえば、**Avg Jitter** カラムのタイトルをクリックすると、平均ジッターが最も低い 5 人のユーザーと平均ジッターが最も高い 5 人のユーザーの表示が切り替わります。選択した期間に HDX トラフィックがあったすべてのユーザーの詳細を確認するには、「影響を受けたユーザーをさらに表示」をクリックします。

各ユーザーの詳細を次に示します。

- ユーザー名: ユーザー名。
- **QoE** スコア **(0～100)**: このユーザーの平均 QoE スコア。
- サイト名: ユーザーがログインしたサイト名。
- 合計セッション: シングルストリームセッションとマルチストリームセッションの両方を含む、そのユーザーのアクティブな HDX セッションの総数です。
- 平均 **WAN** 遅延: クライアント側で発生した、WAN 経由の平均遅延。
- 平均ジッター: 選択した期間の平均ジッター値。
- 平均損失: 選択した期間の平均パケット損失率値。
- 平均スループット: 選択した期間の平均データスループット値。
- ボリューム: このユーザーが使用した総トラフィック量。Citrix SD-WAN Orchestrator for オンプレミス GUI は、数値の値に基づいてユニットを調整および変更する場合があります。

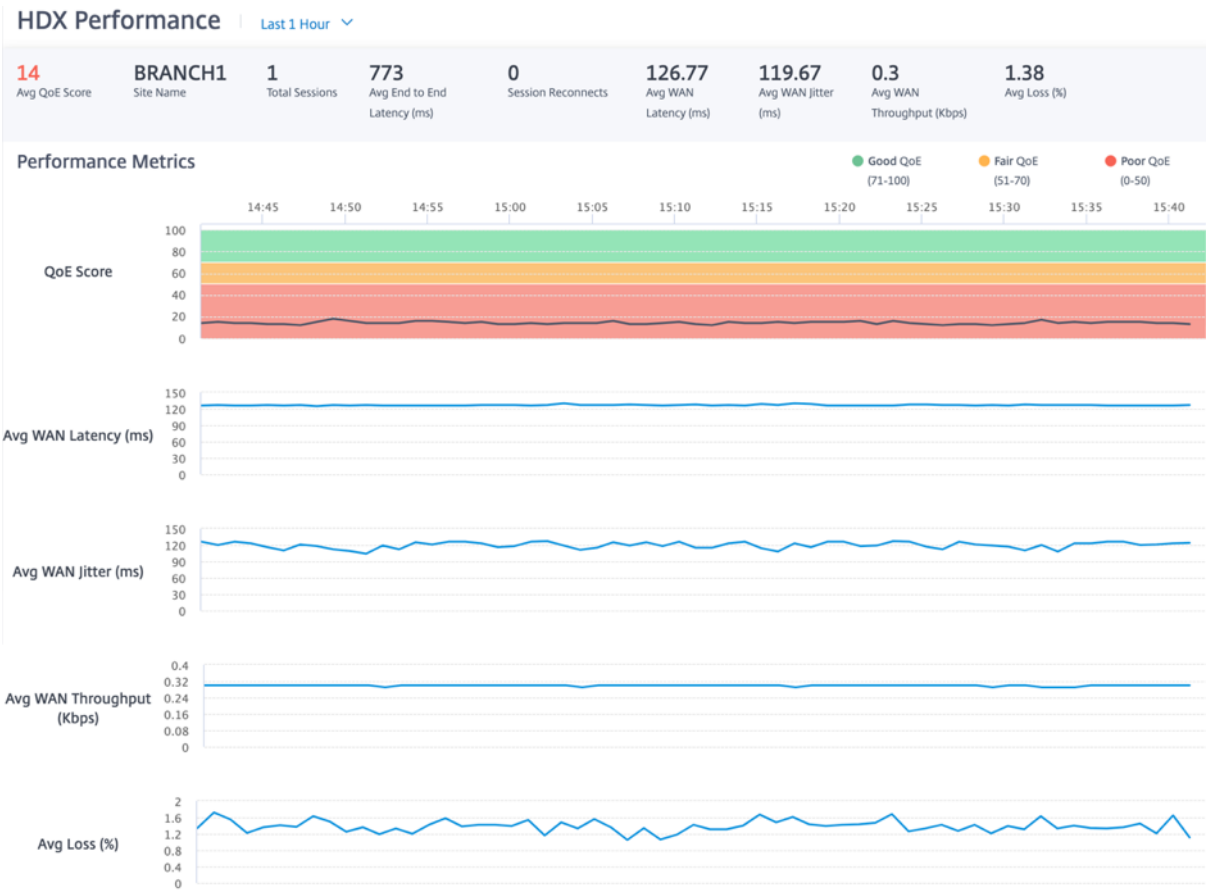
列タイトルをクリックすると、その列でソートされたレポートが表示されます。すべてのユーザーのレポートを表示するには、「影響を受けるユーザーをさらに表示」をクリックします。1 つの行をクリックすると、そのユーザの詳細レポートが表示されます。

次のスクリーンショットは、すべてのユーザーを表示するレポートの例です。この列には、「上位影響を受けたユーザ」テーブルと同じ列があります。



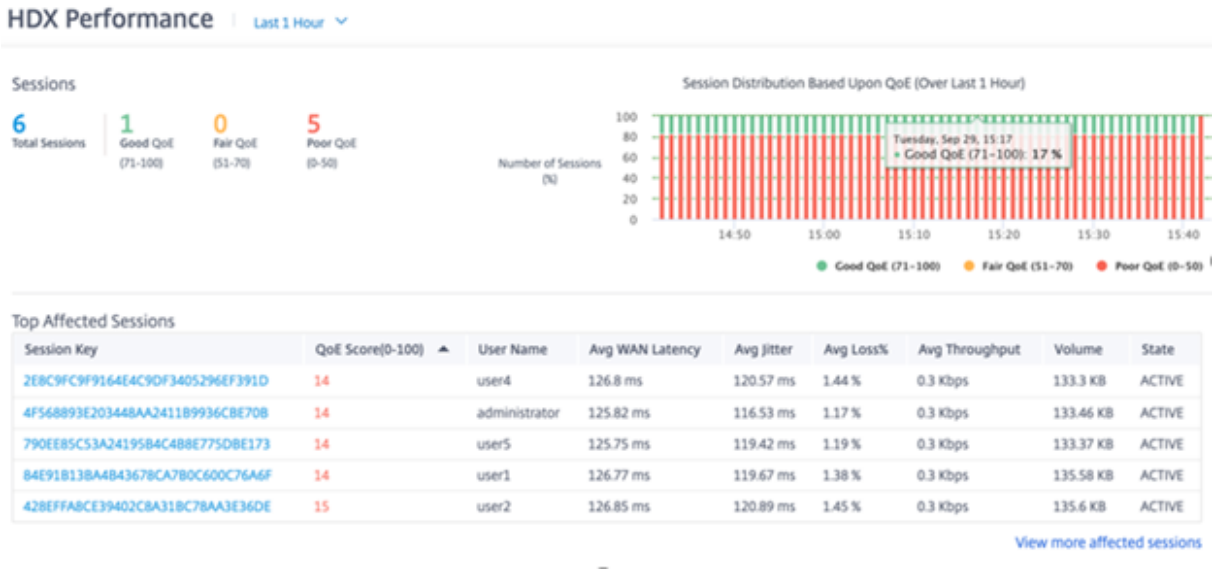
User Name	QoE Score(0-100)	Site Name	Total Sessions	Avg WAN Latency	Avg Jitter	Avg Loss	Avg Throughput	Volume
administrator	14	branch_1100	1	125.84 ms	116.82 ms	1.17 %	0.3 Kbps	135.69 KB
user1	14	BRANCH1	1	126.77 ms	119.67 ms	1.39 %	0.3 Kbps	135.58 KB
user4	14	BRANCH4	1	126.8 ms	120.93 ms	1.44 %	0.3 Kbps	135.52 KB
user5	14	branch_1100	1	125.77 ms	119.56 ms	1.19 %	0.3 Kbps	135.6 KB
user2	15	BRANCH2	1	126.82 ms	121.03 ms	1.44 %	0.3 Kbps	135.6 KB
user3	98	BRANCH3	1	126.89 ms	120.85 ms	0.1 %	0.83 Kbps	377.48 KB

個々のユーザー行をクリックすると、そのユーザーのパフォーマンスメトリックがグラフィカルに表示されます。



セッション

セッションレポートには、セッションレベルで詳細が表示されます。セッションレポートを表示するには、［レポート］>［**HDX**］**>**［セッション］に移動します。



ダッシュボードには、選択した期間に実行された HDX セッションのレポート（たとえば、過去 5 分間、過去 30 分、過去 1 日、過去 1 か月など）が表示されます。セッションは、そのセッションの QoE に基づいて、良い（71-100）、フェア（51-70）、または貧しい（0-50）に分類されます。「要約」セクションおよび「影響上位表」の「QoE」の値は、選択した期間の平均値です。時系列グラフィックレポートには、経過とともに詳細な履歴が表示されます。各バーは、その時点での良好な、公平、貧弱な QoE セッションの割合を示します。

また、「**QoE** に基づくセッション分布」グラフでは、その時点での **QoE** が良い、公平な、悪いセッションの数をパーセンテージで表示できます。カラーバーにマウスを置くと、良好/フェア/貧弱状態のセッション数の割合が表示されます。

> 注
>
> - HDX セッションレポートは、VDA 側の SD-WAN ではなく、クライアント側の SD-WAN からの統計に基づいています。これは、エンドユーザーの HDX エクスペリエンスを反映しています。
> - 上位影響を受けたセッションの表には、最も影響を受けた上位 5 つのセッションのみが反映されています。デフォルトでは、QoE が最も低い上位の 5 つのセッションが表示されます。しかし、各列はソート可能、昇順、または降順であり、クエリ条件として使用されます。たとえば、**Avg Jitter** カラムのタイトルをクリックすると、平均ジッターが最も低い 5 つのセッションと平均ジッターが最も高い 5 つのセッションのいずれかの表示が切り替わります。選択した期間中のすべての HDX セッションの詳細を確認するには、「影響を受けたセッションをさらに表示」をクリックします。

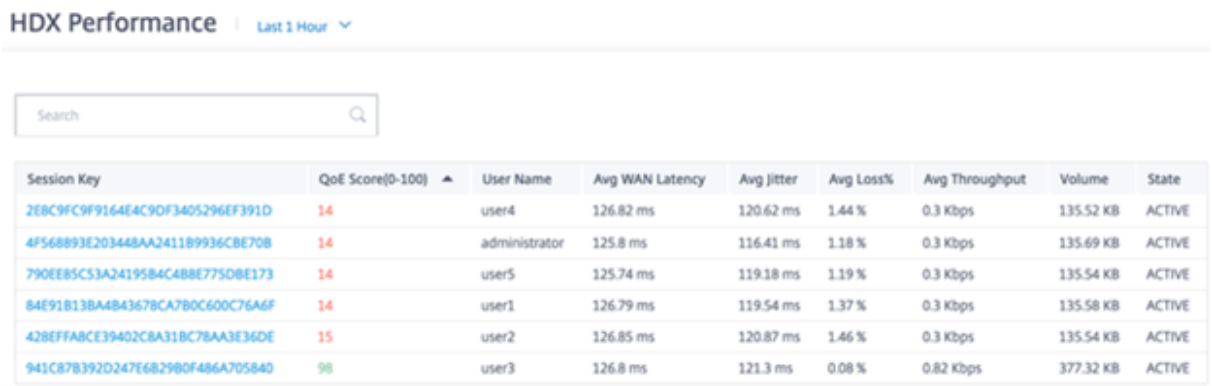
各セッションの上位の詳細を次に示します。

- セッションキー:HDX セッションの一意の ID。

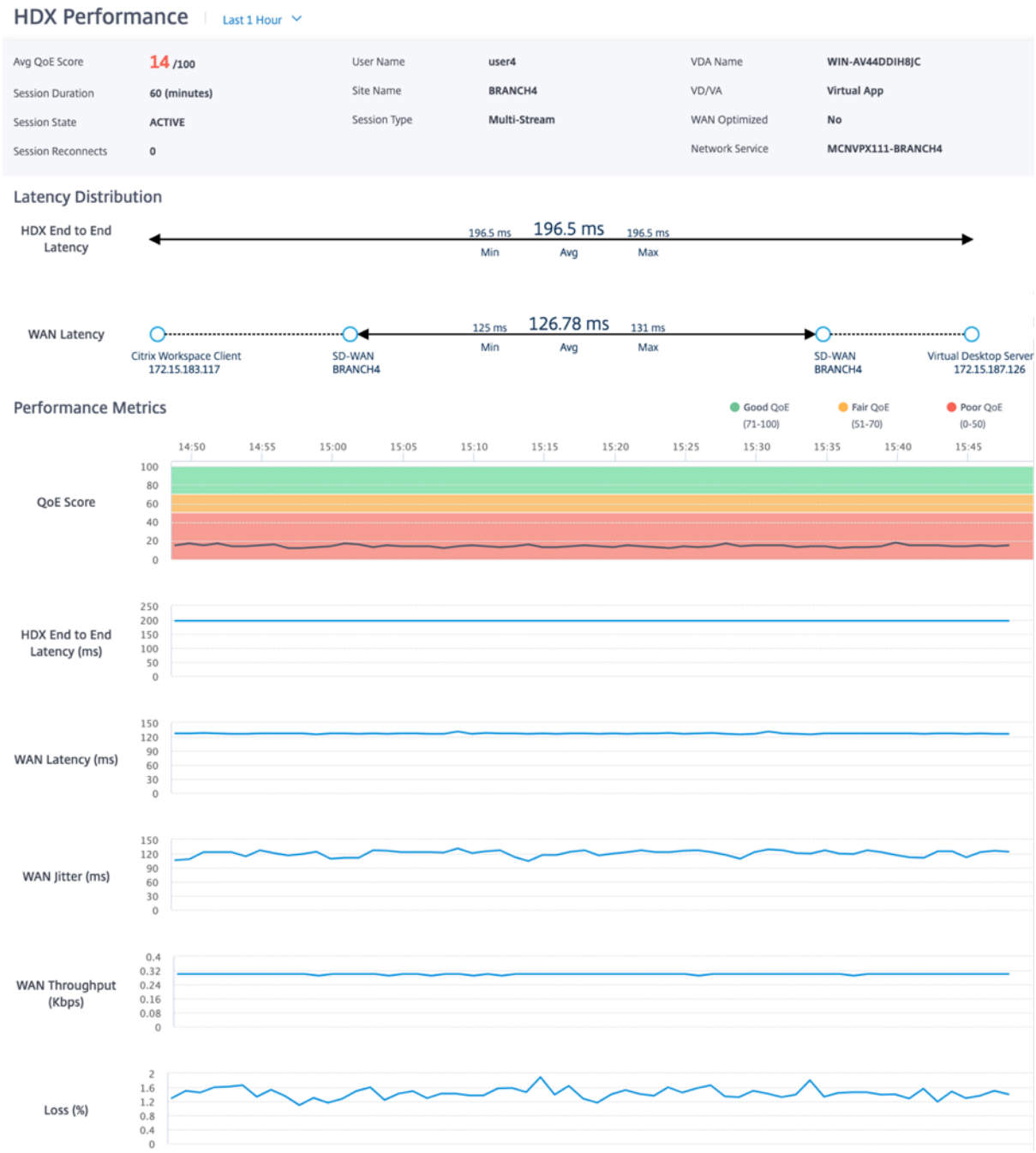
- **QoE** スコア **(0～100)**: このセッションの平均 QoE。
- ユーザー名: ユーザー名。
- 平均 **WAN** 遅延: 選択した期間におけるセッションの平均 WAN 待ち時間で、クライアント側で測定されます。
- 平均ジッター: 選択した期間におけるセッションの平均ジッター値です。
- 平均損失率: 選択した期間におけるセッションの平均損失率値。
- 平均スループット: 選択した期間におけるセッションの平均スループット値。
- ボリューム: このセッションで使用された総トラフィック量。Citrix SD-WAN Orchestrator for オンプレミス GUI は、数値の値に基づいてユニットを調整および変更する場合があります。
- 状態: セッションのステータス。

列タイトルをクリックすると、その列でソートされたレポートが表示されます。「影響を受けたセッションをさらに表示」をクリックすると、すべてのセッションのレポートが表示されます。任意の行をクリックすると、そのセッションの詳細レポートが表示されます。

次のスクリーンショットは、すべてのセッションを示すレポートテーブルの例です。この列は、「上位影響を受けたセッション」の表と同じです。



個々のセッション・キーをクリックすると、QoE に影響を与えるすべての変数に関する詳細とともに、パフォーマンス・メトリックがグラフィカルに表示されます。



- 平均 **QoE** スコア: 選択した期間の平均 QoE スコア。
- ユーザー名: このセッションを起動したユーザー。
- **VDA** 名： 公開デスクトップ/アプリケーションの配信元となる VDA の名前。
- セッション時間**:** 選択した期間におけるこのセッションのアクティブ時間。
- サイト名: セッションが開始されたときのユーザーのクライアントサイト。
- **VD/VA**: ****** このセッションが仮想デスクトップセッションか仮想アプリケーションセッションか ** 。
- セッション状態: 選択した期間終了時のセッションの状態。
- セッションタイプ: セッションが最後に起動されたときのセッションがマルチストリームセッションかシング

ルストリームセッションか。

- **WAN** 最適化: このセッションが WAN 最適化されているかどうか。SD-WAN が PE プラットフォームであり、HDX に対して WAN 最適化が有効になっており、このセッションが最適化されている場合、このフィールドは true と表示されます。
- セッション再接続: ネットワークの問題によりセッションが自動的に切断され、再接続された場合、このフィールドはそのような発生回数です。
- ネットワークサービス: これは、このセッションが配信されるサービス名です。
- **HDX** のエンドツーエンド遅延：VDA とクライアント間の往復時間の半分。
- **WAN** 遅延：VDA 側の SD-WAN からクライアント側の SD-WAN までの遅延。

IP ルール

October 26, 2022

IP ルールは、ネットワークのルールを作成し、そのルールに基づいて特定の Quality of Service (QoS) を決定するのに役立ちます。ネットワーク用のカスタムルールを作成できます。たとえば、次のようなルールを作成できます。送信元 IP アドレスが 172.186.30.74 で、宛先 IP アドレスが 172.186.10.89 の場合、**** トラフィックポリシーを固定パスに、**** トラフィックタイプをリアルタイムに設定します ****。

トラフィックフローのルールを作成し、そのルールをアプリケーションやクラスに関連付けることができます。フローのトラフィックをフィルタリングするための基準を指定し、一般的な動作、LAN から WAN への動作、WAN から LAN への動作、およびパケットインスペクション規則を適用できます。

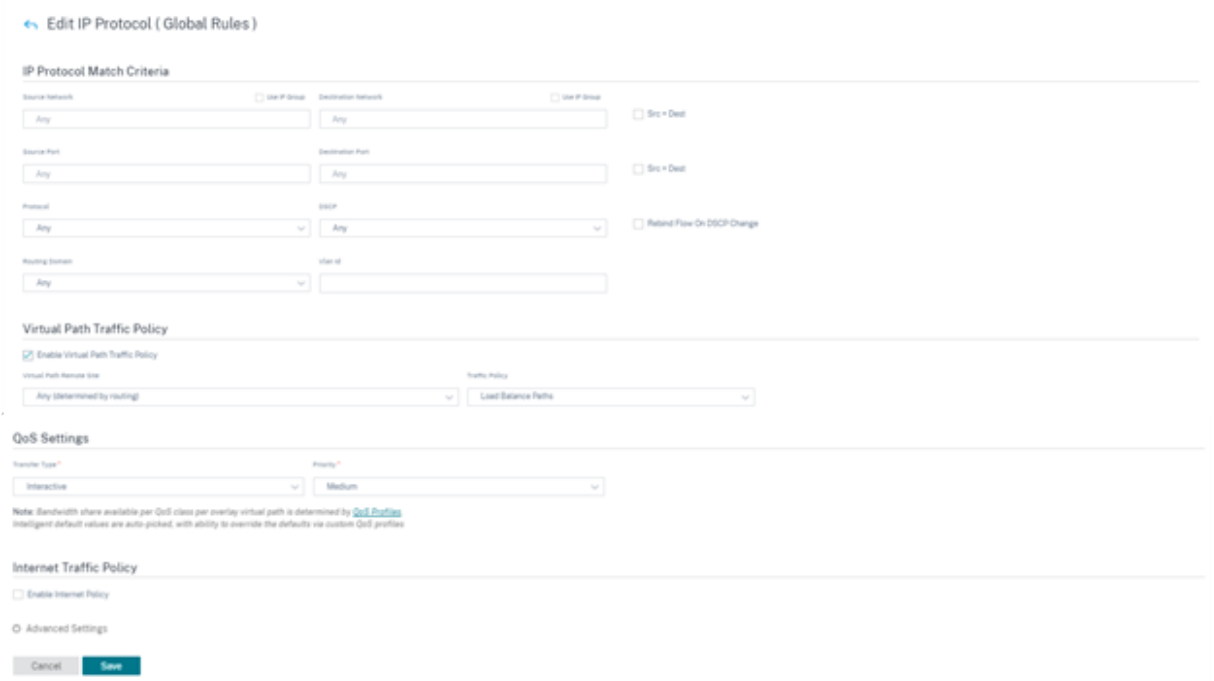
ネットワークレベルでグローバルおよびサイト固有の IP ルールを作成できます。グローバルに作成されたルールにサイトが関連付けられている場合は、サイト固有のルールを作成できます。このような場合、サイト固有のルールが優先され、グローバルに作成されたルールよりも優先されます。

デフォルトの IP プロトコルルール HTTP、HTTPS、および ALTHTTPS は、常にルールテーブルのリストの一番上に表示されます。ただし、サイト固有の IP ルール (作成後) は、ルールテーブルの HTTP、HTTPS、ALTHTTPS、およびグローバル IP ルールの上に表示されます。

IP ルールを作成する

IP ルールを作成するには、[構成**] > [QoS] > [QoS** ポリシー] > [**IP** ルール] に移動します。グローバルレベルで **IP** ルールを作成する場合は [グローバルルール] タブを選択し、サイトレベルでルールを作成する場合は **[**サイト**/**グループ固有のルール] を選択します。

「**IP** ルール」セクションの「新規 **IP** ルール」をクリックします。



- IP プロトコル一致基準
  - サイトの追加/削除:(サイト固有の IP ルールを作成している場合のみ使用可能) サイトを選択し、[確認] をクリックして [完了] をクリックします。
  - ソースネットワーク: ルールが一致するソース IP アドレスとサブネットマスク。
  - 宛先ネットワーク: ルールが一致する宛先 IP アドレスとサブネットマスク。
  - **IP** グループを使用する:「**IP** グループを使用する」チェックボックスを選択して、ドロップダウンリストから既存の IP グループを選択します。
  - **Src = Dst**: 選択すると、送信元 IP アドレスが宛先 IP アドレスとしても使用されます。
  - 送信元ポート: ルールが一致する送信元ポート (または送信元ポート範囲)。
  - 宛先ポート: ルールが一致する宛先ポート (または宛先ポート範囲)。
  - **Src = Dst**: 選択すると、送信元ポートが宛先ポートとしても使用されます。
  - プロトコル: ルールが一致するプロトコル。定義済みのプロトコルのいずれかを選択するか、[任意] または [番号] を選択できます。
  - プロトコル番号: このフィールドは、「プロトコル」ドロップダウンリストから「番号」を選択した場合にのみ表示されます。プロトコル番号を選択すると、プロトコルに関連付けられた整数がバックエンド構成に使用されます。
  - **DSCP**: ルールが一致する IP ヘッダー内の DSCP タグ。
  - ルーティングドメイン: ルールが一致するルーティングドメイン。
  - **VLAN ID**: ルールの VLAN ID を入力します。VLAN ID は、仮想インターフェイスを送受信するトラフィックを識別します。VLAN ID を 0 として使用して、ネイティブトラフィックまたはタグなしトラフィックを指定します。
  - **DSCP** 変更時にフローを再バインド: 選択すると、一致基準が一致しないフローは、DSCP フィールド

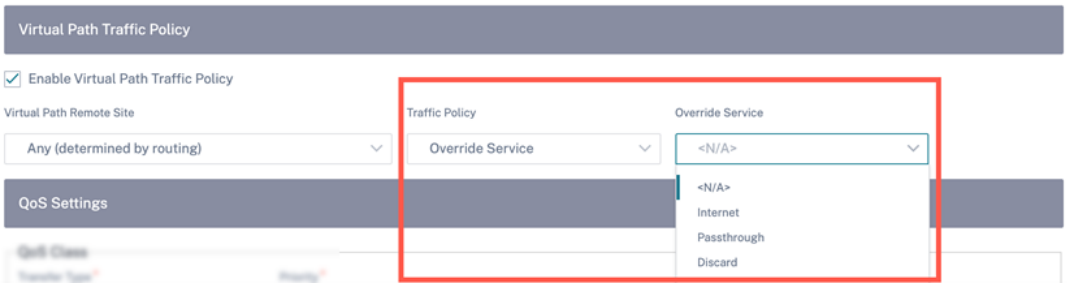
が異なる場合は別のフローとして扱われます。

- 仮想パストラフィックポリシー

「仮想パストラフィックポリシーを有効にする」チェックボックスを選択します。

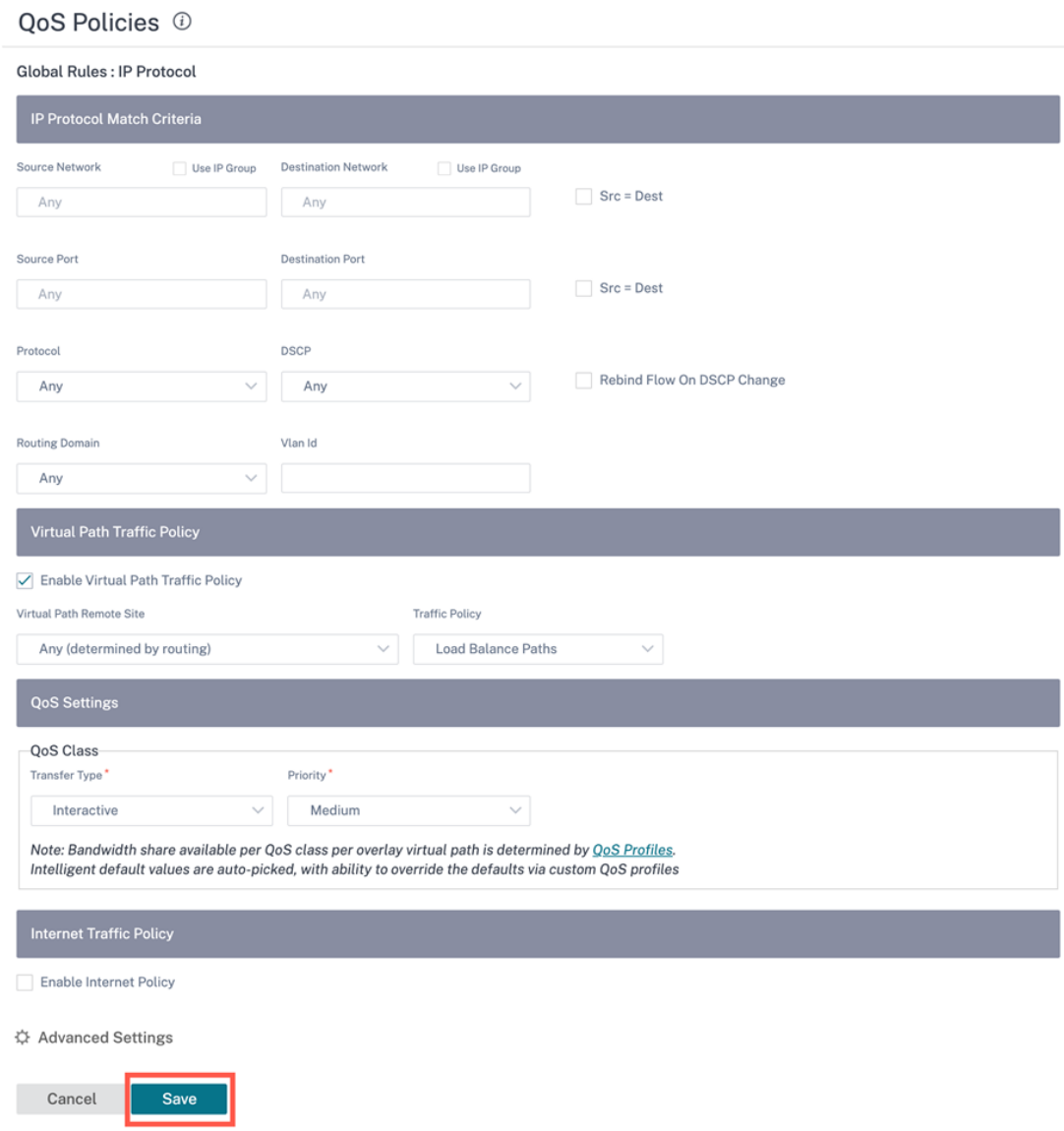
- 仮想パスリモートサイト: リモートサイトの仮想パスを選択します。
- トラフィックポリシー: 必要に応じて、次のトラフィックポリシーのいずれかを選択します。
  - 負荷分散パス: フローのアプリケーショントラフィックは複数のパスに分散されます。トラフィックは、そのパスが使用されるまで、最適パスを介して送信されます。残りのパケットは、次の最適パスを介して送信されます。
  - 永続パス: アプリケーショントラフィックは、パスが使用できなくなるまで同じパス上に残ります。次のパーシスタンスポリシーのいずれかを選択します。
    - 発信元リンクで維持: アプリケーショントラフィックは、パスが使用できなくなるまで発信元リンクにとどまります。
    - 使用可能な場合は **MPLS** リンク上に存続し、それ以外の場合は発信元リンクに存続します。アプリケーショントラフィックは MPLS リンク上に残ります。MPLS リンクが使用できない場合、トラフィックは発信元のリンクに残ります。
    - 利用可能な場合はインターネットリンクを維持し、それ以外の場合は元のリンクで維持する: アプリケーショントラフィックはインターネットリンク上に残ります。インターネットリンクが利用できない場合、トラフィックは元のリンクに残ります。
    - 使用可能な場合はプライベートイントラネットリンクに保持し、それ以外の場合は元のリンクに保持する: アプリケーショントラフィックはプライベートイントラネットリンクに残ります。プライベートイントラネットリンクが使用できない場合、トラフィックは元のリンクに残ります。

    パーシステンスインピーダンスは、アプリケーショントラフィックがリンク上に留まるまでの時間（ミリ秒単位）です。
  - 重複パス: アプリケーショントラフィックは複数のパスにわたって重複するため、信頼性が向上します。
  - **Override Service**: フローのトラフィックは、別のサービスに上書きされます。仮想パスサービスがオーバーライドするサービスタイプを [イントラネット]、[インターネット]、[パススルー]、または [破棄] から選択します。

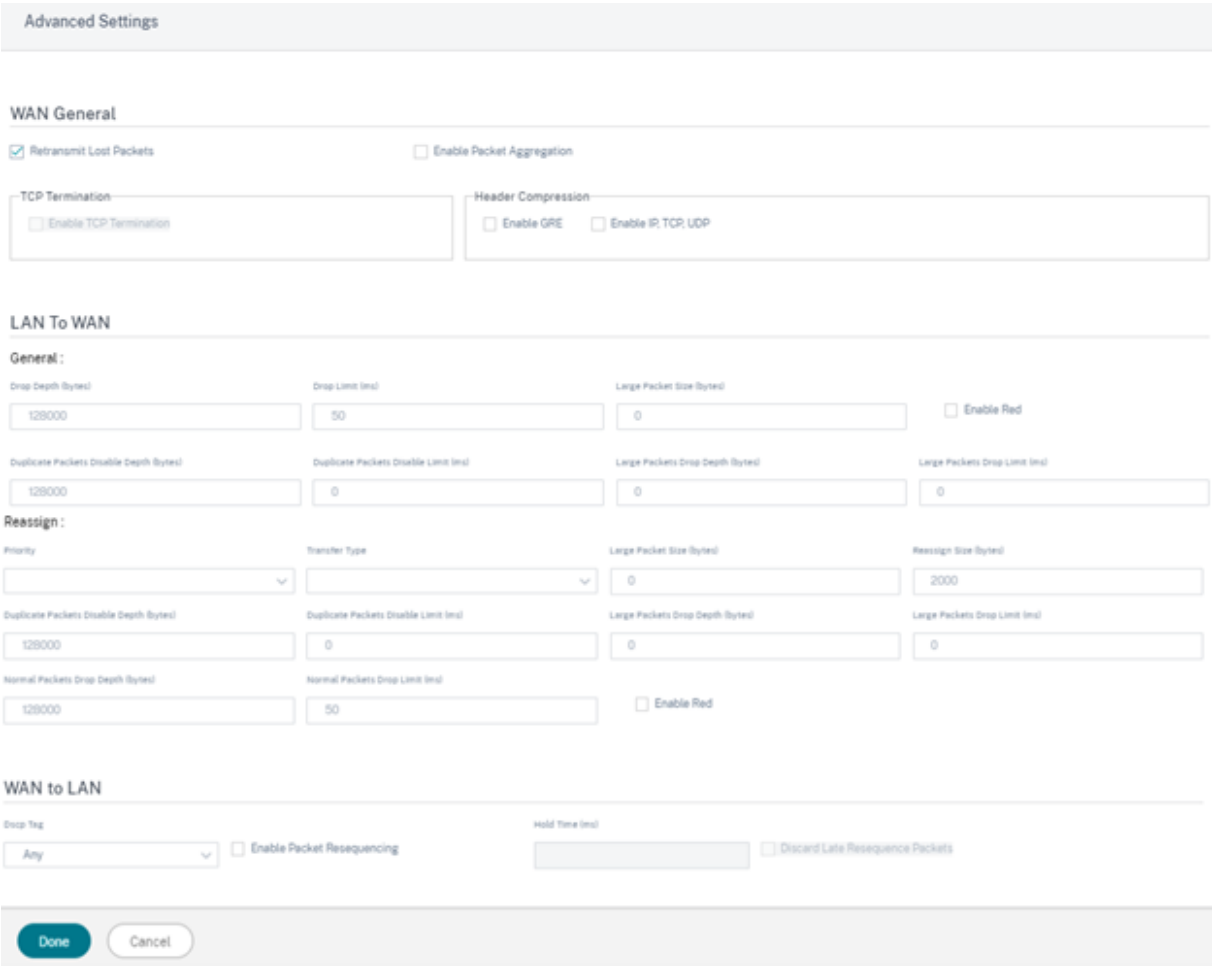


- QoS 設定 (QoS クラス)
  - 転送タイプ: 次の転送タイプのいずれかを選択します。
    - リアルタイム: 低遅延、低帯域幅、時間に敏感なトラフィックに使用されます。リアルタイムアプリケーションは時間に敏感ですが、実際には高い帯域幅（Voice over IP など）は必要ありません。リアルタイムアプリケーションはレイテンシーとジッターに敏感ですが、ある程度の損失は許容できます。
    - **Interactive**: 低〜中レイテンシーおよび低〜中帯域幅要件の対話型トラフィックに使用されます。通常、対話はクライアントとサーバーの間で行われます。通信は、高帯域幅を必要としない場合がありますが、損失や遅延に敏感です。
    - バルク: 高帯域幅トラフィックおよび高遅延に耐えるアプリケーションに使用されます。ファイル転送を処理し、高帯域幅を必要とするアプリケーションは、バルククラスとして分類されます。これらのアプリケーションは、人間の干渉をほとんど伴わず、ほとんどシステム自体によって処理されます。
  - 優先度: 選択した転送タイプの優先度を選択します。
- インターネットトラフィックポリシー
  - インターネットトラフィックポリシーを設定するには、「インターネットポリシーを有効にする」チェックボックスを選択します。
  - モード: ルールに一致するフローのパケットを送受信する方法。必要に応じて [オーバーライドサービス] または [**WAN** リンク] を選択できます。
  - **WAN** リンク: インターネット負荷分散が有効な場合に、ルールに一致するフローが使用する WAN リンク。
  - **Override Service**: ルールに一致するフローの宛先サービス。

> 注**:**
>
> 仮想パスサービスは別の仮想パスサービスをオーバーライドできません。



詳細設定



- WAN ジェネラル
  - 失われたパケットの再送信: このルールに一致するトラフィックを信頼できるサービスを介してリモートアプライアンスに送信し、失われたパケットを再送信します。
  - パケットアグリゲーションを有効にする: 小さなパケットを大きなパケットに集約します。
  - **TCP** ターミネーションを有効にする: このフローのトラフィックの TCP ターミネーションを有効にします。パケットの確認応答のラウンドトリップ時間が短縮されるため、スループットが向上します。
  - **GRE** を有効にする:GRE パケットのヘッダーを圧縮します。
  - **IP**、**TCP**、および **UDP** を有効にする:IP、TCP、および UDP パケットのヘッダーを圧縮します。

    > 注:
    >
    > IPv6 パケットはヘッダー圧縮をサポートしていません。

- LAN から WAN

  一般

  - ドロップ深度 **(**バイト**)**: パケットがドロップされるまでのキュー深度のしきい値。

- ドロップ制限: クラススケジューラで待機しているパケットがドロップされるまでの時間。バルククラスには適用されません。
- ラージパケットサイズ: このサイズ以下のパケットには、ラージパケットドロップ深度 **(**バイト**)** およびラージパケットドロップ制限 (ms) フィールドで指定された [ドロップ制限] と [ドロップ深度 **] の値が割り当てられます。このサイズより大きいパケットには、デフォルトの Drop Limit フィールドと Drop Depth フィールドで指定された値が割り当てられます。
- **ENABLE RED**：ランダム早期検出（RED）は、輻輳が発生したときにパケットを廃棄することにより、クラスリソースの公平な共有を保証します。
- 重複パケット無効化レベル **(**バイト**)**: クラススケジューラのキュー深度。この時点で重複パケットは生成されません。
- 重複パケット無効制限: 重複パケットが帯域幅を消費するのを防ぐために、重複パケットを無効にできる時間。
- ラージパケットドロップ深度（バイト）: キューの深さがこのしきい値を超えると、パケットは破棄され、統計情報がカウントされます。
- ラージパケットドロップリミット **(ms)**: ラージパケットサイズ以上のパケットがクラススケジューラで待機する必要がある推定最大時間。推定時間がこのしきい値を超えると、パケットは破棄され、統計情報がカウントされます。バルククラスには無効です。

再割り当て

- 優先度: 必要に応じてスタンバイ WAN リンクの優先順位を設定できます。スタンバイ WAN リンクプライオリティは、スタンバイ WAN リンクがアクティブになる順序を示します。優先順位の高いスタンバイ WAN リンクが最初にアクティブになります。優先順位の低い WAN リンクが最後にアクティブになります。
- 転送タイプ: このルールを関連付ける転送タイプを選択します。
- 重複パケット無効化レベル **(**バイト**)**: クラススケジューラのキュー深度。この時点で重複パケットは生成されません。
- 重複パケット無効制限: 重複が実行されないまでパケットがキュー内で待機する時間を指定します。これにより、帯域幅が制限されている場合に、重複パケットが帯域幅を消費するのを防ぎます。
- ラージパケットドロップ深度（バイト）: キューの深さがこのしきい値を超えると、パケットは破棄され、統計情報がカウントされます。
- ラージパケットドロップリミット **(ms)**: 推定時間がこのしきい値を超えると、パケットは破棄され、統計情報がカウントされます。バルククラスには無効です。
- 通常のパケットドロップ深度（バイト）: キューの深さがこのしきい値を超えると、パケットは破棄され、統計情報がカウントされます。
- 通常のパケットドロップ制限 **(ms)**: 推定時間がこのしきい値を超えると、パケットは破棄され、統計情報がカウントされます。バルククラスには無効です。

- WAN から LAN へ
  - **DSCP** タグ: このルールに一致するパケットを LAN に送信する前に WAN/LAN 上で適用される DSCP タグ。

- パケットの再順序付けを有効にする: ルールに一致するトラフィックフローにシーケンス順序のタグが付けられ、パケットは WAN-to-LAN アプライアンスで（必要に応じて）並べ替えられます。
- **Hold Time**: パケットが再シーケンシングのために保持される時間間隔。この時間が経過すると、パケットは LAN に送信されます。タイマーが切れると、パケットは前提条件のシーケンス番号を待たずに LAN に送信されます。

  ルールに重複パスとしてのトラフィックポリシーがある場合、デフォルトのホールドタイムは 80 ミリ秒です。それ以外の場合、デフォルトは TCP ルールでは 900 ミリ秒、TCP 以外のルールでは 250 ミリ秒です。
- 遅延再シーケンスパケットの破棄: 再シーケンス処理に必要なパケットが LAN に送信された後に到着した順序どおりでないパケットを廃棄します。

[保存] をクリックして構成設定を保存します。[設定**] > [**QoS** ポリシー] ページで [設定の検証 **] をクリックして、監査エラーを確認します。

IP ルールを検証

IP ルールを確認するには、[レポート**] > [**リアルタイム**] > [**フロー] に移動します。フロー情報と表示するフローの数を表示するサイトを選択します。「列をカスタマイズ」をクリックし、表示したいフロー情報に対応するチェックボックスを選択します。フロー情報が設定された規則に従っているかどうかを確認します。

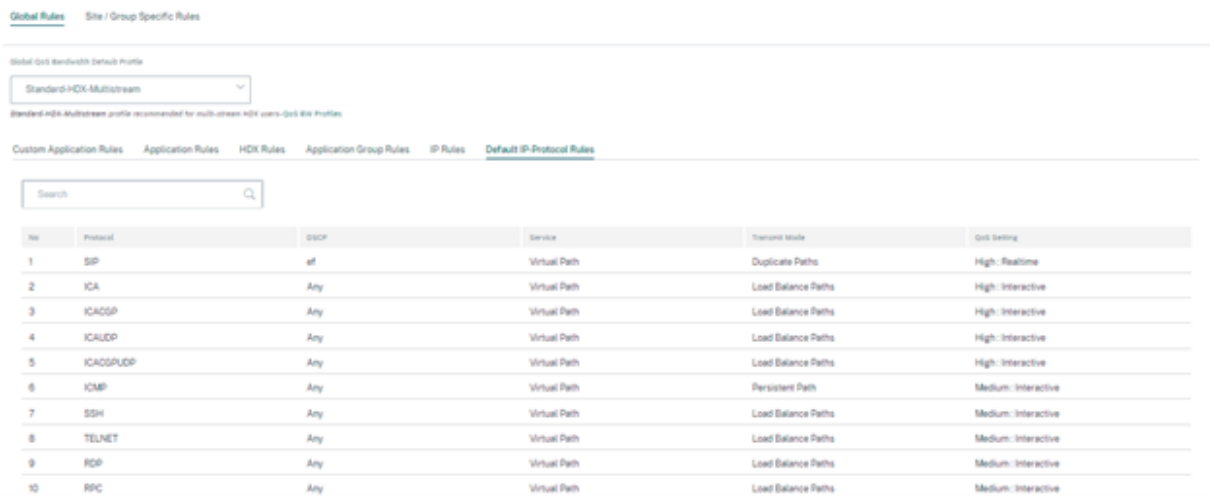
[レポート**] > [**リアルタイム**] > [**統計] に移動し、[ルール] を選択します。サイトを選択し、[最新データを取得] をクリックします。設定したルールを確認します。詳しくは、「サイトレポート」を参照してください。

QoS ポリシー

October 26, 2022

管理者は、アプリケーションポリシーとトラフィックポリシーを定義できます。これらのポリシーは、アプリケーションのトラフィックステアリング、サービス品質（QoS）、およびフィルタリング機能を有効にするのに役立ちます。定義されたルールを、ネットワーク内のすべてのサイトにグローバルに適用できるか、特定のサイトに適用できるかを指定します。

ポリシーは、複数のルールの形式で定義され、ユーザー定義の順序で適用されます。



新しいルールの作成

管理者は、優先度に基づいて定義済みのルールを設定する必要があります。優先順位は、リストの上部、リストの一番下、特定の行などのパラメータに基づいて分類されます。

アプリケーションまたはサブアプリケーションにはより具体的なルールを設定し、トラフィック量の多いルールにはあまり具体的でないルールを設定することをお勧めします。

たとえば、Facebook メッセンジャー (サブアプリケーション) と Facebook (アプリケーション) の両方に特定のルールを作成できます。Facebook メッセンジャールールが選択されるように、Facebook のルールの上に Facebook メッセンジャーのルールを置きます。順序が逆の場合、Facebook メッセンジャーは Facebook アプリケーションのサブアプリケーションであるため、Facebook メッセンジャーのルールは選択されません。注文を正しいものにすることが重要です。

一致基準

次のように、定義されたルールのトラフィックを選択します。

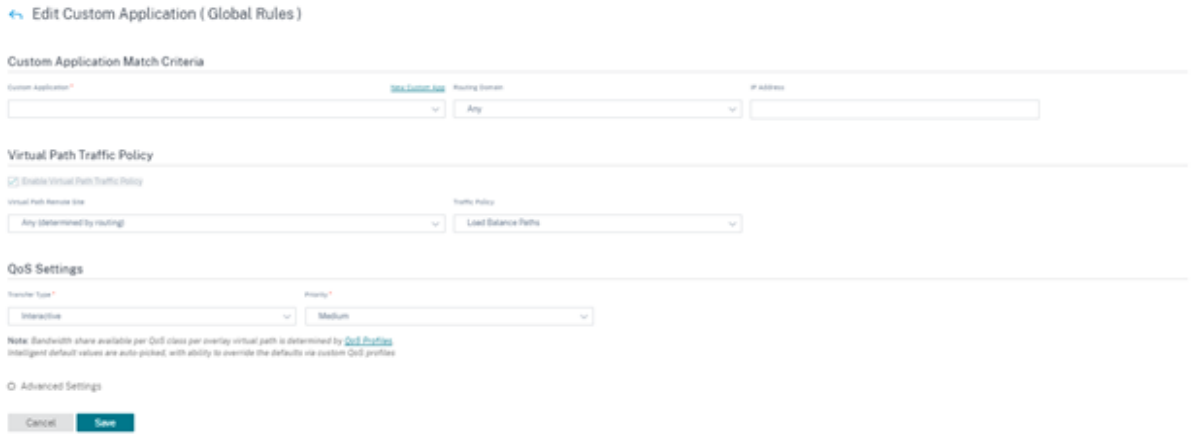
- アプリケーション
- カスタム定義アプリケーション
- アプリケーションのグループまたは IP プロトコルベースのルール

ルールのスコープ

定義されたルールを、ネットワーク内のすべてのサイトにグローバルに適用できるか、特定のサイトに適用できるかを指定します。

アプリケーションステアリング

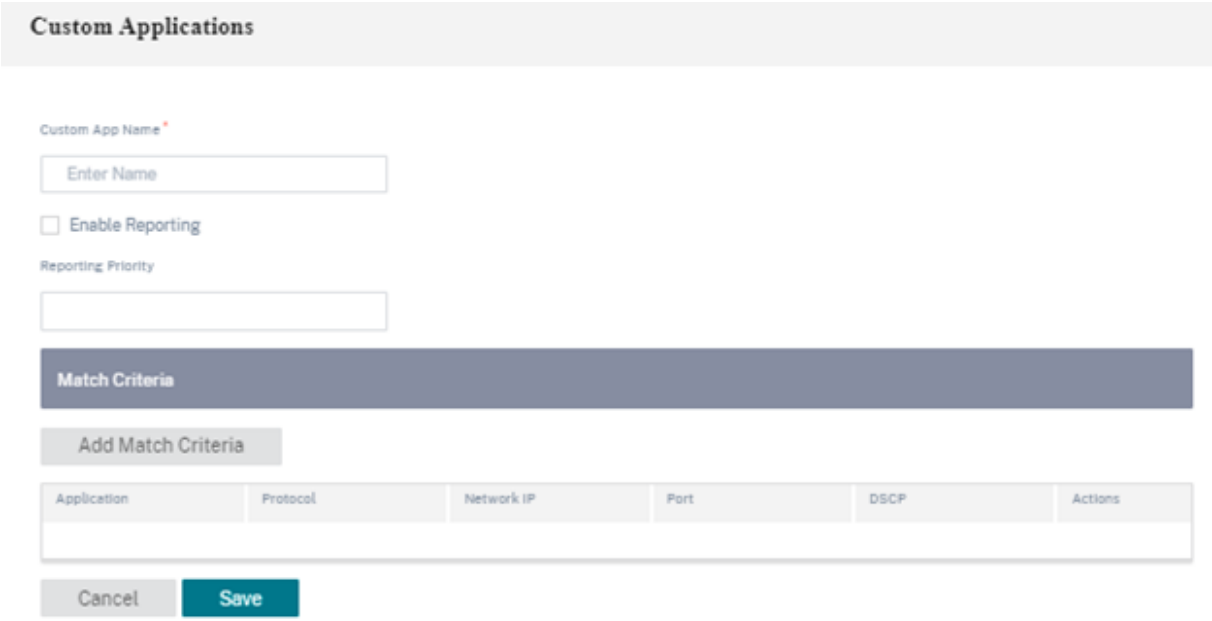
[設定] > [**QoS**] > [カスタムアプリケーションルール] に移動します。トラフィックの操縦方法を指定します。



新しいカスタムアプリ: リストから一致条件を選択します。管理者は次の場所に名前を付けることで、新しいカスタムアプリケーションを追加できます。

- カスタムアプリケーション
- プロトコル (TCP、UDP、ICMP)
- ネットワーク IP /プレフィックス
- ポート
- DSCP タグ

ドメイン名ベースのカスタムアプリケーションを作成することもできます。

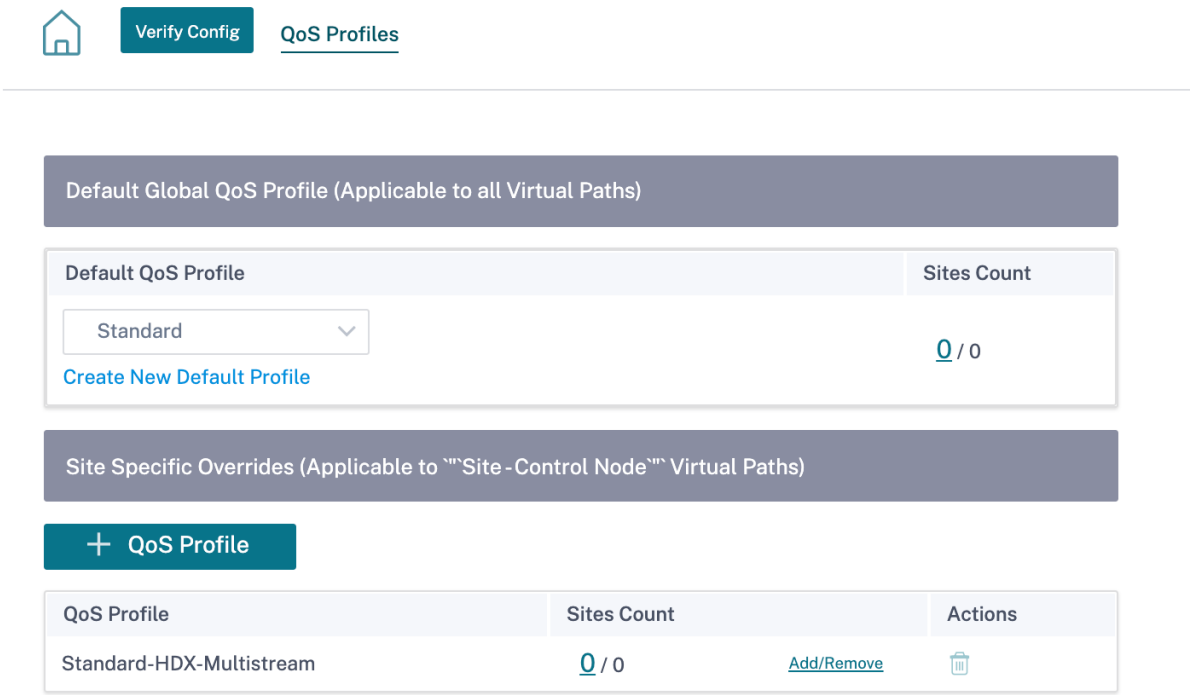


[設定] **> [**QoS** ポリシー] ページで [設定の検証 **] をクリックして、監査エラーを確認します。

IP ルール　**IP** ルールは、ネットワークのルールを作成し、そのルールに基づいて特定の Quality of Service (QoS) を決定するのに役立ちます。IP ルールの詳細については、「IP ルール」を参照してください。

QoS プロファイル

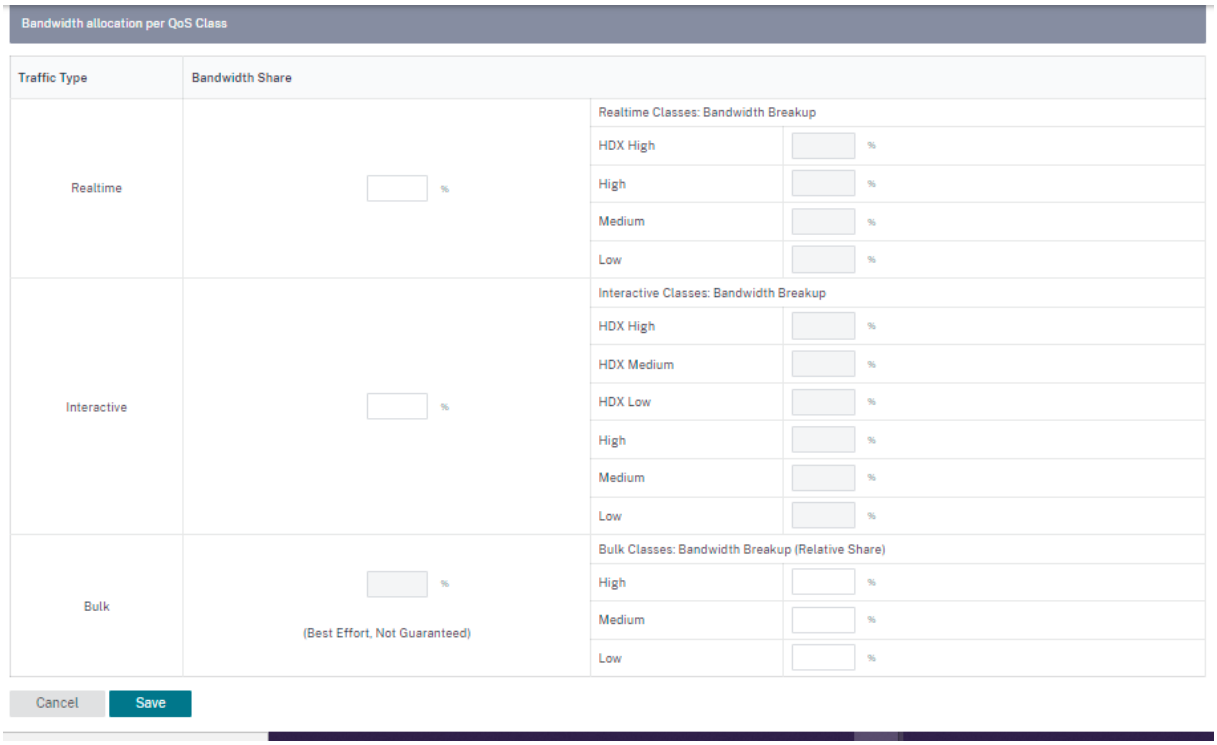
サービス品質 (QoS) セクションでは、**+ QoS** プロファイルオプションを使用して **QoS** プロファイルを作成できます。QoS プロファイルは、特定のトラフィックに対するサービスを改善します。QoS の目的は、トラフィックタイプ（リアルタイム、インタラクティブ、バルククラス）および専用帯域幅を含むプライオリティを提供することです。帯域幅の分割は、% の値で使用できます。これにより、損失特性も改善されました。



[設定**] > [**QoS** ポリシー] ページで [設定の検証 **] をクリックして、監査エラーを確認します。

QoS プロファイルのカスタマイズ

仮想パスのデフォルトセットが使用されている場合、[構成] > [QoS] > [**QoS** プロファイル] でクラスを変更できます。「新規デフォルトプロファイルの作成」をクリックし、デフォルトセットの名前を入力してサイトを選択し、QoS クラスの帯域幅割り当てを更新します。［保存］をクリックします。クラスの詳細については、「クラス」を参照してください。

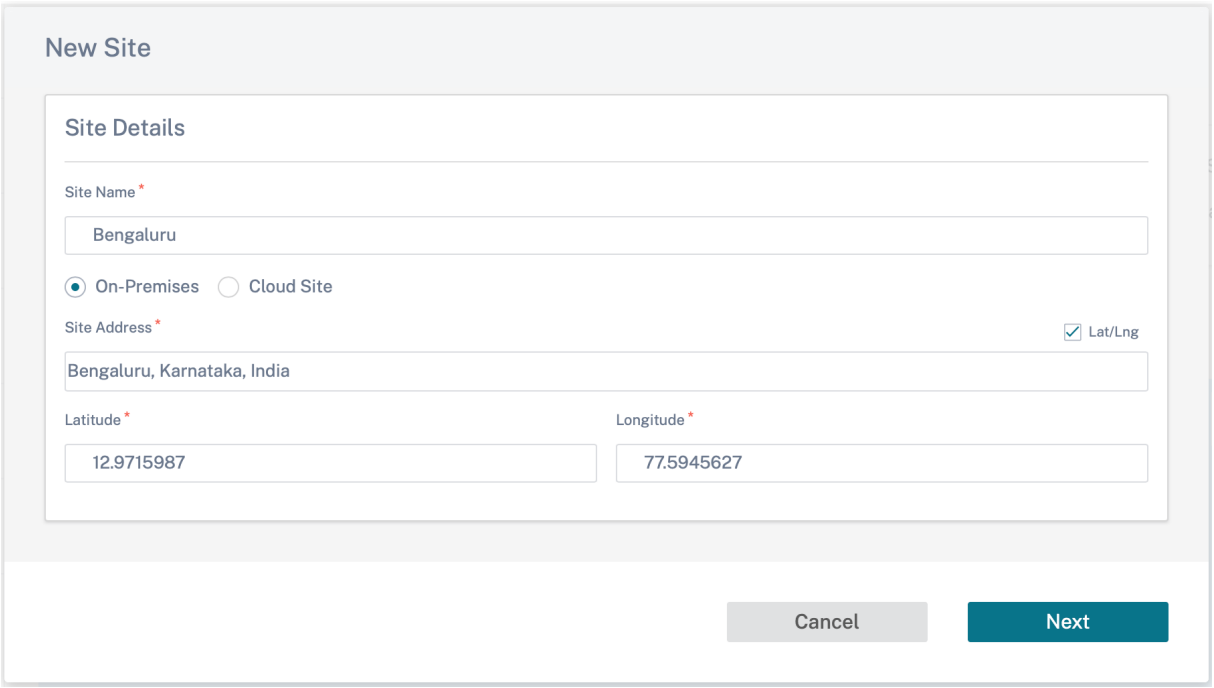


サイト構成

October 26, 2022

ネットワークホームページまたは [プロファイルとテンプレート] セクションから新しいサイトを追加して、SD-WAN ネットワークを設定できます。

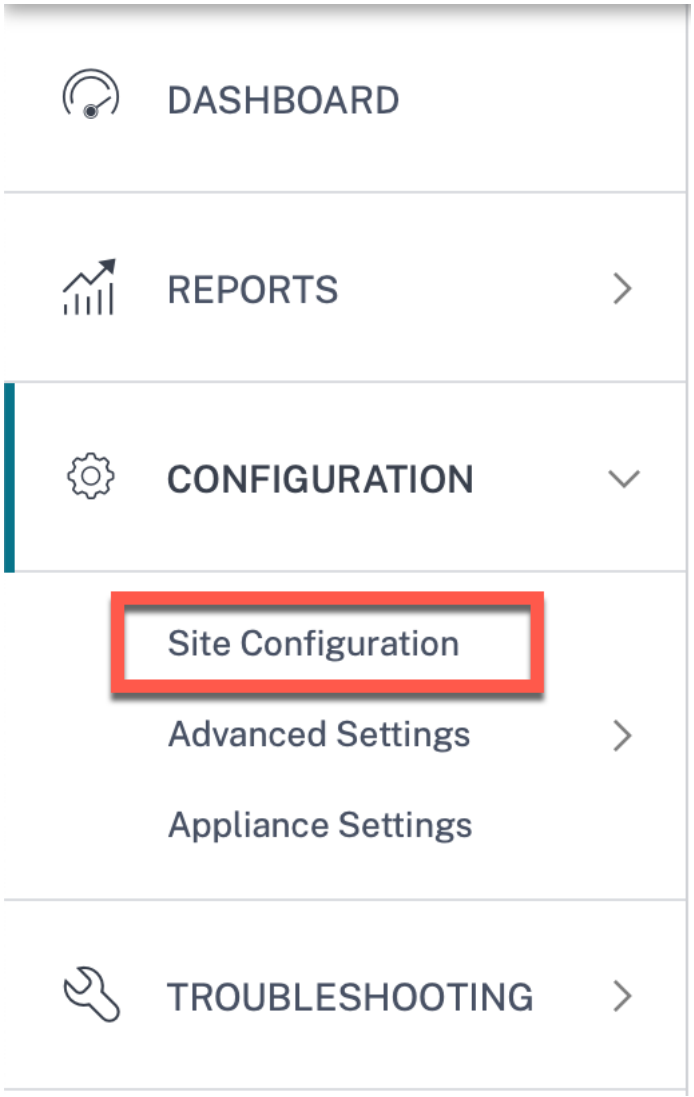
サイトを作成するには、ネットワークダッシュボードの [**+** 新規サイト] をクリックします。サイトの名前と場所を指定します。



サイトを最初から作成することも、サイトプロファイルを使用してサイトをすばやく構成することもできます 。

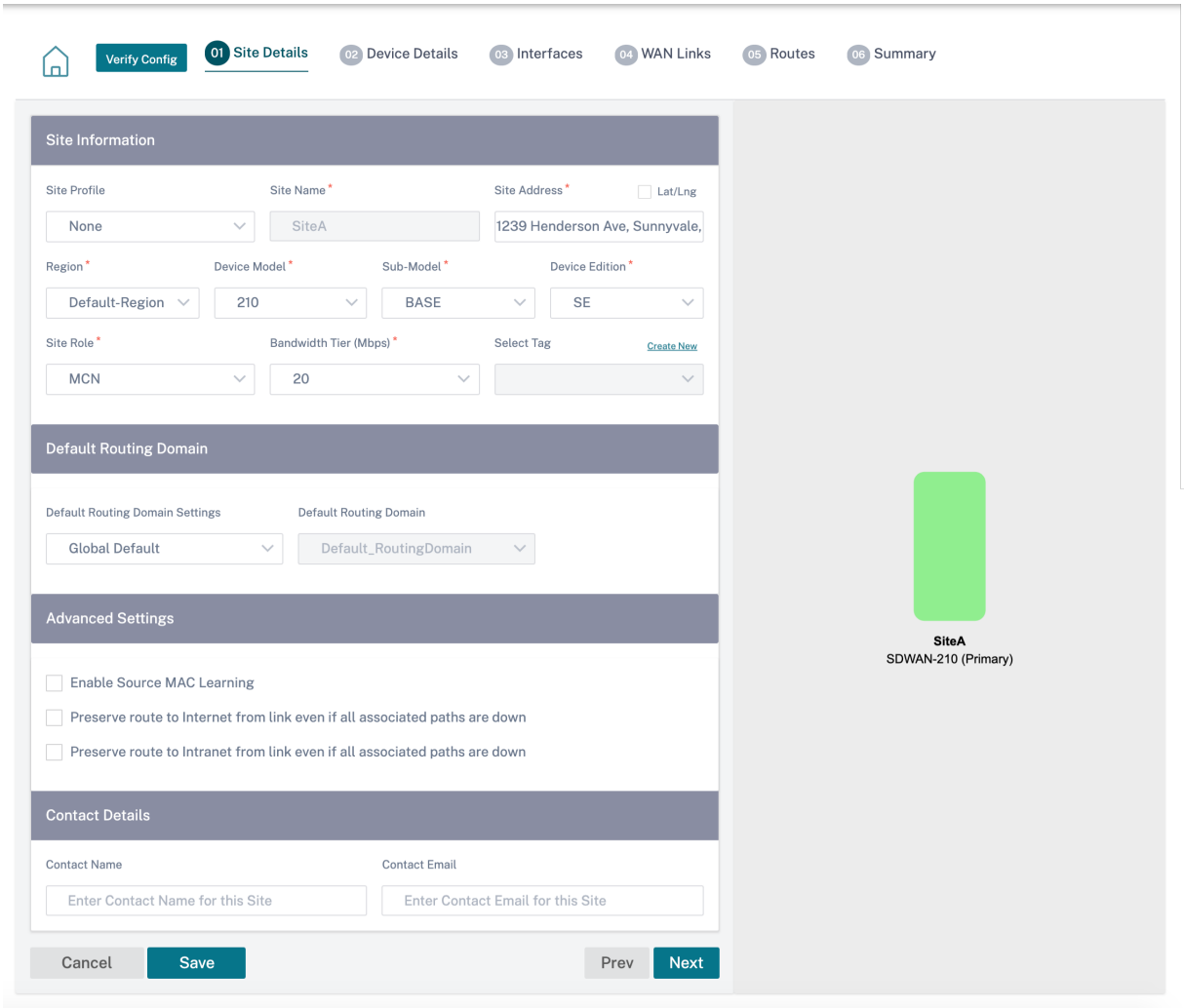
構成を進めると、画面の右側にグラフィカルな表示が表示され、動的なトポロジ図が表示されます。

サイト構成を表示するには、サイトを選択し、構成 **>** サイト構成に移動します。

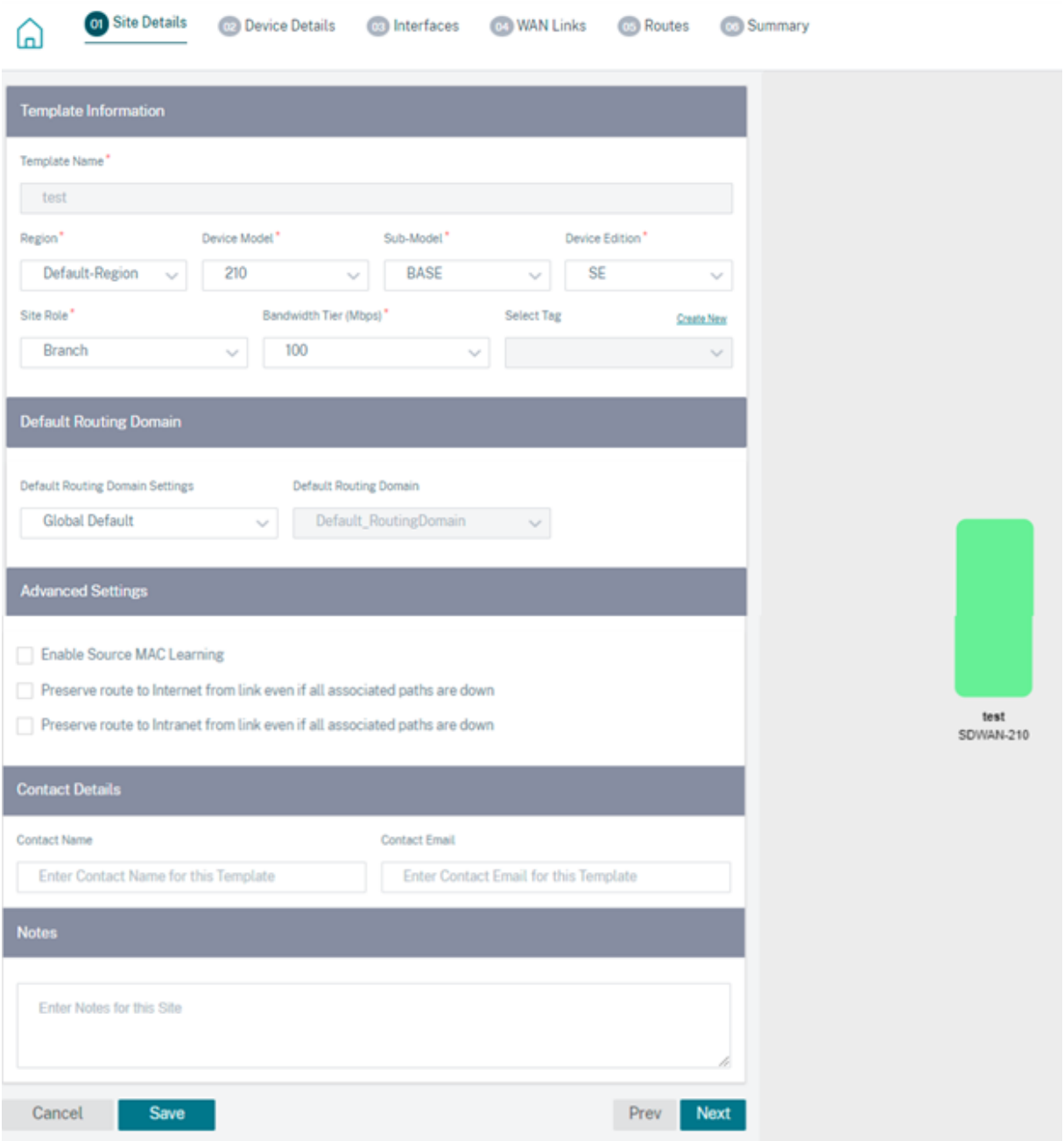


サイトの詳細

最初のステップでは、サイト、デバイス、詳細設定、およびサイトの連絡先の詳細を入力します。



サイトテンプレートを使用してサイトを構成すると、次の画面が表示されます。



サイト/テンプレート情報

- サイトプロファイルを選択すると、サイトプロファイル構成に基づいてサイト、インターフェイス、および WAN リンクのパラメータが自動的に入力されます。
- ** サイトアドレスとサイト名は ** 、前のステップで入力した詳細に基づいて自動入力されます。
- 緯度/経度チェックボックスを有効にすると、サイトの緯度と経度が表示されます。
- ドロップダウンリストから地域を選択します。

- ****** デバイスモデルとサブモデルは ****** 、特定のサイトで使用されているハードウェアモデルまたは仮想アプライアンスに基づいて選択できます。
- デバイスエディションは、選択したデバイスモデルに基づいて自動的に反映されます。現在、Premium Edition (PE)、Advanced Edition (AE)、および Standard Edition (SE) がサポートされています。PE モデルは、1100、2100、5100、および 6100 プラットフォームでのみサポートされています。AE モデルは 210 および 1100 プラットフォームでサポートされています。

  > 注
  >
  > Citrix SD-WAN Orchestrator サービスは、Advanced Edition と Premium Edition のプラットフォームをサポートしていません。

- サイトロールはデバイスのロールを定義します。サイトには、次のいずれかのロールを割り当てることができます。
  - **MCN**: マスターコントロールノード (MCN) はネットワークのコントローラーとして機能し、ネットワーク内の 1 つのアクティブデバイスのみを MCN として指定できます。
  - ブランチ:MCN から設定を受け取り、ブランチオフィスへの仮想 WAN 機能の確立に参加するブランチサイトのアプライアンス。複数のブランチサイトが存在することができます。
  - **RCN**: 地域制御ノード (RCN) は階層型ネットワークアーキテクチャをサポートし、マルチリージョンネットワークの展開を可能にします。MCN は複数の RCN を制御し、各 RCN は複数のブランチサイトを制御します。
  - 地理的冗長 **MCN**: 別の場所にあるサイトで、MCN が利用できない場合は管理機能を引き継ぎ、障害回復を確実にします。地理的に冗長化された MCN は、MCN に高可用性機能やフェイルオーバー機能を提供しません。
  - 地理的冗長 **RCN**: 別の場所にあるサイトで、利用できない場合は RCN の管理機能を引き継ぎ、災害復旧を確実にします。地理的に冗長化された RCN は、RCN に高可用性機能やフェイルオーバー機能を提供しません。
- 帯域幅階層は、デバイスモデルに応じて、どのデバイスでも設定できる課金対象の帯域幅容量です。たとえば、SD-WAN 410 Standard Edition（SE）アプライアンスは、20、50、100、150、および 200 Mbps の帯域幅層をサポートします。特定のサイトの帯域幅ニーズに応じて、必要な層を選択できます。各サイトは、構成された帯域幅層に対して課金されます。

ルーティングドメイン

「ルーティングドメイン」セクションでは、サイトのデフォルトルーティングドメインを選択できます。ルーティングドメイン設定は、グローバルにすることも、サイト固有にすることもできます。**Global Defaults** を選択すると、グローバルに適用可能なデフォルトのルーティングドメインが自動的に選択されます。サイト固有を選択すると、「ルーティングドメイン」ドロップダウンリストからデフォルトのルーティングドメインを選択できます。

LAN セグメンテーションのルーティングサポート

SD-WAN Standard および Enterprise Edition（SE/PE）アプライアンスは、いずれかのアプライアンスが導入されている個別のサイトにわたって LAN セグメンテーションを実装します。アプライアンスは、使用可能な LAN 側の VLAN の記録を認識して保持し、別の SD-WAN SE/PE アプライアンスを使用して離れた場所で他の LAN セグメント（VLAN）が接続できるものに関するルールを設定します。

上記の機能は、SD-WAN SE/PE アプライアンスで管理される仮想ルーティングおよび転送（VRF）テーブルを使用して実装されます。このテーブルは、ローカル LAN セグメントにアクセスできるリモート IP アドレス範囲を追跡します。この VLAN 間トラフィックは、2 つのアプライアンス間で確立された同じ仮想パスを経由して WAN を通過します（新しいパスを作成する必要はありません）。

この機能の使用例としては、WAN 管理者が VLAN を介してローカルブランチネットワーク環境をセグメント化し、それらのセグメント (VLAN) の一部を、インターネットにアクセスできる DC 側の LAN セグメントへのアクセスを許可し、他のセグメント (VLAN) はそのようなアクセスを取得できない場合があります。VLAN と VLAN の関連付けの構成は、Citrix SD-WAN Orchestrator サービスの Web インターフェイスを介して行われます。

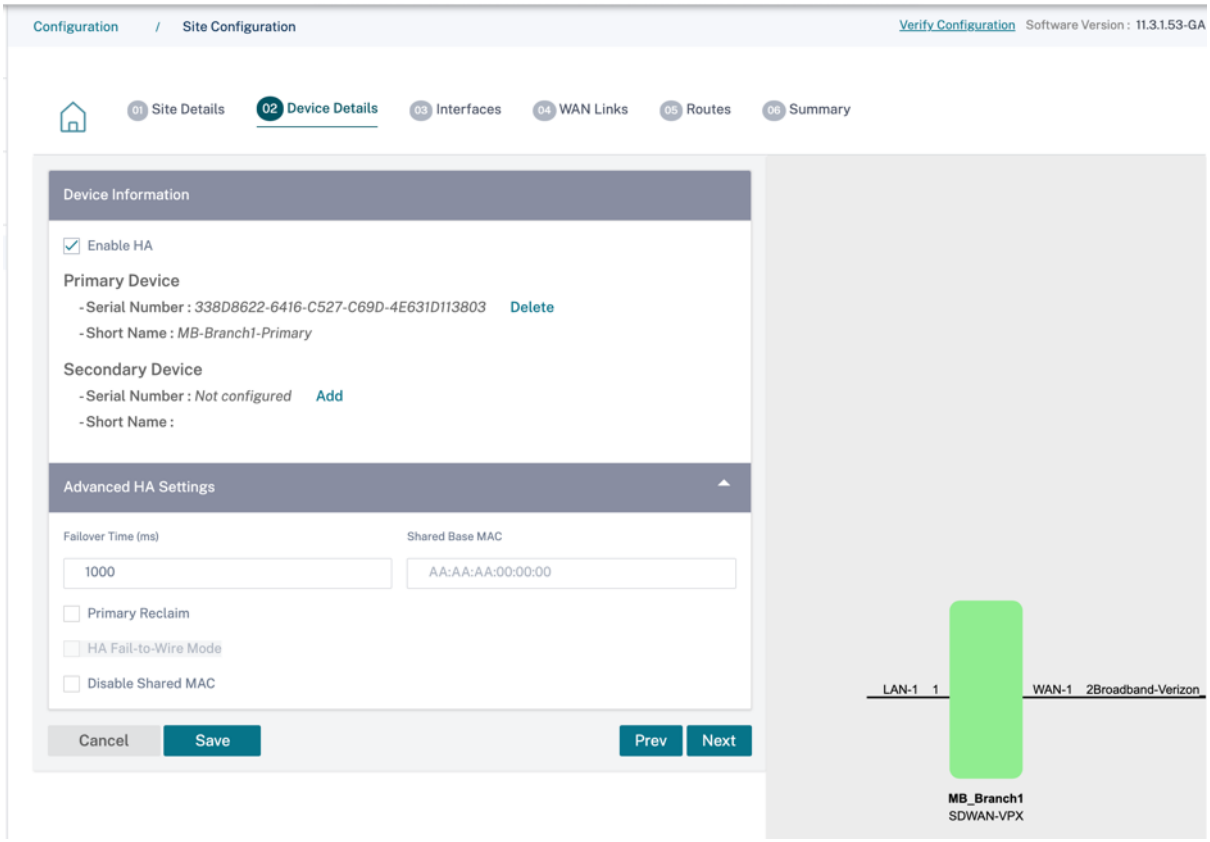
詳細設定

- 送信元 **MAC** 学習を有効にする: 同じ宛先への送信パケットを同じポートに送信できるように、受信したパケットの送信元 MAC アドレスを保存します。
- 関連するすべてのパスがダウンしても、リンクからインターネットへのルートを保存: 有効にすると、インターネットサービスのすべての WAN リンクが使用できなくても、インターネットサービスを宛先とするパケットは引き続きインターネットサービスを選択します。
- 関連するすべてのパスがダウンしても、リンクからイントラネットへのルートを保存: 有効にすると、イントラネットサービスのすべての WAN リンクが使用できなくても、イントラネットサービスを宛先とするパケットは引き続きイントラネットサービスを選択します。
- サイトで利用可能な管理者の連絡先詳細。

構成パネルの右側にある動的ネットワークダイアグラムは、構成プロセスを実行しながら、継続的に視覚的なフィードバックを提供します。

デバイス詳細

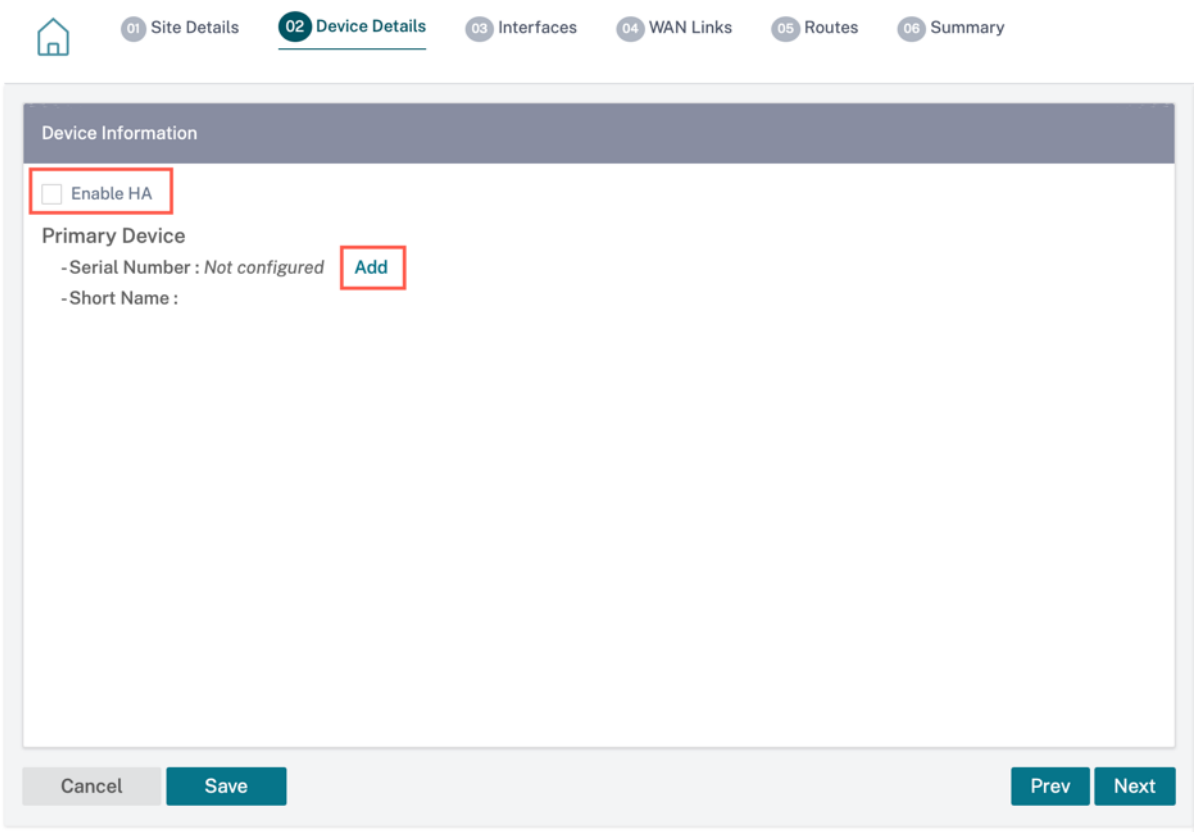
[Device details] セクションでは、サイトで高可用性 (HA) を構成および有効にできます。高可用性を使用すると、アクティブプライマリおよびパッシブセカンダリとして、サイトに 2 つのアプライアンスを導入できます。プライマリに障害が発生すると、セカンダリアプライアンスが引き継ぎます。詳細については、「高可用性」を参照してください。



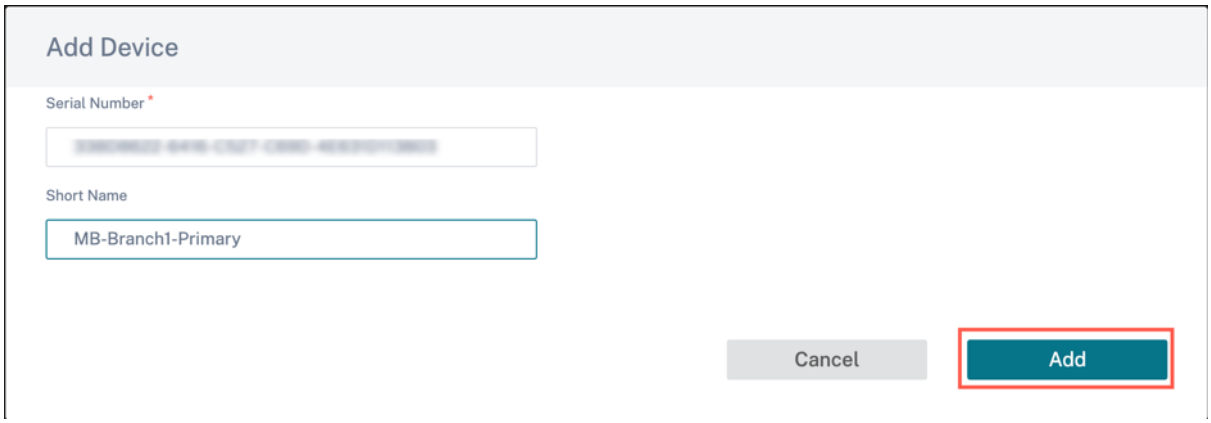
> 注
>
> シリアル番号は、サイトテンプレートを使用して設定することはできません。

デバイス情報

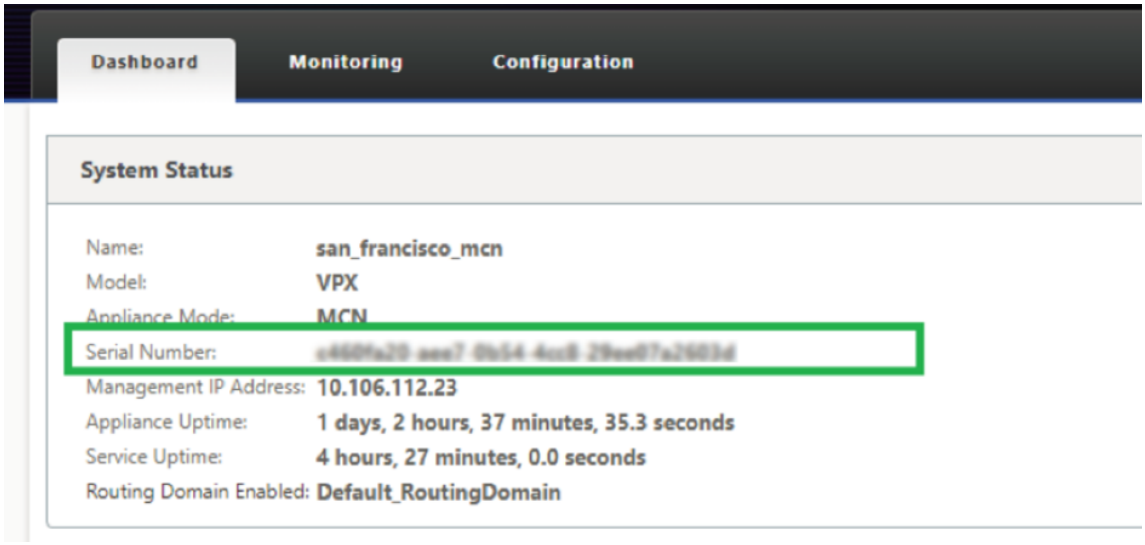
HA を有効にして、プライマリアプライアンスとセカンダリアプライアンスのシリアル番号とショートネームを入力します。[追加] をクリックし、シリアル番号とサイトの短縮名を入力します。



[追加] をクリックします。



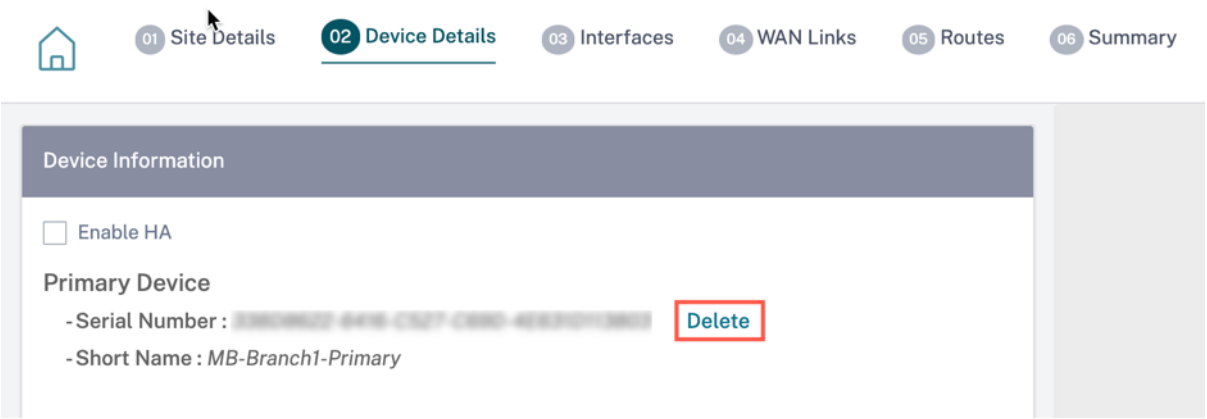
- シリアル番号: 仮想 SD-WAN インスタンス (VPX) のシリアル番号には、次のスクリーンショットで強調表示されているように、VPX Web コンソールからアクセスできます。ハードウェアアプライアンスのシリアル番号は、デバイスラベルにも記載されています。



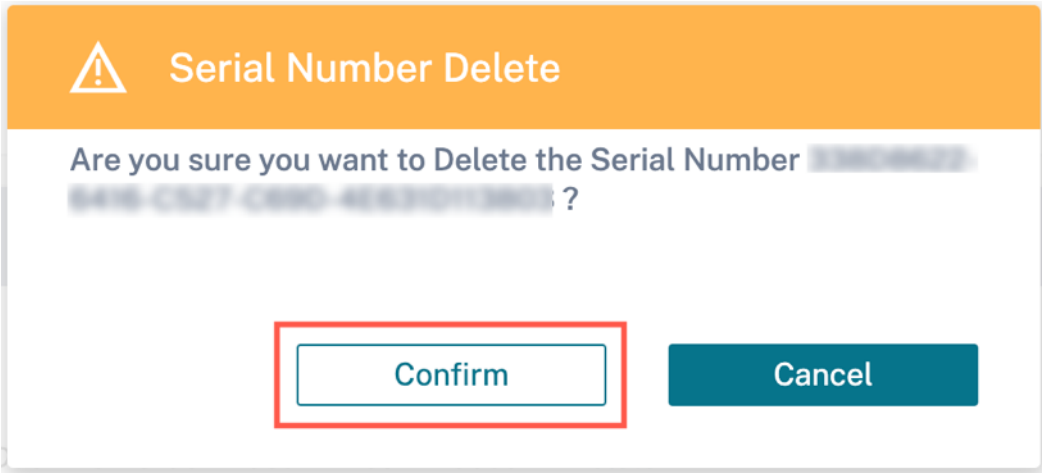
- ショートネーム: ショートネームフィールドは、サイトの識別しやすいショートネームを指定したり、必要に応じてサイトにタグを付けたりするために使用されます。

シリアル番号を削除する場合は、[削除] オプションをクリックします。

> 注:
> シリアル番号を更新するには、既存のシリアル番号を削除し、新しいシリアル番号を追加し直す必要があります。



「削除」オプションをクリックすると、シリアル番号を削除するかどうかを確認するポップアップが表示されます。



高可用性の詳細設定

- フェイルオーバー時間 **(ms)**: プライマリアプライアンスとの接続が失われた後、スタンバイアプライアンスがアクティブになるまでの待機時間。
- 共有ベース **MAC**: 高可用性ペアアプライアンスの共有 MAC アドレス。フェールオーバーが発生すると、セカンダリアプライアンスの仮想 MAC アドレスは、障害が発生したプライマリアプライアンスと同じになります。
- 共有ベース **MAC** を無効にする: このオプションは、ハイパーバイザーおよびクラウドベースのプラットフォームでのみ使用できます。このオプションを選択すると、共有仮想 MAC アドレスが無効になります。
- プライマリの再利用**:** 指定されたプライマリアプライアンスは、フェイルオーバーイベント後の再起動時に制御を取り戻します。
- **HA Fail-to-Wire** モード:HA Fail-to-Wire モードが有効になっています。詳細については、HA 導入モードをご覧ください。
- **Y** 字ケーブルサポートを有効にする:SFP (小型フォームファクタプラガブル) ポートを光ファイバ Y ケーブルと併用することで、Edge モード導入時の高可用性機能を実現できます。このオプションは、Citrix SD-WAN 1100 SE/PE アプライアンスでのみ使用できます。詳細については、「光ファイバ Y ケーブルを使用した Edge モードの高可用性の有効化」を参照してください。

Wi-Fi の詳細

Wi-Fi を Wi-Fi アクセスポイントとしてサポートする Citrix SD-WAN アプライアンスを構成できます。

Citrix SD-WAN 110 プラットフォームの次の 2 つのバリエーションは Wi-Fi をサポートし、Wi-Fi アクセスポイントとして構成できます。

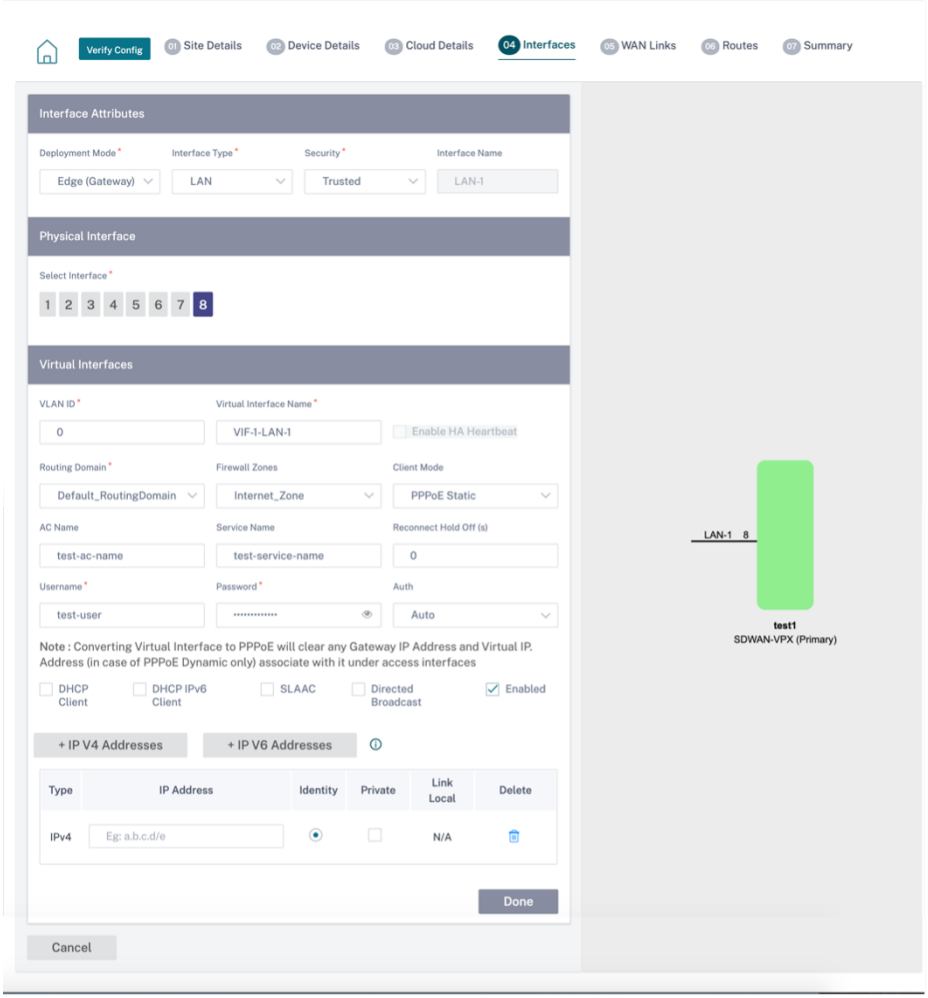
- Citrix SD-WAN 110-WiFi-SE
- Citrix SD-WAN 110-LTE-WiFi

Wi-Fi 設定の詳細については、Wi-Fi アクセスポイントをご覧ください。

インターフェイス

次のステップでは、インターフェイスを追加して設定します。**+ Interface** をクリックして、インターフェイスの構成を開始します。[**+ HA** インターフェイス] をクリックして、HA インターフェイスの設定を開始します。**+ HA** インターフェイスオプションは、セカンダリアプライアンスを高可用性に設定している場合にのみ使用できます。

インターフェイス設定には、デプロイモードの選択とインターフェイスレベル属性の設定が含まれます。この設定は、LAN リンクと WAN リンクの両方に適用されます。



帯域内管理

インバンド管理では、SD-WAN データポートを管理に使用できます。追加の管理パスを設定することなく、データトラフィックと管理トラフィックの両方を伝送します。インバンド管理では、仮想 IP アドレスが Web UI や SSH などの管理サービスに接続できます。管理 IP とインバンド仮想 IP を使用して、Web UI と SSH にアクセスできます。

インバンド管理を有効にするには、インバンド管理 **IP** ドロップダウンリストから IPv4 アドレスを選択するか、インバンド管理 **IPv6** ドロップダウンリストから **IPv6** アドレスを選択します。[帯域内管理 **DNS**] または **[**帯域内管理

DNS **V6] ドロップダウンリストから、**** 帯域内およびバックアップ管理プレーンを介したすべての **DNS** 要求の転送先となる DNS プロキシを選択します。

帯域内管理の詳細については、「帯域内管理」を参照してください。

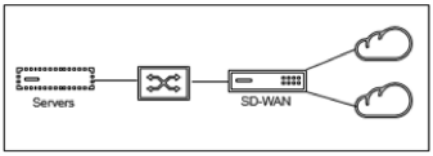
インターフェイスに設定された IP アドレスは、**InBand Management IP** ドロップダウンリストの下に表示されます。**[詳細設定] > [DNS]** で構成された **DNS** プロキシサービスは、**InBand Management DNS** ドロップダウンリストに表示されます。

インターフェイス属性

次の展開モードがサポートされています。

1. Edge (Gateway)
2. インライン: 配線失敗、ブロックへの失敗、仮想インライン。

- 展開モード: 次の展開モードのいずれかを選択します。
  - **Edge (**ゲートウェイ**)**:



    ゲートウェイモードは、SD-WAN がすべての LAN トラフィックの WAN への「ゲートウェイ」として機能することを意味します。ゲートウェイモードはデフォルトモードです。アプライアンスは、LAN 側または WAN 側の Gateway としてデプロイできます。

  - インライン:

    SD-WAN を LAN スイッチと WAN ルーターの間にインラインで展開する場合、SD-WAN は LAN と WAN を「ブリッジ」することが期待されます。

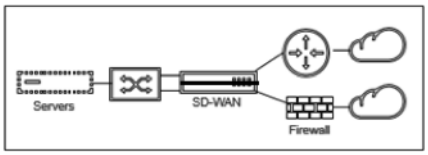
    すべての Citrix SD-WAN アプライアンスには、ブリッジペアリングインターフェイスが事前に定義されています。ブリッジオプションを有効にすると、LAN 側のインターフェイスを選択すると、ブリッジの WAN 側用に予約されているペアリングされたインターフェイスが自動的に強調表示されます。たとえば、物理インターフェイス 1 と 2 はブリッジドペアです。

    * **Fail-To-Wire**: ブリッジ接続されたインターフェイスのペア間の物理接続を可能にし、アプライアンスの再起動や障害時にトラフィックが SD-WAN をバイパスしてブリッジを直接通過できるようにします。

    以前は、DHCP クライアントは Fail-to-Block ポートでのみサポートされていました。Citrix SD-WAN 11.2.0 リリースでは、シリアル高可用性（HA）展開のブランチサイトのフェールツーワイヤポートでの DHCP クライアント機能が拡張されました。この拡張機能:

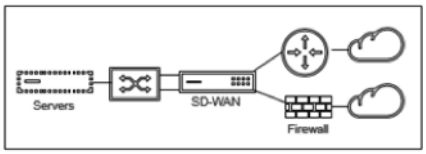
* Fail-to-Wire ブリッジペアおよびシリアル HA 配置を持つ信頼できないインターフェイスグループで DHCP クライアント設定を許可します。
* プライベートイントラネット WAN リンクの一部として DHCP インターフェイスを選択できるようにします。

> 注
>
> * インライン（Fail-to-Wire）オプションは、ハードウェアアプライアンスでのみ使用でき、仮想アプライアンス（VPX/VPXL）では使用できません。
> * DHCP クライアントがプライベートイントラネットリンクでサポートされるようになりました。
> * LAN インターフェイスは、インターフェイス間でパケットがブリッジされる可能性があるため、フェールツーワイヤのペアに接続しないでください。

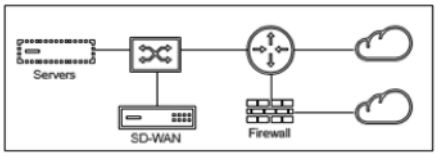


* **Fail-to-Block**：このオプションは、ハードウェアアプライアンス上のブリッジインターフェイス間の物理接続を無効にし、アプライアンスの再起動または障害発生時にトラフィックがブリッジを通過するのを防ぎます。

> 注
>
> インライン（ブロック失敗）は、仮想アプライアンス（VPX/VPXL）で使用できる唯一のブリッジモードオプションです。



* バーチャルインライン **(**ワンアーム**)**:



SD-WAN をこのモードで展開すると、SD-WAN 上の同じインターフェイスを共有する WAN ルーター、LAN、WAN に接続するシングルアームがあります。したがって、インターフェイス設定は LAN リンクと WAN リンク間で共有されます。

- インターフェースの種類**:** ドロップダウンリストからインターフェースの種類を選択します。

- セキュリティ **(**信頼できる**/**信頼できない**)**: インターフェイスのセキュリティレベルを指定します。信頼されたセグメントは、ファイアウォールによって保護されます。
- インターフェース名**:** 選択したデプロイモードに基づいて、「インターフェース名」フィールドが自動的に入力されます。

物理インタフェース

- インターフェースの選択**:** アプライアンスで使用可能な設定可能なイーサネットポートを選択します。

仮想インターフェイス

- **VLAN ID**: インターフェイスに出入りするトラフィックを識別し、マーキングするための ID。
- 仮想インターフェイス名**:** 選択したデプロイモードに基づいて、[仮想インターフェイス名] フィールドが自動的に入力されます。
- **HA** ハートビートを有効にする: このインターフェイスでの HA ハートビートの同期を有効にします。このオプションは、HA 用にセカンダリアプライアンスを構成している場合に有効になります。プライマリアプライアンスとセカンダリアプライアンスが、このインターフェイス上で HA ハートビートを同期できるようにするには、このオプションを選択します。プライマリおよびセカンダリアプライアンスの IP アドレスを指定します。
- ルーティングドメイン: ブランチオフィスネットワークまたはデータセンターネットワークの単一管理ポイントを提供するルーティングドメイン。
- ファイアウォールゾーン: インターフェイスが属するファイアウォールゾーン。ファイアウォールゾーンは、論理ゾーン内のインターフェイスを保護し、制御します。
- クライアントモード**:** ドロップダウンリストから [クライアントモード] を選択します。PPPoE 静的を選択すると、より多くの設定が表示されます。

  > 注
  >
  > サイトモード ([サイトの詳細] タブ) を [ブランチ] に、[セキュリティ**]** フィールド ([インターフェイス] タブ) を [信頼できない] に選択すると、クライアントモードで ****PPPoE Dynamic** オプションが使用可能になります ****。

  Citrix SD-WAN は PPPoE クライアントとして機能します。IPv4 の場合、SD-WAN は動的 IPv4 アドレスを取得するか、静的 IPv4 アドレスを使用します。IPv6 の場合は、PPPoE サーバーからリンクローカルアドレスを取得します。IPv6 ユニキャストアドレスには、スタティック IP、DHCP、または SLAAC を使用できます。
- **DHCP** クライアント: 仮想インタフェースで有効にすると、DHCP サーバーは接続されたクライアントに動的に IPv4 アドレスを割り当てます。
- **DHCP IPv6** クライアント: 仮想インタフェースで有効にすると、DHCP サーバーは接続されたクライアントに IPv6 アドレスを動的に割り当てます。

- **SLAAC**: このオプションは IPv6 アドレスでのみ使用できます。選択すると、インターフェイスはステートレスアドレス自動構成 (SLAAC) を通じて IPv6 アドレスを取得します。
- ダイレクトブロードキャスト: ダイレクトブロードキャストチェックボックスが選択されている場合、ダイレクトブロードキャストは仮想インターフェイス上の仮想 IP サブネットに送信されます。
- 有効: デフォルトでは、すべての仮想インターフェイスで「有効」チェックボックスが選択されています。仮想インターフェイスを無効にする場合は、[有効] チェックボックスをオフにします。

  > 注
  >
  > - 「有効」チェックボックスは、Citrix SD-WAN リリース 11.3.1 以降でのみ使用できます。
  > - 仮想インターフェイスを無効にするオプションは、WAN リンクアクセスインターフェイスで使用されていない場合にのみ使用できます。仮想インターフェイスが WAN リンクアクセスインターフェイスで使用されている場合、このチェックボックスは読み取り専用で、デフォルトでオンになっています。
  > - 有効になっている仮想インターフェイスとともに、他の機能を設定する際に、[**WAN** リンクのアクセスインターフェイス] の下を除き、無効化された仮想インターフェイスも表示されます。無効にした仮想インターフェイスを選択した場合でも、仮想インターフェイスは考慮されず、ネットワーク設定には影響しません。

- **+ IPv4** アドレス: インタフェースの仮想 IPv4 アドレスとネットマスク。
- **+ IPv6** アドレス: インタフェースの仮想 IPv6 アドレスとプレフィックス。
- **ID**: IP サービスに使用する ID を選択します。たとえば、**ID** は BGP ネイバーとの通信の送信元 IP アドレスとして使用されます。
- プライベート: 有効にすると、仮想 IP アドレスはローカルアプライアンスでのみルーティング可能になります。

> 注
>
> - LTE ポートは固定 IP アドレス (IPv4 および IPv6) をサポートしていません。
> - LTE ポートは DHCP と SLAAC の両方をサポートします。DHCPv4 または DHCPv6 の設定は必須です。SLAAC はオプションです。
> - LTE ポートでは、リンクローカルアドレスを IPv6 または SLAAC に設定できます。

PPPoE 認証情報

PPPoE（Point-to-Point Protocol over Ethernet）は、イーサネット LAN 上の複数のコンピュータユーザーを、一般的な顧客構内のアプライアンス（Citrix SD-WAN など）を介してリモートサイトに接続します。PPPoE を使用すると、ユーザーは共通のデジタル加入者線 (DSL)、ケーブルモデム、またはインターネットへのワイヤレス接続を共有できます。PPPoE は、ダイヤルアップ接続で一般的に使用される Point-to-Point Protocol（PPP; ポイントツーポイントプロトコル）と、LAN 内の複数のユーザをサポートするイーサネットプロトコルを組み合わせています。PPP プロトコル情報は、イーサネットフレーム内にカプセル化されます。

Citrix SD-WAN アプライアンスは PPPoE を使用して ISP をサポートし、ダイヤルアップ接続とは異なり、DSL とケーブルモデム接続を継続的かつ継続的に行います。PPPoE は、「検出」と呼ばれる初期交換を通じて互いのネットワークアドレスを学習するために、各ユーザリモートサイトセッションを提供します。個々のユーザーとリモートサイト (ISP プロバイダーなど) の間にセッションが確立されると、セッションを監視できます。企業は、イーサネットと PPPoE を使用して、DSL 回線を介して共有インターネットアクセスを使用します。

Citrix SD-WAN は PPPoE クライアントとして機能します。IPv4 の場合、SD-WAN は動的 IPv4 アドレスを取得するか、静的 IPv4 アドレスを使用します。IPv6 の場合は、PPPoE サーバーからリンクローカルアドレスを取得します。IPv6 ユニキャストアドレスには、スタティック IP、DHCP、または SLAAC を使用できます。

PPPoE セッションを正常に確立するには、次のことが必要です。

- 仮想ネットワークインターフェイス (VNI) を設定します。
- PPPoE セッションを作成するための一意の資格情報。
- WAN リンクを設定します。各 VNI に設定できる WAN リンクは 1 つだけです。
- 仮想 IP アドレスを設定します。各セッションは、提供された構成に基づいて、動的または静的の一意の IP アドレスを取得します。
- アプライアンスをブリッジモードで展開し、静的 IP アドレスで PPPoE を使用し、インターフェイスを「信頼できる」に設定します。
- スタティック IP は、サーバが提示する IP を強制的に設定する場合に適しています。設定されたスタティック IP と異なる場合、エラーが発生する可能性があります。
- アプライアンスを Edge デバイスとして展開し、動的 IP で PPPoE を使用し、インターフェイスを「信頼できない」に設定します。
- サポートされている認証プロトコルは、PAP、CHAP、EAP-MD5、EAP-SRP です。
- 複数のセッションの最大数は、設定されている VNI の数によって異なります。
- インターフェイスグループごとに複数の PPPoE セッションをサポートするために、複数の VNI を作成します。

> （注
>
> ）同じ 802.1Q VLAN タグを使用して複数の VNI を作成できます。

PPPoE 設定の制限事項

- 802.1q VLAN タギングはサポートされません。
- EAP-TLS 認証はサポートされていません。
- アドレス/制御圧縮
- 収縮圧縮。
- プロトコルフィールド圧縮ネゴシエーション
- 圧縮制御プロトコル。
- BSD 圧縮圧縮。
- IPX プロトコル。
- PPP マルチリンク。

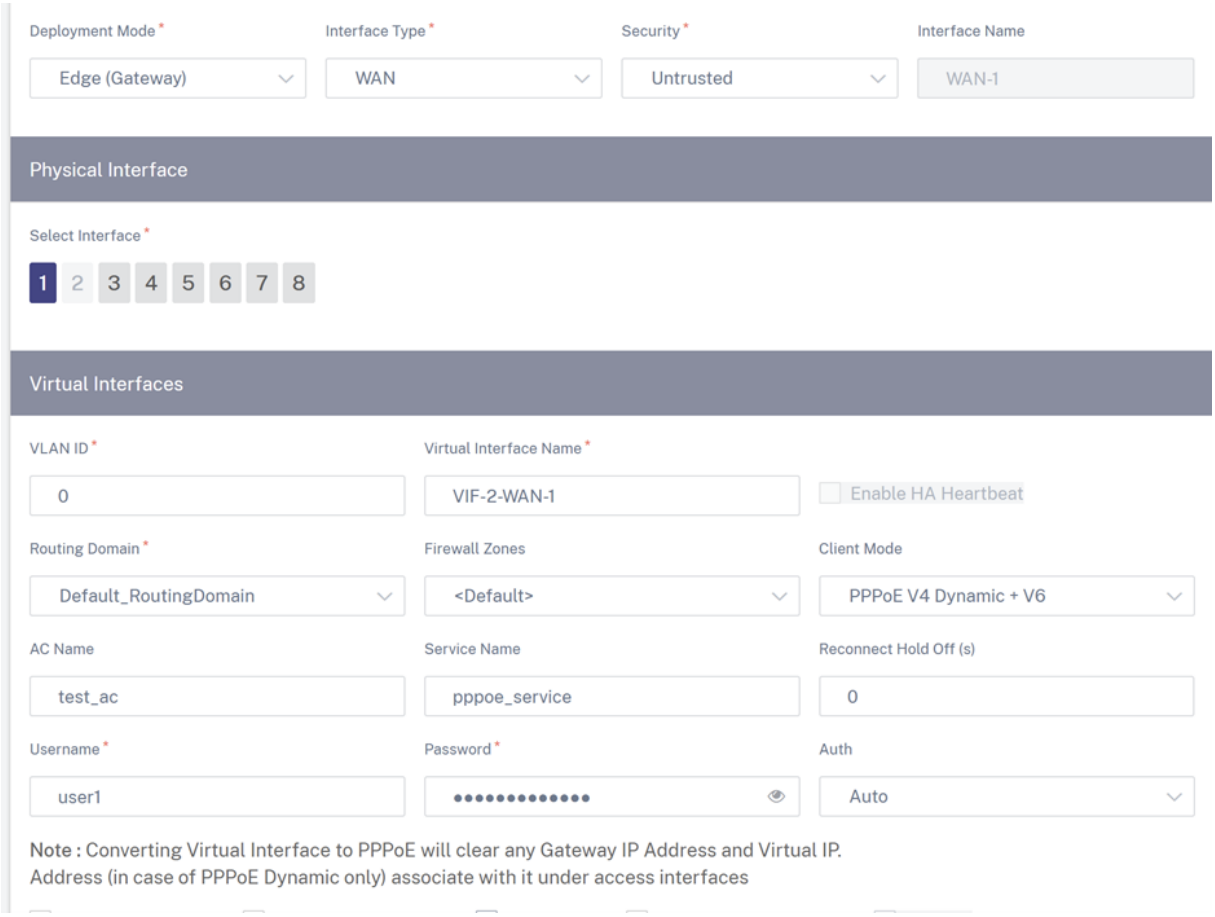
- Van Jacobson スタイルの TCP/IP ヘッダー圧縮。
- Van Jacobson スタイルの TCP/IP ヘッダー圧縮の接続 ID 圧縮オプション。
- PPPoE は LTE インターフェイスではサポートされません。

Citrix SD-WAN 11.3.1 リリースでは、TCP の最大セグメントサイズ（MSS）を調整するために、追加 8 バイトの PPPoE ヘッダーが考慮されています。余分な 8 バイトの PPPoE ヘッダーは、MTU に基づいて同期パケットの MSS を調整します。サポートされている MTU の範囲は 1280 バイトから 1492 バイトです。

PPPoE 構成　MCN では、PPPoE スタティックだけを設定できます。ブランチでは、PPPoE スタティックまたは PPPoE ダイナミックのどちらかを設定できます。

PPPoE を設定するには、サイトレベルの設定で、[構成] > [サイトの構成**] > [**インターフェイス] タブに移動します。仮想インターフェイスセクションで、クライアントモードドロップダウンリストから適切な PPPoE オプションを選択します。

> 注
>
> - 複数のインターフェイスが設定された VNI では、PPPoE 接続に使用できるインターフェイスは 1 つだけです。
> - 複数のインターフェイスで構成された VNI と PPPoE 接続を別のインターフェイスに変更した場合、[**Reports] > [Real Time] > [PPPoE**] ページを使用して既存のセッションを停止し、新しいセッションを開始できます。その後、新しいインターフェース上で新しいセッションを確立できます。
> - [PPPoE ダイナミック] が選択されている場合、VNI は「信頼できない」である必要があります。



- **AC** 名**:** PPPoE 構成のアクセスコンセントレータ (AC) 名を指定します。
- サービス名**:** サービス名を入力します。
- 再接続保留時間**:** 再接続試行の保留時間を入力します。
- ユーザー名**:** PPPoE 設定のユーザー名を入力します。
- パスワード**:** PPPoE 設定のパスワードを入力します。
- 認証**:** ドロップダウンリストから認証プロトコルを選択します。
  - **Auth** オプションが Auto に設定されている場合、SD-WAN アプライアンスはサーバーから受信したサポートされている認証プロトコル要求を受け入れます。
  - **Auth** オプションが PAP/CHAP/EAP に設定されている場合、特定の認証プロトコルのみが適用されます。構成に PAP があり、サーバが CHAP を使用して認証要求を送信すると、接続要求は拒否されます。サーバが PAP とネゴシエートしない場合、認証エラーが発生します。

PPPoE スタティック VNI またはダイナミック VNI ごとに、WAN リンクの作成は 1 つだけ許可されます。WAN リンクの設定は、クライアントモードの VNI の選択によって異なります。

VNI に PPPoE ダイナミッククライアントモードが設定されている場合は、次の手順を実行します。

- IP アドレスフィールドと Gateway IP アドレスフィールドは非アクティブになります。
- 仮想パスモードが「プライマリ」に設定されています。

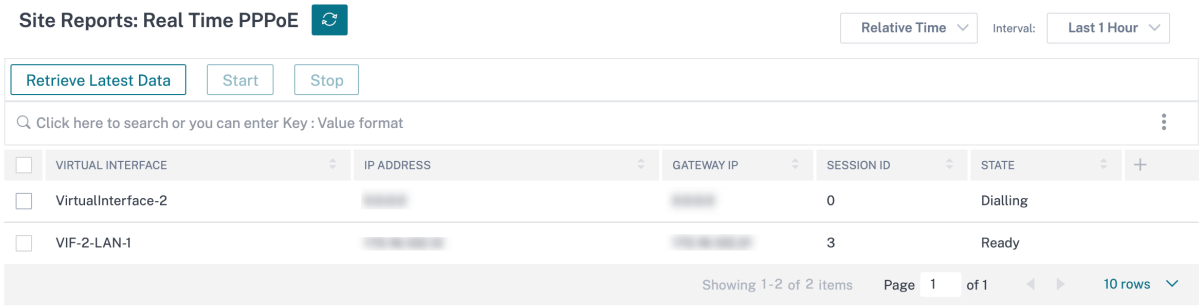
- プロキシ ARP は設定できません。

デフォルトでは、[Gateway MAC アドレスバインディング] が選択されています。

VNI が PPPoE スタティッククライアントモードで設定されている場合は、IP アドレスを設定します。

> 注:
>
> サーバが設定された固定 IP アドレスを使用せず、別の IP アドレスを提供すると、エラーが発生します。PPPoE セッションは、サーバーが設定された IP アドレスを受け入れるまで、定期的に接続の再確立を試みます。

PPPoE モニタリングとトラブルシューティング　サイトレベルで [レポート**] > [**リアルタイム**] > [PPPoE**] セクションに移動すると、PPPoE スタティックまたはダイナミッククライアントモードで設定された VNI に関する情報が表示されます。トラブルシューティングの目的で、手動でセッションを開始または停止できます。



PPPoE セッションを確立する際に問題が発生した場合:

- 失敗ステータスの上にマウスを置くと、最近の障害の原因が表示されます。
- 新しいセッションを確立したり、アクティブな PPPoE セッションをトラブルシューティングしたりするには、セッションを再起動します。
- PPPoE セッションを手動で停止した場合、手動で開始して構成の変更をアクティブにするか、サービスを再起動するまで開始できません。

PPPoE セッションは、次の理由により失敗することがあります。

- 構成内のユーザー名/パスワードが正しくないために SD-WAN がピアに対する認証に失敗した場合。
- PPP ネゴシエーションが失敗します。ネゴシエーションは、少なくとも 1 つのネットワークプロトコルが実行されているポイントに到達しません。
- システムメモリまたはシステムリソースの問題。
- 構成が無効または不正です（AC 名またはサービス名が間違っています）。
- オペレーティングシステムエラーのため、シリアルポートを開けませんでした。
- エコーパケットに対する応答がない（リンク不良またはサーバが応答しない）。
- 1 分以内に、が連続的に失敗したダイヤルセッションがいくつか発生しました。

10 回連続して失敗した後、失敗の理由が観察されます。

- 障害が正常であれば、すぐに再起動します。
- 失敗がエラーの場合、再起動は 10 秒間戻ります。
- 失敗が致命的である場合、再起動は 30 秒間戻ってから再起動します。

LCP Echo 要求パケットは、SD-WAN から 60 秒ごとに生成され、5 つのエコー応答を受信できなかった場合はリンク障害と見なされ、セッションが再確立されます。

- VNI が起動して準備ができている場合は、[IP] 列と [Gateway IP] 列にセッションの現在の値が表示されます。これは、最近受信した値であることを示します。
- VNI が停止しているか、障害状態の場合、値は最後に受信した値です。
- Gateway IP 列の上にマウスを置くと、セッションと IP を受信する PPPoE アクセスコンセントレータの MAC アドレスが表示されます。
- 「状態」の値の上にマウスを置くとメッセージが表示され、「失敗」状態の場合に便利です。

PPPoE セッションタイプ	ステータスカラー	説明
構成済み	黄	VNI には PPPoE が設定されています。これは初期状態です。
ダイヤル中	黄	VNI が設定されると、PPPoE ディスカバリを開始して PPPoE セッション状態がダイヤル状態に移行します。パケット情報がキャプチャされます。
セッション	黄	VNI は Discovery 状態から Session 状態に移行し、動的な場合は IP の受信を待機し、静的な場合はアドバタイズされた IP のサーバーからの確認応答を待ちます。
準備完了	緑	IP パケットが受信され、VNI と関連する WAN リンクが使用可能になります。
失敗	赤	PPP/PPPoE セッションが終了しました。失敗の原因は、無効な構成または致命的なエラーが原因である可能性があります。セッションは 30 秒後に再接続を試みます。
停止しました	黄	PPP/PPPoE セッションは手動で停止されます。

PPPoE セッションタイプ	ステータスカラー	説明
終了中	黄	理由により終了する中間状態。この状態は、一定時間（通常のエラーの場合は 5 秒、致命的なエラーの場合は 30 秒）後に自動的に開始されます。
無効	黄	SD-WAN サービスは無効です。

SDWAN_ip_learned.log ファイルには、PPPoE に関連するログが含まれています。[トラブルシューティング**] > [**デバイスログ] に移動して、*SDWAN_ip_learned.log* ファイルを表示またはダウンロードします。

有線 **802.1X** 構成

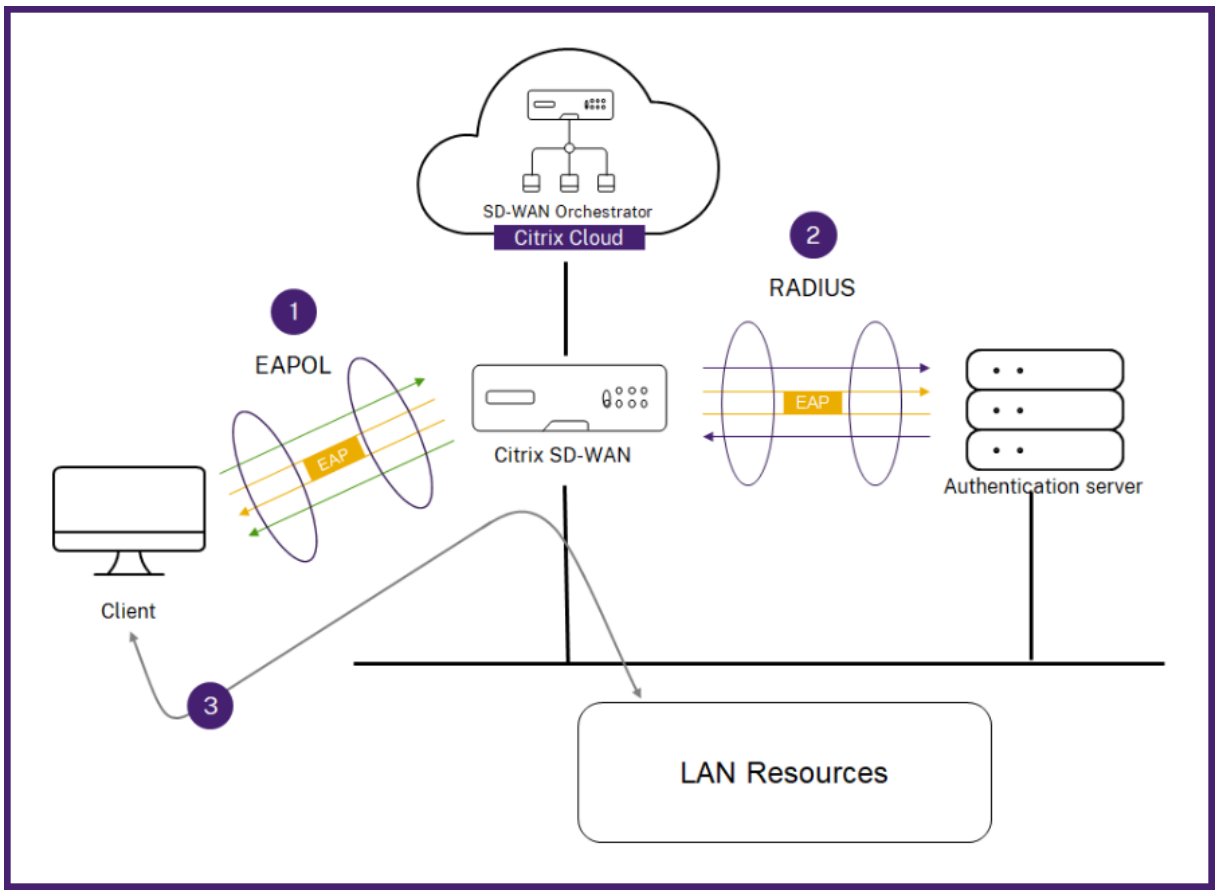
有線 802.1X は、LAN リソースにアクセスする前にクライアントを認証する必要がある認証メカニズムです。Citrix SD-WAN Orchestrator サービスは、LAN インターフェイスでの有線 802.1X 認証の構成をサポートします。

Citrix SD-WAN ネットワークでは、クライアントは認証要求を Citrix SD-WAN アプライアンスに送信し、LAN リソースにアクセスします。Citrix SD-WAN アプライアンスはオーセンティケータとして機能し、認証要求を認証サーバーに送信します。Citrix SD-WAN Orchestrator サービスは、認証サーバーとして構成される RADIUS サーバーのみをサポートします。

初めて認証する場合、処理できるのは EAPOL パケット、またはデフォルトの仮想 LAN から 802.1X 認証を初期化できる DHCP パケットだけです。新しく接続したクライアントは 90 秒以内に認証される必要があります。認証が成功すると、LAN リソースにアクセスします。

認証に失敗すると、クライアントはネットワークアクセスを許可されず、すべてのパケットがドロップされます。Citrix SD-WAN アプライアンスに直接接続されているクライアントは、イーサネットケーブルを抜いて再度挿入することで認証を再試行できます。オプションで、特定の仮想 LAN を定義して、失敗した認証要求に対して制限された LAN リソースへのアクセスを許可できます。このような場合、失敗した認証要求は指定された仮想 LAN にアクセスします。仮想 LAN を作成するときに、異なるルーティングドメインまたはファイアウォールゾーンを使用して、認証されたトラフィックへのアクセスを制限できます。

> 注
>
> - デフォルトの仮想 LAN では、常に 802.1X が有効になっている必要があります。
> - 動的仮想 LAN はサポートされていません。



Citrix SD-WAN アプライアンスは、802.1Q タグのないパケット（タグなしパケット）を受信することを想定しています。Citrix SD-WAN アプライアンスが、割り当てられた仮想 LAN に 802.1Q タグが設定されたパケットを受信した場合、MAC から送信されたすべてのパケットにタグを付ける必要があります。ヘッダーに 802.1Q タグがないパケット、または MAC アドレスが属する仮想 LAN 以外のタグが付いたパケットを受信した場合、パケットはドロップされます。

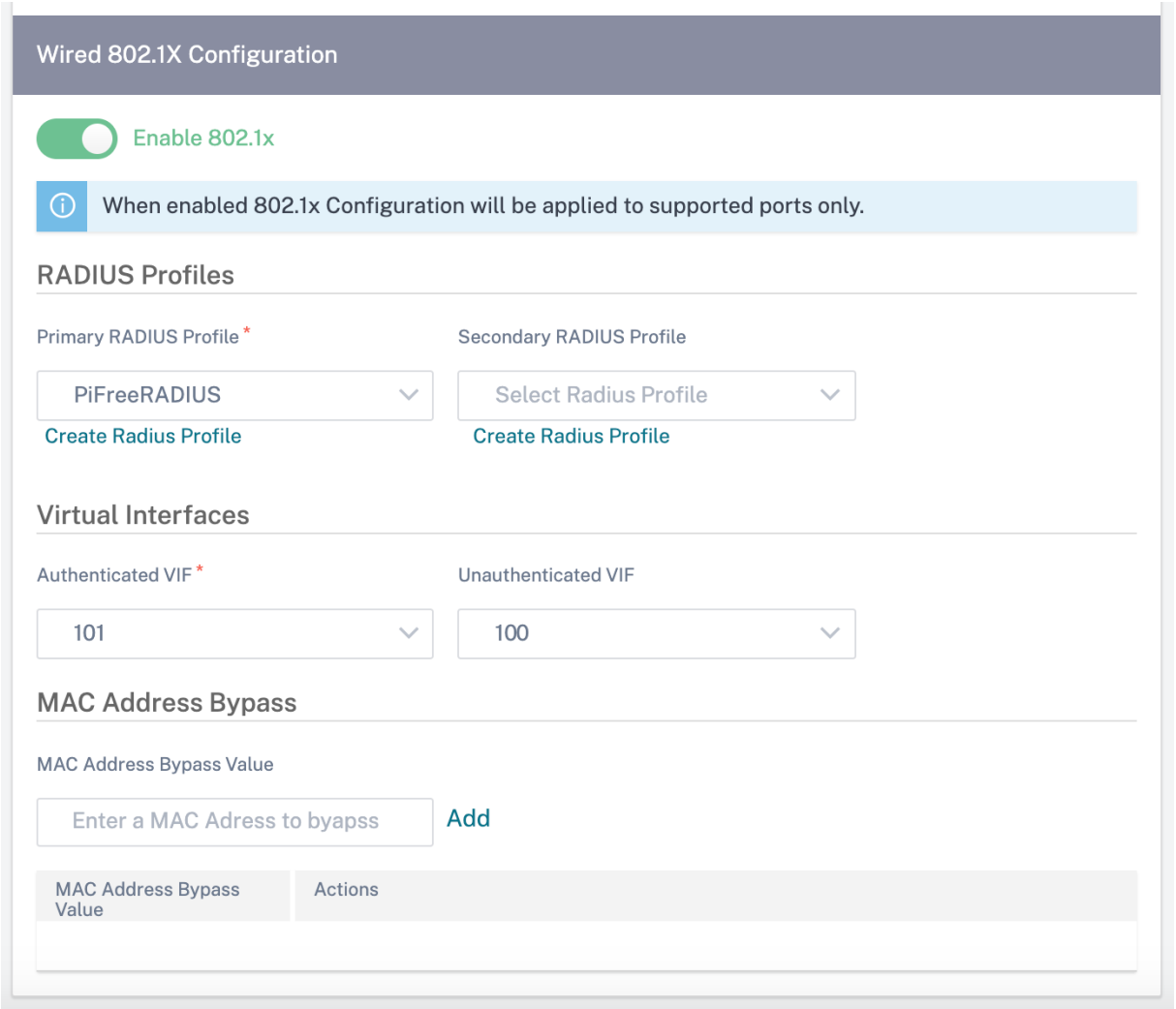
スイッチに接続された複数のクライアントが 1 つのポートで同時に認証を試みると、各クライアントは LAN リソースにアクセスする前に個別に認証されます。認証に失敗したクライアントは、イーサネットケーブルを取り外し、3 分間待ってから、イーサネットケーブルを再挿入することで認証を再試行できます。Citrix SD-WAN 110、210、および 410 プラットフォームは、最大 32 のクライアント（認証済みと非認証の両方）をサポートします。他のすべてのプラットフォームは、最大 64 のクライアント (認証済みと未認証の両方) をサポートします。

802.1X 認証を設定するには、[サイトの構成] **>** [インターフェイス] に移動し、[**802.1X** を有効にする] トグルボタンをオンにします。既存の RADIUS プロファイルを選択するか、[**RADIUS** プロファイルの作成] をクリックして RADIUS プロファイルを作成します。RADIUS プロファイルの作成について詳しくは、「RADIUS サーバープロファイル」を参照してください。アプライアンスがワイヤレス WPA2-Enterprise をサポートしていれば、有線 802.1x 認証とワイヤレス WPA2-エンタープライズ認証に同じ RADIUS プロファイルを使用できます。

認証された **VIF** ドロップダウンリストから仮想インターフェイスを選択します。選択した仮想インターフェイスは、認証要求を正常に実行するために LAN リソースへのアクセスを許可します。

オプションで、**Unauthenticated VIF** ドロップダウンリストからインターフェイスを選択できます。選択した仮想インターフェイスは、失敗した認証要求に対して特定の LAN リソースへのアクセスを許可します。

認証プロセスを省略する MAC アドレスのリストを追加できます。これらの MAC アドレスからのトラフィックは、暗黙的に認証済みとして扱われます。これらの MAC アドレスは悪意のある攻撃を受けやすくなります。そのため、この機能は、物理的に安全な環境で、有線 802.1X 認証をサポートしていないレガシーハードウェアにのみ使用してください。



有線 802.1X 認証要求に関連するアラートは、[レポート] **>** [アラート] で確認できます。詳細については、「アラート」を参照してください。

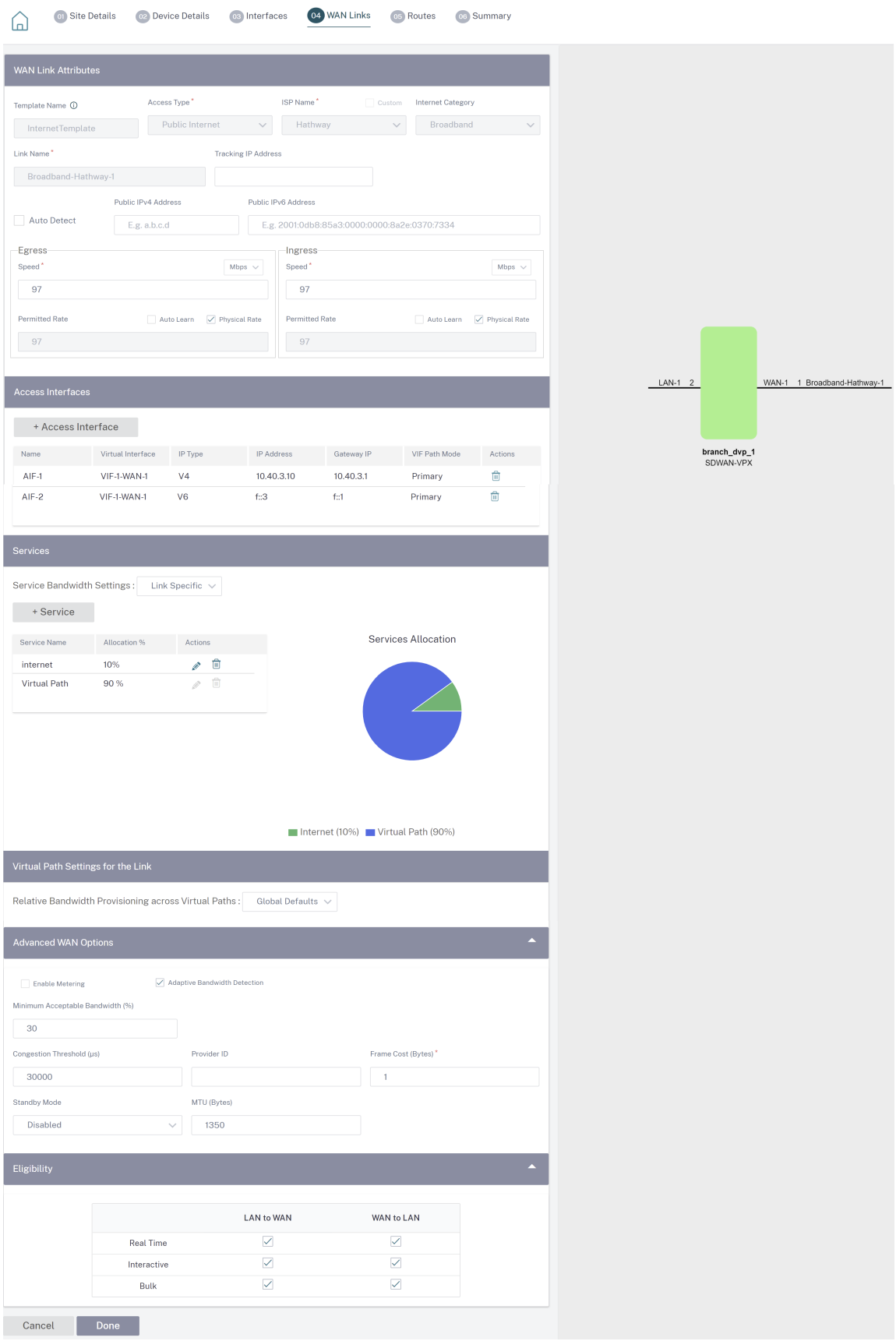
WAN リンク

次のステップでは、WAN リンクを設定します。**+ WAN** リンクをクリックして WAN リンクの設定を開始します。

WAN リンクの設定には、WAN リンクアクセスタイプとアクセスインターフェイス属性の設定が含まれます。

WAN リンク属性は最初から設定することも、WAN リンクテンプレートを使用して WAN リンク属性をすばやく設定することもできます。サイトプロファイルを既に使用している場合は、**WAN** リンク属性が自動入力されます。

WAN リンク属性



- テンプレート名:WAN リンクの作成に使用される WAN リンクテンプレートの名前。WAN リンクテンプレート名は、WAN リンクの作成後に変更することはできません。WAN リンクテンプレートを使用して WAN リンクを作成すると、アクセスタイプ、ISP 名、またはインターネットカテゴリを編集することはできません。
- アクセスタイプ: リンクの WAN 接続タイプを指定します。
  - パブリックインターネット: リンクが ISP 経由でインターネットに接続されていることを示します。
  - プライベートイントラネット: リンクが SD-WAN ネットワーク内の 1 つ以上のサイトに接続されており、SD-WAN ネットワーク外の場所には接続できないことを示します。
  - **MPLS**: プライベートイントラネットの特殊なバリアント。リンクが 1 つ以上の DSCP タグを使用してイントラネット上の 2 つ以上のポイント間のサービス品質を制御し、SD-WAN ネットワークの外部に接続できないことを示します。
- **ISP** 名: サービスプロバイダーの名前。
- インターネットカテゴリ:WAN リンクで有効になっている WAN リンクインターネットアクセステクノロジーサービス (ブロードバンド、衛星、ファイバー、LTE など) のタイプ。
- リンク名: 以前の入力に基づいて自動入力されます。
- トラッキング **IP** アドレス:PING を実行してパスの状態を判断できる仮想パス上の仮想 IP アドレス。
- **** パブリック **IPv4** アドレスとパブリック **IPv6** アドレス **:NAT または DNS サーバーの IP アドレス。このアドレスは、シリアル HA 展開で WAN リンクアクセスタイプが [パブリックインターネット] または [プライベートイントラネット] の場合にのみ適用され、公開されます。パブリック IP は、手動で設定することも、自動学習オプションを使用して自動学習することもできます。
- 自動検出: 有効にすると、SD-WAN アプライアンスはパブリック IP アドレスを自動的に検出します。このオプションは、デバイスロールがブランチであり、マスターコントロールノード **(MCN)** ではない場合にのみ使用できます。
- 出力速度:WAN から LAN への速度。
  - 速度:WAN から LAN へのトラフィックの利用可能または許容される速度（Kbps または Mbps 単位）。
  - 許可レート:WAN リンク容量全体を SD-WAN アプライアンスで使用することが想定されていない場合は、それに応じて許可レートを変更してください。
  - 自動学習: 帯域幅が不明で、リンクの信頼性が低い場合は、自動学習機能を有効にできます。自動学習機能は、基礎となるリンク容量のみを学習し、将来同じ値を使用します。
  - 物理レート:WAN リンクの実際の帯域幅容量。
- 入力速度:LAN から WAN への速度。
  - 速度:LAN から WAN へのトラフィックの利用可能または許容速度（Kbps または Mbps 単位）。
  - 許可レート:SD-WAN アプライアンスが LAN リンク容量全体を使用することを想定していない場合は、それに応じて許可レートを変更してください。
  - 自動学習: 帯域幅が不明で、リンクの信頼性が低い場合は、自動学習機能を有効にできます。自動学習機能は、基礎となるリンク容量のみを学習し、将来同じ値を使用します。
  - 物理レート:LAN リンクの実際の帯域幅容量。

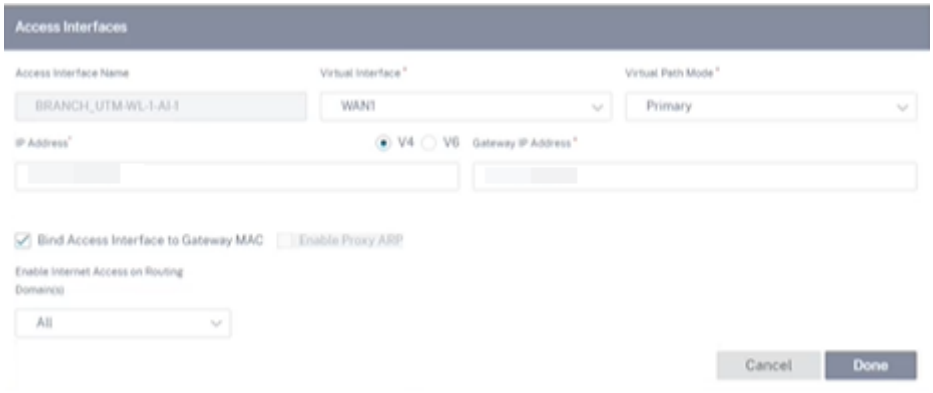
MPLS キュー

MPLS キュー設定は WAN リンクアクセスタイプの MPLS でのみ使用できます。このオプションは、MPLS WAN リンク上のサービスプロバイダー MPLS キューに対応するキューの定義を有効にするためのものです。MPLS キューの追加については、「MPLS キュー」を参照してください。

アクセスインタフェース

アクセスインターフェイスは、WAN リンクの IP アドレスと Gateway IP アドレスを定義します。各 WAN リンクには、少なくとも 1 つのアクセスインターフェイスが必要です。次に、アクセスインターフェイスのパラメータを示します。

- アクセスインターフェイス名: アクセスインターフェイスが参照される名前。デフォルトでは、WAN_link_name-AI-number: WAN_link_name はこのインターフェイスに関連付ける WAN リンクの名前で、number はこのリンクに現在設定されているアクセスインターフェイスの数で、1 ずつ増加します。
- 仮想インターフェイス: アクセスインターフェイスが使用する仮想インターフェイス。現在のブランチサイトに設定されている仮想インターフェイスのドロップダウンメニューからエントリを選択します。
- 仮想パスモード: 現在の WAN リンク上の仮想パストラフィックの優先順位を指定します。オプションは、[プライマリ]、[セカンダリ]、または [除外] [除外] に設定した場合、アクセスインターフェイスはインターネットおよびイントラネットトラフィックにのみ使用されます。
- **IP** アドレス: アプライアンスから WAN までのアクセスインターフェイスエンドポイントの IP アドレス。必要に応じて、V4（IPv4）または V6（IPv6）を選択します。
- ゲートウェイ **IP** アドレス: ゲートウェイルーターの IP アドレス。
- アクセスインターフェイスをゲートウェイ **MAC** にバインド: 有効にした場合、インターネットまたはイントラネットサービスで受信されるパケットの送信元 MAC アドレスは、ゲートウェイ MAC AddressWank Links > Advances WAN オプションと一致する必要があります。
- プロキシ **ARP** を有効にする: 有効にすると、ゲートウェイに到達できないときに、仮想 WAN アプライアンスはゲートウェイ IP アドレスの ARP 要求に応答します。
- ルーティングドメインでインターネットアクセスを有効にする: それぞれのルーティングドメインのすべてのルーティングテーブルにデフォルトルート (0.0.0.0/0) を自動作成します。すべてのルーティングドメインまたは NONE で有効にできます。インターネットアクセスを必要とする場合、すべてのルーティングドメインにわたって排他的な静的ルートを作成する必要性を回避します。

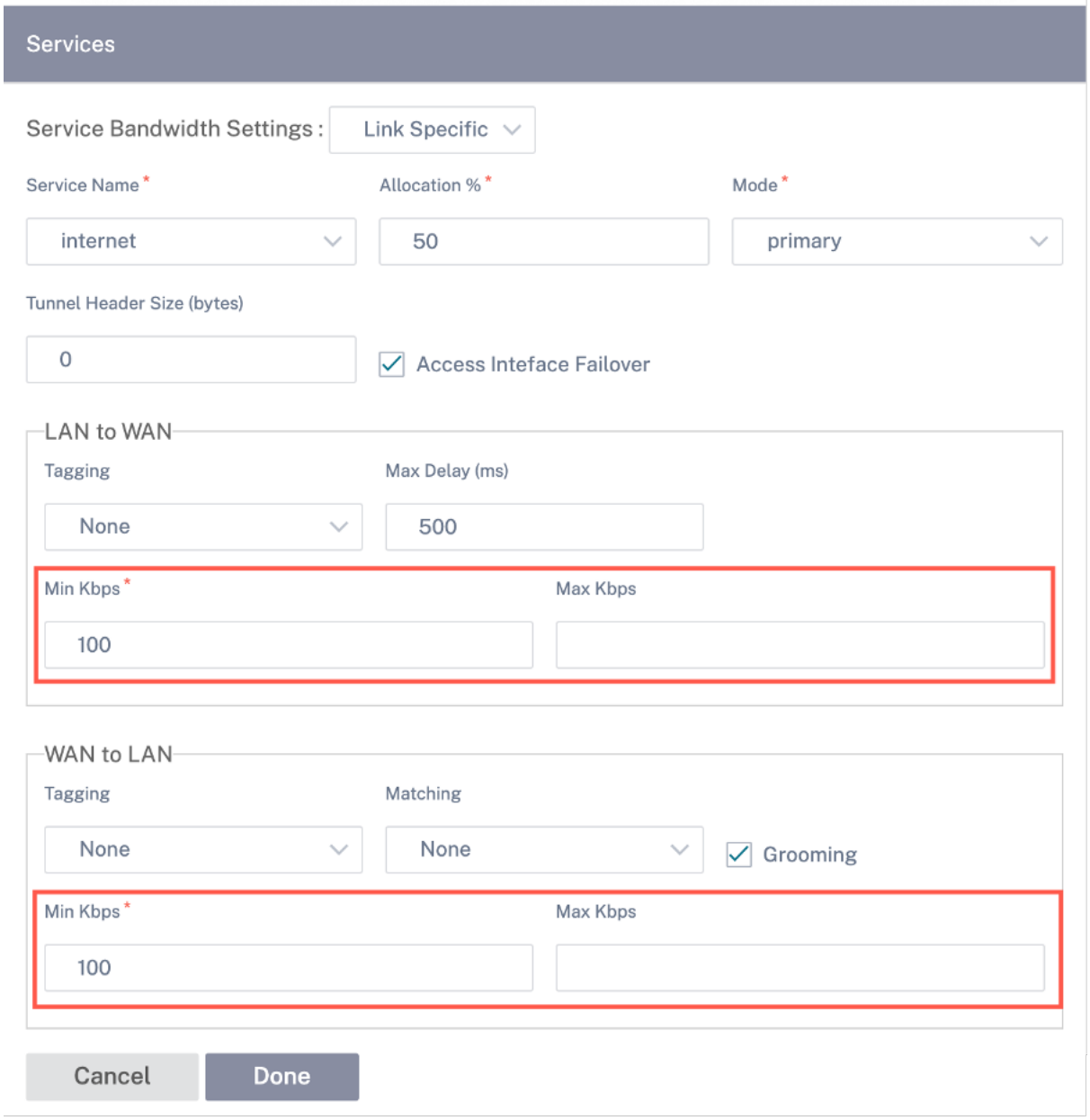


Services

サービスセクションでは、サービスタイプを追加し、各サービスタイプに使用する帯域幅の割合を割り当てることができます。デリバリーサービスセクションからサービスタイプを定義し 、その属性を設定できます。これらのグローバルデフォルトを使用するか、サービス帯域幅設定ドロップダウンリストからリンク固有のサービス帯域幅設定を構成するかを選択できます。リンク固有を選択した場合は、次の詳細を入力します。

- サービス名:WAN リンクサービスの名前。
- 割り当て**%**: リンクの総容量からサービスに割り当てられる帯域幅の公平な配分が保証されています。
- モード: 選択したサービスに基づく WAN リンクの動作モード。インターネットの場合、プライマリ、セカンダリ、およびバランスの 1 つがあり、イントラネットにはプライマリとセカンダリがあります。
- トンネルヘッダーサイズ: トンネルヘッダーのサイズ (バイト単位)。
- **LAN-to-WAN** タグ: サービス上の LAN-to-WAN パケットに適用する DHCP タグ。
- **LAN** から **WAN** への遅延:WAN リンクの帯域幅を超えたときに、パケットをバッファリングする最大時間です。
- **LAN to WAN** 最小 **Kbps**: サービス用に予約されている最小アップロード帯域幅値。**Min Kbps** は必須フィールドです。
- **LAN to WAN Max Kbps**: サービス用に予約されている最大アップロード帯域幅値。**Max Kbps** フィールドはオプションで、設定済みの最小アップロード帯域幅値より小さくすることはできません。この値は、最小アップロード帯域幅値以上でなければなりません。
- **WAN-to-LAN** タグ: サービス上の WAN-to-LAN パケットに適用する DHCP タグ。
- **WAN** と **LAN** の一致: インターネット WAN から LAN へのパケットをサービスに割り当てる際の一致基準。
- **WAN to LAN** 最小 **Kbps**: サービス用に予約されている最小ダウンロード帯域幅値。**Min Kbps** は必須フィールドです。
- **WAN to LAN Max Kbps**: サービス用に予約されている最大ダウンロード帯域幅値。**Max Kbps** フィールドはオプションで、設定済みの最小ダウンロード帯域幅値より小さくすることはできません。この値は、最小ダウンロード帯域幅値以上でなければなりません。
- **WAN** から **LAN** へのグルーミング: 有効にすると、WAN 間のトラフィックがサービスのプロビジョニングされた帯域幅を超えることを防ぐために、パケットはランダムに破棄されます。

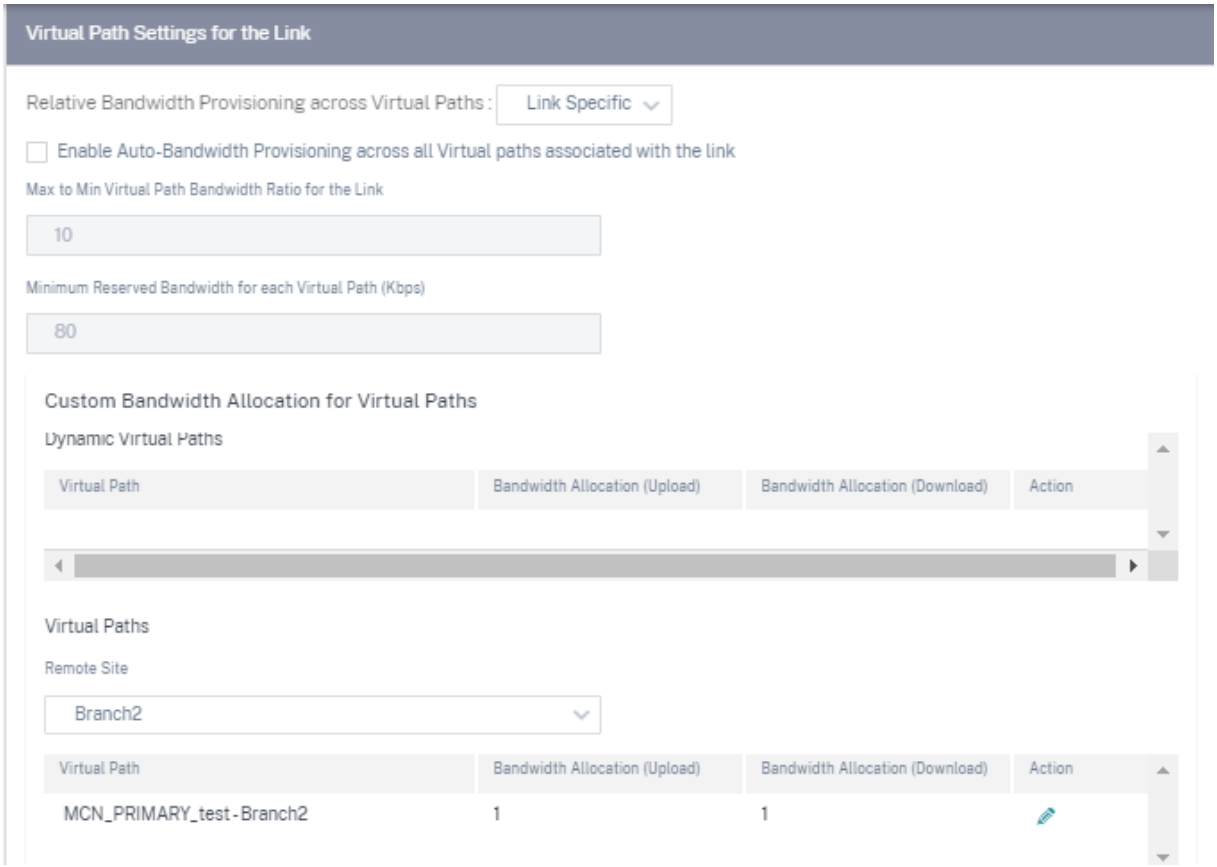
> 注:
>
> 仮想パスでは [最小 Kbps] フィールドと [最大 Kbps] フィールドは使用できません。



リンクの仮想パス設定

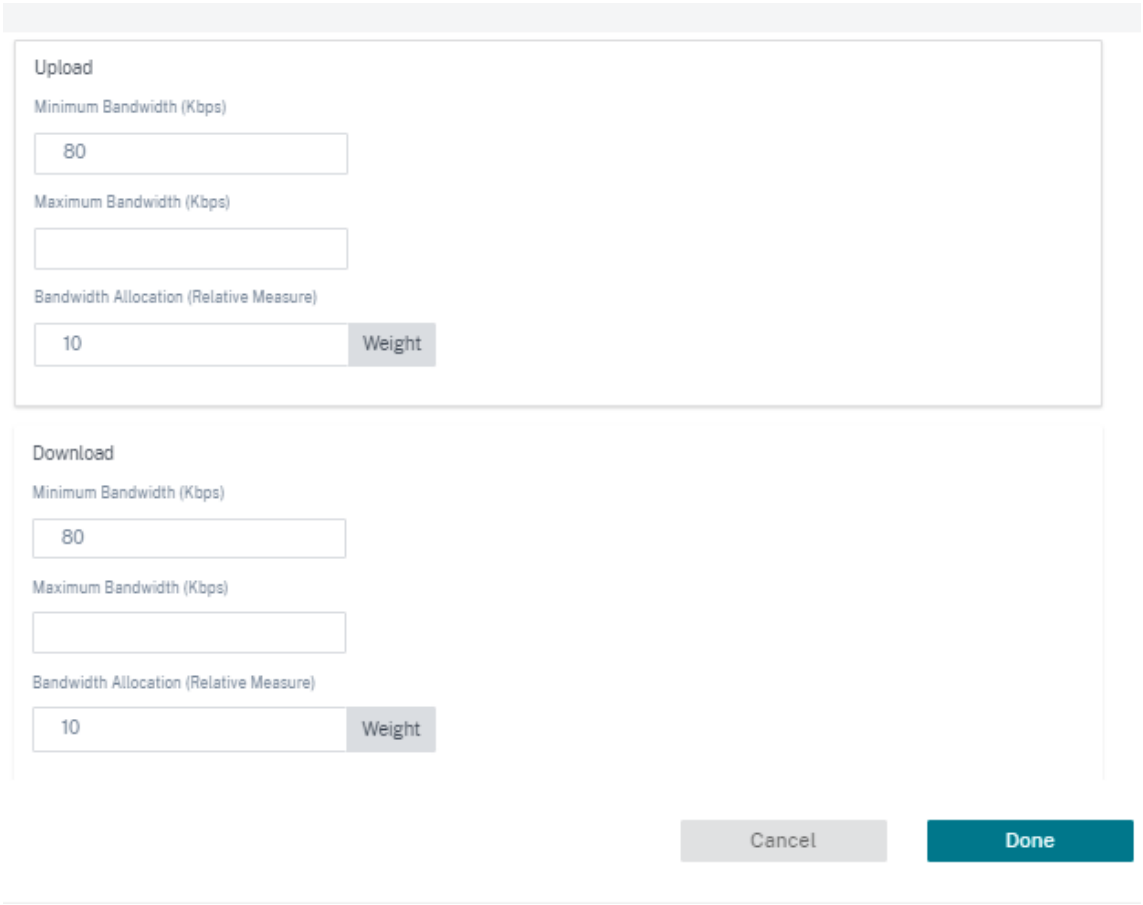
必要に応じて、仮想パス全体にわたる相対的な帯域幅プロビジョニングを [グローバルデフォルト] または [リンク固有] として選択します。**Link Specific** を選択すると、自動帯域幅プロビジョニングを有効にすると、仮想パスサービスの帯域幅のシェアが自動的に計算され、リモートサイトで消費される可能性のある帯域幅の大きさに応じて適用されます。

- リンクの最大対最小仮想パス帯域幅の比率**:** 選択した **WAN** リンクに適用できる最大仮想パスと最小の仮想パスの比率を設定できます。
- 各仮想パスの最小予約帯域幅 **(Kbps)**: 各仮想パスの最小予約帯域幅値を Kbps 単位で設定できます。



WAN リンクに関連する仮想パスの帯域幅をカスタマイズするには:

1. [リンクに関連するすべての仮想パスで自動帯域幅 **Provisioning** を有効にする] チェックボックスをオフにします。
2. 「仮想パスのカスタム帯域幅割り当て」セクションで、リモートサイトを選択します。リモートサイトへの仮想パスの帯域幅をプロビジョニングできます。
    - 最小帯域幅 **(Kbps)**: 仮想パス用に予約されている最小帯域幅。仮想パスに設定できる最小帯域幅は 80 Kbps です。
    - 最大帯域幅 **(Kbps)**: 仮想パスが WAN リンクから利用できる最大帯域幅。最大帯域幅が設定されていない場合、サイトは利用可能な帯域幅をすべて利用します。
    - 帯域幅割り当て（相対的な尺度）：グループの対象となる帯域幅のうち、仮想パスに割り当てられた帯域幅のシェア。たとえば、3 つの仮想パスで構成される WAN リンクグループが 30 Mbps の帯域幅に対応していて、各仮想パスに同じ帯域幅を割り当てたい場合は、リモートサイトの帯域幅割り当てとして 10 を更新します。



3. [完了] をクリックします。

> 注
>
> Citrix SD-WAN Orchestrator サービスは、以前に構成された動的仮想パスが 2 つのサイト間で無効になった後でも、以前に構成されたカスタム帯域幅設定を保持します。動的仮想パスを再構成するときは、必ずカスタム帯域幅設定を手動で更新してください。

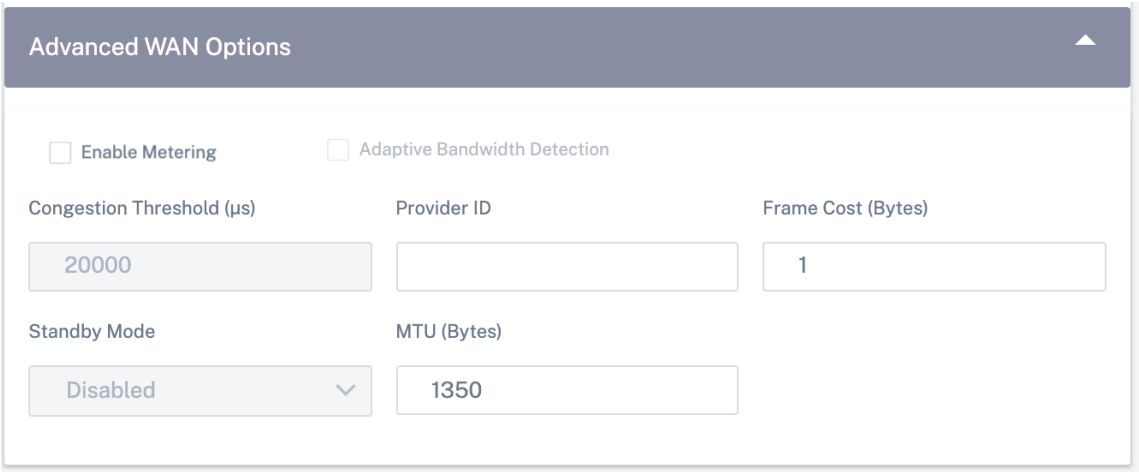
帯域幅のプロビジョニングで考慮すべきポイント

- デフォルトでは、すべてのブランチと WAN サービス (仮想パス/インターネット/イントラネット) にはそれぞれ 1 のウェイトが割り当てられます。
- 帯域幅要件の点で大きな差異がある場合は、帯域幅のカスタマイズが必要です。
- 使用可能なサイト間で動的仮想パスが有効になっている場合、データセンターへの静的仮想パスと動的仮想パスの間で WAN リンクの容量が共有されます。

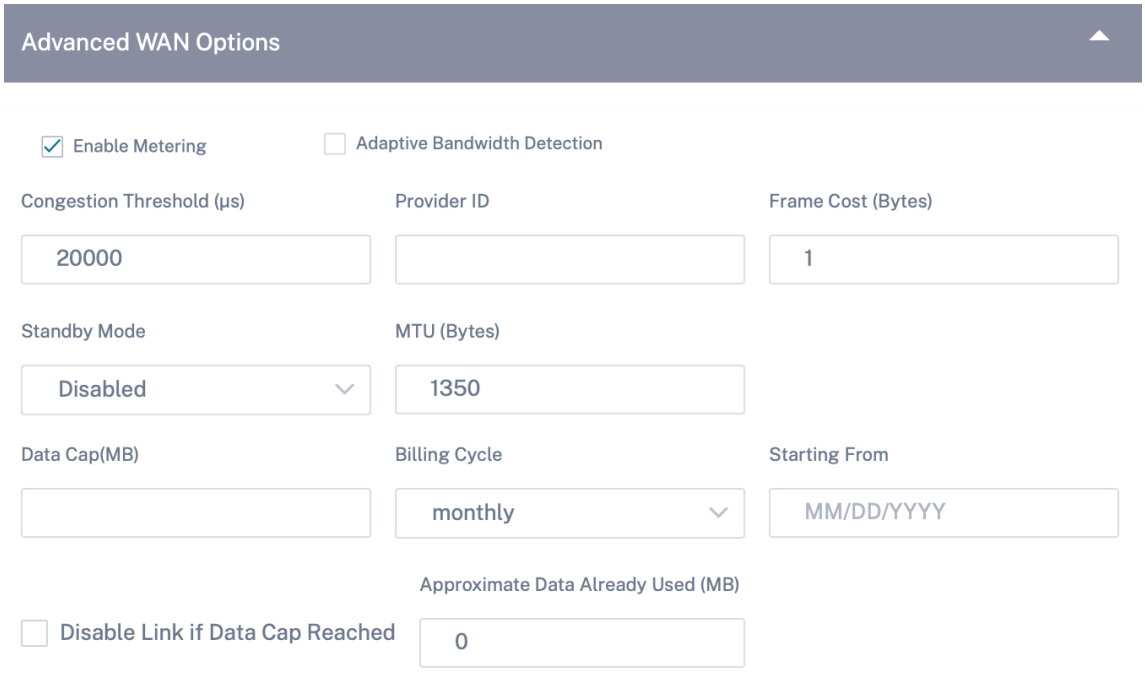
高度な **WAN** オプション

WAN リンクの詳細設定では、**ISP** 固有の属性を設定できます。

- 輻輳しきい値: 輻輳の度合い。この量に達すると、WAN リンクはさらなる輻輳を避けるためにパケットの送信を制限します。
- プロバイダー **ID**: 重複したパケットを送信する際にパスを区別するためのプロバイダーの一意の識別子。
- フレームコスト **(**バイト**)**: イーサネット IPG や AAL5 トレーラなど、パケットごとに追加のヘッダー/トレーラバイトが追加されます。
- **MTU (**バイト**)**: 未加工パケットの最大サイズ (バイト単位)。フレームコストは含まれません。
- スタンバイモード: スタンバイリンクは、アクティブにならない限りユーザトラフィックの伝送には使用されません。WAN リンクのスタンバイモードは、デフォルトで無効になっています。スタンバイモードの詳細については、「スタンバイモード」を参照してください。



- メータリングを有効にする:WAN リンクの使用状況を追跡し、リンク使用量が設定されたデータ上限を超えるとユーザーに警告します。メータリングの詳細については、「メータリングとスタンバイ WAN リンク」を参照してください。



- 適応型帯域幅検出: 損失が検出されると、WAN リンクを低帯域幅レートで使用します。使用可能な帯域幅が設定された最小許容帯域幅を下回ると、パスは BAD とマークされます。パスグループまたは Autopath グループの [適応帯域幅検出] で、カスタム不良損失感度を使用します。

  > 注
  >
  > 適応帯域幅検出は、クライアントでのみ使用でき、MCN では使用できません。

  - 許容可能な最小帯域幅**:** 帯域幅レートが異なる場合、WAN/LAN 間の許容レートのパーセンテージです。これを下回ると、パスは BAD とマークされます。最小 kbps は、仮想パスの各側で異なります。値は 10% ～50% の範囲で指定でき、デフォルトは 30% です。

詳細については、「適応型帯域幅検出」を参照してください。

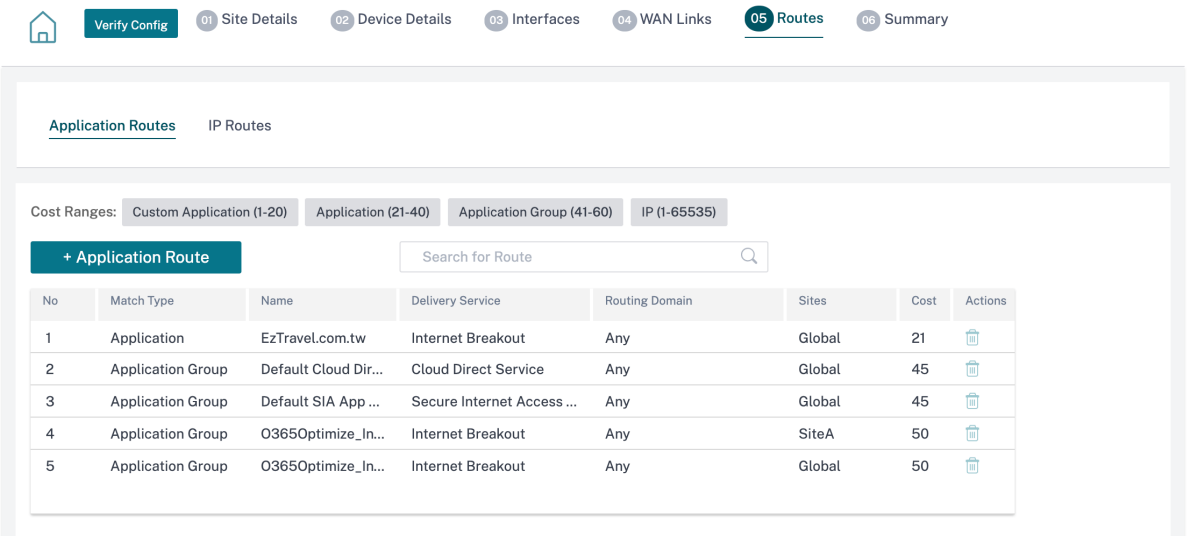
ルート

サイト構成ワークフローの次のステップは、ルートを作成することです。サイトの要件に基づいて、アプリケーションルートと IP ルートを作成できます。

> 注**:**
>
> [アプリケーションルート] タブと [IP ルート] タブを導入する前に追加されたルートは、**[IP** ルート] タブに [配信サービス] を [インターネット] として一覧表示しています。

ネットワークレベルで作成されたグローバルルートとサイト固有のルートは、[ルート] > [アプリケーションルート**]** タブと **[**ルート**] > [**IP** ルート **] タブに自動的に一覧表示されます。グローバルルートは、サイトレベルでのみ表示できます。グローバルルートを編集または削除するには、ネットワークレベル設定に移動します。

サイトレベルでルートを作成、編集、または削除することもできます。



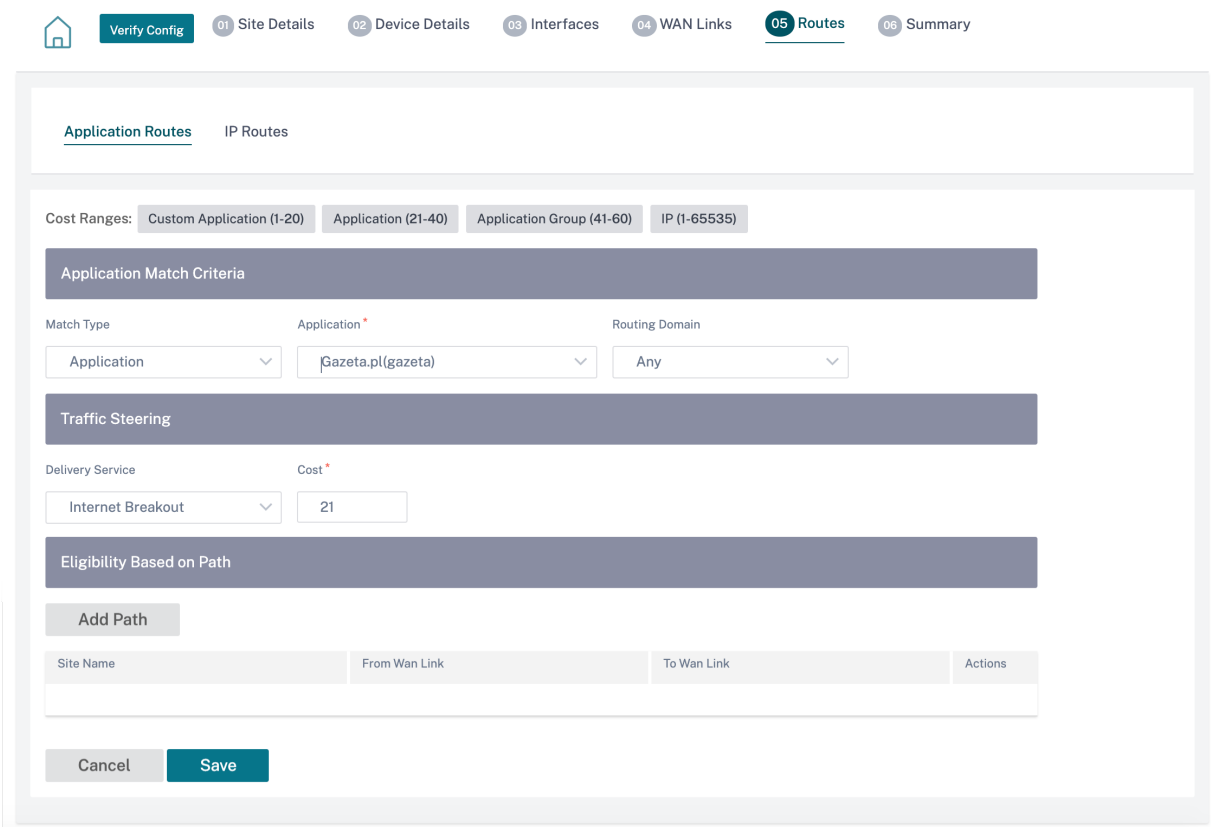
アプリケーションルート

[**+** アプリケーションルート] をクリックして、アプリケーションルートを作成します。

- カスタムアプリケーション一致基準:
  - マッチタイプ: ** ドロップダウンリストからアプリケーション/カスタムアプリケーション/アプリケーショングループとしてマッチタイプを選択します ** 。
  - アプリケーション: ドロップダウンリストからアプリケーションを 1 つ選択します。
  - ルーティングドメイン: ルーティングドメインを選択します。
- トラフィック
  - 配送サービス: 一覧から配送サービスを 1 つ選択します。
  - コスト: 各ルートの相対的な優先順位を反映します。コストを低くすると、優先順位が高くなります。
- パスに基づく資格:
  - パスを追加: サイトと WAN リンク (リンク先、リンク元) を選択します。追加されたパスがダウンすると、アプリケーションルートはトラフィックを受信しません。

新しいアプリケーションルートが追加された場合、ルートコストは次の範囲内にある必要があります。

- カスタムアプリケーション: 1〜20
- アプリケーション: 21〜40
- アプリケーショングループ: 41—60



IP ルート

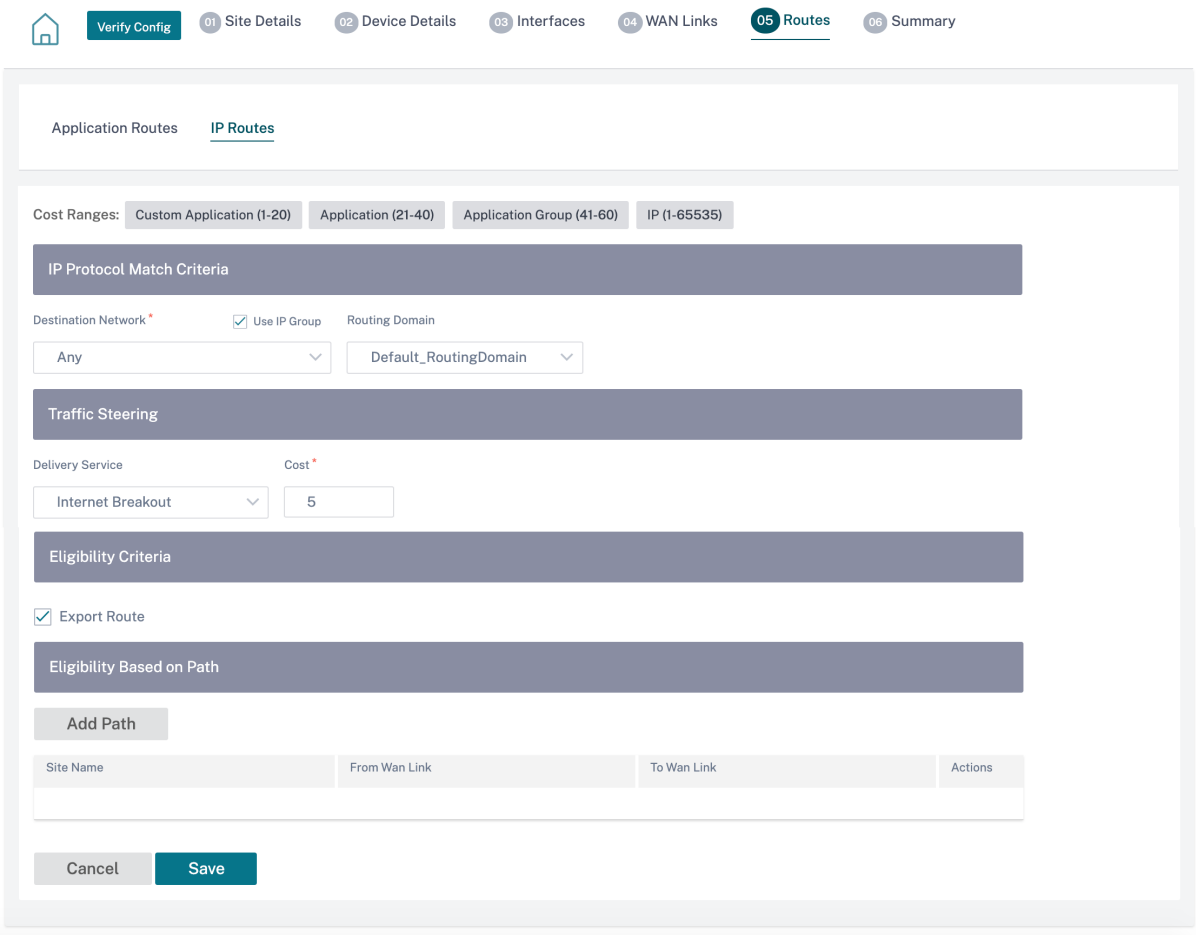
[**IP** ルート] タブに移動し、[**+ IP** ルート] をクリックして、トラフィックを誘導する IP ルートポリシーを作成します。

- **IP** プロトコル一致基準:
  - 宛先ネットワーク: パケットの転送に役立つ宛先ネットワークを追加します。
  - **IP** グループを使用する: 宛先ネットワークを追加するか、[IP グループを使用] チェックボックスをオンにしてドロップダウンリストから任意の IP グループを選択できます。
  - ルーティングドメイン: ドロップダウンリストからルーティングドメインを選択します。
- トラフィック
  - 配信サービス: ドロップダウンリストから配信サービスを 1 つ選択します。
  - コスト: 各ルートの相対的な優先順位を反映します。コストを低くすると、優先順位が高くなります。
- 適格基準:
  - ルートのエクスポート:「ルートのエクスポート」チェックボックスが選択されていて、ルートがローカルルートの場合、ルートはデフォルトでエクスポートできます。ルートがイントラネット/インターネットベースのルートの場合、エクスポートが機能するには、WAN から WAN への転送を有効にする必要

があります。[Export Route] チェックボックスがオフの場合、ローカルルートは他の SD-WAN へのエクスポートに適格ではなく、ローカルな意味を持ちます。

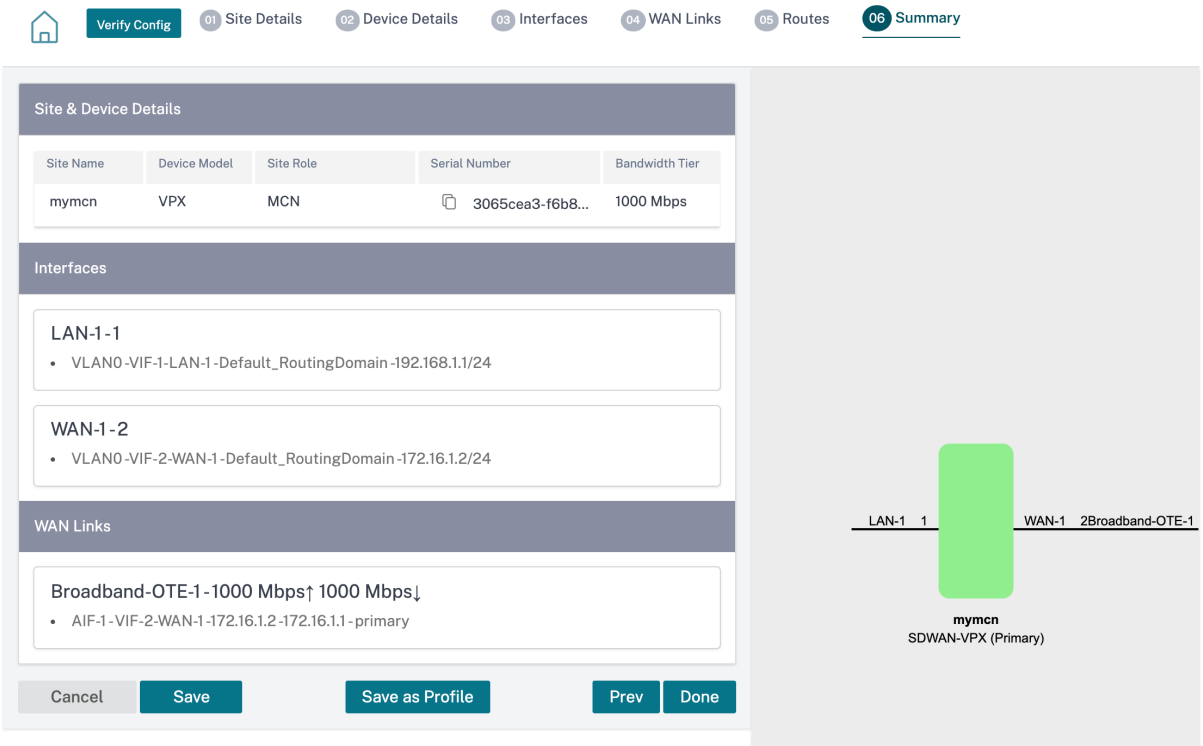
- パスに基づく資格:
  - パスを追加: サイトと WAN リンク (リンク先、リンク元) を選択します。追加されたパスがダウンした場合、IP ルートはトラフィックを受信しません。

新しい IP ルートを追加する場合、ルートコストは 1 ～20 の範囲でなければなりません。



概要

このセクションでは、サイト設定の概要について説明し、サイト設定の概要を説明します。



「テンプレートとして保存」オプションを使用して、サイト構成をテンプレートとして保存し、他のサイトで再利用できます。「完了」をクリックすると、サイト構成が完了し、「ネットワーク構成-ホーム」ページが開き、構成されたすべてのサイトを確認できます。詳細については、「ネットワーク構成」を参照してください。

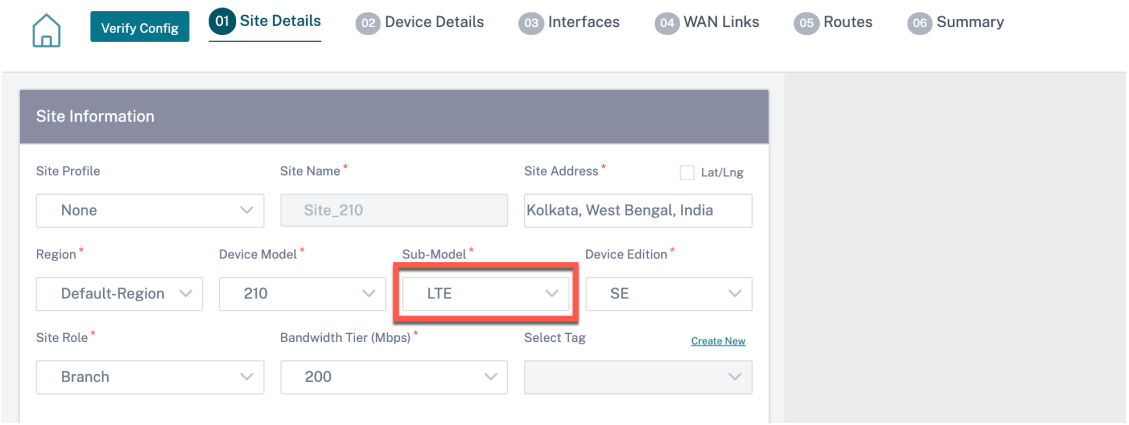
LTE ファームウェアのアップグレード

October 26, 2022

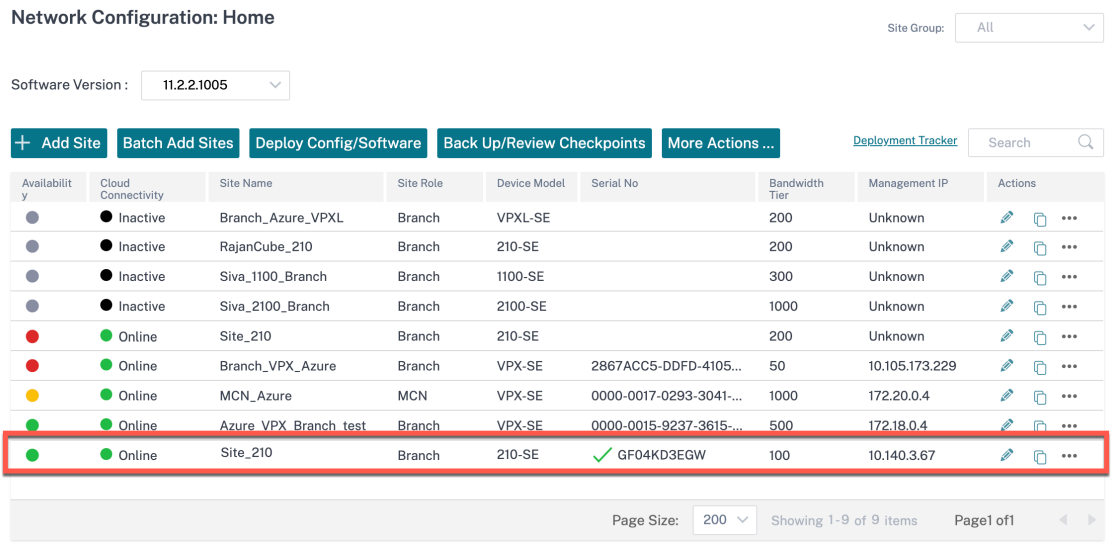
Citrix SD-WAN Orchestrator サービスを使用すると、ネットワーク内のすべての LTE サイトを構成および管理できます。これには、内蔵 LTE モデムまたは外部 USB LTE モデムを介して接続されたアプライアンスが含まれます。

ネットワークで LTE サイトを構成するには、次の手順を実行します。

1. サイトレベルで、[構成] **>** [サイト構成] に移動します。

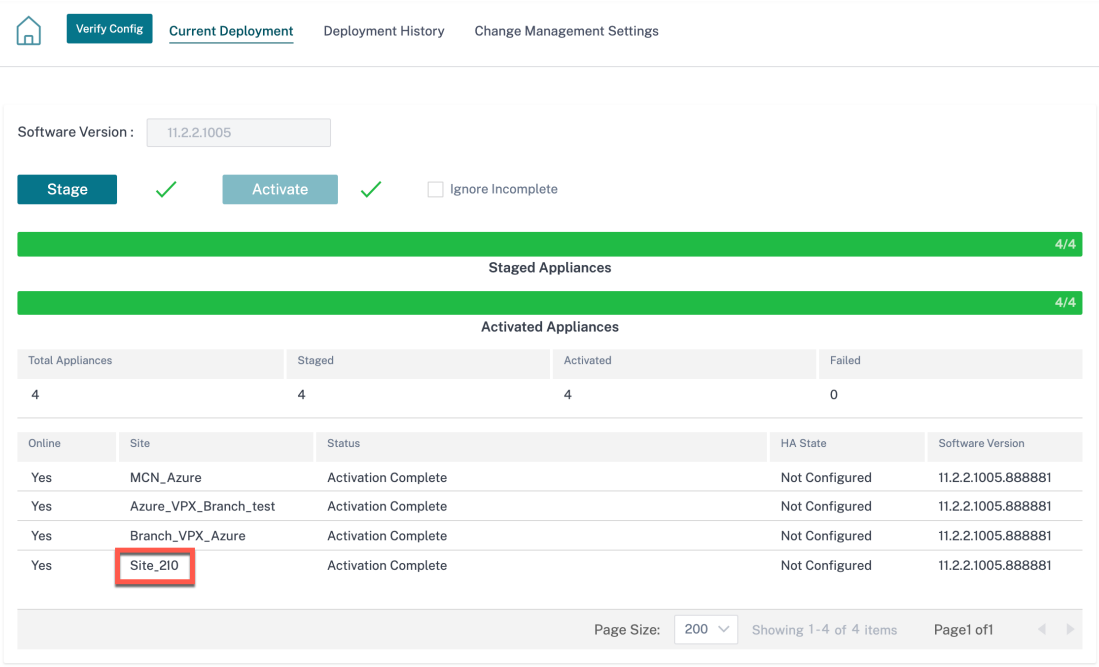


2. サブモデルを **LTE** としてその他の必要な詳細情報とともに選択し、[保存] をクリックします。サイト構成の詳細については、「サイト構成」を参照してください。
3. サイトを作成したら、ネットワーク設定のホームページに移動し、「構成/ソフトウェアの展開 **」ボタンをクリックします。



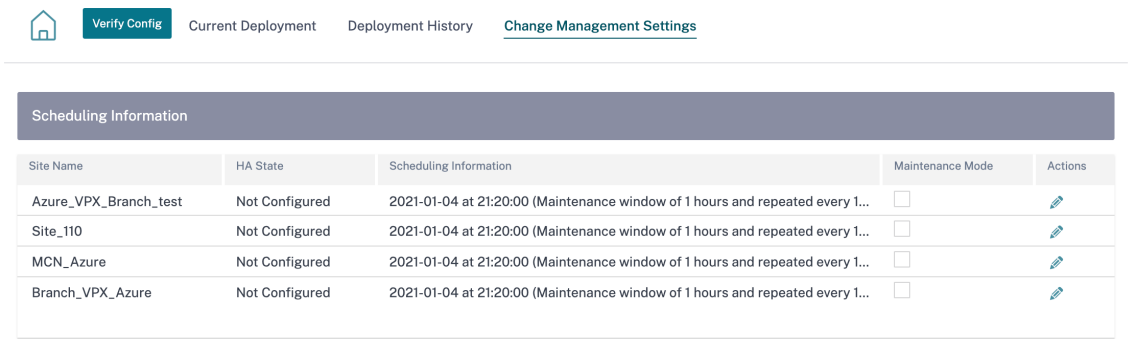
> C
>
> 注:
>
> 現在、LTE のサポートは Citrix SD-WAN 210 アプライアンスで利用できます。

4. ソフトウェアバージョンフィールドには最新のソフトウェアバージョンパッケージが自動的に入力され、このフィールドは編集できません。**Stage** をクリックすると、選択したソフトウェアバージョンに適切な LTE ファームウェアがすべてダウンロードされます。



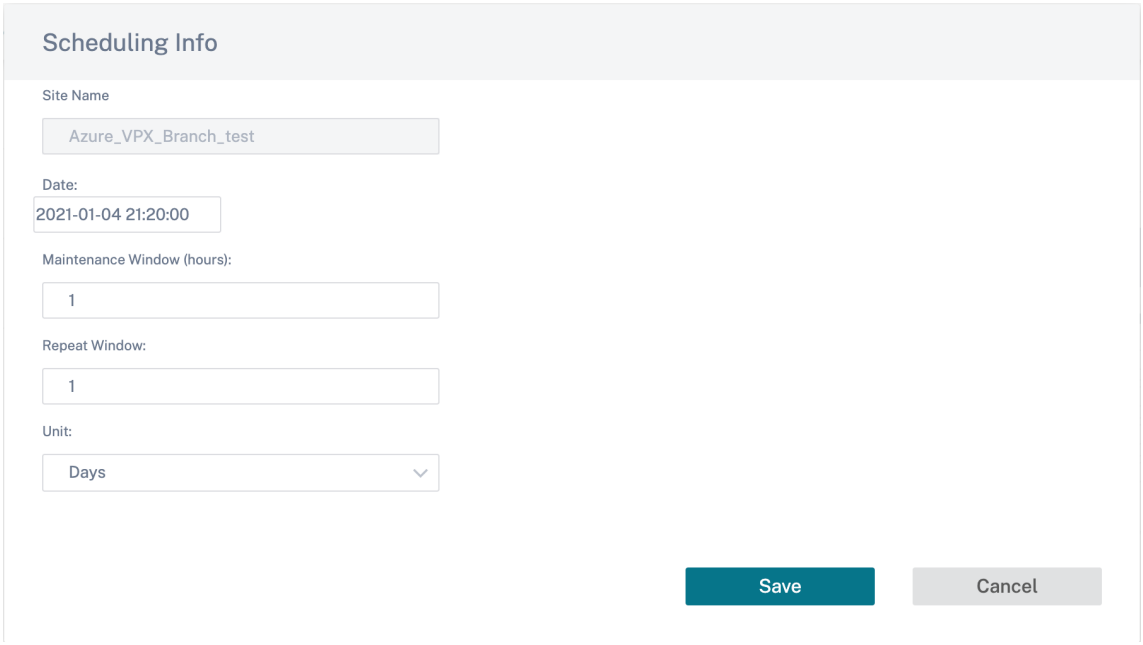
ステージングを完了するには数分かかります。ステータスを表示して、ステージングの進行状況を追跡できます。最初はステータスに「ステージング待ち」、次に「アプライアンスソフトウェアのダウンロード」、最後に「ステージング完了」と表示されます。Cancel Stage ボタンをクリックすると、いつでもステージングをキャンセルできます。

5. ステージングが完了したら、[**Activate**] ボタンをクリックしてソフトウェアをアクティベートします。
6. LTE ソフトウェアのアクティベーションは、スケジューリングウィンドウの一部です。LTE ソフトウェアをアップグレードするには、「変更管理設定」タブに移動します。スケジュール情報およびアクションオプションを含むサイト名のリストを表示できます。



スケジューリングウィンドウでは、LTE ソフトウェアのアップグレードを完了するための特定の時間枠が指定されます。

7. アクション記号をクリックし、スケジュール情報（日付と時刻、メンテナンスウィンドウの期間（時間）、繰り返しウィンドウを日/週/月単位で指定します。［保存］をクリックします。



タイミングが設定されると、情報がアプライアンスに伝播されます。アプライアンスの時刻がスケジュールウィンドウで設定された時刻と一致すると、LTE ファームウェアがアップグレードされます。スケジュールウィンドウでは、LTE ファームウェアをアップグレードする特定の時刻を設定できます。スケジュールウィンドウを設定しても、LTE ファームウェアのアップグレードはすぐには開始されません。

> 注:
>
> すべてのアプライアンスについて、以下はすでに設定されているデフォルトのスケジュール情報です。
>
> - スケジュールウィンドウ -21:20:00
> - メンテナンスウィンドウ -1 時間
> - 繰り返しウィンドウ - 1
>
> 日そのため、変更管理の設定を行わなければ、スケジュールウィンドウが自動的に更新を処理します。また、メンテナンスウィンドウ (時間) の値を **0** に設定すると、LTE ファームウェアのアップグレードが直ちに行われます。

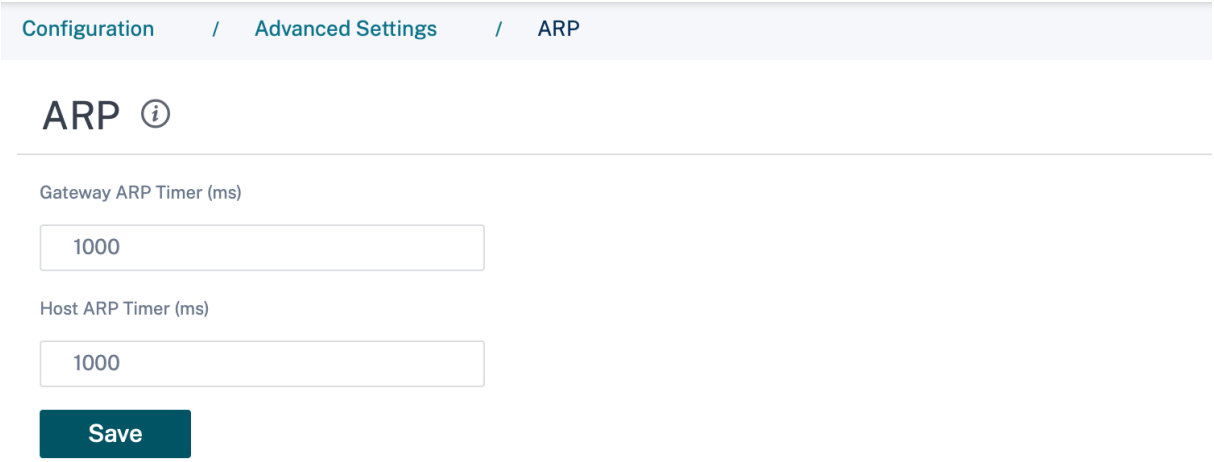
11.1.0 以降、サイトインターフェイスグループページに、インバンド管理設定用の新しい設定ノブが追加されます。これは、インバンド IP を介して管理する必要があるすべてのアプライアンスの必須設定です。Citrix SD-WAN Orchestrator サービスでこの構成がないと、アプライアンスがオフラインになる可能性があります（LTE 経由で管理されていた 210 と 110 が 11.1.0 にアップグレードする場合は特に重要です）。

アドレス解決プロトコル

October 26, 2022

ゲートウェイやワンアームなどの Citrix SD-WAN 展開では、アドレス解決プロトコル（ARP）要求が頻繁に受信されると、アクセスポイントが過負荷になり、トラフィックフローに影響します。トラフィックの過負荷を解消するには、次の ARP タイマーを設定して ARP 要求を特定の間隔で送信できます。

- ゲートウェイ **ARP** タイマー **(ms)**: 設定済みのゲートウェイ IP アドレスに対する ARP リクエスト間の時間 (範囲:100 ～20000 ミリ秒)。
- ホスト **ARP** タイマー **(ms)**: 設定されたホスト IP アドレスの ARP 要求の間隔 (範囲:1000 ～180000 ミリ秒)。



近傍探索プロトコル

October 26, 2022

IPv6 ネットワークでは、Citrix SD-WAN アプライアンスがルーター広告メッセージを定期的にマルチキャストして可用性を通知し、SD-WAN ネットワーク内の隣接するアプライアンスに情報を伝えます。ルータアドバタイズメントには、IPv6 プレフィクス情報が含まれます。Citrix SD-WAN アプライアンスで実行されている近隣探索プロトコル（NDP）は、これらのルーター広告を使用して、同じリンク上の隣接デバイスを特定します。また、NDP は互いのリンク層アドレスを決定し、ネイバーを検索し、アクティブネイバーの到達可能性情報を維持します。

NDP ルーターアドバタイズメントを設定するには、[構成**] > [**詳細設定**] > [NDP**] に移動し、[**+ NDP**] をクリックします。

仮想インターフェイスドロップダウンリストから設定済みの仮想インターフェイスのいずれかを選択します。[アドバタイズメントを有効にする] を選択すると、選択した仮想インターフェイスの定期的なルーターアドバタイズメントの送信とルーター要請への応答が可能になります。

最大、最小、およびルータのライフタイム間隔を指定します。

- **[** 最大間隔]: 定期的な迷惑マルチキャストルータアドバタイズメントを送信するまでの最大許容時間 (秒単位)。

- **Min Interval**：定期的な未承諾マルチキャストルータアドバタイズメントを送信する間隔の最小時間（秒単位）。
- ルーターの有効期間: ルーターがホストによって有効と見なされる時間 (秒単位)。0 はルーターをデフォルトルーターとして使用できないことを示します

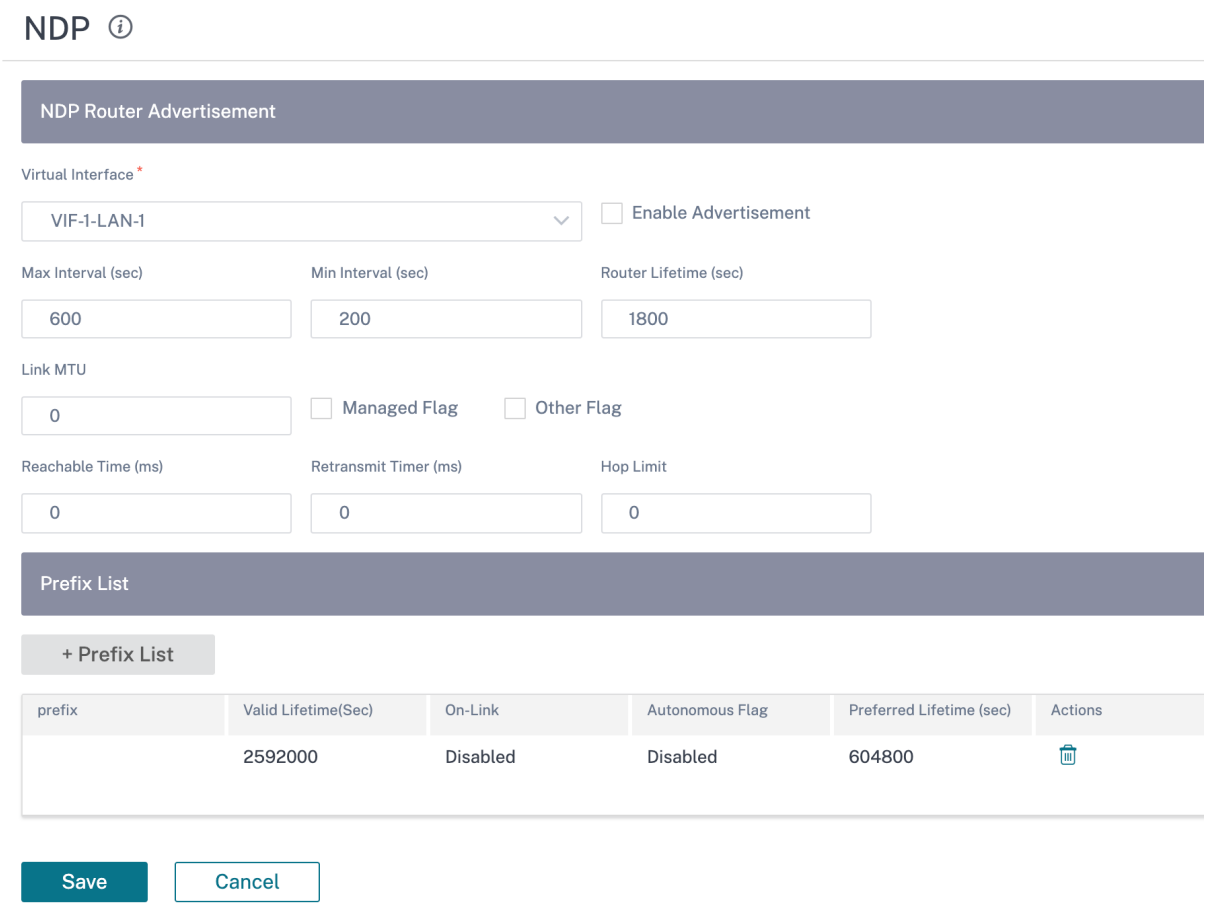
DHCPv6 プロトコルで IP アドレスが使用できる場合は、マネージドフラグを選択します。構成情報 (IP アドレス以外) が DHCPv6 プロトコルで利用できる場合は、「Other **Flag** 」を選択します。

選択したインターフェイスに対して、次の値を指定します。

- リンク **MTU**：インターフェイスの推奨最大伝送ユニット（MTU）。
- 到達可能時間：**NDP** プロトコルが到達可能な状態のままである時間（ミリ秒単位）。
- 再送信タイマー：IP アドレスを解決するか、ネイバーをプローブするときのネイバー送信要求メッセージの再送信間隔（ミリ秒単位）。
- **Hop Limit**：ルータアドバタイズメントに含めるホップの最大数。

[+ プレフィックスリスト] をクリックし、次の値を入力します。

- プレフィクス：クラスレスドメイン間ルーティング（CIDR）表記でのプレフィクスとプレフィクスの長さ。
- 有効有効期間: プレフィックスが有効になるまでの時間（秒）。-1 は無限を表し、プレフィックスが永遠に残ることを意味します。
- オンリンク: 選択すると、プレフィクスはネットワークに対してローカルと見なされます。
- 自律フラグ: 有効にすると、IP アドレスを生成するために、ホストのステートレスアドレス自動構成 (SLAAC) によってプレフィクスが使用されます。
- プレフィクス有効期間: プレフィクスが優先と見なされるまでの時間（秒単位）。



仮想パス

October 26, 2022

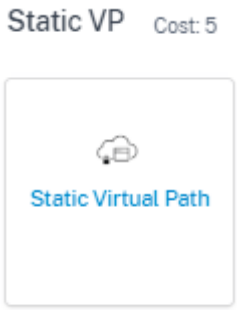
仮想パスは、2 つの WAN リンク間の論理リンクです。これは、2 つの SD-WAN ノード間で高いサービス・レベルの通信を提供するために結合された WAN パスの集合で構成されます。これは、変化するアプリケーション需要と WAN 条件を常に測定し、適応させることによって行われます。SD-WAN アプライアンスは、パスごとにネットワークを測定します。仮想パスは、静的（常に存在）または動的（2 つの SD-WAN アプライアンス間のトラフィックが設定されたしきい値に達したときにのみ存在）にすることができます。

静的仮想パス

仮想パスの設定は、グローバルな WAN リンク自動パス設定から継承されます。これらの構成を上書きし、メンバーパスを追加または削除できます。サイトおよび適用された QoS プロファイルに基づいて、仮想パスをフィルタリングすることもできます。WAN リンクの状態を判断するために ping を送信できる WAN リンクのトラッキング IP ア

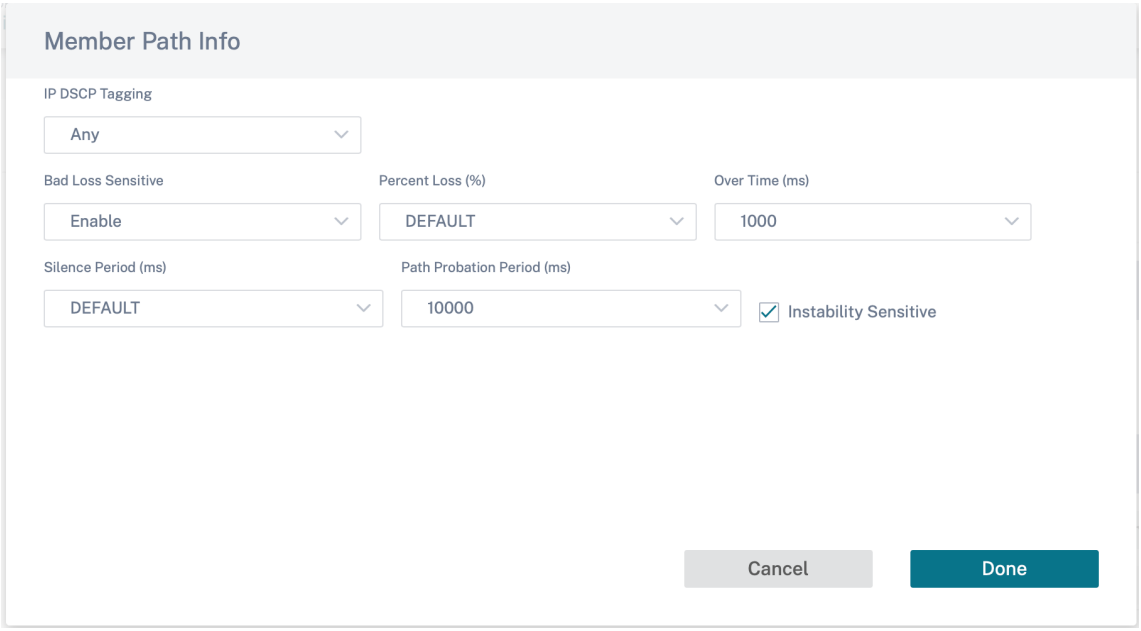
ドレスを指定します。逆方向パスの状態を特定するために ping を実行できるリバースパスのリバーストラッキング IP を指定することもできます。

静的仮想パスを構成するには、サイトレベルから、[構成] > [詳細設定] **> [**** 仮想パス] > [****** 静的仮想パス] に移動します。



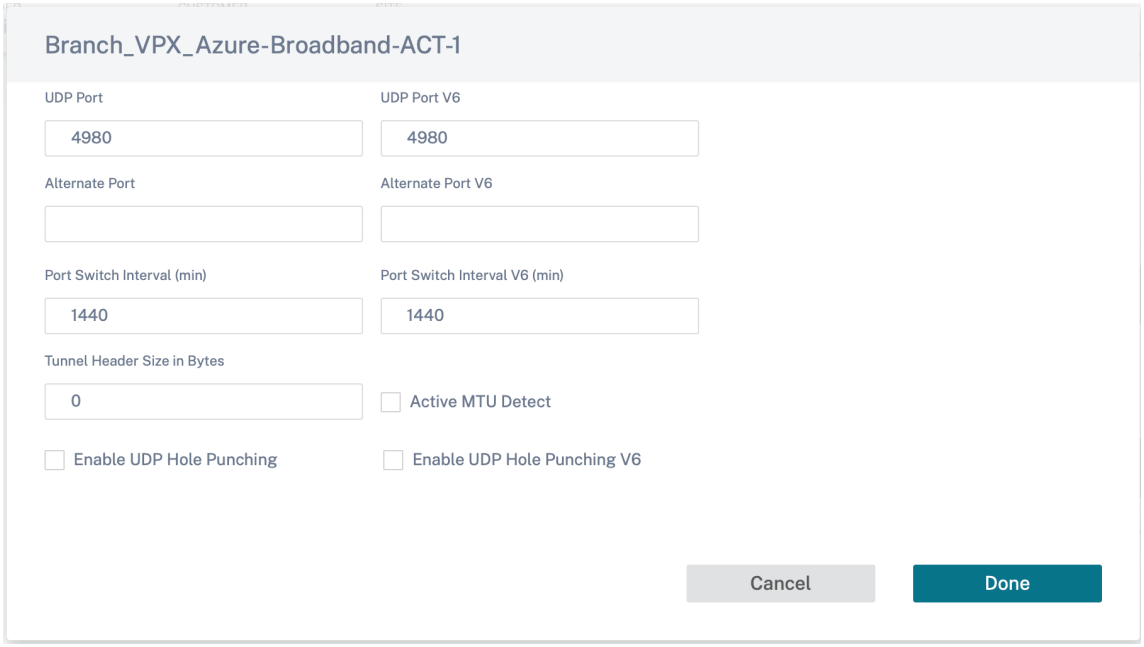
アクティブなメンバーパスは [アクティブメンバーパス] セクションに一覧表示され、メンバーパス設定を表示または編集できます。

- **IP DSCP** タギング: 仮想パス制御プロトコル (VPCP) フレームの外部 IP ヘッダーのタグ。
- **Loss Sensitive**: 有効にすると、損失が原因でパスが BAD としてマークされ、パススコアに遅延ペナルティが生じることがあります。パスを BAD としてマークするのに必要な時間における損失の割合を設定します。帯域幅の損失が許容できない場合は、このオプションを無効にします。
- 損失率: 設定した時間内にパケット損失が設定された割合を超えると、GOOD Path 状態が BAD に変わります。
- **Over Time**: 設定した時間内にパケット損失が設定されたパーセンテージを超えると、パス状態は BAD とマークされます。
- 無音期間: 指定された時間内にパケットが受信されない場合、パスの状態は GOOD から BAD に変わります。
- パスの試用期間: パスの状態が BAD から GOOD に変わるまでの待機期間。
- 不安定性への感受性: 状態が悪いことやその他のレイテンシーの急激な増加によるレイテンシーのペナルティが考慮されます。



選択したアクティブなメンバーパスの WAN リンクの詳細が一覧表示され、必要に応じて設定を変更できます。**UDP** ポート設定は、IPv4 と IPv6 の両方で構成できます。

- **UDP** ポート:LAN から WAN へのパケット転送および WAN から LAN へのパケット転送に使用されるポート。を指定することもできます。
- 代替ポート:UDP ポート切り替えが有効な場合に使用される代替 UDP ポート。
- ポート切り替え間隔:WAN リンクが UDP ポートを切り替える間隔 (分単位)。
- トンネルヘッダーサイズ **(**バイト単位**):** 該当する場合、トンネルヘッダーのサイズ (バイト単位)。
- アクティブな **MTU** 検出: ダイナミック仮想パスの LAN から WAN へのパスは、MTU の有無をアクティブに検出します。
- **UDP** ホールパンチを有効にする:MCN は、互換性のある NAT 保護クライアントサイト間の UDP 接続を支援します。

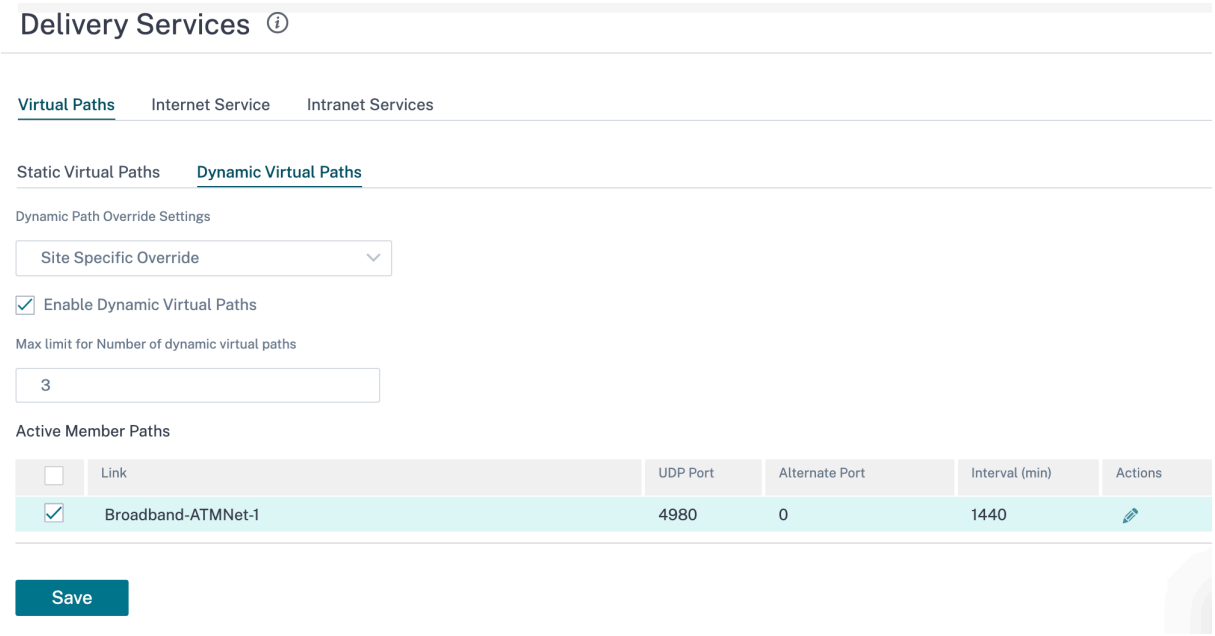


動的仮想パス

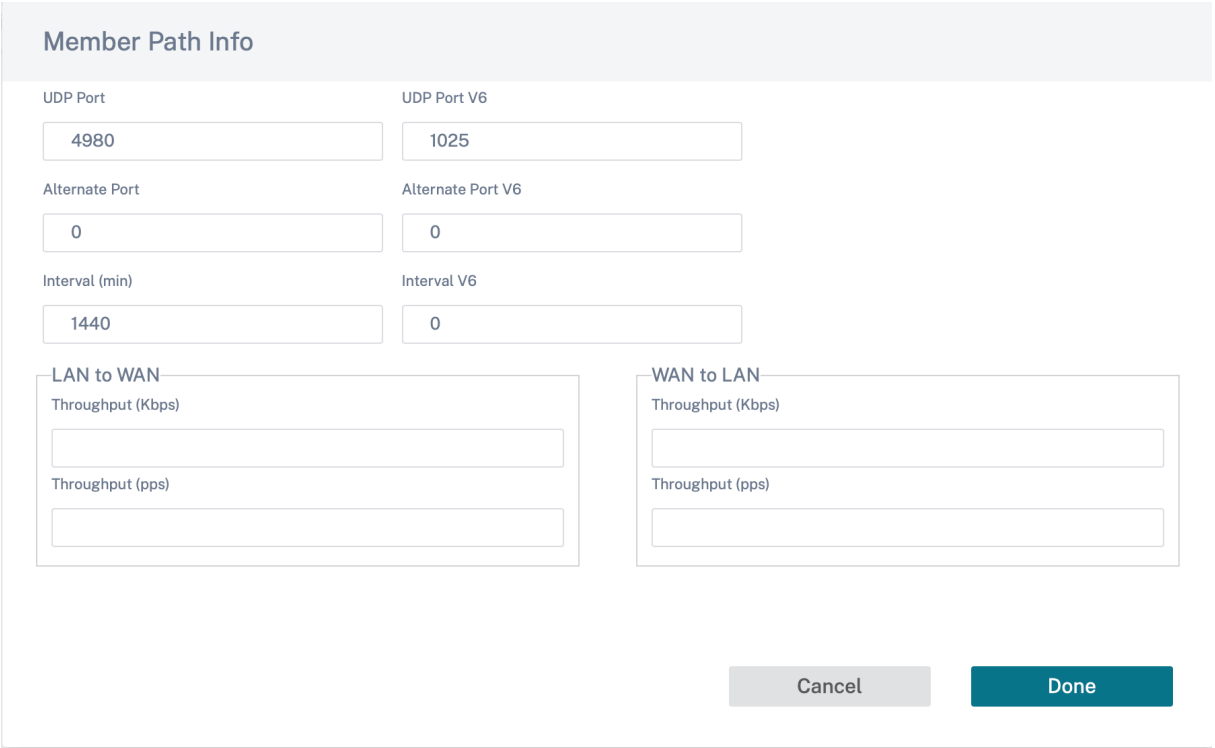
VoIP とビデオ会議の需要により、オフィス間のトラフィックが増加しています。データセンターを介したフルメッシュ接続の設定は、時間がかかり、非効率的です。Citrix SD-WAN では、動的仮想パス機能を使用して、必要に応じてオフィス間のパスを自動的に作成できます。セッションでは、最初に既存の固定パスが使用されます。帯域幅と時間のしきい値が満たされると、新しいパスが固定パスよりも優れたパフォーマンス特性を持つ場合は、新しいパスが動的に作成されます。セッショントラフィックは新しいパスを介して転送されるため、リソースを効率的に使用できます。動的仮想パスは、必要な場合にのみ存在し、データセンターとの間で送受信されるトラフィックの量を削減します。

動的仮想パスを構成するには、サイトレベルから [構成] > [詳細設定] **> [**** 仮想パス] > [****** 動的仮想パス] に移動します。

グローバル **WAN** リンク自動パス設定から継承された仮想パス設定を上書きするには、「グローバルデフォルトを上書き」を選択します。このサイトと中間ノードを介して接続されている他のサイトとの間の動的仮想パスを許可するには、「動的仮想パスを有効にする」を選択します。サイトの動的仮想パスの最大許容値を設定します。



UDP ポートと動的仮想パスのしきい値を設定します。ダイナミック仮想パスが LAN から WAN または WAN から LAN でトリガーされる中間サイトで、スループットしきい値（kbps またはパケット/秒）を指定します。



動的ルーティング

October 26, 2022

ネットワークに SD-WAN アプライアンスを構成および展開した後、接続が確立されると、トラフィックがオーバーレイ SD-WAN ネットワーク経由で適切にリダイレクトされることを確認することが重要です。トラフィックのリダイレクトを確認するには、ping および traceroute 診断ツールを使用します。ping テストと traceroute テストで、アンダーレイパスを介して接続が確立されたことが示された場合、トラフィックのリダイレクトは次のダイナミックルーティングプロトコルを使用して実現できます。

- **Open Shortest Path First (OSPF)**: これは内部ゲートウェイプロトコルであり、企業ネットワークなどの自律システム内のトラフィックをリダイレクトするために使用されます。OSPF は、リンクステートルーティングアルゴリズムを使用してネットワークトポロジの変化を検出し、各ルートの最短パスを最初に計算してパケットを再ルーティングします。MPLS トラフィックをリダイレクトするには、このプロトコルを使用します。詳細については、「**OSPF** 」セクションを参照してください。
- ボーダーゲートウェイプロトコル（**BGP**）: インターネット上のさまざまな自律システム間でトラフィックのルーティングと到達可能性情報をリダイレクトするように設計された外部ゲートウェイプロトコルです。ISP によって決定されたパスに基づいてルーティングを決定できます。このプロトコルを使用して、インターネットトラフィックをリダイレクトします。詳細については、「**BGP** の設定」セクションを参照してください。

以前は、動的ルーティング機能は 1 つのルーター ID でのみ使用できました。設定されているすべてのルーティングドメイン（OSPF と BGP 用）にグローバルに一意のルータ ID を設定することも、ルータ ID を指定しないこともできました。Citrix SD-WAN 11.3.1 リリース以降では、プロトコル全体のルーター ID を構成できるだけでなく、ルーティングドメインごとにルーター ID を構成することもできます。この機能強化により、異なるルータ ID の安定したコンバージェンスを使用して、複数のインスタンス間で安定したダイナミックルーティングを有効にできます。

特定のルーティングドメインにルータ ID を設定する場合、特定のルータ ID がプロトコルレベルのルーティングドメインを上書きします。

OSPF

OSFF を設定するには、[構成] **>** [詳細設定] **>** [ダイナミックルーティング] **>** [**OSPF**] に移動します。

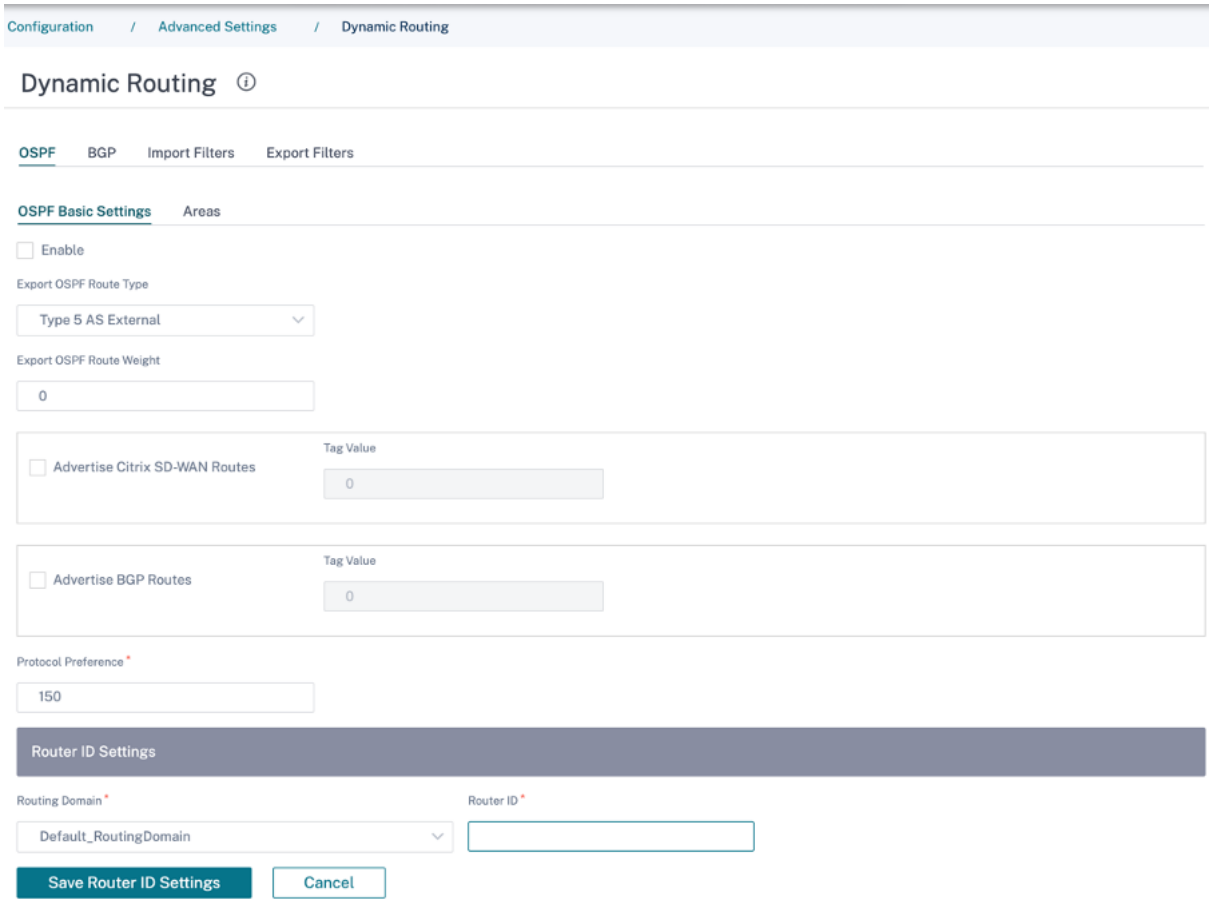
OSPF 基本設定

設定するパラメータは次のとおりです。

- 有効化:SD-WAN アプライアンスの OSPF ルーティングプロトコルが隣接ルーター間で Hello パケットの交換を開始できるようにします。
- ルーター **ID**: OSPF アドバタイズメントに使用される IPv4 アドレス。この情報は入力しなくても構いません。指定されていない場合は、ルーティングに参加している仮想インターフェイスの中で最も低い仮想 IPv4 アドレスが選択されます。IPv6 インターフェースでは、IPv4 形式でルーター ID を指定する必要があります。たとえば、1.1.1.1 と入力します。

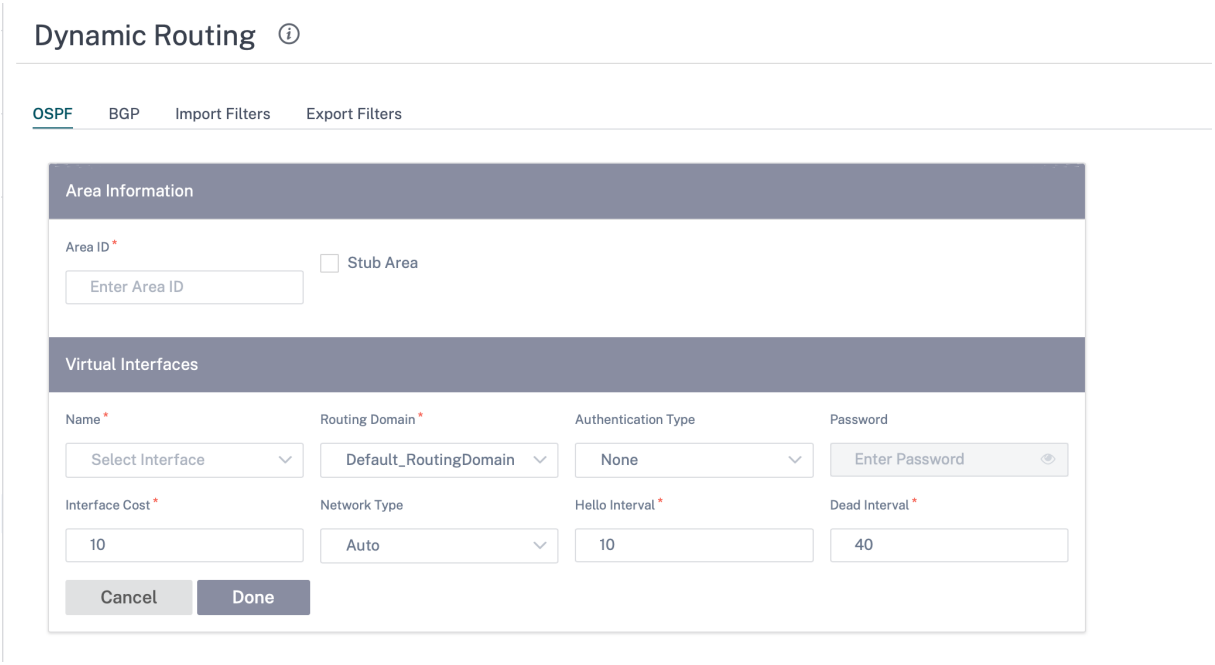
  > 注
  >
  > - IPv4 ネットワークでは、ルーター ID の設定はオプションです。ただし、IPv6 ネットワークの場合、ルーター ID の設定は必須です。IPv6 ネットワークのルーター ID は、同じ IPv4 形式 (32 ビット表記) で設定する必要があります。
  >
  >   * 学習用とアドバタイズ用に、同じルーターへの IPv4 ピアリングと IPv6 ピアリングを個別に作成する必要があります（該当する場合）。

- **OSPF** ルートタイプのエクスポート： SD-WAN ルートを OSPF ネイバーにタイプ 1 のエリア内ルートまたはタイプ 5 の外部ルートとしてアドバタイズします。
- **OSPF** ルートウェイトのエクスポート： OSPF ネイバーにアドバタイズされるコストは、元のルートコストとここで設定したウェイトです。
- **SD-WAN** ルートのアドバタイズ:SD-WAN ルートをピアネットワーク要素にアドバタイズします。
- **BGP** ルートのアドバタイズ:OSPF ドメインへの BGP ルートの再配布を可能にします。



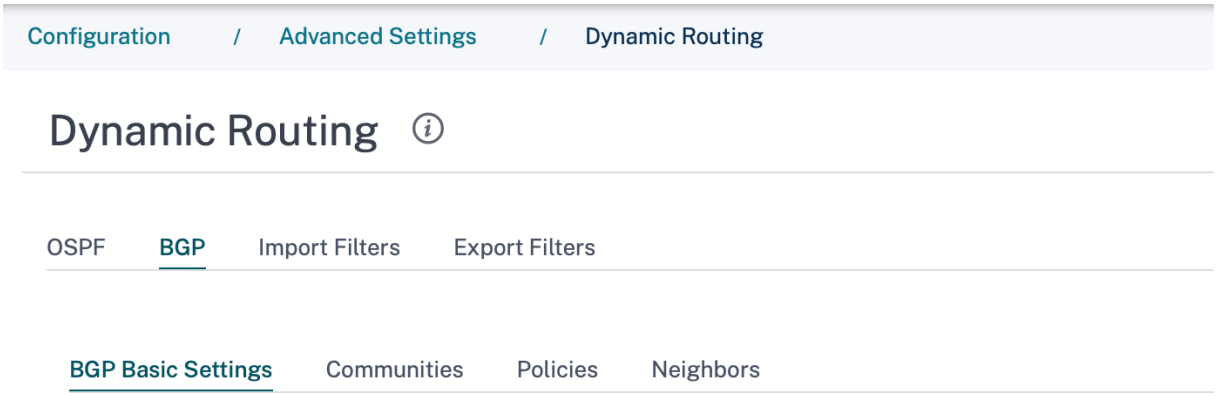
エリア

+ Area をクリックし、OSPF がルートを学習してルートをアドバタイズするネットワークのエリア ID を入力します。スタブエリアにより、このエリアは指定された自律システムの外部からのルートアドバタイズメントを受信しません。仮想インターフェイス設定を構成します。



BGP

BGP を設定するには、[設定] > [詳細設定**] > [**ダイナミックルーティング**] > [BGP**] に移動します。



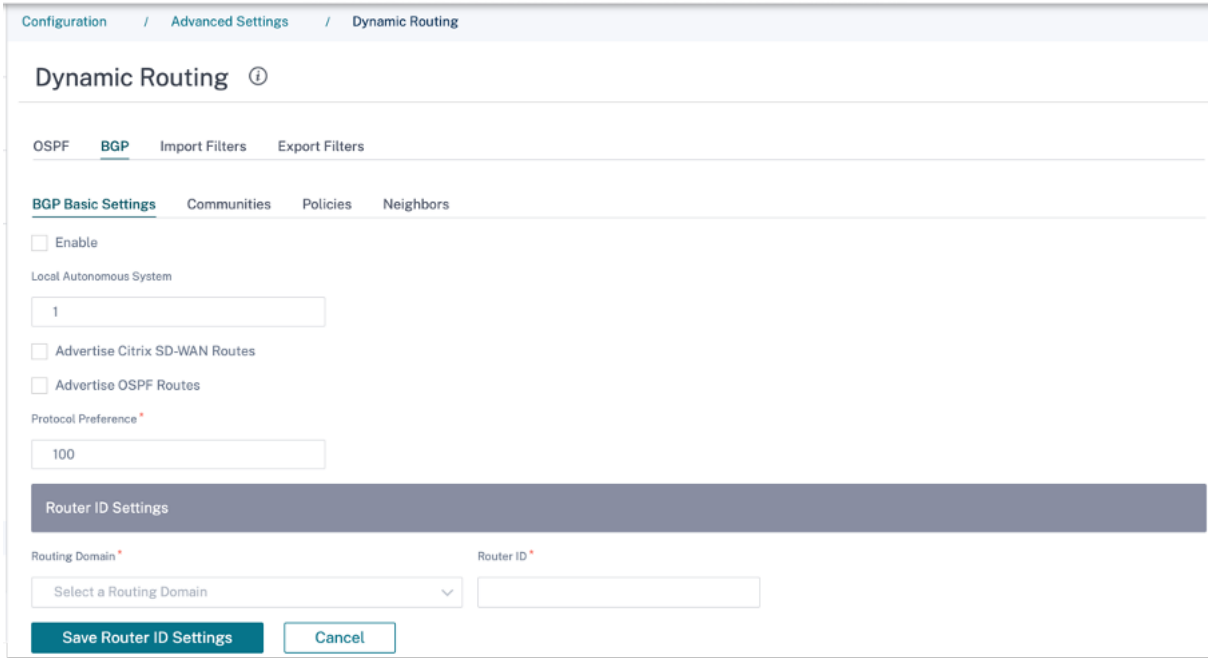
BGP 基本設定

設定するパラメータは次のとおりです。

- 有効化:SD-WAN アプライアンスの BGP ルーティングプロトコルが BGP ピアリングの一部としてオープンメッセージの送信を開始できるようにします。
- ルーター **ID**: BGP アドバタイズメントに使用される IPv4 アドレス。ルータ ID が指定されていない場合は、ルーティングに参加している仮想インターフェイスの最下位の仮想 IPv4 アドレスが選択されます。

> 注
>
> - IPv4 ネットワークでは、ルーター ID の設定はオプションです。ただし、IPv6 ネットワークの場合、ルーター ID の設定は必須です。IPv6 ネットワークのルーター ID は、同じ IPv4 形式 (32 ビット表記) で設定する必要があります。
>
> * 学習用とアドバタイズ用に、同じルーターへの IPv4 ピアリングと IPv6 ピアリングを個別に作成する必要があります（該当する場合）。

- ローカル自律システム:BGP プロトコルが実行されている自律システム番号。
- **SD-WAN** ルートのアドバタイズ:SD-WAN ルートをピアネットワーク要素にアドバタイズします。
- **OSPF** ルートのアドバタイズ:OSPF ルートを BGP ドメインに再配布できるようにします。

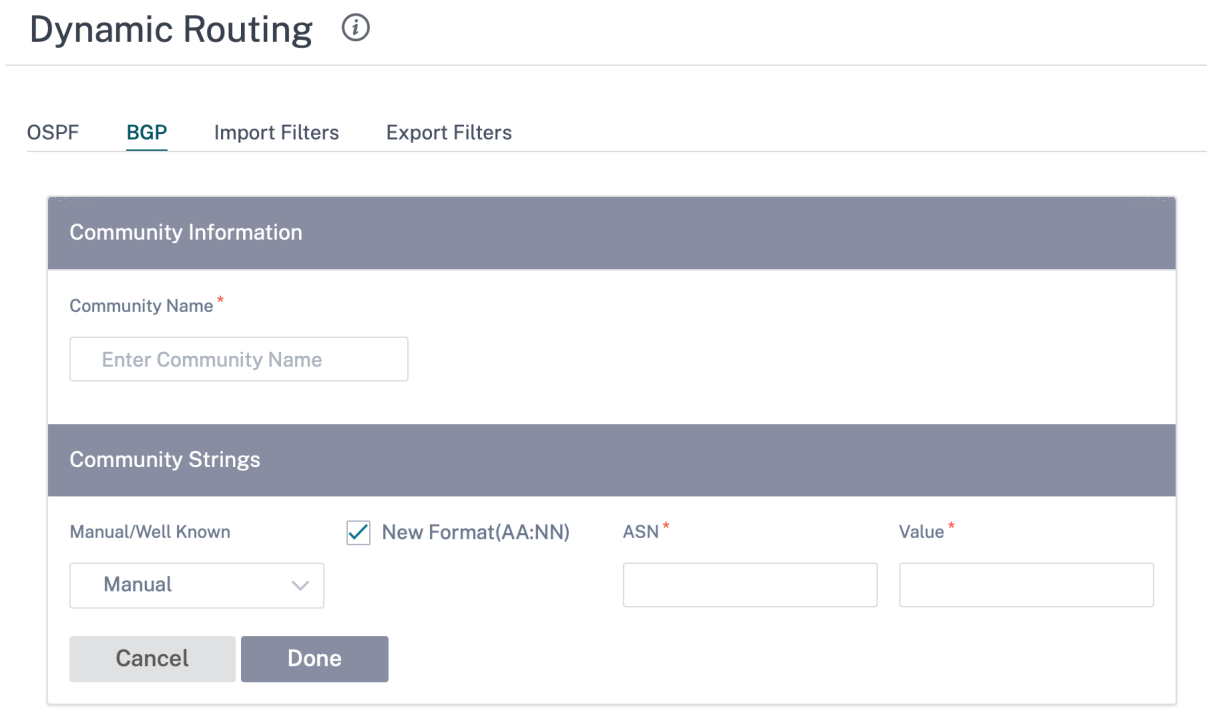


コミュニティ

[**+** コミュニティ] をクリックしてコミュニティを追加します。ルートフィルタリングに使用できる BGP コミュニティの集合。コミュニティリストは、一致するルートのコミュニティを設定または変更するためにも使用できます。

ポリシーごとに、ユーザは複数のコミュニティストリング、AS-PATH-PREPEND、**MED** 属性を設定できます。ユーザーは、ポリシーごとに最大 10 の属性を設定できます。

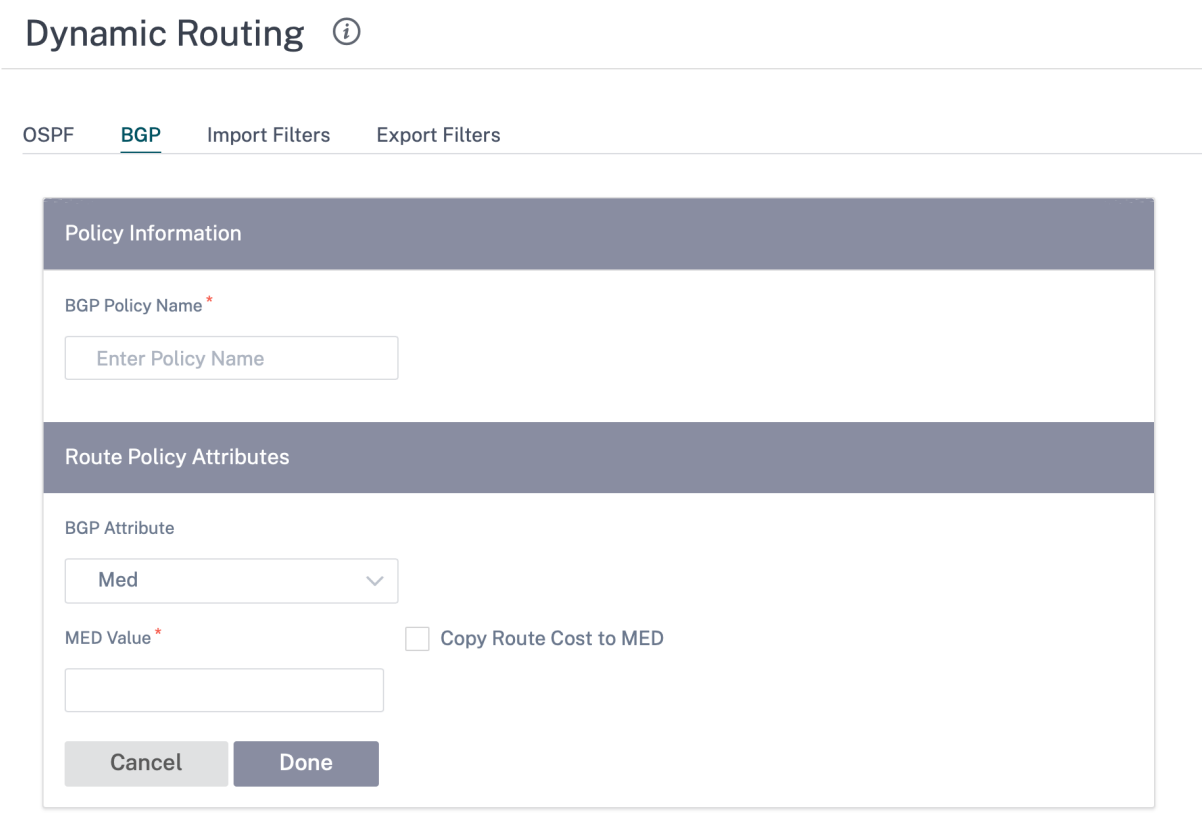
コミュニティの名前を指定し、アドバタイズするコミュニティストリングを入力します。



- コミュニティ名: コミュニティ名を入力します。
- 手動/既知:BGP コミュニティを手動で設定するか、リストから標準の既知の BGP コミュニティを選択します。
- 新しい形式 **(AA: NN)**: 新しい形式を使用して BGP コミュニティを設定するには、このチェックボックスを選択します。
- **ASN**: 新しい構成形式を使用する場合の BGP コミュニティの最初の 16 桁。
- 値:BGP コミュニティ値を入力します。

ポリシー

各 BGP ピアのルート属性の設定または変更に使用できる BGP 属性の集合。いずれかの方向（インポートまたはエクスポート）で、ネイバー単位でネットワークセットに選択的に適用する BGP ポリシーを作成します。SD-WAN アプライアンスは、サイトごとに 8 つのポリシーをサポートし、1 つのポリシーには最大 8 つのネットワークオブジェクト（または 8 つのネットワーク）が関連付けられています。

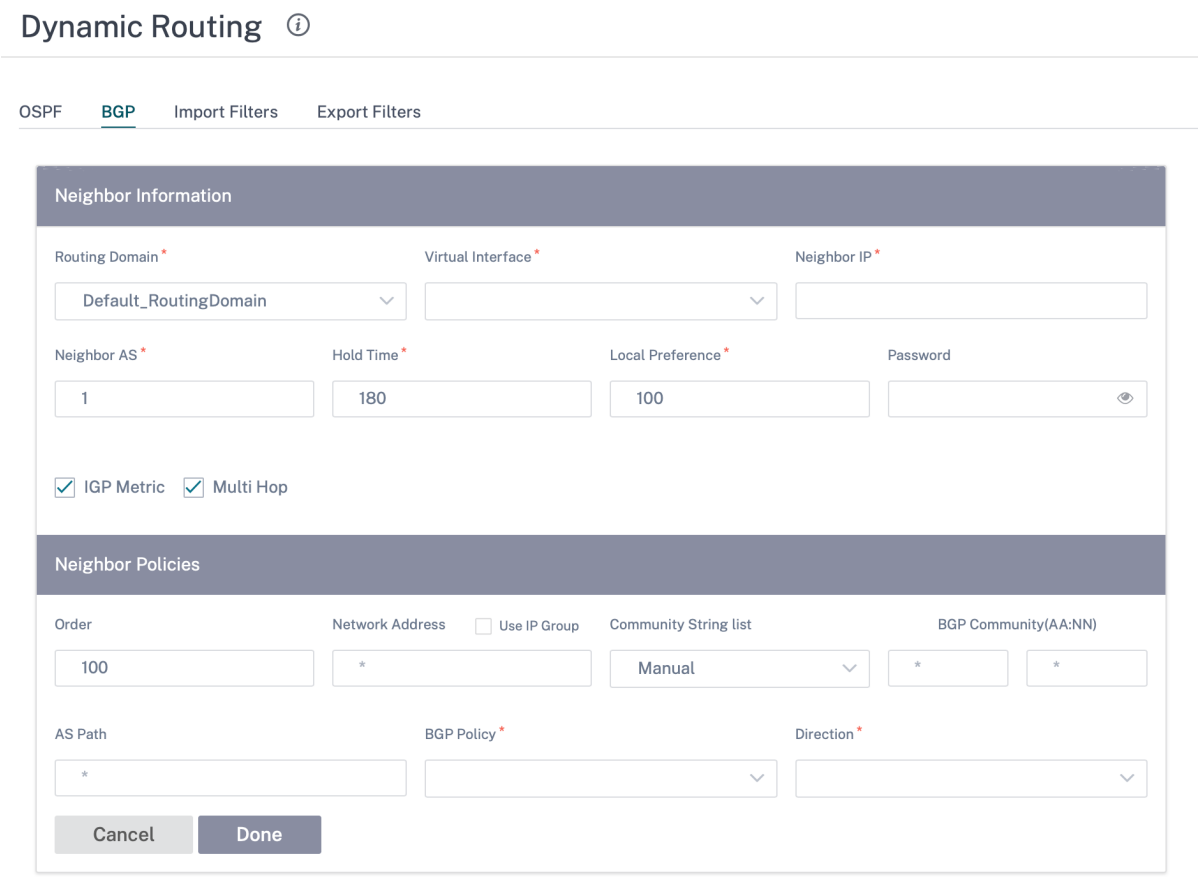


- **BGP** ポリシー名:BGP ポリシー名を入力します。
- **BGP** 属性: リストから BGP 属性を選択し、必要な情報を入力します。

隣人

ネイバーは、ルーティングの最短パスを検出するためにチェックされる、設定された BGP ピアルータのすべてです。すべてのネイバーは、同じ自律システムの一部である必要があります。

+ Neighbor をクリックして、ネイバールータ用の設定済みの BGP ポリシーを追加します。このポリシーが着信ルートまたは発信ルートに適用されているかどうかを示す方向を指定できます。



ルートフィルタリング

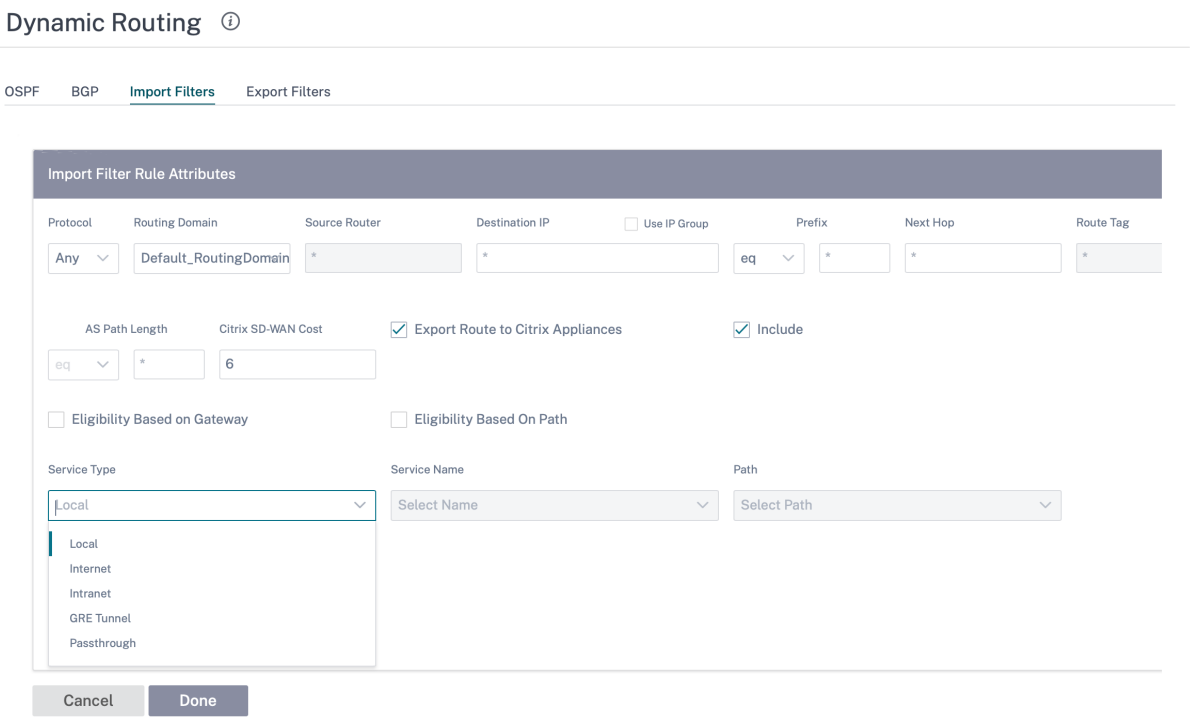
ルート学習が有効なネットワークでは、Citrix SD-WAN Orchestrator を使用すると、すべてのルートをアドバタイズして受け入れないよりも、どの SD-WAN ルートをルーティングネイバーにアドバタイズし、どのルートをルーティングネイバーから受信するかをより細かく制御できます。

フィルタのインポート

インポートフィルタは、特定の一致基準に基づいて OSPF および BGP ネイバーを使用して受信したルートを受け入れるか、受け付けないかに使用します。インポートフィルタルールは、SD-WAN ルートデータベースにダイナミックルートをインポートする前に満たす必要があるルールです。デフォルトでは、ルートはインポートされません。

フィルタを設定して、ルートラーニングがどのように行われるかを微調整できます。

[**+** ルールをインポート] をクリックします。



作成する各エクスポートフィルタを作成するには、次の基準を使用します。

フィールド条件	説明	値
Protocol	ルートの学習に使用するルーティングプロトコル。ドロップダウンリストからプロトコルを選択します。	任意、OSPF、BGP
ルーティングドメイン	ドロップダウンリストからルーティングドメインを入力します。	• ルーティングドメイン名
送信元ルータ	送信元ルータの IP アドレス。iBGP だけに適用されます。	• IP アドレス
接続先 IP	ルートの宛先の IP アドレスとサブネットマスク	• IP アドレス
IP グループを使う	必要に応じて [**IP** グループを使用] チェックボックスを選択します。	-IP グループ
前	プレフィクスでルートを照合するには、メニューから一致述語を選択し、隣接するフィールドに Route プレフィクスを入力します。	• eq: 等しい,- lt: より小さい,- le: より小さい,- gt: より大きい,- ge: より大きい
次ホップ	ネクストホップの IP アドレス	• IP アドレス

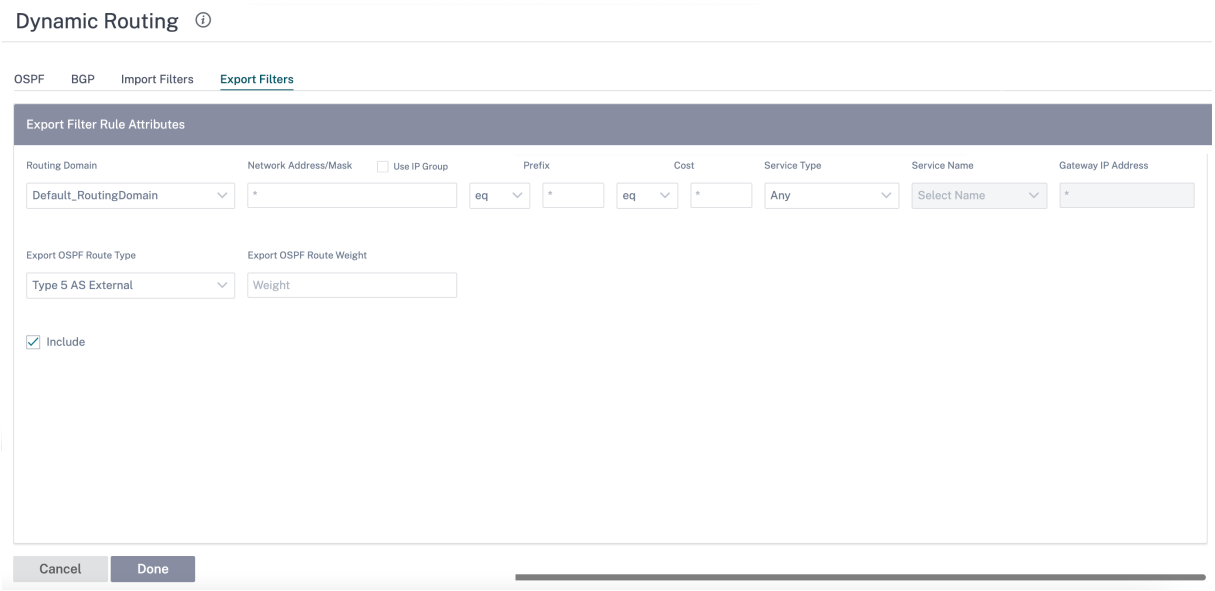
フィールド条件	説明	値
ルートタグ	フィルタが一致する OSPF ルートタグ。OSPF ルートタグにより、OSPF と他のプロトコル間の相互再配布中のルーティングループを防止	数値
コスト	インポート用の OSPF ルートの照合に使用されるルートコスト	数値
AS パスの長さ	インポート用の BGP ルートの照合に使用される AS パスの長さ	数値
Citrix アプライアンスへのルートのエクスポート	チェックボックスを選択してこのフィルターを有効にします。それ以外の場合、フィルタは無視されます	なし
含める	[このフィルタに一致するルートを含める] チェックボックスをオンにします。それ以外の場合、一致するルートは無視されます	なし
ゲートウェイに基づく資格	このチェックボックスを選択し、ドロップダウンリストからサービスタイプ、サービス名、パスを指定します。	サービスタイプ (ローカル、インターネット、イントラネット、GRE トンネル、パススルー)、サービス名、パス
パスに基づく資格	このチェックボックスを選択し、ドロップダウンリストからサービスタイプ、サービス名、パスを指定します。	サービスタイプ (ローカル、インターネット、イントラネット、GRE トンネル、パススルー)、サービス名、パス

[完了] をクリックして設定を保存します。

フィルタのエクスポート

エクスポートフィルタは、特定の一致基準に基づいて OSPF および BGP プロトコルを使用してアドバタイズメント用のルートを含めるか除外するために使用されます。エクスポートフィルタルールは、動的ルーティングプロトコル経由で SD-WAN ルートをアドバタイズする際に満たす必要があるルールです。デフォルトでは、すべてのルートがピアにアドバタイズされます。

[**+** ルールをエクスポート] をクリックします。



作成する各エクスポートフィルタを作成するには、次の基準を使用します。

フィールド条件	説明	値
ルーティングドメイン	ドロップダウンリストからルーティングドメインを選択します。	ルーティングドメイン
ネットワークアドレス/マスク	ルートのネットワークを説明する設定済みのネットワークオブジェクトの **IP** アドレスとサブネットマスクを入力します。	• IP アドレス
IP グループを使う	必要に応じてチェックボックスを選択し、ドロップダウンリストから IP グループを入力します。	• IP グループ
前	プレフィクスでルートを照合するには、メニューから一致述語を選択し、隣接するフィールドに Route プレフィクスを入力します。	• eq: 等しい,- lt: より小さい,- le: より小さい,- gt: より大きい,- ge: より大きい
コスト	エクスポートされたルートの選択を絞り込むために使用される方法（述語）と SD-WAN ルートコスト	数値
サービスの種類	Citrix SD-WAN サービスのリストから、一致するルートに割り当てられるサービスタイプを選択します。	任意、ローカル、仮想パス、インターネット、イントラネット、LAN GRE トンネル、LAN IPsec トンネル

フィールド条件	説明	値
サイト/サービス名	イントラネット、LAN GRE トンネル、および LAN IPsec トンネルの場合は、使用する構成済みのサービスタイプの名前を指定します。	テキスト文字列
Gateway IP アドレス	サービスタイプとして LAN GRE トンネルを選択した場合は、トンネルの Gateway IP を入力します。	IP アドレス
OSPF ルートタイプのエクスポート	Citrix SD-WAN ルートを OSPF ネイバーにタイプ 1 エリア内ルートまたはタイプ 5 外部ルートとしてアドバタイズします。デフォルトルートは常に、ノーマルエリアへのタイプ 5 外部ルート、スタブエリアへのタイプ 3 サマリールートとしてアドバタイズされます。	ルートタイプ
OSPF ルートウェイトのエクスポート	Citrix SD-WAN ルートを OSPF にエクスポートする場合、各ルートの Citrix SD-WAN コストへの重みを合計コストとします。	重要度
含める	[このフィルタに一致するルートを含める] チェックボックスをオンにします。それ以外の場合、一致するルートは無視されます	なし

ルートフィルタリングは、SD-WAN ネットワーク（データセンター/ブランチ）の LAN ルートおよび仮想パスルートに実装され、BGP と OSPF を使用して SD-WAN 以外のネットワークにアドバタイズされます。

最大 512 のエクスポートフィルタと 512 のインポートフィルタを設定できます。これは、ルーティングドメインごとの制限ではなく、全体的な制限です。

ネットワークアドレス変換

October 26, 2022

SD-WAN アプライアンスのネットワークアドレス変換 (NAT) は、限られた数の登録済み IP アドレスを保持するために IP アドレス保存を実行します。内部ネットワークのプライベートアドレスを合法的なパブリックアドレスに変換し、プライベート SD-WAN ネットワークをパブリックインターネットに接続します。パブリック IP アドレスは、イ

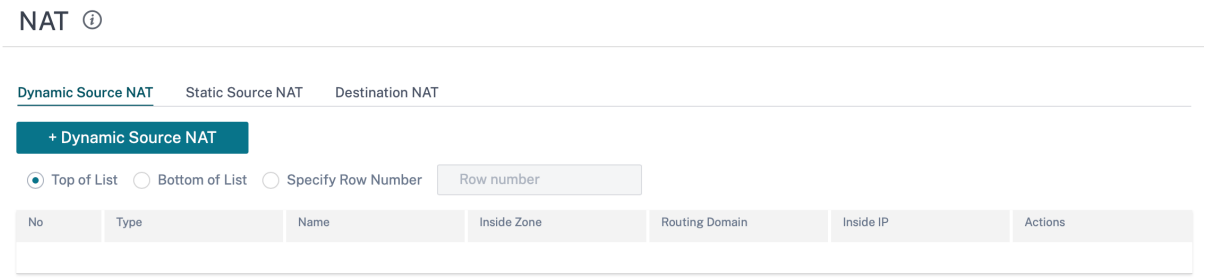
ンターネットを介した通信に使用されます。また、NAT は、ネットワーク全体のアドレスを 1 つだけインターネットにアドバタイズし、内部ネットワーク全体を隠すことで、セキュリティを強化します。

次のタイプの NAT を設定できます。

- ダイナミックソース NAT
- 静的 NAT
- 宛先 NAT

> 注:
>
> NAT 機能はサイトレベルでのみ設定できます。NAT のグローバル構成（テンプレート）はありません。

Citrix SD-WAN Orchestrator サービスを使用してサイトの NAT を構成するには、サイトレベルで [構成] **> [**詳細設定] **> [NAT**] に移動します。



インバウンドおよびアウトバウンド **NAT**

接続の方向は、内側から外側、または外側から内側にできます。NAT ルールを作成したら、受信時チェックボックスを使用して方向を定義できます。このチェックボックスがオンになっている場合、方向は [インバウンド] に設定され、チェックボックスをオフにすると、方向は [アウトバウンド] に設定されます。

- **Inbound**: サービスで受信したパケットについて、送信元アドレスが変換されます。宛先アドレスは、サービス上で送信されるパケットに対して変換されます。たとえば、インターネットサービスから LAN サービスへ—受信したパケット（インターネットから LAN へ）の場合、送信元 IP アドレスが変換されます。送信されたパケット（LAN からインターネットへ）では、宛先 IP アドレスが変換されます。
- **Outbound**: サービスで受信したパケットについて、宛先アドレスが変換されます。送信元アドレスは、サービス上で送信されるパケットに対して変換されます。たとえば、LAN サービスからインターネットサービスへ—送信されたパケット（LAN からインターネット）の場合、送信元 IP アドレスが変換されます。受信パケット（インターネットから LAN へ）の場合、宛先 IP アドレスが変換されます。

ゾーン派生

インバウンドまたはアウトバウンドトラフィックの送信元と宛先のファイアウォールゾーンは同じであってはなりません。送信元と宛先の両方のファイアウォールゾーンが同じ場合、トラフィックに対して NAT は実行されません。

発信 NAT の場合、外部ゾーンはサービスから自動的に派生します。デフォルトでは、SD-WAN 上のすべてのサービスがゾーンに関連付けられます。たとえば、信頼できるインターネットリンク上のインターネットサービスは、信頼できるインターネットゾーンに関連付けられています。同様に、着信 NAT の場合、内部ゾーンはサービスから取得されます。

仮想パスサービスの場合、NAT ゾーンの導出が自動的に行われないため、内部ゾーンと外部ゾーンを手動で入力する必要があります。NAT は、これらのゾーンに属するトラフィックに対してのみ実行されます。仮想パスのサブネット内に複数のゾーンが存在する可能性があるため、仮想パスのゾーンは派生できません。

ダイナミックソース **NAT**

ダイナミックソース **NAT** は、SD-WAN ネットワーク内のプライベート IP アドレスまたはサブネットを SD-WAN ネットワーク外のパブリック IP アドレスまたはサブネットに多対 1 でマッピングすることです。これにより、複数のホストの送信元 IP アドレスを、異なるポート番号の同じパブリック IP アドレスに変換できます。ポート制限 NAT は、内部 IP アドレスとポートのペアに関連するすべての変換に同じ外部ポートを使用します。LAN セグメント内の信頼できる (内部) IP アドレス経由の異なるゾーンおよびサブネットからのトラフィックは、単一のパブリック (外部) IP アドレス経由で送信されます。

> （注
>
> ）ダイナミック NAT 変換では、内部ネットワークから開始されたセッションのすべての相互トラフィックが許可されます。これらの接続をフィルタリングするには、アウトバウンドトラフィックのフィルターポリシーを追加します。

ポートアドレス変換

ダイナミック NAT は、IP アドレス変換とともにポートアドレス変換（PAT）を行います。ポート番号は、どのトラフィックがどの IP アドレスに属しているかを識別するために使用されます。すべての内部プライベート IP アドレスに 1 つのパブリック IP アドレスが使用されますが、各プライベート IP アドレスには異なるポート番号が割り当てられます。PAT は、1 つのパブリック IP アドレスを使用して複数のホストがインターネットに接続できるようにする費用対効果の高い方法です。

Symmetric チェックボックスは PAT 構成を定義します。NAT ルールの設定時に、このチェックボックスがオンになっている場合は Symmetric NAT が設定され、オフにすると、バックエンドで Port Restricted NAT が設定されます。

- ポート制限：ポート制限 NAT は、内部 IP アドレスとポートのペアに関連するすべての変換に同じ外部ポートを使用します。このモードは、通常、インターネット P2P アプリケーションを許可するために使用されます。

- 対称: 対称 NAT は、内部 IP アドレス、内部ポート、外部 IP アドレス、および外部ポートタプルに関連するすべての変換に同じ外部ポートを使用します。通常、このモードは、セキュリティを強化したり、NAT セッションの最大数を拡張するために使用されます。

ポートフォワーディング

ポート転送機能を備えたダイナミック NAT により、外部ネットワークからのトラフィックは、セッションを内部から開始しなくても、内部ネットワーク上の特定のホストやポートにアクセスできます。これは、通常、Web サーバなどの内部ホストで使用されます。

ダイナミック NAT を設定したら、ポートフォワーディングポリシーを定義できます。IP アドレス変換用のダイナミック NAT を設定し、外部ポートを内部ポートにマッピングするポートフォワーディングポリシーを定義します。ダイナミック NAT ポートフォワーディングは、通常、リモートホストがプライベートネットワーク上のホストまたはサーバーに接続できるようにするために使用されます。

ダイナミックソース **NAT** の設定

Citrix SD-WAN Orchestrator サービスを使用してサイトのダイナミック NAT を設定するには、サイトレベルで [構成] **>** [詳細設定] **> [NAT] >** [ダイナミックソース **NAT**] タブに移動します。[**+** ダイナミックソース **NAT**] をクリックします。

- タイプ:NAT ポリシーが適用される SD-WAN サービスタイプ。スタティック NAT でサポートされるサービスタイプは、ローカルサービス、仮想パス、インターネット、イントラネット、インタールーティングドメインサービスです。
- ルーティングドメイン: 選択した変換を適用するルーティングドメインを選択します。
- **IP** アドレスタイプ: 好みに応じて、IPv4 または IPv6 のアドレスタイプを選択します。
- 宛先サービス: サービスタイプに対応するサービスの名前を入力します。
- **Inside Zone**: 変換を許可するために、パケットの送信元となる必要がある内部ファイアウォールゾーンのマッチタイプ。
- **Inside IP/Prefix**: 一致基準が満たされた場合に変換する必要がある内部 IP アドレスとプレフィックス。
- 外部 **IP**: 一致基準が満たされた場合に内部 IP アドレスが変換される外部 IP アドレスとプレフィックス。インターネットサービスおよびイントラネットサービスを使用する発信トラフィックでは、構成された WAN リンク IP アドレスが外部 IP アドレスとして動的に選択されます。
- ポートパリティ: 有効の場合、NAT 接続の外部ポートはパリティを維持します（内部ポートが偶数であっても、外部ポートが奇数の場合は奇数）。
- レスポンダールートのバインド: 非対称ルーティングを回避するために、レスポンストラフィックが受信時と同じサービスを介して送信されるようにします。
- 関連を許可: ルールに一致するフローに関連するトラフィックを許可します。たとえば、ポリシーに一致する特定のフローに関連する ICMP リダイレクション（フローに関連する何らかのタイプのエラーがある場合）。
- **IPsec** パススルー:IPsec (AH/ESP) セッションの変換を許可します。

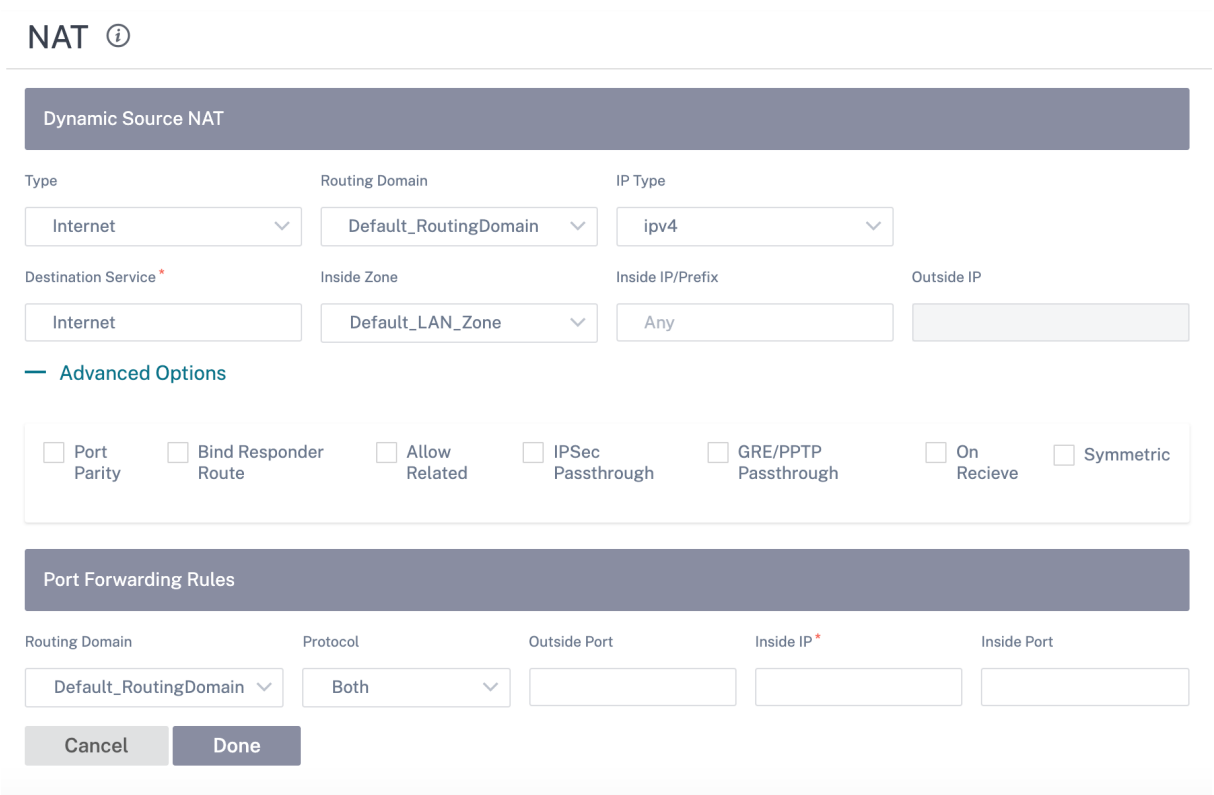
- **GRE/PPTP** パススルー**:** 非対称ルーティングを回避するために、応答トラフィックが受信時と同じサービスを介して送信されるようにします。
- 受信時**:** このチェックボックスがオンになっている場合、インバウンド NAT が設定されます。クリアすると、アウトバウンド NAT が設定されます。
- 対称: このチェックボックスを選択すると、対称 NAT が設定されます。クリアすると、ポート制限付き NAT が設定されます。

ポート転送ルール:

- ルーティングドメイン: 選択した変換を適用するルーティングドメインを選択します。
- プロトコル: TCP、UDP、またはその両方。
- 外部ポート： 内部ポートにポート転送される外部ポート。
- **Inside IP**: 一致するパケットを転送する内部アドレス。
- 内部ポート： 外部ポートが転送される内部ポート。

すべてのポートフォワーディングルールには、親 NAT ルールがあります。外部 IP アドレスは、親 NAT ルールから取得されます。

> 注
>
> Citrix SD-WAN Orchestrator サービス UI には、次の条件が満たされると、自動作成された NAT ルールが表示されます。
>
> - サイトではインターネットサービスが有効になっています。
> - IPv4 アウトバウンドインターネットダイナミックソース NAT ルールがサイトで構成されていません。
> - 少なくとも 1 つの WAN リンクが信頼できないインターフェイス上にあるか、すべてのルーティングドメインでインターネットが有効になっています。



スタティックソース **NAT**

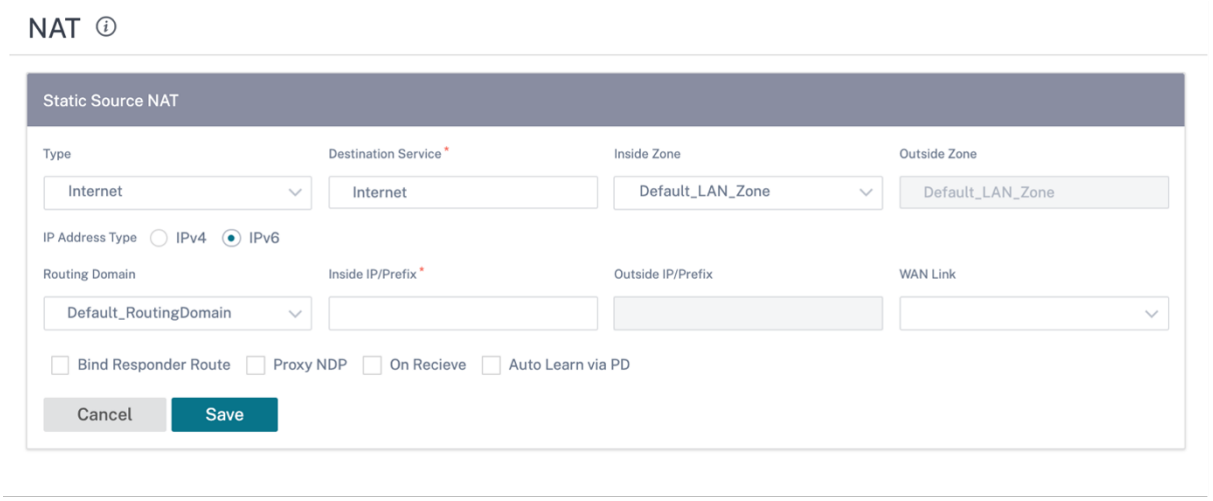
スタティック NAT は、SD-WAN ネットワーク内のプライベート IP アドレスまたはサブネットを、SD-WAN ネットワーク外のパブリック IP アドレスまたはサブネットに 1 対 1 のマッピングです。スタティック NAT を設定するには、内部 IP アドレスと変換先の外部 IP アドレスを手動で入力します。スタティック NAT は、ローカル、仮想パス、インターネット、イントラネット、およびルーティング間ドメインサービスに対して構成できます。

スタティックソース **NAT** の設定

Citrix SD-WAN Orchestrator サービスを使用してサイトの静的 NAT を構成するには、サイトレベルから [構成**] > [**詳細設定**] > [NAT] > [**静的ソース **NAT**] タブに移動します。[**+** スタティックソース **NAT**] をクリックします。

- タイプ:NAT ポリシーが適用される SD-WAN サービスタイプ。スタティック NAT の場合、サポートされるサービスの種類は、ローカル、仮想パス、インターネット、イントラネット、およびインターネットルーティングドメインサービスです。
- 宛先サービス: サービスタイプに対応するサービスの名前を入力します。
- **Inside Zone**: 変換を許可するために、パケットの送信元となる必要がある内部ファイアウォールゾーンのマッチタイプ。
- **Outside Zone**: 変換を許可するために、パケットの送信元となる必要がある外部ファイアウォールゾーンのマッチタイプ。

- **IP** アドレスタイプ: 好みに応じて、IPv4 または IPv6 のアドレスタイプを選択します。
- ルーティングドメイン: 選択した変換を適用するルーティングドメインを選択します。
- **Inside IP/Prefix**: 一致基準が満たされた場合に変換する必要がある内部 IP アドレスとプレフィックス。
- 外部 **IP/**プレフィックス: 一致基準が満たされた場合に内部 IP アドレスが変換される外部 IP アドレスとプレフィックス。
- レスポンダールートのバインド: 非対称ルーティングを回避するために、レスポンストラフィックが受信時と同じサービスを介して送信されるようにします。
- プロキシ **ARP**: アプライアンスが外部 IP アドレスに対するローカル ARP 要求に応答することを保証します。
- プロキシ **NDP**: アプライアンスが外部 IP アドレスに対するローカル NDP 要求に応答することを確認します。
- 受信時**:** このチェックボックスがオンになっている場合、インバウンド NAT が設定されます。クリアすると、アウトバウンド NAT が設定されます。
- **PD** 経由での自動学習: このチェックボックスは、**IP** アドレスタイプとして **IPv6** を選択した場合にのみ有効になります。選択すると、Citrix SD-WAN はアップストリームの委任ルーターにプレフィックスを要求し、委任ルーターは Citrix SD-WAN にプレフィックスで応答します。



IPv6 インターネットサービスのスタティック **NAT** ポリシー

Citrix SD-WAN は、リリース 11.4.0 以降、IPv6 インターネットサービスの静的 NAT ポリシーをサポートしています。IPv6 インターネットサービスのスタティック NAT ポリシーは、内部ネットワークプレフィックスから外部ネットワークプレフィックスへのマッピングを指定します。必要なスタティック NAT ポリシーの数は、内部ネットワークの数と外部ネットワーク（WAN リンク）の数によって異なります。**M** 個の内部ネットワークと **N** 個の **WAN** リンクがある場合、必要なスタティック NAT ポリシーの数は **M x N** です。

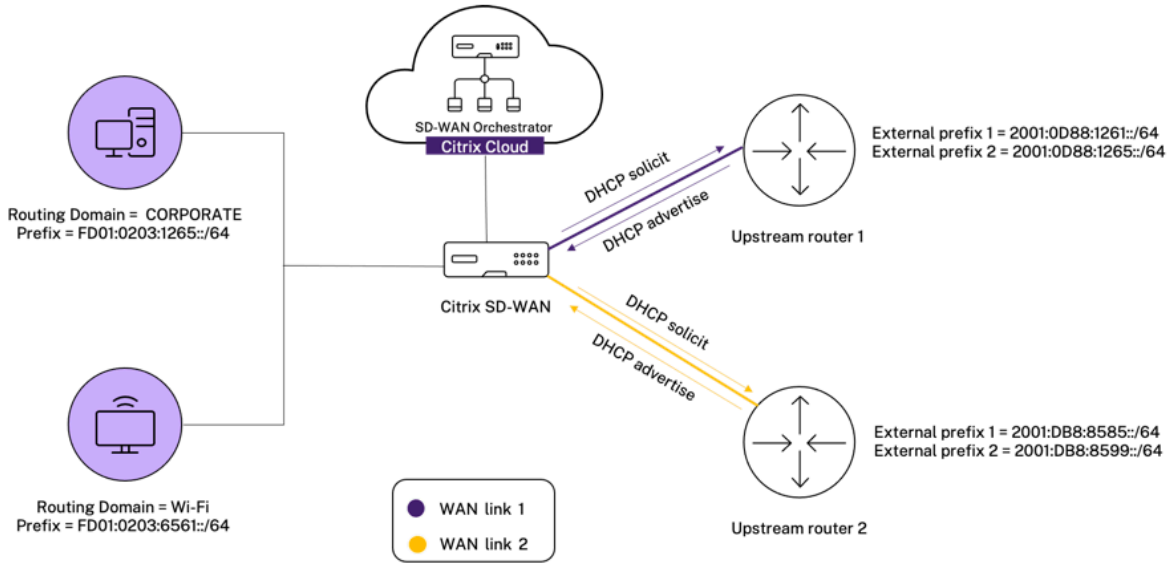
Citrix SD-WAN リリース 11.4.0 以降では、静的 NAT ポリシーを作成するときに、外部 IP アドレスを手動で入力するか、**PD** 経由の自動学習を有効にすることができます。**Auto Learn via PD** が有効になっている場合、SD-WAN アプライアンスは DHCPv6 プレフィックス委任を通じて、アップストリームの委任ルーターから委任されたプレフィックスを受信します。Citrix SD-WAN リリース 11.4.0 より前は、外部 IP アドレスはサービスから自動的に取得され、外部 IP アドレスを手動で入力するオプションはありませんでした。アプライアンスを 11.4.0 以降のリリース

にアップグレードし、IPv6 インターネットサービス用にスタティック NAT ポリシーが設定されている場合は、ポリシーを手動で更新する必要があります。

設定例

次のトポロジでは、Citrix SD-WAN アプライアンスは 2 つの内部ネットワークと 2 つの WAN リンクで構成されます。

- 内部ネットワーク 1 は、ネットワークプレフィクス FD の企業ルーティングドメインに存在します 01:0203:6561 /64
- 内部ネットワーク 2 は、ネットワークプレフィックス FD を持つ Wi-Fi ルーティングドメインに存在します 01:0203:1265 /64
- SD-WAN アプライアンスは、WAN リンク 1 を介して DHCPv6 プレフィクス委任、2 つの委任プレフィックス 2001:0 D 88:1261 /64 および 2001:0 D 88:1265 /64 を介してアップストリーム委任ルータから受信します。これら 2 つの委任プレフィクスは、内部ネットワークからのトラフィックが WAN リンク 1 を通過するときに、外部ネットワークプレフィクスとして使用されます。
- WAN リンク 2 を介して、SD-WAN アプライアンスは DHCPv6 プレフィクス委任を介してアップストリーム委任ルータから、2 つの委任プレフィックス 2001: DB 8:8585 /64 および 2001: DB 8:8599 /64 を受信します。これら 2 つの委任プレフィクスは、内部ネットワークからのトラフィックが WAN リンク 2 を通過するときに、外部ネットワークプレフィクスとして使用されます。



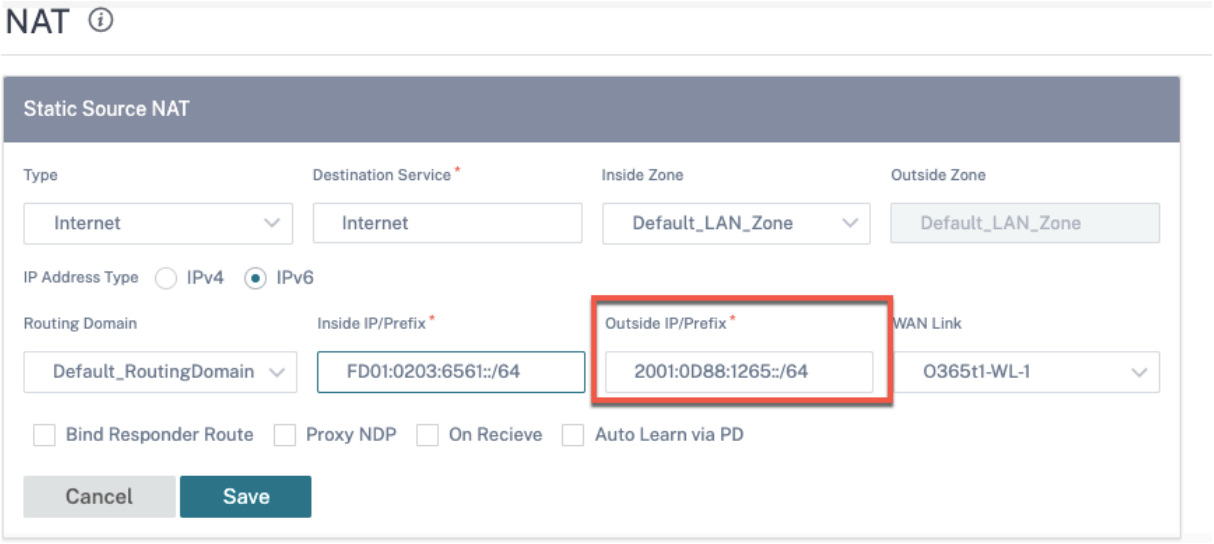
このシナリオでは、M=2 内部ネットワークと N=2 WAN リンクがあります。したがって、IPv6 インターネットサービスを適切に導入するために必要なスタティック NAT ポリシーの数は 2 x 2 = 4 です。次の 4 つのスタティック NAT ポリシーは、次のアドレス変換を指定します。

- 内部ネットワーク 1 から WAN リンク 1 経由
- 内部ネットワーク 1 から WAN リンク 2
- 内部ネットワーク 2 から WAN リンク 1 経由
- 内部ネットワーク 2 から WAN リンク 2 経由

これらのスタティック NAT ポリシーを設定するには、サイトレベルで [設定] > [詳細設定**] > [NAT] > [**スタティックソース **NAT**] に移動します。[**+** スタティックソース **NAT**] をクリックします。

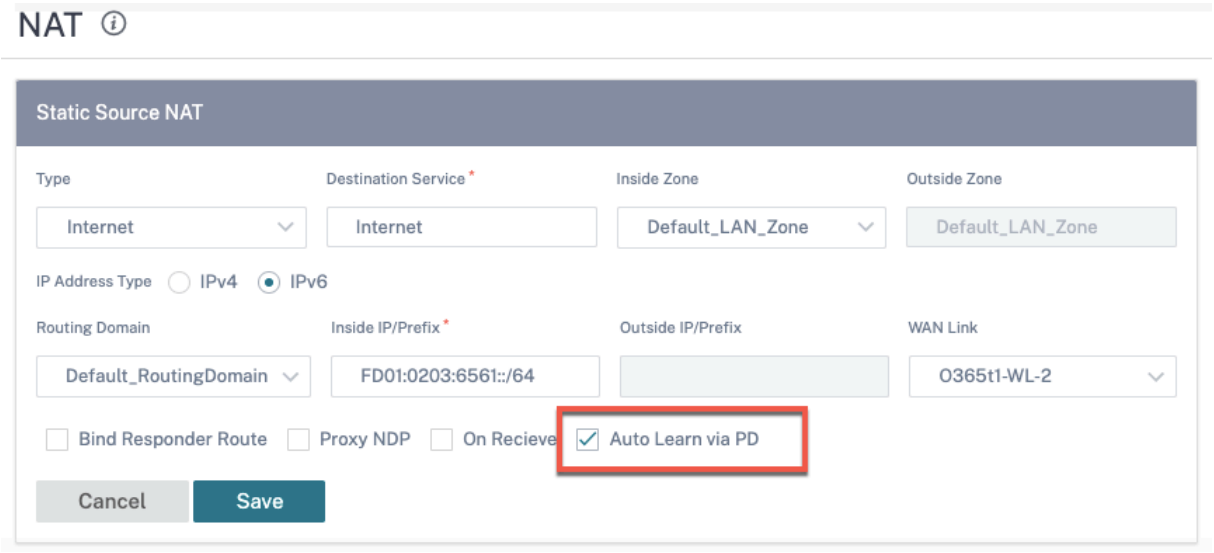
NAT ポリシーを作成するときは、必ず [タイプ] に [インターネット]、[**IP** アドレスタイプ] を [**IPv6**] として選択してください。WAN リンクを選択し、**Inside IP/Prefix** フィールドに内部ネットワークプレフィックスを入力します（/64 プレフィックスのみ使用できます）。「外部 **IP/**プレフィックス」フィールドには、外部ネットワークプレフィックスを手動で入力するか、「**PD** 経由での自動学習」チェックボックスを選択することができます。

次に、外部 IP アドレスがスタティック NAT ポリシーに手動で入力される例を示します。



Auto Learn via PD チェックボックスをオンにする場合は、アップストリームルータが DHCPv6 プレフィックス委任をサポートしていることを確認してください。Citrix SD-WAN はアップストリーム委任ルーターからプレフィックスを要求し、委任ルーターは Citrix SD-WAN にプレフィックスで応答します。Citrix SD-WAN は、この委任プレフィックスを使用して、内部 IP アドレスを外部 IP アドレスに変換します。

次に、**PD** 経由の自動学習が有効になっている例を示します。これにより、DHCPv6 プレフィクス委任によって外部ネットワークプレフィクスが取得されます。



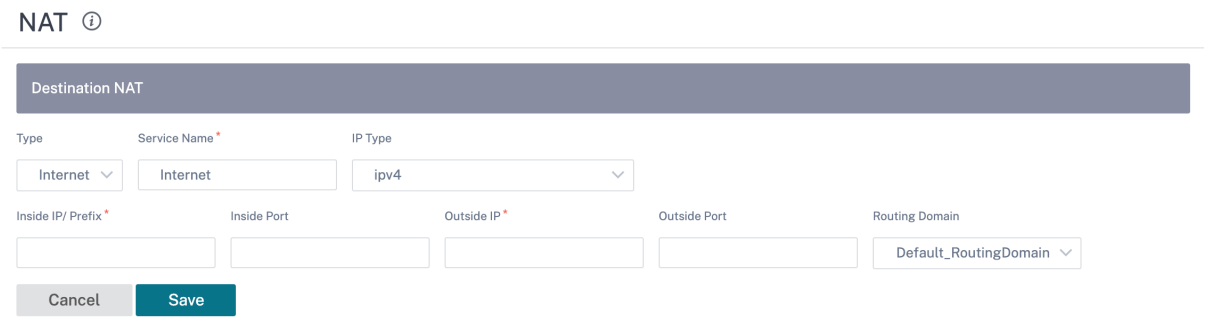
宛先 **NAT**

宛先 NAT ポリシーにより、個々のホストまたはサブネット間のネットワークアドレス変換ポリシーを設定できます。

> 注
>
> - サービスではインバウンド翻訳とアウトバウンド翻訳の両方を同時に設定できますが、最初に一致した翻訳のみが使用されます。パケットを受信するサービスとパケットが送信されるサービスにルールが存在する場合、複数の変換が行われる可能性があります。
> - 宛先 NAT 変換は、ローカルサービスから発信されるトラフィックにのみ適用されます。

これらの宛先 NAT ポリシーを設定するには、サイトレベルで [構成] **>** [詳細設定] **>** **[NAT] >** [宛先 **NAT**] に移動します。**+** 送信先 **NAT** をクリックします。

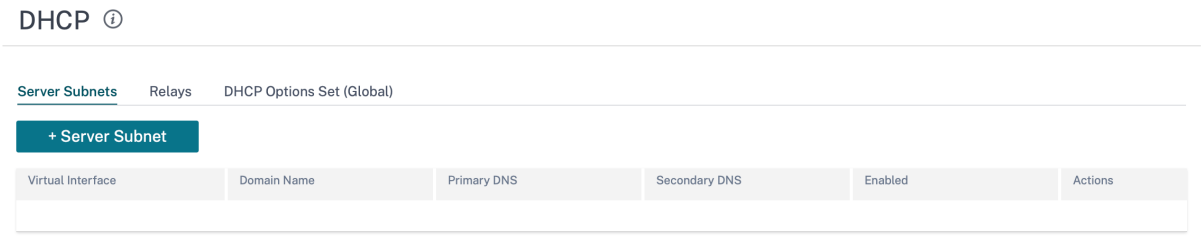
- タイプ:NAT ポリシーが適用される SD-WAN サービスタイプ。スタティック NAT の場合、サポートされるサービスの種類は、ローカル、仮想パス、インターネット、イントラネット、およびインターネットルーティングドメインサービスです。
- サービス名: サービスタイプに対応するサービスの名前を入力します。
- **IP** タイプ: 好みに応じて、IPv4 または IPv6 のアドレスタイプを選択します。
- 内部ポート: 外部ポートが転送される内部ポート。
- 外部 **IP**: 一致基準が満たされた場合に内部 IP アドレスが変換される外部 IP アドレスとプレフィックス。インターネットサービスおよびイントラネットサービスを使用する発信トラフィックでは、構成された WAN リンク IP アドレスが外部 IP アドレスとして動的に選択されます。
- 外部ポート: 内部ポートにポート転送される外部ポート。
- ルーティングドメイン: 選択した変換を適用するルーティングドメインを選択します。
- 受信時**:** このチェックボックスがオンになっている場合、インバウンド NAT が設定されます。クリアすると、アウトバウンド NAT が設定されます。



動的ホスト構成プロトコル

October 26, 2022

SD-WAN アプライアンスは **DHCP** サーバーまたは **DHCP** リレーエージェントとして構成できます。DHCP サーバ機能を使用すると、SD-WAN アプライアンスの LAN/WAN インターフェイスと同じネットワーク上のデバイスは、SD-WAN アプライアンスから IP 設定を取得できます。DHCP リレー機能を使用すると、SD-WAN アプライアンスは DHCP クライアントとサーバ間で DHCP パケットを転送できます。



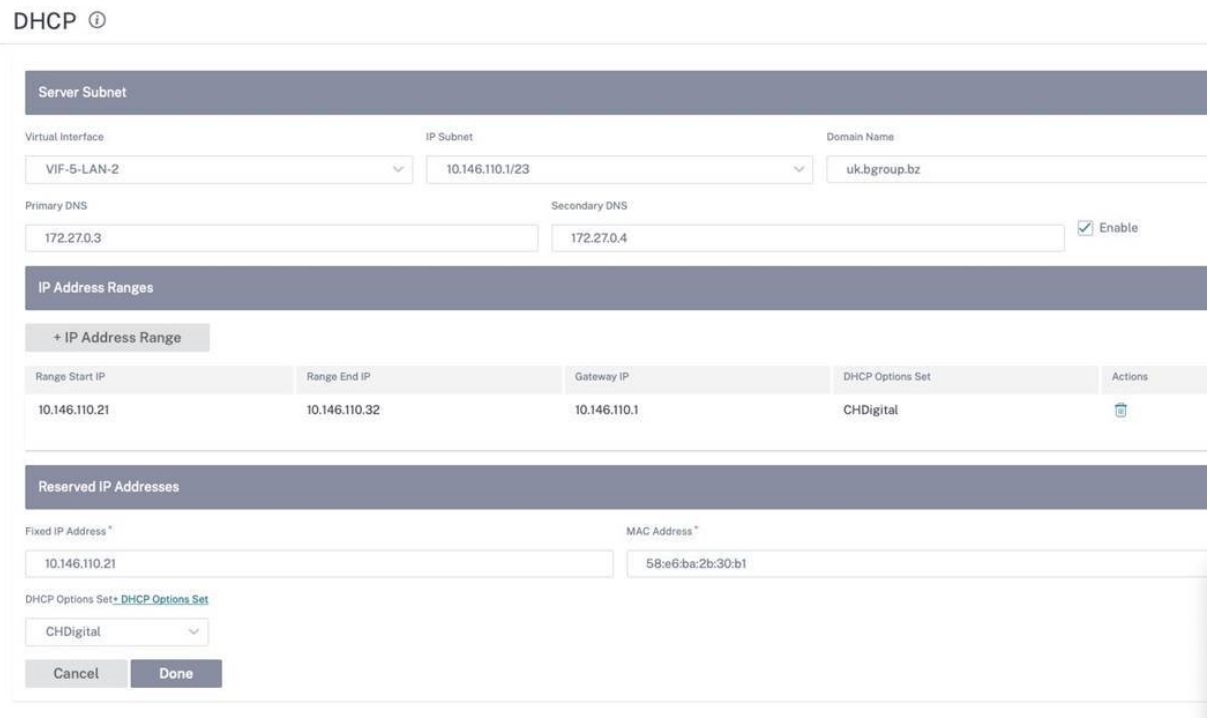
DHCP サーバ

Citrix SD-WAN アプライアンスは、DHCP サーバーとして構成できます。ネットワーク内の指定されたアドレスプールから IP アドレスを DHCP クライアントに割り当てて管理できます。

DHCP サーバは、DNS IP アドレスやデフォルト Gateway などの他のパラメータを割り当てるように設定できます。DHCP サーバは、アドレス割り当て要求と更新を受け入れます。DHCP サーバは、ローカルに接続された LAN セグメントからのブロードキャストや、ネットワーク内の他の DHCP リレーエージェントによって転送された DHCP 要求からのブロードキャストも受け付けます。

DHCP サーバーを構成するには、サイト構成ページのサイトレベルで、[構成] **>** [詳細設定] **>** [**DHCP**] **>** [サーバーサブネット] に移動し、[**+** サーバーサブネット] をクリックします。

DHCP 要求の受信に使用する仮想インターフェイスを選択します。DHCP サーバが IP アドレスを提供する IP サブネットは、自動的に入力されます。



ドメイン名、プライマリ **DNS**、およびセカンダリ **DNS** を入力します。DHCP サーバは、DHCP クライアントにこの情報を転送します。

クライアントへの IP アドレスの割り当てに使用されるダイナミック IP アドレスプールを設定します。開始 IP アドレスと終了 IP アドレスの範囲を指定し、**DHCP** オプションセットを選択します。

> 注
>
> DHCP オプションセットは、個々の IP アドレス範囲に適用できる DHCP 設定のグループです。詳細については、「DHCP オプションセット」を参照してください。

固定 IP アドレスを必要とする個々のホストを MAC アドレスにマッピングして、予約済み IP アドレスを設定します。** 固定 **IP** アドレスと **MAC** アドレスを入力し、****DHCP** オプションセットを選択します。

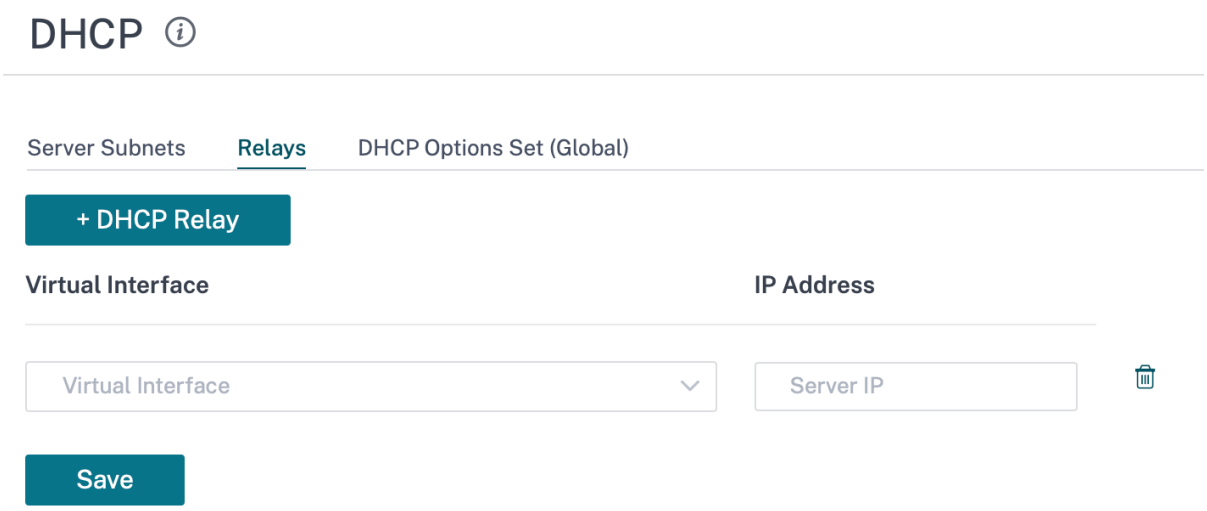
> 注
>
> 予約済み IP アドレスの場合、ゲートウェイ **IP** は **DHCP** オプションセットの Router オプションを設定することによって設定されます。

DHCP リレー

Citrix SD-WAN アプライアンスは、DHCP リレーとして構成できます。ローカルの DHCP クライアントとリモート DHCP サーバ間で DHCP 要求と応答をリレーします。

これにより、ローカルホストはリモート DHCP サーバーからダイナミック IP アドレスを取得できます。リレーエージェントは DHCP メッセージを受信し、新しい DHCP メッセージを生成して別のインターフェイスに送信します。

DHCP サーバーを構成するには、サイト構成ページで、「構成」**>**「詳細設定」**>**「**DHCP**」**>**「リレー」に移動し、「**+ DHCP** リレー」をクリックします。



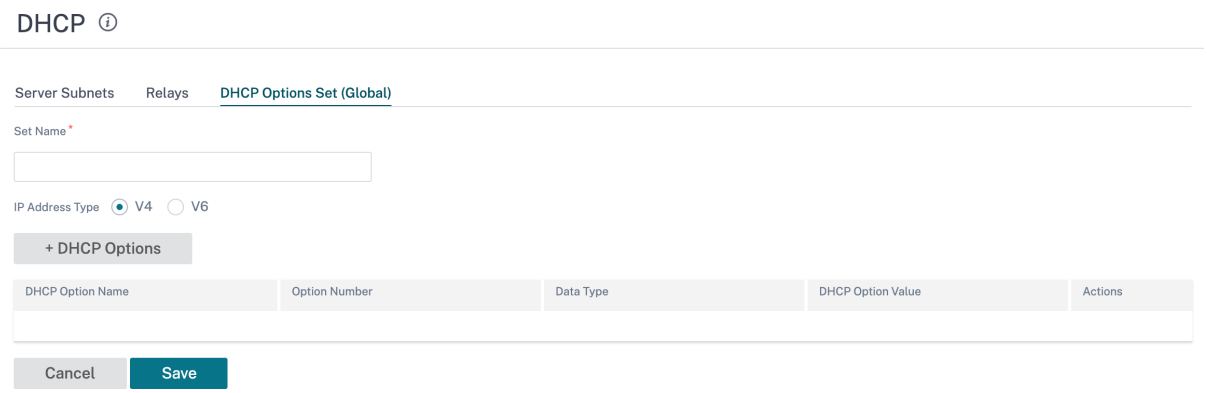
リモート DHCP サーバーと通信する仮想インターフェイスを選択します。リレーがクライアントからの要求と応答を転送するために使用する **DHCP** サーバ **IP** を入力します。

共通の仮想ネットワークインターフェイスを使用して単一の **DHCP** リレーを構成し、それを複数の DHCP サーバーに接続できます。

DHCP オプションセット

DHCP オプションは、個々の IP アドレス範囲または単一のホストに適用できる DHCP 設定のグループです。

DHCP オプションプロファイルの名前を設定し、**IP** アドレスタイプを選択します。[**+ DHCP** オプションセット] をクリックし、リストから DHCP オプション名を選択します。オプション番号は事前設定されています。カスタムオプションの場合、指定できる範囲は 224 ～254 です。データタイプを選択し、オプションの値を入力します。



DHCP クライアントによる **WAN** リンク **IP** アドレスの学習

Citrix SD-WAN アプライアンスは、DHCP クライアントによる WAN リンクの IP アドレス学習をサポートします。この機能により、SD-WAN アプライアンスの導入に必要な手動設定の量が削減され、静的 IP アドレスを購入する必要がなくなり、ISP のコストが削減されます。SD-WAN アプライアンスは、信頼できないインターフェイス上の WAN リンクのダイナミック IP アドレスを取得できます。これにより、この機能を実行するために中間 WAN ルータが不要になります。

> 注
>
> - DHCP クライアントは、クライアントノードとして構成された信頼できないブリッジドインターフェイスに対してのみ構成できます。
> - DHCP クライアントとデータポートは、パブリック IP アドレスが設定されている場合にのみ、MCN/RCN で有効にできます。
> - ワンアームまたはポリシーベースルーティング (PBR) 展開は、DHCP クライアント構成のサイトではサポートされません。
> - DHCP イベントはクライアント側からのみログに記録され、DHCP サーバーログは生成されません。

Fail-to-Block モードと Fail-to-Wire モードで信頼できない仮想インターフェイスの DHCP を設定する方法については、「サイトレベルの設定」を参照してください。

マルチキャストルーティング

October 26, 2022

マルチキャストルーティングにより、1 対多のトラフィックを効率的に配信できます。マルチキャスト送信元は、マルチキャストトラフィックを 1 つのストリームでマルチキャストグループに送信します。マルチキャストグループには、マルチキャスト通信に IGMP プロトコルを使用するホストや隣接ルータなどのレシーバが含まれます。Voice over IP、ビデオオンデマンド、IP テレビ、およびビデオ会議は、マルチキャストルーティングを使用する一般的なテクノロジの一部です。Citrix SD-WAN アプライアンスでマルチキャストルーティングを有効にすると、アプライアンスはマルチキャストルーターとして機能します。

送信元固有のマルチキャスト

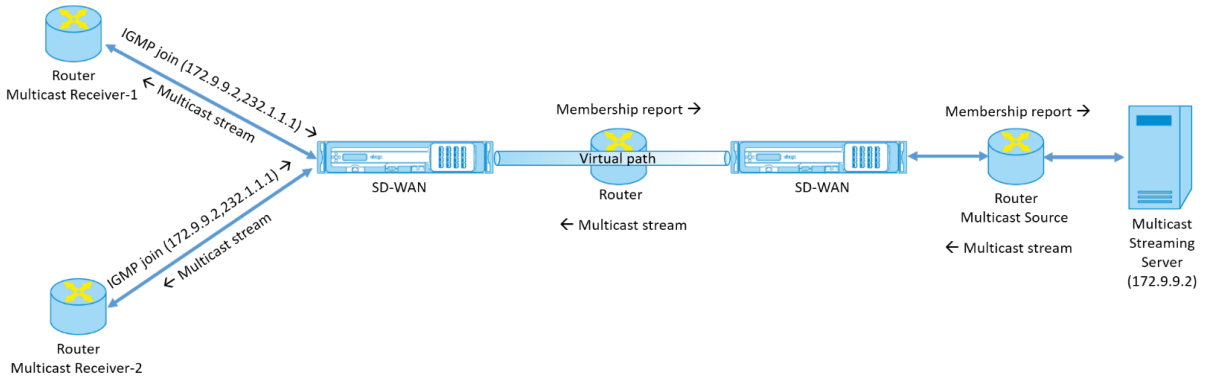
通常、マルチキャストプロトコルを使用すると、マルチキャストレシーバは任意の送信元からマルチキャストトラフィックを受信できます。

送信元固有マルチキャスト（SSM）を使用すると、レシーバがマルチキャストトラフィックを受信する送信元を指定できます。これにより、レシーバは、マルチキャストストリームを送信するすべてのソースに対してオープンリスナーではなく、特定のマルチキャストソースをリッスンすることを保証します。

SSM は、考えられるすべての送信元からのトラフィックの消費に使用されるリソースのコストを削減します。SSM は、受信側が既知の送信者からトラフィックを受信できるようにすることで、セキュリティ層も提供します。

次のトポロジは、ブランチサイトの 2 つのマルチキャストレシーバと、データセンターの 1 つのマルチキャストサーバ（172.9.9.2）を示しています。マルチキャストサーバは特定のグループ（232.1.1.1）でトラフィックをストリーミングし、レシーバはグループに参加します。マルチキャストグループでストリーミングされるトラフィックは、グループに加入したすべてのレシーバに中継されます。

> 注
>
> SSM が機能するためには、マルチキャストグループ IP が 232.0.0.0/8 の範囲内にある必要があります。



1. マルチキャストレシーバは、IP IGMP Join 要求を送信します。これは、レシーバがマルチキャストグループに加入し、送信元からマルチキャストストリームを受信することを示します。

   IGMP Join には、マルチキャスト送信元とグループ（S, G）の 2 つの属性が含まれます。IGMP バージョン 3 は、マルチキャスト送信元および受信側の SSM に使用され、一部の include 特定の送信元アドレスをリレーします。

   SSM を使用すると、レシーバは特定のマルチキャストサーバからストリームを明示的に受信できます。その送信元アドレスは、受信側から JOIN 要求の一部として明示的に提供されます。この例では、IGMP v3 Join 要求が、ソース 172.9.9.2 を含む明示的なインクルード送信元リストを使用してトリガーされ、グループ 232.1.1.1 経由でマルチキャストストリームを送信するアドレスになります。

2. 支店の Citrix SD-WAN は、これらの受信機からのすべての IGMP 要求をリッスンし、それをメンバーシップレポートに変換し、仮想パス経由でデータセンターの SD-WAN アプライアンスに送信します。
3. データセンターの Citrix SD-WAN アプライアンスは、仮想パスを介してメンバーシップレポートを受信し、マルチキャストソースに転送し、制御チャネルを確立します。
4. マルチキャスト送信元は、仮想パスを介してマルチキャストストリームをマルチキャストレシーバに送信します。

コントロールチャネルトラフィックとマルチキャストストリームは、ブランチとデータセンター間の確立された仮想パスを通過します。Citrix SD-WAN オーバーレイパスにより、マルチキャストトラフィックが WAN の劣化やリンクの停止を防ぐことができます。

マルチキャスト設定

マルチキャストを設定するには、送信元と宛先の両方の SD-WAN Orchestrator サービスで以下を実行します。

1. マルチキャストグループの作成：マルチキャストグループの名前と IP アドレスを指定します。マルチキャストグループ IP は、送信元固有のマルチキャストに対して 232.0.0.0/8 の範囲内にある必要があります。
2. IGMP プロキシを有効にする—Citrix SD-WAN アプライアンスを IGMP/MLD プロキシとして構成し、マルチキャストルーティング用の IGMP 制御チャネル情報を伝送できます。
3. アップストリームおよびダウンストリームサービスの定義：アップストリームインターフェイスにより、IGMP PROXY は、トラフィックをストリームする実際のマルチキャストソースに近い SD-WAN アプライアンスに接続できます。ダウンストリームインターフェイスを使用すると、IGMP Proxy は、トラフィックをストリームする実際のマルチキャストソースから遠く離れたホストに接続できます。
   アップストリームサービスとダウンストリームサービスは、ソースのアプライアンスと宛先のアプライアンスで異なります。

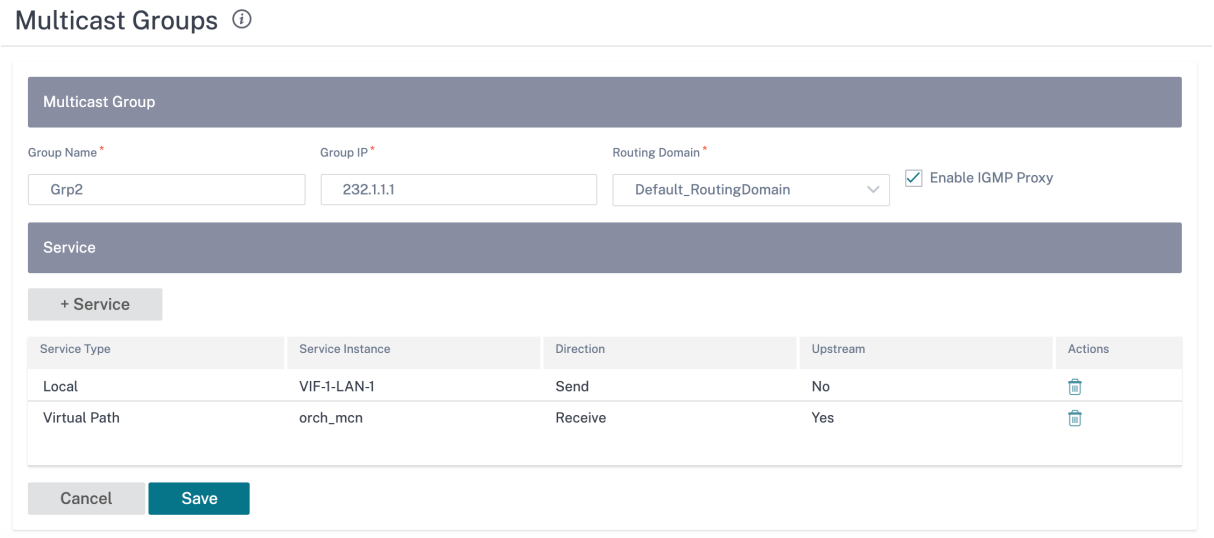
> 注:
>
> ブランチまたは MCN をアップストリームとして設定したら、他のグループでもアップストリームとして設定する必要があります。

マルチキャストを設定するには、サイトレベルで [構成] > [詳細設定] > [マルチキャストグループ] に移動します。マルチキャストグループの名前と IP アドレス (IPv4 または IPv6) を指定して、マルチキャストグループを作成します。[**IGMP** プロキシを有効にする] をクリックします。

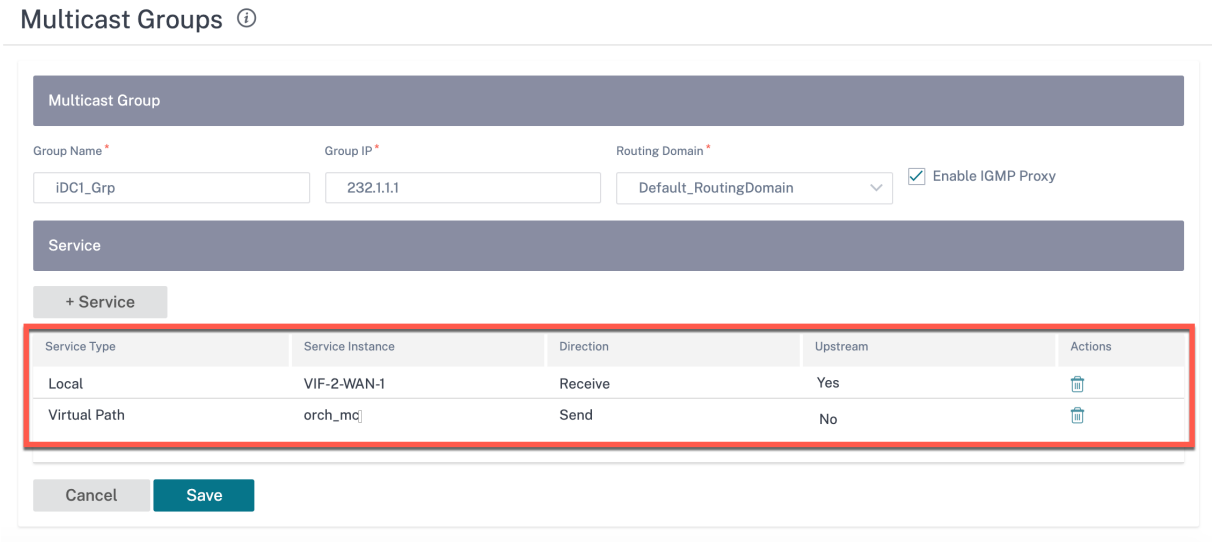
ブランチアプライアンスおよびデータセンターアプライアンスのアップストリームパスとダウンストリームパスを設定します。

アプライアンスがマルチキャストレシーバ（ブランチ）に近い場合、アプライアンスは仮想パスインターフェイスでマルチキャストトラフィックを受信し、ローカルインターフェイス上のトラフィックを受信者に送信します。

> 注:
>
> - マルチキャストソースをイントラネットサービスとして構成する場合、マルチキャストストリームのソース IP には、イントラネットサービスにマップされたルートが必要です。
> - SD-WAN アプライアンスでマルチキャストトラフィックを許可する適切なファイアウォールポリシーを必ず作成してください。



アプライアンスがマルチキャストソース（データセンター）に近い場合、アプライアンスはローカルインターフェイスでマルチキャストトラフィックを受信し、仮想パスインターフェイス上でトラフィックを送信します。



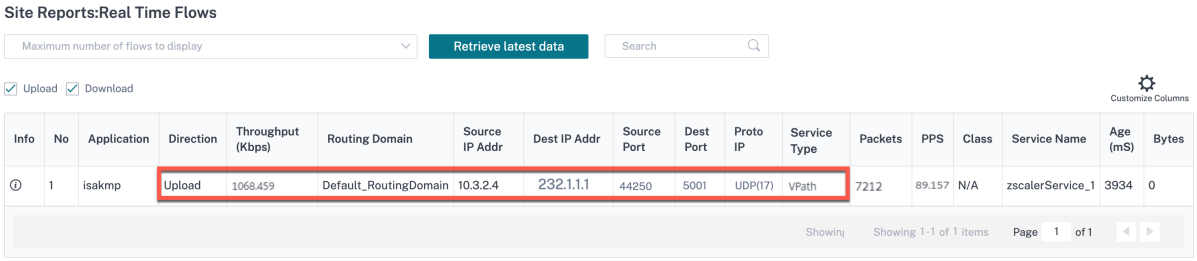
監視

フロー統計情報

マルチキャスト制御チャネルが確立され、マルチキャストソースがストリーミングを開始すると、マルチキャストフロー統計情報を表示できます。マルチキャスト UDP トラフィックが仮想パスサービスで受信側からマルチキャストグループ 232.1.1.1 に送信されたことがわかります。

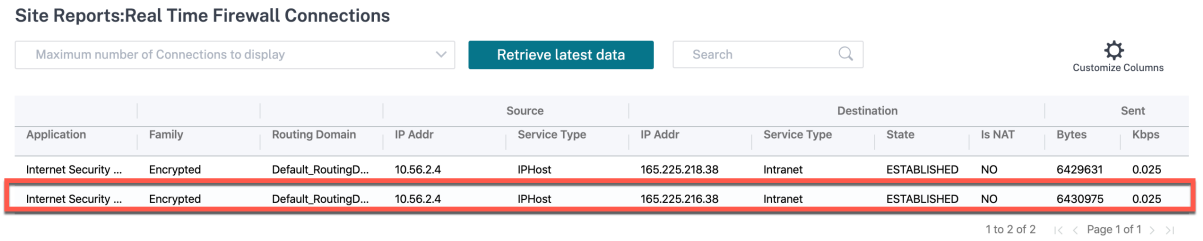
> 注:
>
> SSM が有効で、トラフィックが送信元送信者の予想リストに含まれていない別のサーバから受信された場合、

> SD-WAN アプライアンスはレポートデータを持ちません。



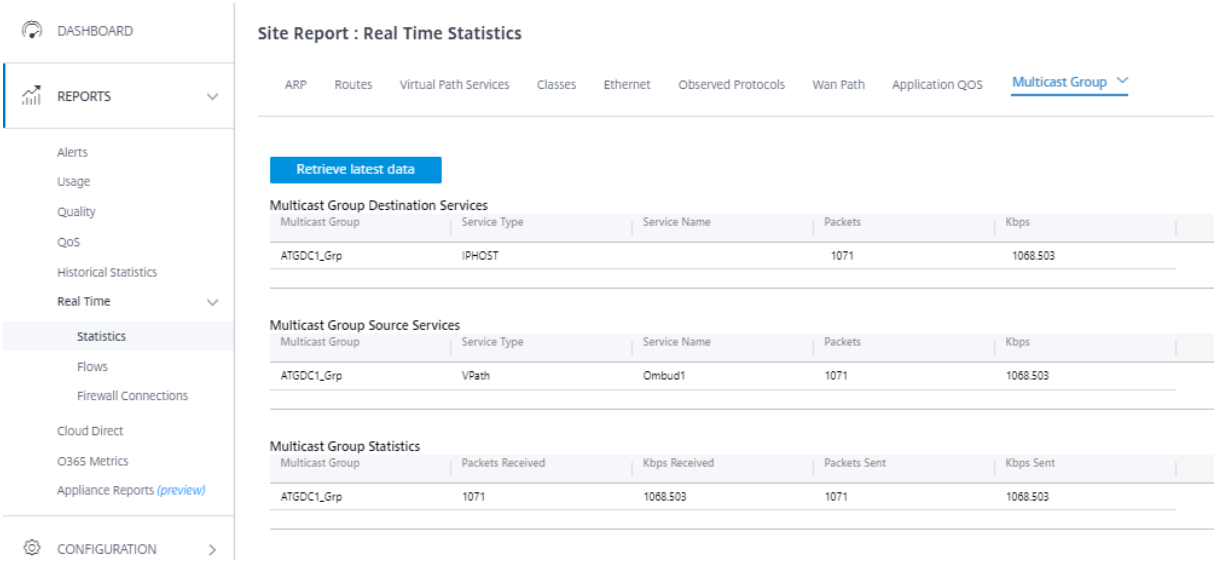
ファイアウォールの統計情報

ファイアウォールテーブルには、マルチキャストグループ IP アドレス経由で LAN インターフェイス経由で着信し、仮想パス経由で送信されるマルチキャストトラフィックが表示されます。



マルチキャストグループの統計情報

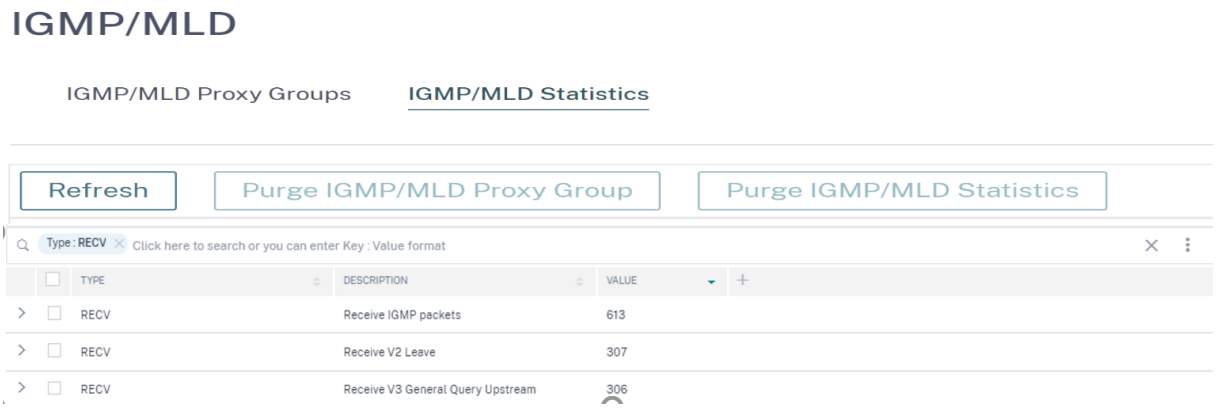
マルチキャストグループテーブルには、送信元、宛先、および両方の集約で送受信されるパケットなど、マルチキャストトラフィックの詳細が表示されます。



IGMP/MLD

マルチキャストレシーバがグループ加入要求を開始すると、[レポート] > [リアルタイム] > [IGMP/MLD] > [**IGMP/MLD** 統計情報] にレシーバの詳細が表示されます。この情報は、送信元と宛先の両方で確認できます。[更新] をクリックして、現在のデータを取得します。

次の図は、受信した IGMP/MLD パケットと、フィルタタイプ RECV を使用して IGMP/MLD 受信パケットが含まれていることを示しています。



IGMP プロキシグループの詳細を表示するには、[レポート] > [リアルタイム] > [**IGMP/MLD**] > [**IGMP/MLD** プロキシグループ] に移動します。[更新] をクリックして、現在のデータを取得します。

IGMP 統計情報テーブルから **IGMP** 統計データを消去するには、[IGMP 統計情報の消去] を選択します。

IGMP グループテーブルから **IGMP** グループデータを消去するには、**[IGMP /MLD** グループの消去] を選択します。

仮想ルータ冗長プロトコル

October 26, 2022

Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）は、デバイスの冗長性を提供し、スタティックなデフォルトルーティング環境に固有の単一障害点を排除する、広く使用されているプロトコルです。

VRRP を使用すると、1 つのグループを形成するように 2 つ以上のルータを設定できます。このグループは、1 つの仮想 IP アドレスと 1 つの仮想 MAC アドレスを持つ単一のデフォルト Gateway として表示されます。

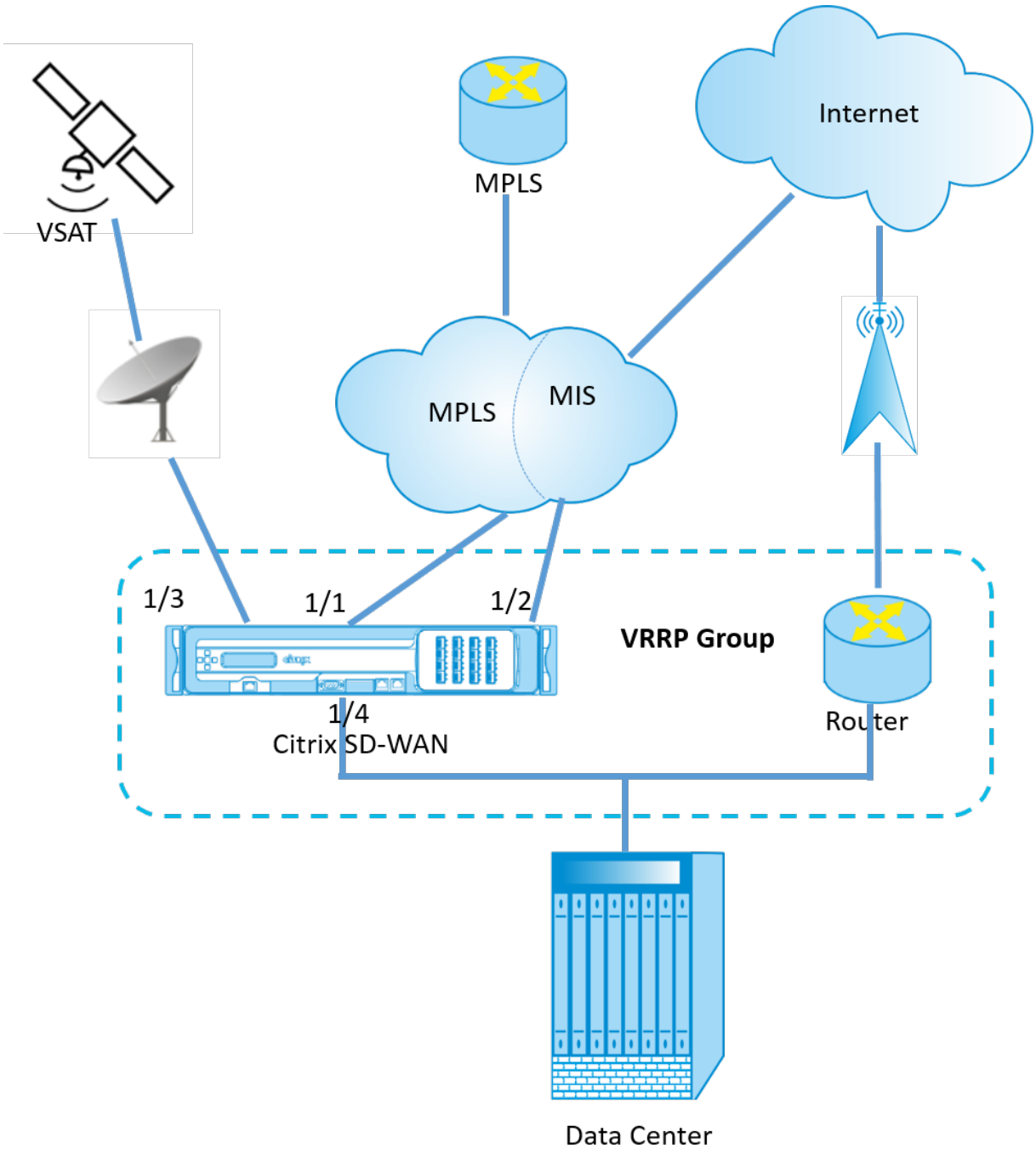
プライマリ/メインルーターに障害が発生すると、バックアップルーターが自動的に引き継ぎます。VRRP セットアップでは、メインルータがアドバタイズメントと呼ばれる VRRP パケットをバックアップルータに送信します。メインルータがアドバタイズメントの送信を停止すると、バックアップルータはインターバルタイマーを設定します。この保留期間内にアドバタイズメントが受信されない場合、バックアップルータはフェールオーバールーチンを開始します。

VRRP は、優先順位が最も高いルータをメインルータにする選択プロセスを指定します。優先順位がルーター間で同じ場合は、IP アドレスが最も大きいルーターがメインルーターになります。他のルータはバックアップ状態です。メインルータに障害が発生したり、新しいルータがグループに参加したり、既存のルータがグループから脱退したりすると、選定プロセスが再び開始されます。

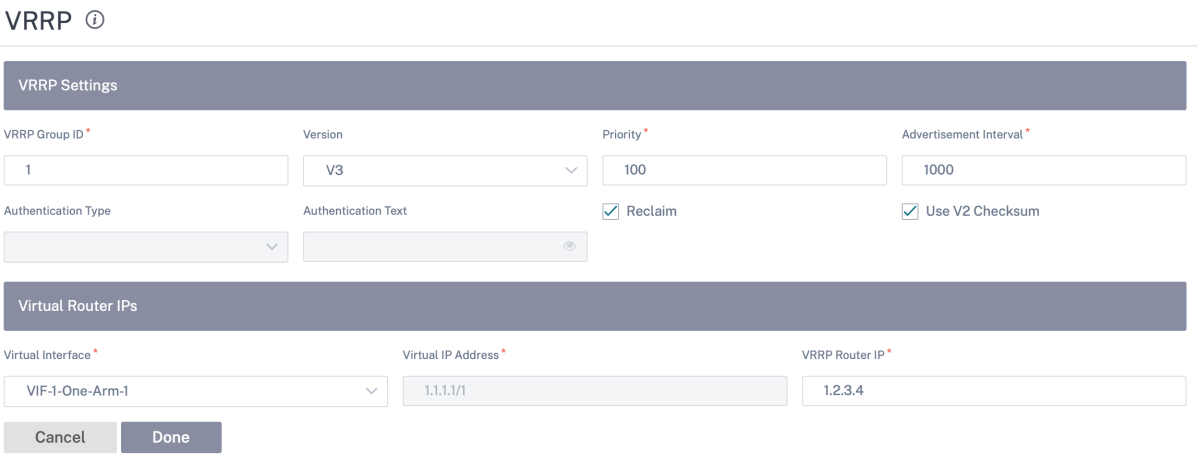
VRRP は、すべてのエンドホストでダイナミックルーティングまたはルータディスカバリプロトコルを設定せずに、高可用性デフォルトパスを保証します。

Citrix SD-WAN リリースバージョン 10.1 では、VRRP バージョン 2 およびバージョン 3 がサポートされ、サードパーティ製のルーターとの相互動作が可能です。Citrix SD-WAN リリースバージョン 11.5 はバージョン 6 をサポートしています。SD-WAN アプライアンスはメインルーターとして機能し、サイト間の仮想パスサービスを使用するようにトラフィックを誘導します。仮想インターフェイス IP を VRRP IP として設定し、手動で優先順位をピアルータよりも高い値に設定することで、SD-WAN アプライアンスを VRRP メインルータとして設定できます。アドバタイズメント間隔と preempt オプションを設定できます。

以下のネットワーク図は、Citrix SD-WAN アプライアンスと VRRP グループとして構成されたルーターを示しています。SD-WAN アプライアンスはメインルーターとして構成されています。SD-WAN アプライアンスに障害が発生した場合、バックアップルータはミリ秒以内に停止し、ダウンタイムが発生しないようにします。



VRRP を設定するには、サイト設定ページで、**[**構成**] > [**** 詳細設定] > [**VRRP**] に移動し、[**+ VRRP** を追加] をクリックします。**



次のメンバー・パス・パラメータを編集できます:

- **VRRP** グループ **ID**: VRRP グループ ID。グループ ID は、1 ～255 の値の範囲である必要があります。バックアップルータでも同じグループ ID を設定する必要があります。
- バージョン:VRRP プロトコルのバージョン。VRRP プロトコル V2 と V3 のいずれかを選択できます。
- 優先度:VRRP グループの Citrix SD-WAN アプライアンスの優先順位。プライオリティの範囲は 1 ～254 です。SD-WAN アプライアンスをメインルーターにするには、この値を最大（254）に設定します。

  > 注
  >
  > ルータが VRRP IP アドレスの所有者である場合、プライオリティはデフォルトで 255 に設定されます。

- アドバタイズメント間隔:SD-WAN アプライアンスがメインルーターである場合に VRRP アドバタイズメントが送信される頻度（ミリ秒単位）。デフォルトのアドバタイズメント間隔は 1 秒です。
- 認証タイプ: プレーンテキストを選択して認証文字列を入力できます。認証文字列は、VRRP アドバタイズメントで暗号化なしでプレーンテキストとして送信されます。認証を設定しない場合は、[**None**] を選択します。
- 認証テキスト:VRRP アドバタイズメントで送信される認証文字列。このオプションは、[認証タイプ] が [プレーンテキスト] の場合に有効になります。

  > 注
  >
  > ** 認証タイプと認証テキストのパラメータは ** 、VRRP プロトコルバージョン 2 でのみ有効です。

- **V2** チェックサムを使用:VRRPv3 のサードパーティ製ネットワークデバイスとの互換性を有効にします。デフォルトでは、VRRPv3 は v3 チェックサム計算方式を使用します。一部のサードパーティデバイスでは、VRRPv2 チェックサム計算しかサポートされない場合があります。そのような場合は、このオプションを有効にします。
- 仮想インターフェイス: VRRP に使用される仮想インターフェイス。IPv6 を使用する場合、仮想インターフェイスでは NDP RA がデフォルトで有効になります。設定済みの仮想インターフェイスの 1 つを選択します。

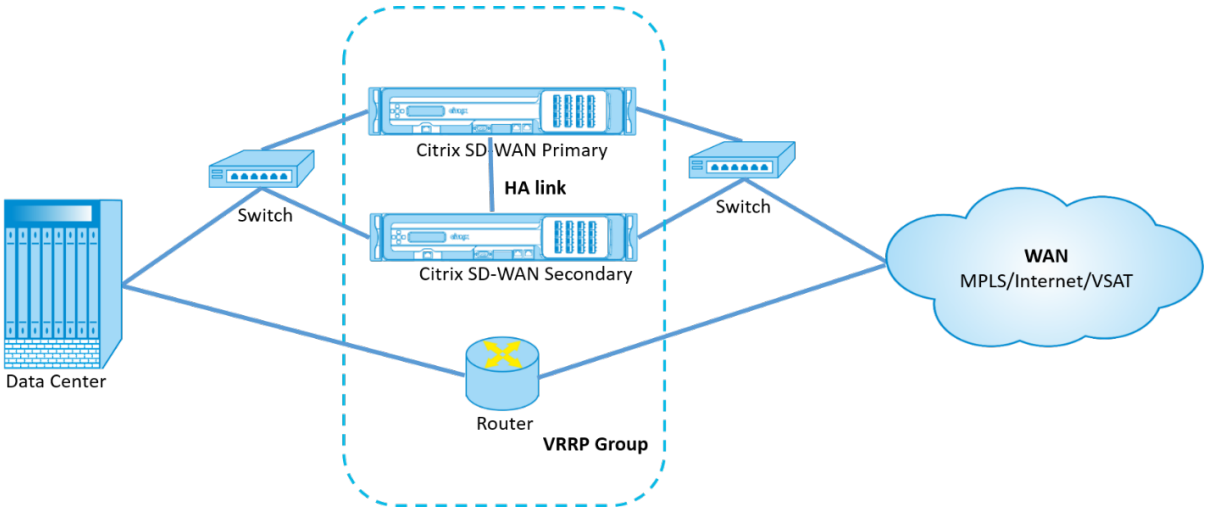
- 仮想 **IP** アドレス: 仮想インターフェイスに割り当てられた仮想 IP アドレス。仮想インターフェイスに設定済みの仮想 IP アドレスのいずれかを選択します。IPv4 アドレスと IPv6 アドレスのどちらかを指定できます。
- **VRRP** ルータ **IP**: VRRP グループの仮想ルータの IP アドレス。デフォルトでは、SD-WAN アプライアンスの仮想 IP アドレスが仮想ルータ IP アドレスとして割り当てられます。VRRP 仮想ルータ IP はリンクローカル IPv6 アドレスでなければなりません。

制限事項

- VRRP は、Gateway モード配置でのみサポートされます。
- 最大 4 つの VRRP ID（VRID）を設定できます。
- VRID には、最大 16 個の仮想ネットワークインターフェイスを使用できます。

高可用性および **VRRP**

SD-WAN ネットワークに高可用性機能と VRRP 機能の両方を適用することで、ネットワークのダウンタイムとトラフィックの中断を大幅に減らすことができます。アクティブ/スタンバイの役割で Citrix SD-WAN アプライアンスのペアをスタンバイルーターとともに展開し、VRRP グループを形成します。このグループは、1 つの仮想 IP アドレスと 1 つの仮想 MAC アドレスを持つ単一のデフォルト Gateway として表示されます。



高可用性と VRRP の導入には、次の 2 つのケースがあります。

1 番目のケース: **SD-WAN** での高可用性フェールオーバータイマーは、**VRRP** フェールオーバータイマーと同じです。

予想される動作は、VRRP スイッチオーバーの前に高可用性スイッチオーバーが発生することです。つまり、トラフィックは新しい Active SD-WAN アプライアンスを引き続き通過します。この場合、SD-WAN は VRRP マスターロールを継続します。

2 番目のケース: **VRRP** フェールオーバータイマーよりも大きい **SD-WAN** での高可用性フェールオーバータイマーです。

想定される動作は、ルータへの VRRP スイッチオーバーが発生することです。つまり、ルータが VRRP マスターになり、トラフィックが SD-WAN アプライアンスをバイパスして、ルータを一時的に流れる可能性があります。

ただし、高可用性スイッチオーバーが発生すると、SD-WAN が再び VRRP マスターになります。つまり、トラフィックは新しいアクティブ SD-WAN アプライアンスを通過します。

高可用性展開モードの詳細については、「高可用性」を参照してください。

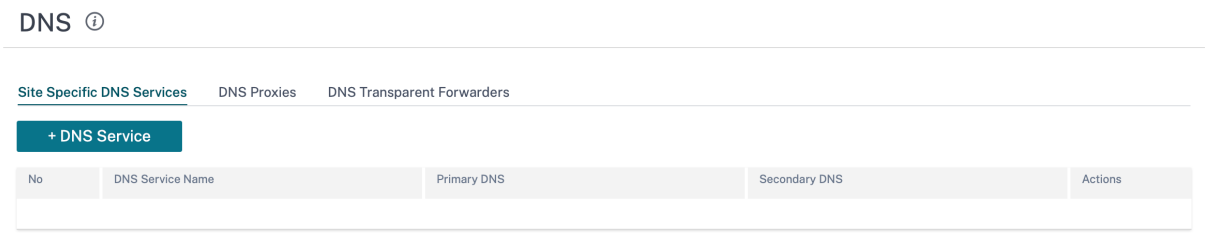
ドメインネームシステムの設定

October 26, 2022

ドメインネームシステム (DNS) は、人間が読めるドメイン名をマシン読み取り可能な IP アドレスに変換し、その逆の方法です。Citrix SD-WAN には、次の DNS 機能があります。

- DNS プロキシ
- DNS 透過転送

DNS 設定を構成するには、サイト構成ページで、構成 **>** 詳細設定 ****DNS 設定に移動します ****。



サイト固有の **DNS** サーバー

サイト固有の **DNS** サーバータブで、**+ DNS** サーバをクリックして、DNS 要求がルーティングされるサイト固有の DNS サーバを設定します。DNS サーバーの名前を指定します。次のサービスタイプから 1 つを選択します。

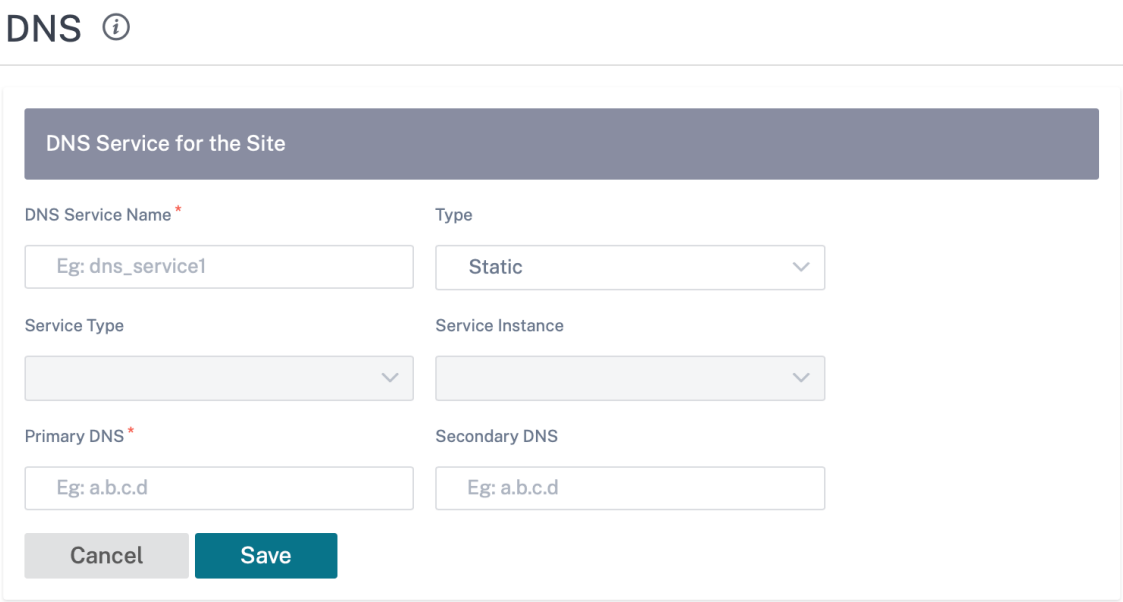
- 静的: Citrix SD-WAN IP アドレス宛ての DNS 要求を傍受し、指定された IPv4 DNS サーバーに転送します。内部、ISP、グーグル、またはその他のオープンソースの DNS サービスを作成できます。
- 動的: Citrix SD-WAN IP アドレス宛ての DNS 要求を傍受し、DHCP ベースの WAN リンクから学習した IPv4 DNS サーバーの 1 つにリダイレクトします。WAN リンクがダウンすると、別の DHCP ベースの WAN リンク DNS サーバが選択されます。この機能は、ISP がホストする DNS サーバーへの DNS 要求のみを許可する展開で役立ちます。動的 DNS サービスは、サイトレベルでのみ構成できます。サイトごとに許可される動的 DNS サービスは 1 つだけです。
- **Staticv6**: Citrix SD-WAN IP アドレス宛ての DNS 要求を傍受し、指定された IPv6 DNS サーバーに転送します。内部、ISP、グーグル、またはその他のオープンソースの DNS サービスを作成できます。

- **Dynamicv6**: Citrix SD-WAN IP アドレス宛ての DNS 要求を傍受し、DHCP ベースの WAN リンクから学習した IPv6 DNS サーバーの 1 つにリダイレクトします。WAN リンクがダウンすると、別の DHCP ベースの WAN リンク DNS サーバが選択されます。この機能は、ISP がホストする DNS サーバーへの DNS 要求のみを許可する展開で役立ちます。動的 DNS サービスは、サイトレベルでのみ構成できます。サイトごとに許可される動的 DNS サービスは 1 つだけです。

スタティック DNS サービスを設定するには、タイプとして [スタティック **(IPv4** アドレスの場合**)]** または **[**スタティック **v6(IPv6** アドレスの場合)] を選択し、プライマリ **DNS** サーバの IP アドレスとセカンダリ **DNS** サーバの IP アドレスのペアを入力します。

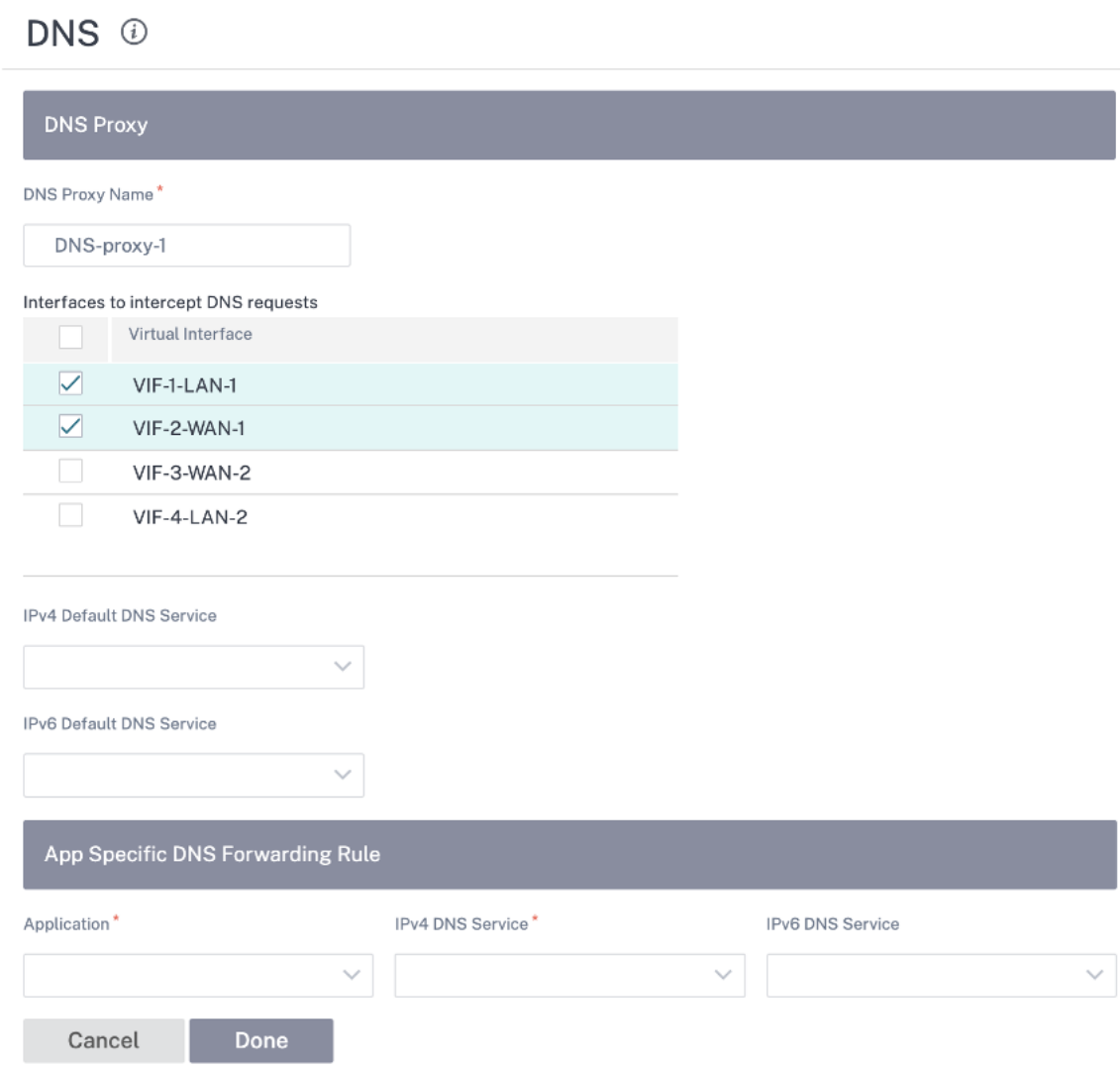
ダイナミック DNS サービスを設定するには、****** タイプをダイナミック ** (IPv4 アドレスの場合) または **Dynamicv6** (IPv6 アドレスの場合) として選択し、[サービスタイプ**]** と **[**** サービスインスタンス **] で [インターネット] を選択します。

対応する DNS プロキシサービスは、[サイトの設定**] > [**インターフェイス] の [**InBand Management DNS**] ドロップダウンリストに表示されます。



DNS プロキシ

DNS プロキシは、SD-WAN IP アドレス宛の DNS 要求を代行受信し、選択した DNS サーバーに転送します。アプリケーションのドメイン名に基づいて DNS 要求の操作に役立つ複数のフォワーダーを持つプロキシを構成できます。

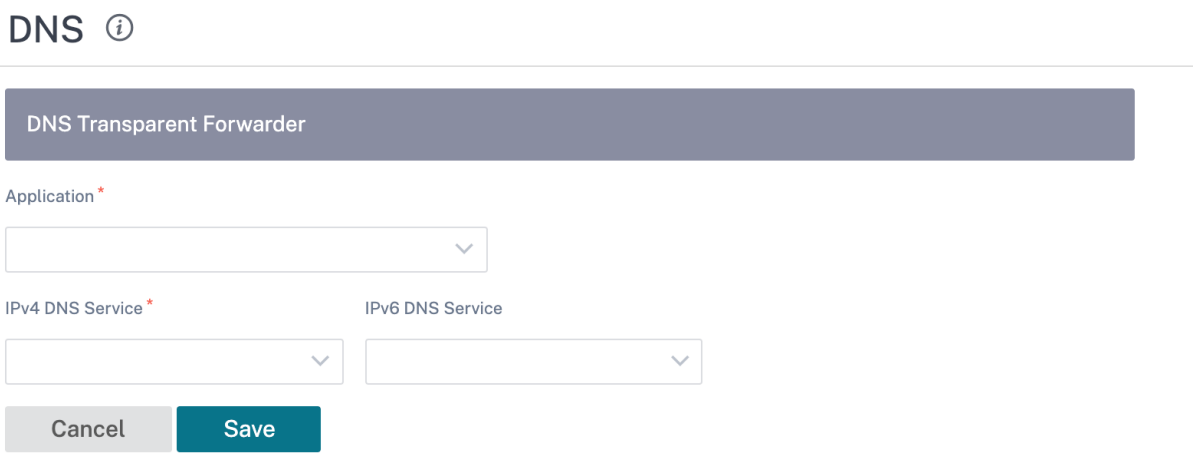


- DNS プロキシ設定:
  - **DNS** プロキシ名:DNS プロキシの名前。
  - **DNS** リクエストをインターセプトするインターフェース:DNS リクエストがインターセプトされるインターフェース。信頼できるインターフェイスだけが許可されます。
  - 全トラフィックのデフォルト DNS サーバー:DNS フォワーダーの検索で一致するアプリケーションがない場合の DNS リクエストの転送先となるデフォルトの DNS サーバー。
  - **IPv4** デフォルト **DNS** サービス:DNS フォワーダ検索で一致するアプリケーションがない場合の DNS 要求の転送先となる IPv4 デフォルト DNS サービス。
  - **IPv6** デフォルト **DNS** サービス:DNS フォワーダ検索で一致するアプリケーションがない場合の DNS 要求の転送先となる IPv6 デフォルト DNS サービス。
- アプリ固有の DNS 転送ルール:
  - アプリケーション: 選択した DNS サーバに DNS 要求を転送する必要があるアプリケーション。

- **IPv4 DNS** サービス: 指定されたアプリケーションの DNS リクエストが転送される IPv4 DNS サービス。
- **IPv6 DNS** サービス: 指定されたアプリケーションの DNS 要求が転送される IPv6 DNS サービス。

DNS トランスペアレントフォワーダ

Citrix SD-WAN は、透過的な DNS フォワーダとして構成できます。このモードでは、SD-WAN は、IP アドレス宛ではない DNS 要求を代行受信し、指定された DNS サーバに転送できます。信頼できるインターフェイス上のローカルサービスからの DNS 要求だけが代行受信されます。DNS 要求が DNS フォワーダリスト内のアプリケーションと一致する場合、その要求は設定された DNS サービスに転送されます。



- アプリケーション: 選択した DNS サーバに DNS 要求を転送する必要があるアプリケーション。
- **IPv4 DNS** サービス: 指定されたアプリケーションの DNS リクエストが転送される IPv4 DNS サービス。
- **IPv6 DNS** サービス: 指定されたアプリケーションの DNS 要求が転送される IPv6 DNS サービス。

プレフィックス委託グループ

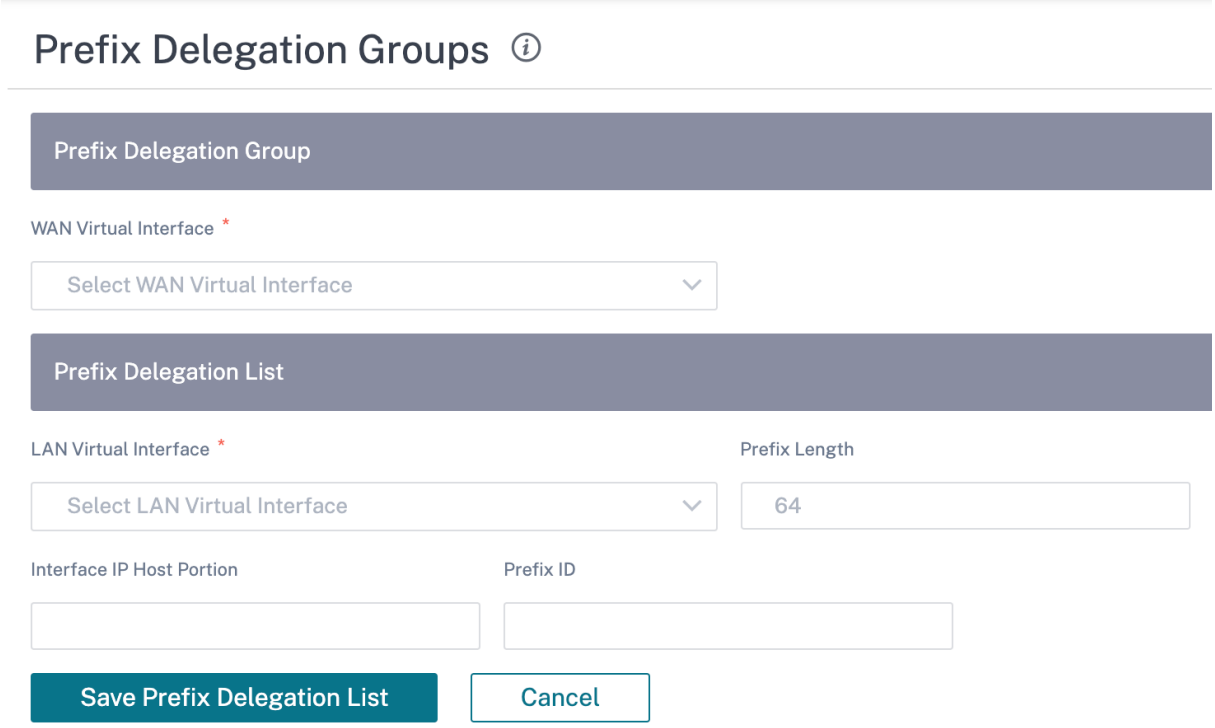
October 26, 2022

Citrix SD-WAN アプライアンスは、DHCPv6 クライアントとして構成し、構成された WAN ポートを使用して ISP にプレフィクスを要求できます。Citrix SD-WAN アプライアンスはプレフィックスを受信すると、そのプレフィックスを使用して LAN クライアントに対応する IP アドレスのプールを作成します。その後、Citrix SD-WAN アプライアンスは DHCP サーバーとして動作し、LAN ポートのプレフィックスを LAN 側のクライアントに通知します。

プレフィックス委任を設定するには、設定 **>** 詳細設定 **>** プレフィックス委任グループに移動し、**+** プレフィックス委任グループをクリックします。

ISP からプレフィックスが要求される設定済みの WAN 仮想インターフェイスを選択し、次の詳細を入力します。

- **LAN** 仮想インターフェイス：プレフィクスが要求される設定済みの LAN 仮想インターフェイスのいずれかを選択します。
- プレフィクス長：プレフィクスの一部であるグローバルユニキャスト IPv6 アドレスのビット数。
- インターフェイス **IP** ホスト部分: インターフェイスの IP アドレスに使用されるホスト部分。
- プレフィクス **ID**：LAN インターフェイスのプレフィクス委任要求を識別する一意の識別子。



リンク集約グループ

October 26, 2022

リンク集約グループ（LAG）機能を使用すると、SD-WAN アプライアンス上の 2 つ以上のポートをグループ化して、1 つのポートとして連携させることができます。これにより、可用性の向上、リンクの冗長性、およびパフォーマンスの向上が保証されます。

オンプレミス向け Citrix SD-WAN Orchestrator は、シンプルなリンクアグリゲーショングループ（ACTIVE-BACKUP 802.3ad LACP プロトコルベースのネゴシエーションは、現在のリリースではサポートされていません。アクティブなポートは 1 つだけで、他のポートはバックアップモードになります。アクティブサポートおよびバックアップサポートは、LAG 機能についてデータプレーン開発キット (DPDK) パッケージに依存しています。

LAG 機能は次のプラットフォームでのみ使用できます。

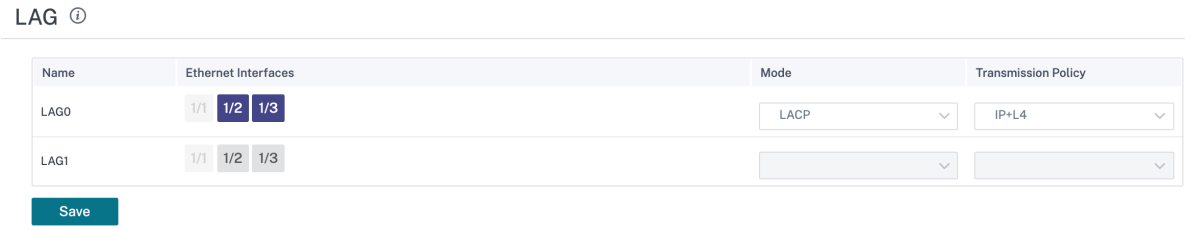
- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE
- Citrix SD-WAN 410 SE
- Citrix SD-WAN 1100 SE/PE
- Citrix SD-WAN 2100 SE/PE
- Citrix SD-WAN 4100 SE
- Citrix SD-WAN 5100 SE/PE
- Citrix SD-WAN 6100 SE/PE

> 注
>
> - LAG 機能は、VPX/VPXL プラットフォームではサポートされていません。
> - LAG ごとに最低 2 つのポート、最大 4 つのポートがサポートされます。
> - LAG のメンバーはすべて同じタイプ (たとえば 1/1 または 1/2) でなければなりません。1/1 と 10/1 は LAG 構成ではサポートされていません。
> - LAG がインターフェイスグループのイーサネットインターフェイスとして使用される場合、リンクステート伝播（LSP）機能はサポートされません。

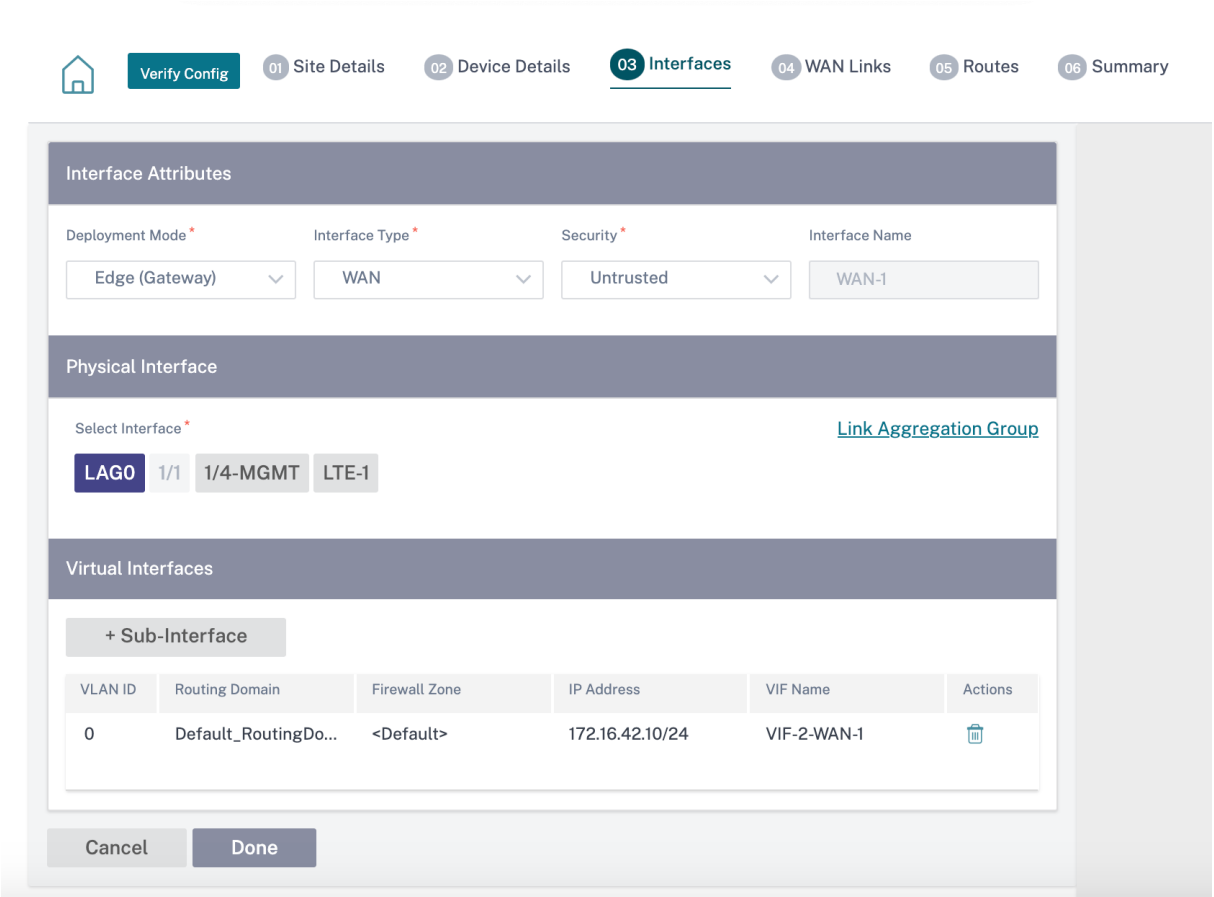
プラットフォーム	サポートされる LAG の最大数	LACP がサポートするポート
110	1	1/1
210	2	1/1 または 1/2
410	1	1/1 または 1/2
1100	3	1/1 または 1/2

プラットフォーム	サポートされる LAG の最大数	LACP がサポートするポート
2100	3	1/1 または 1/2
4100	4	1/1 または 1/2
5100	3	10/1 または 10/2
6100	4	1/1 または 1/2

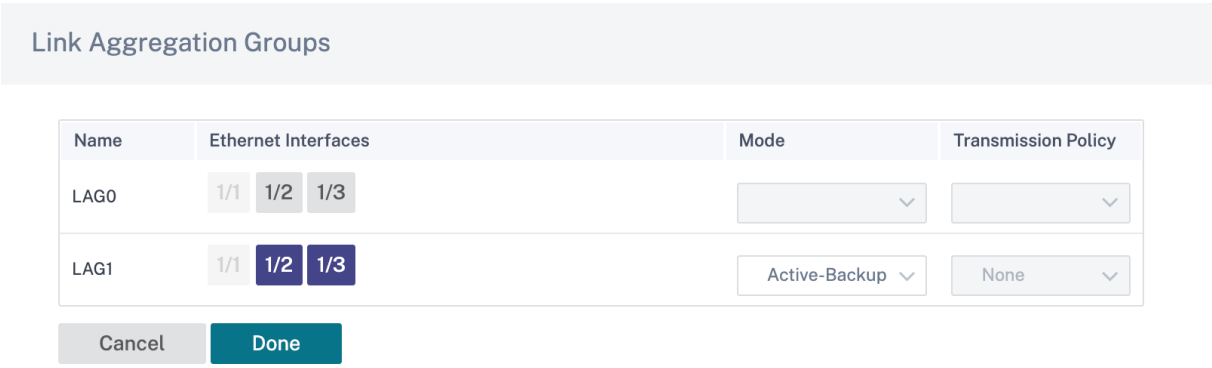
リンクアグリゲーショングループを設定するには、サイトレベルで [設定] **> [**詳細設定**] > [LAG**] に移動し、メンバーイーサネットインターフェイスを選択してリンクアグリゲーショングループを形成します。



ポートを LAG に追加したら、LAG を選択して [サイト構成] でインターフェイスを設定できます。これらのインターフェイスは、LAN/WAN リンクと HA の設定にも使用されます。個々のメンバポートの設定は変更できません。LAG に対する構成の変更は、メンバポートに自動的にプッシュされます。



インターフェイスセクションで [リンクアグリゲーショングループ] をクリックすると、必要に応じて LAG 設定をすばやく変更できます。



LAG と LACP で構成されているインターフェースの詳細は、「レポート」>「アプライアンス・レポート」**>**「**LACP LAG** グループ」で確認できます。詳しくは、「アプライアンスレポート」を参照してください。

アプライアンスの設定

October 26, 2022

Citrix SD-WAN Orchestrator サービスを使用すると、サイトレベルでアプライアンス設定を構成し、それをリモートアプライアンスにプッシュできます。

ユーザー、ネットワークアダプター、NetFlow、AppFlow、SNMP、フォールバック構成、およびパージフローの設定を構成できます。

> 注:
>
> サイトテンプレートの作成中または編集中は、アプライアンス設定を構成するオプションは使用できません。

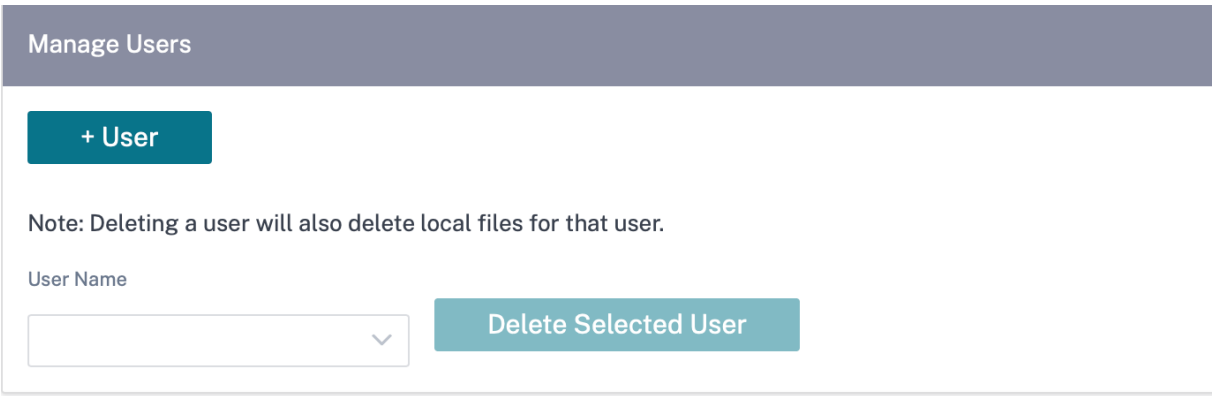
高可用性が設定されている場合は、アプライアンス設定を変更するプライマリまたはセカンダリアプライアンスを選択します。

管理インタフェース

管理インターフェイスを使用すると、ローカルユーザーアカウントとリモートユーザーアカウントを追加および管理できます。リモートユーザアカウントは、RADIUS または TACACS+ 認証サーバを使用して認証されます。

ユーザーの管理

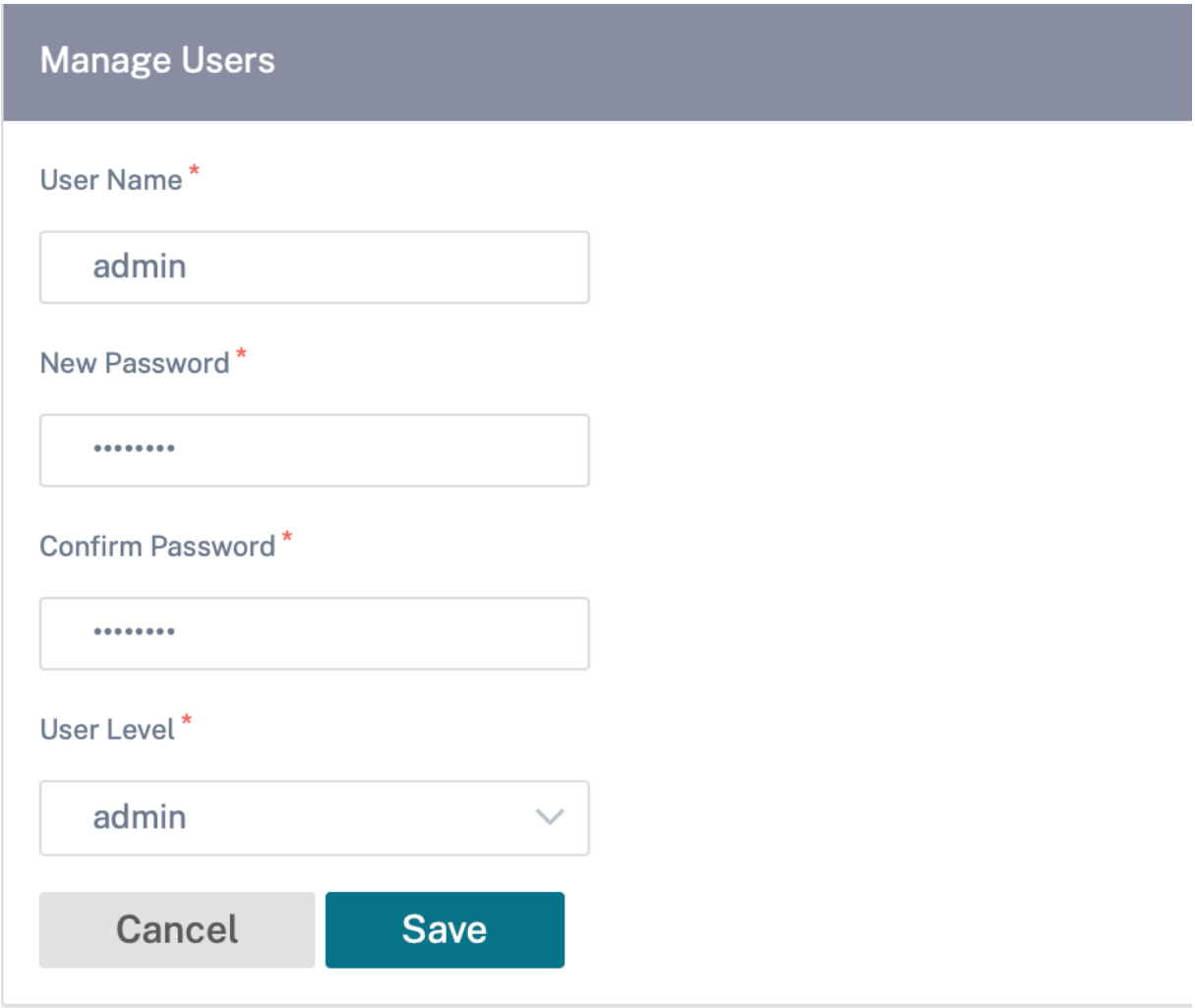
サイトに新しいユーザーアカウントを追加できます。新しいユーザーを追加するには、[構成] > [アプライアンス設定] > [管理者インターフェイス] > [ユーザーの管理] に移動し、[+ ユーザー] をクリックします。



次の詳細を入力します。

- ユーザー名: ユーザーアカウントのユーザー名。
- 新しいパスワード: ユーザーアカウントのパスワード。
- パスワードの確認: パスワードを再入力して確認します。
- ユーザーレベル: 次のアカウント権限のいずれかを選択します。
  - 管理者: 管理者アカウントには、すべての設定への読み取り/書き込み権限があります。管理者は、ネットワークに対する設定とソフトウェアの更新を実行できます。
  - 閲覧者: 閲覧者アカウントは、ダッシュボード、レポート、監視の各セクションにアクセスできる読み取り専用のアカウントです。
  - ネットワーク管理者: ネットワーク管理者には、ネットワーク設定への読み取り/書き込みアクセス権と、その他の設定への読み取り専用アクセス権があります。
  - セキュリティ管理者: セキュリティ管理者は、ファイアウォール/セキュリティ関連設定への読み取り/書き込みアクセス権を持ち、他の設定については読み取り専用アクセス権を持ちます。

    > 注
    >
    > セキュリティ管理者は、他のユーザー（管理者/閲覧者）のファイアウォールへの書き込みアクセスを無効にする権限があります。

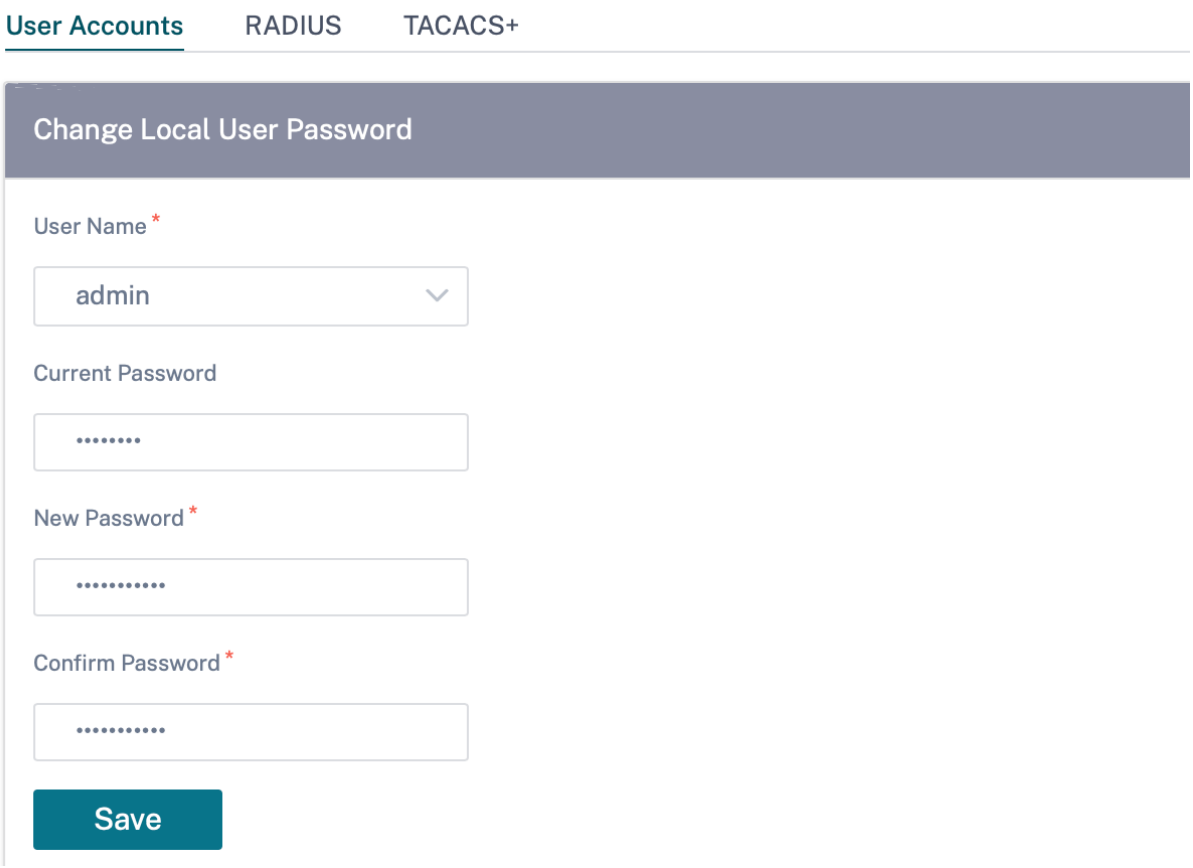


ユーザーを削除するには、ユーザー名を選択し、「選択したユーザーを削除」をクリックします。ユーザーアカウントとローカルファイルが削除されます。

ローカルユーザーパスワードの変更

ローカルユーザーパスワードを変更するには、「構成」>「アプライアンス設定」>「管理インターフェイス」>「ユーザーアカウント」>「ローカルユーザーパスワードの変更」に移動し、次の値を入力します。

- ユーザー名: サイトで構成されているユーザーのリストから、パスワードを変更するユーザー名を選択します。
- 現在のパスワード: 現在のパスワードを入力します。管理者ユーザの場合、このフィールドはオプションです。
- 新しいパスワード: お好きな新しいパスワードを入力します。
- パスワードの確認: パスワードを再入力して確認します。



RADIUS 認証サーバー

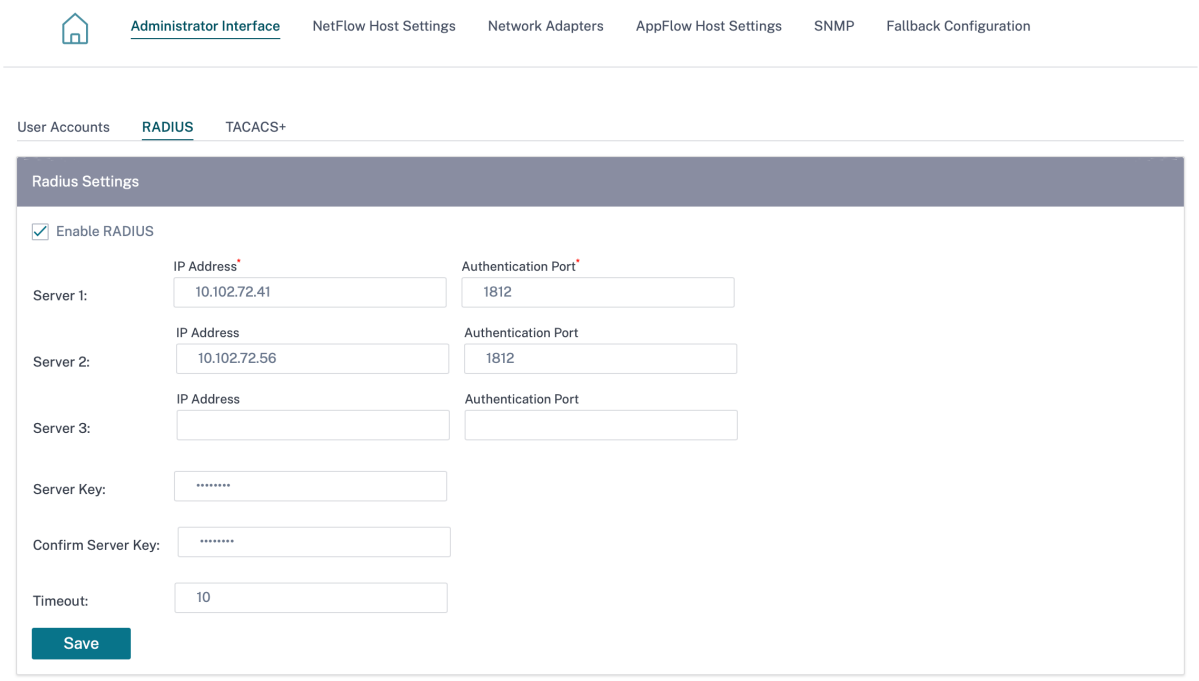
RADIUS は、アプライアンス上でリモートユーザー認証を有効にします。RADIUS 認証を使用するには、少なくとも 1 つの RADIUS サーバーを指定して設定する必要があります。オプションで、最大 3 台の冗長バックアップ RADIUS サーバを設定できます。サーバーは順番にチェックされます。必要なユーザーアカウントが RADIUS 認証サーバーで作成されていることを確認します。

RADIUS 認証を設定するには、構成 > アプライアンス設定 > 管理インタフェース > **RADIUS** に移動し、「RADIUS を有効にする **」をクリックします。

> 注
>
> サイトで RADIUS 認証または TACACS+ 認証を有効にできます。両方を同時に有効にすることはできません。

RADIUS サーバのホスト IP アドレスと認証ポート番号を指定します。デフォルトのポート番号は 1812 です。サーバキーを入力し、それを確認します。これは RADIUS サーバへの接続に使用される秘密キーです。RADIUS サーバからの認証応答を待機する時間間隔を指定します。タイムアウト値は 60 秒以下である必要があります。

> 注
>
> ** サーバーキーとタイムアウトの設定は ** 、設定されているすべてのサーバーに適用されます。



TACACS+ 認証サーバー

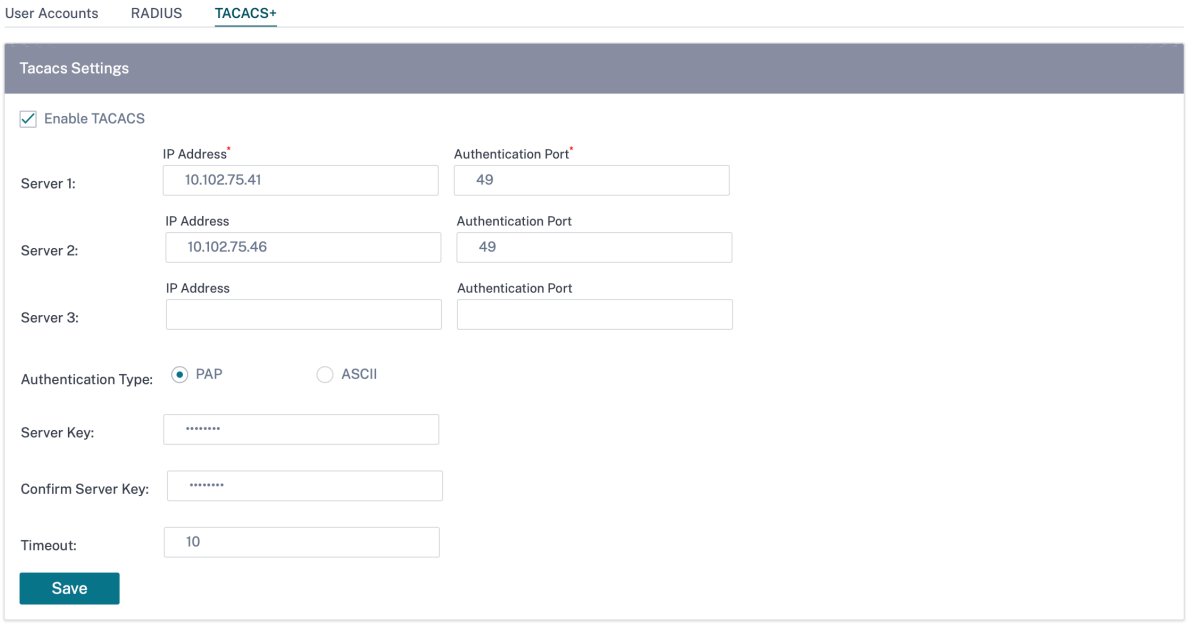
TACACS+ は、アプライアンスでのリモートユーザー認証を可能にします。TACACS+ 認証を使用するには、少なくとも 1 つの TACACS+ サーバを指定し、設定する必要があります。オプションで、最大 3 台の冗長バックアップ TACACS+ サーバを設定できます。サーバーは順番にチェックされます。必要なユーザーアカウントが TACACS+ 認証サーバーで作成されていることを確認します。

TACACS+ 認証を設定するには、「構成」>「アプライアンスの設定」>「管理インタフェース」>「**TACACS+** 」に移動し、「**TACACS+** を有効にする」をクリックします。

> 注
>
> サイトで RADIUS 認証または TACACS+ 認証を有効にできます。両方を同時に有効にすることはできません。

1. ユーザ名とパスワードを TACACS+ サーバに送信する暗号化方式を選択します。
2. TACACS+ サーバのホスト IP アドレスと認証ポート番号を指定します。デフォルトのポート番号は 49 です。
3. サーバーキーを入力して確認します。TACACS+ サーバへの接続に使用される秘密鍵です。
4. TACACS+ サーバからの認証応答を待機する時間間隔を指定します。タイムアウト値は 60 秒以下である必要があります。

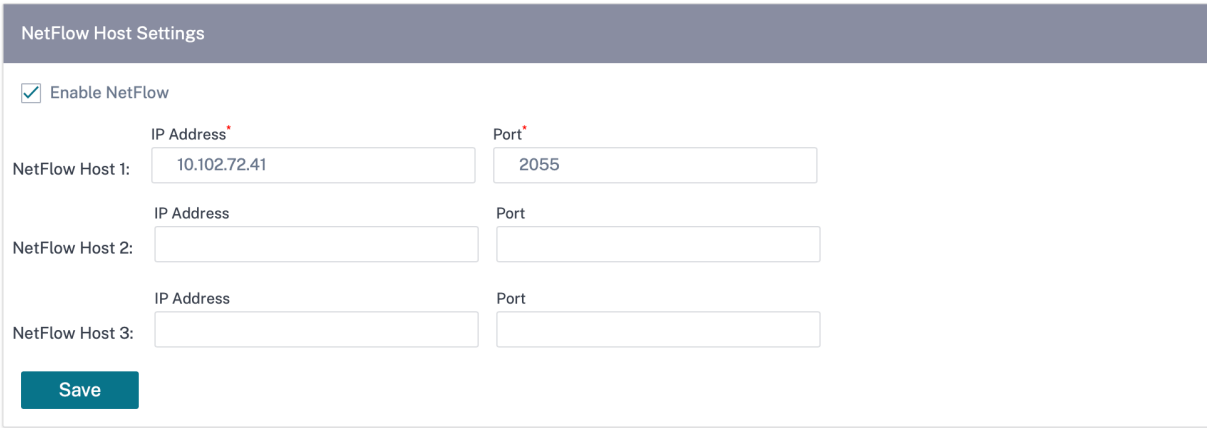
> 注
>
> 認証タイプ、サーバーキー、およびタイムアウト設定は、構成されているすべてのサーバーに適用されます。



NetFlow ホストの設定

NetFlow コレクタは、SD-WAN インターフェイスに出入りすると、IP ネットワークトラフィックを収集します。NetFlow データを使用して、トラフィックの送信元と宛先、サービスクラス、およびトラフィック輻輳の原因を特定できます。詳細については、マルチ NetFlow コレクタを参照してください。

最大 3 つの NetFlow ホストを設定できます。NetFlow ホスト設定を行うには、[構成] > [アプライアンス設定] > **[NetFlow** ホスト設定] に移動します。[**NetFlow** を有効にする] を選択し、NetFlow ホストの IP アドレスとポート番号を指定します。

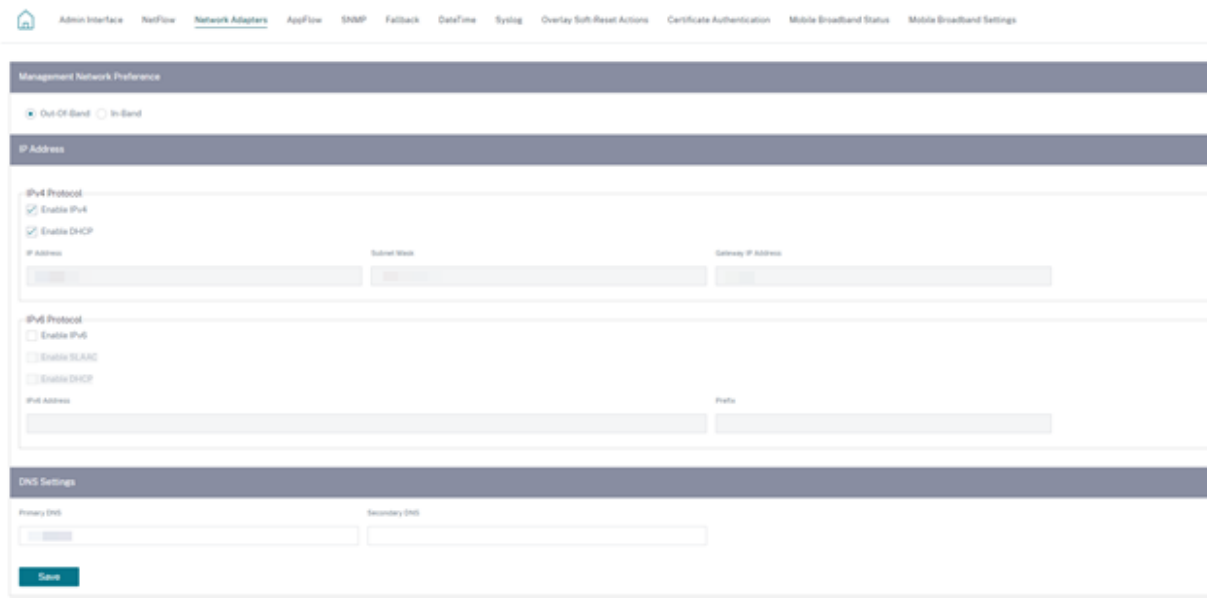


ネットワーク・アダプタ

Citrix SD-WAN アプライアンスの場合、管理ネットワーク設定、管理 IP アドレス、およびその他のネットワークパラメータを手動で変更できます。アプライアンスの IPv4 アドレス、サブネットマスク、ゲートウェイ IP アドレス、IPv6 アドレス、プレフィックスを変更したり、DHCP または SLAAC（IPv6 アドレスのみ）を有効にして IP アドレスを自動的に取得したりできます。詳しくは、「動的ホスト構成プロトコル」を参照してください。

> 注
>
> - インターフェイスが帯域内管理に使用されている場合、IP アドレスは変更できません。帯域内管理の詳細については、「帯域内管理」を参照してください。
> - 帯域内オプションは、データポートを帯域内管理ポートとして設定し、インターネットサービスが設定されている場合にのみ機能します。管理設定を設定する前に、SD-WAN アプライアンスの帯域内管理をサポートする構成があることを確認してください。
> - アプライアンスが 11.4.2 以降のソフトウェアバージョンを実行している場合は、管理ネットワーク設定（帯域内および帯域外）セクションが表示されます。

ネットワークアダプタ設定を行うには、構成 > アプライアンス設定 > ネットワークアダプタに移動します。



AppFlow ホスト設定

AppFlow および IPFIX は、ネットワークインフラストラクチャ内のアプリケーションおよびトランザクションデータを識別および収集するために使用されるフローエクスポート標準です。このデータにより、アプリケーショントラフィックの使用率とパフォーマンスの可視性が向上します。

収集されたデータは、フローレコードと呼ばれ、1 つ以上の IPv4 コレクタに送信されます。コレクターはフローレコードを集約し、リアルタイムレポートまたは履歴レポートを生成します。詳細については、「AppFlow と IPFIX」を

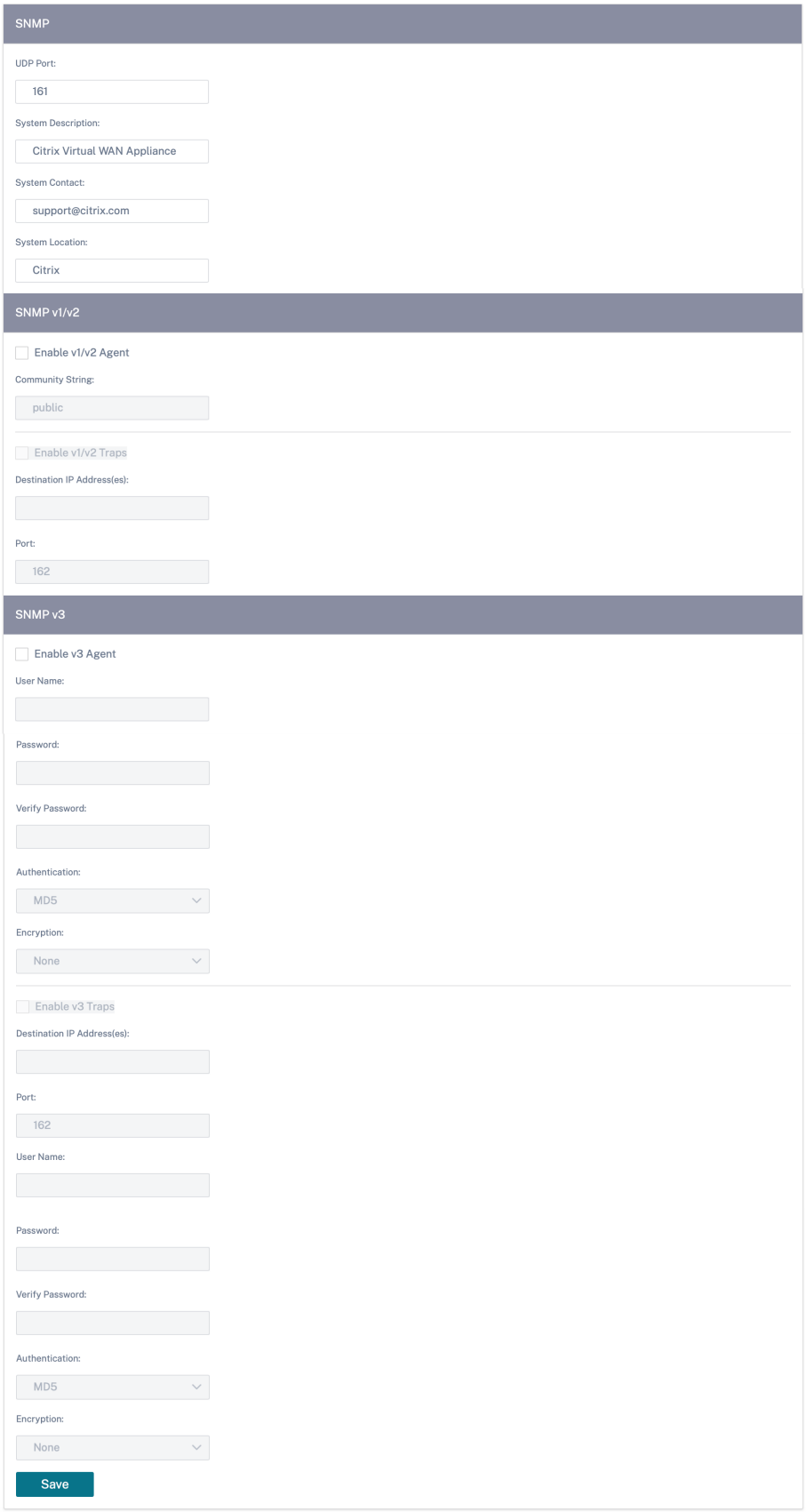
参照してください。

SNMP

SNMP は、ネットワークデバイス間で管理情報を交換するために使用されます。SNMPv1 は、SNMP プロトコルの最初のバージョンです。SNMPv2 は改訂されたプロトコルで、プロトコルパケットタイプ、トランスポートマッピング、MIB 構造要素の機能強化が含まれています。SNMPv3 は、SNMP のセキュアバージョンを定義します。SNMPv3 プロトコルは、SNMP エンティティのリモート設定も容易にします。

SNMP エージェントは、アプライアンスからローカルで管理情報を収集し、クエリーが行われるたびに SNMP マネージャに送信します。エージェントは、アプライアンス上で緊急イベントを検出すると、データのクエリーを待たずにマネージャに警告メッセージを送信します。この緊急メッセージはトラップと呼ばれます。必要な SNMP バージョンエージェントと対応するトラップを有効にし、必要な情報を入力します。詳細については、「SNMP」を参照してください。

SNMP 設定を構成するには、「構成」>「アプライアンス設定」>「**SNMP**」に移動します。

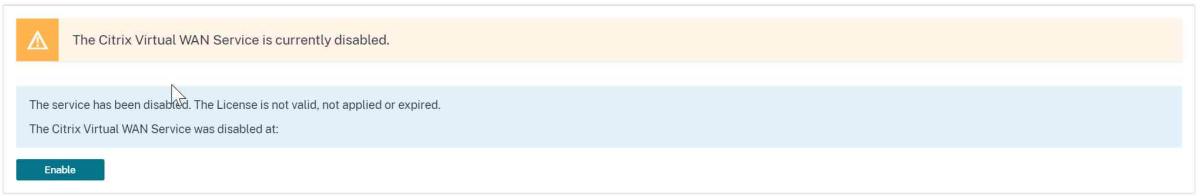


フォールバック構成

フォールバック設定により、リンク障害、設定の不一致、またはソフトウェアの不一致が発生した場合でも、アプライアンスはゼロタッチ展開サービスに接続したままになります。フォールバック構成は、デフォルト構成プロファイルを持つアプライアンスではデフォルトで有効になっています。また、既存の LAN ネットワーク設定に従ってフォールバック構成を編集することもできます。詳しくは、「フォールバック構成」を参照してください。

フロー

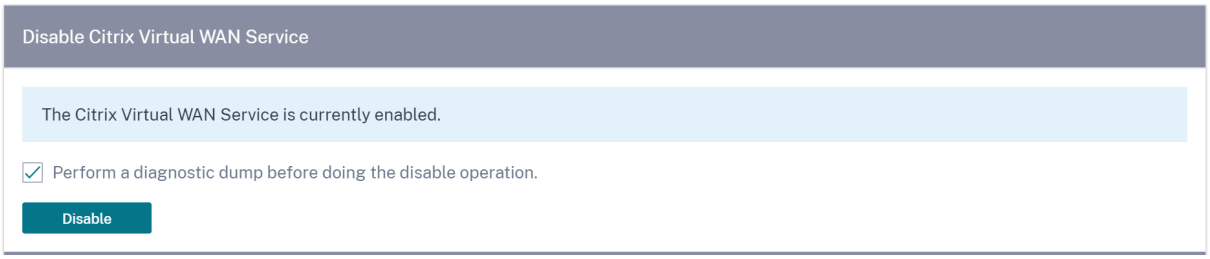
フローセクションでは、アプライアンス上の Citrix Virtual WAN サービスを有効または無効にできます。サービスを有効にすると、仮想 WAN デーモンが有効になり、起動します。サービスが無効になっている場合は、Citrix Virtual WAN サービスを有効にするオプションを使用できます。



Citrix 仮想 **WAN** サービスを無効にする

Citrix Virtual WAN サービスを無効にするオプションは、サービスが有効になっている場合に使用できます。サービスを無効にすると、アプライアンスの仮想 WAN デーモンが停止します。

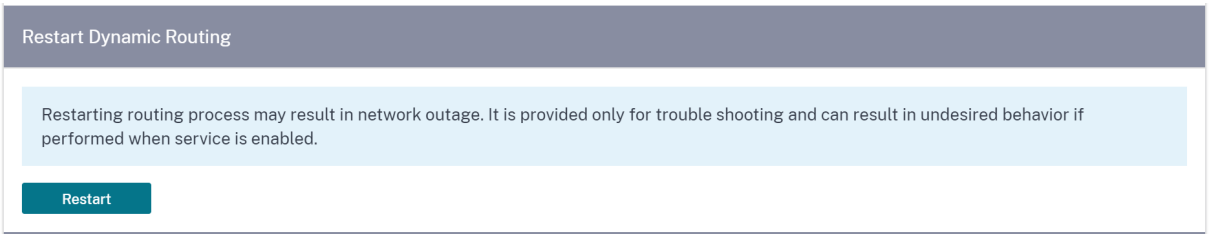
Citrix Virtual WAN サービスを無効にする前に、仮想 WAN ネットワークの診断ダンプを収集することを選択できます。



動的ルーティングを再起動

ダイナミックルートラーニングプロセスは、OSPF および BGP ルーティングプロトコルを使用して再開できます。ダイナミックルーティングを再起動するオプションは、トラブルシューティングのみを目的としています。

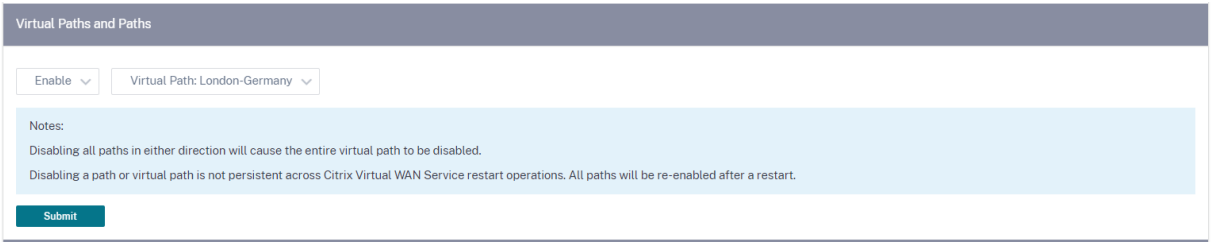
> 警告
>
> 動的ルーティングを再起動すると、ネットワークが停止する可能性があります。



仮想パス

2 つのサイト間の仮想パスを有効にするか無効にするかを選択できます。基になる個々のパス（どちらの方向でも）を選択することも、オーバーレイ仮想パスを選択することもできます。個々のパスを無効にすると、仮想パス全体が無効になります。

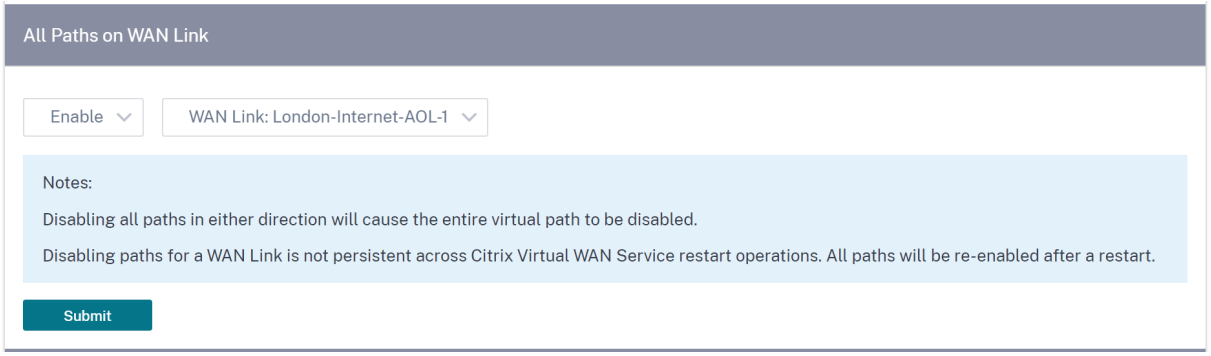
> 注
>
> Citrix 仮想 WAN サービスを再起動すると、すべてのパスが再び有効になります。



WAN リンク上のすべてのパス

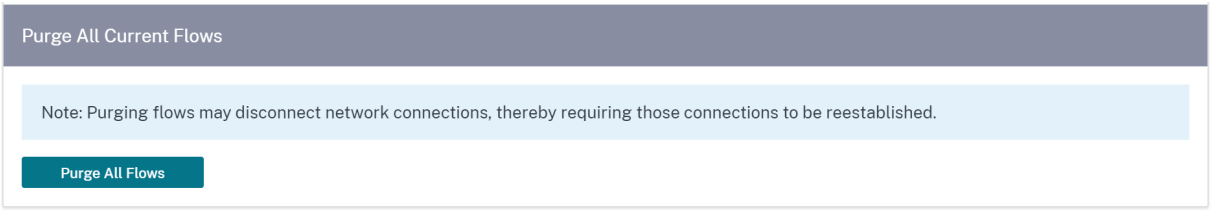
2 つのサイト間の WAN リンクを有効または無効にできます。すべての WAN リンクを無効にすると、仮想パスが無効になります。

> 注
>
> Citrix 仮想 WAN サービスを再起動すると、すべての WAN リンクが再び有効になります。



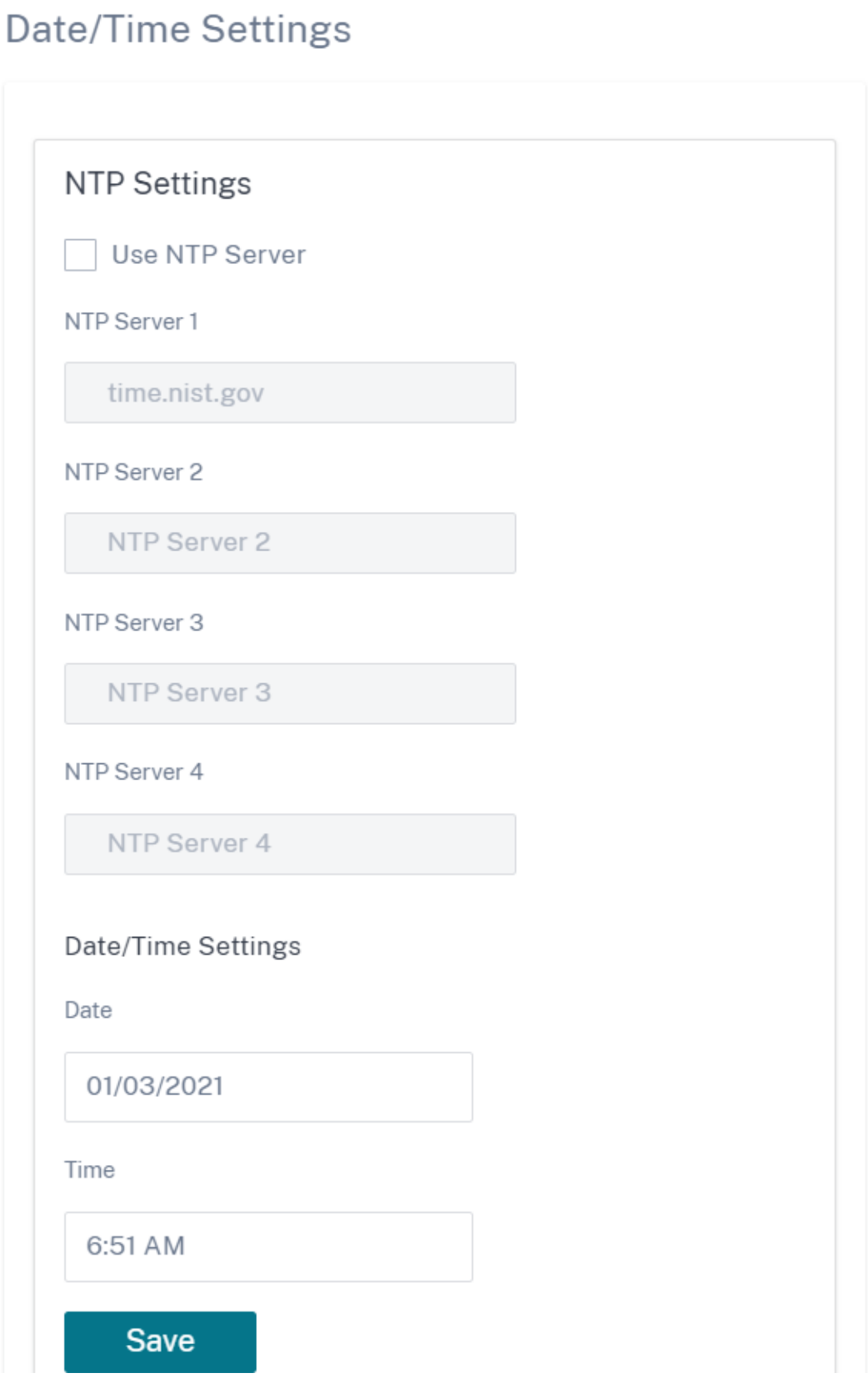
現在のフローをすべて消去

フローを削除すると、現在のフローがすべて終了し、フローテーブルがクリアされ、フロー接続が再確立され、フローテーブルが再入力されます。

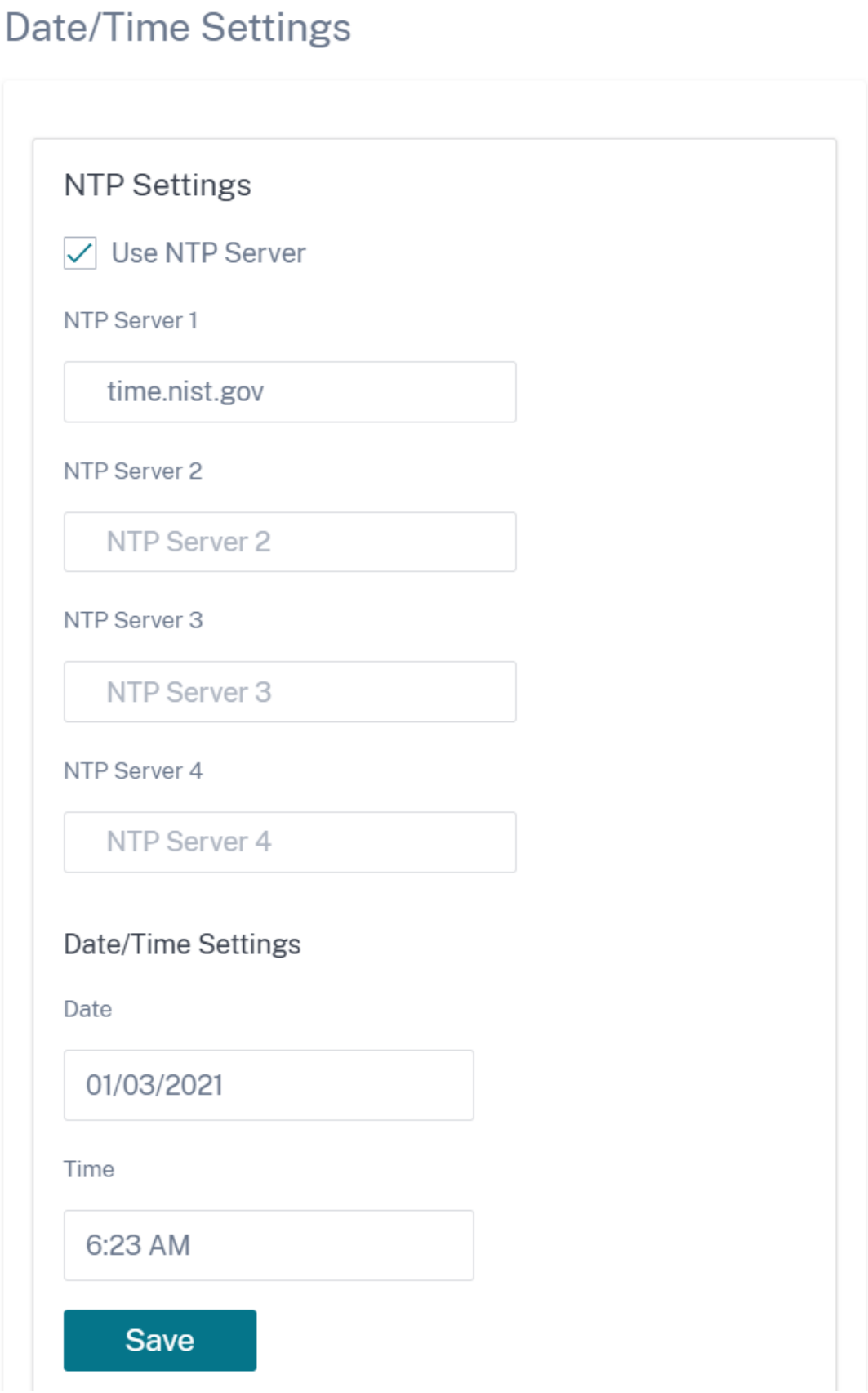


日付と時刻

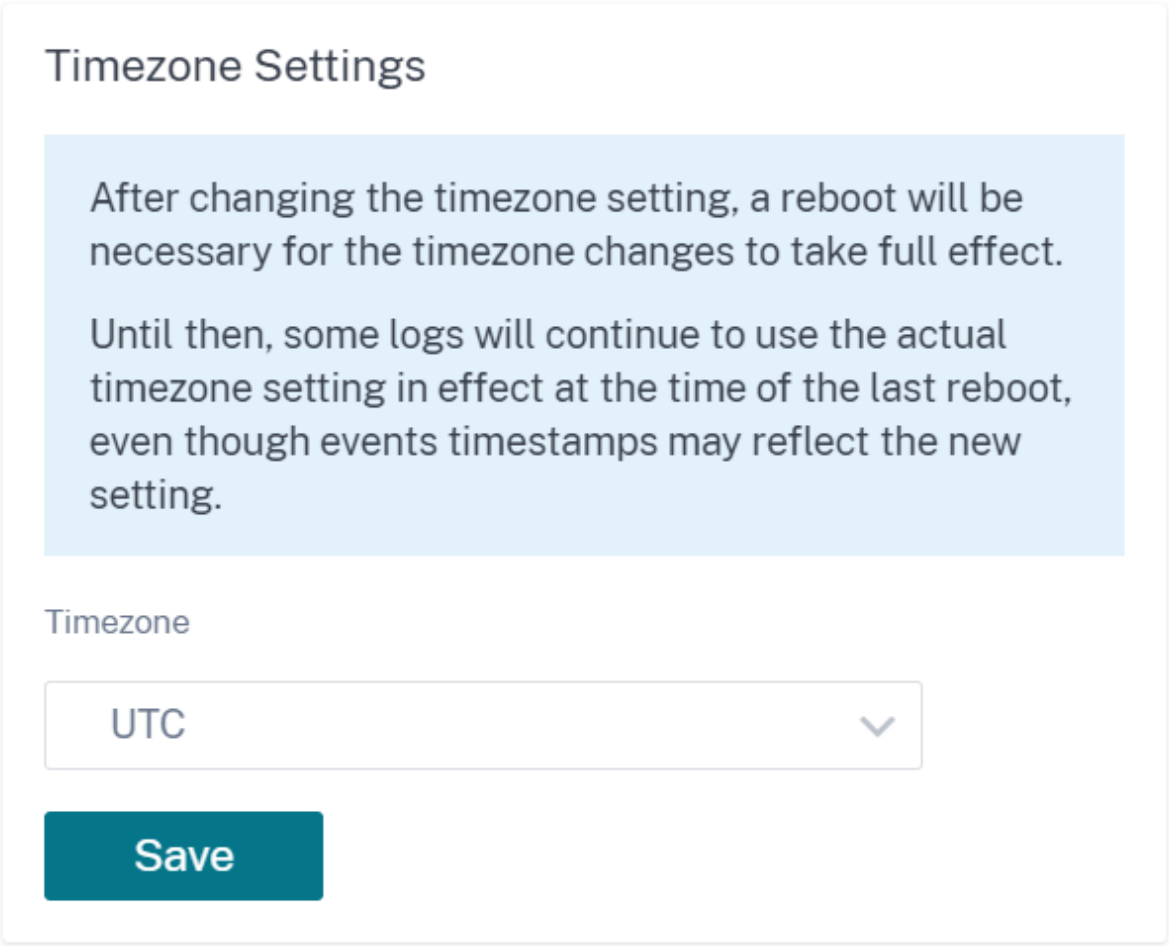
アプライアンスの日付と時刻は、手動で変更することも、NTP サーバーを使用して変更することもできます。日付と時刻を手動で設定するには、「**NTP** サーバーを使用」オプションが選択されていないことを確認し、日付と時刻を指定します。



「**NTP** サーバーを使用」オプションを選択した場合、現在の日付と時刻を手動で入力することはできません。NTP サーバは 4 つまで指定できますが、少なくとも 1 つは指定する必要があります。これらはバックアップ NTP サーバーとして機能し、一方のサーバーがダウンした場合、アプライアンスはもう一方の NTP サーバーと自動的に同期します。NTP サーバーのドメイン名を指定する場合、DNS サーバーも設定する必要があります。ただし、まだ設定していない場合は別です。

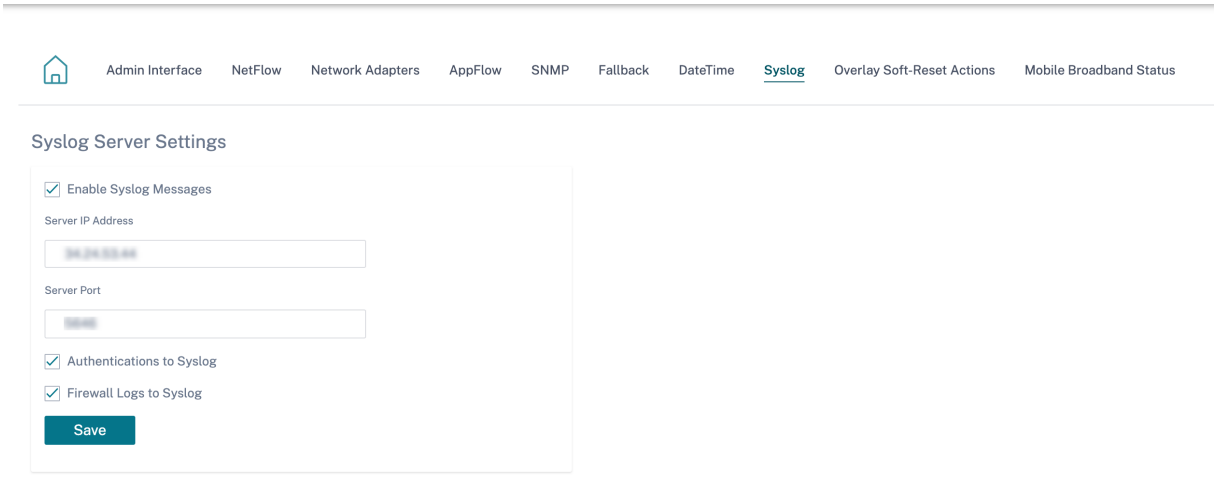


タイムゾーンを変更する必要がある場合は、日付と時刻を設定する前に変更してください。そうしないと、設定が保持されません。タイムゾーンを変更したら、アプライアンスを再起動します。



Syslog サーバー設定

Citrix SD-WAN Orchestrator サービスを使用して SD-WAN アプライアンスの Syslog サーバー設定を構成できます。Syslog 設定を有効にすると、SD-WAN アプライアンスのシステムアラートとイベント詳細を外部 Syslog サーバーに送信できます。ただし、SD-WAN アプライアンスの UI で [構成] > [アプライアンス設定] > [ログ/監視] > [アラームオプション] に移動して、イベントタイプを選択する必要があります。詳細については、「アラームの設定」を参照してください。



次の Syslog サーバー設定は、Citrix SD-WAN Orchestrator サービスを通じて構成できます。

- **Syslog** メッセージを有効にする:Syslog サーバーへのログまたはイベントメッセージの送信を有効または無効にします。
- サーバー **IP** アドレス:Syslog サーバーの IP アドレス。
- サーバーポート:Syslog サーバーのポート番号。
- **Syslog** への認証:Syslog サーバーへの認証ログまたはイベントメッセージの送信を有効または無効にします。
- **Syslog** へのファイアウォールログ:Syslog サーバーへのファイアウォールログの送信を有効または無効にします。

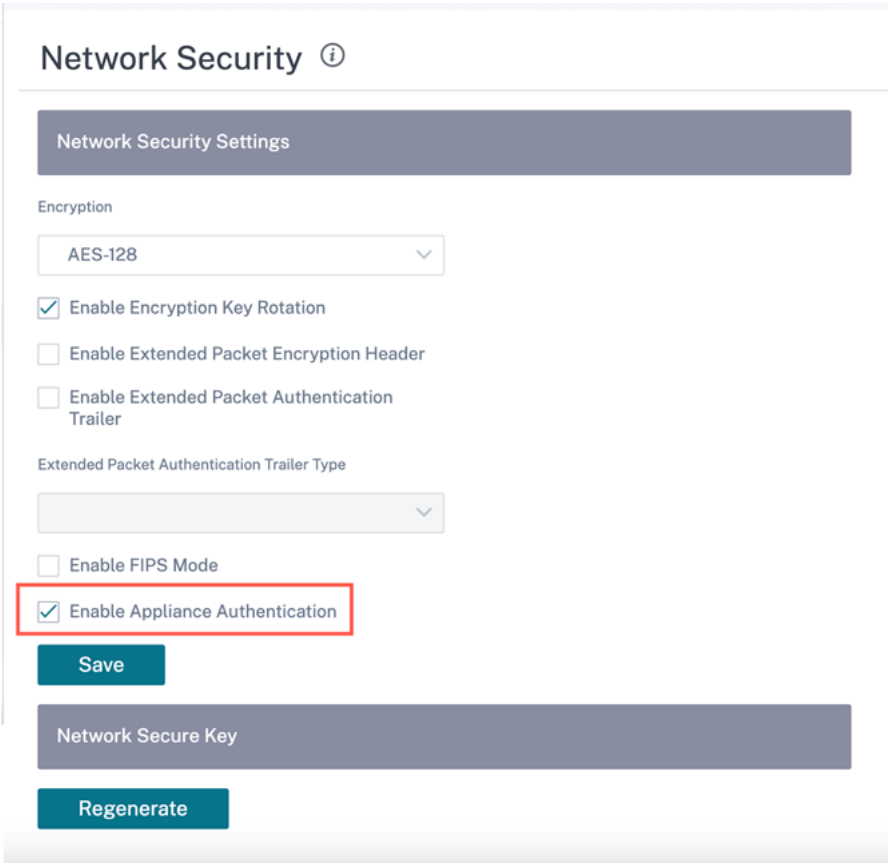
証明書の認証

Citrix SD-WAN Orchestrator サービスは、ネットワーク暗号化や仮想パス IPsec トンネルなどのセキュリティ技術を使用して、SD-WAN ネットワーク内のアプライアンス間に安全なパスを確立します。既存のセキュリティ対策に加えて、Citrix SD-WAN Orchestrator サービスでは証明書ベースの認証が導入されています。

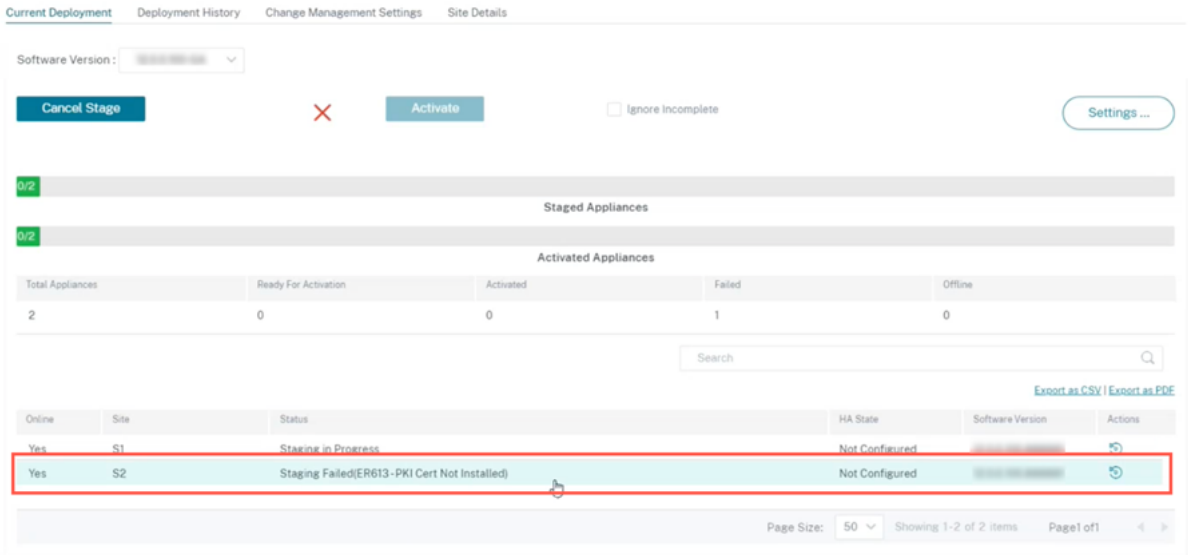
証明書認証により、組織はプライベート認証局（CA）によって発行された証明書を使用してアプライアンスを認証できます。アプライアンスは、仮想パスを確立する前に認証されます。たとえば、ブランチアプライアンスがデータセンターに接続しようとしたときに、ブランチからの証明書がデータセンターで想定される証明書と一致しない場合、仮想パスは確立されません。

CA によって発行された証明書は、公開鍵をアプライアンスの名前にバインドします。公開キーは、証明書で識別されるアプライアンスが所有する対応する秘密キーで動作します。

アプライアンス認証をネットワークレベルで有効にするには、[構成] > [セキュリティ] > [** ネットワークセキュリティ **] に移動し、[アプライアンス認証を有効にする] を選択します。[保存] をクリックします。

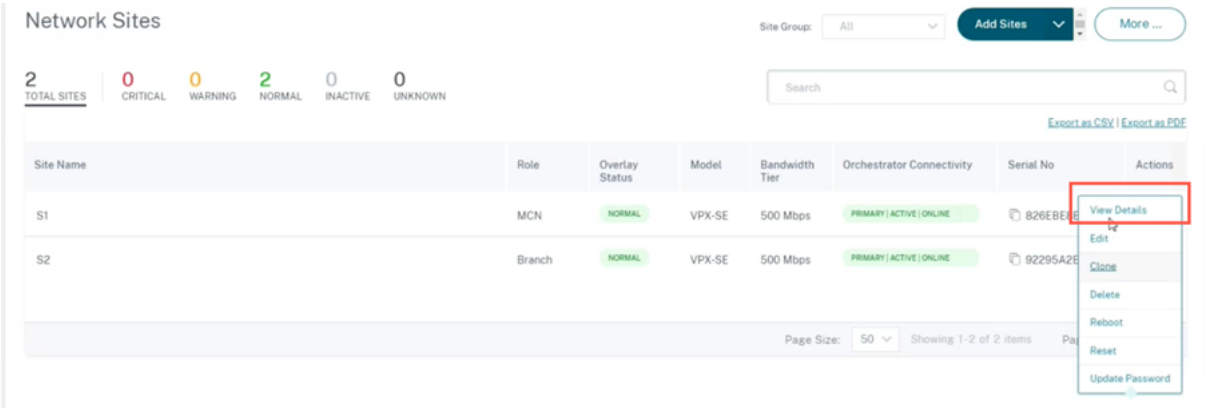


デプロイ中に、アプライアンス認証が有効になっていても PKI 証明書がアプライアンスにインストールされていない場合、ステージングは失敗ステータスと表示されます。

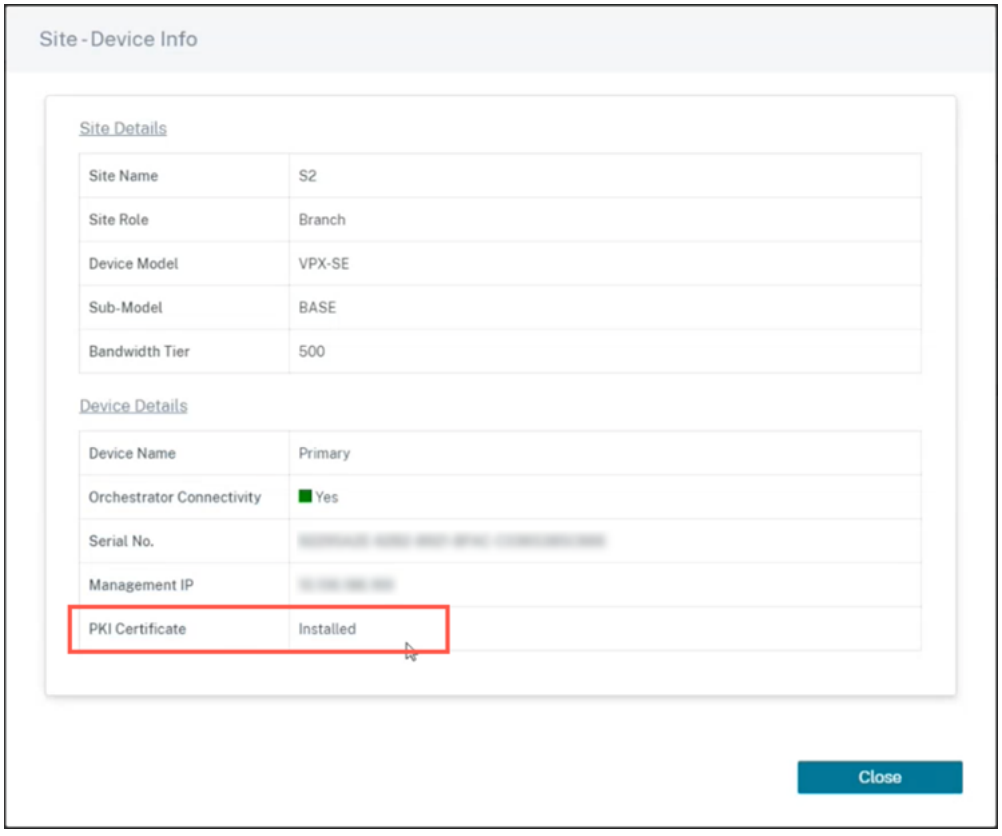


証明書を表示

デバイスの詳細ページに移動して、PKI 証明書がインストールされているかどうかを確認できます。そのためには、[構成] > [ネットワークホーム] に移動し、証明書を検証するサイトのアクションアイコンをクリックし、[詳細を表示] をクリックします。



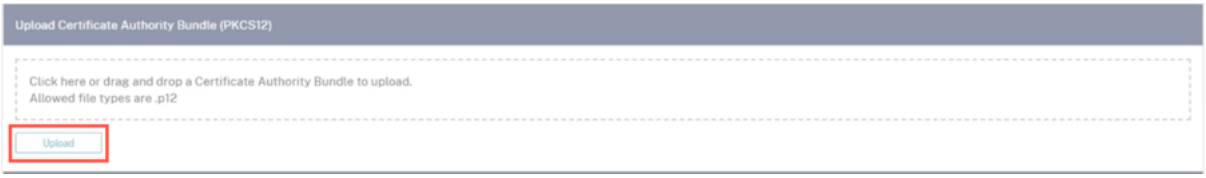
次の画面には、サイトとデバイスの詳細が表示されます。



「デバイスの詳細」セクションでは、PKI 証明書のインストール状況を確認できます。

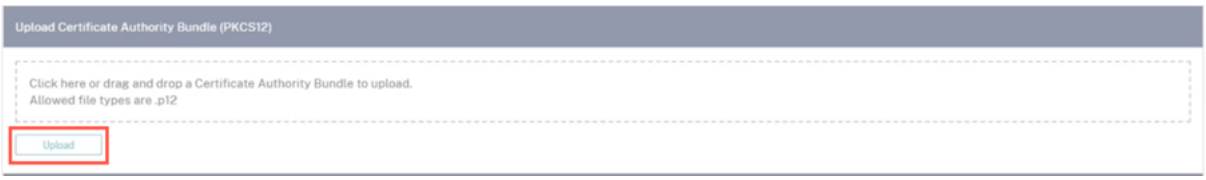
ID バンドルのアップロード

Identity バンドルには、秘密鍵と秘密鍵に関連付けられた証明書が含まれます。CA によって発行されたアプライアンス証明書をアプライアンスにアップロードできます。証明書バンドルは、拡張子が.p12 の PKCS12 ファイルです。パスワードで保護することを選択できます。PKCS12 ファイルをドラッグアンドドロップし、パスワードを入力して [アップロード] をクリックします。パスワードフィールドを空白のままにすると、パスワード保護なしとして扱われます。



認証局バンドルのアップロード

証明書署名機関に対応する PKCS12 バンドルをアップロードします。認証局バンドルには、署名のチェーン全体、ルート、およびすべての中間署名機関が含まれています。PKCS12 バンドルをドラッグし、[アップロード] をクリックします。



証明書署名リクエストの作成

アプライアンスは署名されていない証明書を生成し、証明書署名要求（CSR）を作成できます。アプライアンスの CSR を作成するには、組織名、部署、町/市、都道府県/地域/郡/市、国、および電子メールアドレスを入力します。アプライアンスの共通名は、自動的に入力され、編集できないサイト名です。[**Create CSR**] をクリックします。

証明書署名リクエストの管理

CSR がバックエンドから正常に生成されたら、アプライアンスから CSR をダウンロードして CA による署名を取得し、PEM または DER 形式でアプライアンスにアップロードし直す必要があります。これは、アプライアンスのアイデンティティ証明書として使用されます。まず CA をアップロードして証明書に署名します。

CA がアップロードされたら、署名された CSR をアップロードします。

証明書失効リストマネージャ

証明書失効リスト (CRL) は、ネットワークで有効でなくなった証明書のシリアル番号の公開リストです。CRL ファイルは定期的にダウンロードされ、すべてのアプライアンスにローカルに保存されます。証明書が認証されると、応答側は CRL を調べて、イニシエータ証明書がすでに失効しているかどうかを確認します。Citrix SD-WAN は現在、PEM および DER 形式のバージョン 1 の CRL をサポートしています。

CRL を有効にするには、「CRL 有効」チェックボックスを選択します。CRL ファイルが維持される場所を指定します。HTTP、HTTPS、および FTP の場所がサポートされています。CRL ファイルを確認およびダウンロードする間隔を指定します。範囲は 1 ～1440 分です。「アップロード設定」をクリックします。

> 注:
>
> virtua1 パスの再認証期間は 10 ～15 分です。CRL の更新間隔を短く設定すると、更新される CRL リストに現在アクティブなシリアル番号が含まれることがあります。使用頻度の低い証明書をネットワークで短期間使用できるようにします。

モバイルブロードバンド設定

Citrix SD-WAN Orchestrator サービスを使用すると、モバイルブロードバンド接続を使用して、Citrix SD-WAN アプライアンスをブランチサイトからネットワークに接続できます。

モバイルブロードバンド設定を行うには、サイトレベルで [構成] > [アプライアンス設定**] > [**モバイルブロードバンド設定**]** に移動します。

現在、モバイルブロードバンド設定は Citrix SD-WAN 110 および Citrix SD-WAN-210 アプライアンスで構成できます。

Citrix SD-WAN Orchestrator サービスでは、次のモバイルブロードバンド設定を構成できます。

SIM 暗証番号ステータス

PIN でロックされている SIM カードを挿入した場合、SIM の状態は [有効**]** になります。SIM PIN で認証されるまで、SIM カードは使用できません。SIM PIN は通信事業者から入手できます。[**Verify**] をクリック します。

配送業者が提供した SIM PIN を入力し、[確認] をクリックします。

SIM PIN を無効にする　SIM PIN が有効で検証されている SIM の SIM PIN 機能を無効にすることができます。[無効化] をクリックします。SIM PIN を入力して [無効化] をクリックします。

SIM PIN を有効にする　SIM PIN を有効にするには、「有効にする」をクリックします。通信事業者から提供された SIM PIN を入力し、[有効] をクリックします。

SIM PIN の状態が **[**有効**]** と **[**未検証] に変わる場合は、PIN が検証されていないことを意味し、PIN が確認されるまで操作を実行できません。

PIN を確認をクリックします。通信事業者から提供された SIM PIN を入力し、[**PIN** の確認] をクリックします。

SIM PIN の変更　PIN が有効で確認済みの状態になったら、 PIN の変更を選択できます。

[修正**]** をクリックします。通信事業者から提供された SIM PIN を入力します。新しい SIM PIN を入力し、確認します。[修正**]** をクリックします。

SIM のブロック解除　SIM PIN を忘れた場合、通信事業者から取得した SIM PUK を使用して SIM PIN をリセットすることができます。

SIM のブロックを解除するには、[ブロック解除] をクリックします。通信事業者から入手した SIM PIN と SIM PUK を入力し、「ブロック解除」をクリックします。

> 注
>
> SIM カードは、SIM のブロックを解除しながら、PUK を 10 回失敗すると永久にブロックされます。新しい SIM カードについては、通信事業者のサービスプロバイダーにお問い合わせください。

APN 設定

APN 設定を構成するには、通信事業者から提供された APN、ユーザー名、パスワード、認証を入力します。**PAP**、**CHAP**、または ****PAPCHAP** 認証プロトコルから選択できます。通信事業者が認証タイプを提供していない場合は、**[**** なし**]** に設定します。

ネットワーク設定

内部モデムをサポートする Citrix SD-WAN アプライアンス上のモバイルネットワークを選択できます。

ローミング

ローミングオプションは、お使いのデバイスではデフォルトで有効になっています。無効にすることもできます。

ファームウェアの管理

LTE が有効になっているすべてのアプライアンスには、使用可能なファームウェアのセットがあります。既存のファームウェアのリストから選択するか、ファームウェアをアップロードして適用することができます。使用するファームウェアがわからない場合は、AUTO-SIM オプションを選択して、LTE モデムがアプライアンスに挿入されている SIM カードに基づいて最も一致するファームウェアを選択できるようにします。

> 注
>
> 現在、ファームウェアは SD-WAN SE 210 LTE アプライアンスにのみ適用できます。

モデムの有効化/無効化

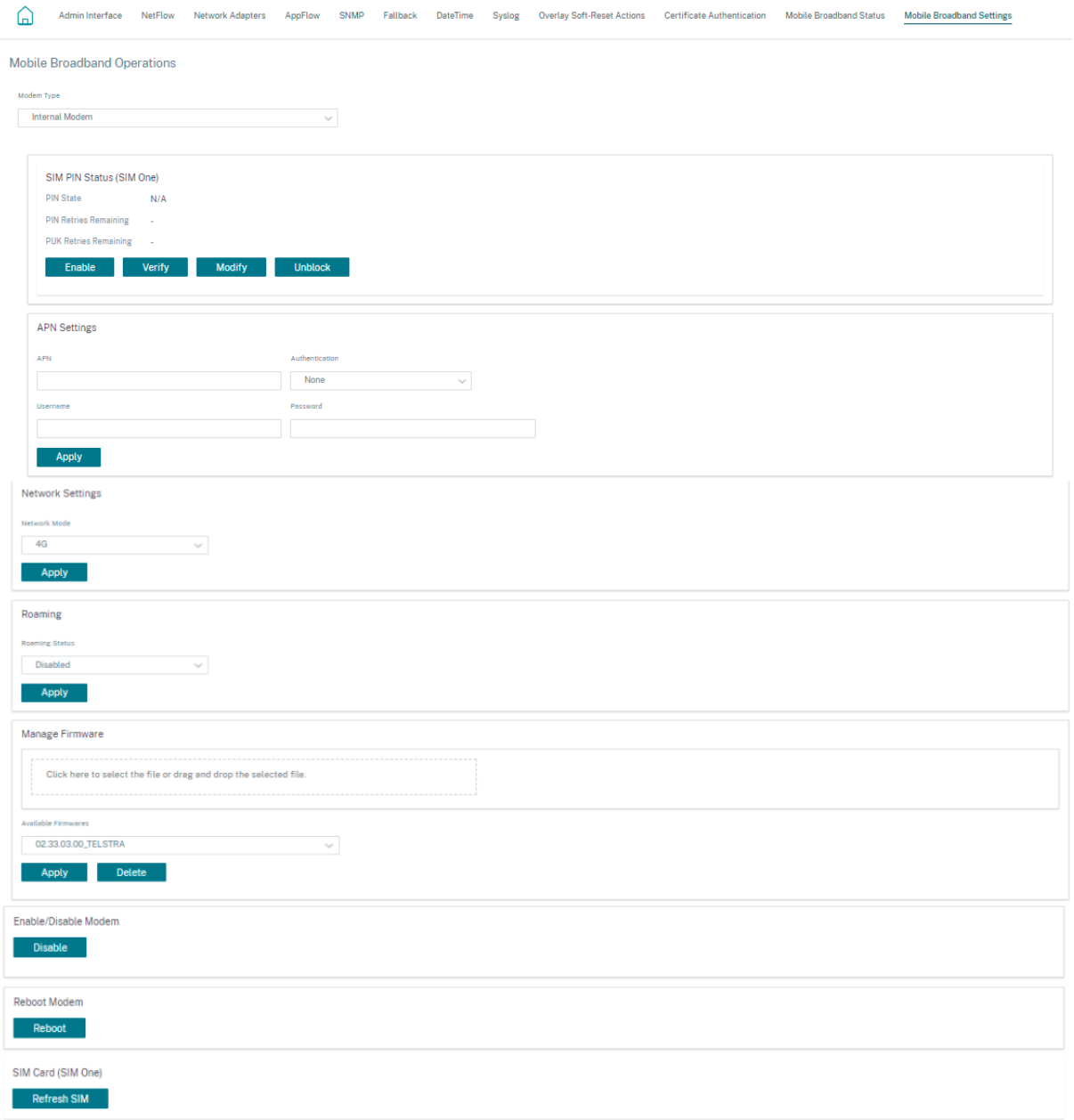
ブロードバンド機能を使用する目的に応じて、モデムを有効または無効にします。デフォルトでは、モデムは有効になっています。

モデムの再起動

モデムをリブートします。このプロセスは、再起動操作が完了するまでに最大 3 ～5 分かかることがあります。

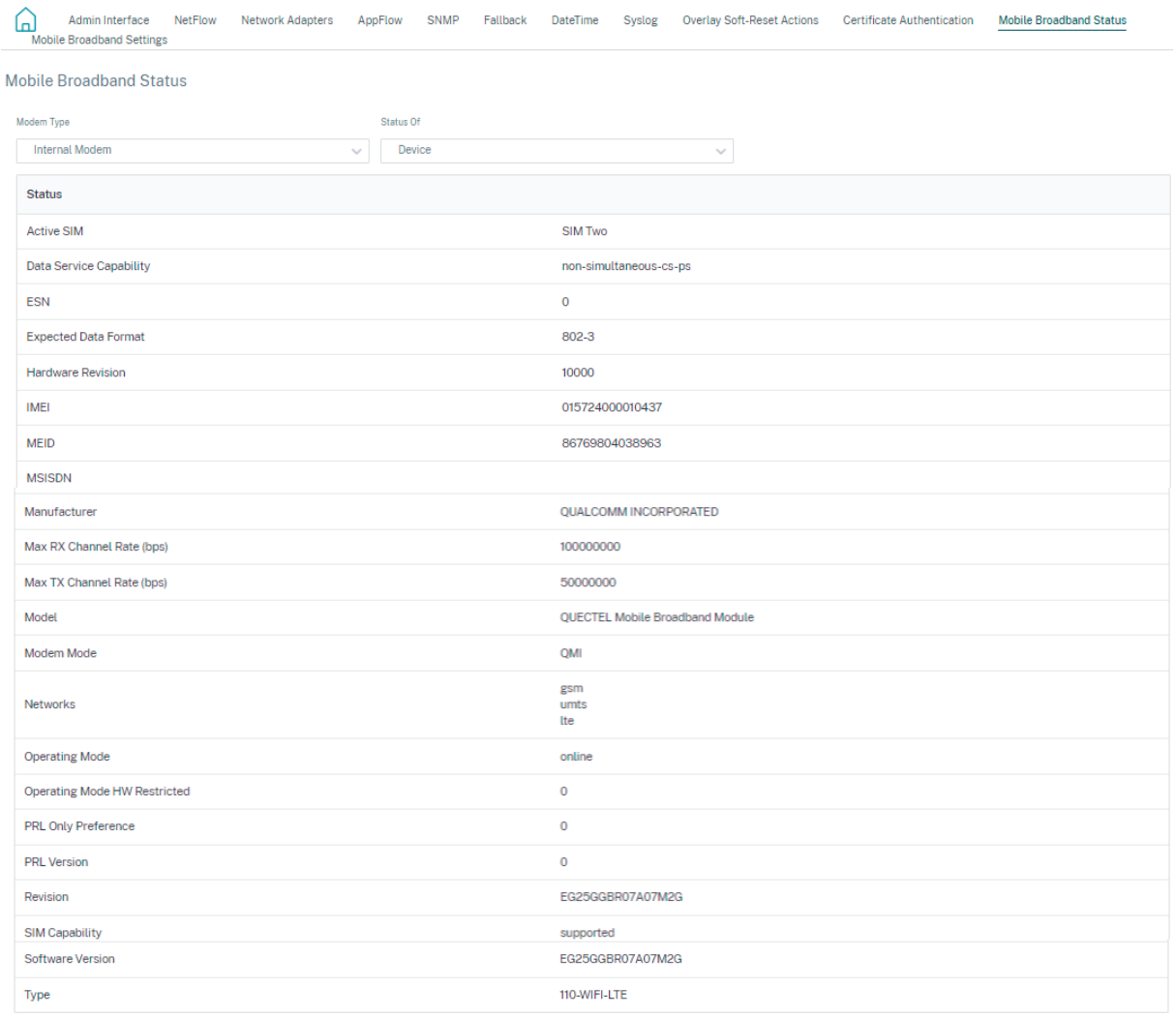
SIM のリフレッシュ

このオプションは、SIM カードをホットスワップして新しい SIM カードを検出する場合に使用します。



モバイルブロードバンドステータス

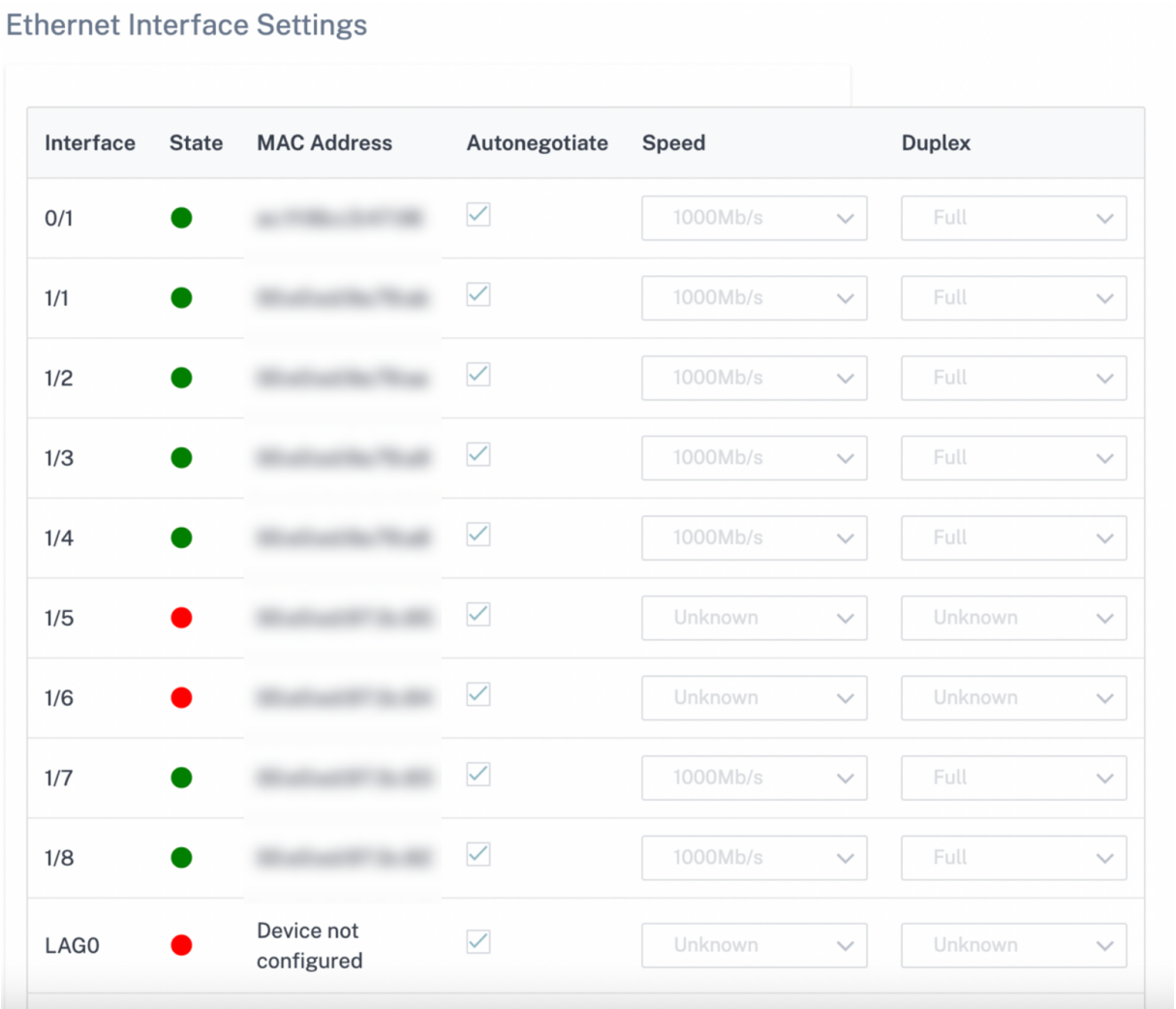
モバイルブロードバンドステータスセクションには、ブロードバンド構成設定のステータスが表示されます。モバイルブロードバンドステータスを表示するには、サイトレベルで [構成] > [アプライアンス設定] **>** [モバイルブロードバンドステータス] に移動します。デバイスとアクティブな SIM の状態を表示できます。



イーサネットインターフェイス設定

Ethernet Interface status セクションには、イーサネットポートの接続ステータス、インターフェイスタイプ、MAC アドレス、オートネゴシエーション、およびデュプレックス設定情報が表示されます。イーサネットインターフェイス設定を表示するには、サイトレベルで [構成] > [アプライアンス設定**] > [**イーサネットインターフェイス設定**]** に移動します。管理上ダウンしているポートは赤色で表示されます。

> 注**:**
>
> この設定は現在、Citrix SD-WAN Orchestrator サービス UI では読み取り専用モードで使用できます。イーサネットインターフェイスの設定を変更する場合は、SD-WAN アプライアンスの新しいユーザーインターフェイスを使用して変更できます。



帯域内管理

October 26, 2022

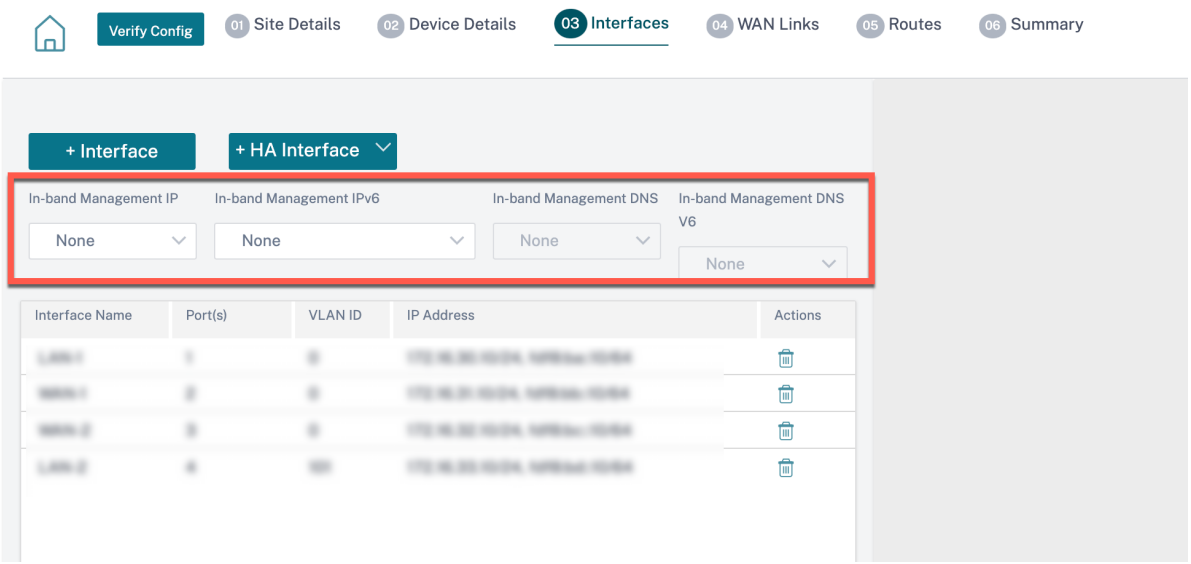
Citrix SD-WAN Orchestrator サービスを使用すると、SD-WAN アプライアンスを帯域外管理と帯域内管理の 2 つの方法で管理できます。アウトオブバンド管理では、管理トラフィックだけを伝送する管理用に予約されたポートを使用して管理 IP を作成できます。インバンド管理では、SD-WAN データポートを管理に使用できます。追加の管理パスを設定することなく、データトラフィックと管理トラフィックの両方を伝送します。

インバンド管理では、仮想 IP アドレスが Web UI や SSH などの管理サービスに接続できます。IP サービスの使用が有効になっている信頼できるインターフェイスで、帯域内管理を有効にできます。管理 IP とインバンド仮想 IP を使用して、Web UI と SSH にアクセスできます。

> 注
>
> Citrix SD-WAN Orchestrator サービスの帯域内管理は、Citrix SD-WAN 11.1.1 以降でサポートされています。

仮想 IP の帯域内管理を有効にするには、サイトレベルで [構成] > [****** サイト構成 **] > [インターフェイス] に移動します。帯域内管理ポートとして使用する仮想 IP を選択します。インバンド管理 **IP** またはインバンド管理 **IPv6** を使用して Web UI と SSH にアクセスできます。

> 注
>
> 帯域内管理は、LAN ポートだけでサポートされます。



仮想 IP アドレスの設定手順の詳細については、「インターフェイス」を参照してください。

帯域内管理 IP は、バックアップ管理 IP としても機能します。管理ポートにデフォルト Gateway が設定されていない場合、管理 IP アドレスとして使用されます。帯域内管理プレーンを介したすべての DNS 要求の転送先となる DNS プロキシを選択します。DNS プロキシの設定については、「DNS プロキシ」を参照してください。

Citrix SD-WAN Orchestrator サービスへのアプライアンス接続が管理ポートと帯域内ポートを切り替えるユースケースでは、**Citrix SD-WAN**Orchestrator サービスの接続が中断されないようにインバンド管理 DNS またはインバンド管理 DNS V6 を構成します。

帯域内 **Provisioning**

SD-WAN アプライアンスを家庭や小規模の支店などのシンプルな環境に導入する必要性が大幅に高まっています。シンプルな展開のために個別の管理アクセスを構成すると、オーバーヘッドが増えます。ゼロタッチ導入とインバン

ド管理機能により、指定されたデータポートを介した Provisioning と設定管理が可能になります。ゼロタッチ配置は、指定されたデータポートでサポートされ、ゼロタッチ配置用に別の管理ポートを使用する必要はありません。

データポートまたは管理ポートをインターネットに接続することで、インバンド Provisioning をサポートする、出荷時の状態のアプライアンスをプロビジョニングできます。インバンド Provisioning をサポートするアプライアンスには、LAN および WAN 用の特定のポートがあります。工場出荷時の状態にリセットされたアプライアンスには、ゼロタッチデプロイメントサービスとの接続を確立できるデフォルト設定があります。LAN ポートは DHCP サーバーとして機能し、DHCP クライアントとして機能する WAN ポートにダイナミック IP を割り当てます。WAN リンクは、Quad 9 DNS サービスを監視して WAN 接続を決定します。

IP アドレスが取得され、ゼロタッチ展開サービスとの接続が確立されると、構成パッケージがダウンロードされ、アプライアンスにインストールされます。Citrix SD-WAN Orchestrator サービスを介したゼロタッチ展開については、「ゼロタッチ展開」を参照してください。

> 注
>
> - インバンド Provisioning はすべてのプラットフォームに適用されます。ただし、デフォルトの構成は、Citrix SD-WAN 110 および VPX プラットフォームでのみ有効になります。これは、他のプラットフォームには古いソフトウェアバージョンが付属しているためです。
> - データポートを介した SD-WAN アプライアンスの日 0Provisioning では、アプライアンスソフトウェアのバージョンが Citrix SD-WAN 11.1.1 以降である必要があります。

工場出荷時リセット状態のアプライアンスのデフォルト設定には、次の設定が含まれます。

- LAN ポート上の DHCP サーバ
- WAN ポート上の DHCP クライアント
- DNS の QUAD9 構成
- 工場出荷時のイメージを持つ Citrix SD-WAN アプライアンスの場合、デフォルトの LAN IP は 192.168.101.1/24 です。
- 工場出荷時のイメージを持つ Citrix SD-WAN 110 アプライアンスの場合、デフォルトの LAN IP は 192.168.0.1/24 です。
- 35 日間の猶予ライセンス

アプライアンスがプロビジョニングされると、デフォルトの構成は無効になり、ゼロタッチデプロイメントサービスから受信した設定によって上書きされます。アプライアンスライセンスまたは猶予ライセンスの有効期限が切れると、デフォルト設定がアクティブ化され、アプライアンスがゼロタッチ展開サービスに接続されたままになり、ライセンス管理されたサービスを受け取るようになります。

フォールバック構成

フォールバック設定により、リンク障害、設定の不一致、またはソフトウェアの不一致が発生した場合でも、アプライアンスはゼロタッチ展開サービスに接続したままになります。フォールバック構成は、デフォルト構成プロファイ

ルを持つアプライアンスではデフォルトで有効になっています。また、既存の LAN ネットワーク設定に従ってフォールバック構成を編集することもできます。

フォールバック構成では、次のシナリオでは、アプライアンスの帯域内管理 IP および Citrix SD-WAN Orchestrator サービスを介したアプライアンスへの接続が維持されます。

- t2_app がクラッシュする場所
- 設定のリセットを実行しようとしています

アプライアンスに帯域内管理が設定されていて、手動で設定リセットを実行した場合、またはユーザー構成が原因で t2_app が 120 秒間に 4 回以上クラッシュするシナリオの場合。このようなフレームワークでは、サービスが無効になるため、Citrix SD-WAN Orchestrator サービスとアプライアンスへの接続が失われます。

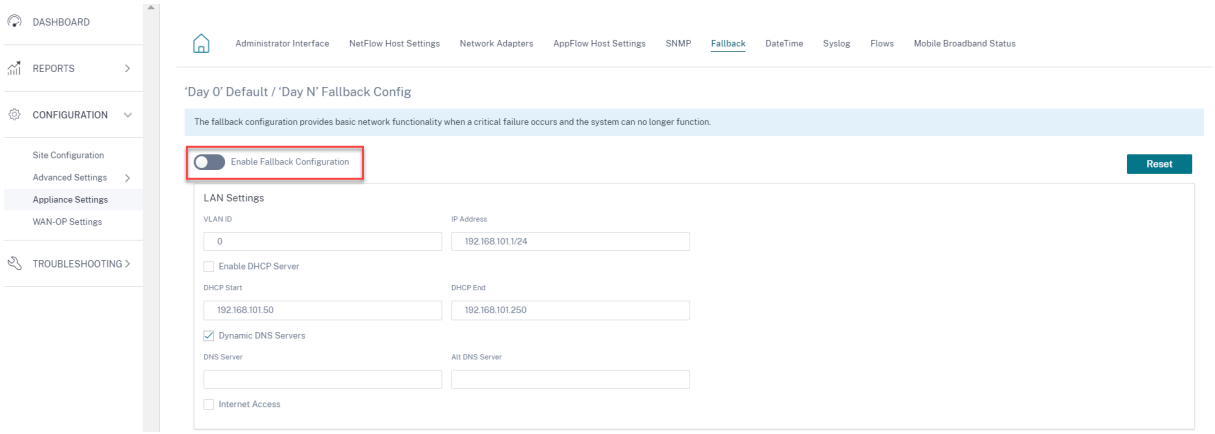
しかし、フォールバック設定を有効にしている場合は、以下の機能が得られます。

- 管理機能（Web UI/SSH/SNMP）への基本的な帯域内アクセス
- アプライアンスが帯域内ポートを介して外部サービスに接続する機能（Citrix SD-WAN Orchestrator サービス/ZTD）

このようなシナリオでは、サービスを無効にする代わりに、アプライアンスはサービスを有効にしたフォールバック構成に戻ります。インバンド管理 IP を介した Citrix SD-WAN Orchestrator サービスとアプライアンスへの接続は、リンクがインターネットに接続されている限りそのまま残ります。

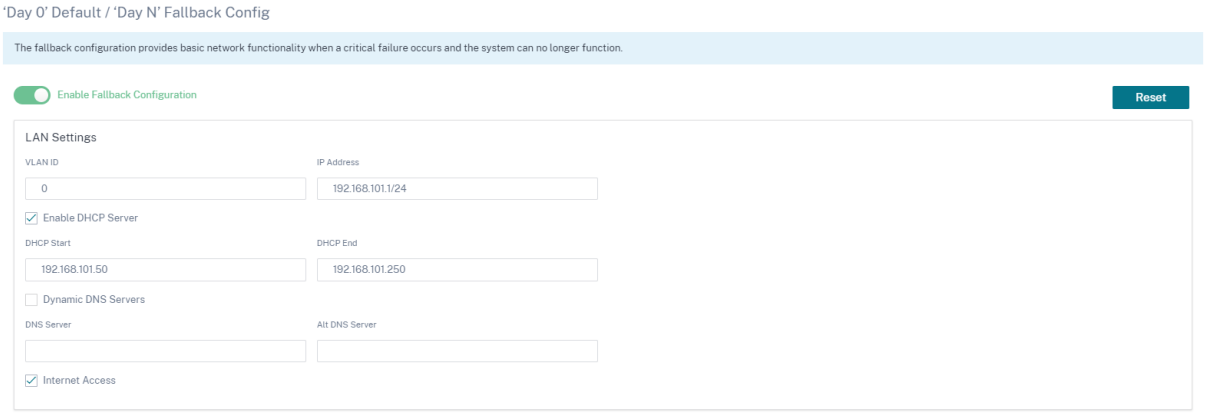
> 注
>
> アプライアンスの初回プロビジョニング後に、ゼロタッチ導入サービス接続のフォールバック構成が有効になっていることを確認します。

フォールバック構成が無効になっている場合は、Citrix SD-WAN Orchestrator サービスを介してサイトレベルで有効にするには、［構成］>［アプライアンス設定］>［フォールバック］に移動し、［フォールバック構成を有効にする**］をクリックします。



LAN ネットワークに従ってフォールバック構成をカスタマイズするには、ネットワーク要件に従って次の LAN 設定の値を編集します。これは、ゼロタッチ展開サービスとの接続を確立するために必要な最小構成です。

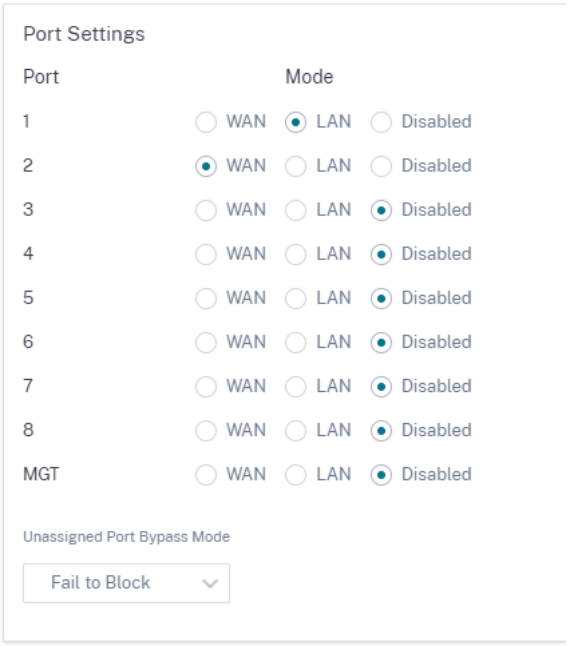
- **VLAN ID**: LAN ポートをグループ化する必要がある VLAN ID。
- **IP** アドレス:LAN ポートに割り当てられた仮想 IP アドレス。
- **DHCP** サーバーを有効にする:LAN ポートを DHCP サーバーとして有効にします。DHCP サーバーは、ダイナミック IP アドレスを WAN ポートに割り当てます。
- **DHCP** の開始と **DHCP** 終了:DHCP が WAN ポートに IP を動的に割り当てるために使用する IP アドレスの範囲。
- ダイナミック **DNS** サーバー:LAN ポートをドメインネームサーバーとして有効にします。
- **DNS** サーバー: プライマリ DNS サーバーの IP アドレス。
- 代替 **DNS** サーバー: セカンダリ DNS サーバーの IP アドレス。
- インターネットアクセス: 他のフィルタリングを行わずに、すべての LAN クライアントへのインターネットアクセスを許可します。



各ポートのモードを設定します。ポートは LAN ポートまたは WAN ポートにすることも、無効にすることもできます。表示されるポートは、アプライアンスのモデルによって異なります。また、ポートバイパスモードを **Fail-to-Block** または **Fail-to-Wire** に設定します。

次の表に、異なるプラットフォームでのフォールバック構成用に事前に指定された WAN ポートおよび LAN ポートの詳細を示します。

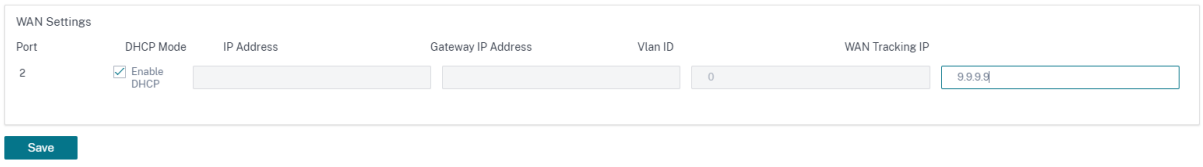
プラットフォーム	WAN ポート	LAN ポート
110	1/2	1/1
110-LTE	1/2、LTE-1	1/1
210	1/4, 1/5	1/3
210-LTE	1/4, 1/5, LTE-1	1/3
VPX	2	1
410	1/4, 1/5, 1/6	1/3 (FTB)
1100	1/4, 1/5, 1/6	1/3 (FTB)



WAN ポートは、DHCP クライアントを使用して独立した WAN リンクとして構成し、Quad9 DNS サービスを監視して WAN 接続を判断できます。DHCP がない場合、WAN ポートに WAN IP/スタティック IP を設定して、初期プロビジョニングにインバンド管理を使用できます。

> 注
>
> イーサネットポートには固定 IP のみを設定できます。スタティック IP は、LTE-1 ポートおよび LTE-E1 ポートでは設定できません。LTE-1 ポートと LTE-E1 ポートを WAN として追加できますが、設定フィールドは編集できません。

WAN ポートを追加すると、デフォルトで [**DHCP** を有効にする] チェックボックスがオンになって **[WAN** 設定 **(**ポート**:2)**] セクションに追加されます。**DHCP** モードチェックボックスが選択されている場合、**IP** アドレス、ゲートウェイ **IP** アドレス、および **VLAN ID** のテキストフィールドはグレー表示されます。固定 IP を設定する場合は、[**DHCP** を有効にする] チェックボックスをオフにします。



デフォルトでは、**WAN** トラッキング **IP** アドレスフィールドには 9.9.9.9 が自動的に入力されます。必要に応じて住所を変更できます。

> 注
>
> **Dynamic DNS Servers** チェックボックスを選択する場合は、**DHCP** モードを選択した状態で WAN ポートを少なくとも 1 つ追加/構成してください。

フォールバック設定をデフォルト設定にリセットするには、[**Reset**] をクリックします。

> 注
>
> LAN サブネットに接続された帯域内/管理ポート経由で Orchestrator に接続されているすべてのアプライアンスでフォールバック構成を有効にすることをお勧めします。デフォルトのフォールバック構成がネットワークサブネット要件に従って設定されていることを確認してください。

ポートのフェイルオーバー

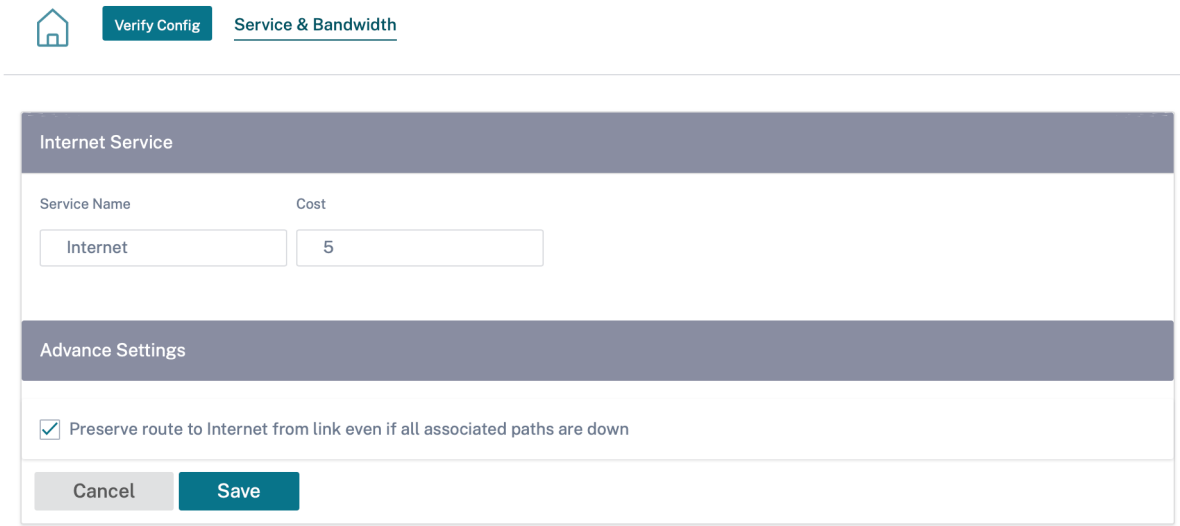
Citrix SD-WAN Orchestrator サービスでは、データポートがダウンしたときや、その逆になったときに、管理トラフィックを管理ポートにシームレスにフェールオーバーすることもできます。アプライアンスが管理ポートと帯域内ポートの両方を使用してインターネットに接続できる場合、管理ポートはゼロタッチ展開用に選択されます。

アプライアンスを再起動すると、管理ポートではなく帯域内ポートを介してインターネットが使用できる場合、アプライアンスはすぐに Citrix SD-WAN Orchestrator サービスに接続されます。

接続が確立されると、アプライアンスで実行されているサービスエージェントが 10 秒ごとに Citrix SD-WAN Orchestrator サービスにハートビート情報を送信します。Citrix SD-WAN Orchestrator サービスがハートビートを 5 分間受信しない場合、帯域内ポートフェールオーバーがアクティブになります。Citrix SD-WAN Orchestrator サービスは、この期間中にアプライアンスがオフラインになったと報告します。

アプライアンスの再起動時に、管理ポートと帯域内ポートの両方でインターネットが利用できず、インターネット接続が再確立されると、サービスエージェントが再起動して接続の確立に約 5 分かかります。

ネットワークレベルで、[構成] > [デリバリーサービス] > [インターネット] で [関連するすべてのパスがダウンしていてもリンクからインターネットへのルートを保存 **] オプションが有効になっていることを確認します。仮想パスがダウンしていても、Citrix SD-WAN Orchestrator サービスへの接続が維持されるようにします。



構成可能な管理ポートまたはデータポート

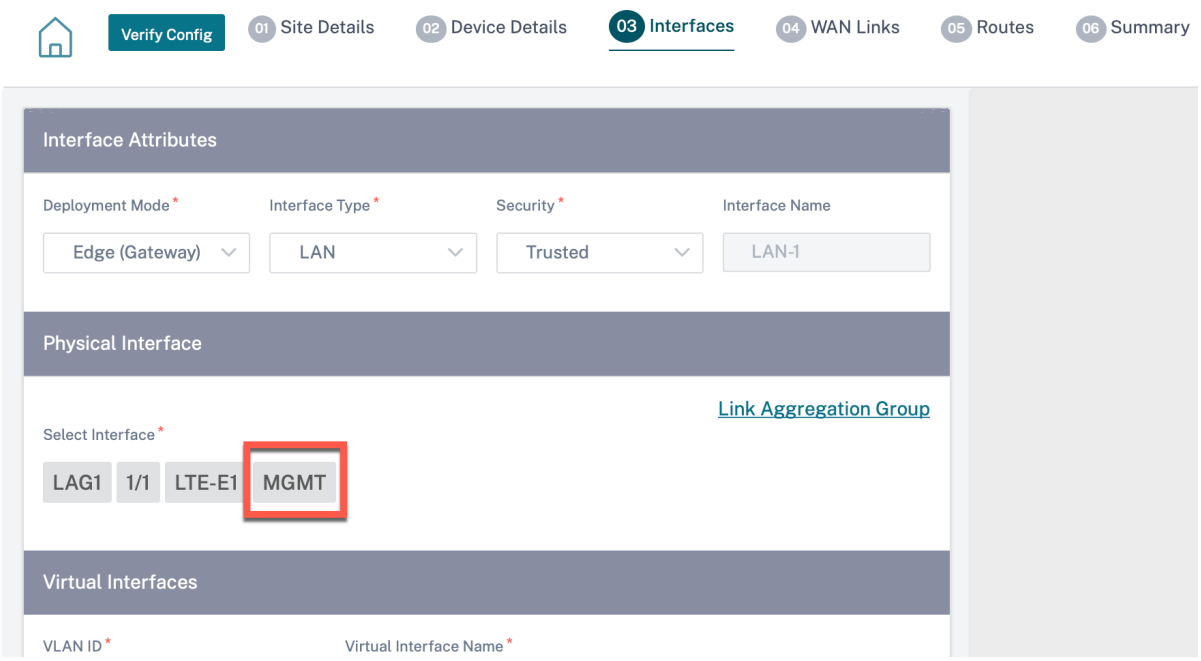
インバンド管理により、データポートはデータトラフィックと管理トラフィックの両方を伝送できるため、専用の管理ポートは不要です。ローエンドアプライアンスの管理ポートは、すでに低いポート密度の低いエンドアプライアンスでは使用されません。Citrix SD-WAN を使用すると、管理ポートをデータポートまたは管理ポートとして動作するように構成できます。

> 注
>
> 管理ポートをデータポートに変換できるのは、次のプラットフォームだけです。
>
> - Citrix SD-WAN 110 SE/LTE
> - Citrix SD-WAN 210 SE/LTE

サイトの構成時には、構成の管理ポートを使用します。構成がアクティブになると、管理ポートはデータポートに変換されます。

> 注
>
> 管理ポートを設定できるのは、アプライアンスの他の信頼できるインターフェイスでインバンド管理が有効になっている場合だけです。

管理インターフェイスを設定するには、サイトレベルで [構成] > [** サイト構成 **] > [インターフェイス] に移動し、MGMT インターフェイスを選択します。インターフェイスグループの設定の詳細については、「インターフェイス」を参照してください。



管理機能を実行するように管理ポートを再設定するには、設定を削除します。管理ポートを使用せずに構成を作成し、アクティブにします。

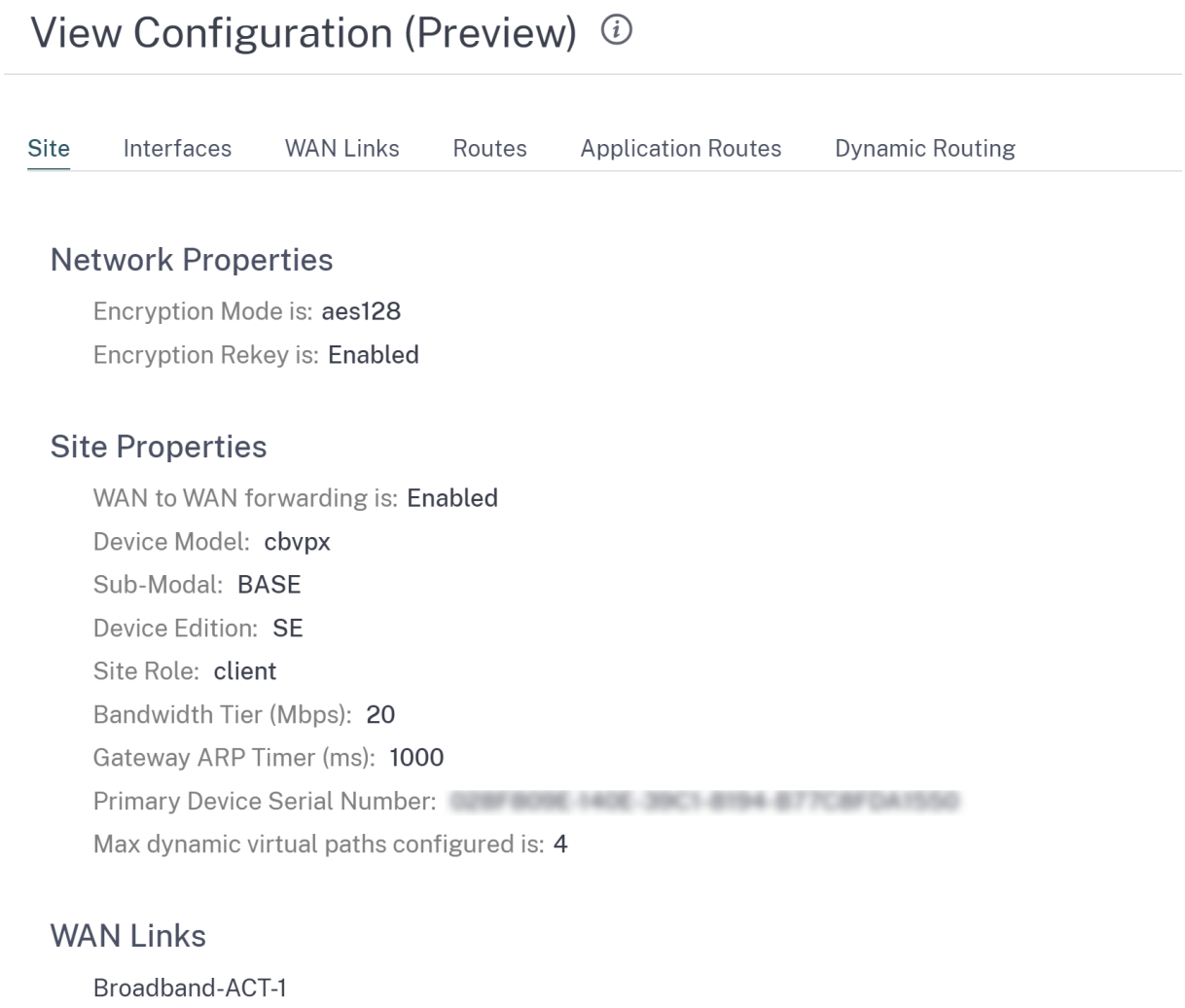
構成を表示 (プレビュー)

October 26, 2022

「構成を表示」ページには、サイトの構成設定の概要がまとめられています。構成を表示するには、サイトレベルで [構成] > [** 構成の表示 **] に移動します。サイト構成の詳細については、「サイト構成」を参照してください。

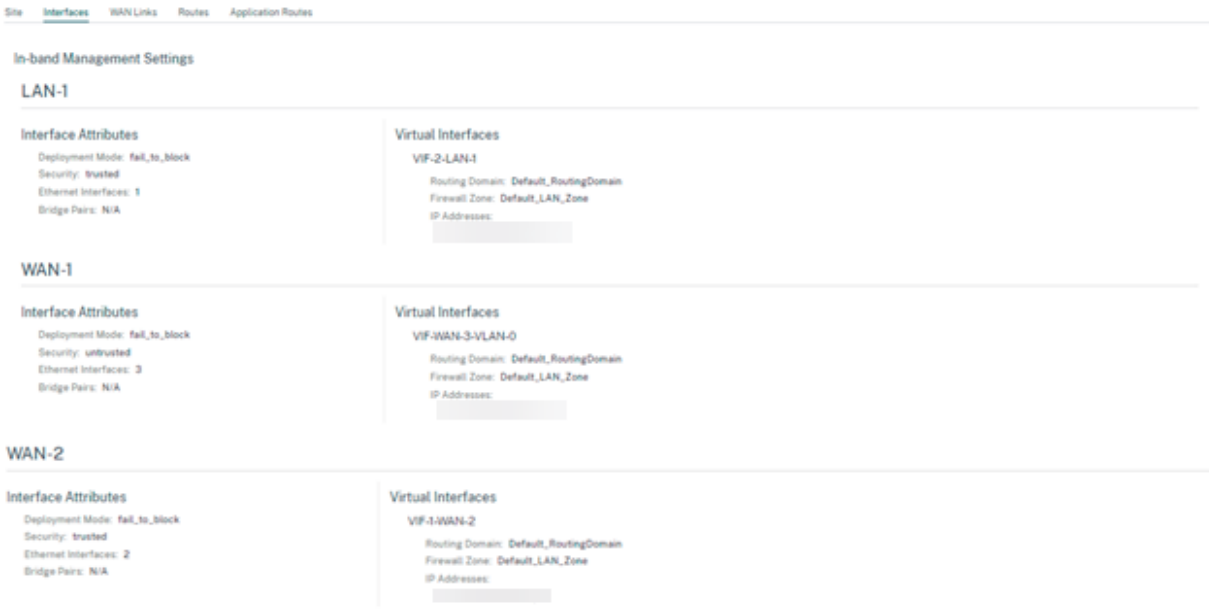
サイト

サイトページには、サイトの詳細の概要が表示されます。サイトの概要には、ネットワークプロパティ、サイトプロパティ、および WAN リンクステータスが含まれます。サイト構成の詳細を表示するには、[構成] > [** 構成の表示 **] > [サイト] に移動します。



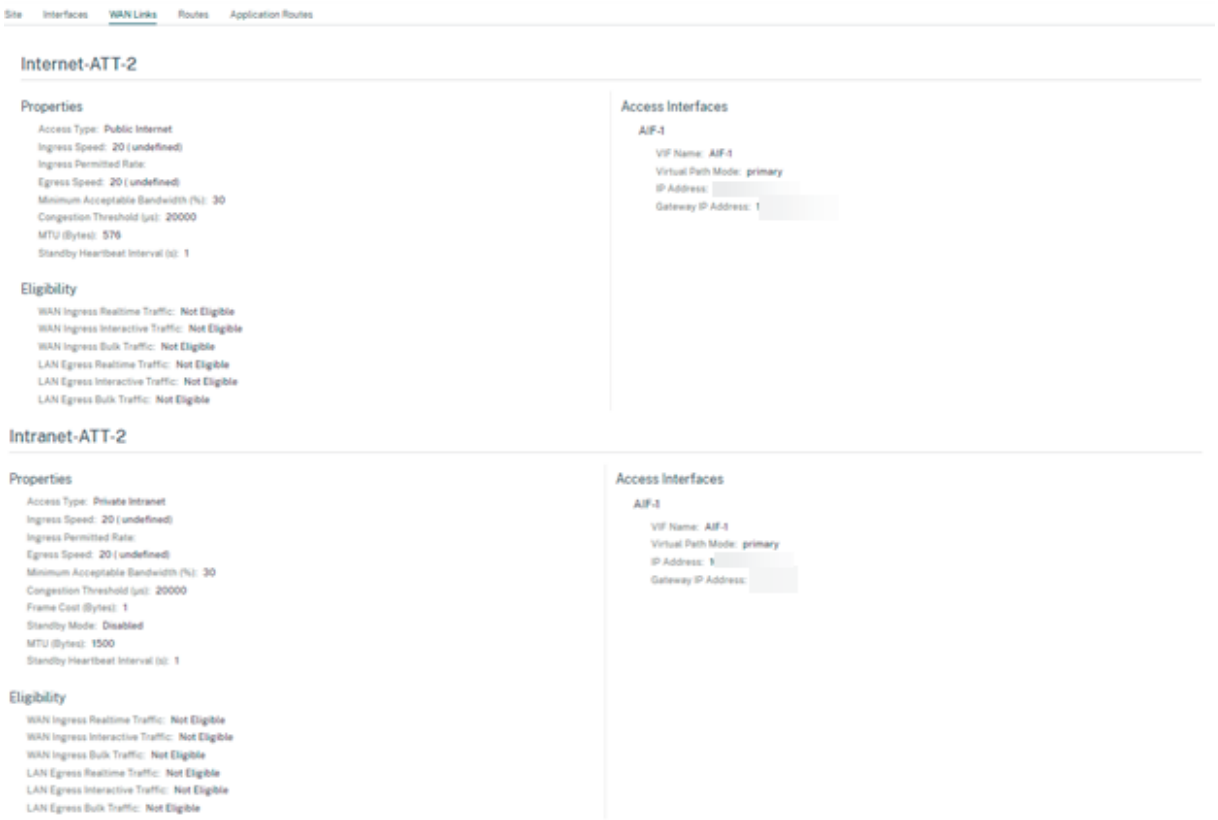
インターフェイス

インターフェースページには、設定されているインターフェースの概要が表示されます。仮想インターフェイスの構成の詳細を表示するには、[構成] > [****** 構成の表示 **] > [インターフェイス] に移動します。



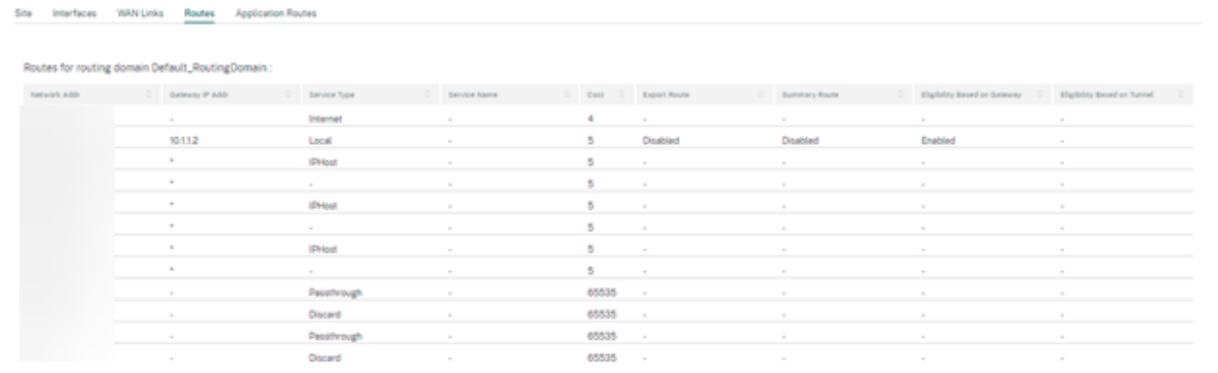
WAN リンク

設定された WAN リンクの設定の詳細を表示するには、[構成] > [****** 構成の表示 **] > [**WAN** リンク] に移動します。



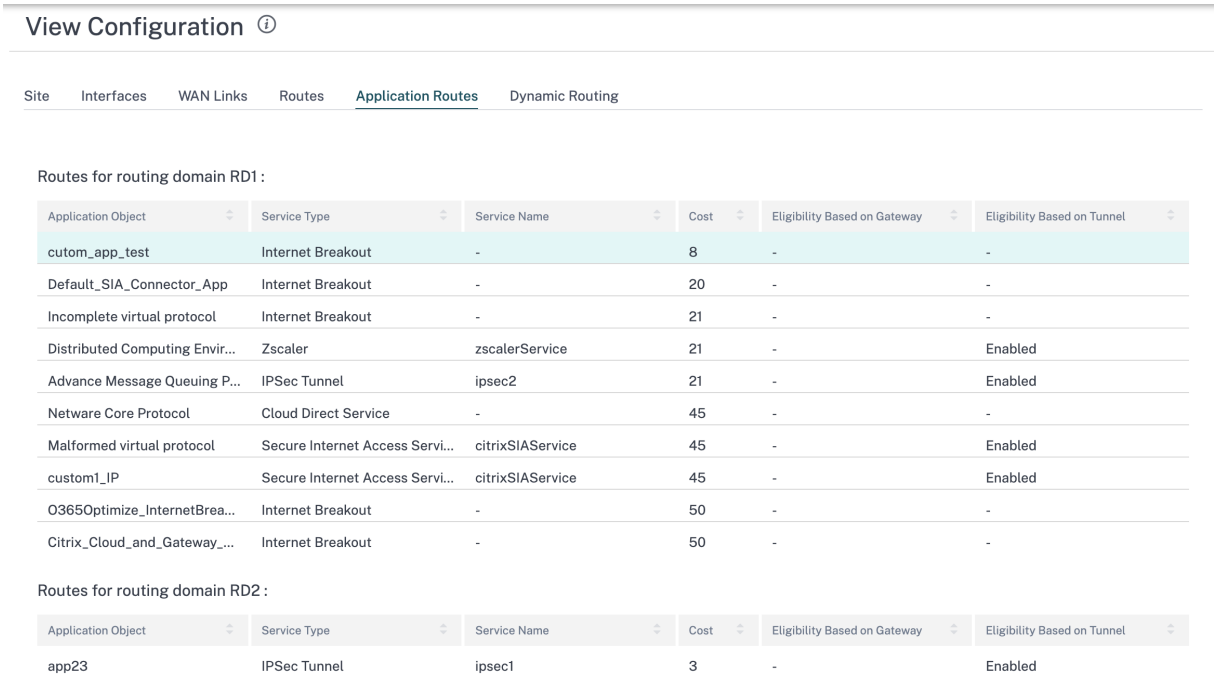
ルート

作成された IP ルートのルート情報を表示するには、[設定] > [****** 設定の表示 **] > [ルート] に移動します。



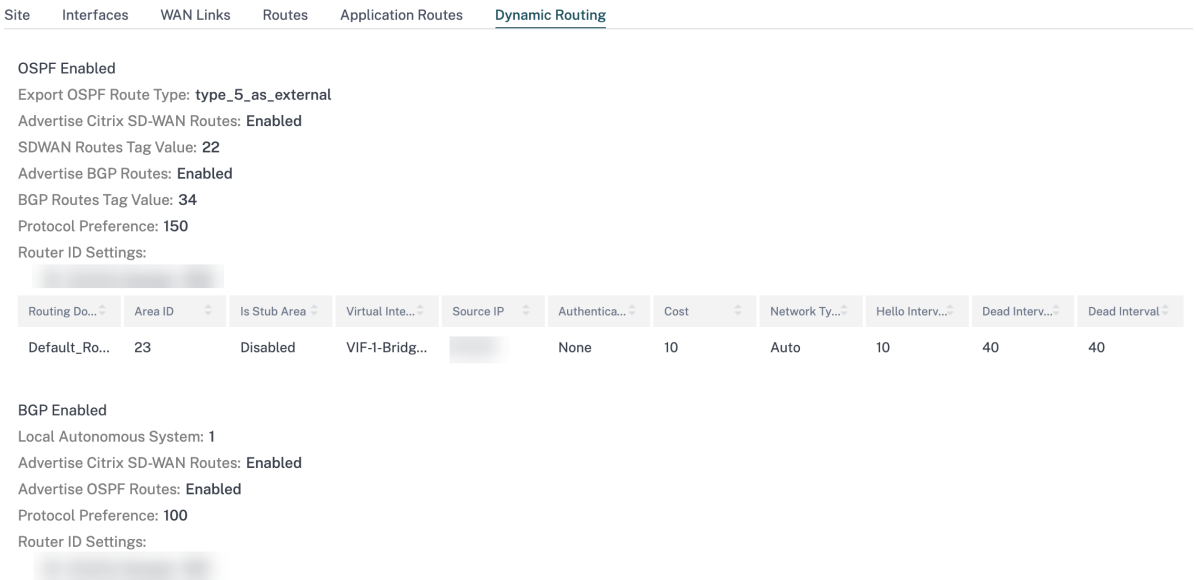
アプリケーションルート

特定のアプリケーションルートの概要を表示するには、[構成] > [****** 構成の表示 **] > [アプリケーションルート] に移動します。



動的ルーティング

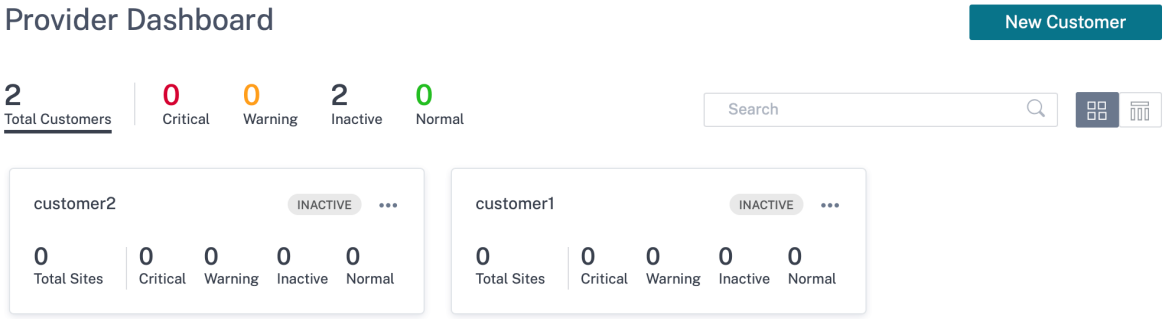
OSPF、BGP、インポートフィルタ、およびエクスポートフィルタの設定の概要を表示するには、[設定] > [** 設定の表示 **] > [ダイナミックルーティング] に移動します。



プロバイダダッシュボード

November 30, 2020

Citrix パートナーとしてログインすると、** プロバイダーダッシュボードが表示されます。サービスプロバイダーが管理するすべての SD-WAN 顧客の野鳥瞰図を提供します。



各顧客の SD-WAN ネットワークの健全性スナップショットが色分けされ、お客様固有の詳細情報をドリルダウンできるプロビジョニングが提供されます。ダッシュボードは、** タイル表示とリストビューの両方で使用できます **。

お客様のネットワークに使用される色分け基準は次のとおりです。

- 重大 (赤): 1 つ以上のサイトがダウンしています
- 警告 (オレンジ色): ダウンしているサイトはありませんが、クリティカルアラートが 1 つ以上あります。
- 標準（緑）: ダウンしているサイトはなく、クリティカルアラートもありません。
- 非アクティブ（灰色）: ネットワークは構成中ですが、まだ展開されていません。

色分け基準により、管理者は注意を要する顧客に集中できます。

顧客/ネットワークダッシュボード

July 10, 2024

ネットワークダッシュボードには、組織の SD-WAN ネットワークを全サイトの状態と使用状況の観点から全体像で把握できます。ダッシュボードは、ネットワーク全体のアラートの概要、オーバーレイとアンダーレイパスの稼働時間をキャプチャし、使用傾向を強調表示し、ネットワークのグローバルビューを提供します。

ダッシュボードには、ネットワークの次の側面が要約され、詳細についてドリルダウンできます。

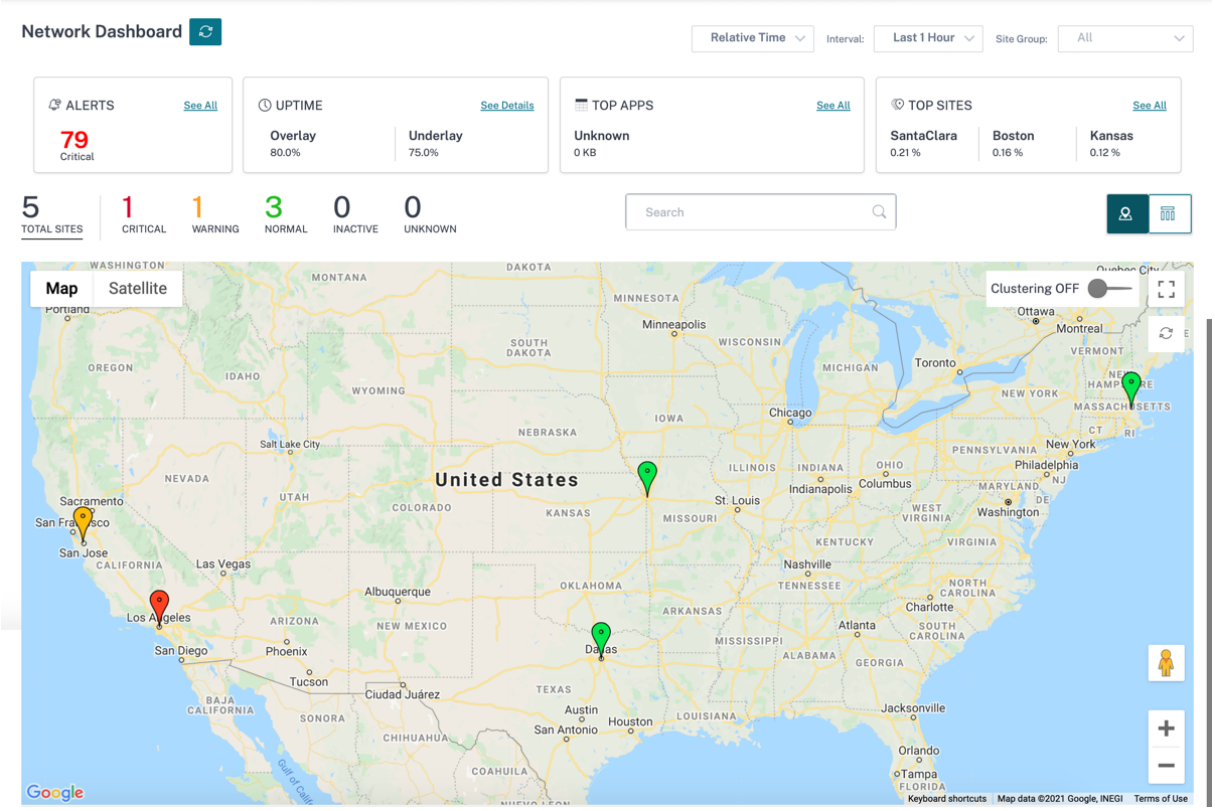
- クリティカル・アラート: ネットワーク上で発生しているクリティカル・ヘルス・アラートの実行回数 (存在する場合)。

- 稼働時間:SD-WAN 仮想オーバーレイネットワークと物理アンダーレイネットワークの平均稼働時間を並べて比較します。
- 使用傾向: トラフィック量に基づく上位アプリと容量使用率に基づく上位サイト。
- ネットワークビュー: ネットワーク上のすべてのサイトを視覚的に表示します。マップビューとリストビューの両方で利用できます。

ダッシュボードには、ネットワーク内のサイトの総数が一覧表示され、接続ステータスに基づいてサイトが分類されます。番号付きのリンクを選択すると、次のステータスカテゴリに基づいてサイトが表示されます。

- 重要—関連する仮想パスがすべてダウンしているサイト。
- 警告 -少なくとも 1 つの仮想パスがダウンしているサイト。
- 標準 -サイトのすべての仮想パスと関連するメンバーパスが稼働しています。
- 非アクティブ -未展開で非アクティブな状態のサイト。
- 不明 -サイトのステータスは不明です。

ステータスをクリックすると、ステータスに基づいてサイトがフィルタリングされ、詳細が表示されます。検索バーを使用して、サイト名、役割、オーバーレイ接続、モデル、帯域幅層、およびシリアル番号パラメータに基づいてサイトの詳細を表示することもできます。



このマップでは、組織のすべてのサイトが場所に基づいて世界地図上に描かれたグローバルネットワークのリアルタイムビューを提供します。各サイトの色は、現在の状態を反映しています。

各サイトで使用される色分け基準は次のとおりです。

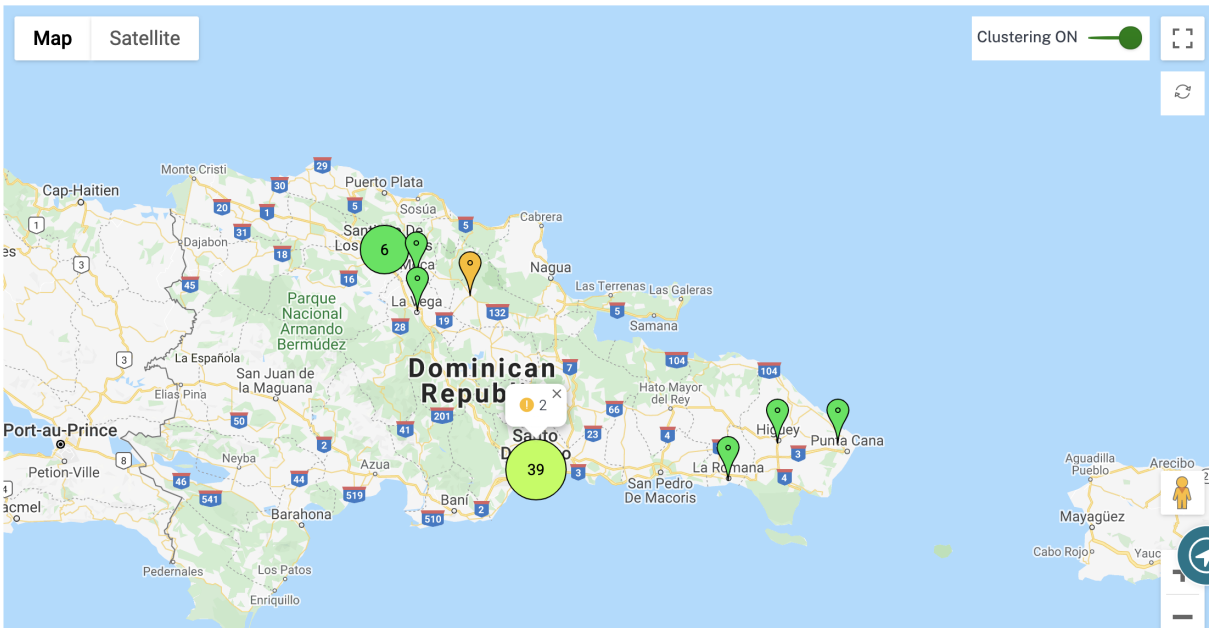
- クリティカル **(**赤**)**: サイトに関連付けられている少なくとも 1 つのオーバーレイ仮想パスがダウンしています。
- 警告 **(**オレンジ**)**: 少なくとも 1 つのアンダーレイメンバーパスがダウンしていますが、オーバーレイ仮想パスはすべてアップしています。
- 標準 **(**緑**)**: すべてのオーバーレイ仮想パスと関連するアンダーレイメンバーパスが稼働しています。
- 非アクティブ **(**グレー**)**: サイトは構成中であり、まだ導入されていません。

サイト上にマウスポインタを置くと、サイトの役割、デバイスモデル、帯域幅層など、サイト固有の主要な詳細の一部が表示されます。サイトに関連付けられた仮想パスは、その正常性を反映した適切なカラーコードで表示されます。リストビューでは、各サイトの同じ詳細がエントリとして表にまとめられて表示されます。

クラスタリング

Clustering ON 機能は、クラスタまたはクラスタの組み合わせのさまざまなサイトの整合性、ステータス、および状態を監視します。クラスタリング ON サービスは、フェールオーバーとサイトの現在の状態を監視するのに役立つサイトのリアルタイムビューを提供します。

このクラスタリングオン機能は、高密度のサイトを管理するために導入されました。数千のサイトがあり、パフォーマンスが低下する場合は、クラスタリングオフオプションを使用することは推奨されません。



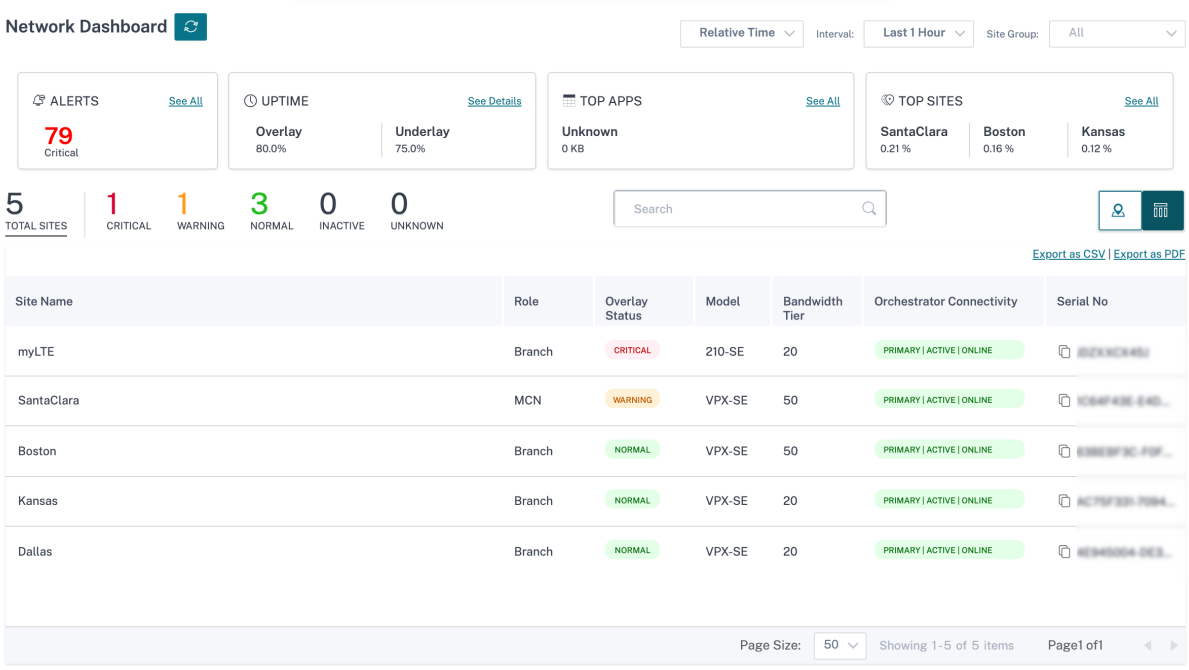
次の表に、クラスターでサイトの健全性を表すために使用される 5 つの色分けを示します。

カラー凡例	説明
	クラスタ内のすべてのサイトが緑色になります。つまり、各サイトにはすべての仮想パスがあり、関連するメンバーパスが UP
	クラスタ内のすべてのサイトはオレンジ色です。つまり、各サイトには少なくとも 1 つのメンバーパスが DOWN でも、すべての仮想パスが UP になっているということです。
	クラスタ内のすべてのサイトが赤で表示されます。つまり、各サイトには少なくとも 1 つの仮想パス DOWN があります。
	クラスタには、緑とオレンジのサイトの組み合わせがあります
	クラスターには、赤サイトと非赤サイトの組み合わせがあります

また、任意のクラスタ上にマウスを置いて、ネットワークの側面を確認することもできます。クリティカルアラートまたは警告アラートは、クラスタの上部にポップアップとして表示されます。

クラスタをクリックすると、そのクラスタが拡大表示され、他のクラスタが表示されます。クラスターの数を示すビューバーが表示されます。矢印オプションは、あなたを一歩戻すために役立ちます。閉じる **(X)** ボタンをクリックすると、元のページに戻ります。

または、ネットワーク概要をリストビューで表示することもできます。



- まだデプロイされていない非アクティブな「構成中」のサイトをクリックすると、サイト構成ワークフローに移動します。
- すでにデプロイされているアクティブなサイトをクリックすると、サイトダッシュボードが表示されます。

> 注
>
> Citrix SD-WAN オーバーレイトンネルは、仮想パスと呼ばれます。通常、各サイトとマスターコントロールノード（MCN）の間には 1 つの仮想パストンネルがあり、必要に応じて追加のサイトサイト仮想パスが作成されます。仮想パスは、アンダーレイの WAN リンク/パスを結合することによって形成されます。したがって、各仮想パスは複数のメンバーパスで構成されます。
>
> これは、ユーザーが仮想パスまたはメンバーパスという用語の上に移動したときに表示されます。

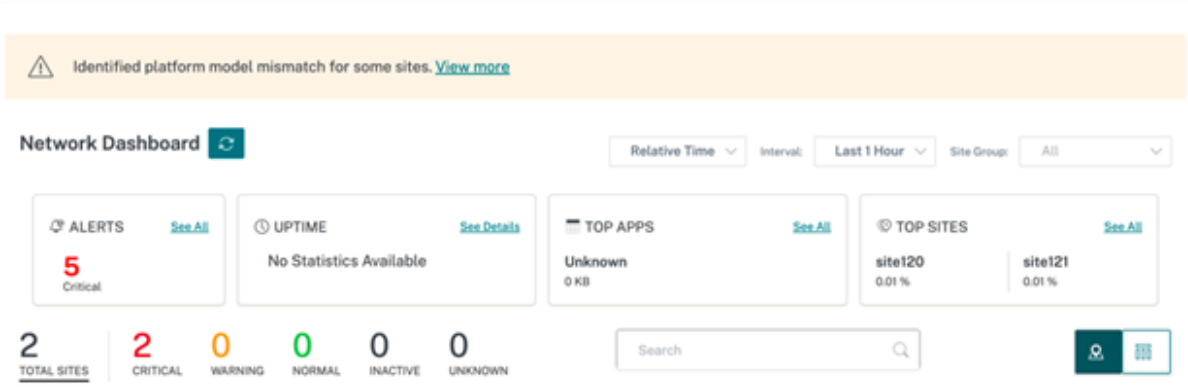
ペグマンをマップ上にドラッグすると、ストリートビューを開くことができます。

デバイスの不一致を記録する

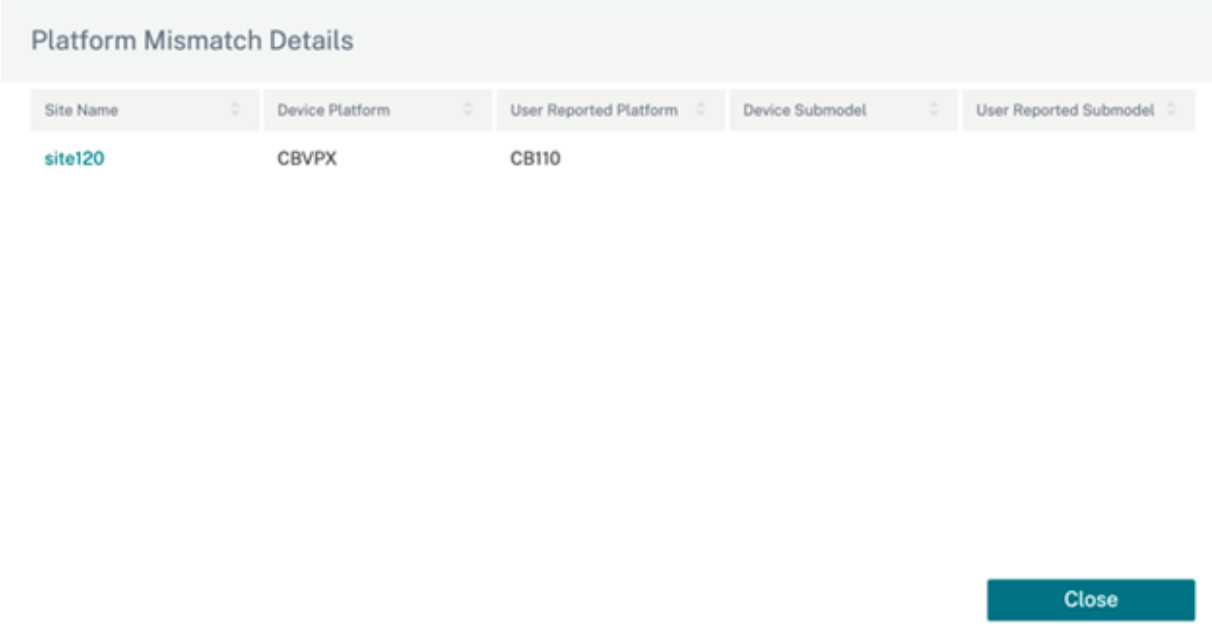
Citrix SD-WAN Orchestrator サービスが、アプライアンスで報告されたプラットフォームモデルとユーザーから報告されたプラットフォームモデルの不一致を特定したことを報告します。

サイト構成時にユーザーが提供したプラットフォームモデルとサブモデルが、Citrix SD-WAN Orchestrator サービスへの初回登録時にアプライアンスによって提供されたプラットフォームモデルおよびサブモデルと一致しない場合、不一致に関する通知がネットワークダッシュボードに表示されます。このようなシナリオでは、アプライアンスによって報告されたプラットフォームモデルを必ず設定してください。

「詳細を表示」をクリックすると、各サイトのプラットフォームモデルの不一致が表形式で表示されます。



Platform Mismatch Details には、サイト名、アプライアンスから報告されたプラットフォームモデルとサブモデル、ユーザーから報告されたプラットフォームモデルとサブモデルなどの情報が表示されます。



サイトダッシュボード

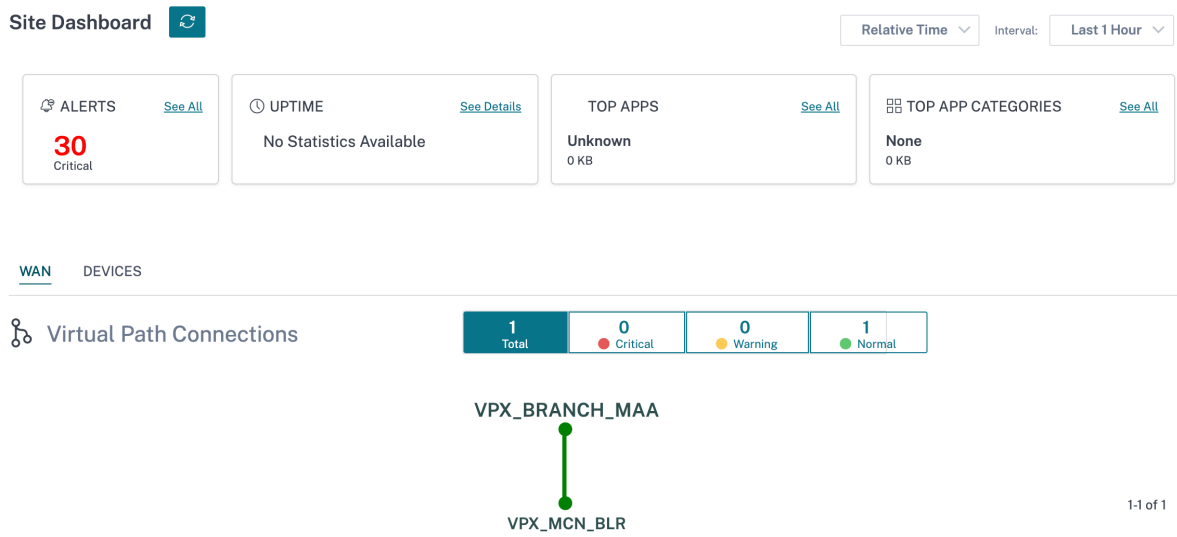
October 26, 2022

サイトダッシュボードには、サイトの正常性と使用状況の傾向の概要が表示されます。

ダッシュボードには、サイトの次の側面が要約され、詳細についてドリルダウンできます。

- クリティカル・アラート: サイトに発生したクリティカル・ヘルス・アラートの実行回数（存在する場合）。
- 稼働時間:SD-WAN 仮想オーバーレイパスとサイトに関連する物理アンダーレイパスの平均稼働時間を並べて比較します。

- 利用傾向: トラフィック量に基づく、サイトに関連する上位のアプリとアプリカテゴリ
- サイトの詳細:WAN 接続、およびサイトに関連するデバイス



> ヒント
>
> [すべて表示] または [詳細を表示] をクリックすると、より詳細な統計情報が表示されます。

サイトに関連付けられたすべてのオーバーレイ仮想パス接続は、各接続の正常性を反映する適切な色分けで表示されます。

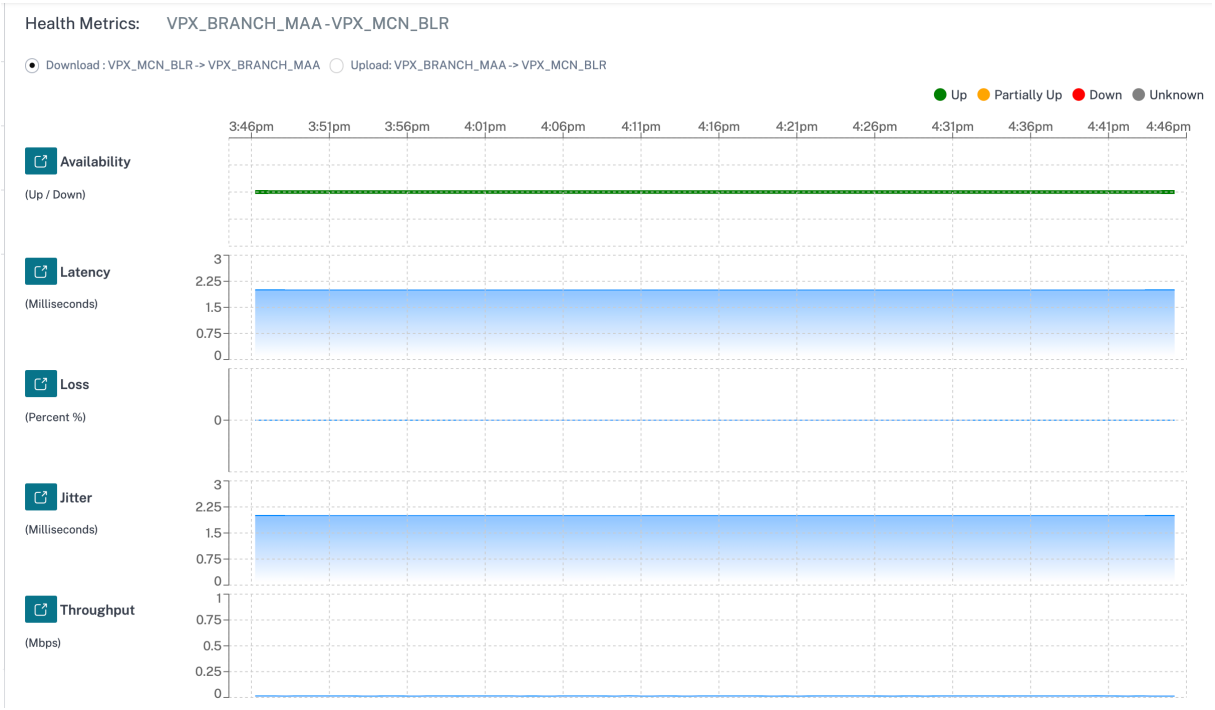
任意の仮想パス接続を選択して、対応する正常性メトリックと傾向を確認できます。

仮想パス接続に使用される色分け基準は次のとおりです。

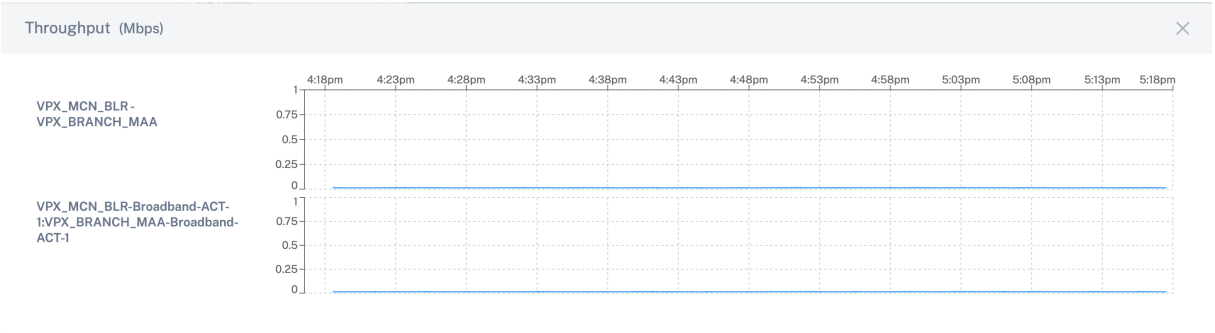
- クリティカル **(**赤**)**: 仮想パスがダウンしています。
- 警告 **(**オレンジ色**)**: 仮想パスは稼働していますが、少なくとも 1 つのメンバーパスが停止しています。
- 正常 **(**緑**)**: 仮想パスとすべてのメンバーパスが稼働しています。

健全性指標

選択した仮想パス接続について、稼働状態メトリックと可用性、遅延、損失、ジッタ、スループットに関するグラフィカルな傾向が表示されます。これらの統計情報は、WAN から LAN、LAN から WAN の両方の方向で使用できます。すべてのメトリックを共通のタイムラインに照らし合わせて確認できるため、トラブルシューティング中に問題のドメインをすばやく絞り込むことができます。



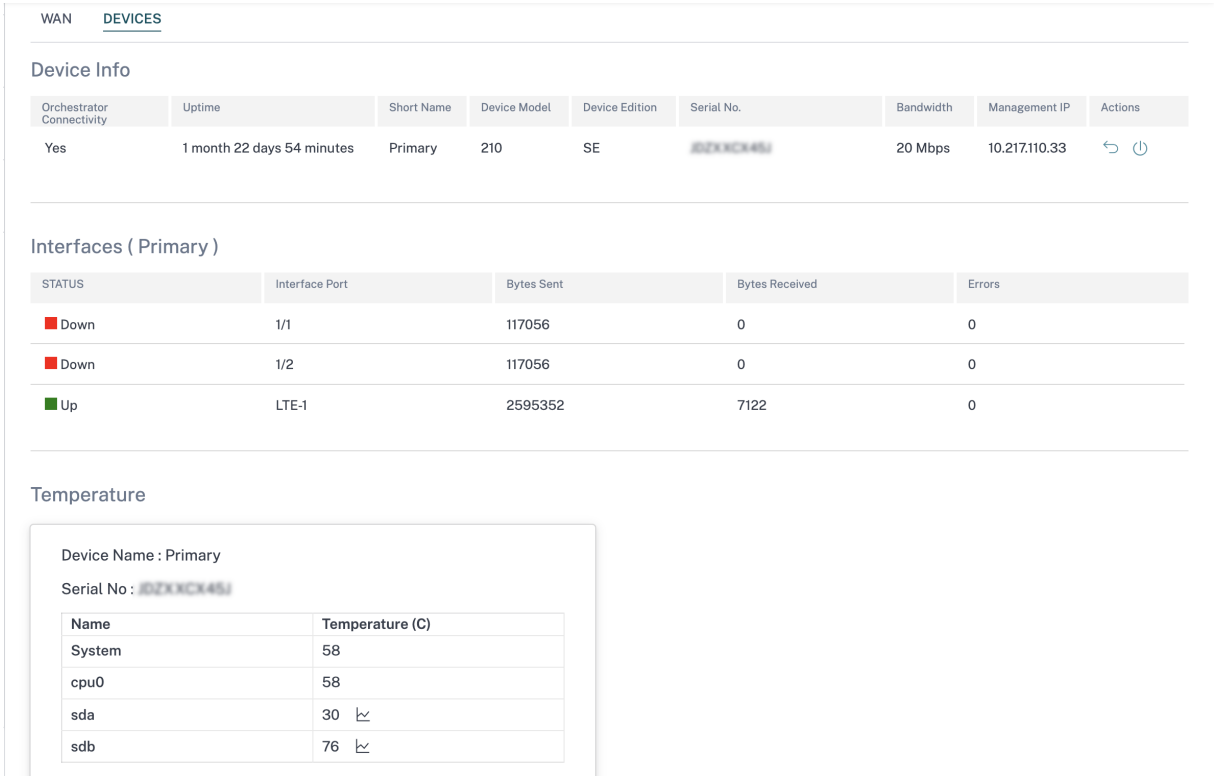
各正常性メトリックをさらにドリルダウンして、同じメトリックのオーバーレイ仮想パスとアンダーレイメンバパスの比較ビューを取得できます。これは、オーバーレイとアンダーレイの問題のトラブルシューティングに役立ちます。



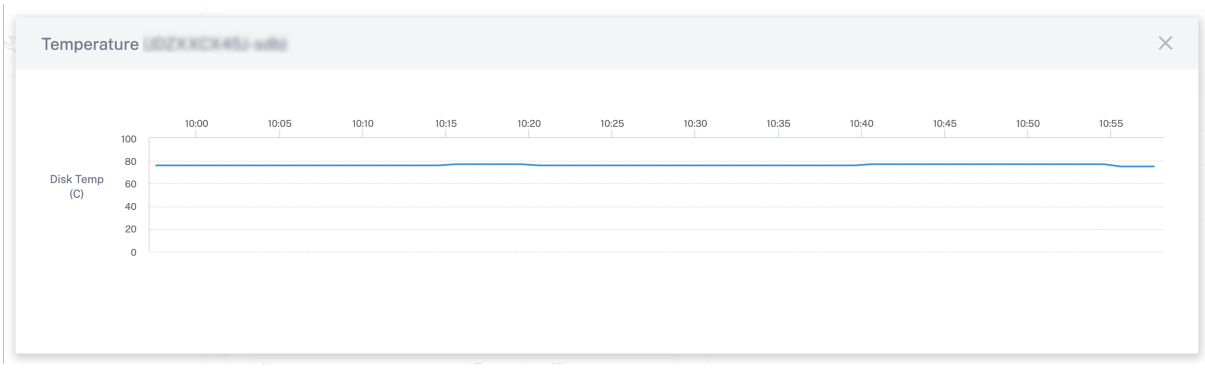
デバイス

デバイスタブには、サイトのデバイス、インターフェイス、およびディスク温度に関連する詳細が表示されます。アプライアンスの再起動、アプライアンス構成のリセット、またはデバイスログのダウンロードも可能です。

温度セクションには、システム、CPU、ディスクの温度が摂氏で表示されます。



温度 **(C)** 列のグラフアイコンをクリックして、情報をグラフ形式で表示することもできます。



プロバイダのトラブルシューティング

October 26, 2022

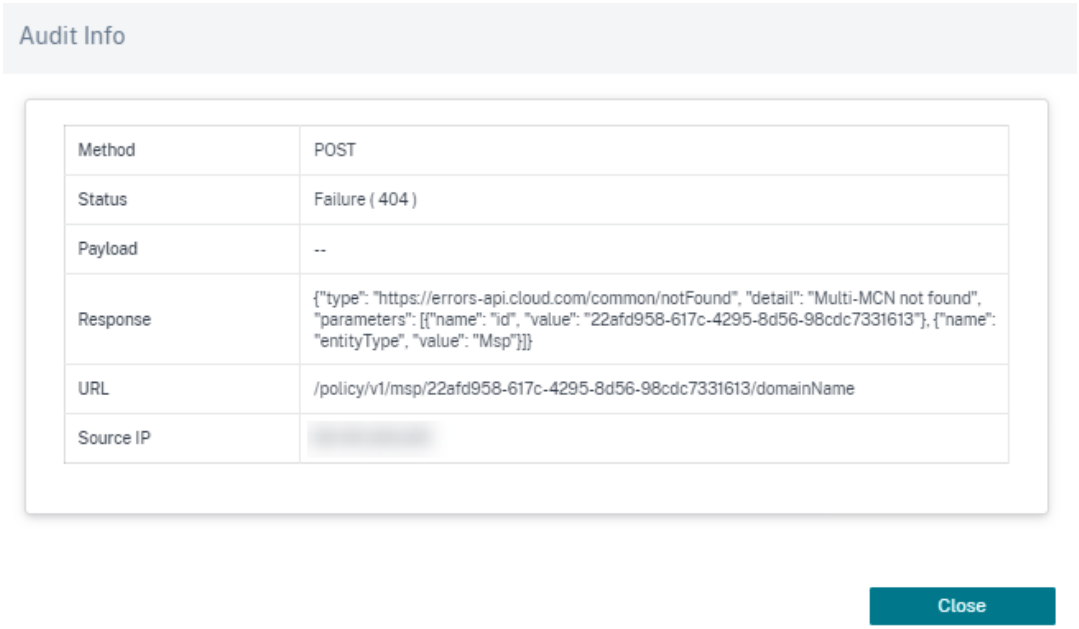
プロバイダー監査ログページには、プロバイダーレベルのログとデバイスログが表示されるため、迅速なトラブルシューティングが可能になります。

監査ログ

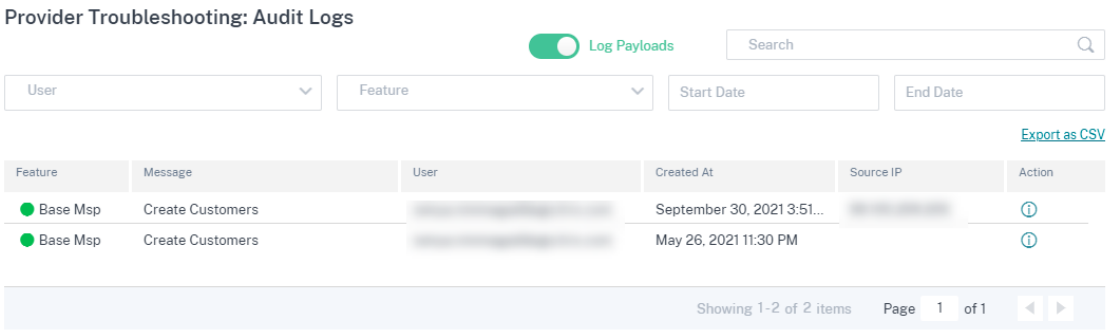
監査ログには、プロバイダーによって実行されたアクション、時間、およびアクションの結果が記録されます。トラブルシューティング > 監査ログに移動して、プロバイダーのトラブルシューティング**:** 監査ログページを表示します。

プロバイダー監査ログページには、次の情報が表示されます。

- 検索バー: キーワードに基づいて監査アクティビティを検索します。
- フィルタリングオプション: 次の基準に基づいてフィルタリングして監査ログ検索を実行します。
  - ユーザー
  - 機能
  - 時間範囲
- **CSV** としてエクスポート: このオプションをクリックすると、監査ログエントリが CSV ファイルにエクスポートされます。
- 監査情報:「アクション」列のアイコンを選択して、「監査情報」セクションに移動します。このセクションでは、次の内容について説明します:
  - メソッド: 呼び出された API の HTTP リクエストメソッド。
  - ステータス:API リクエストの結果。
  - ペイロード:API を介して送信されたリクエストの本文。
  - 応答:API リクエストが失敗したときのエラー応答。このフィールドは、API リクエストが失敗した場合にのみ表示されます。
  - **URL**: 取り消された API の HTTP URL。
  - ソース **IP**: 機能を設定したエンドポイントの IP アドレス。このフィールドは、「監査ログ」ページと「監査情報」ページに表示されます。



- ログペイロード: デフォルトでは、このオプションは無効になっています。有効にすると、API メッセージのリクエスト本文が **Audit Info** セクションに表示されます。API の詳細については、Citrix SD-WAN Orchestrator の API ガイドを参照してください。



ネットワークのトラブルシューティング

October 26, 2022

お客様は、すべてのネットワークアプライアンスのログを表示できるため、迅速なトラブルシューティングが可能になります。

監査ログ

監査ログには、お客様のネットワーク上でユーザーが実行したアクション、時間、およびアクションの結果が記録されます。**SD-WAN** トラブルシューティング > 監査ログに移動して **SD-WAN** トラブルシューティング監査ログページを表示します。

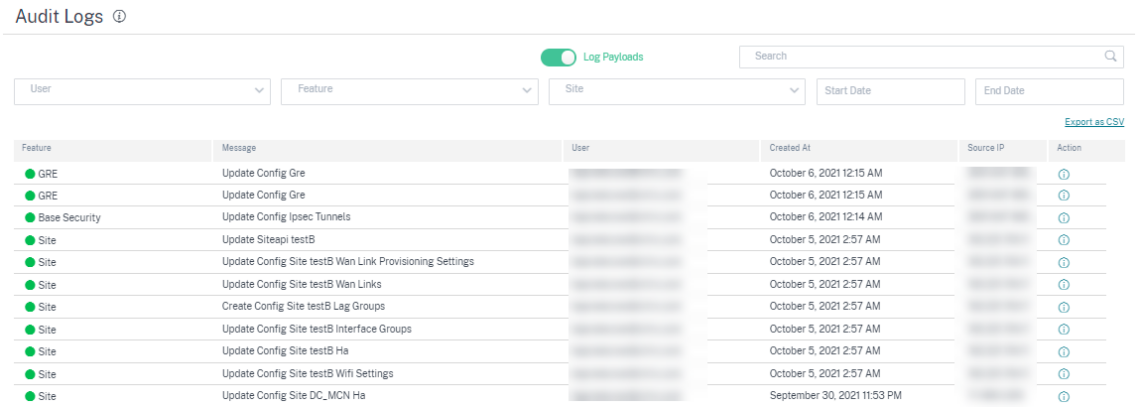
SD-WAN トラブルシューティング監査ログページには、次の情報が表示されます。

- 検索バー: キーワードに基づいて監査アクティビティを検索します。
- フィルタリングオプション: 次の基準に基づいてフィルタリングして監査ログ検索を実行します。
  - ユーザー
  - 機能
  - サイト
  - 時間範囲
- **CSV** としてエクスポート: このオプションをクリックすると、監査ログエントリが CSV ファイルにエクスポートされます。
- 監査情報:「アクション」列のアイコンを選択して、「監査情報」セクションに移動します。このセクションでは、次の内容について説明します:
  - メソッド: 呼び出された API の HTTP リクエストメソッド。
  - ステータス:API リクエストの結果。API リクエストが失敗すると、次のエラーレスポンスが表示されます。
  - ペイロード:API を介して送信されたリクエストの本文。
  - 応答:API リクエストが失敗したときのエラー応答。このフィールドは、API リクエストが失敗した場合にのみ表示されます。
  - **URL**: 取り消された API の HTTP URL。

- ソース **IP**: 機能を設定したエンドポイントの IP アドレス。このフィールドは、「監査ログ」ページと「監査情報」ページに表示されます。

- 変更内容: このセクションには、UI を通じて機能に加えられたすべての変更のログが表示されます。[ログペイロード] トグルボタンを有効にすると、[監査情報] セクションに変更が表示されます。

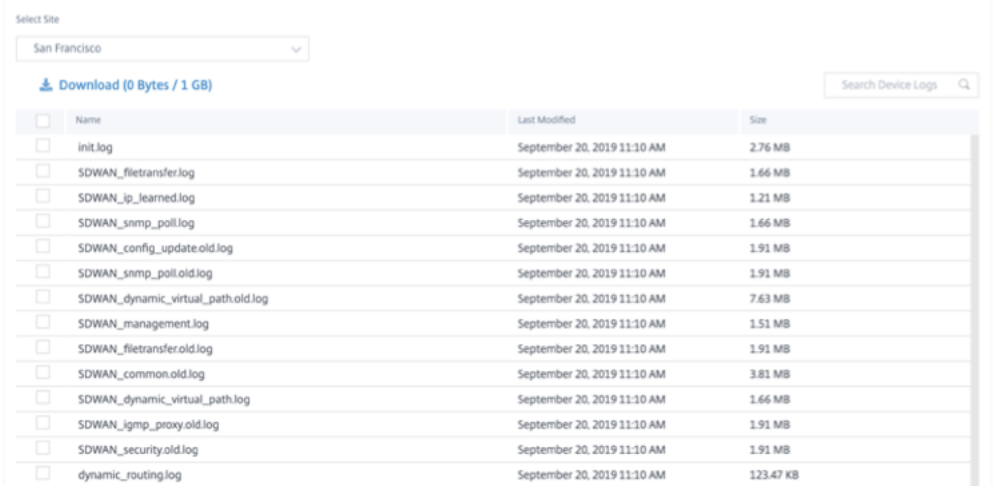
- ログペイロード: デフォルトでは、このオプションは無効になっています。有効にすると、API メッセージのリクエスト本文が **Audit Info** セクションに表示されます。API の詳細については、「Citrix SD-WAN Orchestrator API ガイド」を参照してください。



デバイスログ

お客様は、サイトに固有のデバイスログを表示できます。

必要に応じて、特定のデバイスログを選択してダウンロードし、サイト管理者と共有できます。

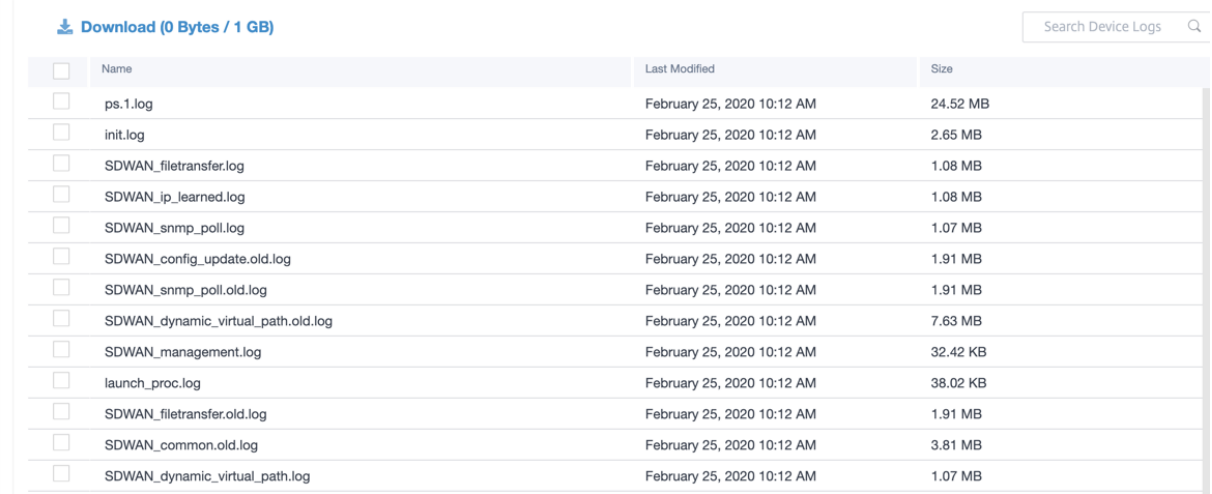


サイトのトラブルシューティング

October 26, 2022

デバイスログ

ログは、問題のトラブルシューティングに役立ちます。サイト管理者は、サイト内のすべてのデバイスでキャプチャされたすべてのログの一覧を表示できます。さらに検証するためにログをダウンロードすることもできます。



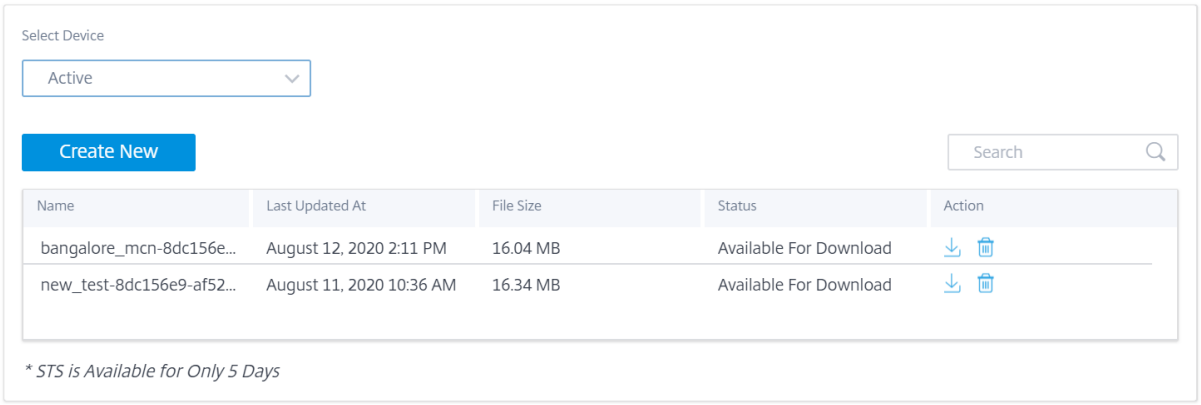
テクニカルサポートバンドルの表示

Show Tech Support（STS; 技術サポート）バンドルには、アクセスログ、診断ログ、ファイアウォールログなどの重要なリアルタイムシステム情報が含まれています。STS バンドルは、SD-WAN アプライアンスの問題のトラブル

シューティングに使用されます。STS バンドルの作成、ダウンロード、および Citrix サポート担当者と共有できます。

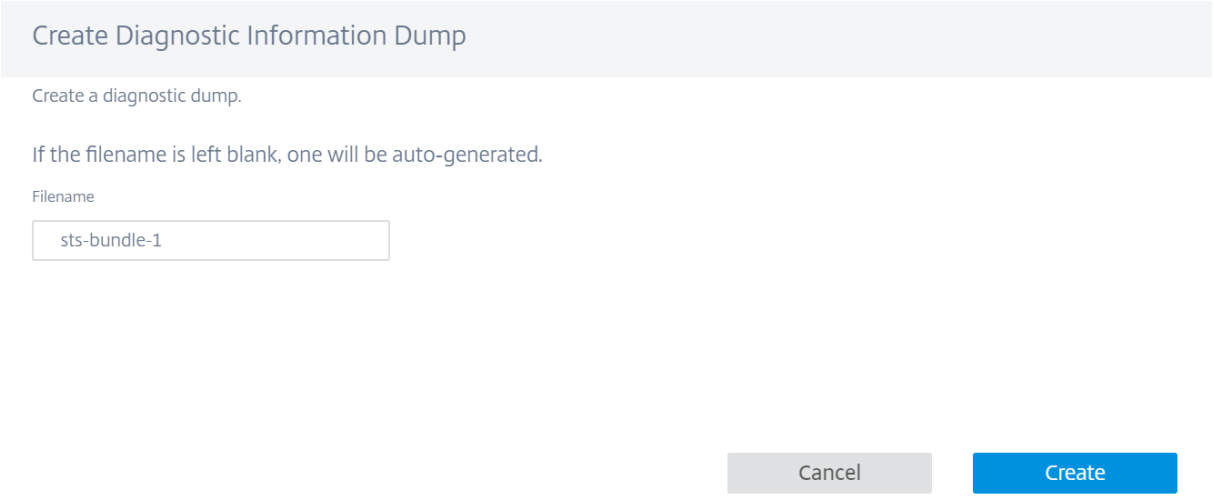
サイトが HA デプロイメントモードで構成されている場合、STS バンドルを作成またはダウンロードするアクティブまたはスタンバイのアプライアンスを選択できます。

サイトアプライアンスの STS バンドルを作成するには、サイトレベルで [トラブルシューティング] > [**STS** バンドル] に移動し、[新規作成] をクリックします。



STS バンドルの名前を指定します。名前は、英字で始まる必要があり、英字、数字、ダッシュ、およびアンダースコアを使用できます。名前の最大長は 32 文字です。ユーザーが指定した名前は、最終的な名前のプレフィックスとして使用されます。ファイル名が一意であることを保証し (タイムスタンプ)、STS パッケージ (シリアル番号) からデバイスを認識しやすくするために、サービスはフルネームを生成します。名前を指定しない場合、バンドルの作成時に名前が自動生成されます。

新しい STS をリクエストできるのは、デバイスがオンラインで、アプライアンスで STS プロセスが現在実行されていない場合だけです。デバイスがオフラインの場合でも、Citrix SD-WAN Orchestrator サービスから既に使用可能な STS をダウンロードできます。



STS プロセスは次のいずれかの状態になります。

STS ステータス	説明
リクエストされた	新しい STS バンドルが要求されます。リクエストが処理されるまで数分かかります。必要に応じて、STS 作成プロセスをキャンセルできます。
アップロード中	作成された STS パッケージがクラウドサービスにアップロードされます。期間はパッケージのサイズによって異なります。ステータスは 5 秒ごとに更新されます。STS アップロードプロセスはキャンセルできません。
失敗	作成中またはアップロード中に STS プロセスが失敗しました。失敗した STS 操作のエントリを削除できます。
ダウンロード可能	STS の作成およびアップロードプロセスは正常に完了しました。これで、STS パッケージをダウンロードまたは削除できます。

アプライアンスで STS プロセスが開始されると、進捗状況はステータス列で定期的に更新されます。たとえば、「リクエスト済み **(**ログファイルの収集**)**」などです。

STS バンドルと障害レコードは 7 日間保持され、その後自動的に削除されます。

プロバイダレポート

October 26, 2022

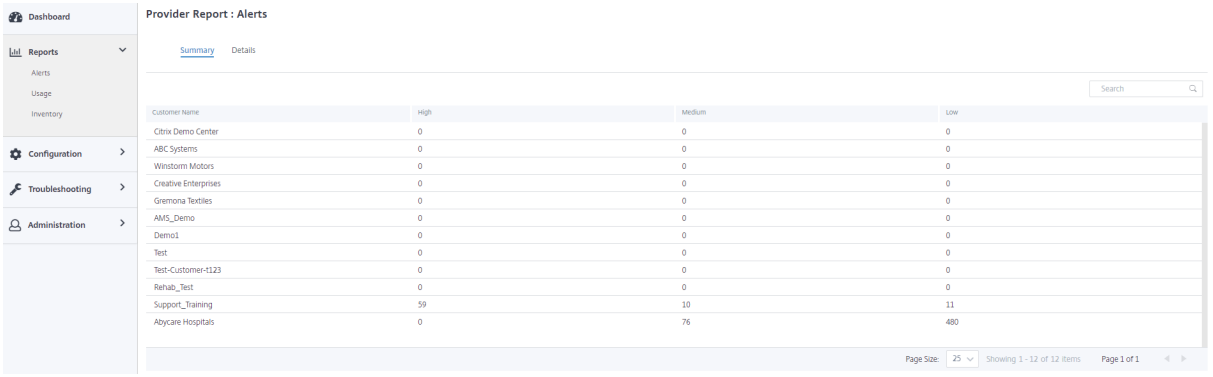
プロバイダーレポートは、プロバイダーが管理するすべての顧客を対象に集計されたアラート、使用量の傾向、インベントリを可視化します。

Citrix SD-WAN Orchestrator サービスプロバイダーレベルの UI で、レポートに移動します。

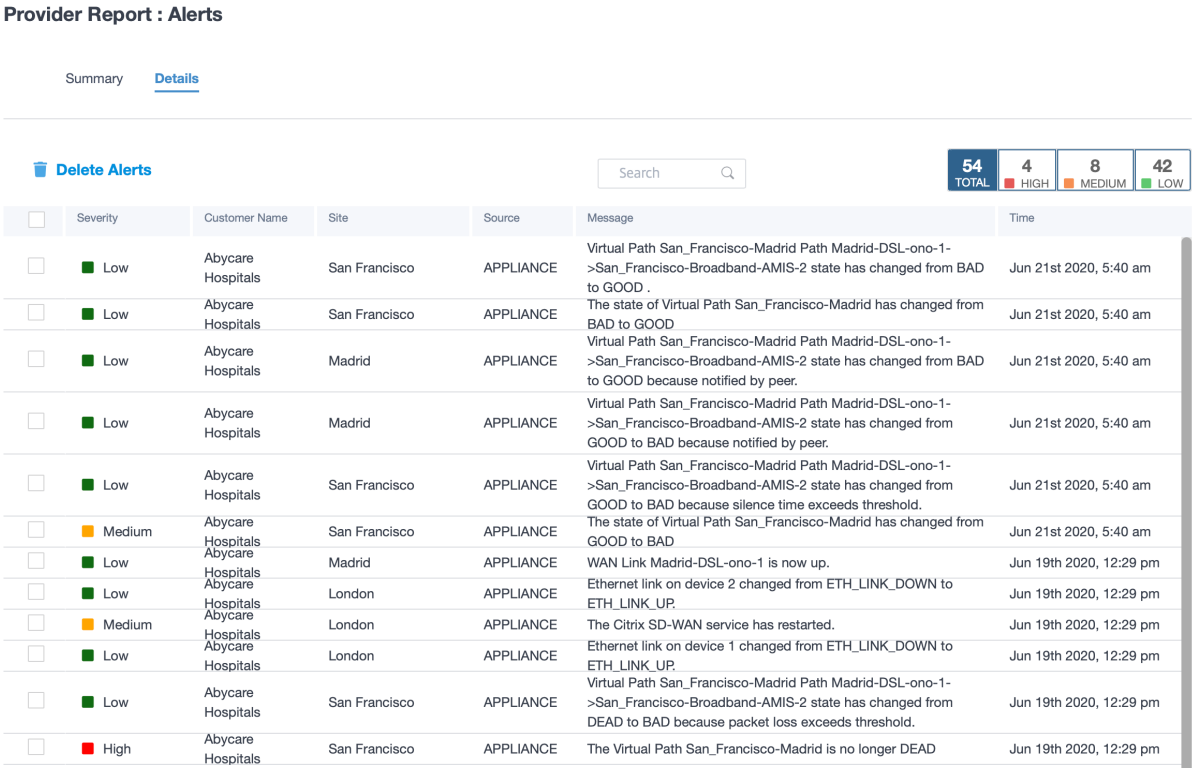
アラート

プロバイダーは、すべてのカスタマーネットワークで生成されたすべてのイベントとアラートを確認できます。

概要ビューには、顧客ごとの高、中、低のアラートの数が表示されます。



重要度、アラートが発生したサイト、アラートメッセージ、時間、およびその他の情報を [詳細] で確認することもできます。



必要に応じて、適切なフィルタリングオプションを使用できます。たとえば、すべての顧客にわたって重大度の高いアラートや、特定の顧客のアラートを探します。

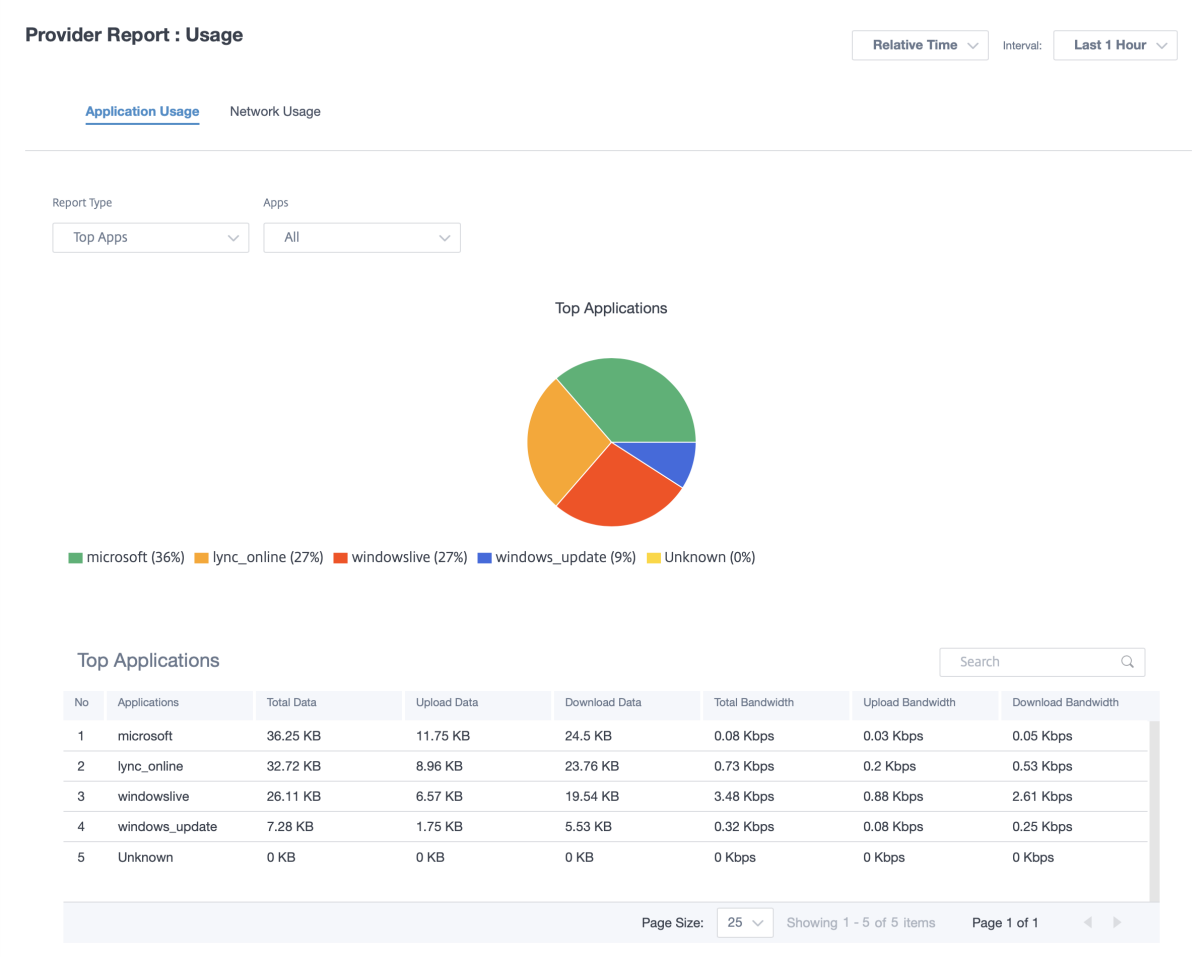
アラートを選択して削除することもできます。

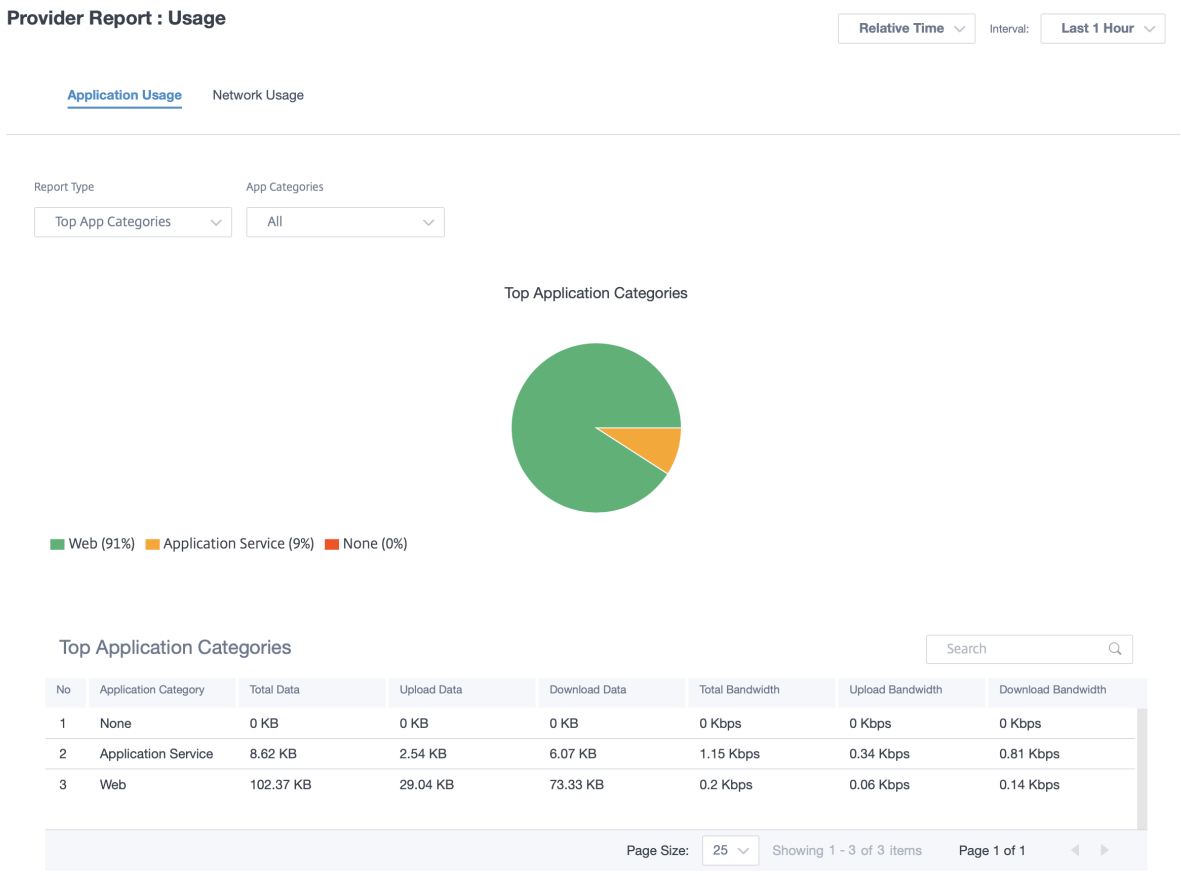
使用状況

プロバイダーは、上位アプリケーション、上位アプリケーションカテゴリ、アプリケーション帯域幅 **、上位サイトなど **、顧客間の使用傾向を確認できます。

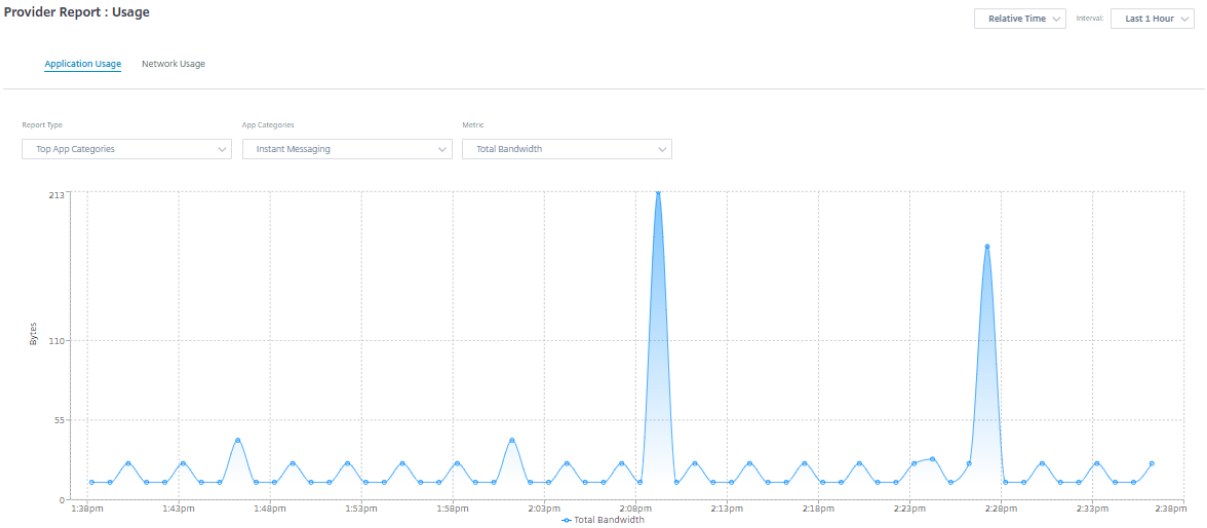
上位アプリケーションとアプリケーションカテゴリ

** 上位アプリケーションと上位アプリケーションカテゴリのグラフには ** 、すべての顧客ネットワークで広く使用されているアプリケーションとアプリケーションファミリが表示されます。これにより、データ消費パターンを分析し、必要に応じてデータクラスごとに帯域幅制限を再割り当てできます。





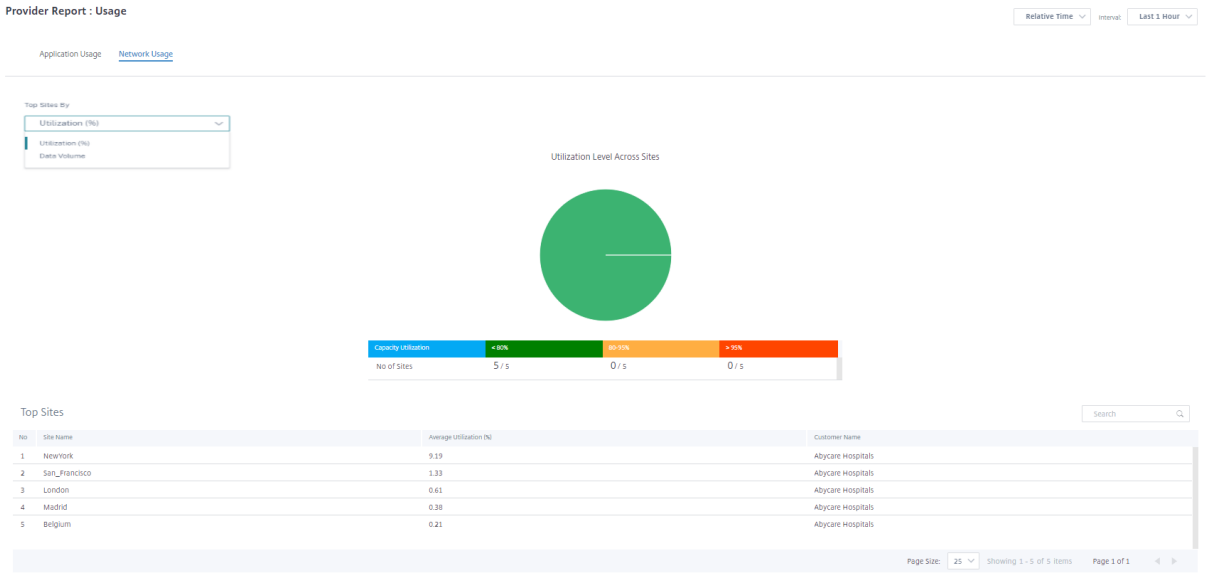
帯域幅使用状況の統計を表示できます。選択した時間間隔について、帯域幅統計情報が収集されます。レポートタイプ、アプリまたはアプリカテゴリ、および指標に基づいて統計レポートをフィルタリングできます **。



- レポートタイプ**:** リストから [上位のアプリ] または **[**アプリカテゴリ] を選択します。
- アプリ/アプリカテゴリ**:** リストから上位のアプリケーションまたはカテゴリを選択します。
- メトリック**:** リストから帯域幅メトリック (合計データ、受信データ、合計帯域幅など) を選択します。

ネットワーク使用状況

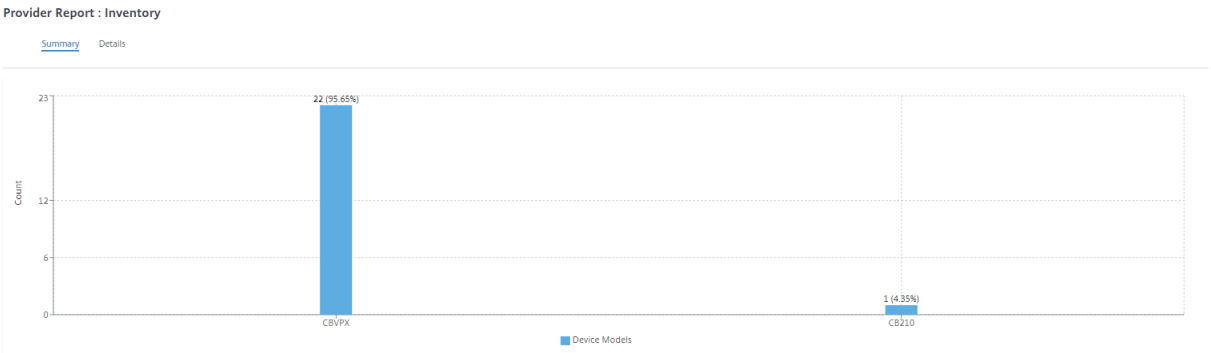
ネットワーク使用量チャートには、帯域幅使用率が最も高いすべての顧客の上位 10 サイトが表示されます。サイトは使用率 (%) またはデータ量 (MB) 別に表示できます。



Inventory

プロバイダーは、すべての顧客のデバイスインベントリ全体を表示できます。在庫概要を表示するか、詳細ビューを表示するかを選択できます。

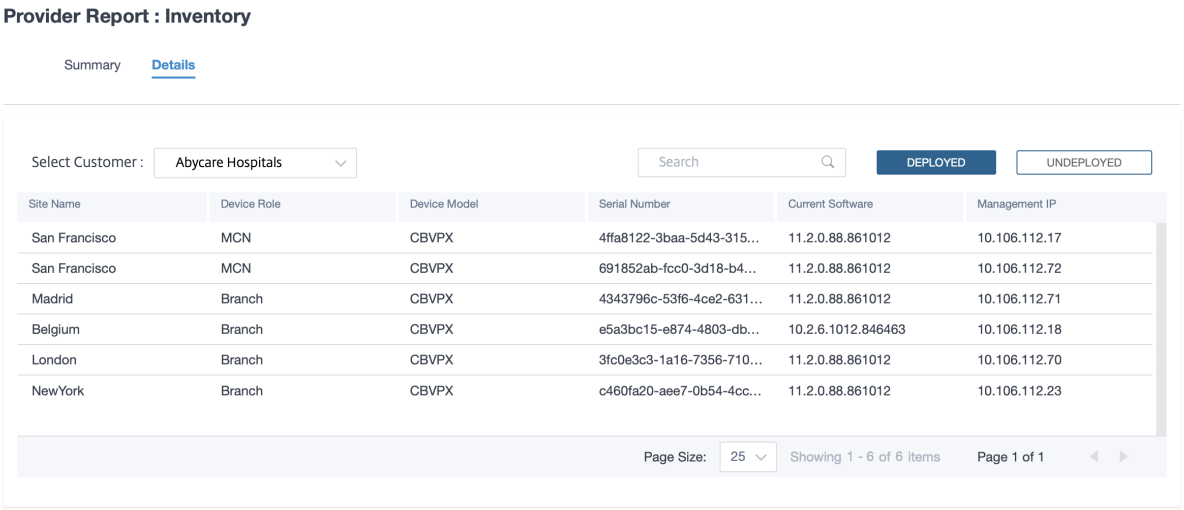
Inventory Summary ビューには、インベントリスプレッドのチャートが表示され、さまざまなアプライアンスモデルと、カスタマーネットワークで使用される各タイプのアプライアンスの数が表示されます。



必要に応じて、適切なフィルタリングオプションを使用できます。たとえば、特定の顧客に属するすべてのアプライアンス、または特定のデバイスモデルを持つすべてのアプライアンスを探します。

インベントリ詳細ビューには、展開されているすべてのアプライアンスと、構成済みだがまだ展開されていないアプライアンスのリストが表示されます。「顧客を選択」ドロップダウンリストから顧客を選択します。サイト名、デバイ

スロール、デバイスモデル、デバイスシリアル番号、現在のソフトウェア、およびデバイス管理 IP アドレスを表示できます。



顧客/ネットワークレポート

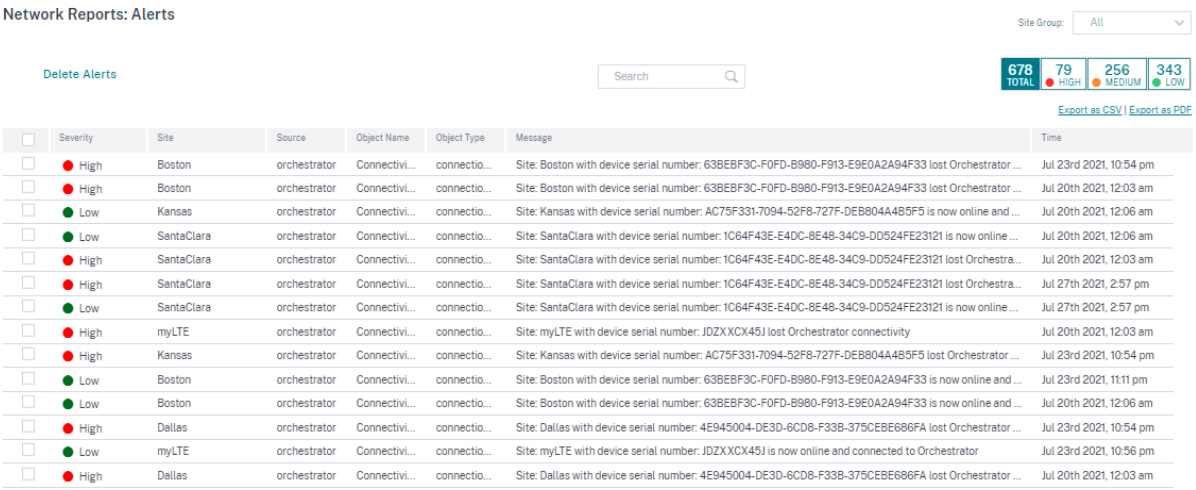
October 26, 2022

顧客レポートでは、ネットワーク全体のアラート、使用状況の傾向、インベントリ、品質、診断、ファイアウォールの状態を顧客ネットワーク内のすべてのサイトで集計して可視化できます。

アラート

お客様は、このネットワーク内のすべてのサイトで生成されたすべてのイベントとアラートの詳細レポートを確認できます。

重大度、アラートが発生したサイト、アラート・メッセージ、時刻、その他の詳細情報が含まれます。



必要に応じて、適切なフィルタリングオプションを使用できます。たとえば、すべてのサイトで重要度の高いアラートをすべて検索したり、特定のサイトのすべてのアラートを検索したりできます。

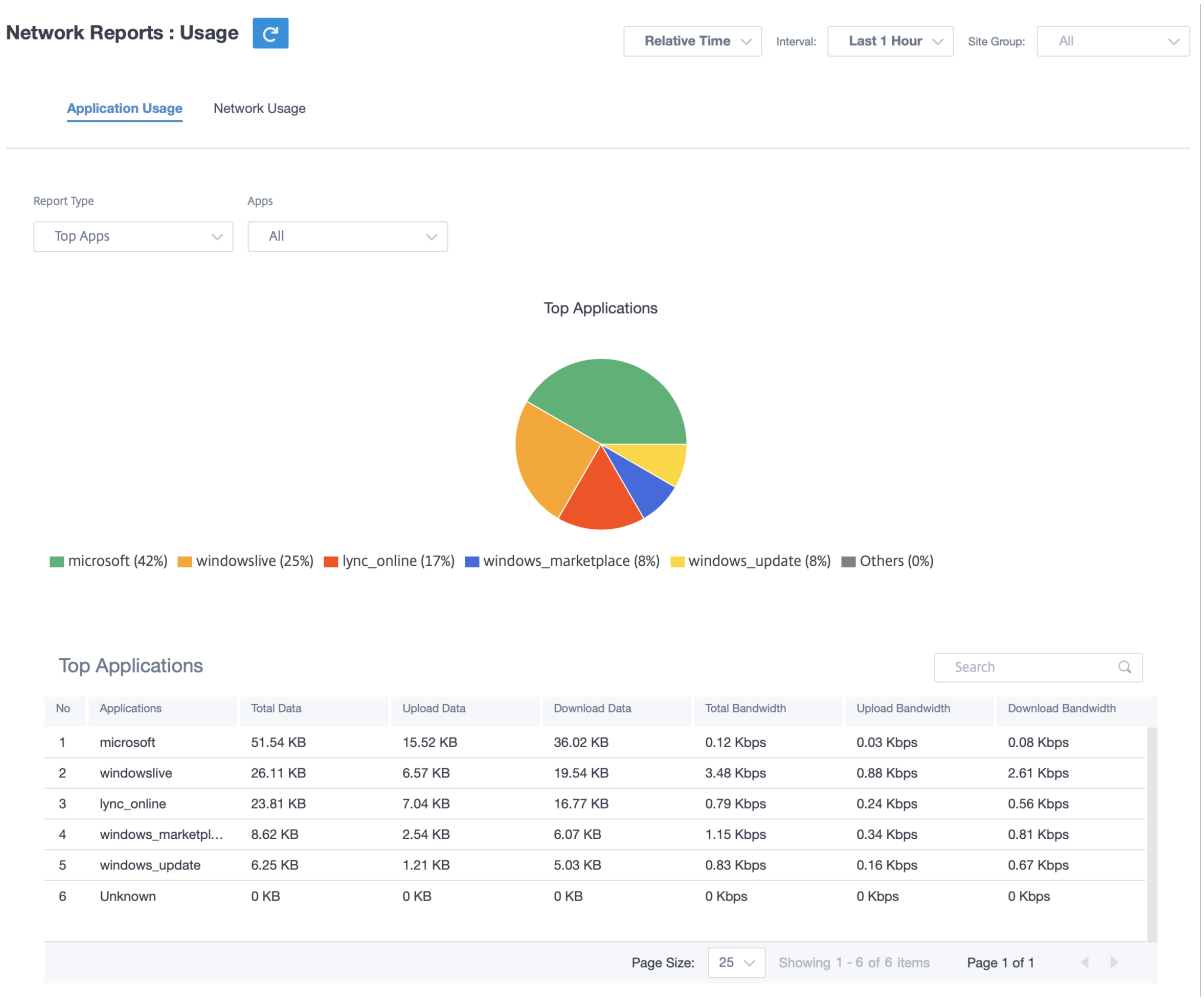
アラートを選択およびクリアすることもできます。

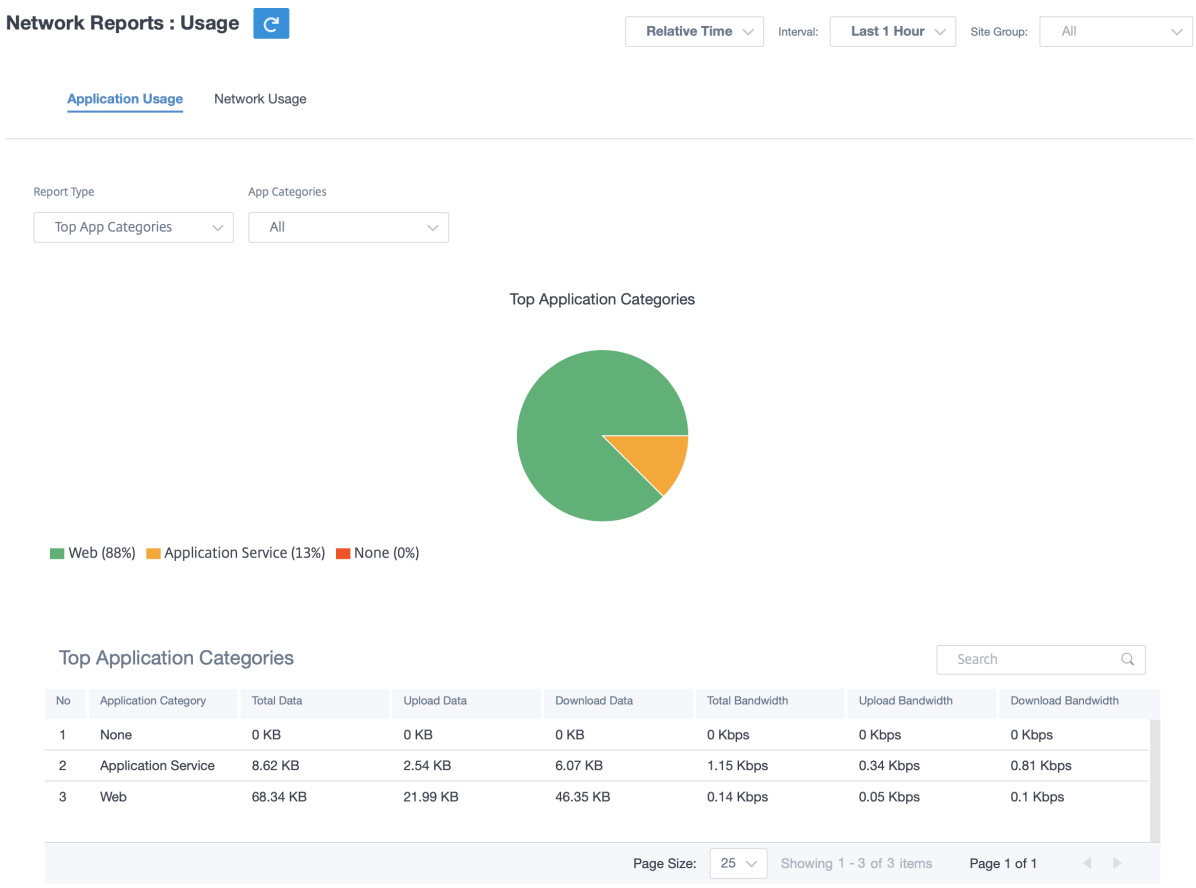
使用状況

お客様は、ネットワーク内のすべてのサイトにおける上位アプリケーション、** 上位アプリケーションカテゴリ、アプリ帯域幅、上位サイトなどの使用傾向を確認できます ** 。

上位アプリケーションとアプリケーションカテゴリ

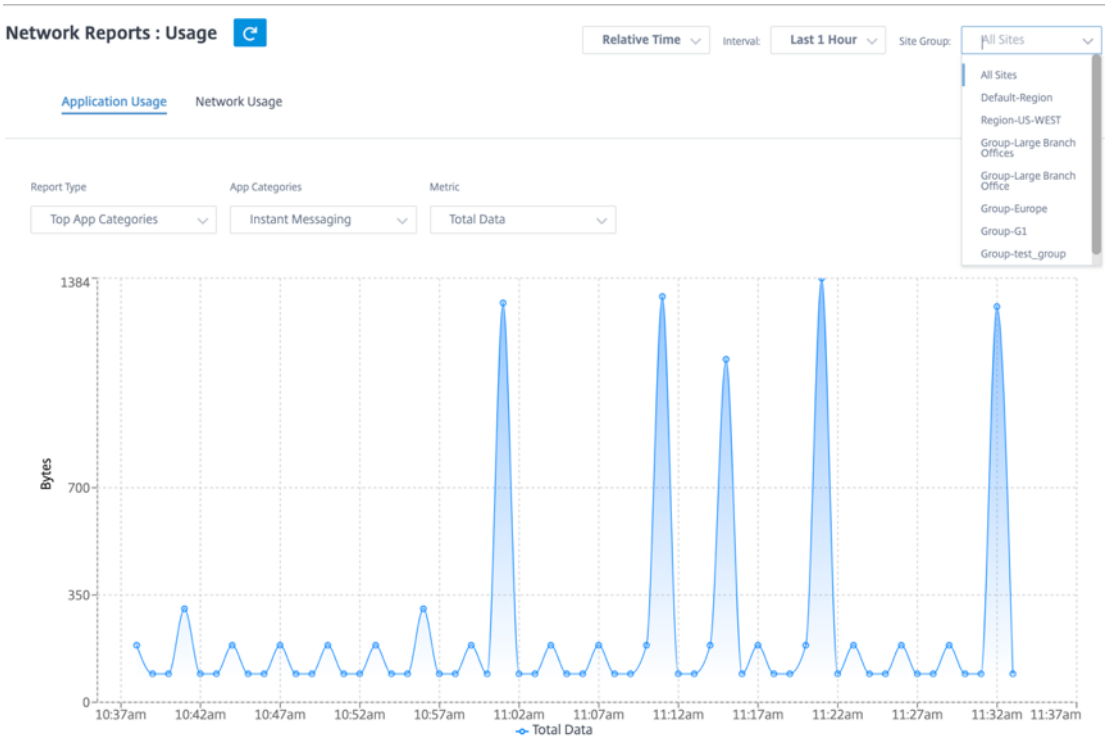
** 上位アプリケーションと上位アプリケーションカテゴリのグラフには ** 、すべてのサイトで広く使用されている上位アプリケーションと上位アプリケーションファミリが表示されます。これにより、データ消費パターンを分析し、ネットワーク内のデータクラスごとに帯域幅制限を再割り当てできます。





アプリケーション帯域幅

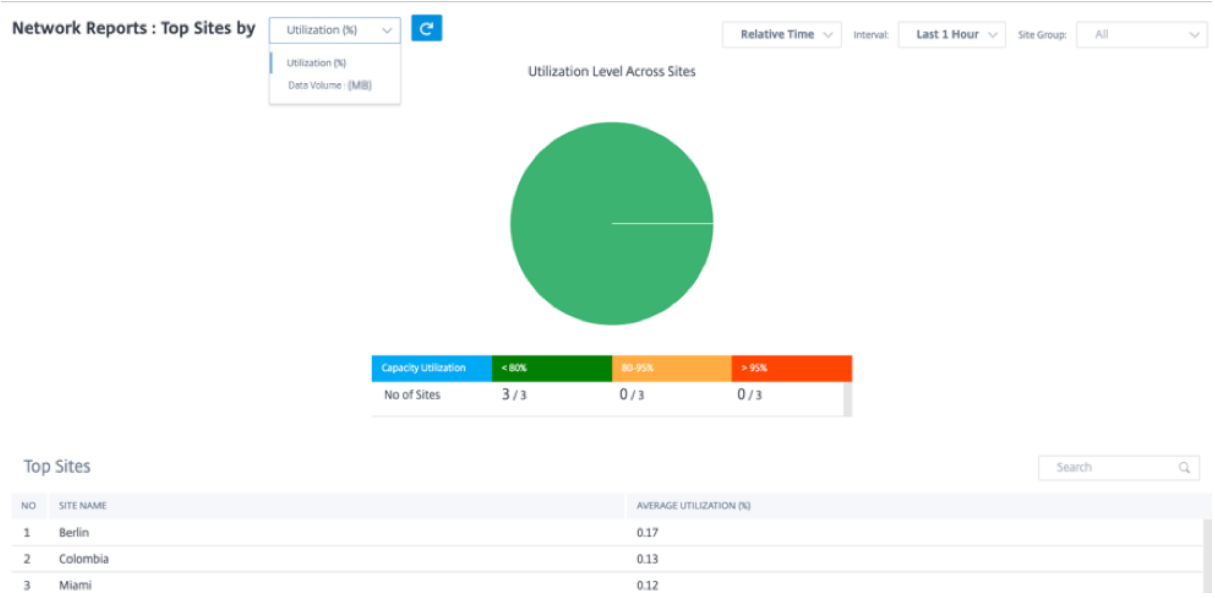
選択したサイトグループまたはすべてのサイトの帯域幅使用状況の統計を表示できます。選択した時間間隔について、帯域幅統計情報が収集されます。レポートタイプ、アプリまたはアプリカテゴリ、および指標に基づいて統計レポートをフィルタリングできます **。



- レポートタイプ**:** リストから [上位のアプリ**]** または **[**アプリカテゴリ] を選択します。
- アプリ**/**アプリカテゴリ**:** 一覧から上位のアプリケーションまたはカテゴリ (ネットワークサービスなど) を選択します。
- メトリック**:** リストから帯域幅メトリック (合計データ、受信データ、合計帯域幅など) を選択します。

ネットワーク使用状況

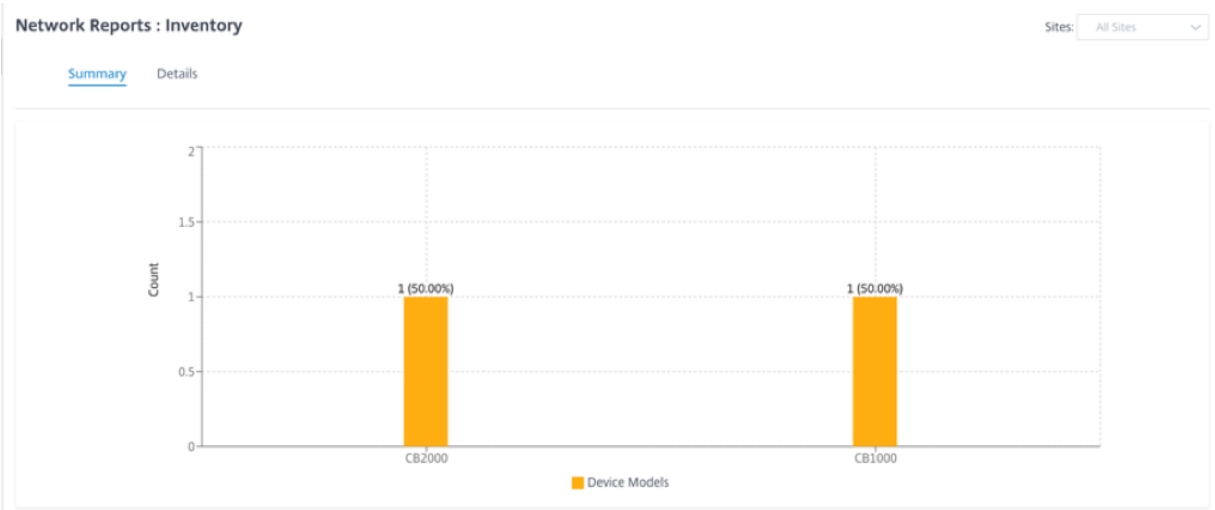
Top Sites グラフには、帯域幅使用率が最も高い顧客ネットワークの上位サイトが表示されます。サイトは、使用率（%）またはトラフィック量（MB）別に表示できます。



Inventory

お客様は、ネットワーク内のすべてのサイトのデバイスインベントリ全体を表示できます。在庫概要を表示するか、詳細ビューを表示するかを選択できます。

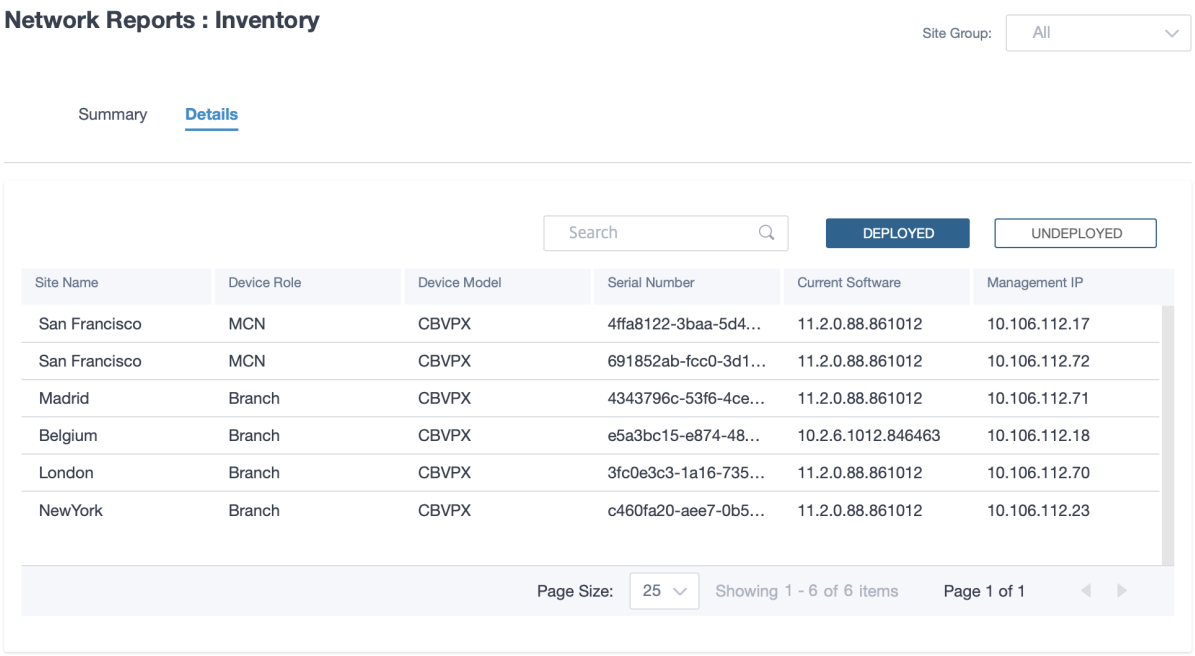
Inventory Summary ビューには、インベントリスプレッドのチャートが表示され、カスタマーネットワーク内のすべてのサイトで使用されているさまざまなアプライアンスモデルと各タイプのアプライアンスの数が表示されます。



必要に応じて、適切なフィルタリングオプションを使用できます。たとえば、特定のサイトに属するすべてのアプライアンスや、特定のデバイスモデルのすべてのアプライアンスを検索するなどです。

インベントリ詳細ビューには、展開されているすべてのアプライアンスと、構成済みだがまだ展開されていないアプライアンスのリストが表示されます。お客様、サイト名、デバイスの役割、デバイスのシリアル番号、現在のソフト

ウェア、デバイス管理 IP アドレスとともに。

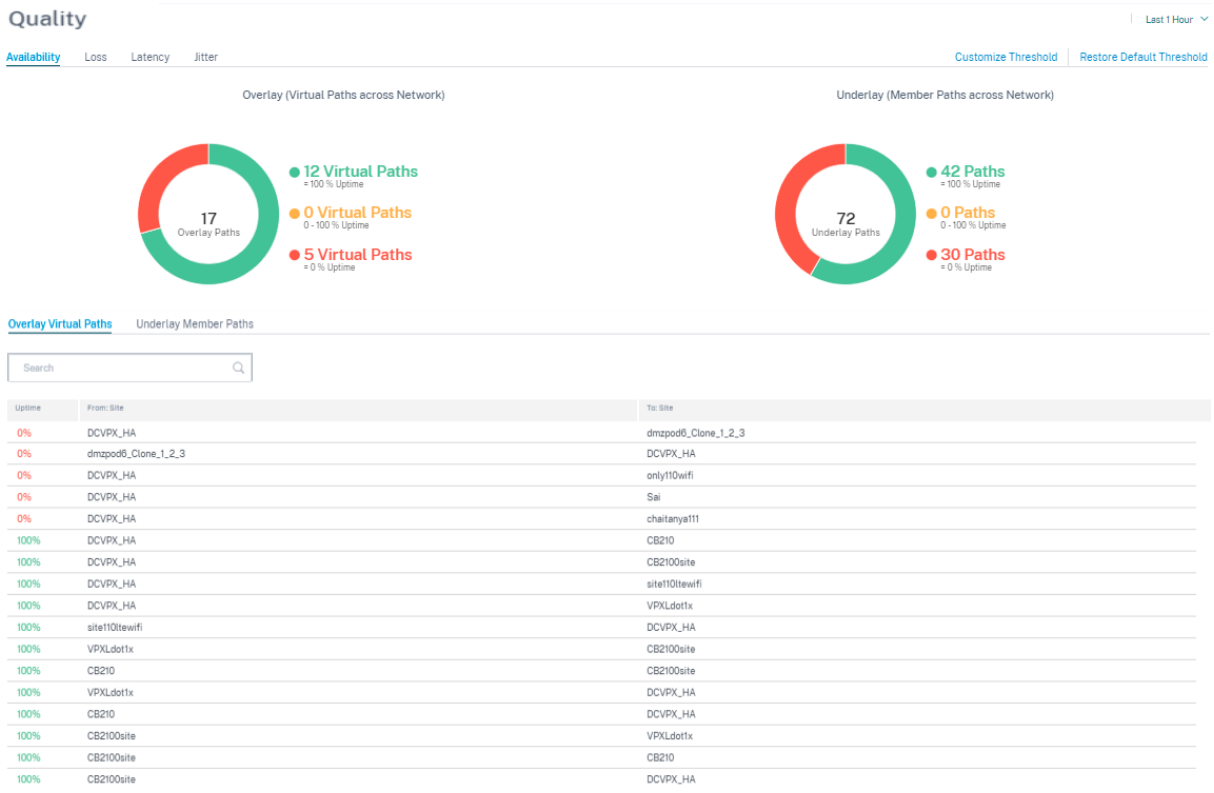


HDX ダッシュボードとレポート

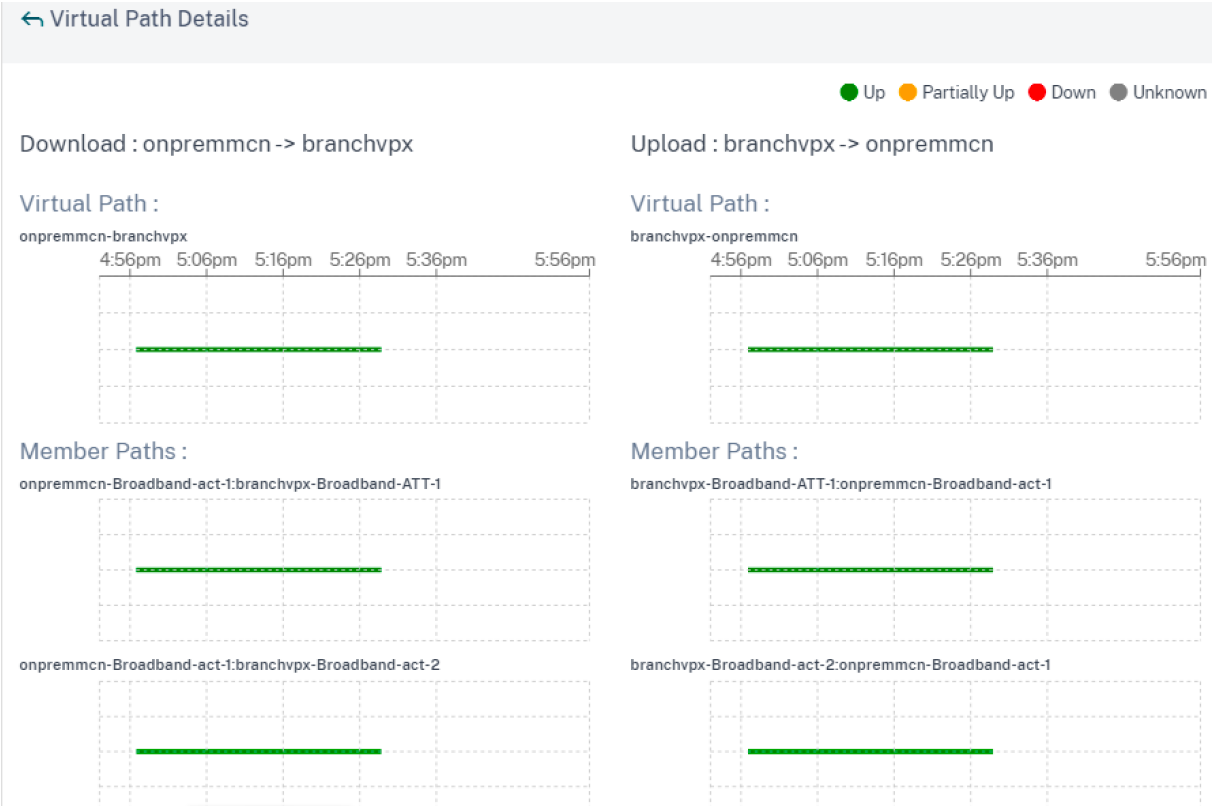
HDX ダッシュボードとレポートの詳細については、「HDX ダッシュボードとレポート」を参照してください。

品質

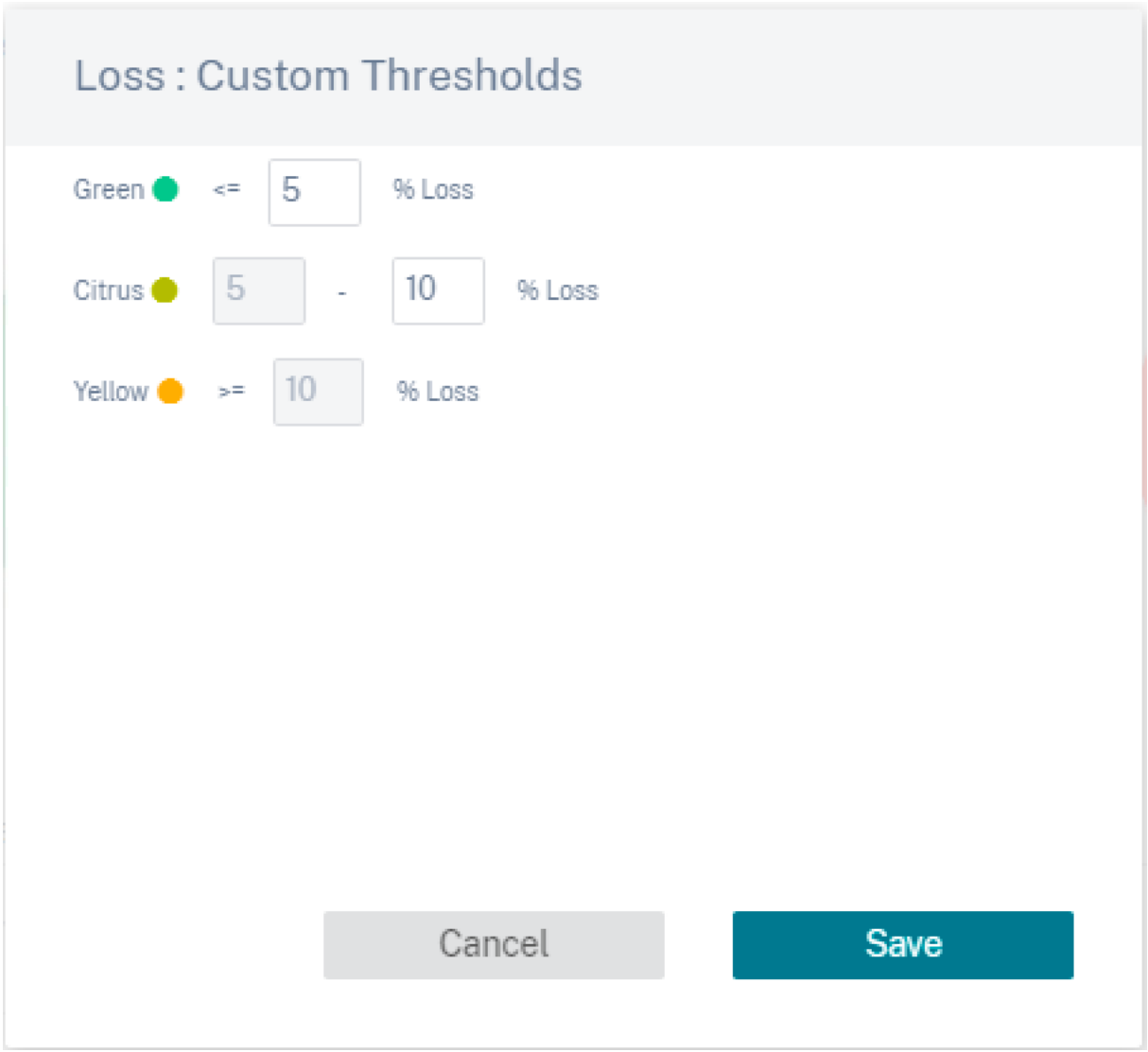
ネットワーク品質レポートでは、可用性、損失、遅延、ジッターの観点から、仮想オーバーレイパスと物理アンダーレイパスをネットワークレベルで比較できます。これにより、オーバーレイがアンダーレイネットワークに対してどのように変化しているかを効果的に監視でき、トラブルシューティングにも役立ちます。レイテンシーとジッターについては、アンダーレイメンバーパスの詳細のみが表示されます。



テーブルエントリをクリックすると、詳細ビューが表示されます。



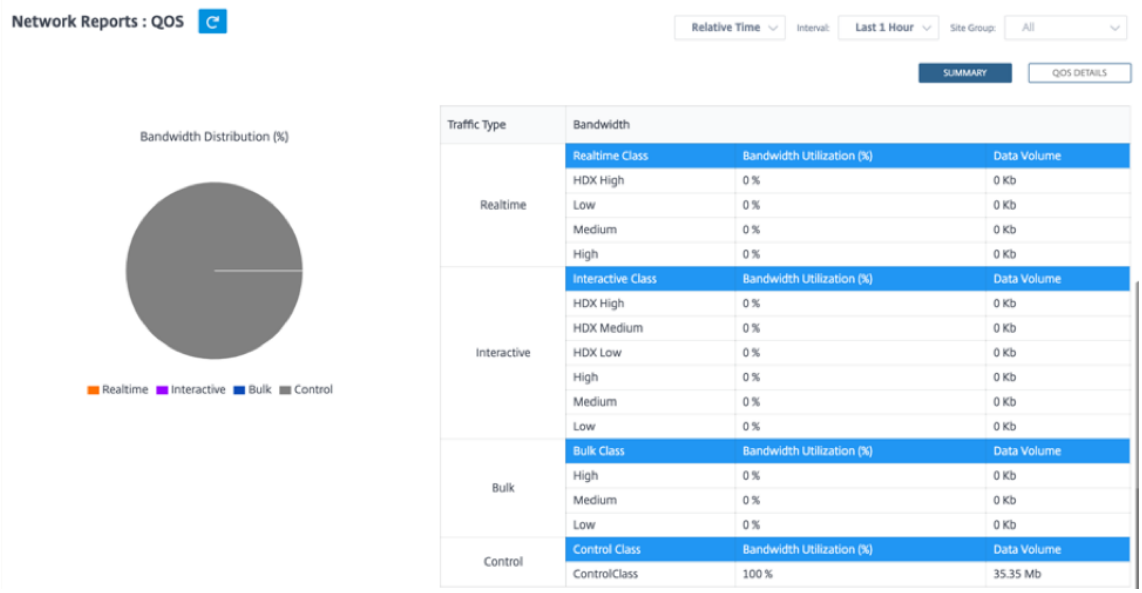
各ネットワーク品質パラメータの閾値はカスタマイズできます。



サービス品質

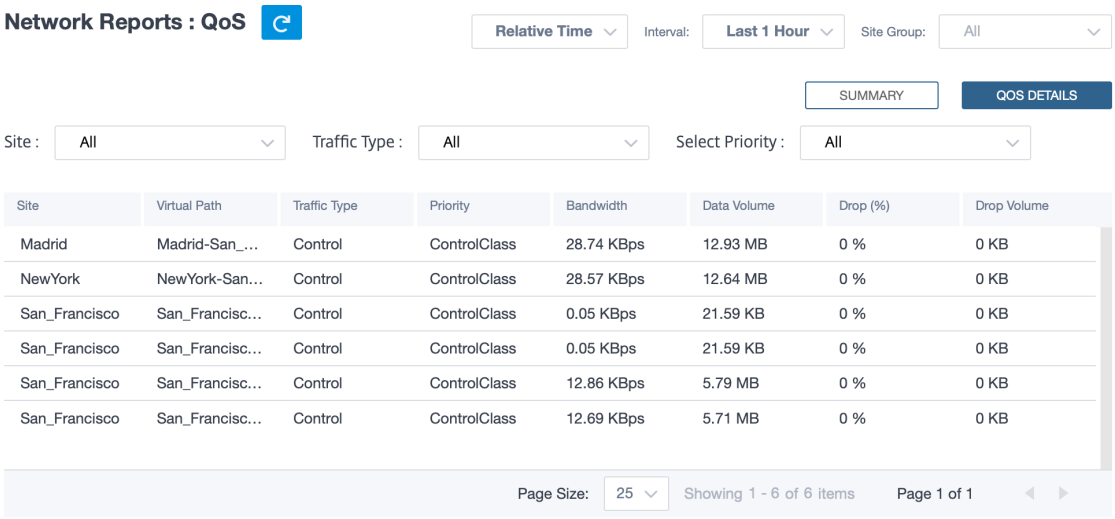
Quality of Service（QoS; サービス品質）は、データトラフィックを管理し、ネットワーク上のパケット損失、遅延、ジッタを削減します。詳細については、「サービス品質」を参照してください。QoS（サービス品質）レポートを表示するには、次の 2 つの方法があります。

- 概要ビュー**:** 概要ビューには、あらゆる種類のトラフィック（リアルタイム、インタラクティブ、バルク、ネットワーク全体およびサイトごとの制御）の帯域幅消費量の概要が表示されます。



  - リアルタイム**:** 低遅延、低帯域幅、時間に敏感なトラフィックに使用されます。リアルタイムアプリケーションは時間に依存しますが、実際には高帯域幅（Voice over IP など）を必要としません。リアルタイムアプリケーションは、レイテンシーとジッタの影響を受けますが、ある程度の損失を許容できます。
  - インタラクティブ**:** 低から中程度の遅延要件と低から中程度の帯域幅要件を持つインタラクティブトラフィックに使用されます。インタラクティブなアプリケーションは、マウスクリックまたはカーソル移動の形で人間の入力を伴います。通常、対話はクライアントとサーバーの間で行われます。通信は、高帯域幅を必要としない場合がありますが、損失や遅延に敏感です。ただし、サーバからクライアントへのグラフィック情報の転送には高い帯域幅が必要であり、損失の影響を受けない可能性があります。
  - バルク**:** 高遅延を許容できる高帯域幅のトラフィックに使用されます。ファイル転送を処理し、高帯域幅を必要とするアプリケーションは、バルククラスに分類されます。これらのアプリケーションは、人間の干渉をほとんど伴わず、ほとんどシステム自体によって処理されます。
  - コントロール**:** ルーティング、スケジューリング、およびリンク統計情報を含むコントロールパケットの転送に使用されます。

- 詳細ビュー**:** 詳細ビューでは、オーバーレイ仮想パスに関連する各 QoS クラスについて、帯域幅消費量、トラフィック量、ドロップされたパケット数などの傾向を把握できます。



このレポートは、2 つのサイト間の仮想パスに基づいて QoS 統計を表示できるサイトレベルで使用できます。詳しくは、「サイトレポート」を参照してください。

履歴統計

サイトごとに、次のネットワークパラメータの統計をグラフとして表示できます。

- サイト
- 仮想パス
- パス
- WAN リンク
- インターフェイス
- クラス
- GRE トンネル
- IPsec トンネル

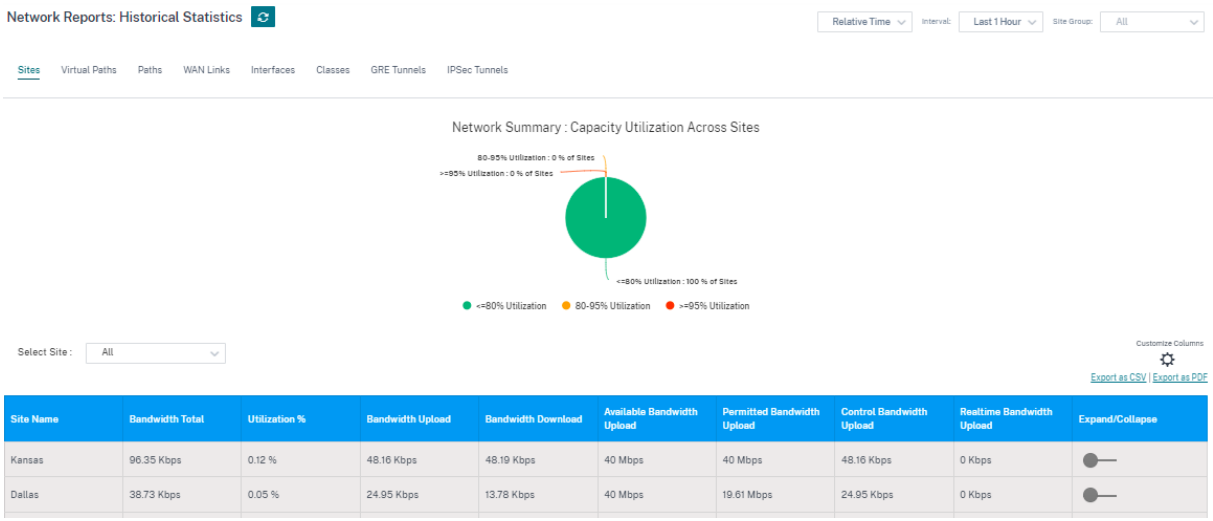
統計はグラフとして収集されます。これらのグラフはタイムライン対使用量としてプロットされるため、さまざまなネットワークオブジェクトプロパティの使用傾向を把握できます。ネットワーク全体のアプリケーション統計のグラフを表示できます。

必要に応じて、グラフの表示と非表示を切り替えたり、列をカスタマイズしたりできます。

サイト

サイト統計を表示するには、[レポート] **>** [履歴統計] **>** [サイト] タブに移動します。

リストからサイト名を選択します。

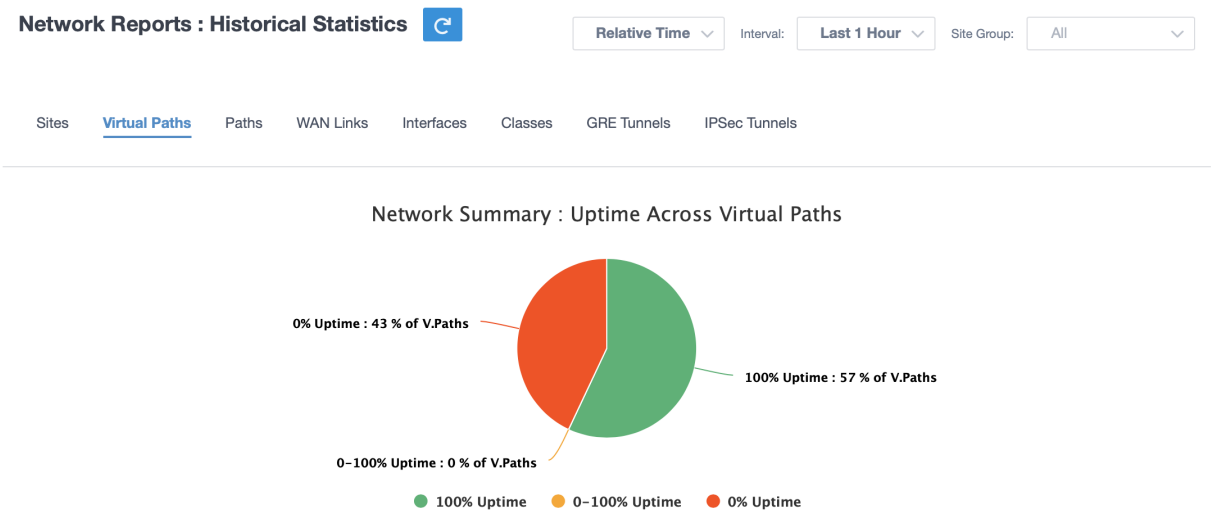


次のメトリックを表示できます。

- サイト名: サイト名。
- 帯域幅合計: すべてのパケットタイプで消費された合計帯域幅。帯域幅 = 制御帯域幅 + リアルタイム帯域幅 + 対話型帯域幅 + バルク帯域幅
- 使用率: サイトの統計情報を利用率 (%) 別に表示できます。
- 帯域幅入力:WAN ポート経由の最大ダウンロード速度と最小ダウンロード速度。
- 下り帯域幅:WAN ポート経由の最大アップロード速度と最小アップロード速度。
- 使用可能な入力帯域幅: サイトのすべての WAN リンクに割り当てられた合計帯域幅。
- 許容帯域幅: 情報の送信に使用できる帯域幅。
- 制御帯域幅入力: ルーティング、スケジューリング、およびリンク統計情報を含む制御パケットの転送に使用される帯域幅。
- リアルタイム帯域幅イングレス:NetScaler SD-WAN 構成のリアルタイムクラスタイプに属するアプリケーションによって消費される帯域幅。このようなアプリケーションのパフォーマンスは、ネットワーク遅延に大きく依存します。遅延したパケットは、失われたパケットよりも劣ります（たとえば、VoIP、Skype for Business）。
- 展開/折りたたみ: 必要に応じてデータを展開または縮小できます。

仮想パス

仮想パスの統計情報を表示するには、[レポート] **>** [統計] **>** [仮想パス] タブに移動します。



Virtual Path Name	Uptime %	Latency	Loss	Jitter	Bandwidth Upload	Control Bandwidth	Realtime Bandwidth	Interactive Bandwidth	Expand/Collapse
San_Francisco - Belgium	0 %	--	--	--	3.12 Kbps	--	--	--	
San_Francisco - London	0 %	--	--	--	1.04 Kbps	--	--	--	
London - San_Francisco	0 %	--	--	--	0 Kbps	--	--	--	
San_Francisco - Madrid	100 %	2 ms	0 %	2 ms	12.7 Kbps	12.7 Kbps	0 Kbps	0 Kbps	
Madrid - San_Francisco	100 %	2 ms	0 %	2 ms	24.35 Kbps	24.35 Kbps	0 Kbps	0 Kbps	
NewYork - San_Francisco	100 %	2 ms	0 %	2 ms	24.22 Kbps	24.22 Kbps	0 Kbps	0 Kbps	
San_Francisco - NewYork	100 %	2 ms	0 %	2 ms	12.61 Kbps	12.61 Kbps	0 Kbps	0 Kbps	

次のメトリックを表示できます。

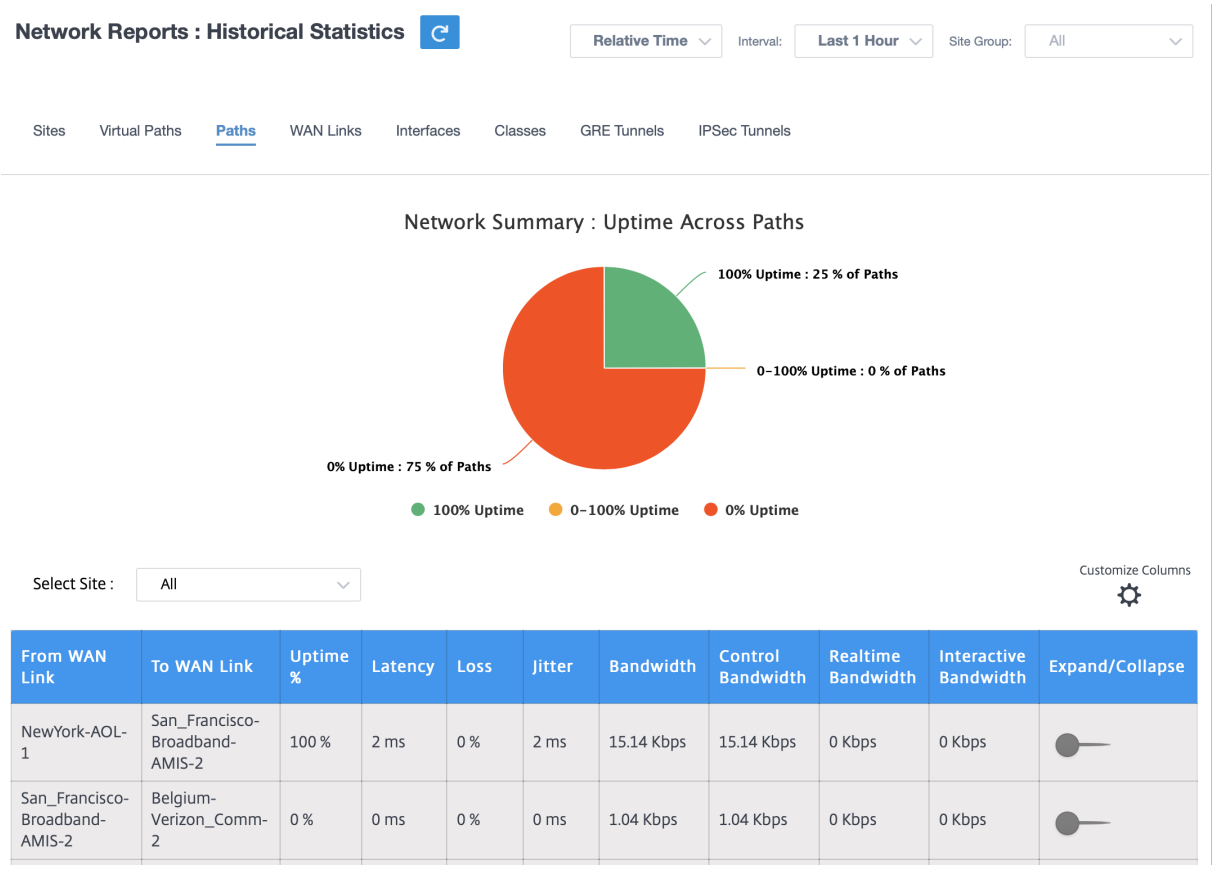
- 仮想パス名: 仮想パス名。
- レイテンシー: リアルタイムトラフィックのレイテンシー (ミリ秒単位)。
- 損失: 失われたパケットの割合。
- ジッター: 受信パケットの遅延の変動（ミリ秒単位)。
- 入力帯域幅: 入力側 (LAN から WAN 間) 選択した期間の帯域幅使用量。
- 制御帯域幅: ルーティング、スケジューリング、およびリンク統計情報を含む制御パケットの転送に使用される帯域幅。
- リアルタイム帯域幅:SD-WAN 構成のリアルタイムクラスタイプに属するアプリケーションによって消費される帯域幅。このようなアプリケーションのパフォーマンスは、ネットワーク遅延に大きく依存します。遅延したパケットは、失われたパケットよりも劣ります（たとえば、VoIP、Skype for Business)。
- インタラクティブ帯域幅:SD-WAN 構成のインタラクティブクラスタイプに属するアプリケーションによって消費される帯域幅。このようなアプリケーションのパフォーマンスは、ネットワーク遅延とパケット損失に大

きく依存します（たとえば、XenDesktop、XenApp）。

- バルク帯域幅:SD-WAN 構成のバルククラスタイプに属するアプリケーションによって消費される帯域幅。これらのアプリケーションは、人間の介入がほとんどなく、システム自体（FTP、バックアップ操作など）によって処理されます。
- 展開/折りたたみ: 必要に応じてデータを展開または縮小できます。

パス

パス統計を表示するには、[レポート] **>** [統計] **>** [パス] タブに移動します。



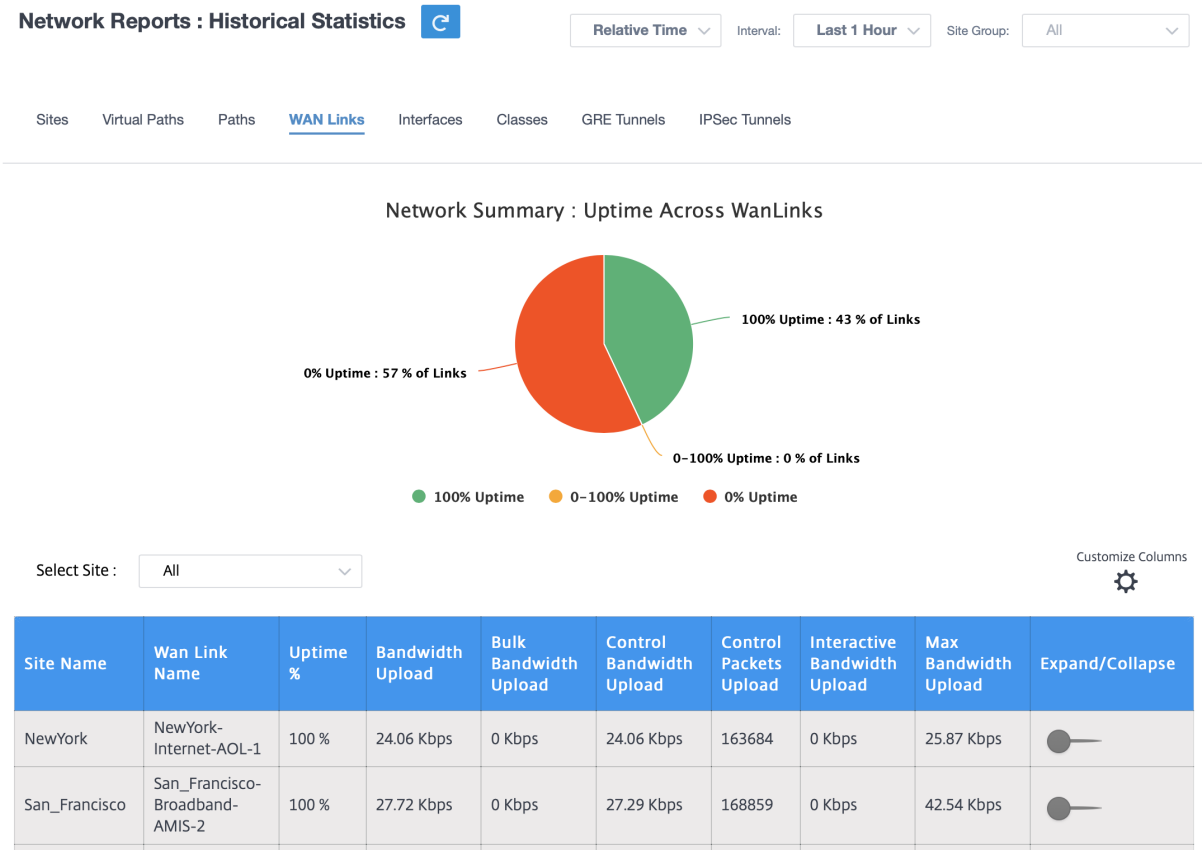
次のメトリックを表示できます。

- **WAN** リンクから: ソース WAN リンク。
- **WAN** リンクへ: 宛先 WAN リンク。
- レイテンシー: リアルタイムトラフィックのレイテンシー (ミリ秒単位)。
- 損失: 失われたパケットの割合。
- ジッター: 受信パケットの遅延の変動（ミリ秒単位）。
- 帯域幅: すべてのパケットタイプで消費される合計帯域幅。帯域幅 = 制御帯域幅 + リアルタイム帯域幅 + インタラクティブ帯域幅 + バルク帯域幅

- 制御帯域幅: ルーティング、スケジューリング、およびリンク統計情報を含む制御パケットの転送に使用される帯域幅。
- リアルタイム帯域幅:SD-WAN 構成のリアルタイムクラスタイプに属するアプリケーションによって消費される帯域幅。このようなアプリケーションのパフォーマンスは、ネットワーク遅延に大きく依存します。遅延したパケットは、失われたパケットよりも劣ります（たとえば、VoIP、Skype for Business）。
- インタラクティブ帯域幅:SD-WAN 構成のインタラクティブクラスタイプに属するアプリケーションによって消費される帯域幅。このようなアプリケーションのパフォーマンスは、ネットワーク遅延とパケット損失に大きく依存します（たとえば、XenDesktop、XenApp）。
- バルク帯域幅:SD-WAN 構成のバルククラスタイプに属するアプリケーションによって消費される帯域幅。これらのアプリケーションは、人間の介入がほとんどなく、システム自体（FTP、バックアップ操作など）によって処理されます。
- 展開/折りたたみ: 必要に応じてデータを展開または縮小できます。

WAN リンク

WAN リンクレベルで統計情報を表示するには、[レポート] **>** [統計] **>** [**WAN** リンク] タブに移動します。



次のメトリックを表示できます。

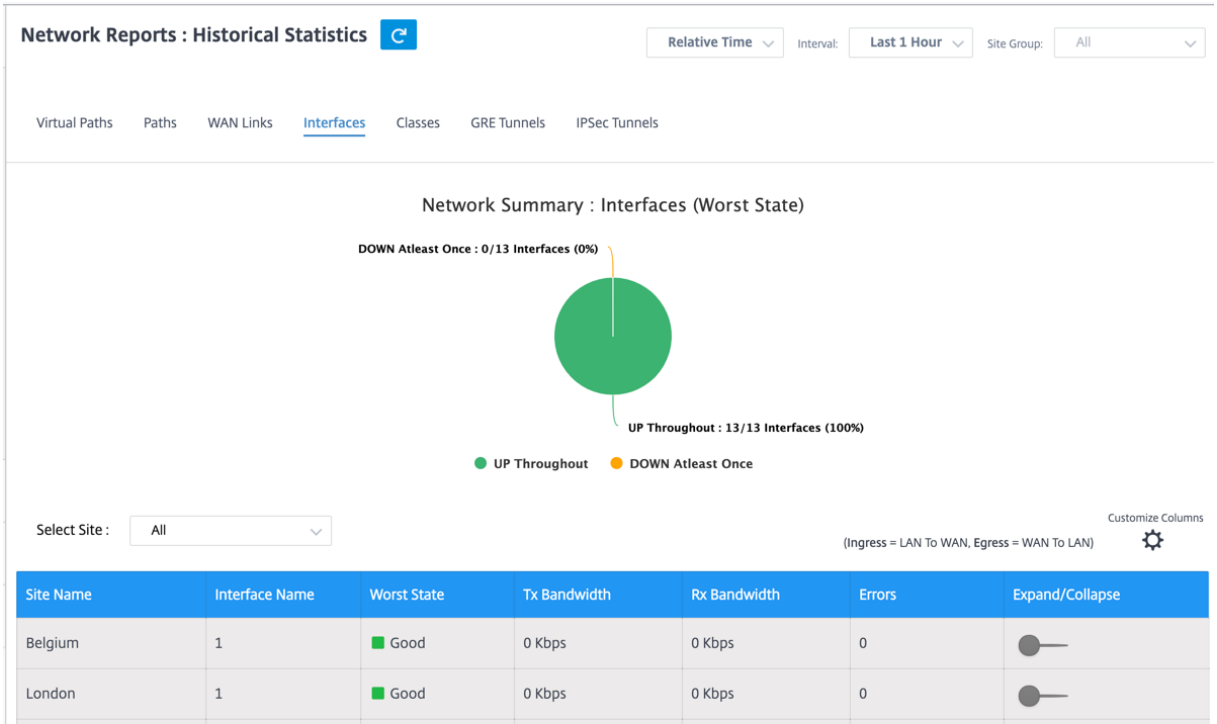
- **WAN** リンク名: パス名。

- 入力帯域幅: 入力側 (LAN から WAN 間) 選択した期間の帯域幅使用量。
- バルク帯域幅イングレス: 入力側 (LAN-to-WAN) 仮想パス選択した期間にバルクトラフィックが使用する帯域幅。
- 制御帯域幅入力: 選択した期間に制御トラフィックが使用した入力（LAN から WAN）の仮想パス帯域幅。
- コントロール・パケット・イングレス: 選択した期間の入力（LAN から WAN）の仮想パス制御パケット。
- インタラクティブ帯域幅イングレス: 入力側 (LAN-to-WAN) 仮想パスインタラクティブトラフィックが選択した期間に使用した帯域幅。
- 最大入力帯域幅: 選択した期間の 1 分間の最大入力帯域幅 (LAN から WAN)。
- 最小入力帯域幅: 選択した期間の 1 分間の最小入力帯域幅 (LAN から WAN)。
- 展開/折りたたみ: 必要に応じてデータを展開または縮小できます。

インターフェイス

インターフェイス統計レポートは、トラブルシューティング中に、いずれかのポートがダウンしているかどうかをすばやく確認するのに役立ちます。また、各ポートの送受信帯域幅、またはパケットの詳細を表示することもできます。また、特定の期間にこれらのインターフェイスで発生したエラーの数を表示することもできます。

インターフェイス統計を表示するには、[レポート] **>** [統計] **>** [インターフェイス] タブに移動します。



次のメトリックを表示できます。

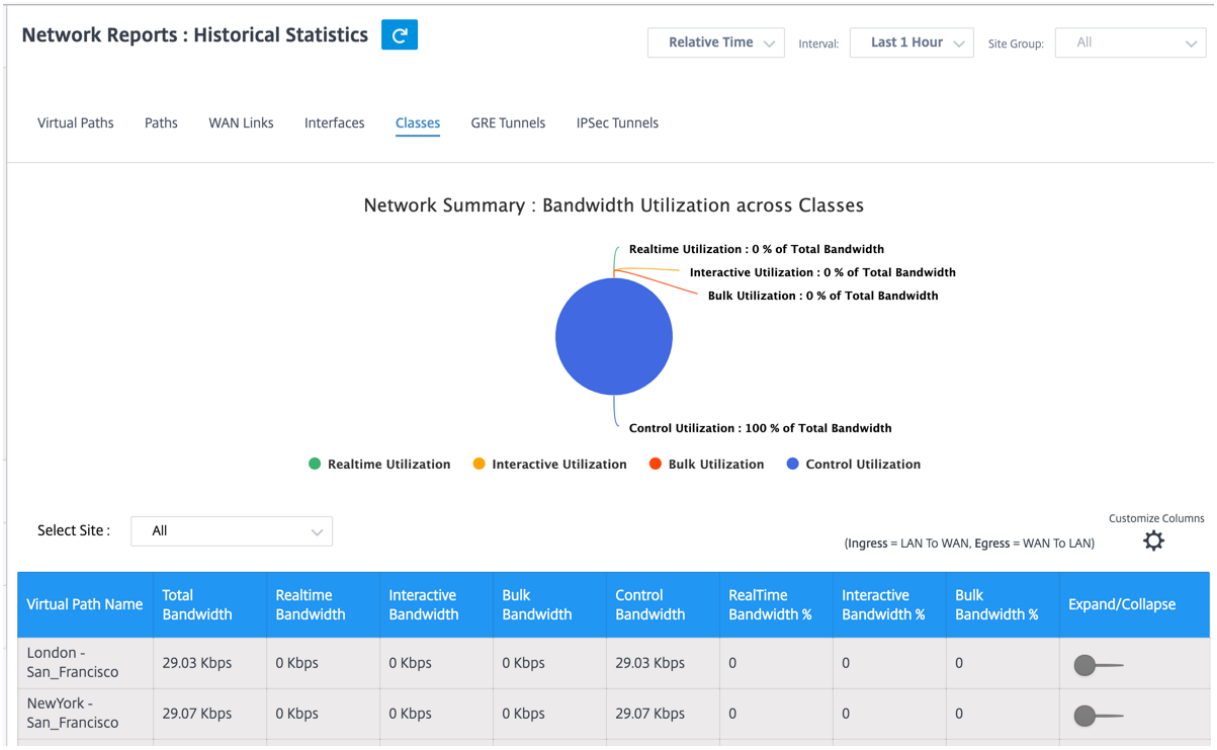
- インターフェース名: イーサネットインターフェースの名前。
- **Tx** 帯域幅: 送信された帯域幅。
- 受信帯域幅: 受信した帯域幅。

- エラー: 選択した期間中に発生したエラーの数。
- 展開/折りたたみ: 必要に応じてデータを展開または縮小できます。

クラス

仮想サービスは特定の QoS クラスに割り当てることができ、クラスごとに異なる帯域幅制限を適用できます。

クラス統計を表示するには、[レポート] **>** [統計] **>** [クラス] タブに移動します。



次のメトリックを表示できます。

- **QoS** クラス: クラス名。
- 帯域幅: 送信帯域幅。
- データ量: 送信されたデータ（Kbps 単位）。
- ドロップボリューム: ドロップされたデータの割合。
- ドロップ率: ドロップされたデータの割合。
- 展開/折りたたみ: 必要に応じてデータを展開または縮小できます。

GRE トンネル

トンネリングメカニズムを使用して、あるプロトコルのパケットを別のプロトコル内で転送できます。他のプロトコルを伝送するプロトコルはトランスポートプロトコルと呼ばれ、伝送されたプロトコルはパッセンジャープロトコル

と呼ばれます。Generic Routing Encapsulation（GRE）は、トランスポートプロトコルとして IP を使用し、さまざまなパッセンジャープロトコルを伝送できるトンネリングメカニズムです。

トンネルの送信元アドレスと宛先アドレスは、トンネル内の仮想ポイントツーポイントリンクの 2 つのエンドポイントを識別するために使用されます。Citrix SD-WAN アプライアンスでの GRE トンネルの構成について詳しくは、「GRE トンネル」を参照してください。

GRE トンネルの統計情報を表示するには、[レポート**] > [**統計**] > [GRE** トンネル] タブに移動します。

次のメトリックを表示できます。

- サイト名: サイト名。
- **Tx** 帯域幅: 送信された帯域幅。
- 受信帯域幅: 受信した帯域幅。
- **Packet Dropped**：ネットワークの輻輳が原因でドロップされたパケットの数。
- フラグメント化されたパケット: フラグメント化されたパケットの数。パケットはフラグメント化されて、元のデータグラムよりも小さい MTU を持つリンクを通過できる小さなパケットを作成します。フラグメントは受信ホストによって再構成されます。
- 展開/折りたたみ: 必要に応じてデータを展開または縮小できます。

IPSec トンネル

IP セキュリティ（IPsec）プロトコルは、機密データの暗号化、認証、再生に対する保護、IP パケットのデータ機密性などのセキュリティサービスを提供します。カプセル化セキュリティペイロード (ESP) および認証ヘッダー (AH) は、これらのセキュリティサービスを提供するために使用される 2 つの IPsec セキュリティプロトコルです。

IPsec トンネルモードでは、元の IP パケット全体が IPsec によって保護されます。元の IP パケットはラップおよび暗号化され、VPN トンネルを介してパケットを送信する前に新しい IP ヘッダーが追加されます。
Citrix SD-WAN アプライアンスの IPsec トンネルの構成について詳しくは、「IPsec トンネル終了」を参照してください。

IPsec トンネルの統計情報を表示するには、[レポート**] > [**統計**] > [IPsec** トンネル] タブに移動します。

次のメトリックを表示できます。

- トンネル名: トンネル名。
- トンネルの状態:IPsec トンネルの状態。
- **MTU**: 最大伝送ユニット：特定のリンクを介して転送できる最大の IP データグラムのサイズ。
- 受信パケット**:** 受信したパケットの数。
- 送信されたパケット**:** 送信されたパケットの数。
- **Packet Dropped**：ネットワークの輻輳が原因でドロップされたパケットの数。
- ドロップされたバイト数: ドロップされたバイト数。
- 展開/折りたたみ: 必要に応じてデータを展開または縮小できます。

リアルタイム統計

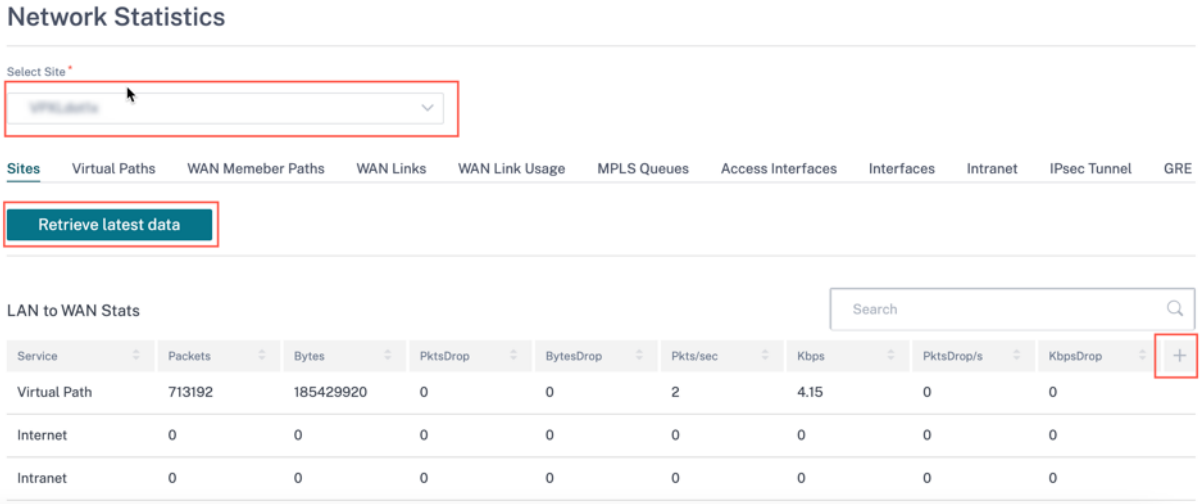
リアルタイム統計ページには、顧客レベルで次の統計情報が表示されます。

ネットワーク統計

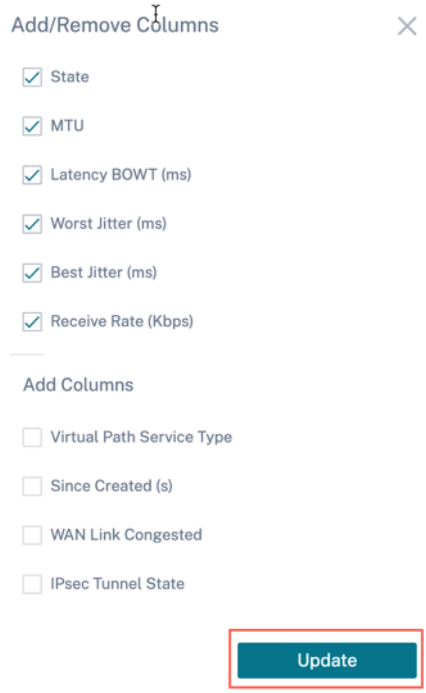
ネットワーク統計ページには、[レポート] > [リアルタイム] > [ネットワーク統計**] ** に次のリアルタイム統計情報が表示されます **。

- サイト
- 仮想パス
- WAN メンバーパス
- WAN リンク
- WAN リンクの使用状況
- MPLS キュー
- アクセスインターフェイス
- インターフェイス
- イントラネット
- IPSec トンネル
- GRE

リアルタイムの統計レポートを取得するには、必要なタブ（サイト、仮想パス、WAN リンクなど）に移動し、ドロップダウンリストからサイトを選択して、「最新データの取得」をクリックします。



プラス (+) 記号をクリックして統計表の列を追加または削除し、[更新] をクリックします。

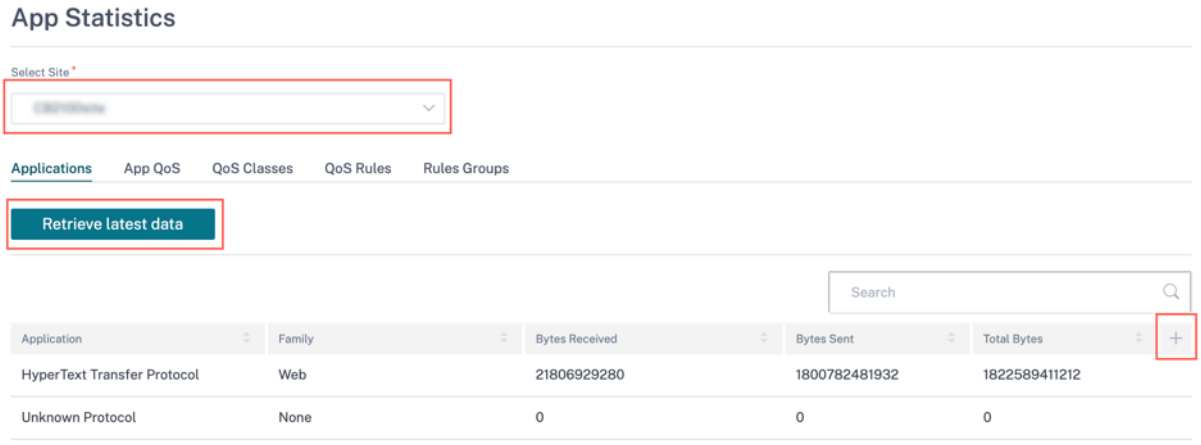


アプリ統計

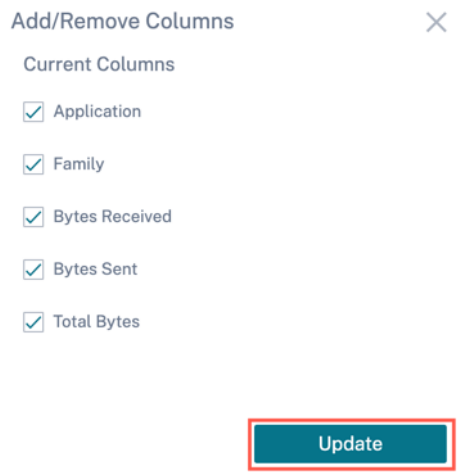
アプリ統計ページには、[レポート] **>** [リアルタイム] **>** [アプリ統計] に、次のリアルタイム統計情報が表示されます。

- アプリケーション
- アプリ QoS
- QoS クラス
- QoS ルール
- ルール・グループ

リアルタイムの統計レポートを取得するには、必要なタブ（アプリケーション、QoS ルール、QoS クラスなど）に移動し、ドロップダウンリストからサイトを選択し、「最新データの取得」をクリックします。



統計情報の表に列を追加または削除する場合は、プラス (+) 記号をクリックし、[更新] をクリックします。

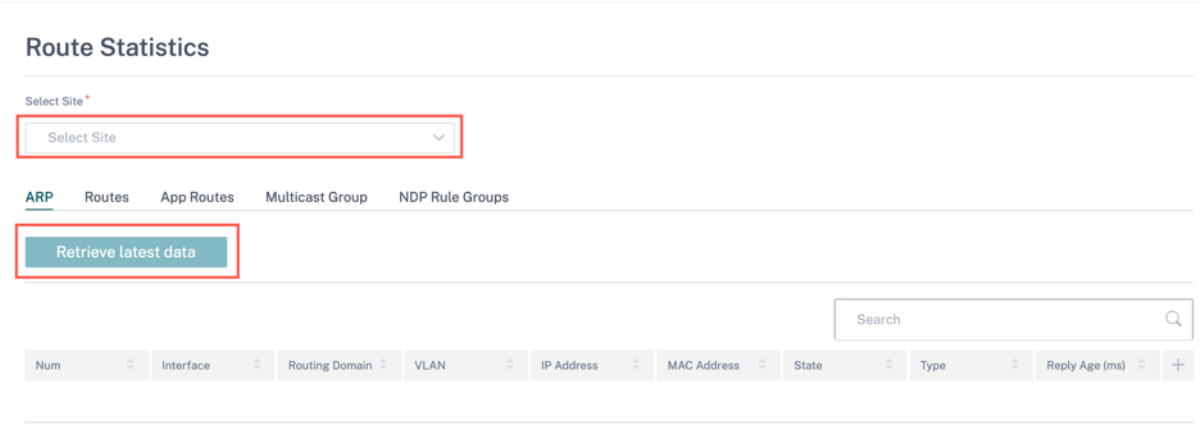


ルート統計情報

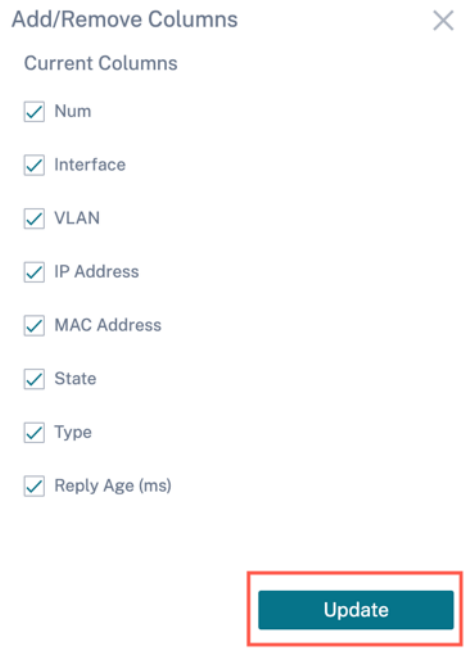
ルート統計ページには、[レポート] **>** [リアルタイム] **>** [ルート統計] に次のリアルタイム統計情報が表示されます。

- ARP
- ルート
- アプリケーションルート
- 観測されたプロトコル
- マルチキャストグループ
- NDP ルールグループ

リアルタイムの統計レポートを取得するには、必要なタブ（ARP、ルート、アプリケーションルートなど）に移動し、ドロップダウンリストからサイトを選択し、「最新データを取得」をクリックします。

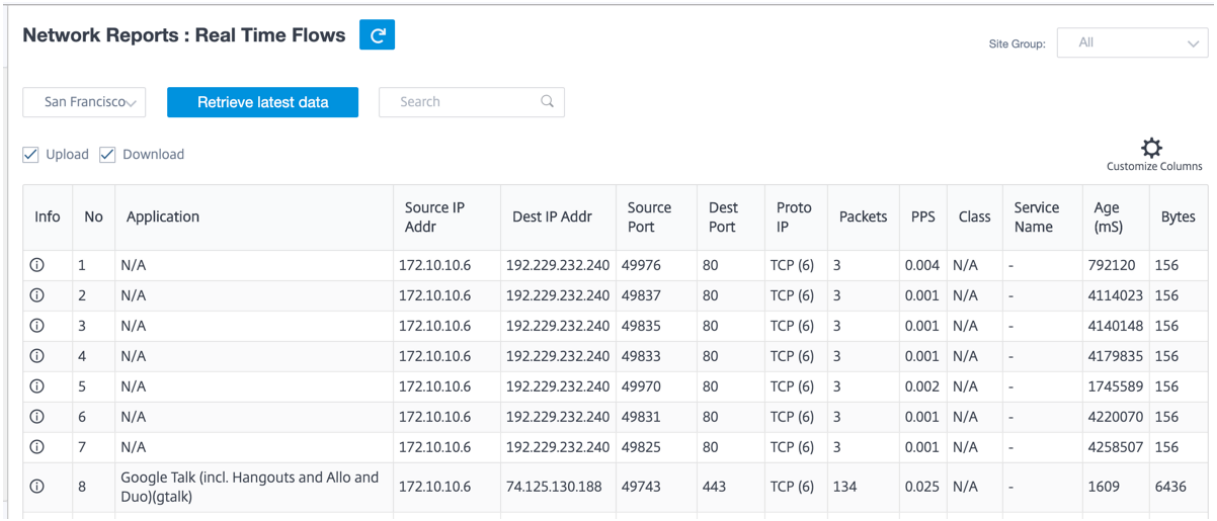


統計情報の表に列を追加または削除する場合は、プラス (+) 記号をクリックし、[更新] をクリックします。



フロー

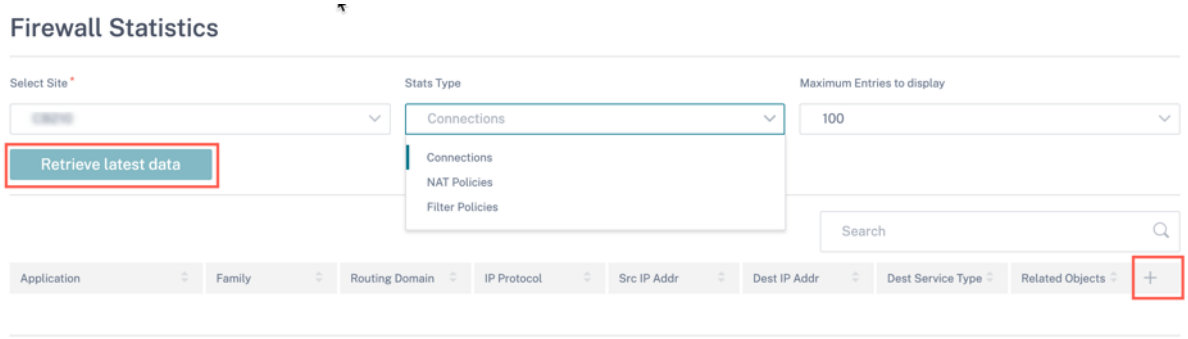
統計情報を取得する前に、ネットワーク・レベルで、ドロップダウン・リストからサイトを選択します。フロー機能は、アプライアンスを通過する特定のセッションに関連する単方向のフロー情報を提供します。これにより、フローが該当する宛先サービスタイプに関する情報と、ルールとクラスタイプ、および伝送モードに関連する情報も提供されます。



Info	No	Application	Source IP Addr	Dest IP Addr	Source Port	Dest Port	Proto IP	Packets	PPS	Class	Service Name	Age (mS)	Bytes
ⓘ	1	N/A	172.10.10.6	192.229.232.240	49976	80	TCP (6)	3	0.004	N/A	-	792120	156
ⓘ	2	N/A	172.10.10.6	192.229.232.240	49837	80	TCP (6)	3	0.001	N/A	-	4114023	156
ⓘ	3	N/A	172.10.10.6	192.229.232.240	49835	80	TCP (6)	3	0.001	N/A	-	4140148	156
ⓘ	4	N/A	172.10.10.6	192.229.232.240	49833	80	TCP (6)	3	0.001	N/A	-	4179835	156
ⓘ	5	N/A	172.10.10.6	192.229.232.240	49970	80	TCP (6)	3	0.002	N/A	-	1745589	156
ⓘ	6	N/A	172.10.10.6	192.229.232.240	49831	80	TCP (6)	3	0.001	N/A	-	4220070	156
ⓘ	7	N/A	172.10.10.6	192.229.232.240	49825	80	TCP (6)	3	0.001	N/A	-	4258507	156
ⓘ	8	Google Talk (incl. Hangouts and Allo and Duo)(gtalk)	172.10.10.6	74.125.130.188	49743	443	TCP (6)	134	0.025	N/A	-	1609	6436

ファイアウォールの統計情報

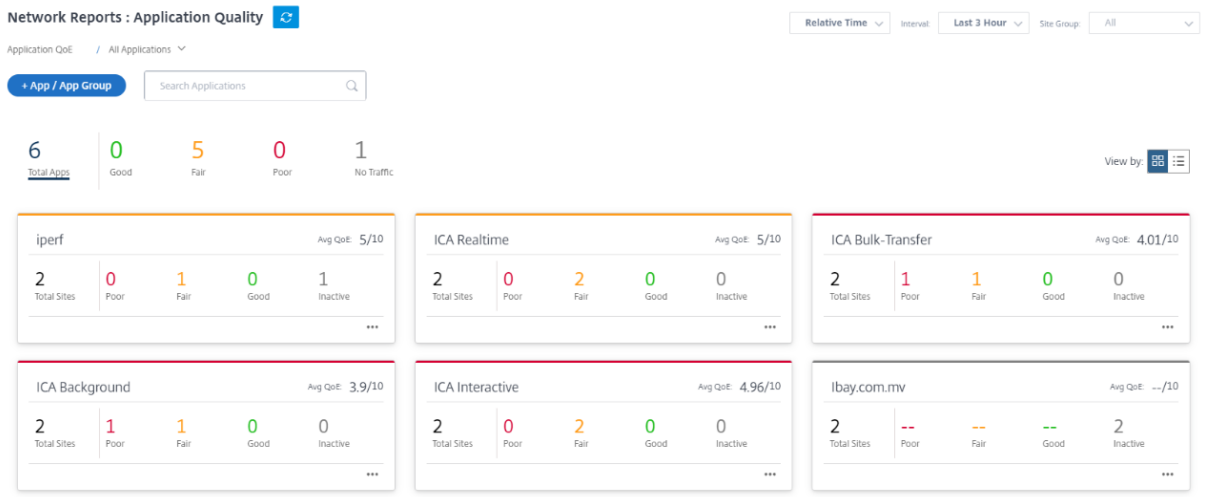
統計情報を取得する前に、ネットワーク・レベルで、ドロップダウン・リストからサイトを選択します。ファイアウォールの統計情報は、設定されたファイアウォールアクションに基づいて、特定のセッションに関連する接続の状態を示します。ファイアウォール接続では、接続の送信元と宛先に関する詳細な情報も提供されます。



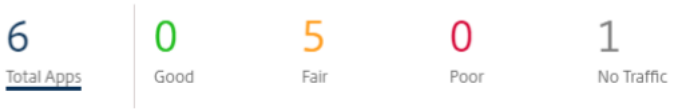
アプリケーション品質

アプリケーション QoE は、SD-WAN ネットワーク内のアプリケーションのエクスペリエンス品質の尺度です。2 つの SD-WAN アプライアンス間の仮想パスを通過するアプリケーションの品質を測定します。アプリケーション QoE スコアは 0 ～10 の値です。該当するスコア範囲によって、アプリケーションの品質が決まります。アプリケーション QoE を使用すると、ネットワーク管理者はアプリケーションのエクスペリエンスの品質を確認し、品質が許容可能なしきい値を下回ったときにプロアクティブな対策を講じることができます。

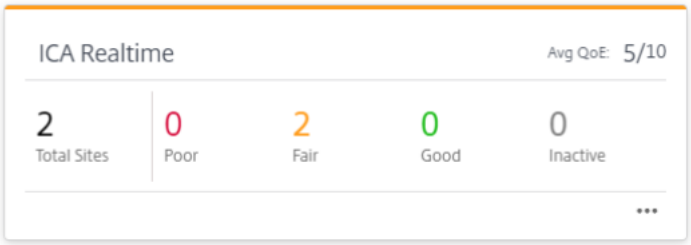
品質	範囲	カラーコーディング
高	8–10	緑
標準	4–8	オレンジ
低	0–4	赤



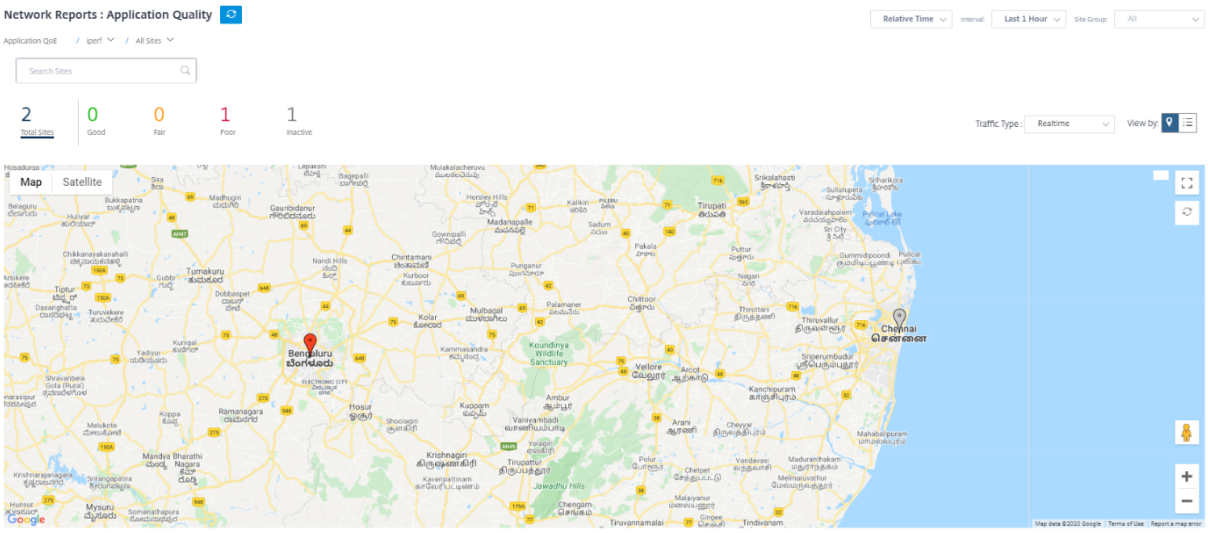
ダッシュボードの上部には、アプリケーションの総数と、ネットワーク内のアプリケーション QoE が良い、公正、または貧弱なアプリケーションの数が表示されます。また、トラフィックがないアプリケーションの数も表示されます。



個々のアプリケーションカードには、特定のアプリケーションについて不良、公正、または良好なアプリケーション QoE を持つサイトの数が表示されます。また、アプリケーションをアクティブに使用していないサイトの数も表示されます。平均 QoE は、ネットワーク内のすべてのサイトにおけるアプリケーションの平均 QoE スコアです。

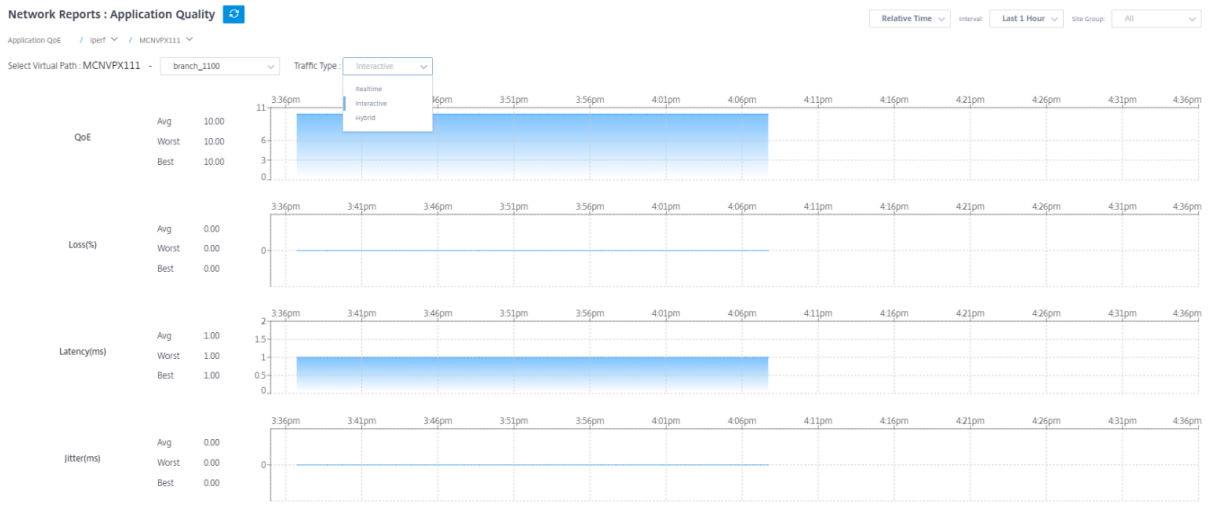


個々のアプリケーション・カードをクリックすると、選択したアプリケーションの QoE が良い、公平、または貧弱なサイトの数の詳細が表示されます。選択したアプリケーションを実行しているすべてのサイトのマップビューが表示されます。マップ内のサイトをクリックして、そのサイトのさまざまな仮想パスのアプリケーション QoE 統計をさらにドリルダウンして表示します。



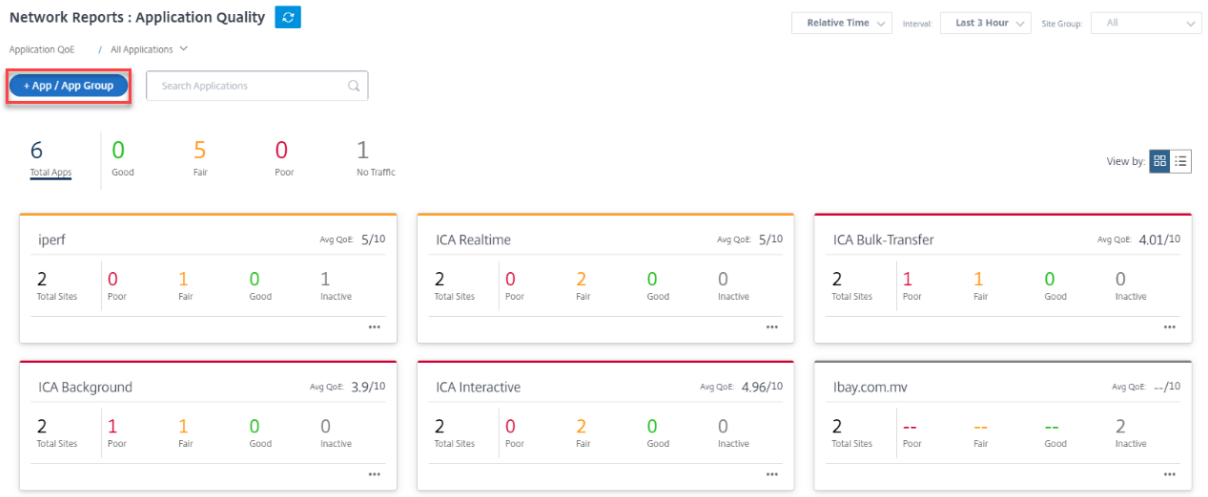
選択した期間における、リアルタイムトラフィック、インタラクティブトラフィック、ハイブリッドトラフィックについて、次のメトリックを表示できます。

- **QoE**: トラフィックの QoE スコア。
- 損失: トラフィックの損失率。
- レイテンシー: トラフィックのレイテンシー (ミリ秒単位)。
- ジッター: トラフィックで観測されたジッター（ミリ秒単位)。

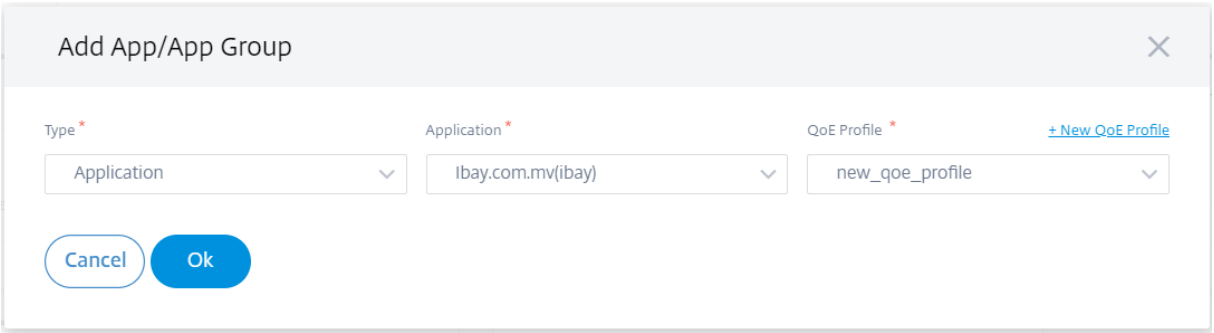


アプリケーション **QoE** プロファイル

[**+ App/App Group**] をクリックして、アプリケーション、カスタムアプリケーション、またはアプリケーショングループをデフォルトまたはカスタムの QoE プロファイルにマッピングします。



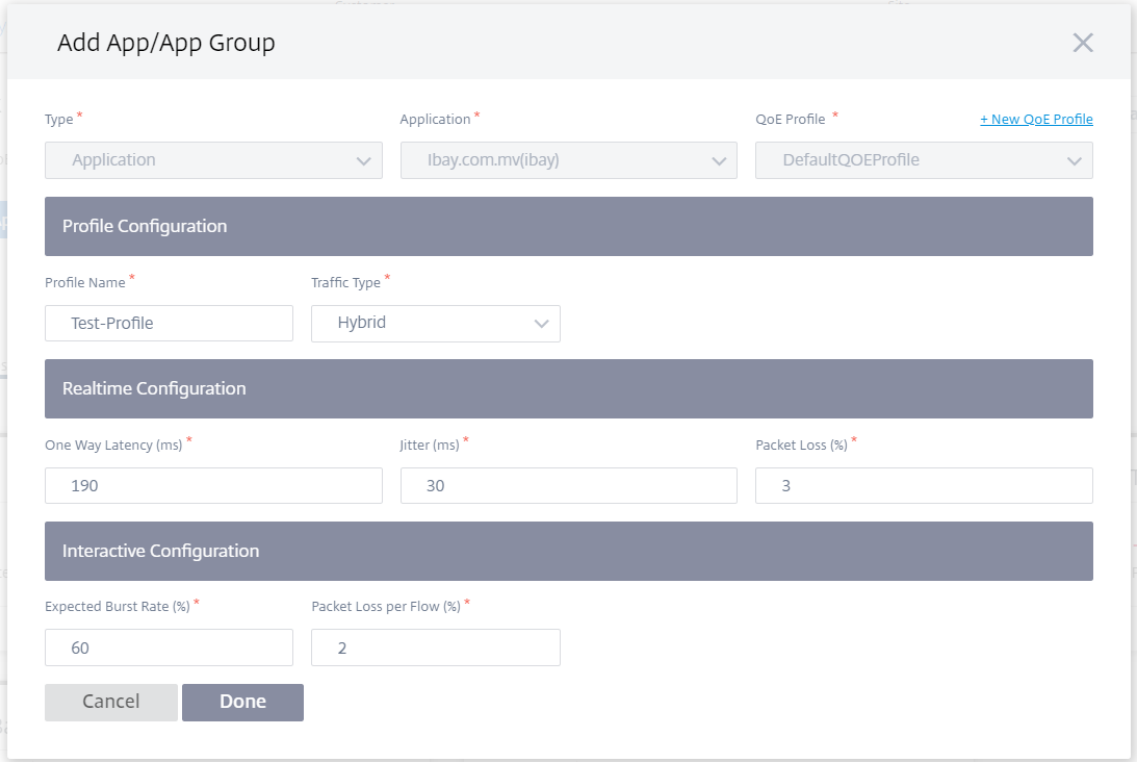
QoE プロファイルは、リアルタイム、インタラクティブ、およびハイブリッドトラフィックのしきい値を定義します。QoE プロファイルごとの QoE しきい値は、選択したアプリケーションまたはアプリケーショングループに適用されます。



[**+ New QoE Profile**] をクリックして新しいアプリケーションの QoE プロファイルを作成し、次のパラメータの値を入力します。

- **Profile Name**: リアルタイムおよびインタラクティブトラフィックのしきい値を設定するプロファイルを識別するための名前。
- トラフィックの種類: トラフィックのタイプ (リアルタイム、インタラクティブ、ハイブリッド) を選択します。トラフィックタイプが Hybrid の場合は、リアルタイムとインタラクティブ QoE プロファイルのしきい値の両方を設定できます。
- リアルタイム設定**:** リアルタイム QoS ポリシーを選択するトラフィックフローのしきい値を設定します。レイテンシ、損失、ジッタに関する次のしきい値を満たすリアルタイムアプリケーションのフローは、高品質と見なされます。
  - 一方向遅延: 遅延しきい値 (ミリ秒)。デフォルトの QoE プロファイル値は 160 ミリ秒です。
  - ジッター: ジッターしきい値（ミリ秒）。デフォルトの QoE プロファイル値は 30 ミリ秒です。
  - パケット損失: パケット損失の割合。デフォルトの QoE プロファイル値は 2% です。

- インタラクティブ設定: インタラクティブ QoS ポリシーを選択するトラフィックフローのしきい値を設定します。バースト比とパケット損失に関する次のしきい値を満たす対話型アプリケーションのフローは、高品質と見なされます。
  - 予想バーストレート値: 予想バーストレートに対するパーセンテージ。出力バーストレートは、入力バーストレートに対して設定されている割合以上でなければなりません。デフォルトの QoE プロファイル値は 60% です。
  - フローごとのパケット損失: パケット損失の割合。デフォルトの QoE プロファイル値は 1% です。



新しく追加されたアプリケーションが [アプリケーションの品質] ダッシュボードに表示されます。

また、アプリと DNS の設定からアプリケーションの QoE を定義および構成することもできます。詳細については、「アプリケーション品質プロファイル 」および「アプリケーション品質構成」を参照してください。

サイトレポート

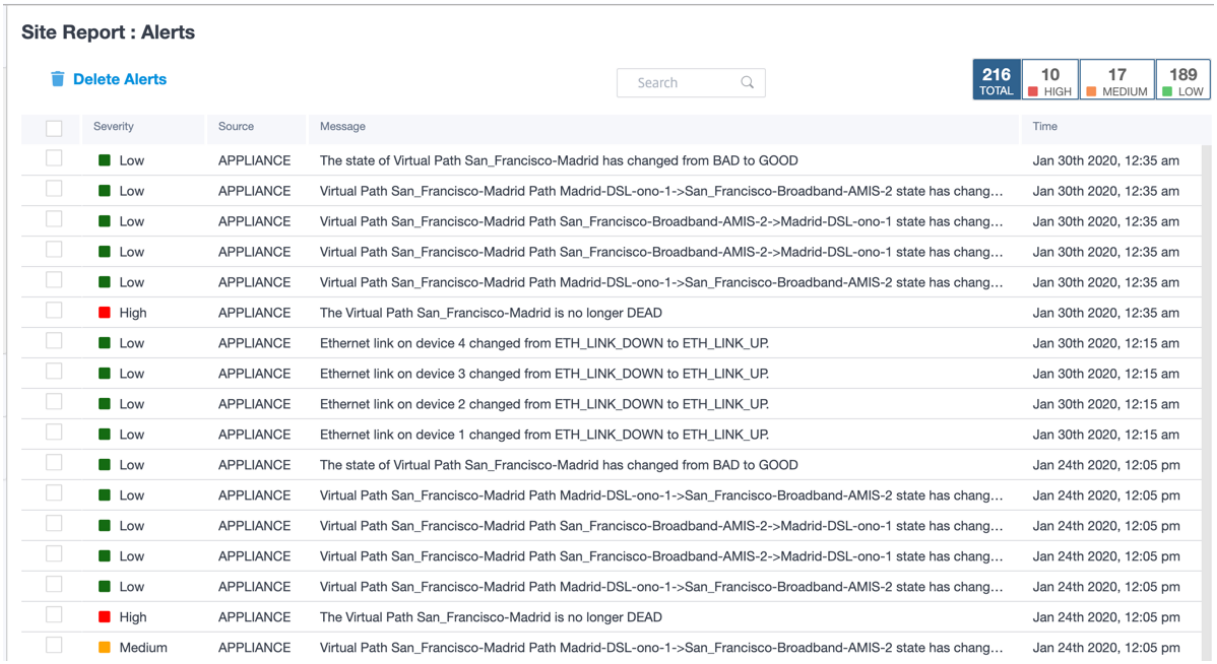
October 26, 2022

サイトレポートは、サイトレベルのアラート、使用傾向、品質、デバイス情報、およびファイアウォール統計を可視化します。

アラート

サイト管理者は、サイトレベルで生成されたすべてのイベントとアラートの詳細なレポートを確認できます。

重大度、アラートが発生したサイト、アラート・メッセージ、時刻、その他の詳細情報が含まれます。



Severity	Source	Message	Time
Low	APPLIANCE	The state of Virtual Path San_Francisco-Madrid has changed from BAD to GOOD	Jan 30th 2020, 12:35 am
Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang…	Jan 30th 2020, 12:35 am
Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DSL-ono-1 state has chang…	Jan 30th 2020, 12:35 am
Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DSL-ono-1 state has chang…	Jan 30th 2020, 12:35 am
Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang…	Jan 30th 2020, 12:35 am
High	APPLIANCE	The Virtual Path San_Francisco-Madrid is no longer DEAD	Jan 30th 2020, 12:35 am
Low	APPLIANCE	Ethernet link on device 4 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am
Low	APPLIANCE	Ethernet link on device 3 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am
Low	APPLIANCE	Ethernet link on device 2 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am
Low	APPLIANCE	Ethernet link on device 1 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am
Low	APPLIANCE	The state of Virtual Path San_Francisco-Madrid has changed from BAD to GOOD	Jan 24th 2020, 12:05 pm
Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang…	Jan 24th 2020, 12:05 pm
Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DSL-ono-1 state has chang…	Jan 24th 2020, 12:05 pm
Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DSL-ono-1 state has chang…	Jan 24th 2020, 12:05 pm
Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang…	Jan 24th 2020, 12:05 pm
High	APPLIANCE	The Virtual Path San_Francisco-Madrid is no longer DEAD	Jan 24th 2020, 12:05 pm
Medium	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang…	Jan 24th 2020, 12:05 pm

必要に応じて、適切なフィルタリングオプションを使用できます。たとえば、サイトで重大度の高いアラートをすべて検索するか、特定の期間に発生したアラートを探します。

アラートを選択およびクリアすることもできます。

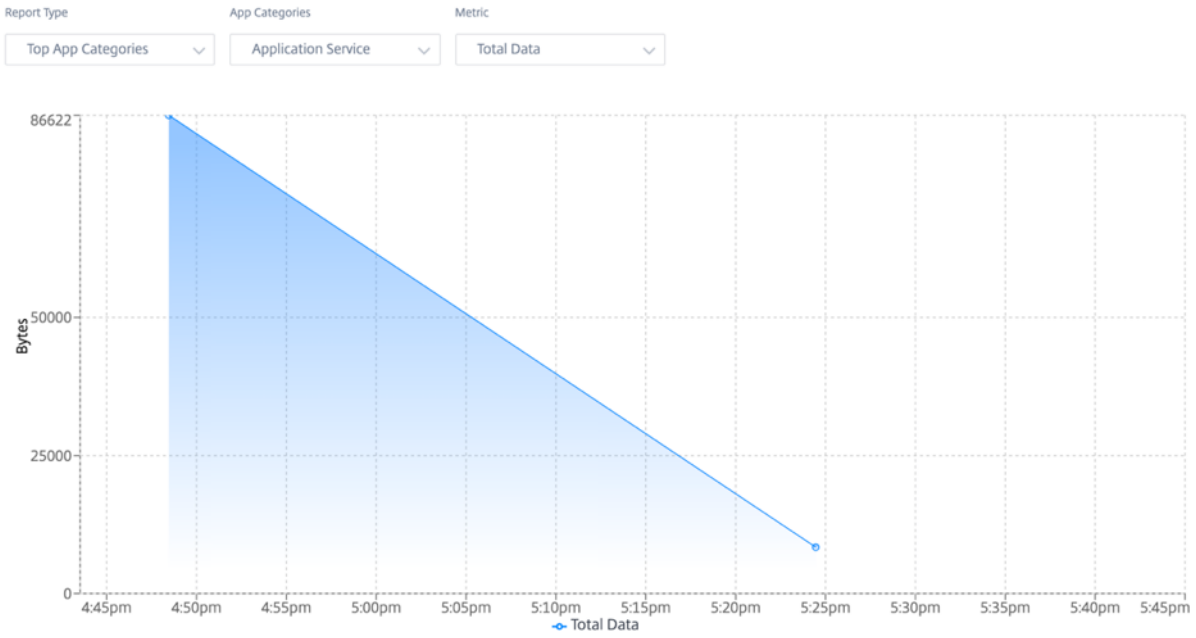
使用状況

サイト管理者は、特定のサイトにおける上位アプリケーション、上位アプリケーションカテゴリ、アプリ帯域幅などの使用傾向を確認できます。

上位アプリケーションとアプリケーションカテゴリ

**** 上位アプリケーションと上位アプリケーションカテゴリのグラフには ** 、サイトで広く使用されている上位アプリケーションと上位アプリケーションファミリが表示されます。これにより、データ消費パターンを分析し、サイト内のデータクラスごとに帯域幅制限を再割り当てできます。

また、帯域幅使用状況の統計も表示できます。選択した時間間隔について、帯域幅統計情報が収集されます。統計レポートは、レポートタイプ、アプリまたはアプリカテゴリ、および指標に基づいてフィルタリングできます。

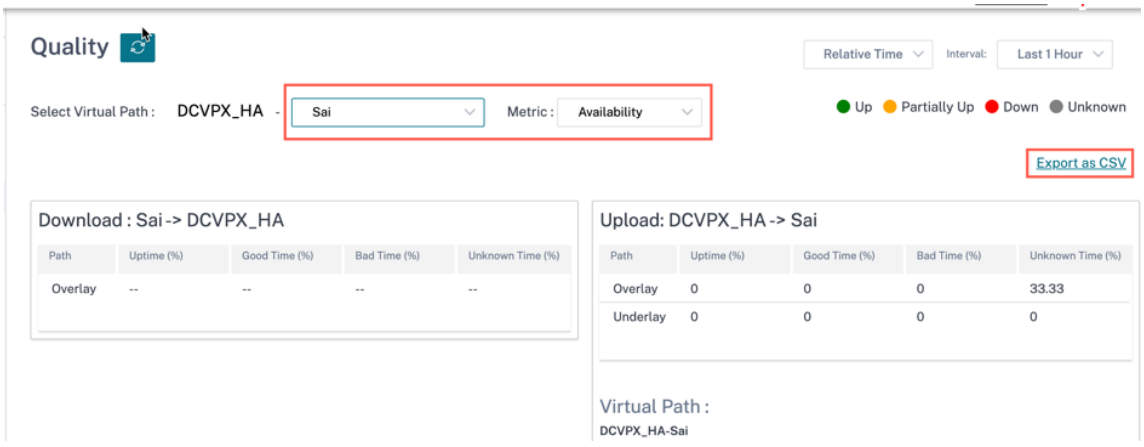


- レポートタイプ**:** リストから [上位のアプリ**]** または **[**アプリカテゴリ] を選択します。
- アプリ**/**アプリカテゴリ**:** 一覧から上位のアプリケーションまたはカテゴリ (ネットワークサービスなど) を選択します。
- メトリック**:** リストから帯域幅メトリック (合計データ、受信データ、合計帯域幅など) を選択します。

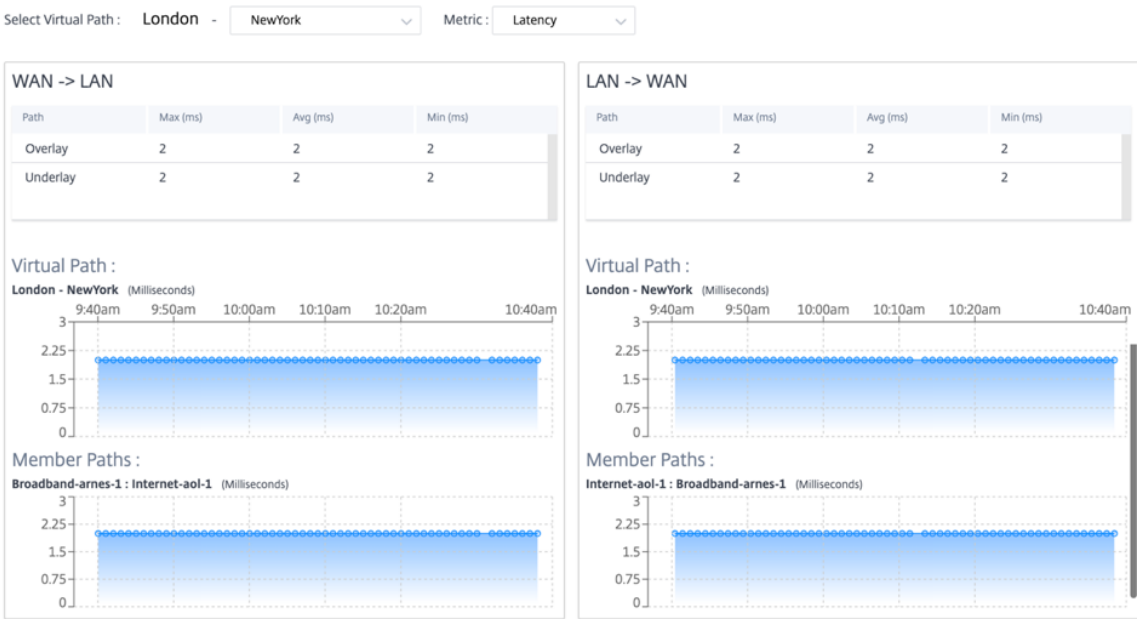
品質

サイト管理者は、品質レポートを使用して、可用性、損失、遅延、ジッタなどの各 QoS メトリックについて、サイトの Quality of Experience（QoE）を分析できます。品質メトリックは、オーバーレイ仮想パスとその基になるメンバーパスの両方に対して表示されます。

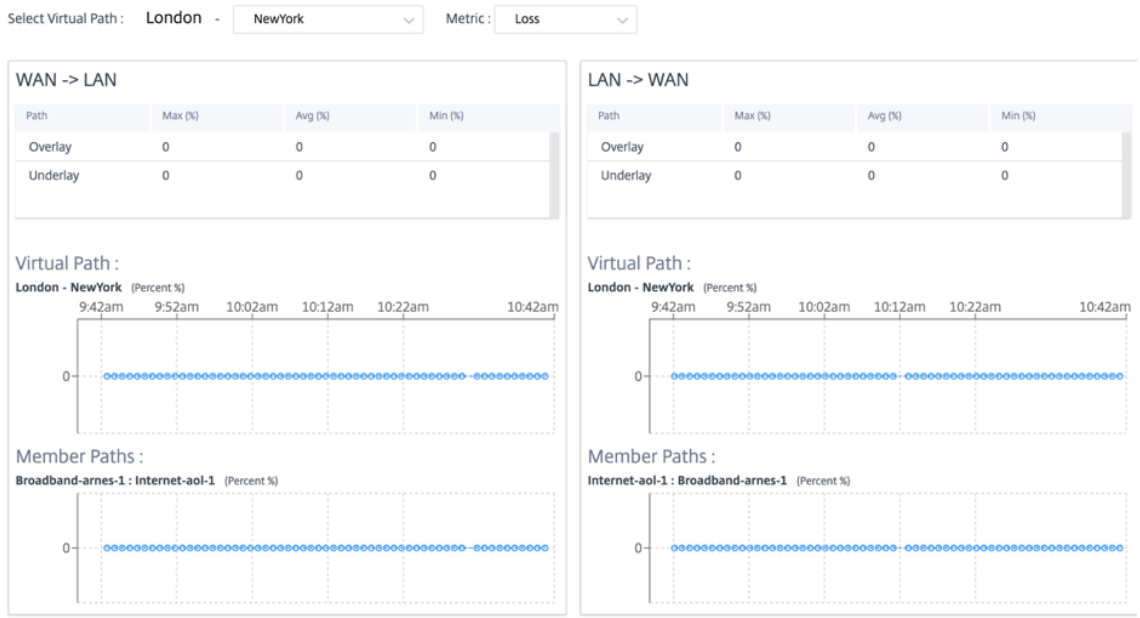
- 可用性



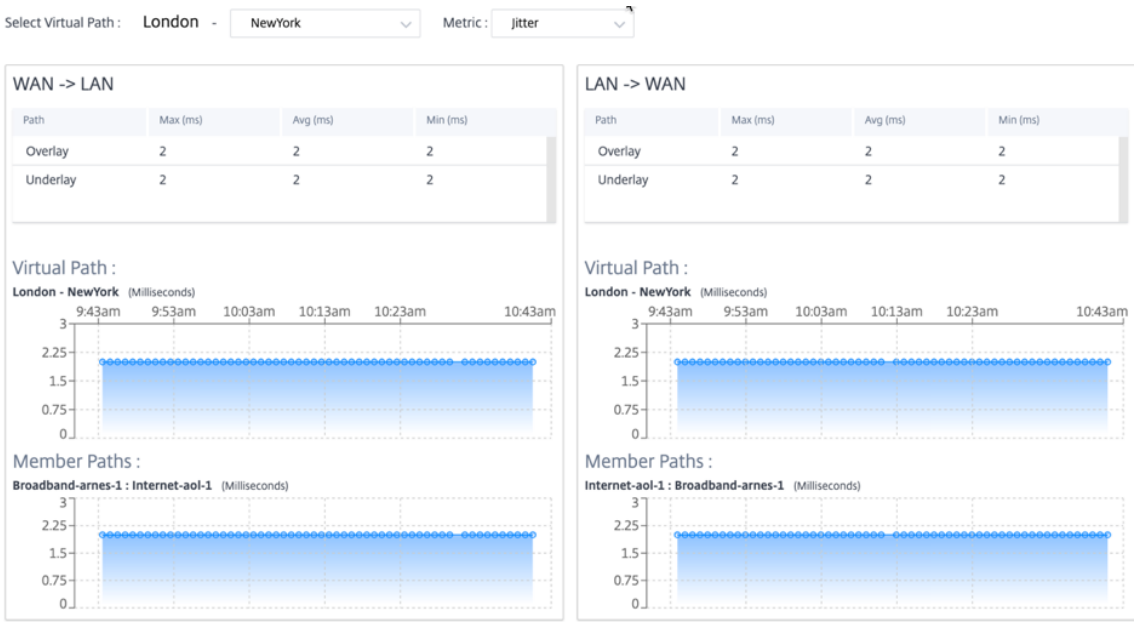
- 遅延



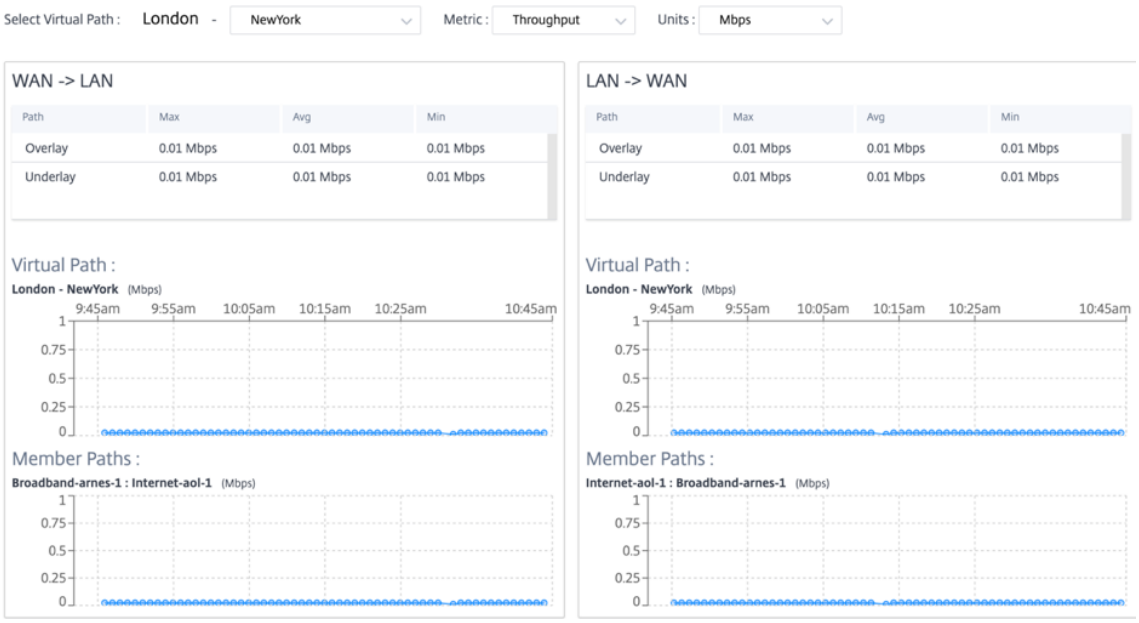
- 損失



- ジッター



- スループット

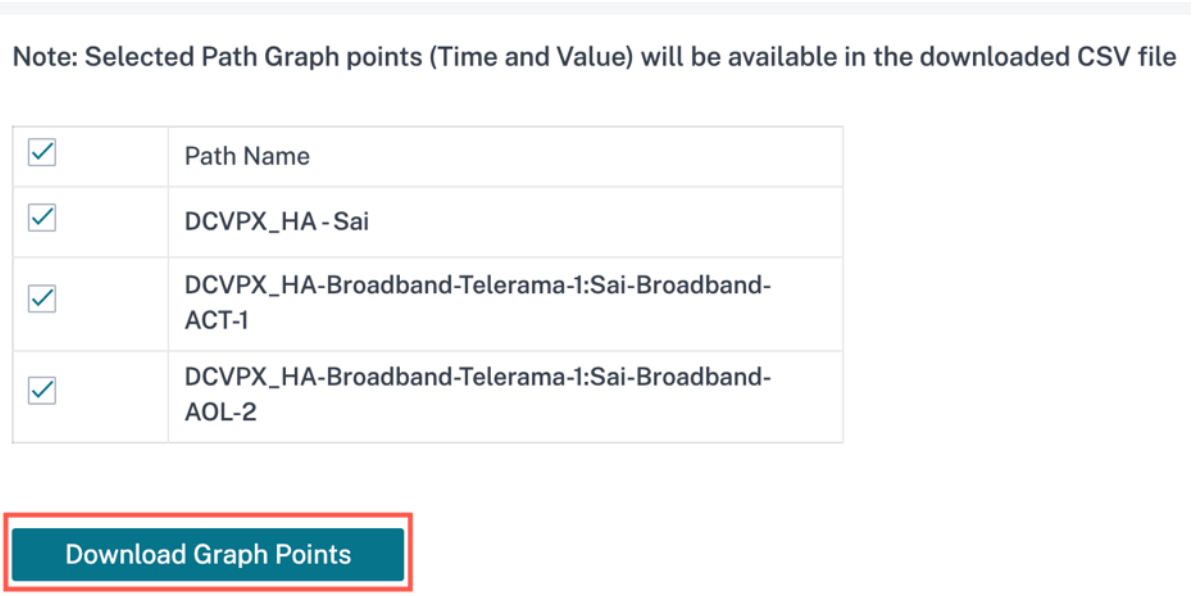


CSV としてエクスポート

CSV 形式でエクスポート機能を使用すると、任意の時系列 (時間単位、週単位など) のパスグラフポイント (仮想パス/メンバーパス) を Excel カンマ区切り値 (CSV) ファイルとしてダウンロードし、特定のサイトレポートのすべての異なるデータポイントをプロットできます。

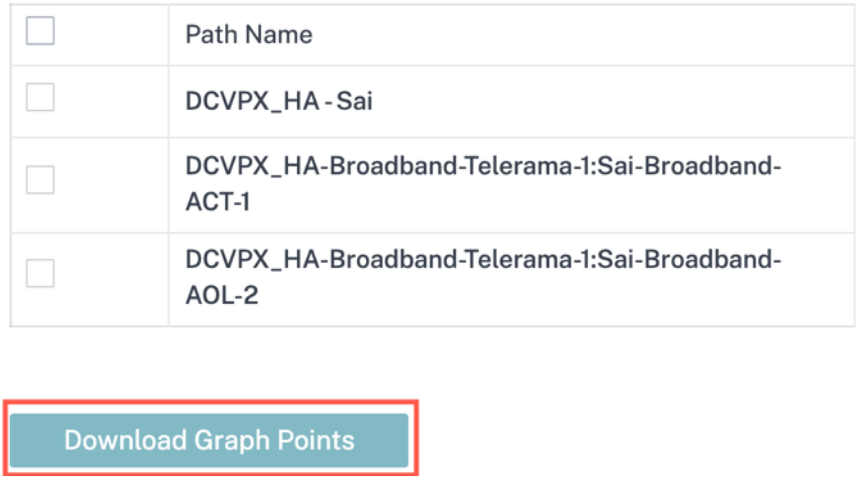
パスグラフを CSV 形式でダウンロード/エクスポートするには、サイトレベルで [レポート] > [品質] に移動します。ドロップダウンリストからサイトとメトリックを選択し、「**CSV** としてエクスポート」リンクをクリックします。

データを取得したいパスを選択し、「グラフポイントをダウンロード」をクリックします。

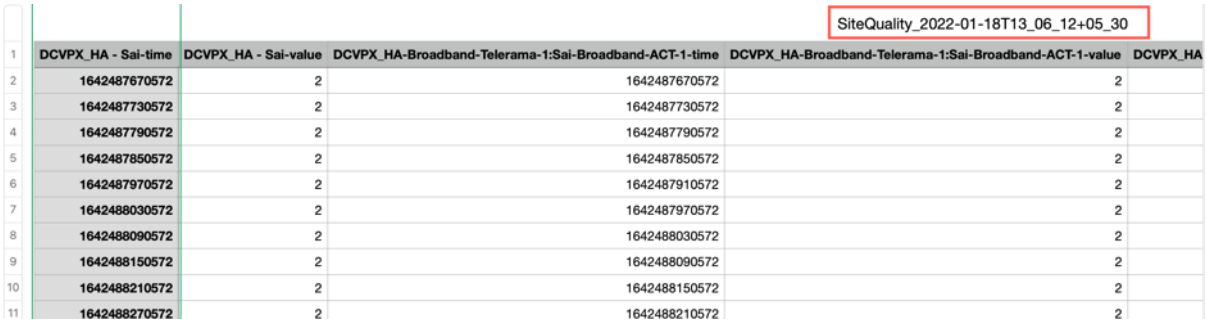


デフォルトでは、すべてのパスチェックボックスが自動的に選択されます。必要に応じて変更できます。

> 注:
>
> どのパスも選択されていない場合、[グラフポイントのダウンロード] ボタンは無効のままになります。



ダウンロードされた CSV ファイルの命名規則は、**SiteQuality** の後にダウンロードのタイムスタンプが続くというものです。時間と値のペアと一意の識別子で各パスを表示できます。時間はミリ秒単位で表示され、値は単位として表示されます。



			SiteQuality_2022-01-18T13_06_12+05_30		
1	DCVPX_HA - Sai-time	DCVPX_HA - Sai-value	DCVPX_HA-Broadband-Telerama-1:Sai-Broadband-ACT-1-time	DCVPX_HA-Broadband-Telerama-1:Sai-Broadband-ACT-1-value	DCVPX_HA
2	1642487670572	2	1642487670572	2	
3	1642487730572	2	1642487730572	2	
4	1642487790572	2	1642487790572	2	
5	1642487850572	2	1642487850572	2	
6	1642487970572	2	1642487910572	2	
7	1642488030572	2	1642487970572	2	
8	1642488090572	2	1642488030572	2	
9	1642488150572	2	1642488090572	2	
10	1642488210572	2	1642488150572	2	
11	1642488270572	2	1642488210572	2	

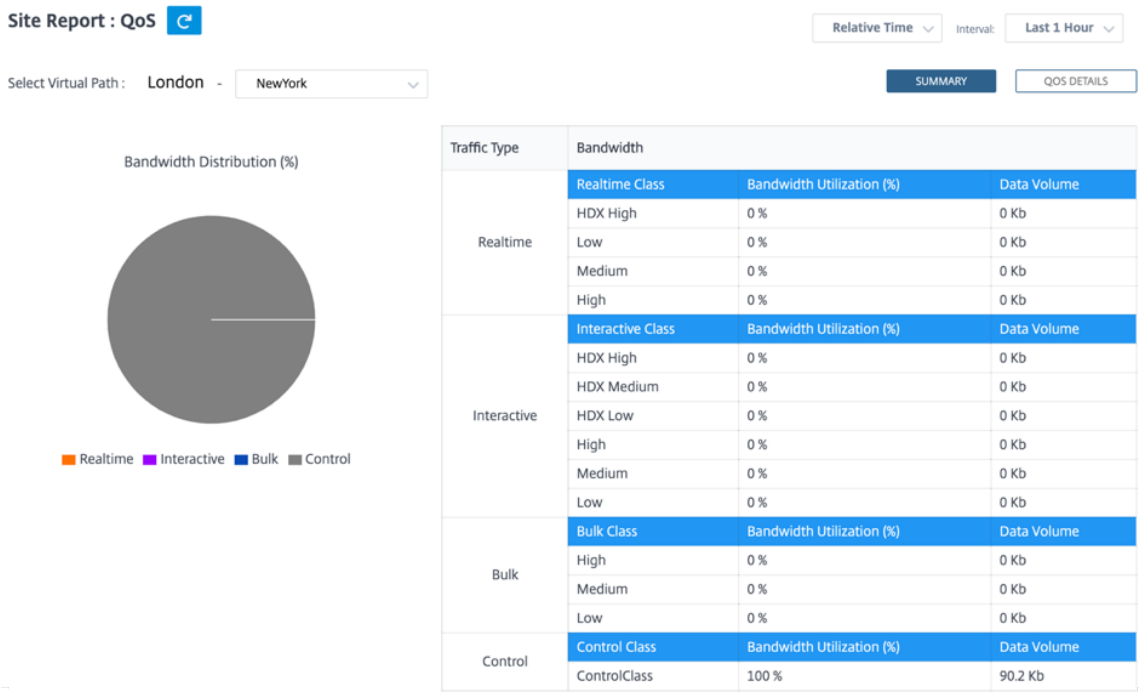
次の指標の選択に基づいて、CSV ファイルに異なる値が生成されていることがわかります。

- 損失**:** 値は%で表示されます。
- レイテンシーとジッター**:** 値はミリ秒単位で表示されます。
- スループット**:** 値は Kbps 単位で表示されます。
- アベイラビリティ**:** アップパス、一部アップパス、ダウン時間、および不明な時間が表示されます。
  - 値が 4 の場合、パスは Up 状態です。
  - 値が 3 の場合、パスは部分的にアップ状態になります。
  - 値が 3 未満の場合、パスは不良/停止状態です。

サービス品質

Quality of Service（QoS; サービス品質）は、データトラフィックを管理し、ネットワーク上のパケット損失、遅延、ジッタを削減します。詳細については、「サービス品質」を参照してください。QoS（サービス品質）レポートを表示するには、次の 2 つの方法があります。

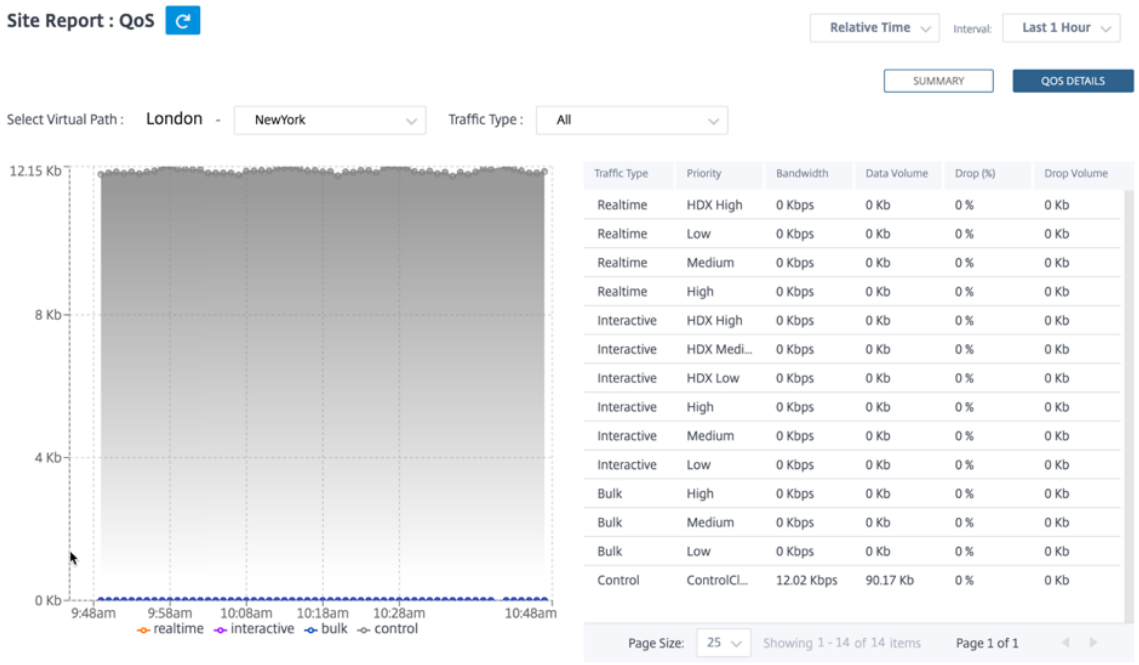
- 概要ビュー**:** 概要ビューには、あらゆる種類のトラフィック（リアルタイム、インタラクティブ、バルク、ネットワーク全体およびサイトごとの制御）の帯域幅消費量の概要が表示されます。



Traffic Type	Bandwidth		
Realtime	Realtime Class	Bandwidth Utilization (%)	Data Volume
	HDX High	0 %	0 Kb
	Low	0 %	0 Kb
	Medium	0 %	0 Kb
	High	0 %	0 Kb
Interactive	Interactive Class	Bandwidth Utilization (%)	Data Volume
	HDX High	0 %	0 Kb
	HDX Medium	0 %	0 Kb
	HDX Low	0 %	0 Kb
	High	0 %	0 Kb
	Medium	0 %	0 Kb
	Low	0 %	0 Kb
Bulk	Bulk Class	Bandwidth Utilization (%)	Data Volume
	High	0 %	0 Kb
	Medium	0 %	0 Kb
	Low	0 %	0 Kb
Control	Control Class	Bandwidth Utilization (%)	Data Volume
	ControlClass	100 %	90.2 Kb

  - リアルタイム**:** 低遅延、低帯域幅、時間に敏感なトラフィックに使用されます。リアルタイムアプリケーションは時間に敏感ですが、実際には高い帯域幅（Voice over IP など）は必要ありません。リアルタイムアプリケーションは、レイテンシーとジッタの影響を受けますが、ある程度の損失を許容できます。
  - インタラクティブ**:** 低から中程度の遅延要件と低から中程度の帯域幅要件を持つインタラクティブトラフィックに使用されます。インタラクティブなアプリケーションは、マウスクリックまたはカーソル移動の形で人間の入力を伴います。通常、対話はクライアントとサーバーの間で行われます。通信は、高帯域幅を必要としない場合がありますが、損失や遅延に敏感です。ただし、サーバからクライアントへのグラフィック情報の転送には高い帯域幅が必要であり、損失の影響を受けない可能性があります。
  - バルク**:** 高遅延を許容できる高帯域幅のトラフィックに使用されます。ファイル転送を処理し、高帯域幅を必要とするアプリケーションは、バルククラスに分類されます。これらのアプリケーションは、人間の干渉をほとんど伴わず、ほとんどシステム自体によって処理されます。
  - コントロール**:** ルーティング、スケジューリング、およびリンク統計情報を含むコントロールパケットの転送に使用されます。

- 詳細ビュー**:** 詳細ビューには、オーバーレイ仮想パスに関連付けられている各 QoS クラスについて、帯域幅消費量、トラフィック量、ドロップされたパケットなどの傾向がキャプチャされます。2 つのサイト間の仮想パスに基づいて QoS 統計を表示できます。



履歴統計

サイトごとに、次のネットワークパラメータの統計をグラフとして表示できます。

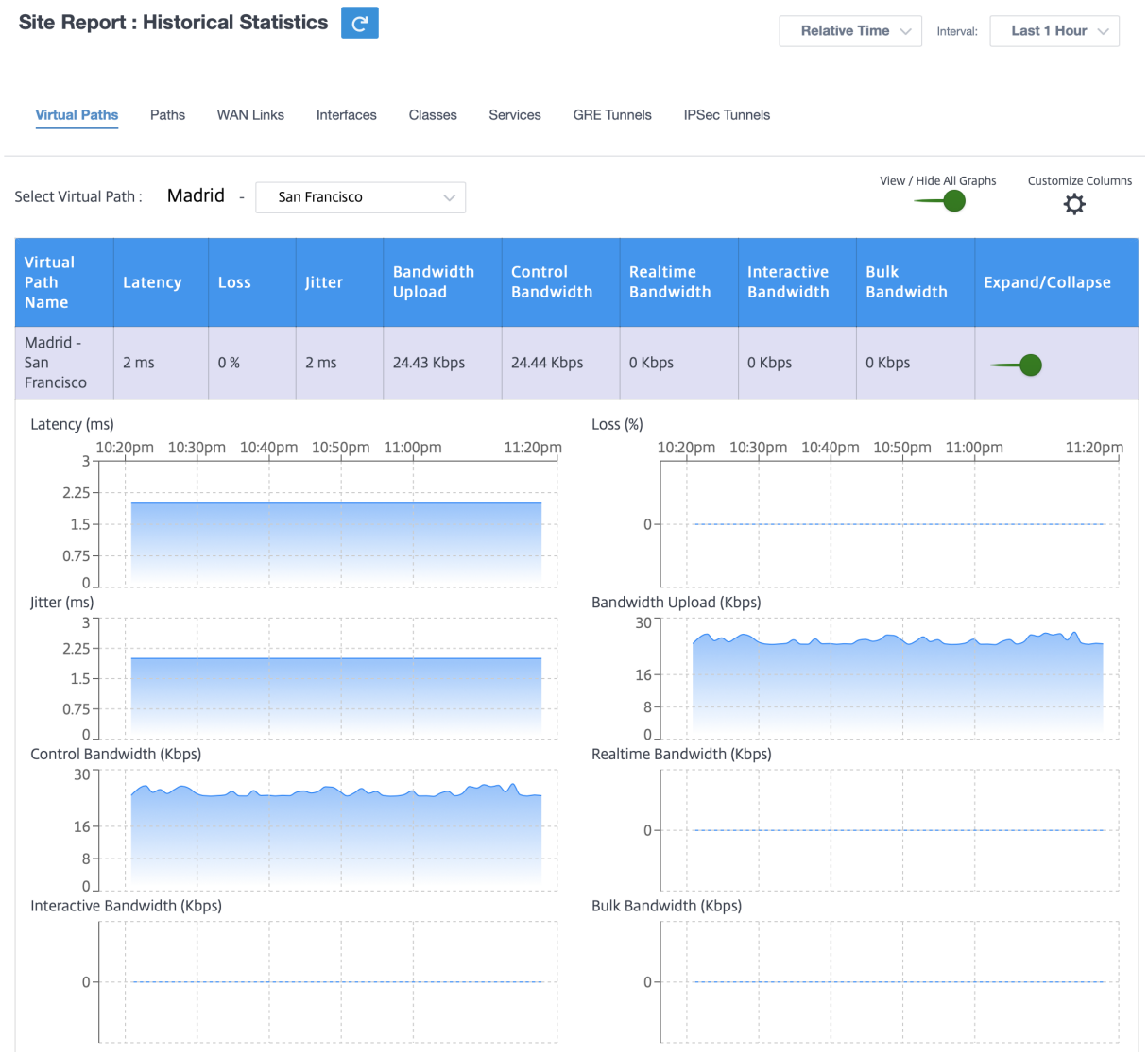
- 仮想パス
- パス
- WAN リンク
- インターフェイス
- クラス
- Services
- GRE トンネル
- IPsec トンネル

統計はグラフとして収集されます。これらのグラフはタイムライン対使用量としてプロットされるため、さまざまなネットワークオブジェクトプロパティの使用傾向を把握できます。ネットワーク全体のアプリケーション統計のグラフを表示できます。

必要に応じて、グラフの表示と非表示を切り替えたり、列をカスタマイズしたりできます。

仮想パス

仮想パスの統計情報を表示するには、[レポート] **>** [統計] **>** [仮想パス] タブに移動します。



次のメトリックを表示できます。

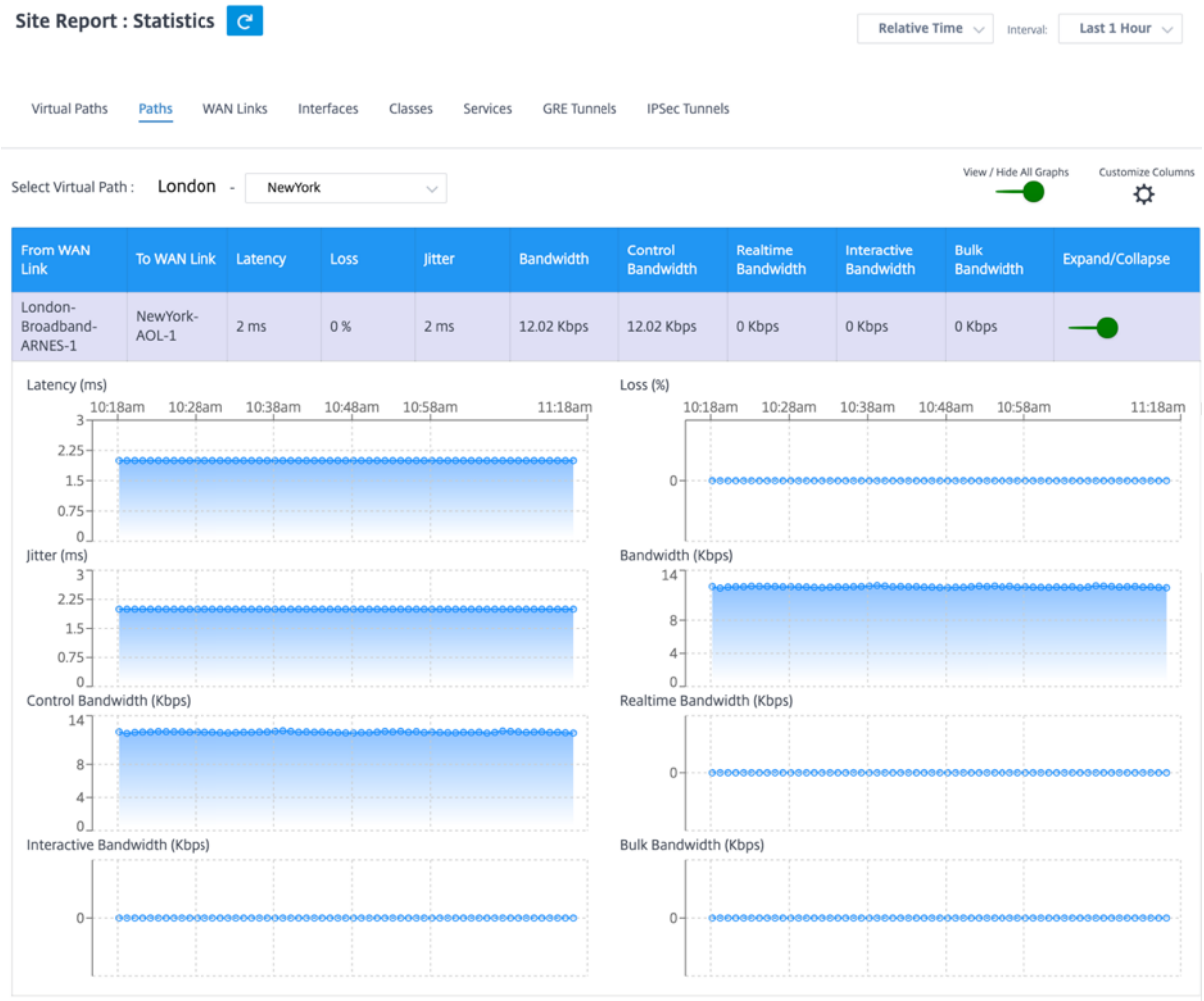
- 仮想パス名: 仮想パス名。
- レイテンシー: リアルタイムトラフィックのレイテンシー (ミリ秒単位)。
- 損失: 失われたパケットの割合。
- ジッター: 受信パケットの遅延の変動（ミリ秒単位）。
- 帯域幅入力**:** 入力側 **(LAN > WAN)** 選択した期間の帯域幅使用量。
- 制御帯域幅: ルーティング、スケジューリング、およびリンク統計情報を含む制御パケットの転送に使用される帯域幅。
- リアルタイム帯域幅:SD-WAN 構成のリアルタイムクラスタイプに属するアプリケーションによって消費される帯域幅。このようなアプリケーションのパフォーマンスは、ネットワーク遅延に大きく依存します。遅延したパケットは、失われたパケットよりも劣ります（たとえば、VoIP、Skype for Business）。
- インタラクティブ帯域幅:SD-WAN 構成のインタラクティブクラスタイプに属するアプリケーションによって

消費される帯域幅。このようなアプリケーションのパフォーマンスは、ネットワーク遅延とパケット損失に大きく依存します（たとえば、XenDesktop、XenApp）。

- バルク帯域幅:SD-WAN 構成のバルククラスタイプに属するアプリケーションによって消費される帯域幅。これらのアプリケーションは、人的介入がほとんどなく、ほとんどがシステム自体（FTP、バックアップ操作など）によって処理されます。
- 展開/折りたたみ: 必要に応じてデータを展開または縮小できます。

パス

パス統計を表示するには、[レポート] **>** [統計] **>** [パス] タブに移動します。



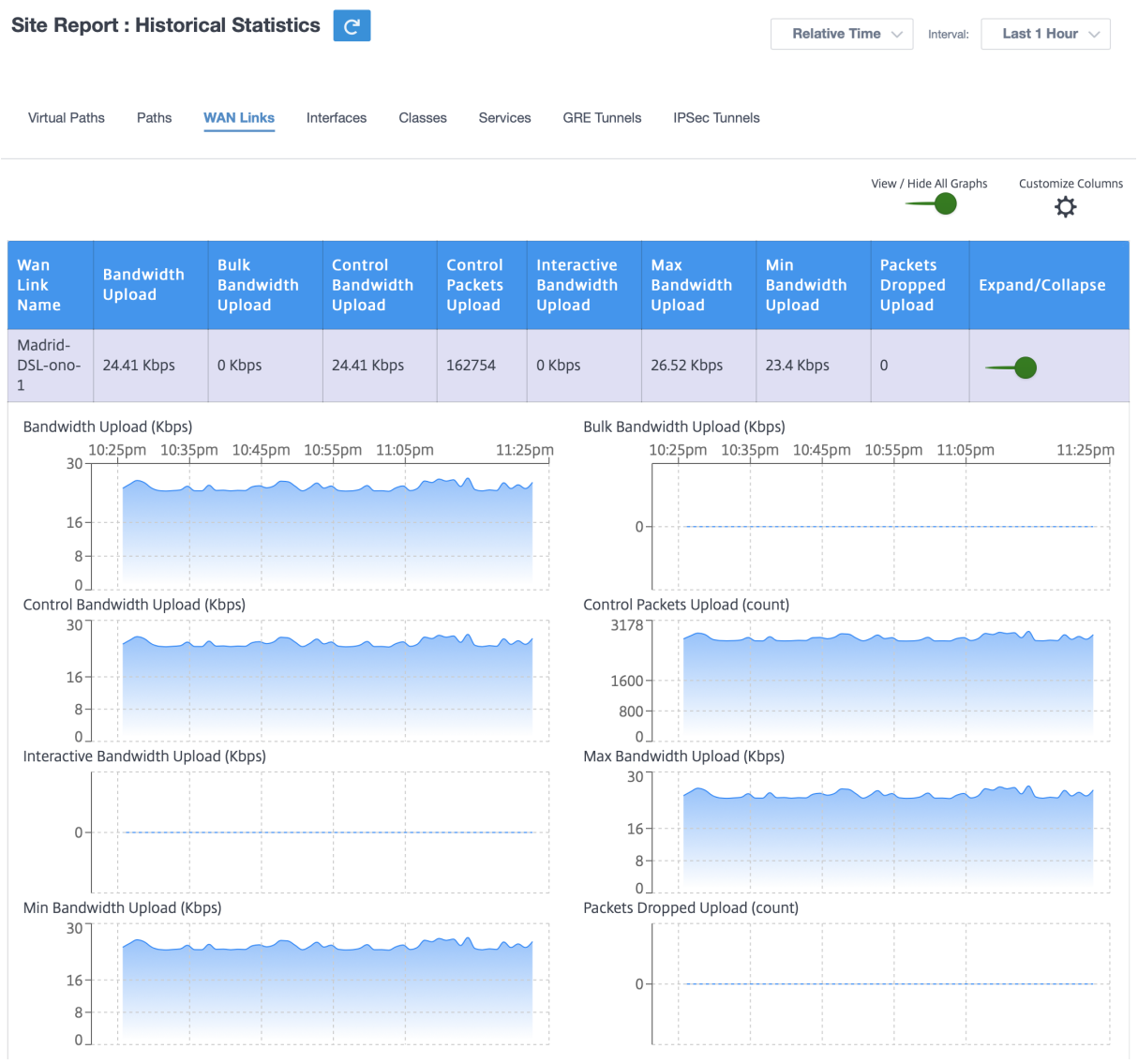
次のメトリックを表示できます。

- **WAN** リンクから: ソース WAN リンク。
- **WAN** リンクへ: 宛先 WAN リンク。
- レイテンシー: リアルタイムトラフィックのレイテンシー (ミリ秒単位)。
- 損失: 失われたパケットの割合。

- ジッター: 受信パケットの遅延の変動（ミリ秒単位）。
- 帯域幅: すべてのパケットタイプで消費される合計帯域幅。帯域幅 = 制御帯域幅 + リアルタイム帯域幅 + インタラクティブ帯域幅 + バルク帯域幅
- 制御帯域幅: ルーティング、スケジューリング、およびリンク統計情報を含む制御パケットの転送に使用される帯域幅。
- リアルタイム帯域幅:SD-WAN 構成のリアルタイムクラスタイプに属するアプリケーションによって消費される帯域幅。このようなアプリケーションのパフォーマンスは、ネットワーク遅延に大きく依存します。遅延したパケットは、失われたパケットよりも劣ります（たとえば、VoIP、Skype for Business）。
- インタラクティブ帯域幅:SD-WAN 構成のインタラクティブクラスタイプに属するアプリケーションによって消費される帯域幅。このようなアプリケーションのパフォーマンスは、ネットワーク遅延とパケット損失に大きく依存します（たとえば、XenDesktop、XenApp）。
- バルク帯域幅:SD-WAN 構成のバルククラスタイプに属するアプリケーションによって消費される帯域幅。これらのアプリケーションは、人的介入がほとんどなく、ほとんどがシステム自体（FTP、バックアップ操作など）によって処理されます。
- 展開/折りたたみ: 必要に応じてデータを展開または縮小できます。

WAN リンク

WAN リンクレベルで統計情報を表示するには、[レポート] **>** [統計] **>** [**WAN** リンク] タブに移動します。



次のメトリックを表示できます。

- **WAN** リンク名: パス名。
- 帯域幅入力**:** 入力側 **(LAN > WAN)** 選択した期間の帯域幅使用量。
- バルク帯域幅イングレス: 選択した期間にバルクトラフィックが使用するイングレス **(LAN > WAN)** の仮想パス帯域幅。
- コントロール帯域幅イングレス: 選択した期間にコントロールトラフィックが使用したイングレス **(LAN > WAN)** 仮想パス帯域幅。
- コントロール・パケット・イングレス: 選択した期間のイングレス（**LAN > WAN**）仮想パス制御パケット。
- インタラクティブ帯域幅イングレス: 選択した期間に対話型トラフィックが使用したイングレス **(LAN > WAN)** の仮想パス帯域幅。
- 最大入力帯域幅**:** 選択した期間の **1** 分間の最大入力 **(LAN > WAN)** 帯域幅。
- 最小入力帯域幅**:** 選択した期間の **1** 分間の最小入力 **(LAN > WAN)** 帯域幅。

- 展開/折りたたみ: 必要に応じてデータを展開または縮小できます。

インターフェイス

インターフェイス統計レポートは、トラブルシューティング中にダウンしているポートがないかをすばやく確認するのに役立ちます。また、各ポートの送受信帯域幅、またはパケットの詳細を表示することもできます。また、特定の期間にこれらのインターフェイスで発生したエラーの数を表示することもできます。

インターフェイス統計を表示するには、[レポート] **>** [統計] **>** [インターフェイス] タブに移動します。

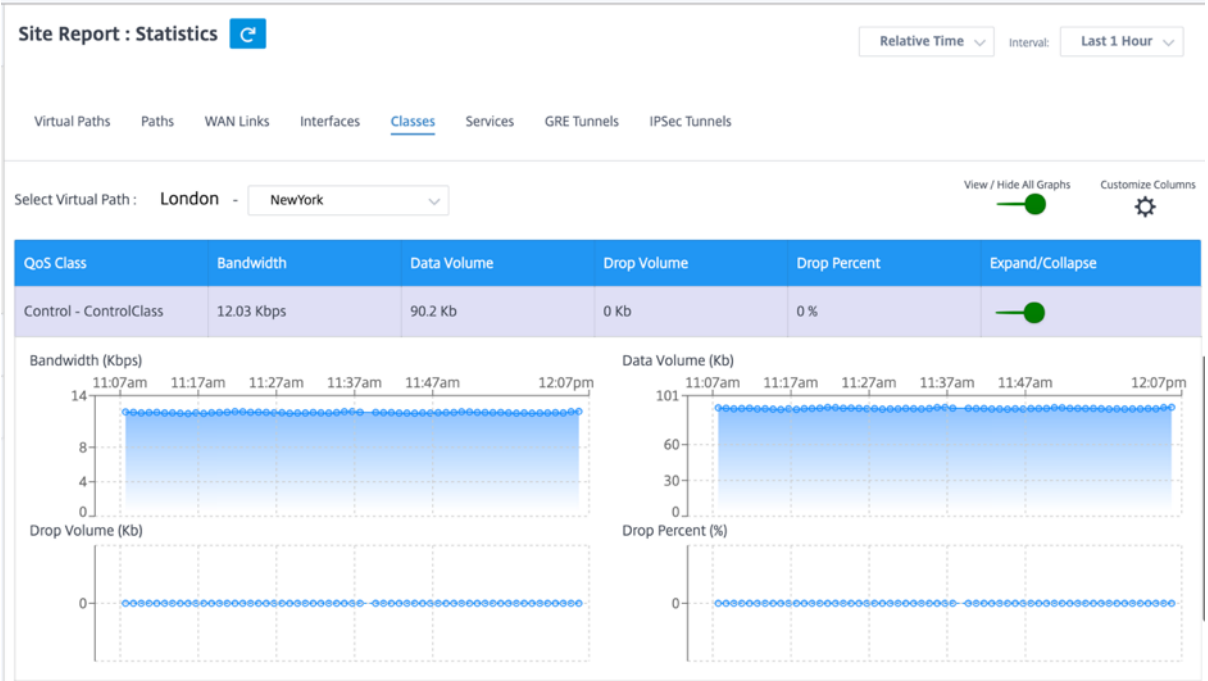
次のメトリックを表示できます。

- インターフェース名: イーサネットインターフェースの名前。
- **Tx** 帯域幅: 送信された帯域幅。
- 受信帯域幅: 受信した帯域幅。
- エラー: 選択した期間中に発生したエラーの数。
- 展開/折りたたみ: 必要に応じてデータを展開または縮小できます。

クラス

仮想サービスは特定の QoS クラスに割り当てることができ、クラスごとに異なる帯域幅制限を適用できます。

クラス統計を表示するには、[レポート] **>** [統計] **>** [クラス] タブに移動します。



次のメトリックを表示できます。

- **QoS** クラス: クラス名。

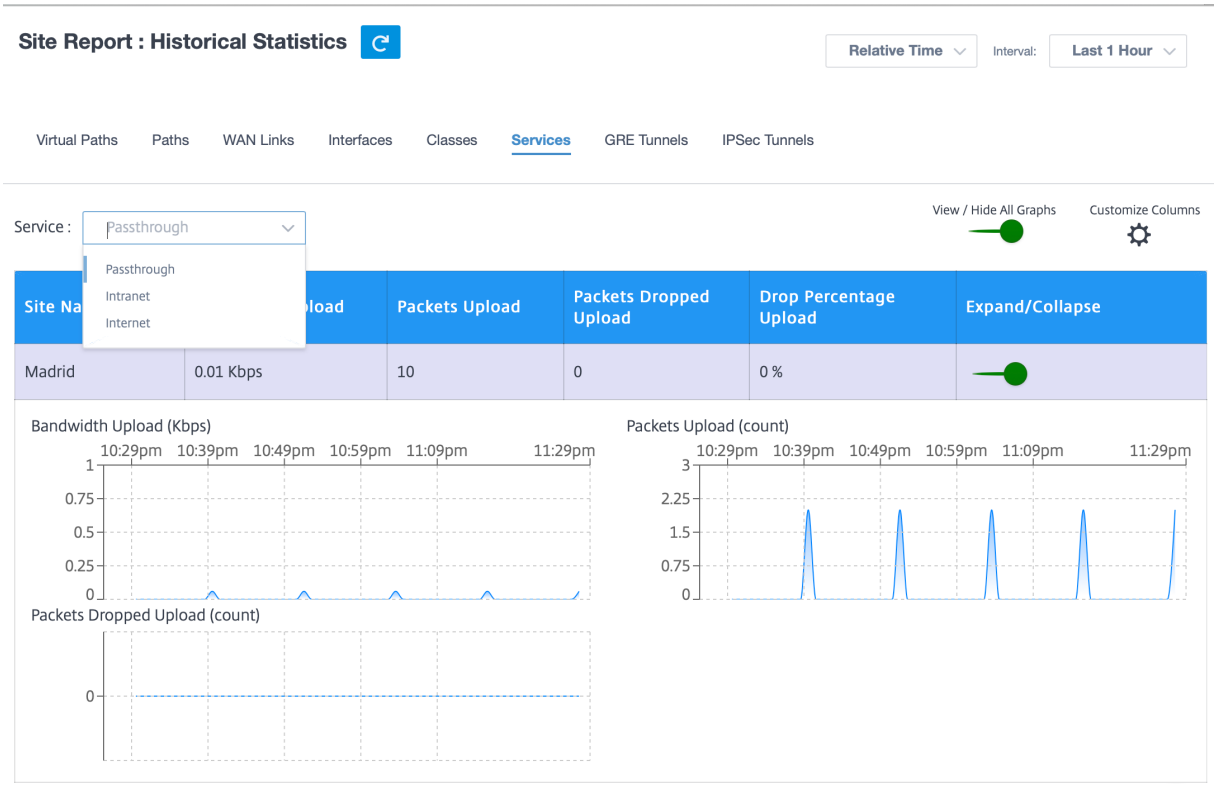
- 帯域幅: 送信帯域幅。
- データ量: 送信されたデータ（Kbps 単位）。
- ドロップボリューム: ドロップされたデータの割合。
- ドロップ率: ドロップされたデータの割合。
- 展開/折りたたみ: 必要に応じてデータを展開または縮小できます。

Services

サービス統計を表示するには、[レポート] **>** [統計] **>** [サービス] タブに移動します。

リストからサービスタイプを選択します。使用できるオプションは、次のとおりです。

- パススルー—このサービスは、SD-WAN によって傍受、遅延、シェーピング、または変更されないトラフィックを管理します。パススルーサービスに送信されるトラフィックには、ブロードキャスト、ARP、その他の非 IPv4 トラフィック、および Virtual WAN アプライアンスのローカルサブネット、構成済みサブネット、またはネットワーク管理者が適用したルール上のトラフィックが含まれます。このトラフィックは、SD-WAN によって遅延、シェーピング、または変更されません。したがって、SD-WAN アプライアンスが他のサービスで使用するように構成されている WAN リンク上で、パススルートラフィックが実質的なリソースを消費しないようにする必要があります。
- イントラネット -このサービスは、仮想パスを介した伝送用に定義されていないエンタープライズイントラネットトラフィックを管理します。インターネットトラフィックと同様に、カプセル化されていないままであり、SD-WAN は、輻輳時にこのトラフィックを他のサービスタイプと比較してレート制限することで、帯域幅を管理します。特定の条件下では、仮想パス上のイントラネットフォールバック用に構成されている場合、通常は仮想パスとともに移動するトラフィックは、代わりにイントラネットトラフィックとして扱われ、ネットワークの信頼性を維持できます。
- インターネット—このサービスは、エンタープライズサイトとパブリックインターネット上のサイト間のトラフィックを管理します。このタイプのトラフィックはカプセル化されません。輻輳時には、SD-WAN は、仮想パスに対するレート制限によるインターネットトラフィックと、管理者が確立した SD-WAN 構成に従ってイントラネットトラフィックによって、帯域幅を積極的に管理します。



次のメトリックを表示できます。

- サイト名: サイト名。
- 帯域幅入力**:** 入力側 **(LAN > WAN)** 選択した期間の帯域幅使用量。
- パケット入力: **(LAN > WAN)** 選択した時間間隔で送信されたパケット。
- 展開**/**折りたたみ: 必要に応じてデータを展開または縮小できます。

GRE トンネル

トンネリングメカニズムを使用して、あるプロトコルのパケットを別のプロトコル内で転送できます。他のプロトコルを伝送するプロトコルはトランスポートプロトコルと呼ばれ、伝送されたプロトコルはパッセンジャープロトコルと呼ばれます。Generic Routing Encapsulation（GRE）は、トランスポートプロトコルとして IP を使用し、さまざまなパッセンジャープロトコルを伝送できるトンネリングメカニズムです。

トンネルの送信元アドレスと宛先アドレスは、トンネル内の仮想ポイントツーポイントリンクの 2 つのエンドポイントを識別するために使用されます。Citrix SD-WAN アプライアンスでの GRE トンネルの構成について詳しくは、「GRE トンネル」を参照してください。

GRE トンネルの統計情報を表示するには、[レポート**] > [**統計**] > [GRE** トンネル] タブに移動します。

次のメトリックを表示できます。

- サイト名: サイト名。
- **Tx** 帯域幅: 送信された帯域幅。

- 受信帯域幅: 受信した帯域幅。
- **Packet Dropped**: ネットワークの輻輳が原因でドロップされたパケットの数。
- フラグメント化されたパケット: フラグメント化されたパケットの数。パケットはフラグメント化されて、元のデータグラムよりも小さい MTU を持つリンクを通過できる小さなパケットを作成します。フラグメントは受信ホストによって再構成されます。
- 展開/折りたたみ: 必要に応じてデータを展開または縮小できます。

IPSec トンネル

IP セキュリティ（IPsec）プロトコルは、機密データの暗号化、認証、再生に対する保護、IP パケットのデータ機密性などのセキュリティサービスを提供します。カプセル化セキュリティペイロード (ESP) および認証ヘッダー (AH) は、これらのセキュリティサービスを提供するために使用される 2 つの IPsec セキュリティプロトコルです。

IPsec トンネルモードでは、元の IP パケット全体が IPsec によって保護されます。元の IP パケットはラップおよび暗号化され、VPN トンネルを介してパケットを送信する前に新しい IP ヘッダーが追加されます。
Citrix SD-WAN アプライアンスの IPsec トンネルの構成について詳しくは、「IPsec トンネル終了」を参照してください。

IPsec トンネルの統計情報を表示するには、[レポート] **>** [統計] **>** [**IPsec** トンネル] タブに移動します。

次のメトリックを表示できます。

- トンネル名: トンネル名。
- トンネルの状態:IPsec トンネルの状態。
- **MTU**: 最大伝送ユニット: 特定のリンクを介して転送できる最大の IP データグラムのサイズ。
- 受信パケット**:** 受信したパケットの数。
- 送信されたパケット**:** 送信されたパケットの数。
- **Packet Dropped**: ネットワークの輻輳が原因でドロップされたパケットの数。
- ドロップされたバイト数: ドロップされたバイト数。
- 展開/折りたたみ: 必要に応じてデータを展開または縮小できます。

リアルタイム統計

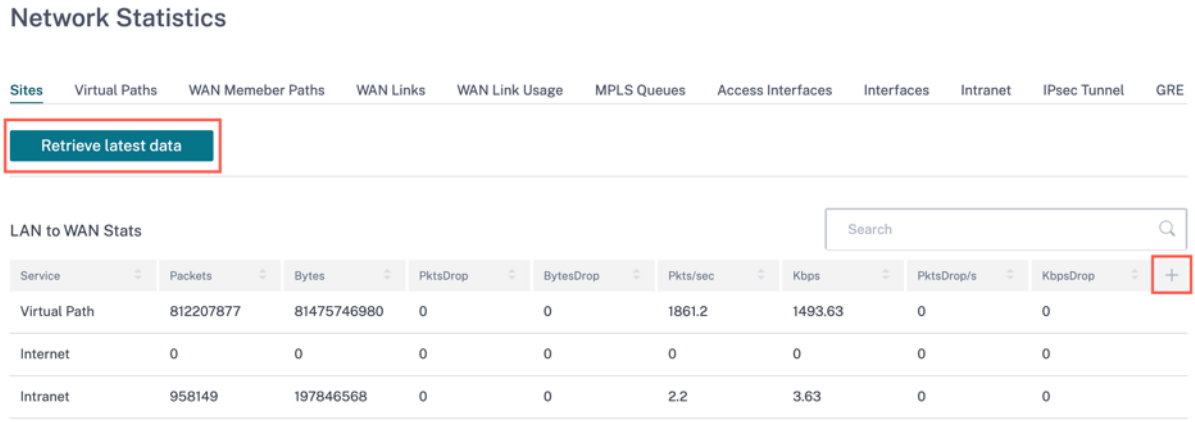
ネットワーク統計

[レポート] **>** [リアルタイム] **>** [ネットワーク統計] では、次のリアルタイム統計情報を取得できます。

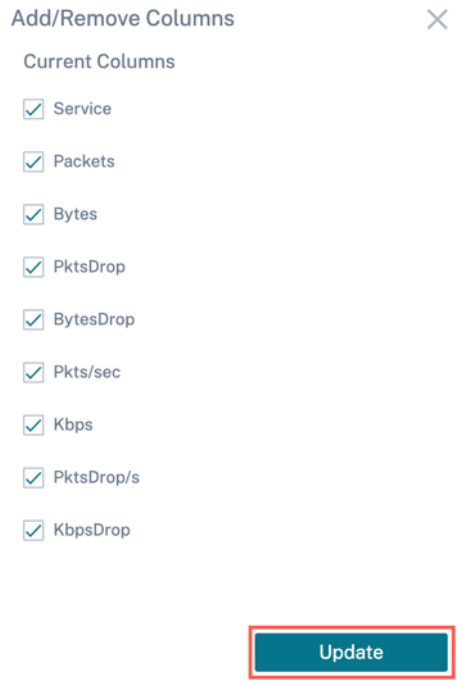
- サイト
- 仮想パス
- WAN メンバーパス
- WAN リンク
- WAN リンクの使用状況

- MPLS キュー
- アクセスインターフェイス
- インターフェイス
- イントラネット
- IPSec トンネル
- GRE

リアルタイムの統計レポートを取得するには、必要なタブ (サイト、仮想パス、WAN リンクなど) に移動し、[最新データの取得] をクリックします。



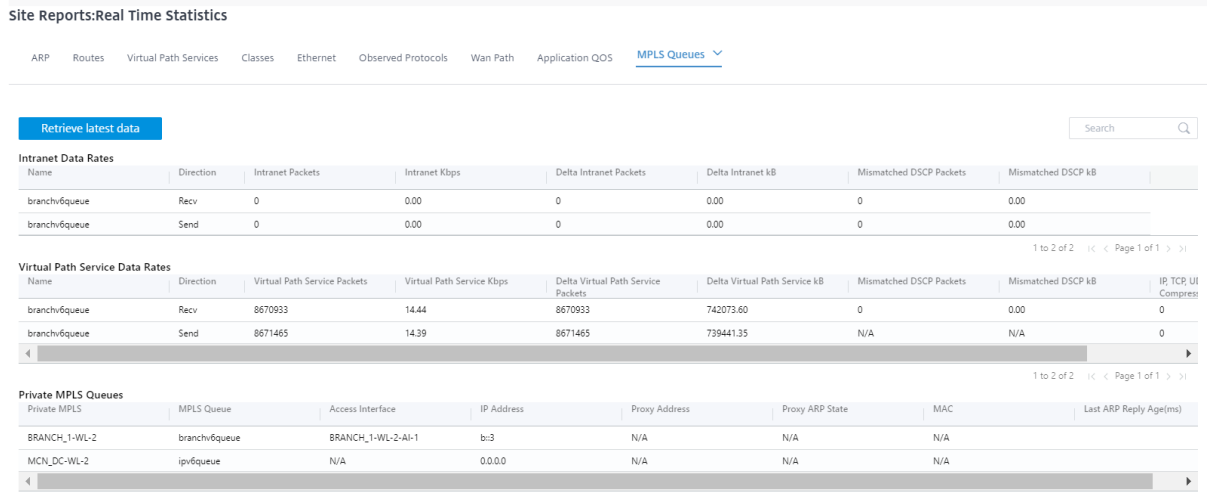
統計情報の表に列を追加または削除する場合は、プラス (+) 記号をクリックし、[更新] をクリックします。



MPLS キュー　MPLS キューを使用すると、MPLS WAN リンク上で、サービスプロバイダー MPLS キューに対応するキューを定義できます。MPLS キューの設定については、「MPLS キュー」を参照してください。

MPLS キュー統計情報をサイトレベルで表示するには、[レポート] > [リアルタイム] > [ネットワーク統計] に移動します。[**MPLS** キュー] をクリックし、[最新データの取得] をクリックします。最新の MPLS キューデータはアプライアンスから取得され、オンプレミス向け Citrix SD-WAN Orchestrator に表示されます。

イントラネットサービスおよび仮想パスサービスの方向、パケット数、デルタパケット、および一致しない DSCP パケットを表示できます。



プライベート MPLS キューの場合、次の詳細を表示できます。

- プライベート **MPLS**: プライベート MPLS WAN リンク。
- **MPLS** キュー:MPLS WAN リンクに関連付けられた MPLS キュー。
- アクセスインターフェイス:MPLS キューに関連するアクセスインターフェイス。
- **IP** アドレス:MPLS キューに関連付けられた IP アドレス。
- プロキシアドレス:MPLS キューに関連付けられているプロキシ IP アドレス。
- プロキシ **ARP** 状態: プロキシアドレス解決プロトコルの状態。有効、無効、または該当なし
- **MAC**: MPLS キューに関連付けられているインターフェイスの MAC アドレス。
- 最後の **ARP** 応答時間: 最後の ARP 応答が受信された時間 (ミリ秒単位)。

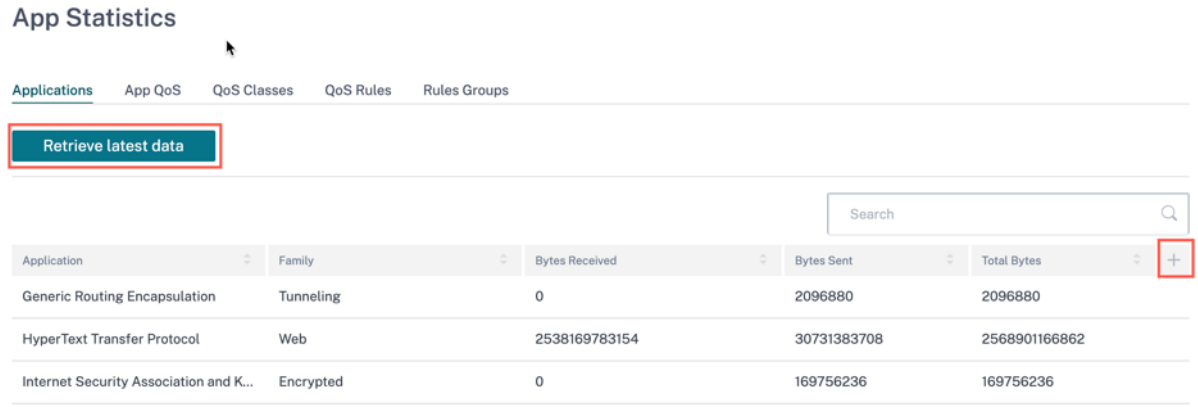
トラブルシューティングの詳細については、「MPLS キューのトラブルシューティング」を参照してください。

アプリ統計

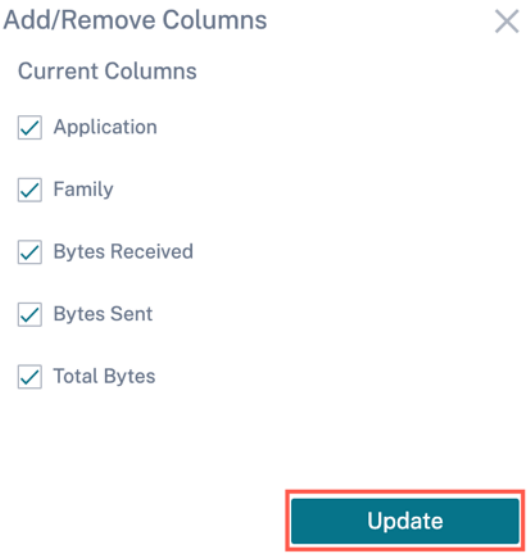
[レポート] **>** [リアルタイム] **>** [アプリ統計] では、次のリアルタイム統計情報を確認できます。

- アプリケーション
- 観測されたプロトコル
- アプリ QoS
- QoS クラス
- QoS ルール
- ルール・グループ

リアルタイムの統計レポートを取得するには、必要なタブ（アプリケーション、アプリ QoS、QoS ルールなど）に移動し、「最新データを取得」をクリックします。



統計情報の表に列を追加または削除する場合は、プラス (+) 記号をクリックし、[更新] をクリックします。

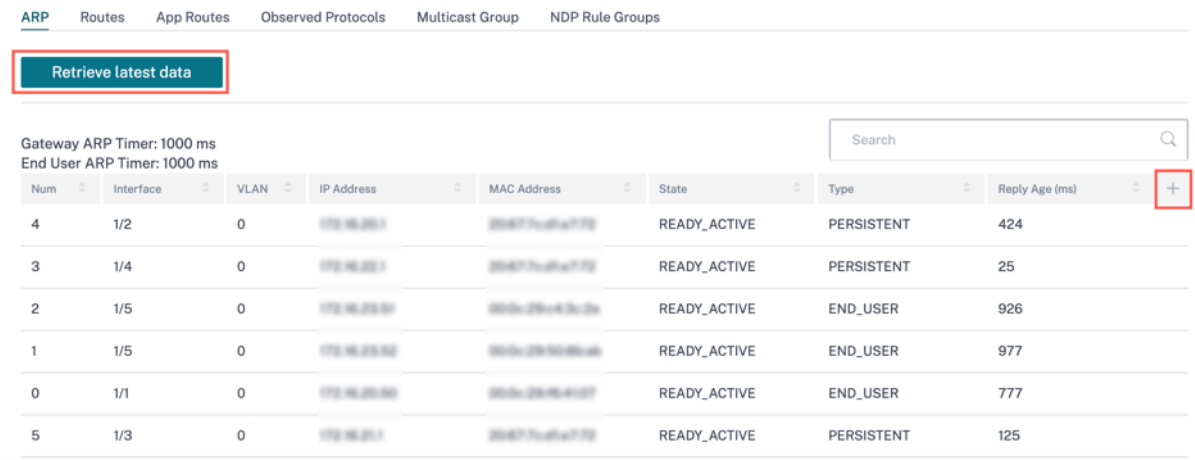


ルート統計情報

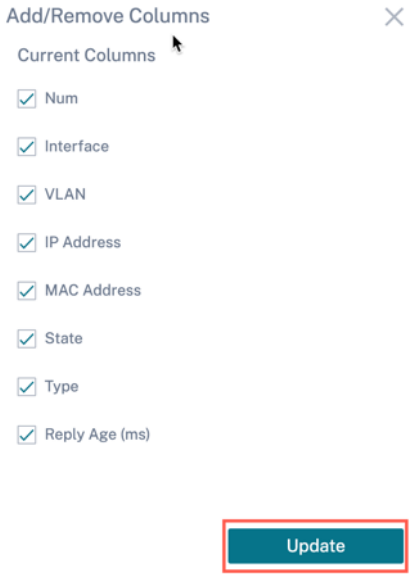
[レポート] > [リアルタイム] > [ルート統計] では、次のリアルタイムルート統計情報を取得できます。

- ARP (アドレス解決プロトコル)
- ルート
- アプリルート
- 観測されたプロトコル
- マルチキャストグループ
- NDP ルールグループ

リアルタイムの統計レポートを取得するには、必要なタブ (ARP、ルート、アプリルートなど) に移動し、「最新データを取得」をクリックします。



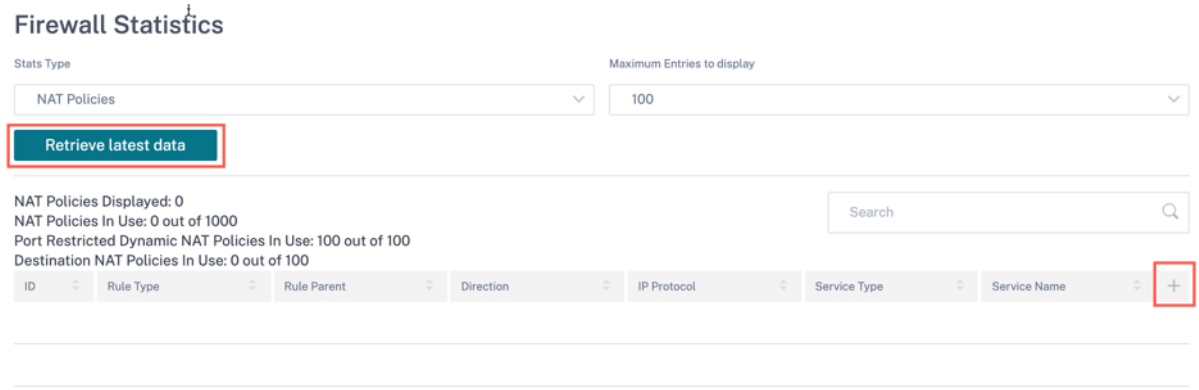
統計情報の表に列を追加または削除する場合は、プラス (+) 記号をクリックし、[更新] をクリックします。



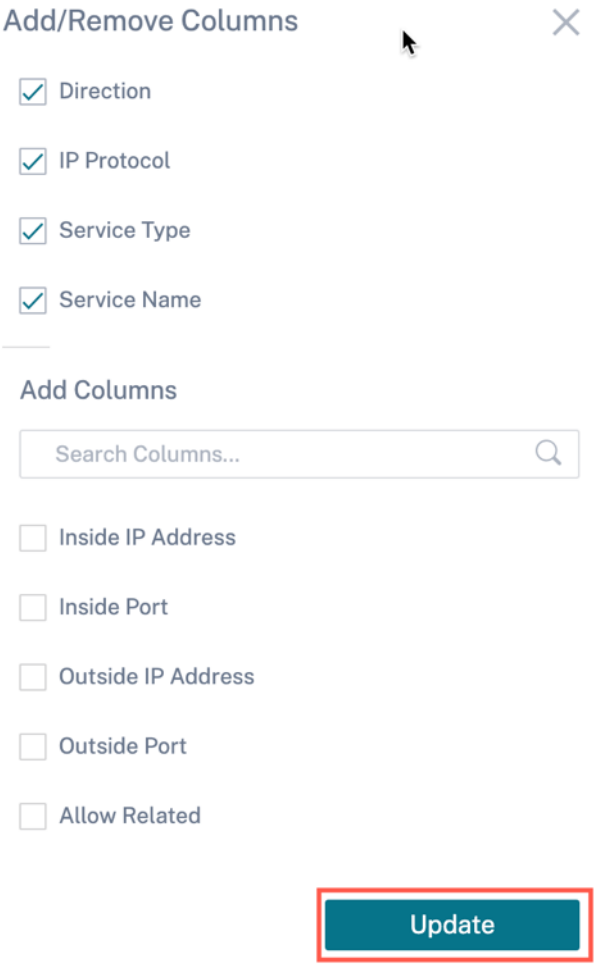
ファイアウォールの統計情報

ファイアウォールの統計ページには、接続の状態、ネットワークアドレスプロトコル (NAT) ポリシー、設定されたファイアウォールアクションに基づく特定のセッションに関連するフィルターポリシーが表示されます。ファイアウォール接続では、接続の送信元と宛先に関する詳細な情報も提供されます。

リアルタイムのファイアウォール統計情報は、[レポート] **>** [リアルタイム] **>** [ファイアウォール統計] で確認できます。ドロップダウンリストから統計タイプ (接続、NAT ポリシー、フィルタポリシー) を選択します。表示する最大エントリ数を選択し、「最新データを取得」をクリックします。

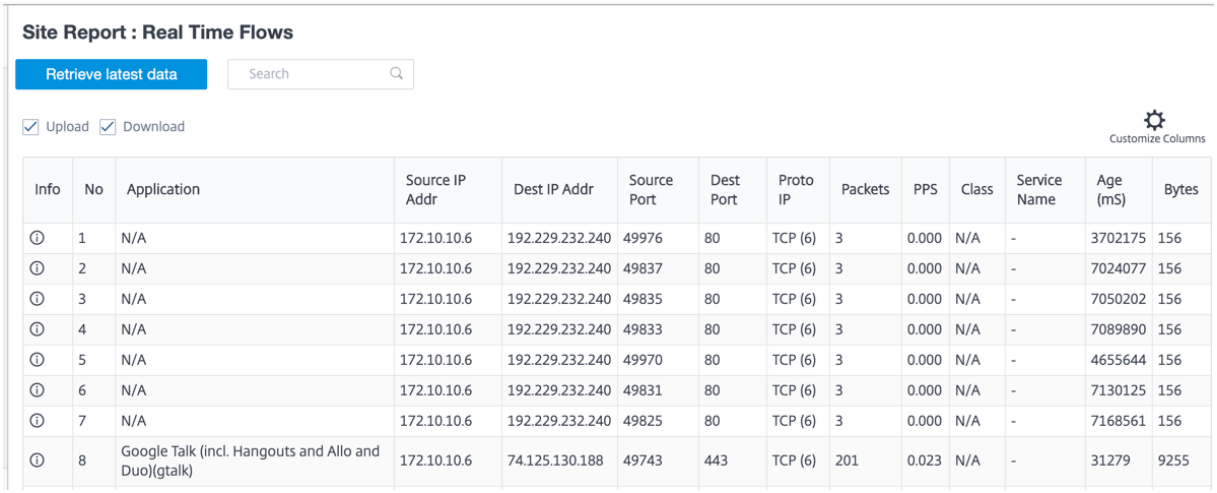


統計情報の表に列を追加または削除する場合は、プラス (+) 記号をクリックし、[更新] をクリックします。



フロー

フロー機能は、アプライアンスを通過する特定のセッションに関連する単方向のフロー情報を提供します。これにより、フローが該当する宛先サービスタイプに関する情報と、ルールとクラスタイプ、および伝送モードに関連する情報も提供されます。



Site Report : Real Time Flows

Retrieve latest data | Search

Upload | Download | Customize Columns

Info	No	Application	Source IP Addr	Dest IP Addr	Source Port	Dest Port	Proto IP	Packets	PPS	Class	Service Name	Age (mS)	Bytes
ⓘ	1	N/A	172.10.10.6	192.229.232.240	49976	80	TCP (6)	3	0.000	N/A	-	3702175	156
ⓘ	2	N/A	172.10.10.6	192.229.232.240	49837	80	TCP (6)	3	0.000	N/A	-	7024077	156
ⓘ	3	N/A	172.10.10.6	192.229.232.240	49835	80	TCP (6)	3	0.000	N/A	-	7050202	156
ⓘ	4	N/A	172.10.10.6	192.229.232.240	49833	80	TCP (6)	3	0.000	N/A	-	7089890	156
ⓘ	5	N/A	172.10.10.6	192.229.232.240	49970	80	TCP (6)	3	0.000	N/A	-	4655644	156
ⓘ	6	N/A	172.10.10.6	192.229.232.240	49831	80	TCP (6)	3	0.000	N/A	-	7130125	156
ⓘ	7	N/A	172.10.10.6	192.229.232.240	49825	80	TCP (6)	3	0.000	N/A	-	7168561	156
ⓘ	8	Google Talk (incl. Hangouts and Allo and Duo)(gtalk)	172.10.10.6	74.125.130.188	49743	443	TCP (6)	201	0.023	N/A	-	31279	9255

ルーティングプロトコル

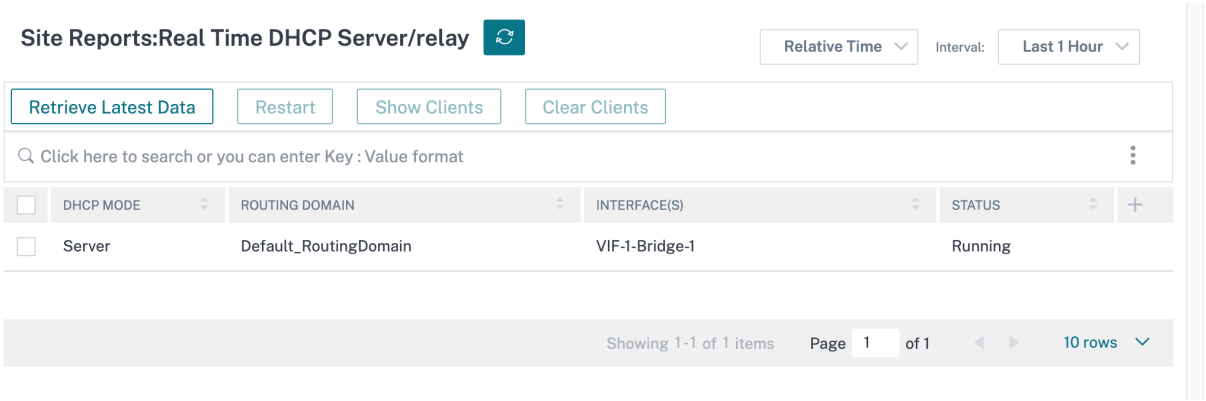
ルーティングプロトコルレポートには、ルーティングプロトコルに関連するパラメータの詳細が表示されます。「ビュー」ドロップダウンリストからプロトコルを選択し、「ルーティングドメイン」ドロップダウンリストからルーティングドメインを選択します。「最新データを取得」をクリックして、現在のデータを表示します。

以下に関連するパラメータの詳細を表示できます。

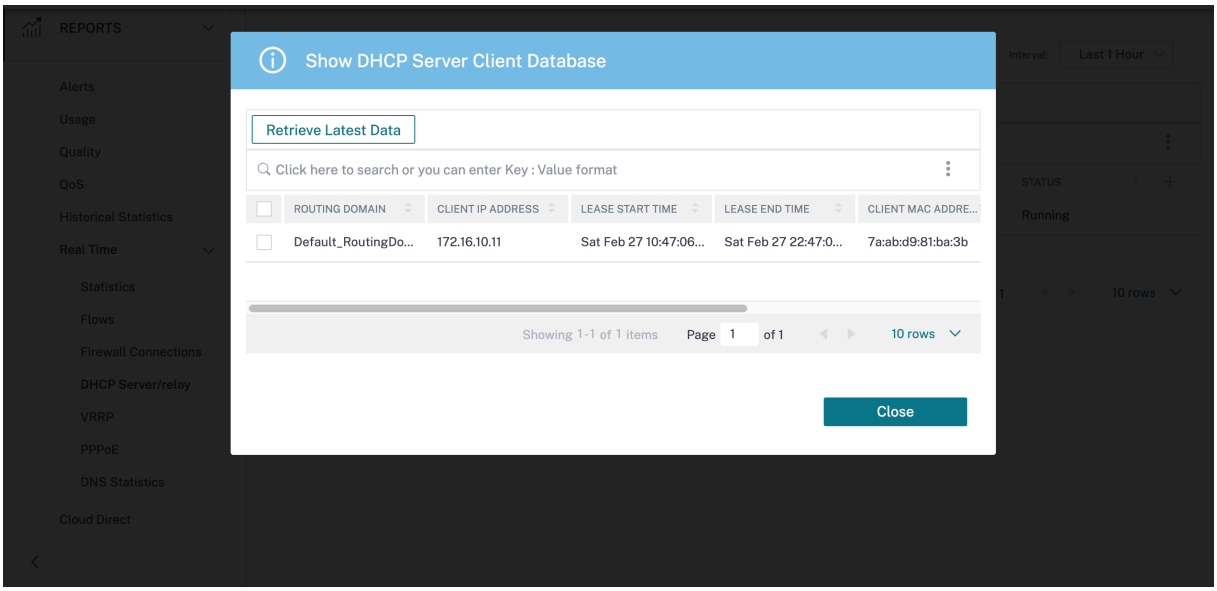
- BGP ステート
- OSPF ステート
- OSPF トポロジ
- OSPF インターフェイス
- OSPF LSADB
- OSPF ネイバーズ
- ルートテーブル

DHCP サーバー & リレー

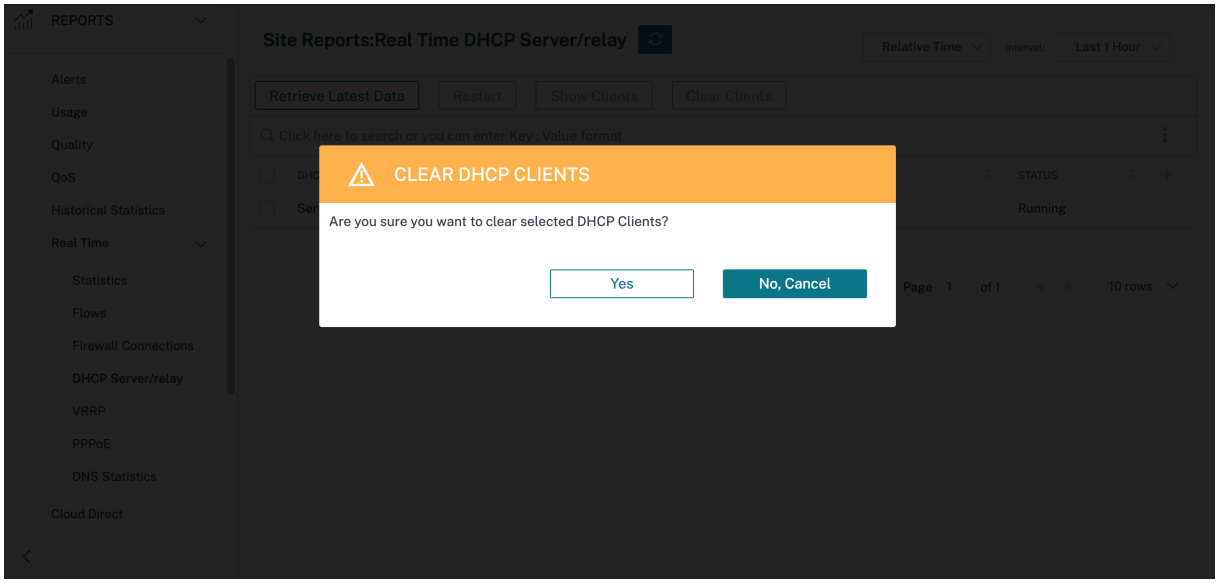
DHCP Server/Relay レポートには、DHCP サーバーまたはリレーとして設定されているインターフェイスと、関連するルーティングドメインとステータスに関する情報が表示されます。**Key: Value** 形式を使用して、必要な DHCP サーバーまたはリレー情報を検索できます。



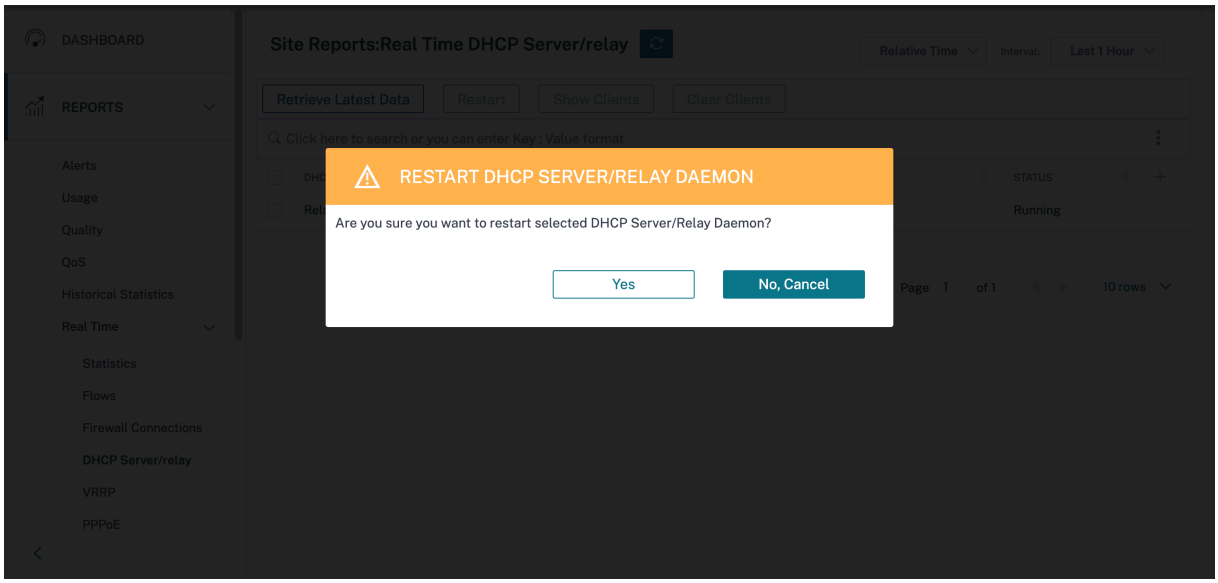
モードが [サーバ] の場合は、[クライアントを表示] をクリックして、DHCP サーバに関連する DHCP クライアントのリストを表示できます。



Clear Clients をクリックして、現在 DHCP サーバーに関連付けられている DHCP クライアントを削除します。



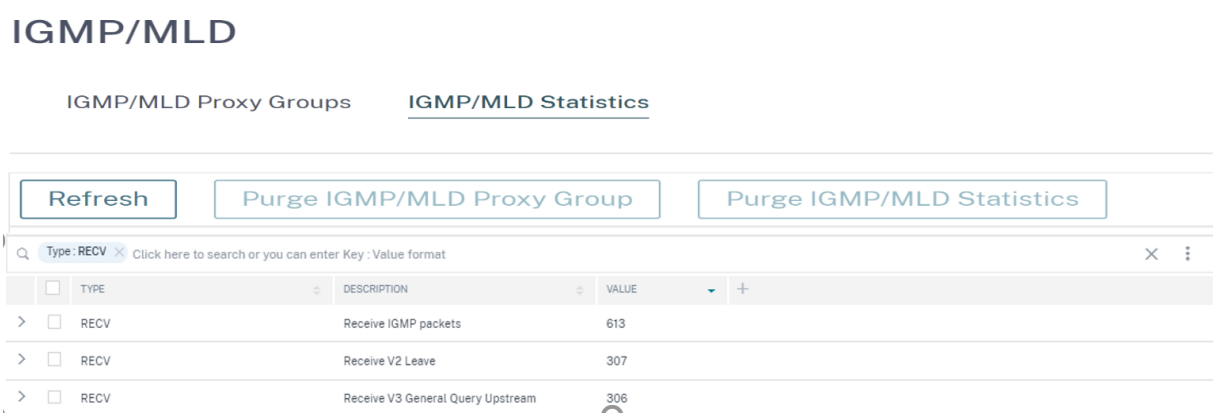
[再起動] をクリックして DHCP サーバーまたはリレーを再起動します。



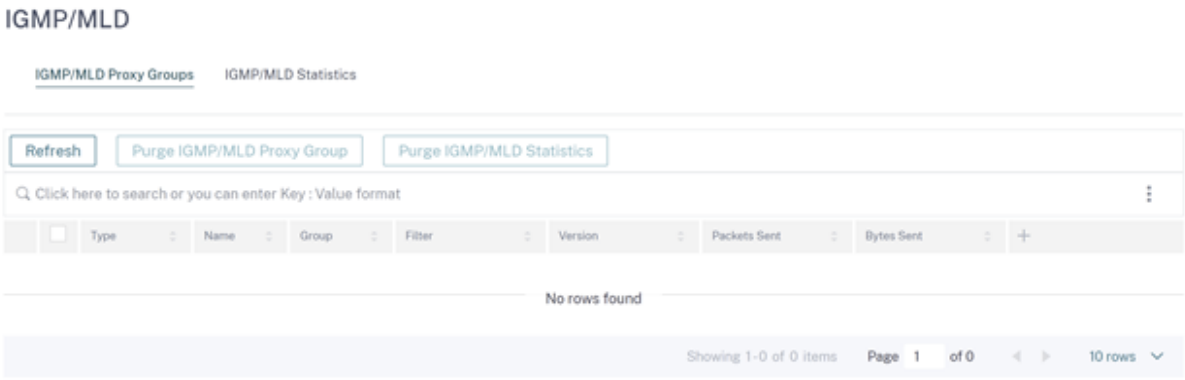
IGMP/MLD

マルチキャストレシーバがグループ加入要求を開始すると、[レポート] > [リアルタイム] > [IGMP/MLD] > [**IGMP/MLD** 統計情報] にレシーバの詳細が表示されます。この情報は、送信元と宛先の両方で確認できます。[更新] をクリックして、現在のデータを取得します。

次の図は、受信した IGMP パケットと、フィルタタイプ RECV を使用して IGMP 受信パケットが含まれていることを示しています。



IGMP プロキシグループの詳細を表示するには、[レポート] > [リアルタイム] > [**IGMP/MLD**] > [**IGMP/MLD** プロキシグループ] に移動します。[更新] をクリックして、現在のデータを取得します。

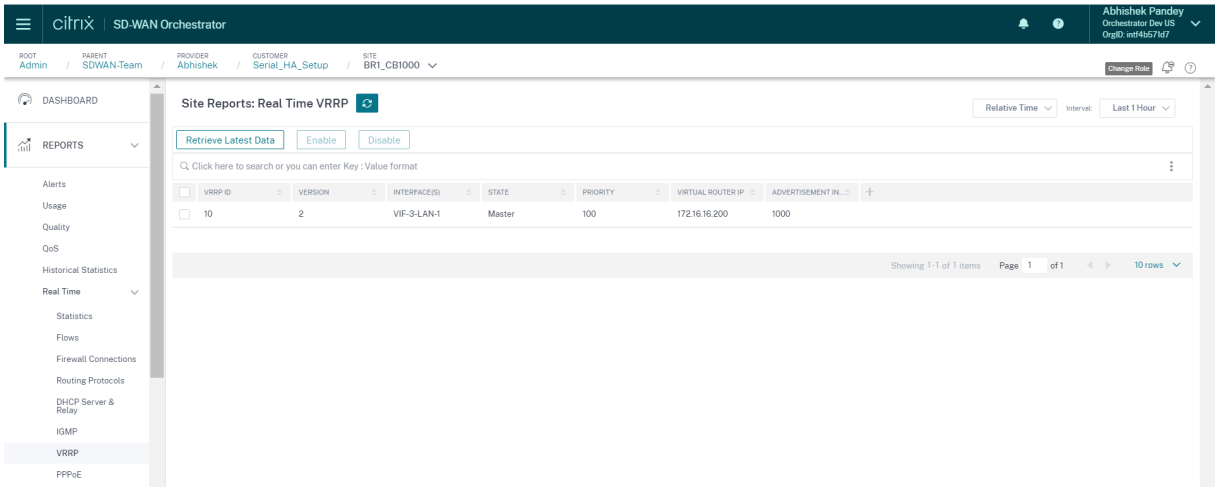


IGMP 統計情報テーブルから **IGMP** 統計データを削除するには、**[IGMP** 統計情報の消去] を選択します。

IGMP グループテーブルから **IGMP** グループデータを削除するには、**[IGMP /MLD** グループの消去] を選択します。

VRRP

VRRP リアルタイムレポートには、設定されている VRRP グループの詳細が表示されます。
仮想ルータ冗長プロトコル（**VRRP**）レポートを表示するには、**[**レポート**] > [**** リアルタイム] > [**VRRP**] に移動します。「****** 最新データを取得」をクリックして、現在のデータを取得します。



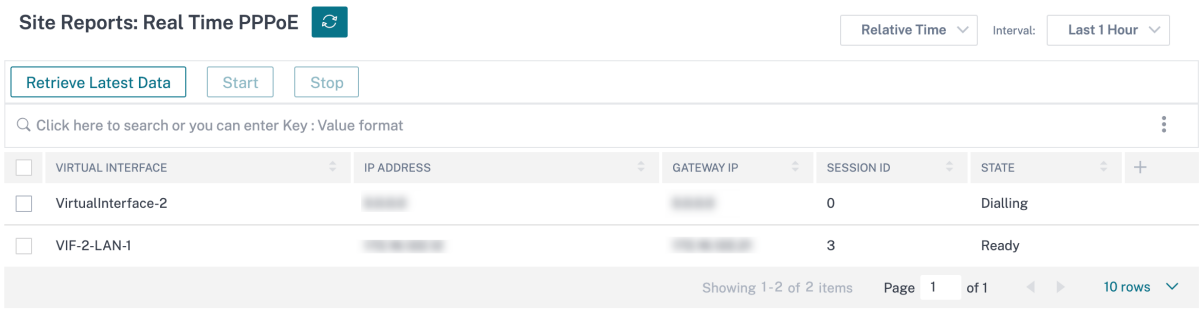
PPPoE

PPPoE レポートは、PPPoE スタティックまたはダイナミッククライアントモードで設定された仮想インターフェイスのステータス情報を提供します。トラブルシューティングの目的で、手動でセッションを開始または停止できます。

- 仮想インターフェイス:PPPoE に関連する仮想インターフェイス。
- **IP** アドレス: 仮想インターフェイスに関連付けられた IP アドレス。仮想インターフェイスが起動していて準備が完了したら、最近受信した値を表示します。仮想インターフェイスが停止しているか、障害状態になっている場合は、最後に受信した値を表示します。
- ゲートウェイ **IP:** ゲートウェイに関連付けられた IP アドレス。仮想インターフェイスが起動していて準備が完了したら、最近受信した値を表示します。仮想インターフェイスが停止しているか、障害状態になっている場合は、最後に受信した値を表示します。
- セッション **ID**: PPPoE セッションに関連する一意の識別子。
- 状態: 状態列には PPPoE セッションのステータスが表示されます。次の表では、状態と説明について説明します。

PPPoE セッションタイプ	説明
構成済み	VNI には PPPoE が設定されています。これは初期状態です。
ダイヤル中	VNI が設定されると、PPPoE ディスカバリを開始して PPPoE セッション状態がダイヤル状態に移行します。パケット情報がキャプチャされます。
セッション	VNI はディスカバリー状態からセッション状態に移行し、動的な場合は IP の受信を待機し、静的な場合はアドバタイズされた IP のサーバーからの確認応答を待ちます。

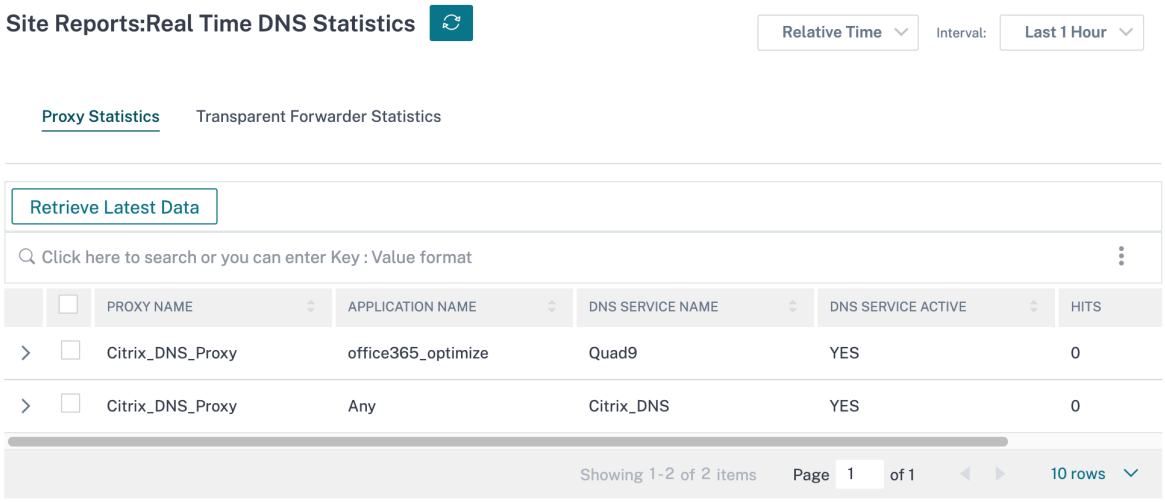
PPPoE セッションタイプ	説明
準備完了	IP パケットが受信され、VNI および関連する WAN リンクが使用可能になります。
失敗	PPP/PPPoE セッションが終了しました。失敗の原因は、無効な構成または致命的なエラーが原因である可能性があります。セッションは 30 秒後に再接続を試みます。
停止しました	PPP/PPPoE セッションは手動で停止されます。
終了中	理由により終了する中間状態。この状態は、一定時間（通常のエラーの場合は 5 秒、致命的なエラーの場合は 30 秒）後に自動的に開始されます。
無効	SD-WAN サービスは無効です。



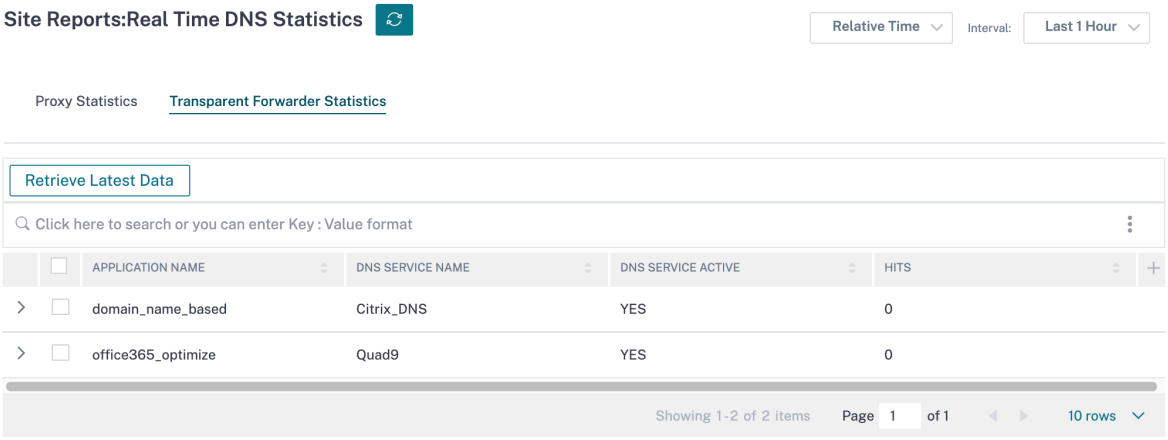
DNS 統計情報

DNS 統計は、アプリケーション名、DNS サービス名、DNS サービスのステータス、および`hits`の量に関する情報を DNS サービスに提供します。DNS プロキシと DNS トランスペアレントフォワーダの情報は、2 つの異なるタブに表示されます。

プロキシ統計情報



トランスペアレントフォワーダの統計



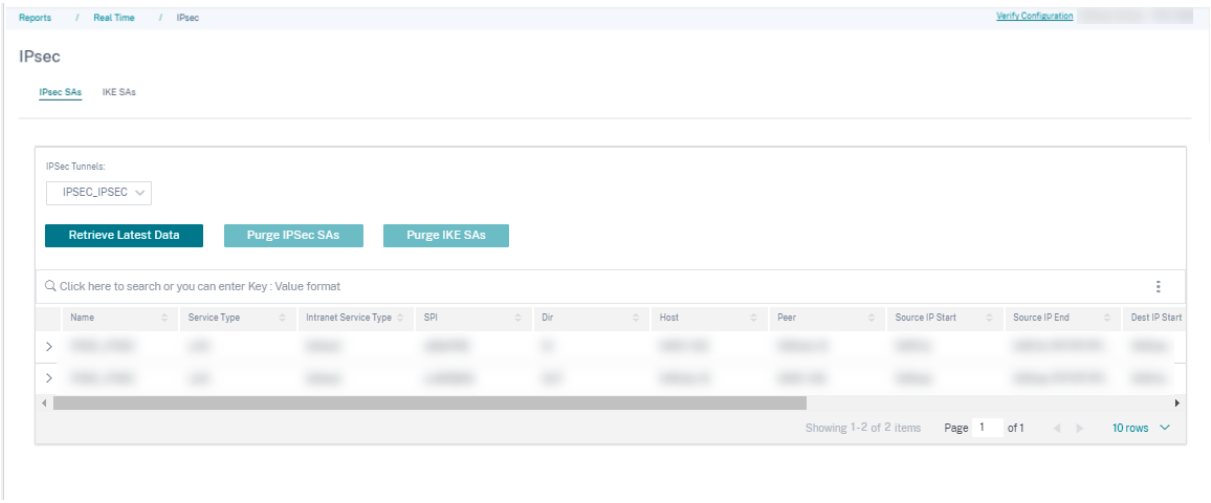
IPsec

IPsec リアルタイムレポートには、ネットワーク上の IPsec トンネル設定に関する詳細が表示されます。

IPsec セキュリティアソシエーション (IPsec SA) の詳細を表示するには、[レポート] > [リアルタイム] > [**IPsec **SA]** に移動します。****** 最新のデータを取得するには、**[**最新のデータを取得] をクリックします。

インターネット鍵交換セキュリティアソシエーション (IKE SA) の詳細を表示するには、[レポート] > [リアルタイム] > [**IPsec**] > [**IKE SA**] に移動します。最新のデータを取得するには、**[**最新のデータを取得] をクリックします。

IPsec グループデータおよび統計データを消去するには、それぞれ [IPsec グループの消去] と [**IKE** 統計情報の消去] を選択します。

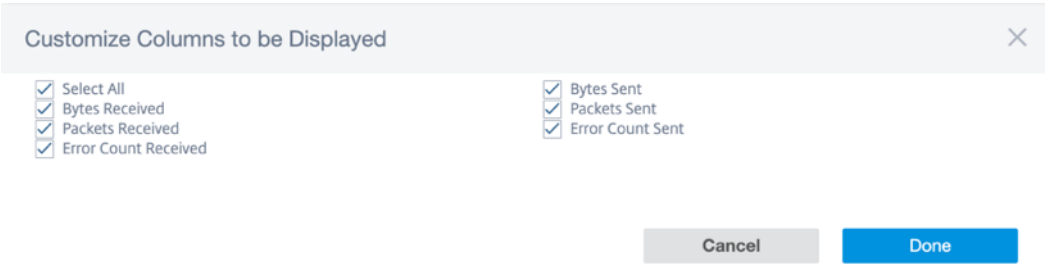


アプライアンスレポート（プレビュー）

アプライアンスレポートは、ネットワークトラフィックとシステム使用状況レポートを提供します。このデータを使用して、ネットワークの問題をトラブルシューティングしたり、Citrix SD-WAN デバイスの動作を分析したりできます。「アプライアンス・レポート」ページには、次のタブが表示されます。

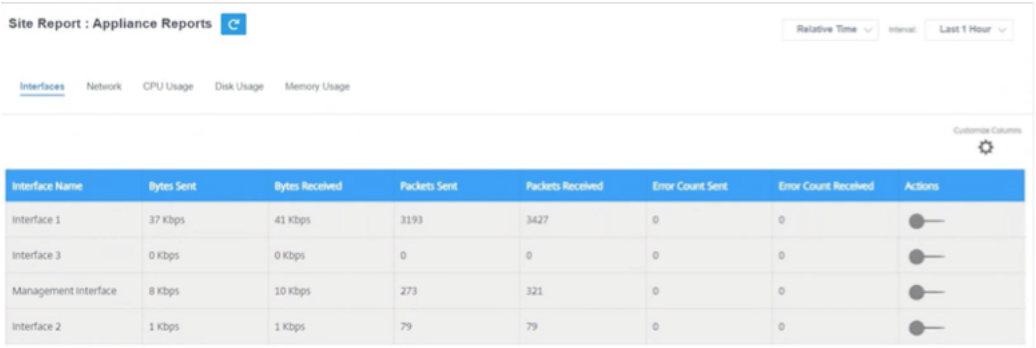
- インターフェイス
- ネットワーク
- CPU 使用率
- ディスク使用量
- メモリ使用率

各タブをクリックして、時間、日、週、月ごとにアプライアンスのグラフを表示または監視します。必要に応じて、[絶対時間] と [相対時間] を切り替えることができます。テーブルの列はカスタマイズ可能です。表の右上隅にある [列をカスタマイズ] をクリックし、表に表示または非表示にするオプションを選択または選択解除します。



インターフェイス

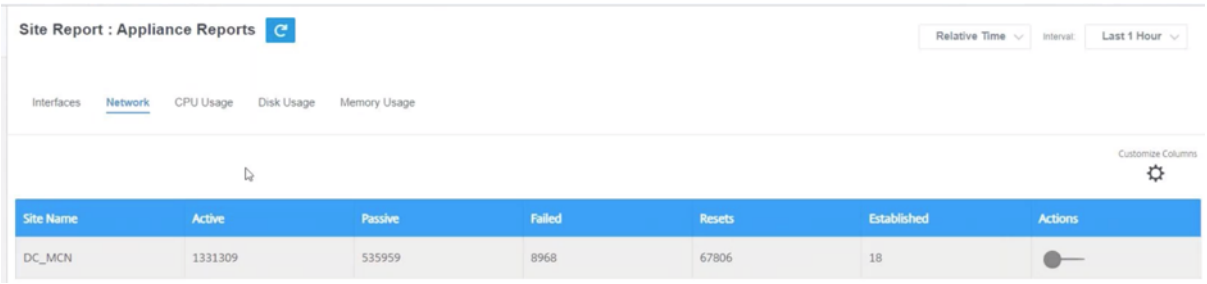
インターフェースページには、管理インターフェースのエラー/トラフィックが表示されます。すべてのネットワークは、管理インターフェイス、インターフェイス 1/2/3 などの異なるインターフェイスに分割されています。



- インターフェース名—インターフェース名を表示します。
- 送信バイト数—選択した期間に送信された平均バイト数 (Kbps)。
- 受信バイト数—選択した期間に受信した平均バイト数 (Kbps)。
- 送信されたパケット—選択した期間に送信されたパケットの平均数。
- 受信パケット—選択した期間に受信された平均パケット数。
- 送信されたエラー数—選択した期間に送信されたエラーカウントの数。
- 受信したエラー数—選択した期間に受信したエラー件数。
- アクション—アクションボタンをオンにすると、ネットワークグラフを表示できます。

ネットワーク

ネットワークページには、構成された各サイトの TCP 接続の数が表示されます。



- サイト名—サイト名を表示します。
- アクティブ—選択した期間におけるアクティブな TCP 接続数の平均値。
- パッシブ—選択した期間におけるパッシブ TCP 接続数の平均値。
- 失敗—選択した期間における TCP 接続失敗回数の平均値。
- リセット—選択した期間におけるリセット TCP 接続数の平均回数。
- 確立済み—選択した期間における確立された TCP 接続数の平均値。
- アクション—アクションボタンをオンにすると、ネットワークグラフを表示できます。

CPU 使用率

CPU 使用率ページには、SD-WAN デバイスの CPU 使用率がパーセンテージで表示されます。[CPU] グラフには、選択した時間における一定間隔の平均の CPU 消費量が表示されます。

- サイト名—サイト名を表示します。
- システム—CPU がシステム領域プログラムの処理に費やした合計時間の割合。
- ユーザ—CPU がユーザースペースのプログラムの処理に費やした合計時間の割合。
- いいね—CPU が通常より低い優先度のユーザータスクを実行している場合に便利です。
- アイドル—CPU がアイドルモードになっていた合計時間の割合。
- **Io Wait** —CPU が I/O 操作の待機に費やした合計時間のパーセンテージ。
- **Irq** —カーネルが処理する割り込み要求 (IRQ) 値。
- スティール -仮想化環境で実行する場合、ハイパーバイザーはさまざまな理由で、CPU 用のサイクルを盗んで別の CPU に渡すことがあります。この時間は、盗むとして知られています。
- アクション—アクションボタンをオンにすると、ネットワークグラフを表示できます。

ディスク使用率

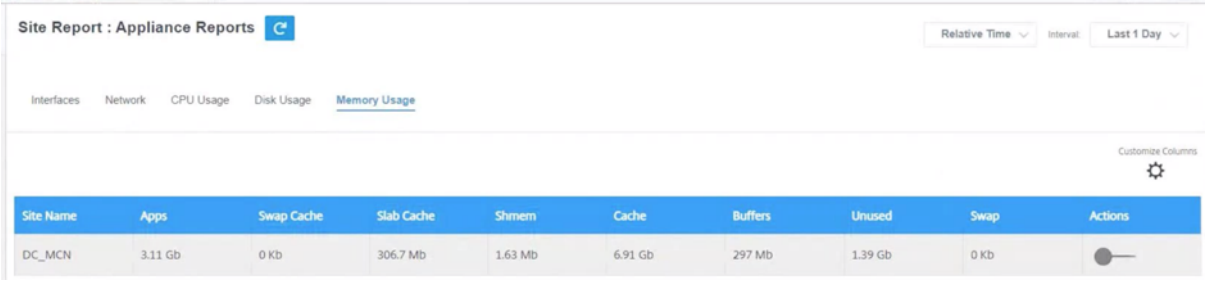
ディスク使用量ページには、オペレーティングシステムとデータパーティションが使用しているハードディスク容量が I/O /秒 (IOPS) の値で表示されます。

- サイト名—サイト名を表示します。
- ディスク名—ハードディスク名を表示します。
- **Read IOPS** —選択した期間における 1 秒あたりの平均読み取り IOPS 数を表示します。
- **Write IOPS** —選択した時間枠における 1 秒あたりの平均書き込み IOPS 数を表示します。

- レイテンシー—選択した時間枠における、選択したボリュームワークロードからの正常な読み取りおよび書き込みリクエストのレイテンシー値を表示します。I/O パフォーマンスには、10 ミリ秒未満のレイテンシー値が最適であることが推奨されます。
- 読み取りスループット—選択した時間におけるディスク読み取り操作の平均ディスクスループット値を Kbps 単位で表示します。
- 書き込みスループット—選択した時間におけるディスク書き込み操作の平均ディスクスループット値を Kbps 単位で表示します。
- ディスク使用率—選択した期間における平均ディスク使用率をパーセンテージで表示します。
- アクション—アクションボタンをオンにすると、ネットワークグラフを表示できます。

メモリ使用率

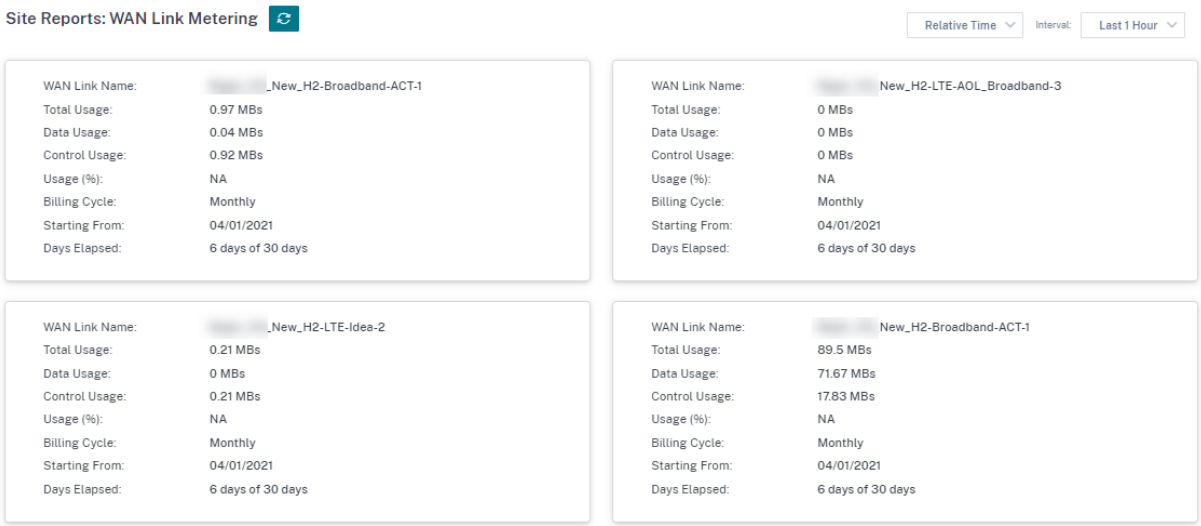
メモリ使用量ページには、メモリ使用量のレポートが表示されます。



- サイト名—サイト名を表示します。
- アプリ—使用中のアプリケーション値を GB 単位で表示します。
- スワップキャッシュ—スワップキャッシュの数を MB 単位で表示します。スワップキャッシュは、物理ページごとに 1 つのエントリを持つページテーブルエントリのリストです。
- スラブキャッシュ—事前に割り当てられたメモリのスラブの数を表示します。MB で
- **Shmem** —使用済みの共有メモリの合計値を MB 単位で表示します。
- キャッシュ—使用されているキャッシュメモリの数を GB 単位で表示します。
- **Buffers** —バッファキャッシュが使用している物理メモリの数を表示します。
- 未使用—キャッシュの未使用メモリの数を表示します。
- スワップ—スワップスペースの数を表示します。スワップ領域は、物理メモリにスペース拡張が必要な場合に使用されます。
- アクション—アクションボタンをオンにすると、ネットワークグラフを表示できます。

WAN リンクメータリング

WAN リンクメータリングレポートには、従量制 WAN リンクの使用状況に関する詳細が表示されます。レポートを表示して、従量制課金 WAN リンクのデータ消費に関する洞察を得ることができます。WAN リンクメータリングレポートを表示するには、[レポート] **> [WAN** リンクメータリング] に移動します。

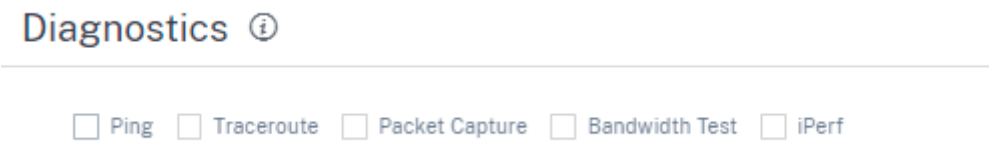


診断

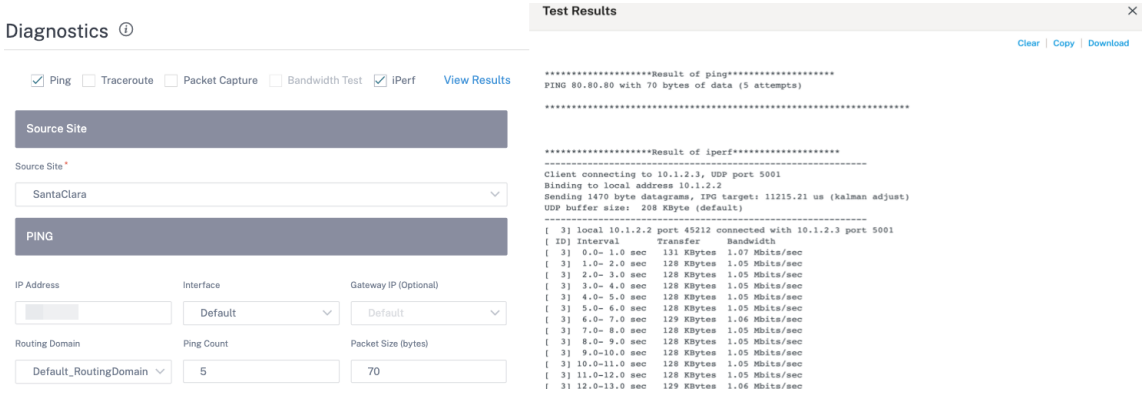
October 26, 2022

Ping、Traceroute、パケットキャプチャ、帯域幅テスト、iPerf 診断ユーティリティを使用して、SD-WAN ネットワーク上のネットワーク接続の問題をテストおよび調査できます。診断ページを表示するには、トラブルシューティング > 診断に移動します。

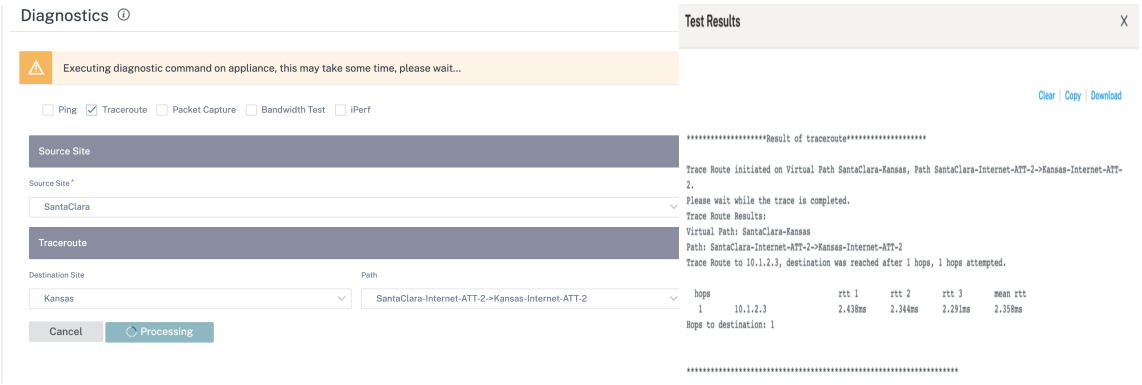
診断結果を表示するには、診断ページの右上隅にある「結果を表示」をクリックします。レポート結果は、必要に応じてダウンロード、コピー、クリアできます。



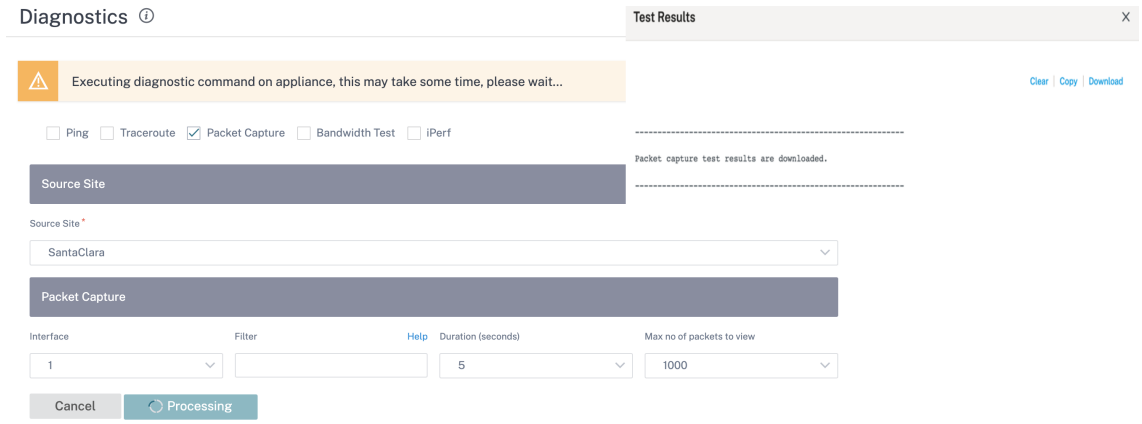
- **Ping** —リモートホストまたはサイトに **ping** を送信することで、ネットワーク接続を確認できます。宛先の詳細を入力し、ping 要求を送信する回数およびデータバイト数を指定します。宛先 **IP** アドレスを指定し、[実行] をクリックします。



- **traceroute** -ルートとサイト間のホップ数をトレースできます。ソースサイトとデスティネーションサイト、およびトレースするパスを選択し、[実行] をクリックします。

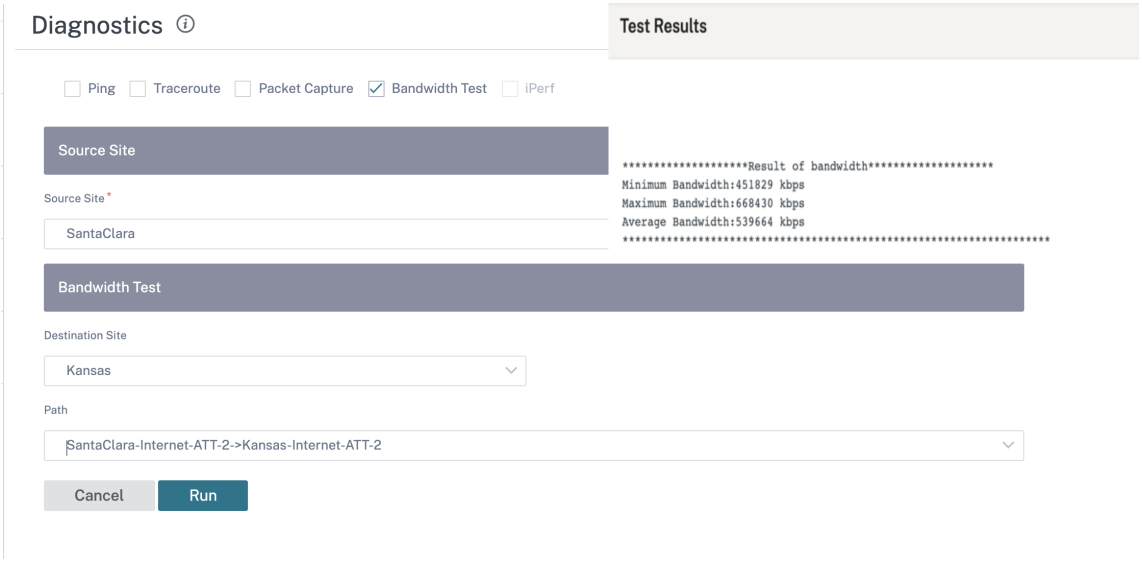


- パケットキャプチャ—選択したサイトにある選択したアクティブインターフェイスを通過するデータパケットを傍受できます。ソースと宛先の詳細を表示できます。



ヘルプオプションには、フィルターオプションの詳細が表示されます。

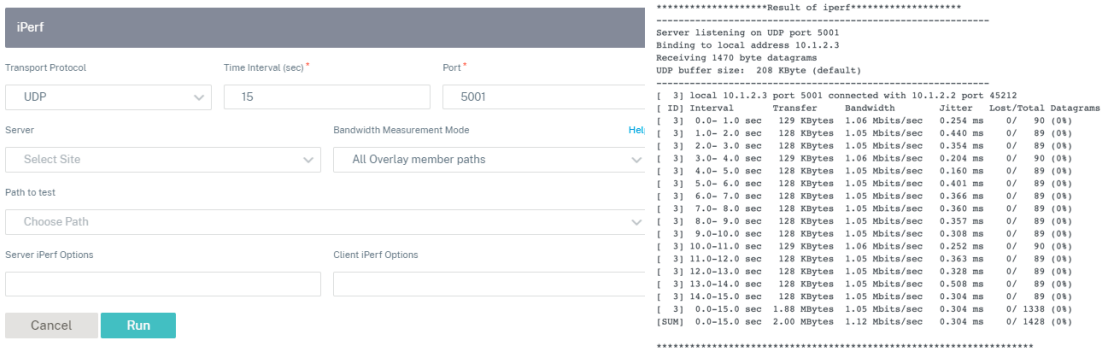
- 帯域幅テスト—サイトの特定のパスで帯域幅テストを実行して、最大、最小、および平均の帯域幅使用量を確認できます。ソースサイト、宛先サイトを入力し、パスを選択します。[実行] をクリックします。



- **iPerf** —サイトの特定のパスで iPerf テストを実行できます。iPerf 診断ツールを使用してテストトラフィックを生成すると、次のような原因となるネットワーク問題のトラブルシューティングが可能になります。

  - パスの状態が「良い」から「悪い」に頻繁に変化
  - アプリケーションのパフォーマンスが低い
  - パケット損失の増加

  iPerf 診断テストを実行するには、カスタマーレベルで [トラブルシューティング] > [診断] に移動し、[**iPerf**] チェックボックスを選択します。トランスポートプロトコル、時間間隔、ポート番号、サーバー、帯域幅測定モード、テストパス、サーバー iPerf オプションを入力し、[実行] をクリックします。

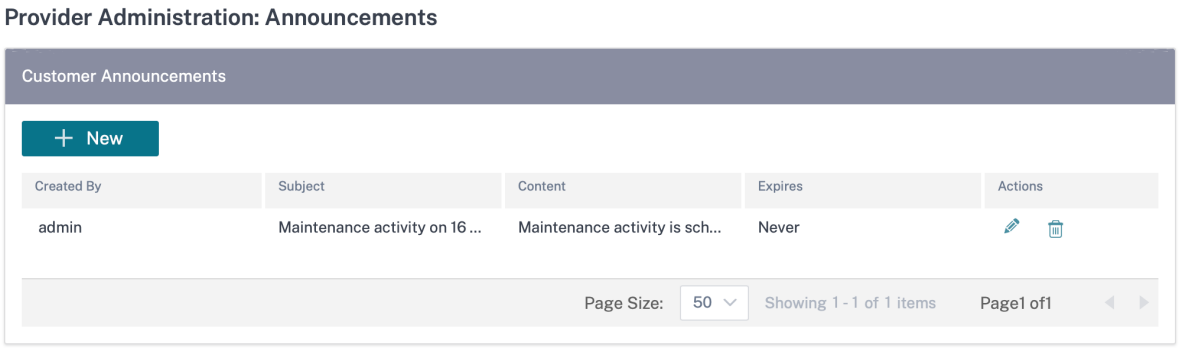


お知らせ

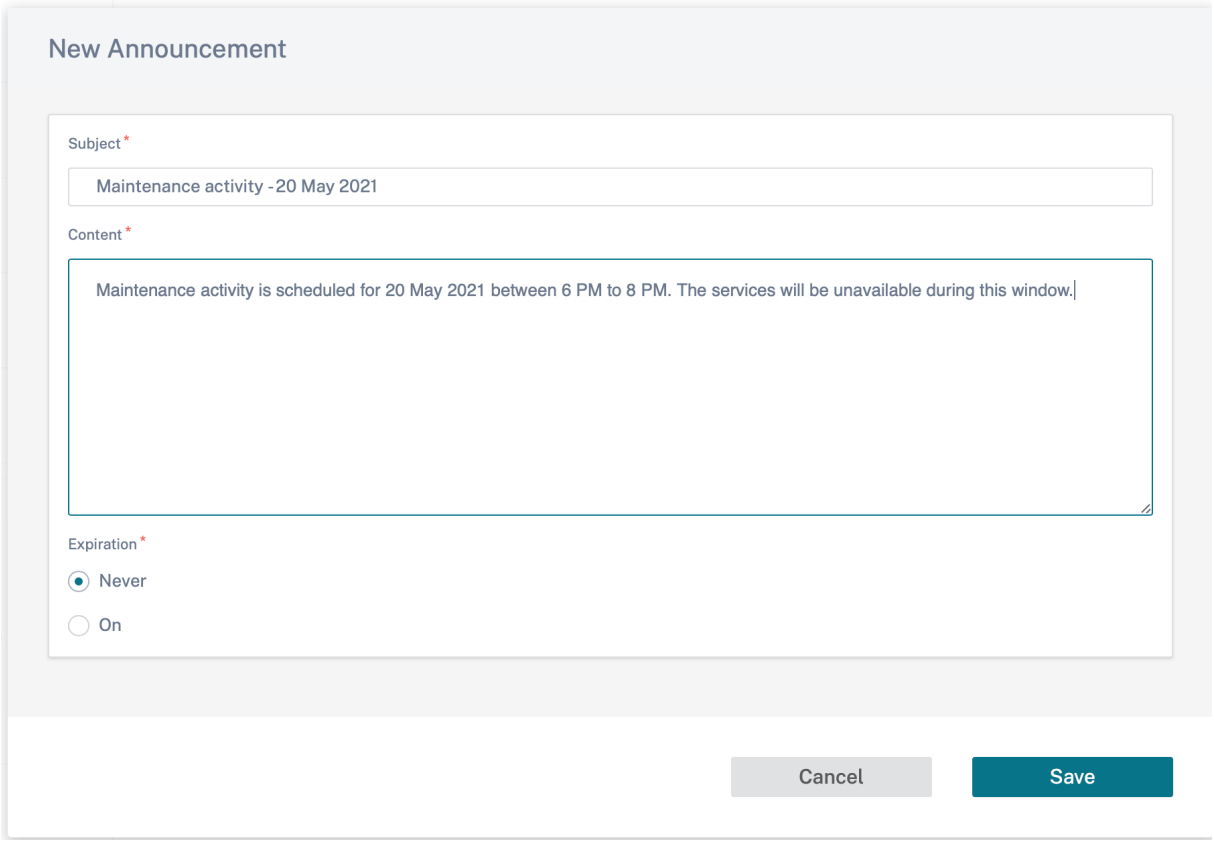
October 26, 2022

プロバイダーは [アナウンス] オプションを使用して、アナウンスや通知を顧客に送信できます。

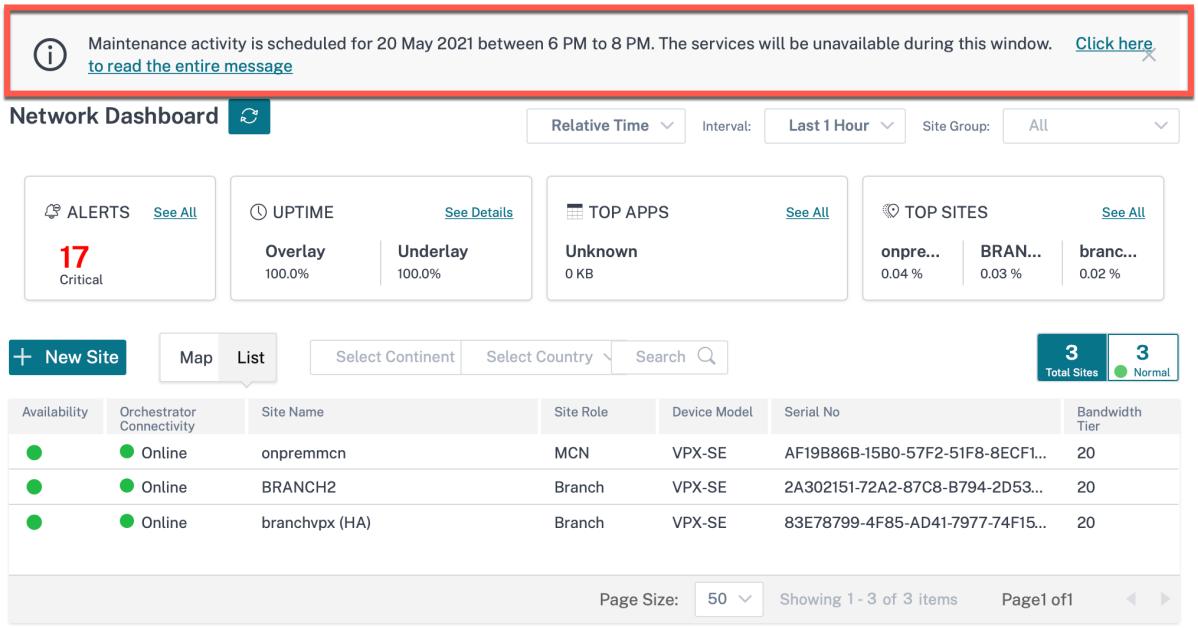
プロバイダーアナウンスを作成するには、[管理] **>** [アナウンス] に移動し、[**+** 新規] オプションをクリックします。



件名を入力し、コンテンツを HTML 形式またはプレーンテキスト形式で入力します。お知らせの有効期限を設定することもできます。



保存したお知らせは、すべての顧客に表示されます。



ユーザー管理

October 2, 2024

オンプレミス向け Citrix SD-WAN Orchestrator は、役割ベースのアクセス制御（RBAC）をサポートしています。RBAC は、個々のユーザーに割り当てられたロールに基づいて SD-WAN Orchestrator リソースへのアクセスを規制します。RBAC を使用すると、ユーザーはロールが要求するデータのみにアクセスでき、他のデータを制限できます。

役割は、オンプレミス向け Citrix SD-WAN Orchestrator のさまざまなアクティビティを表示および実行する権限を定義します。定義済みの役割のリストから役割をユーザーに割り当てることができます。

デフォルトでは、ユーザーアカウントはオンプレミス用 Citrix SD-WAN Orchestrator に作成され、ユーザー名は **admin** 、パスワードはパスワードとして設定されます。ユーザーは、初回ログイン時にデフォルトのパスワードを変更するように求められます。

ローカルおよびリモートで認証できるユーザーを追加できます。リモートで認証されたユーザは、RADIUS または TACACS+ 認証サーバを通じて認証されます。

プロバイダの役割

次の表に、事前定義されたプロバイダーの役割を示します。

プロバイダーロール	説明
プロバイダー-マスター-管理者-すべて	プロバイダーとそのすべての顧客情報を管理できる管理者
プロバイダー-マスター-管理者-テナント	プロバイダーとその顧客情報の一部を管理できる管理者
Provider-master-readonly-all	プロバイダーと顧客の情報のみを閲覧できる管理者
プロバイダー-ネットワーク-管理者 (プレビュー)	ネットワーク関連情報の閲覧と編集のみができる管理者
プロバイダー-セキュリティ-管理者 (プレビュー)	セキュリティ関連情報の閲覧と編集のみができる管理者

Provider-Master-Admin-All ロールは次のことを実行できます。

- プロバイダーネットワークとカスタマーネットワークのユーザーにロールを割り当てる
- その他すべての管理者ロールの顧客へのアクセスを管理する
- 割り当てられたロールを編集または削除する

お客様の役割

次の表は、事前定義済みの顧客ロールを一覧表示しています。

役割	説明
カスタマ-マスター/管理者	顧客情報を閲覧および編集できる顧客管理者
カスタマーマスター-レディオンリー管理者	顧客情報のみを閲覧できる顧客管理者
カスタマーネットワーク管理者 (プレビュー)	ネットワーク関連の情報のみを表示および編集できる顧客管理者
顧客-セキュリティ-管理者 (プレビュー)	セキュリティ関連情報のみを表示および編集できる顧客管理者

カスタマー**-**マスター**-**管理者の役割を持つユーザーは、次の操作を実行できます。

- ユーザーを追加して顧客の役割を割り当てる
- 割り当てられたロールを編集または削除する

> 注**:**
>
> 重要な役割 (マスター管理者、セキュリティ管理者、ネットワーク管理者) を信頼できるユーザーにのみ割り当てることが重要です。

サポートロール

トラブルシューティングの目的で、お客様はサポートの役割を割り当て、サポートチームのメンバーが情報を表示および編集できるようにすることができます。サポートロールには、ロールの割り当て時に定義された有効期間があります。有効期間が終了すると、サポートユーザーは顧客情報にアクセスできなくなります。ただし、サポートユーザーの詳細は、[管理] **> [**ユーザー管理**]** の下に引き続き表示されます。必要に応じて、お客様の管理者はサポートロールの削除または有効期間の延長を行うことができます。

役割	説明
カスタマーサポート-ReadWrite	顧客情報を閲覧および編集できるサポートチームメンバー
カスタマーサポート-読み取り専用	顧客情報のみを閲覧できるサポートチームメンバー

認証タイプ

オンプレミス向け Citrix SD-WAN Orchestrator は、次の種類の認証をサポートします。

- 単一要素認証：一要素認証は、ユーザーがオンプレミス向け Citrix SD-WAN Orchestrator にアクセスするための 1 つの認証方法を提供します。
- 二要素認証（**TFA**）：二要素認証は、ユーザーがオンプレミス向け Citrix SD-WAN Orchestrator にアクセスするための 2 つの認証方法を提供します。これにより、ログインシーケンスに追加のセキュリティ層が導入されます。

一要素認証と二要素認証では、次の認証方法がサポートされています。

- ローカル: 選択した場合、ユーザーはオンプレミス用 Citrix SD-WAN Orchestrator で構成されたパスワードを使用してアクセスする必要があります。
- **RADIUS**: 選択した場合、ユーザーは RADIUS サーバーのパスワードを使用してアクセスする必要があります。
- **TACACS+**: 選択した場合、ユーザーは TACACS+ サーバーのパスワードを使用してアクセスする必要があります。

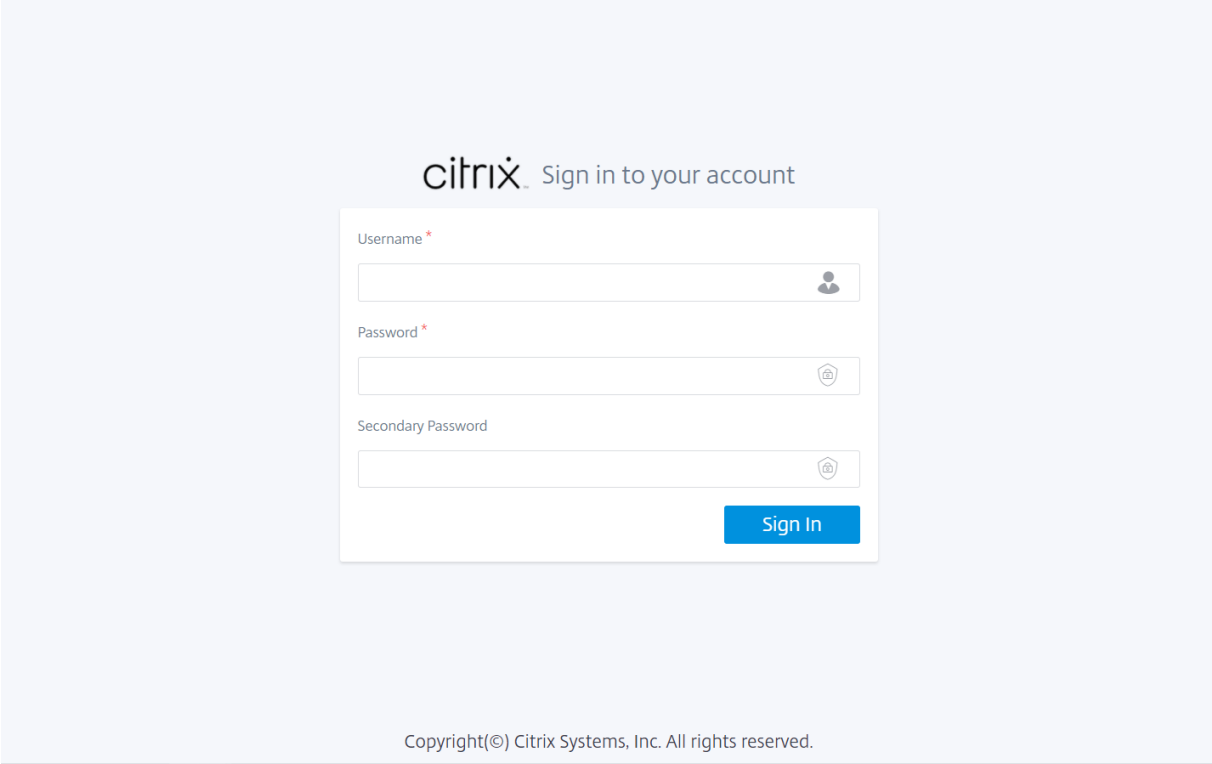
次の表は、ローカルで認証されるユーザーがサポートする一次認証方法と二次認証方法を示しています。

	プライマリ認証タイプ	二次認証タイプ
単一要素認証	ローカル	-
2 要素認証	ローカル	RADIUS または TACACS+

次の表は、リモート認証されるユーザーがサポートする一次認証方法と二次認証方法を示しています。

	プライマリ認証タイプ	二次認証タイプ
単一要素認証	ローカル、RADIUS、または TACACS+	-
2 要素認証	ローカル、RADIUS、または TACACS+	RADIUS または TACACS+

二要素認証が有効で、RADIUS/TACACS+ サーバが二次認証タイプとして設定されている場合、ログインページに「二次パスワード」フィールドが表示されます。



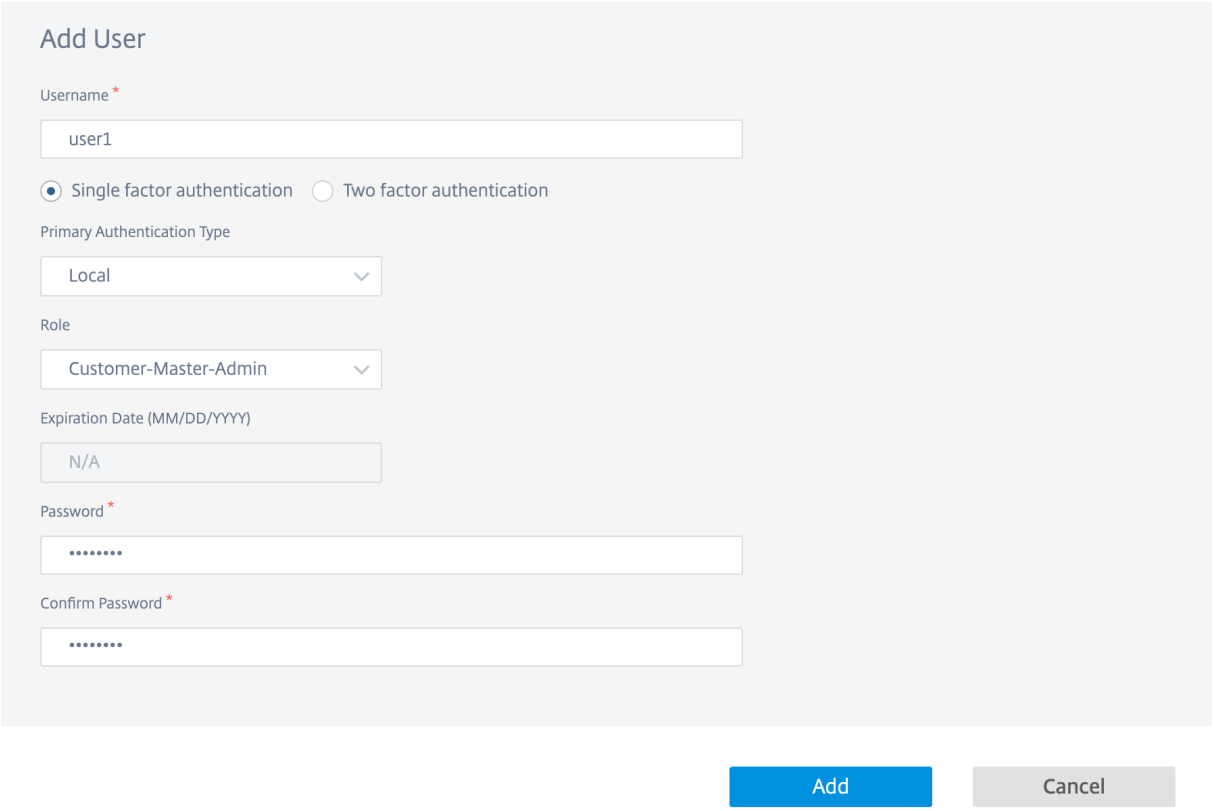
ユーザーの追加

[管理] > [ユーザー管理] に移動し、[**+** 新規] をクリックし、次の詳細を入力して [追加] をクリックします。

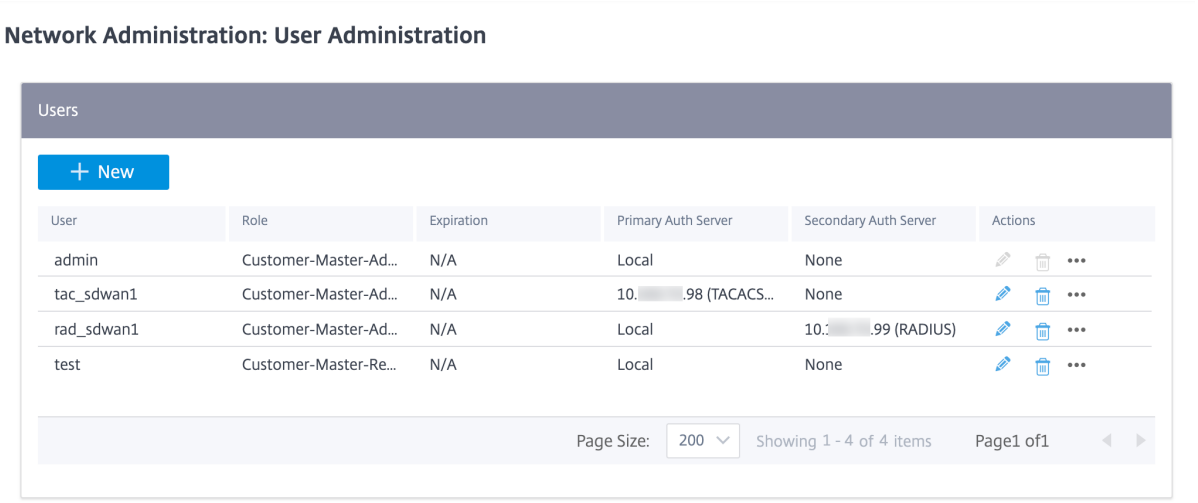
- ユーザー名を入力します。
- 単一要素認証: ユーザーのログインに一次認証のみを有効にします。
- 二要素認証: ユーザーのログインに一次認証と二次認証の両方を有効にします。詳細については、「リモート認証サーバー」を参照してください。
- 一次認証タイプ: ローカルまたはリモート認証サーバーの IP アドレスを選択します。
- 二次認証タイプ: リモート認証サーバーの IP アドレスを選択します。

> 注記
>
> 単一要素認証を選択した場合、「二次認証タイプ」フィールドは灰色表示されます。

- 役割: 使用可能な役割の一覧から役割を選択します。
- 顧客へのアクセスを拒否:(プロバイダーレベルのみで利用可能)。ユーザーを追加する際、プロバイダーは特定の顧客へのアクセスを拒否できます。
- 有効期限 **(MM/DD/YYYY)**: サポートユーザーが顧客情報にアクセスできる日付。デフォルトの有効期間は、ロールが割り当てられた日付から 2 週間です。
- パスワードを入力します。パスワードの長さは 8 ～128 文字でなければなりません。



アクション列を使用して、ユーザーロールの変更、パスワードの更新、認証タイプの編集を行うことができます。必要に応じてユーザーを削除することもできます。



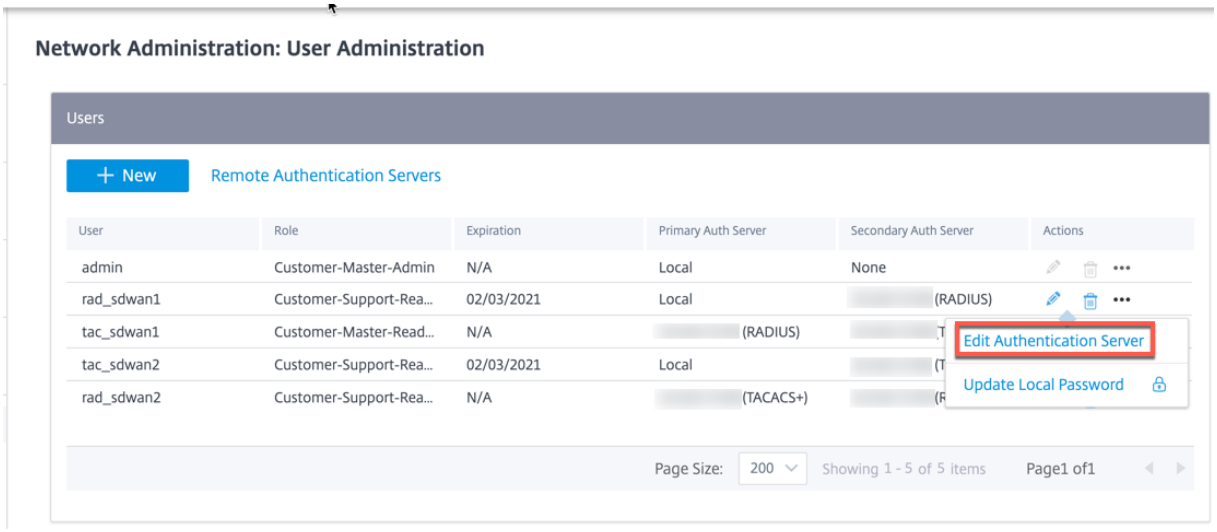
制限事項

オンプレミス向け Citrix SD-WAN Orchestrator は、同じプロバイダーでの異なる顧客のユーザー名の重複をサポートしていません。このアクションを実行すると、アカウント作成中にエラーというエラーメッセージが表示されます。

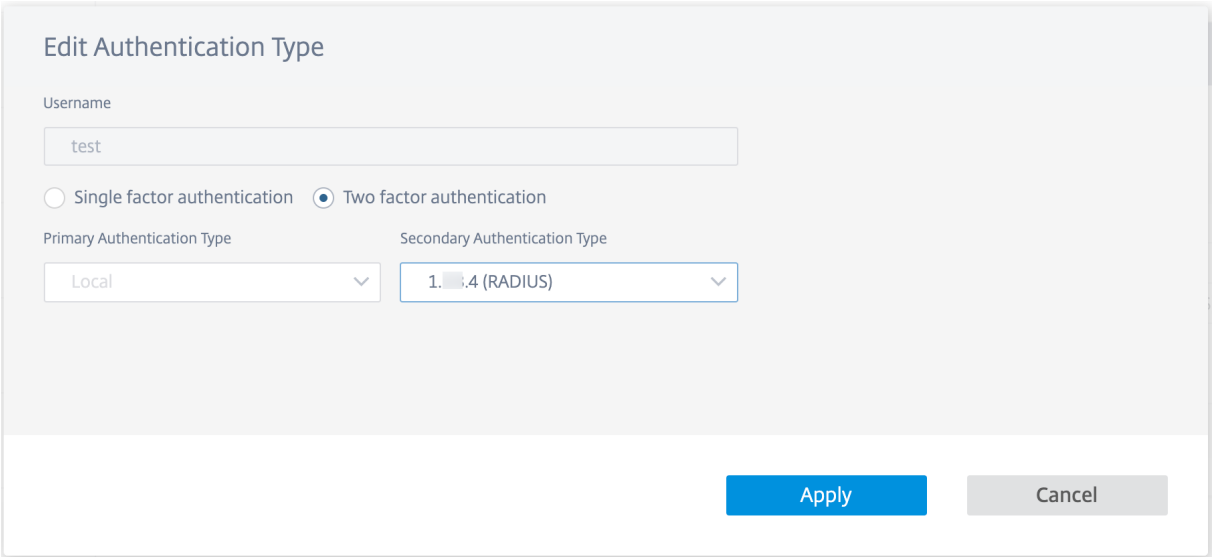
認証タイプを変更

ユーザーの認証タイプを 1 要素認証から 2 要素認証に、またはその逆に変更できます。

ユーザーの認証タイプを変更するには、「アクション」列で「…」をクリックし、「認証サーバーの編集」をクリックします。



現在 **1** 段階認証を選択している場合は、2 要素認証に切り替えることができます。「二要素認証」をクリックし、「二次認証タイプ」ドロップダウンリストからリモートサーバーを選択します。［適用］をクリックします。



現在 2 段階認証を選択している場合は、2 次認証タイプのみを変更するか、一要素認証に切り替えるかを選択できます。

単一要素認証に切り替えるには、「単一要素認証」をクリックします。[二次認証タイプ] ドロップダウンリストは無効になり、[一次認証タイプ] ドロップダウンリストのみが有効になります。

プライマリ認証タイプはユーザー作成時にのみ設定でき、後で編集することはできません。

パスワードの変更

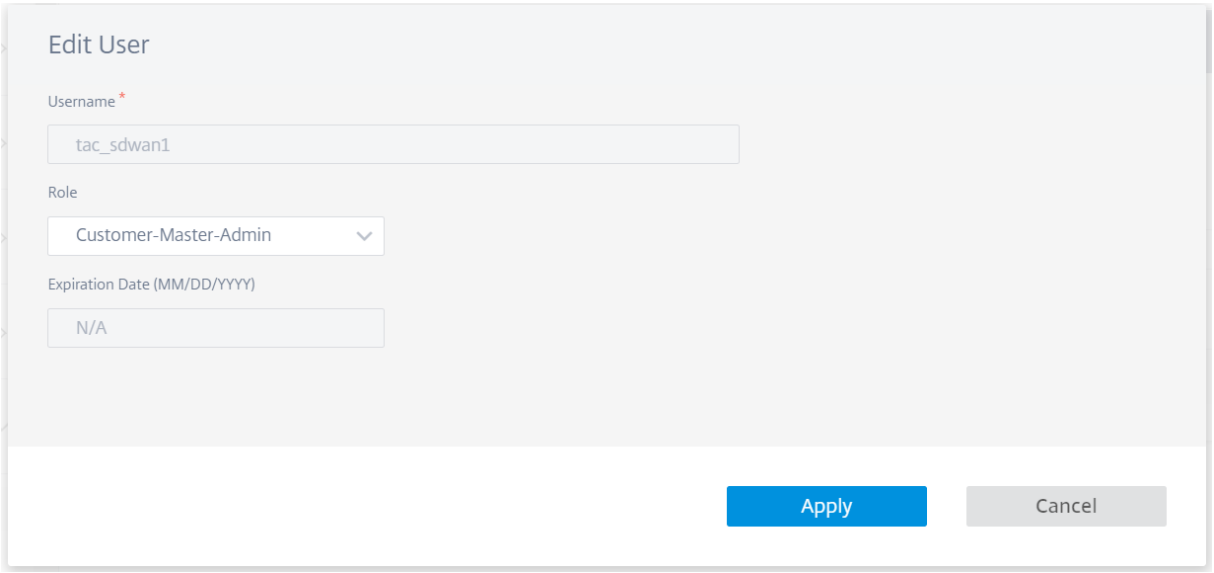
ローカルユーザーのパスワードを変更できます。ユーザーのパスワードを変更するには、「アクション」列で「…」をクリックし、「ローカルパスワードの更新」をクリックします。

> 注記
>
> パスワードを変更できるのはローカルユーザーのみです。リモートで認証されたユーザーの場合は、外部サーバーでパスワードを更新する必要があります。

ユーザーロールの変更

ユーザーロールを変更するには、** アクション列の編集アイコンをクリックします ** 。ロールを選択し、[適用] をクリックします。

> 注記
>
> デフォルトの管理者ユーザーのロールは編集できません。



ドメイン名

October 26, 2022

ドメイン名は、オンプレミス向け Citrix SD-WAN Orchestrator にアクセスするためにアドレスバーに使用されるバニティ URL です。ドメイン名を使用すると覚えやすくなり、会社のブランド名も使用できます。

ドメイン名を使用するには、ドメイン名をオンプレミス管理 IP アドレス用の Citrix SD-WAN Orchestrator にリンクする DNS レコードで構成されたローカル DNS サーバーがあることを確認してください。初期設定時にドメイン名が設定されていることを確認します。ドメイン名を設定すると、オンプレミス用 Citrix SD-WAN Orchestrator が再起動し、証明書が自動的に再生成されます。個々のアプライアンスには同じドメイン名を設定する必要があります。詳細については、SD-WAN アプライアンスでのオンプレミス SD-WAN Orchestrator 構成を参照してください。

ドメイン名の設定は必須ではありません。ドメイン名がなく、IP アドレス解決に DNS サーバーを使用したい場合は、次の 3 つの FQDN について、オンプレミス IP 用の Citrix SD-WAN Orchestrator を指す DNS レコードを構成します。

- sdwanzt.citrixnetworkapi.net
- download.citrixnetworkapi.net
- sdwan-home.citrixnetworkapi.net

たとえば、オンプレミスドメイン用の Citrix SD-WAN Orchestrator が **citrix.com** として構成されている場合、次の FQDN 用の DNS レコードと、オンプレミスの IP アドレス用の Citrix SD-WAN Orchestrator を DNS サーバに作成する必要があります。

- download.citrix.com
- sdwanzt.citrix.com

- sdwan-home.citrix.com

高度な構成では、次のようになります。

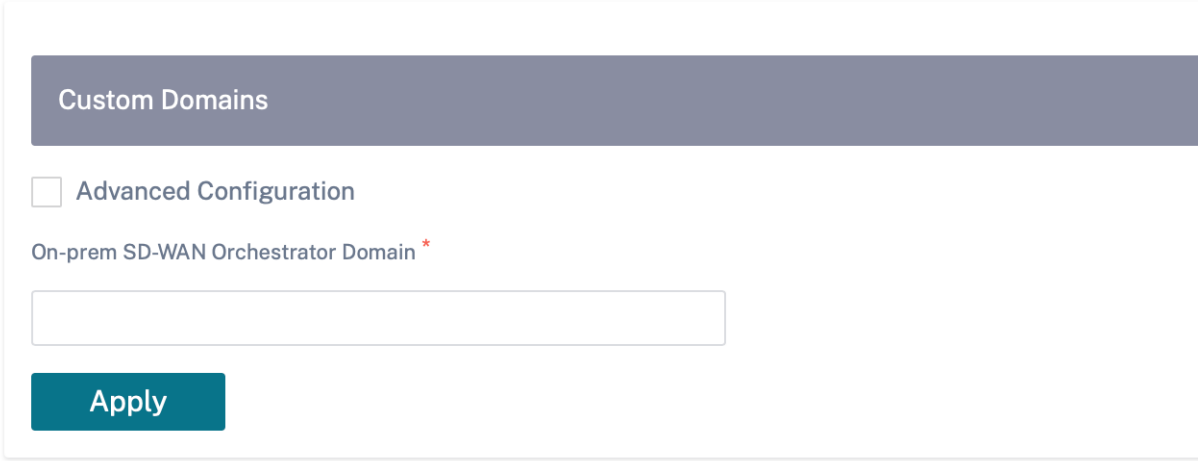
例：オンプレミス用 Citrix SD-WAN **Orchestrator** ドメインが **citrix.com** として構成されている場合、**** ダウンロード管理サービスドメインは **download.citrix.com** として構成され、**** 統計管理サービスドメインは統計として構成されます。**citrix.com** の場合は、以下の FQDN と対応する IP アドレスの DNS レコードを DNS サーバーに作成する必要があります。

- download.citrix.com
- sdwanzt.citrix.com
- statistics.citrix.com

既存の構成のドメイン名を構成または変更すると、Citrix SD-WAN Orchestrator for オンプレミスおよびアプライアンス接続に影響します。証明書認証プロセスを手動で実行するか 、サイトゼロタッチ展開設定オプションを使用する必要があります 。

> 注:
>
> プロバイダー管理の設定では、プロバイダー管理者のみがドメイン名関連情報を編集できます。

ドメイン名を設定するには、ネットワークレベルで [管理] **>** [ドメイン名] に移動し、オンプレミスドメイン名用の Citrix SD-WAN Orchestrator を指定します。



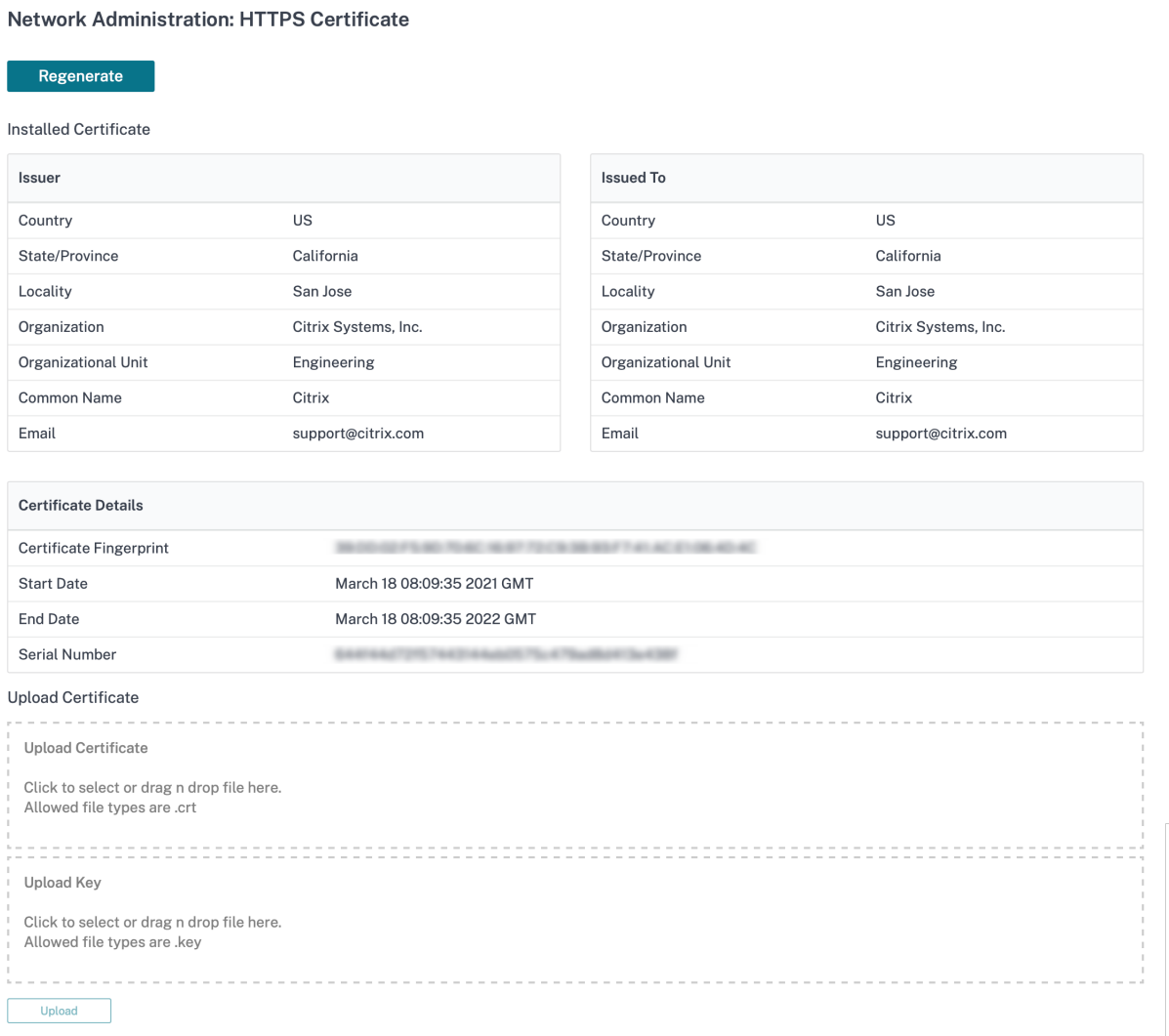
HTTPS 証明書

October 26, 2022

オンプレミス用 Citrix SD-WAN Orchestrator への安全な管理 HTTPS 接続を確立するには、HTTPS 証明書が必要です。Citrix SD-WAN Orchestrator for オンプレミス GUI で利用可能なデフォルトの HTTPS 証明書を使用するか、OpenSSL などの他のフレームワークや信頼できる機関から生成されたカスタム HTTPS 証明書をアップロードできます。カスタム HTTPS 証明書を使用すると、証明書に関連するセキュリティやその他のサブジェクトパラメータを制御できます。

デフォルトの証明書を表示するには、[管理] **> [HTTPS** 証明書] に移動します。

> 注:
>
> プロバイダー管理の設定では、プロバイダー管理者のみが HTTPS 証明書の再生成とアップロードにアクセスできます。



[インストールされた証明書（Installed Certificate）] セクションには、アプライアンスにインストールされている証明書の概要が表示されます。アプライアンスは、この証明書を使用してネットワーク内で自身を識別します。

発行先セクションには、証明書の発行先に関する詳細が表示されます。証明書はアプライアンス名にバインドされて

いるため、証明書の共通名はアプライアンスの名前と一致します。[**Issuer**] セクションには、証明書に署名した認証局の詳細が表示されます。証明書の詳細には、証明書のフィンガープリント、シリアル番号、および証明書の有効期間が含まれます。

証明書を再生成するには、[管理**] > [HTTPS** 証明書] に移動し、[再作成] をクリックします。

> 注**:**
>
> 証明書を再生成すると、接続されている既存の HTTPS セッションがすべて切断され、HTTPS サーバが再起動されます。証明書が正常に再生成されると、GUI は自動的に更新されます。

HTTPS 証明書は、OpenSSL などの他のフレームワークまたは信頼できる機関から生成し、オンプレミス向け Citrix SD-WAN Orchestrator にアップロードできます。サポートされている証明書形式は.crt で、サポートされているキー形式は.key です。

カスタム HTTPS 証明書をアップロードするには、[アップロード] をクリックするか、証明書とキーファイルを [証明書のアップロード] ボックスと [キーのアップロード] ボックスにそれぞれドラッグします。アップロードが成功すると、GUI は自動的に更新されます。

ディスク容量管理

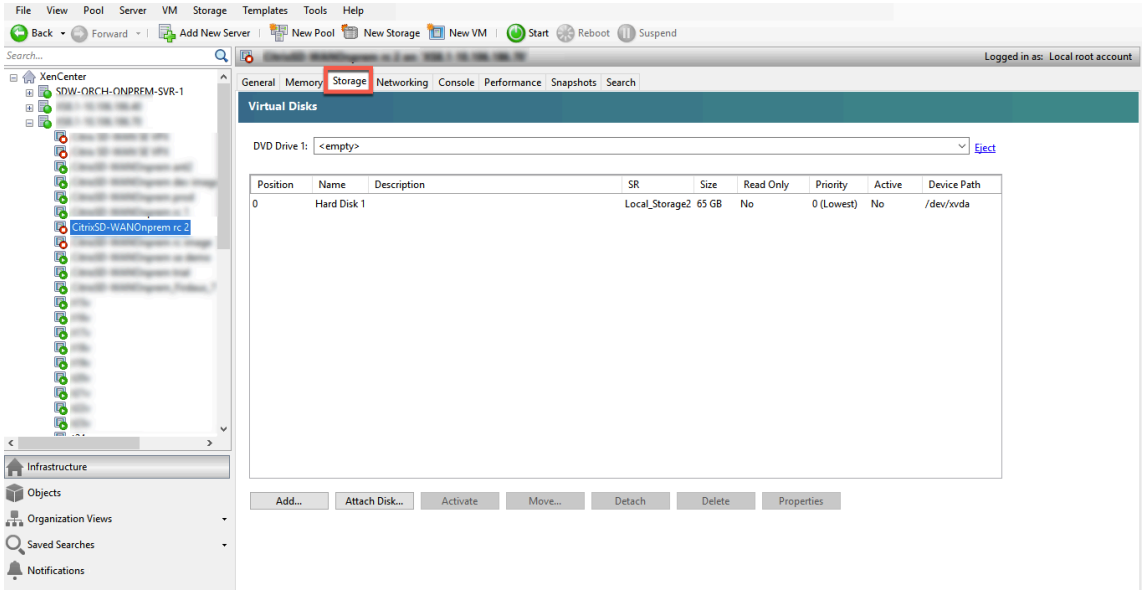
October 26, 2022

オンプレミス用 Citrix SD-WAN Orchestrator に割り当てられるディスク容量を増やすことができます。

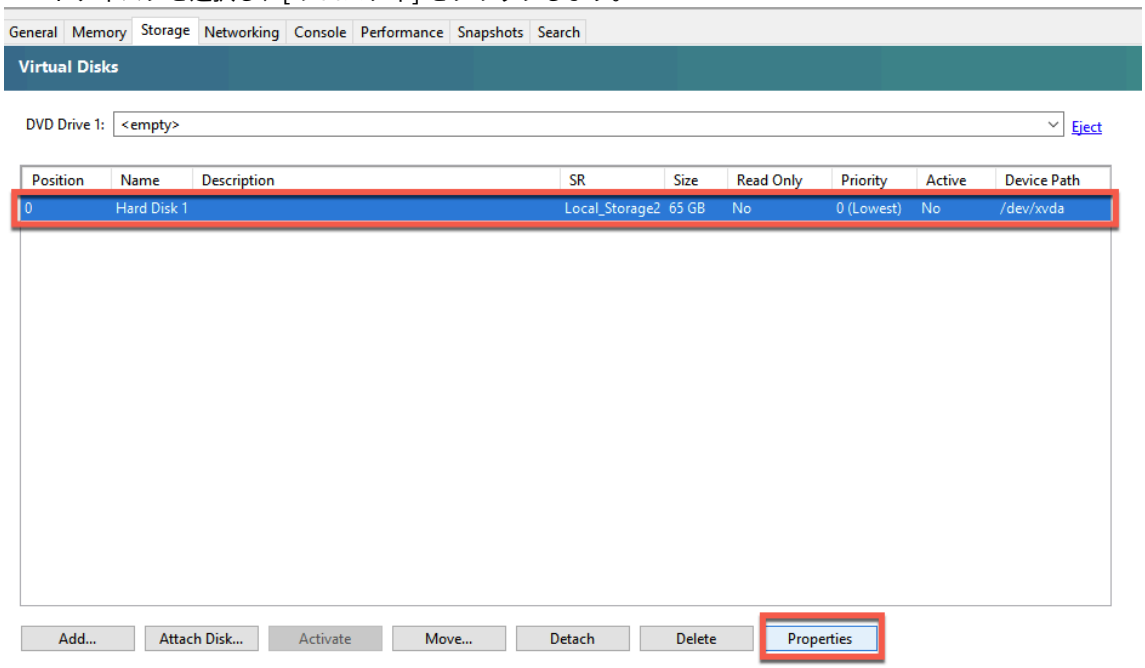
Citrix Hypervisor のディスク容量を増やしてください

Citrix Hypervisor のディスク容量を増やすため。

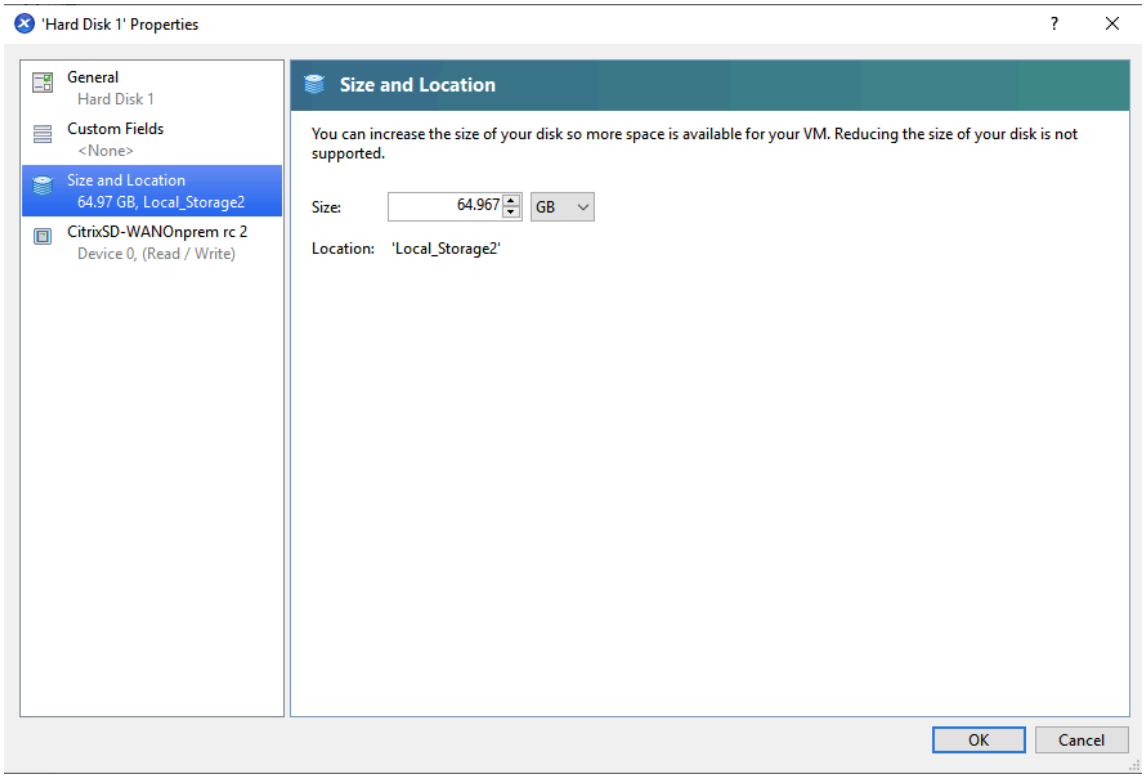
1. ハイパーバイザーから仮想マシン (VM) をシャットダウンします。
2. 仮想マシンを選択し、[ストレージ] タブをクリックします。



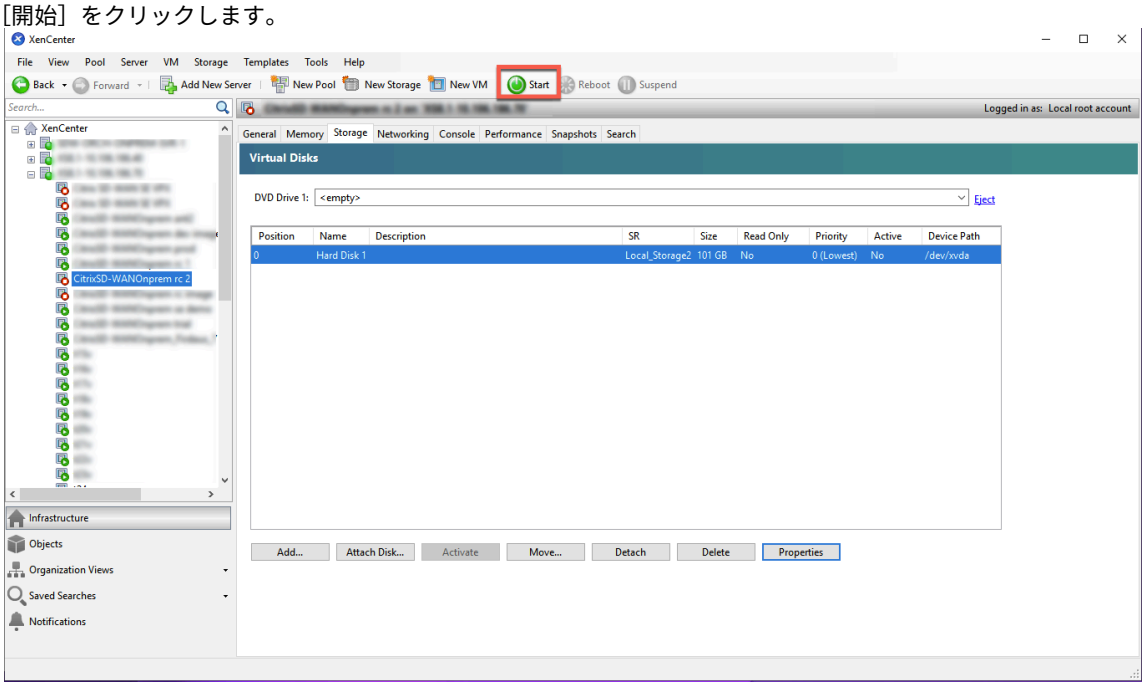
3. ハードディスクを選択し、[プロパティ] をクリックします。



4. [サイズと場所] オプションをクリックし、ディスク容量のサイズを更新します。[**OK**] をクリックします。



5. [開始] をクリックします。

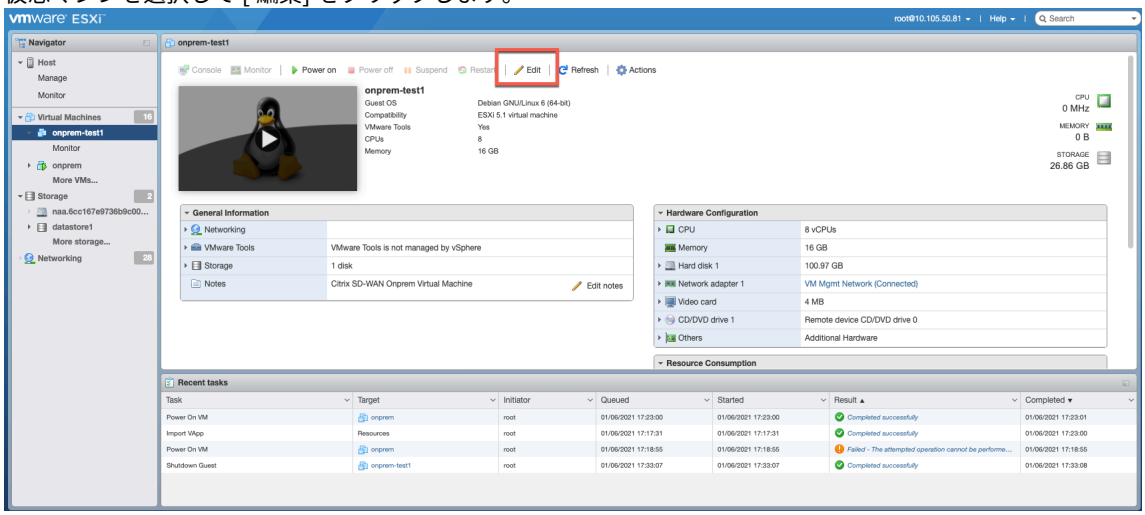


ESXi サーバのディスク容量を増やす

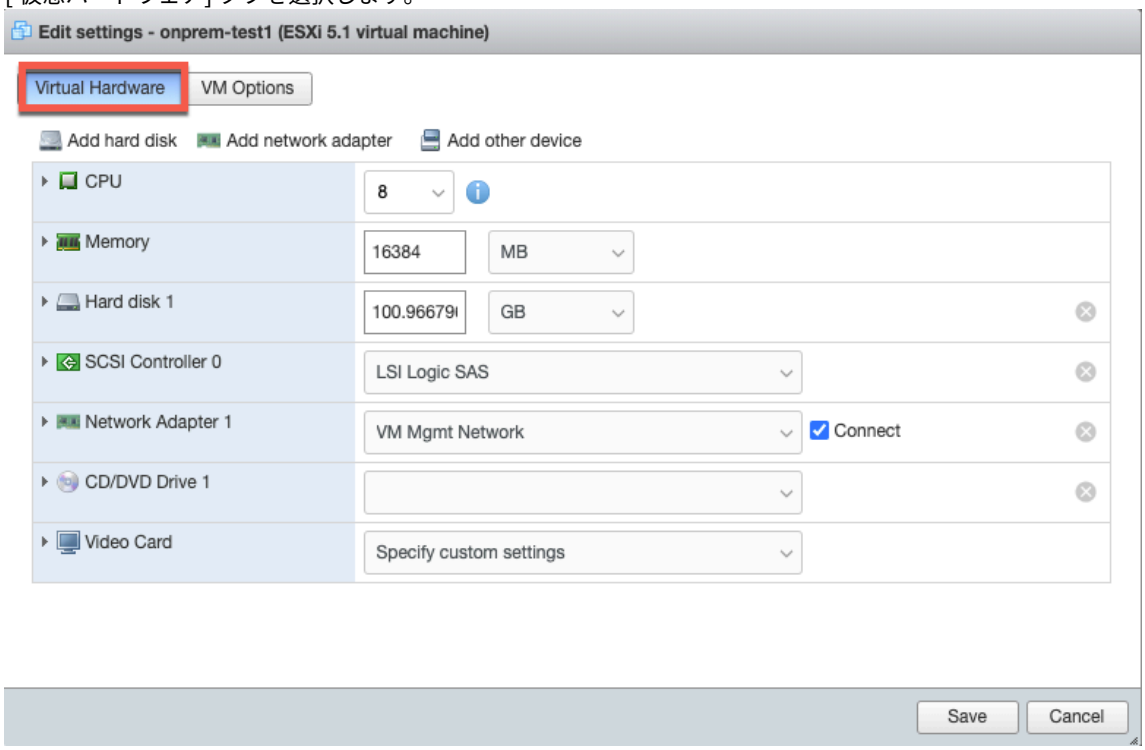
ESXi サーバのディスク容量を増やすため。

1. ハイパーバイザーから仮想マシン (VM) をシャットダウンします。

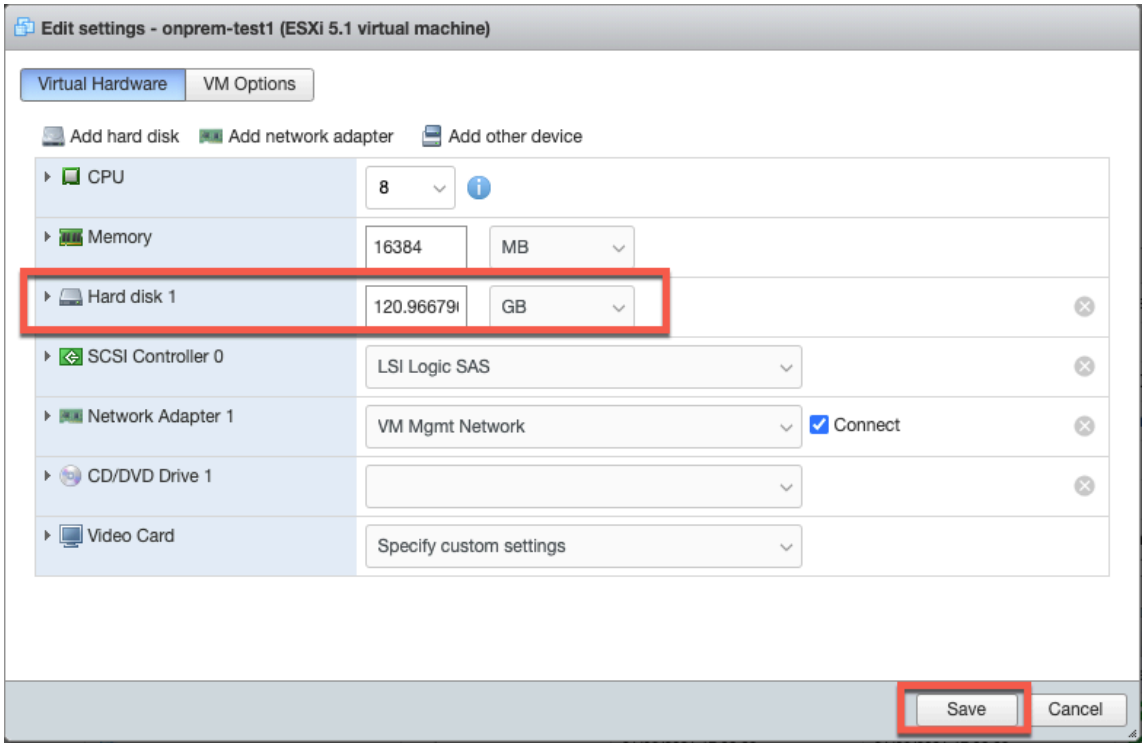
2. 仮想マシンを選択して [編集] をクリックします。



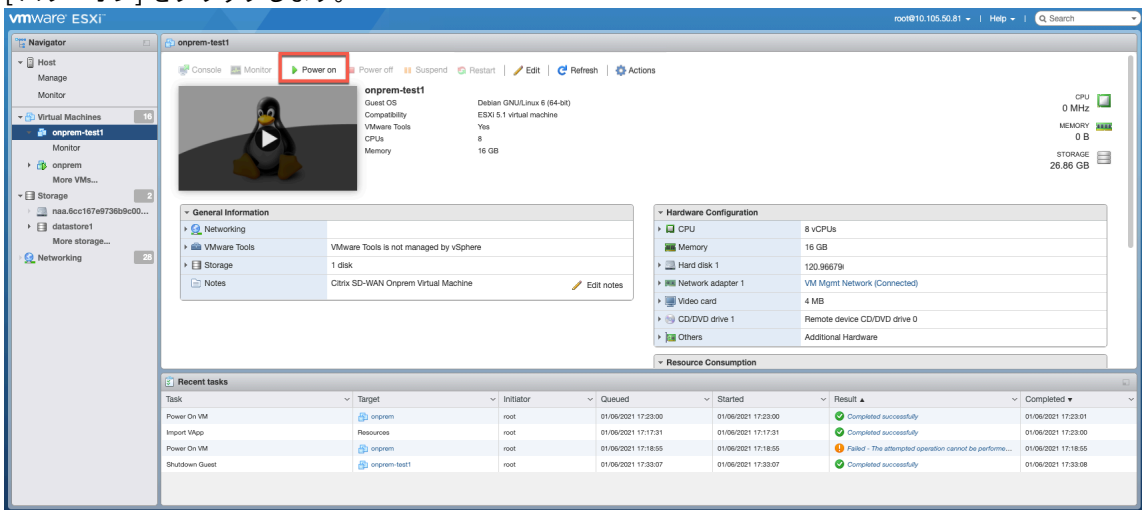
3. [仮想ハードウェア] タブを選択します。



4. [ハードディスク] フィールドのハードディスク容量を増やし、[保存] をクリックします。



5. [パワーオン] をクリックします。



該当する **Citrix SD-WAN** アプライアンスを交換してください

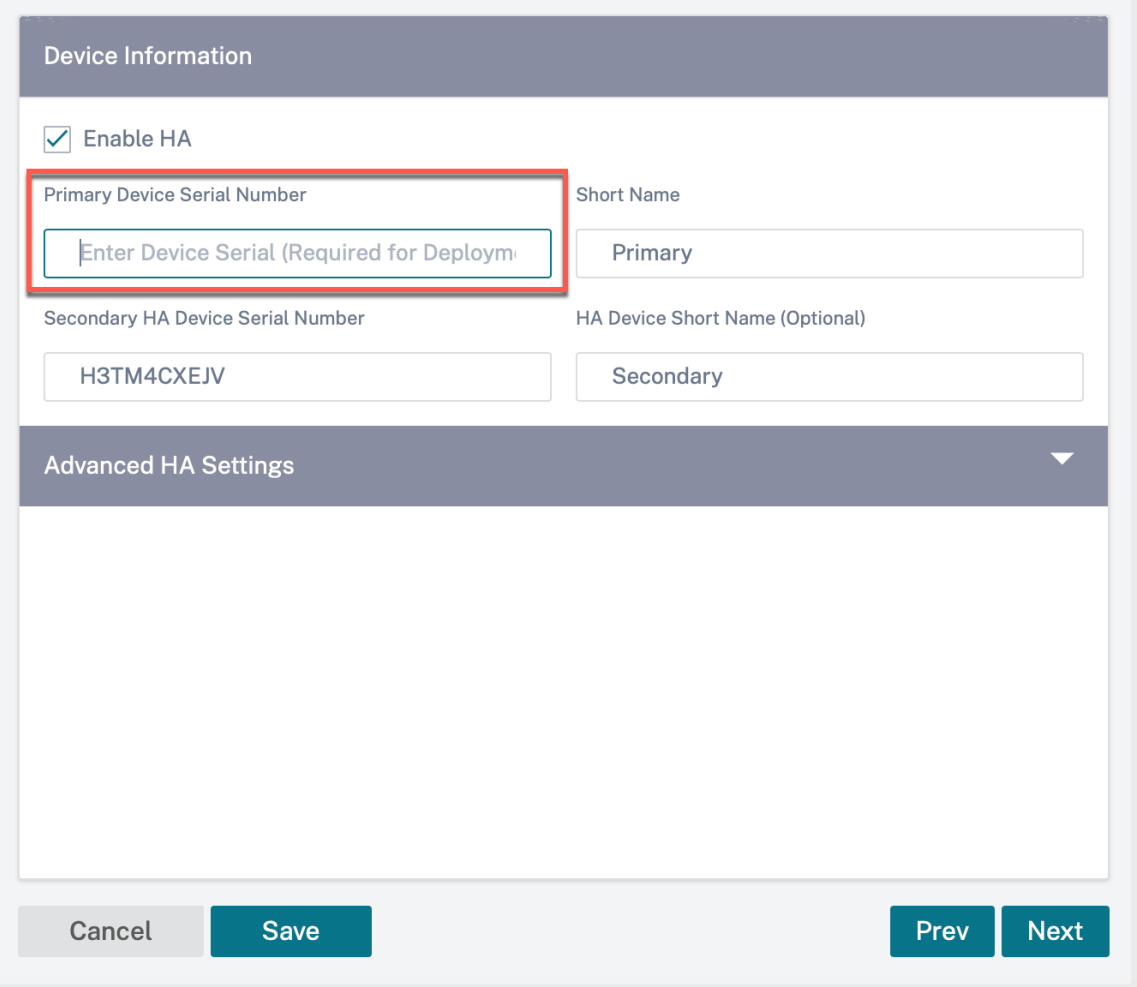
October 26, 2022

オンプレミス用 Citrix SD-WAN Orchestrator で該当するアプライアンスを交換するには:

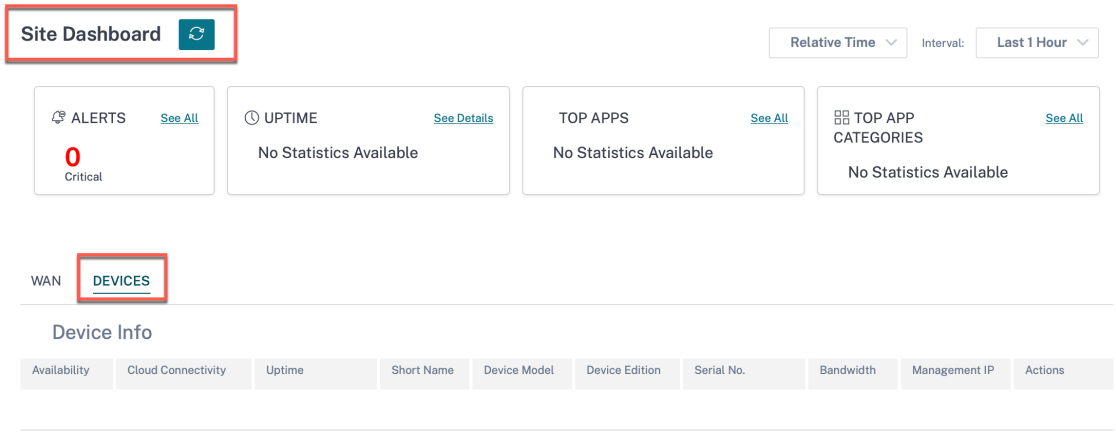
1. オンプレミス用 Citrix SD-WAN Orchestrator にログインし、影響を受けるサイトを選択します。サイトレベルで、[構成] > [サイト構成] > [デバイス情報] に移動し、[プライマリデバイスシリアル番号] フィール

ドからシリアル番号を削除します。［保存］をクリックします。

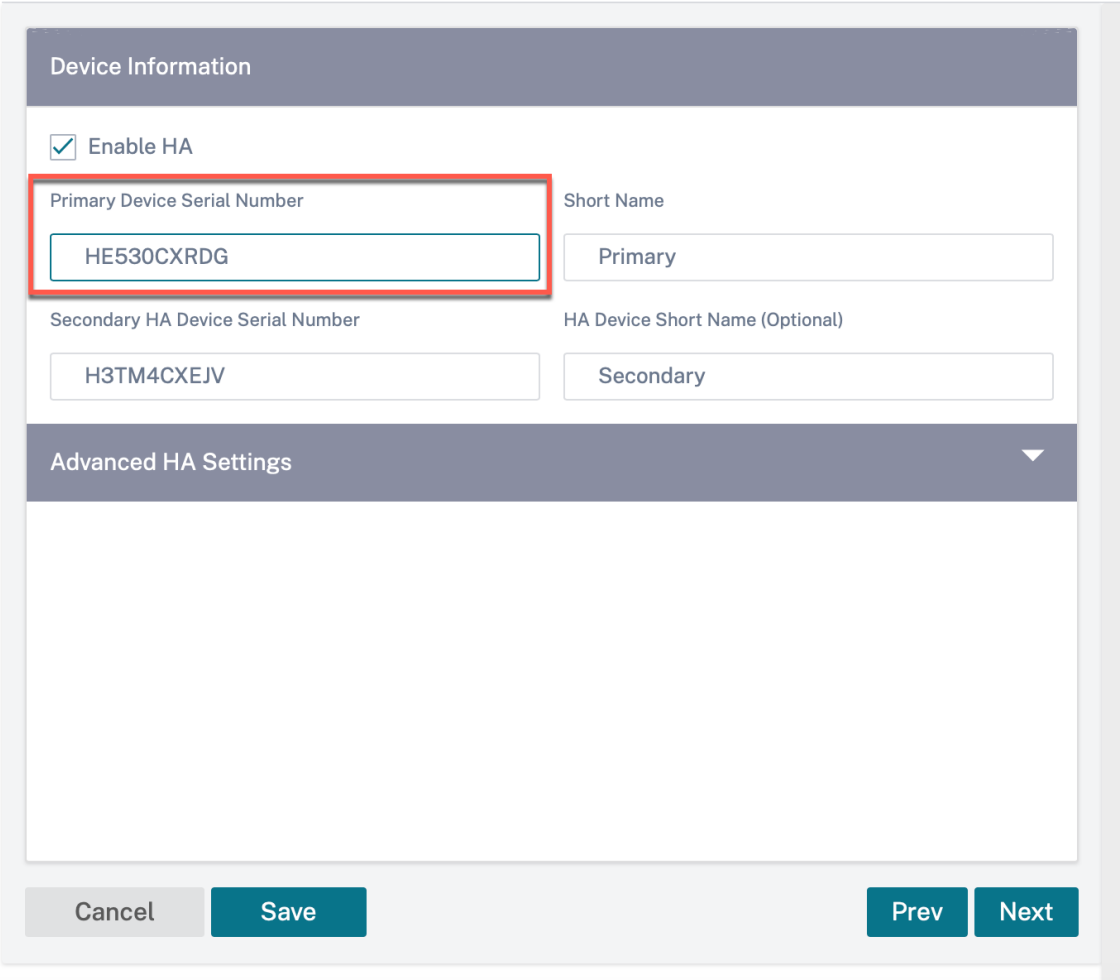
> 注:
>
> オンプレミス向け Citrix SD-WAN Orchestrator を介してアプライアンスにまだアクセスできる場合、アプライアンスは「工場出荷時設定にリセット」状態になります。



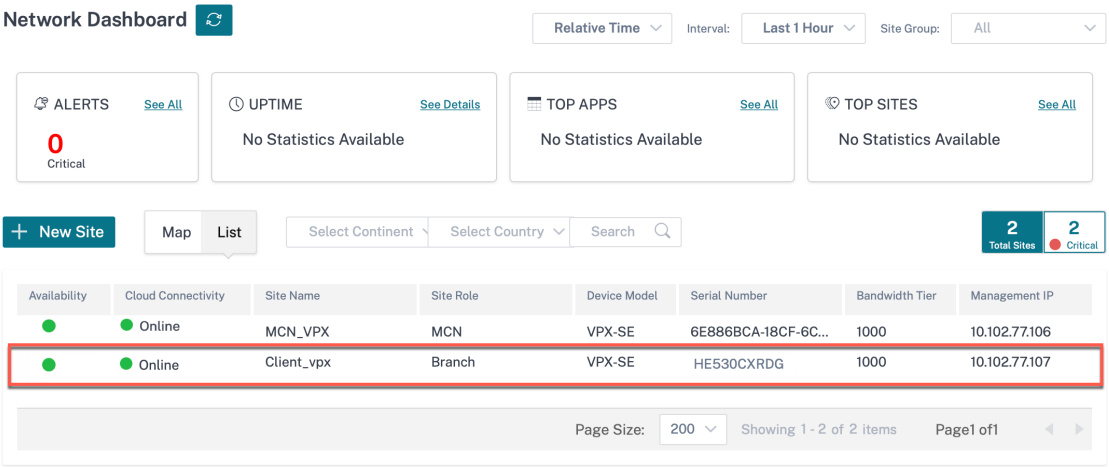
2. ダッシュボード > デバイスに移動して、影響を受けるアプライアンスがリストから削除されていることを確認します。



3. 該当するアプライアンスの電源とケーブルの設定を書き留めてから、アプライアンスをラックから取り外します。
4. 新しいアプライアンスをラックにマウントし、該当するアプライアンスの電源とケーブル接続をやり直します。
5. オンプレミス UI 向け Citrix SD-WAN Orchestrator のサイトレベルで、［構成］>［サイト構成］**>**［デバイスの詳細］に移動します。プライマリデバイスシリアル番号フィールドに新しいアプライアンスのシリアル番号を追加します。［保存］をクリックします。

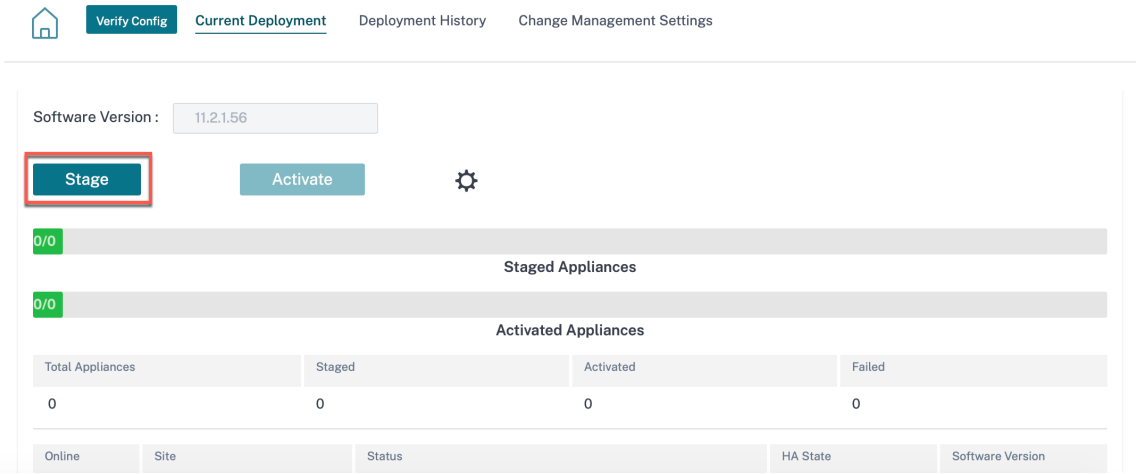


6. ゼロタッチ導入を設定します。詳しくは、「ゼロタッチ展開」を参照してください。
7. アプライアンスがサイトダッシュボードのクラウド接続を更新するまで数分かかります。



8. ネットワークレベルで、[構成] **>** [ネットワーク構成ホーム] に移動し、[構成/ソフトウェアの展開] をクリックします。

9. ステージをクリックします。



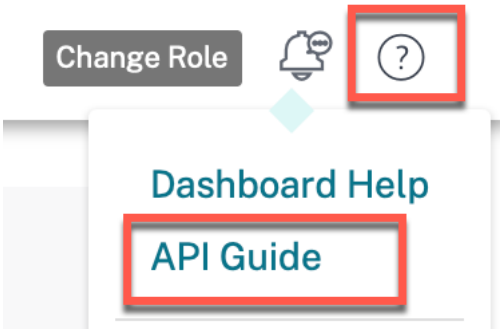
10. ステージングが完了したら、[**Activate**] をクリックします。
11. サイトダッシュボードに移動し、アプライアンスが正常にアクティブ化されていることを確認します。

オンプレミス用 **Citrix SD-WAN Orchestrator** の **API** ガイド

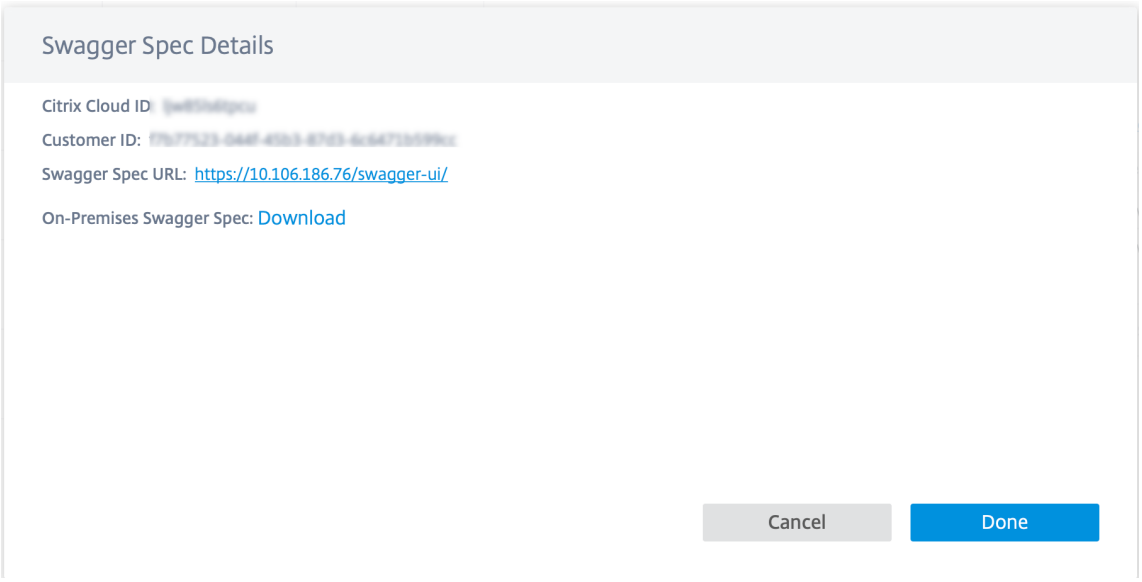
October 26, 2022

Swagger UI でオンプレミス用 Citrix SD-WAN Orchestrator API ガイドにアクセスするには:

1. オンプレミス用 Citrix SD-WAN Orchestrator にログインし、「**?**」をクリックします UI の右上隅にある [**API** ガイド] をクリックします。



Swagger スペックの詳細が表示されます。



2. Swagger 仕様の URL をクリックして、API ガイドにアクセスします。

curl によるオンプレミス API 用 Citrix SD-WAN Orchestrator

前提条件

- クラウドログイン
- ローカルログイン

curl を使用して Citrix オンプレミス Orchestrator API を使用するには、次の手順を実行します。

1. クラウドログイン: 新しい XVA の場合は、まずクラウドにログインする必要があります。

```
curl -k -X POST -H "Content-Type: application/json "https://<
    onprem-orchestrator-ip>/policy/v1/onprem/cloudLogon  - data '{
 "clientId":"<clientId>","clientSecret":"<clientSecret> ","ccId":"
    <ccid>", "pop": "<popName>" }
 '
```

`clientId`、`clientSecret`、および`ccId`は IAM ページから入手できます。

> 注:
>
> クラウドログオンを試みる前に、顧客アカウントがクラウドですでに作成されていることを確認してください。

2. ローカルログイン: 次に、ローカルログインを実行して認証トークンを取得します。

```
curl -k -X POST -H "Content-Type: application/json" https://<
    onprem-orchestrator-ip>/onpm/v1/logon --data '{
 "username":"admin","password":"<passwordField>" }
 '
```


これにより、** 応答としてトークンと **customerID** が返されます ** 。CustomerID は固定されたままで、他の API 呼び出しで必要です。後で使用できるように **customerID** を保存します。トークンは 1 時間有効です。後で、新しいログインを実行する必要があります。

例: ** 認証トークンと **CustomerID** を使用して ** 、他の Citrix オンプレミス API を起動します。

```
curl -k -X GET -H "authorization:CWSAuth bearer= <token> " -H "
    Content-Type: application/json"https://<onprem-orchestrator-ip
    >/onpm/v1/scope/<customerId>/globalSettings/ntpSettings
```

Orchestrator 管理

October 26, 2022

このセクションでは、オンプレミスプラットフォーム向け Citrix SD-WAN Orchestrator で実行できる管理アクティビティについて説明します。

ソフトウェア

ネットワーク内のすべてのアプライアンスに必要な、オンプレミス用 Citrix SD-WAN Orchestrator に保存されている Citrix SD-WAN アプライアンスソフトウェアバージョンをダウンロードできます。保存されているソフトウェアを使用して、オンプレミス向け Citrix SD-WAN Orchestrator ソフトウェアを最新バージョンにアップグレードします。

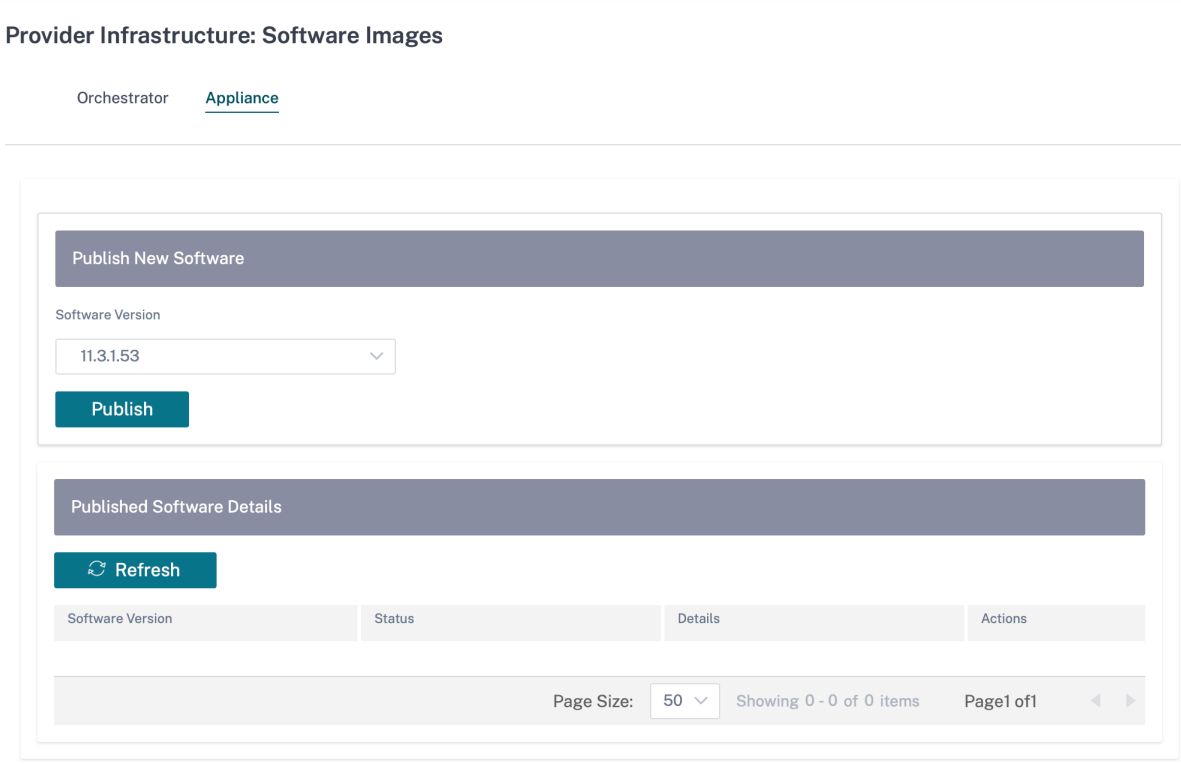
> 注:
>
> プロバイダー管理セットアップは、オンプレミス 10.3 リリース用 Citrix SD-WAN Orchestrator から導入されました。オンプレミス 10.3 リリースの Citrix SD-WAN Orchestrator よりも低いソフトウェアリリースへのダウングレードはサポートされていません。

ソフトウェアを公開

プロバイダー管理のセットアップでは、Citrix SD-WAN Orchestrator for On-Premises を使用すると、プロバイダー管理者はネットワーク内のすべてのアプライアンスに必要な Citrix SD-WAN アプライアンスソフトウェアバージョンをダウンロードできます。プロバイダー管理者は、ダウンロードしたソフトウェアバージョンを公開できます。公開されたソフトウェアは、オンプレミス向け Citrix SD-WAN Orchestrator にダウンロードされ、保存されます。顧客管理者は、公開されたソフトウェアを Citrix SD-WAN Orchestrator for On-Premises によって管理されるすべてのアプライアンスに展開できます。

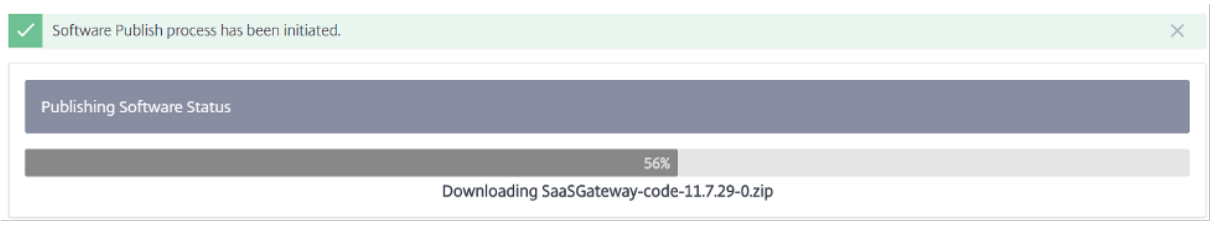
顧客管理のセットアップでは、顧客管理者はネットワーク内のすべてのアプライアンスに必要な Citrix SD-WAN アプライアンスソフトウェアバージョンをダウンロードできます。オンプレミス向け Citrix SD-WAN Orchestrator でソフトウェアを公開し、ソフトウェアをすべてのアプライアンスに展開できます。

ソフトウェアを公開するには、インフラストラクチャ **> Orchestrator** 管理 **>** ソフトウェアイメージ **>** アプライアンスに移動します。

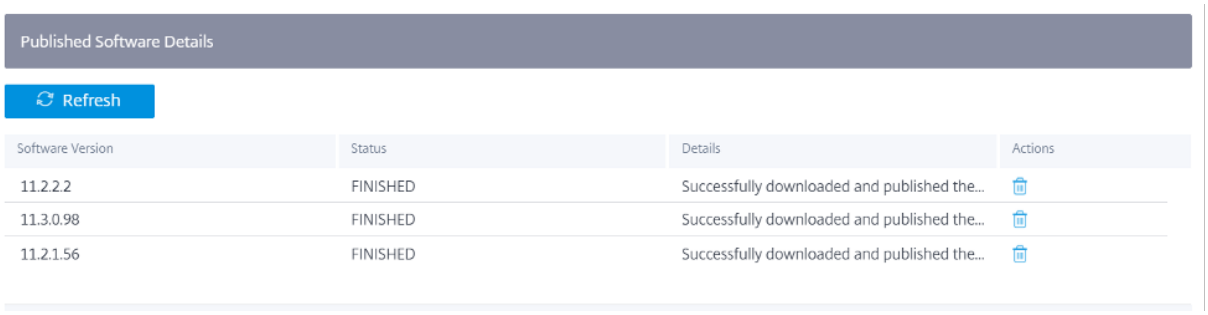


現在の Citrix SD-WAN Orchestrator for On-Premises でサポートされているソフトウェアバージョンのリストから、公開するソフトウェアバージョンを選択できます。リストにない新しいソフトウェアバージョンについては、新しいソフトウェアバージョンをサポートする最新の Citrix SD-WAN Orchestrator for On-Premises リリースにアップグレードしてください。オンプレミス用 Citrix SD-WAN Orchestrator のアップグレードについては、「ソフトウェアアップグレード」を参照してください。

オンプレミス向け Citrix SD-WAN Orchestrator は、すべてのプラットフォーム用に選択したバージョンの Citrix SD-WAN ソフトウェアをダウンロードします。プログレスバーには、公開プロセスの進行状況が表示されます。



公開されているソフトウェアバージョンが [公開ソフトウェアの詳細] に表示されます。オンプレミス向け Citrix SD-WAN Orchestrator は、いつでも最大 3 つの公開済みソフトウェアバージョンを保存できます。別のソフトウェアバージョンを公開する場合は、公開プロセスを開始する前に、利用可能な 3 つのバージョンのうちの 1 つを削除してください。



公開が成功したら、ネットワーク設定ページからネットワーク上のすべてのアプライアンスにソフトウェアをデプロイ、ステージング、アクティベートできます。詳細については、「ネットワーク構成」を参照してください。正常に展開するには、すべてのアプライアンスがオンプレミス向け Citrix SD-WAN Orchestrator に接続されていることを確認してください。詳細については、「Citrix SD-WAN アプライアンスとの接続」を参照してください。

ソフトウェアの更新

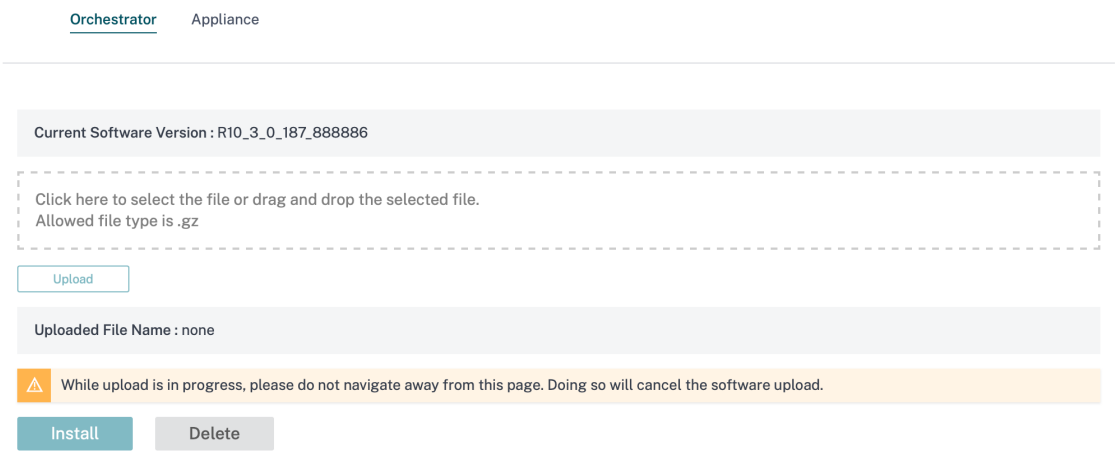
プロバイダーが管理するセットアップでは、プロバイダー管理者のみがオンプレミス向け Citrix SD-WAN Orchestrator ソフトウェアを最新バージョンにアップグレードできます。

顧客管理のセットアップでは、顧客管理者はオンプレミス向け Citrix SD-WAN Orchestrator ソフトウェアを最新バージョンにアップグレードできます。

> 注
>
> - オンプレミス向け適切な Citrix SD-WAN Orchestrator ソフトウェアパッケージをローカルコンピューターにダウンロードします。このパッケージはダウンロードページからダウンロードできます 。
> - Citrix では、ハイパーバイザー内の仮想マシンのスナップショットを作成することを推奨しています。また、SD-WAN 構成はアップグレードの前にダウンロードされます。
> - Citrix では、仮想マシンと SD-WAN 構成のスナップショットを定期的に作成することも推奨しています。

以下の手順を実行して、オンプレミス向け Citrix SD-WAN Orchestrator の新しいバージョンをアップロードしてインストールします。

1. オンプレミス用 Citrix SD-WAN Orchestrator UI で、［インフラストラクチャ］**>**［**Orchestrator** 管理］**>**［ソフトウェアイメージ］**>**［**Orchestrator**］に移動します。
2. ボックス内をクリックし、ローカルシステムにダウンロードして保存した ctx-onprem-1（最新の日付）.tar.gz バイナリファイルを選択します。



3. [アップロード] をクリックして、選択したソフトウェアパッケージを現在の Citrix SD-WAN Orchestrator for オンプレミス仮想マシンにアップロードします。
4. アップロードが完了したら、[インストール] をクリックします。
5. 確認を求められたら、[インストール] をクリックします。

管理設定

> 注**:**
>
> プロバイダーが管理するセットアップでは、プロバイダー管理者のみが [インフラストラクチャ] **>** [**Orchestrator** 管理] **>** [管理設定] で構成を編集できます。

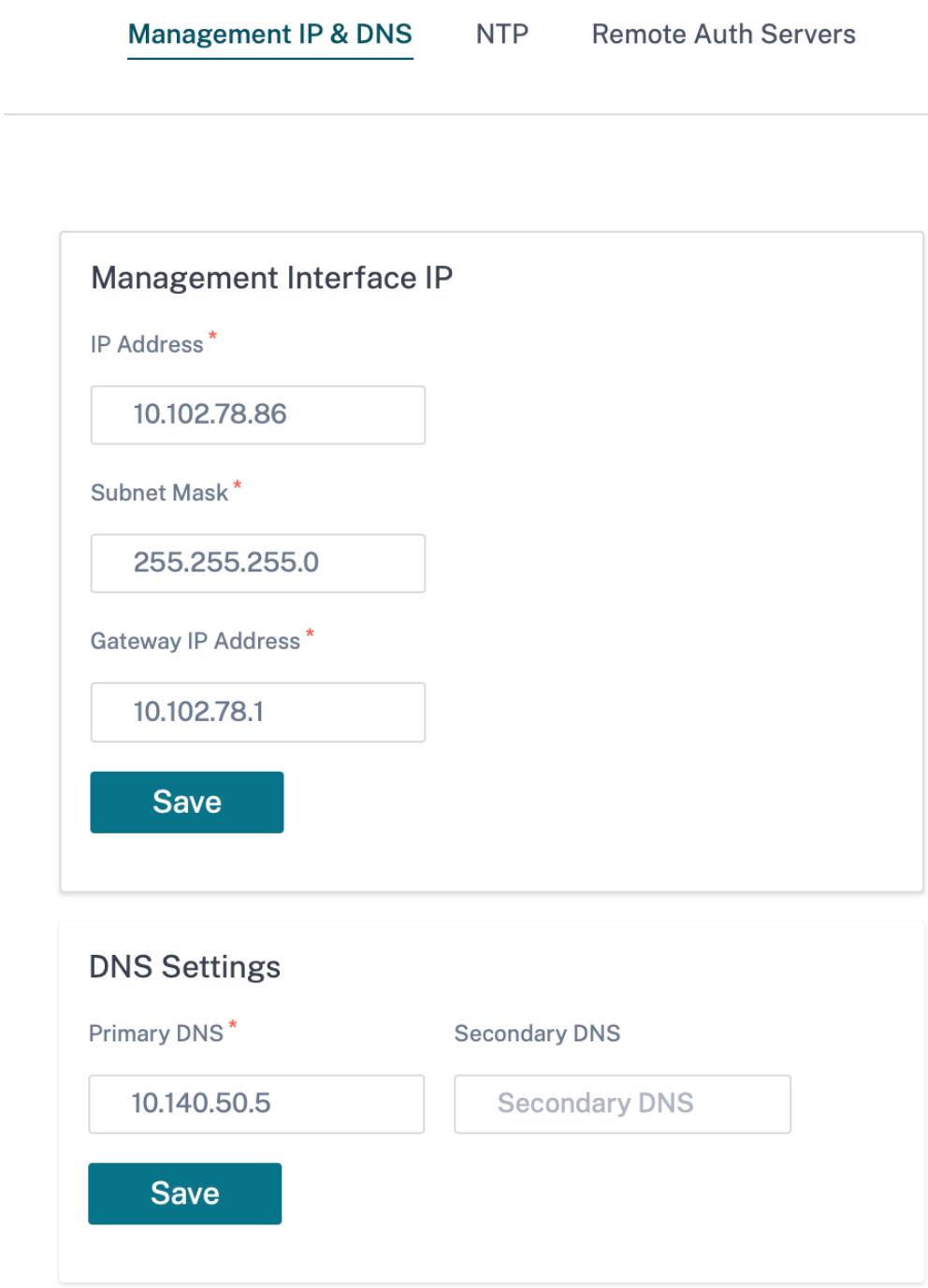
管理 **IP** と **DNS**

オンプレミス仮想マシン（VM）用 Citrix SD-WAN Orchestrator を展開し、管理 IP を手動または DHCP を介して構成したら、オンプレミス用 Citrix SD-WAN Orchestrator for オンプレミス GUI を使用して管理 **IP** と **DNS** 設定を変更できます。Citrix SD-WAN Orchestrator for オンプレミススタックの再起動には約 3 分かかります。管理 IP アドレスが変更されると、SSH 接続が再確立されます。

管理 IP および DNS 設定を構成または変更するには、ネットワークレベルで [インフラストラクチャ] **>** [**Orchestrator** 管理] **>** [管理設定] **>** [管理 **IP** と **DNS**] に移動します。

次の詳細を入力します。

- **IP** アドレス: オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator の IP アドレス。
- ゲートウェイ **IP** アドレス: オンプレミス向け Citrix SD-WAN Orchestrator が外部ネットワークとの通信に使用するゲートウェイ IP アドレス。
- サブネットマスク: オンプレミス用 Citrix SD-WAN Orchestrator が使用できるネットワークを定義するサブネットマスク。
- プライマリ **DNS**: オンプレミス用 Citrix SD-WAN Orchestrator からのすべての DNS 要求の転送先となるプライマリ DNS サーバーの IP アドレス。
- セカンダリ **DNS**: プライマリ DNS サーバが使用できない場合に DNS 要求を解決するためのセカンダリ DNS サーバの IP アドレス。

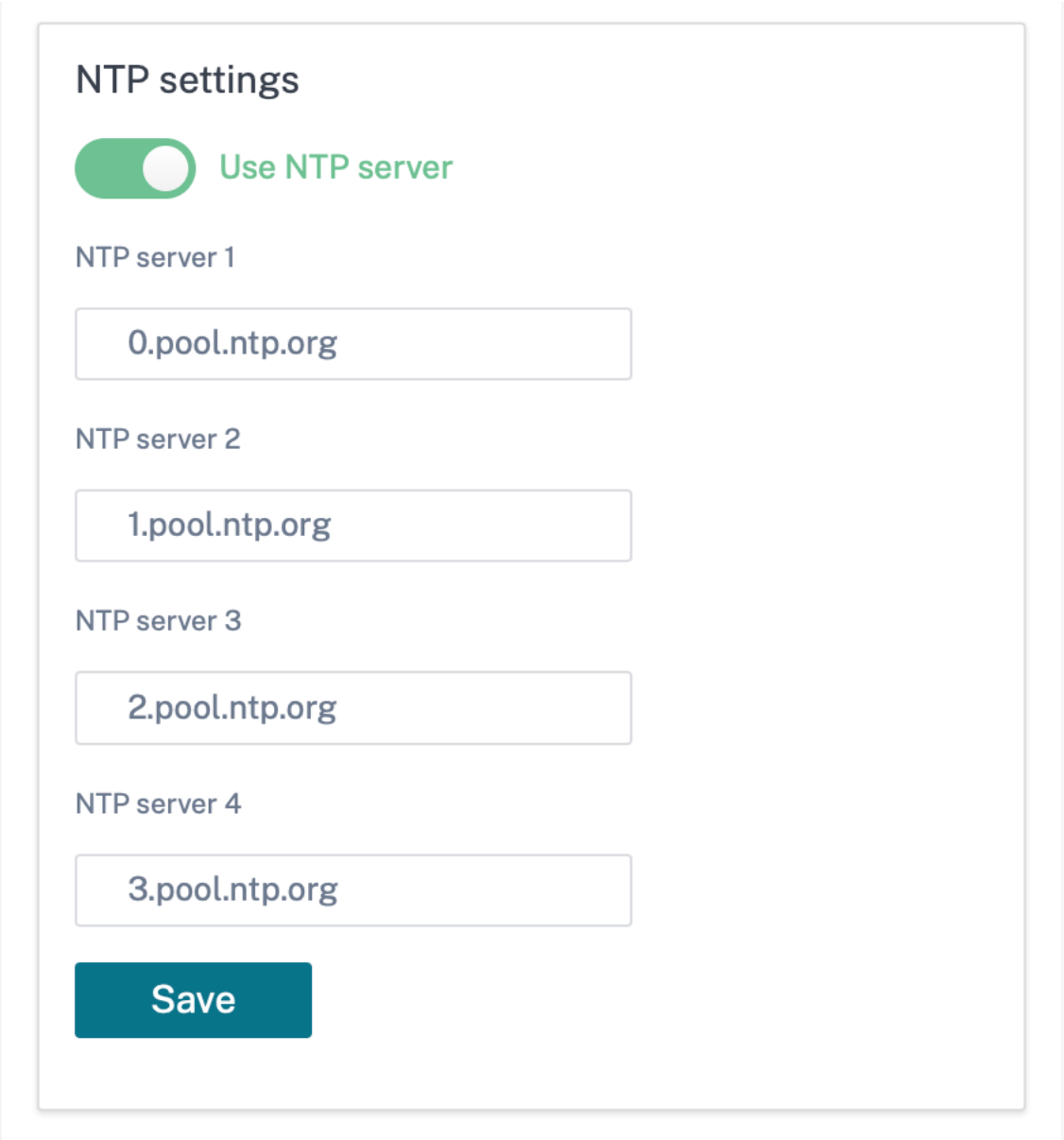


NTP 設定

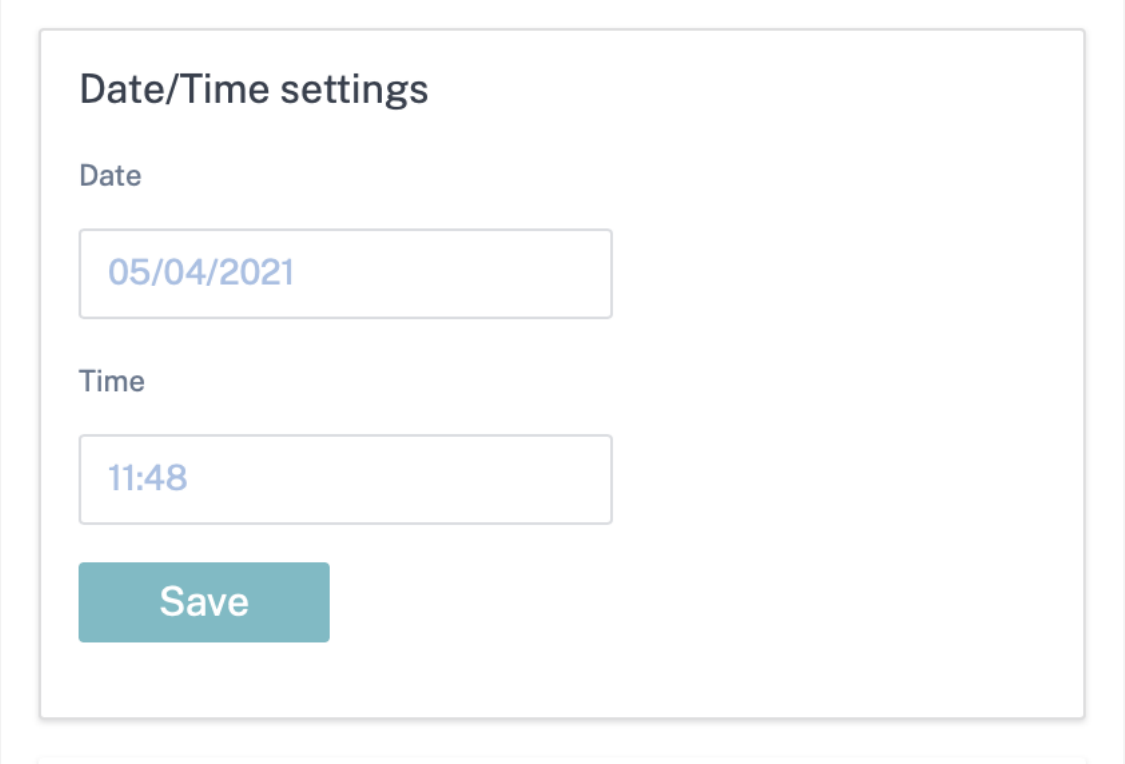
日付と時刻を手動で設定するか、ネットワークタイムプロトコル（NTP）サーバーを使用してオンプレミス用 Citrix SD-WAN Orchestrator のクロックタイムを協定世界時（UTC）と同期させることができます。

NTP サーバを設定するには、ネットワークレベルで [インフラストラクチャ**] > [Orchestrator** 管理**] > [**管理設定**] > [NTP]** に移動し、**[NTP** サーバを使用] を有効にします。

NTP サーバーの IP アドレスまたはドメイン名を指定します。最大 4 台の NTP サーバを提供できますが、少なくとも 1 つは設定してください。片方の NTP サーバーがダウンした場合、オンプレミス向け Citrix SD-WAN Orchestrator はもう一方の NTP サーバーと自動的に同期します。NTP サーバーのドメイン名を指定する場合は、外部 DNS サーバーがドメイン名を IP アドレスにポイントするように設定されていることを確認してください。

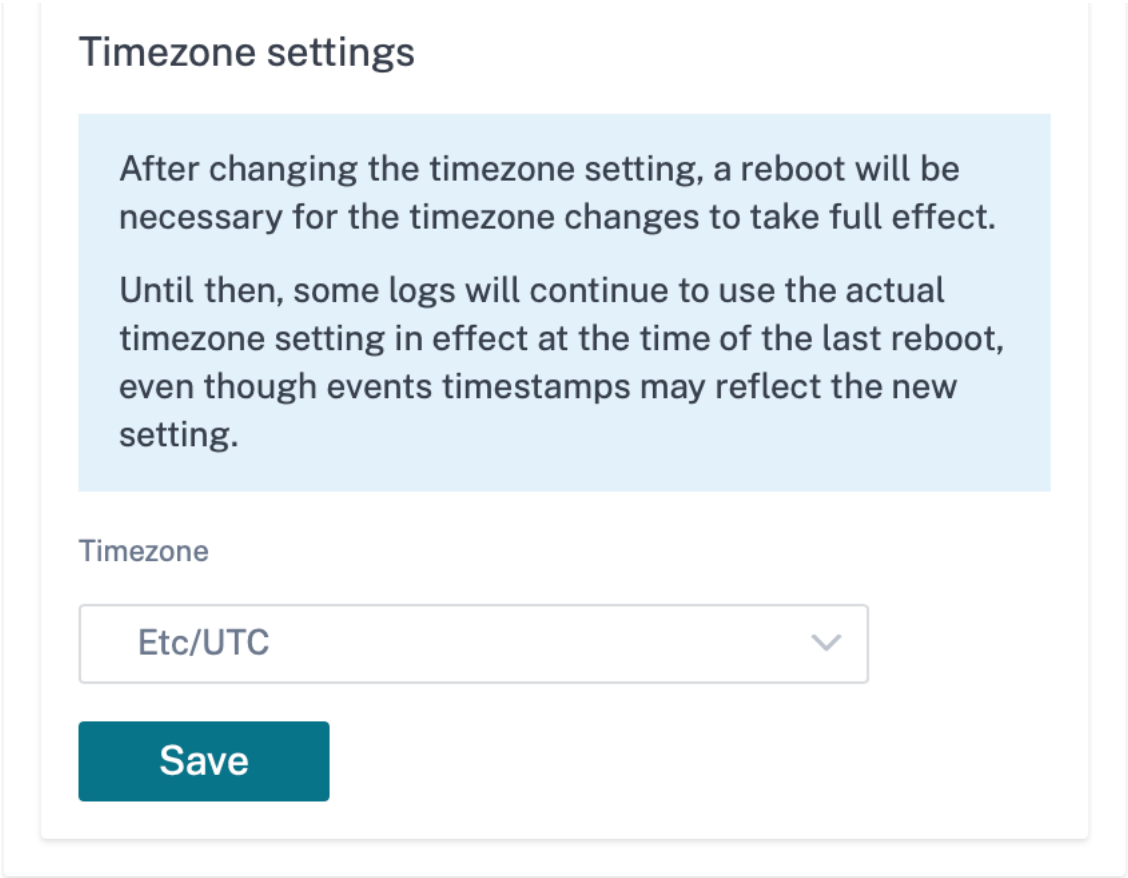


日付と時刻を手動で設定するには、「**NTP** サーバーを使用」オプションを無効にして、手動で日付と時刻を選択します。



国/都市に基づいてタイムゾーンを選択します。

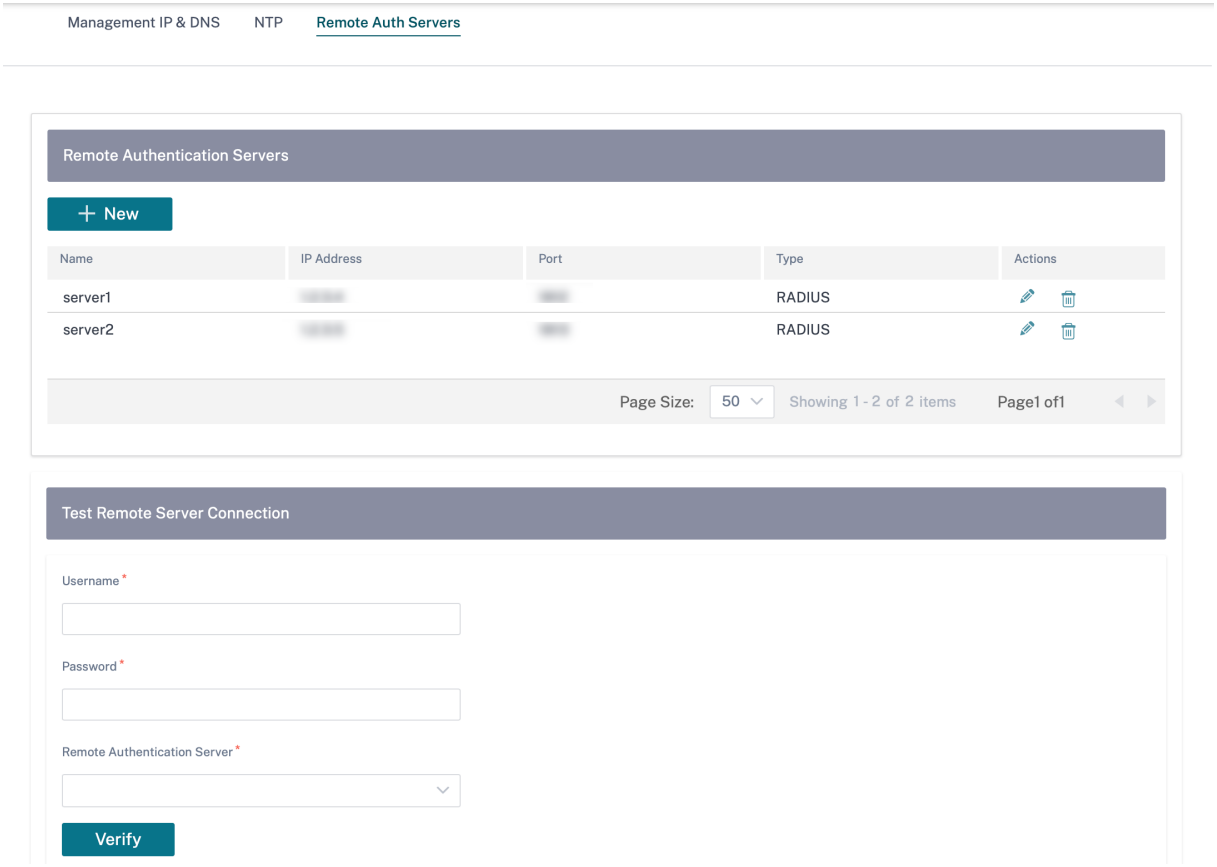
> 注:
>
> タイムゾーンを変更したら、Orchestrator 仮想マシンを再起動します。一部のログは、再起動が完了するまで前のタイムゾーンを使用し続けます。手順については、「Orchestrator 仮想マシンの再起動」を参照してください。



リモート認証サーバー

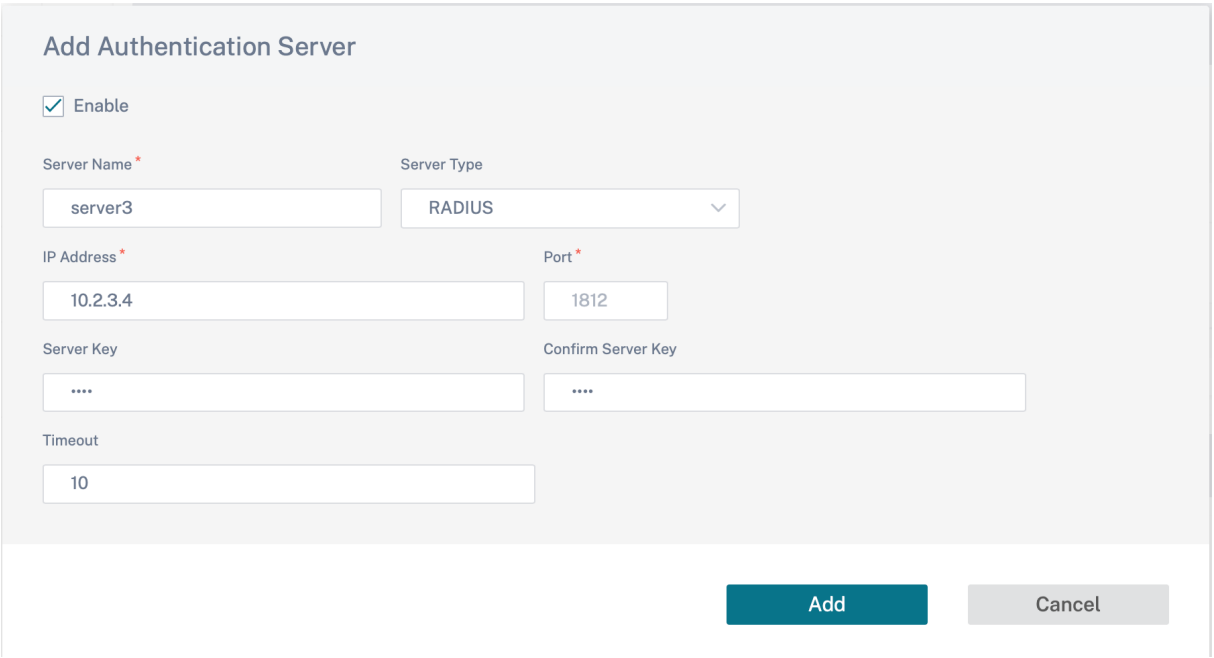
プロバイダー管理のセットアップでは、プロバイダー管理者のみがリモート認証されたユーザー用に RADIUS または TACACS+ サーバーを設定できます。顧客管理者は、プロバイダー管理者が設定したリモート認証サーバーを使用できます。顧客管理のセットアップでは、顧客管理者が RADIUS または TACACS+ サーバを設定できます。

> 注:
>
> 必要なユーザーアカウントが RADIUS または TACACS+ 認証サーバー上に作成されていることを確認してください。



リモート認証を設定するには、[インフラストラクチャ] **> [Orchestrator** 管理] **> [**管理設定] **> [**リモート認証サーバ] に移動します。[**+** 新規] をクリックします。次の詳細情報を入力します:

- 有効化: リモート認証サーバーの設定を有効にします。
- サーバー名: リモート認証サーバーの名前。
- サーバータイプ: リモート認証サーバーのタイプ (RADIUS または TACACS+)。
- **IP** アドレス: リモート認証サーバーのホスト IP アドレス。
- ポート: リモート認証サーバーのポート番号。RADIUS サーバのデフォルトポートは 1812 で、TACACS+ サーバは 49 です。
- **** サーバーキーと確認サーバーキー ****: リモート認証サーバーに接続するときに使用するシークレットキー。
- 認証タイプ:(TACACS+ サーバーでのみ使用可能) ユーザー名とパスワードを TACACS+ サーバーに送信するために使用する暗号化方法を選択します。
  - **PAP**: パスワード認証プロトコル (PAP) を使用して、TACACS+ サーバに強力な共有シークレットを割り当てることにより、ユーザー認証を強化します。
  - **ASCII**: ASCII 文字セットを使用して TACACS+ サーバに強力な共有秘密を割り当てることにより、ユーザー認証を強化します。
- タイムアウト: リモート認証サーバーからの認証応答を待つ時間間隔 (秒単位)。



リモートサーバー接続をテストすることもできます。[リモートサーバー接続のテスト] で、[ユーザー名] と [パスワード] を入力します。リモート認証サーバーを選択し、[**Verify**] をクリックします。

データベース管理

オンプレミス用 Citrix SD-WAN Orchestrator で実行されている現在のデータベースのバックアップを作成し、後でそのバックアップファイルを使用して同じデータベース状態を復元できます。

> 注
>
> - プロバイダー管理のセットアップでは、プロバイダーの管理者のみがデータベースのバックアップを作成および復元できます。
> - プロバイダー管理セットアップで作成されたデータベースバックアップをカスタマー管理セットアップに復元することはできません。同様に、顧客管理設定で作成したデータベースバックアップをプロバイダー管理セットアップに復元することはできません。

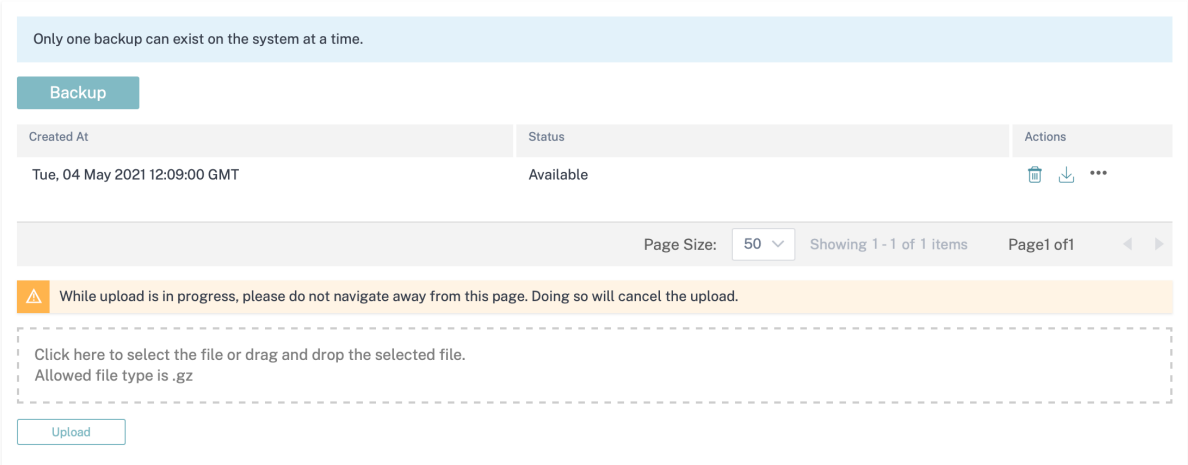
データベースバックアップを作成するには、[インフラストラクチャ] > [**Orchestrator** 管理] > [データベース管理] に移動します。[バックアップ] をクリックします。

「アクション」列の「ダウンロード」をクリックして、バックアップされたデータベースをダウンロードします。

[アップロード] をクリックして、ダウンロードしたファイルを参照してアップロードします。ダウンロードしたファイルをドラッグして画面にドロップすることもできます。

復元するには、「アクション」列の「復元」をクリックします。

> 注
>
> - 一度に保存できるデータベースバックアップは 1 つだけです。既存のバックアップを最新のバックアップに置き換えるには、既存のバックアップを削除して [バックアップ] をクリックします。
> - データベースの復元は、データバックアップが作成されたのと同じリリースのオンプレミス用 Citrix SD-WAN Orchestrator で実行する必要があります。
> - データベースのバックアップは、設定と統計のバックアップのみを行います。プラットフォーム関連のデータはバックアップしません。



ストレージ管理

オンプレミス向け Citrix SD-WAN Orchestrator は、お客様の構成、統計、ローカルデータベース、および公開されている Citrix SD-WAN リリースバージョンを既存のディスクから新しいディスクに移行することをサポートします。

プロバイダーが管理するセットアップでは、プロバイダー管理者のみがディスク移行を実行できます。プロバイダ管理セットアップの顧客管理者には、ディスク移行を実行する権限がありません。顧客管理のセットアップでは、顧客管理者はディスク移行を実行できます。

ディスクマイグレーションは、ディスク容量を増やすため、または障害回復のために実行できます。

- 新しいディスクの追加: オンプレミス用 Citrix SD-WAN Orchestrator が使用している現在のデータの少なくとも 2 倍のストレージサイズの新しいディスクを追加できます。オンプレミス UI 用の Citrix SD-WAN Orchestrator を使用して、新しいディスクをアクティブ化し、既存の顧客構成、統計、ローカルデータベース、および公開されている Citrix SD-WAN リリースバージョンを移行できます。新しく追加されたディスクがアクティブ化されると、オンプレミス用 Citrix SD-WAN Orchestrator が再起動されます。
- 障害回復: 災害が発生した場合、データを含むディスクを、オンプレミス用 Citrix SD-WAN Orchestrator と同じバージョンにあるオンプレミス仮想マシン用 Citrix SD-WAN Orchestrator の新しいインスタンスに

接続できます。Citrix SD-WAN Orchestrator for On-Premises UI の [データの移行] オプションを選択せずにディスクをアクティブ化します。ディスクがアクティブ化されると、オンプレミス用 Citrix SD-WAN Orchestrator が再起動されます。

> 注
>
> - ディスクの移行中は、オンプレミス用 Citrix SD-WAN Orchestrator の電源を切ったり、手動で再起動したりしないでください。電源を切るか、手動で再起動すると、データが失われる可能性があります。
> - 以前に追加されたディスクパーティションから新しく作成されたディスクパーティションにディスクを移行しても、移行後、古いディスクのデータは削除されません。古いディスクのデータを削除するには、そのディスクを別のオペレーティングシステムに接続し、データを安全に削除します。

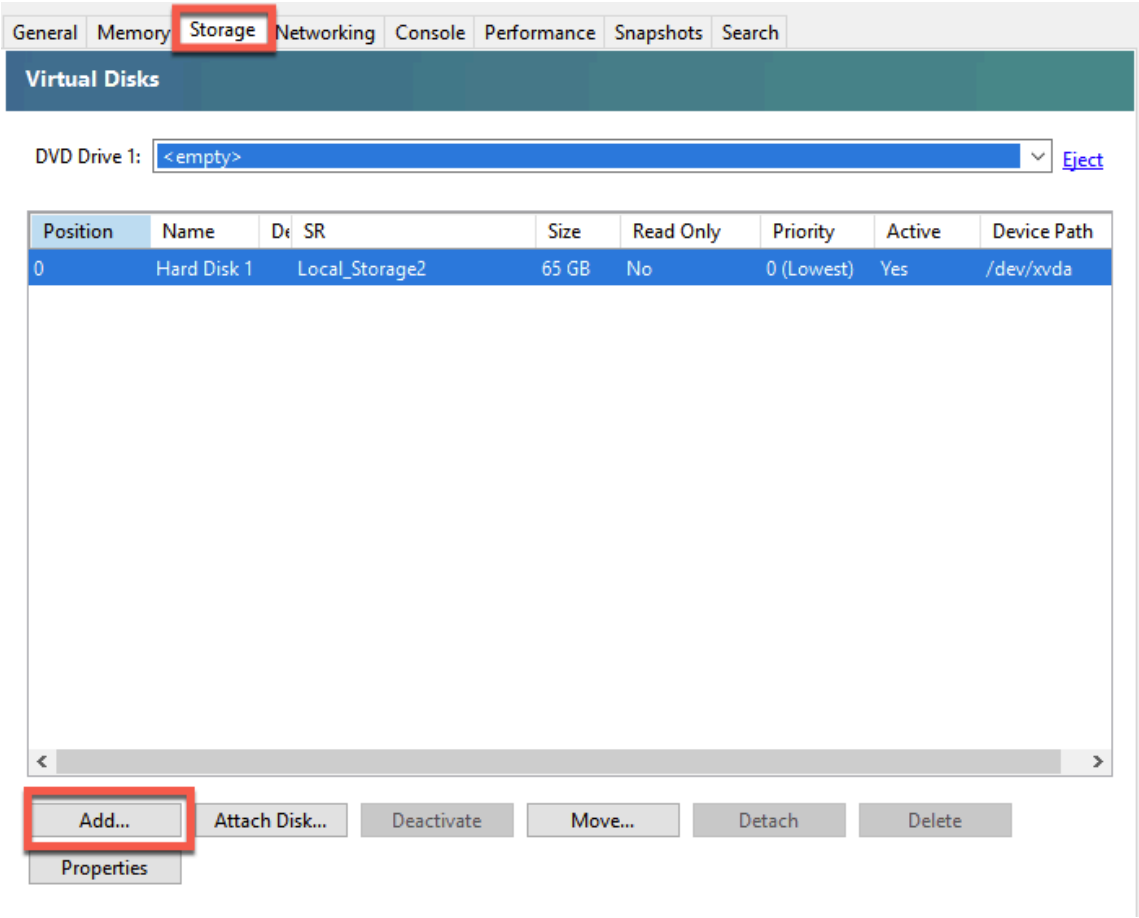
制限事項

ディスク移行プロセスの制限は次のとおりです。

- 古いリリースのユーザーは新しいリリースに移行されません。移行後、ユーザーを削除して再度作成してください。
- オンプレミス仮想マシン用の古い Citrix SD-WAN Orchestrator で作成された STS は移行されません。ただし、移行後、UI には、オンプレミス仮想マシン用の古い Citrix SD-WAN Orchestrator で生成された STS が一覧表示されます。STS を手動で削除します。
- オンプレミス用の古い Citrix SD-WAN Orchestrator で作成されたデータベースバックアップは移行されません。マイグレーション後、リストに載っている場合は手動で削除してください。
- デフォルトでは、ディスクの移行先となる新しいオンプレミス向け Citrix SD-WAN Orchestrator は、すべての二要素認証サーバーに接続されていると想定されます。管理者アカウントが二要素認証サーバーを使用していて、二要素認証サーバーへの接続が使用できない場合、管理者でもログインできません。このようなシナリオでは、Citrix サポートに連絡してください。
- 新しいディスクに移行した後は、オンプレミス用 Citrix SD-WAN Orchestrator に割り当てられるディスク容量を増やすことはできません。
- 障害回復シナリオでは、ディスクをアクティブにした後にカスタムドメインを再構成する必要があります。
- 障害復旧シナリオでは、ディスクをアクティブ化した後、非クラウドゼロタッチ展開またはクラウド仲介ゼロタッチ展開を実行して、オンプレミス用 Citrix SD-WAN Orchestrator がインストールされているサイト上の Citrix SD-WAN アプライアンス間の接続を確立する必要があります。

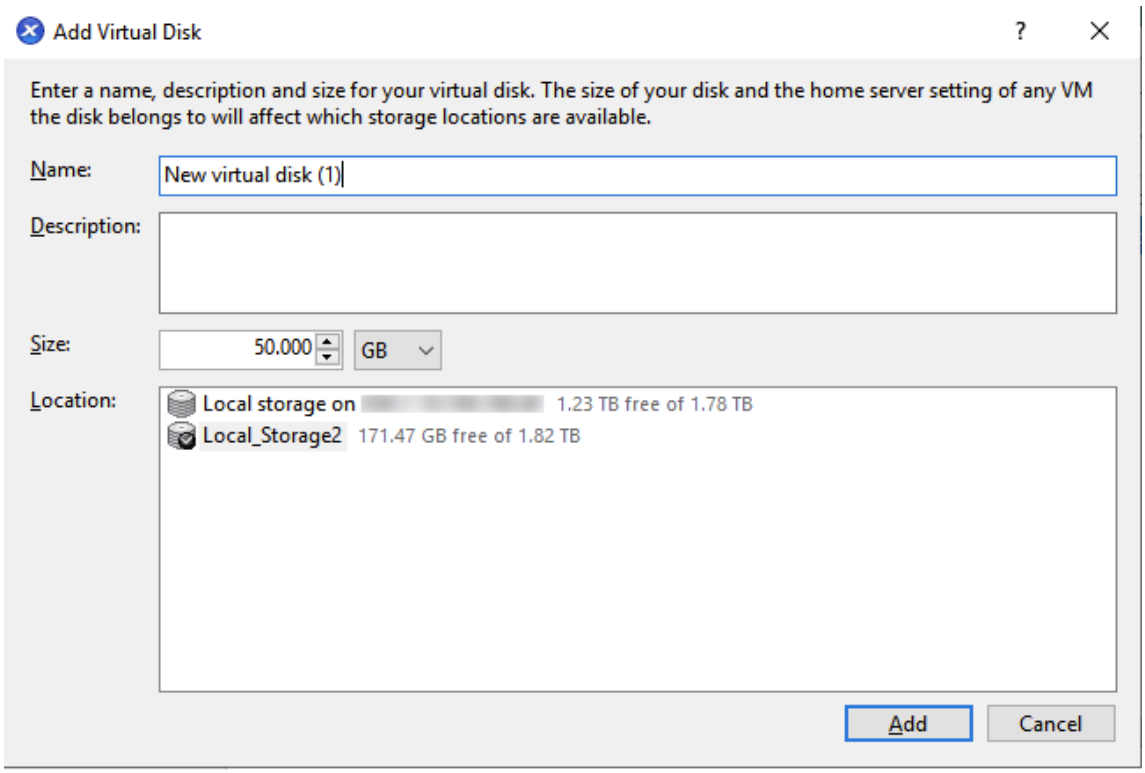
Citrix Hypervisor に新しいディスクを追加します

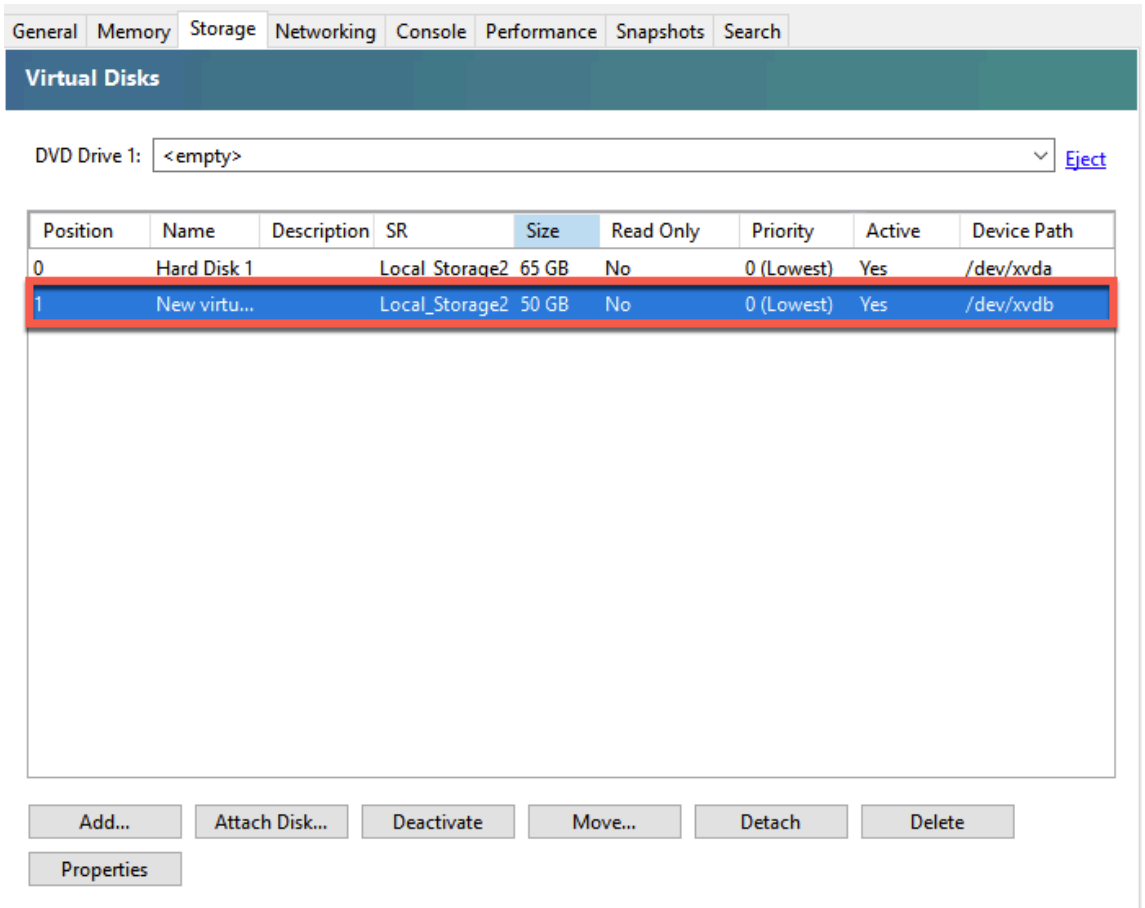
1. ハイパーバイザーから仮想マシン (VM) を選択します。[ストレージ] タブを選択し、[追加] をクリックします。



2. 新しいディスクの名前、説明、サイズ、場所などの詳細を入力します。[追加] をクリックします。新しく追加されたディスクは [ストレージ] タブに表示されます。

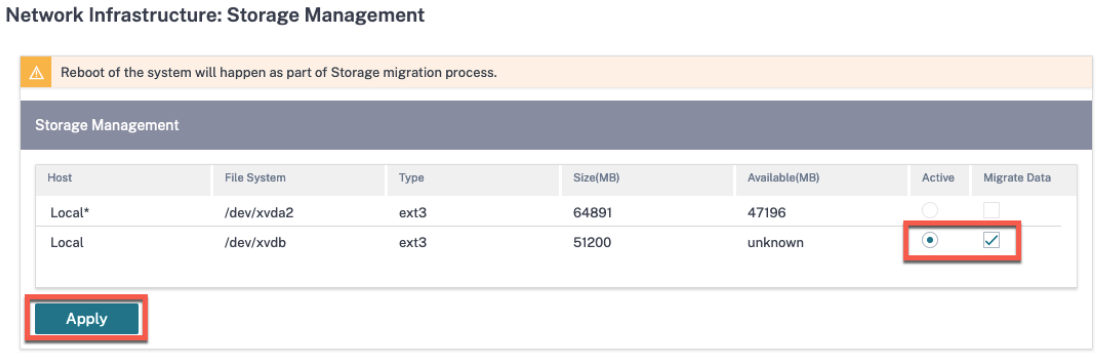
> 注:
>
> ディスクサイズは、オンプレミス用 Citrix SD-WAN Orchestrator が使用している現在のデータの少なくとも 2 倍でなければなりません。



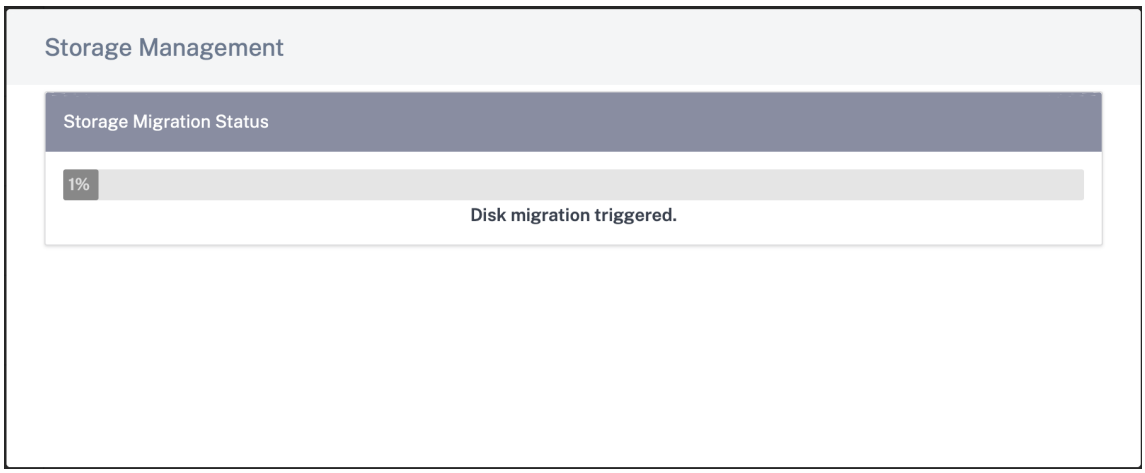


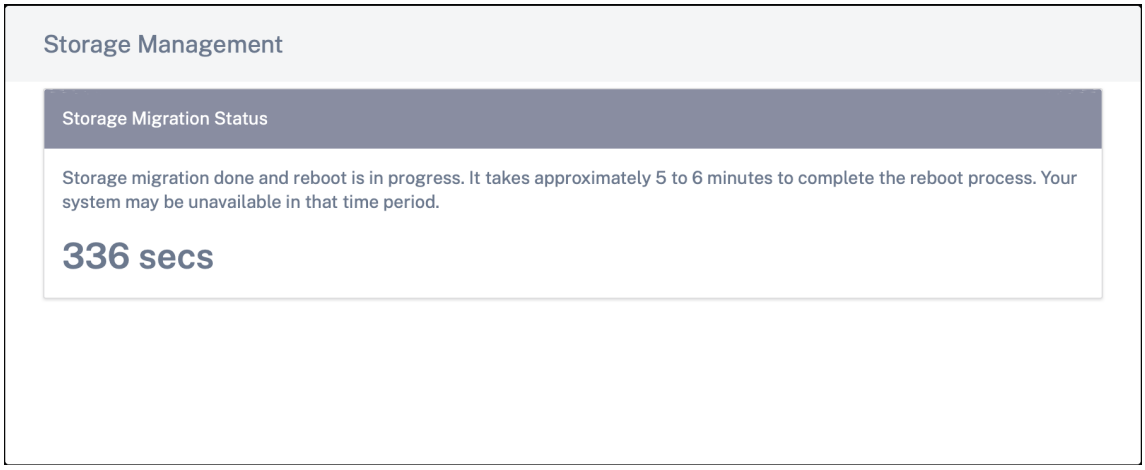
3. オンプレミス UI 用 Citrix SD-WAN Orchestrator にログインし、[インフラストラクチャ] **> [Orchestrator** 管理] **> [**ストレージ管理] に移動します。新しく接続したディスクは、自動的に [ストレージ管理] に表示されます。

4. 「アクティブ」ラジオ・ボタンを選択し、「データを移行」チェック・ボックスを選択します。［適用］をクリックします。



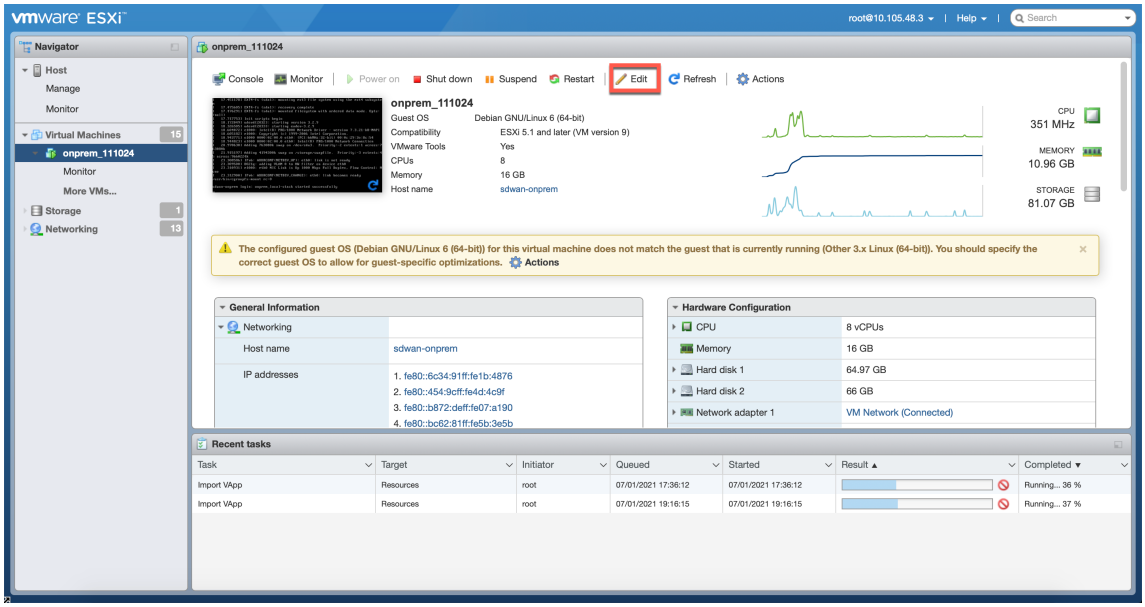
5. ディスク移行プロセスが開始されます。既存のディスク上のお客様の構成、統計、ローカルデータベース、Citrix SD-WAN リリースバージョンは新しいディスクに移行されます。移行が完了すると、オンプレミス用 Citrix SD-WAN Orchestrator が再起動されます。



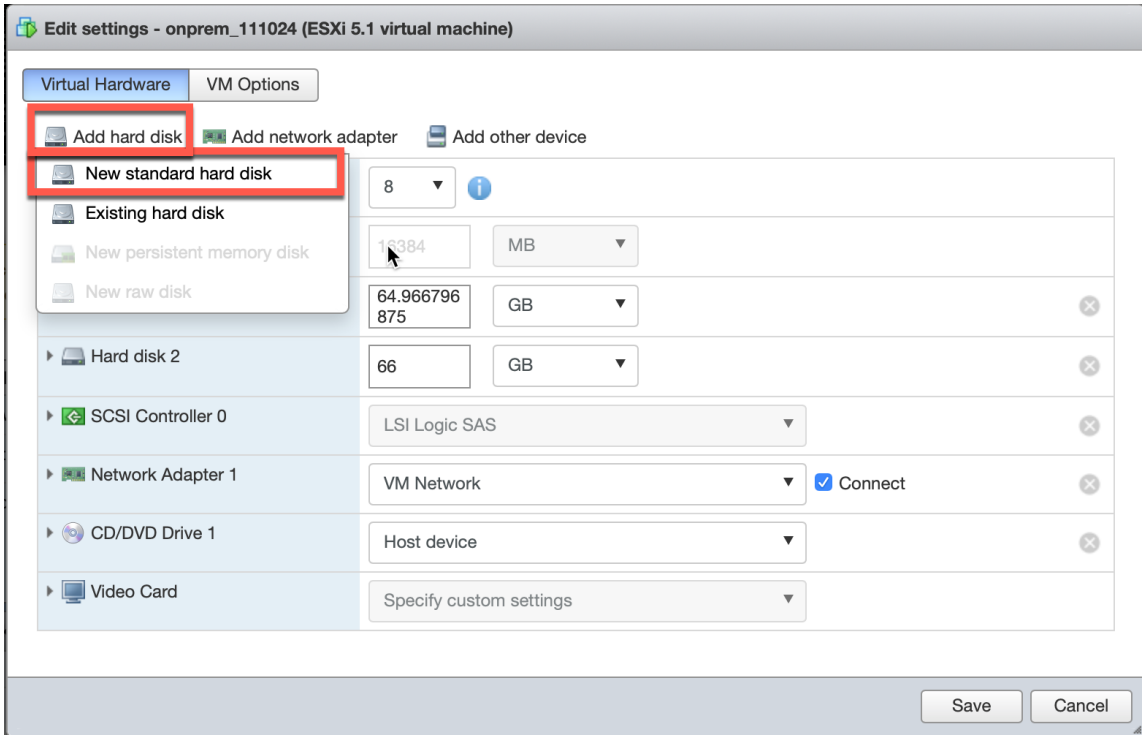


ESXi サーバに新しいディスクを追加します

1. ESXi サーバにログインし、仮想マシンを選択します。[編集] をクリックします。

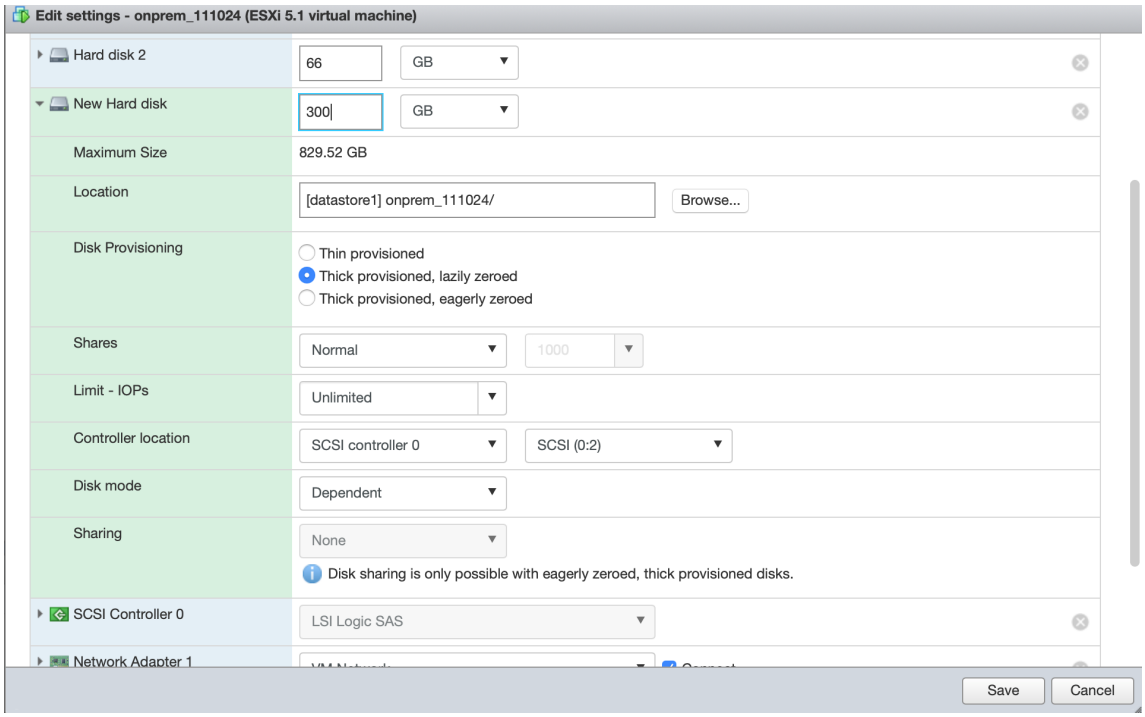


2. [ハードディスクの追加] **>** [新しい標準ハードディスク] をクリックします。

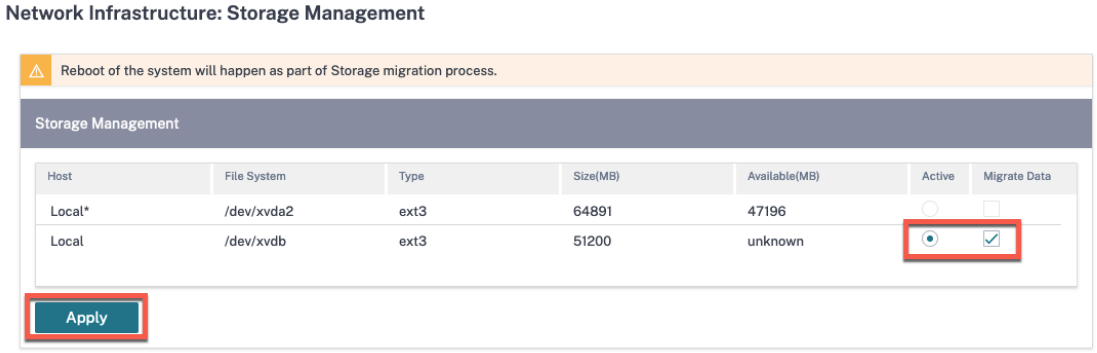


3. 必要に応じてディスクストレージ容量やその他の設定を入力します。[保存] をクリックします。

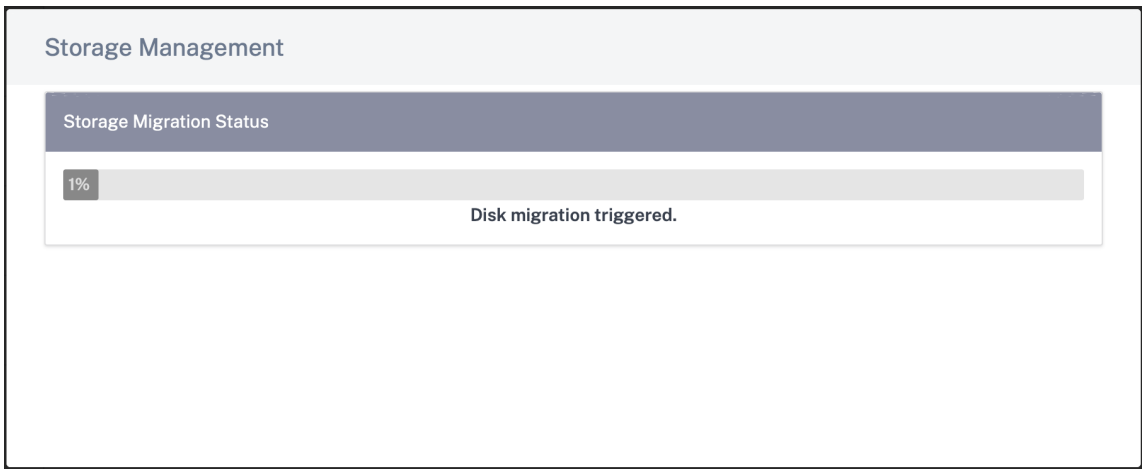
> 注:
>
> ディスクサイズは、オンプレミス用 Citrix SD-WAN Orchestrator が使用している現在のデータの少なくとも 2 倍でなければなりません。

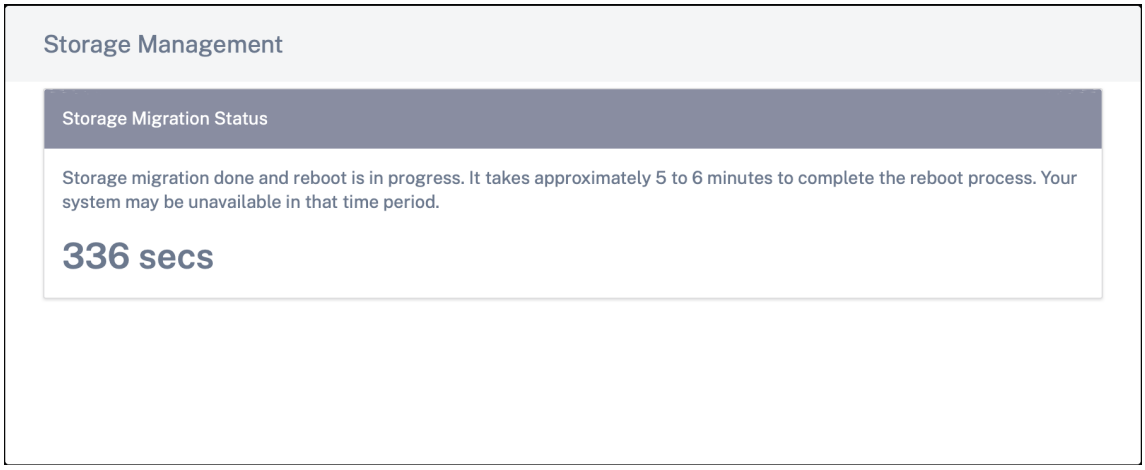


4. オンプレミス用 Citrix SD-WAN Orchestrator にログインし、[インフラストラクチャ] **> [Orchestrator** 管理] **> [**ストレージ管理] に移動します。新しく接続されたディスクがここに表示されます。
5. 「アクティブ」ラジオ・ボタンを選択し、「データを移行」チェック・ボックスを選択します。[適用] をクリックします。



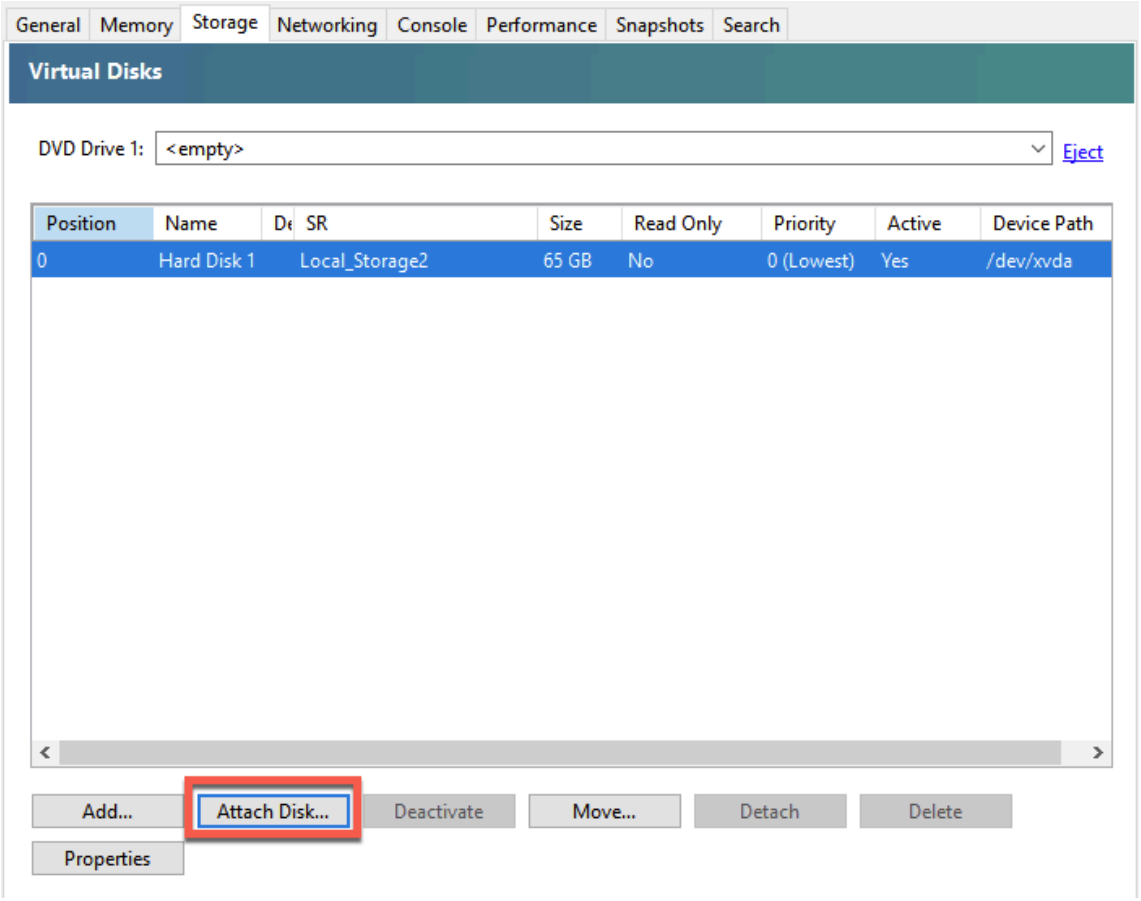
6. ディスク移行プロセスが開始されます。既存のディスク上のお客様の構成、ローカルデータベース、Citrix SD-WAN リリースバージョン、およびデータベース統計は、新しいディスクに移行されます。移行が完了すると、オンプレミス用 Citrix SD-WAN Orchestrator が再起動されます。





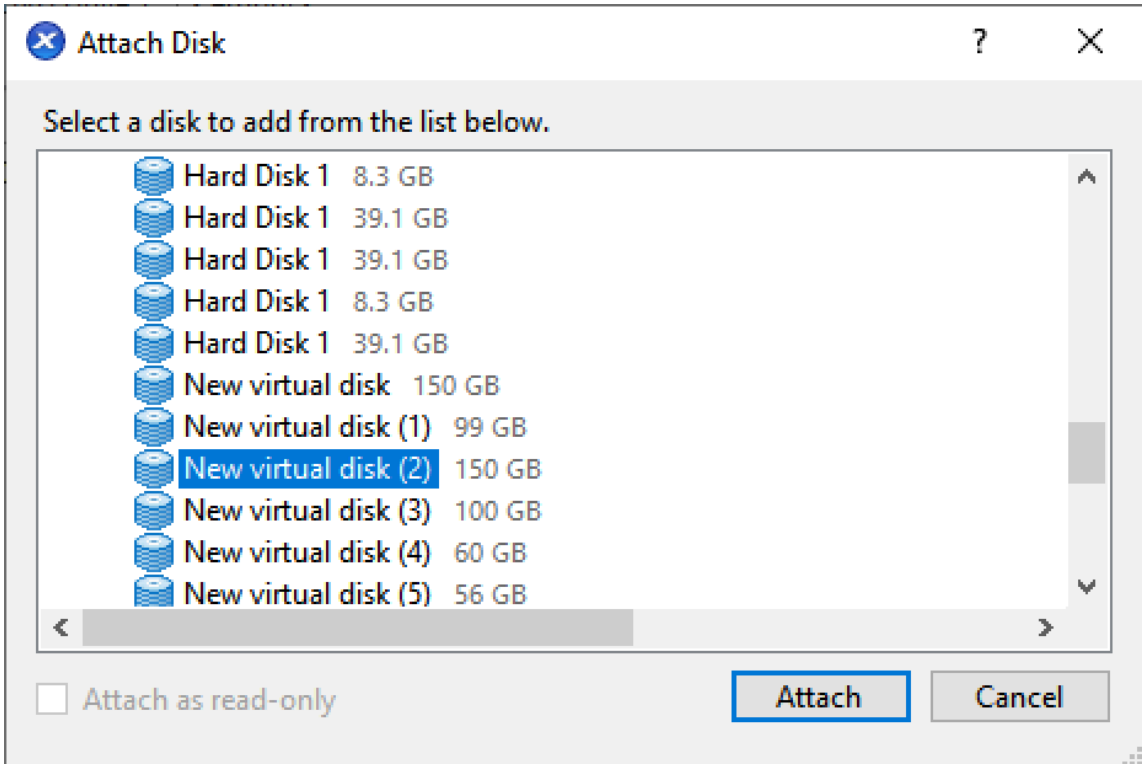
Citrix Hypervisor でのディザスタリカバリ

1. ハイパーバイザーから仮想マシン (VM) を選択します。[ストレージ] タブを選択し、[ディスクを接続] をクリックします。



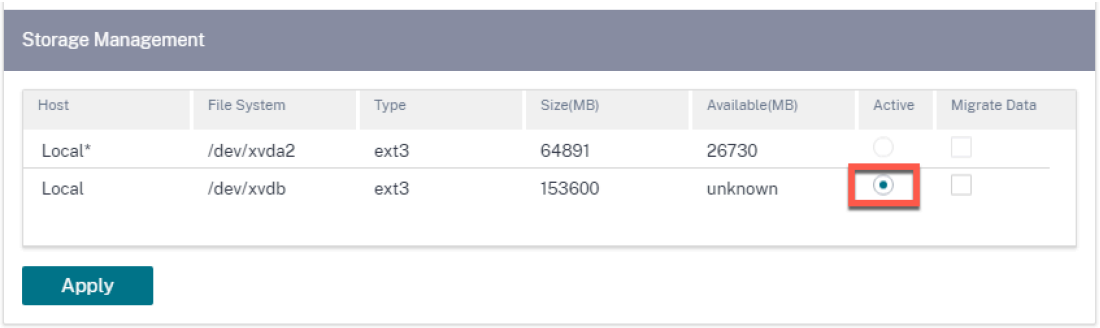
2. 障害が発生したオンプレミス用 Citrix SD-WAN Orchestrator に接続されているディスクを選択し、[接続] をクリックします。

   ディスクがリストにない場合は、障害が発生したオンプレミス用 Citrix SD-WAN Orchestrator に接続されているディスクが切り離され、オンプレミス用 Citrix SD-WAN Orchestrator がシャットダウン状態であることを確認してください。

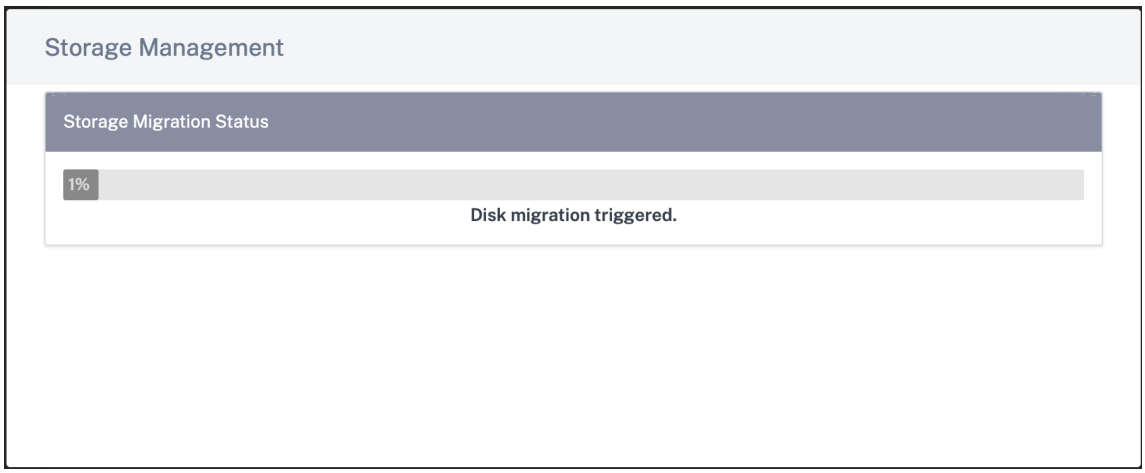


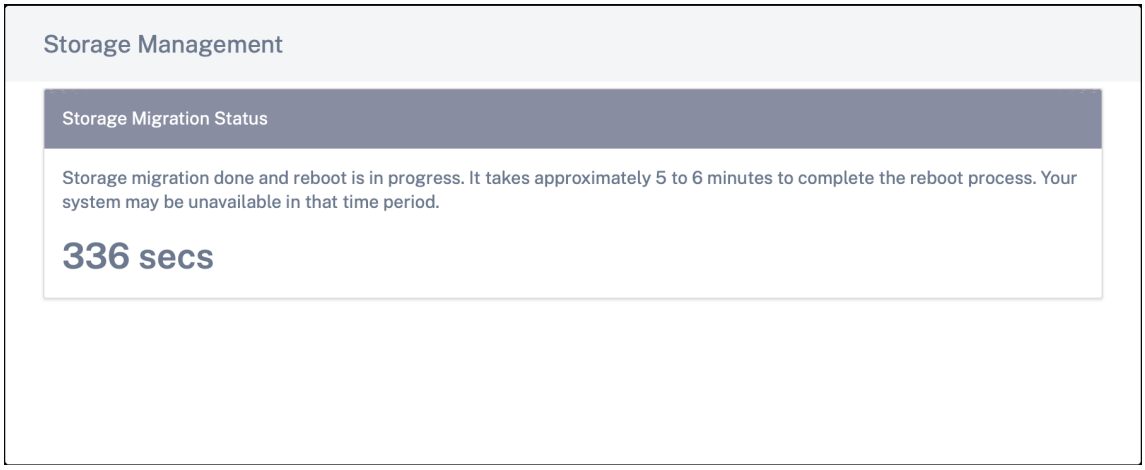
3. オンプレミス UI 用 Citrix SD-WAN Orchestrator にログインし、[インフラストラクチャ] **> [Orchestrator** 管理] **> [**ストレージ管理] に移動します。新しく接続されたディスクがここに表示されます。
4. 「アクティブ」ラジオボタンのみを選択し (「データを移行」チェックボックスが選択されている場合はオフ)、「適用」をクリックします。

> 注:
>
> [データの移行] チェックボックスは選択しないでください。オンプレミス向け Citrix SD-WAN Orchestrator は、バックエンドで移行をトリガーし、移行が完了すると自動的に再起動します。



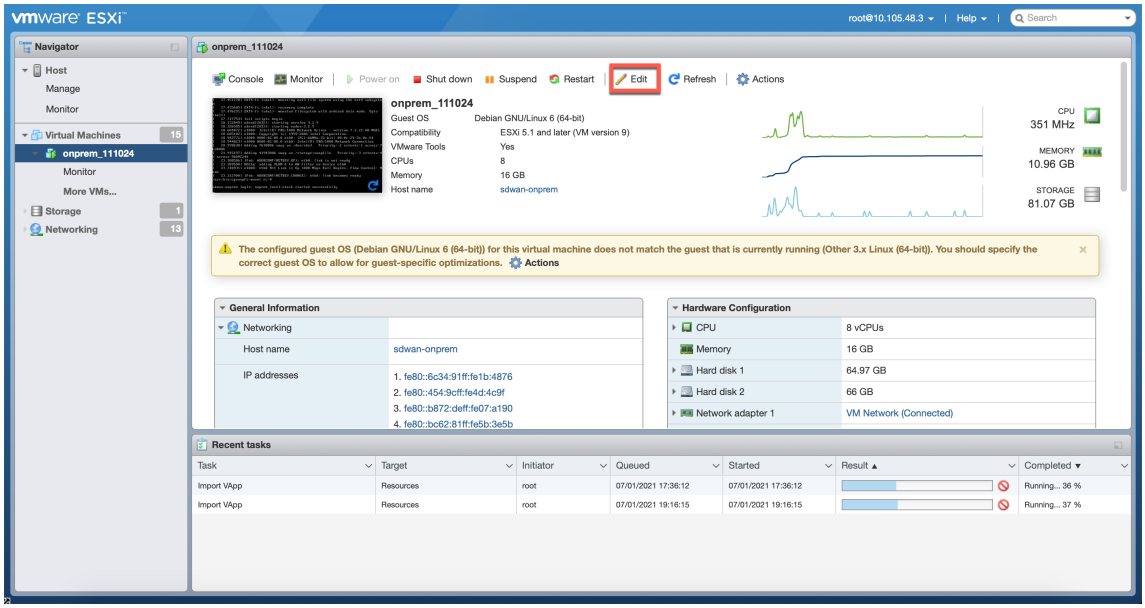
5. 移行が完了すると、オンプレミス用 Citrix SD-WAN Orchestrator が再起動されます。



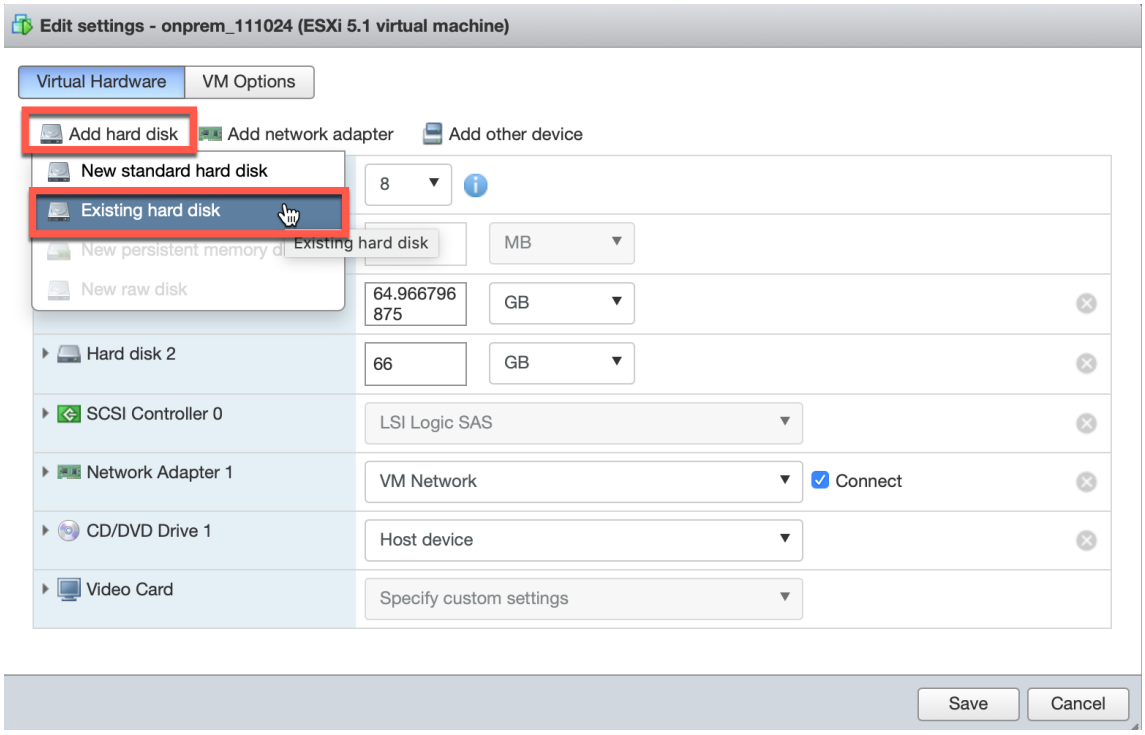


ESXi サーバでの障害復旧

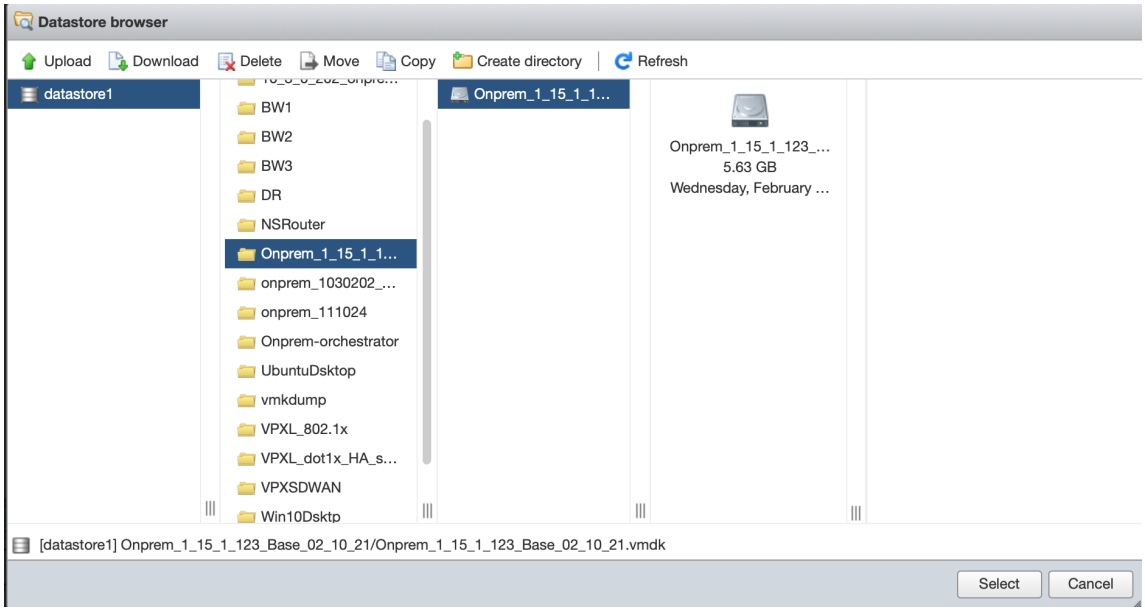
1. ESXi サーバにログインし、仮想マシンを選択します。［編集］をクリックします。



2. [ハードディスクの追加] **>** [既存のハードディスク] をクリックします。

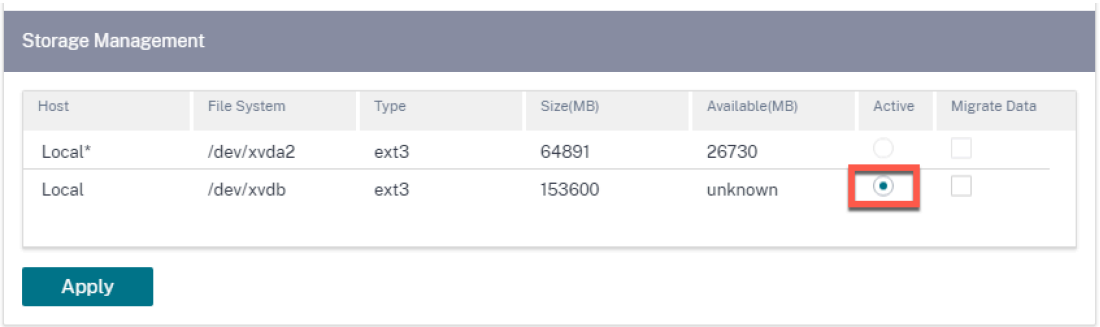


3. 障害が発生したオンプレミス用 Citrix SD-WAN Orchestrator に接続されているディスクを参照し、[選択] をクリックします。

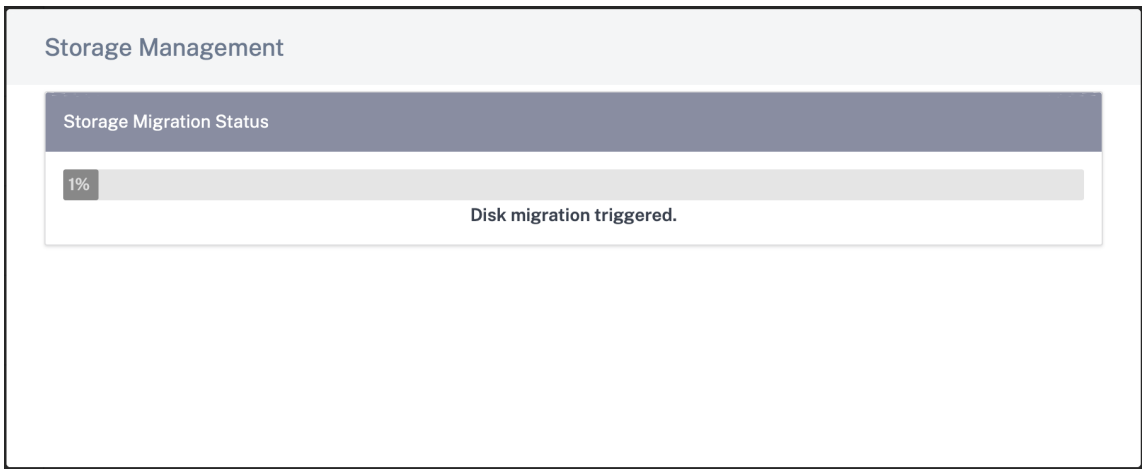


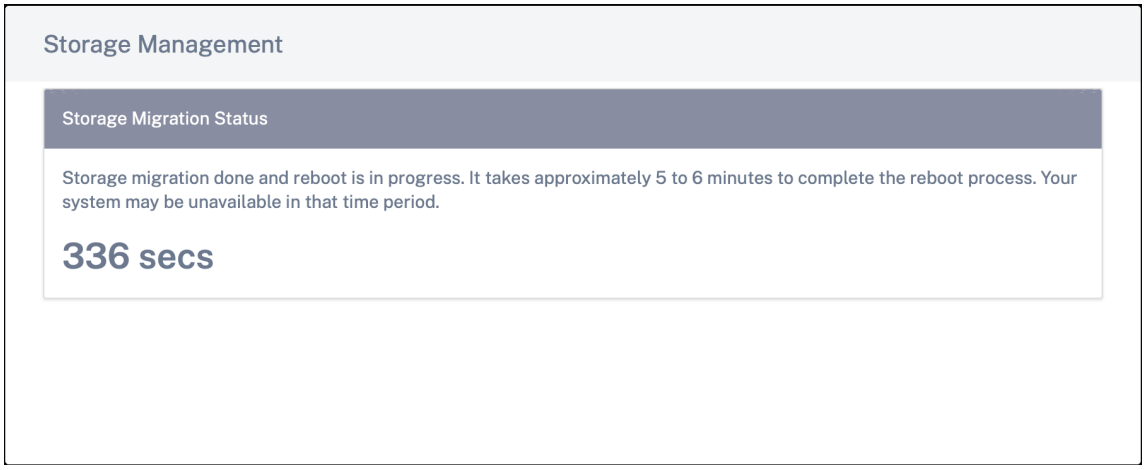
4. オンプレミス UI 用 Citrix SD-WAN Orchestrator にログインし、[インフラストラクチャ] **> [Orchestrator 管理] > [**ストレージ管理] に移動します。新しく接続されたディスクがここに表示されます。
5. 「アクティブ」ラジオボタンのみを選択し (「データを移行」チェックボックスが選択されている場合はオフ)、「適用」をクリックします。

> **注:**
>
> [データの移行] チェックボックスは選択しないでください。オンプレミス向け Citrix SD-WAN Orchestrator は、バックエンドで移行をトリガーし、移行が完了すると自動的に再起動します。



6. 移行が完了すると、オンプレミス用 Citrix SD-WAN Orchestrator が再起動されます。





HTTP プロキシ

オンプレミス向け Citrix SD-WAN Orchestrator には、ライセンス、クラウドログイン、クラウド仲介 ZTD、クラウドダイレクト、およびソフトウェアの公開にインターネット接続が必要です。オンプレミス用 Citrix SD-WAN Orchestrator が HTTP プロキシサーバー経由でインターネットに接続されている場合、オンプレミス仮想マシン用 Citrix SD-WAN Orchestrator で HTTP プロキシサーバー設定を構成できます。

HTTP プロキシ設定は、Citrix Cloud へのすべての送信要求を一元管理します。管理者は、オンプレミス用 Citrix SD-WAN Orchestrator からの送信要求を HTTP プロキシサーバー経由で Citrix Cloud にルーティングできます。

はじめに

クラウドログインに HTTP プロキシを初めて使用するには、オンプレミス用 Citrix SD-WAN Orchestrator の CLI コンソールから HTTP プロキシ設定を構成する必要があります。

オンプレミス仮想マシンの新しい Citrix SD-WAN Orchestrator のクラウドログインページで、オンプレミス用 Citrix SD-WAN Orchestrator から Citrix SD-WAN Orchestrator サービスへのすべてのアウトバウンド接続に

HTTP プロキシを使用する場合は、CLI を使用して HTTP プロキシの詳細を構成する必要があります。クラウドへのログインが完了し、設定ページにアクセスすると、UI で HTTP プロキシサーバーの詳細を設定できます。

CLI での **HTTP** プロキシ設定の構成

`set_http_proxy` コマンドを実行して HTTP プロキシを設定します。HTTP プロキシは、以下のいずれかのオプションを使用して設定できます。

- プロキシサーバーで認証が有効になっている場合:

  `set <ip address> <port> <user name> <password>`

- プロキシサーバーで認証が有効になっていない場合:

  `set <ip address> <port>`

HTTP プロキシ設定を表示

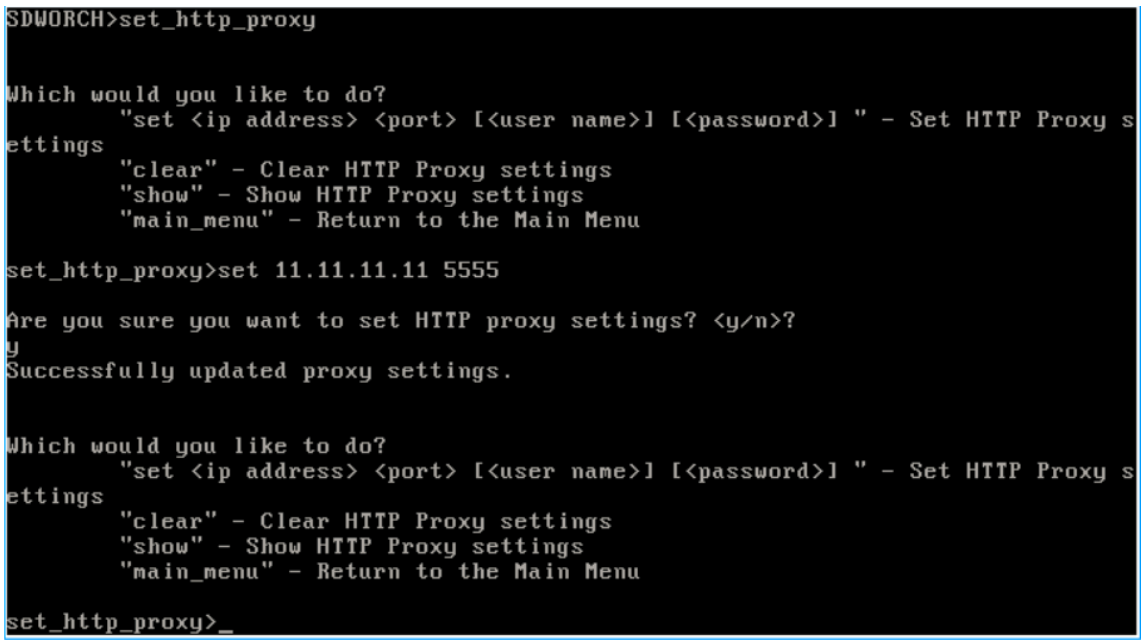
- `show`: このコマンドは CLI のプロキシ設定を表示します。出力にはパスワードは表示されません。

HTTP プロキシ設定をクリア

- `clear`: このコマンドは HTTP プロキシ設定を削除します。

main_menu に戻る

- `main_menu`: このコマンドは、オンプレミス用 Citrix SD-WAN Orchestrator の CLI コンソールにリダイレクトします。



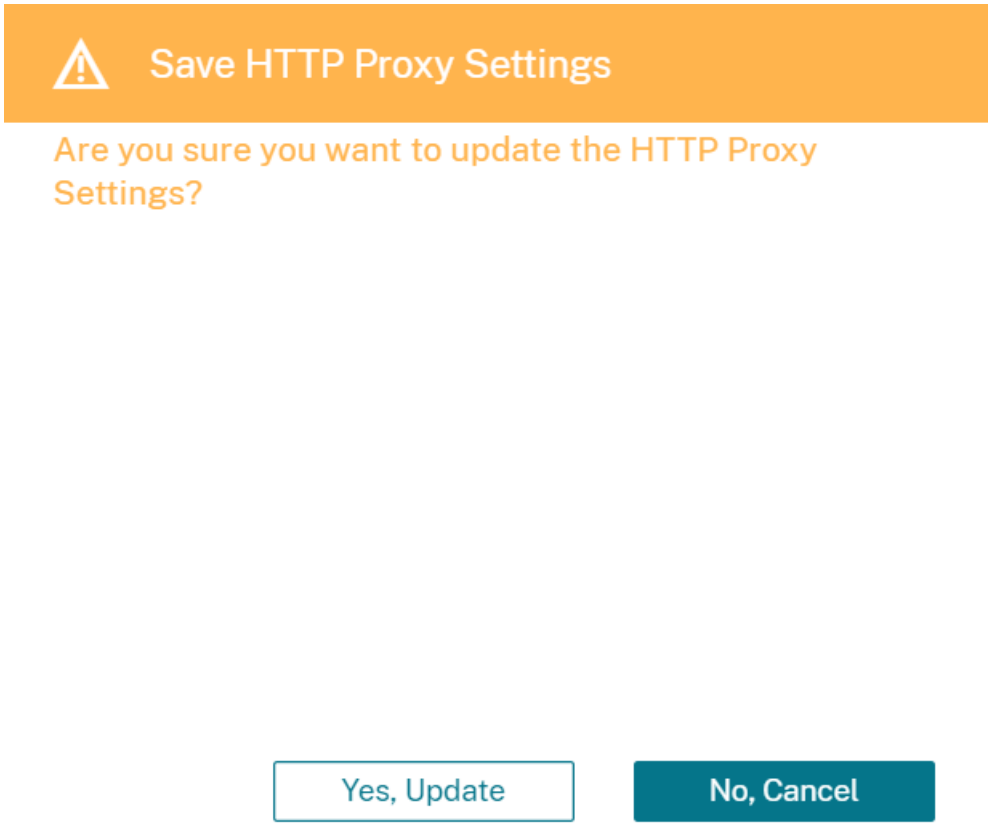
UI での **HTTP** プロキシサーバー設定の構成

1. オンプレミス UI 用 Citrix SD-WAN Orchestrator にログインし、[インフラストラクチャ] > [**Orchestrator** 管理] > [**HTTP** プロキシ] に移動します。
2.「ネットワークインフラストラクチャ**:HTTP** プロキシ」セクションで、次のフィールドに値を入力します。

   - **IP** アドレス: プロキシサーバーの IP アドレス。
   - ポート: プロキシサーバーが接続を受け入れるネットワークポート番号。
   - ユーザー名: プロキシサーバーのユーザー名。
   - パスワード: プロキシサーバーのパスワード。

   > 注:
   >
   > プロキシサーバーで認証が設定されていない場合は、[ユーザー名] フィールドと [パスワード] フィールドを空白のままにできます。

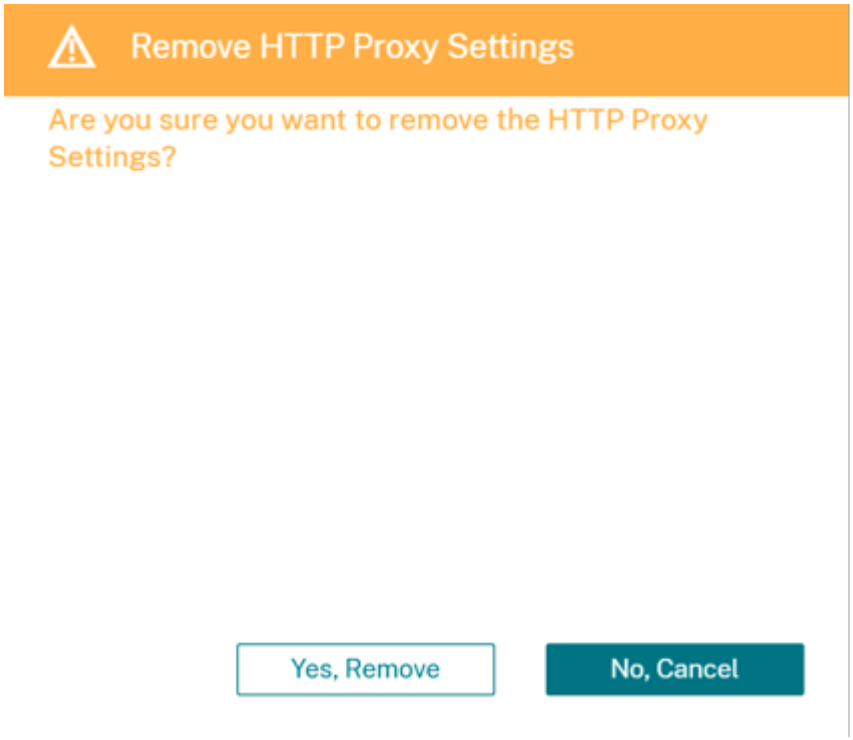
3. [適用] をクリックします。確認ダイアログボックスが開きます。
4. [Yes, Update] をクリックします。



> 注
>
> - オンプレミス用 Citrix SD-WAN Orchestrator から Citrix Cloud へのアウトバウンドトラフィックに HTTP プロキシサーバーを使用するには、プロキシサーバーを透過的な SSL HTTP プロキシまたは SSL バイパス HTTP プロキシサーバーとして構成する必要があります。サーバーは、Citrix SD-WAN Orchestrator サービスの SSL 証明書をスプーフィングしてはなりません。
> - オンプレミス用 Citrix SD-WAN Orchestrator がインターネットに直接接続されている場合は、プロキシサーバーの設定を完全に削除できます。必要に応じて、プロキシサーバーの設定を削除して別のプロキシサーバーを構成することもできます。

UI のプロキシサーバー設定を削除する

1. オンプレミス用 Citrix SD-WAN Orchestrator UI で、［インフラストラクチャ］>［**Orchestrator** 管理］>［**HTTP** プロキシ］に移動します。
2.「ネットワークインフラストラクチャ**:HTTP** プロキシ」セクションで、「削除」をクリックします。確認ダイアログボックスが開きます。
3. [はい、削除] をクリックします。



消去設定

選択した時間間隔の履歴統計/データを消去できます。設定した日より古い統計/データはクリアされます。データが消去されると、そのデータは使用できなくなります。デフォルトでは、オンプレミス向け Citrix SD-WAN Orchestrator は、30 日以上前の履歴統計/データを消去します。

ネットワークレベルで、[インフラストラクチャ] > [**Orchestrator** 管理] > [消去設定] に移動し、時間間隔を選択して [適用] をクリックします。たとえば、180 日以上前の履歴統計/データを消去する場合は、「統計情報の消去間隔 **(**日数**)** 」ドロップダウンリストから「180」を選択し、「適用」をクリックします。消去処理は、SD-WAN アプライアンスに設定されているタイムゾーンで、毎日午前 12 時 48 分頃に行われます。

Orchestrator 診断

October 26, 2022

このセクションでは、オンプレミスインフラストラクチャ向け Citrix SD-WAN Orchestrator で実行できる診断アクティビティについて説明します。

> 注**:**
>
> プロバイダー管理の設定では、プロバイダー管理者はすべての GUI ページの [インフラストラクチャ**] > [Orchestrator** 診断**]** にアクセスできます。顧客管理者は、プラットフォームのイベントとログ、****** およびプラットフォームヘルス ****** GUI ページのみを表示できます。

プラットフォームイベントとログ

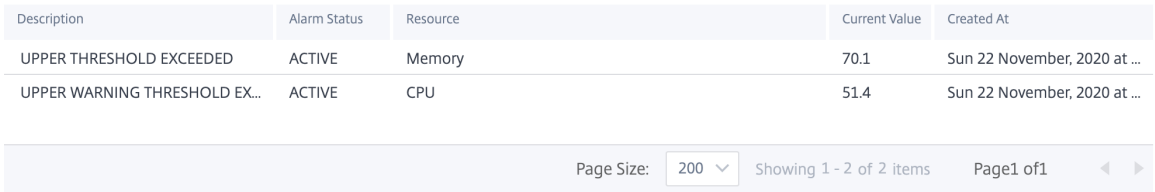
システム内の CPU、メモリ、ストレージなどのプラットフォームレベルの属性の変更は、イベントとして記録され、オンプレミス用 Citrix SD-WAN Orchestrator に表示されます。

たとえば、CPU 使用率が設定された制限を超えると、プラットフォームイベントがログに記録され、アラームがトリガーされます。アラームは通知バーに表示されます。CPU 使用率が減少すると、通知はクリアされます。プラットフォームイベントとログページには、トリガーされたすべてのプラットフォーム関連アラームの履歴が保持されます。CPU 使用率が減少すると、アラームステータスは INACTIVE になります。それでも制限を超えている場合、アラームステータスは ACTIVE のままです。

プラットフォームイベントを表示するには、[インフラストラクチャ] > [**Orchestrator** 診断] > [プラットフォームイベントとログ] に移動します。

ログに記録されたプラットフォームイベントには、次の詳細が表示されます。

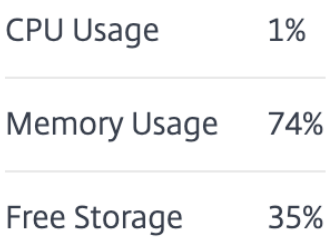
- 説明: プラットフォームイベントの説明。
- アラームステータス: アラームのステータス。プラットフォーム属性が設定された制限を超えると、ステータスは ACTIVE になります。プラットフォームレベルの属性が設定された制限内の値まで下がると、アラームステータスは INACTIVE になります。
- リソース: プラットフォームレベルの属性—CPU、メモリ、またはストレージ。
- 現在の値: 記録されたプラットフォーム属性の最新の値。
- 作成日: プラットフォームイベントが発生した日時。



プラットフォームヘルス

オンプレミスプラットフォーム用 Citrix SD-WAN Orchestrator の状態を表示できます。ヘルス情報には、CPU 使用率、メモリ使用量、使用可能な空きストレージのリアルタイム値 (パーセンテージ) が含まれます。

プラットフォームの状態を確認するには、[インフラストラクチャ] **> [Orchestrator** 診断] **> [**プラットフォームヘルス] に移動します。

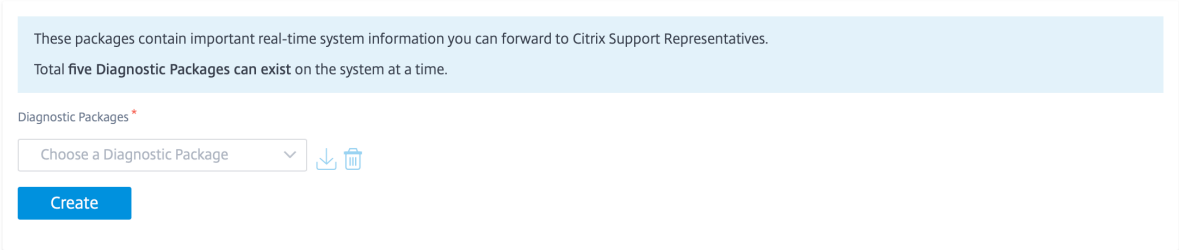


診断情報

診断パッケージは、システムログファイル、システム情報、およびサポートチームがシステムの問題を診断および解決するのに役立つその他の必要な詳細で構成されています。

診断パッケージを作成するには、[インフラストラクチャ] > [**Orchestrator** 診断] > [診断情報] に移動します。[**Create**] をクリックします。パッケージを作成したら、それをコンピューターにダウンロードして、サポートチームと共有できます。

> 注:
>
> オンプレミス向け Citrix SD-WAN Orchestrator は、一度に最大 5 つの診断パッケージを保存できます。

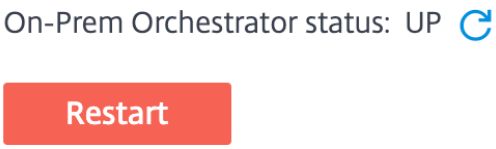


オンプレミスアプリ用 **Citrix SD-WAN Orchestrator** を再起動します

オペレーティングシステム（OS）を再起動せずに、オンプレミスアプリ用 Citrix SD-WAN Orchestrator のみを再起動できます。再起動中、Citrix SD-WAN Orchestrator for On-Premises アプリがオフラインになり、すべての

サービスが利用できなくなります。再起動が完了するまでに約 6 分かかります。再起動後、オンプレミス用 Citrix SD-WAN Orchestrator ログインページが表示されます。

Citrix SD-WAN Orchestrator for On-Premises アプリを再起動するには、[インフラストラクチャ] **> [Orchestrator** 診断] **> [Orchestrator** アプリケーションの再起動] に移動します。[再起動] をクリックし 、**[**はい、再起動]

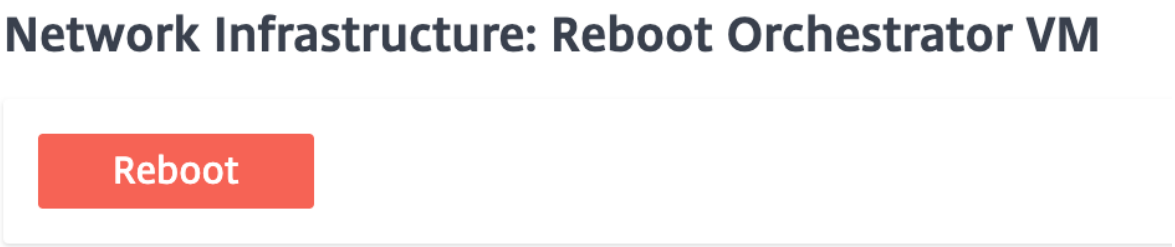


オンプレミス仮想マシン用 **Citrix SD-WAN Orchestrator** を再起動する

再起動プロセスにより、オンプレミス用 Citrix SD-WAN Orchestrator のオペレーティングシステム（OS）が再起動されます。再起動中、オンプレミス用 Citrix SD-WAN Orchestrator はオフラインになり、すべてのサービスが利用できなくなります。再起動が完了するまでに約 6 ～8 分かかります。再起動後、オンプレミス用 Citrix SD-WAN Orchestrator ログインページが表示されます。

トラブルシューティングアクティビティの一部として、またはメンテナンスアクティビティ中に、オンプレミス用 Citrix SD-WAN Orchestrator を再起動できます。

再起動するには、[インフラストラクチャ] **> [Orchestrator** 診断] **> [Orchestrator** 仮想マシンの再起動] に移動します。再起動をクリックし、はい再起動をクリックして確定します。



アラーム

October 26, 2022

オンプレミス向け Citrix SD-WAN Orchestrator に関連するプラットフォーム固有およびサービス固有のアラームを表示できます。プラットフォーム固有のアラームは、ストレージの問題、RAM、CPU などのプラットフォーム関連のアラートを表示します。サービスアラームには、オンプレミス用 Citrix SD-WAN Orchestrator で実行されているマイクロサービスのステータスが表示されます。

アラームを表示するには、Citrix SD-WAN Orchestrator for On-Premises UI の右上隅にあるベルのアイコンをクリックし、必要に応じて [プラットフォームアラーム] または [サービスアラーム] を選択します。