Citrix SD-WAN Center 11.4

Machine translated content

Disclaimer

Contents

システム要件とインストール

February 18, 2022

Citrix SD-WAN Center を 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、シングルリージョンネットワークとマルチリージョンネットワークの両方で共通です。

ハードウェア要件

Citrix SD-WAN Center には、次のハードウェア要件があります。

プロセッサ

- 最大 64 サイトを管理するサーバーには、4 コア、3 GHz（または同等の）プロセッサー以上。
- 最大 128 のサイトを管理するサーバーには、8 コア、3 GHz（または同等の）プロセッサー以上。
- 最大 256 サイトを管理するサーバーには、16 コア、3 GHz（または同等）プロセッサー以上。
- 32 コア、3 GHz（または同等）のプロセッサ、または最大 550 サイトを管理するサーバーに最適。

メモリ

- 最大 64 のサイトを管理する VM には、最低 8GB の RAM を強くお勧めします。
- 最大 128 のサイトを管理する VM には、最低 16GB の RAM を強くお勧めします。
- 最大 256 サイトを管理する VM には、最低 32GB の RAM を強くお勧めします。
- 最大 550 サイトを管理する VM には、最低 32GB の RAM を強くお勧めします。

ディスクスペースの要件

次の表に、Citrix SD-WAN Center データストレージのディスク容量要件を決定するためのガイドラインを示します。SSD が 5000 ～10000 IOPS のダイレクトアクセスストレージを使用します。

推定ディスク容量要件

# クライアントサイト	平均 # サイトごとの WAN リンク	平均 # Intranet/Internet サイトごとのサービス	平均 # サイトごとの仮想パス	**1** 年間のデータベースサイズ（**TB**）
32	2	2	2	1.2T
32	4	4	4	1.8T
32	8	8	8	5.3T
64	2	2	2	1.5T
64	4	4	4	2.6T
64	8	8	8	9.6T
96	2	2	2	1.8T
96	4	4	4	3.3T
96	8	8	8	14.0T
128	2	2	2	2.0T
128	4	4	4	4.1T
128	8	8	8	18.0T
192	2	2	2	2.6T
192	4	4	4	5.6T
192	8	8	8	27.0T
256	2	2	2	3.0T
256	4	4	4	7.2T
256	8	8	8	35.0T
550	2	2	2	15.9T
550	4	4	4	41.9T
550	8	8	8	195.6T

ネットワーク帯域幅

次の表に、Citrix SD-WAN Center VM のネットワーク帯域幅要件を決定するためのガイドラインを示します。

推定ネットワーク帯域幅要件

# クライアントサイト	平均 # WAN リンク	平均 # サイトごとの仮想パス	**5** 分ポーリングごとの合計 **VWAN** データ（**MB**）	**5** 分ポーリングごとに構成する帯域幅レート（**Kbps**）
32	2	2	1.2	デフォルト 1000
32	4	4	3.6	デフォルト 1000
32	8	8	20.0	デフォルト 1000
64	2	2	2.3	デフォルト 1000
64	4	4	7.2	デフォルト 1000
64	8	8	40.0	2000
96	2	2	3.5	デフォルト 1000
96	4	4	10.8	デフォルト 1000
96	8	8	60.0	3000
128	2	2	4.6	デフォルト 1000
128	4	4	14.4	デフォルト 1000
128	8	8	80.0	4000
192	2	2	6.9	デフォルト 1000
192	4	4	21.6	2000
192	8	8	120.0	6000
256	2	2	9.2	デフォルト 1000
256	4	4	28.8	2000
256	8	8	160	10000
550	2	2	34.0	2000
550	4	4	89.3	6000
550	8	8	415.7	24000

ソフトウェア

Citrix SD-WAN Center VPX 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 サーバー、バージョン 6.5。
- Citrix XenServer 6.5 以降。

- Microsoft Hyper-V 2012 R2 以降。

クラウドプラットフォーム

- Microsoft Azure
- Amazon Web Services

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 Center Web インターフェイスは、次のブラウザー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

Citrix SD-WAN Center 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）および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。
- DHCP サーバーを利用可能にし、SD-WAN ネットワークで構成することをお勧めします。
- Citrix SD-WAN Center のインストールファイルが必要です。

> 注
>
> Citrix SD-WAN Center でサードパーティソフトウェアをカスタマイズまたはインストールすることはできません。ただし、vCPU、メモリ、ストレージの設定は変更できます。

Citrix SD-WAN Center ソフトウェアのダウンロード

[ダウンロード] ページから、必要なリリースとプラットフォーム用の Citrix SD-WAN Center Management Console ソフトウェアインストールファイルをダウンロードします 。

Citrix SD-WAN Center のインストールファイルは、次の命名規則を使用しています。

ctx-sdwc バージョン番号-プラットフォーム拡張子

- version_number Citrix SD-WAN Center のリリースバージョン番号です。**
- *platform* は、プラットフォームタイプ、ハイパーバイザー、またはクラウドプラットフォーム名です。
- *extension* は、インストールファイルの拡張子です。

プラットフォーム	ファイル拡張子
Citrix XenServer	xva
VMware ESXi	-vmware.ova
Microsoft Hyper-V	-hyperv.vhd.zip
Microsoft Azure	-azure.vhd.zip

Citrix SD-WAN Center のインストールおよび構成情報を収集する

このセクションでは、Citrix SD-WAN Center 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ます。

- Citrix SD-WAN Center 仮想マシン（VM）をホストする ESXi サーバー、XenServer、Hyper-V サーバー、または Azure の IP アドレス。
- Citrix SD-WAN Center VM に割り当てる一意の名前。
- Citrix SD-WAN Center VM に割り当てるメモリの量。
- VM の仮想ディスクに割り当てるディスク容量。
- Citrix SD-WAN Center が外部ネットワークとの通信に使用する Gateway IP アドレス。
- Citrix SD-WAN Center VM がインストールされるネットワークのサブネットマスク。

ESXi サーバーに **Citrix SD-WAN Center** をインストールして構成する

April 13, 2021

VMware VSphere クライアントをインストールする

次に、Citrix SD-WAN Center 仮想マシン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を示します。詳細については、VMware vSphere Client のドキュメントを参照してください。

VMware vSphere Client をダウンロードしてインストールするには、次の手順を実行します。

1. ブラウザーを開き、vSphere Client および Citrix SD-WAN Center 仮想マシン（VM）インスタンスをホストする ESXi サーバーに移動します。

   VMware ESXi のようこそページが表示されます。

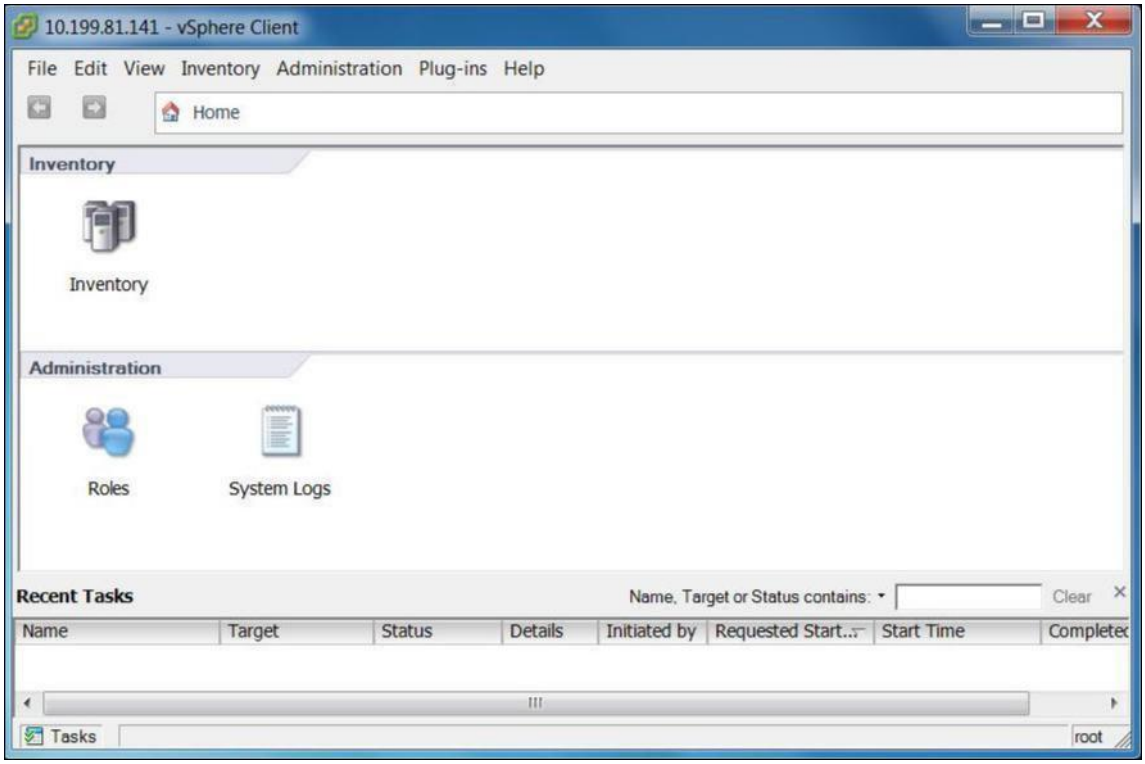
2. [**vSphere Client** のダウンロード] リンクをクリックして、vSphere Client インストールファイルをダウンロードします。
3. vSphere Client をインストールします。

   ダウンロードした vSphere Client インストーラーファイルを実行し、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 サーバーのログイン認証情報の入力を求められます。
5. ESXi サーバー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 Center VM 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 Client 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 **Citrix SD-WAN Center VM** の作成

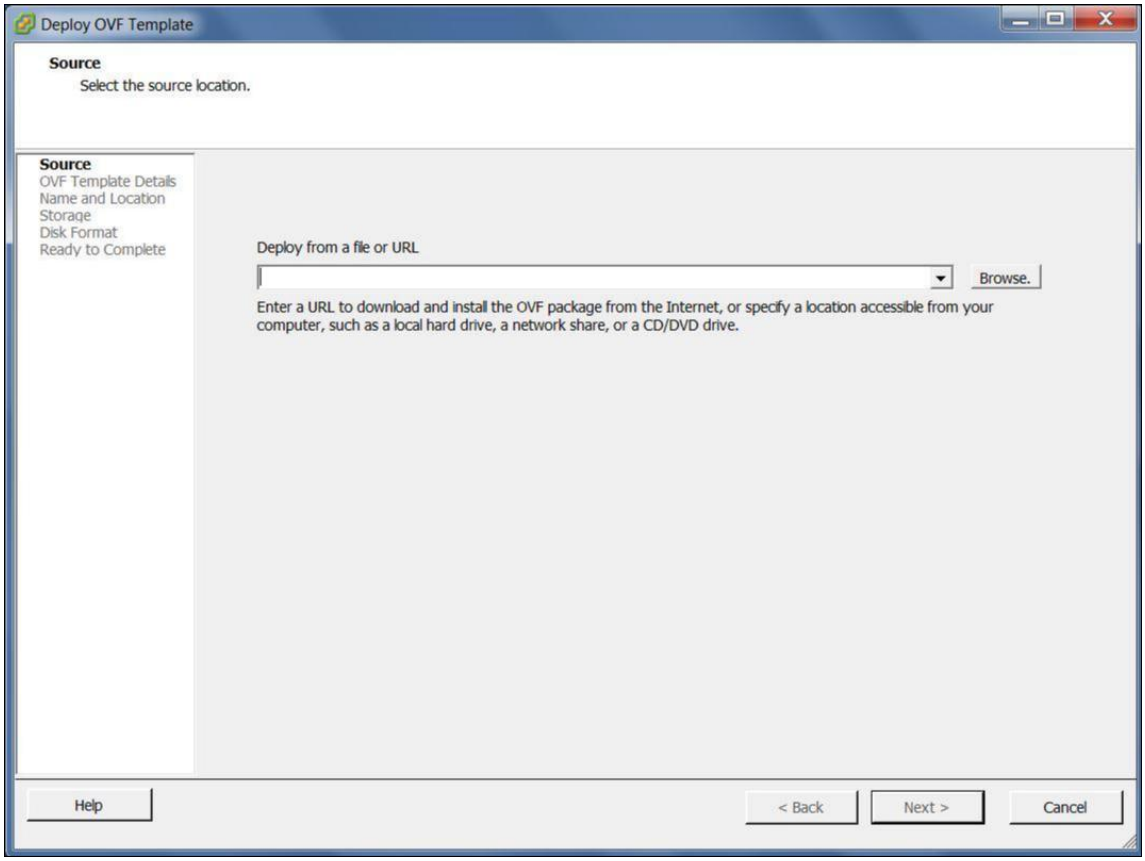
VMware VSphere クライアントをインストールした後、Citrix SD-WAN Center 仮想マシンを作成します。

1. まだ行っていない場合は、Citrix SD-WAN Center 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、[ファイル] をクリックし、ドロップダウンメニューから [**OVF** テンプレートのデプロイ] を選択します。

   OVF テンプレート の展開ウィザードが表示されます。



3. [参照] をクリックして、インストールする Citrix SD-WAN Center OVF テンプレート（.ova ファイル）を選択します。

4. ［次へ］をクリックします。

   ova ファイルがインポートされ、OVF テンプレートの詳細ページが表示されます。

5. ［次へ］をクリックします。

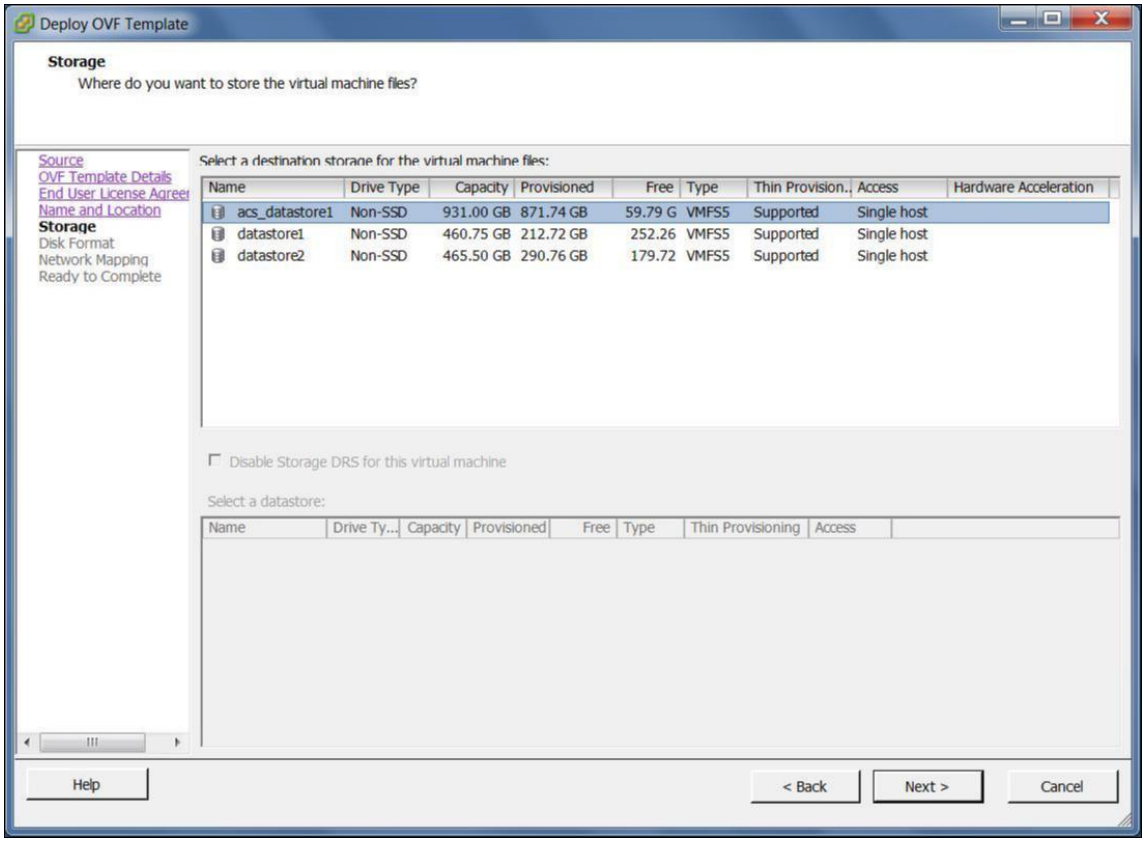
6. エンドユーザー使用許諾契約書] ページで 、**[Accept]** をクリックし、[次へ] をクリックします。

7. [名前と場所] ページで、新しい VM の一意の名前を入力します（またはデフォルト値を受け入れます）。

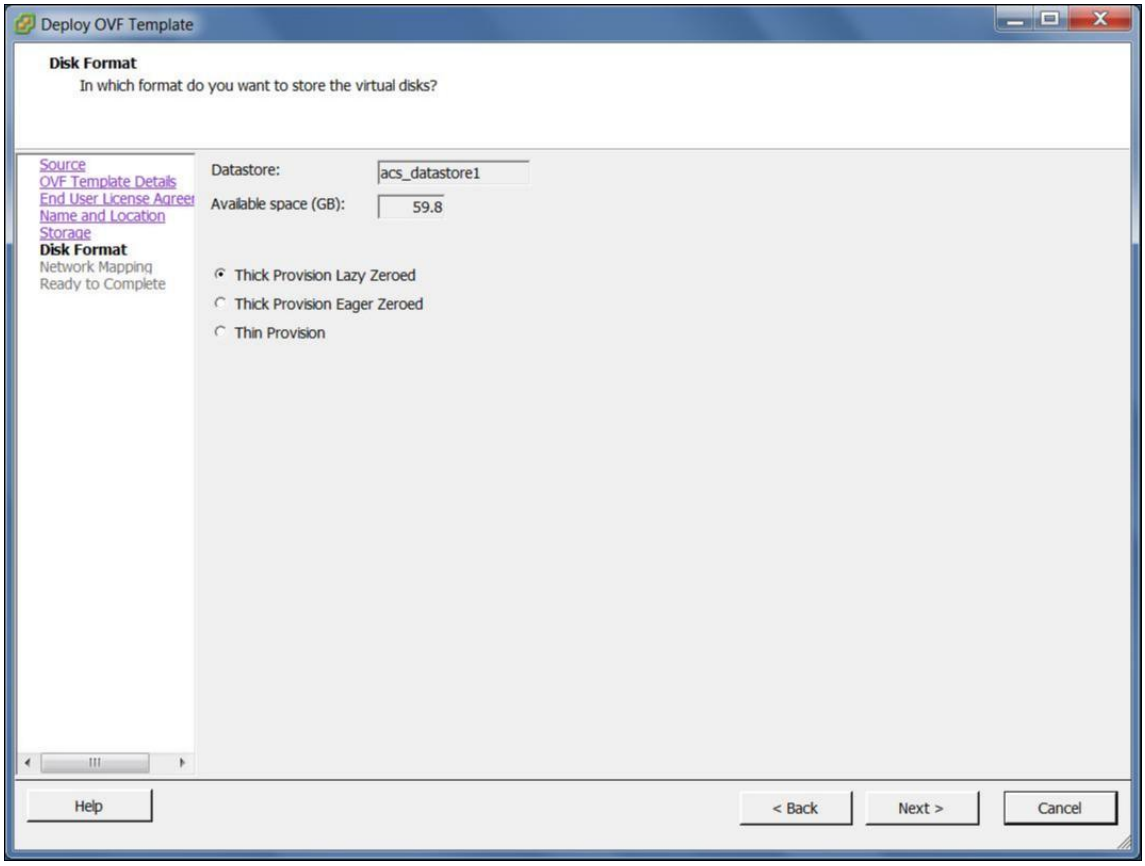
   この名前は、現在の **Inventory** フォルダー内で固有でなければならず、長さは最大 80 文字です。

8. ［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。



9. ここでは、[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受け入れます。データストアを構成することもできます。詳しくは、ESXi サーバーにデータストアを追加して構成するを参照してください。



10. [Disk Format] ページで、デフォルトの設定を受け入れて、[**Next**] をクリックします。
11. [ネットワークマッピング] ページで、デフォルト（VM ネットワーク）を受け入れ、[次へ] をクリックします。
12. [Ready to Complete] ページで、[**Finish**] をクリックして VM を作成します。

    > 注意:
    >
    > ディスクイメージをサーバーに解凍するには、数分かかる場合があります。

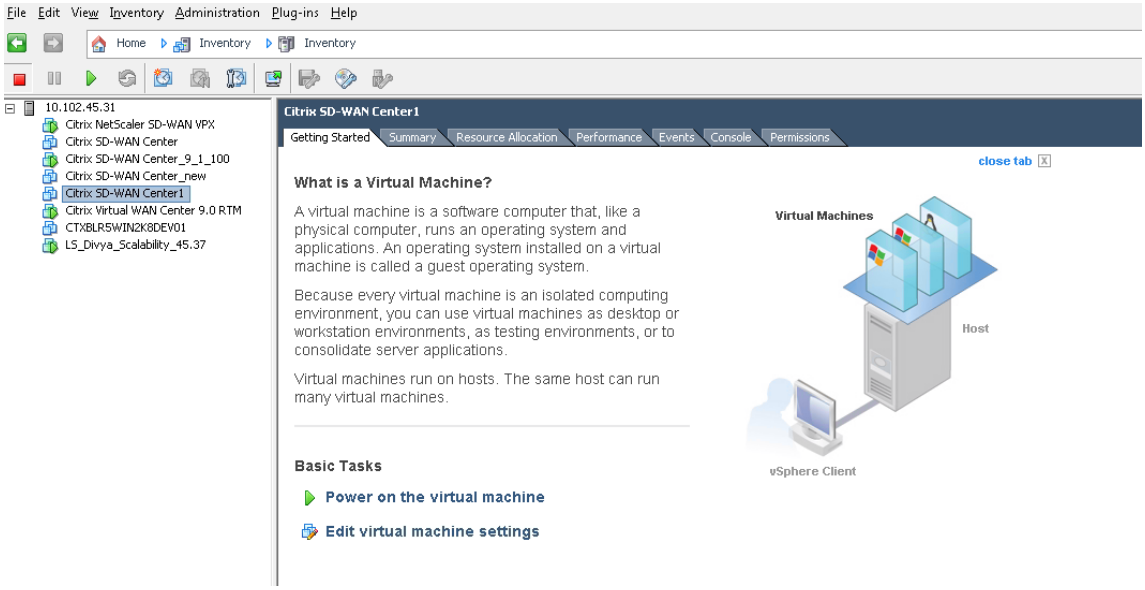
13. ［閉じる］をクリックします。

ESXi サーバーの管理 **IP** アドレスの表示と記録

管理 IP アドレスは SD-WAN Center VM の IP アドレスです。この IP アドレスを使用して、Citrix SD-WAN Center Web UI にログインします。

管理 IP アドレスを表示するには、次の手順を実行します。

1. vSphere クライアントの [インベントリ] ページの インベントリ ツリー（左ペイン）で新しい Citrix SD-WAN Center VM を選択します。

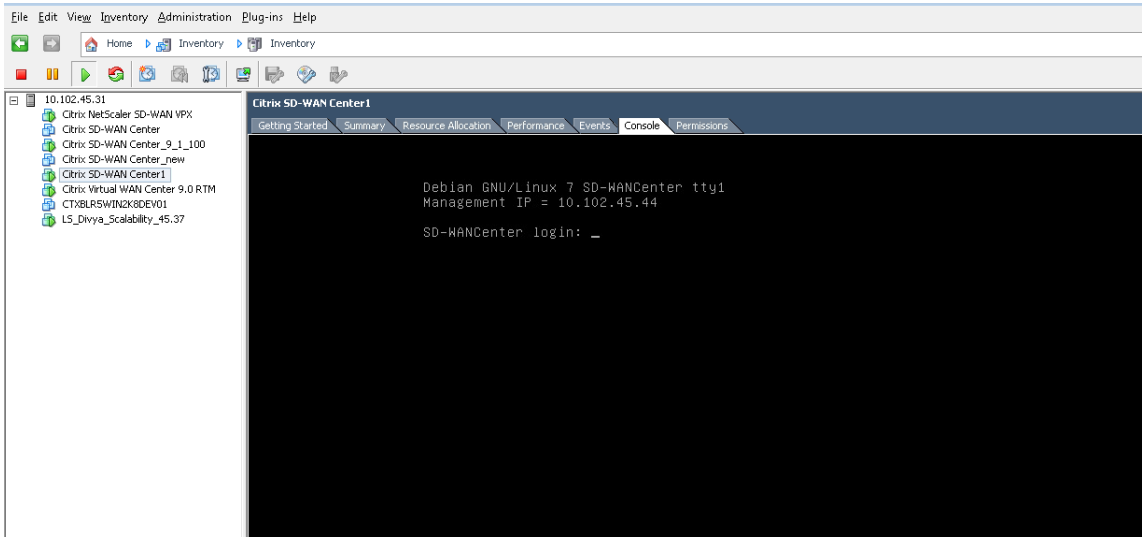


2. Citrix SD-WAN Center ページの [基本タスク] で、[仮想マシンのパワーオン] をクリックします。
3. [コンソール] タブを選択し、コンソール領域内の任意の場所をクリックして、コンソールモードに入ります。

   これにより、マウスカーソルの制御が VM コンソールに移ります。

   > 注意
   >
   > カーソルのコンソール制御を解放するには、< Ctrl> 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。

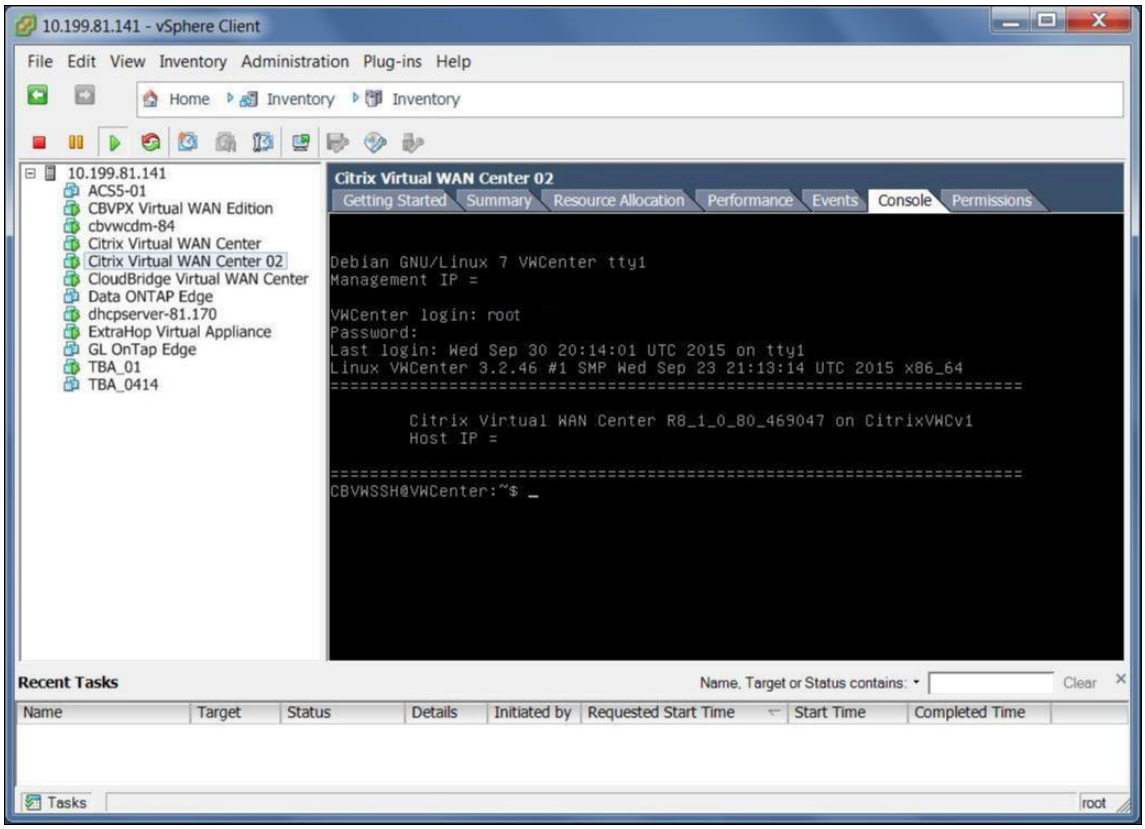


5. VM コンソールにログインします。

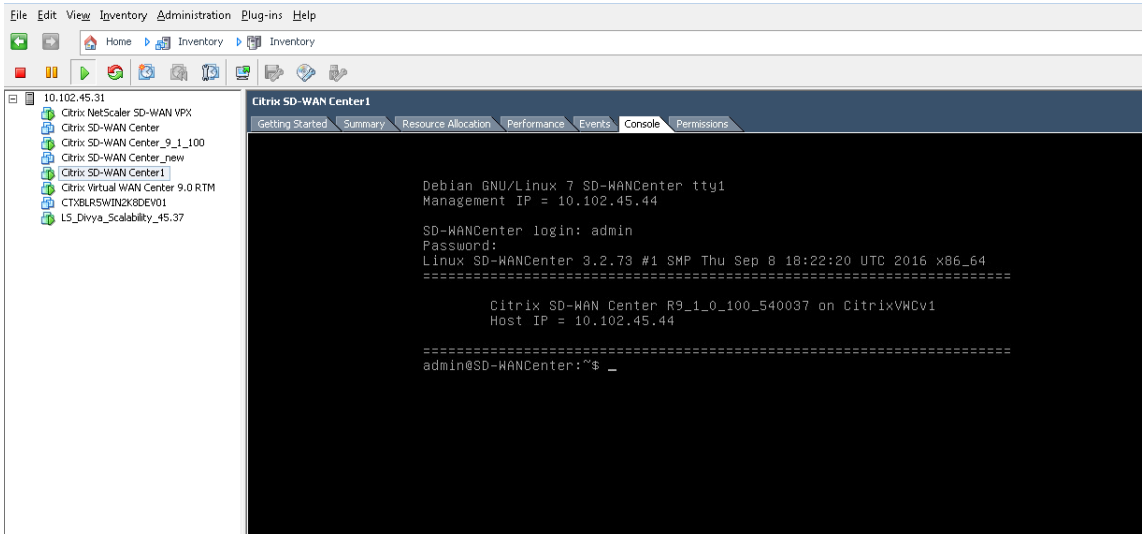
   新しい Citrix SD-WAN Center VM のデフォルトのログイン認証情報は次のとおりです。

   - ログイン: admin

- パスワード: password



6. Citrix SD-WAN Center VM 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 サーバーが存在し、SD-WAN ネットワークで利用可能である必要があります。そうでない場合、この手順は完了できません。

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 アドレスとして構成するには:

1. VM が起動したら、[コンソール] タブをクリックします。
2. VM にログインします。新しい Citrix SD-WAN Center VM のデフォルトのログイン認証情報は次のとおりです。

   ログインする: 管理者

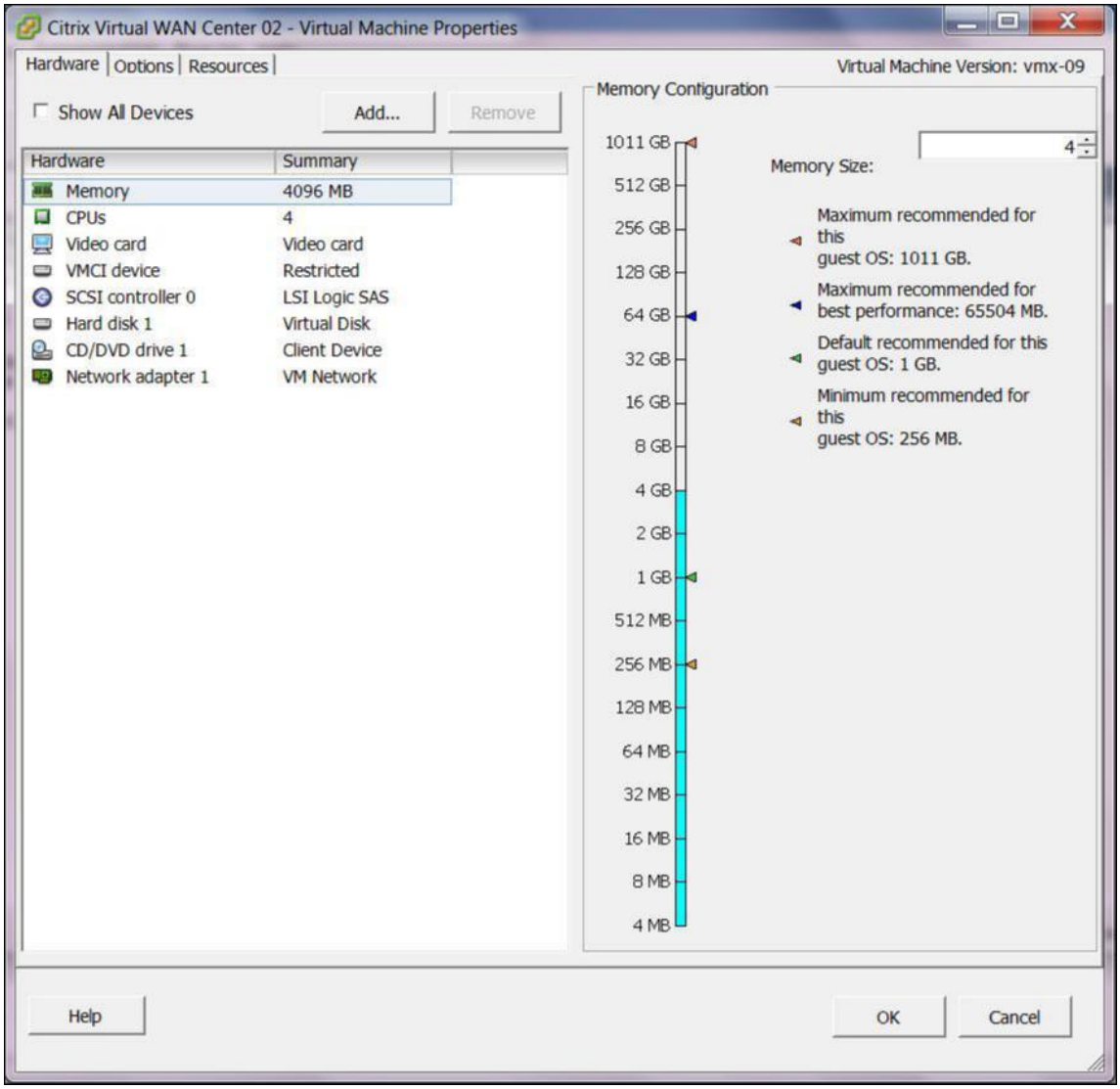
   Password: password
3. コンソールで CLI コマンドを入力します management_ip 。**
4. コマンドセットインターフェイスを入力してください < ipaddress> < サブネットマスク > < gateway> 、管理 IP を構成します。

ESXi サーバーでのデータストアの追加と構成

Citrix SD-WAN Center からの統計を保存するデータストアを追加および構成できます。

データストアを追加して構成するには:

1. vSphere クライアントで、[インベントリ] アイコンをクリックして [インベントリ] ページを開きます。
2. Citrix SD-WAN Center VM ホストサーバーの インベントリ ツリーブランチを展開します。
3. 左側のペインで、+ 作成した Citrix SD-WAN Center VM をホストするサーバーの IP アドレスの横 **
4. 編集のために新しい Citrix SD-WAN Center VM を開きます。
5. インベントリ ツリーで、作成した Citrix SD-WAN Center VM の名前を右クリックし、ドロップダウンメニューから [設定の編集] を選択します。

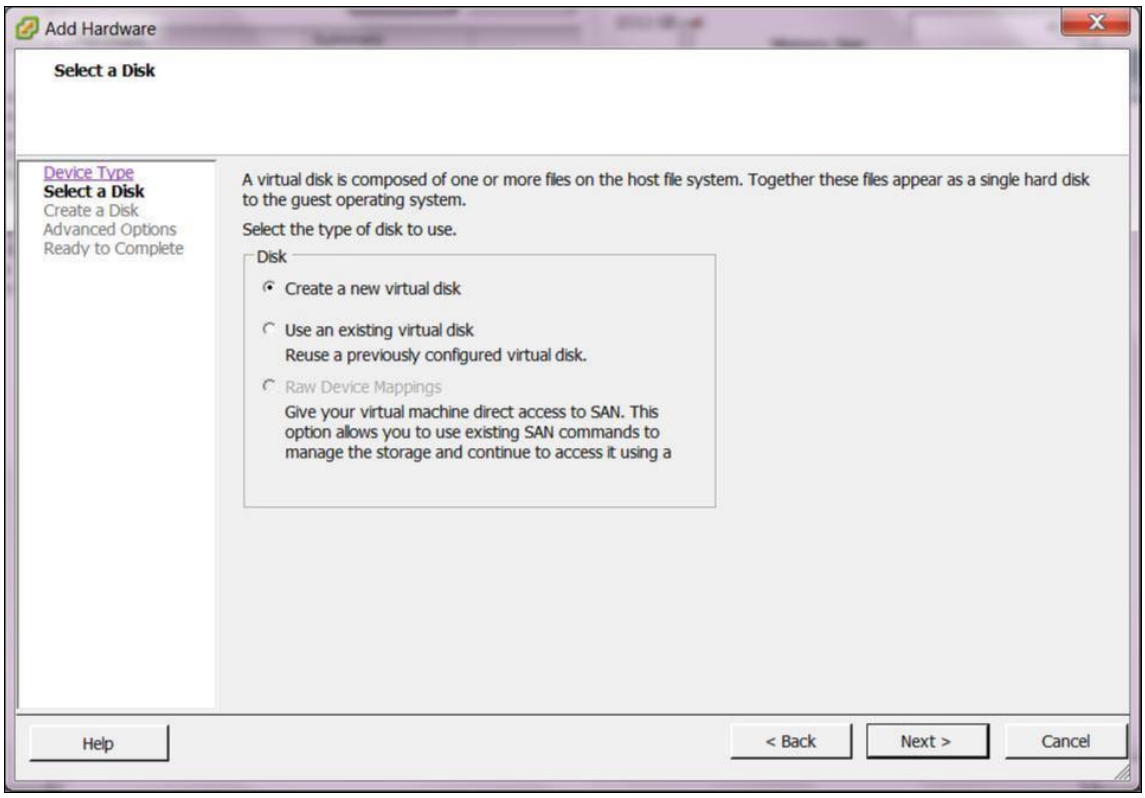


6. [メモリサイズ] フィールドに、この VM に割り当てるメモリの量を入力します。

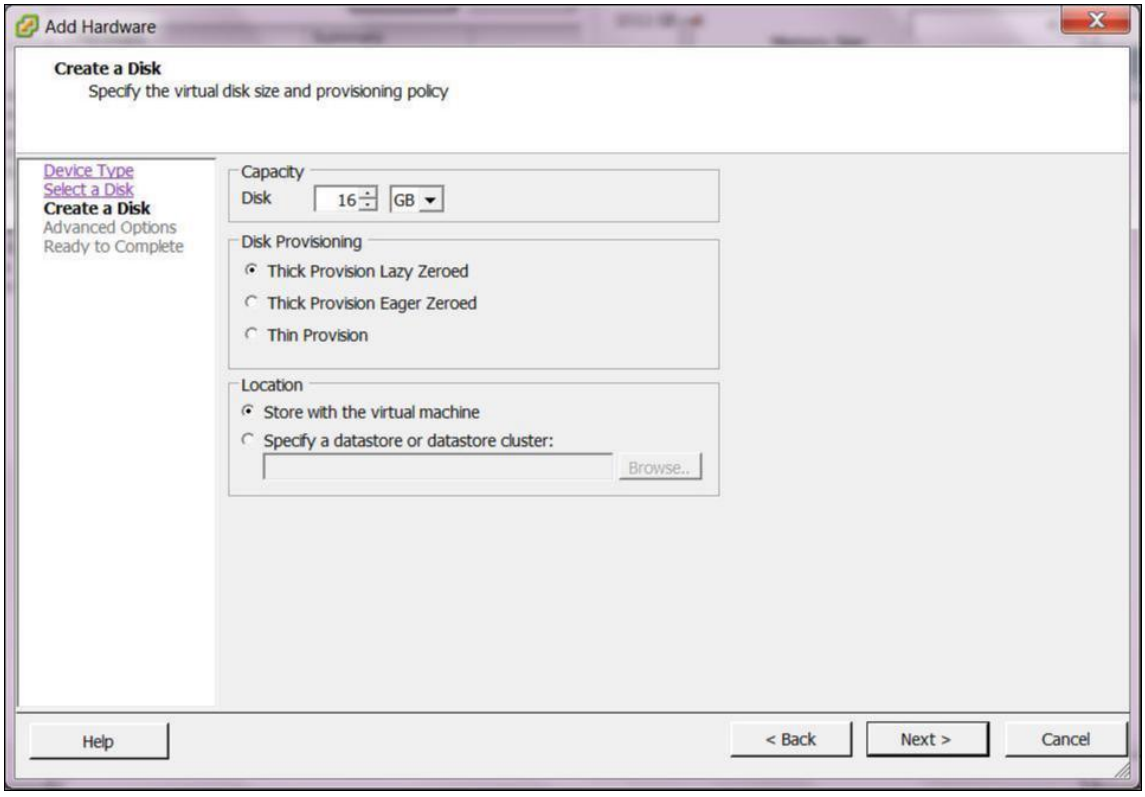
   詳しくは、「メモリ要件」を参照してください。

7. [追加] をクリックします。

8. ハードウェアの追加ウィザードの [デバイスの種類] ページで、[ハードディスク] を選択し、[次へ] をクリックします。

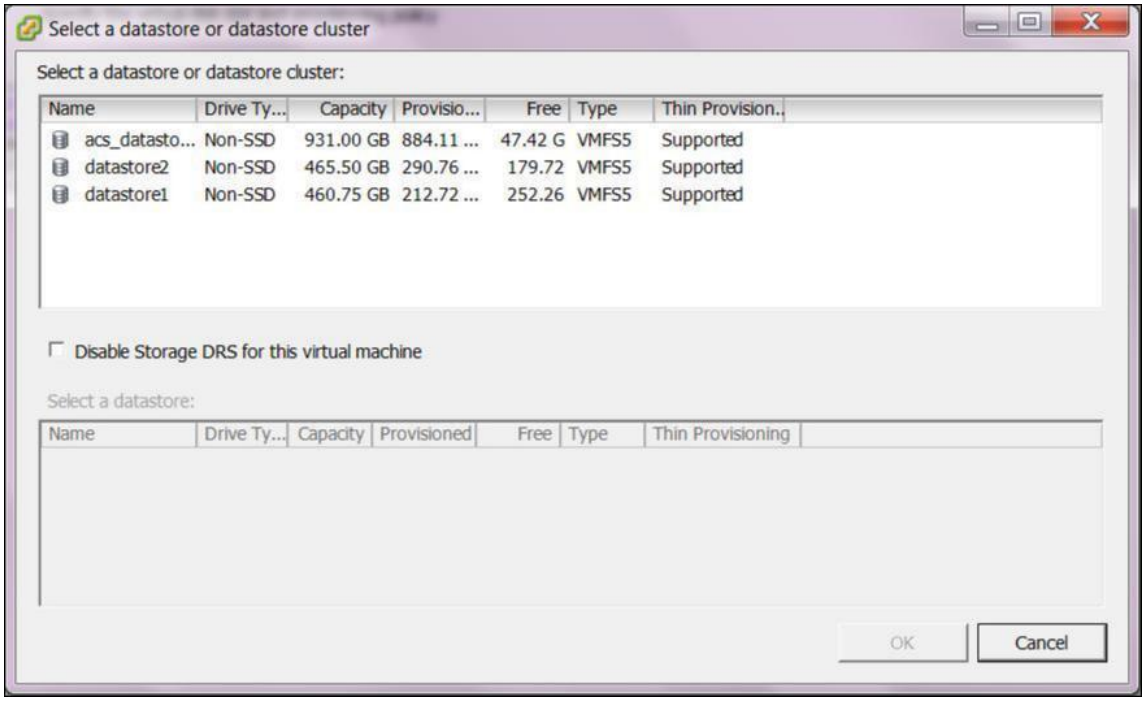


9. [Select a Disk] ページで、[**Create a new virtual disk**] を選択し、[**Next**] をクリックします。

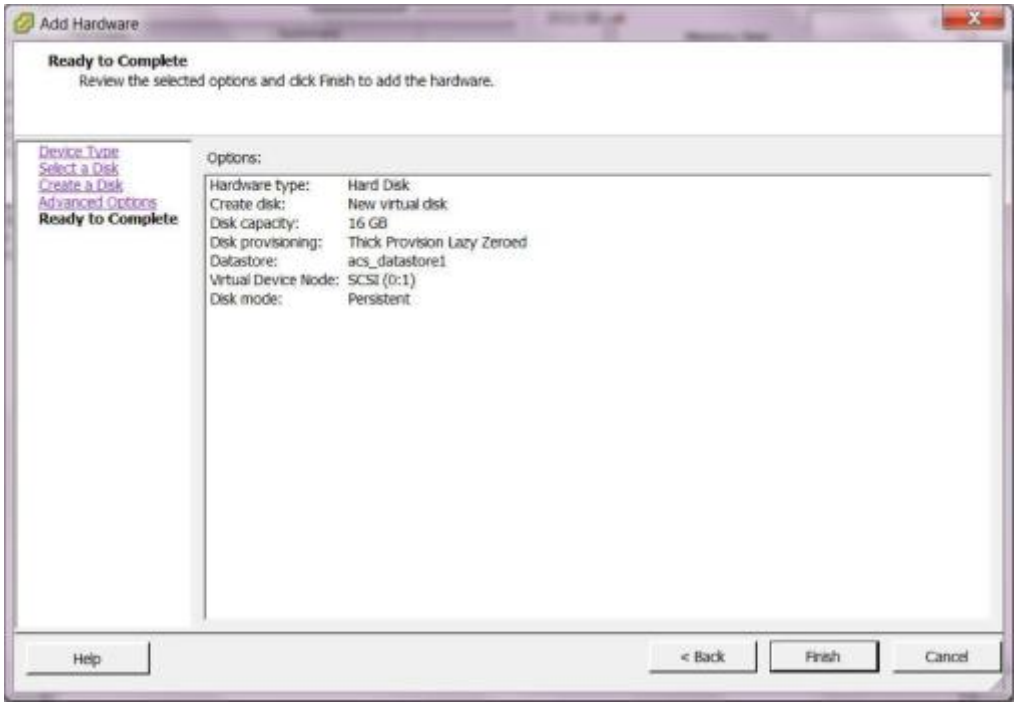


10. [ディスクの作成] ページの [容量**]** セクションで、新しい仮想ディスクのディスク容量を選択します。

11. [ディスクのプロビジョニング] セクションで、[シックプロビジョニングレイジーゼロ**]**（デフォルト）を選択します。
12. [場所] セクションで、[データストアまたはデータストアクラスターの指定**]** を選択します。
13. [**Browse**] をクリックします。



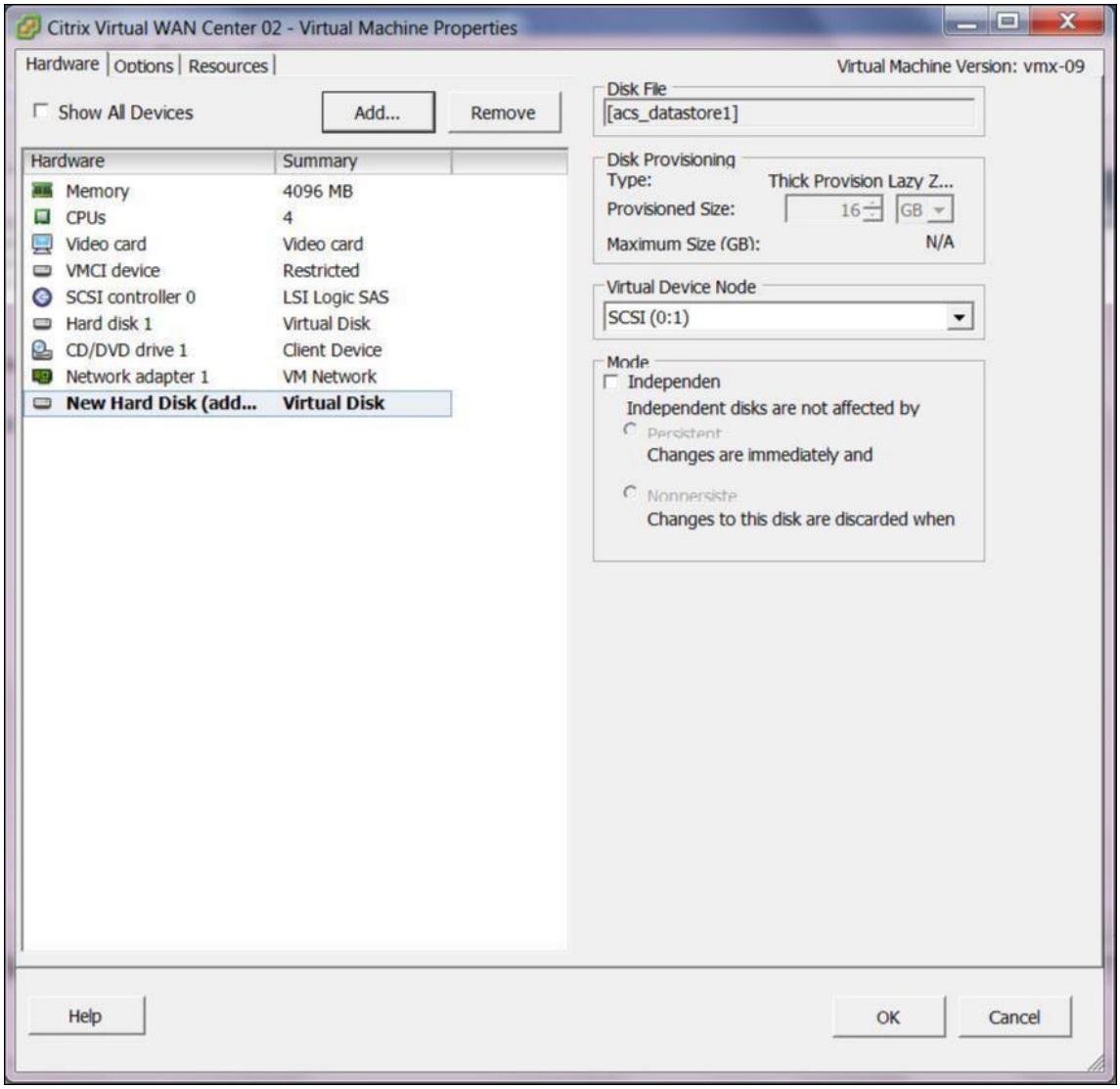
14. 十分な空き容量があるデータストアを選択し、[**OK**] をクリックします。
15. [次へ] をクリックします。
16. [詳細オプション] ページで、[詳細オプション] のデフォルト設定を受け入れ、[次へ] をクリックします。



17. ［完了］をクリックします。

    これにより、新しい仮想ディスクが追加され、ハードウェアの追加ウィザードが終了して、仮想マシンのプロパティページに戻ります。

18. ［**OK**］をクリックします。



XenServer に **Citrix SD-WAN Center** をインストールして構成する

April 13, 2021

XenServer サーバーに Citrix SD-WAN Center 仮想マシンをインストールする前に、「Citrix SD-WAN Center のインストールと構成情報の収集」の説明に従って必要な情報を収集します。

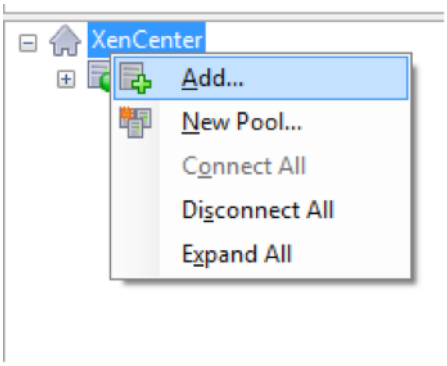
XenServer サーバーをインストールする

Citrix SD-WAN Center 仮想マシンを展開する Citrix XenServer サーバーをインストールするには、XenCenter がコンピューターにインストールされている必要があります。XenCenter をまだダウンロードしていない場合は、

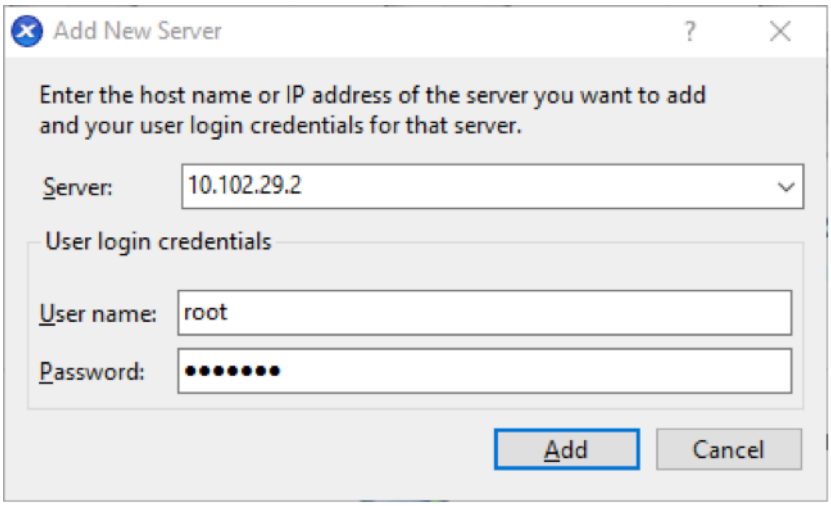
ダウンロードしてインストールします。

XenServer サーバーをインストールするには:

1. コンピューターで 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. [新しいサーバー 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: Citrix SD-WAN Center VM 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。

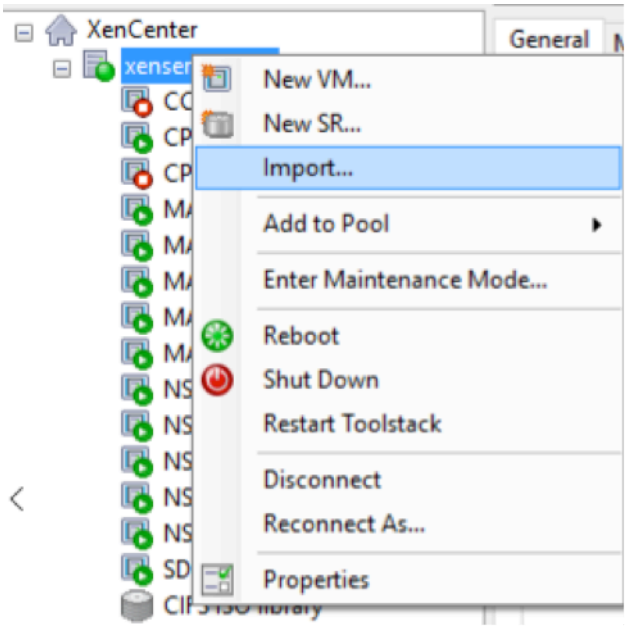
   新しいサーバーの IP アドレスが左側のペインに表示されます。

XVA ファイルを使用して Citrix SD-WAN Center VM を作成する

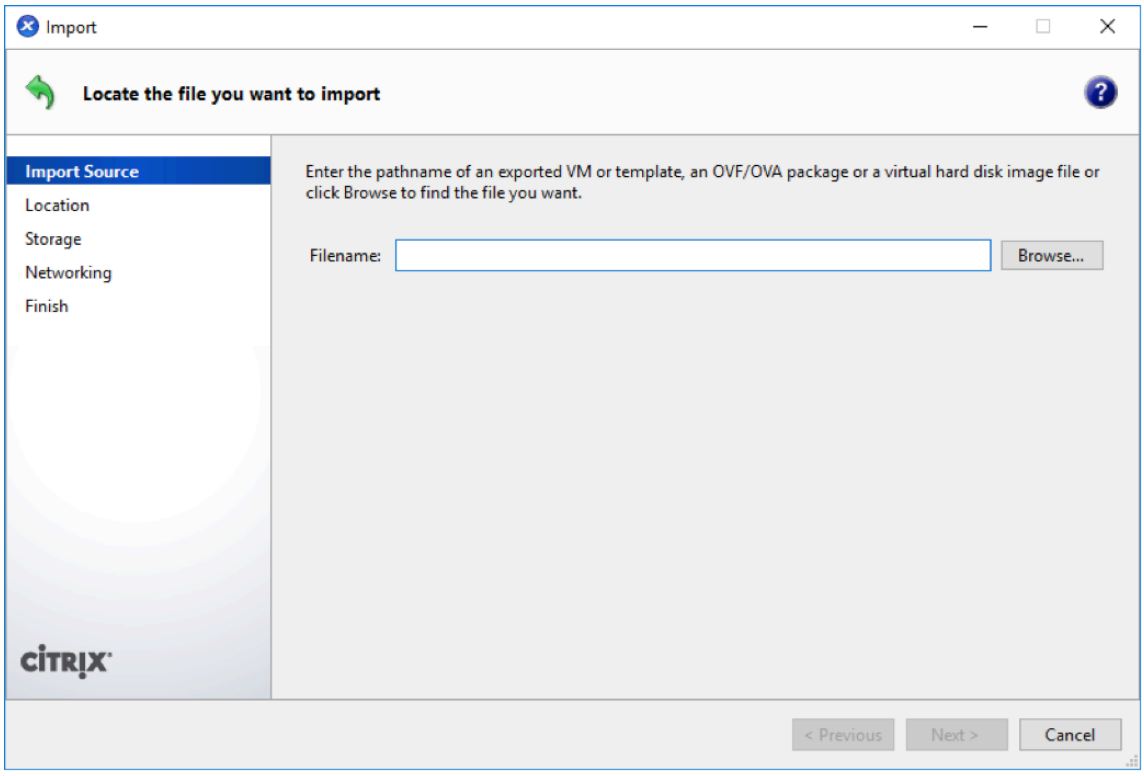
Citrix SD-WAN Center 仮想マシンソフトウェアは、XVA ファイルとして配布されます。まだ行っていない場合は、.xva ファイルをダウンロードします。詳しくは、「システム要件とインストール」を参照してください。

Citrix SD-WAN Center VM を作成するには:

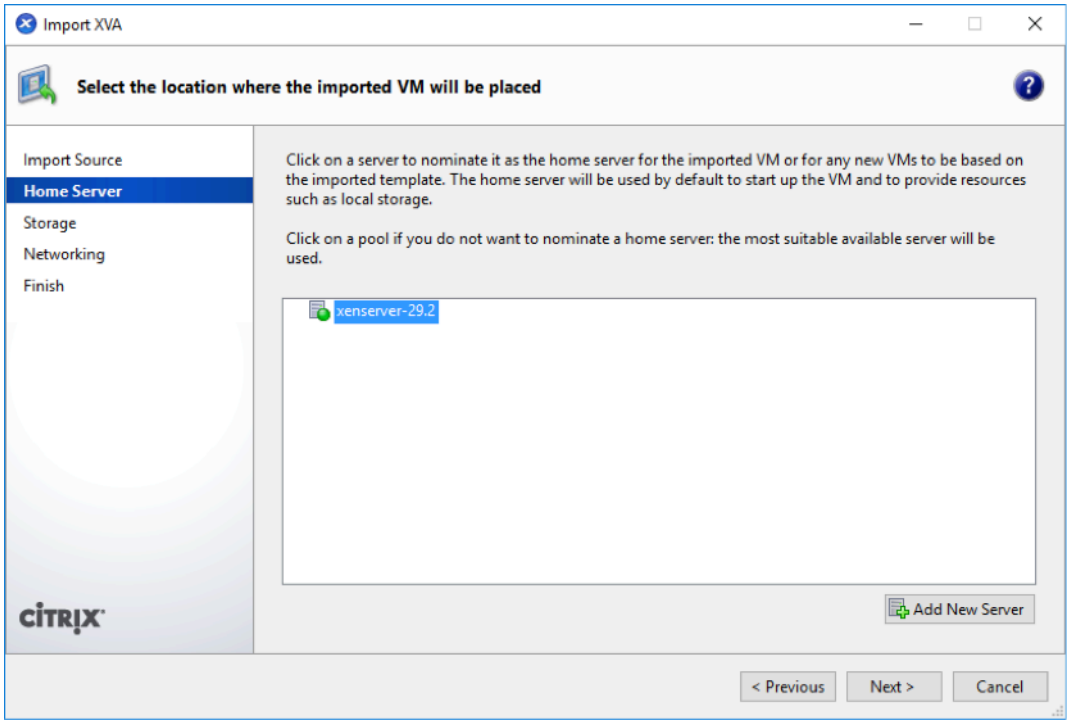
1. XenCenter で、「**XenServer**」を右クリックし、「インポート」をクリックします。



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。

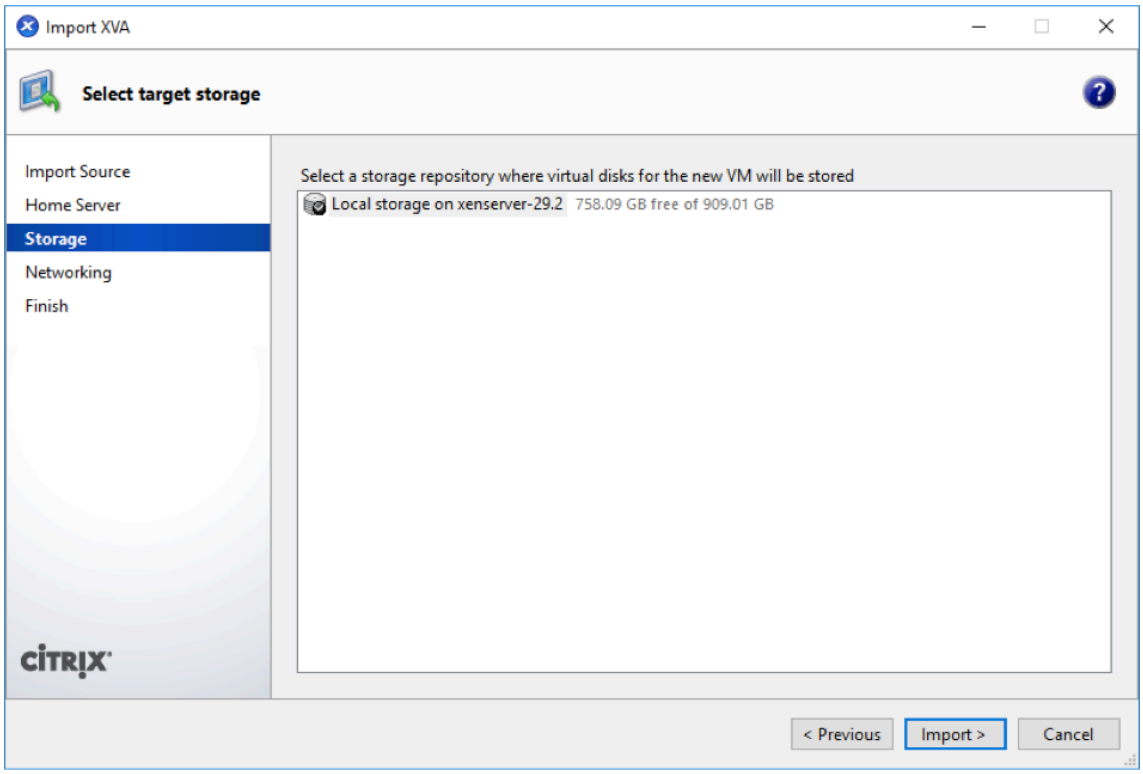


3. VM をインポートする場所として以前に作成した XenServer サーバーを選択し、[次へ] をクリックします。



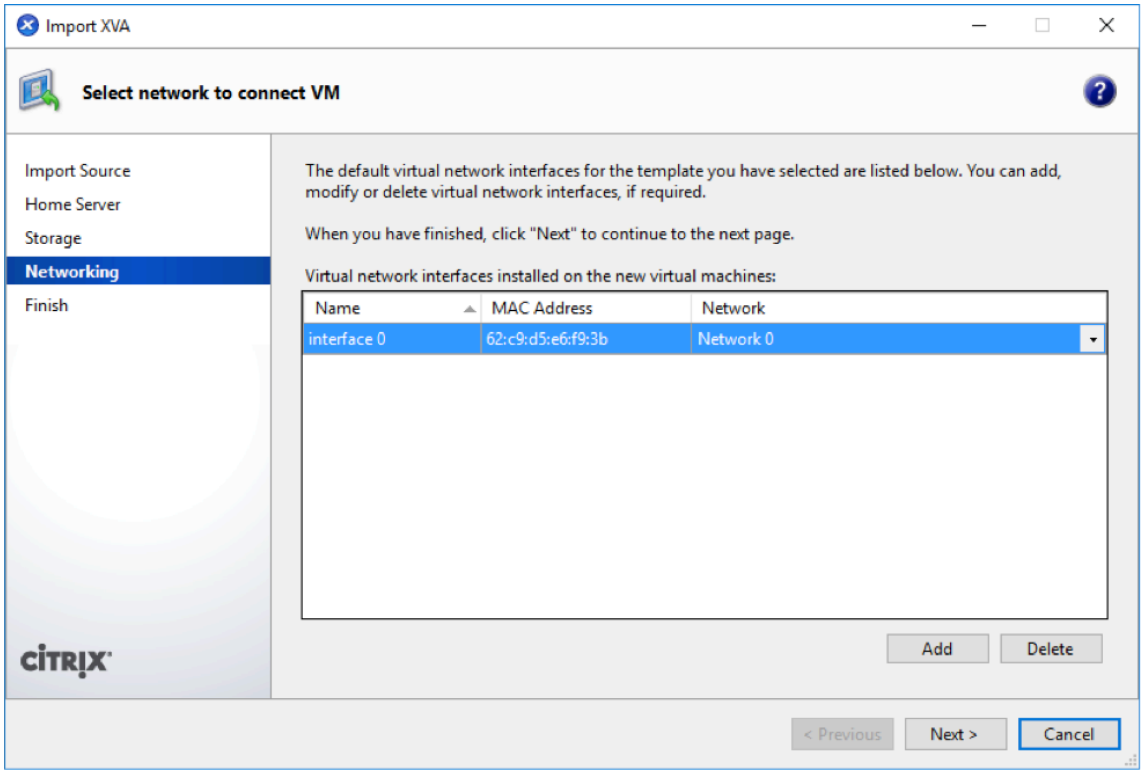
4. 新しい VM の仮想ディスクを保存するストレージリポジトリを選択し、[インポート] をクリックします。

   現時点では、デフォルトのストレージリソースを受け入れることができます。または、データストアを構成できます。詳細については、「**XenServer** でのデータストアの追加と構成」セクションを参照してください。



   インポートされた Citrix SD-WAN Center VM が左側のペインに表示されます。

5. VM 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。

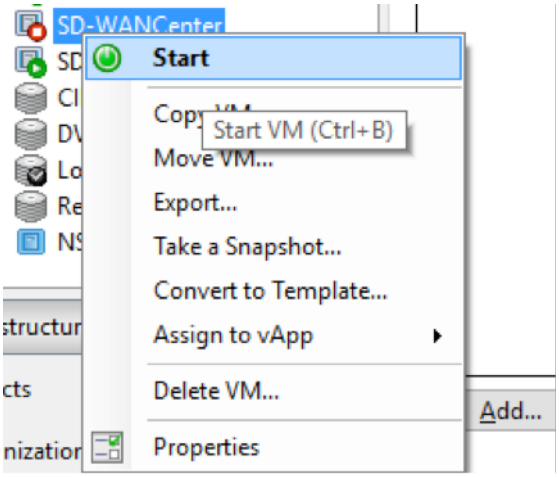
XenServer の管理 IP アドレスの表示と記録

管理 IP アドレスは、Citrix SD-WAN Center VM の IP アドレスです。この IP アドレスを使用して、Citrix SD-WAN Center Web UI にログインします。

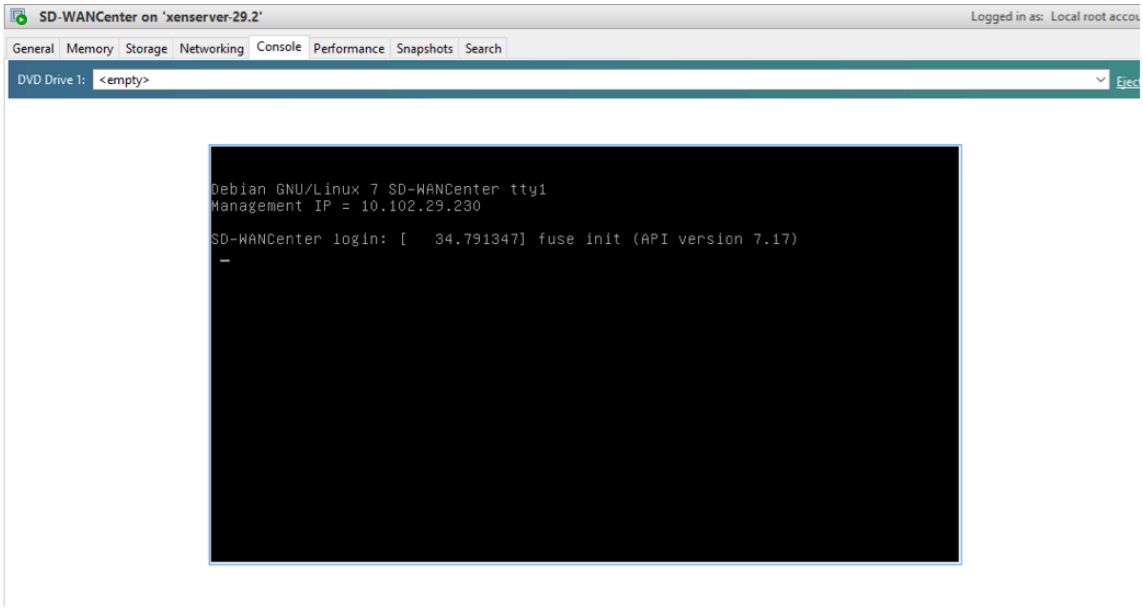
> 注
>
> DHCP サーバーが存在し、SD-WAN ネットワークで利用可能である必要があります。

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、新しい Citrix SD-WAN Center VM を右クリックし、[開始] を選択します。



2. VM 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ます。

> 注
>
> DHCP サーバーが存在し、SD-WAN ネットワークで利用可能である必要があります。そうでない場合、この手順は完了できません。

4. VM にログインします。新しい Citrix SD-WAN Center VM のデフォルトのログイン資格情報は次のとおりです。

   ログイン: 管理者

   Password: password

   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 アドレスとして構成するには:

1. VM が起動したら、[コンソール] タブをクリックします。
2. VM にログインします。新しい Citrix SD-WAN Center VM のデフォルトのログイン認証情報は次のとおりです。

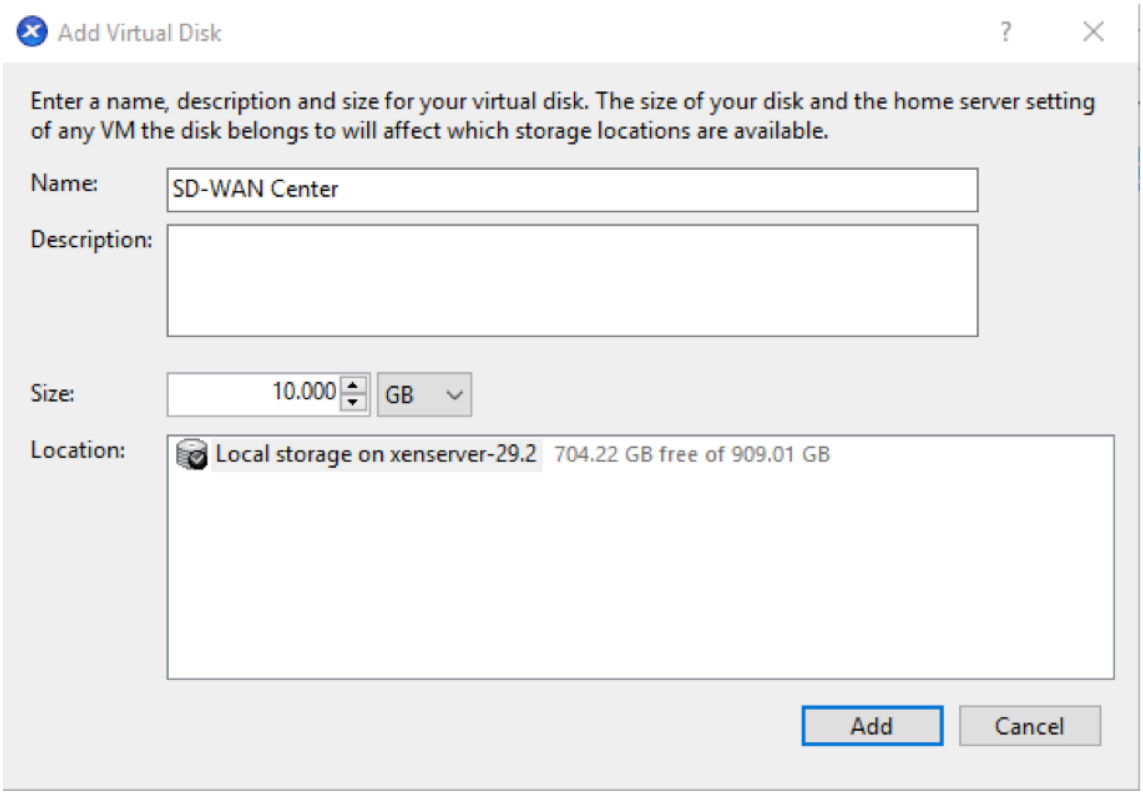
   ログインする: 管理者
   、パスワード: パスワード
3. コンソールで CLI コマンドを入力します management_ip.**
4. コマンド セットインターフェイスを入力してください < ipaddress> < サブネットマスク > < gateway> 、管理 IP を構成します。

XenServer サーバーのデータストレージの追加と構成

Citrix SD-WAN Center からの統計情報を格納するデータストレージを追加および構成できます。

データストレージを追加して設定するには:

1. XenCenter で、Citrix SD-WAN Center VM をシャットダウンします。
2. [ストレージ] タブで、[追加] をクリックします。



3.「名前」フィールドに、仮想ディスクの名前を入力します。

4.「説明」フィールドに、仮想ディスクの説明を入力します。

5.［サイズ］フィールドで、必要なサイズを選択します。

6.［場所］フィールドでローカルストレージを選択します。

7.［追加］をクリックします。

Microsoft Hyper-V に Citrix SD-WAN Center をインストールして構成する

April 13, 2021

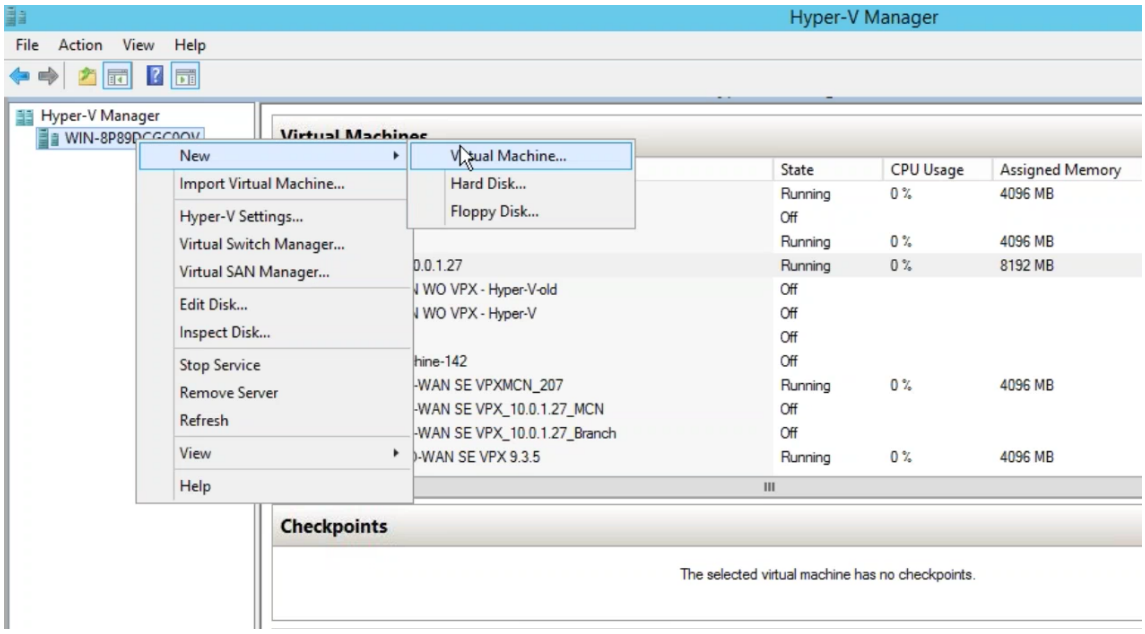
Microsoft Hyper-V サーバーに Citrix SD-WAN Center 仮想マシン（VM）をインストールする前に、「システム要件とインストール」の説明に従って必要な情報を収集します。

システム要件とインストールの Citrix SD-WAN Center ソフトウェアのダウンロードセクションの説明に従って、Hyper-V 用の SD-WAN Center ソフトウェアをダウンロードします。

Windows サーバーで Hyper-V 機能と管理ツールが有効になっていることを確認します。

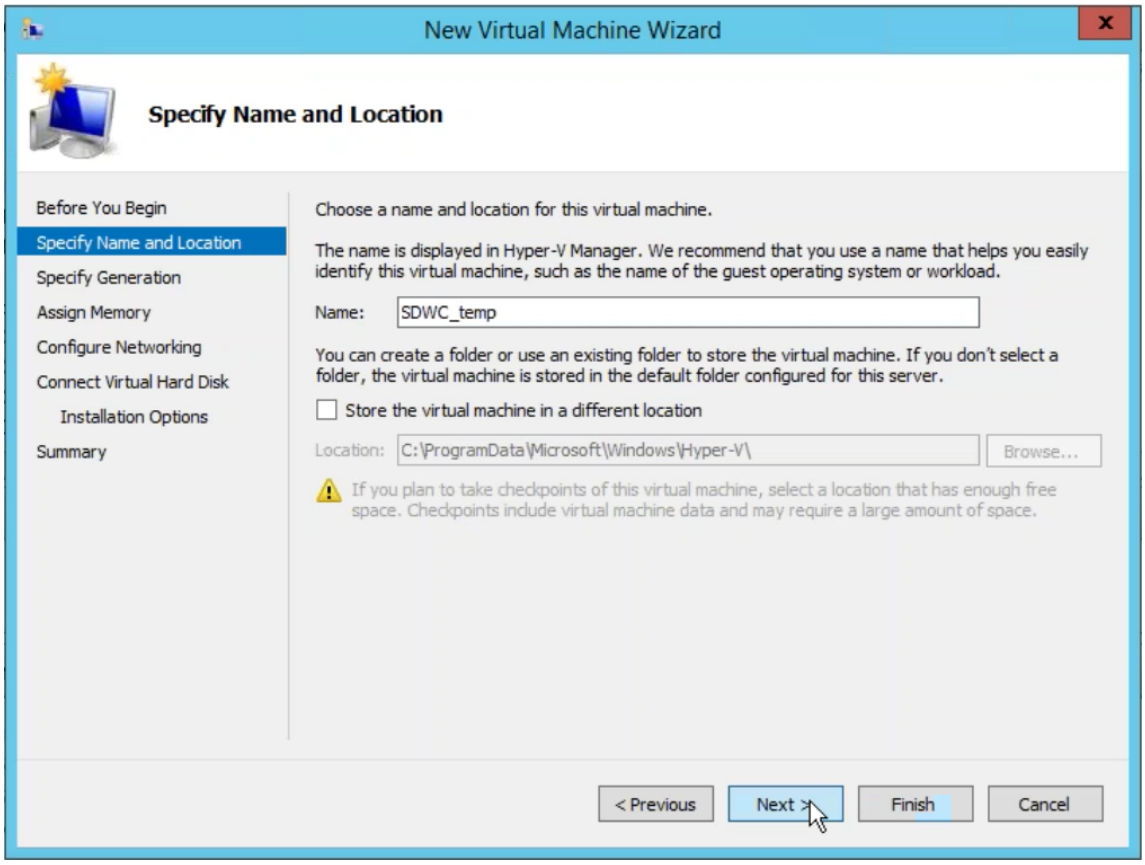
Hyper-V サーバーに SD-WAN Center VM を作成するには：

1. Hyper-V マネージャーで、Hyper-V サーバーを右クリックし、［新規］> 仮想マシンを選択します。。



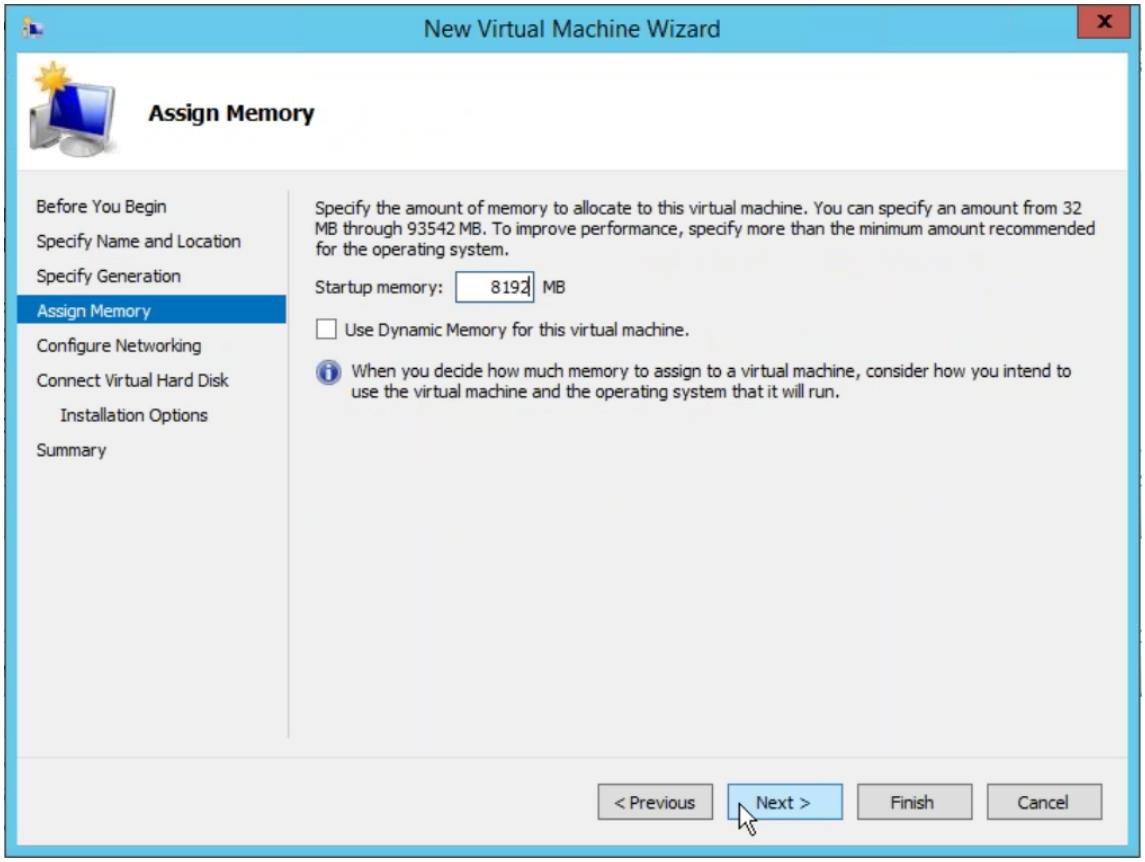
新しい仮想マシンウィザード が表示されます。［次へ］をクリックします。

2. SD-WAN Center VM の名前を指定し、必要に応じて VM ストレージの場所を変更します。次へをクリックします。

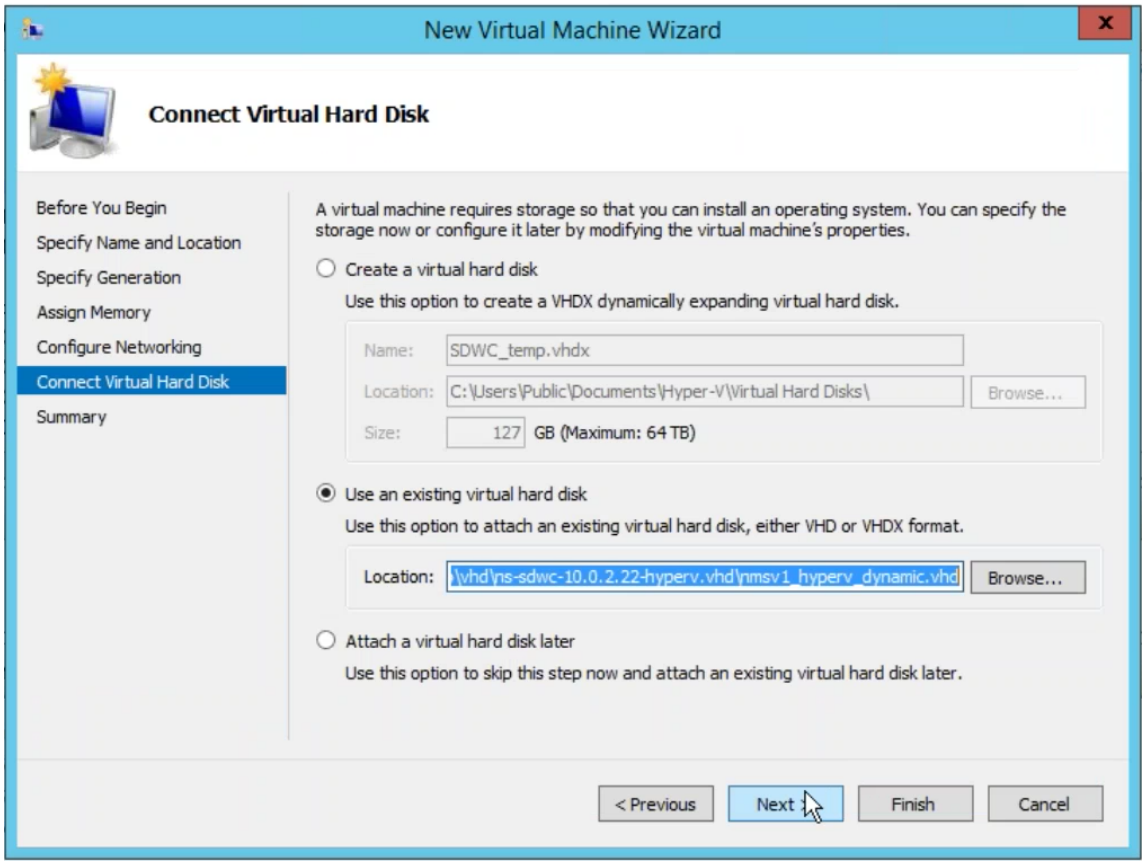


3. 必要な VM 生成を選択します。［次へ］をクリックします。
4. VM に 8 GB のメモリを割り当てます。［次へ］をクリックします。

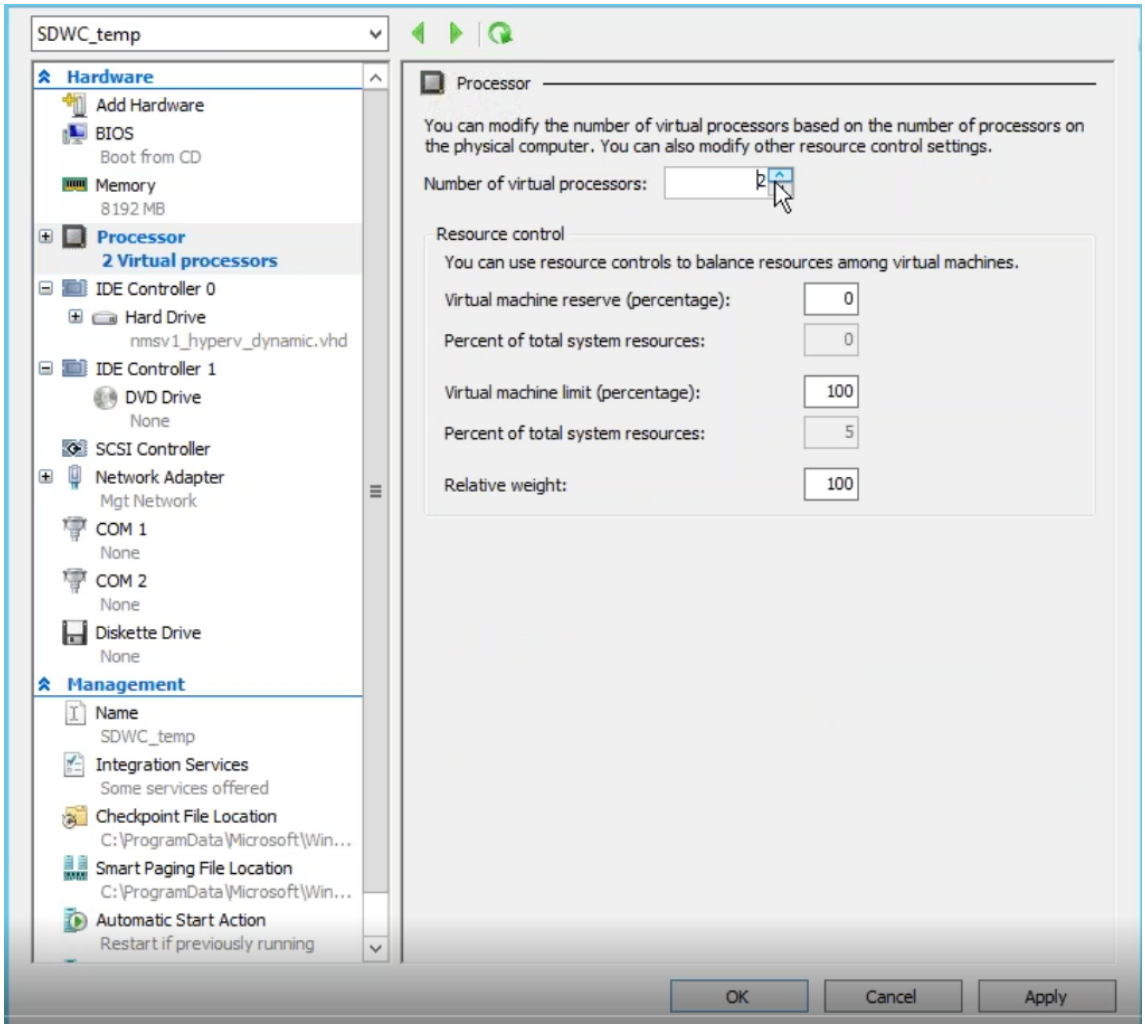
> 注
>
> Citrix SD-WAN Center VM では、最大 64 のサイトを管理するために最低 8 GB のメモリが必要です。メモリとサイト数のマッピングの詳細については、「システム要件とインストール」を参照してください。



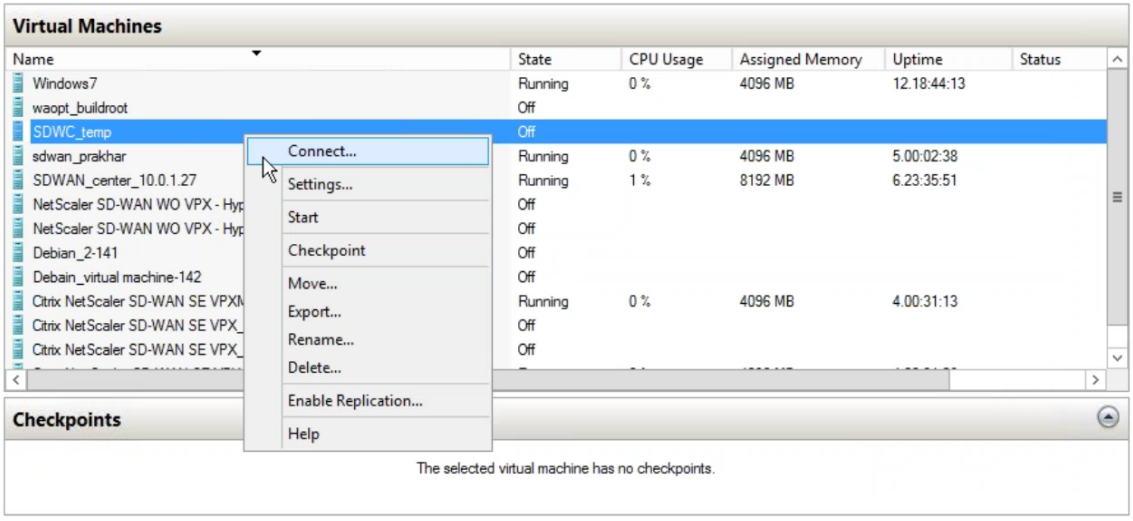
5. VM のネットワークアダプターで使用する仮想スイッチを選択し、[次へ] をクリックします。
6. [既存の仮想ハードディスクを使用する] を選択し、ダウンロードした SD-WAN Center VHD ファイルを参照して選択します。［次へ］をクリックします。



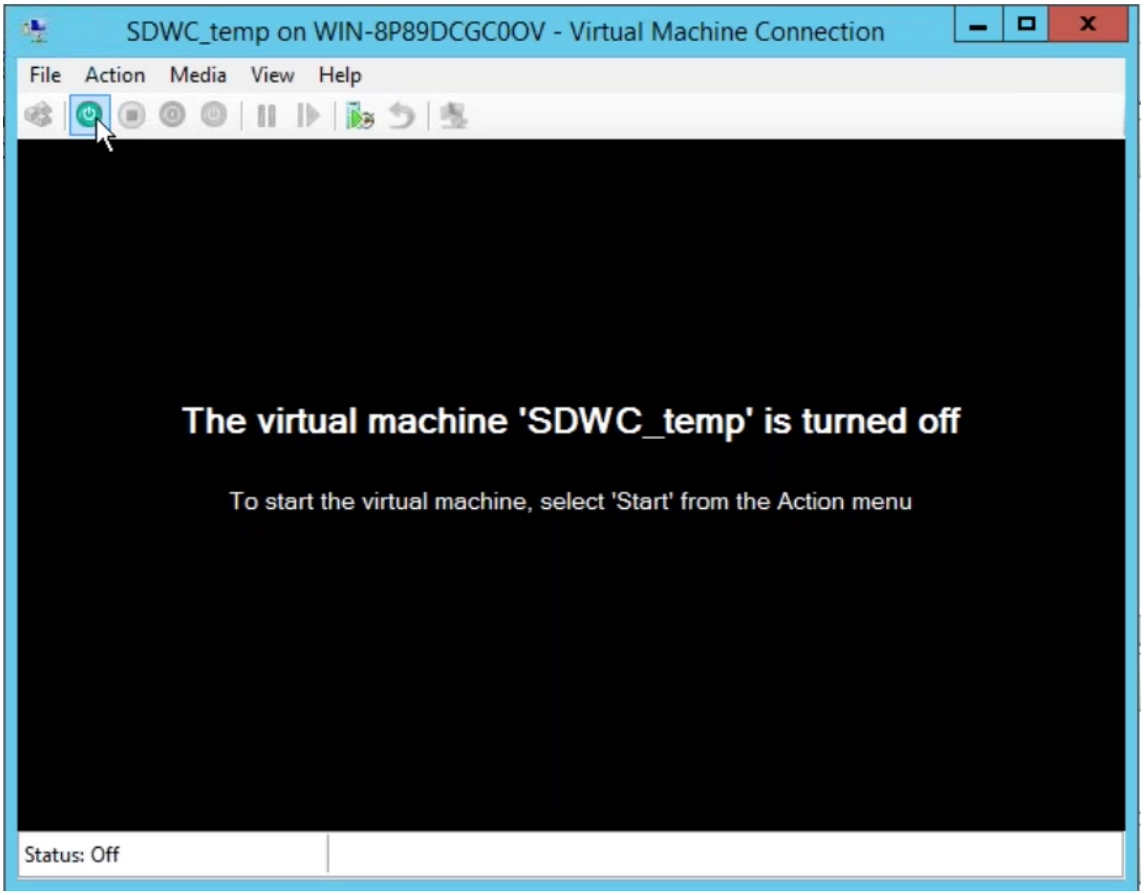
7. VM の概要を確認し、必要に応じて設定を変更します。それ以外の場合は、[完了] をクリックします。SD-WAN Center VM が作成され、仮想マシン セクションにリストされます。
8. SD-WAN Center VM を右クリックし、[設定] を選択します。仮想プロセッサの数を 4 に設定し、[適用] をクリックします。



9. SD-WAN Center VM を右クリックし、[接続] をクリックします。

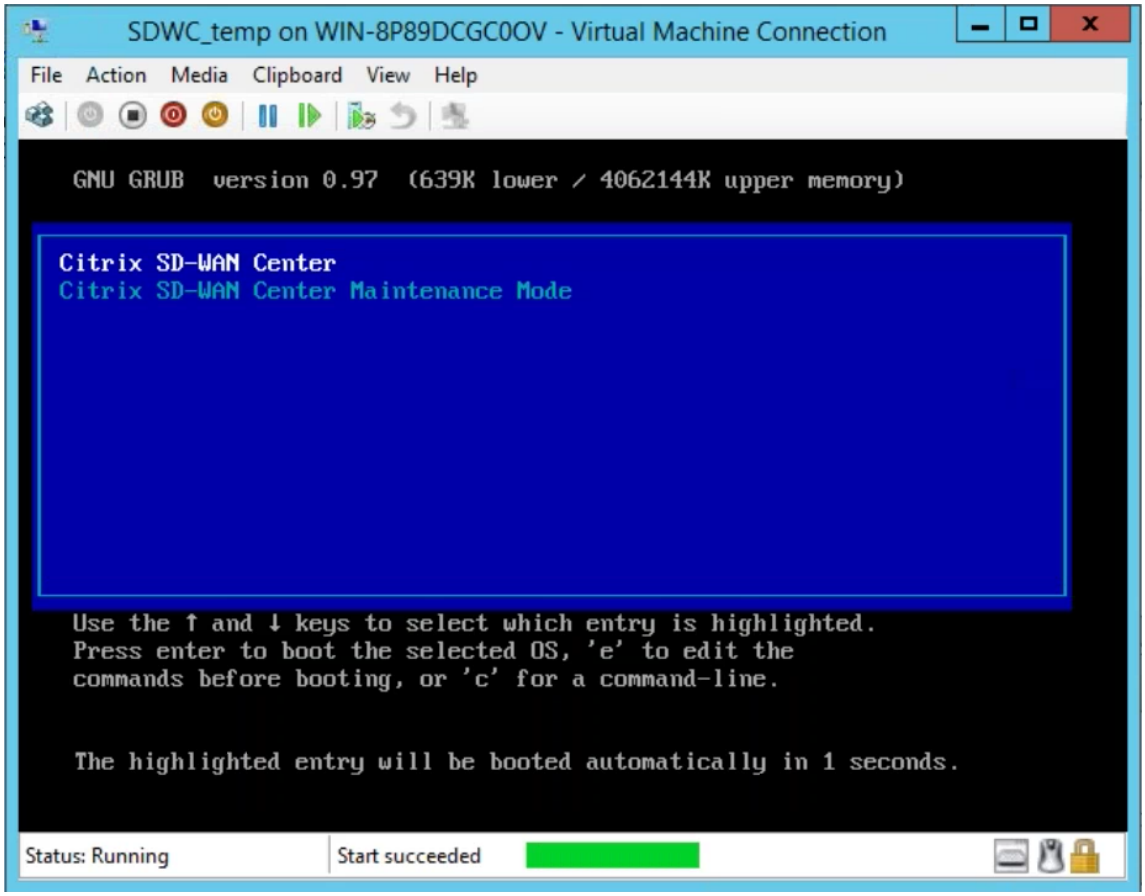


10. スタート ボタンをクリックします。



> 注
>
> 構成した CPU と RAM の数によっては、初期インストールに最大 50 分かかる場合があります。

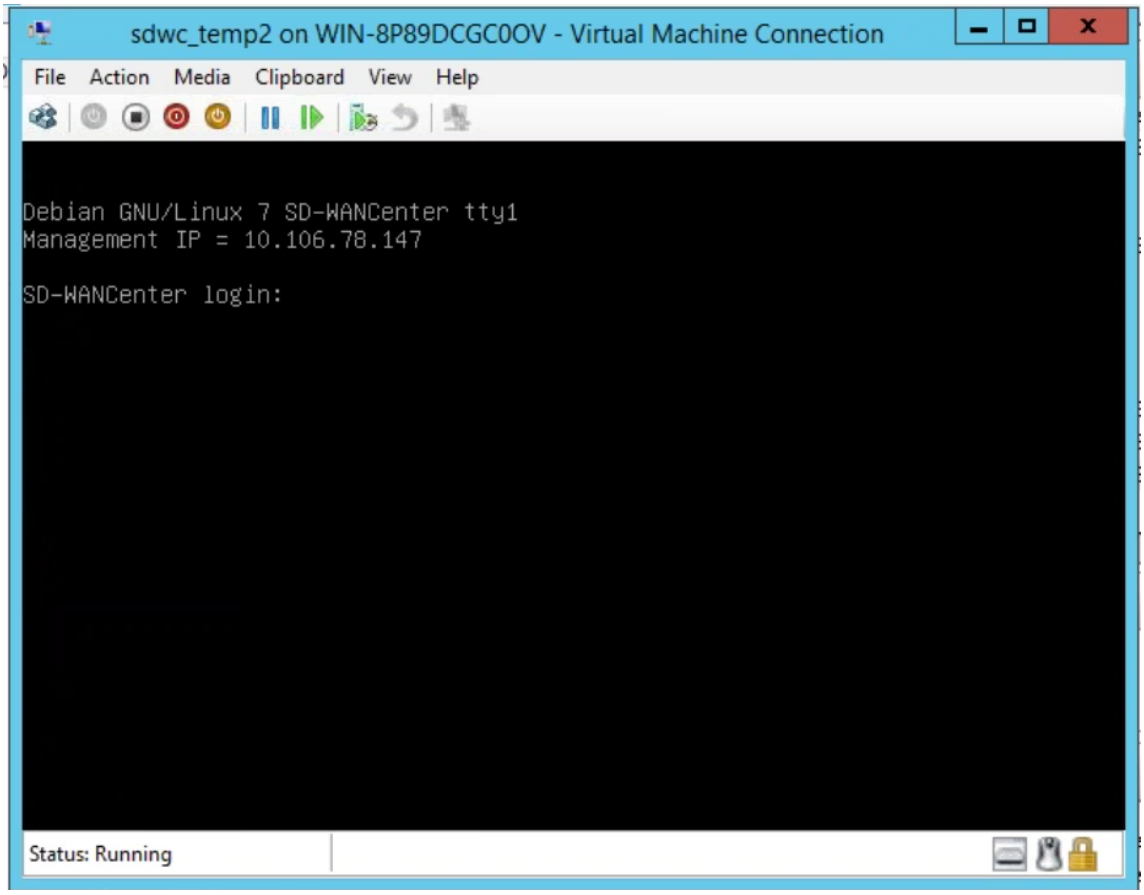
11. VM が起動したら、Citrix SD-WAN Center を選択して Enter キーを押します。



12. VM にログインします。新しい SD-WAN Center VM 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: 管理者

    Password: password



管理 IP アドレスがコンソールに表示され、この IP を使用して SD-WAN Center Web インターフェイスにアクセスします。

> 注
>
> SD-WAN ネットワークで DHCP が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 アドレスとして構成するには:

1. VM にログインします。新しい SD-WAN Center VM 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: 管理者

   Password: password

2. コンソールで、CLI コマンドを入力します management_ip 。**
3. コマンド セットインターフェイスを入力してください < ipaddress> < サブネットマスク > < gateway> 、管理 IP を構成します。

管理 IP を使用して、Citrix SD-WAN Center の Web インターフェイスにアクセスします。

ソリューションテンプレートを使用した **Azure Marketplace** 上の **Citrix SD-WAN Center**

April 13, 2021

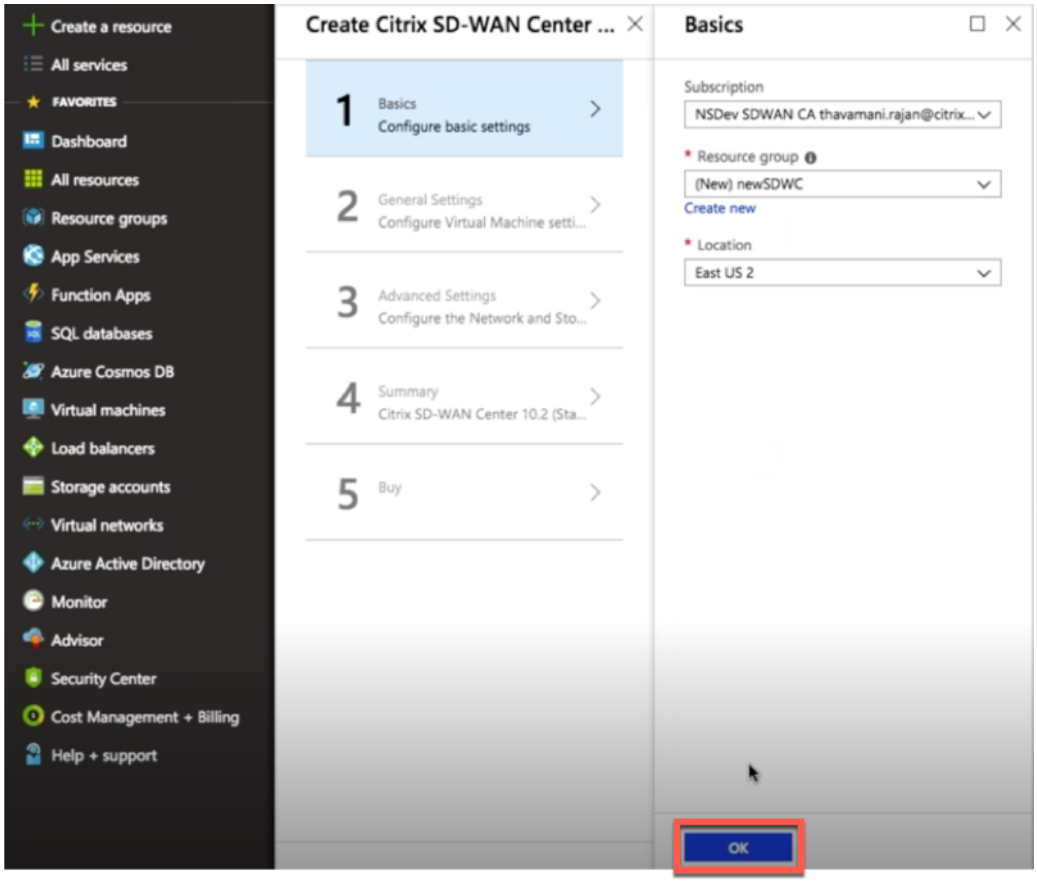
Citrix SD-WAN Center が Azure Marketplace で利用可能になりました。ソリューションテンプレートを使用して、Azure Cloud の仮想マシン（VM）として Citrix SD-WAN Center をデプロイできます。

Microsoft Azure に Citrix SD-WAN Center 仮想マシン（VM）をインストールする前に、「システム要件とインストール」の説明に従って必要な情報を収集します。

Microsoft Azure にアクセスできることを確認します。

Microsoft Azure に Citrix SD-WAN Center VPX をデプロイするには:

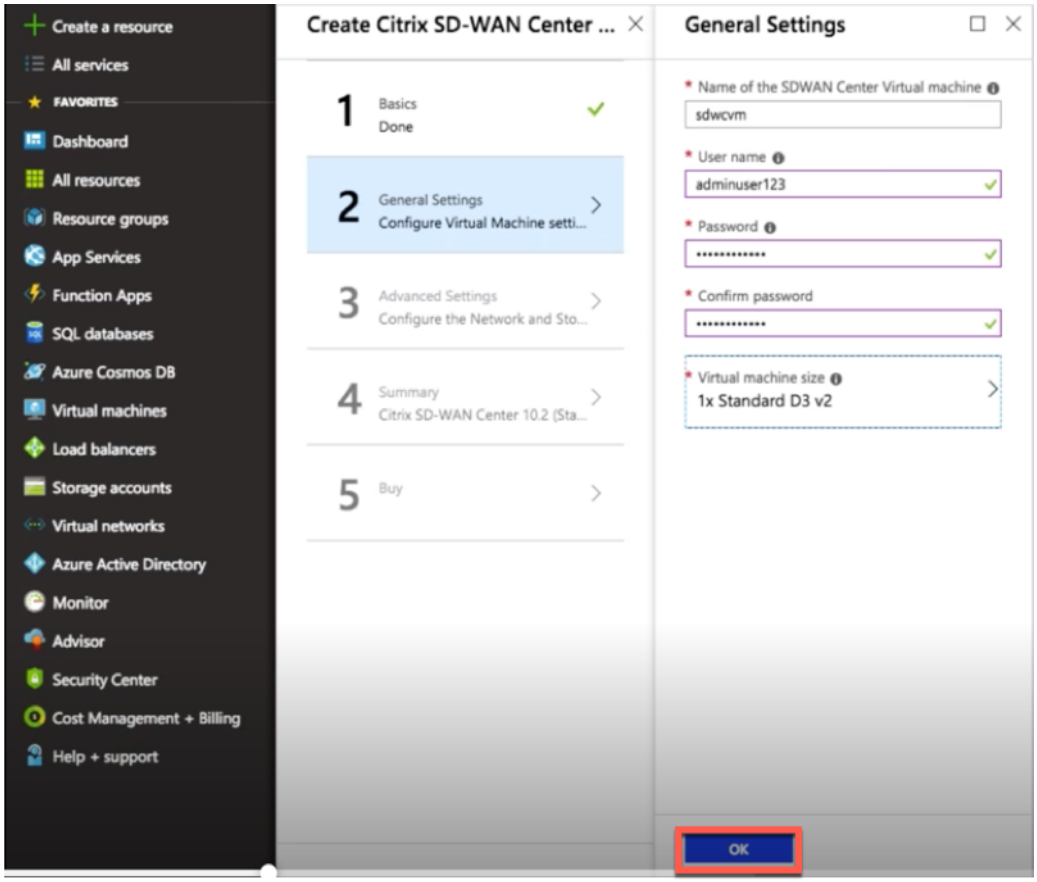
1. Microsoft Azure で、ホーム **>** マーケットプレイスに移動します。**Citrix SD-WAN Center** を検索して選択します。
2. **Citrix SD-WAN Center** ページで [作成**]** をクリックします。[**Citrix SD-WAN Center** の作成] ページが表示されます。
3. [基本] セクションで、サブスクリプションの種類、リソースグループ、および場所を選択します。[**OK**] をクリックします。



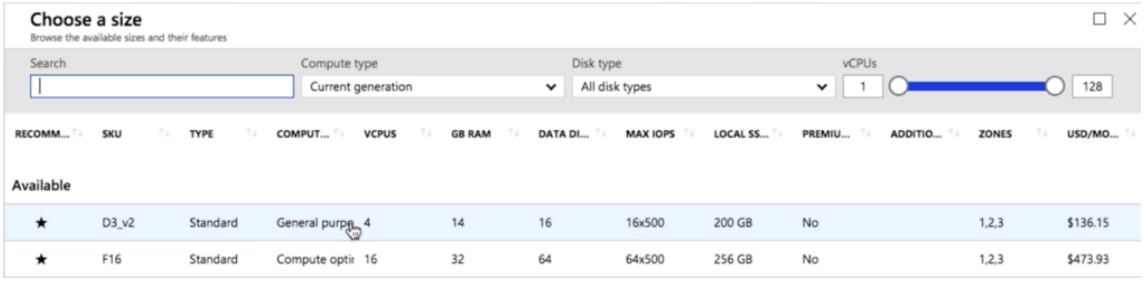
> 注:
>
> リソースグループは、Azure ソリューションの関連リソースを保持するコンテナーです。リソースグループには、ソリューションのすべてのリソースを含めることも、グループとして管理するリソースのみを含めることもできます。デプロイメントに基づいて、リソースをリソースグループに割り当てる方法を決定できます。

4. **[全般設定]** セクションで、Citrix SD-WAN Center 仮想マシンに管理者レベルのアクセスまたは権限を提供する名前と認証情報を入力します。

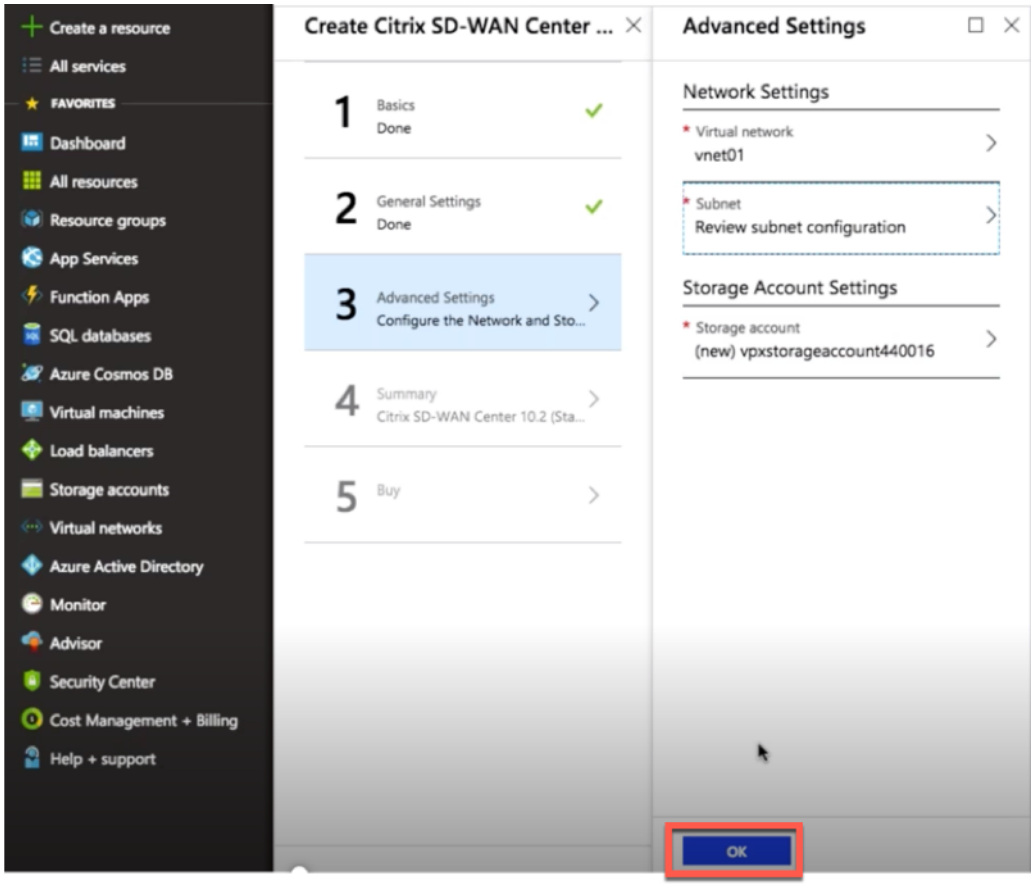
   この手順 4 で提供される資格情報は、管理 ユーザーのログインアカウントのパスワードを設定するためにも使用されます（この管理者アカウントのパスワードは、このパスワード資格情報で変更できます）。[**OK**] をクリックします。



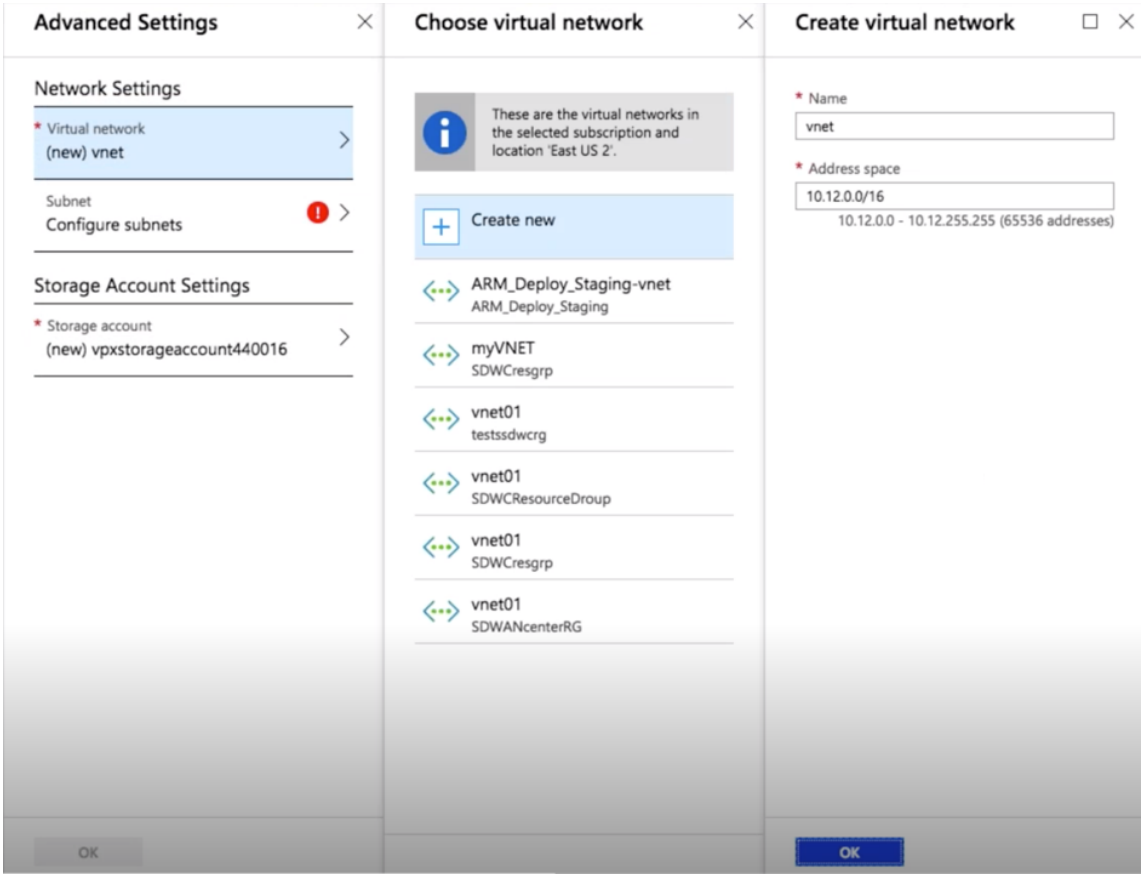
> 注:
>
> 現在、2 つのサイズのインスタンスタイプが利用可能です–Standard_D3_v2 そして Standard_F16。****D3_v2 インスタンスを使用して、最大 64 サイトのネットワークを監視できます。F16 インスタンスは、最大 128 サイトのネットワークを監視するのに役立ちます。使用可能な仮想マシンのサイズを検索して選択することもできます。



5. [詳細設定] セクションで、監視するサイトの数に基づいて、**Citrix SD-WAN Center VPX** の ネットワークおよびストレージアカウント 設定を構成します。

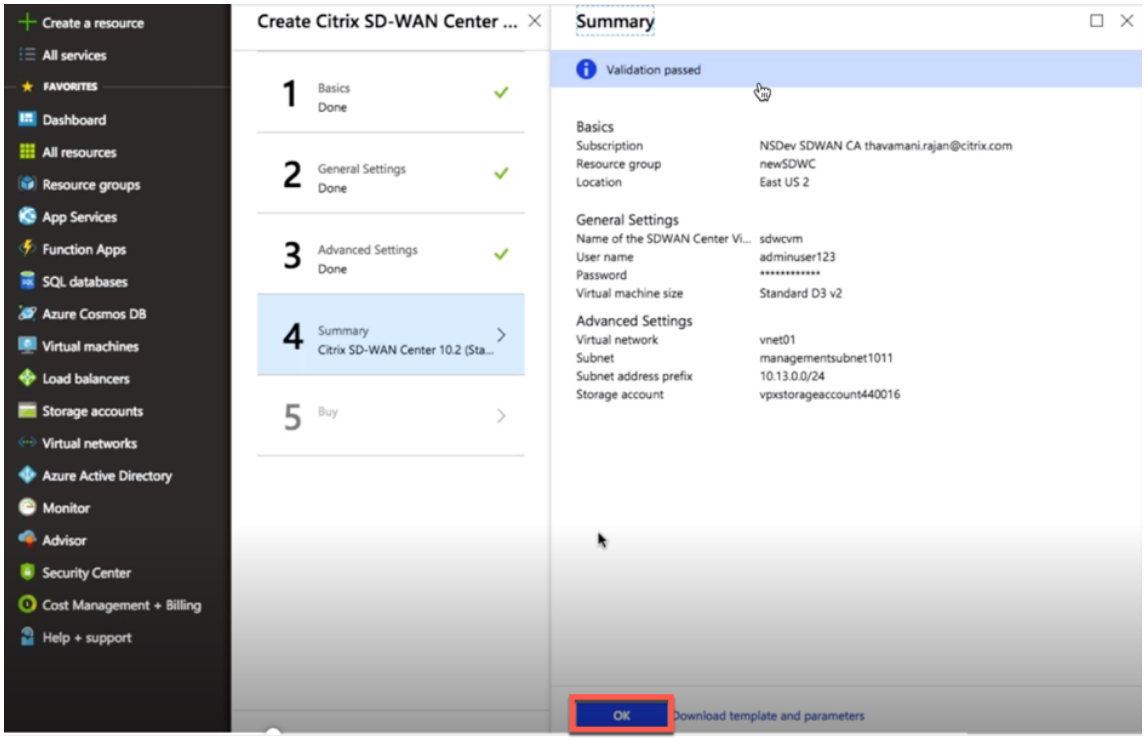


利用可能なリストから仮想ネットワークを選択するか、名前 と アドレススペースを指定して新しい仮想ネットワークを作成できます。

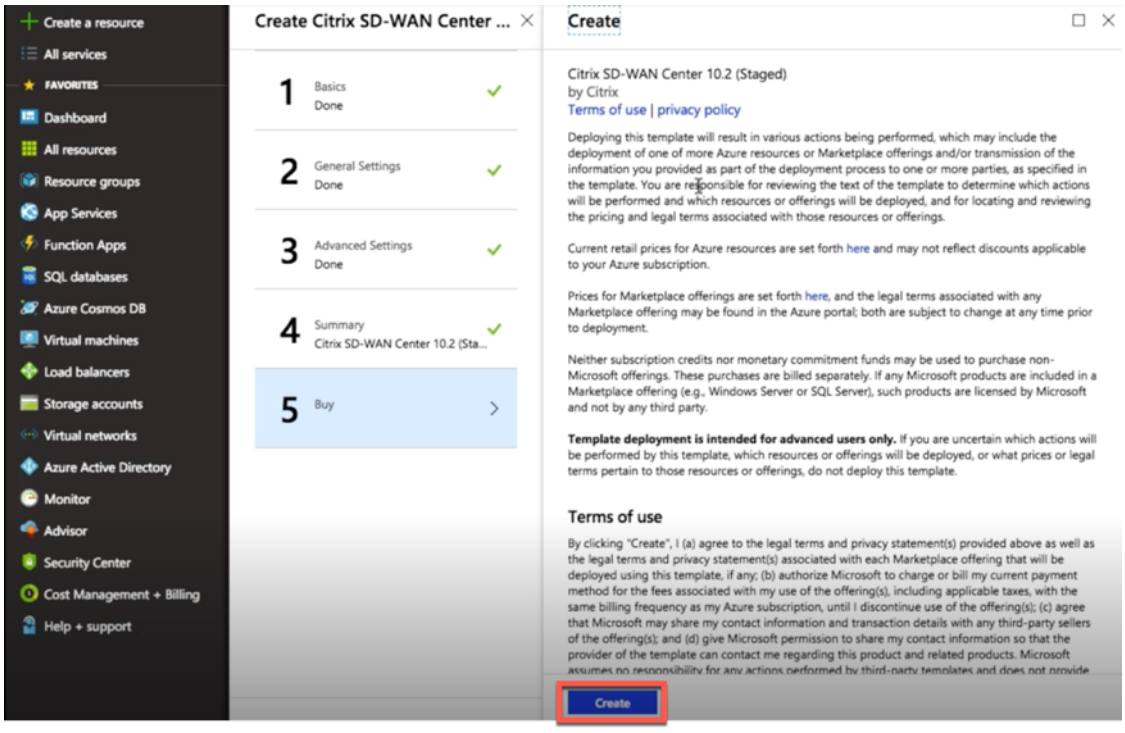


ドロップダウンリストから [サブネット] を選択します。ストレージアカウント を作成し、[**OK**] をクリックします。

6. 前の手順で指定した構成が検証され、適用されます。正しく構成した場合、検証に合格したメッセージが表示されます。[**OK**] をクリックします。



7. デプロイが成功すると、[作成] ページが表示されます。利用規約とプライバシーポリシーを よく読み、[作成] をクリックします。



VM のプロビジョニングが完了するのを待ってから、その VM に割り当てられている IP でログインし（ネットワークセクションを確認し、手順 4 で設定した管理者の資格情報を使用）、SD-WAN Center の一般的な展開ガイドライン

に従います。。

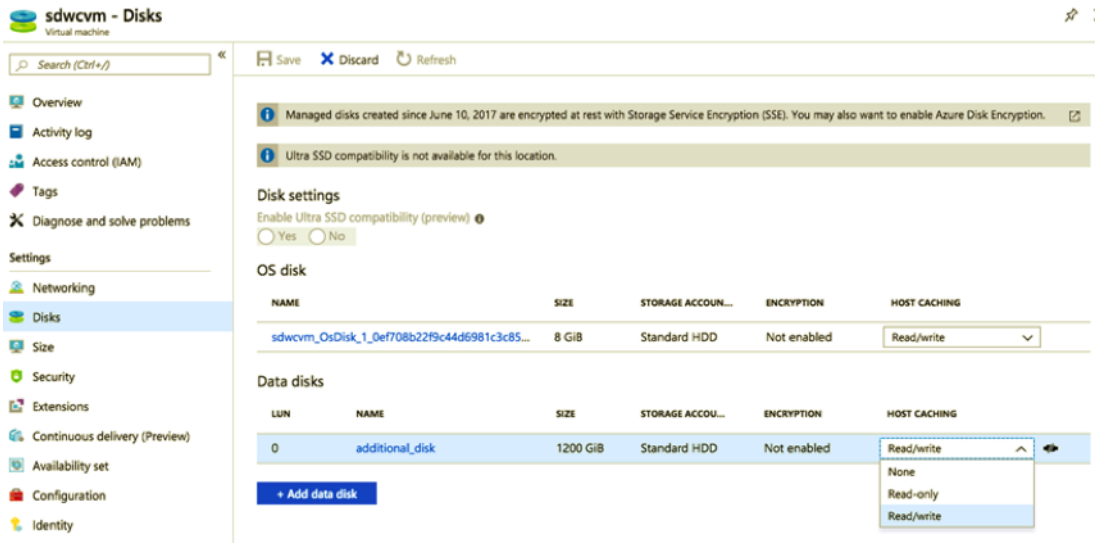
データディスクを追加

このセクションでは、Azure ポータルを使用して、新しい管理対象データディスクを仮想マシン（VM）に接続する方法について説明します。VM サイズによって、接続できるデータディスクの数が決まります。

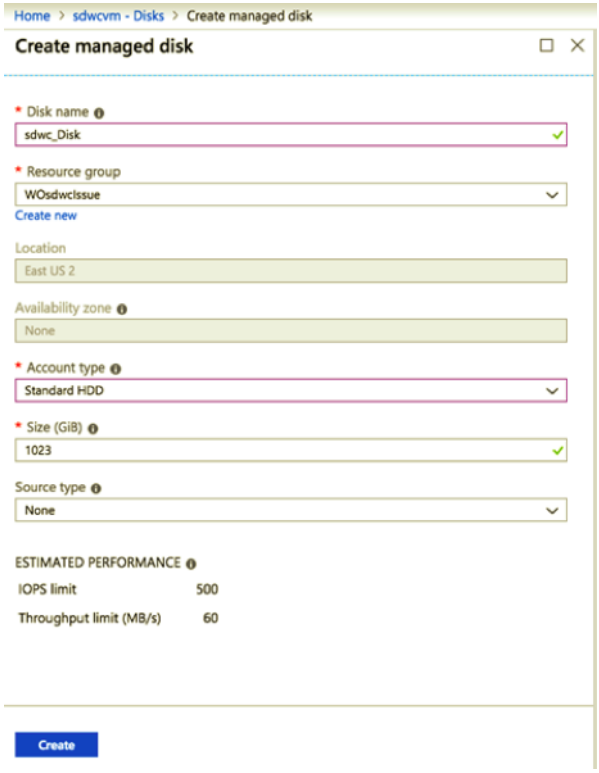
Azure ポータルで、左側のメニューから [仮想マシン] を選択し、リストから仮想マシンを選択します。

Azure SD-WAN Center に追加のデータディスクを追加するには、次の操作を実行します。

1. 仮想マシンをシャットダウンします。
2. VM ダッシュボードで、[設定] セクションの [ディスク] を選択します。



3. クリック + データディスク を追加し、読み取りおよび書き込み権限を持つ新しいデータディスクを作成します。



次の必須の詳細を入力して、ディスクを接続します。

- ディスク名–SD-WAN Center データディスクの名前を入力します。
- リソースグループ–ドロップダウンリストからリソースグループを選択します。
- アカウントの種類–ドロップダウンリストからアカウントの種類を選択します。
- サイズ（**GIB**）–サイズをギビバイトで指定します。
- ストレージタイプ -ドロップダウンリストからソースタイプを選択します。

4. 完了したら、[**OK]** をクリックします。

VM をオンにするには、「アクティブなストレージを新しいデータストレージに切り替える」トピックを参照してください。

VM のインポート可能なイメージ形式の AWS 上の Citrix SD-WAN Center

April 13, 2021

Citrix SD-WAN Center は、企業が WAN 上のすべての Citrix SD-WAN アプライアンスを構成、監視、および分析できるようにする集中管理システムまたは単一のガラス管理ソリューションです。

AWS での **SD-WAN Center** 仮想アプライアンス（**AMI**）のインスタンス化

SD-WAN Center 仮想アプライアンスを AWS VPC にインストールするには、AWS アカウントが必要です。AWS アカウントここを作成できます。SD-WAN Center は、Amazon マーケットプレイスイメージ（AMI）として AWS Marketplace で入手できます。

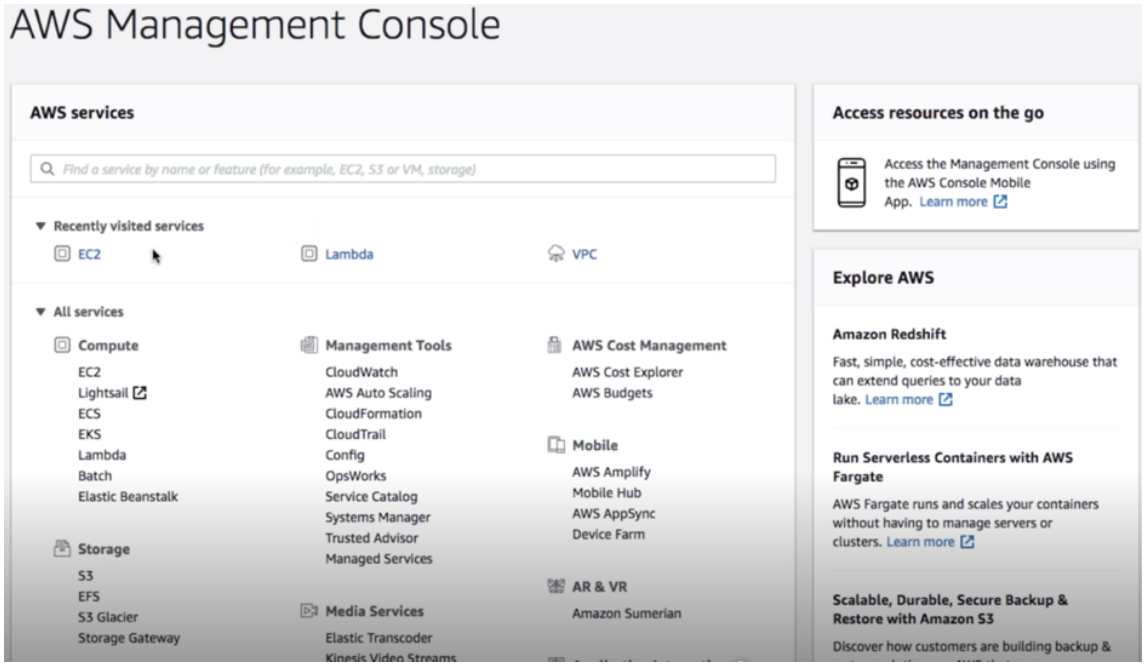
> 注:
>
> Amazon は AWS ページを頻繁に変更するため、次の手順は最新ではない場合があります。

AWS で SD-WAN Center 仮想アプライアンス（AMI）をインスタンス化するには、2 つの方法があります。

1. 最初のアプローチ：Web ブラウザーで、http://aws.amazon.com/と入力します。[My Account] で [AWS Management Console] を選択して、Amazon Web Services（AWS）を開きます。

   2 番目のアプローチ:
   Web ブラウザーで、http://console.aws.amazon.com と入力して **Amazon Web Services** を開きます。

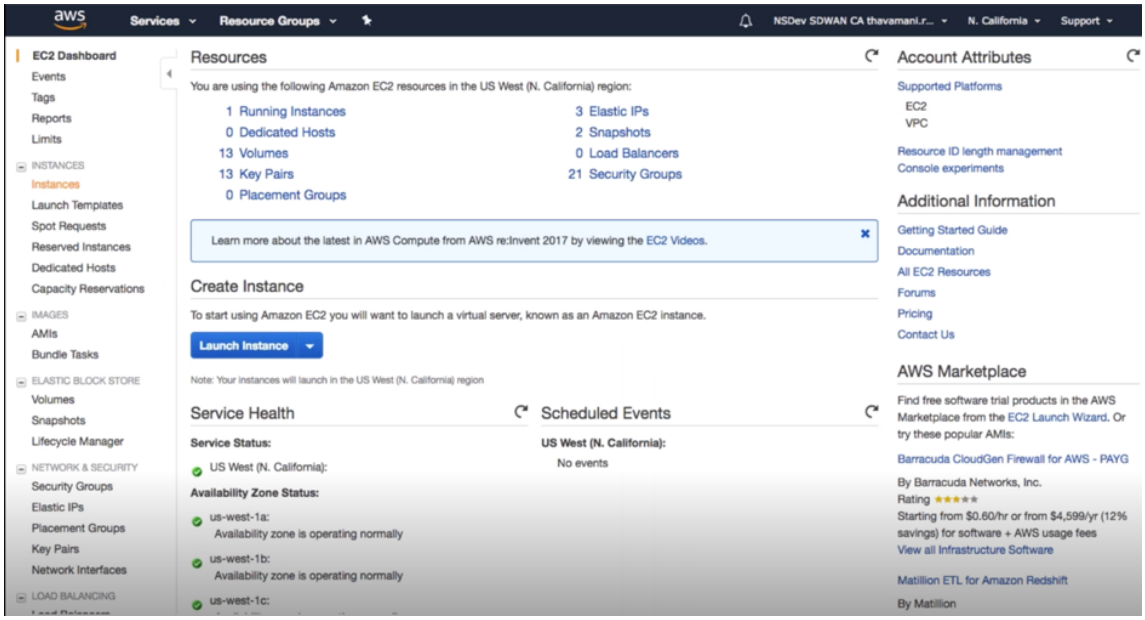
2. AWS アカウントの認証情報を使用してサインインします。これにより、**Amazon Web Services** ページに移動します。最近アクセスしたサービスの リストを他のすべてのサービスとともに表示できます。

   Citrix SD-WAN Center アプライアンスは、EC2 を AWS サービスインスタンスとして提供します。

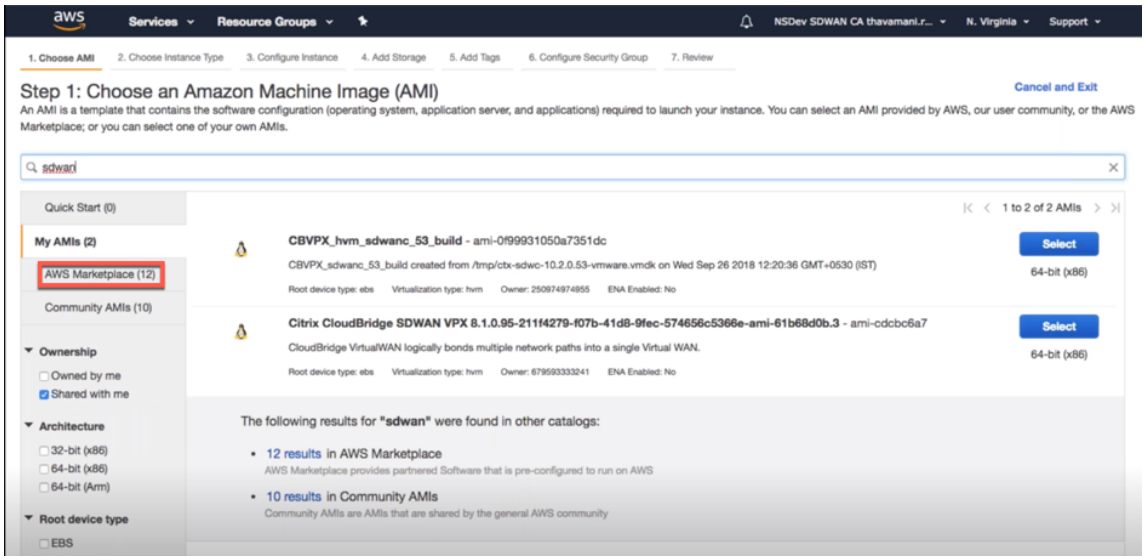
   - **EC2** ダッシュボード -エラスティックコンピューティングクラウド、サイズ変更可能な仮想サービス / インスタンス

3. [コンピューティング] セクションで [**EC2]** をクリックし、[インスタンスの起動] を選択します。



どちらの 起動インスタンス オプションを選択するか、手動で（上記のスクリーンショットを参照）インスタンス の下左側に インスタンス オプションの場所を選択することにより、インスタンス画面 に到達することができます。

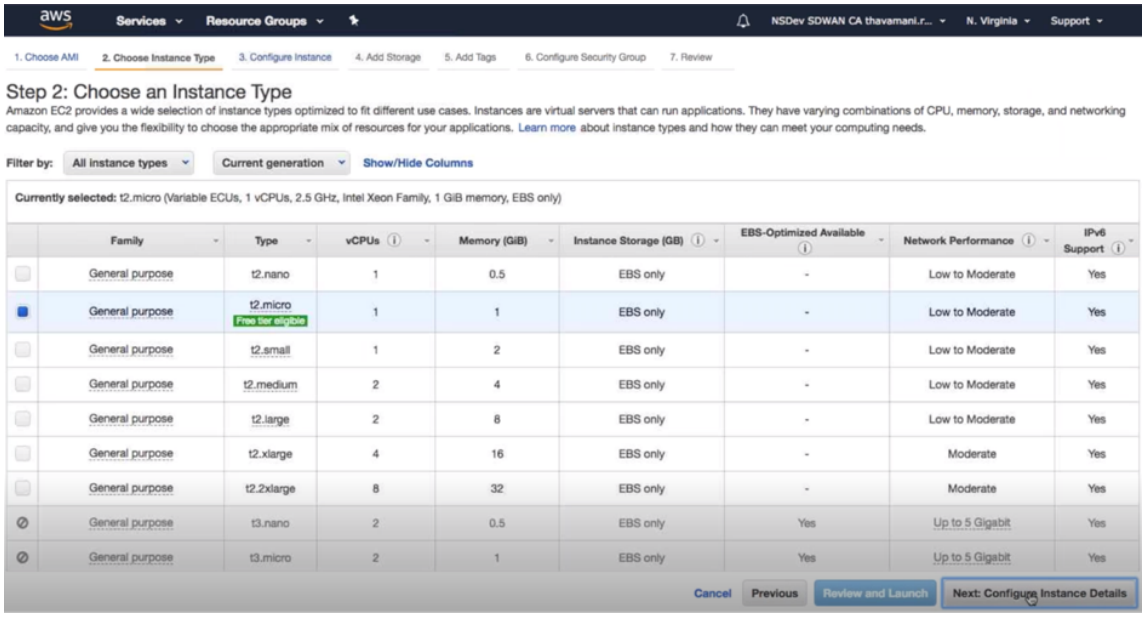
4. [**AMI** の選択] ページで、[**AWS Marketplace**] タブをクリックします。
5. [検索] テキストフィールドに「SD-WAN」と入力して SD-WAN AMI を検索し、[検索] をクリックします。



検索結果ページで、最新リリースの Citrix SD-WAN Center AMI の 1 つを 選択し、[選択] をクリックします。

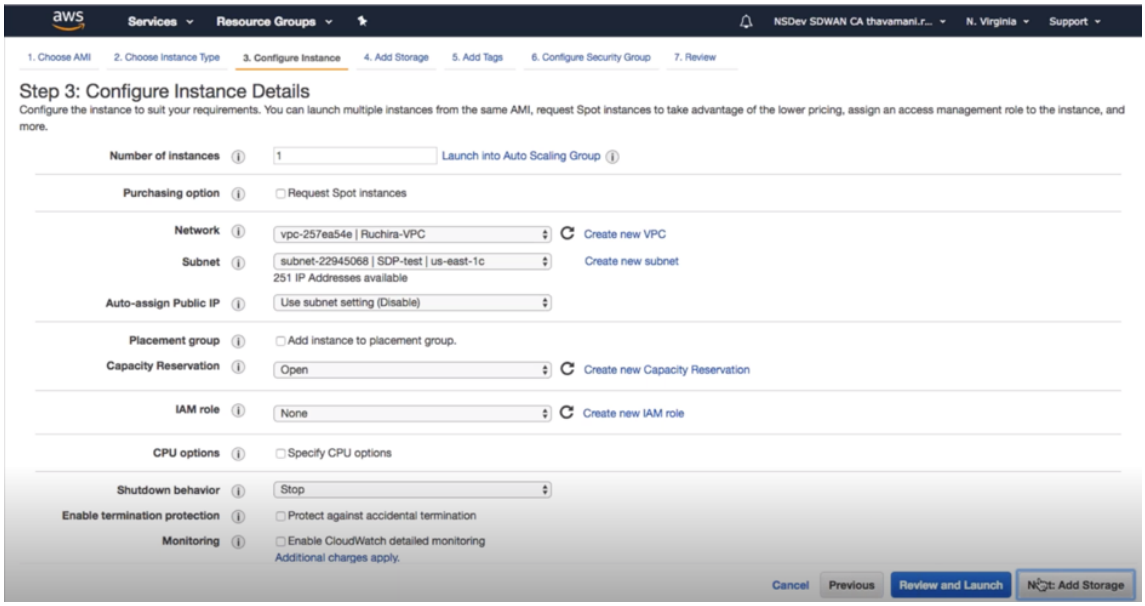
AMI テンプレートには、オペレーティングシステム、アプリケーションサーバー、アプリケーションなどのソフトウェア構成が含まれています。このテンプレートは、インスタンスを起動するために必要です。

6. インスタンスタイプを選択し、[次：インスタンスの詳細を設定] を選択します。特定のインスタンスタイプまたは現在の世代のすべてのインスタンスタイプを選択して、検索をフィルタリングできます。

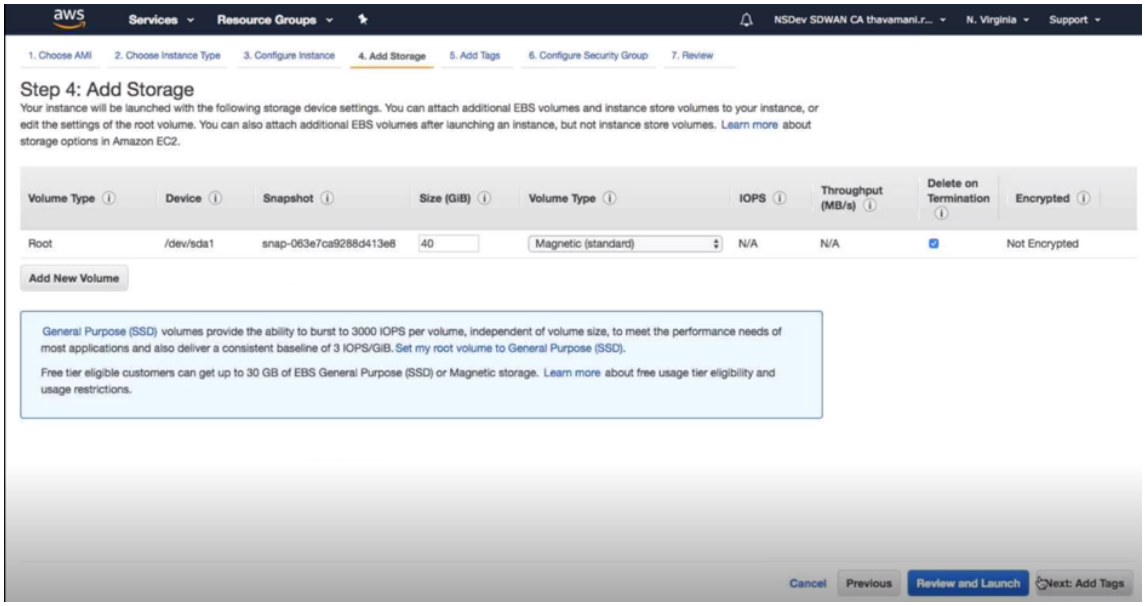


Amazon EC2 は、さまざまなユースケースに適合するように最適化されたインスタンスタイプの幅広い選択肢を提供します。インスタンスは、アプリケーションを実行できる仮想サーバーです。

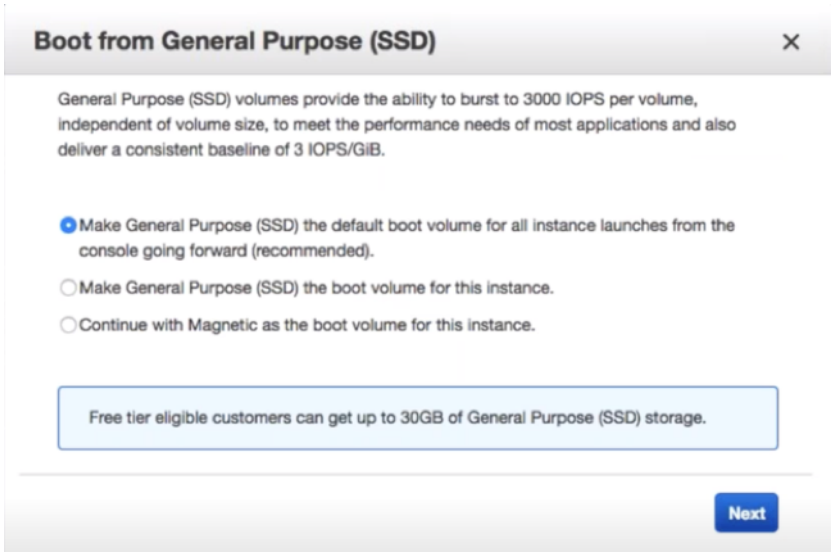
7. [インスタンス の構成] ページで、[インスタンスの 数] テキストボックスに「1」と入力し、必要に応じて、特定のインスタンスのその他の詳細（ネットワーク、サブネットなど）を入力します。[**Next**: **Add Storage]** をクリックします。



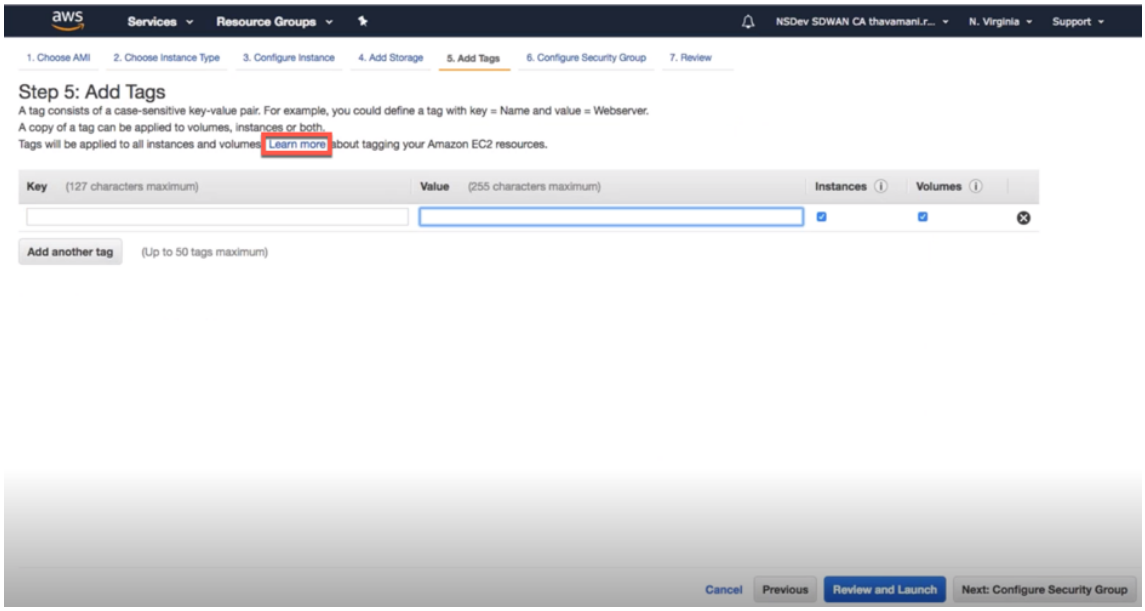
8. インスタンスは、ストレージデバイスの設定で起動されます。インスタンスがプロビジョニングされたら、新しいボリュームを個別に追加できます。



9. [確認して起動] をクリックして、要件に応じてブートボリュームオプションを選択します。［次へ］をクリックします。



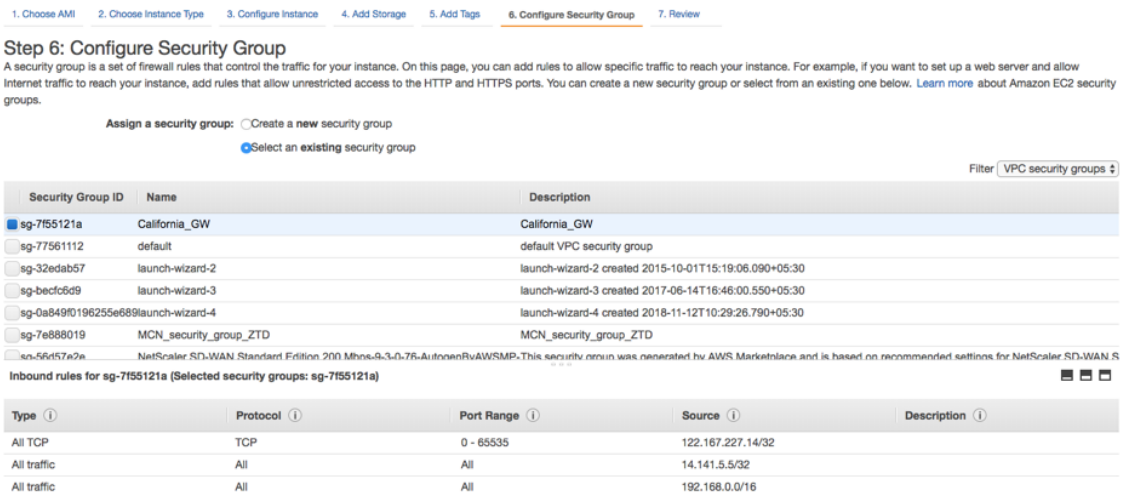
10. キーの名前 と 値を含むタグを追加または定義します。タグ付けの詳細については、[詳細] をクリックしてください。最大 50 個のタグを追加できます。[**Next**: **Configure Security Group**] をクリックします。



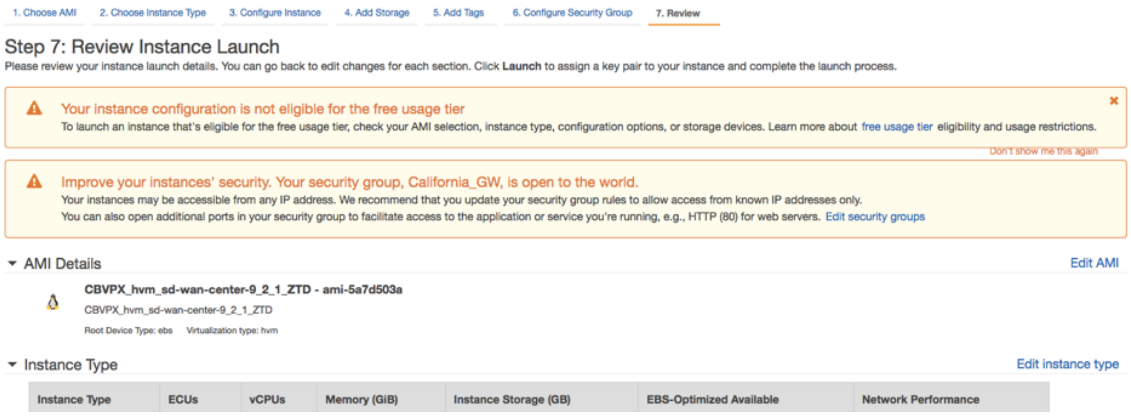
> 注:
>
> 注：タグキーの長さは 1～127 文字にする必要があります。

11. インスタンスのトラフィックの制御に役立つ一般的なセキュリティグループを作成できます。新しいセキュリティグループを作成するか、リストから既存のセキュリティグループを選択できます。

> 注:
>
> セキュリティグループが 2156 ポートを介したインバウンド接続を許可して、Citrix SD-WAN アプライアンスからデータを収集できるようにします。



12. インスタンスの起動の詳細を確認し、[起動] をクリックします。鍵ペアの作成を求めるポップアップボックスが表示されます。インスタンスのキーペアを作成する必要があります。



二要素認証

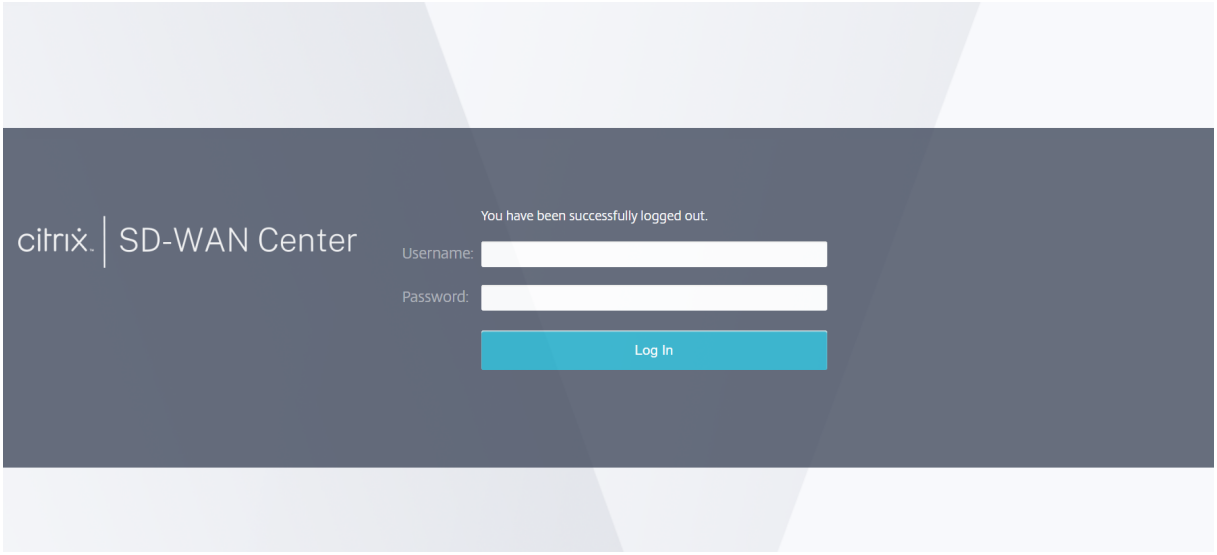
April 13, 2021

二要素認証（TFA）は、ローカルおよびリモートの両方のユーザーアカウントで Citrix SD-WAN Center にアクセスするための 2 つの認証要素を提供します。Citrix SD-WAN Center のログインシーケンスに追加のセキュリティレイヤーを導入します。

ローカルユーザーアカウントの第 1 レベルの認証は、Citrix SD-WAN Center で構成されたパスワードを使用して実現されます。詳しくは、「ユーザーアカウント」を参照してください。

リモートユーザーアカウントの第 1 レベルの認証は、プライマリ RADIUS または TACACS + 認証サーバーを使用して実現されます。詳しくは、「一次認証」を参照してください。

追加のセカンダリ RADIUS または TACACS + 認証サーバーを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の両方に構成して、2 要素認証を有効にすることができます。詳しくは、「二次認証」を参照してください。



Citrix SD-WAN Center のログイン認証情報:

- ユーザー名: SD-WAN Center またはプライマリ認証サーバーで構成されたユーザー名。
- パスワード: SD-WAN Center またはプライマリ認証サーバーで構成されたパスワード。
- 二次パスワード: セカンダリ認証サーバーで構成されたパスワード。

> 注
>
> [**Secondary Password**] オプションは、セカンダリ認証サーバーが構成されている場合にのみ表示されます。

一次認証

April 13, 2021

RADIUS や TACACS + などの認証サーバーを構成して、Citrix SD-WAN Center にログオンするリモートユーザーを認証できます。2 要素認証が有効になっている場合、プライマリユーザーはリモートユーザーの最初の認証要素です。詳しくは、「2 要素認証」を参照してください。

> 注
>
> 必要な認証サーバーにユーザーアカウントが作成されていることを確認します。

RADIUS 認証サーバー

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構成する必要があります。オプションで、最大 3 つの RADIUS サーバーまでの冗長バックアップサーバーを構成します。サーバーは、[サーバー] セクションに最初にリストされているサーバーから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 認証サーバーに作成されていることを確認します。

RADIUS 認証を有効にして設定するには:

1. Citrix SD-WAN Center Web インターフェイスで、管理 > **User/Authentication** 設定に移動します。
2. 一次認証 > **[RADIUS** 認証] セクションで、[**RADIUS** 認証を有効にする] チェックボックスをオンにします。

   > 注
   >
   > TACACS + 認証がすでに有効になっている場合は、無効になります。

3. [タイムアウト] フィールドに、RADIUS サーバーからの認証応答を待つ時間間隔（秒単位）を入力します。

   タイムアウト値は 60 秒以下にする必要があります。

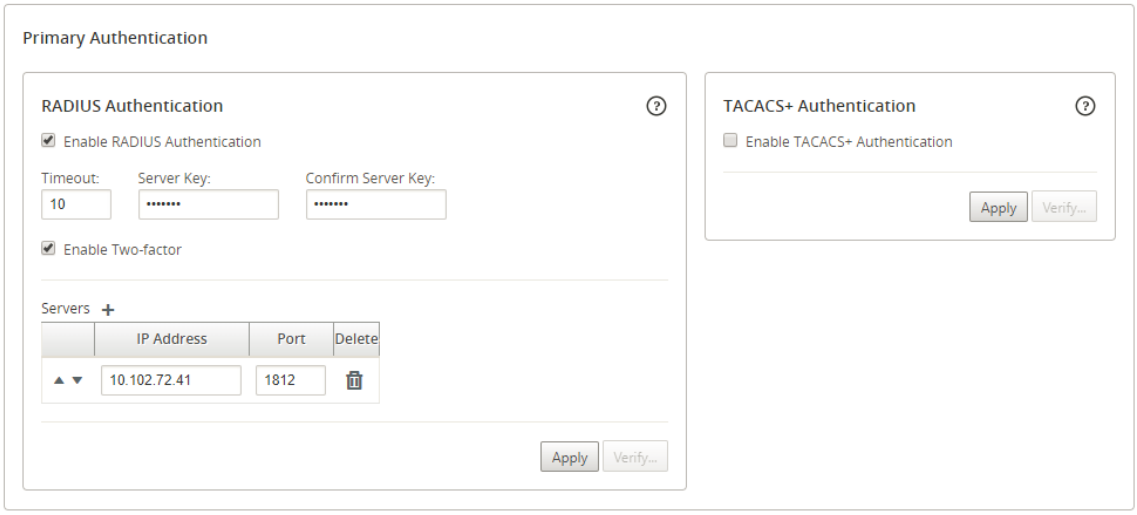
4. [**Server Key]** フィールドに、RADIUS サーバーに接続するときに使用する秘密鍵を入力します。
5. 「サーバー鍵 の確認」フィールドに、秘密鍵を再入力します。

> 注
>
> タイムアウトとサーバーキーの設定は、構成されているすべてのサーバーに適用されます **。**

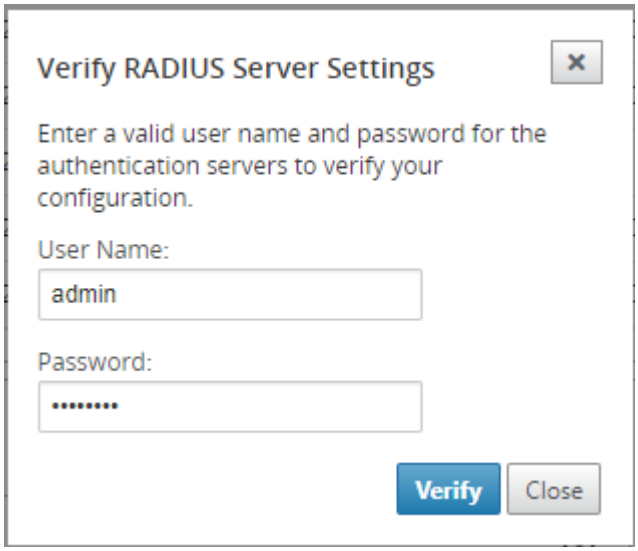
6. 2 要素認証を有効にするには、[**2** 要素を有効にする] を選択します。

> 注
>
> [**2** 要素を有効に する] オプションは、セカンダリ認証サーバーが構成されている場合にのみ表示されます。
>
> RADIUS、または TACAS+ のいずれかでセカンダリ認証サーバーを構成する詳しくは、「二次認証」を参照してください。

7. プラスアイコンをクリックします (+) サーバーの 横にある RADIUS サーバーを追加します。
8. [**IP** アドレス] フィールドに、RADIUS サーバーのホスト IP アドレスを入力します。
9. [ポート] フィールドに、RADIUS サーバーのポート番号を入力します。デフォルトのポート番号は 1812 です。



10. [**Apply**] をクリックします。
11. [確認] をクリックして、RADIUS サーバーへの接続を確認します。[**RADIUS** サーバー設定 の確認] ダイアログボックスが表示されます。



12. 認証サーバーの有効なユーザー名とパスワードを入力し、[確認] をクリックします。

さらにサーバーを構成するには、手順 7～12 を繰り返します。

TACACS + 認証サーバー

使用するには TACACS+, 少なくとも 1 つの TACACS + サーバーを指定して構成する必要があります。オプションで、最大 3 つの TACACS + サーバーまでの冗長バックアップサーバーを構成します。サーバーは、[サーバー] セクションに最初にリストされているサーバーから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 + 認証サーバーに作成されていることを確認します。

TACACS + 認証を有効にして設定するには:

1. Citrix SD-WAN Center Web インターフェイスで、管理 > **User/Authentication** 設定に移動します。
2. 一次認証 > **[TACACS +** 認証] セクションで、[**TACACS +** 認証を有効にする] チェックボックスをオンにします。

   > 注
   >
   > RADIUS 認証がすでに有効になっている場合は、無効になります。

3. [タイムアウト] フィールドに、TACACS + サーバーからの認証応答を待つ時間間隔（秒単位）を入力します。

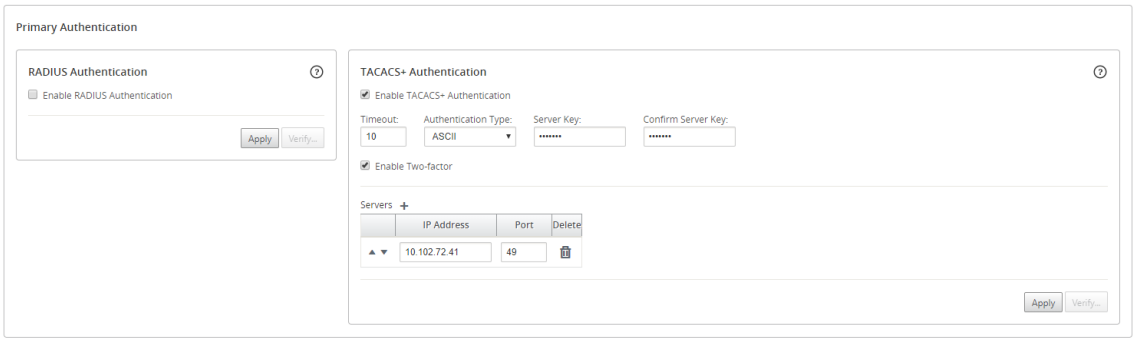
   タイムアウト値は 60 秒以下にする必要があります。
4. 「認証タイプ」フィールドで、ユーザー名とパスワードを TACACS + サーバーに送信するために使用する暗号化方式を選択します。
5. [**Server Key**] フィールドに、TACACS + サーバーに接続するときに使用する秘密鍵を入力します。
6. 「サーバー鍵 の確認」フィールドに、秘密鍵を再入力します。

> 注
>
> **Timeout**、**Authentication Type**、および **Server Key** の設定 は、構成されているすべてのサーバーに適用されます。

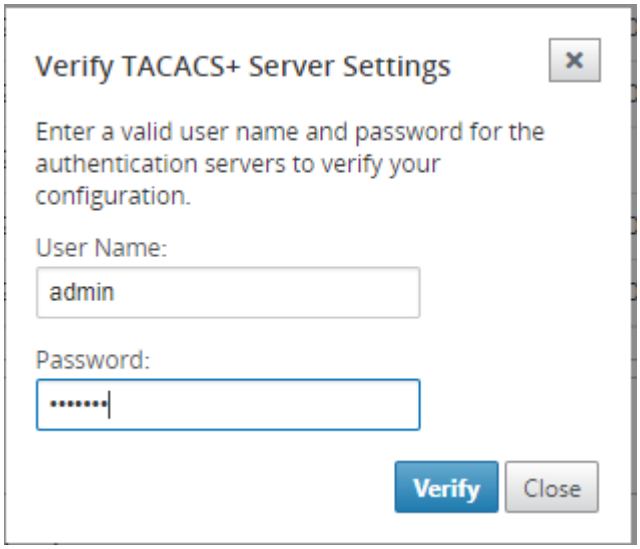
7. 2 要素認証を有効にするには、[**2** 要素を有効にする] を選択します。

> 注
>
> [**2** 要素を有効に する] オプションは、セカンダリ認証サーバーが構成されている場合にのみ表示されます。
>
> RADIUS、または TACAS+ のいずれかでセカンダリ認証サーバーを構成する詳しくは、「二次認証」を参照してください。

8. プラスアイコンをクリックします (+) サーバーの 横にある TACACS + サーバーを追加します。
9. [**IP** アドレス**]** フィールドに、TACACS + サーバーのホスト IP アドレスを入力します。
10. [ポート**]** フィールドに、TACACS + サーバーのポート番号を入力します。デフォルトのポート番号は 49 です。



11. [**Apply**] をクリックします。
12. [確認] をクリックして、RADIUS サーバーへの接続を確認します。**Verify TACACS + Server Settings** ダイアログボックスが表示されます。



13. 認証サーバーの有効なユーザー名とパスワードを入力し、[確認] をクリックします。

    さらにサーバーを構成するには、手順 8～13 を繰り返します。

二次認証

April 13, 2021

セカンダリ認証は、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の 2 要素認証を有効にするように構成されています。RADIUS または TACACS + 認証サーバーをセカンダリ認証サーバーとして構成できます。詳しくは、「2 要素認証」を参照してください。

> 注
>
> 必要な認証サーバーにユーザーアカウントが作成されていることを確認します。ユーザーアカウントのパスワードは、Citrix SD-WAN Center のログインシーケンスの 2 番目の要素として使用されます。

セカンダリ **RADIUS** 認証サーバー

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構成する必要があります。オプションで、最大 3 つの RADIUS サーバーまでの冗長バックアップサーバーを構成します。サーバーは、[サーバー] セクションに最初にリストされているサーバーから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 認証サーバーに作成されていることを確認します。

RADIUS 認証を有効にして設定するには:

1. Citrix SD-WAN Center Web インターフェイスで、管理 > **User/Authentication** 設定に移動します。

2. 二次認証 > **[RADIUS** 認証**]** セクションで、[セカンダリ **RADIUS** 認証を有効にする] チェックボックスをオンにします。

   > 注
   >
   > TACACS + 認証がすでに有効になっている場合は、無効になります。

3. [タイムアウト**]** フィールドに、RADIUS サーバーからの認証応答を待つ時間間隔（秒単位）を入力します。

   タイムアウト値は 60 秒以下にする必要があります。

4. [**Server Key]** フィールドに、RADIUS サーバーに接続するときに使用する秘密鍵を入力します。

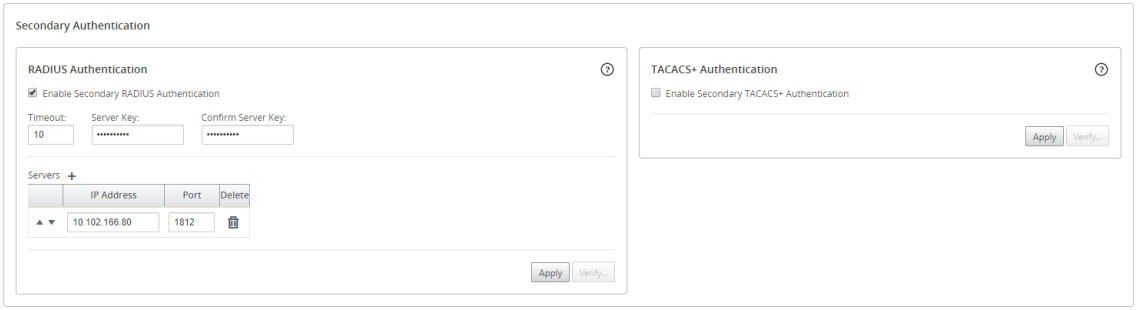
5. 「サーバー鍵 の確認」フィールドに、秘密鍵を再入力します。

   > 注
   >
   > タイムアウトとサーバーキーの設定は、構成されているすべてのサーバーに適用されます **。**

6. プラスアイコンをクリックします (+) サーバーの 横にある RADIUS サーバーを追加します。

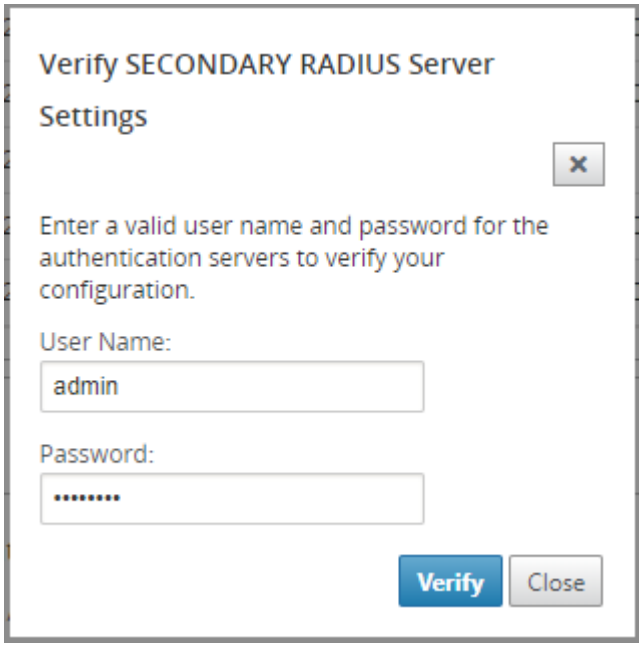
7. [**IP** アドレス**]** フィールドに、RADIUS サーバーのホスト IP アドレスを入力します。

8. [ポート**]** フィールドに、RADIUS サーバーのポート番号を入力します。デフォルトのポート番号は 1812 です。



9. [**Apply**] をクリックします。

10. [確認] をクリックして、RADIUS サーバーへの接続を確認します。[セカンダリ **RADIUS** サーバー設定 の確認] ダイアログボックスが表示されます。



11. 認証サーバーの有効なユーザー名とパスワードを入力し、[確認] をクリックします。

さらにサーバーを構成するには、手順 6〜11 を繰り返します。

セカンダリ **TACACS +** 認証サーバー

使用するには TACACS+, 少なくとも 1 つの TACACS + サーバーを指定して構成する必要があります。オプションで、最大 3 つの TACACS + サーバーまでの冗長バックアップサーバーを構成します。サーバーは、[サーバー] セクションに最初にリストされているサーバーから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 + 認証サーバーに作成されていることを確認します。

TACACS + 認証を有効にして設定するには:

1. SD-WAN Center の Web インターフェイスで、[管理]>**User/Authentication ** 設定に移動します。
2. 二次認証 > **TACACS + Authentication** セクションで、**Enable Secondary TACACS + Authentication** チェックボックスを選択します。

   > 注
   >
   > RADIUS 認証がすでに有効になっている場合は、無効になります。

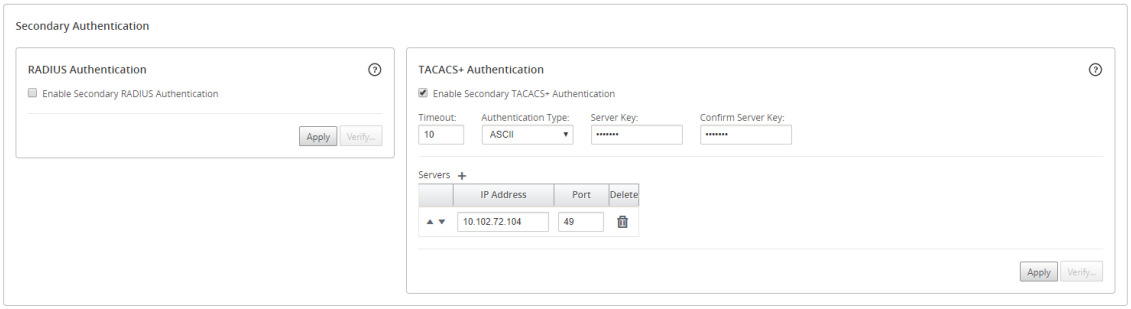
3. [タイムアウト] フィールドに、TACACS + サーバーからの認証応答を待つ時間間隔（秒単位）を入力します。

   タイムアウト値は 60 秒以下にする必要があります。
4. 「認証タイプ」フィールドで、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式を選択します。
5. [**Server Key**] フィールドに、TACACS + サーバーに接続するときに使用する秘密鍵を入力します。

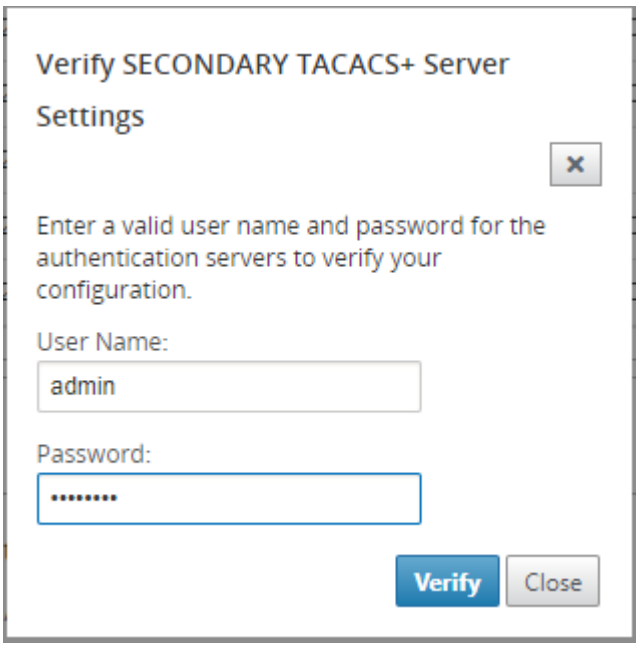
6. 「サーバー鍵 の確認」フィールドに、秘密鍵を再入力します。

> 注
>
> **Timeout**、**Authentication Type**、および **Server Key** の設定 は、構成されているすべてのサーバーに適用されます。

7. プラスアイコンをクリックします (+) サーバーの 横にある TACACS + サーバーを追加します。
8. [**IP** アドレス] フィールドに、TACACS + サーバーのホスト IP アドレスを入力します。
9. [ポート] フィールドに、TACACS + サーバーのポート番号を入力します。デフォルトのポート番号は 49 です。



10. [**Apply**] をクリックします。
11. [確認] をクリックして、RADIUS サーバーへの接続を確認します。**Verify TACACS + Server Settings** ダイアログボックスが表示されます。



12. 認証サーバーの有効なユーザー名とパスワードを入力し、[確認] をクリックします。

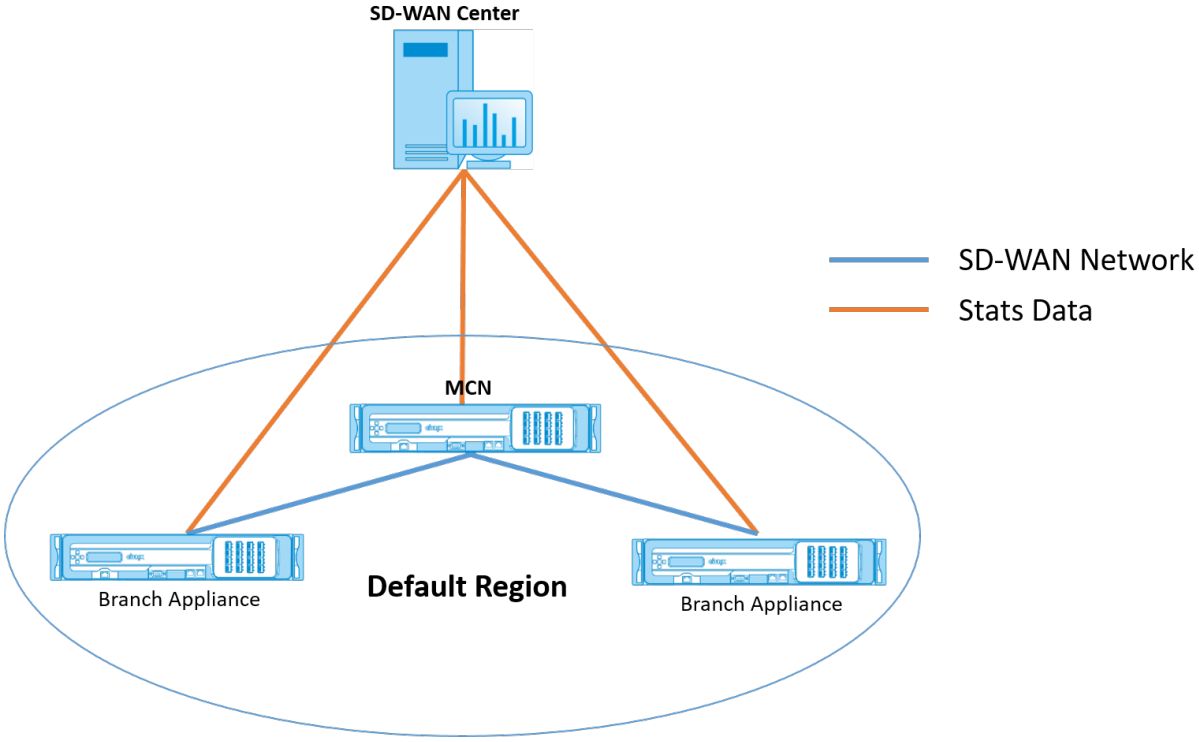
    さらにサーバーを構成するには、手順 7～12 を繰り返します。

単一リージョンネットワークの展開

April 13, 2021

組織に単一の管理（または地理的）境界にまたがる小規模なネットワークがある場合、Citrix SD-WAN Center をデフォルトモード（単一の「デフォルトリージョン」）で使用できます。リージョンは最大 550 サイトをサポートできます。

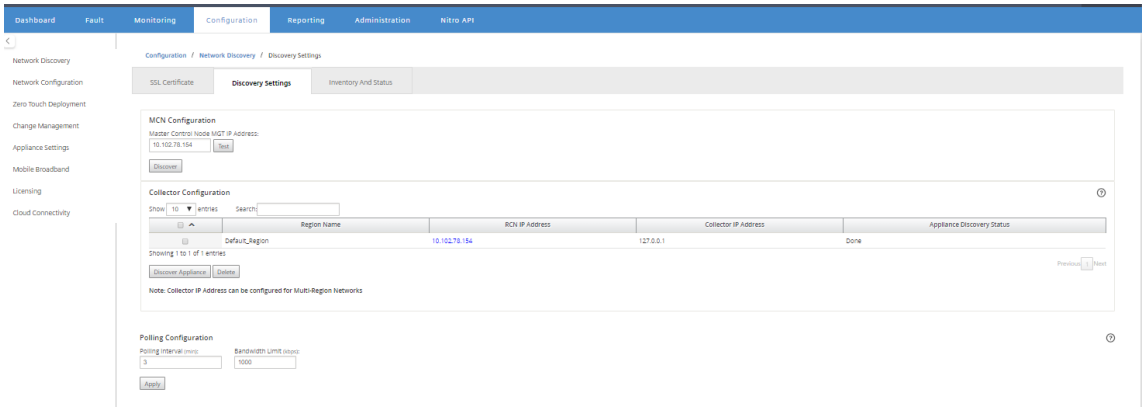
単一リージョンネットワークには、集中管理用のマスターコントロールノード（MCN）と集中管理用の Citrix SD-WAN Center があります。MCN に関連付けられ、MCN によって制御される領域は、デフォルト領域と呼ばれます。Citrix SD-WAN Center は、デフォルトリージョンの MCN とすべてのブランチアプライアンスをポーリングします。



単一リージョンに Citrix SD-WAN Center を展開するには：

1. Citrix SD-WAN Center ソフトウェア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。(/en-us/citrix-sd-wan-center/current-release/system-requirements-and-installation.html)
2. ESXi サーバー、XenServer、Hyper-VまたはAzureに Citrix SD-WAN Center をインストールします。
3. 管理インターフェース設定の構成。詳しくは、「管理インターフェース設定を構成する」を参照してください。
4. SD-WAN Center で SD-WAN MCN SSL 証明書を生成、ダウンロード、インストールします。詳しくは、「Citrix SD-WAN SSL 証明書をインストールする」を参照してください。

5. MCN アプライアンスで SD-WAN Center SSL 証明書を生成、ダウンロード、インストールします。詳しくは、「Citrix SD-WAN Center SSL 証明書をインストールする」を参照してください。
6. Citrix SD-WAN Center GUI で、構成 > ネットワーク発見 > 設定を確認に移動します。
7. [**Master Controller Node MGT IP Address**] フィールドに MCN IP アドレスを入力し、[**Test**] をクリックします。これにより、MCN と Citrix SD-WAN Center 間の接続が確立されます。



8. [検出] をクリックします。MCN をすでに検出している場合、このオプションは **Rediscover** に変わります。

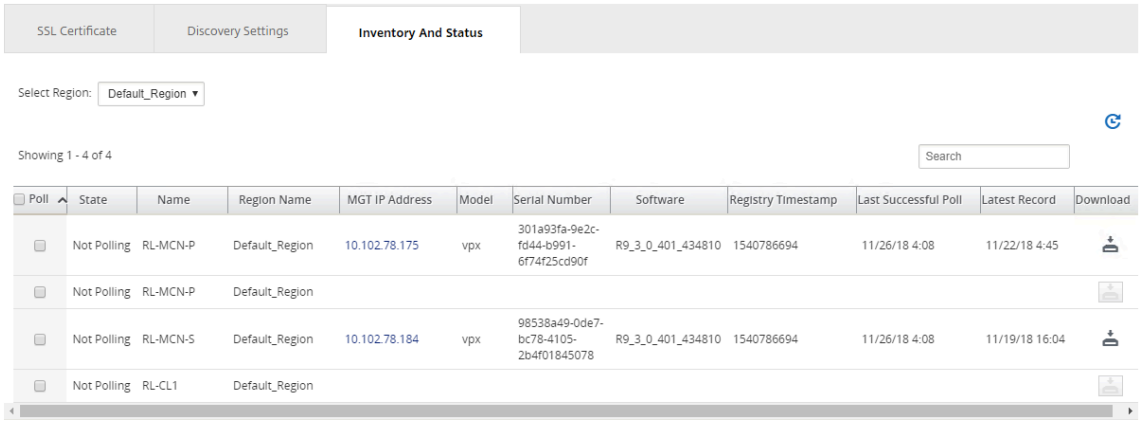
> 注
>
> MCN がアクティブで、SD-WAN サービスが有効になっている必要があります。詳しくは、「SD-WAN サービスの有効化」を参照してください。

9. 検出操作が完了したら、[インベントリとステータス] タブをクリックします。

   Inventory and Status テーブルには、検出されたすべての Citrix SD-WAN アプライアンスのステータス情報が表示されます。

10. 表の見出しの左上隅にある [投票] チェックボックスを選択します。

    これにより、表にリストされている各アプライアンスの「ポーリング」チェックボックスが選択されます。アプライアンスをポーリングリストから除外するには、そのチェックボックスをオフにします。



11. [**Apply**] をクリックします。

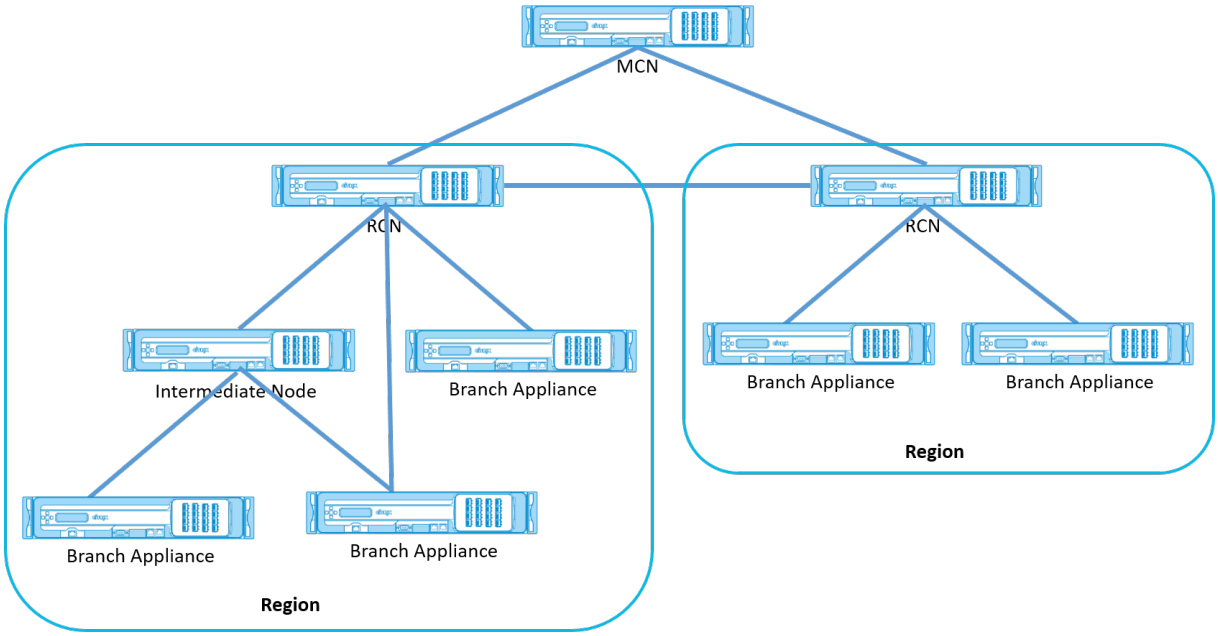
> ヒント
>
> 仮想マシン上にデータストアを作成し、データストアを切り替えることにより、Citrix SD-WAN Center のストレージサイズを増やすことができます。詳しくは、「アクティブなストレージを新しいデータストレージに切り替える」を参照してください。

マルチリージョンネットワークの導入

April 13, 2021

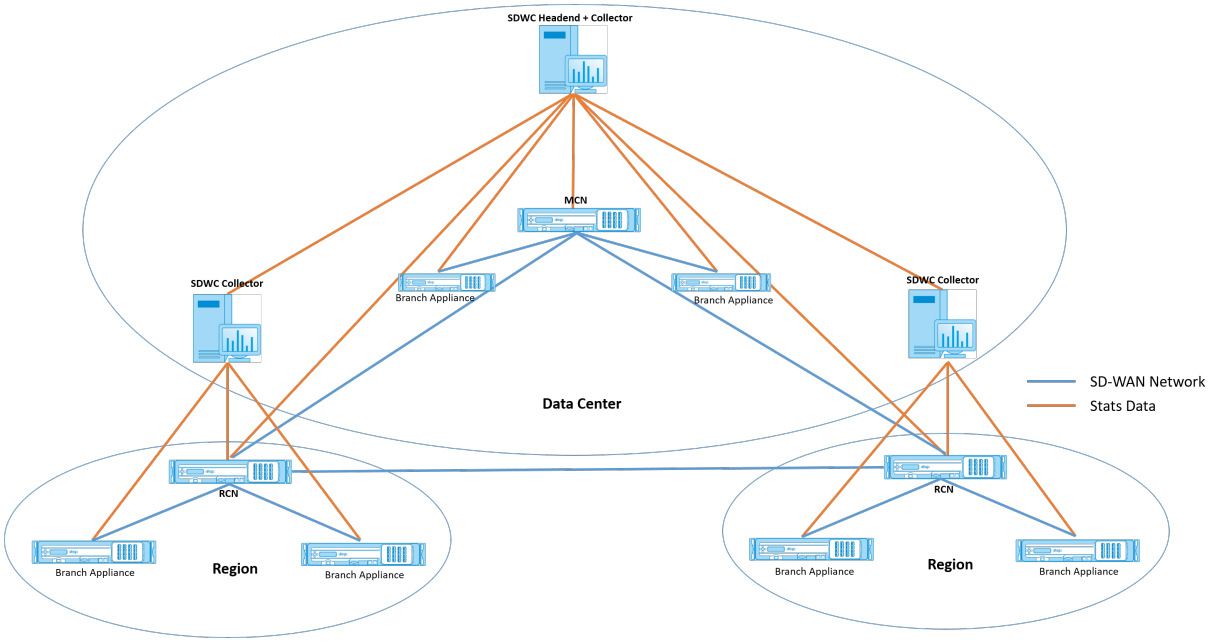
組織に複数の管理（または地理的）境界にまたがる大規模なネットワークがある場合、Citrix SD-WAN Center をマルチリージョンモードで使用できます。各リージョンは最大 550 サイトをサポートします。

マルチリージョンネットワークは、複数のリージョナルコントロールノード（RCN）を制御するマスターコントロールノード（MCN）による階層アーキテクチャをサポートします。各 RCN は、複数のクライアントサイトを制御します。MCN をオプションで使用して、「デフォルトの地域」の一部として一部のクライアントサイトを直接制御することもできます。この階層型の分散型アーキテクチャにより、地域管理のより大規模で効果的な委任が可能になります。



Citrix SD-WAN Center は、MCN、RCN、および関連するすべてのブランチアプライアンスをポーリングします。

マルチリージョンの Citrix SD-WAN Center アーキテクチャでは、リージョンレベルのデータと統計を収集して保存するために、リージョンごとにコレクターを追加する必要があります。この分散型アーキテクチャにより、ネットワーク全体を管理するための「単一の窓ガラス」ビューを維持しながら、複数のリージョンにまたがる大規模化が可能になります。

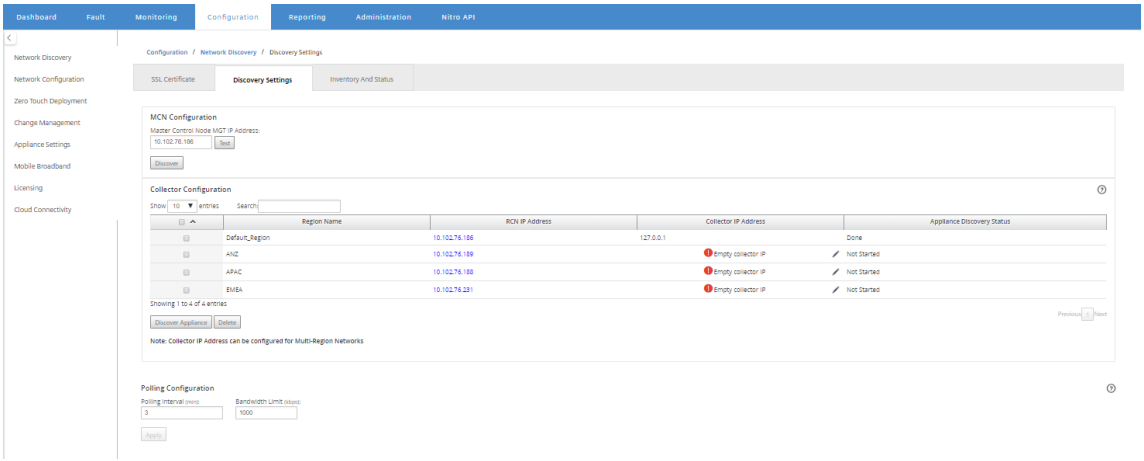


> 注
>
> マルチリージョン展開の場合、デフォルトのリージョン統計には、MCN と RCN によって管理されるすべてのサイトの統計が含まれます。ただし、RCN データは SD-WAN Center コレクターに保存されません。SD-WAN Center コレクターは、各地域コレクターから RCN サイトデータを取得します。

マルチリージョン用の **Citrix SD-WAN Center** を展開するには:

1. Citrix SD-WAN Center ソフトウェア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。(/en-us/citrix-sd-wan-center/current-release/system-requirements-and-installation.html)
2. ESXi サーバー、XenServer、Hyper-VまたはAzureに Citrix SD-WAN Center をインストールします。
3. 管理インターフェース設定の構成。詳しくは、「管理インターフェース設定を構成する」を参照してください。
4. SD-WAN Center で SD-WAN MCN SSL 証明書を生成、ダウンロード、インストールします。詳しくは、「Citrix SD-WAN SSL 証明書をインストールする」を参照してください。
5. MCN アプライアンスで SD-WAN Center SSL 証明書を生成、ダウンロード、インストールします。詳しくは、「Citrix SD-WAN Center SSL 証明書をインストールする」を参照してください。
6. Citrix SD-WAN Center GUI で、構成 > ネットワーク発見 > 設定を確認に移動します。
7. [**Master Controller Node MGT IP Address**] フィールドに MCN IP アドレスを入力し、[**Test**] をクリックします。これにより、MCN と Citrix SD-WAN Center 間の接続が確立されます。
8. [検出] をクリックします。MCN に接続されているすべての RCN のリストが [コレクタの構成] セクションに表示されます。デフォルト以外の地域サイトを検出するには、MCN へのアクティブなパスを持つアクティブな RCN が必要です。

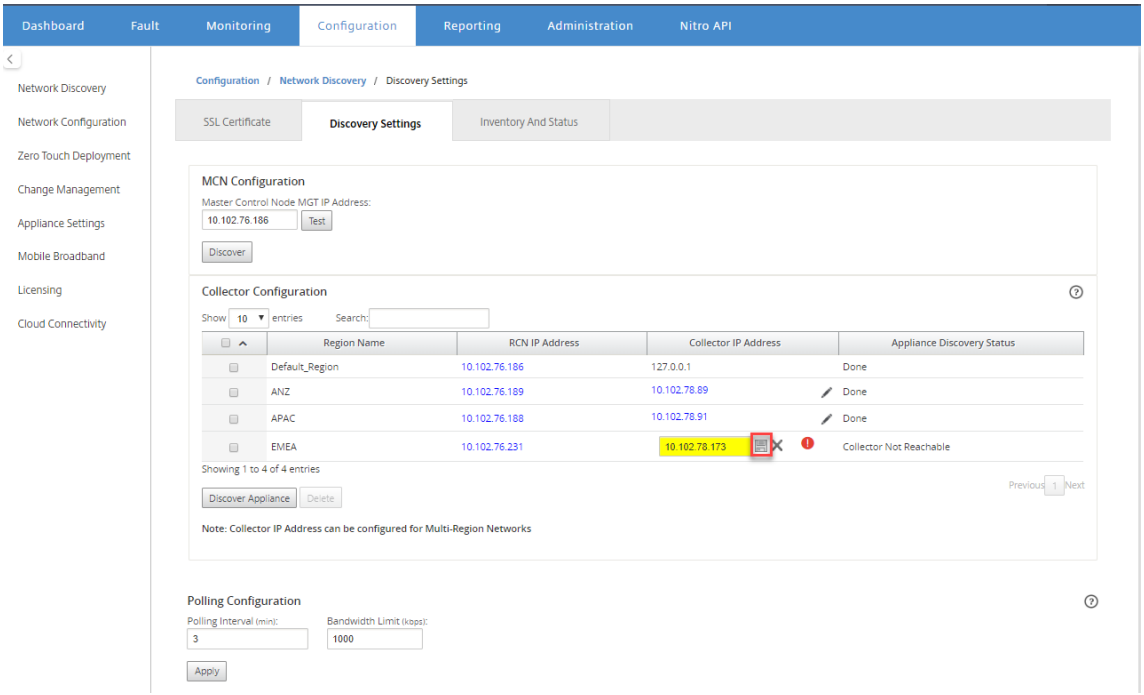
> 注
>
> Citrix SD-WAN Center は、デフォルトリージョンのコレクタとして機能します。



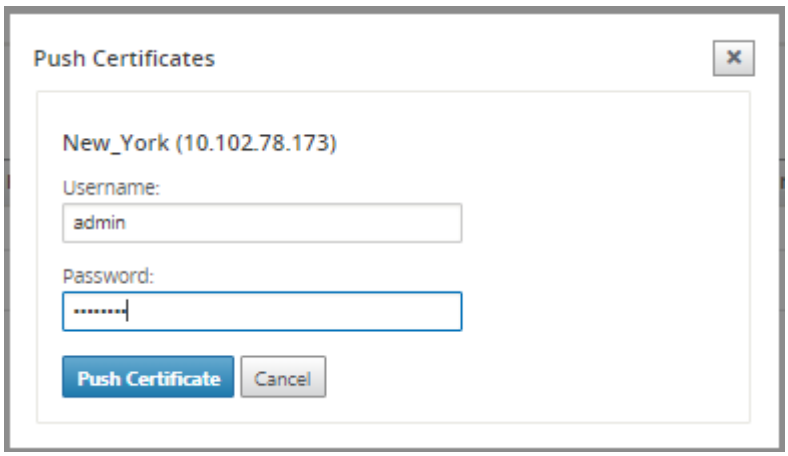
9. 編集アイコンをクリックし、[コレクター **IP]** フィールドに、リージョンのコレクターとして構成する Citrix SD-WAN Center の IP アドレスを入力します。

> 注
>
> コレクターをセットアップするには、Citrix SD-WAN Center VM をインストールし、管理 IP アドレスを構成します。その Citrix SD-WAN Center の管理 IP アドレスがコレクター IP アドレスです。

10. 「保存」アイコンをクリックしてコレクターの IP アドレスを保存し、証明書とキーのペアを RCN にプッシュします。

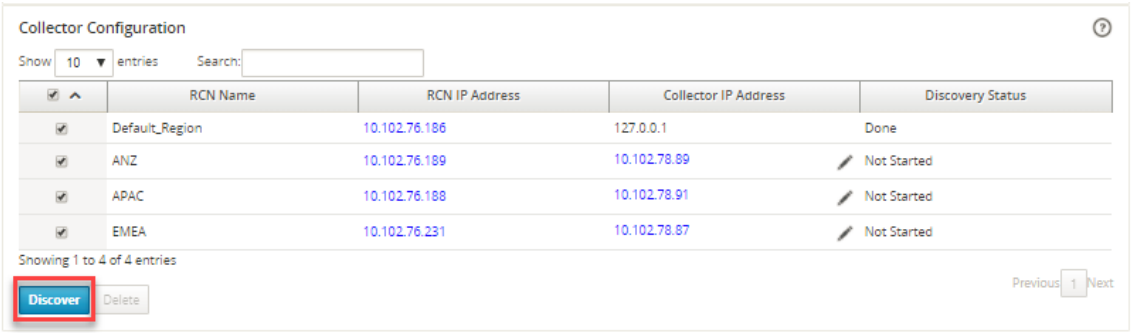


11. RCN の資格情報を入力し、[証明書のプッシュ] をクリックします。

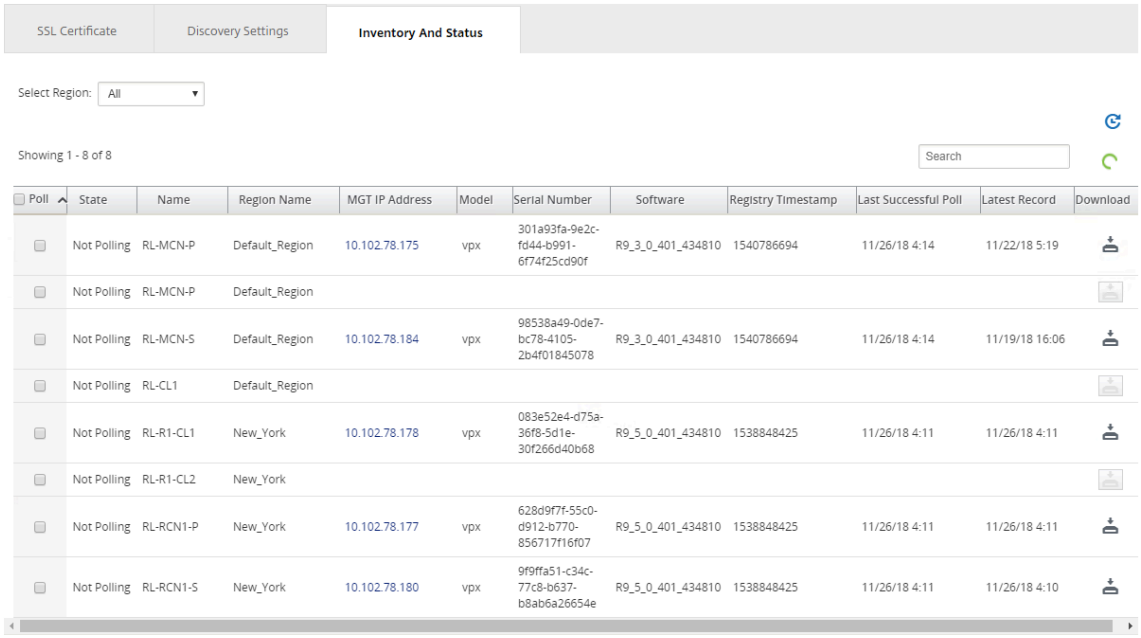


12. 同様に、すべての RCN のコレクター IP アドレスを構成します。

> 注
>
> アプライアンスは 30 分ごとに自動的に検出されます。新しい RCN がネットワークに追加され、変更管理が行われた場合、アプライアンスを選択して [アプライアンスの検出] をクリックすると、アプライアンスがすぐに検出されます。



検出ステータス が [完了] に変わったら、検出されたサイトを [インベントリとステータス] ページで表示できます。



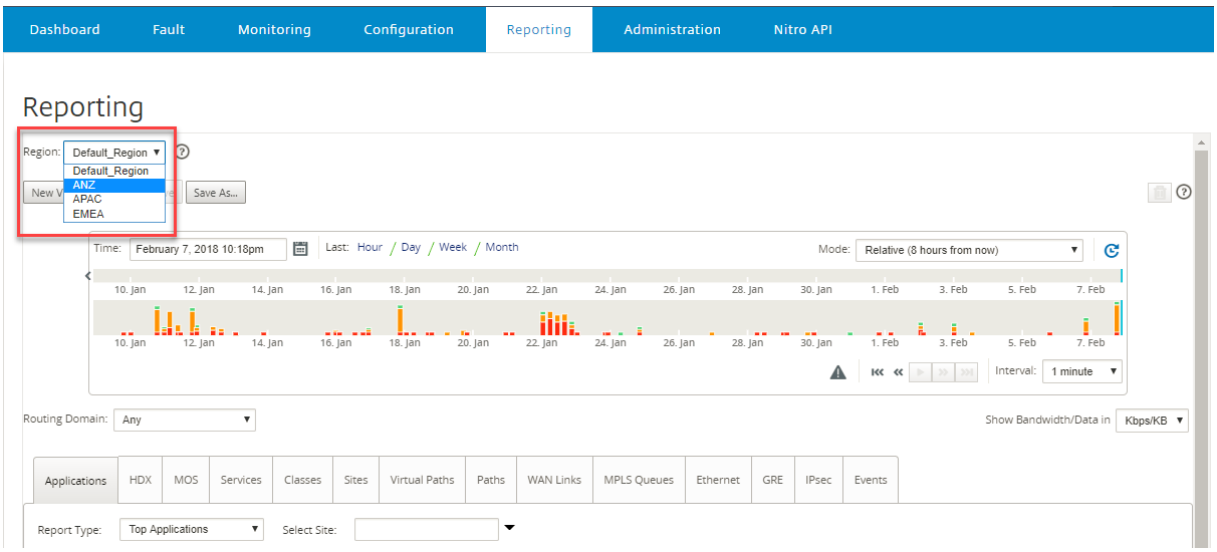
> ヒント
>
> 地域名に基づいてサイトをフィルタリングできます。[地域 の選択] フィールドで、地域を選択します。

13. [インベントリとステータス] ページで、ポーリングを開始するサイトを選択し、[適用] をクリックします。

> ヒント
>
> 仮想マシン上にデータストアを作成することにより、コレクターのストレージサイズを増やすことができます。詳しくは、「アクティブストレージを新しいデータストレージに切り替える」を参照してください。

特定の地域を選択して、イベントおよび統計レポートを表示できます。

イベントと統計レポートのデータは、それぞれのリージョンのコレクターからフェッチされます。



構成

April 13, 2021

Citrix SD-WAN Center を構成する最初のいくつかの手順は、シングルリージョンネットワークとマルチリージョンネットワークの両方に共通です。以下は、一般的な構成手順のリストです。

- 管理インターフェース設定を構成する
- Citrix SD-WAN Center 証明書をインストールします。
- activre ストレージを新しいデータ sorage に切り替えます。

管理インターフェース設定を構成する

April 9, 2021

Citrix SD-WAN Center Web インターフェイスを使用して、管理インターフェイスの設定を構成できます。

管理インターフェイスの設定には、次のものが含まれます。

- Citrix SD-WAN Center 管理 IP アドレス
- Gateway IP アドレス
- サブネット マスク
- プライマリ DNS
- セカンダリ DNS

管理インターフェース設定を構成するには:

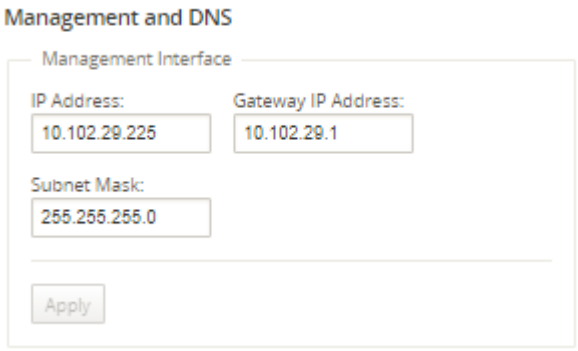
1. Citrix SD-WAN Center Web インターフェイスで、[管理] タブを選択します。

   デフォルトでは、**User/Authentication** 設定 ページが表示されます。

2. ナビゲーションツリーで、[グローバル設定] を選択します。
3. 管理と DNS 設定を構成します。

   [管理と **DNS]** セクションで、次のフィールドに必要な情報を追加します。

   - **IP** アドレス: Citirx SD-WAN Center の IP アドレスを入力します。
   - **Gateway IP** アドレス: Citrix SD-WAN Center VM が外部ネットワークとの通信に使用する Gateway IP アドレスを入力します。
   - サブネットマスク: サブネットマスクを入力して、Citrix SD-WAN Center VM が存在するネットワークを定義します。



4. [適用] をクリックします。

> 注
>
> 変更が適用されると、Citrix SD-WAN Center への接続が終了します。

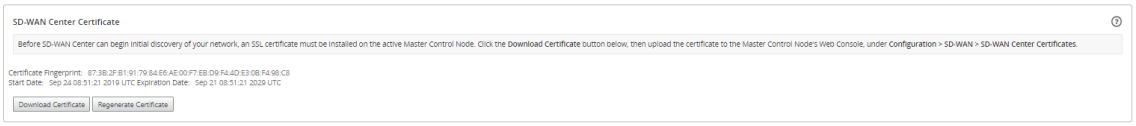
SD-WAN Center SSL 証明書をインストールする

April 9, 2021

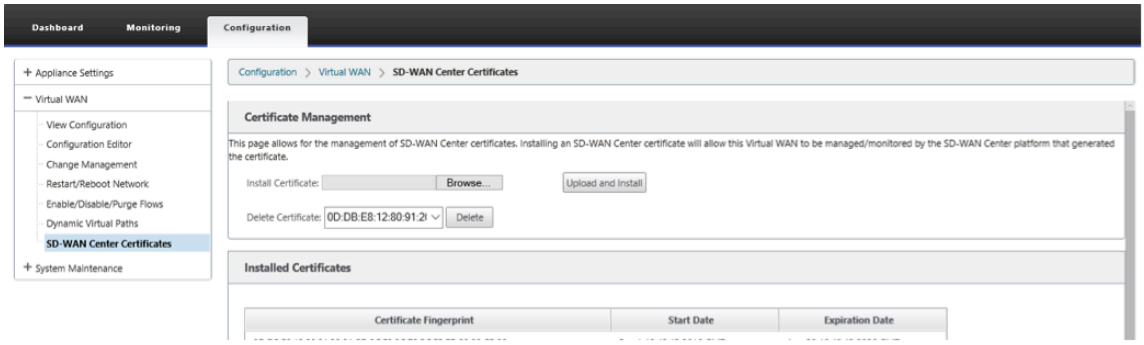
Citrix SD-WAN Center と Citrix SD-WAN マスターコントロールノード (MCN) 間の接続を確立するには、SD-WAN Center から SSL 証明書をダウンロードし、MCN にインストールします。

Citrix SD-WAN Center 証明書を生成してインストールするには:

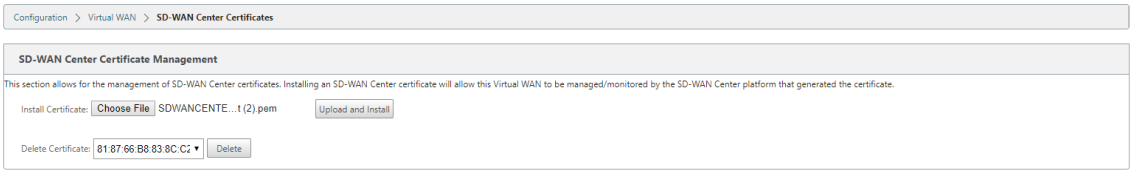
1. Citrix SD-WAN Center の Web インターフェイスで、設定 > ネットワーク発見 > **SSL** 証明書 > **SD-WAN Center** 証明書 に移動します。
2. [証明書の再生成] をクリックして、MCN との通信を確立するための新しい SSL 証明書を生成します。



3. [証明書のダウンロード] をクリックします。目的の場所に移動し、証明書を保存します。
4. Citrix SD-WAN MCN Web インターフェイスで、**Configuration** > 仮想 **WAN** > **SD-WAN Center** 証明書 > **SD-WAN Center** 証明書管理に移動します。



5. [ファイルの選択**]** をクリックし、ダウンロードした SD-WAN Center SSL 証明書を参照して選択します。



6. [**Upload and Install]** をクリックすると、SD-WAN Center の SSL 証明書が MCN にアップロードされ、インストールが完了すると成功メッセージが表示されます。

Citrix SD-WAN SSL 証明書をインストールする

April 13, 2021

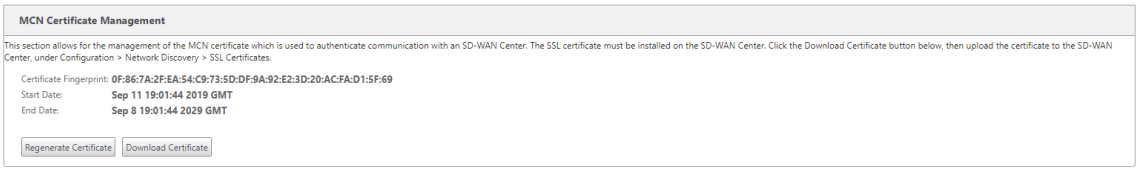
Citrix SD-WAN MCN と Citrix SD-WAN Center 間の接続を確立するには、MCN SD-WAN アプライアンスから SSL 証明書をダウンロードし、SD-WAN Center にインストールします。

事前定義された証明書を置き換える MCN でアプライアンス証明書を再生成して、SD-WAN Center にインストールできます。

新しい展開と SSL 通信を機能させるには、SD-WAN Center へのアプライアンス証明書のインストールが必須です。MCN はネットワーク証明書を生成し、証明書マネージャーを介してすべてのノードに秘密キーと共に証明書を配布します。証明書は、SD-WAN Center を認証するために各ブランチで使用されます。

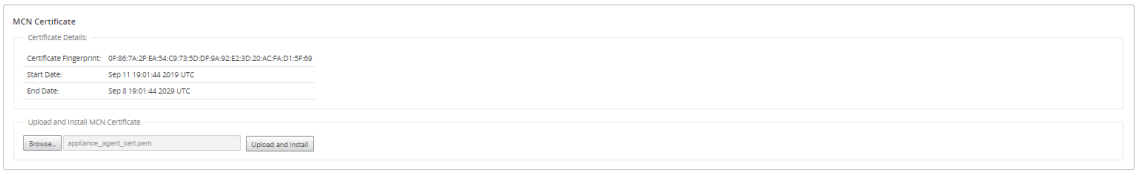
SD-WAN 証明書を生成してインストールするには:

1. MCN SD-WAN アプライアンスで、[構成**]**> 仮想 **WAN**>**SD-WAN Center** 証明書 >**MCN** 証明書の管理 に移動します。
2. [証明書の再 生成] をクリックして、SD-WAN Center との通信を確立するための新しい SSL 証明書を生成します。

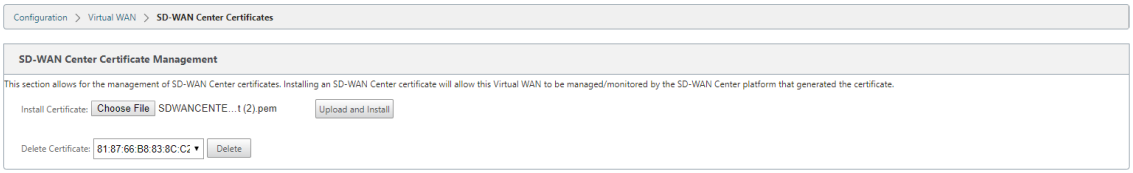


> 注:
>
> SSL 証明書を再生成すると、SD-WAN アプライアンスは新しい証明書をすぐに使用して、検出された SD-WAN Center との通信を行います。ただし、新しく生成された証明書を SD-WAN Center にダウンロードしてインストールするまで、アプライアンスとの通信は確立されません。

3. [証明書のダウンロード] をクリックします。目的の場所に移動し、証明書を保存します。
4. Citrix SD-WAN Center の Web インターフェイスで、設定 > **SSL** 証明書 > **MCN** 証明書 に移動します。



5. [参照] をクリックして、ダウンロードした MCN SSL 証明書を選択します。



6. [アップロードしてインストール] をクリックすると、MCN SSL 証明書が SD-WAN Center にアップロードされます。

アクティブなストレージを新しいデータストレージに切り替える

April 13, 2021

Citrix SD-WAN Center では、アクティブストレージを仮想サーバー上に作成したデータストアに切り替えることができます。これにより、WAN 内のすべての Citrix SD-WAN アプライアンスをポーリングして取得した統計データをより多く保存できます。ESXi サーバーでのデータストアの作成については、「ESXi サーバーでのデータストアの追加と構成」を参照してください。XenServer でのデータストアの作成については、「XenServer でのデータストレージの追加と構成」参照してください。

Citrix SD-WAN Center VM のアクティブストレージを指定するには:

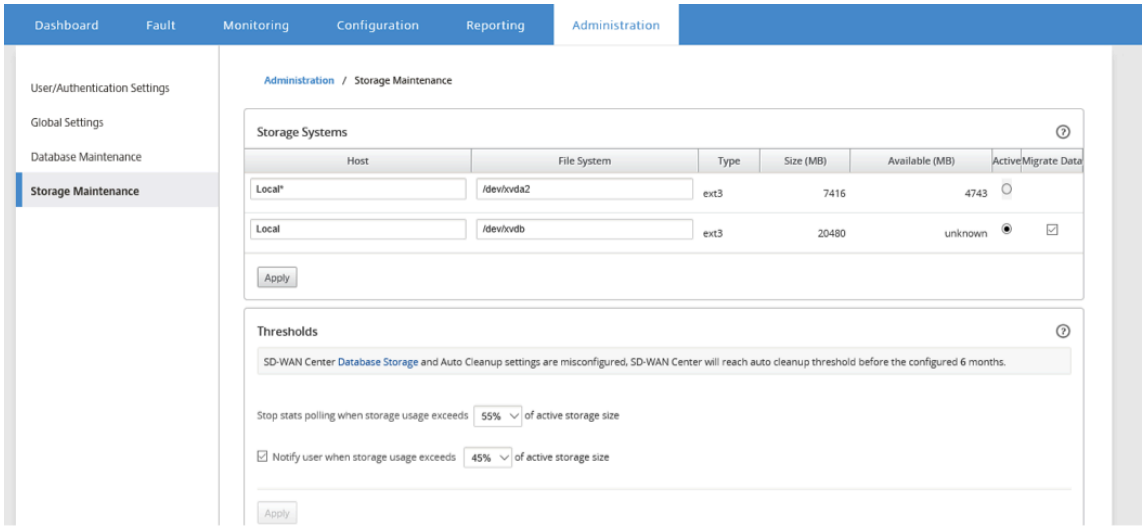
1. Citrix SD-WAN Center VM にログインします。

Citrix SD-WAN Center のデフォルトのログイン認証情報は次のとおりです。

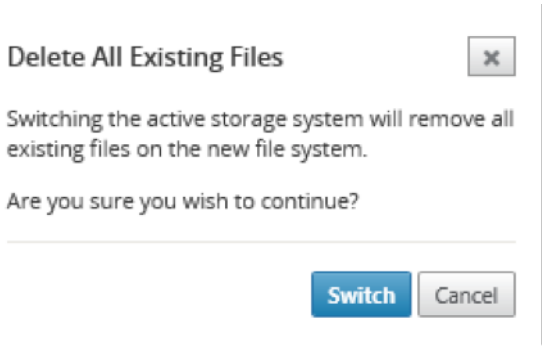
ログイン：**admin**

パスワード：**password**

2. [管理] タブをクリックし、[ストレージのメンテナンス] をクリックします。



3. [ストレージシステム] テーブルの [アクティブ] 列で、作成したストレージを選択します。
4. [データの移行] を選択し、[適用] をクリックします。
5. **[**既存のファイルをすべて削除**]** メッセージが表示されたら、[切り替え] をクリックします。



これにより、Citrix SD-WAN Center が メンテナンスモードに なり、メインページ領域に進行状況バーが表示されます。

6. アクティベーションが完了したら、[続行] をクリックします。

これにより、進行状況バーが閉じ、メインの [ストレージメンテナンス**]** ページに戻ります。

Citrix SD-WAN アプライアンスの導入

April 13, 2021

Citrix SD-WAN Center を使用してアプライアンス構成またはアプライアンス設定ファイルを作成し、変更管理ウィザードを使用して構成をネットワーク上のアプライアンスにプッシュできます。詳しくは、「Citrix SD-WAN アプライアンスの構成」を参照してください。

中央ライセンスサーバーとして機能するように Citrix SD-WAN Center を構成し、ネットワーク内のすべてのノードにライセンスサービスを提供できます。これにより、個々のノードにローカルでライセンスをインストールする必要がなくなります。詳しくは、「ライセンスサーバーとしての Citrix SD-WAN Center」を参照してください。

Citrix SD-WAN Center を使用すると、ゼロタッチ展開機能を使用して、ブランチオフィスに SD-WAN アプライアンスを展開するプロセスを合理化できます。詳しくは、「ゼロタッチ展開」を参照してください。

Citrix SD-WAN アプライアンスの構成

April 13, 2021

構成エディターを使用して、構成設定を編集し、構成パッケージを MCN にエクスポートします。詳しくは、「構成エディター」を参照してください。

MCN アプライアンスの変更管理ウィザードは、Citrix SD-WAN Center から使用できます。詳しくは、「変更管理ウィザード」を参照してください。

Citrix SD-WAN Center でアプライアンス設定を構成し、SD-WAN ネットワーク内の管理された Citrix SD-WAN アプライアンスのセットにエクスポートできます。詳細については、アプライアンスの設定を参照してください。

構成エディター

April 9, 2021

構成エディターは、Citrix SD-WAN Center Web インターフェイスのコンポーネントとして、および SD-WAN ネットワークのマスターコントロールノード（MCN）で実行されている Citrix SD-WAN 管理 Web インターフェイスで使用できます。

> 注
>
> 検出されたアプライアンスに構成を Citrix SD-WAN Center から直接プッシュすることはできません。構成エディターを使用して、構成設定を編集し、構成パッケージを作成できます。構成パッケージが作成されたら、

> MCN にエクスポートしてインストールできます。変更は MCN に反映されます。
>
> Citrix SD-WAN Center アプライアンスと MCN に管理者権限でログオンし、Citrix SD-WAN Center の構成を編集し、MCN に構成をエクスポートしてインストールする必要があります。

構成エディターを使用して Citrix SD-WAN を構成する方法の詳細については、「Citrix SD-WAN 10.1」ドキュメントを参照してください。

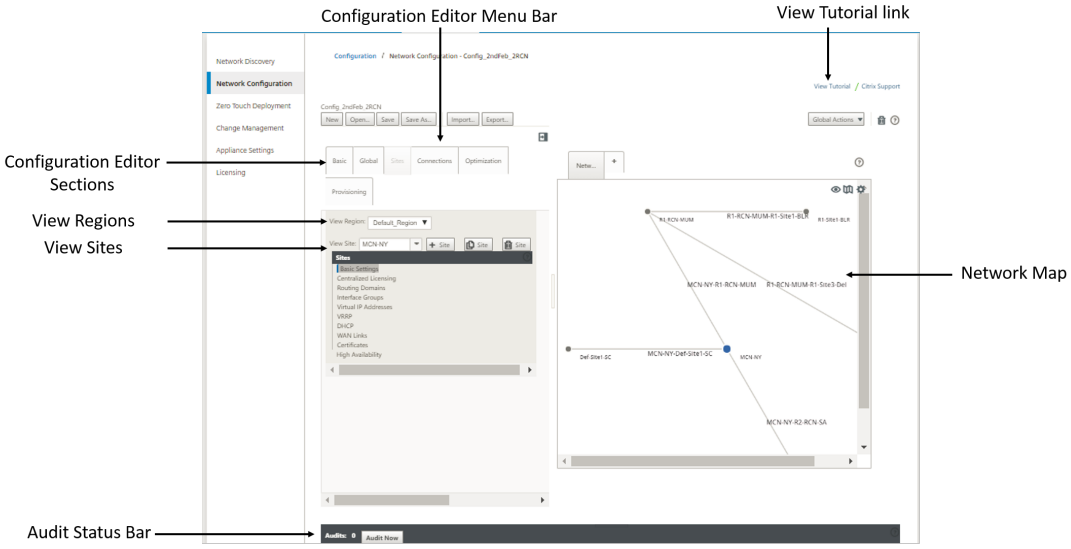
構成エディターを使用すると、以下を実行できます。

- Citrix SD-WAN アプライアンスのサイトと接続を追加して構成します。
- Citrix SD-WAN アプライアンスをプロビジョニングします。
- Citrix SD-WAN 構成を作成および定義します。
- SD-WAN システムのネットワークマップを定義して表示します。

構成エディターを開くには:

1. Citrix SD-WAN Center の Web インターフェイスで、[構成] タブをクリックします。
2. [**Network Configuration]** をクリックします。

   以下の図は、構成エディターの基本的なナビゲーションとページ要素、およびこのガイドでそれらを識別するために使用される用語の概要を示しています。



   構成エディターのメイン画面には、次のナビゲーション要素があります。

- 構成エディターのメニューバー: 構成エディターの操作のための主要なアクティビティボタンが含まれています。さらに、メニューバーの右端には、構成エディターのチュートリアルを開始するための **[**チュートリアルの表示] リンクボタンがあります。このチュートリアルでは、構成エディターの表示の各要素について、一連のバブルの説明を示します。

- 構成エディターのセクション: 各タブはトップレベルのセクションを表します。基本、グローバル、サイト、接続、最適化、プロビジョニングの 6 つのセクションがあります。セクションタブをクリックして、そのセクションの構成ツリーを表示します。
- 地域を見る: マルチリージョンのデプロイの場合、構成されているすべてのリージョンが一覧表示されます。単一リージョンのデプロイの場合、デフォルトで default-region が表示されます。地域内のサイトを表示するには、ドロップダウンリストから地域を選択します。
- サイトの表示: 構成に追加され、現在構成エディターで開かれているサイトノードを一覧表示します。サイト構成を表示するには、ドロップダウンリストからサイトを選択します。
- ネットワークマップ: SD-WAN ネットワークの概略図を提供します。マウスカーソルをサイトまたはパスの上に置くと、詳細が表示されます。サイトをクリックして、レポートオプションを表示します。
- 監査ステータスバー: 構成エディターページの下部にある濃い灰色のバーで、構成エディターページの幅全体に広がります。監査 ステータスバーは、構成エディター が開いているときにのみ使用できます。ステータスバーの左端にある監査アラートアイコン（赤い点またはゴールデンロッドデルタ）は、現在開いている構成に 1 つ以上のエラーが存在することを示します。ステータスバーをクリックして、その構成のすべての未解決の監査アラートの完全なリストを表示します。

変更管理ウィザード

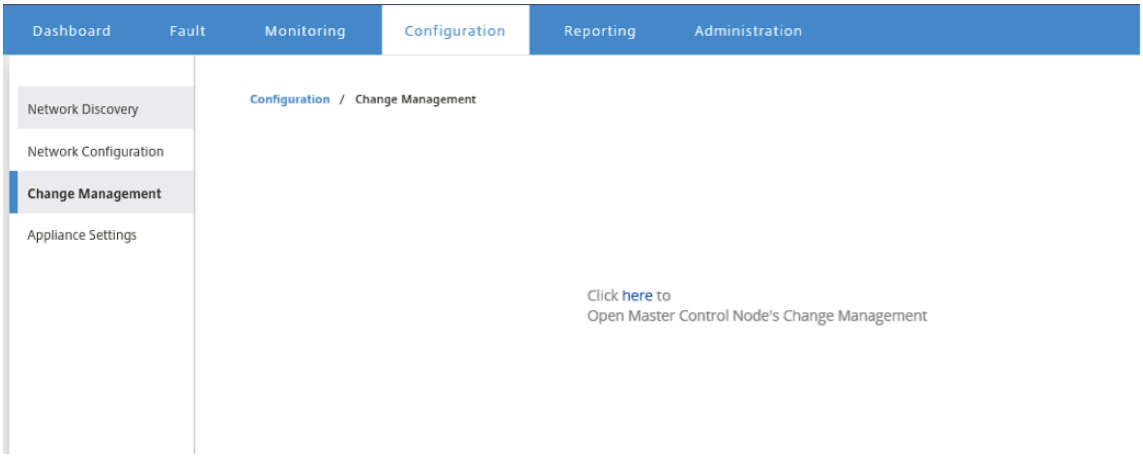
April 13, 2021

変更管理ウィザードは、マスターコントロールノード（MCN）アプライアンスとクライアントアプライアンスでの Citrix SD-WAN ソフトウェアと構成のアップロード、ダウンロード、ステージング、アクティブ化のプロセスをガイドします。

変更管理ウィザードは、MCN で実行される Citrix SD-WAN 管理 Web インターフェイスのコンポーネントであり、Citrix SD-WAN Center の一部ではありません。ただし、Citrix SD-WAN Center を使用して、指定した MCN に接続し、変更管理ウィザードにアクセスできます。

変更管理ウィザードを開くには:

1. Citrix SD-WAN Center の Web インターフェイスで、[構成] タブをクリックします。
2. [変更管理] をクリックします。



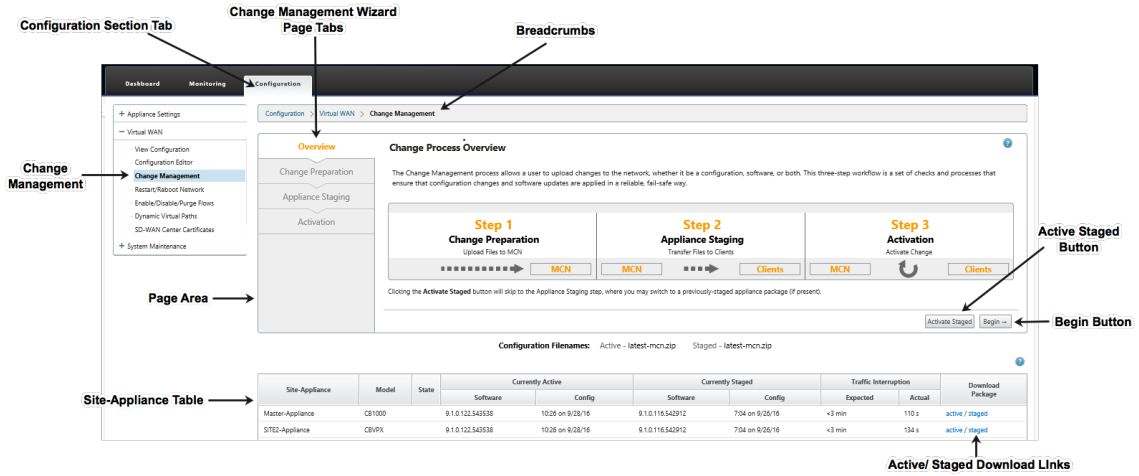
3. **[**ここをクリックしてマスターコントロールノードを開く] の [変更管理] プロンプトで、[ここ] リンクをクリックします。

   MCN GUI に自動的にログインします。

   > 注
   >
   > MCN 認証情報を使用して MCN GUI にログインする必要はありません。自動ログイン機能によりシングルサインオンが可能になります。

4. MCN 管理 Web インターフェイスで、[構成] タブをクリックします。
5. ナビゲーションツリー（左側のペイン）で、+ 仮想 **WAN** ブランチの横にあるそのブランチを展開します。**
6. [変更管理**]** をクリックします。

   次の図に示すように、変更管理 ウィザードの最初のページである [変更プロセスの概要**]** ページが表示されます。



7. ウィザードを起動するには、クリックして 開始します。

> 注
>
> ウィザードを使用して、アプライアンスで SD-WAN ソフトウェアと構成をアップロード、ステージング、アクティブ化する手順の詳細については、SD-WAN 9.1.0 ユーザーガイドを参照してください。

変更管理 ウィザードには、次のナビゲーション要素があります。

- ページ領域: 変更管理 ウィザードの各ページのフォーム、テーブル、およびアクティビティボタンを表示します。
- 変更管理ウィザードのページタブ: ページ領域の左側のウィザードの各ページには、ウィザードプロセスで対応する手順が発生する順にタブが一覧表示されます。タブがアクティブになっている場合、タブをクリックしてウィザードの前のページに戻ることができます。アクティブなタブの名前は青色のフォントで表示されます。灰色のフォントは、非アクティブなタブを示します。すべての依存関係（前の手順）がエラーなしで実行されるまで、タブは非アクティブです。
- アプライアンス-サイトテーブル: ウィザードページ領域の下部にあるこのテーブルには、構成済みの各アプライアンスサイトに関する情報と、そのアプライアンスモデルとサイトのアクティブまたはステージングされたアプライアンスパッケージをダウンロードするためのリンクが含まれています。このコンテキストのパッケージは、そのアプライアンスモデルに適切な SD-WAN ソフトウェアパッケージと指定された構成パッケージを含む zip ファイルバンドルです。表の上にある [構成ファイル名] セクションには、ローカルアプライアンスで現在アクティブでステージングされているパッケージのパッケージ名が表示されます。
- Active/Staged ダウンロードリンク: **Appliance-Site** テーブルの各エントリの [**Download Package]** フィールド（右端の列）で、エントリのリンクをクリックして、そのアプライアンスのサイトのアクティブなパッケージまたはステージングされたパッケージをダウンロードできます。
- 開始ボタン: 変更管理ウィザード のプロセスを開始し、変更の準備タブ ページに進み 開始] をクリックします。
- ステージングボタンをアクティブにする: これが初期展開ではなく、現在ステージングされている構成をアクティブ化する場合は、アクティブ化 ステップに直接進むことができます。[ステージングの アクティブ化] をクリックして、[アクティブ 化] ページに直接進み、現在ステージングされている構成のアクティブ化を開始します。

アプライアンスの設定

April 9, 2021

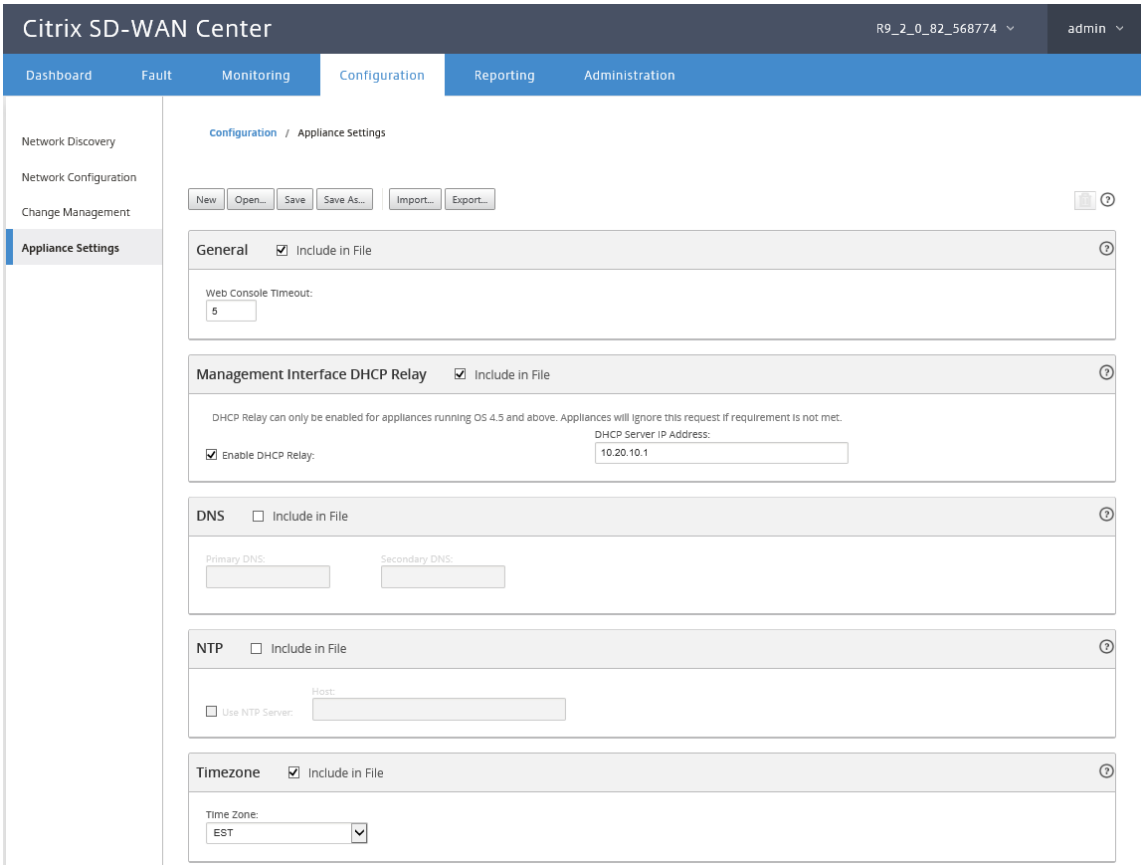
Citrix SD-WAN Center でアプライアンス設定を構成し、SD-WAN ネットワーク内の管理された Citrix SD-WAN アプライアンスのセットにエクスポートできます。アプライアンスの設定 ページでは、次の操作を実行できます。

- 新しいアプライアンス設定ファイルを作成します。
- 既存のアプライアンス設定ファイルを開いて編集します。

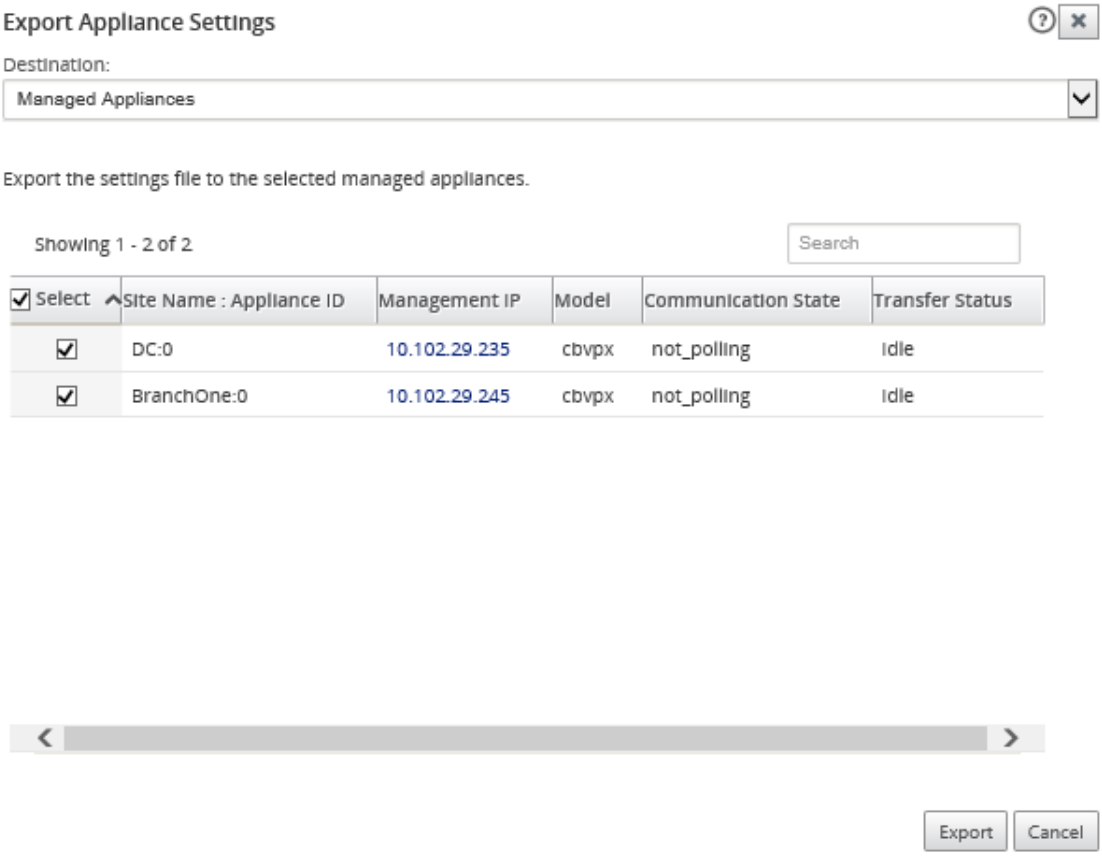
- ローカルコンピュータからアプライアンス設定ファイルをインポートします。
- アプライアンス設定ファイルをローカルコンピューターにダウンロードします。
- アプライアンス設定ファイルを管理アプライアンスにエクスポートします。

アプライアンス設定ファイルを作成して管理アプライアンスにエクスポートするには:

1. Citrix SD-WAN Center の Web インターフェイスで、[構成] タブをクリックします。
2. [アプライアンスの設定] をクリックし、[新規] をクリックします。



3. 必要な設定について [ファイル に含める] を選択し、設定のパラメーター値を指定します。詳しくは、「アプライアンス設定表」を参照してください。
4. [エクスポート] をクリックします。[名前を付けて 保存] ダイアログボックスで、アプライアンス設定ファイルの名前を入力し、[保存] をクリックします。[アプライアンス設定 のエクスポート] ダイアログボックスが表示されます。
5. 「宛先」フィールドで「管理アプライアンス」を選択し、アプライアンス設定をエクスポートするアプライアンスを選択します。



> 注
>
> アプライアンスの設定をローカルコンピューターに ダウンロード するには、[送信先] フィールドで [ファイルのダウンロード] を選択します。

6. エクスポートをクリックします。

リモート **LTE** サイト管理

February 18, 2022

Citrix SD-WAN Center を使用すると、ネットワーク内のすべての LTE サイトをリモートで表示および管理できます。これには、内部 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。

Citrix SD-WAN 210 SE LTE や 110LTE Wi-Fi アプライアンスなどの Citrix SD-WAN アプライアンスには、LTE モデムが内蔵されています。外部 3G/4G USB モデムは、以下の Citrix SD-WAN アプライアンスでも接続できます。

- Citrix SD-WAN 210 SE
- Citrix SD-WAN 210 SE LTE

- Citrix SD-WAN 110 SE
- Citrix SD-WAN 110 LTE Wi-Fi SE

サポートされている外部 USB モデムは、CDC イーサネット、MBIM、および NCM の 3 種類です。新しい Citrix SD-WAN GUI および Citrix SD-WANCitrix SD-WAN Center を使用して、APN 設定とモデムの有効化/無効化を構成できます。モバイルブロードバンド操作は、CDC イーサネット USB モデムではサポートされていません。

外部 LTE モデムの関連事項:

- サポートされている USB LTE ドングルを使用してください。対応ドングルのハードウェアモデルは Verizon USB730L と AT&T USB800 である。
- SIM カードが USB LTE ドングルに挿入されていることを確認します。CDC イーサネット LTE ドングルには静的 IP アドレスがあらかじめ設定されているため、SIM カードが挿入されていないと、設定が妨げられ、接続障害や断続的な接続が発生します。
- CDC イーサネット LTE ドングルを SD-WAN アプライアンスに挿入する前に、外部 USB スティックを Windows/Linux マシンに接続し、適切な APN およびモバイルデータローミング構成でインターネットが正常に動作していることを確認します。USB ドングルの接続モードがデフォルト値の手動から自動に変更されていることを確認します。

> 注
>
> - Citrix SD-WAN アプライアンスは、一度に 1 つの USB LTE ドングルしかサポートしません。複数の USB ドングルが接続されている場合は、すべてのドングルを外し、1 つのドングルだけを接続します。
> - Citrix SD-WAN アプライアンスは、USB モデムのユーザー名とパスワードをサポートしていません。セットアップ中に、モデムでユーザー名とパスワードの機能が無効になっていることを確認してください。
> - 外部 MBIM ドングルのプラグを抜いたり再起動したりすると、内部 LTE モデムのデータセッションに影響します。これは予想される動作です。
> - 外部 LTE モデムを接続すると、SD-WAN アプライアンスで認識されるまでに約 3 分かかります。

内部モデムと外部モデムでサポートされる操作:

操作	内蔵モデム	外部モデム-CDC イーサネット	外部モデム-MBIM および NCM
SIM プリファレンス	はい-デュアル SIM をサポートするアプライアンスの場合	いいえ	いいえ
SIM ピン	はい	いいえ	いいえ
APN 設定	はい	いいえ	はい
ネットワーク設定	はい	いいえ	いいえ
ローミング	はい	いいえ	いいえ
ファームウェアを管理する	はい	いいえ	いいえ

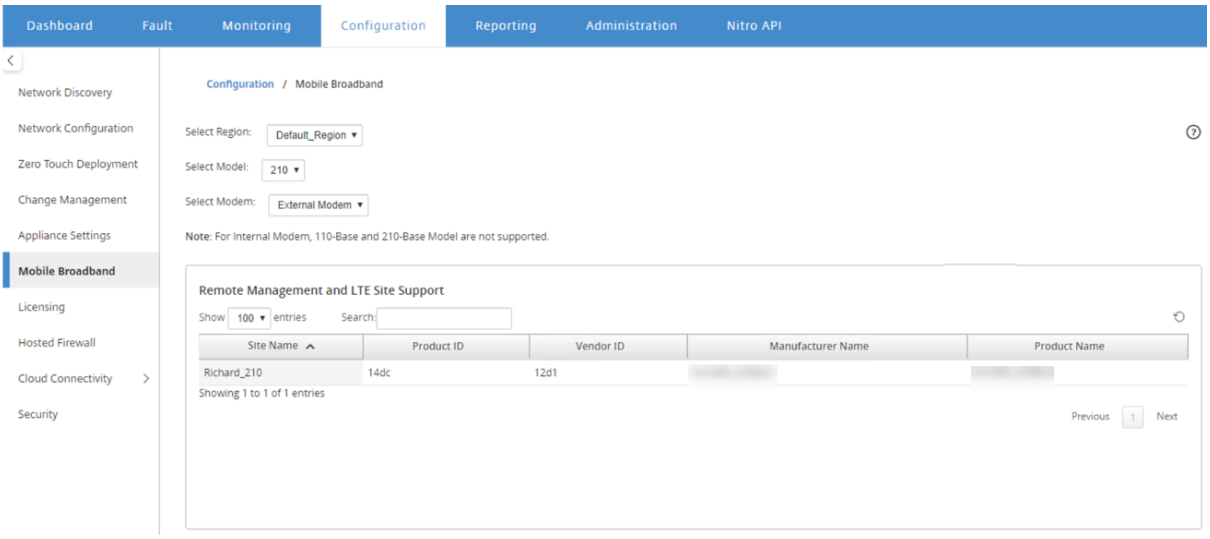
操作	内蔵モデム	外部モデム-CDC イーサネット	外部モデム-MBIM および NCM
モデムの有効化/無効化	はい	いいえ	はい
モデムの再起動	はい	いいえ	いいえ
SIM をリフレッシュ	はい	いいえ	いいえ

ネットワーク内の LTE サイトをリモート管理するには、SD-WAN Center UI で、構成 **>** モバイルブロードバンド に移動します。ここには、SD-WAN Center によって管理される、サイト全体のすべての LTE アプライアンスがリストされます。

マルチリージョン展開では、LTE サイトを管理するリージョンを選択できます。Default_Region が デフォルトで選択されています。

LTE アプライアンスモデルとモデムタイプを選択することもできます。

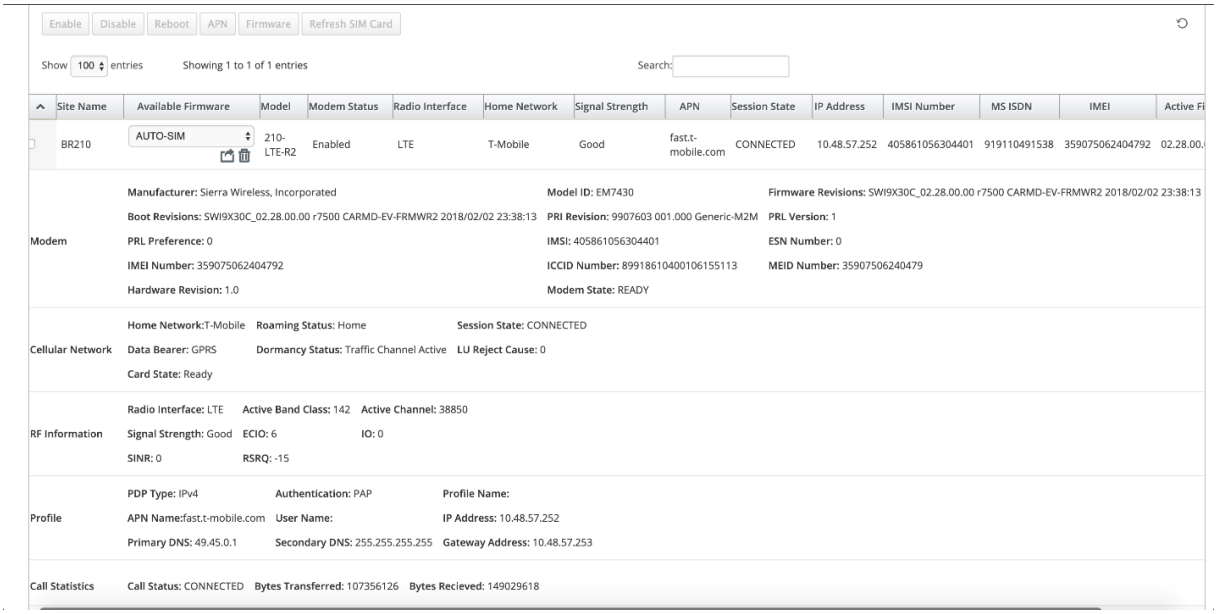
外部モデムを使用してアプライアンスを一覧表示するには、構成 > モバイルブロードバンドに移動します。モデムの種類として [外部モデム] を選択します。



> 注
>
> SIM PIN およびその他の LTE モデム構成は、現在、外部モデムではサポートされていません。

内蔵モデムを使用してアプライアンスを一覧表示するには、設定 > モバイルブロードバンドに移動します。モデムの種類として [内蔵モデム] を選択します。

> 注
>
> LTE の操作は、LTE モデルによって異なります。



単一のアプライアンスまたは複数のアプライアンスを選択して、次の LTE モデム操作を実行できます。

- 有効にする: 選択したサイトでモデムを有効にします。
- 無効にする: 選択したサイトでモデムを無効にします。
- リブート: 選択したサイトでモデムを再起動します。
- **APN**: 選択したサイトの APN 設定を構成します。詳細については、「APN 設定の構成」を参照してください。
- ファームウェア: このオプションは、210 LTE アプライアンスにのみ適用されます。必要なファームウェアを参照して選択します。アップロードのみを選択するか、選択したサイトにファームウェアファイルをアップロードして適用するかを選択できます。利用可能なファームウェアのリストから、それを適用するか削除するかを選択できます。

  > 注
  >
  > マルチリージョン展開では、デフォルト以外のリージョンサイトのファームウェア操作を SD-WAN Center ヘッドエンドから実行することはできません。特定のリージョンのコレクター SD-WAN Center からファームウェア操作を実行できます。

- **SIM** カードを更新: 選択したサイトで SIM カードをオフにしてからオンに戻し、SIM カードを更新します。この操作は、210 SE LTE モデムに挿入された新しい SIM カードを検出するために実行されます。
- **SIM** 設定: このオプションは、110 LTE アプライアンスにのみ適用されます。110 LTE アプライアンスはデュアル SIM をサポートし、SIM 設定を設定できます。
- ネットワークモード: 内部 LTE モデムをサポートする Citrix SD-WAN アプライアンスでモバイルネットワークを選択できます。サポートされるネットワークは、3G、4G、またはその両方です。110 LTE アプライアンスの場合、変更を適用する SIM を選択します。

- ローミング: ローミングオプションは、LTE アプライアンスでデフォルトで有効になっています。無効にすることを選択できます。110 LTE アプライアンスの場合、変更を適用する SIM を選択します。

個々の LTE アプライアンスで LTE 機能を構成することもできます。詳細については、「210 SE LTE で LTE 機能を構成する」を参照してください。

110-LTE-WIFI アプライアンスの設定について詳しくは、110 LTE Wi-Fi での LTE 機能の構成を参照してください。

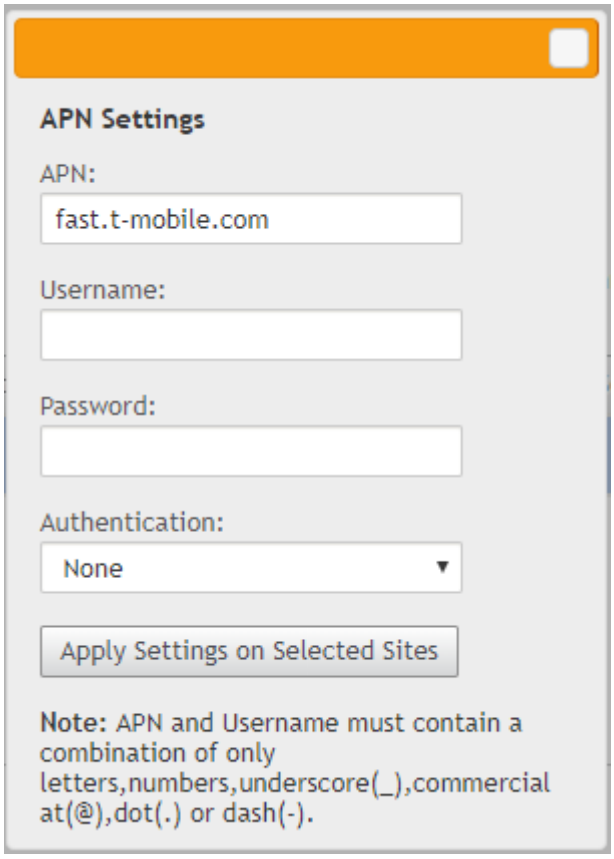
APN 設定

APN は、キャリアのセルラーネットワークと公衆インターネット間のゲートウェイへの接続をセットアップするためにアプライアンスが読み取る設定の名前です。キャリアから APN 情報を取得し、1 つ以上の LTE アプライアンスで **APN** 設定をリモートで構成できます。

> 注
>
> APN 設定は、キャリアごとに異なります。

APN 設定を構成するには:

1. SD-WAN Center UI で、構成 **>** モバイルブロードバンドに移動します。APN 設定を構成する LTE サイトを選択し、[**APN**] をクリックします。



2. 110 LTE アプライアンスの場合、APN 設定が適用される SIM を選択します。
3. 携帯通信会社から提供された **APN** 名、ユーザー名、パスワード、認証を 入力します。PAP、CHAP、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。
4. [選択したサイトに設定を適用] をクリックします。

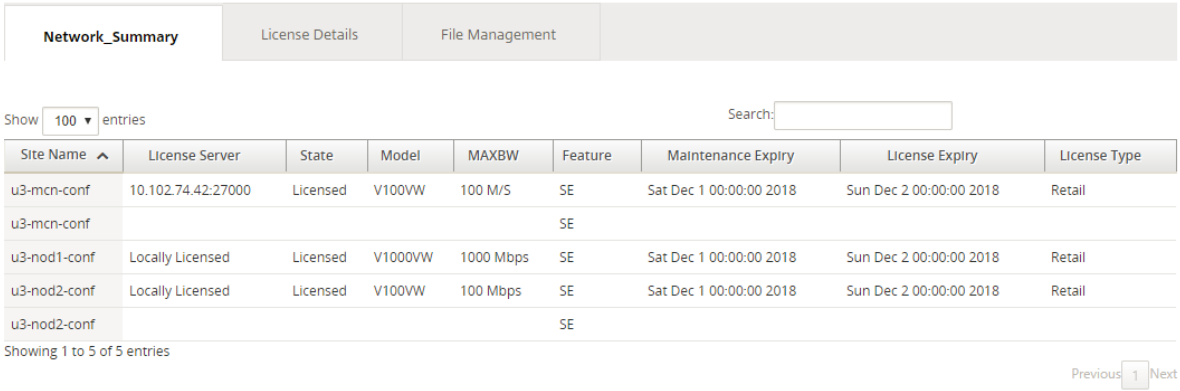
ライセンスサーバーとしての **Citrix SD-WAN Center**

April 13, 2021

ネットワーク内のアプライアンスのライセンスを取得し、アップロードして SD-WAN Center にインストールできます。SD-WAN Center をリモートライセンスサーバーとして使用するには、SD-WAN Center の IP アドレスをリモートサーバーとして構成し、ライセンスを集中管理します。詳しくは、「一元化されたライセンス管理」を参照してください。

変更管理プロセスを通じてネットワーク構成をサイトにプッシュした後、構成がアクティブ化されると、ブランチアプライアンスは SD-WAN Center からライセンスを自動的に取得します。
これらのライセンスを使用するには、ライセンスを SD-WAN Center 自体のホストに割り当てる必要があります。

SD-WAN Center によって検出されたすべてのアプライアンスのライセンスの詳細を表示するには、構成 > ライセンス > ネットワークの概要に移動します。



次のパラメータが表示されます。

- サイト名: サイトの名前。
- ライセンスサーバー: ライセンスサーバーの IP アドレスとポート番号。ライセンスがアプライアンスにローカルにインストールされている場合、「ローカルライセンス」と表示されます。
- 状態: アプライアンスの現在のライセンス状態、ライセンス済みまたはライセンスなし。
- モデル: ライセンスがサポートするアプライアンスモデル。

- **MAXBW**: ライセンスで許可されている最大帯域幅。
- 特徴: ライセンスがサポートする Citrix SD-WAN エディション。
- メンテナンスの有効期限: Citrix Subscription Advantage の有効期限。

  > 注
  >
  > ソフトウェアのアップグレード中に、ソフトウェアのビルド日がメンテナンスの有効期限よりも後の場合、ソフトウェアのアップグレードは許可されません。

- ライセンスの有効期限: ライセンスの有効期限。
- ライセンスの種類: ライセンスのタイプ。

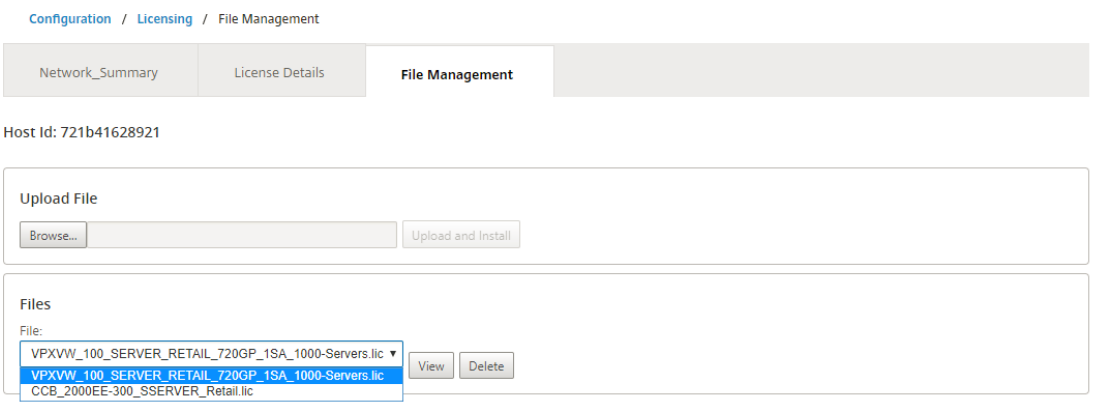
SD-WAN Center にライセンスファイルをアップロードしてインストールするには:

1. Citrix SD-WAN アプライアンスのライセンスを取得し、ローカルコンピューターに保存します。

   > 注
   >
   > Citrix SD-WAN ソフトウェアライセンスの取得手順については、Citrix SD-WAN カスタマーサポートにお問い合わせください。

2. SD-WAN Center GUI で、[ライセンス]> ファイル管理に移動します。
3. [ファイル のアップロード] セクションで、[参照] をクリックします。ローカルコンピュータからライセンスファイルを選択し、[アップロードしてインストール] をクリックします。

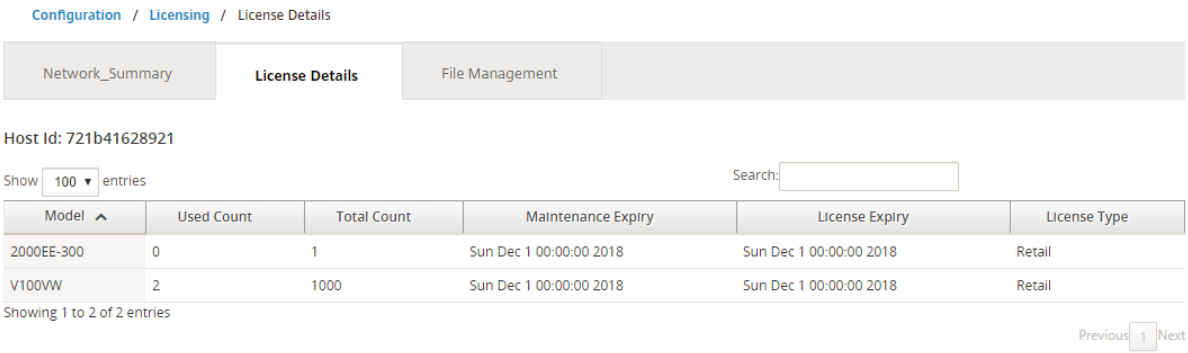
   インストールされているライセンスファイルが [ファイル] ドロップダウンメニューに一覧表示され、ライセンスファイルの表示または削除を選択できます。



> 注
>
> ホスト ID は、ライセンスファイルの生成に使用される SD-WAN Center のホスト ID です。別のホスト ID を

> 使用して生成されたライセンスファイルをアップロードして、Citrix SD-WAN Center にインストールすることはできません。

構成 > ライセンス > ライセンスの詳細 に移動すると、Citrix SD-WAN Center にアップロードおよびインストールされたすべてのライセンスファイルの詳細を一目で確認できます。



次のパラメータが表示されます。

- モデル：ライセンスがサポートするアプライアンスモデル。
- 使用数：このライセンスがインストールされているアプライアンスの数。
- 総数：このライセンスをインストールできるアプライアンスの総数。
- メンテナンスの有効期限: Citrix Subscription Advantage の有効期限。
- ライセンスの有効期限: ライセンスの有効期限。
- ライセンスの種類：ライセンスのタイプ。

Citrix SD-WAN Center から Azure に Citrix SD-WAN をデプロイする

April 13, 2021

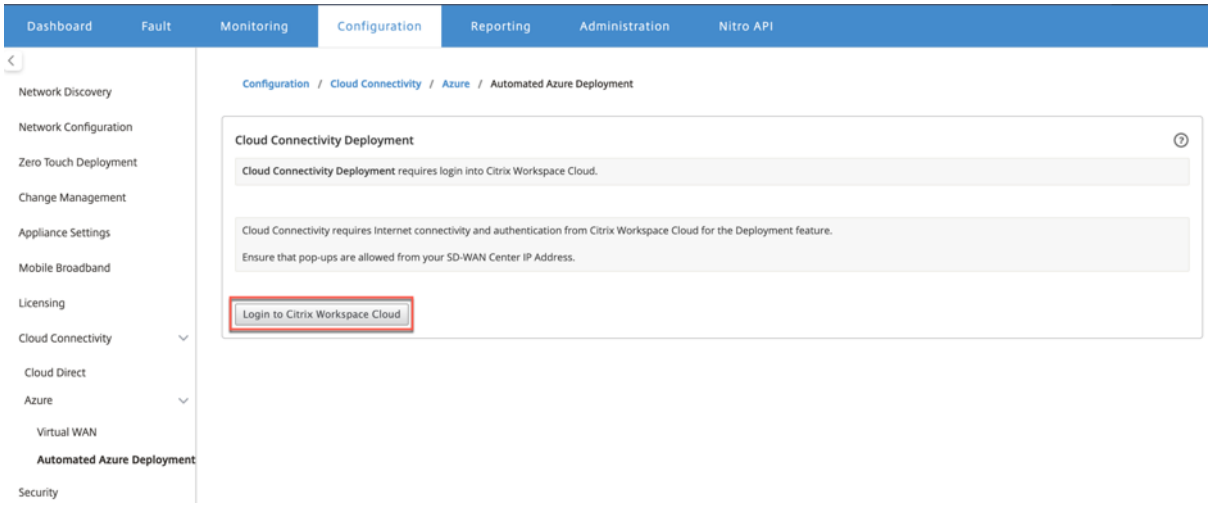
Citrix SD-WAN for Azure を使用すると、組織は各ブランチから Azure でホストされているアプリケーションに直接安全に接続でき、クラウドにバインドされたトラフィックをデータセンター経由でバックホールする必要がなくなります。

前提条件

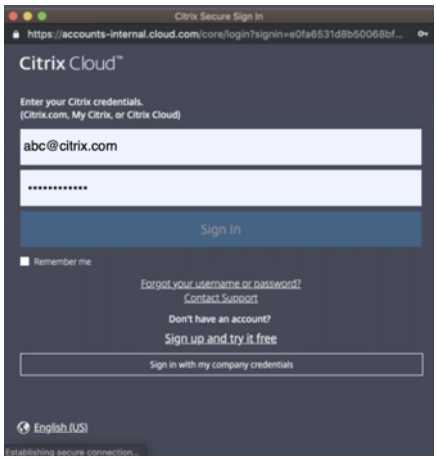
- Citrix Workspace Cloud 資格情報。
- Azure サブスクリプションの資格情報
- ロールベースのアクセス制御を備えた Azure アプリケーションとサービスプリンシパル。方法：ポータルを使用して、リソースにアクセスできる Azure AD アプリケーションとサービスプリンシパルを作成するを参照してください。

- サービスプリンシパルが作成されたら、次の詳細を書き留めます。
  - Azure サブスクライバー ID
  - テナント ID
  - アプリケーション ID
  - 秘密キー
- 変更管理を MCN/SD-WAN ctx-sdw-sw-xxxxxxx.zip を使用してセンタリングします。
- Citrix SD-WAN Center から MCN を検出し、アクティブな構成をプルします。

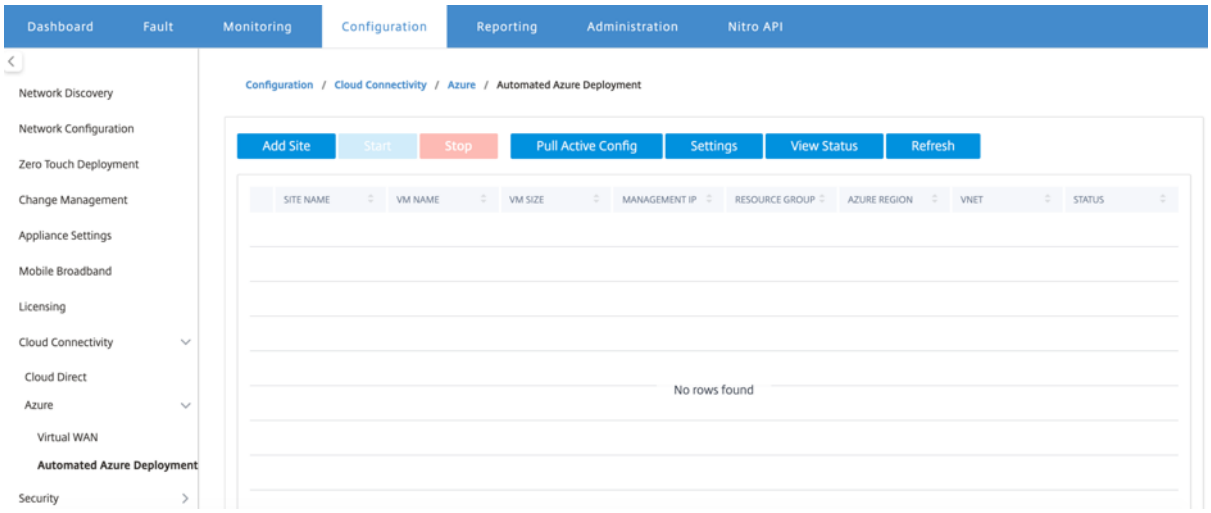
SD-WAN Center から Azure に Citrix SD-WAN をデプロイするには、構成 **>** クラウド接続 **> Azure> Azure** の自動展開に移動します。



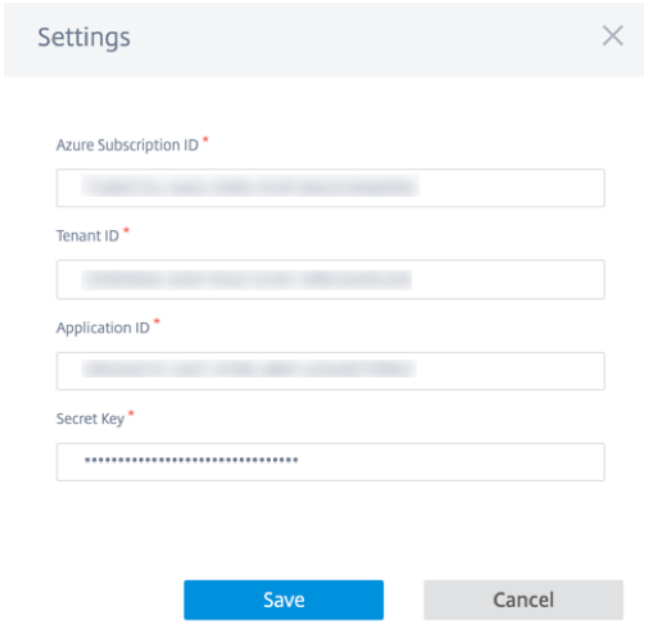
Citrix Cloud 資格情報でログインします。



Azure の自動展開



[設定] オプションをクリックして、Azure サブスクリプションの詳細を入力します。MCN からアクティブな実行構成を取得するには、[アクティブ構成のプル] オプションをクリックします。



Azure に Citrix SD-WAN をデプロイする

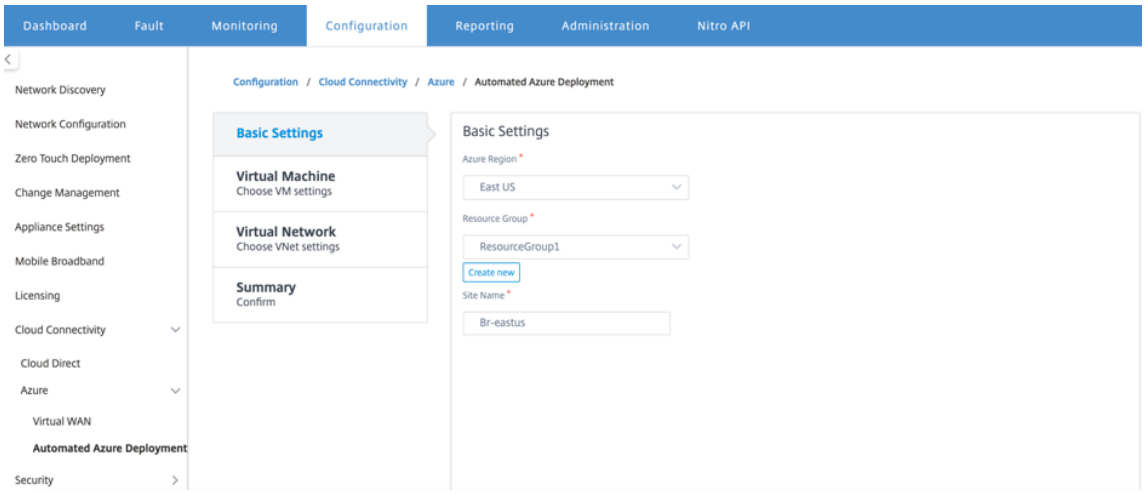
Microsoft Azure に Citrix SD-WAN をデプロイするには:

1. [サイトの追加] を クリックして、新しい SD-WAN インスタンスを追加します。現在のサブスクリプションで Azure 上の SD-WAN 仮想マシンの作成を開始します。

   この展開の一部として、次のことも行います。

- 新しく追加されたサイトの SD-WAN 構成を MCN の現在アクティブな構成に自動的に追加します。
- 変更管理を実行します。
- MCN のソフトウェアバージョンと構成をこの新しいサイトに適用します。

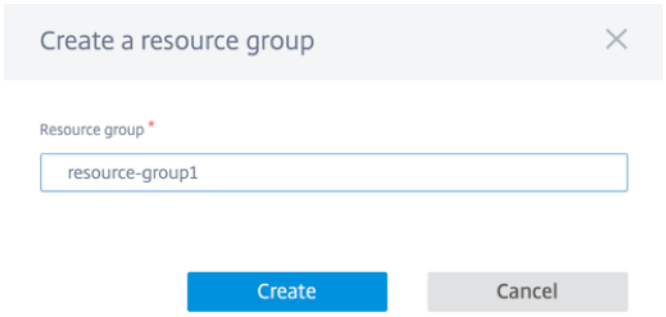
基本設定、仮想マシン、および 仮想ネットワーク 設定を完了します。



[基本設定] で、ドロップダウンリストからリージョンとリソースグループを選択します。リージョンを選択すると、リソースグループのドロップダウンリストに、このサブスクリプションのこのリージョンにあるすべての既存のリソースグループが表示されます。

> 注:
>
> サイトを追加するには、リソースグループが空である必要があります。

既存の空のリソースグループを選択するか、[新規作成] オプションをクリックして新しいリソースグループを作成できます。

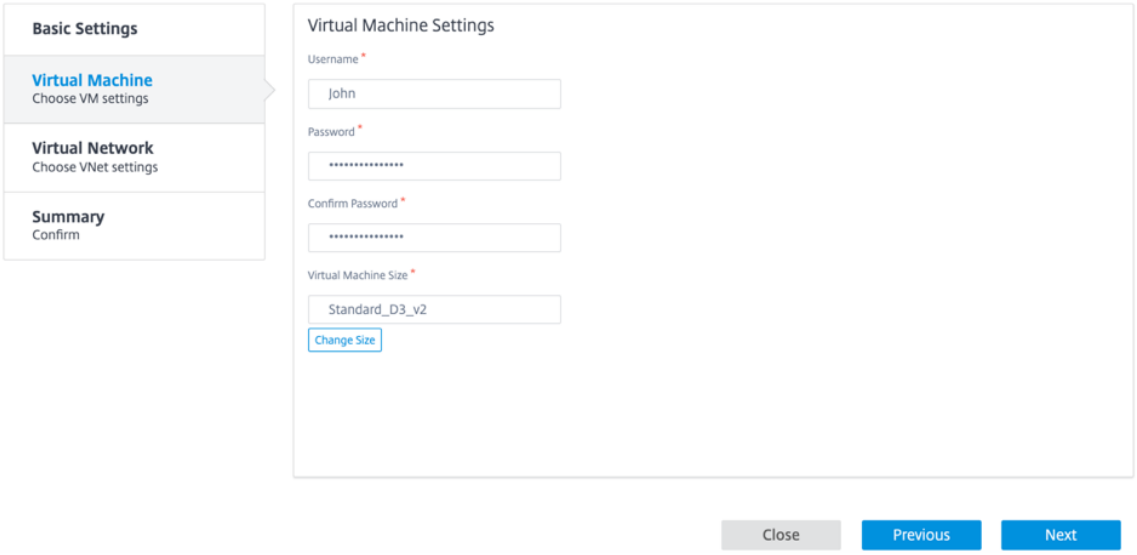


2. サイト名は地域名で自動生成されます。サイト名は必要に応じて編集できます。

> 注:
>
> サイト名が SD-WAN サイト名の要件を維持し、SD-WAN ネットワーク内で一意であることを確認してください。

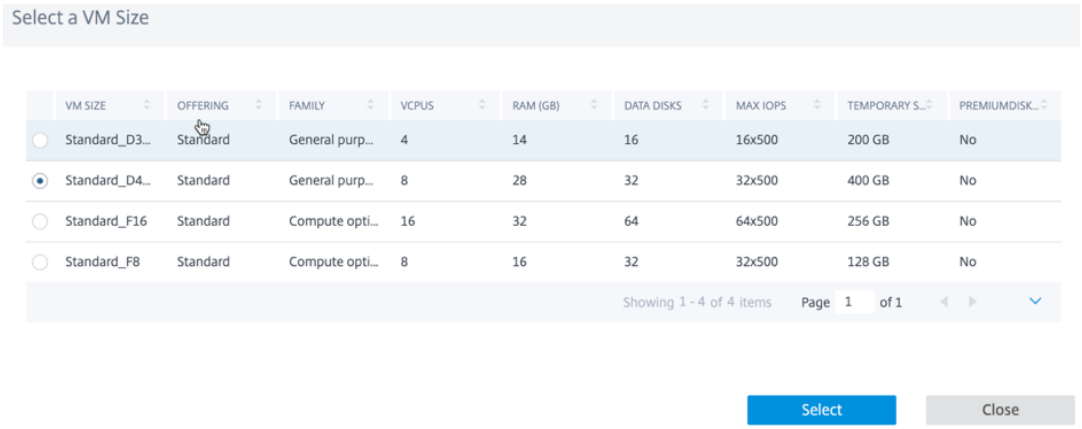
> Azure VM 名は、**AZ-regionname-sitename** 形式のサイト名から生成されます。

3. [次へ] をクリックして、仮想マシンを構成します。

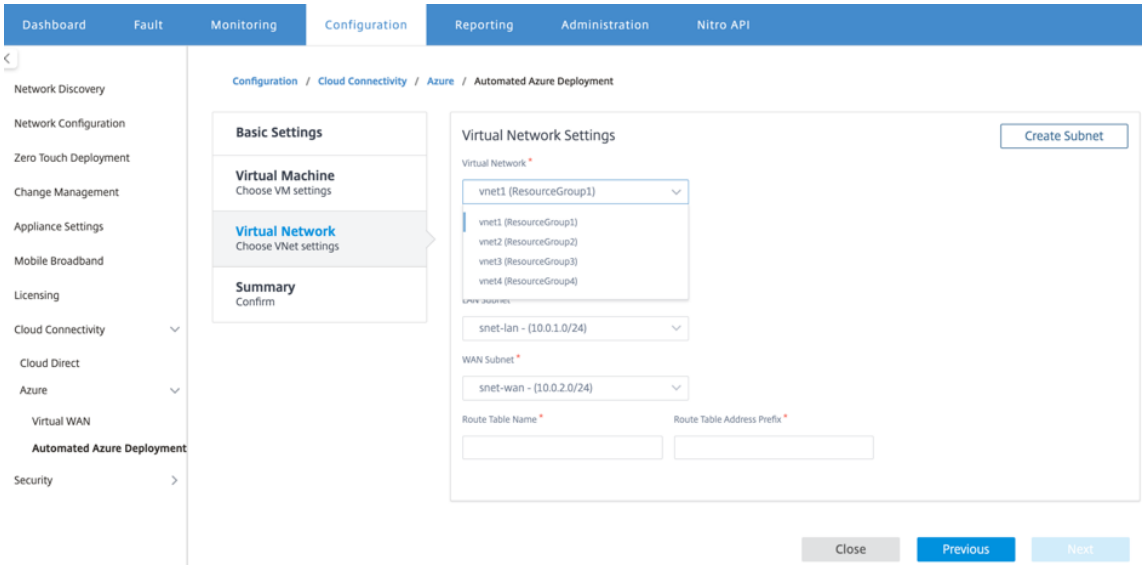


ユーザー名、パスワード、パスワードの確認を入力します。デフォルトでは、VM サイズは標準サイズで自動入力されます。必要に応じて、[サイズの変更] を クリックして別の VM サイズを選択します。

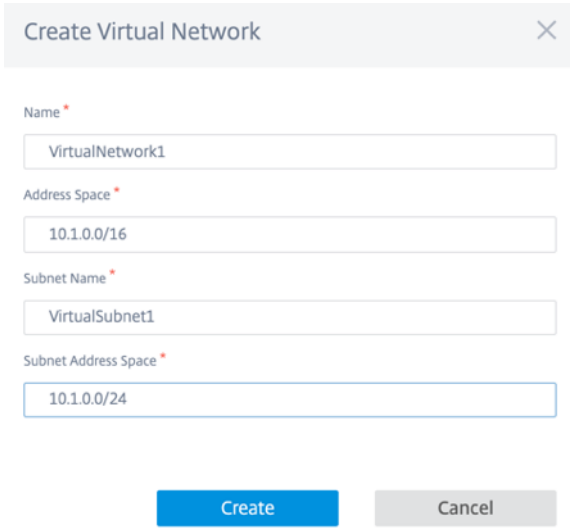
> 注:
>
> 展開中に提供されるこのユーザー資格情報には、Azure SD-WAN への読み取り専用アクセス権があります。管理者権限については、管理者資格情報を使用してください。



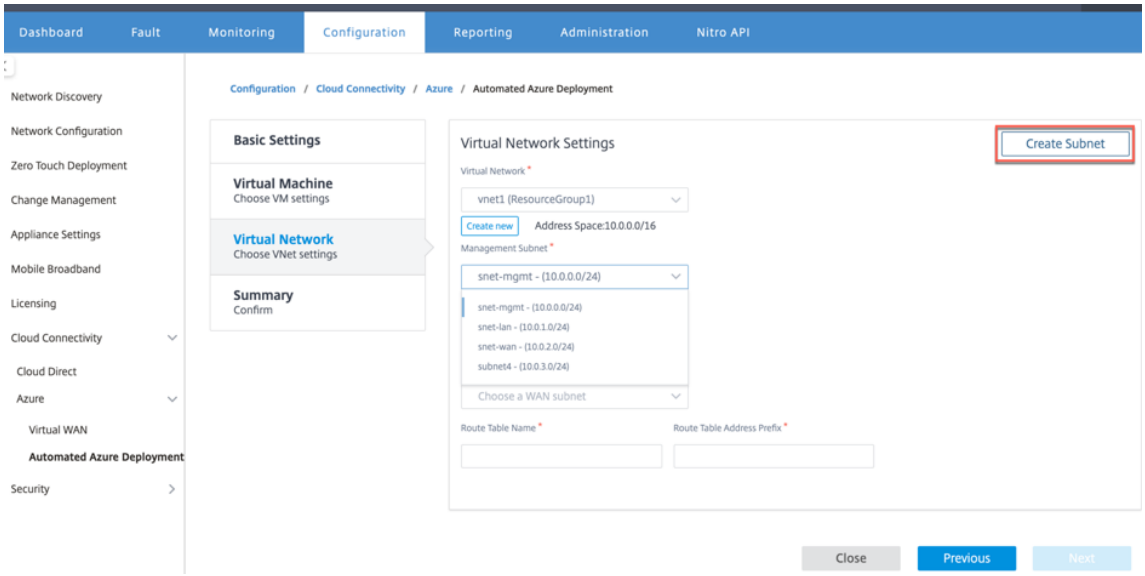
4. [次へ] をクリックして、仮想ネットワーク設定を実行します。
5. ドロップダウンリストから仮想ネットワークを選択します。リストには、選択した Azure リージョンのすべての仮想ネットワークが含まれています。



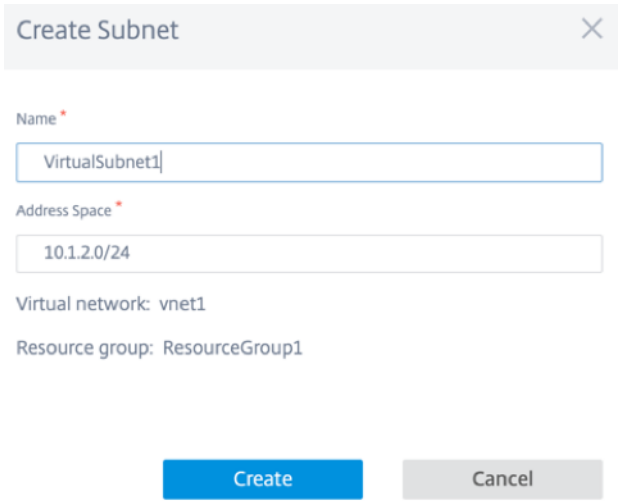
サイトを既存の仮想ネットワークに展開するか、新しい仮想ネットワークを作成できます。[新規作成] を クリックして、新しい仮想ネットワークを作成します。仮想ネットワーク名、アドレススペース（カスタムプライベート IP アドレススペースを指定）、サブネット名、およびサブネットアドレススペースを指定します。



6. 管理するサブネットを選択します。



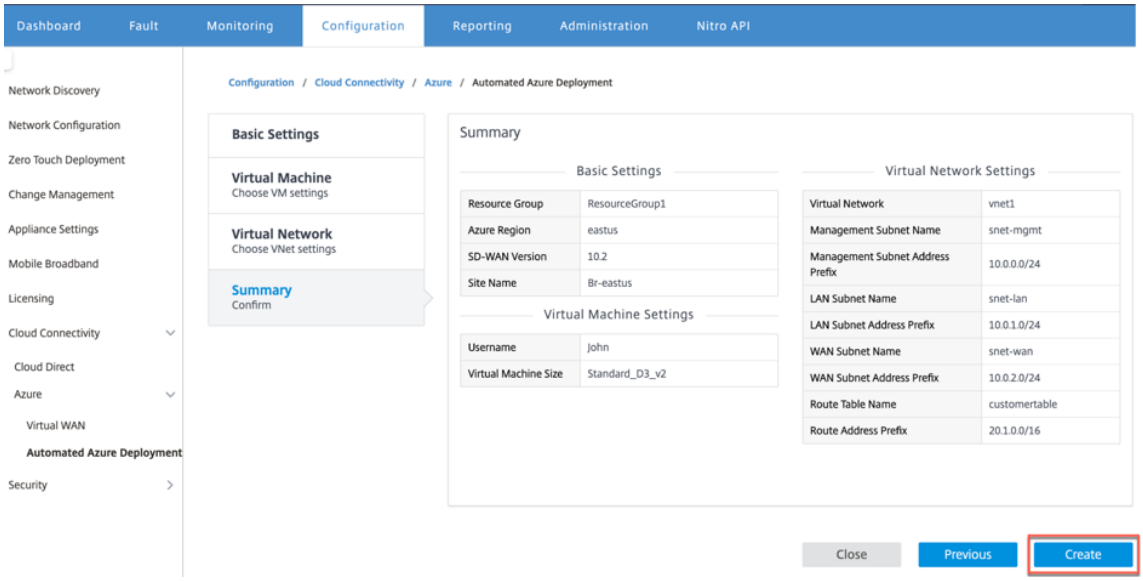
7. （右上隅から）[サブネット の作成] オプションを使用してサブネットを作成することもできます。



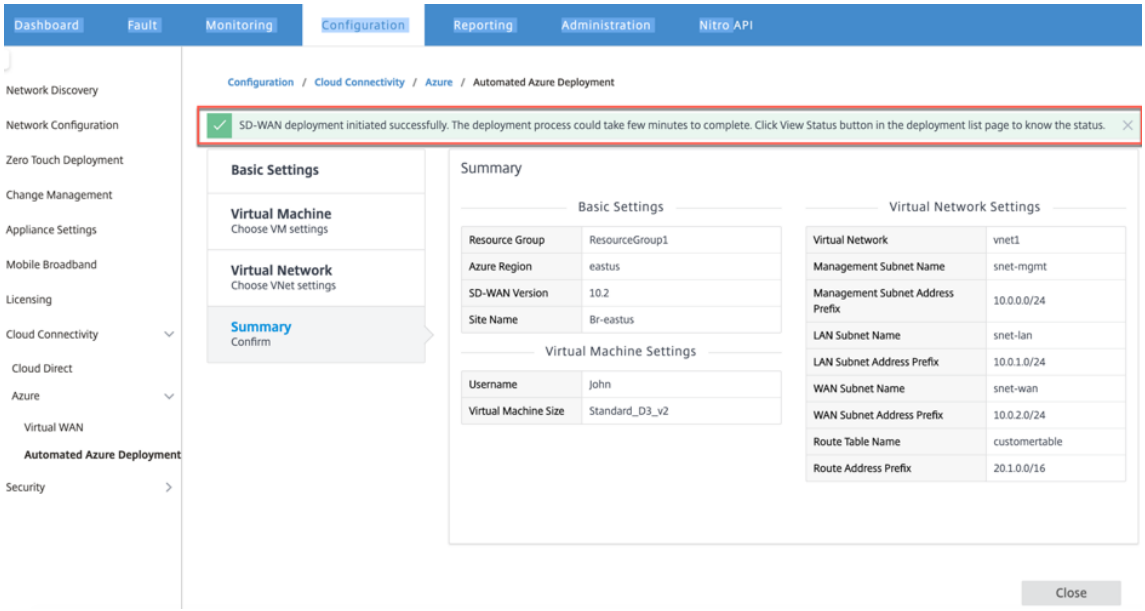
8. ドロップダウンリストから、LAN と WAN に異なるサブネットを選択し、ルーティングテーブル名 と ルーティングテーブルアドレスプレフィックスを入力します。ルーティングテーブルアドレスプレフィックス は、この SD-WAN アプライアンスにリダイレクトされる宛先アドレススペースです。他のターゲットアドレスは Azure ルーティングによってリダイレクトされます。

> 注:
>
> ルーティングテーブルは LAN サブネットに関連付けられています。選択した LAN サブネットにすでに関連付けられたルートテーブルがある場合、そのルートテーブルが表示され、変更できません。それ以外の場合は、ルーティングテーブル名を指定できます。

9. [次 へ] をクリックして設定の詳細を確認し、[作成] をクリックします。



デプロイメントが正常に開始されたことを示すステータスメッセージが上部に表示されます。



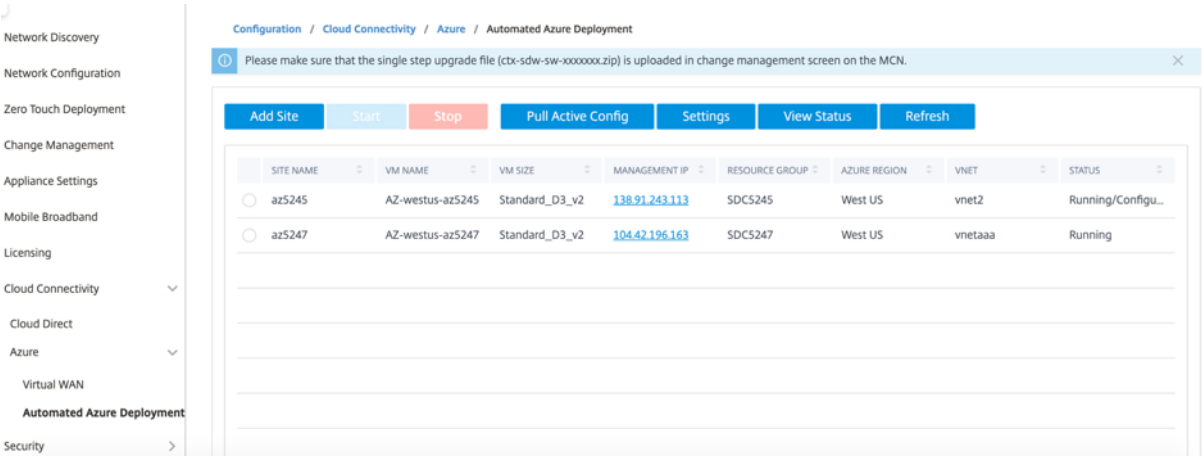
展開の完了には時間がかかる場合があるため、[ステータスの表示] をクリックして、展開ステータスに関する最新の更新を取得することをお勧めします。

展開の一部として:

- 選択した Azure リージョンに仮想マシンが作成されます。
- サイトは、SD-WAN のアクティブな SD-WAN 構成に自動的に追加されます。
- 変更管理は、新しくプロビジョニングされた Azure VM で実行されます。

デプロイが成功すると、MCN と Azure サイトの間に仮想パスが形成されます。デプロイメントでエラーが発生した場合、プロセスはロールバックされ、自動作成されたすべてのリソースが元に戻ります。

デフォルトでは、サイトはデフォルトのルーティングドメインの一部として配置されます。デフォルトの自動パスグループを使用して、デフォルトのリージョンに属しています。



- サイト名: Citrix SD-WAN サイトの名前。このサイト名は、Citrix SD-WAN 構成で使用されます。
- **VM** 名: Azure でプロビジョニングされる仮想マシン（VM）の名前。
- **VM** サイズ: サイトの作成中に選択された VM サイズ。
- 管理 **IP**: 新しく作成された SD-WAN VM に割り当てられた管理 IP アドレス。
- リソースグループ: リソースグループは論理的な構造であり、リソースグループ間のデータ交換は常に可能です。Azure 仮想マシンはこのリソースグループに属しています。Citrix SD-WAN の展開中に作成された新しいリソースは、このリソースグループの下にグループ化されます。デプロイメント中にエラーが発生した場合、このリソースグループで作成されたリソースは削除されます。
- **Azure** リージョン: リソースグループとそのリソースの場所を表します。
- **VNet**: サイトで使用されている仮想ネットワーク。
- 状態: VM のステータスを提供します。

最新のサイトステータスを取得するには、[更新] ボタンをクリックします。選択したサイトの VM はいつでも 開始 または 停止 できます。一度に選択できるサイトは 1 つだけです。

展開が完了したら、MCN または Citrix SD-WAN Center にログインして、仮想パスのステータスを表示します。

ゼロタッチ展開

April 13, 2021

> 注
>
> ゼロタッチ展開サービスは、一部の Citrix SD-WAN アプライアンスでのみサポートされています。
>
> - SD-WAN 110 Standard Edition
> - SD-WAN 210 Standard Edition
> - SD-WAN 410 Standard Edition
> - SD-WAN 2100 Standard Edition
> - SD-WAN 1000 Standard Edition（再イメージ化が必要）
> - SD-WAN 1000 Enterprise Edition（Premium Edition）（再イメージが必要です）
> - SD-WAN 1100 Standard Edition
> - SD-WAN 1100 Premium (Enterprise) Edition
> - SD-WAN 2000 Standard Edition（再イメージ化が必要）
> - SD-WAN 2000 Enterprise Edition（Premium Edition（再イメージが必要です）
> - SD-WAN AWS VPX インスタンス

ゼロタッチ展開（ZTD）サービスは、Citrix が運営および管理するクラウドサービスであり、Citrix SD-WAN ネットワークで新しいアプライアンスを検出し、ブランチオフィスの展開プロセスを自動化します。ZTD クラウドサービスは、インターネット経由で、Secure Socket Layer（SSL）プロトコルを介してネットワーク内の任意のノードからアクセスできます。

ZTD クラウドサービスは、ゼロタッチ対応デバイス（SD-WAN 410-SE、2100-SE など）を購入した顧客の ID を格納するバックエンド Citrix ネットワークサービスと安全に通信します。ゼロタッチ展開リクエストを認証するためのバックエンドサービスが用意されており、カスタマーアカウントと Citrix SD-WAN アプライアンスのシリアル番号との関連付けが適切に検証されます。

ZTD の高レベルのアーキテクチャとワークフロー

データセンターサイト

Citrix SD-WAN 管理者–SD-WAN 環境の管理者権限を持つユーザー。主な役割は次のとおりです。

- Citrix SD-WAN Center ネットワーク構成ツールを使用した構成の作成、またはマスターコントロールノード（MCN）SD-WAN アプライアンスからの構成のインポート
- 新しいサイトノードの展開のためにゼロタッチ展開サービスを開始する Citrix Cloud ログイン。

> 注
>
> SD-WAN Center がプロキシサーバ経由でインターネットに接続されている場合は、SD-WAN Center でプロキシサーバの設定を構成する必要があります。詳しくは、「ゼロタッチ展開のプロキシサーバー設定」を参照してください。

ネットワーク管理者–エンタープライズネットワーク管理（DHCP、DNS、インターネット、ファイアウォールなど）を担当するユーザー

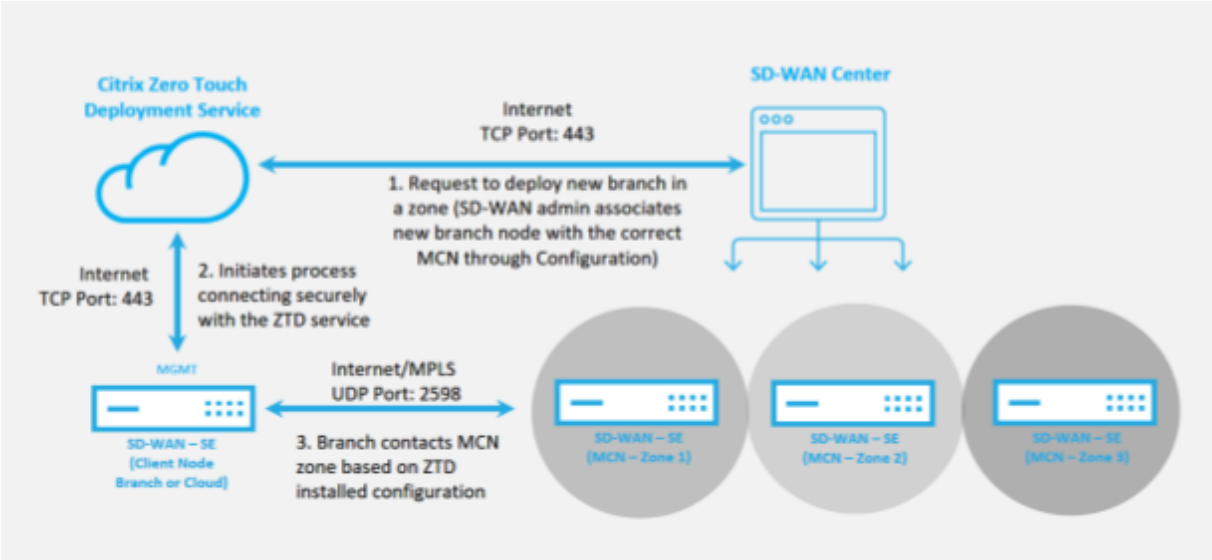
- 必要に応じて、***SD-WAN Center*** から ***FQDN sdwanzt.citrixnetworkapi.net*** へのアウトバウンド通信用のファイアウォールを構成します。

リモートサイト

オンサイトインストーラー–次の主な責任を持つオンサイト活動のためのローカルの連絡先または雇われたインストーラー:

- Citrix SD-WAN アプライアンスを物理的に開梱します。
- ZTD 対応でないアプライアンスのイメージを再作成します。
  - 必須: SD-WAN 1000-SE、2000-SE、1000-EE、2000-EE
  - 必要ありません for: SD-WAN 410-SE、2100-SE
- アプライアンスの電源ケーブル。
- 管理インターフェイス（MGMT、0/1 など）でインターネットに接続するためにアプライアンスをケーブルで接続します。
- データインターフェース（例: apA.WAN、apB.WAN、apC.WAN、0/2, 0/3, 0/5, 等）。

> 注
>
> インターフェイスのレイアウトはモデルごとに異なります。データと管理ポートの識別については、ドキュメントを参照してください。

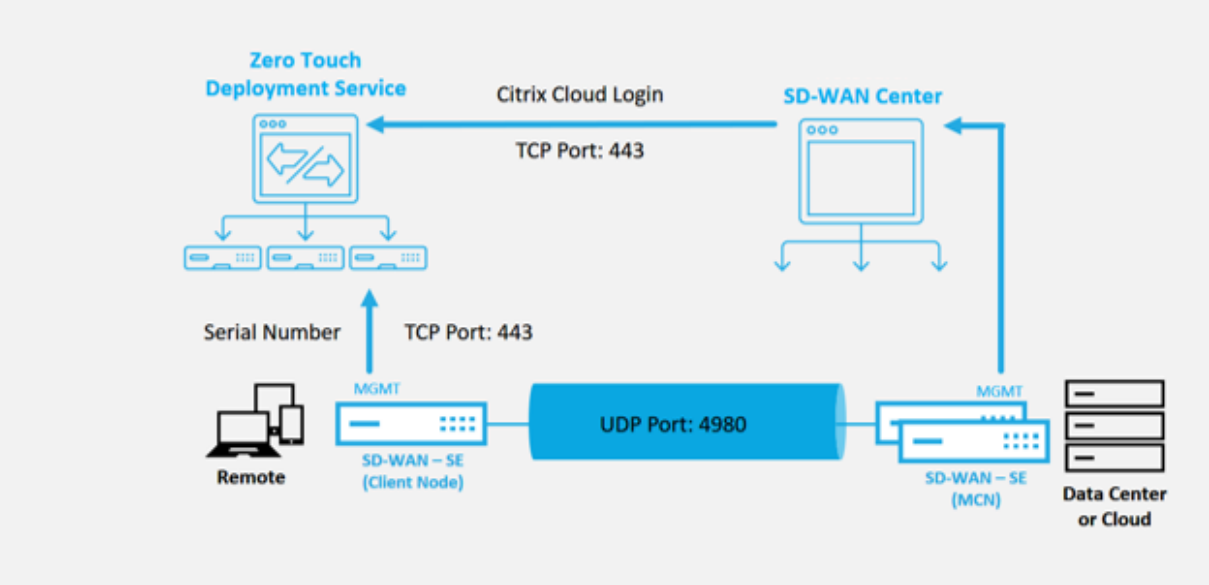


ゼロタッチ展開サービスを開始する前に、次の前提条件が必要です。

- マスターコントロールノード（MCN）に昇格したアクティブに実行されている SD-WAN。
- 仮想パスを介して MCN に接続し、SD-WAN Center をアクティブに実行します。

- https://onboarding.cloud.comで Citrix Cloud ログイン認証情報が作成されました（アカウント作成については、以下の手順を参照してください）。
- 管理ネットワーク接続（SD-WAN Center および SD-WAN アプライアンス）をポート 443 でインターネットに直接接続するか、プロキシサーバー経由で接続します。
- ZTD の初期設定用の SD-WAN Center Web ポータルにアクセスするためのポート 443 でのインターネット接続。
- （オプション）MCN への有効な仮想パス接続を使用してクライアントモードでブランチオフィスで動作するアクティブに実行されている少なくとも 1 つの SD-WAN アプライアンス。

最後の前提条件は必須ではありませんが、SD-WAN 管理者は、ゼロタッチ展開が新しく追加されたサイトで完了したときに、アンダーレイネットワークが仮想パスの確立を許可することを検証できます。主に、これにより、適切なファイアウォールおよびルートポリシーが適切に NAT トラフィックに配置されていること、または UDP ポート 4980 がネットワークを貫通して MCN に到達できることを確認します。



ゼロタッチ展開サービスの概要

Zero Touch Deployment Service は、SD-WAN Center と連携して機能し、ブランチオフィスの SD-WAN アプライアンスを簡単に導入できます。SD-WAN Center は、SD-WAN Standard および Enterprise（Premium）Edition アプライアンスの中央管理ツールとして構成および使用されます。ゼロタッチ展開サービス（または ZTD クラウドサービス）を利用するには、管理者は最初の SD-WAN デバイスを環境に展開し、次に SD-WAN Center を管理の中心点として構成および展開する必要があります。SD-WAN Center のリリース 9.1 以降がポート 443 でパブリックインターネットに接続してインストールされると、SD-WAN Center は自動的にクラウドサービスを開始し、必要なコンポーネントをインストールしてゼロタッチ展開機能のロックを解除し、ゼロタッチを作成します。SD-WAN Center の GUI で利用可能な展開オプション。SD-WAN Center ソフトウェアでは、ゼロタッチ展開はデフォルトでは使用できません。これは、管理者がゼロタッチ展開を含むオンサイトアクティビティを開始する前に、

アンダーレイネットワーク上の適切な予備コンポーネントが存在することを確認するために意図的に設計されています。

SD-WAN 環境が稼働し始めたら、Citrix Cloud アカウントのログインを作成することにより、ゼロタッチ展開サービスへの登録が完了します。SD-WAN Center が ZTD サービスと通信できるため、GUI の [構成] タブにゼロタッチ展開オプションが表示されます。ゼロタッチサービスにログインすると、特定の SD-WAN 環境に関連付けられたお客様 ID が認証され、SD-WAN Center が登録されます。さらに、ZTD アプライアンスの展開をさらに認証するためにアカウントのロックが解除されます。

SD-WAN Center のネットワーク構成ツールを使用して、SD-WAN 管理者はテンプレートまたはクローンサイト機能を利用して、SD-WAN 構成を構築し、新しいサイトを追加する必要があります。SD-WAN Center は、新しい構成を使用して、新しく追加されたサイトの ZTD の展開を開始します。SD-WAN 管理者は、ZTD プロセスを使用して展開用のサイトを開始するときに、シリアル番号を事前に入力し、オンサイトインストーラーへの電子メール通信を開始することにより、ZTD に使用するアプライアンスを事前認証するオプションがありますオンサイト活動を開始します。

オンサイトインストーラーは、サイトがゼロタッチ展開の準備ができているという電子メール通信を受信し、DHCP IP アドレスの割り当てと MGMT ポートでのインターネットアクセスのためにアプライアンスの電源を入れてケーブル接続するインストール手順を開始できます。また、LAN および WAN ポートのケーブル接続。その他はすべて ZTD サービスによって開始され、進捗状況はアクティベーション URL を使用して監視されます。インストールするリモートノードがクラウドインスタンスである場合、アクティベーション URL を開くと、ワークフローが開始され、指定されたクラウド環境にインスタンスが自動的にインストールされます。ローカルインストーラーによるアクションは必要ありません。

Zero Touch Deployment Cloud Service は以下アクションを自動化します:

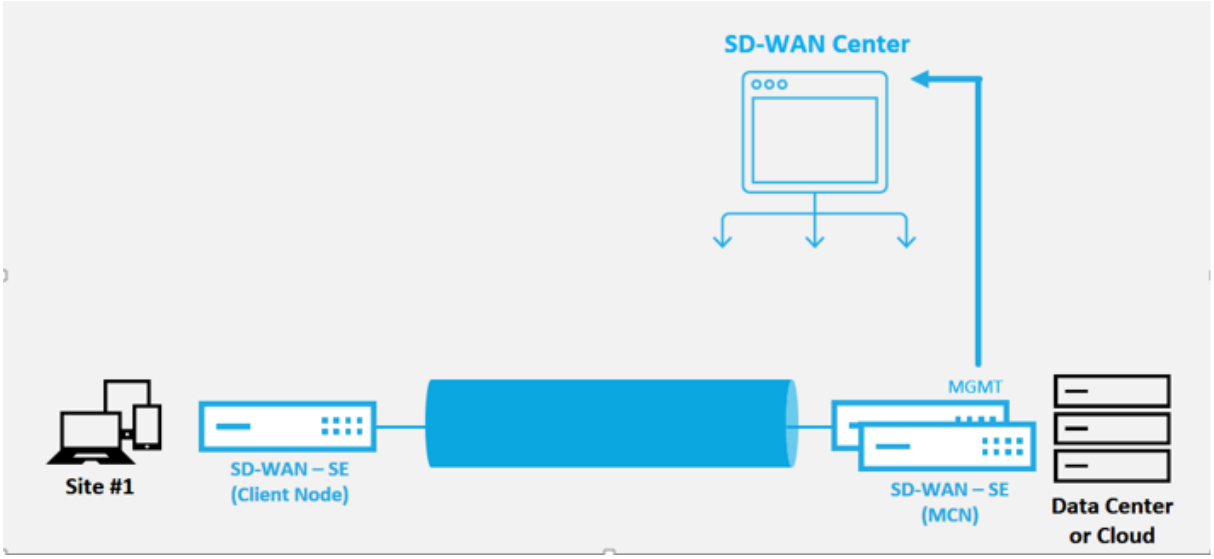
ブランチアプライアンスで新しい機能を利用できる場合は、ZTD エージェントをダウンロードして更新します。

- シリアル番号を検証して、ブランチアプライアンスを認証します。
- SD-WAN 管理者が SD-WAN Center を使用して ZTD のサイトを受け入れたことを認証します。
- SD-WAN Center から、ターゲットアプライアンスに固有の設定ファイルをプルします。
- 対象のアプライアンスに固有の構成ファイルをブランチアプライアンスにプッシュします。
- ブランチアプライアンスに構成ファイルをインストールします。
- 不足している SD-WAN ソフトウェアコンポーネントまたは必要な更新をブランチアプライアンスにプッシュします。
- 仮想パスの確立を確認するための一時的な 10 Mbps ライセンスファイルをブランチアプライアンスにプッシュします。
- ブランチアプライアンスで SD-WAN サービスを有効にします。

SD-WAN 管理者がアプライアンスに永久ライセンスファイルをインストールするには、さらに多くの手順が必要です。

ゼロタッチ展開サービスの手順

次の手順では、ゼロタッチ展開サービスを使用して新しいサイトを展開するために必要な手順を詳しく説明します。実行中の MCN と 1 つのクライアントノードが既に SD-WAN Center への適切な通信を行っていること、および確立された仮想パスがアンダーレイネットワーク全体の接続を確認していること。SD-WAN 管理者がゼロタッチの展開を開始するには、次の手順が必要です。



ゼロタッチ展開サービスを構成する方法

SD-WAN Center には、新しく接続されたアプライアンスから SD-WAN エンタープライズネットワークに参加するための要求を受け付ける機能があります。要求は、ゼロタッチ展開サービスを介して Web インターフェイスに転送されます。アプライアンスがサービスに接続すると、構成とソフトウェアのアップグレードパッケージがダウンロードされます。

構成ワークフロー:

- [**SD-WAN Center**] > [新しいサイト構成の作成] または既存の構成をインポートして保存します。
- Citrix Workspace Cloud にログインして ZTD サービスを有効にします。ゼロタッチ展開メニューオプションが SD-WAN Center の Web 管理インターフェースに表示されるようになりました。
- SD-WAN Center で、設定 > ゼロタッチ展開 > 新しいサイトを展開しますに移動します。
- アプライアンスを選択し、[有効にする] をクリックして、[展開] をクリックします。
- インストーラーはアクティベーションメールを受け取ります > シリアル番号を入力してください > 活性化 > アプライアンスは正常に展開されました。

ゼロタッチ展開サービスを構成するには:

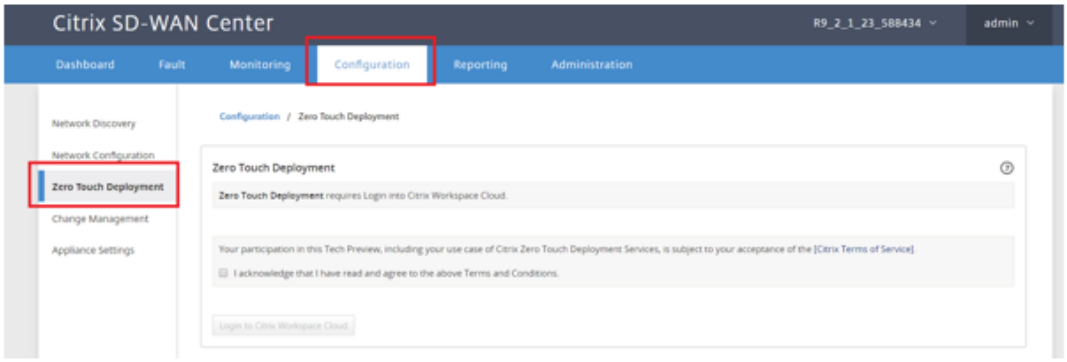
1. ゼロタッチ展開機能を有効にして SD-WAN Center をインストールします。

    a) DHCP が割り当てた IP アドレスを使用して SD-WAN Center をインストールします。

b) SD-WAN Center に適切な管理 IP アドレスとネットワーク DNS アドレスが割り当てられ、管理ネットワークを介してパブリックインターネットに接続できることを確認します。

c) SD-WAN Center を最新の SD-WAN ソフトウェアリリースバージョンにアップグレードします。

d) 適切なインターネット接続により、SD-WAN Center はゼロタッチ展開（ZTD）クラウドサービスを開始し、このコールホーム手順が失敗した場合、ZTD に固有のファームウェアアップデートを自動的にダウンロードしてインストールします。次のゼロタッチ展開オプションは、GUI。



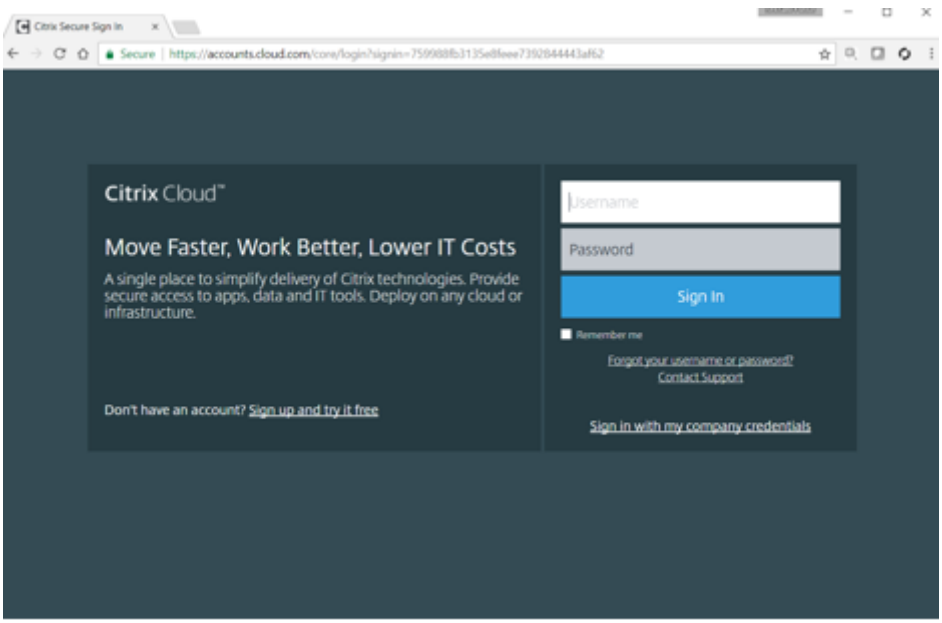
e) 利用規約を読み、「上記の利用規約を読んで同意したことを認めます」を選択します。

f) Citrix Cloud アカウントがすでに作成されている場合は、「**Citrix Workspace Cloud** にログイン」ボタンをクリックします。

g) Citrix Cloud アカウントにログインし、ログイン成功の次のメッセージを受け取っ たら、このウィンドウを閉じないでください。プロセスには別のウィンドウが必要です ~20 SD-WAN Center GUI を更新するための秒数。完了すると、ウィンドウは自動的に閉じます。**

h) クラウドログインアカウントを作成するには、次の手順に従います。

- Web ブラウザーを開いて、https://onboarding.cloud.comに移動します。
- 「お待ちください、**Citrix.com** アカウントを持っています。」のリンクをクリックします。



i) 既存の Citrix アカウントでサインインします。

j) SD-WAN Center のゼロタッチ展開ページにログインすると、次の理由により、ZTD の展開に使用できるサイトがないことがわかります。

- アクティブな構成が [構成] ドロップダウンメニューから選択されていません
- 現在アクティブな構成のすべてのサイトが既に展開されています
- 構成は SD-WAN Center を使用して構築されたものではなく、MCN で利用可能な構成エディタを使用して構築されたものでした。
- ゼロタッチ対応のアプライアンス（410-SE、2100-SE、Cloud VPX など）を参照する構成でサイ

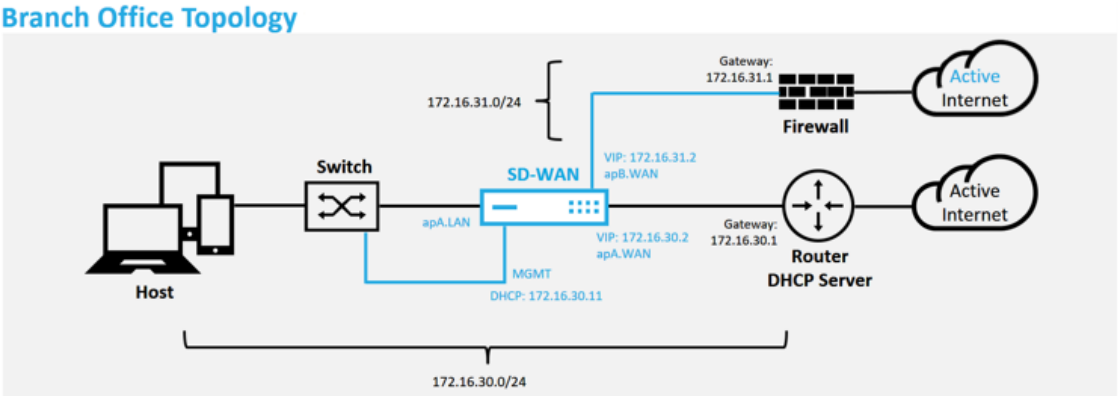
トが構築されていない

2. SD-WAN Center ネットワーク構成を使用して、**ZTD** 対応 **SD-WAN** アプライアンスを 持つ 新しいリモートサイトを追加するように構成を更新します。

   SD-WAN 設定が SD-WAN Center ネットワーク設定を使用して構築されていない場合は、MCN からアクティブな設定をインポートし、SD-WAN Center を使用して設定の変更を開始します。ゼロタッチ展開機能の場合、SD-WAN 管理者は SD-WAN Center を使用して構成を構築する必要があります。ゼロタッチ展開を対象とする新しいサイトを追加するには、次の手順を使用する必要があります。

   新しいサイトの詳細（つまり、アプライアンスモデル、インターフェイスグループの使用、仮想 IP アドレス、帯域幅を備えた WAN リンク、およびそれぞれの Gateway）を最初に概説することにより、SD-WAN アプライアンス展開用の新しいサイトを設計します。

   > 重要
   >
   > モデルとして VPX が選択されているサイトノードも一覧表示されますが、現在、ZTD サポートは AWS VPX インスタンスでのみ使用できます。
   >
   > 注
   >
   > - Citrix SD-WAN Center のサポート Web ブラウザを使用していることを確認します
   > - Citrix Workspace ログイン中に Web ブラウザがポップアップウィンドウをブロックしていないことを確認してください

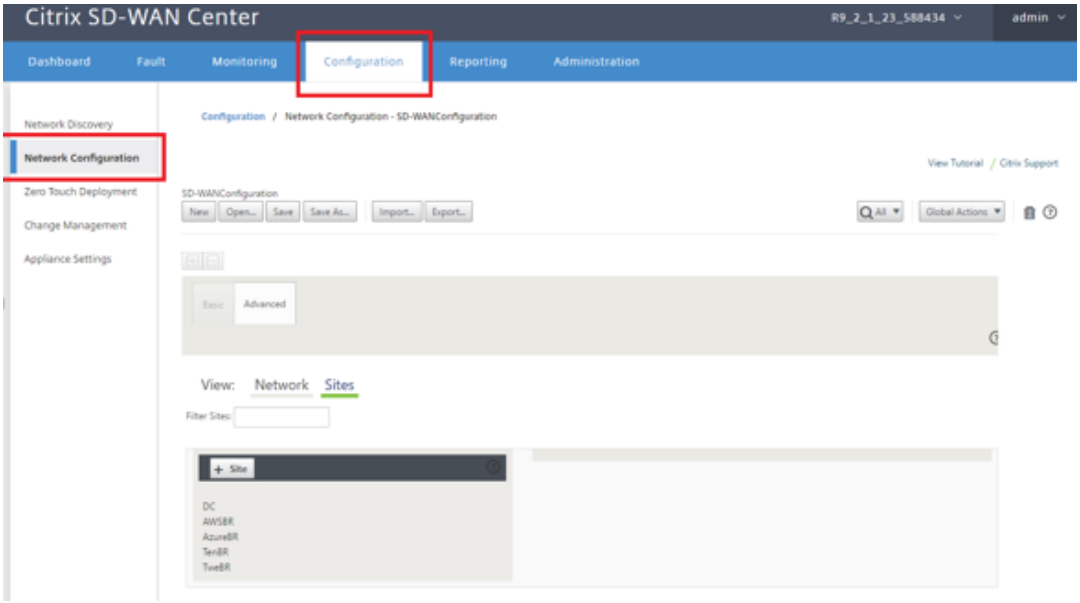
   

   これは、ブランチオフィスサイトの配置例です。SD-WAN アプライアンスは、既存の MPLS WAN リンクのパスに物理的に配置されます。172.16.30.0/24 ネットワーク、および既存のバックアップリンクを使用してアクティブ状態にし、その 2 番目の WAN リンクを別のサブネット 172.16.31.0/24 上の SD-WAN アプライアンスに直接終端する。

   > 注
   >
   > SD-WAN アプライアンスは、デフォルトの IP アドレス 192.168.100.1/16 を自動的に割り当てます。DHCP がデフォルトで有効になっていると、ネットワーク内の DHCP サーバーが、デフォルトと重複するサブネット内の 2 番目の IP アドレスをアプライアンスに提供する場合があります。これにより、アプ

> ライアンスでルーティングの問題が発生し、アプライアンスが ZTD クラウドサービスへの接続に失敗する可能性があります。DHCP サーバーを構成して、192.168.0.0/16 の範囲外の IP アドレスを割り当てます。
>
> ネットワーク内の SD-WAN 製品の配置には、さまざまな展開モードを使用できます。上記の例では、SD-WAN が既存のネットワークインフラストラクチャの上にオーバーレイとして展開されています。新しいサイトの場合、SD-WAN 管理者は、SD-WAN を Edge モードまたは Gateway モードで展開することを選択できます。これにより、WAN エッジルーターとファイアウォールの必要がなくなり、エッジルーティングとファイアウォールのネットワークニーズが SD-WAN ソリューションに統合されます。。

a) **SD-WAN Center** の **Web** 管理インターフェイスを開き、構成 > ネットワーク設定 ページに移動します。

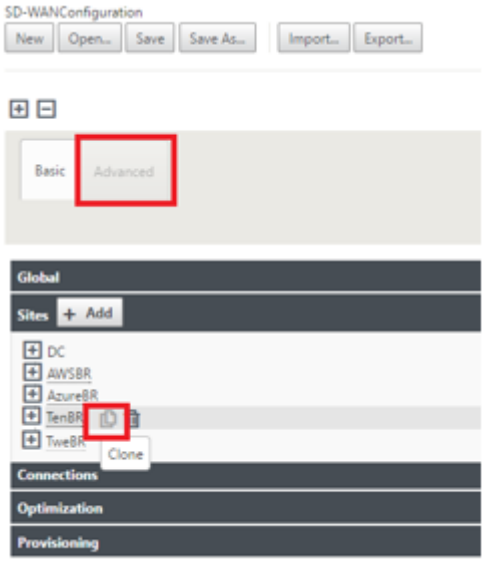


b) 動作中の構成がすでに配置されていることを確認するか、MCN から構成をインポートします。

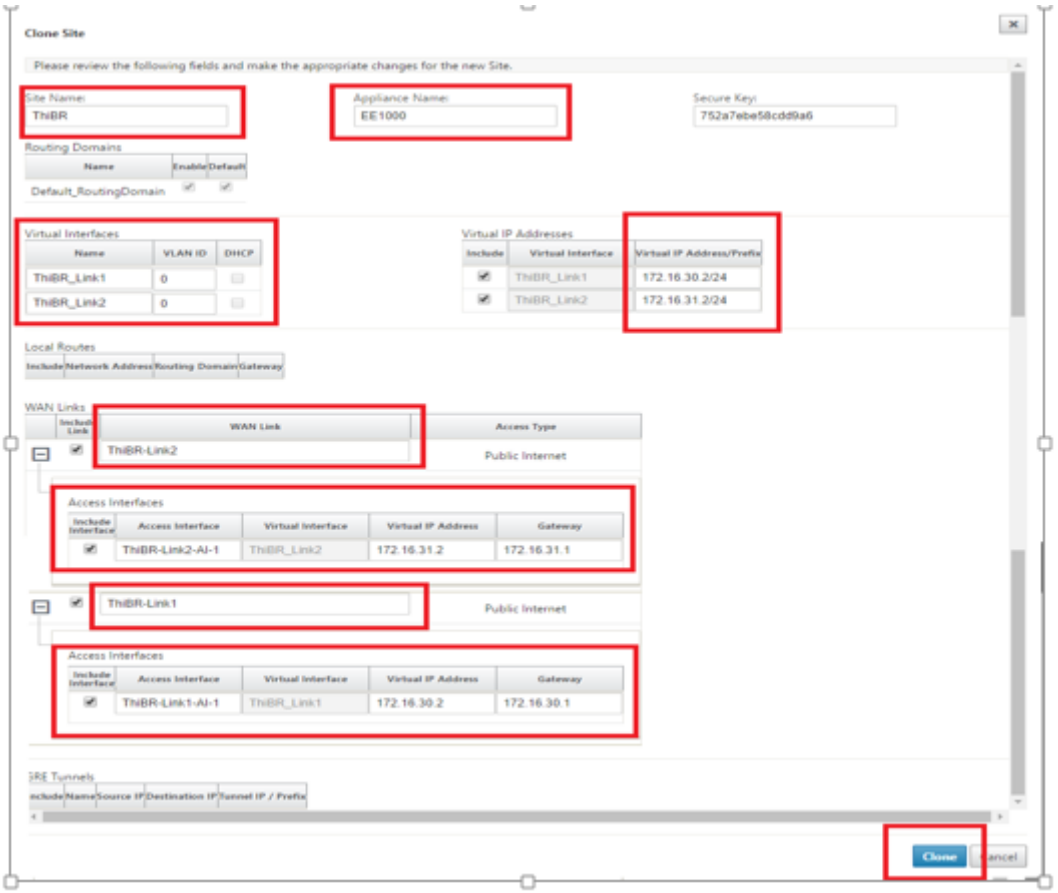
c) [詳細] タブに移動して、サイトを作成します。

d) [サイト] タイルを開いて、現在構成されているサイトを表示します。

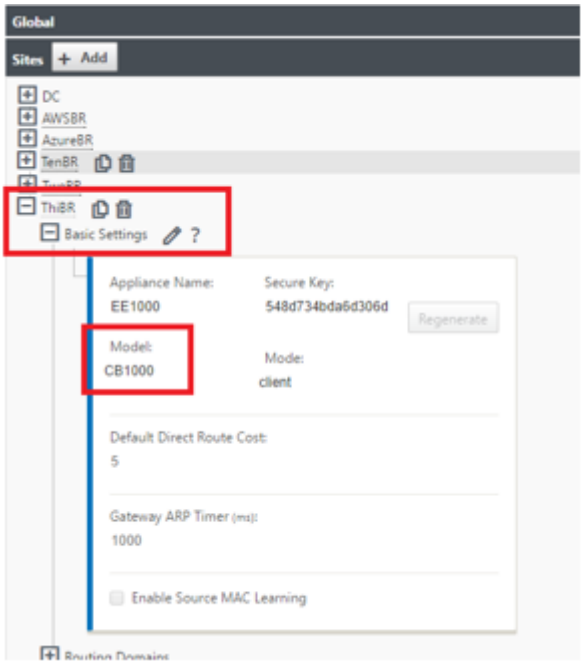
e) 既存のサイトのクローン機能を利用して、新しいサイトの構成をすばやく構築しました。



f) この新しいブランチサイト用に設計されたトポロジからすべての必須フィールドを入力します。



g) 新しいサイトのクローンを作成した後、サイトの **[基本設定]** に移動し、ゼロタッチサービスをサポートする SD-WAN のモデルが正しく選択されていることを確認します。



h) サイトの SD-WAN モデルは更新できますが、更新されたアプライアンスには、クローン作成に使用されたものと同じ新しいインターフェイスレイアウトがあるため、インターフェイスグループを再定義する必要がある場合があることに注意してください。

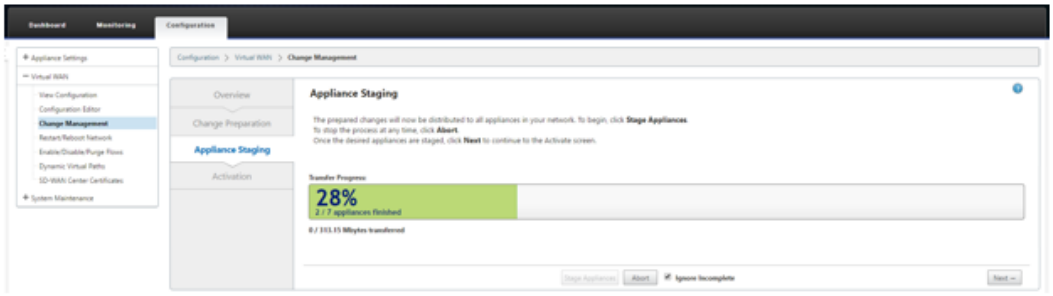
i) SD-WAN Center に新しい構成を保存し、「変更管理の受信トレイ」オプションへのエクスポートを使用して、変更管理を使用して構成をプッシュします。

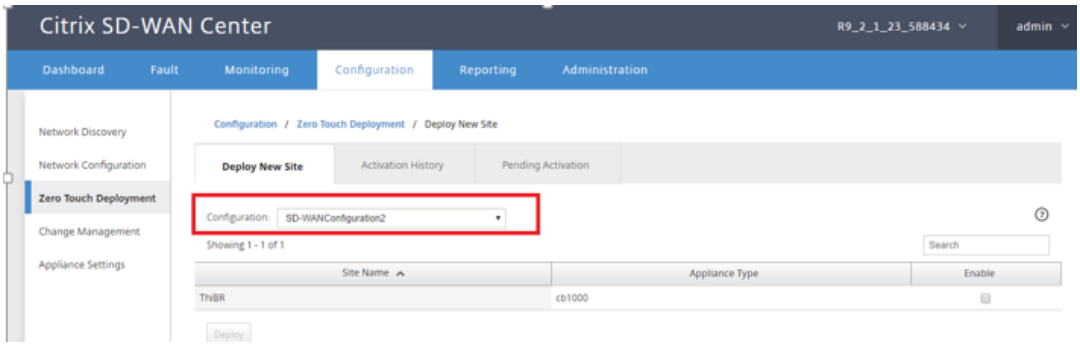
j) 変更管理手順に従って、新しい構成を適切にステージングします。これにより、既存の SD-WAN デバイスは、ゼロタッチで展開される新しいサイトを認識します。構成をプッシュしようとする試みをスキップするには、「不完全を無視」オプションを使用する必要があります。ZTD ワークフローを通過する必要がある新しいサイト。

3. SD-WAN Center のゼロタッチ展開ページに戻り、新しいアクティブな構成が実行されている状態で、新しいサイトを展開できます。

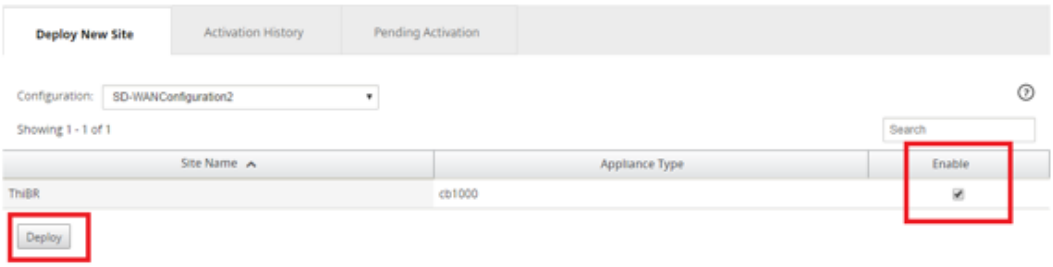
a) [ゼロタッチ展開] ページの [新しいサイト の展開] タブで、実行中のネットワーク構成ファイルを選択します

b) 実行構成ファイルを選択すると、ゼロタッチがサポートされている未展開の SD-WAN デバイスを含むすべてのブランチサイトのリストが表示されます

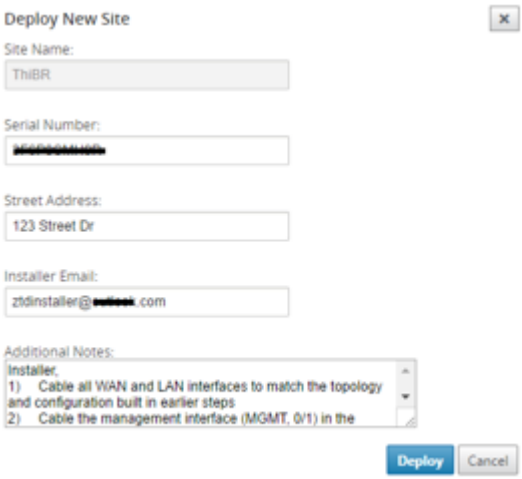




c) ゼロタッチサービス用に構成するブランチサイトを選択し、[有効にする]、[展開] の順にクリックします。



d) Deploy New Site ポップアップウィンドウが表示されます。管理者は、必要に応じて、シリアル番号、ブランチサイトのストリートアドレス、インストーラの電子メールアドレス、その他のメモを提供できます。

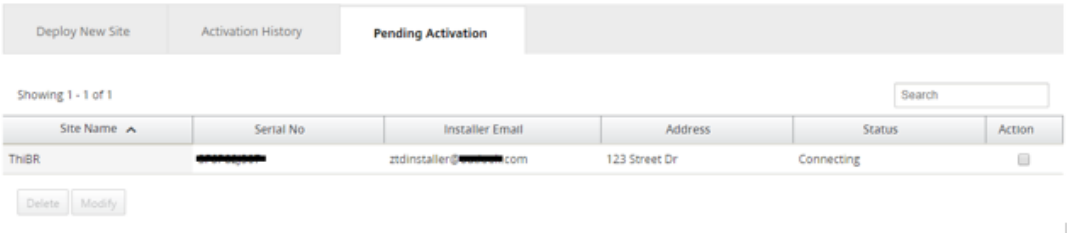


> 注
>
> シリアル番号入力フィールドはオプションであり、入力されているかどうかに応じて、インストーラーが担当するオンサイトのアクティビティが変更されます。
>
> - シリアル番号フィールドが入力されている場合–インストーラーは、サイトのデプロイコマンドで生成されたアクティベーション URL にシリアル番号を入力する必要はありません
> - シリアル番号フィールドが黒のままの場合–インストーラーは、アプライアンスの正しいシリアル番号を、サイト展開コマンドで生成されたアクティベーション URL に入力する必要があります。

a) [展開] ボタンをクリックすると、「サイト構成が展開されました」というメッセージが表示されます。

b) このアクションにより、以前に ZTD クラウドサービスに登録された SD-WAN Center がトリガーされ、この特定のサイトの構成を共有して、一時的に ZTD クラウドサービスに保存されます。

c) [保留中のアクティブ化] タブに移動して、ブランチサイト情報が正常に入力され、インストーラーアクティビティが保留中の状態になったことを確認します。

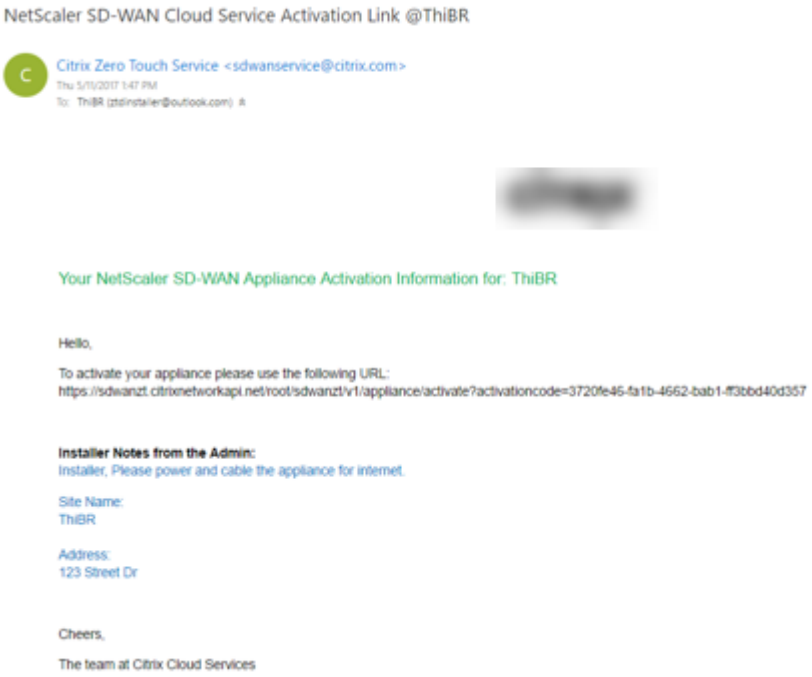


> 注
>
> 情報が正しくない場合、「アクティブ化保留中」状態のゼロタッチ展開を選択して削除または変更できます。保留中のアクティブ化ページからサイトが削除されると、そのサイトは [新しいサイトのデプロイ] タブページでデプロイできるようになります。アクティベーションの保留からブランチサイトを削除することを選択すると、インストーラーに送信されたアクティベーションリンクは無効になります。
>
> シリアル番号フィールドが SD-WAN 管理者によって入力されなかった場合、ステータスフィールドは

> 「接続中」ではなく「インストーラーの待機中」を示します。

4. 次の一連のアクティビティは、オンサイトインストーラーによって実行されます。

   a) インストーラーは、SD-WAN 管理者がサイトの展開時に使用した電子メールアドレスのメールボックスを確認します。


NetScaler SD-WAN Cloud Service Activation Link @ThiBR

Citrix Zero Touch Service <sdwanservice@citrix.com>

Your NetScaler SD-WAN Appliance Activation Information for: ThiBR

Hello,

To activate your appliance please use the following URL:
https://sdwanzt.citrixnetworkapi.net/root/sdwanzt/v1/appliance/activate?activationcode=3720fe46-fa1b-4662-bab1-ff3bbd40d357

Installer Notes from the Admin:
Installer, Please power and cable the appliance for internet.

Site Name:
ThiBR

Address:
123 Street Dr

Cheers,

The team at Citrix Cloud Services

   b) インターネットブラウザーウィンドウでゼロタッチ展開アクティベーション URL を開きます。

   c) SD-WAN 管理者がデプロイサイトの手順でシリアル番号を事前に入力しなかった場合、インストーラーが物理アプライアンス上のシリアル番号を見つけ、アクティベーション URL に手動でシリアル番号を入力し、[アクティベート] ボタンをクリックします。

   d) 管理者がシリアル番号情報を事前に入力している場合、アクティベーション URL は次のステップに進んでいます。

e) 次のアクションを実行するには、設置者が現場にいる必要があります。

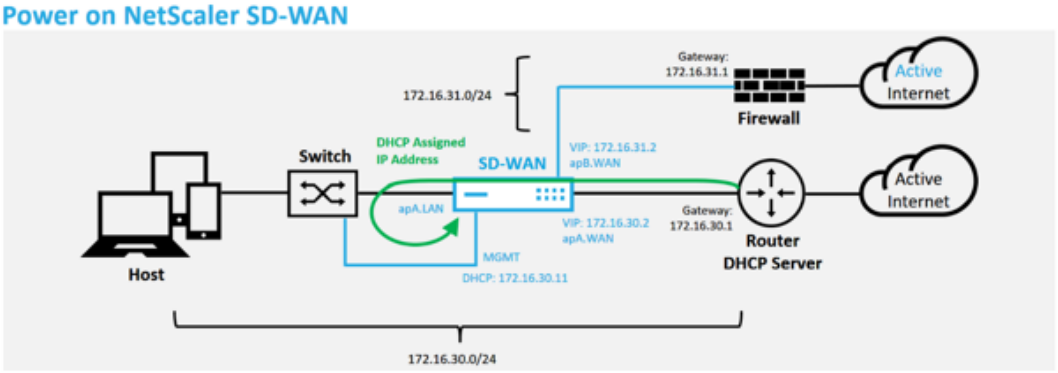
- 前の手順で構築したトポロジと構成に一致するように、すべての WAN および LAN インターフェイスをケーブルで接続します。
- 管理インターフェース（MGMT、0/1) DHCP IP アドレスと、DNS および FQDN から IP アドレスへの解決によりインターネットへの接続を提供するネットワークのセグメント内。
- SD-WAN アプライアンスの電源ケーブル。
- アプライアンスの電源スイッチをオンにします。

> 注
>
> ほとんどのアプライアンスは、電源ケーブルを接続すると自動的に電源が入ります。アプライアンスの前面にある電源スイッチを使用して電源をオンにする必要があるアプライアンスもあれば、アプライアンスの背面にある電源スイッチを搭載しているアプライアンスもあります。一部の電源スイッチでは、ユニットの電源が入るまで電源ボタンを押し続ける必要があります。

5. 次の一連のステップは、ゼロタッチ展開サービスの助けを借りて自動化されますが、次の前提条件が利用可能であることが必要です。

- ブランチアプライアンスの電源を入れる必要があります
- 管理と DNS IP アドレスを割り当てるには、既存のネットワークで DHCP を使用できる必要があります
- DHCP が割り当てた IP アドレスには、FQDN を解決する機能を備えたインターネットへの接続が必要です
- 他の前提条件が満たされている限り、IP 割り当てを手動で構成できます。

a) アプライアンスはネットワークの DHCP サーバーから IP アドレスを取得します。この例のトポロジでは、これは工場出荷時のデフォルト状態のアプライアンスのバイパスされたデータインターフェイスを介して行われます。

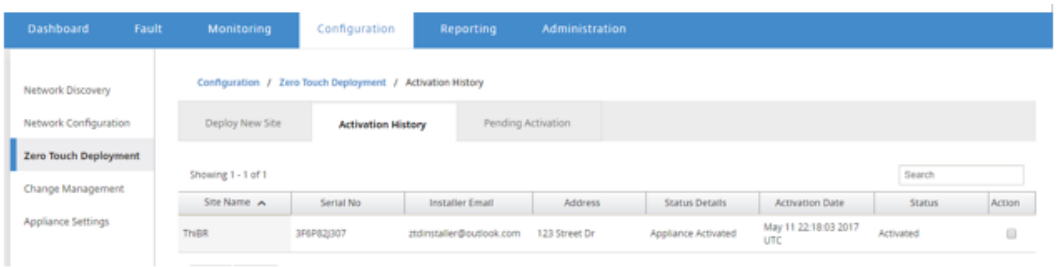


b) アプライアンスがアンダーレイネットワーク DHCP サーバーから Web 管理と DNS IP アドレスを取得すると、アプライアンスはゼロタッチ展開サービスを開始し、ZTD 関連のソフトウェア更新をダウンロードします。

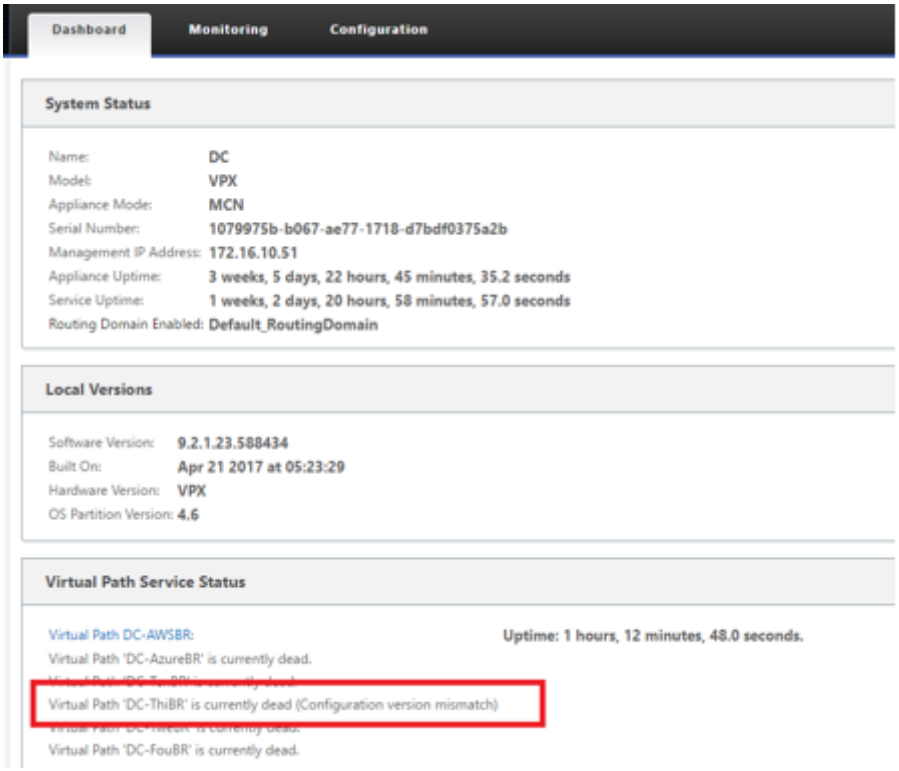
c) ZTD クラウドサービスへの接続が成功すると、展開プロセスは自動的に以下を実行します。

- SD-WAN Center によって以前に保存された構成ファイルをダウンロードします。
- ローカルアプライアンスへの構成の適用
- 10 MB の一時ライセンスファイルをダウンロードしてインストールする
- 必要に応じて、ソフトウェアの更新をダウンロードしてインストールします
- SD-WAN サービスをアクティブ化する

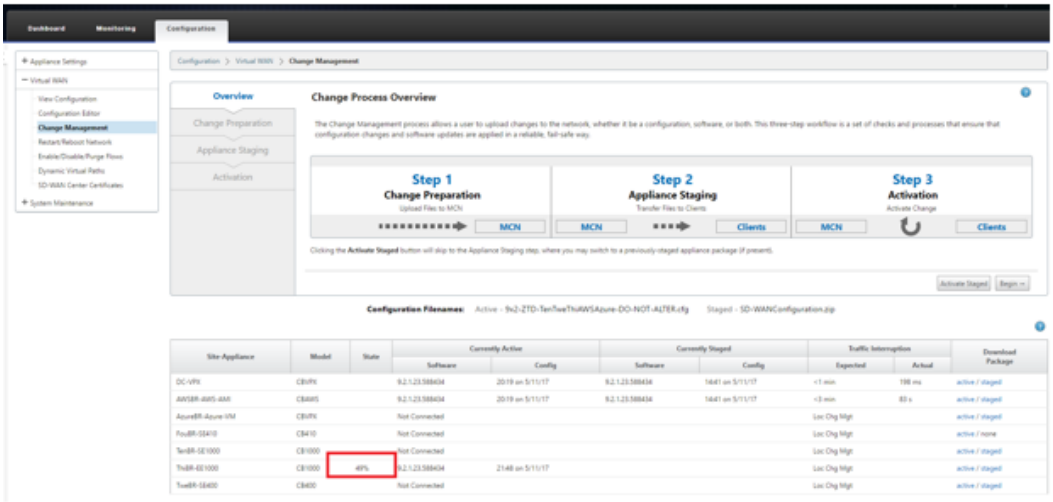
d) SD-WAN Center の Web 管理インターフェイスでさらに確認を行うことができます。ゼロタッチ展開メニューの [アクティベーション履歴] タブに、正常にアクティベートされたアプライアンスが表示されます。



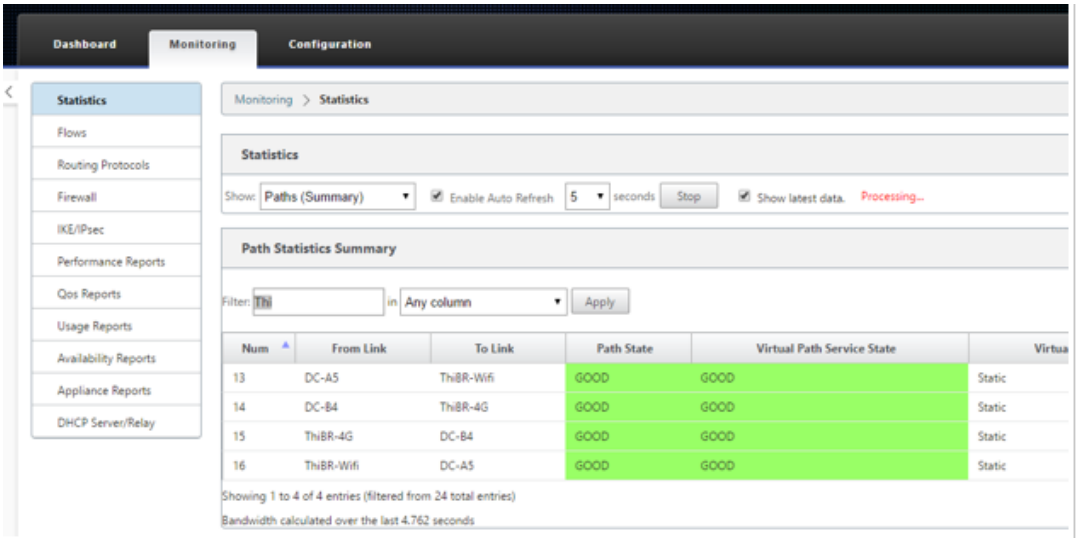
e) MCN は ZTD Cloud Service から渡された構成を信頼しておらず、MCN ダッシュボードに「構成バージョンの不一致」を報告するため、仮想パスは接続状態ですぐに表示されない場合があります。



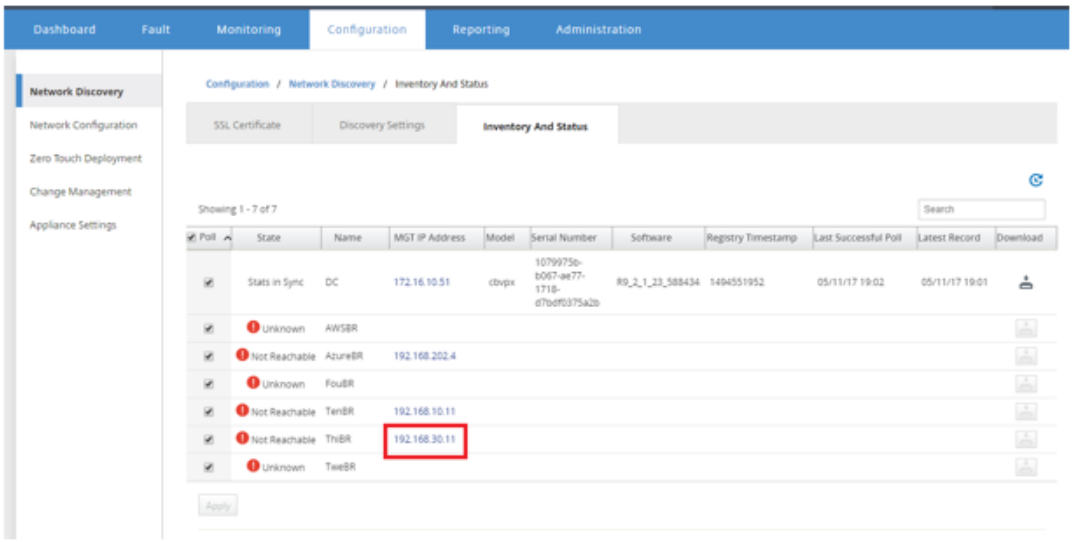
f) 構成は新しくインストールされたブランチオフィスアプライアンスに再配信され、ステータスは **MCN** > 構成 > 仮想 **WAN** > 変更管理 ページ（このプロセスは完了するまでに数分かかる場合があります）で監視されます。



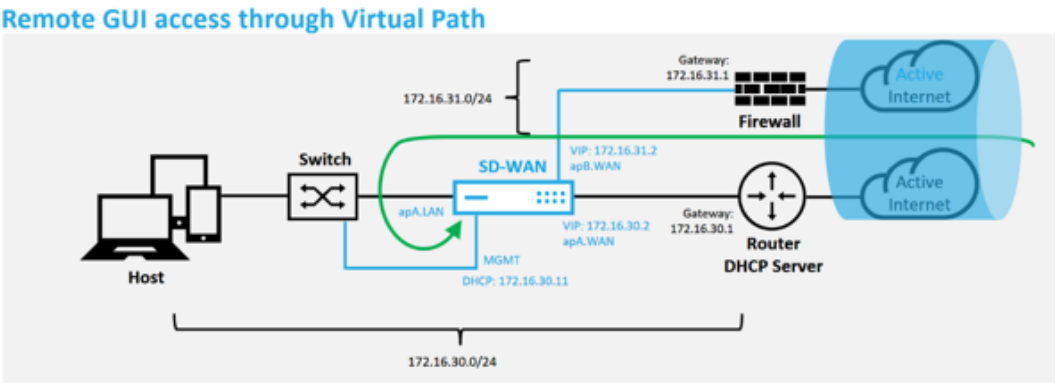
g) SD-WAN 管理者は、リモートサイトの確立された仮想パスのヘッドエンド MCN Web 管理ページを監視できます。



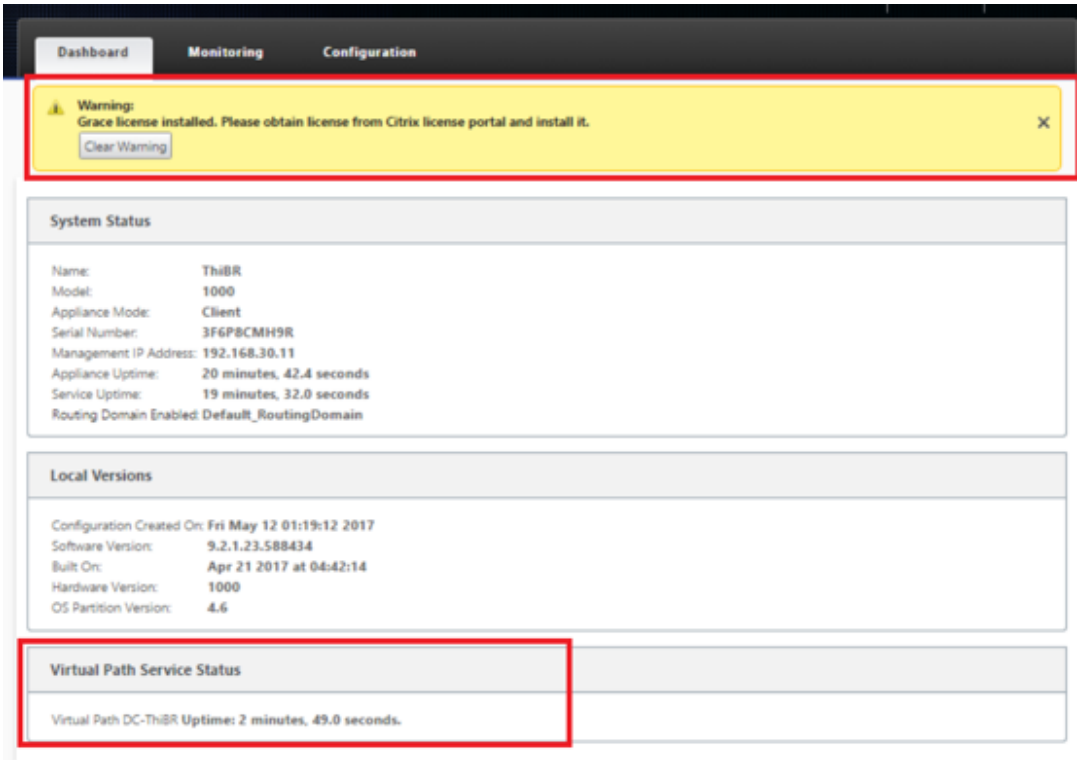
h) SD-WAN Center を使用して、[構成] > [ネットワーク検出] > [インベントリとステータス] ページから、オンサイトアプライアンスの DHCP 割り当てられた IP アドレスを識別することもできます。



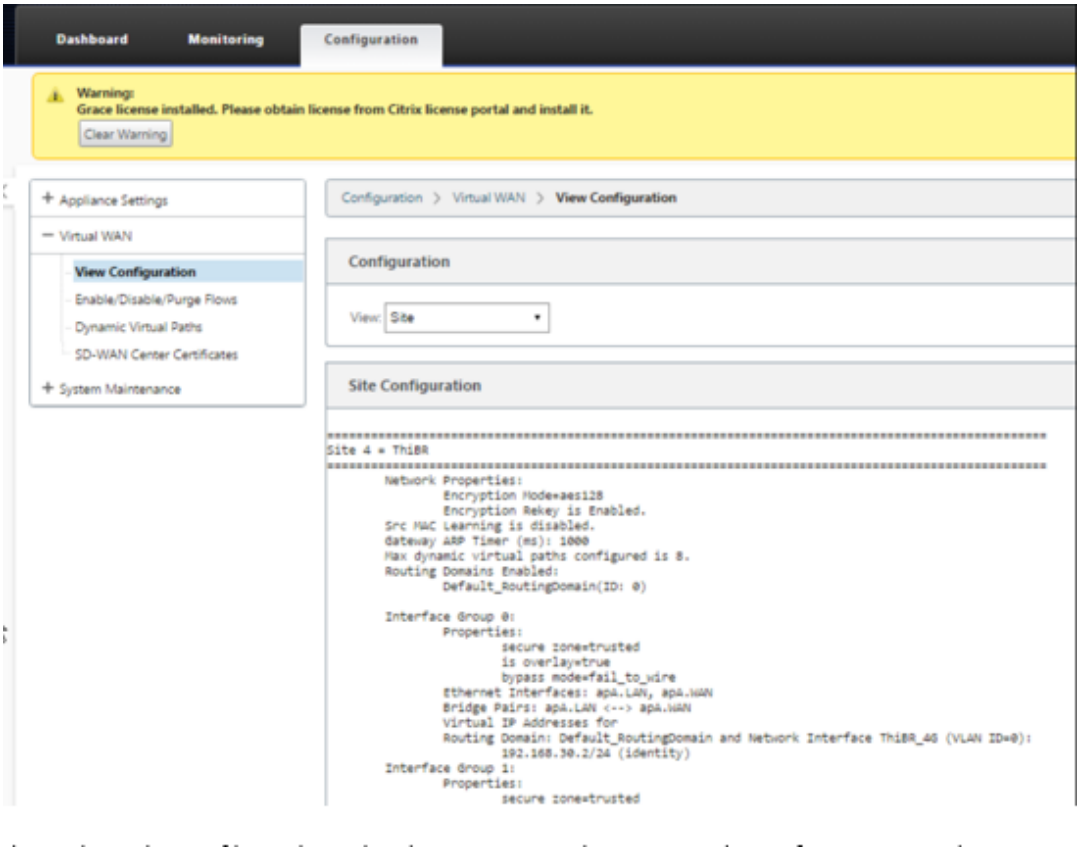
i) この時点で、SD-WAN ネットワーク管理者は、SD-WAN オーバーレイネットワークを利用して、オンサイトアプライアンスへの Web 管理アクセスを取得できます。



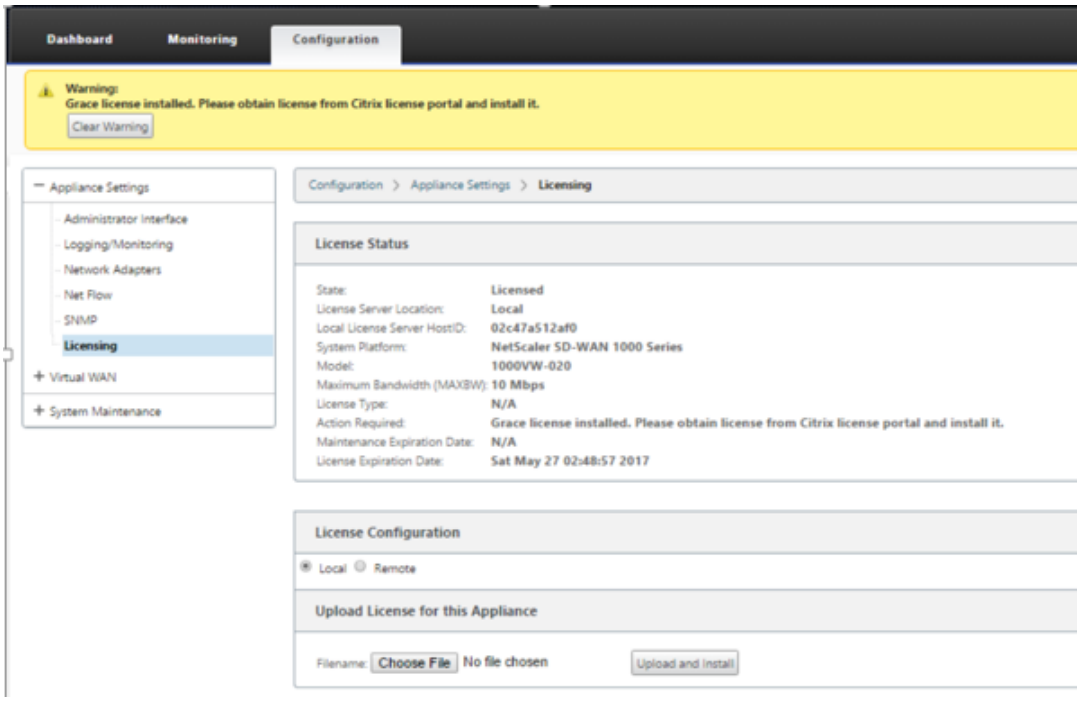
j) リモートサイトアプライアンスへの Web 管理アクセスは、アプライアンスに 10 Mbps の一時的な猶予ライセンスがインストールされていることを示しています。これにより、仮想パスサービスステータスをアクティブとして報告することができます。



k) アプライアンスの構成は、構成 > 仮想 **WAN** > 「構成の 表示」ページを使用して検証できます。



l) アプライアンスライセンスファイルは、構成 > アプライアンスの設定 > ライセンス ページを使用して永久ライセンスに更新できます。



m) 永久ライセンスファイルをアップロードしてインストールすると、グレースライセンス警告バナーが

消え、ライセンスのインストールプロセス中にリモートサイトへの接続が失われることはありません（ping はドロップされません）。

オンプレミスのゼロタッチ

April 13, 2021

ゼロタッチサービスを使用して SD-WAN アプライアンスをデプロイする方法については、トピック「ゼロタッチ展開サービスを構成する方法」を参照してください。

AWS

April 9, 2021

AWS へのデプロイ

SD-WAN リリース 9.3 では、ゼロタッチ展開機能がクラウドインスタンスに拡張されました。ゼロタッチ展開プロセス 4 つのクラウドインスタンスを展開する手順は、ゼロタッチサービスのアプライアンス展開とは少し異なります。

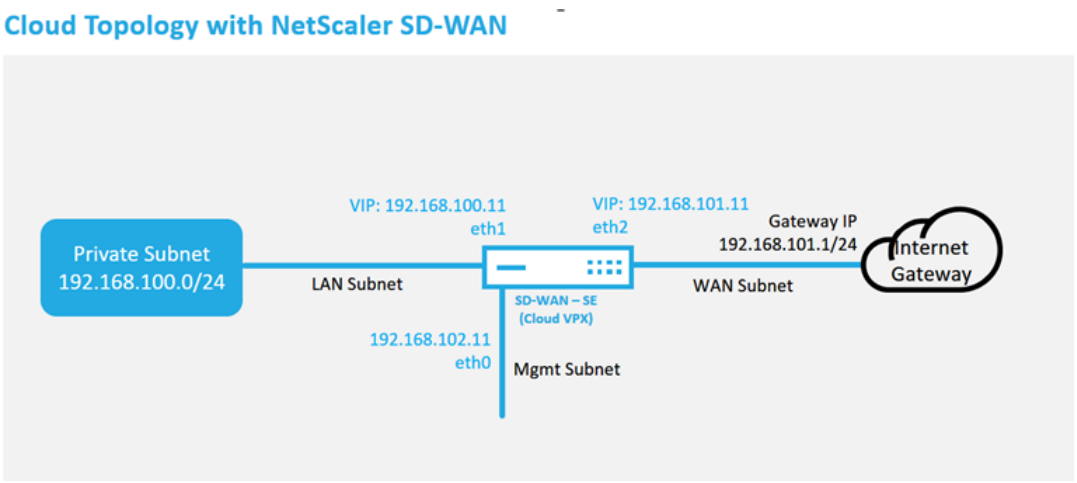
1. SD-WAN Center ネットワーク構成を使用して、ZTD 対応の SD-WAN クラウドデバイスを持つ新しいリモートサイトを追加するように構成を更新します。

   SD-WAN 設定が SD-WAN Center ネットワーク設定を使用して構築されていない場合は、MCN からアクティブな設定をインポートし、SD-WAN Center を使用して設定の変更を開始します。ゼロタッチ展開機能の場合、SD-WAN 管理者は SD-WAN Center を使用して構成を構築する必要があります。ゼロタッチ展開を対象とする新しいクラウドノードを追加するには、次の手順を使用する必要があります。

   a) 最初に新しいサイトの詳細（つまり、VPX サイズ、インターフェイスグループの使用状況、仮想 IP アドレス、帯域幅を備えた WAN リンク、およびそれぞれの Gateway）を概説することにより、SD-WAN クラウド展開用の新しいサイトを設計します。

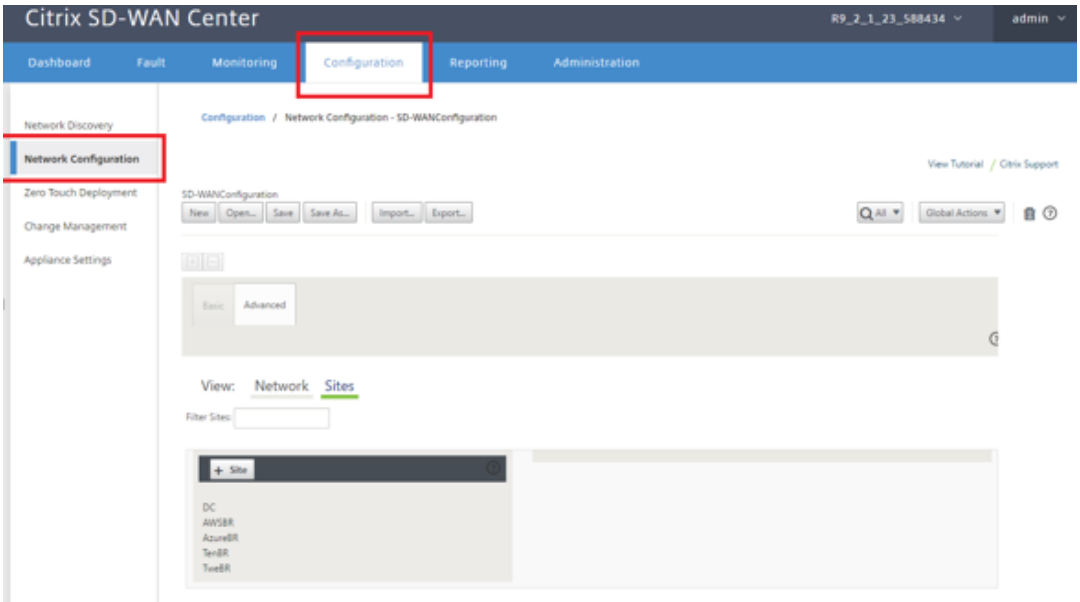
      > 注
      >
      > - クラウドにデプロイされた SD-WAN インスタンスは、Edge/Gateway モード。
      > - クラウドインスタンスのテンプレートは 3 つのインターフェースに制限されています。管理、LAN、WAN（この順序で）。

- SD-WAN VPX で利用可能なクラウドテンプレートは、現在、#.#.#.#.11 VPC で使用可能なサブネットの IP アドレス。



これは、SD-WAN クラウド展開サイトの展開例です。CitrixSD-WAN デバイスは、このクラウドネットワークで単一のインターネット WAN リンクにサービスを提供するエッジデバイスとして展開されます。リモートサイトは、クラウド用のこの同じ Internet Gateway に接続する複数の異なるインターネット WAN リンクを活用して、SD-WAN 展開サイトからクラウドインフラストラクチャへの復元力と集約された帯域幅接続を提供できます。これにより、費用効果が高く、信頼性の高いクラウドへの接続が提供されます。

b) SD-WAN Center の Web 管理インターフェイスを開き、構成に > ネットワーク設定ページに移動します。

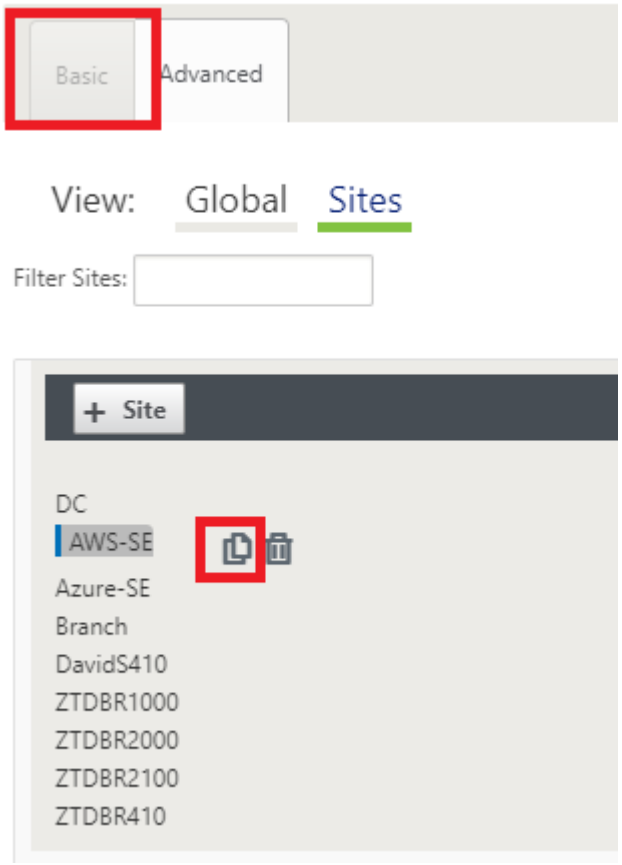


c) 動作中の構成がすでに配置されていることを確認するか、MCN から構成をインポートします。

d) [基本] タブに移動して、新しいサイトを作成します。

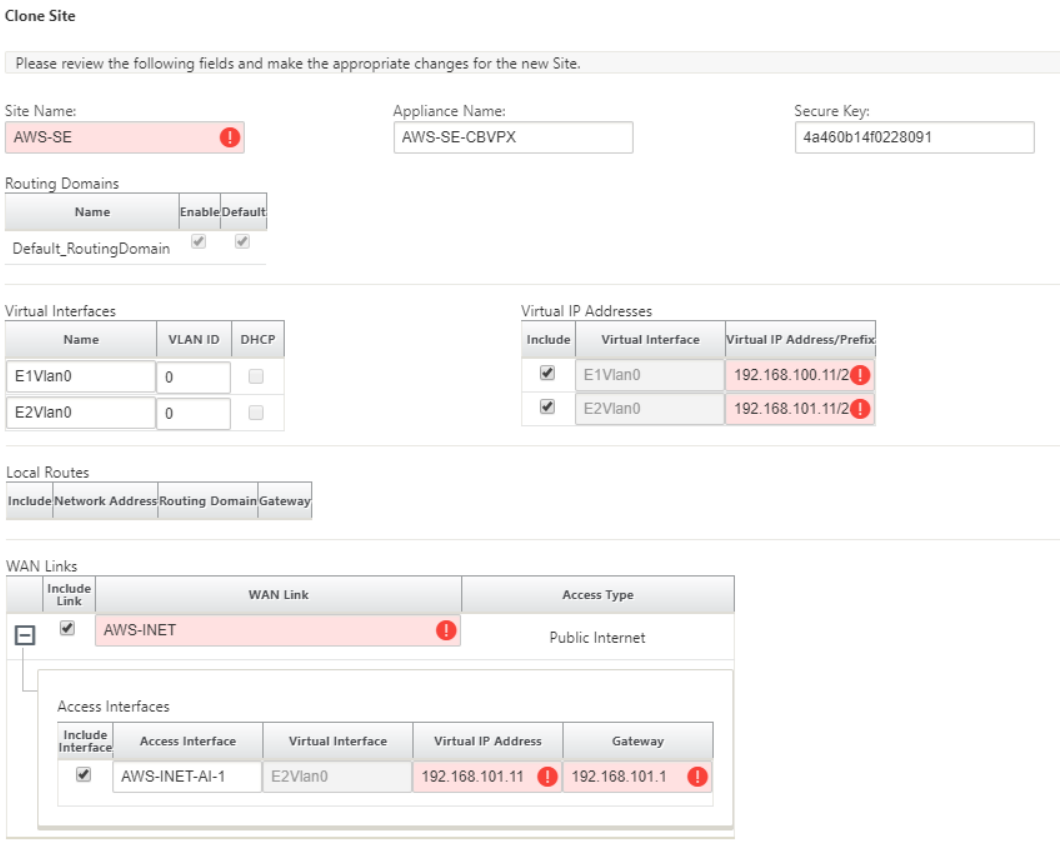
e) [サイト] タイルを開いて、現在構成されているサイトを表示します。

f) 既存のサイトのクローン機能を利用して新しいクラウドサイトの構成をすばやく構築するか、新しいサイトを手動で構築します。

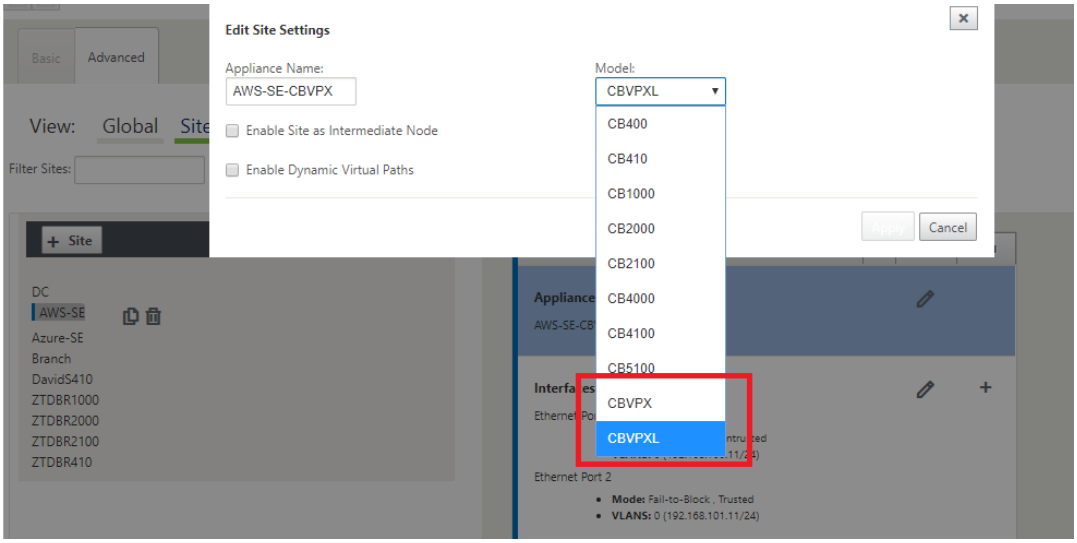


g) この新しいクラウドサイト用に以前に設計したトポロジからすべての必須フィールドに入力します

クラウド ZTD デプロイメントに使用できるテンプレートは、#.#.#.11 管理、LAN、および WAN サブネットの IP アドレス。構成が各インターフェイスの予想される.11 IP ホストアドレスと一致するように設定されていない場合、デバイスは、クラウド環境ゲートウェイへの ARP および MCN の仮想パスへの IP 接続を適切に確立できません。



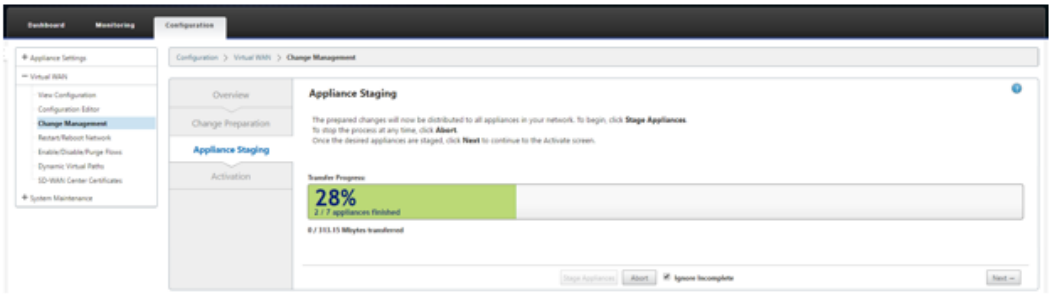
h) 新しいサイトのクローンを作成した後、サイトの **[基本設定]** に移動し、ゼロタッチサービスをサポートする SD-WAN のモデルが正しく選択されていることを確認します。



i) SD-WAN Center に新しい構成を保存し、「変更管理の受信トレイ」オプションへのエクスポートを使用して、変更管理を使用して構成をプッシュします。

j) 変更管理手順に従って、新しい構成を適切にステージングします。これにより、既存の SD-WAN デバ

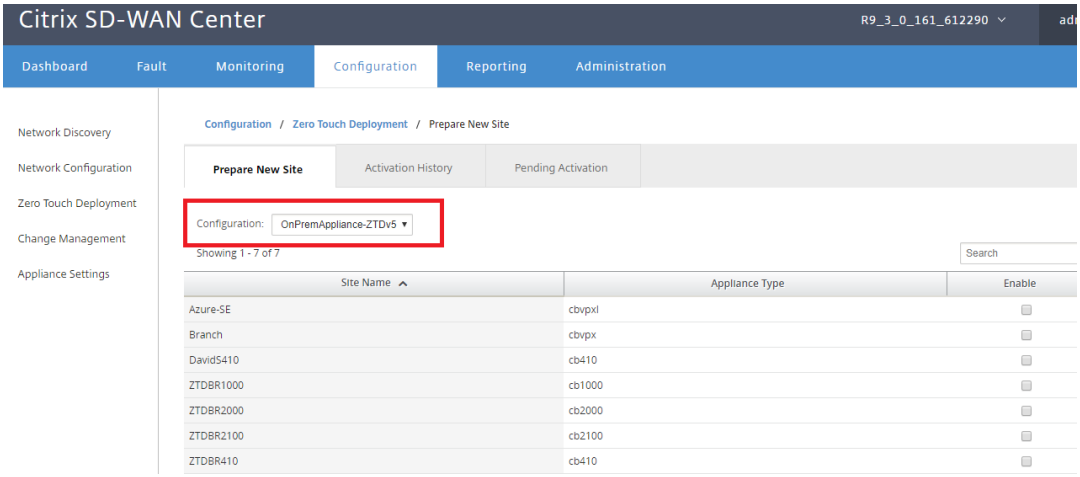
イスは、ゼロタッチで展開される新しいサイトを認識します。構成をプッシュする試みをスキップするには、「不完全を無視」オプションを使用する必要があります。ZTD ワークフローを通過する必要がある新しいサイトに移動します。



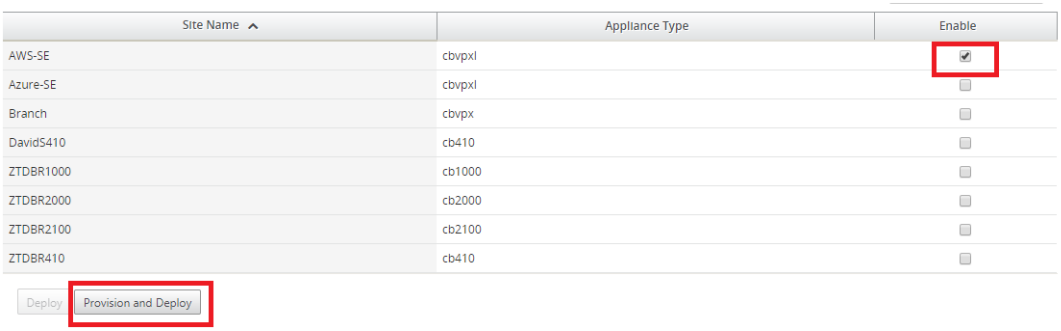
2. SD-WAN Center のゼロタッチ展開ページに戻り、新しいアクティブな構成を実行すると、新しいサイトを展開できるようになります。

   a) [ゼロタッチ展開] ページの [新しいサイトの展開] タブで、実行中のネットワーク構成ファイルを選択します。

   b) 実行構成ファイルを選択すると、ゼロタッチがサポートされている未展開の Citrix SD-WAN デバイスを含むすべてのブランチサイトのリストが表示されます。



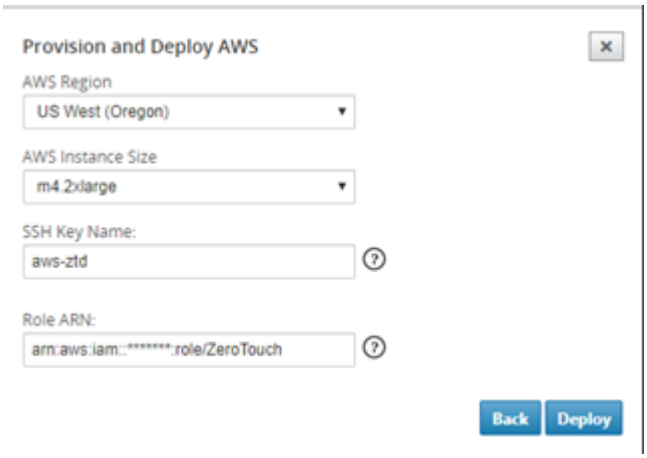
   c) ゼロタッチサービスを使用して展開するターゲットクラウドサイトを選択し、［有効にする］、［プロビジョニングと］と［展開］の順にクリックします。



d) ポップアップウィンドウが表示され、Citrix SD-WAN 管理者がゼロタッチの展開を開始できます。

アクティベーション URL を配信できるメールアドレスを 入力 し、目的のクラウドのプロビジョニングタイプを選択します。

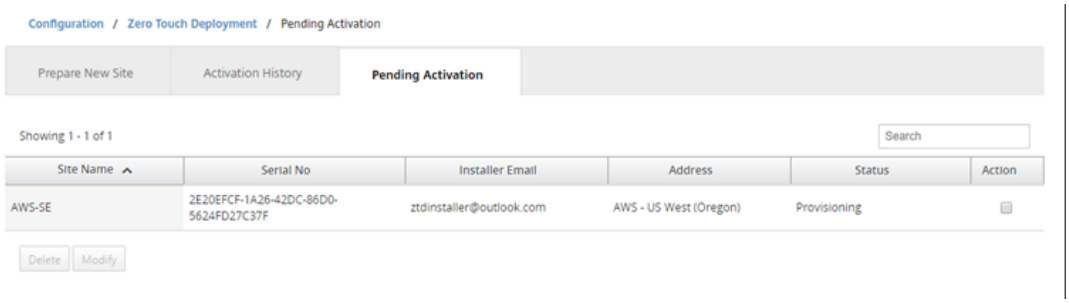
e) [次へ] をクリックした後、適切なリージョン、インスタンスサイズを選択し、SSH キー名とロール ARN フィールドに適切に入力します。



> 注
>
> クラウドアカウントで SSH キーとロール ARN を設定する方法のガイダンスについては、ヘルプリンクを利用してください。また、選択したリージョンがアカウントで利用可能なものと一致していること、および選択したインスタンスサイズが SD-WAN 構成で選択したモデルとして VPX または VPXL と一致していることを確認してください。

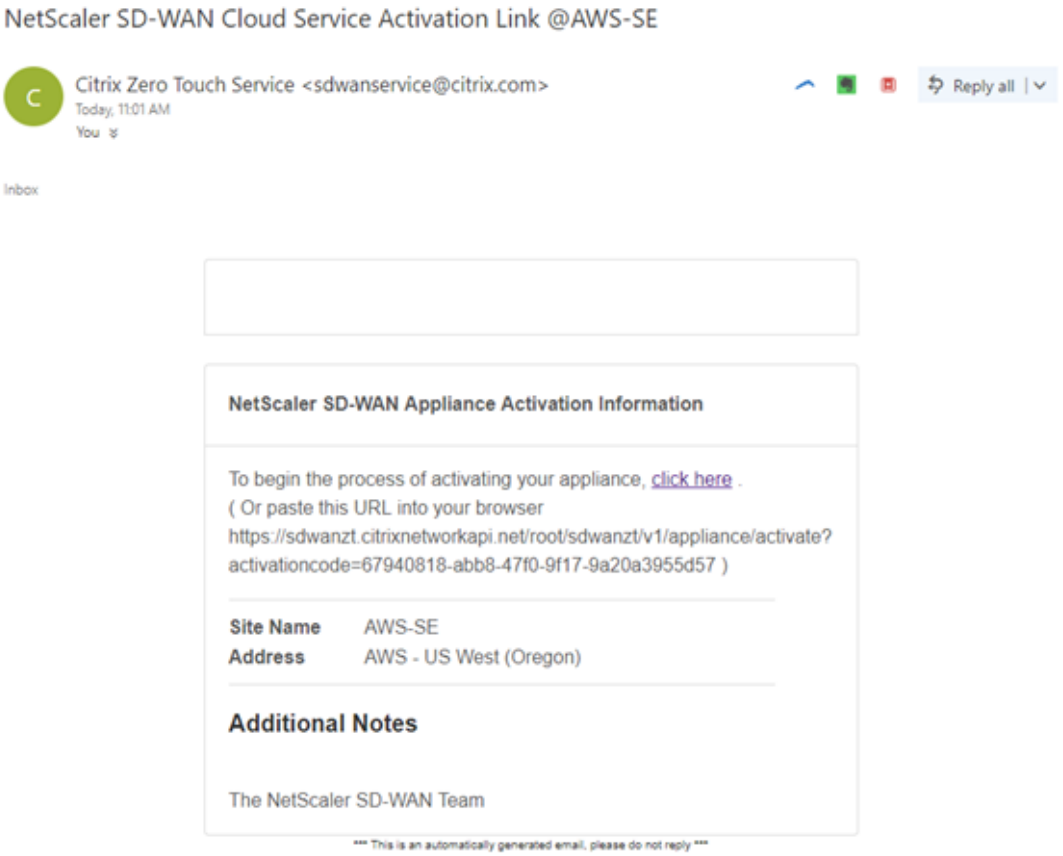
f) 以前に ZTD クラウドサービスに登録されていた SD-WAN Center を起動して、ZTD クラウドサービスに保存されているサイトの設定を共有します。

g) [保留中のアクティブ化] タブに移動して、サイト情報が正常に入力され、プロビジョニングステータスになったことを確認します。



3. クラウド管理者としてゼロタッチ導入プロセスを開始します。

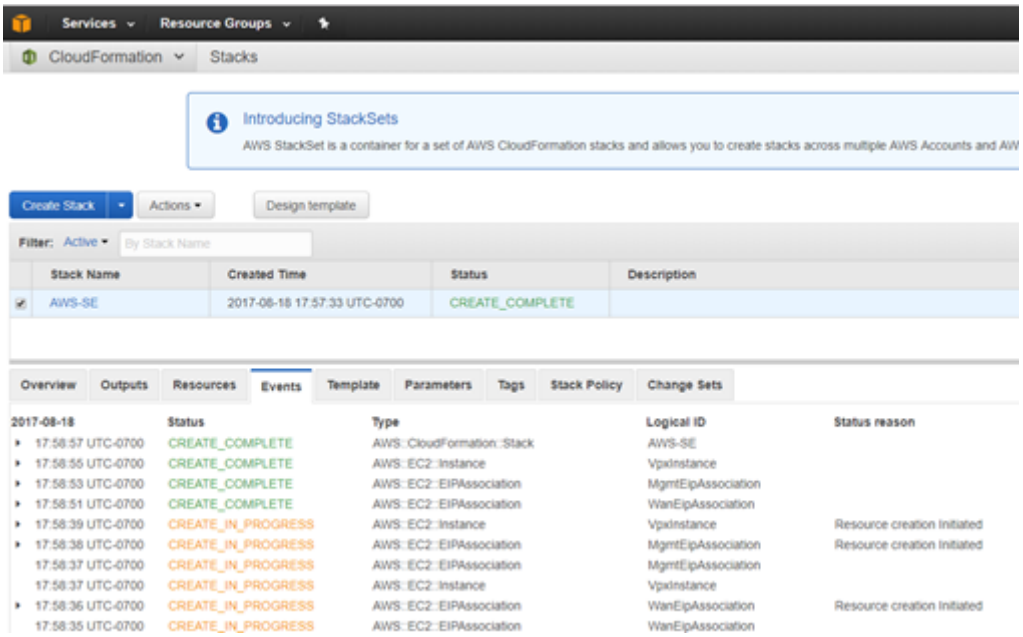
   a) インストーラーは、サイトの展開時に SD-WAN 管理者が使用した電子メールアドレスのメールボックスを確認する必要があります。



   b) メールに記載されているアクティベーション URL をインターネットブラウザウィンドウで開きます。

   c) SSH キーとロール ARN が正しく入力されている場合、ゼロタッチ展開サービスはすぐに SD-WAN インスタンスのプロビジョニングを開始します。それ以外の場合は、接続エラーがすぐに表示されます。

d) AWS コンソールでの追加のトラブルシューティングでは、クラウド形成サービスを利用して、プロビジョニングプロセス中に発生するイベントをキャッチできます。

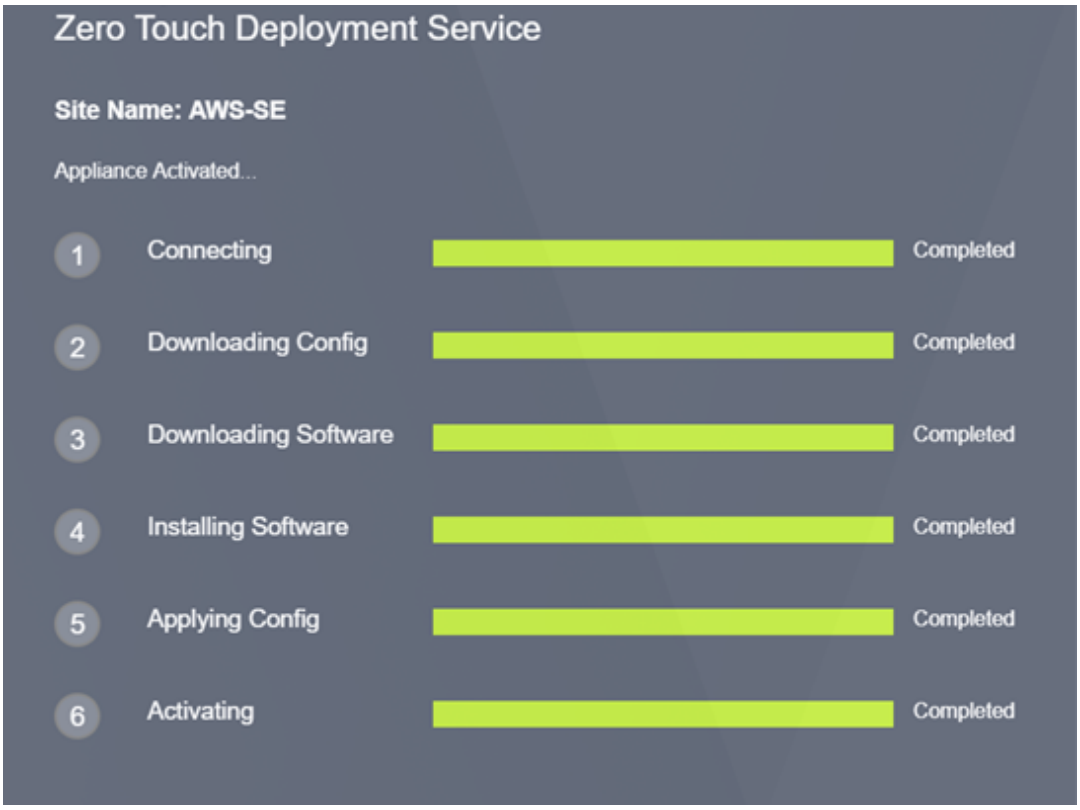


e) プロビジョニングプロセスを許可する ~8-10 分とアクティベーション別 ~3-5 完全に完了するまで数分。

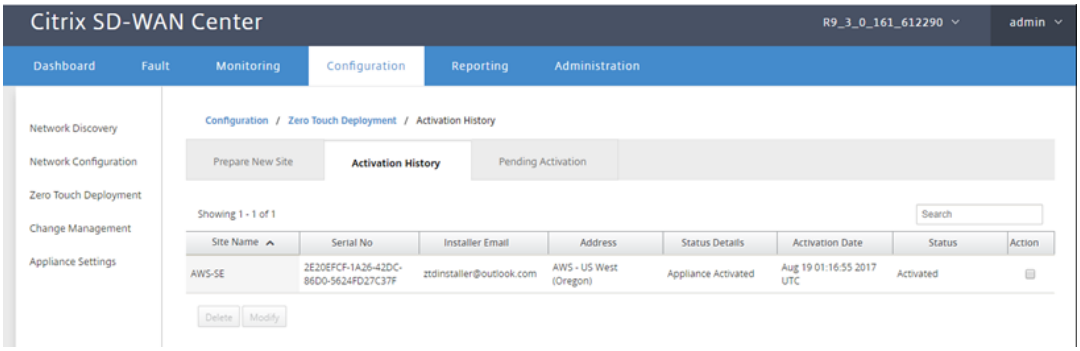
f) SD-WAN クラウドインスタンスの ZTD クラウドサービスへの接続が成功すると、サービスは自動的に以下を実行します。

- SD-WAN Center によって以前に保存されたサイト固有の設定ファイルをダウンロードします。

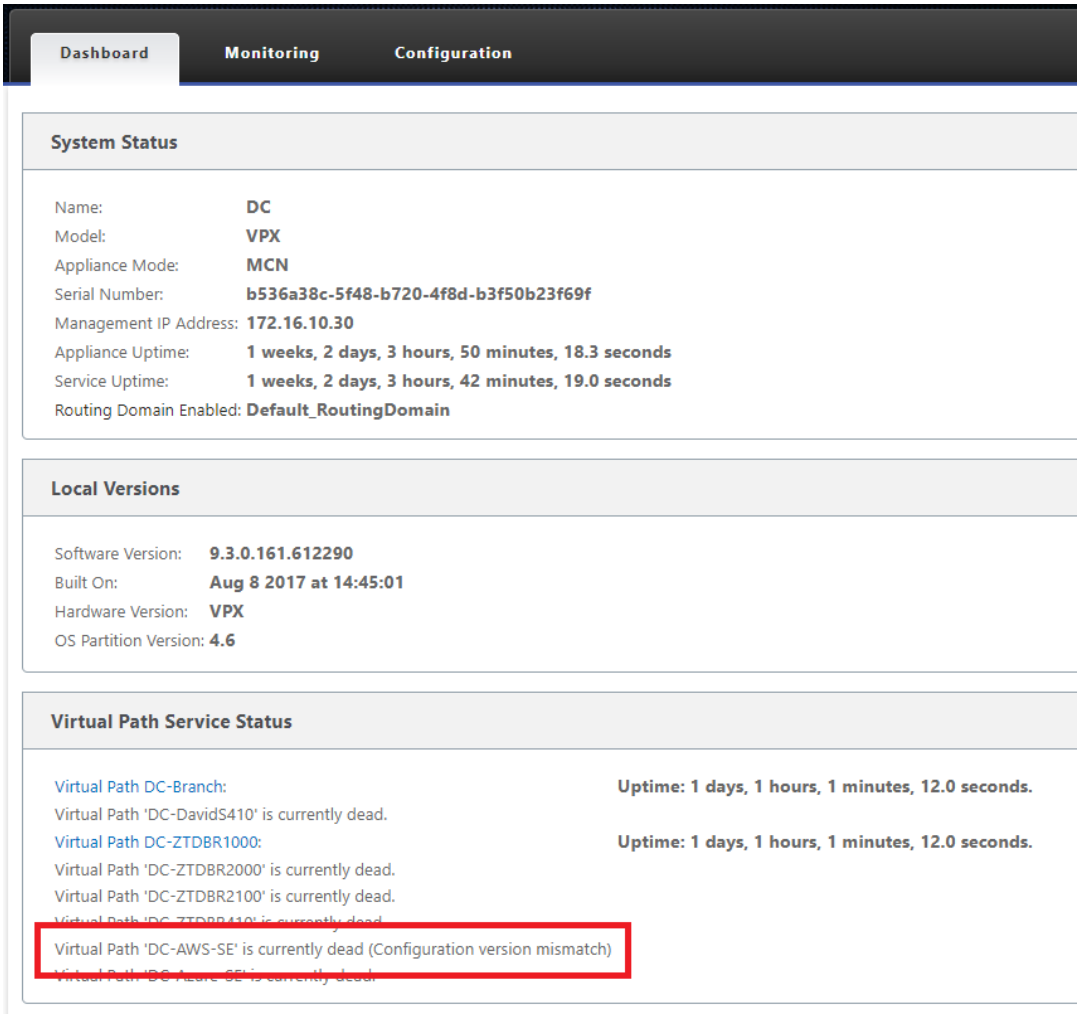
- ローカルインスタンスへの構成の適用
- 10 MB の一時ライセンスファイルをダウンロードしてインストールする
- 必要に応じて、ソフトウェアの更新をダウンロードしてインストールします
- SD-WAN サービスをアクティブ化する



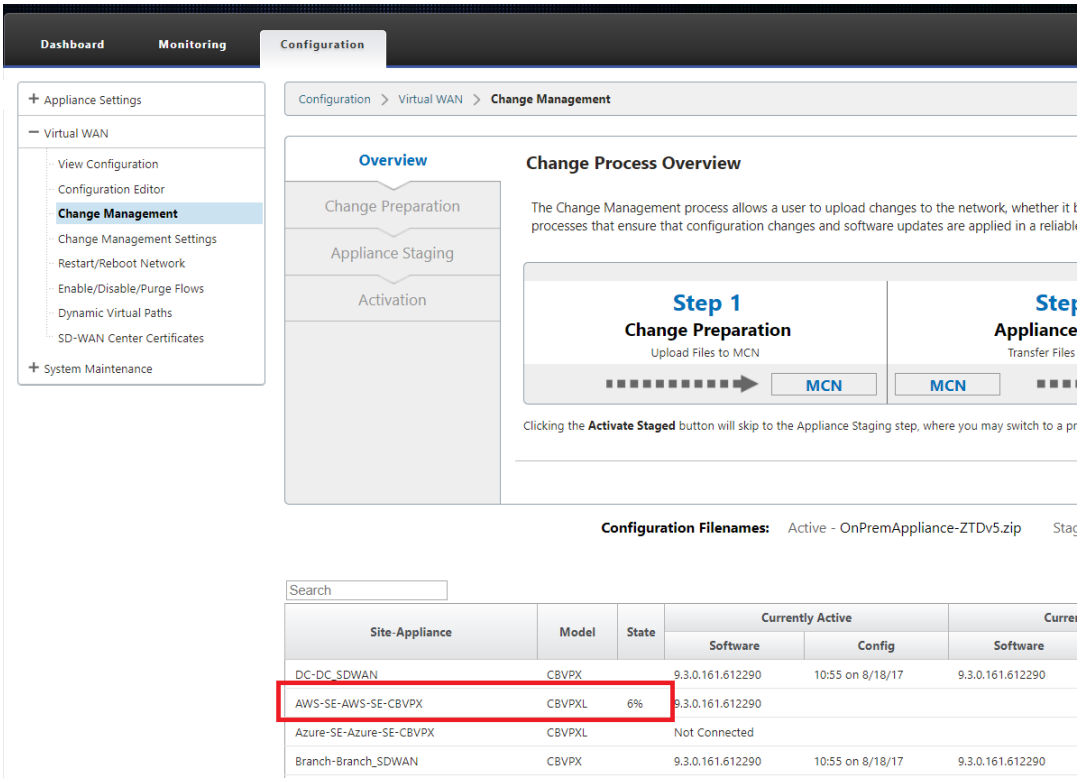
g) SD-WAN Center の Web 管理インターフェースでさらに確認を行うことができます。ゼロタッチ展開メニューでは、正常にアクティブ化されたアプライアンスが [アクティベーション履歴] タブに表示されます。



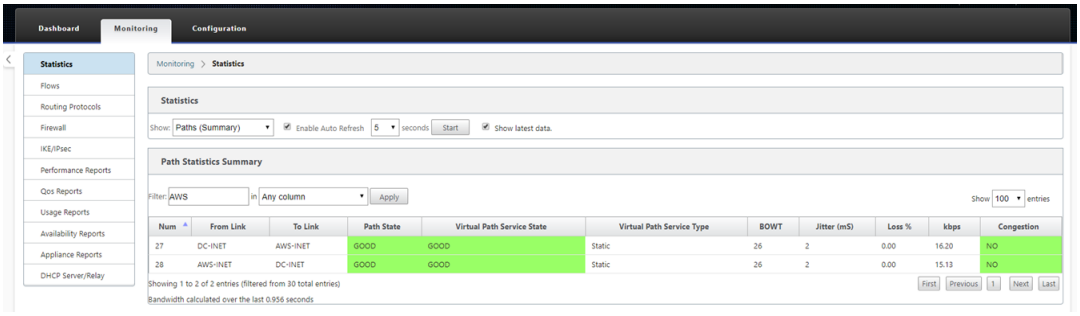
h) 仮想パスが接続状態ですぐに表示されない場合があります。これは、MCN が ZTD クラウドサービスから渡された構成を信頼しておらず、MCN ダッシュボードで「構成バージョンの不一致」を報告するためです。



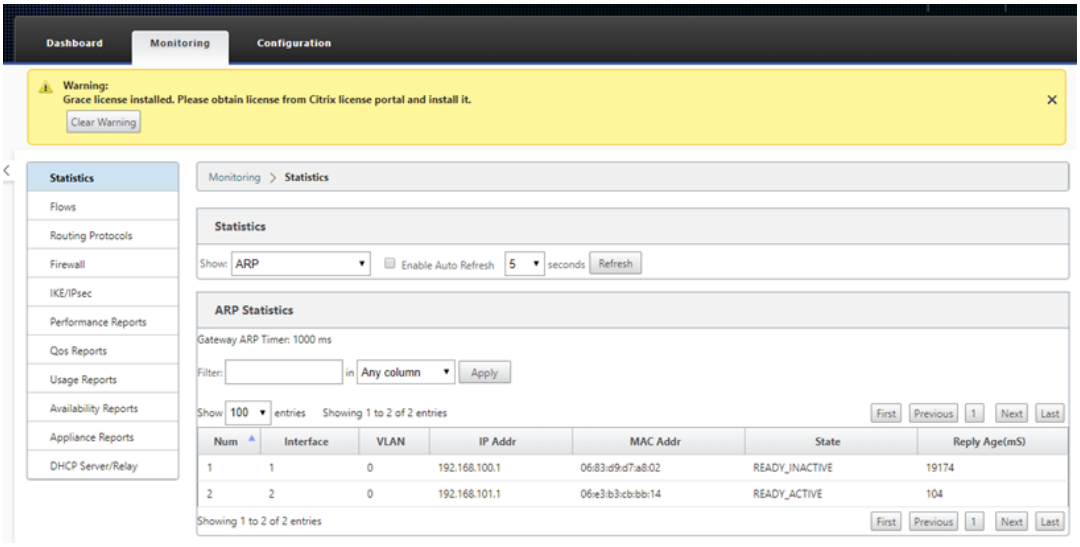
i) 構成は自動的に新しくインストールされたブランチオフィスアプライアンスに再配信されます。このステータスは **MCN**> 構成 > 仮想 **WAN**> 変更管理ページ（接続によっては、このプロセスが完了するまでに数分かかる場合があります）で監視できます。



j) SD-WAN 管理者は、新しく追加されたクラウドサイトの確立された仮想パスについて、ヘッドエンドの MCN Web 管理ページを監視できます。



k) トラブルシューティングが必要な場合は、プロビジョニング中にクラウド環境によって割り当てられたパブリック IP を使用して SD-WAN インスタンスのユーザーインターフェイスを開き、モニタリングの ARP テーブルを利用します > 予想されるゲートウェイへの接続の問題を特定するための 統計 ページ、または診断でトレースルートとパケットキャプチャオプションを利用します。



Azure

April 13, 2021

SD-WAN リリース 9.3 では、ゼロタッチ展開機能がクラウドインスタンスに拡張されました。クラウドインスタンスのゼロタッチ展開プロセスを展開する手順は、ゼロタッチサービスのアプライアンス展開とは少し異なります。

SD-WAN Center ネットワーク構成を使用して、**ZTD** 対応の **SD-WAN** クラウドデバイスで新しいリモートサイトを追加するための構成の更新

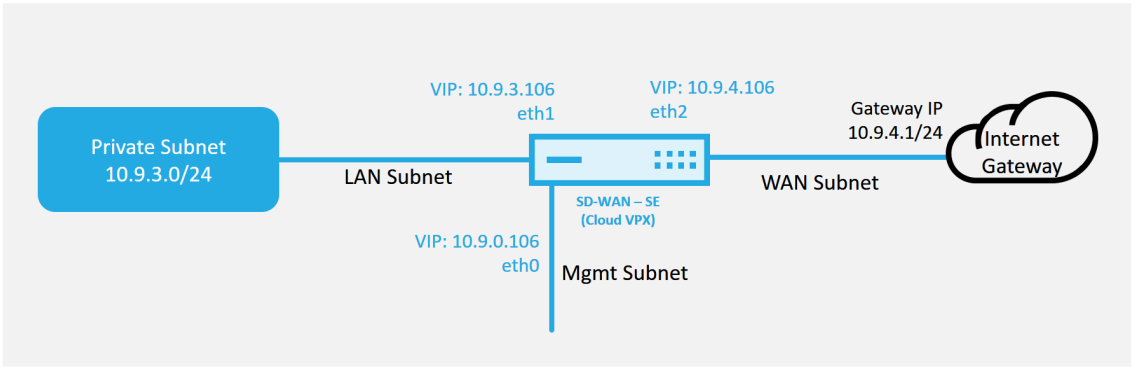
SD-WAN 設定が SD-WAN Center ネットワーク設定を使用して構築されていない場合は、MCN からアクティブな設定をインポートし、SD-WAN Center を使用して設定の変更を開始します。Zero Touch Deployment 機能を使用するには、SD-WAN 管理者は SD-WAN Center を使用して設定を構築する必要があります。ゼロタッチ展開を対象とする新しいクラウドノードを追加するには、次の手順を使用する必要があります。

1. 最初に新しいサイトの詳細（つまり、VPX サイズ、インターフェイスグループの使用状況、仮想 IP アドレス、帯域幅を備えた WAN リンク、およびそれぞれの Gateway）を概説することにより、SD-WAN クラウド展開用の新しいサイトを設計します。

   > 注
   >
   > - クラウドにデプロイされた SD-WAN インスタンスは、Edge/Gateway モード。
   > - クラウドインスタンスのテンプレートは 3 つのインターフェースに制限されています。管理、LAN、WAN（この順序で）。
   > - SD-WAN VPX で使用できる Azure クラウドテンプレートは、現在、WAN に 10.9.4.106 IP、LAN

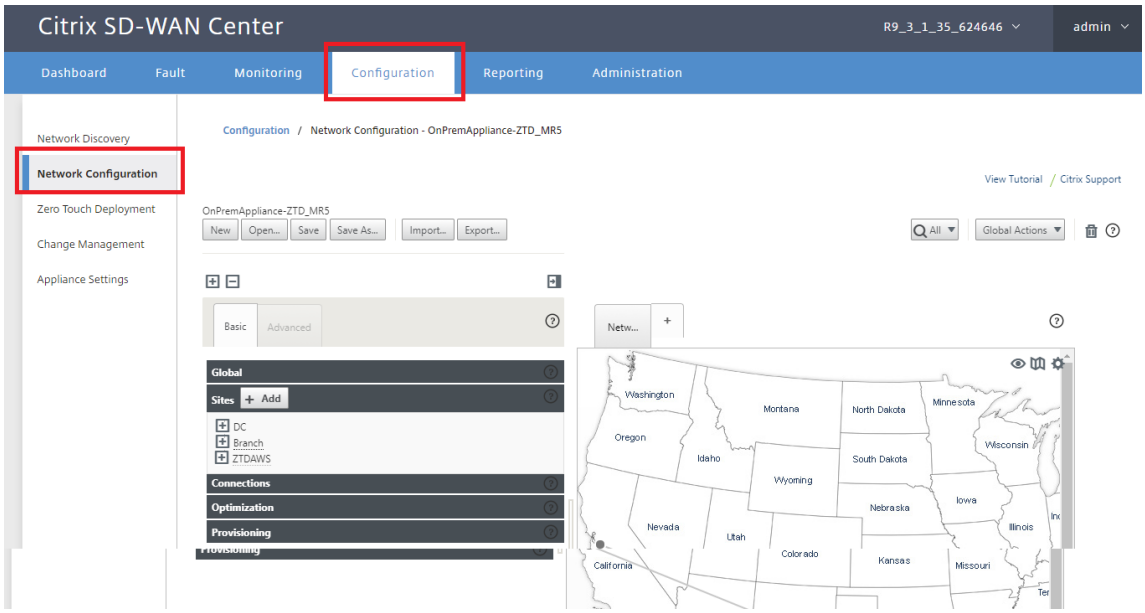
> に 10.9.3.106 IP、管理アドレスに 10.9.0.16 IP を取得するようにハードセットされています。ゼロタッチを対象とする Azure ノードの SD-WAN 構成は、このレイアウトと一致する必要があります。
>
> - 構成内の Azure サイト名は、特殊文字を含まないすべて小文字にする必要があります（ztdazure など）。

Azure Cloud Topology with NetScaler SD-WAN



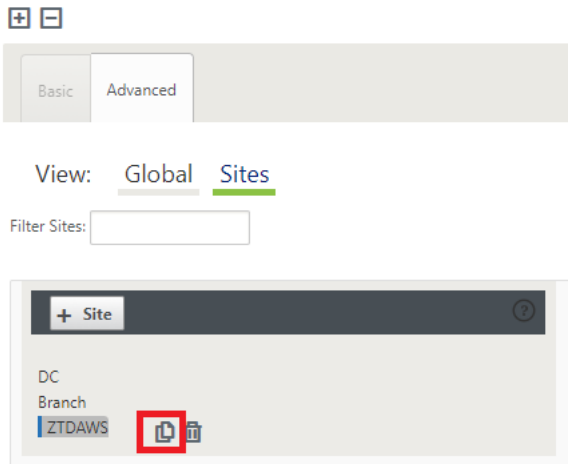
これは、SD-WAN クラウド展開サイトの展開例です。CitrixSD-WAN デバイスは、このクラウドネットワークで単一のインターネット WAN リンクにサービスを提供するエッジデバイスとして展開されます。リモートサイトは、クラウド用のこの同じ Internet Gateway に接続する複数の異なるインターネット WAN リンクを活用して、SD-WAN 展開サイトからクラウドインフラストラクチャへの復元力と集約された帯域幅接続を提供できます。これにより、費用効果が高く、信頼性の高いクラウドへの接続が提供されます。

2. SD-WAN Center の Web 管理インターフェイスを開き、構成に > ネットワーク設定ページに移動します。



3. 動作中の構成がすでに配置されていることを確認するか、MCN から構成をインポートします。
4. [基本] タブに移動して、新しいサイトを作成します。

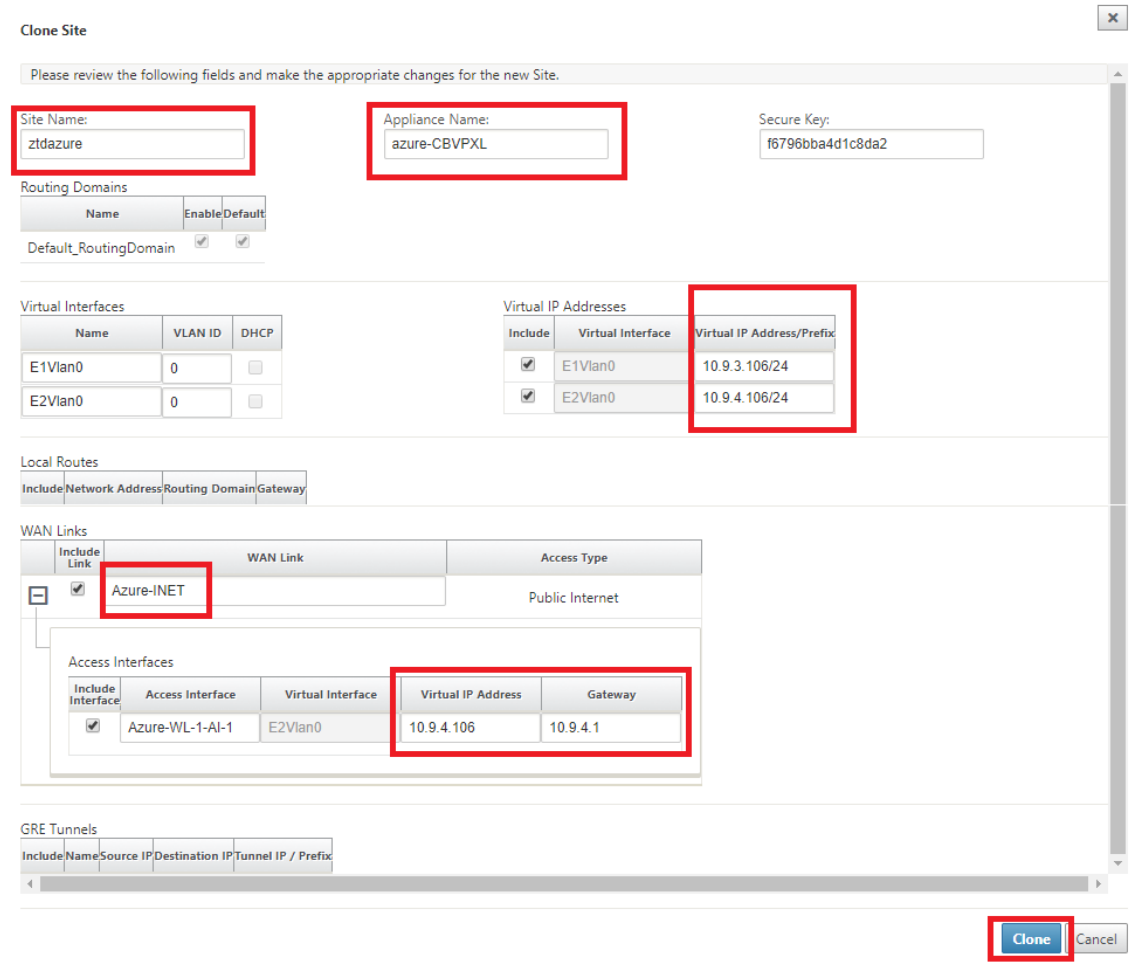
5. [サイト] タイルを開いて、現在構成されているサイトを表示します。
6. 既存のサイトのクローン機能を利用して新しいクラウドサイトの構成をすばやく構築するか、新しいサイトを手動で構築します。



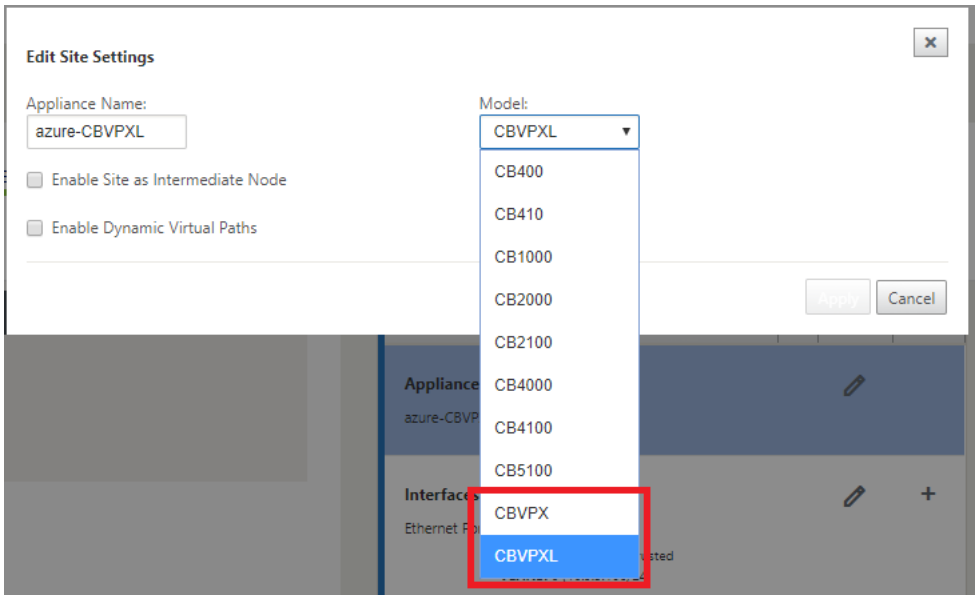
7. この新しいクラウドサイト用に以前に設計されたトポロジのすべての必須フィールドに入力します。

   Azure クラウド ZTD デプロイメントに使用できるテンプレートは現在、WAN に 10.9.4.106 IP、LAN に 10.9.3.106 IP、管理アドレスに 10.9.0.16 IP を取得するようにハードセットされていることに注意してください。構成が各インターフェイスの予想される VIP アドレスと一致するように設定されていない場合、デバイスはクラウド環境ゲートウェイへの ARP および MCN の仮想パスへの IP 接続を適切に確立できません。

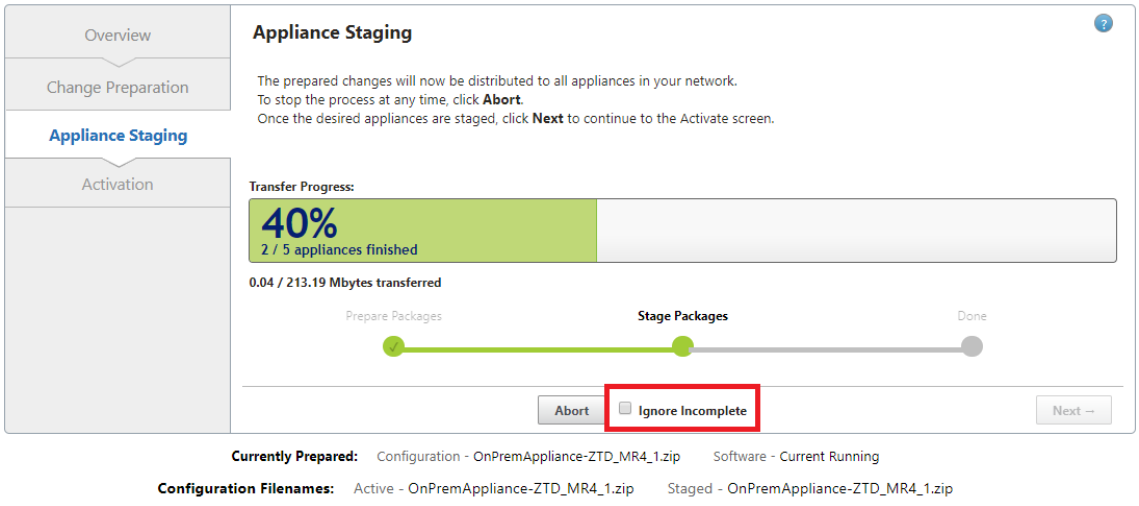
   サイト名が Azure が期待するものに準拠していることが重要です。サイト名はすべて小文字で、6 文字以上で、特殊文字を含まない必要があり、次の正規表現で確認する必要があります ^[a-z][a-z0-9-]{1,61}[a-z0-9]$.**



8. 新しいサイトのクローンを作成した後、サイトの **[基本設定]** に移動し、ゼロタッチサービスをサポートする SD-WAN のモデルが正しく選択されていることを確認します。

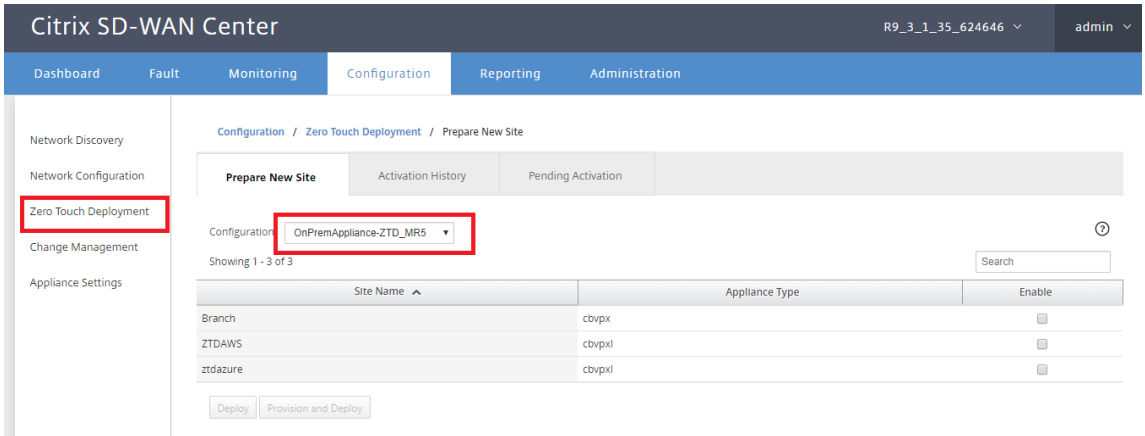


9. SD-WAN Center に新しい構成を保存し、「変更管理の受信トレイ」オプションへのエクスポートを使用して、変更管理を使用して構成をプッシュします。
10. 変更管理手順に従って、新しい構成を適切にステージングします。これにより、既存の SD-WAN デバイスは、ゼロタッチで展開される新しいサイトを認識します。構成をプッシュする試みをスキップするには、「不完全を無視」オプションを使用する必要があります。ZTD ワークフローを通過する必要がある新しいサイトに移動します。

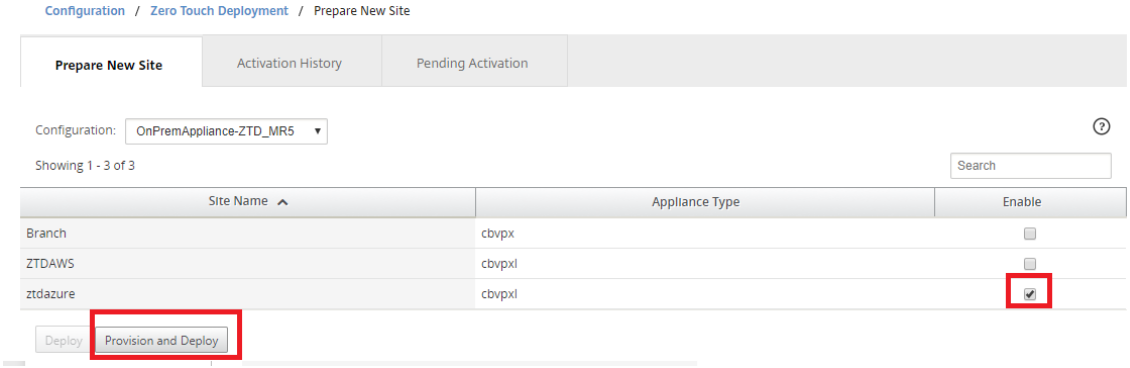


SD-WAN Center の **[ゼロタッチデプロイ]** ページに移動し、新しいアクティブな構成が実行されている状態で、新しいサイトを **SD-WAN Center** のプロビジョニングとデプロイ **Azure** で使用できるようになります **(ステップ 1/2)**

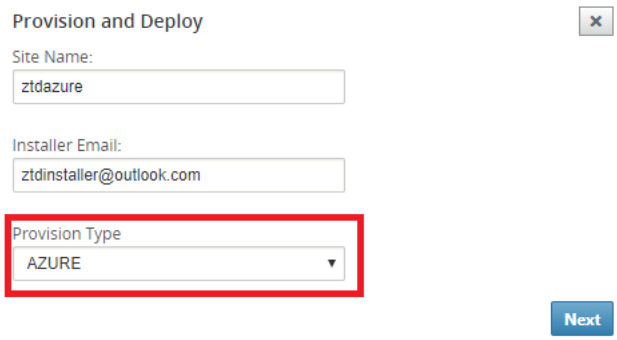
1. Zero Touch Deployment ページで、Citrix アカウントの認証情報を使用してログインします。[**Deploy New Site**] タブで、実行中のネットワーク構成ファイルを選択します。
2. 実行構成ファイルを選択すると、ZTD 対応の Citrix SD-WAN デバイスを備えたすべてのブランチサイトのリストが表示されます。



3. ゼロタッチサービスを使用して展開するターゲットクラウドサイトを選択し、[有効にする]、[プロビジョニングと] と [展開] の順にクリックします。

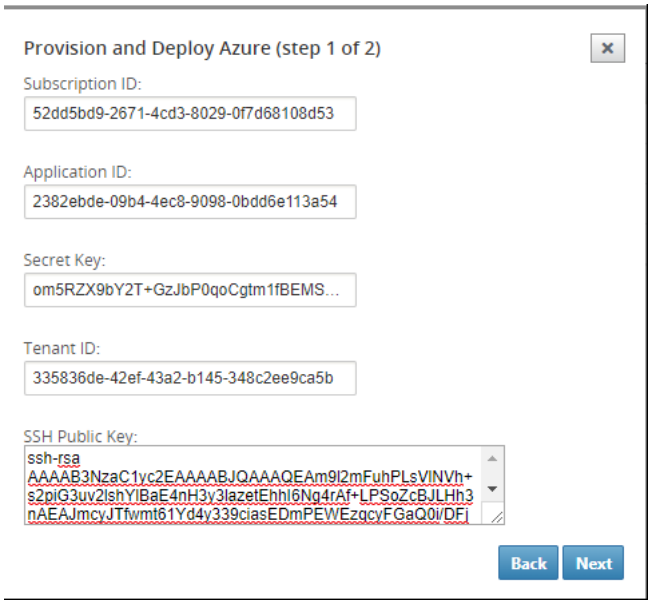


4. ポップアップウィンドウが表示され、Citrix SD-WAN 管理者がゼロタッチの展開を開始できます。サイト名が Azure の要件（特殊文字を含まない小文字）に準拠していることを確認します。[次へ] をクリックする前に、アクティベーション URL を配信できる電子メールアドレスを入力し、目的のクラウドのプロビジョニングタイプとして Azure を選択します。

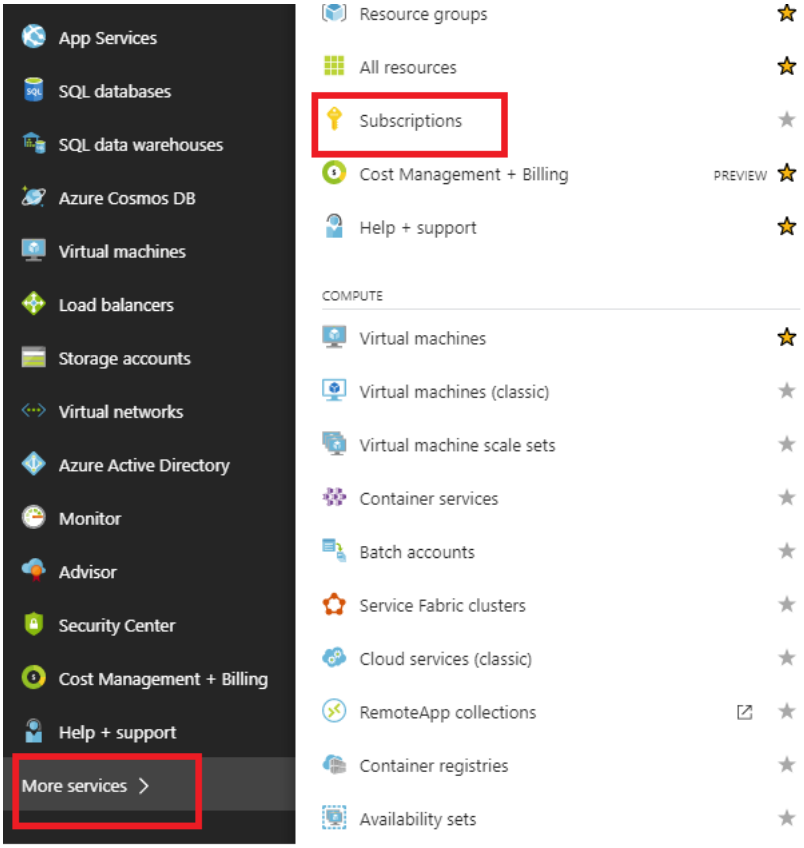


5. [次へ] をクリックした後、[Azure のプロビジョニングとデプロイ（ステップ 1/2）] ウィンドウで、Azure アカウントから取得した情報を入力する必要があります。

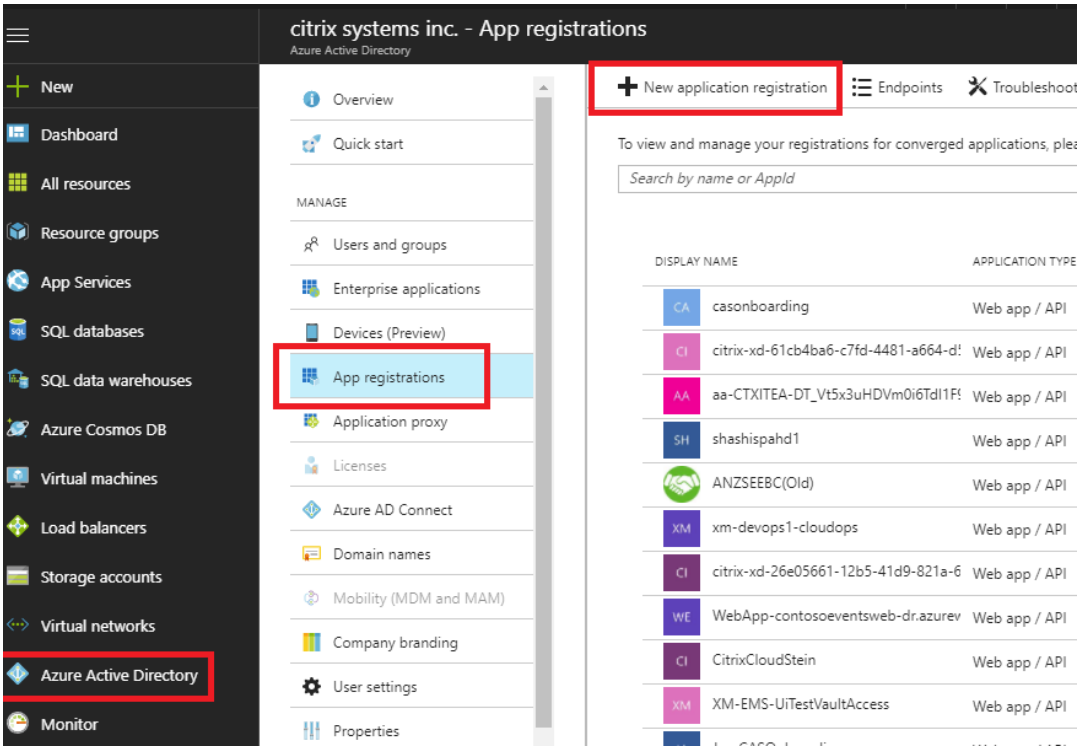
   Azure アカウントから情報を取得したら、各必須フィールドをコピーして貼り付けます。以下の手順は、Azure アカウントから必要なサブスクリプション ID、アプリケーション ID、シークレットキー、およびテナント ID を取得する方法の概要を示した後、[次へ] をクリックして続行します。



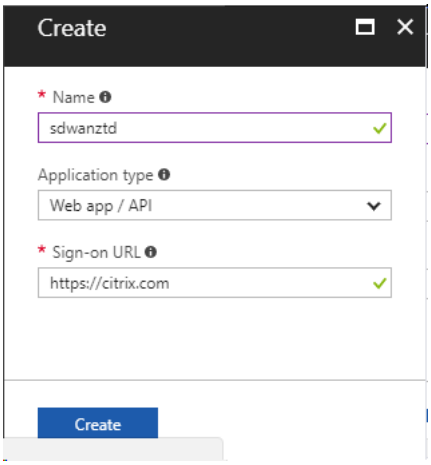
a) Azure アカウントでは、[その他のサービス] に移動して [サブスクリプション*]* を選択することで、必要な サブスクリプション **ID** を識別できます。



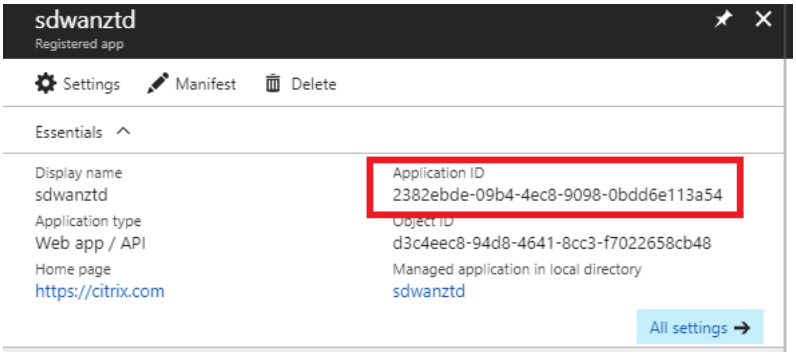
b) 必要な アプリケーション ***ID*** を識別するには、Azure Active Directory、アプリケーション登録に移動し、[新しいアプリケーション登録] をクリックします。



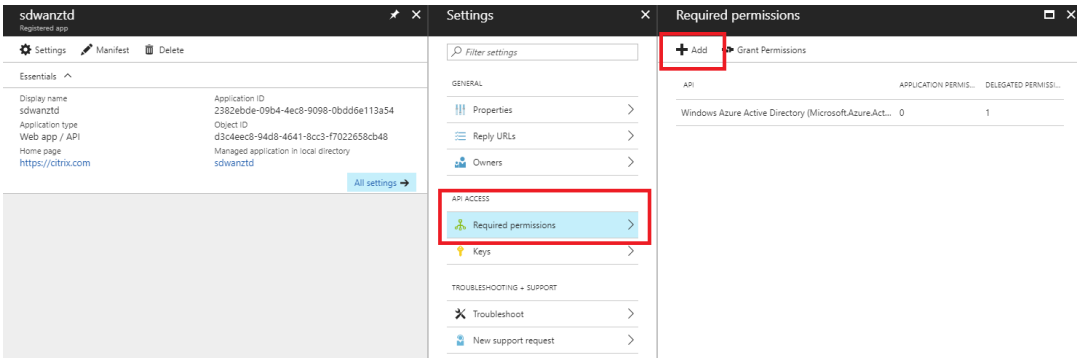
c) アプリ登録の作成メニューで、名前とサインオン URL（これは任意の URL にすることができますが、唯一の要件は有効でなければならない）を入力し、[作成] をクリックします。



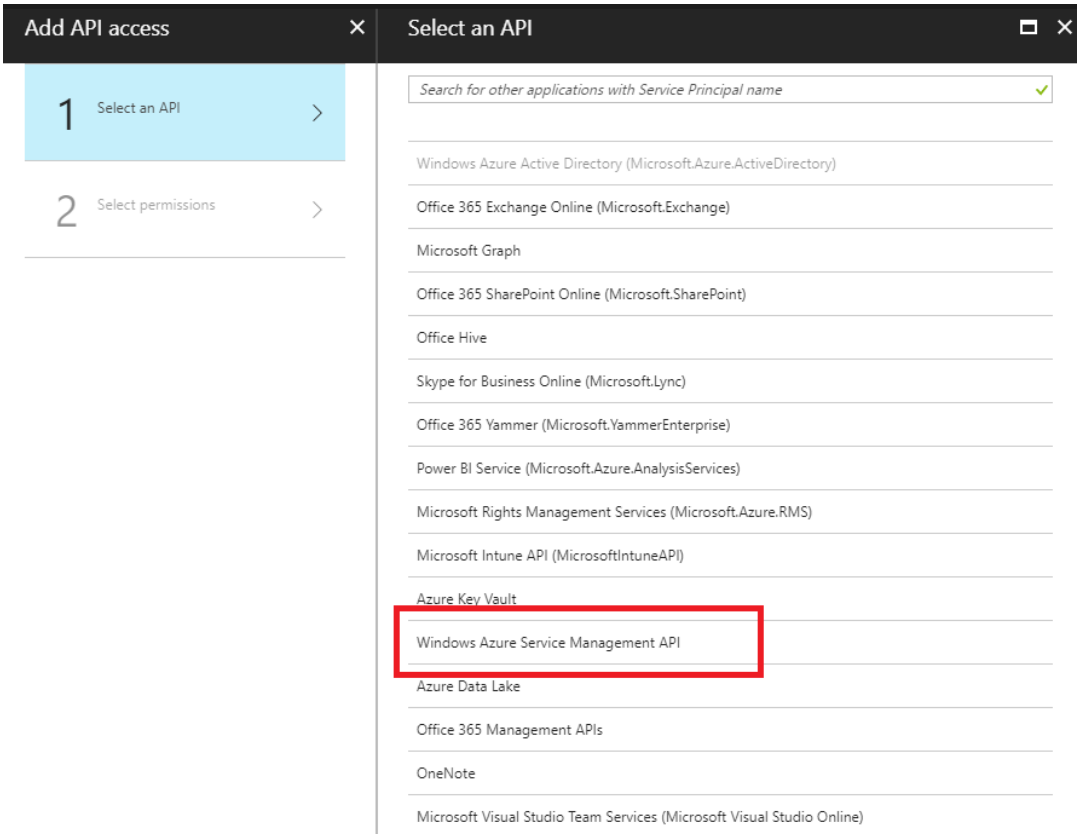
d) 新しく作成された登録済みアプリを検索して開き、アプリケーション ID をメモします。



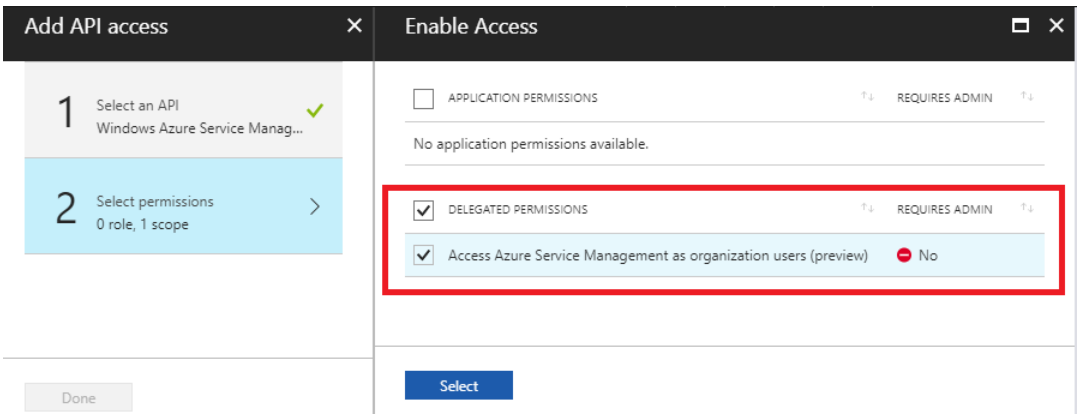
e) 新しく作成した登録アプリを再度開き、必要な セキュリティキーを特定するために、[API アクセス] で [必要な 権限] を選択して、サードパーティによるプロビジョニングとインスタンス化を許可します。次に [追加] を選択します。



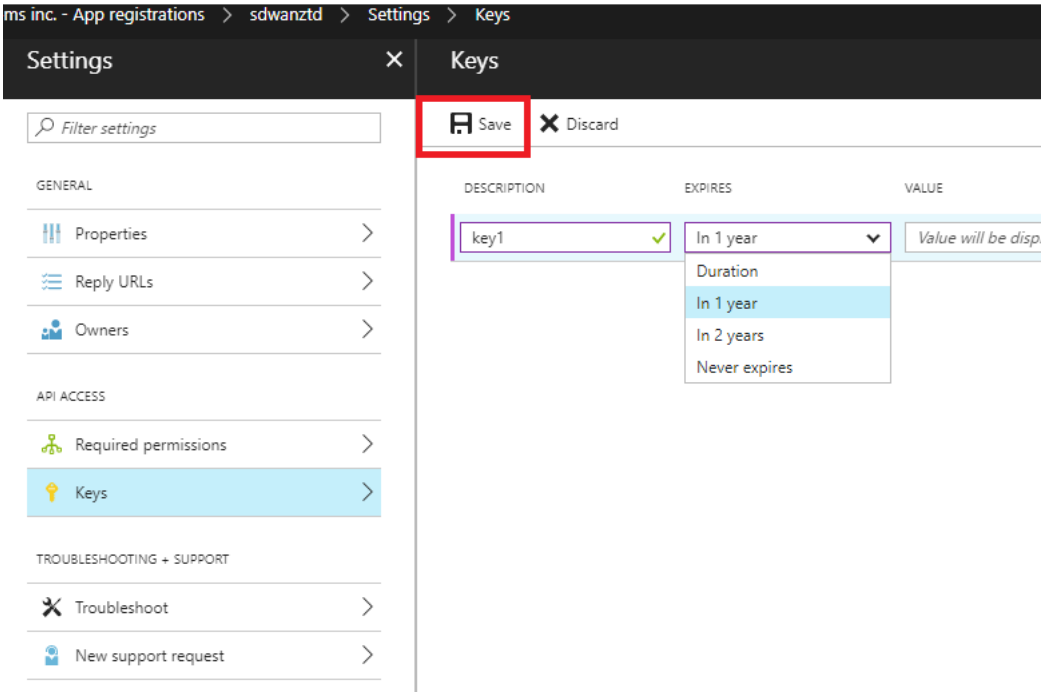
f) 必要なアクセス許可を追加する場合は 、**API** を選択し、**Windows Azure** サービス管理 **API** を強調表示します。



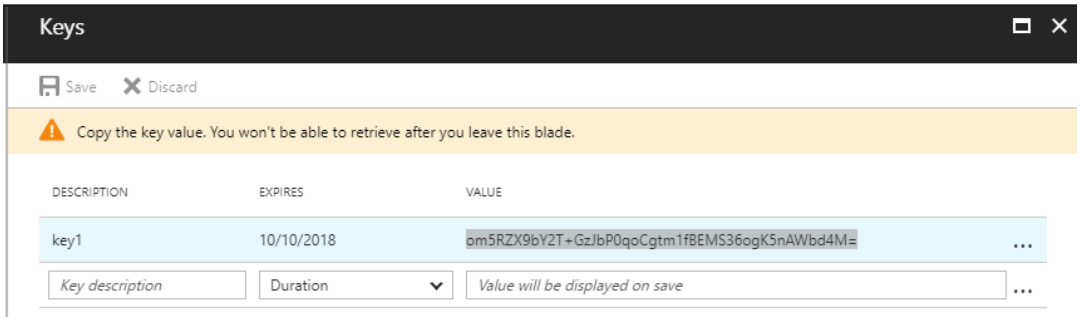
g) 委任権限 を有効にしてインスタンスをプロビジョニングし、[選択 して 完了] をクリックします。



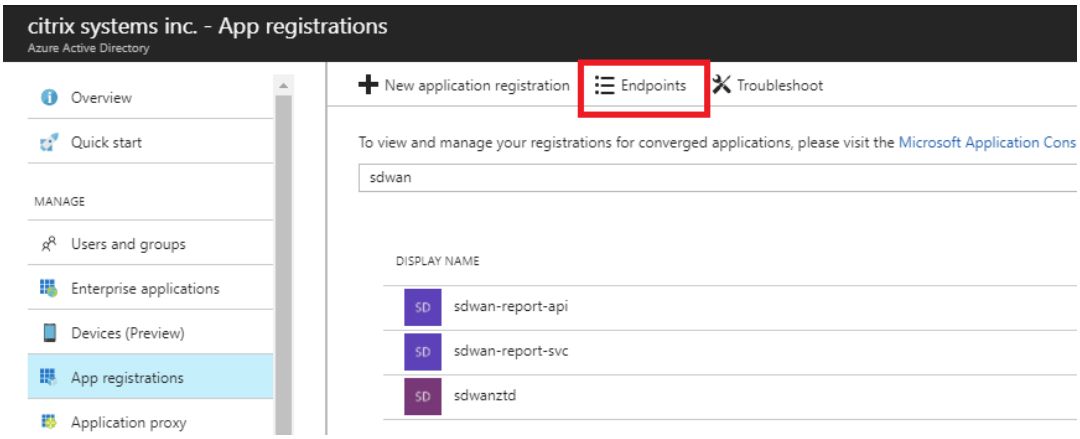
h) この登録済みアプリの場合、[API アクセス] で [キー] を選択し、秘密キーの説明と、キーが有効になるための必要な期間を作成します。そして、秘密鍵を生成します保存を（インスタンスが使用可能にされた後、キーのみ、それを削除することができ、プロビジョニングプロセスのために必要とされる）をクリックします。**



i) 秘密鍵をコピーして保存します（後でこれを取得することはできません）。

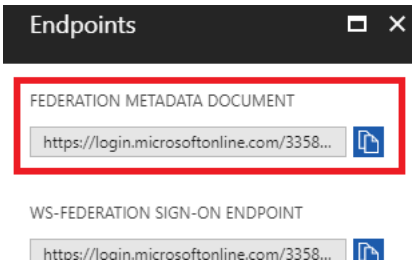


j) 必要なものを特定するには ***Tenant ID*** アプリの登録ペインに戻り、[エンドポイント] を選択します。

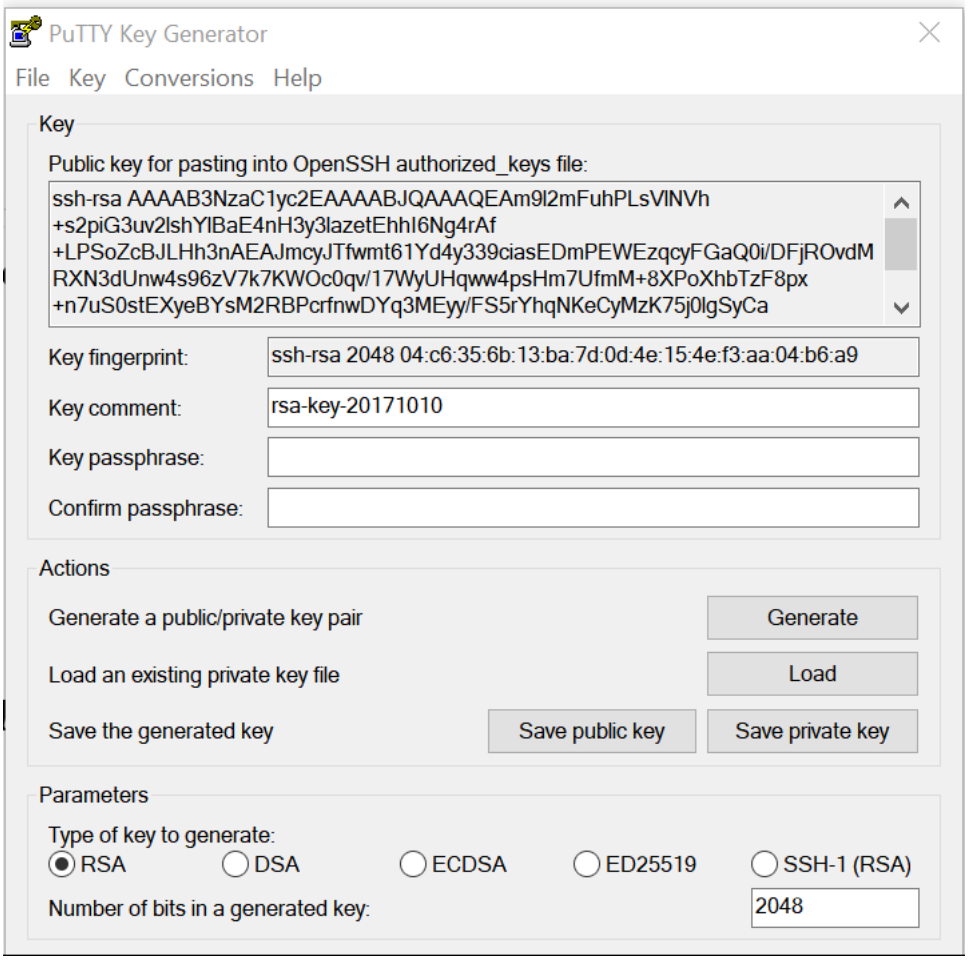


k) フェデレーションメタデータドキュメントをコピーして、テナント ID を識別します（テナント ID

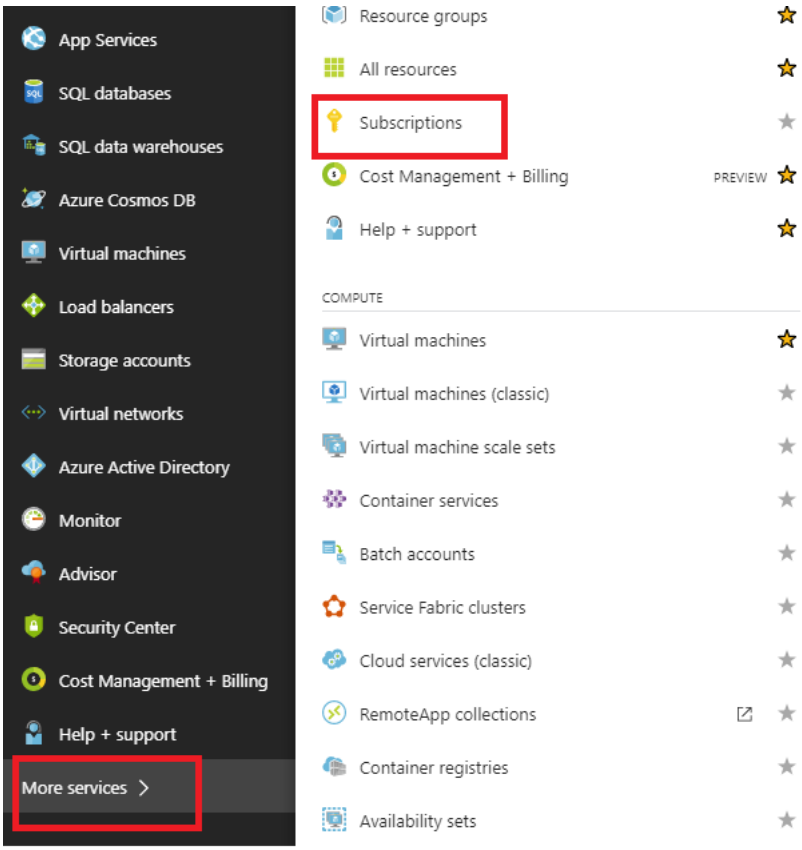
は、“online.com/” そしてその “/federation” URL で)。



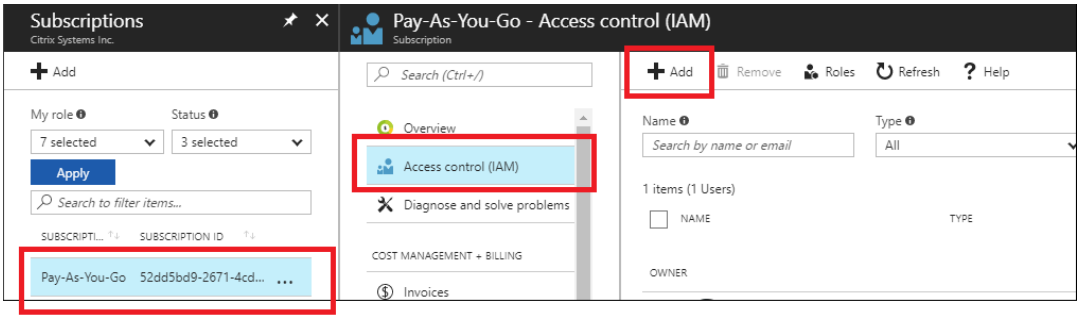
l) 必要な最後の項目は ***SSH*** 公開鍵です。これは、Putty Key Generator または ssh-keygen を使用して作成でき、認証に利用されるため、ログインするためのパスワードが不要になります。SSH 公開鍵をコピーできます（見出し ssh-rsa および末尾の rsa-key 文字列を含む)。この公開鍵は、Citrix Zero Touch Deployment Service への SD-WAN Center 入力を通じて共有されます。



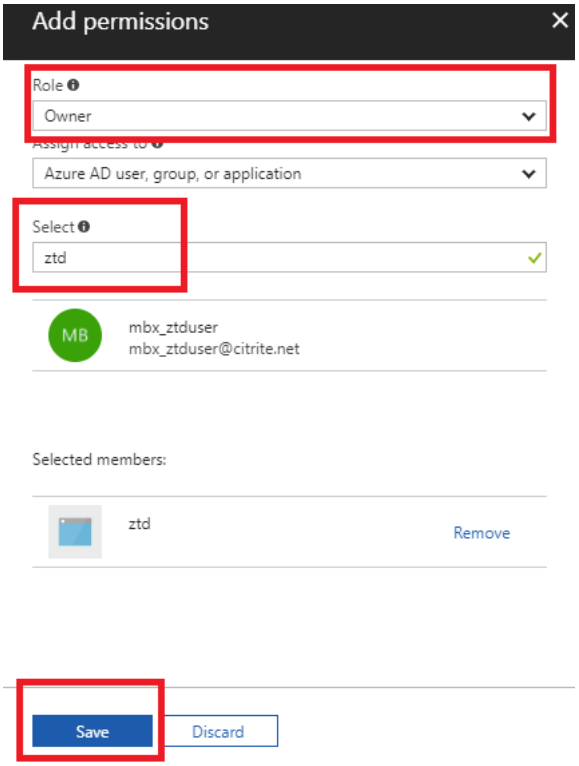
m) アプリケーションにロールを割り当てるには、追加の手順が必要です。[その他のサービス]、[サブスクリプション] に戻ります。



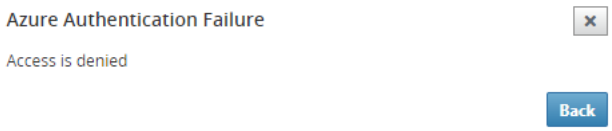
n) アクティブなサブスクリプションを選択し、次に [アクセス制御（**AIM**）] を選択して、[追加] をクリックします。



o) 権限の追加ペインで、「所有者」ロールを選択し、「**Azure AD** ユーザー、グループ、またはアプリケーション」へのアクセスを割り当て、選択フィールド で登録済みアプリを検索して、ゼロタッチ導入クラウドサービスがインスタンスを作成および構成できるようにします。Azure サブスクリプション。アプリが特定されたら、それを選択し、[保存] をクリックする前に、アプリが選択されたメンバーとして読み込まれることを確認します。

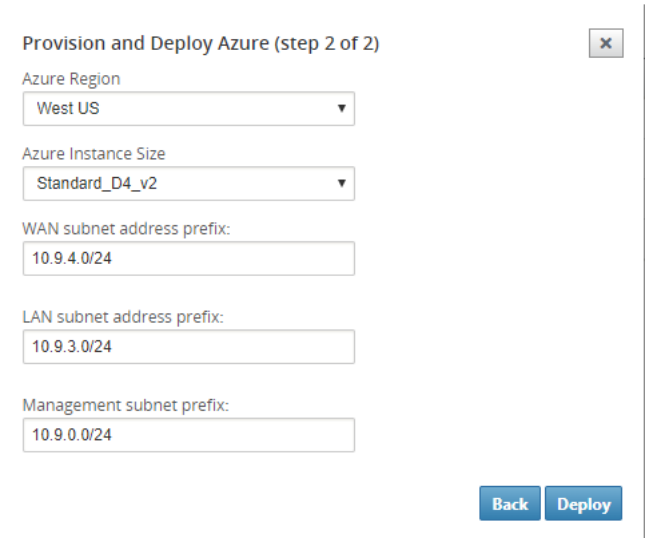


p) 必要な入力を収集して SD-WAN Center に入力したら、[次へ] をクリックします。入力が正しくない場合、認証エラーが発生します。

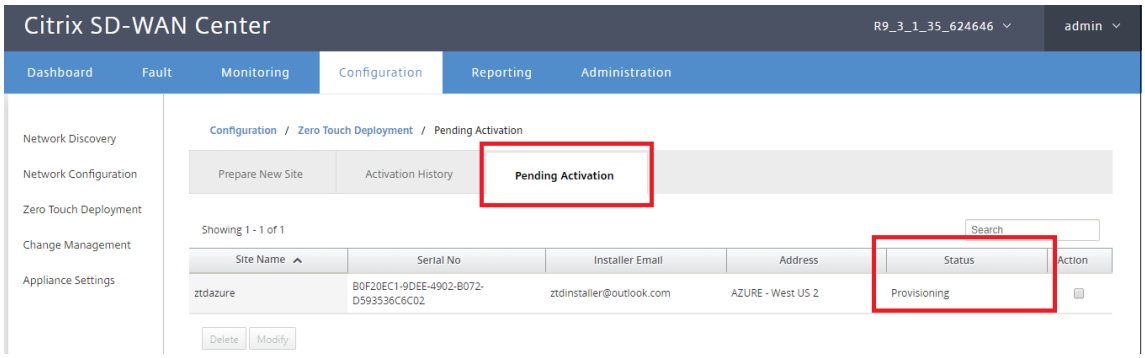


SD-WAN Center での **Azure** のプロビジョニングと展開（ステップ **2/2**）

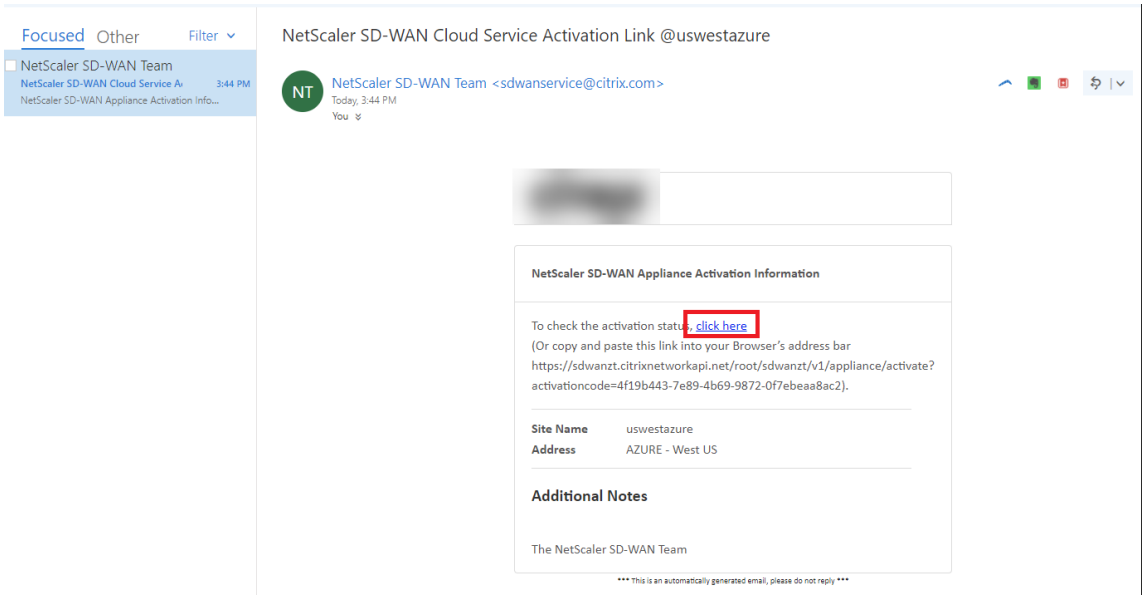
1. Azure 認証が成功したら、適切なフィールドにデータを入力して、目的の Azure リージョンと適切なインスタンスサイズを選択し、[デプロイ] をクリックします。



2. SD-WAN Center の [アクティブ化を保留中] タブに移動すると、展開の現在のステータスを追跡できます。

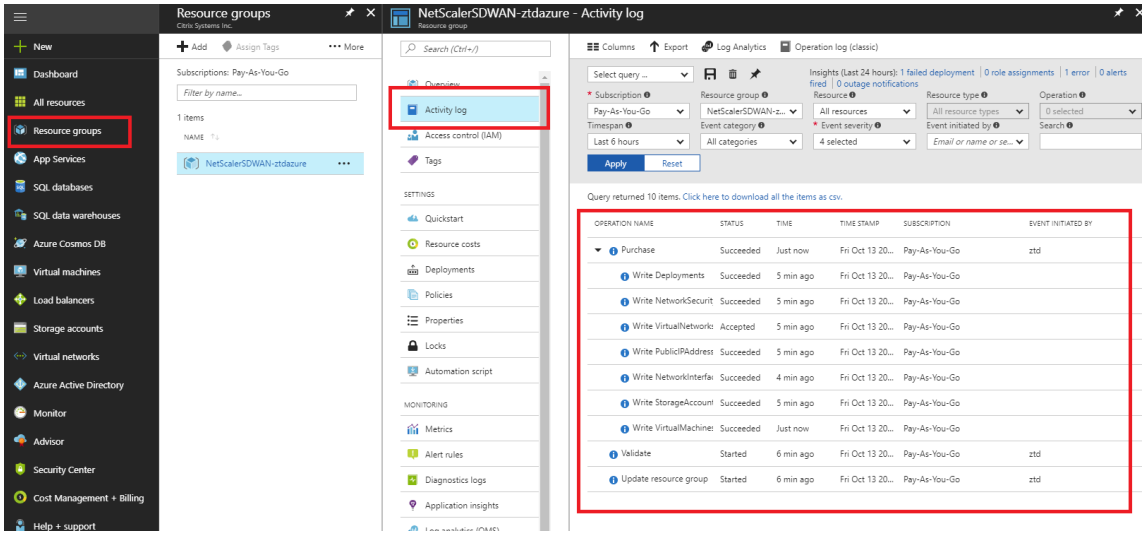


3. 手順 1 で入力したメールアドレスにアクティベーションコードが記載されたメールが配信されます。メールを取得し、アクティベーション **URL** を開いてプロセスをトリガーし、アクティベーションステータスを確認します。

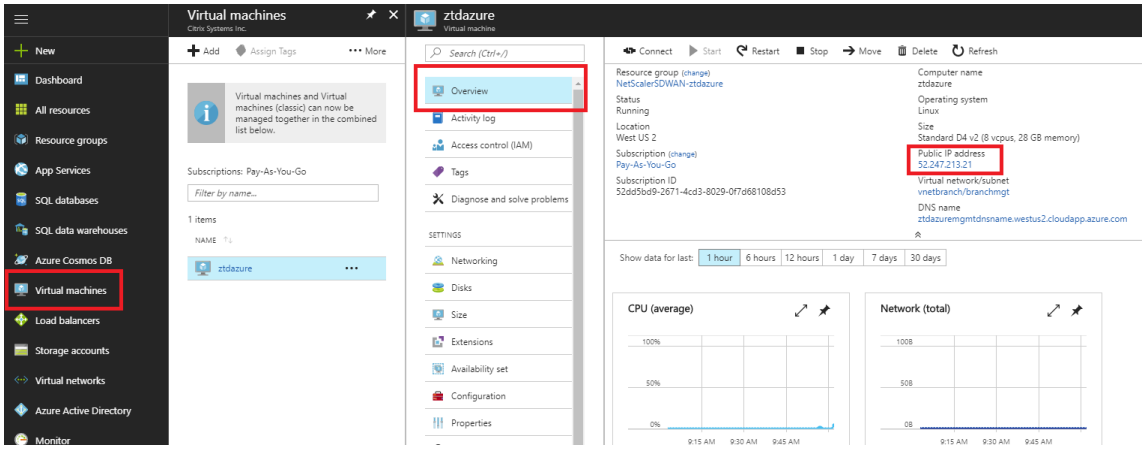


4. 手順 1 で入力したメールアドレスにアクティベーション URL が記載されたメールが届きます。電子メールを取得し、アクティベーション **URL** を開いてプロセスをトリガーし、アクティベーションステータスを確認します。

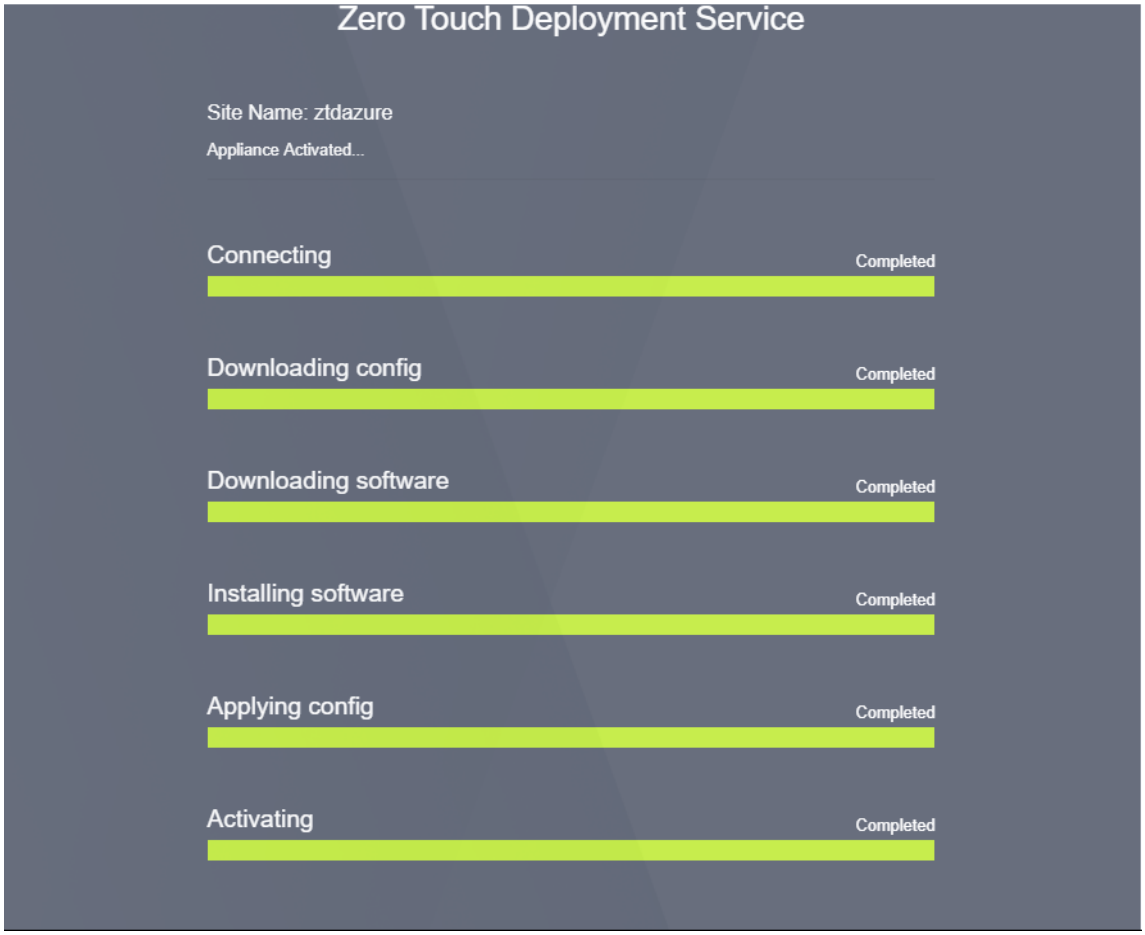
5. SD-WAN クラウドサービスによってインスタンスがプロビジョニングされるまで数分かかります。自動的に作成される リソースグループのアクティビティログ で、Azure ポータルのアクティビティを監視できます。プロビジョニングに関する問題やエラーはここに入力され、アクティベーションステータスで SD-WAN Center に複製されます。



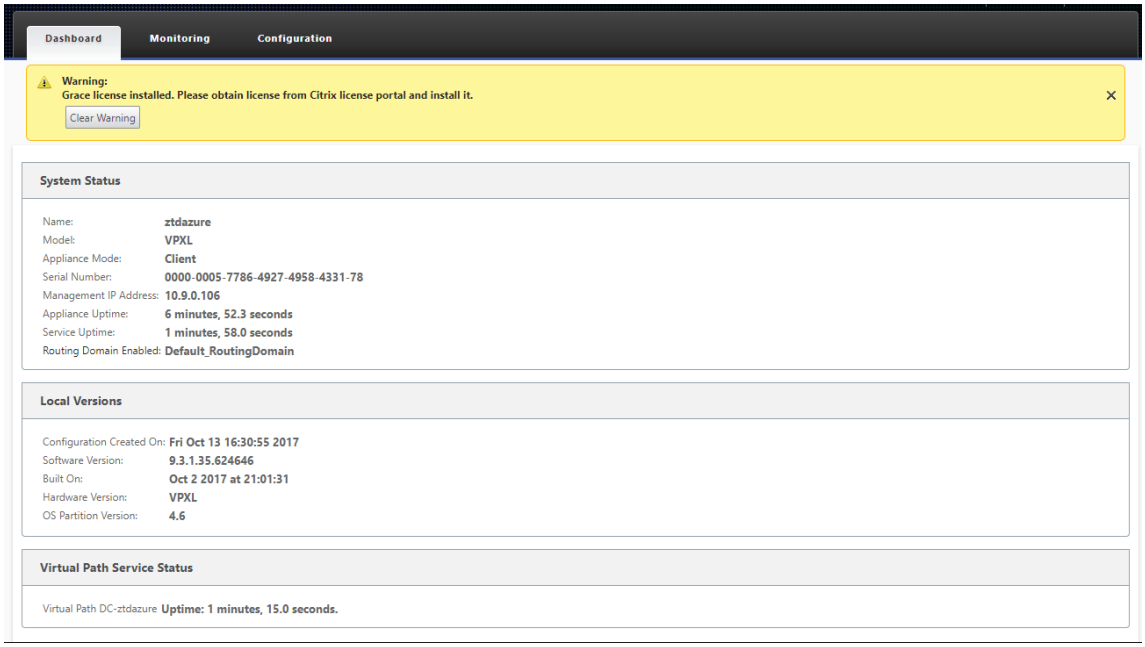
6. Azure ポータルでは、正常に起動されたインスタンスが 仮想マシンで利用できるようになります。割り当てられたパブリック IP を取得するには、インスタンスの概要に移動します。



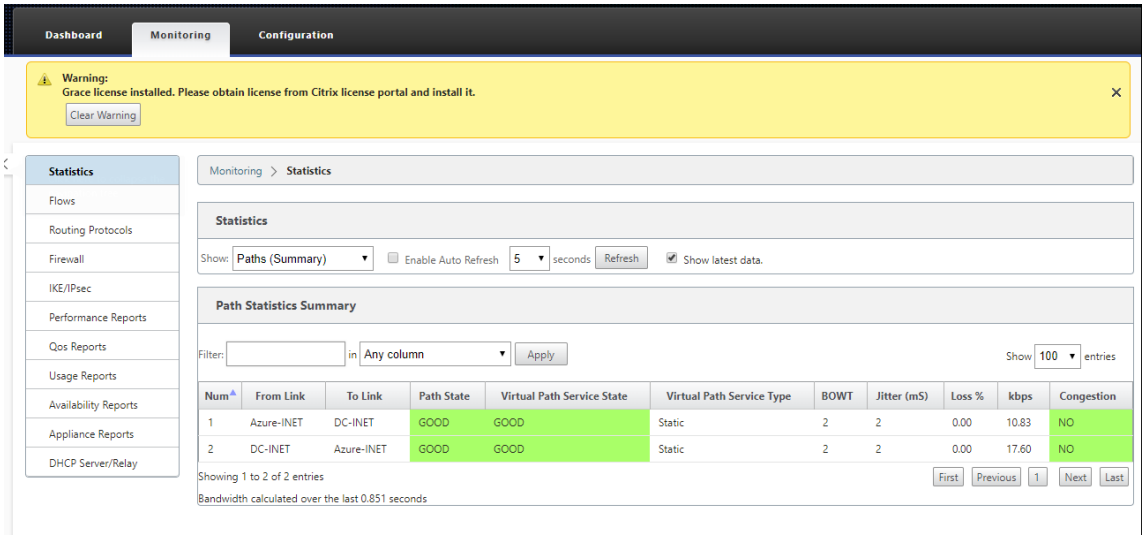
7. VM が実行状態になった後、サービスが到達し、構成、ソフトウェア、およびライセンスのダウンロードプロセスを開始するまでに 1 分かかります。



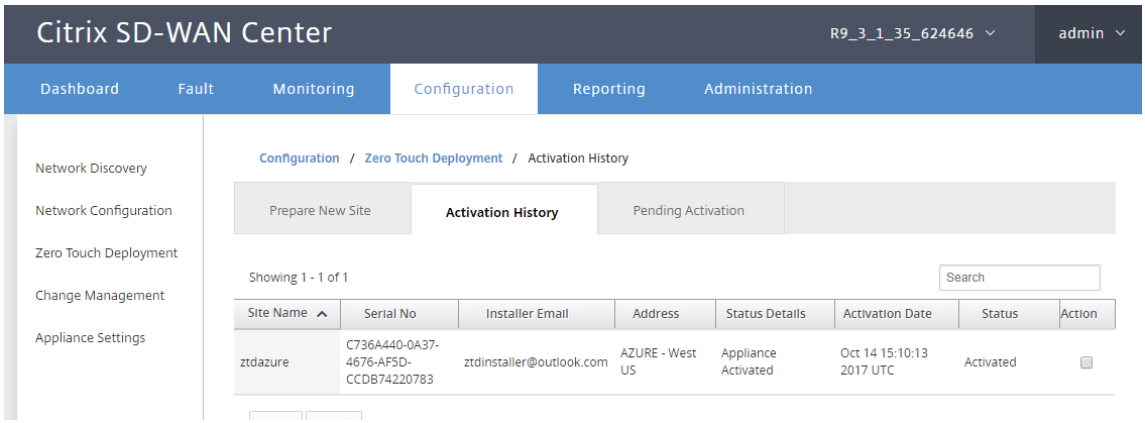
8. SD-WAN クラウドサービスの各手順が自動的に複雑になった後、Azure ポータルから取得したパブリック IP を使用して SD-WAN インスタンスの Web インターフェイスにログインします。



9. Citrix SD-WAN 監視統計ページでは、MCN から Azure の SD-WAN インスタンスへの接続が成功したことが示されます。



10. さらに、Provisioning の成功（または失敗）は、SD-WAN Center の [アクティベーション履歴] ページに記録されます。



ゼロタッチ展開のプロキシサーバー設定

April 13, 2021

ゼロタッチ展開の前提条件として、Citrix SD-WAN Center をインターネットに接続する必要があります。Citrix SD-WAN Center が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は、Citrix SD-WAN Center でプロキシサーバー設定を構成する必要があります。

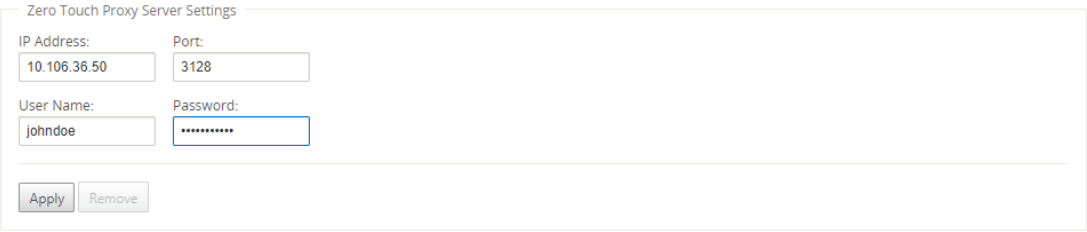
> 注
>
> このプロキシサーバー設定は、ゼロタッチ展開でのみ使用されます。

ゼロタッチプロキシサーバーの設定を構成するには:

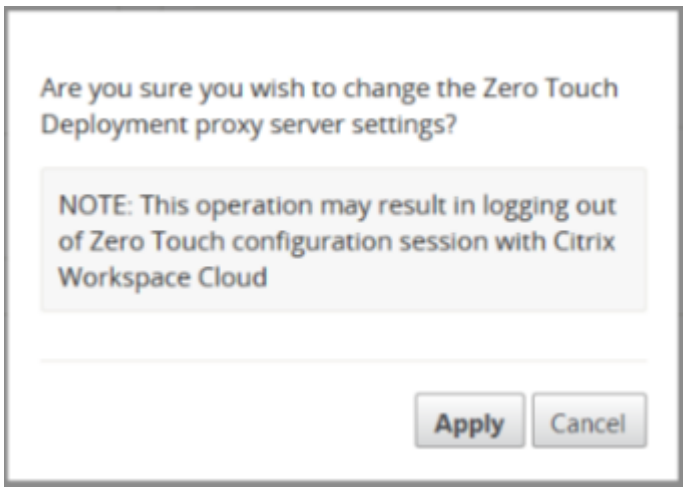
1. SD-WAN Center の Web インターフェイスで、[管理]> 全体設定 > 管理インターフェースに移動します。
2. [ゼロタッチプロキシサーバーの設定] セクションで、次のフィールドに値を入力します。

   - **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構成されていない場合は、[ユーザー名 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] をクリックすると、確認ダイアログボックスが表示されます。

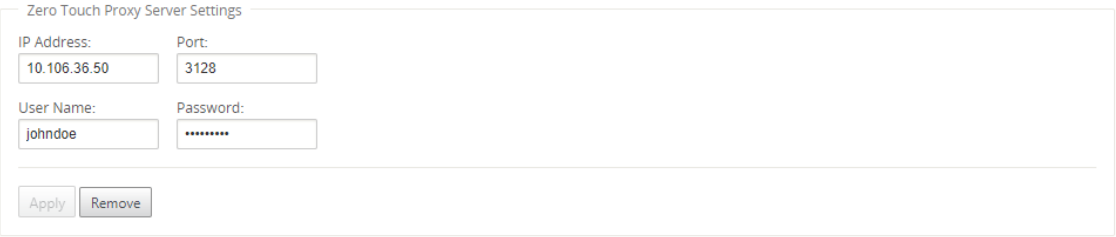


4. [**Apply**] をクリックします。

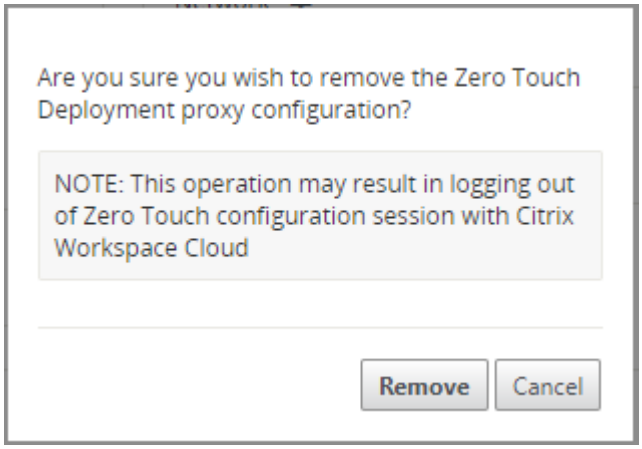
> 注
>
> Citrix SD-WAN Center がインターネットに直接接続されている場合は、プロキシサーバーの設定を完全に削除できます。必要に応じて、プロキシサーバーの設定を削除し、別のプロキシサーバーを構成することもできます。

プロキシサーバーの設定を削除するには:

1. Citrix SD-WAN Center Web インターフェイスで、管理 > 全体設定 > 管理インターフェース に移動します。
2. [ゼロタッチプロキシサーバーの設定] セクションで、[削除] をクリックします。



3. [削除] をクリックすると、確認ダイアログボックスが表示されます。



4. [削除] をクリックします。

パロアルトネットワーク統合

April 13, 2021

パロアルトネットワークは、リモートネットワークを保護するためのクラウドベースのセキュリティインフラストラクチャを提供します。組織が SD-WAN ファブリックを保護する地域的なクラウドベースのファイアウォールをセットアップできるようにすることで、セキュリティを提供します。

リモートネットワーク用の Prisma Access サービスを使用すると、リモートネットワークロケーションをオンボードし、ユーザーにセキュリティを提供できます。すべてのリモートロケーションでのデバイスの設定と管理の複雑さを取り除きます。このサービスは、新しいリモートネットワークの場所を簡単に追加して運用上の課題を最小限に抑える効率的な方法を提供し、これらの場所のユーザーが常に接続されて安全であることを保証します。また、Panorama からポリシーを一元管理して、リモートネットワークの一貫した合理的なセキュリティを実現できます。場所。

リモートネットワークロケーションを Prisma Access サービスに接続するには、Palo Alto Networks 次世代ファイアウォール、またはサービスへの IPsec トンネルを確立できる
SD-WAN を含むサードパーティの IPSec 準拠デバイスを使用できます。

- リモートネットワーク用の Prisma アクセスサービスを計画する
- リモートネットワーク用の Prisma Access サービスの構成
- 設定インポートを備えたオンボードリモートネットワーク

Citrix SD-WAN ソリューションは、ブランチからのインターネットトラフィックを分割する機能をすでに提供しています。これは、各ブランチでの高価なセキュリティスタックの導入を回避しながら、より信頼性が高く、待機時間の短いユーザーエクスペリエンスを提供するために重要です。Citrix SD-WAN と Palo Alto Networks は、分散企業に、ブランチ内のユーザーをクラウド内のアプリケーションに接続するためのより信頼性が高く安全な方法を提供します。

Citrix SD-WAN アプライアンスは、最小限の構成で SD-WAN アプライアンスの場所から IPsec トンネルを介して Palo Alto クラウドサービス（Prisma Access Service）ネットワークに接続できます。あなたは、Citrix SD-WAN Center でパロアルトネットワークを構成することができます.

リモートネットワーク用の Prisma Access Service の構成を開始する前に、サービスを正常に有効にしてリモートネットワークの場所のユーザーにポリシーを適用できるように、次の構成の準備ができていることを確認してください。

1. サービス接続—ユーザーを認証するため、または重要なネットワーク資産へのアクセスを可能にするために、リモートネットワークロケーションが本社のインフラストラクチャにアクセスする必要がある場合は、本社とリモートネットワークロケーションが接続されるように企業ネットワークへのアクセスを設定する必要があります。

リモートネットワークの場所が自律的で、他の場所にあるインフラストラクチャにアクセスする必要がない場合は、サービス接続を設定する必要はありません（モバイルユーザーがアクセスを必要とする場合を除く）。

1. テンプレート—Prisma Access サービスは自動的にテンプレートスタックを作成します (Remote_Network_Template_Stack) そしてトップレベルのテンプレート (Remote_Network_Template) リモートネットワーク用の Prisma Access サービス用。リモートネットワーク用の Prisma アクセスサービスを構成するには、最上位のテンプレートを最初から構成するか、既存の Palo Alto Networks ファイアウォールを既にオンプレミスで実行している場合は既存の構成を利用します。

   テンプレートには、リモートネットワークの場所とリモートネットワーク用の Prisma Access サービス、セキュリティポリシーで参照できるゾーン、およびログ転送プロファイル間のプロトコルネゴシエーションのための IPsec トンネルとインターネットキーエクスチェンジ（IKE）構成を確立するための設定が必要です。リモートネットワークの Prisma Access サービスからログサービスにログを転送できること。

2. 親デバイスグループ—リモートネットワークの Prisma Access サービスでは、セキュリティポリシー、セキュリティプロファイル、およびその他のポリシーオブジェクト（アプリケーショングループとオブジェクト、アドレスグループなど）、および認証ポリシーを含む親デバイスグループを指定する必要がありますそのた

め、リモートネットワークの Prisma Access サービスは、IPsec トンネルを介してリモートネットワークの Prisma Access サービスにルーティングされるトラフィックのポリシーを一貫して適用できます。パノラマでポリシールールとオブジェクトを定義するか、既存のデバイスグループを使用してリモートネットワークの場所でユーザーを保護する必要があります。

> 注:
>
> ゾーンを参照する既存のデバイスグループを使用する場合は、ゾーンを定義する対応するテンプレートを Remote_Network_Template_Stack に追加してください。

これにより、Prisma Access Service for Remote Networks を構成するときにゾーンマッピングを完了することができます。

3. **IP** サブネット—Prisma Access サービスがトラフィックをリモートネットワークにルーティングするためには、Prisma Access サービスを使用して保護するサブネットワークのルーティング情報を提供する必要があります。リモートネットワークの場所で各サブネットワークへの静的ルートを定義するか、サービス接続場所と Prisma Access サービスの間に BGP を構成するか、両方の方法を組み合わせて使用できます。

   スタティックルートを設定し、BGP を有効にすると、スタティックルートが優先されます。リモートネットワークの場所にいくつかのサブネットワークしかない場合は静的ルートを使用すると便利な場合がありますが、サブネットが重複している多くのリモートネットワークがある大規模な展開では、BGP を使用するとより簡単にスケーリングできます。

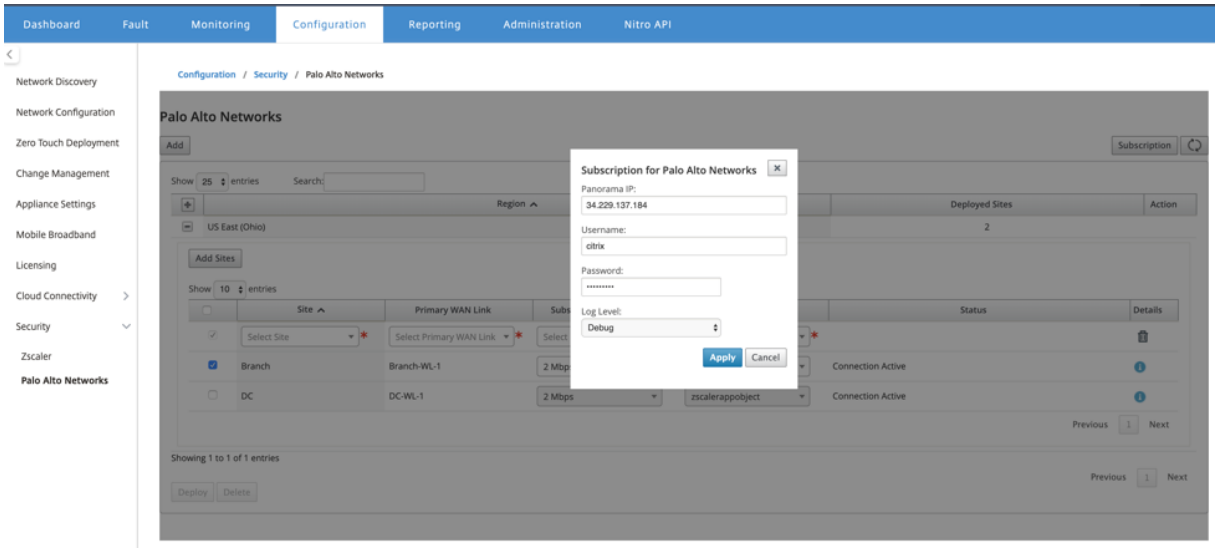
SD-WAN Center の Palo Alto Networks

以下の前提条件が満たされていることを確認してください。

- PRISMA ACCESS サービスからパノラマ IP アドレスを取得します。
- PRISMA ACCESS サービスでユーザー名とパスワードを取得します。
- SD-WAN アプライアンス GUI で IPsec トンネルを構成します。
- サイトが Citrix-IKE-Crypto-Default/Citrix-IPSec-Crypto-Default 以外の ike/ipsec プロファイルで構成された異なるサイトのあるリージョンにオンボーディングされていないことを確認してください。
- SD-WAN Center によって設定が更新されるときに、Prisma Access の設定を手動で変更しないようにしてください。

Citrix SD-WAN Center の GUI で、Palo Alto のサブスクリプション情報を入力します。

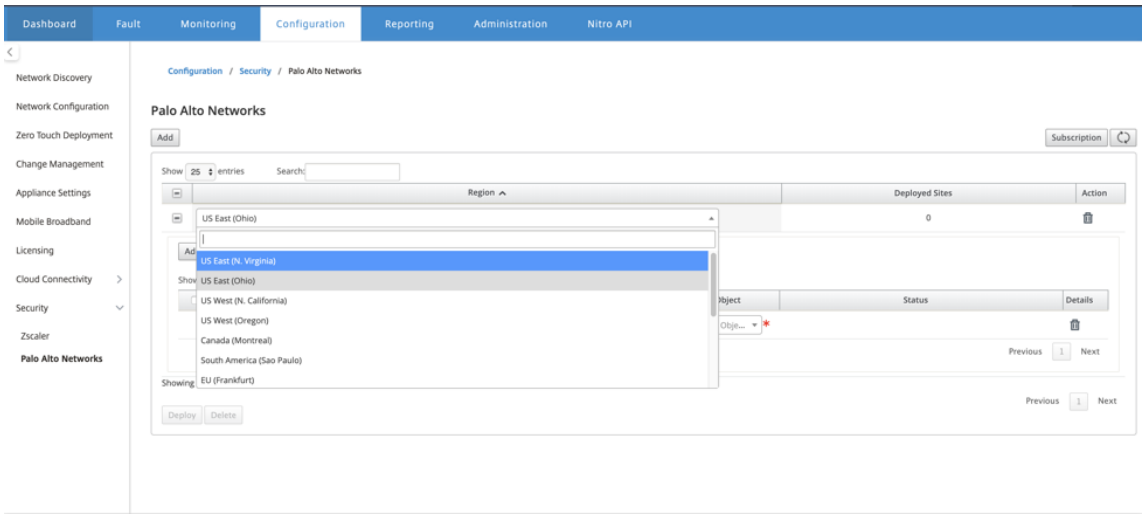
- パノラマ IP アドレスを設定します。この IP アドレスは Palo Alto（PRISMA ACCESS サービス）から取得できます。
- PRISMA ACCESS サービスで使用するユーザー名とパスワードを設定します。

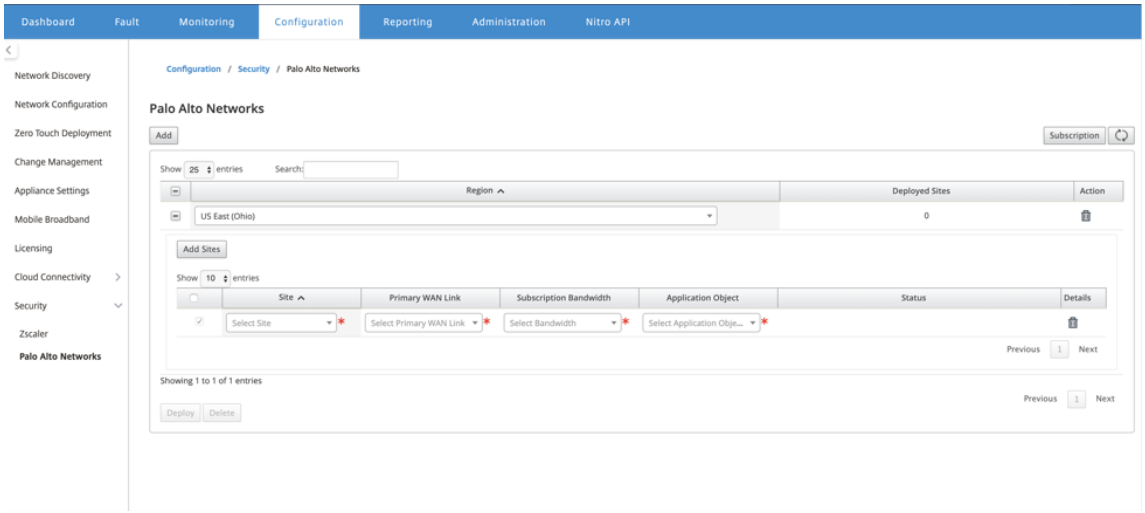


サイトを追加して展開する

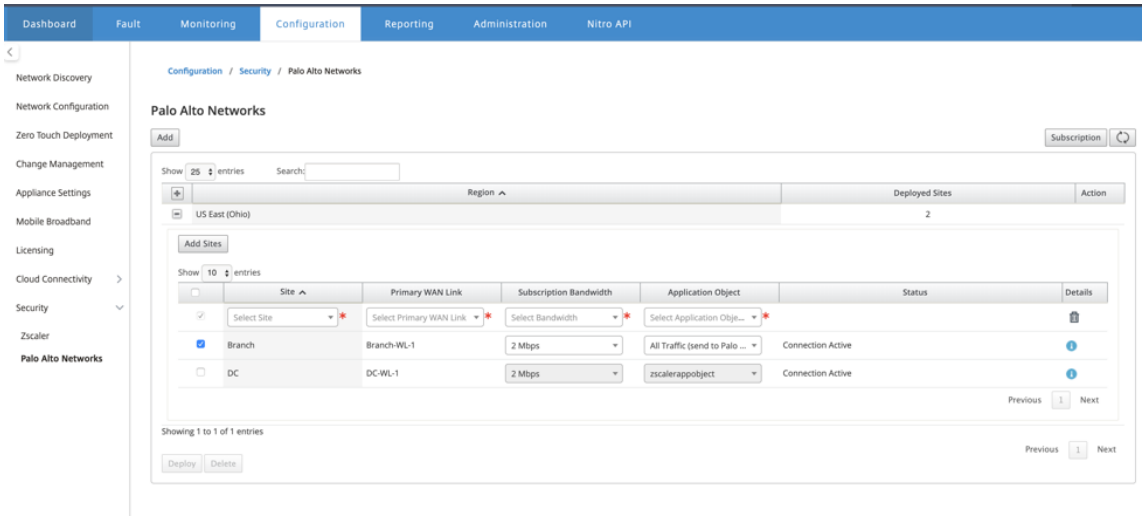
1. サイトをデプロイするには、PRISMA ACCESS ネットワークリージョンと Prisma Access リージョン用に構成する SD-WAN サイトを選択し、サイト WAN リンク、帯域幅、およびトラフィック選択用のアプリケーションオブジェクトを選択します。

   > 注:
   >
   > 選択した帯域幅が使用可能な帯域幅の範囲を超えると、トラフィックフローが影響を受けます。
   >
   > アプリケーションオブジェクトの選択で [すべてのトラフィック] オプションを選択することにより、インターネットにバインドされたすべてのトラフィックを PRISMA ACCESS サービスにリダイレクトすることを選択できます。

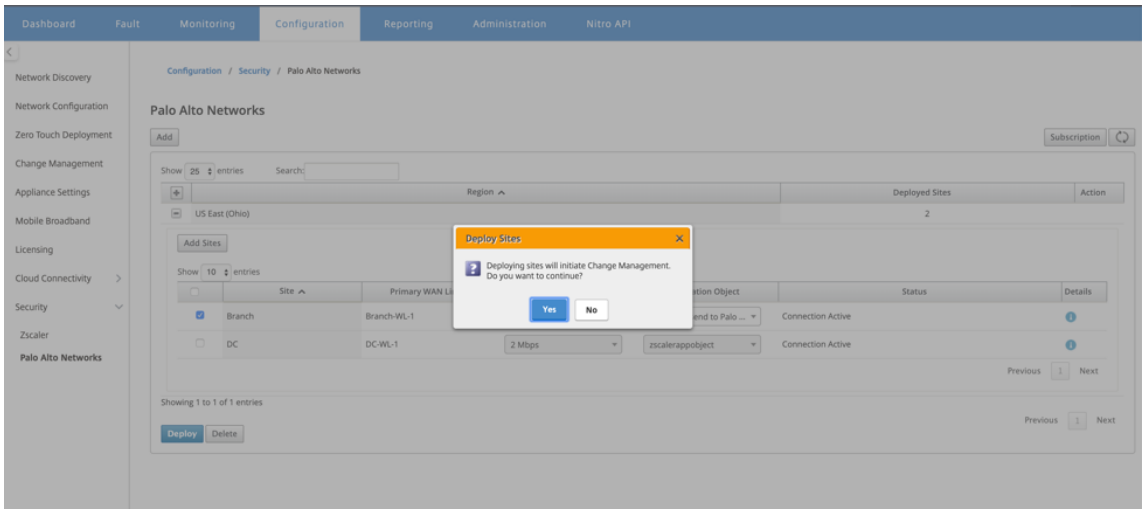




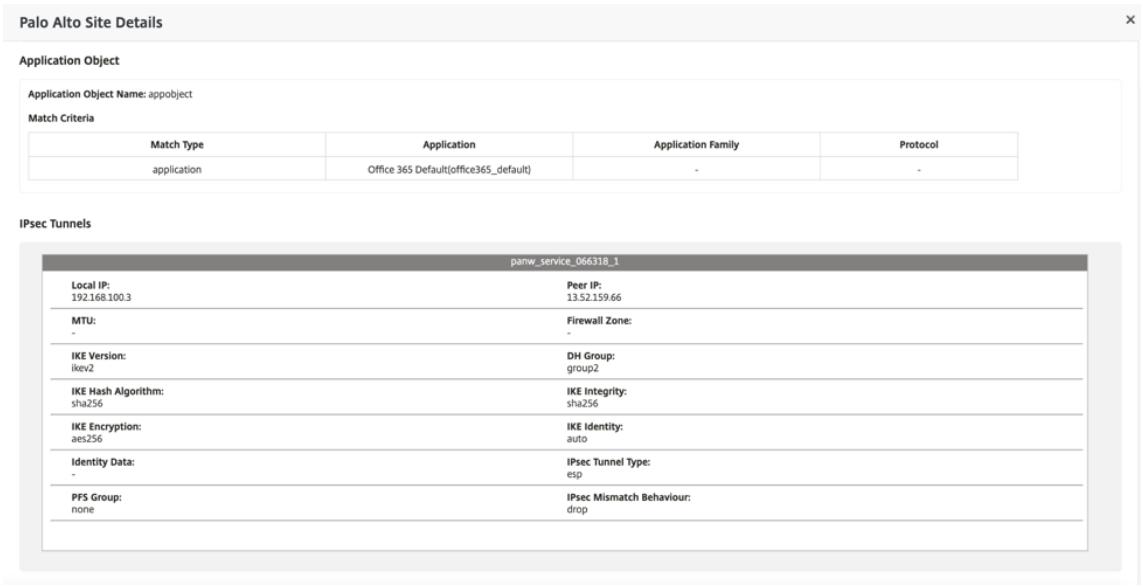
2. 必要に応じて、引き続き SD-WAN ブランチサイトを追加できます。



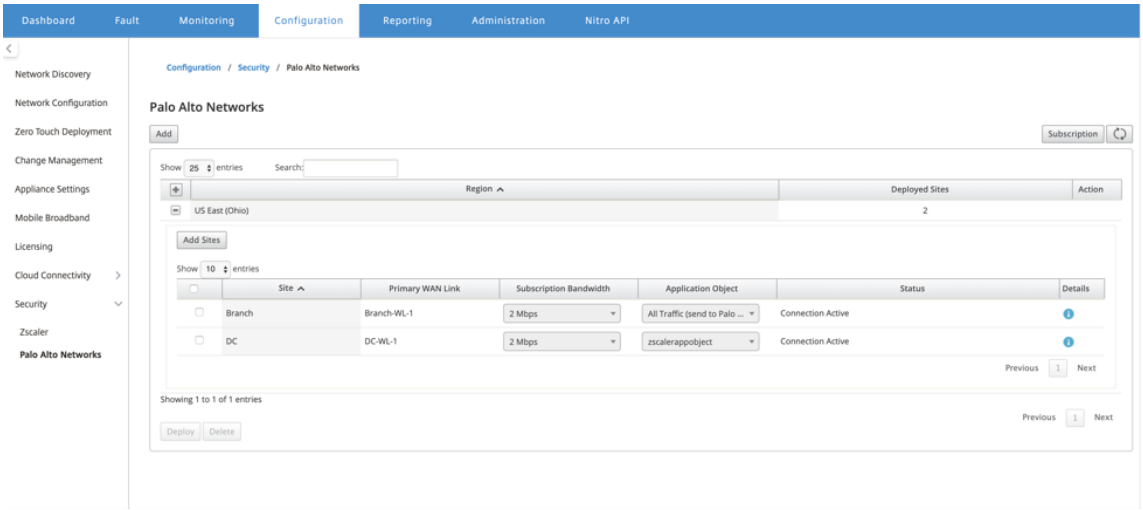
3. [展開] をクリックします。変更管理プロセスが開始されます。[**Yes**] をクリックして続行します。



展開後、トンネルの確立に使用される IPsec トンネル構成は次のとおりです。



ランディングページには、さまざまな SD-WAN リージョンで構成およびグループ化されたすべてのサイトのリストが表示されます。



エンドツーエンドのトラフィック接続を確認します。

- ブランチの LAN サブネットから、インターネットリソースにアクセスします。
- トラフィックが Citrix SD-WAN IPsec トンネルを通過して Palo Alto Prisma Access に到達することを確認します。
- Palo Alto セキュリティポリシーが [監視] タブのトラフィックに適用されていることを確認します。
- ブランチのホストへのインターネットからの応答が到達することを確認します。

Microsoft Azure 仮想 WAN

April 13, 2021

Microsoft Azure Virtual WAN と Citrix SD-WAN は、ハイブリッドクラウドワークロード全体のネットワーク接続と集中管理を簡素化します。ブランチアプライアンスの構成を自動化して Azure WAN に接続し、ビジネス要件に応じてブランチトラフィック管理ポリシーを構成できます。組み込みのダッシュボードインターフェースは、時間を節約し、大規模なサイト間接続の可視性を提供するインスタントトラブルシューティングの洞察を提供します。

Microsoft Azure Virtual WAN を使用すると、Azure Cloud ワークロードへの接続を簡素化し、Azure バックボーンネットワークを越えてトラフィックをルーティングできます。Azure には 54 以上のリージョンがあり、世界中に複数の拠点が存在します。Azure リージョンは、ブランチに接続するために選択できるハブとして機能します。ブランチが接続されたら、ハブ間接続を介して Azure クラウドサービスを使用します。Azure VNET とのハブピアリングを含む複数の Azure サービスを適用することで、接続を簡素化できます。ハブは、ブランチのトラフィックゲートウェイとして機能します。

Microsoft Azure Virtual WAN には次の利点があります。

- ハブアンドスポークの統合接続ソリューション-接続パートナーソリューションを含むさまざまなソースからのオンプレミスと Azure ハブ間のサイト間接続と構成を自動化します。
- 自動セットアップと構成–仮想ネットワークを Azure ハブにシームレスに接続します。
- 直感的なトラブルシューティング–Azure 内のエンドツーエンドのフローを確認し、この情報を使用して必要なアクションを実行できます。

ハブ間通信

11.1.0 リリース以降、Azure 仮想 WAN は、標準 タイプの方法を使用したハブ間通信をサポートしています。

Azure Virtual WAN のお客様は、リージョン間のハブ間通信（グローバルトランジットネットワークアーキテクチャ）に Microsoft のグローバルバックボーンネットワークを活用できるようになりました。これにより、ブランチから Azure、ブランチからブランチへの Azure バックボーン、ブランチからハブ（すべての Azure リージョン）の通信が可能になります。

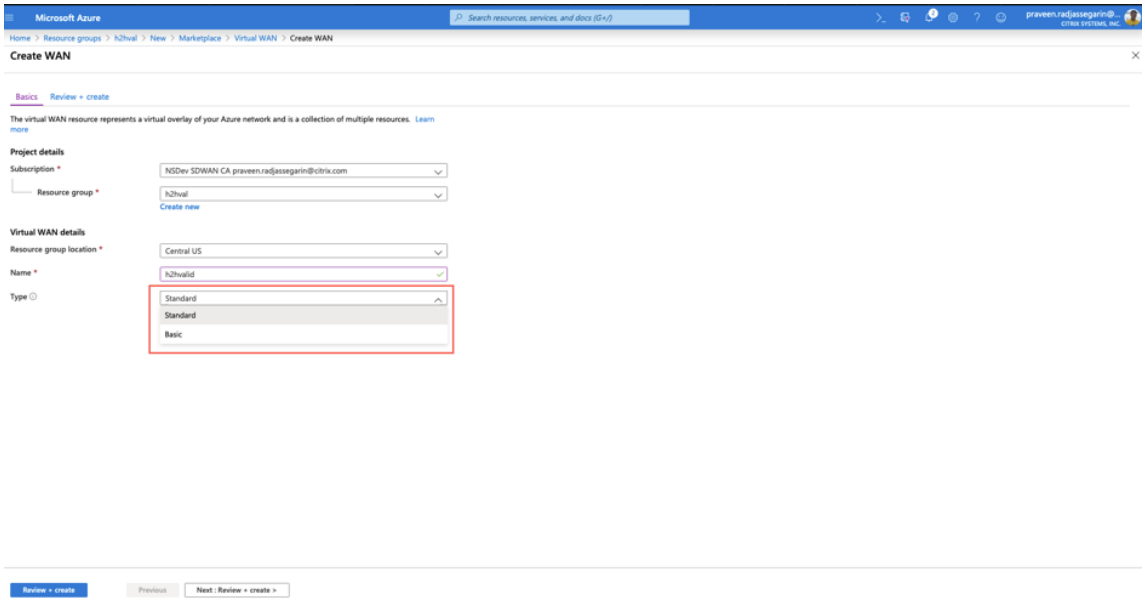
Azure 仮想 WAN 用の標準 SKU を購入した場合にのみ、リージョン間通信に Azure のバックボーンを利用できます。料金の詳細については、「仮想 WAN の料金」を参照してください。Basic SKU では、リージョン間のハブ間通信に Azure のバックボーンを使用できません。詳しくは、「グローバルトランジットネットワークアーキテクチャと仮想 WAN」を参照してください。

ハブはすべて仮想 WAN で相互に接続されています。これは、ローカルハブに接続されたブランチ、ユーザー、または VNet が、接続されたハブのフルメッシュアーキテクチャを使用して別のブランチまたは VNet と通信できることを意味します。

ハブ間接続フレームワークを使用して、仮想ハブを通過するハブ内の VNet、およびハブ間で VNet を接続することもできます。

仮想 WAN には 2 つのタイプがあります。

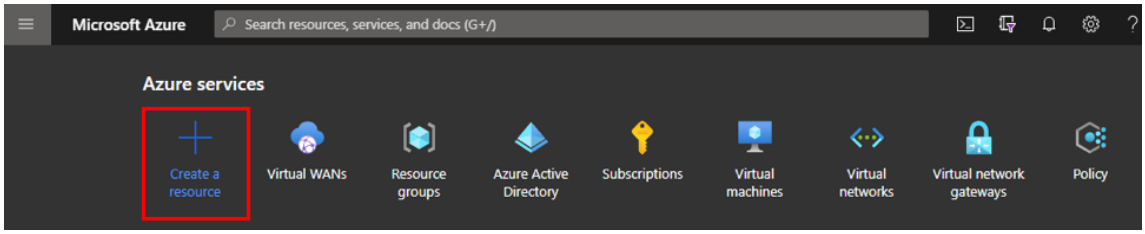
- ベーシック: 基本的な 方法を使用すると、ハブ間の通信は 1 つのリージョン内で行われます。基本的な WAN タイプは、基本的なハブ（SKU = 基本）。基本的なハブは、サイト間 VPN 機能に制限されています。
- 標準: 標準的な 方法を使用すると、ハブ間通信は異なるリージョン間で行われます。標準 WAN は、標準ハブ（SKU の作成に役立ちます = 標準）。標準 ハブには、ExpressRoute、ユーザー VPN（P2S）、フルメッシュハブ、およびハブを介した VNet-to-VNet トランジットが含まれます。



Microsoft Azure で Azure Virtual WAN サービスを作成する

Azure Virtual WAN リソースを作成するには、次の手順を実行します。

1. Azure ポータルにログインし、[リソースの作成] をクリックします。

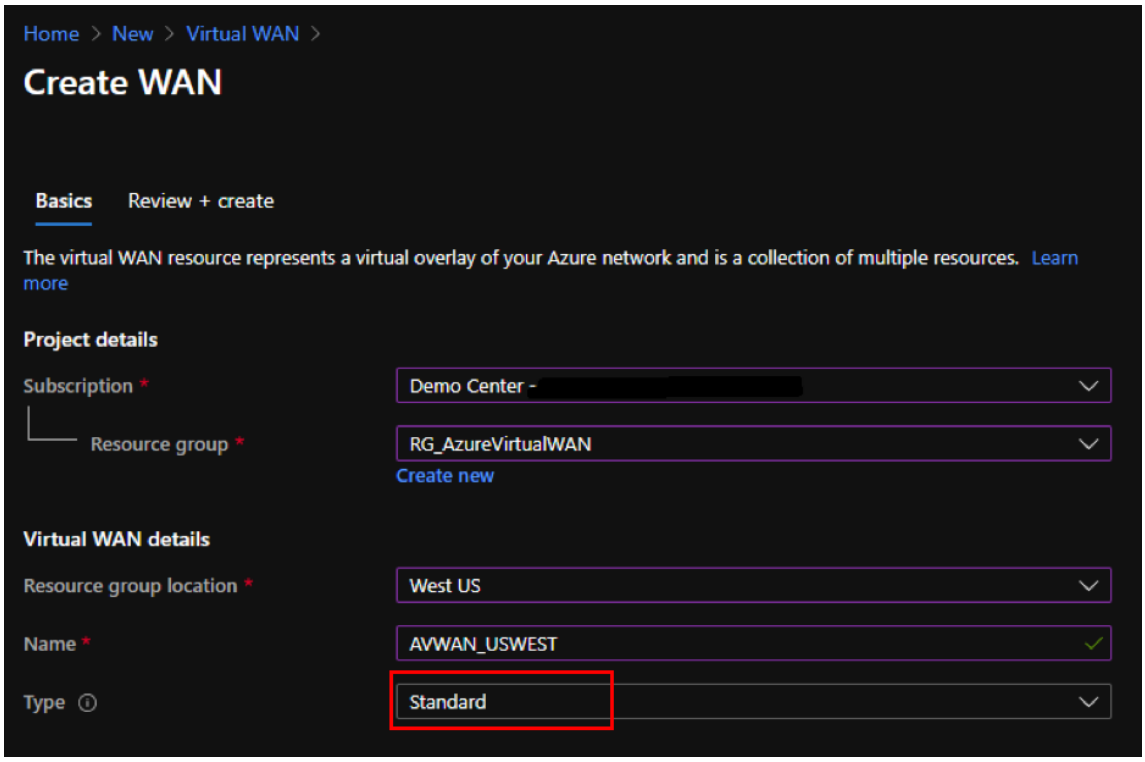


2. 仮想 **WAN** を検索し、[作成] をクリックします。
3. [基本] で、次のフィールドに値を入力します。
    - 申し込み: ドロップダウンリストからサブスクリプションの詳細を選択して提供します。

- リソースグループ: 既存のリソースグループを選択するか、新しいリソースグループを作成します。

  > 注
  >
  > Azure API 通信を許可するサービスプリンシパルを作成するときは、仮想 WAN を含む同じリソースグループを使用するようにしてください。そうしないと、SD-WAN オーケストレーターには、自動接続を可能にする Azure Virtual WAN API を認証するための十分な権限がありません。

- リソースグループの場所: ドロップダウンリストから Azure リージョンを選択します。
- 名前: 新しい仮想 WAN の名前を入力します。
- タイプ: 異なるリージョン間でハブ間通信を使用する場合は [標準] タイプを選択し、それ以外の場合は [基本] を選択します。



4. 確認と作成をクリックします。
5. 仮想 WAN を作成するために入力した詳細を確認し、[作成] をクリックして仮想 WAN の作成を完了します。

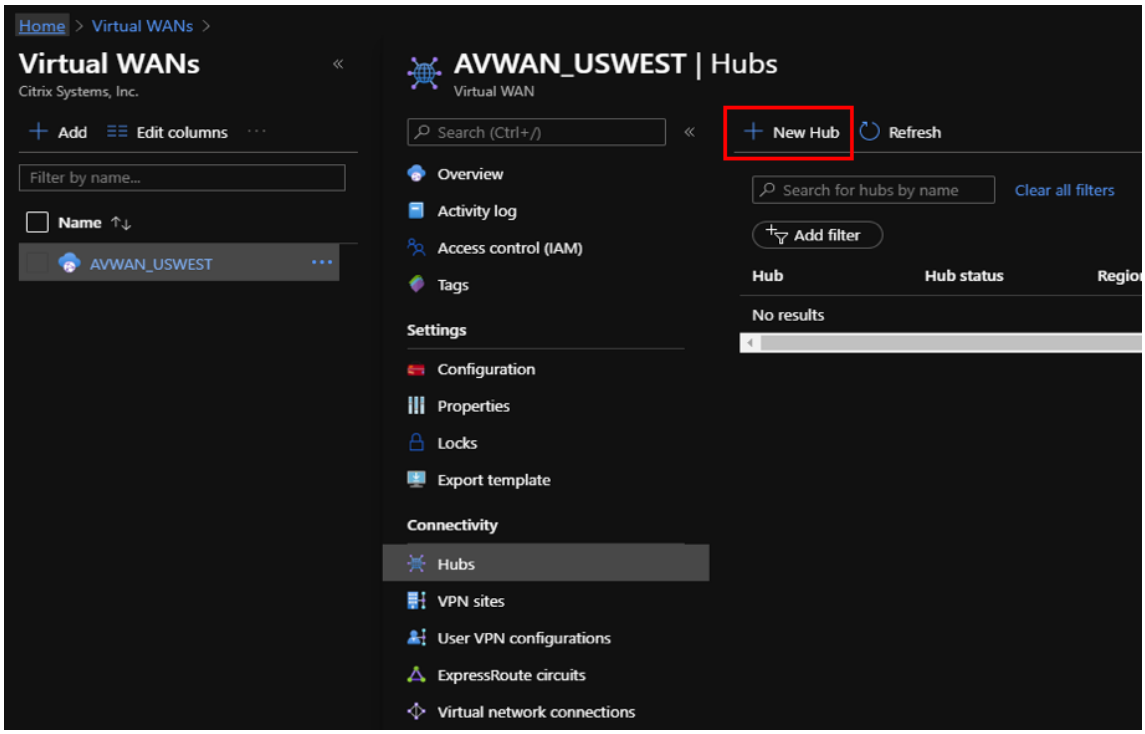
リソースのデプロイには 1 分もかかりません。

> 注意
>
> 基本から標準にアップグレードできますが、標準から基本に戻すことはできません。仮想 WAN をアップグレードする手順については、仮想 WAN を基本から標準にアップグレードするを参照してください。

Azure Virtual WAN でハブを作成する

次の手順を実行して、さまざまなエンドポイント（オンプレミス VPN デバイス、SD-WAN デバイスなど）からの接続を可能にするハブを作成します。

1. 以前に作成した Azure Virtual WAN を選択します。
2. [接続] セクションで [ハブ] を選択し、+ 新しいハブ。

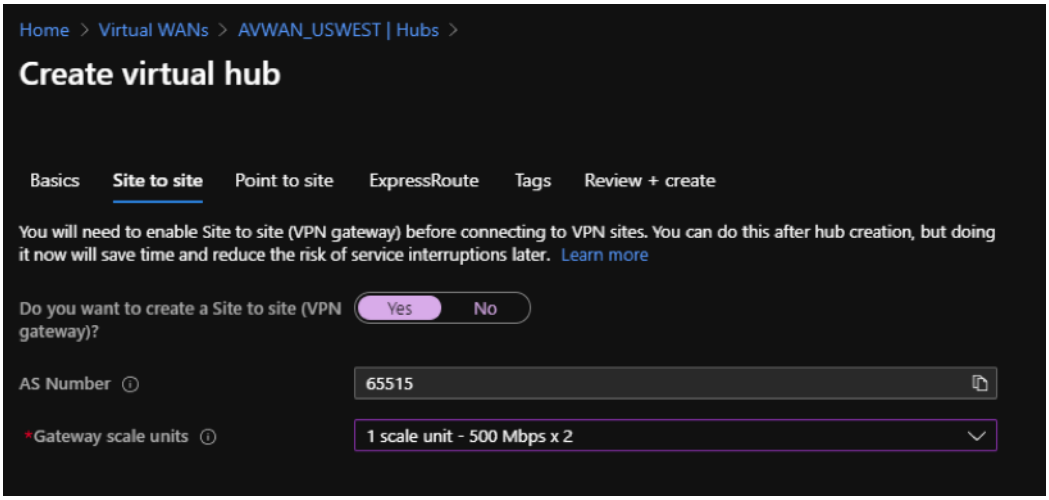


3. [基本] で、次のフィールドに値を入力します。

   - リージョン–ドロップダウンリストから Azure リージョンを選択します。
   - 名前–新しいハブの名前を入力します。
   - ハブのプライベートアドレススペース–CIDR にアドレス範囲を入力します。ハブ専用の一意のネットワークを選択してください。

4. [次へ] を クリックします: サイト間 > 次のフィールドに値を入力します。

   - サイト間（**VPN** ゲートウェイ）を作成しますか?–はいを選択します。
   - **Gateway** スケール単位–必要に応じて、ドロップダウンリストからスケール単位を選択します。



5. 確認と作成をクリックします。
6. 設定を確認し、[作成] をクリックして仮想 HUB の作成を開始します。

リソースのデプロイには最大 30 分かかる場合があります。

Azure Virtual WAN のサービスプリンシパルを作成し、**ID** を特定する

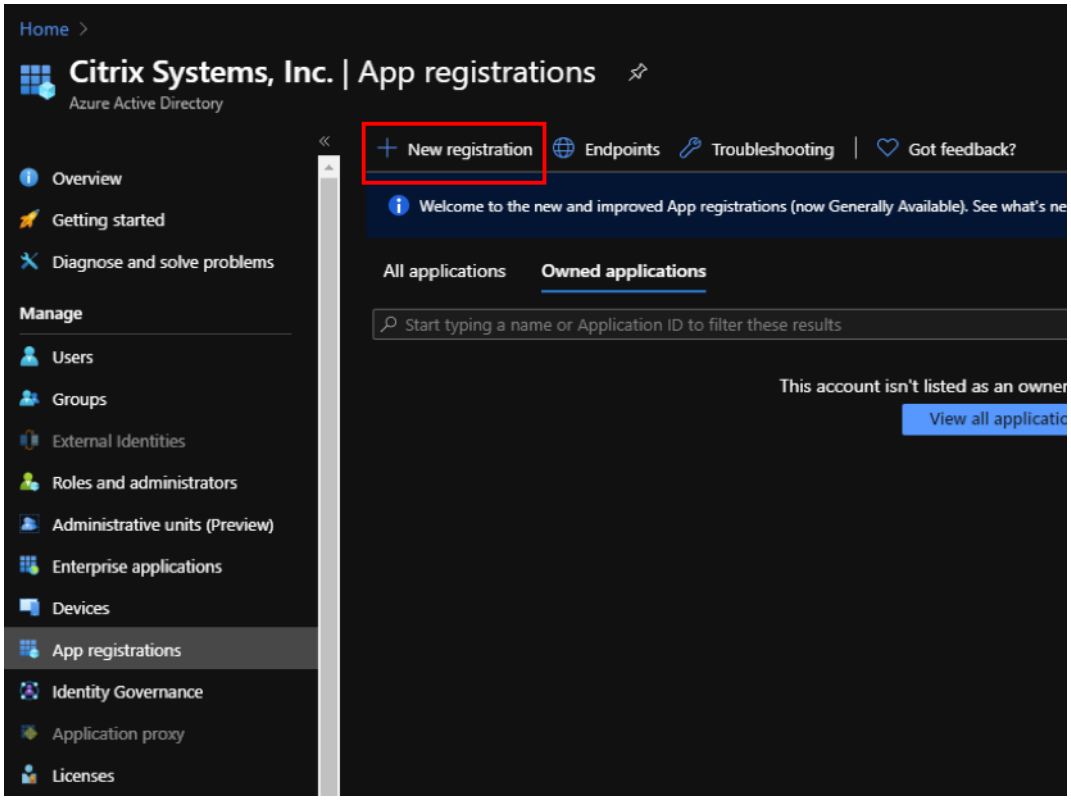
SD-WAN オーケストレーターが Azure Virtual WAN API を介して認証し、自動接続を有効にするには、登録されたアプリケーションを作成して、次の認証資格情報で識別する必要があります。

- サブスクリプション ID
- クライアント ID
- クライアントシークレット
- テナント ID

> 注
>
> Azure API 通信を許可するサービスプリンシパルを作成するときは、仮想 WAN を含む同じリソースグループを使用するようにしてください。そうしないと、SD-WAN オーケストレーターには、自動接続を可能にする Azure Virtual WAN API を認証するための十分な権限がありません。

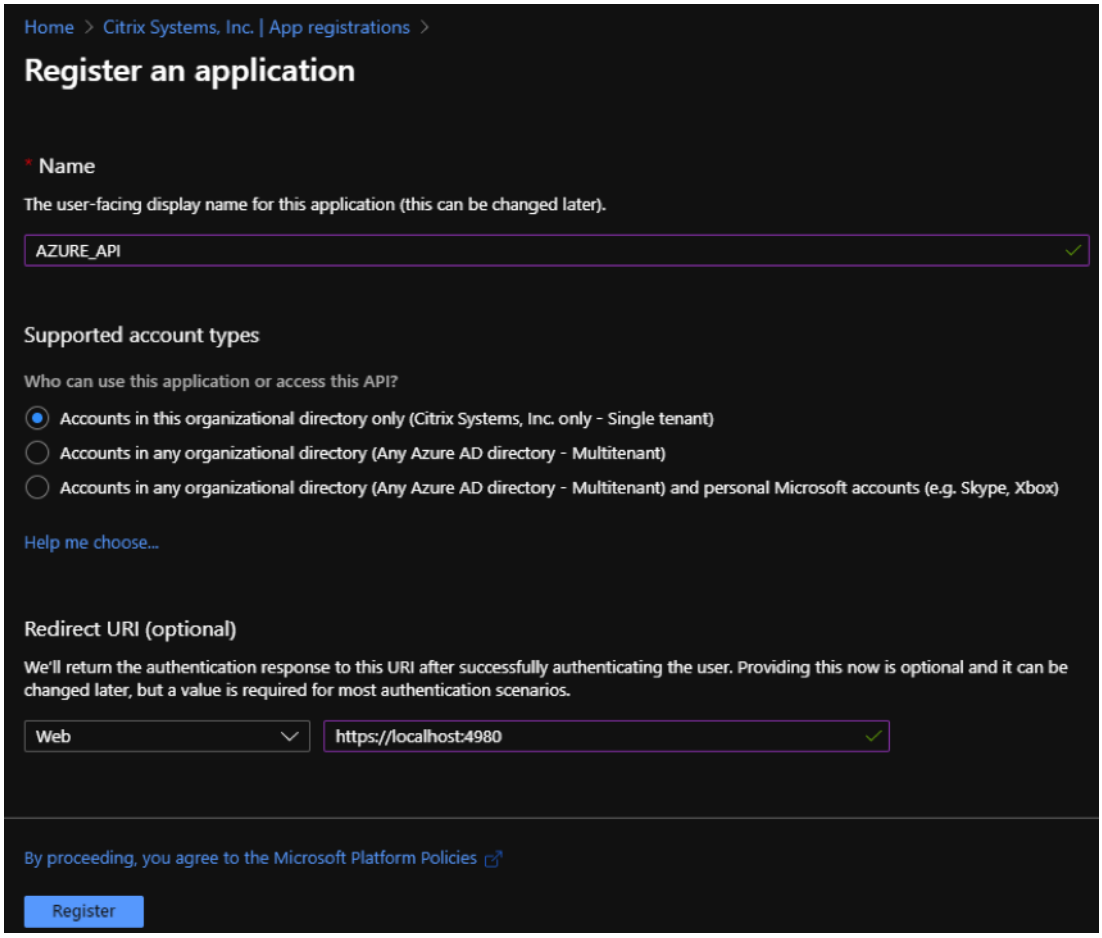
新しいアプリケーション登録を作成するには、次の手順を実行します。

1. Azure ポータルで、**Azure Active Directory** に移動します。
2. [管理] で [アプリの登録] を選択します。
3. クリック + 新規登録。

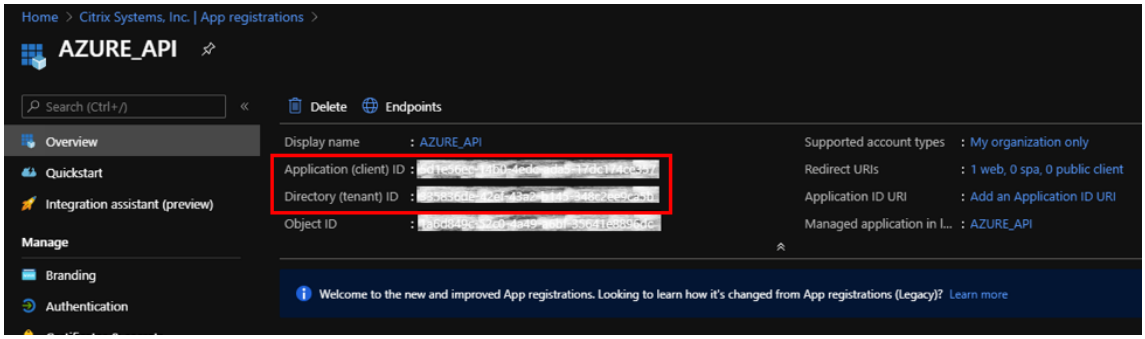


4. 次のフィールドに値を入力して、アプリケーションを登録します。

   - 名前–アプリケーション登録の名前を入力します。
   - サポートされるアカウントの種類–この組織ディレクトリのアカウントのみを選択します (* -シングルテナント）オプション。
   - リダイレクト **URI**（オプション）–ドロップダウンリストから [Web] を選択し、ランダムな一意の URL（たとえば、https:// localhost:4980)
   - [登録] をクリックします。



API の使用のために、Azure サブスクリプションへの認証に SD-WAN Orchestrator で使用できる アプリケーション（クライアント）**ID** と ディレクトリ（テナント）**ID** をコピーして保存できます。



アプリケーション登録の次のステップでは、認証のためにサービスプリンシパルキーを作成します。

サービスプリンシパルキーを作成するには、次の手順を実行します。

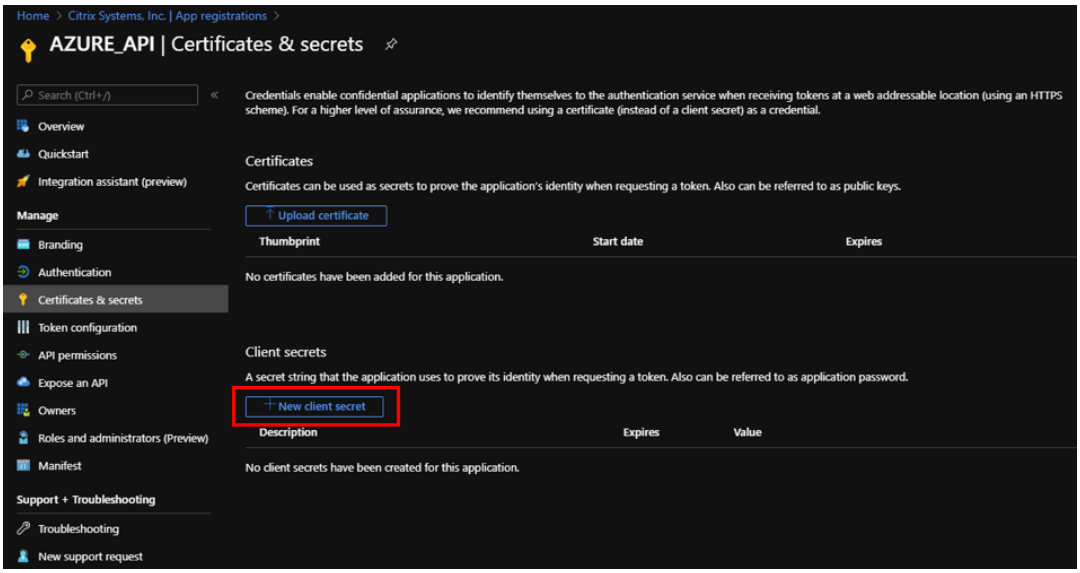
a) Azure ポータルで、**Azure Active Directory** に移動します。

b) **[管理]** で、[アプリの登録] に移動します。

c) 登録済みのアプリケーション（以前に作成したもの）を選択します。

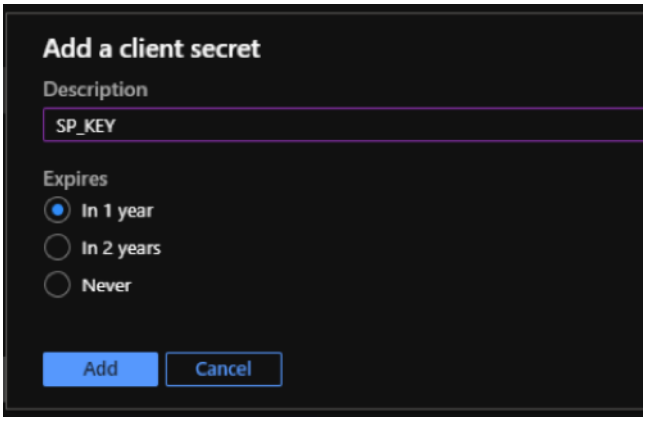
d) **[管理]** で、[証明書] を選択します & 秘密。

e) [クライアントシークレット] で、+ 新しいクライアントシークレット。



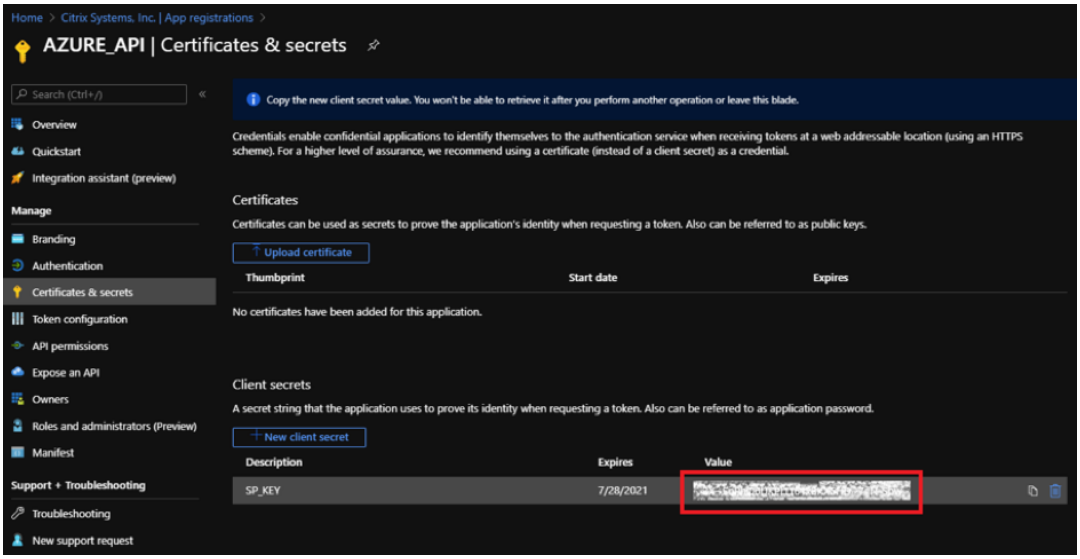
f) クライアントシークレットを追加するには、次のフィールドに値を入力します。

- 説明: サービスプリンシパルキーの名前を指定します。
- 期限切れ: 必要に応じて、有効期限を選択します。



g) [追加] をクリックします。

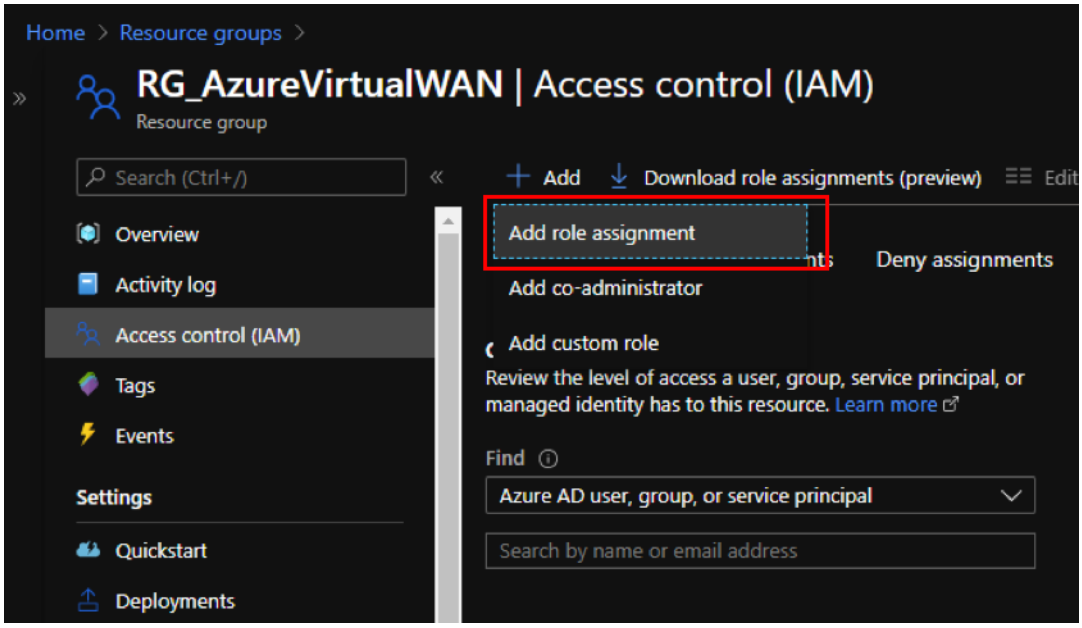
h) [値] 列でクライアントシークレットが無効になっています。キーをクリップボードにコピーします。これは、SD-WAN オーケストレータに入力する必要があるクライアントシークレットです。



> 注意
>
> 後で表示されなくなるため、ページをリロードする前に秘密鍵の値をコピーして保存する必要があります。

認証の目的で適切な役割を割り当てるには、次の手順を実行します。

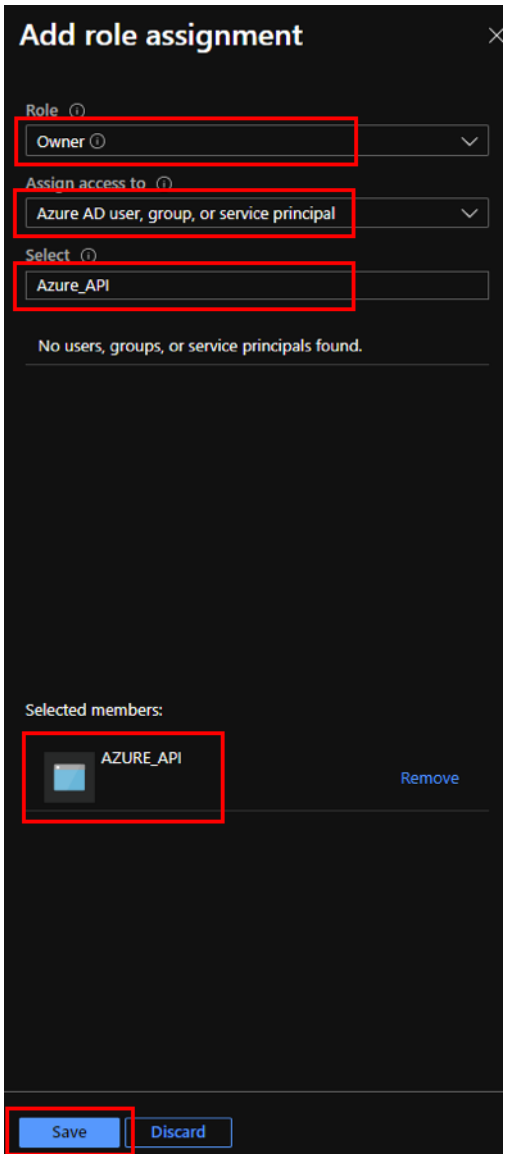
1. Azure ポータルで、仮想 WAN が作成された リソースグループに 移動します。
2. アクセス制御（**IAM**）に移動します。
3. クリック + [役割の割り当てを追加] を選択します。



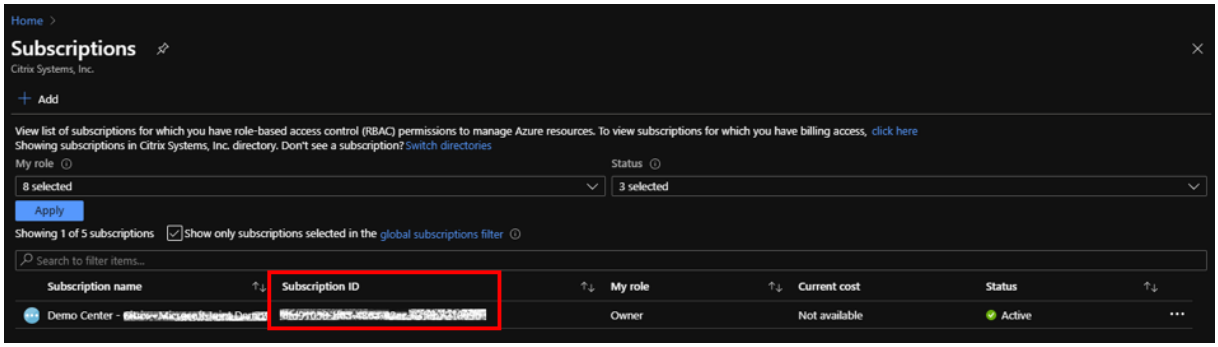
4. 役割の割り当てを追加するには、次のフィールドに値を入力します。

- 役割–ドロップダウンリストから [所有者] を選択します。この役割は、リソースへのアクセスを含むすべての管理を許可します。
- アクセスの割り当て–**Azure AD** ユーザー、グループ、または サービスプリンシパルを選択します。
- 選択 -以前に作成した登録済みアプリケーションの名前を入力し、対応するエントリが表示されたら選択します。

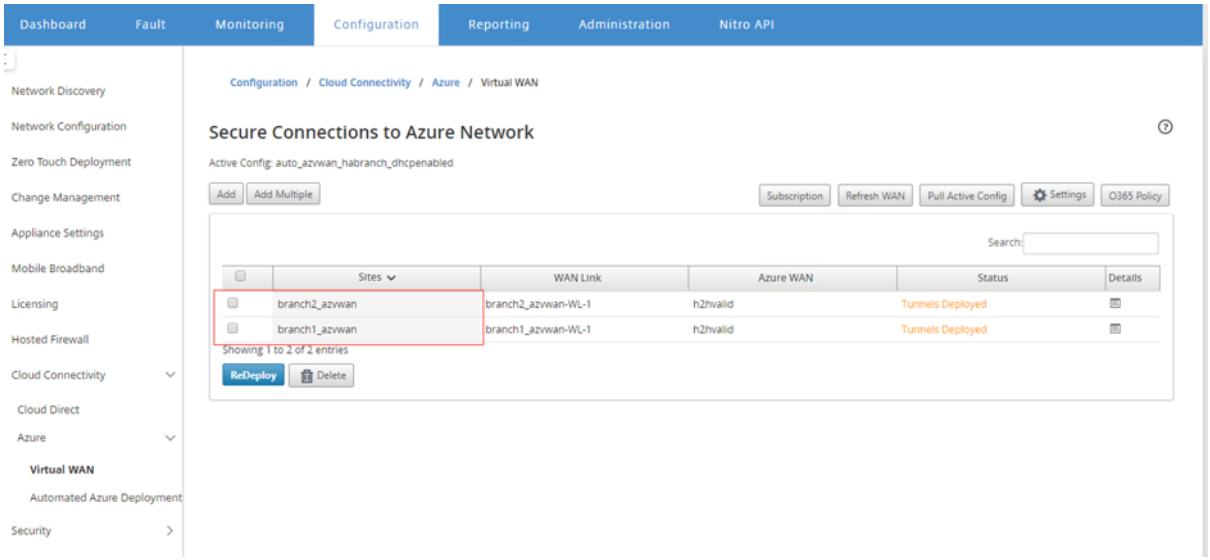
5. [保存] をクリックします。



最後に、Azure アカウントのサブスクリプション ID を取得する必要があります。Azure ポータルでサブスクリプションを検索すると、サブスクリプション **ID** を識別できます。



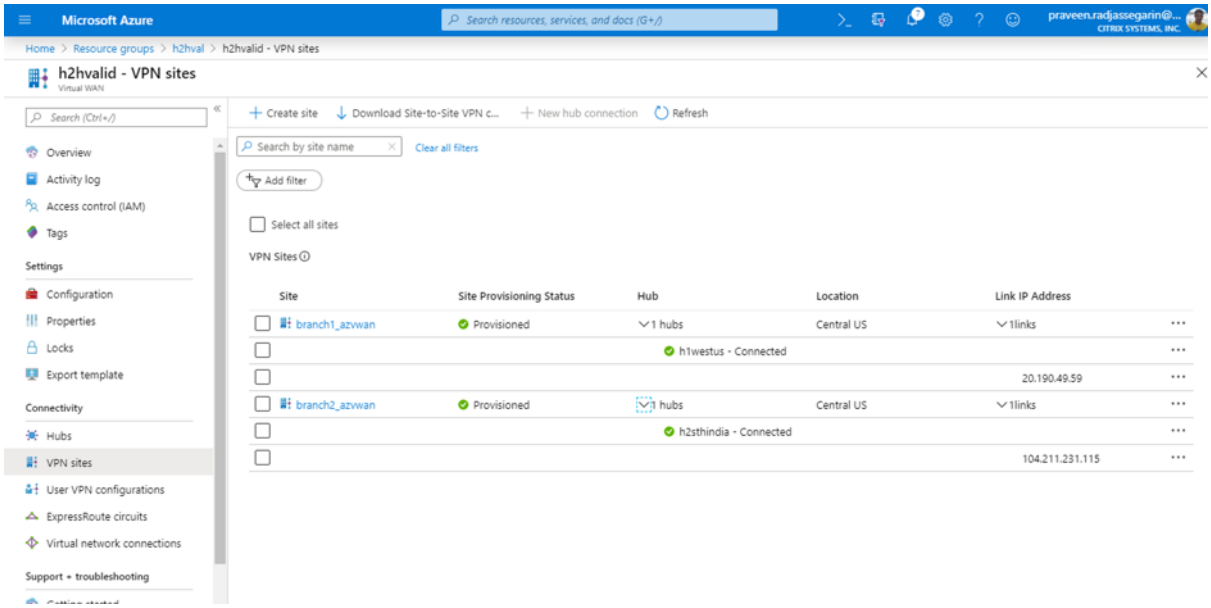
仮想 WAN を作成したら、**SD-WAN Center UI>** 構成 **> Azure>** 仮想 **WAN** にログインします。



2 つの異なるサイトを選択して、展開を開始します。サイトを展開したら、両方のサイトを 2 つの異なるハブに関連付けることができます。

> メモ
> デフォルトでは、ブランチ間と BGP は無効になっています。静的ルートを作成するか、BGP（設定の下）およびブランチ間接続を有効にすることができます。

BGP およびブランチツーブランチチェックボックスを有効にして、トンネルを展開します。トンネルが正常にデプロイされたら、**Microsoft Azure>** リソースグループでステータスを確認し、作成したリソースグループを選択し、**[VPN** サイト**]** をクリックします。



Citrix SD-WAN を使用した **Microsoft Azure Virtual WAN** への接続

February 18, 2022

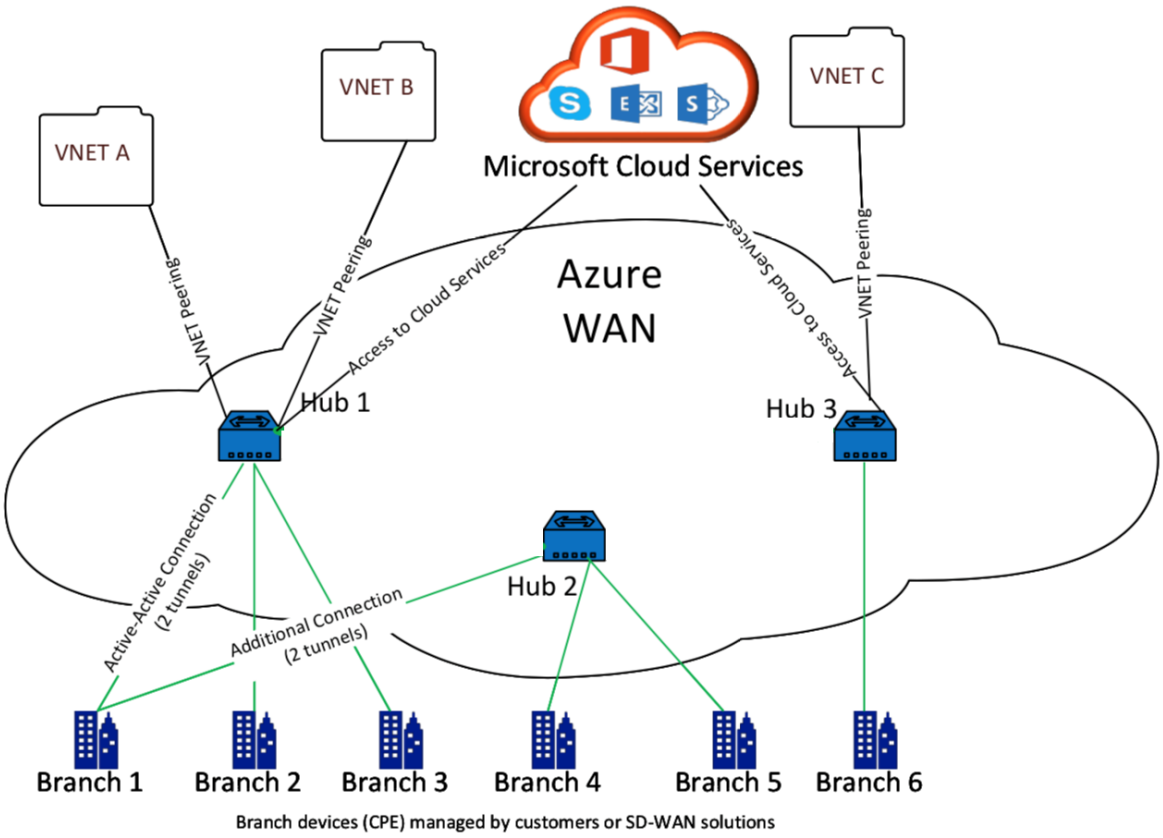
オンプレミスデバイスを Azure に接続するには、コントローラーが必要です。コントローラーは Azure API を取り込み、Azure WAN およびハブとのサイト間接続を確立します。

Microsoft Azure Virtual WAN には、次のコンポーネントとリソースが含まれています。

- WAN：Microsoft Azure のネットワーク全体を表します。この WAN 内に含めるすべてのハブへのリンクが含まれています。WAN は互いに分離されており、共通のハブや、異なる WAN 内の 2 つのハブ間の接続を含めることはできません。
- サイト：オンプレミス VPN デバイスとその設定を表します。サイトは複数のハブに接続できます。Citrix SD-WAN を使用すると、この情報を Azure に自動的にエクスポートする組み込みソリューションを使用できます。
- ハブ：特定の地域におけるネットワークの中核を表します。ハブには、オンプレミスネットワークへの接続やその他のソリューションを可能にするさまざまなサービスエンドポイントが含まれています。サイト間接続は、サイト間でハブ VPN エンドポイントに確立されます。
- ハブ仮想ネットワーク接続：ハブネットワークは、Azure 仮想 WAN ハブを仮想ネットワークにシームレスに接続します。現在、同じ仮想 HUB リージョン内にある仮想ネットワークへの接続が可能です。
- ブランチ：ブランチはオンプレミスの Citrix SD-WAN アプライアンスであり、顧客のオフィスの場所に存在します。SD-WAN コントローラは、ブランチを集中管理します。接続はこれらのブランチの背後から始まり、

Azure で終了します。SD-WAN コントローラーは、これらのブランチと Azure ハブに必要な構成を適用する役割を果たします。

次の図は、仮想 WAN コンポーネントについて説明しています。



Microsoft Azure Virtual WAN の仕組み

1. SD-WAN Center は、Azure GUI で有効になっているサービスプリンシパル、プリンシパル、またはロールベースのアクセス機能を使用して認証されます。
2. SD-WAN Center は Azure 接続構成を取得し、ローカルデバイスを更新します。これにより、オンプレミスデバイスの構成のダウンロード、編集、更新が自動化されます。
3. デバイスに正しい Azure 構成が設定されると、Azure WAN へのサイト間接続（2 つのアクティブな IPsec トンネル）が確立されます。Azure では、IKEv2 設定をサポートするためにブランチデバイスコネクタが必要です。BGP 構成はオプションです。

   注：IPsec トンネルを確立するための IPsec パラメーターは標準化されています。

IPsec プロパティ	パラメーター
Ike 暗号化アルゴリズム	AES 256
Ike 整合性アルゴリズム	SHA 256
Dh グループ	DH2
IPsec 暗号化アルゴリズム	GCM AES 256
IPsec 整合性アルゴリズム	GCM AES 256
PFS グループ	なし

Azure Virtual WAN は、ワークロード仮想ネットワークとハブ間の接続を自動化します。ハブ仮想ネットワーク接続を作成すると、プロビジョニングされたハブとワークロード仮想ネットワーク（VNET）の間に適切な構成が設定されます。

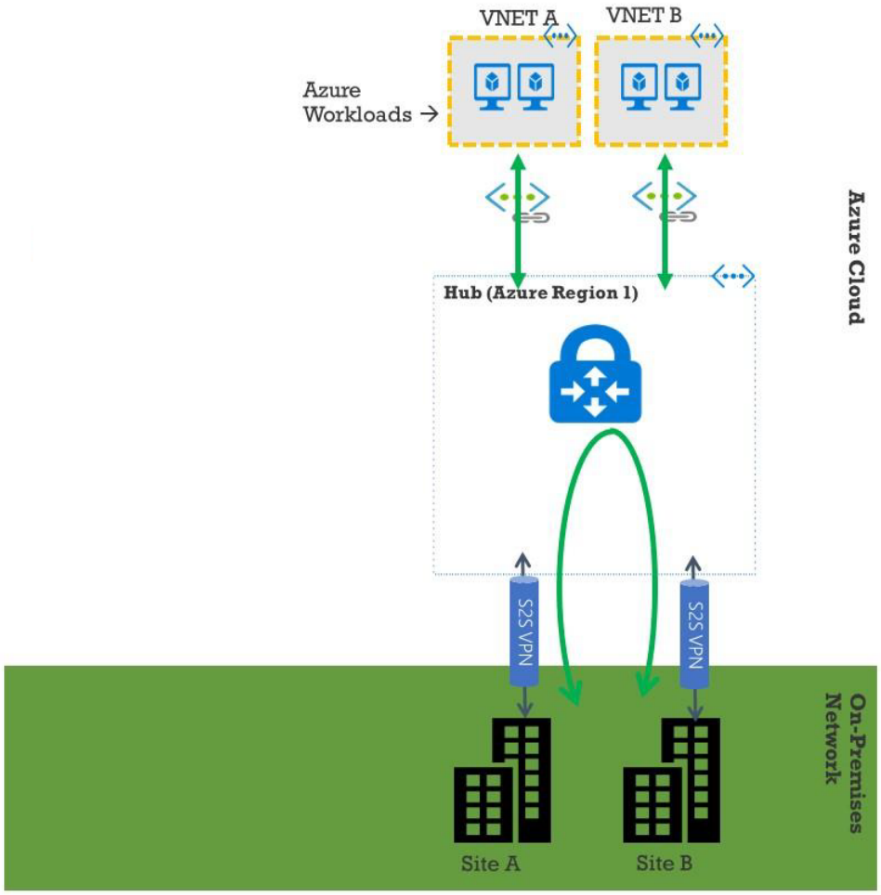
前提条件と要件

Azure ハブに接続するブランチサイトを管理するために Azure および SD-WAN を構成する前に、次の要件をお読みください。

1. 仮想 WAN の Azure サブスクリプションをホワイトリストに登録している。
2. Azure リソースへの IPsec を確立する SD-WAN アプライアンスなどのオンプレミスアプライアンスを用意します。
3. パブリック IP アドレスとのインターネットリンクがあります。Azure への接続を確立するには 1 つのインターネットリンクで十分ですが、同じ WAN リンクを使用するには 2 つの IPsec トンネルが必要です。
4. SD-WAN コントローラー–コントローラーは、Azure に接続するための SD-WAN アプライアンスの構成を担当するインターフェイスです。
5. 少なくとも 1 つのワークロードを持つ Azure の VNET。たとえば、サービスをホストしている VM です。次の点を考慮してください。

    a) 仮想ネットワークには、Azure VPN または Express Route ゲートウェイ、またはネットワーク仮想アプライアンスがあってはなりません。
    b) 仮想ネットワークには、オンプレミスのブランチからアクセスされるワークロードのトラフィックを非仮想 WAN 仮想ネットワークにルーティングするユーザー定義のルートがあってはなりません。
    c) ワークロードにアクセスするための適切な権限を構成する必要があります。たとえば、ubuntu VM のポート 22 SSH アクセス。

次の図は、Microsoft Azure に 2 つのサイトと 2 つの仮想ネットワークがあるネットワークを示しています。



Microsoft Azure Virtual WAN を設定する

オンプレミスの SD-WAN ブランチが Azure に接続し、IPsec トンネルを介してリソースにアクセスするには、次の手順を完了する必要があります。

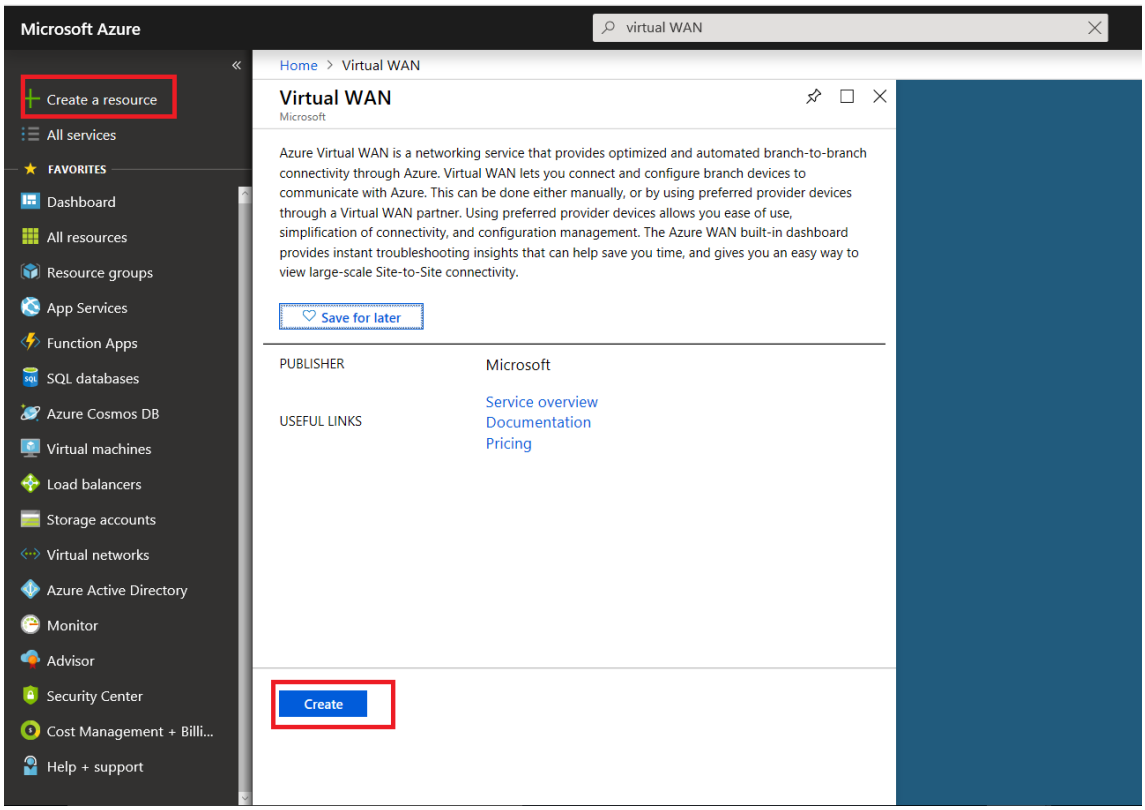
1. WAN リソースの構成。
2. SDsec-WAN ブランチが IPsec トンネルを使用して Azure に接続できるようにします。

SD-WAN アプライアンスに接続するために必要な Azure リソースが事前に利用可能である必要があるため、SD-WAN ネットワークを構成する前に Azure ネットワークを構成します。ただし、必要に応じて、Azure リソースを構成する前に SD-WAN 構成を構成できます。このトピックでは、SD-WAN アプライアンスを構成する前に、まず Azure 仮想 WAN ネットワークをセットアップする方法について説明します。https://microsoft.com Azure 仮想 WAN。

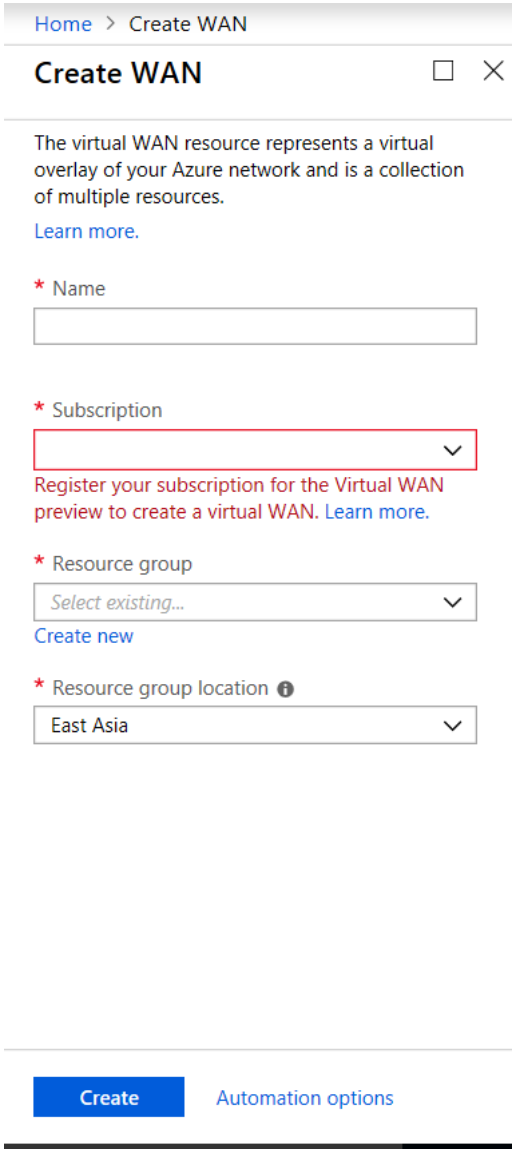
WAN リソースを作成する

仮想 WAN 機能を使用してオンプレミスのブランチアプライアンスを Azure に接続するには:

1. Azure Marketplaceにサインインし、仮想 WAN アプリに移動して、[**WAN** の作成] を選択します。



2. WAN の名前を入力し、WAN に使用するサブスクリプションを選択します。



3. 既存のリソースグループを選択するか、新しいリソースグループを作成します。リソースグループは論理的な構造であり、リソースグループ間のデータ交換は常に可能です。
4. リソースグループを配置する場所を選択します。WAN は、場所を持たないグローバルリソースです。ただし、WAN リソースのメタデータを含むリソースグループの場所を入力する必要があります。
5. [**Create**] をクリックします。これにより、設定を検証して展開するプロセスが開始されます。

サイトを作成

優先ベンダーを使用してサイトを作成できます。優先ベンダーは、デバイスとサイトに関する情報を Azure に送信するか、デバイスを自分で管理することを決定できます。デバイスを管理する場合は、Azure Portal でサイトを作成する必要があります。

SD-WAN ネットワークと **Microsoft Azure** 仮想 **WAN** ワークフロー

SD-WAN アプライアンスを構成します。

1. Citrix SD-WAN アプライアンスのプロビジョニング
    - SD-WAN ブランチアプライアンスを MCN アプライアンスに接続します。
2. SD-WAN アプライアンスを構成する
    - アクティブ/アクティブ接続用のイントラネットサービスを構成します。

SD-WAN Center を構成します。

- SD-WAN Center を構成して Microsoft Azure に接続します。

Azure 設定を構成する:

- テナント ID、クライアント ID、セキュアキー、サブスクライバー ID、およびリソースグループを提供します。

WAN アソシエーションへのブランチサイトの構成:

1. 1 つの WAN リソースをブランチに関連付けます。同じサイトを複数の WAN に接続することはできません。
2. [新規**]** をクリックして、サイトと WAN の関連付けを構成します。
3. **Azure Wan-resources** を選択します。
4. サイトの [サービス（イントラネット）] を選択します。Active-Standby サポート用に 2 つのサービスを選択します。
5. WAN リソースに関連付ける サイト名 を選択します。
6. [デプロイ**]** をクリックして、関連付けを確認します。
7. ステータスが [**Tunnels Deployed]** に変わるのを待って、**IPsec** トンネル 設定を表示します。
8. SD-WAN Center レポートビューを使用して、それぞれの IPsec トンネルのステータスを確認します。

Citrix SD-WAN ネットワークを構成する

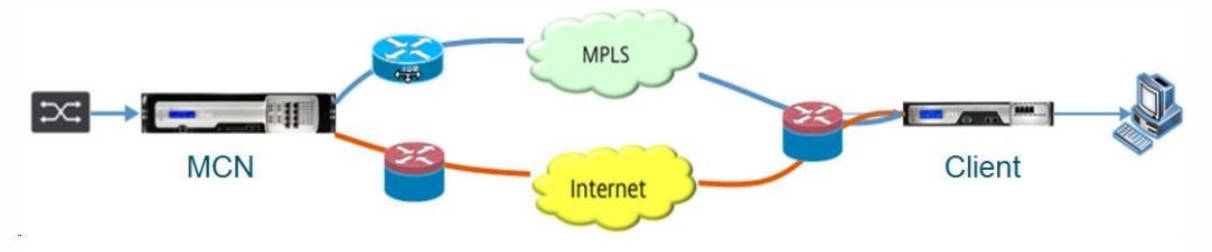
MCN:

MCN は、初期システム構成およびその後の構成変更の配布ポイントとして機能します。仮想 WAN に存在できるアクティブな MCN は 1 つだけです。
デフォルトでは、アプライアンスにはクライアントの役割が事前に割り当てられています。アプライアンスを MCN として確立するには、まずサイトを MCN として追加して構成する必要があります。ネットワーク構成 GUI は、サイトが MCN として構成された後に使用可能になります。アップグレードおよび構成の変更は、MCN または SD-WAN Center からのみ実行する必要があります。

MCN の役割:

MCN は、SD-WAN ネットワークのコントローラーとして機能する中央ノードであり、クライアントノードの中央管理ポイントです。ファームウェアパッケージの準備とクライアントへの配布に加えて、すべての構成アクティビティ

は MCN で構成されます。また、監視情報は MCN でのみ利用できます。MCN は SD-WAN ネットワーク全体を監視できますが、クライアントノードはローカルイントラネットとそれらが接続されているクライアントの一部の情報のみを監視できます。MCN の主な目的は、エンタープライズサイト間通信のために SD-WAN ネットワーク全体に配置された 1 つ以上のクライアントノードとのオーバーレイ接続（仮想パス）を確立することです。MCN は、複数のクライアントノードを管理し、仮想パスを持つことができます。複数の MCN を設定できますが、一度にアクティブにできるのは 1 つだけです。次の図は、小規模な 2 サイトネットワークの MCN およびクライアント（ブランチノード）アプライアンスの基本的な図を示しています。

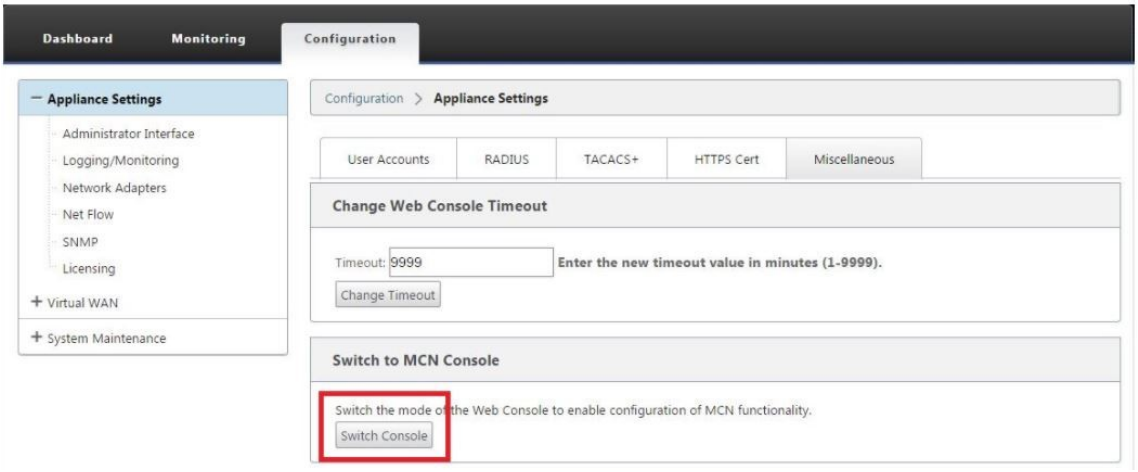


SD-WAN アプライアンスを **MCN** として構成する

MCN を追加して構成するには、まず MCN として指定しているアプライアンスの管理 Web インターフェイスにログインし、管理 Web インターフェイスを MCN コンソールモードに切り替える必要があります。MCN コンソールモードでは、現在接続している管理 Web インターフェイスの設定エディタにアクセスできます。その後、構成エディターを使用して MCN サイトを追加および構成できます。

管理 Web インターフェイスを MCN コンソールモードに切り替えるには、次の手順を実行します。

1. MCN として構成するアプライアンスの SD-WAN 管理 Web インターフェイスにログインします。
2. Management Web Interface のメイン画面のメインメニューバー (ページ上部の青いバー) で、[構成] をクリックします。
3. ナビゲーション・ツリー (左側のペイン) で、「アプライアンスの設定」ブランチを開き、「管理者インタフェース」をクリックします。
4. [その他] タブを選択します。その他の管理設定ページが開きます。



[その他] タブページの下部には、[クライアントへの切り替え、MCN コンソール] セクションがあります。**[] このセクションには、** アプライアンスのコンソールモードを切り替えるための [Switch Console] ボタンがあります。

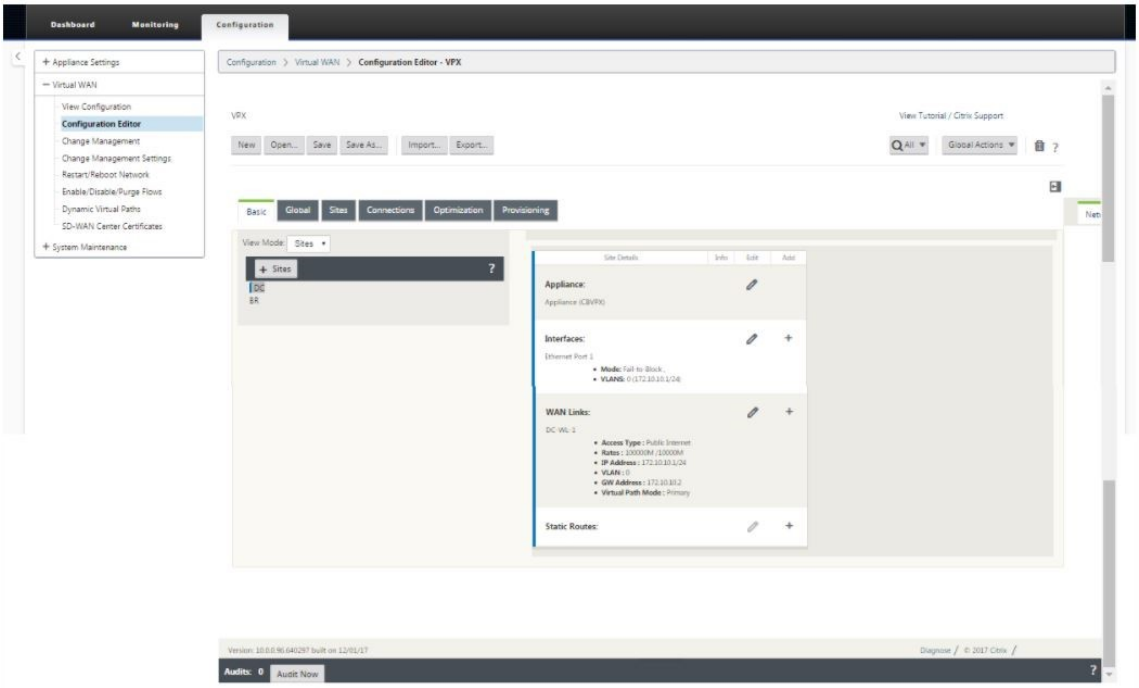
セクション見出しは、次のように現在のコンソールモードを示します。

- クライアントコンソールモード (デフォルト) の場合、セクション見出しは [MCN コンソールに切り替え] です。
- MCN コンソールモードの場合、セクション見出しは [クライアントコンソールに切り替える] です。

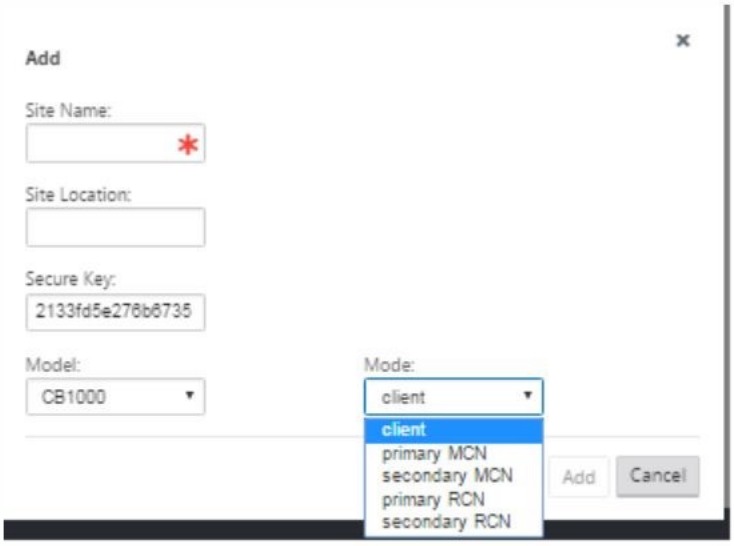
デフォルトでは、新しいアプライアンスはクライアントコンソールモードです。MCN コンソールモードでは、ナビゲーションツリーの構成エディタービューが有効になります。設定エディタは MCN アプライアンスでのみ使用できます。

MCN の設定　MCN アプライアンスサイトを追加して構成を開始するには、次の手順を実行します。

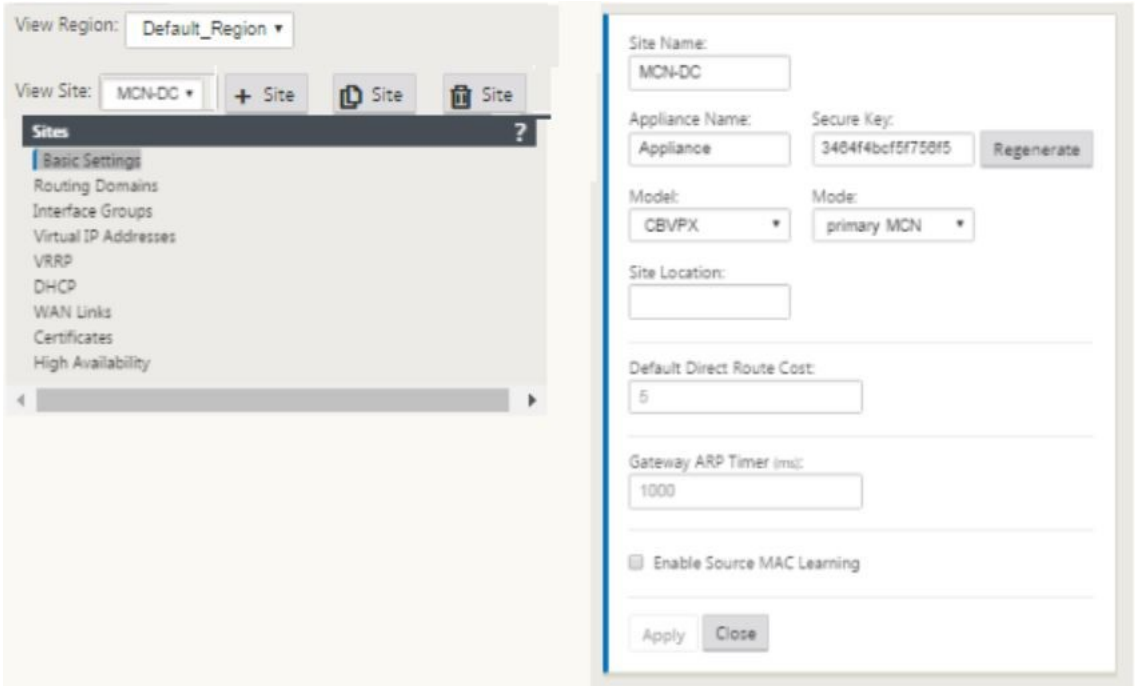
1. SD-WAN アプライアンス GUI で、仮想 **WAN** > 構成エディターに移動します。



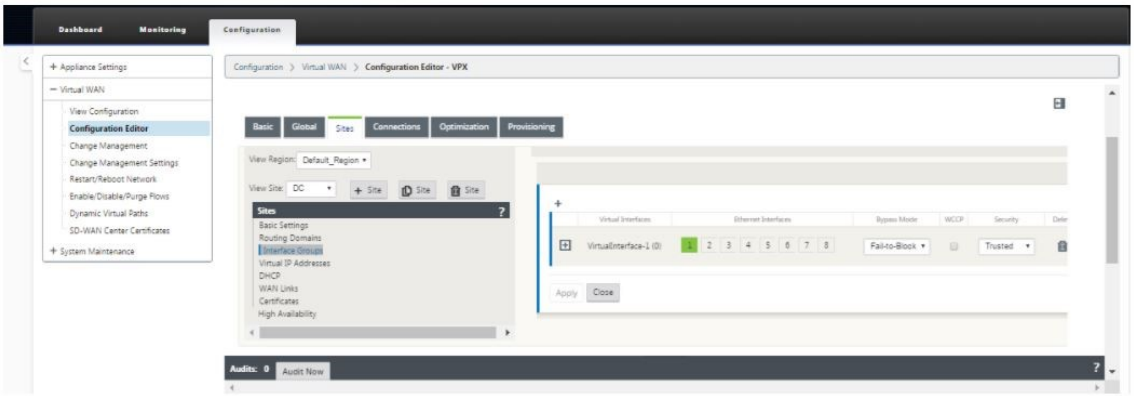
2. サイトバーの [**+** サイト] をクリックして、MCN サイトの追加と構成を開始します。[サイト の追加] ダイアログボックスが表示されます。



3. アプライアンスの地理的な場所と役割を決定できるサイト名を入力します (DC/secondary DC)。正しいアプライアンスモデルを選択します。ハードウェアプラットフォームは処理能力とライセンスの点で互いに異なるため、正しいアプライアンスを選択することが重要です。このアプライアンスをプライマリヘッドエンドアプライアンスとして構成しているため、モードをプライマリ MCN として選択し、[追加] をクリックします。
4. これにより、サイトツリーに新しいサイトが追加され、デフォルトビューには、以下に示すような基本設定の構成ページが表示されます。

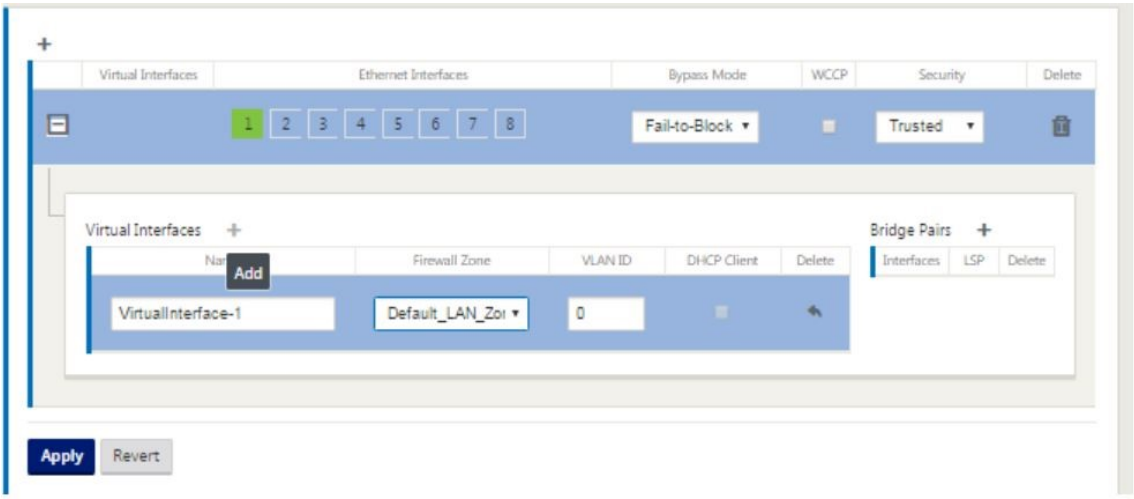


5. 場所、サイト名などの基本設定を入力します。
6. からのトラフィックを受け入れることができるようにアプライアンスを構成します Internet/MPLS/Broadband. リンクが終端するインターフェースを定義します。これは、アプライアンスがオーバーレイモードかアンダーレイモードかによって異なります。
7. [インターフェースグループ] をクリックして、インターフェースの定義を開始します。



8. クリック + 仮想インターフェイスグループを追加します。これにより、新しい仮想インターフェースグループが追加されます。仮想インターフェースの数は、アプライアンスで処理するリンクによって異なります。アプライアンスが処理できるリンクの数は、アプライアンスモデルによって異なり、最大リンク数は最大 8 です。

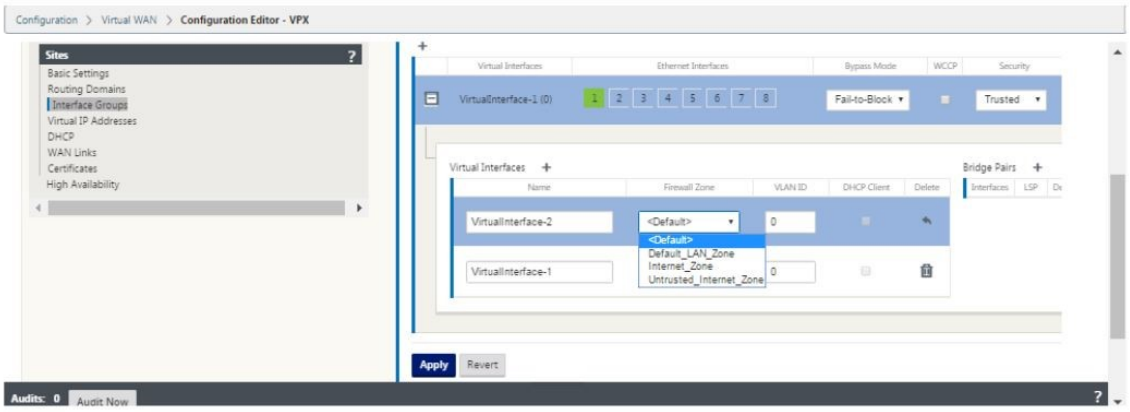
9. クリック + 以下に示すように、仮想インターフェイスの右側にある画面を表示します。



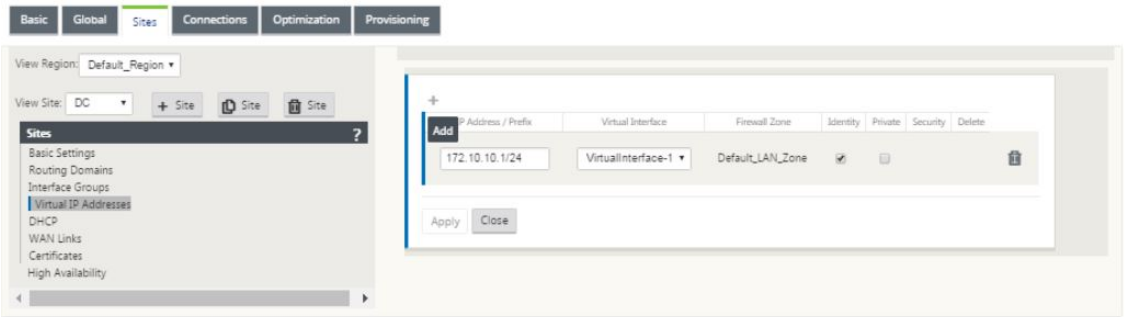
10. この仮想インターフェイスの一部を形成する イーサネットインターフェイスを選択します。プラットフォームモデルに応じて、アプライアンスには事前に構成されたフェイルツーワイヤーインターフェイスのペアがあります。アプライアンスでワイヤーフェイルを有効にする場合は、正しいインターフェイスのペアを選択していることを確認し、バイパスモード 列でワイヤーフェイルを選択していることを確認してください。

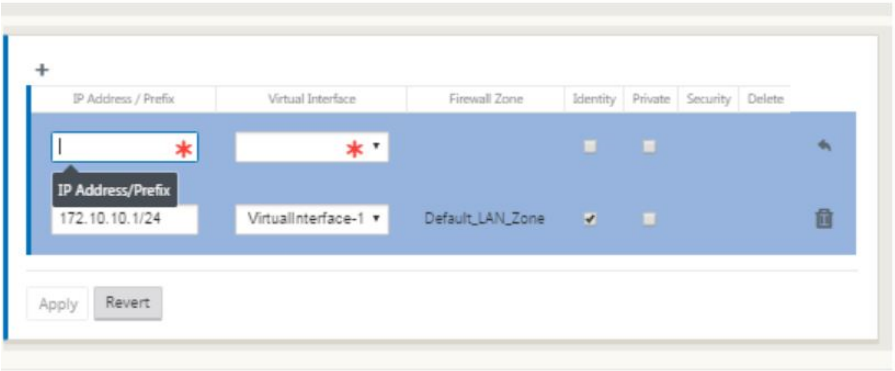
11. ドロップダウンリストからセキュリティレベルを選択します。インターフェイスが MPLS リンクを提供している場合は信頼モードが選択され、それぞれのインターフェイスでインターネットリンクが使用されている場合は非信頼モードが選択されます。

12. クリック + 仮想インターフェースという名前のラベルの右側。名前、ファイアウォールゾーン、VLAN ID が表示されます。この仮想インターフェイスグループの 名前と **VLAN ID** を入力します。VLAN ID は、仮想インターフェースとの間のトラフィックの識別とマーキングに使用され、0（ゼロ）を使用して native/untagged トラフィック。



13. 配線に失敗したインターフェイスを設定するには、[ブリッジペア] をクリックします。これにより、新しいブリッジペアが追加され、編集が可能になります。[適用] をクリックして、これらの設定を確認します。
14. さらに仮想インターフェイスグループを追加するには、+ インターフェースグループの右側に分岐し、上記のように進みます。
15. インターフェイスを選択したら、次のステップはこれらのインターフェイスに IP アドレスを設定することです。Citrix SD-WAN 用語では、これは VIP（仮想 IP）と呼ばれます。
16. サイトビューで続行し、仮想 IP アドレスをクリックして、VIP を構成するためのインターフェイスを表示します。

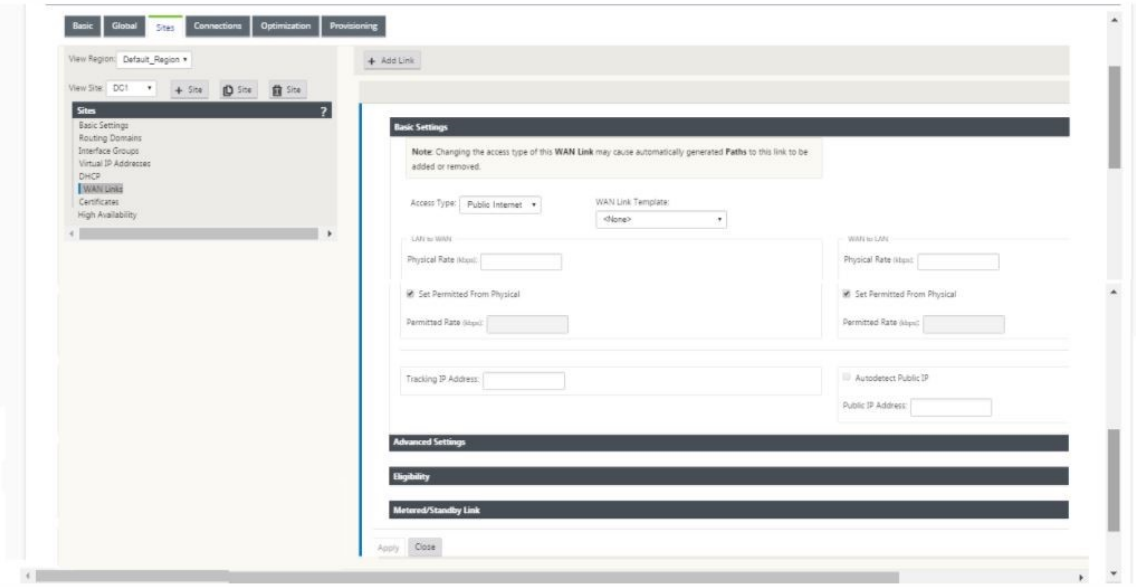




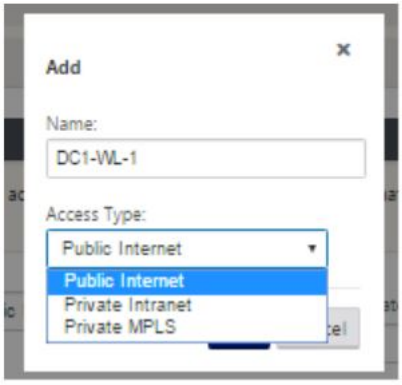
17. IP アドレス/プレフィックス情報を入力し、アドレスが関連付けられている仮想インターフェイスを選択しま

す。仮想 IP アドレスには、完全なホストアドレスとネットマスクを含める必要があります。ファイアウォールゾーン、ID、プライベート、セキュリティなど、仮想 IP アドレスに必要な設定を選択します。［適用］をクリックします。これにより、アドレス情報がサイトに追加され、サイトの仮想 IP アドレステーブルに追加されます。さらに仮想 IP アドレスを追加するには、[仮想 IP アドレス] の右側にある [+] をクリックし、上記の手順を実行します。

18. サイトセクションに進み、サイトの WAN リンクを構成します。



19. 右側のパネルの上部にある [リンクを追加] をクリックします。これによりダイアログボックスが開き、設定するリンクのタイプを選択できます。

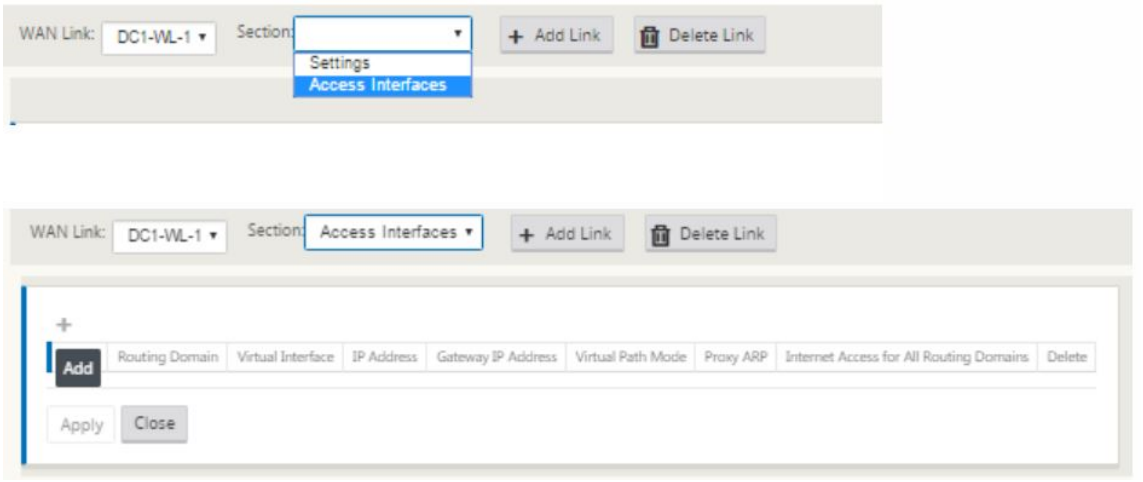


20. 公衆インターネットは Internet/broadband/DSL/ADSL プライベート MPLS は MPLS リンク用です。プライベートイントラネットも MPLS リンク用です。プライベート MPLS とプライベートイントラネットリンクの違いは、プライベート MPLS では MPLS リンクの QoS ポリシーを保持できることです。

21. パブリックインターネットを選択していて、IP が DHCP 経由で割り当てられている場合は、IP の自動検出オプションを選択します。

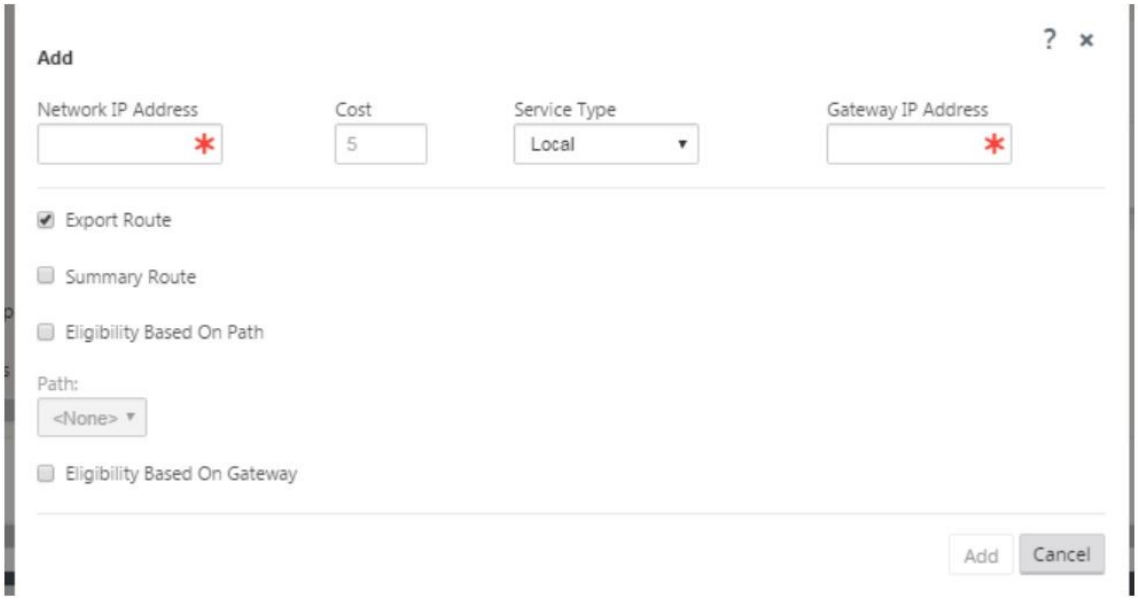
22. WAN リンク構成ページで [アクセスインターフェイス] を選択します。これにより、サイトの [アクセスイン

ターフェイス] ビューが開きます。以下に示すように、各リンクの VIP およびゲートウェイ IP を追加して構成します。



23. [**+**] をクリックして、インターフェイスを追加します。これにより、テーブルに空白のエントリが追加され、編集用に開かれます。
24. このインターフェイスに割り当てる名前を入力します。リンクの種類と場所に基づいて名前を付けることができます。ネットワークを分離してインターフェイスに IP を割り当てない場合は、ルーティングドメインをデフォルトのままにします。
25. リンクがインターネットリンクの場合はパブリックに到達可能なゲートウェイ IP アドレスを、リンクが MPLS リンクの場合はプライベート IP を指定してください。このパスが仮想パスを形成するために必要なので、仮想パスモードをプライマリのままにします。

    注意: ゲートウェイに到達できない場合、アプライアンスはゲートウェイ IP アドレスの ARP 要求に応答するため、プロキシ ARP を有効にします。
26. 「適用」をクリックして、WAN リンクの構成を完了します。さらに WAN リンクを構成する場合は、別のリンクに対して手順を繰り返します。
27. サイトのルートを構成します。[接続] ビューをクリックして、ルートを選択します。
28. クリック + ルートを追加するには、次のようなダイアログボックスを開きます。



29. 新しいルートで利用できる次の情報を入力します。

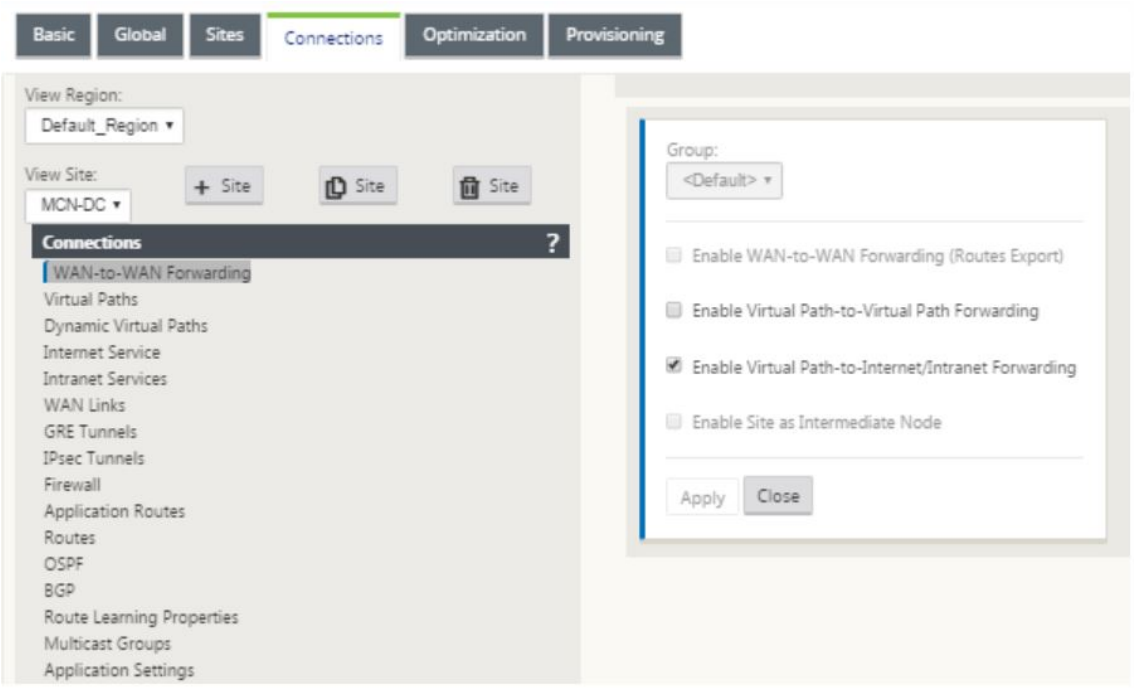
    - ネットワーク IP アドレス
    - コスト–コストは、他のルートよりも優先されるルートを決定します。低コストのパスは、高コストのルートよりも優先されます。デフォルト値は 5 です。
    - サービスの種類–サービスを選択します。サービスは次のいずれかです。
        - 仮想パス
        - イントラネット
        - インターネット
        - パススルー
        - ローカル
        - GRE トンネル
        - LAN IPsec トンネル

30. [適用] をクリックします。

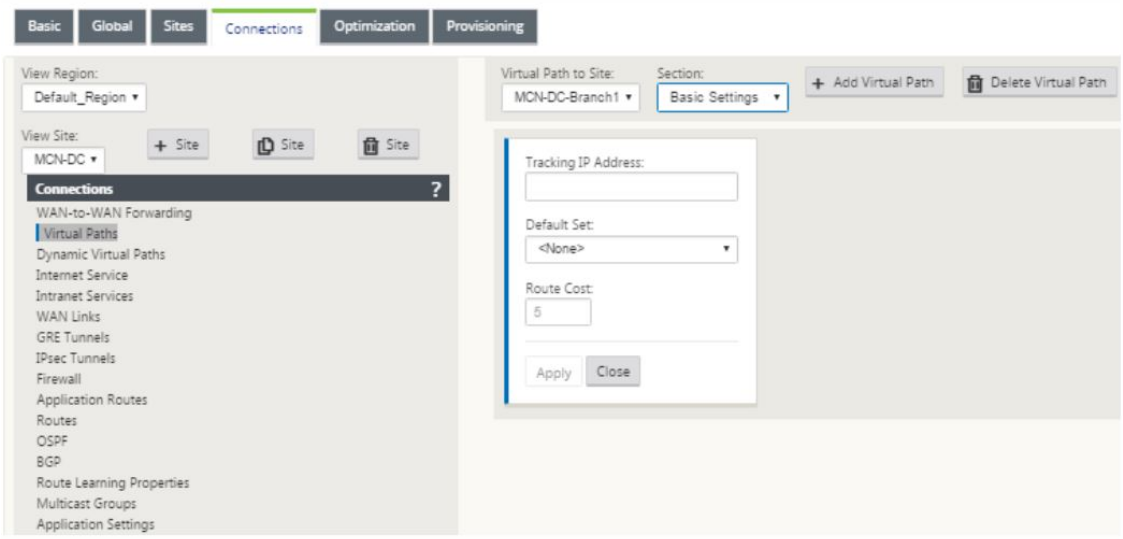
サイトのルートをさらに追加するには、+ ルート分岐の右側にあり、上記のように進みます。詳細については、「MCN の構成」を参照してください。

MCN とブランチサイト間の仮想パスを構成する　MCN とブランチノード間の接続を確立します。これを行うには、これら 2 つのサイト間に仮想パスを構成します。構成エディターの構成ツリーの「接続」タブにナビゲートします。

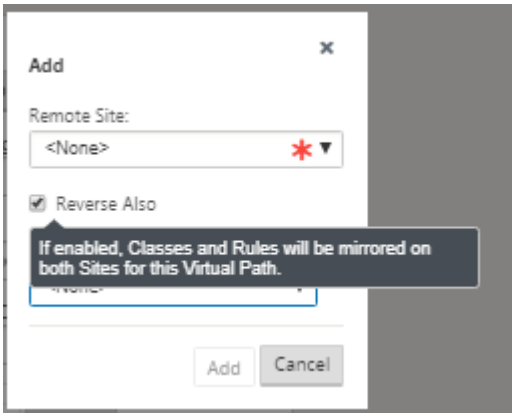
1. 構成セクションの [接続] タブをクリックします。これにより、構成ツリーの接続セクションが表示されます。
2. 接続 セクションページの [サイトを表示] ドロップダウンメニューから **MCN** を選択します。



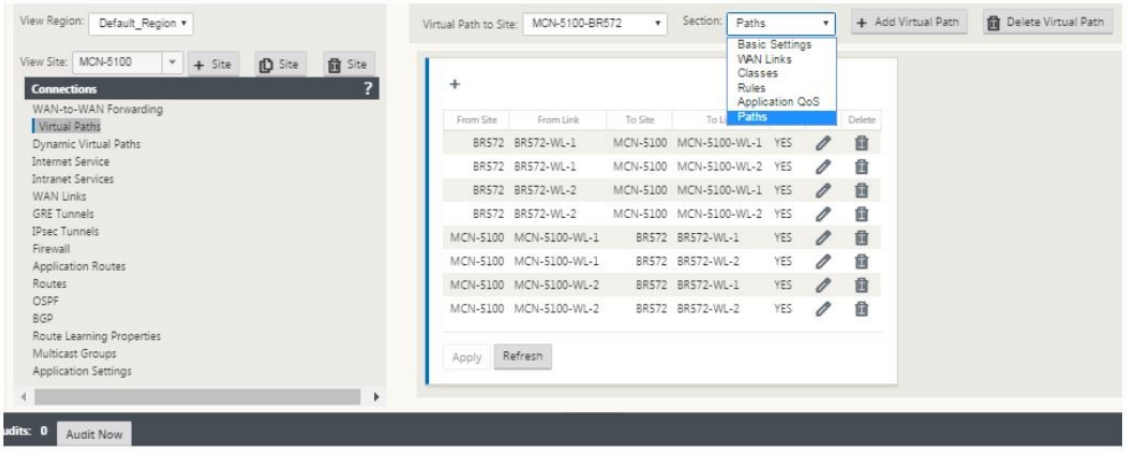
3. [接続] タブの下から仮想パスを選択して、MCN とブランチサイトの間に仮想パスを作成します。



4. 仮想パスセクションの静的仮想パスの名前の横にある [仮想パスの追加] を クリックします。これにより、次のようなダイアログボックスが開きます。仮想パスを構成するブランチを選択します。これは、リモートサイトというラベルで構成する必要があります。このドロップダウンリストからブランチノードを選択し、チェックボックス [逆も同様] をクリックします。



トラフィックの分類とステアリングは、仮想パスの両方のサイトでミラーリングされます。これが完了したら、以下に示すように、セクションというラベルの下のドロップダウンメニューからパスを選択します。



5. クリック + [パスの追加] ダイアログボックスを表示するパステーブルの上に 追加し ます。仮想パスを構成する必要があるエンドポイントを指定します。次に、[追加] をクリックしてパスを作成し、[逆も同様] チェックボックスをクリックします。

   注意: Citrix SD-WAN は、双方向のリンク品質を測定します。つまり、ポイント A からポイント B は 1 つのパスであり、ポイント B からポイント A は別のパスです。リンク状態の単方向測定を利用して、SD-WAN はトラフィックを送信するための最適なルートを選択できます。これは、レイテンシを測定するための双方向メトリックである RTT などの測定とは異なります。たとえば、ポイント A とポイント B の間の 1 つの接続は 2 つのパスとして表示され、それぞれについてリンクパフォーマンスメトリックが個別に計算されます。

この設定は、MCN とブランチの間の仮想パスを起動するのに十分です。他の構成オプションも使用できます。詳細については、「
MCN サイトとクライアントサイト間の仮想パスサービスの構成」を参照してください。

MCN 構成を展開する　次のステップは、構成をデプロイすることです。これには、次の 2 つの手順が含まれます。

1. SD-WAN 構成パッケージを変更管理にエクスポートします。

- アプライアンスパッケージを生成する前に、まず、完成した構成パッケージを構成エディタから MCN のグローバル変更管理ステージングインボックスにエクスポートする必要があります。「変更管理の実行」セクションに記載されている手順を参照してください。

2. アプライアンスパッケージを生成してステージングします。

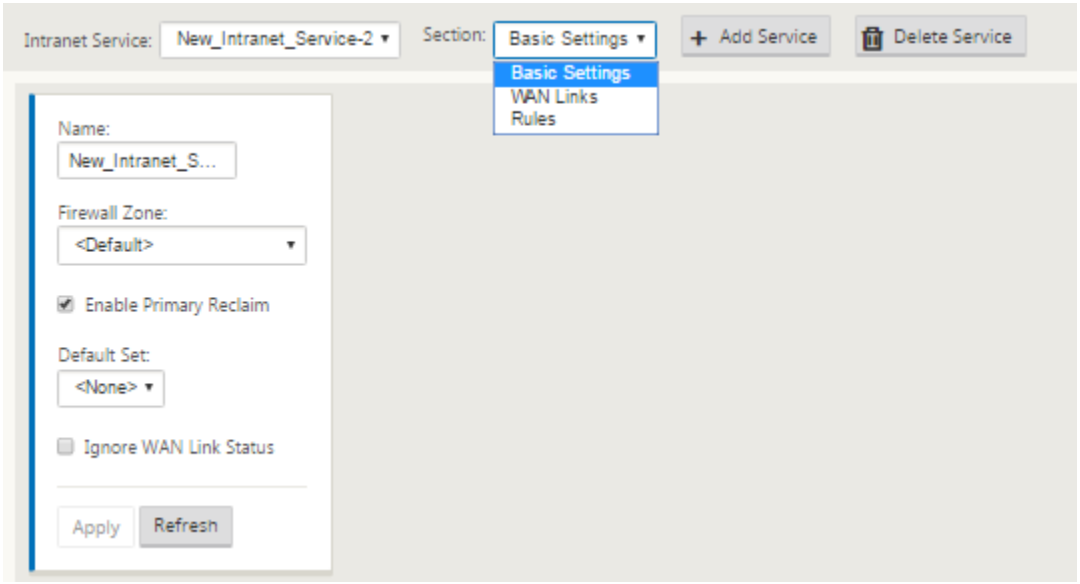
   - 新しい構成パッケージを変更管理の受信ボックスに追加したら、ブランチサイトでアプライアンスパッケージを生成してステージングできます。これを行うには、MCN の管理 Web インターフェイスで変更管理ウィザードを使用します。「アプライアンスパッケージのステージング」セクションに記載されている手順を参照してください。

Azure WAN リソースと接続するようにイントラネットサービスを構成する

1. SD-WAN アプライアンス GUI で、[構成エディター] に移動し、[接続] タイルに移動します。クリック + サービス を追加して、そのサイトのイントラネットサービスを追加します。

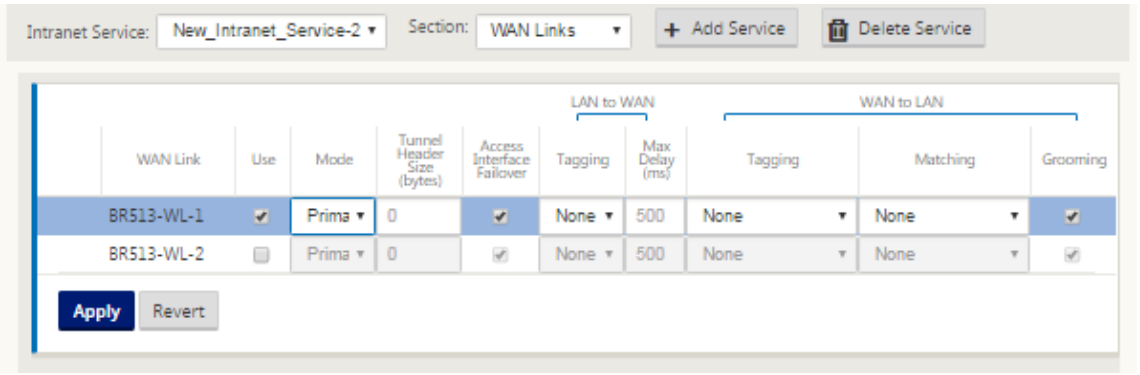
2. イントラネットサービスの 基本設定 には、WAN リンクが使用できないときにイントラネットサービスをどのように動作させるかについて、いくつかのオプションがあります。

   - プライマリ再利用を有効にする–選択したプライマリリンクがフェイルオーバー後に起動したときに引き継ぐ場合は、このボックスをオンにします。ただし、このオプションをオンにしない場合は、セカンダリリンクがトラフィックを送信し続けます。
   - **WAN** リンクステータスを無視する–このオプションを有効にすると、構成要素の WAN リンクが利用できない場合でも、このイントラネットサービス宛てのパケットは引き続きこのサービスを使用します。

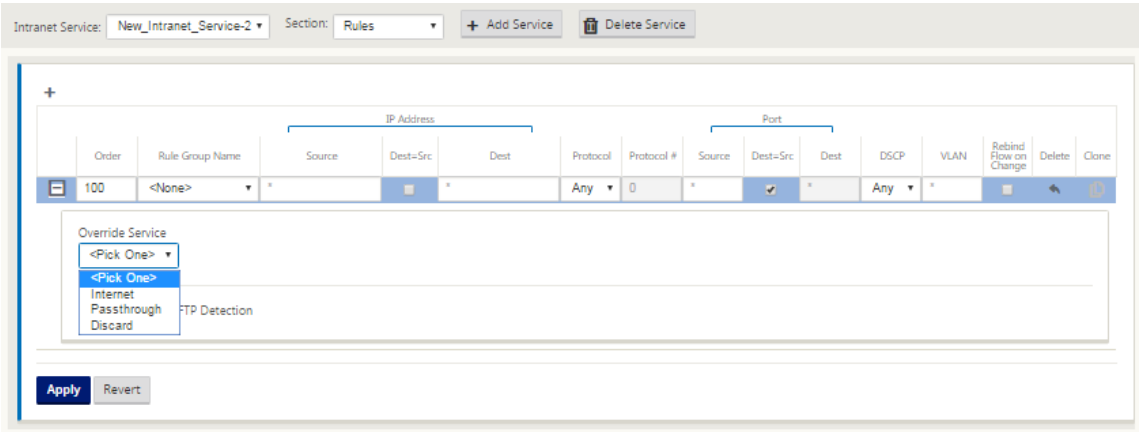


3. 基本設定を構成したら、次のステップは、このサービスの構成 WAN リンクを選択することです。1 つのイントラネットサービスに対して最大 2 つのリンクが選択されます。WAN リンクを選択するには、セクションというラベルの付いたドロップダウンリストから WAN リンクオプションを選択してください。WAN リンクはプライマリモードとセカンダリモードで機能し、1 つのリンクのみがプライマリ WAN リンクとして選択されます。

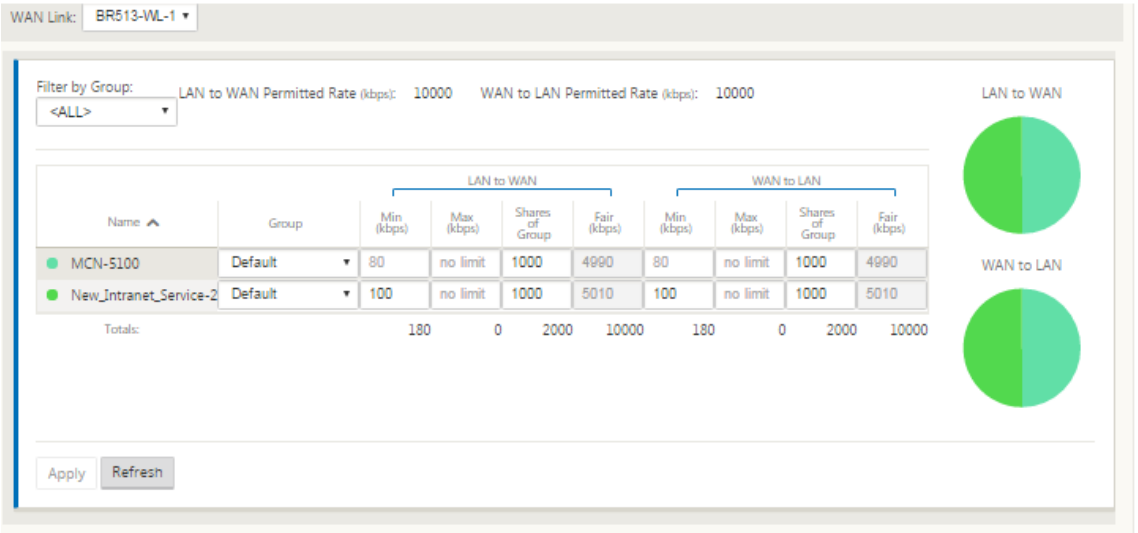
   注意: 2 番目のイントラネットサービスを作成するときは、プライマリとセカンダリの wan-link マッピングが必要です。



4. ブランチサイト固有のルールを使用できるので、グローバルなデフォルトセットで構成されている一般的な設定をオーバーライドして、各ブランチサイトをカスタマイズできます。モードには、特定の WAN リンクを介した望ましい配信や、フィルタリングされたトラフィックのパススルーまたは破棄を可能にする上書きサービスとしての配信が含まれます。たとえば、イントラネットサービスを経由したくないトラフィックがある場合、そのトラフィックを破棄するか、別のサービス（インターネットまたはパススルー）を介して送信するルールを作成できます。

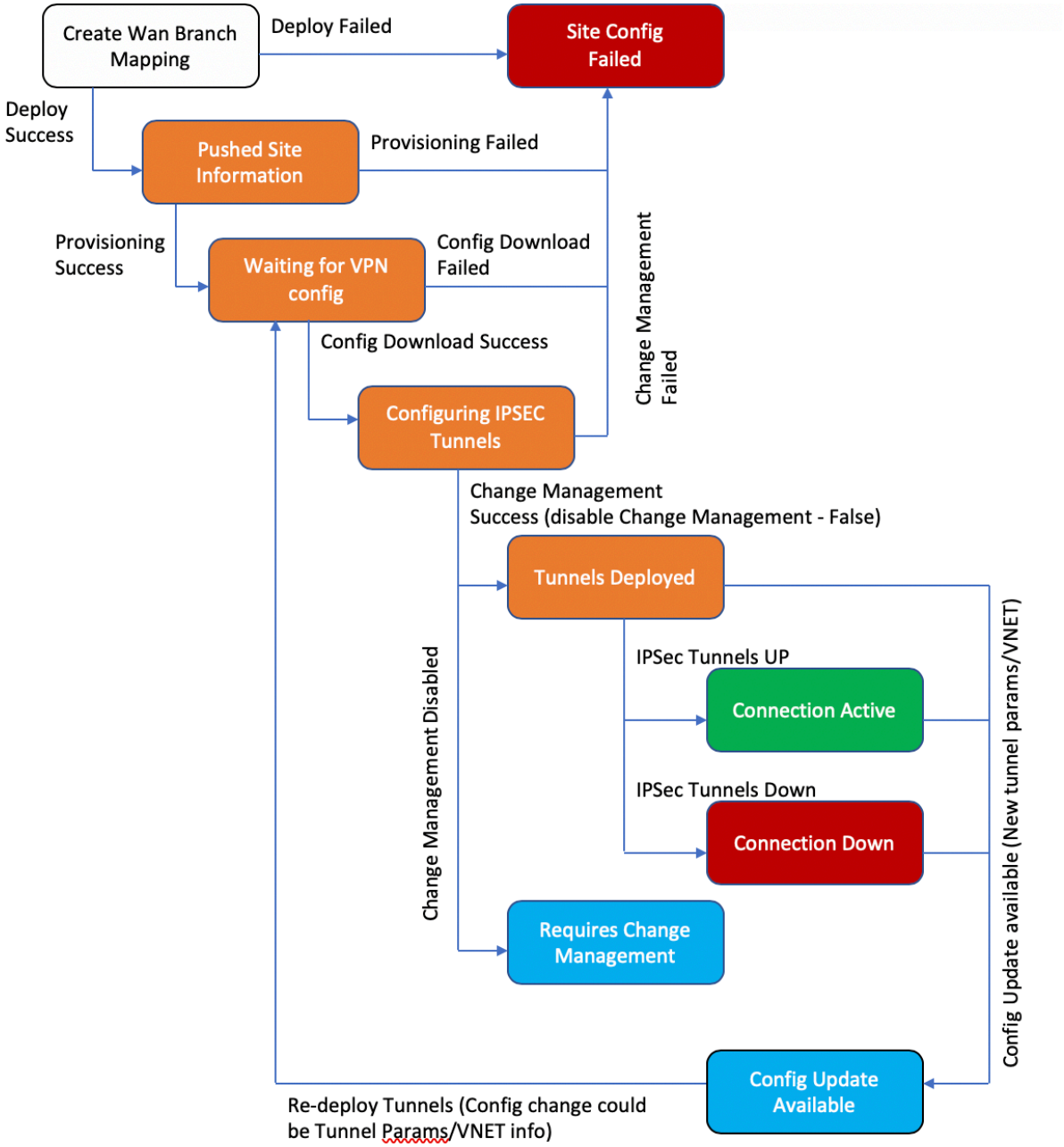


5. サイトでイントラネットサービスを有効にすると、プロビジョニング タイルが利用可能になり、双方向（LAN から WAN へ）が可能になります / WAN to LAN）WAN リンクを利用するさまざまなサービス間での WAN リンクの帯域幅の分配。「サービス」セクションでは、帯域幅の割り当てをさらに微調整できます。さらに、公平配分を有効にして、公平配分が実施される前にサービスが最小予約帯域幅を受信できるようにすることができます。



SD-WAN Center の構成

次の図は、SD-WAN Center と Azure Virtual WAN 接続の高レベルのワークフロー、および対応するデプロイメントの状態遷移を示しています。



Azure 設定を構成する:

- Azure テナント ID、アプリケーション ID、シークレットキー、およびサブスクリプション ID（サービスプリ

ンシパルとも呼ばれる）を提供します。

WAN アソシエーションへのブランチサイトの構成:

- ブランチサイトを WAN リソースに関連付けます。同じサイトを複数の WAN に接続することはできません。
- [新規] をクリックして、サイトと WAN の関連付けを構成します。
- [**Azure WAN-resources]** を選択します。
- WAN リソースに関連付ける サイト名 を選択します。
- [デプロイ] をクリックして、関連付けを確認します。トンネルの展開に使用される WAN リンクは、リンク容量が最適なもので自動的に読み込まれます。
- ステータスが「展開された トンネル」に変わるのを待って、IPsec トンネル設定を表示します。
- SD-WAN Center レポートビューを使用して、それぞれの IPsec トンネルのステータスを確認します。データトラフィックが流れるには、接続がアクティブであることを示す IPsec トンネルステータスが緑である必要があります。

SD-WAN Center のプロビジョニング:

SD-WAN Center は、Citrix SD-WAN の管理およびレポートツールです。仮想 WAN に必要な構成は、SD-WAN Center で実行されます。SD-WAN Center は仮想フォームファクター（VPX）としてのみ利用可能であり、VMware ESXi または XenServer ハイパーバイザーにインストールする必要があります。SD-WAN Center アプライアンスの構成に必要な最小リソースは、8 GB の RAM と 4 つの CPU コアです。SD-WAN [センター仮想マシンをインストールして構成する手順は次のとおりです](https://docs.citrix.com/en-us/netscaler-sd-wan-center/10/common-configuration.html) 。

Azure 接続用に **SD-WAN Center** を構成する

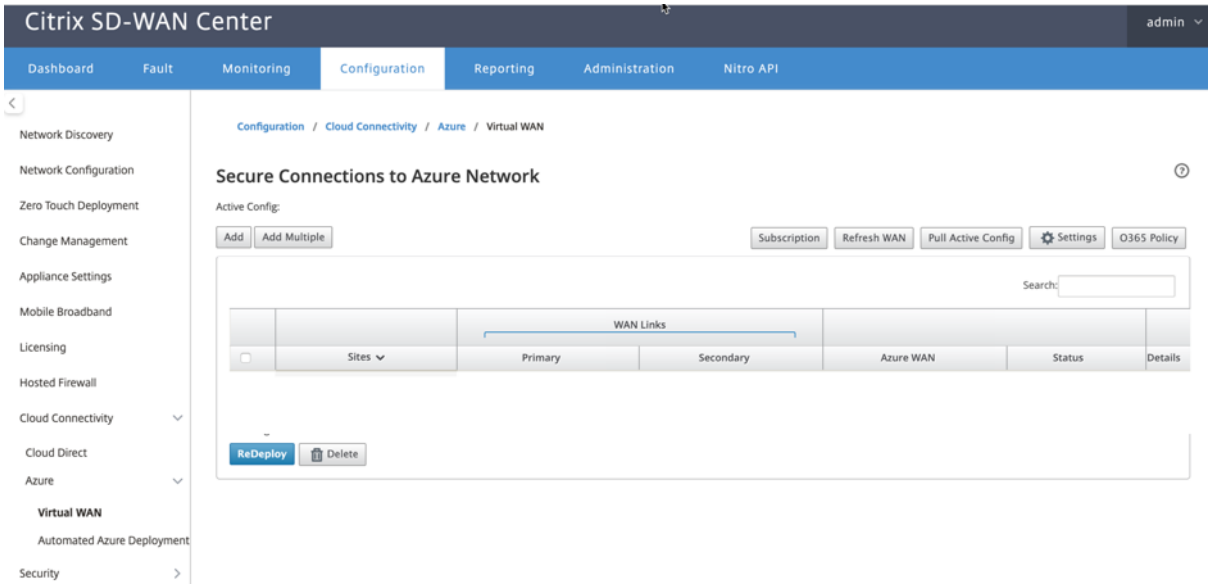
詳細については 、「サービスプリンシパルの作成 」を参照してください。

Azure で SD-WAN Center を正常に認証するには、次のパラメーターを使用できる必要があります。

- ディレクトリ（テナント ID）
- アプリケーション（クライアント ID）
- セキュアキー（クライアントシークレット）
- サブスクライバー ID

SD-WAN Center の認証:

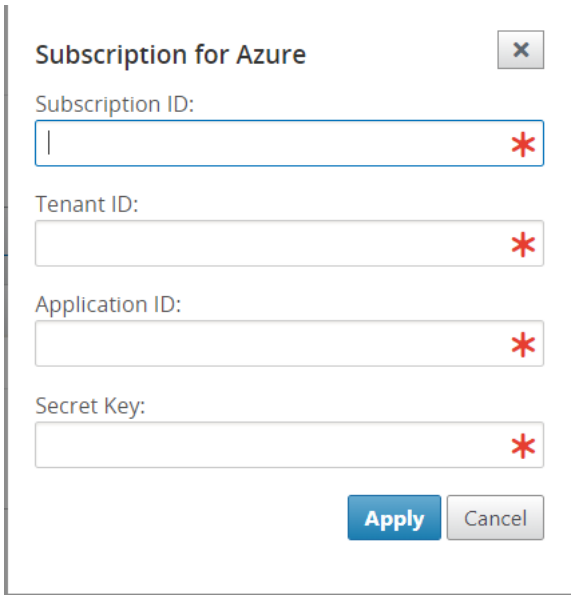
SD-WAN Center UI で、構成 > クラウド接続 > **Azure** > 仮想 **WAN** に移動します。Azure 接続設定を構成します。Azure VPN 接続、
Azure Resource Managerの設定の詳細については、次のリンクを参照してください。



11.1.0 以降のリリースでは、Azure Virtual WAN 統合のプライマリおよびセカンダリ WAN リンク構成がサポートされています。セカンダリ WAN リンクを追加する主な理由は、Citrix SD-WAN サイトに冗長性を持たせるためです。

以前の実装では、WAN リンクに障害が発生すると、トラフィックが中断し、Azure Virtual WAN への接続が失われる可能性があります。現在の実装では、プライマリ WAN リンクがダウンしていても、サイトから Azure への仮想 WAN 接続は維持されます。

サブスクリプション **ID**、テナント **ID**、アプリケーション **ID** 、および シークレットキーを入力します。この手順は、Azure で SD-WAN Center を認証するために必要です。上記で入力した資格情報が正しくない場合、認証は失敗し、それ以上のアクションは許可されません。[適用] をクリックします。

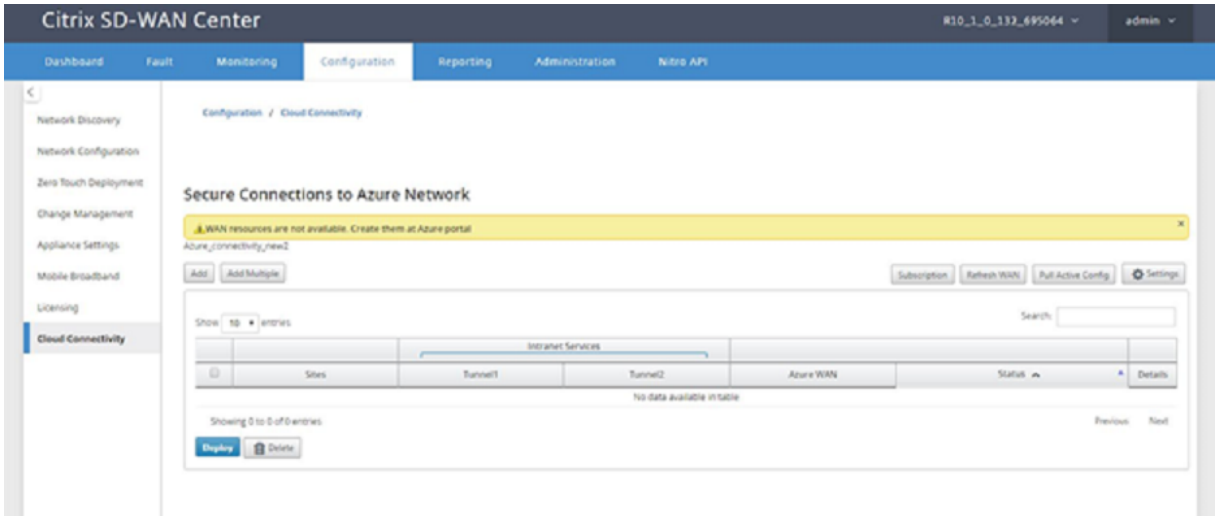


[ストレージアカウント] フィールドは、Azure で作成したストレージアカウントを指します。ストレージアカウントを作成していない場合、[適用] をクリックすると、サブスクリプションに新しいストレージアカウントが自動的に作

成されます。

Azure Virtual WAN リソースを取得する:

認証が成功すると、Citrix SD-WAN は Azure をポーリングして、Azure ポータルにログインした後の最初のステップで作成した Azure 仮想 WAN リソースのリストを取得します。WAN リソースは、Azure 内のネットワーク全体を表します。この WAN 内に含めるすべてのハブへのリンクが含まれています。WAN は互いに分離されており、共通のハブや、異なる WAN リソースの 2 つの異なるハブ間の接続を含めることはできません。



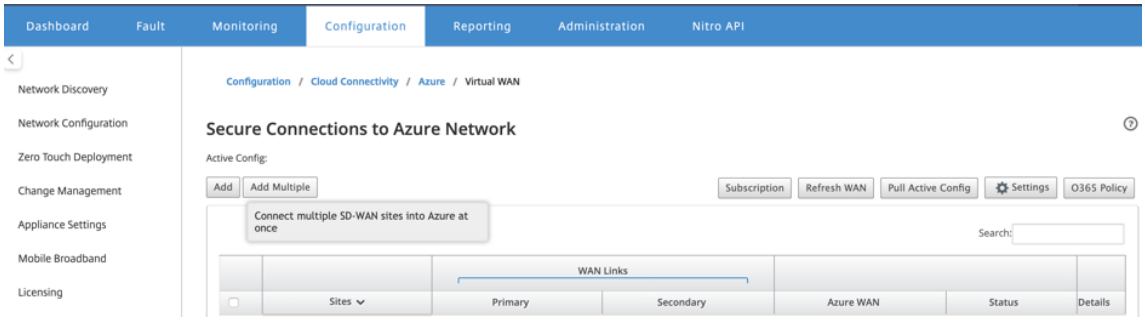
ブランチサイトと Azure WAN リソースを関連付けるには:

IPsec トンネルを確立するには、ブランチサイトを Azure WAN リソースに関連付ける必要があります。1 つのブランチは Azure 仮想 WAN リソース内の複数のハブに接続でき、1 つの Azure 仮想 WAN リソースは複数のオンプレミスブランチサイトに接続できます。各ブランチから Azure への仮想 WAN リソースデプロイメントの単一行を作成します。

複数のサイトを追加するには:

それぞれのサイトをすべて追加して、選択した単一の WAN リソースに関連付けることができます。

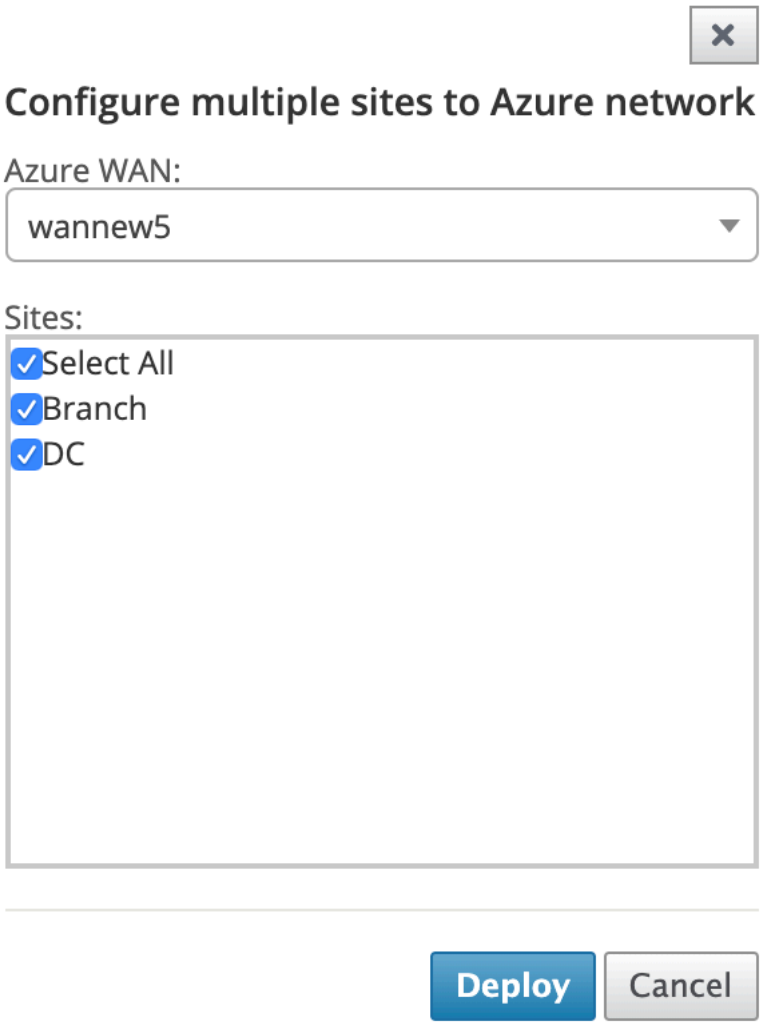
1. [複数追加] を クリックして、選択した WAN リソースに関連付ける必要のあるすべてのサイトを追加します。



2. Azure WAN リソースのドロップダウンリスト（下に表示）には、Azure アカウントに属するリソースが事前に入力されています。WAN リソースが作成されていない場合、このリストは空であるため、Azure ポータル

に移動してリソースを作成する必要があります。リストに WAN リソースが入力されている場合は、ブランチサイトの接続先となる **Azure WAN** リソース を選択します。

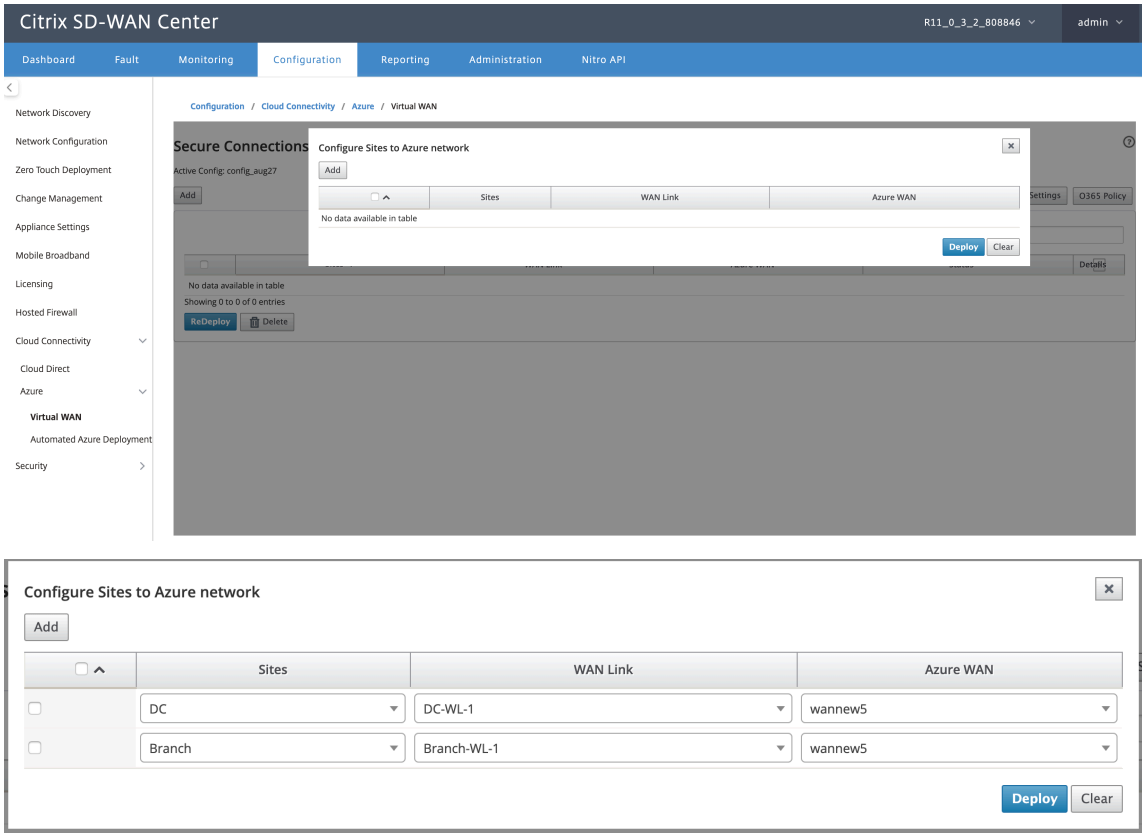
3. 1 つまたはすべてのブランチサイトを選択して、IPsec トンネルの確立プロセスを開始します。サイトの最高容量のパブリックインターネット WAN リンクが自動的に選択され、Azure VPN Gateway への IPsec トンネルが確立されます。



単一のサイトを追加するには:

また、サイトを 1 つずつ（単一）追加し、ネットワークの拡大に合わせて追加することもできます。サイトごとの展開を実行している場合は、上記のように複数のサイトを追加することもできます。

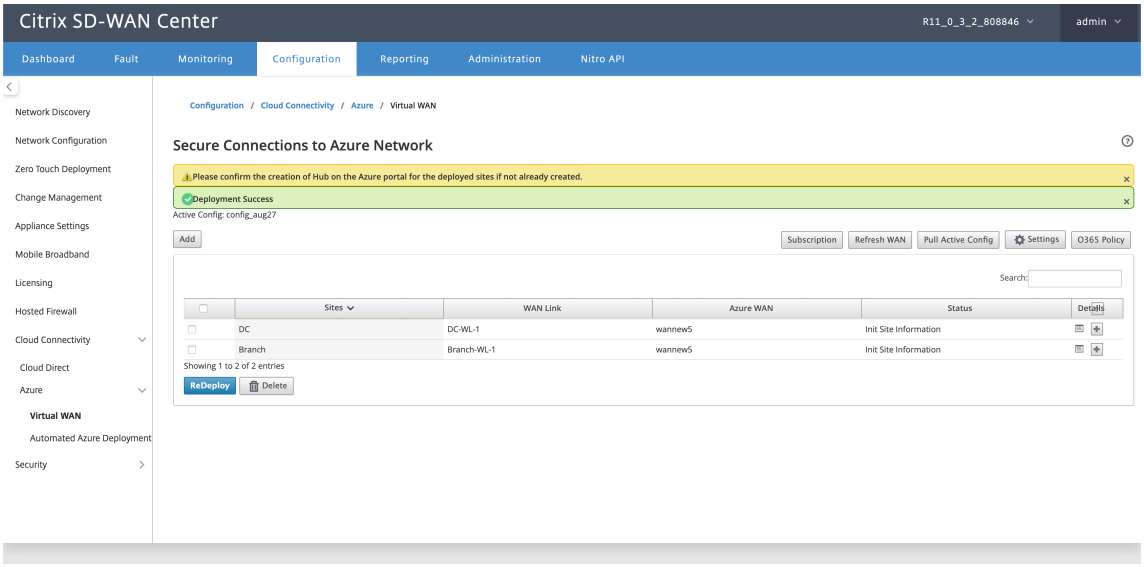
1. **Add New Entry** をクリックして、Site-Wan アソシエーションのサイト名を 1 つ選択します。[**Azure** ネットワーク へのサイトの構成] ダイアログボックスでサイトを追加します。



2. Azure Virtual WAN ネットワークに構成するブランチサイトを選択します。
3. サイトに関連付けられている WAN リンクを選択します（パブリックインターネットタイプのリンクは、物理リンクの容量が大きい順にリストされています）
4. **Azure Virtual WANs** ドロップダウンメニューから、サイトを関連付ける必要がある WAN リソースを選択します。
5. [デプロイ] をクリックして、関連付けを確認します。ステータス（「初期化サイト情報」「プッシュされたサイト情報」& 「VPN 構成を待機しています」）が更新され、プロセスについて通知されます。

デプロイプロセスには次のステータスが含まれます。

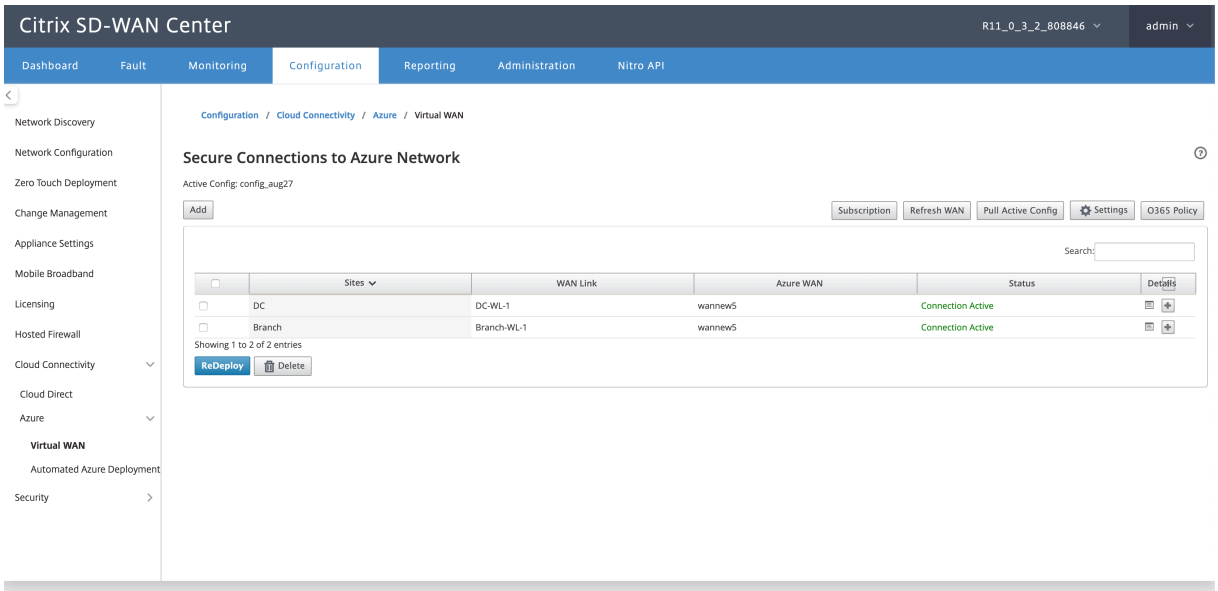
- サイト情報をプッシュ
- VPN 構成を待機しています
- 展開されたトンネル
- Connection Active（IPsec Tunnel is up）または Connection Down（IPsec Tunnel is down）

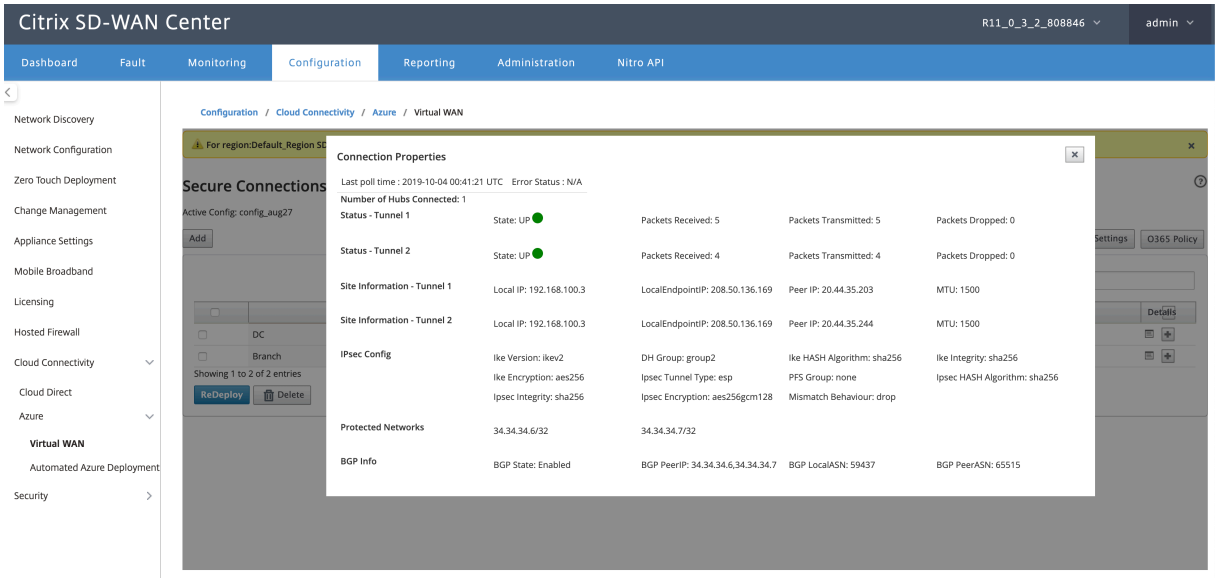


Associate Site Wan Resource Mappings（**Azure** ポータル）：

Azure ポータルにデプロイされたサイトを、Azure 仮想 WAN リソースの下に作成された仮想 HUB に関連付けます。1 つ以上の仮想 HUB をブランチサイトに関連付けることができます。各仮想 HUB は特定のリージョンに作成され、仮想ネットワーク接続を作成することにより、特定のワークロードを仮想 HUB に関連付けることができます。ブランチサイトと仮想 HUB の関連付けが成功した後にのみ、VPN 構成がダウンロードされ、サイトから VPN Gateway へのそれぞれの IPsec トンネルが確立されます。

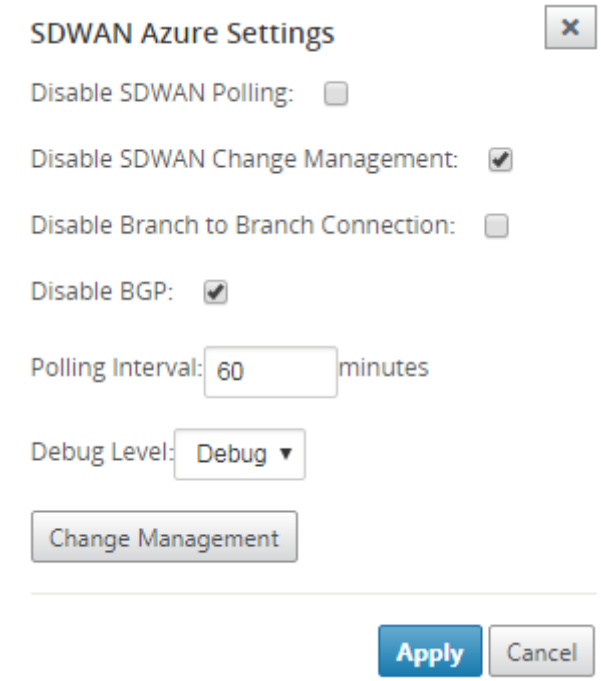
ステータスが [展開されたトンネル] または [接続がアクティブ] に変わるのを待って、**IPsec** トンネル 設定を表示します。選択したサービスに関連付けられている IPsec 設定を表示します。





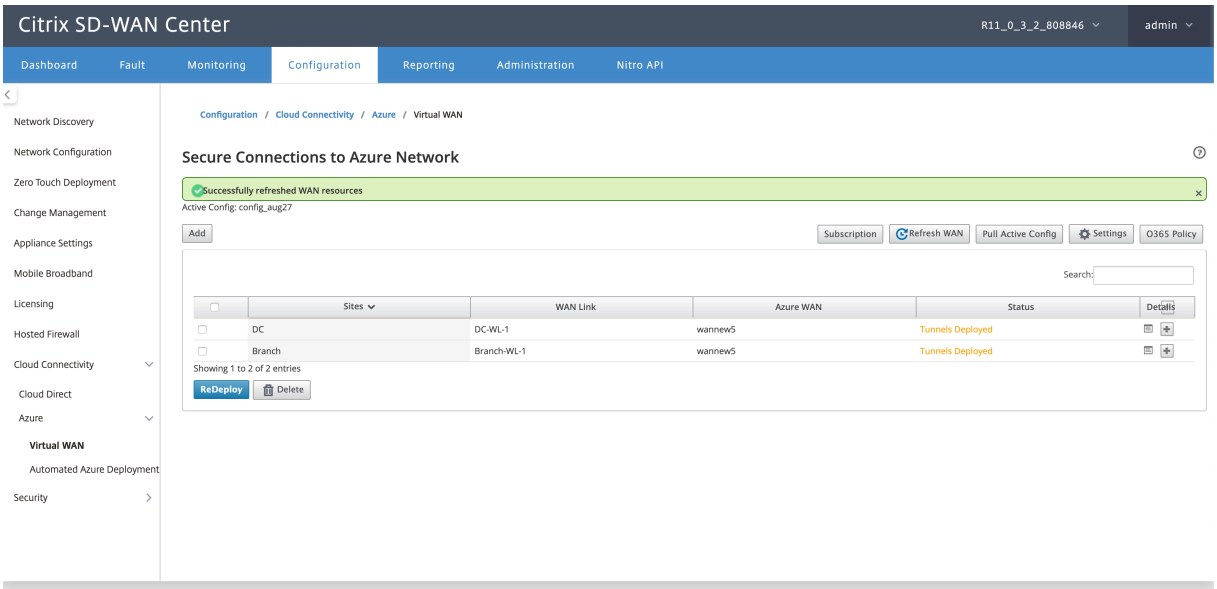
SD-WAN Azure 設定:

- **SD-WAN** 変更管理を無効にする–デフォルトでは、変更管理プロセスは自動化されています。つまり、Azure Virtual WAN インフラストラクチャで新しい構成が利用可能になると、SD-WAN Center はそれを取得して、ブランチへの適用を自動的に開始します。ただし、構成をブランチに適用する必要がある場合を制御する場合は、この動作が制御されます。自動変更管理を無効にする利点の 1 つは、この機能と他の SD-WAN 機能の構成が個別に管理されることです。
- **SDWAN** ポーリングを無効にする–すべての SD-WAN Azure の新しい展開と既存の展開でのポーリングを無効にします。
- ポーリング間隔 - ポーリング間隔オプションは、Azure 仮想 WAN インフラストラクチャで構成の更新を検索する間隔を制御します。ポーリング間隔の推奨時間は 1 時間です。
- ブランチ間の接続を 無効にする–Azure Virtual WAN インフラストラクチャを介したブランチ間の通信を無効にします。デフォルトでは、このオプションは無効になっています。これを有効にすると、オンプレミスのブランチが相互に通信でき、Azure の仮想 WAN インフラを介して IPsec を介してブランチの背後にあるリソースと通信できるようになります。これは、SD-WAN 仮想パスを介したブランチ間通信には影響を与えません。ブランチは相互に通信でき、それぞれのブランチと通信できます resources/end このオプションが無効になっている場合でも、仮想パスをポイントします。
- **BGP** を無効にする–BGP over IP を無効にします。デフォルトでは無効になっています。有効にすると、サイトルートが BGP を介してアドバタイズされます。
- デバッグレベル–接続の問題がある場合、ログをキャプチャしてデバッグすることができます。

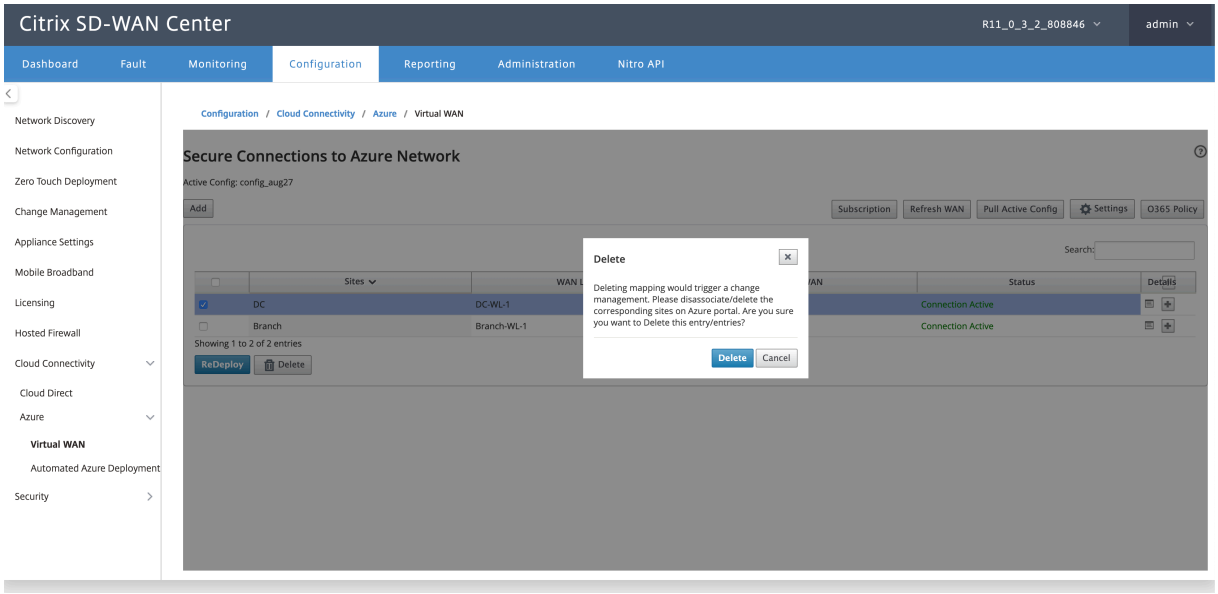


WAN リソースを更新する:

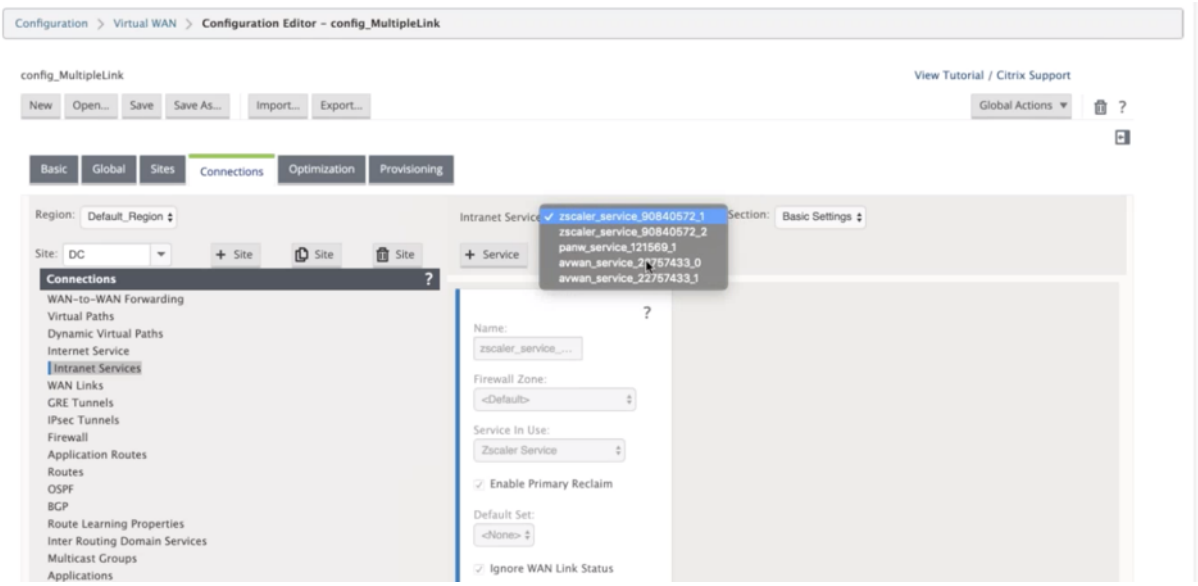
[更新] アイコンをクリックして、Azure Portal で更新した WAN リソースの最新のセットを取得します。更新プロセスが完了すると、「WAN リソースが正常に更新されました」というメッセージが表示されます。



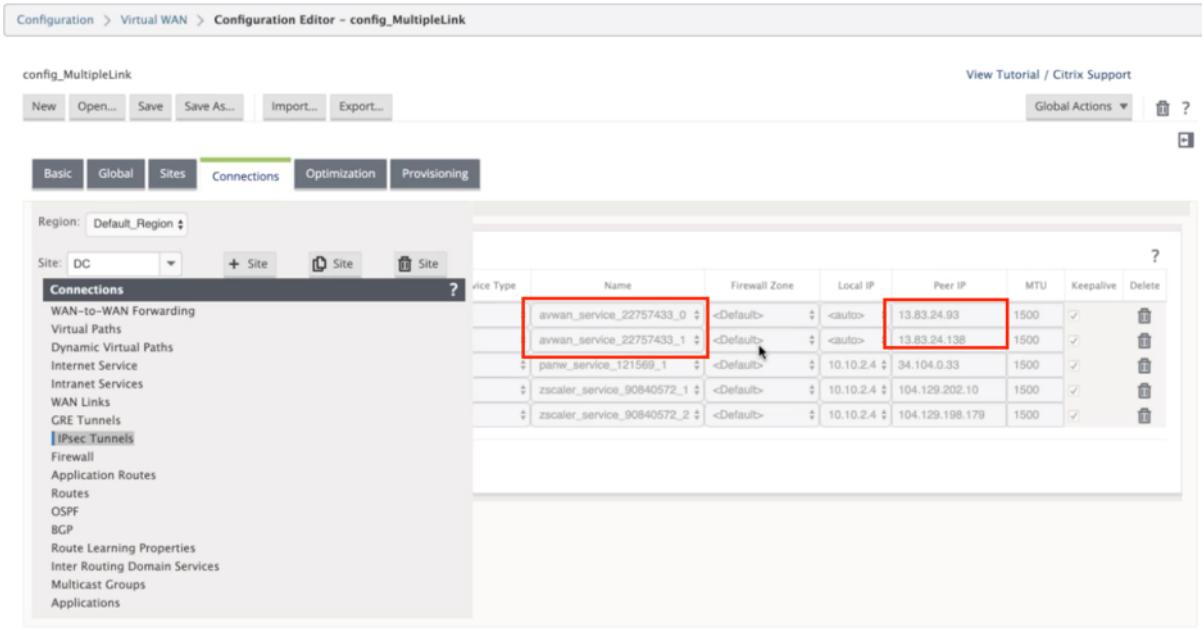
サイト **WAN** リソースの関連付けを削除する　削除を実行する 1 つまたは複数のマッピングを選択します。内部的には、SD-WAN アプライアンスの変更管理プロセスがトリガーされ、成功するまで、[削除] オプションは無効になり、それ以上の削除は実行されません。マッピングを削除するには、Azure ポータルで対応するサイトの関連付けを解除するか削除する必要があります。ユーザーはこの操作を手動で実行する必要があります。



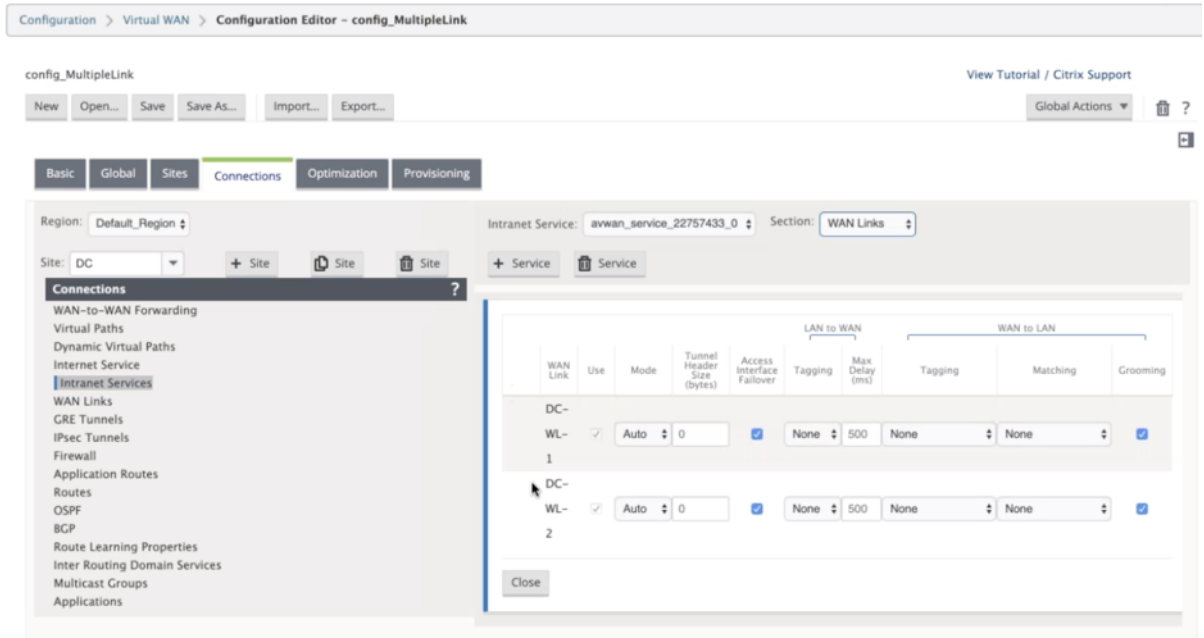
トンネルが作成されると、MCN に作成された 2 つのイントラネットサービスが表示されます。



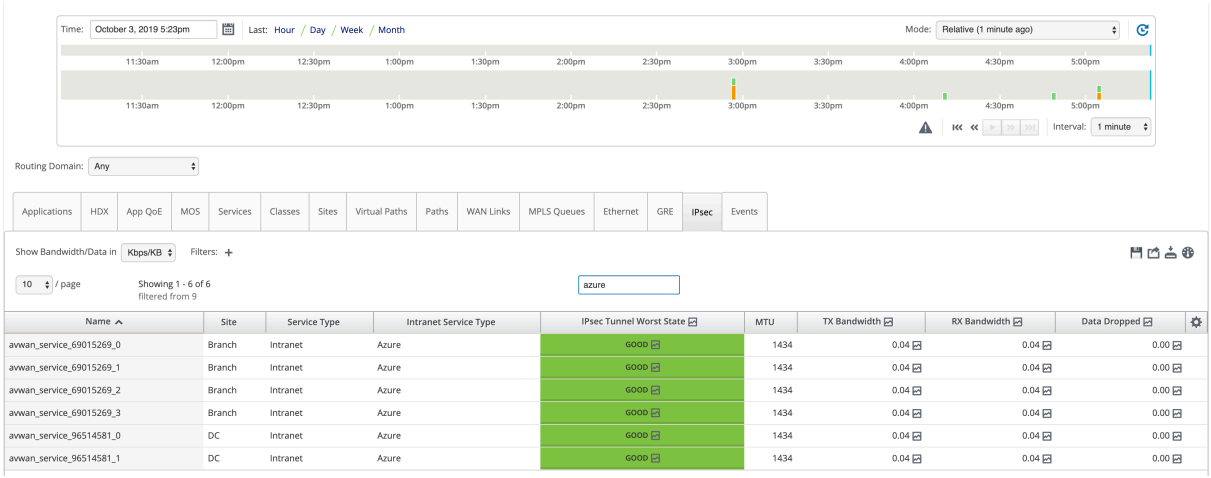
各イントラネットサービスは、ピア IP（Azure 仮想 WAN エンドポイント IP）で作成された IPsec トンネルに対応しています。



イントラネットサービスで、[セクション] ドロップダウンリストから [**WAN** リンク] を選択すると、指定したプライマリとセカンダリの両方の WAN リンクが表示されます。デフォルトでは、モードは **Auto** に設定されています。



IPsec トンネルの監視　SD-WAN Center UI で、レポート > **IPsec** で IPsec トンネルのステータスをチェックする。データトラフィックが流れるためには、トンネルステータスが緑である必要があります。



Cloud Direct サービス

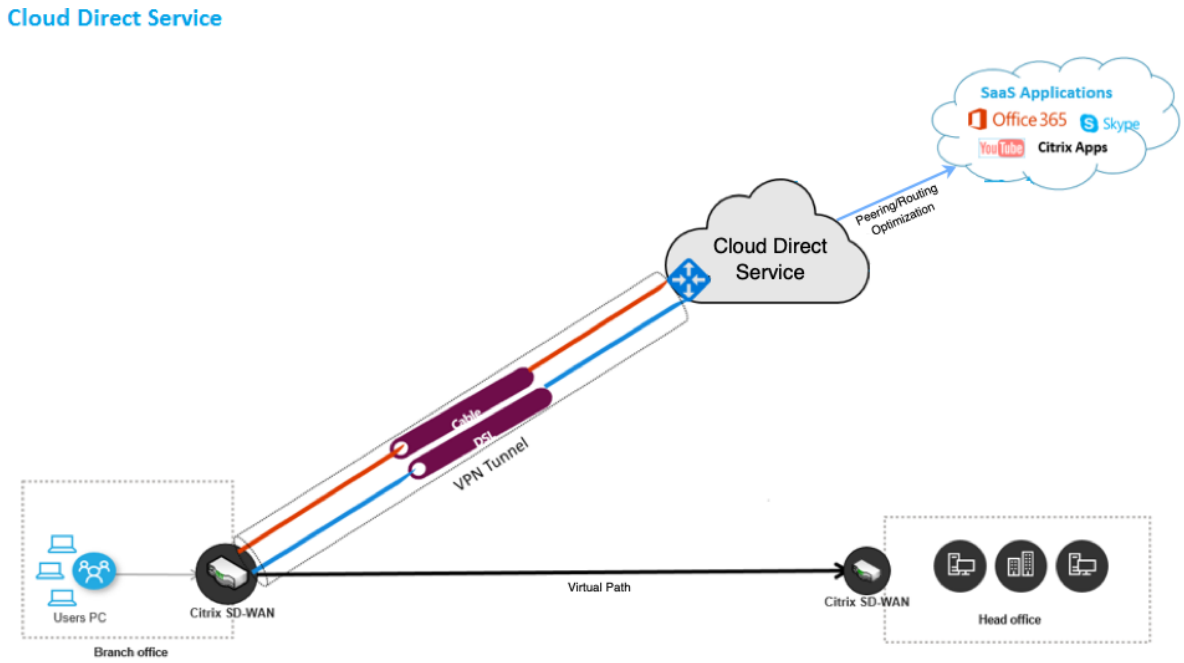
April 13, 2021

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、すべてのインターネット行きのトラフィックに信頼性の高い安全な配信を通じて SD-WAN 機能をクラウドサービスとして提供します。ネットワークの可視性と管理が向上します。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。

Cloud Direct サービスには次の利点があります。

- 冗長性 -複数のインターネット WAN リンクを使用し、シームレスなフェイルオーバーを提供します。
- リンク集約 -すべてのインターネット WAN リンクを同時に使用します。
- さまざまなプロバイダーからの WAN 接続間でのインテリジェントな負荷分散:
  - パケット損失、ジッター、スループットの測定。
  - カスタムアプリケーションの識別。
  - アプリケーション要件と回路パフォーマンスのマッチング（リアルタイムのネットワーク条件に適応）。
- インターネット回線への SLA グレードの動的 QoS 機能:
  - 変化する回路スループットに動的に適応します。
  - 入力および出力エンドポイントでのトンネルを介した適応。
- コールをドロップせずに、回線間で VOIP コールを再ルーティングする
- エンドツーエンドの監視と可視性。

Cloud Direct サービスワークフロー



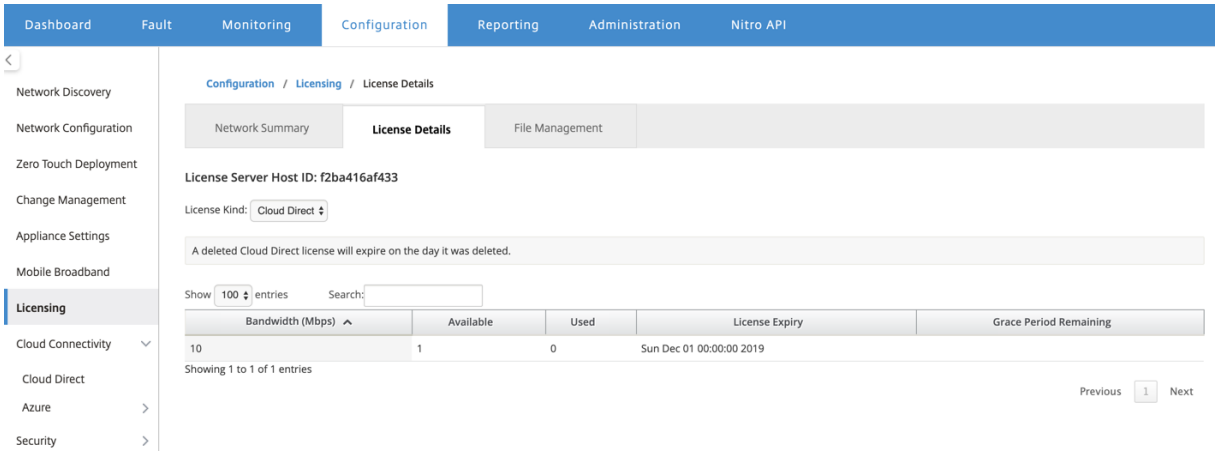
Cloud Direct Service のデプロイを開始する前に、次の手順が完了していることを確認してください:

1. 410-SE、210-SE、または 1100-SE/PE エディションアプライアンス。工場出荷時のアプライアンスの SD-WAN バージョンが 9.3.5 より前の場合は、USB の再イメージ化手順に従って、アプライアンスを最新の出荷ベースイメージにアップグレードする必要があります。
2. シングルステップアップグレード 手順を実行して、Cloud Direct Service をサポートするソフトウェアバージョンをインストールします。
3. MCN アプライアンスを構成し、ブランチで仮想パスを確立します。
    - ブランチサイトを構成します。詳しくは、「ブランチを構成する」を参照してください。
    - アプリケーションベースのルートのアプリケーションオブジェクトを作成します。
        - Cloud Direct サービスを介してアプリケーションを選択的に操作する場合は、対応するアプリケーションを含めてアプリケーションオブジェクトを作成します。Cloud ダイレクトサービスを介してルーティングされるアプリケーションオブジェクトの作成方法を参照してください。インターネット行きのトラフィックを管理するには、アプライアンス構成エディターからインターネットサービスを作成する必要があります。詳しくは、「インターネットサービス」を参照してください。
        - Citrix Cloud Direct サービスを介してインターネットにバインドされたすべてのトラフィックを誘導する場合は、特定のアプリケーションオブジェクトの作成をスキップできます。

ライセンス

Cloud Direct サービス機能は、SD-WAN の基本ライセンスとは別にライセンスされます。Cloud Direct サービスに必要なライセンスが SD-WAN Center にインストールされていることを確認します。詳細については、ライセンスサーバーとしての Citrix SD-WAN Center.sd-wan-center-as-license-server を参照してください。

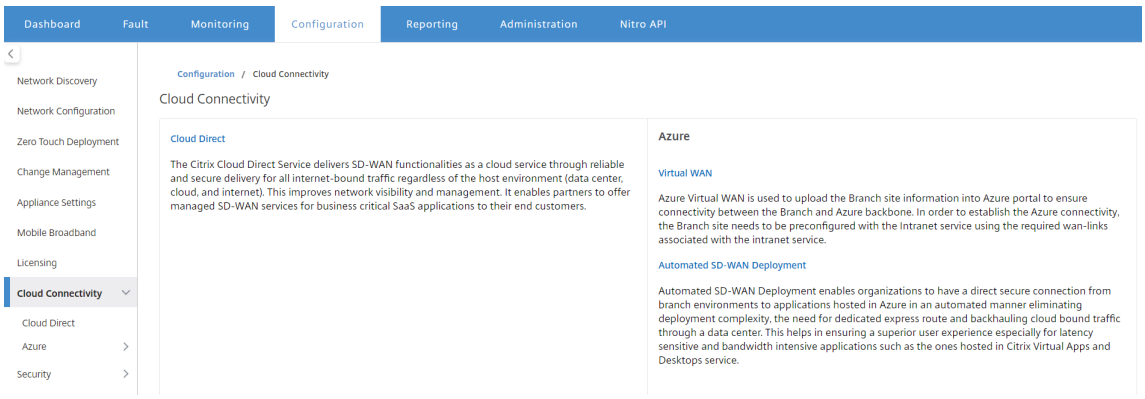
[ライセンス] ページには、インストールされている Cloud Direct サービスライセンス情報の詳細が表示されます。



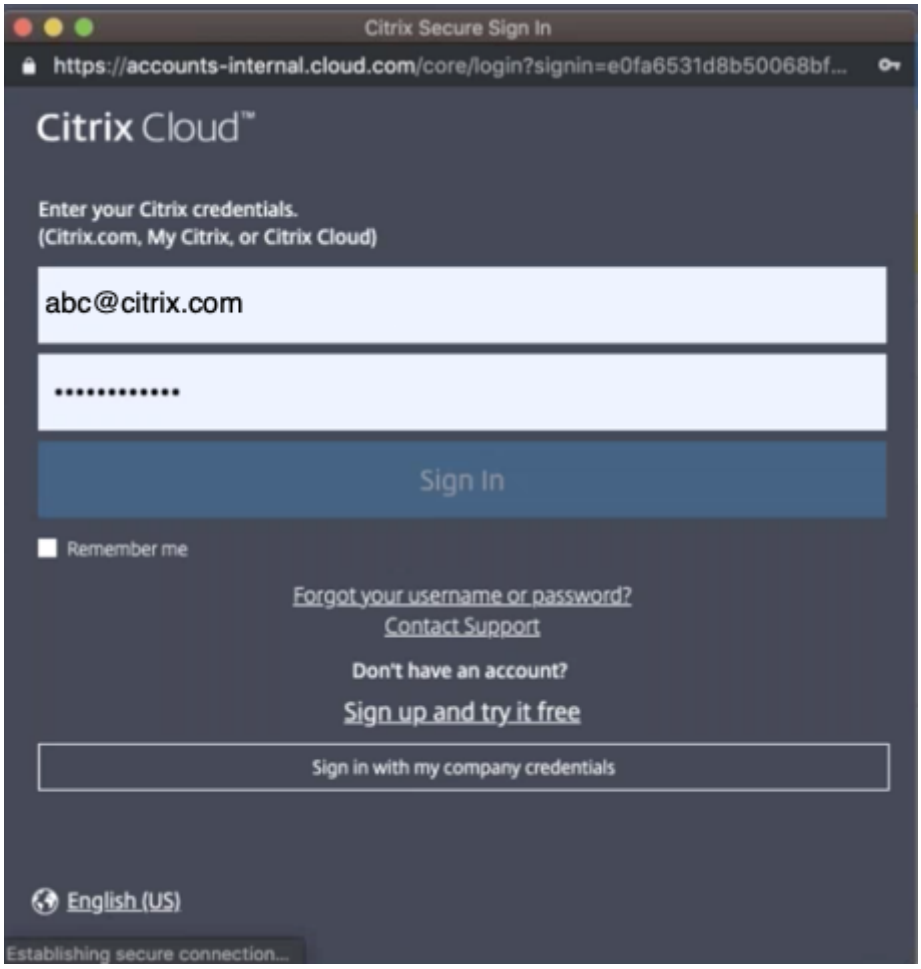
> 注
> 期限切れまたは削除された Cloud Direct ライセンスには 30 日間の猶予期間があり、その前に、デプロイされた Cloud Direct サイトが機能するための有効なライセンスをインストールする必要があります。猶予期間が満了する前に有効なライセンスがインストールされていない場合、SD-WAN Center は、期限切れのライセンスを使用してサイトの Cloud Direct サービスを無効にします。

SD-WAN Center で Cloud Direct サービスを構成する

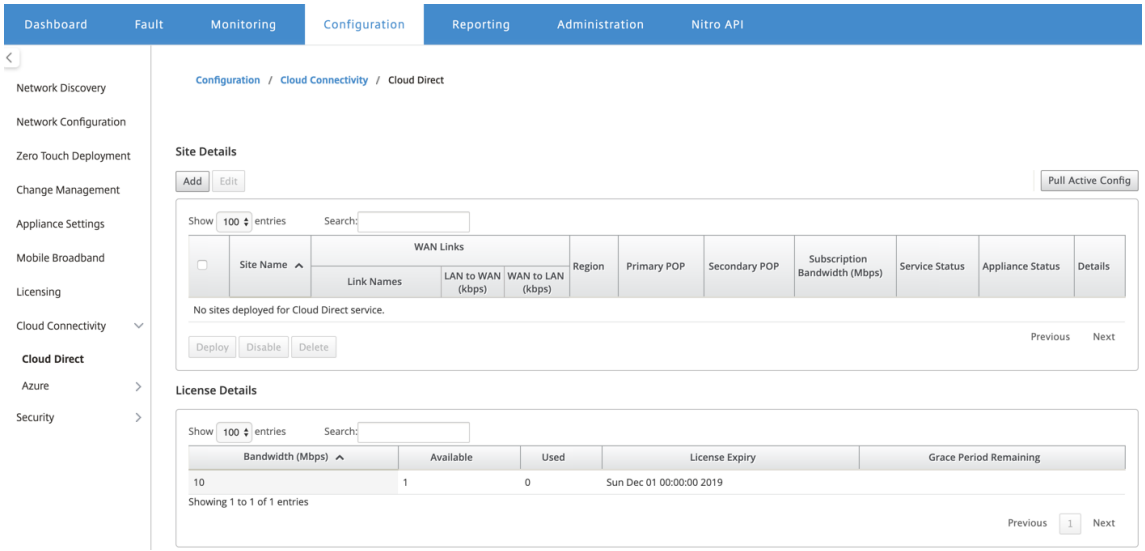
1. SD-WAN Center GUI で、設定 > クラウド接続 > **Cloud Direct** に移動します。



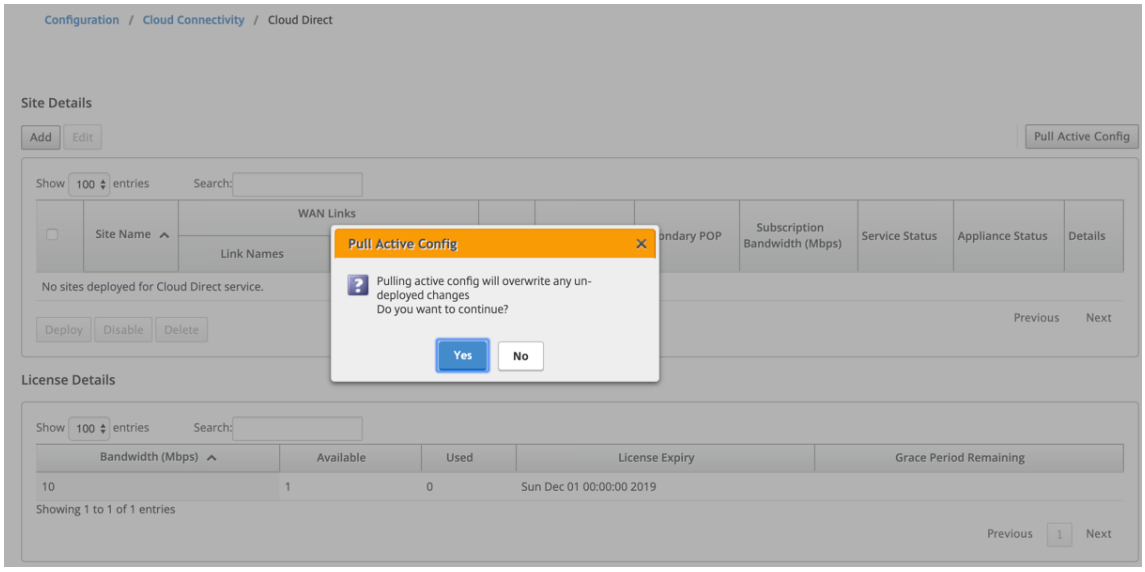
2. Citrix Cloud 資格情報でログインします。



Citrix Cloud Service に正常にログインすると、Cloud Direct のホームページが表示されます。

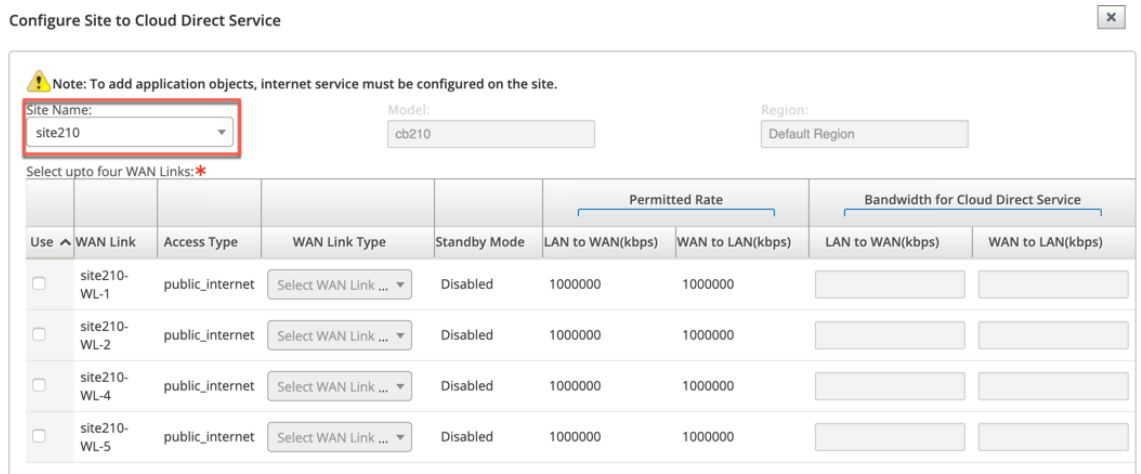


3. [アクティブな構成 をプル] をクリックして、最新のアクティブな MCN 構成を取得します。



4. [新しいサイトを追加] をクリックします。Cloud Direct サービスの展開に適格なサイトがメニューに表示されます。

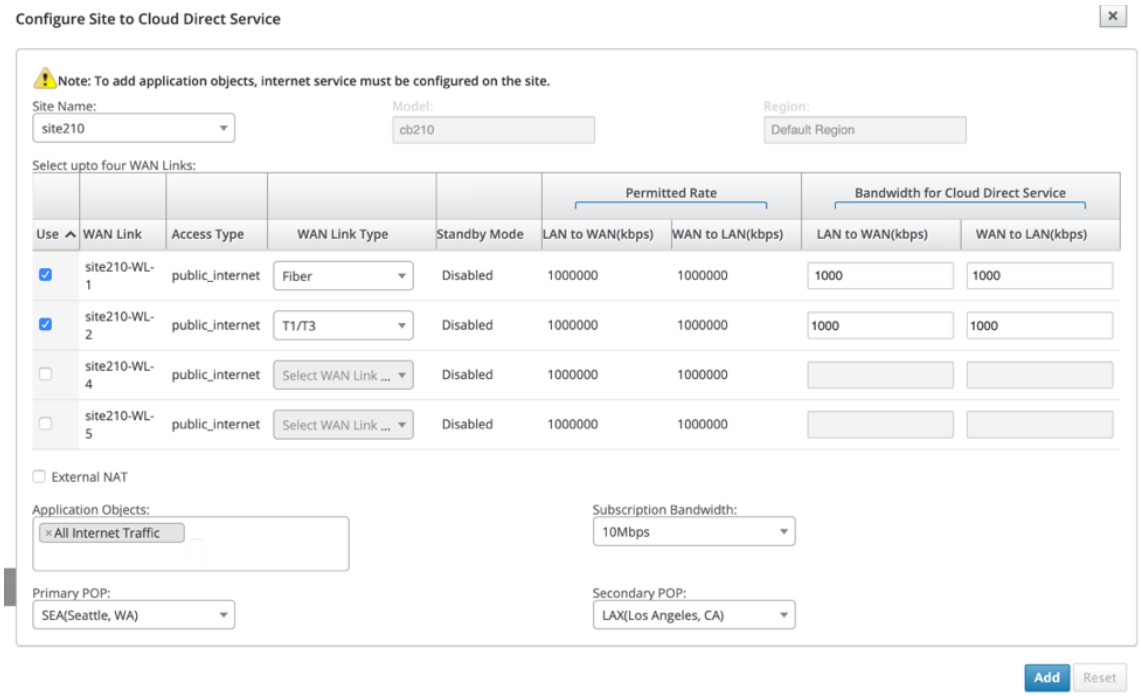
> 注
>
> - Cloud Direct サービス機能は、210、410、および 1100 ハードウェアアプライアンスでサポートされています。
> - 11.2 リリース以降、Cloud Direct サービスは SD-WAN 2100、4100、および 6100 アプライアンスでサポートされます。SD-WAN Center とオーケストレータの両方で、Cloud Direct サービス機能を SD-WAN 2100、4100、および 6100 アプライアンスに展開できます。SD-WAN Center は、Cloud Direct の最大 250 Mbps サブスクリプションライセンスをサポートします。



5. サイトを選択すると、選択したサイトに関連付けられているパブリックインターネット WAN リンクが、アプライアンスモデル情報とアプライアンスが展開されているリージョンとともに表示されます。
6. Cloud Direct サービストラフィックに使用する **WAN** リンクを、WAN リンクタイプ、アプリケーションオ

ブジェクト、サブスクリプション帯域幅、プライマリ **POP**、セカンダリ **POP** の各 オプションとともに選択します。

> 注
>
> - Cloud Direct サービスでは、最大 4 つの WAN リンクがサポートされています。
> - WAN リンク帯域幅を Cloud Direct サービス専用に予約する必要はなくなりました。Cloud Direct サービスがアクティブでない場合、仮想パス、インターネット、イントラネットサービスなど、その WAN リンクで構成された他のサービスは、構成された共有に従って帯域幅を使用できます。



- サイト名: Cloud Direct 機能の展開に適格なサイトを表示します。
- 型番: 選択したサイトでは、対応するアプライアンスモデル名が自動的に入力されます。
- 領域: 選択したサイトについて、アプライアンス固有の展開されたリージョンの詳細が自動的に入力されます。
- **WAN** リンク: 選択したサイトには、関連するパブリックインターネット WAN リンクが表示されます。
- **WAN** リンクタイプ: メニューから WAN リンクタイプを選択します。
- スタンバイモード: スタンバイモード は、WAN リンク構成から取得されます。
- **Cloud Direct Service** の帯域幅: Cloud Direct サービスが独占的に使用できる帯域幅を入力します。選択された帯域幅は、構成された許可帯域幅より小さくなければならず、仮想パス、インターネット、およびイントラネットサービスで使用できません。

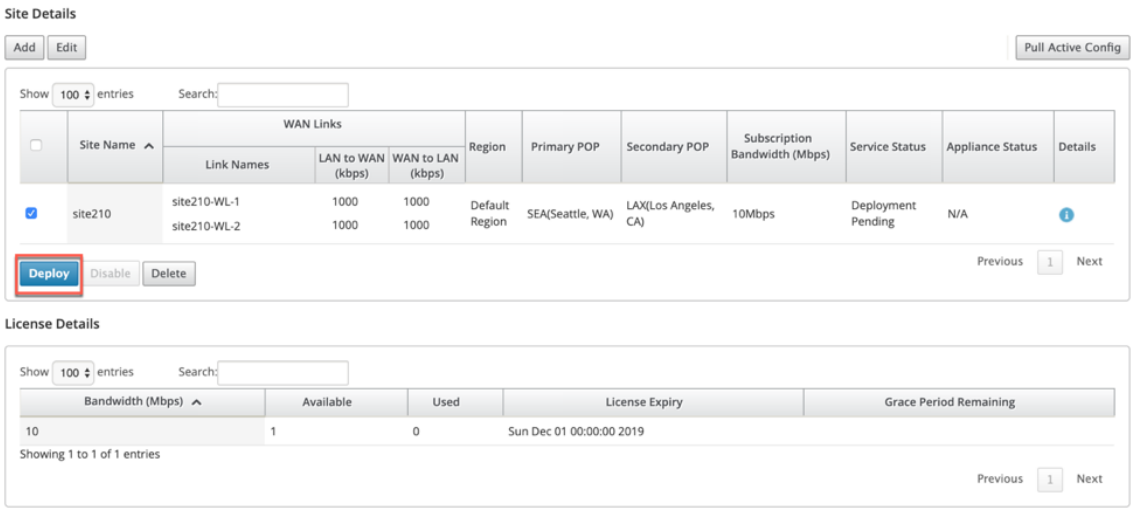
- 外部 **NAT**: ブランチ LAN ネットワークから発信されたパブリックインターネットトラフィックは、特定の IP アドレスからの送信元 NAT である必要があります。デフォルトでは、これは SD-WAN ネットワーク構成の一部として自動的に実行され、処理されます。SD-WAN デバイスの外部（外部ファイアウォールなど）で NAT IP（LAN ネットワーク）を構成する場合は、サイトの展開時に外部 NAT オプションを選択できます。LAN トラフィックを送信元 NAT にする必要がある IP は、デプロイされた Cloud Direct サイトの 詳細 ページで利用できます。
- アプリケーションオブジェクト: 特定のアプリケーションオブジェクトを選択するか、「すべてのインターネットトラフィック」を選択して、Cloud Direct サービスを介してリダイレクトできます。特定のアプリケーションオブジェクトが選択されている場合、それらのアプリケーションのトラフィックは Cloud Direct サービスを介して送信され、残りのトラフィックはアプライアンスに設定されているインターネットサービスを使用してステアリングされます。
- サブスクリプション帯域幅: サブスクリプション帯域幅は、Cloud Direct サービスのライセンスに関連付けられています。
- 課金モード: 顧客が概念実証（POC）の検証の一環として Cloud Direct サイトを展開することを計画している場合、[請求モード] フィールドを **Demo** に設定する必要があります。その他の場合はすべて、課金モードを **Production** に設定します。

> 注：請求モードがデモ または 本番として選択されている場合、次の状況が発生します:
>
> - Cloud Direct サイトが 請求モード を デモとして作成した場合、設定を本番用に編集できます。
> - Cloud Direct サイトが 請求モード で 本番環境として作成されている場合、設定を デモに編集することはできません。

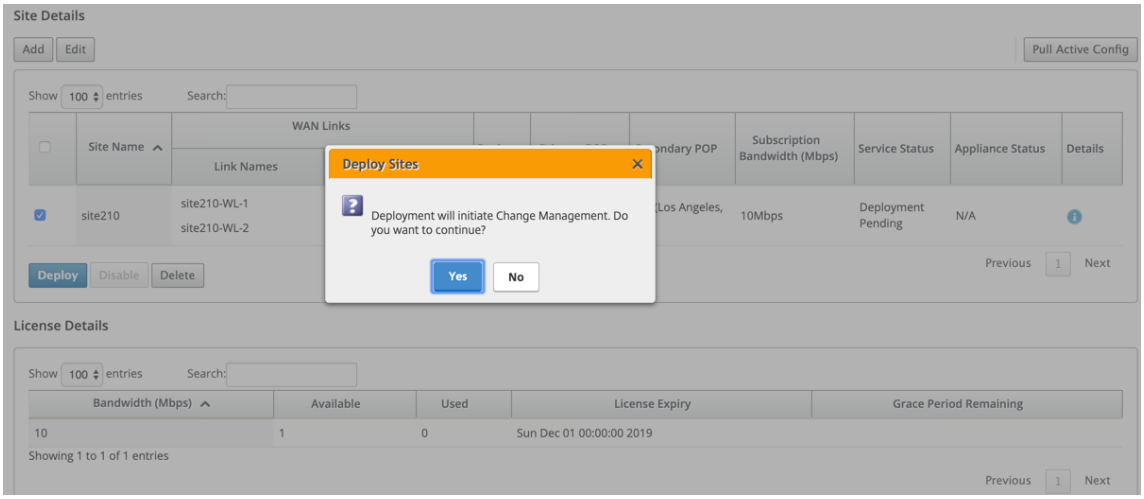
請求モード オプションは Cloud Direct の使用を有効にします trial/evaluation ライセンスは、Citrix セールスまたは認定パートナーが提供できます。Cloud Direct 評価ライセンスで動作するサイトは、デモ請求モード オプションに設定する必要があります。完全な Cloud Direct サブスクリプションライセンスにアップグレードするサイトは、**Production Billing Mode** オプションに設定する必要があります。

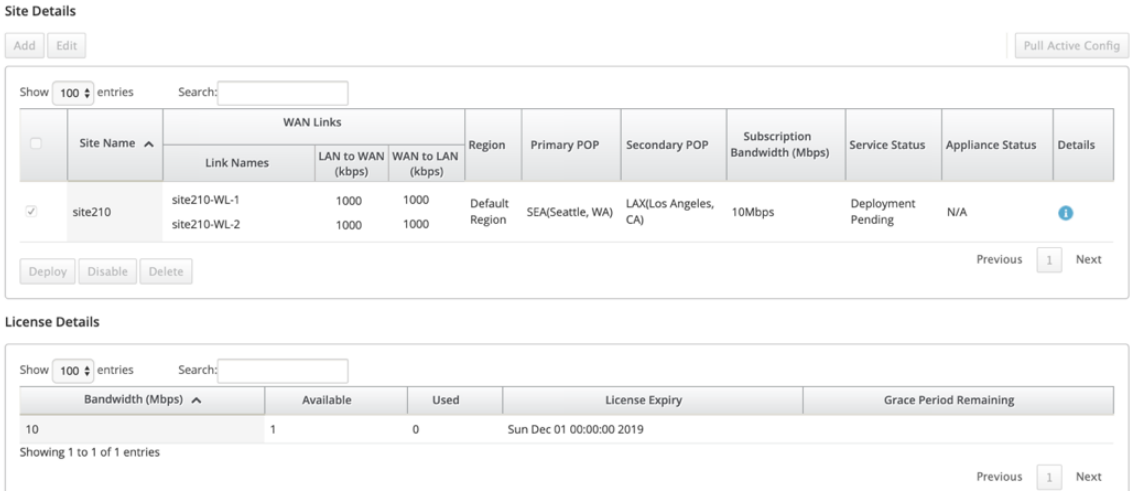
- Primary/Secondary ポップ: プライマリ POP とセカンダリ POP が同じでないことを確認してください。場所の近接度に応じて POP を選択します。[追加] をクリックします。

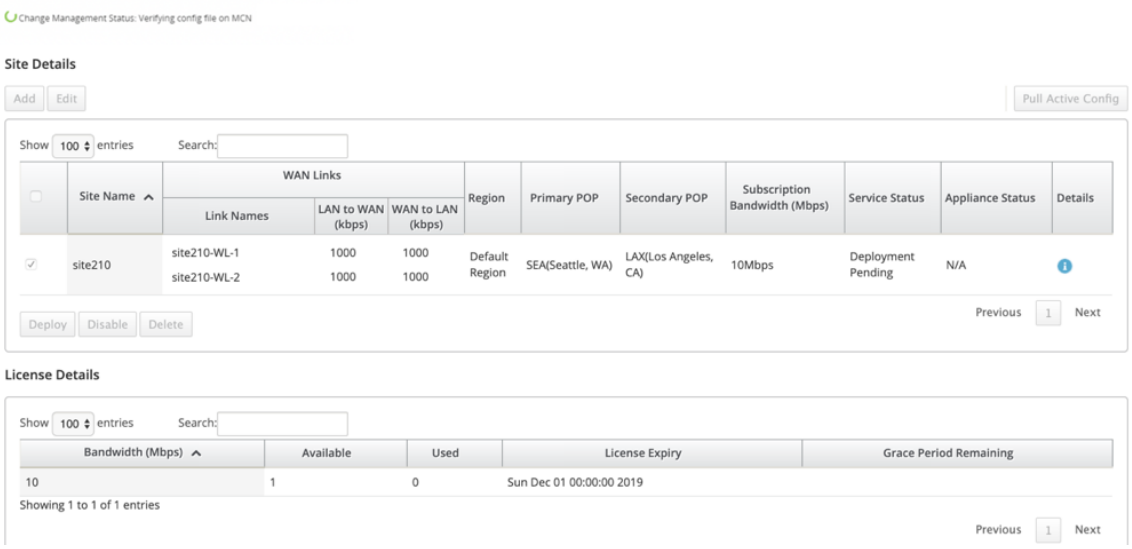
7. サイトが追加された後、サービスのステータス は **[Deployment is Pending]** と表示されます。Cloud Direct サービスをデプロイするサイトを選択し、[デプロイ] をクリックします。

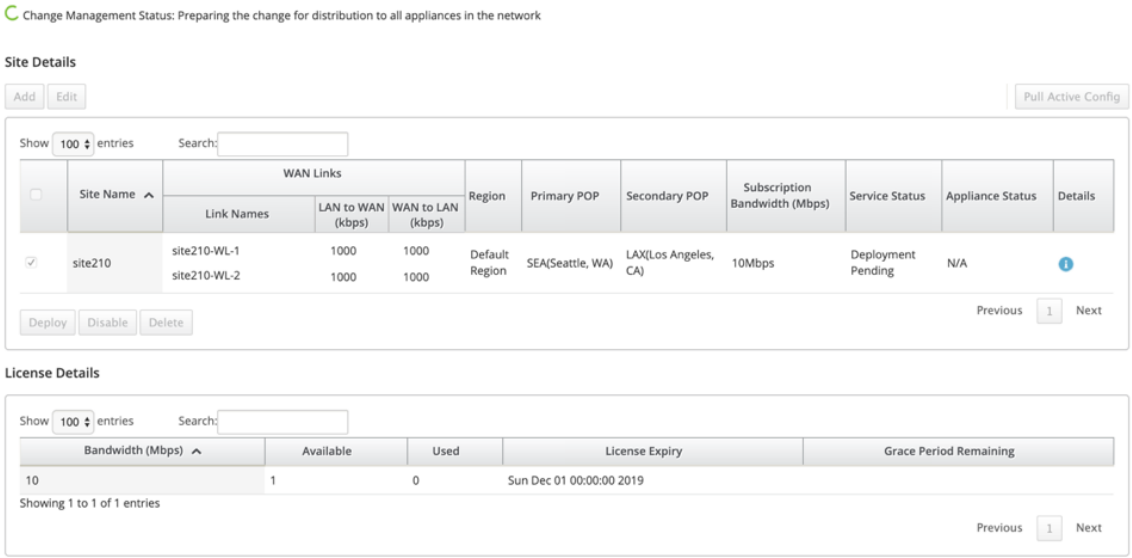


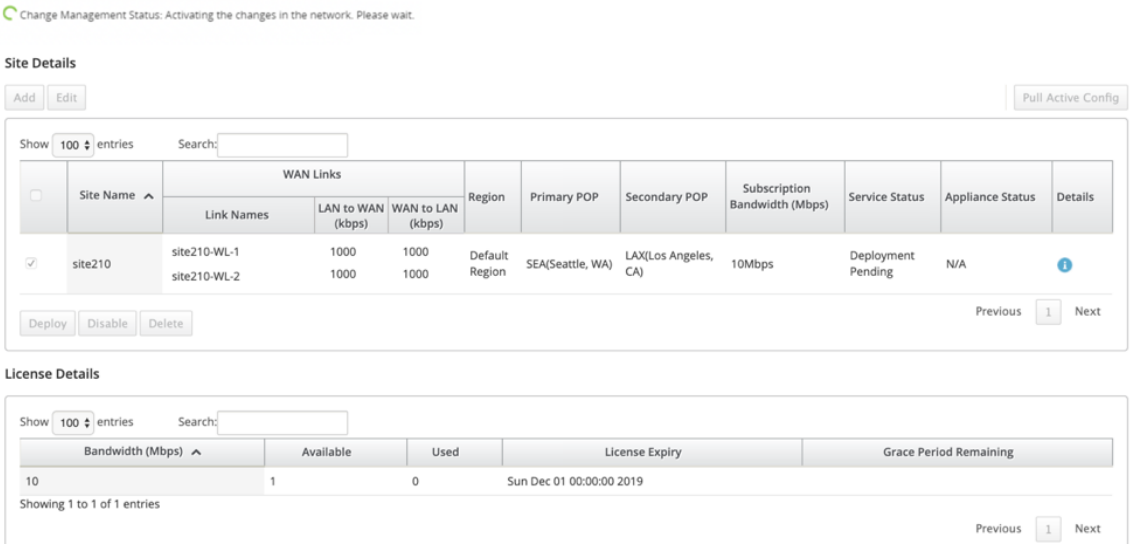
デプロイ操作が MCN アプライアンスで変更管理を開始することを示す通知が表示されます。[はい] または [いいえ] をクリックします。

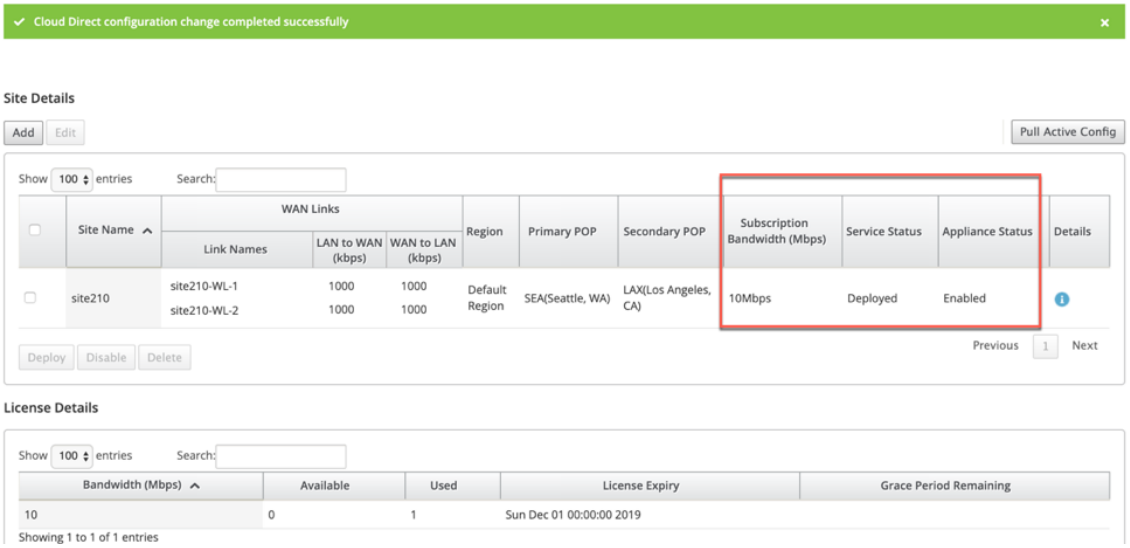










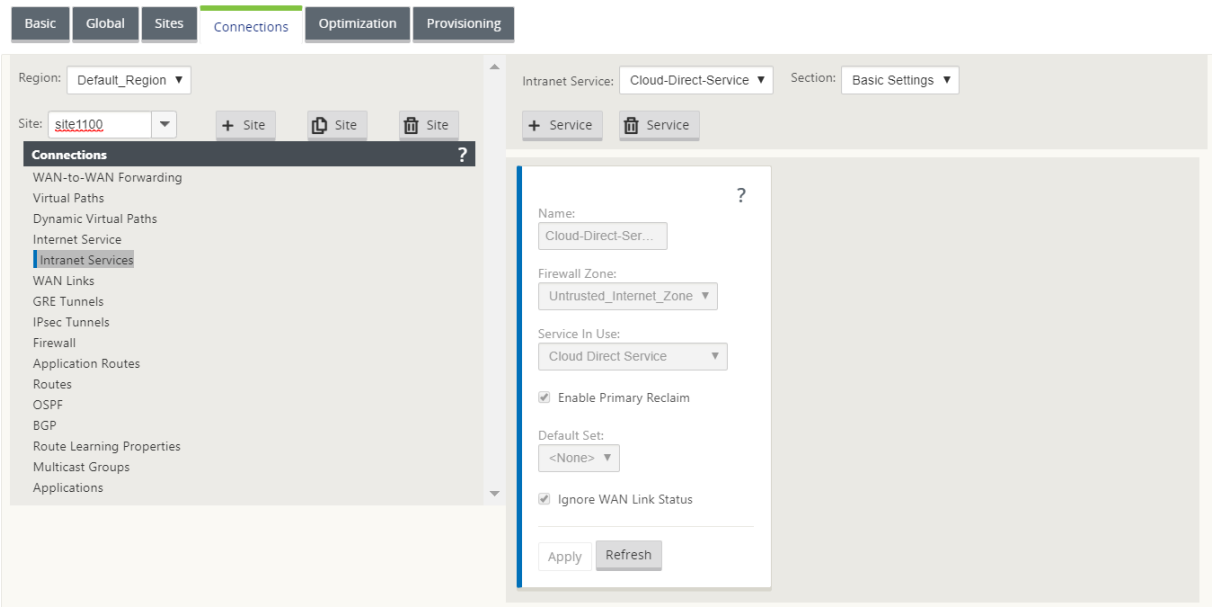


サイトが正常にデプロイされると、Cloud Direct サービスページに次のように表示されます。

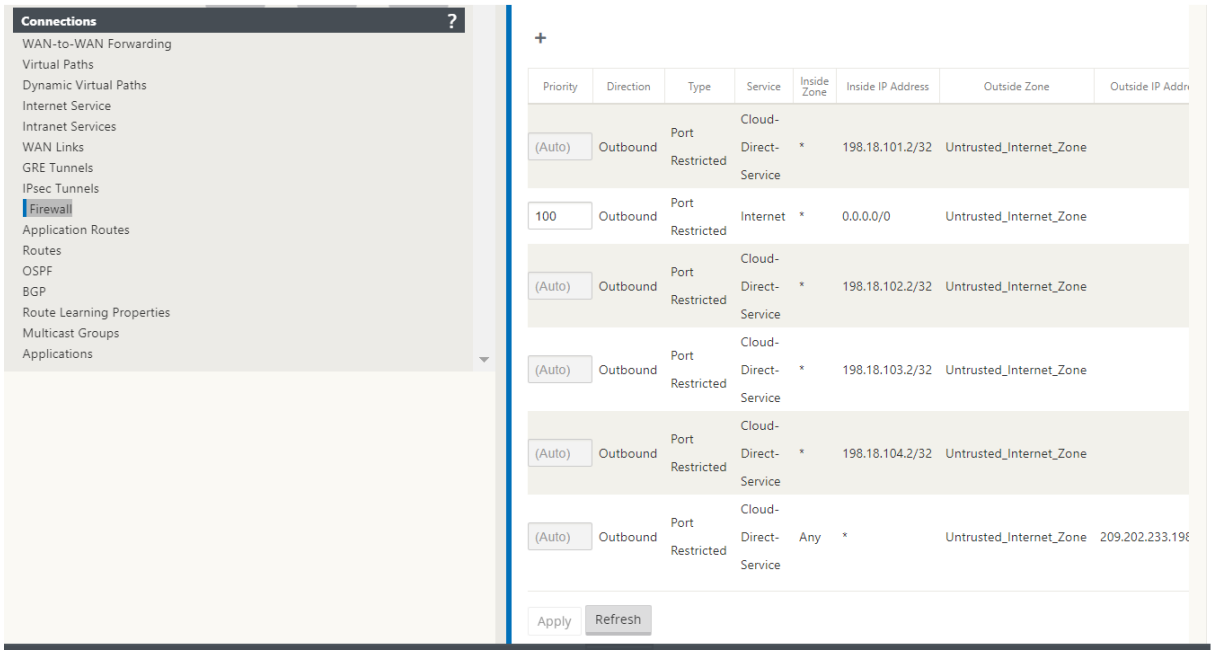
- サービス状況: 配備済み
- アプライアンスのステータス: 有効
- サブスクリプション帯域幅（**Mbps**）: 10 Mbps
- インストールされたライセンスを消費しました

上記の変更管理ステップでは、必要な Cloud Direct サービス構成が自動生成され、実行中の構成に追加されます。

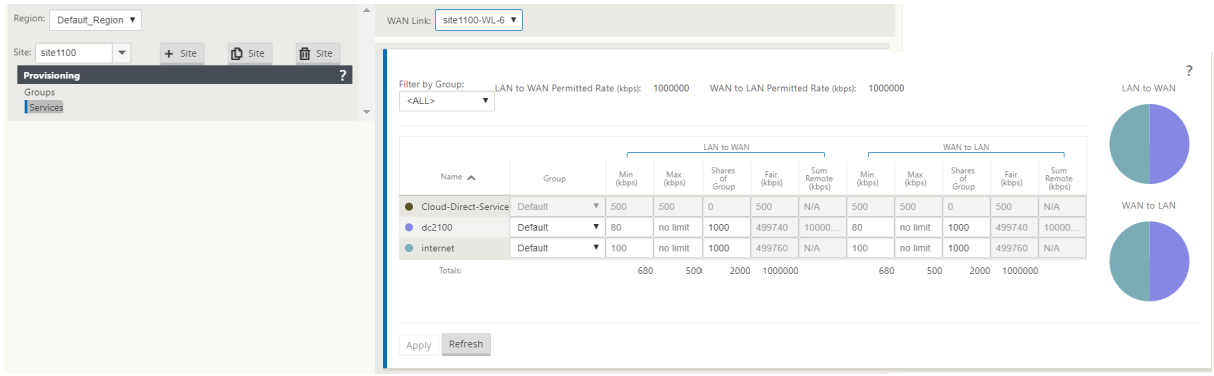
> 注
>
> 自動作成された **Cloud Direct Service** （イントラネットサービス）は、Default_RoutingDomain に関連付けられています。



ファイアウォールの設定

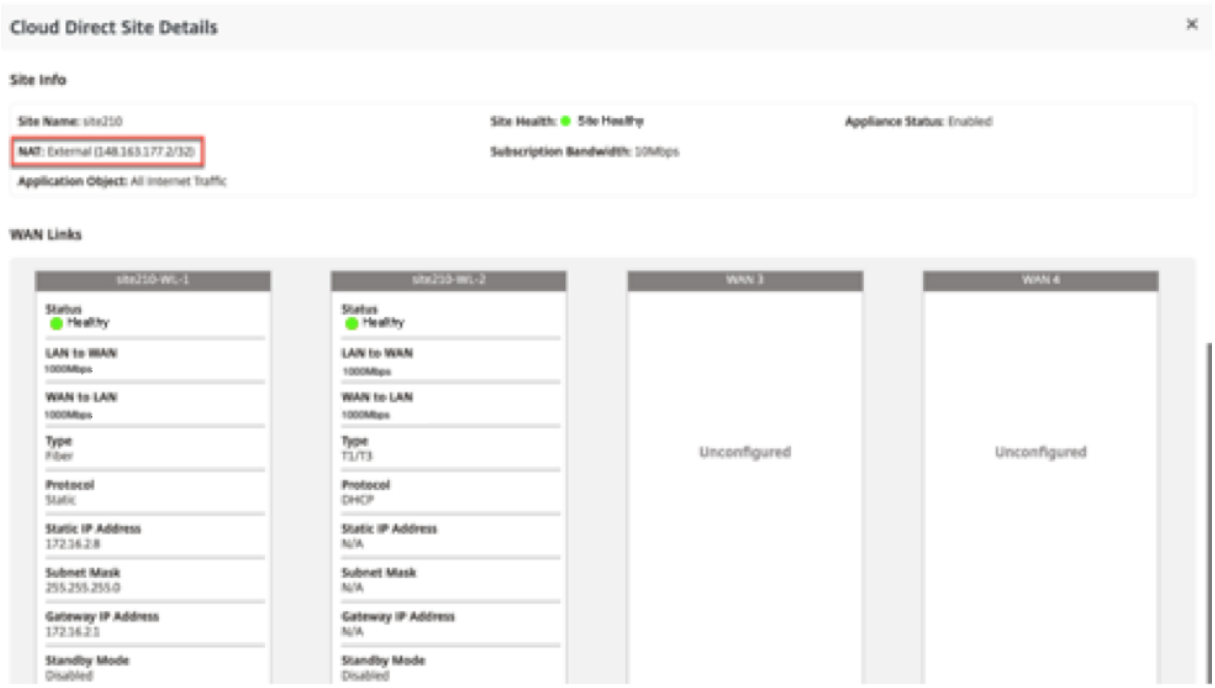


SD-WAN アプリケーション GUI でのサイトのプロビジョニング

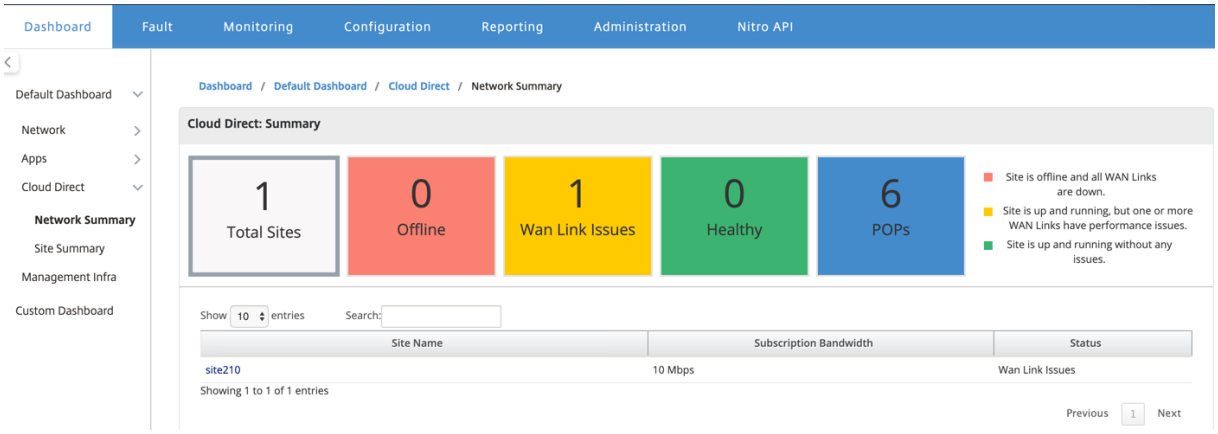


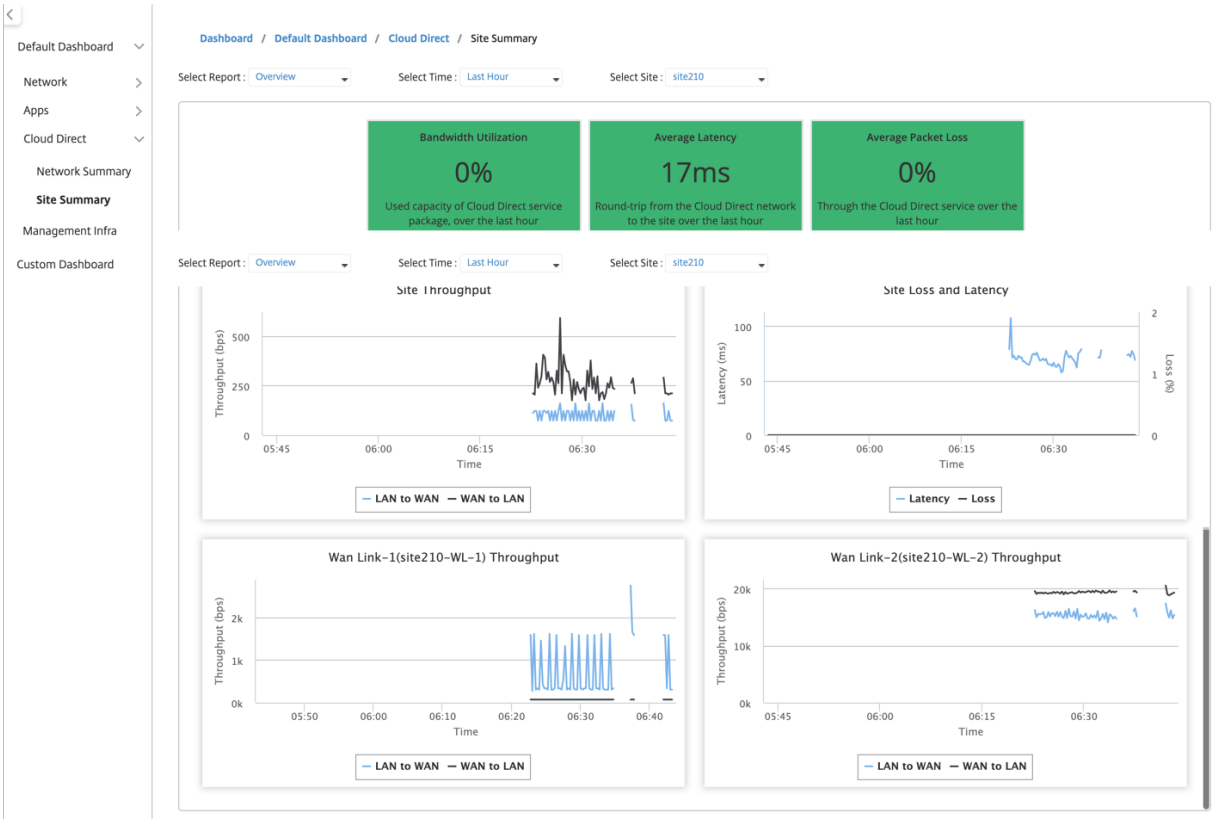
Cloud Direct サービスのモニタリング

サイトがデプロイされて有効にされた後、構成された Cloud Direct サービスを表示できます。[詳細] 列の感嘆符アイコンをクリックして、サイトの詳細を表示します。



ダッシュボード > クラウドダイレクト > ネットワークの概要 と サイトの概要 に移動すると、サイトの概要グラフを表示できます

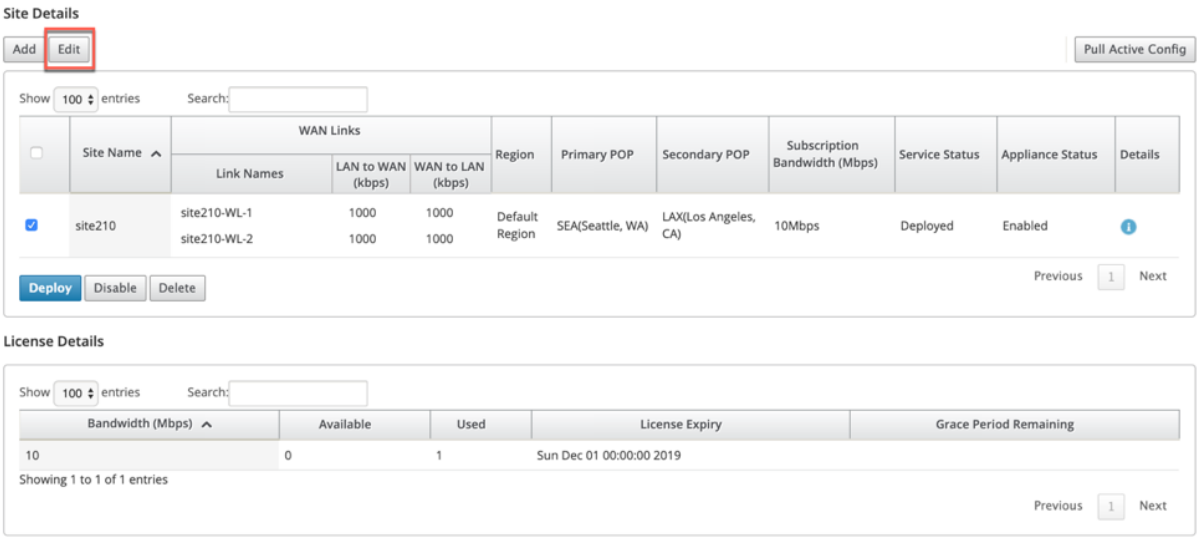


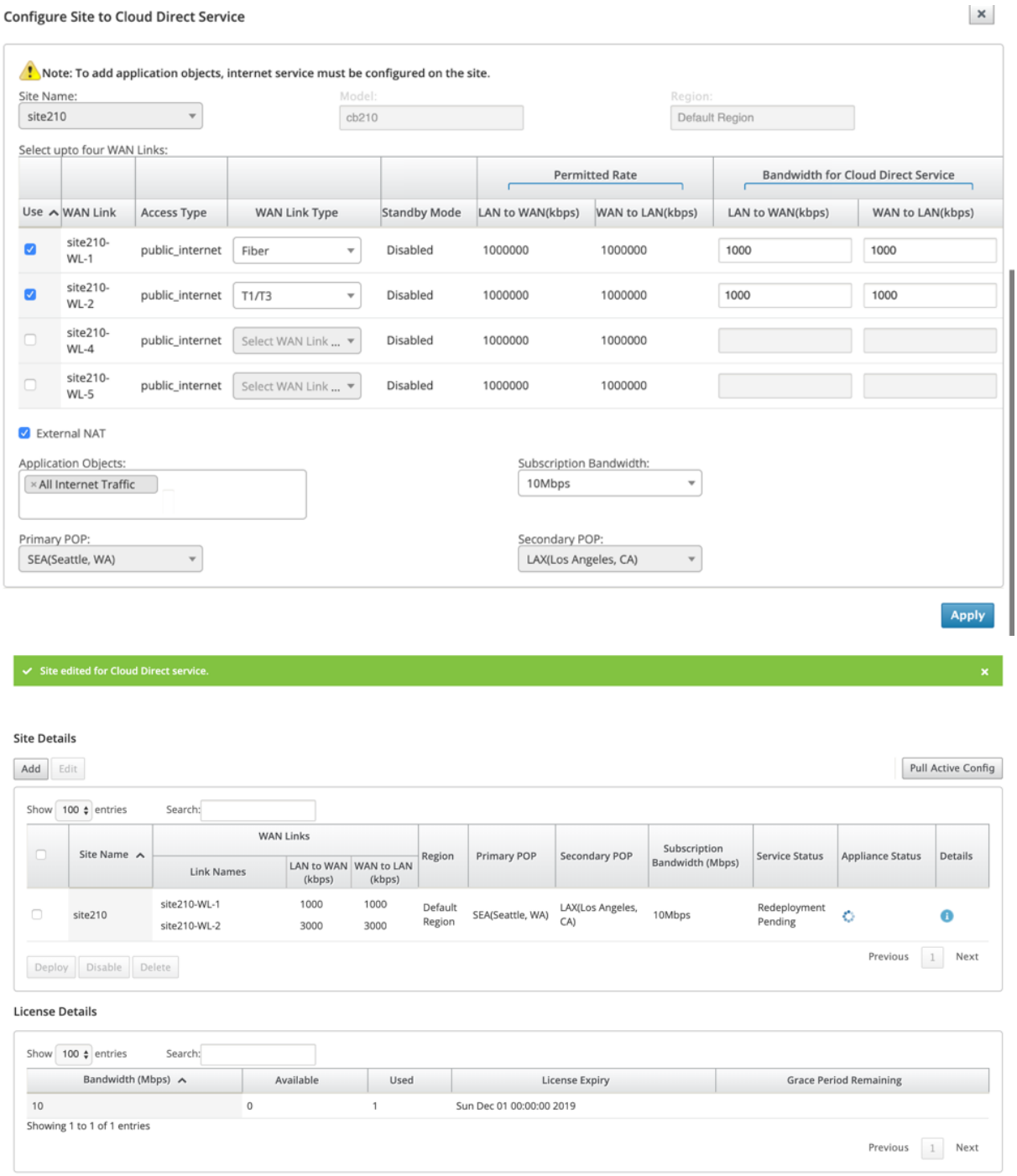


SD-WAN Center の編集サイト

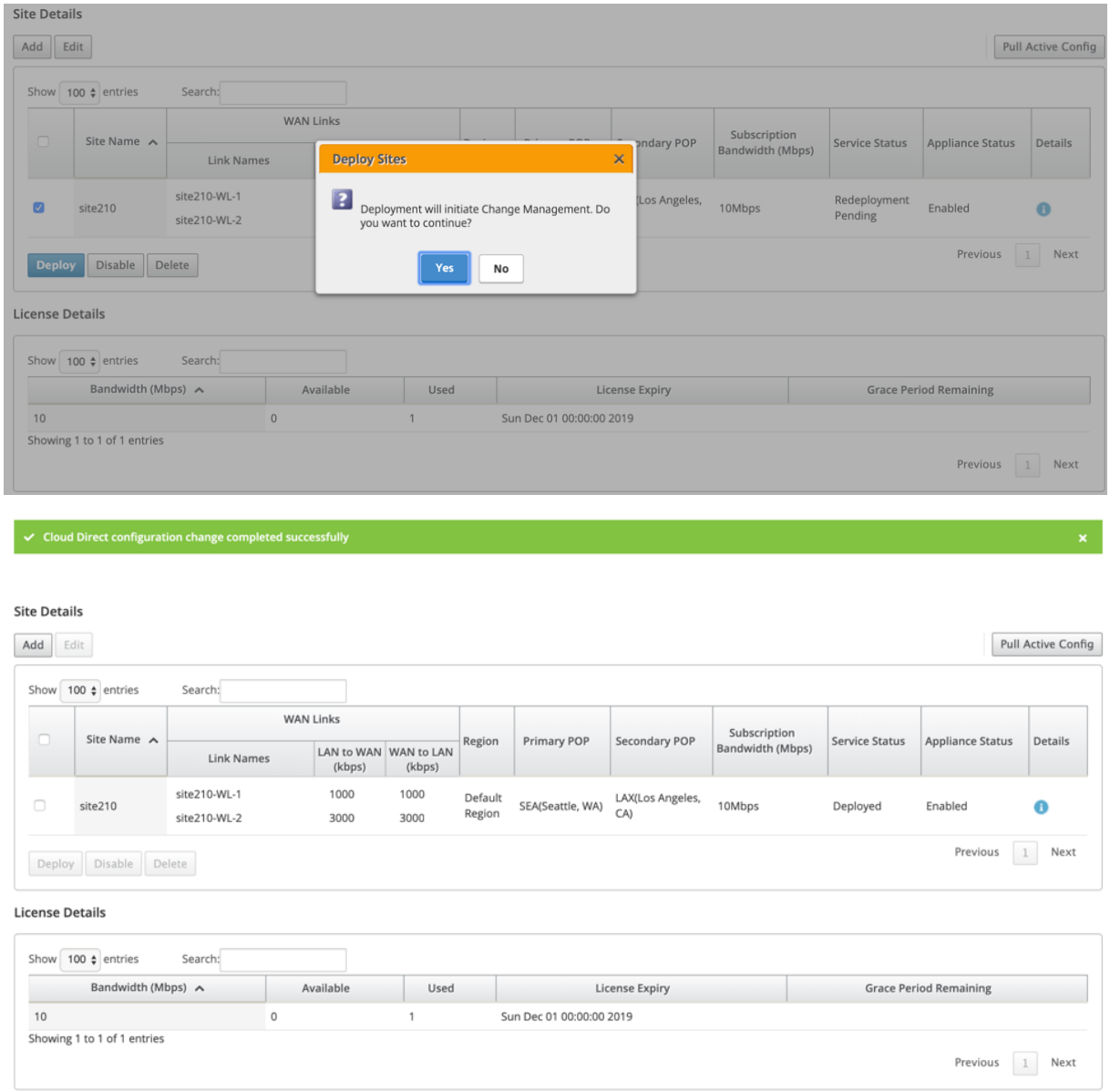
サイトを編集して、帯域幅と WAN リンクタイプを変更できます。

> 注
>
> POP 選択は編集できません。



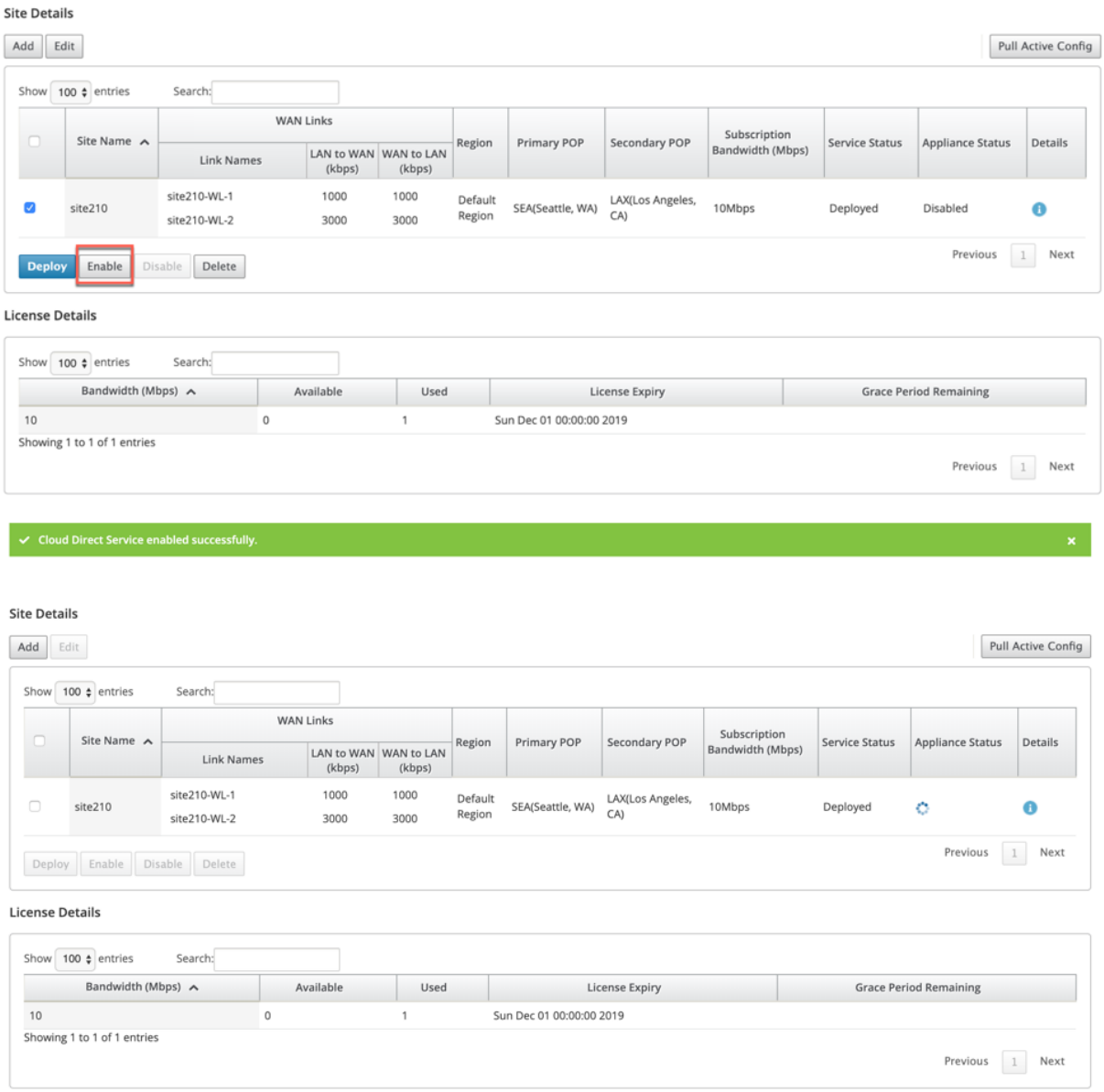


サービスステータスは、再展開保留中と表示されます。サイトをデプロイします。編集したサイトの展開プロセスが完了しました。

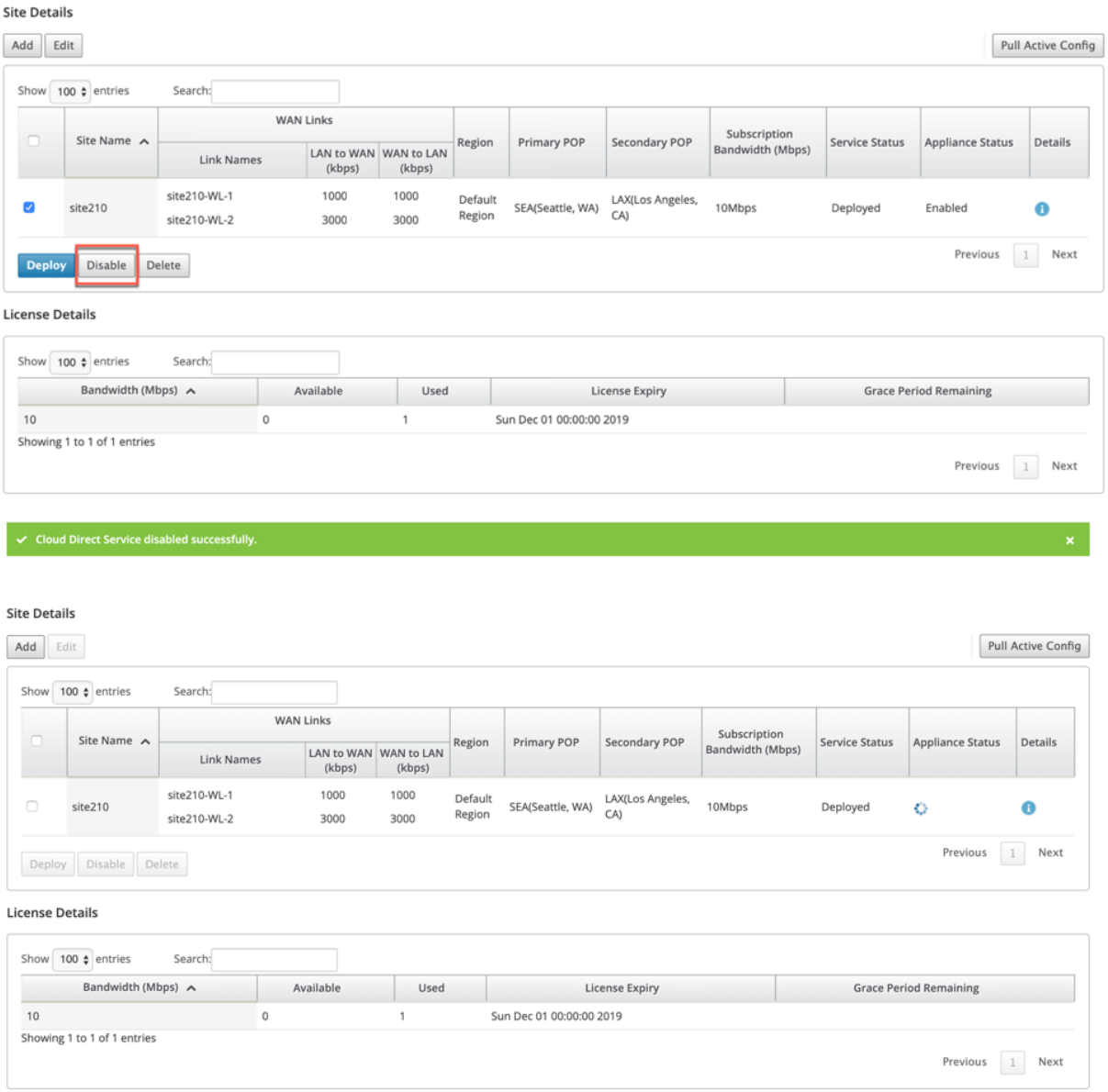


サイトを有効および無効にする

アプライアンスのステータスが無効と表示されているデプロイ済みサイトを有効にすることができます。サイトを有効にするには、[有効にする] をクリックします。

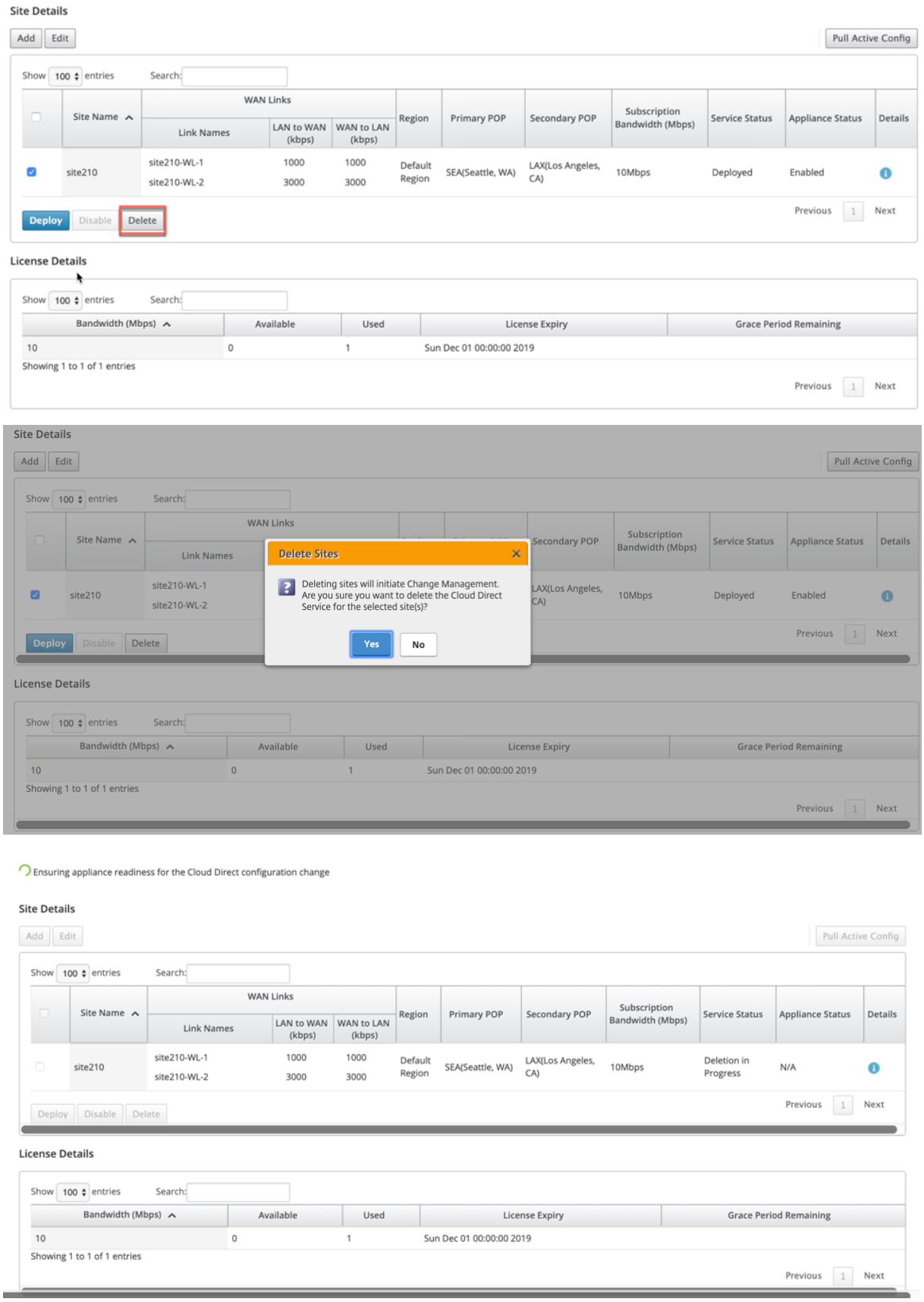


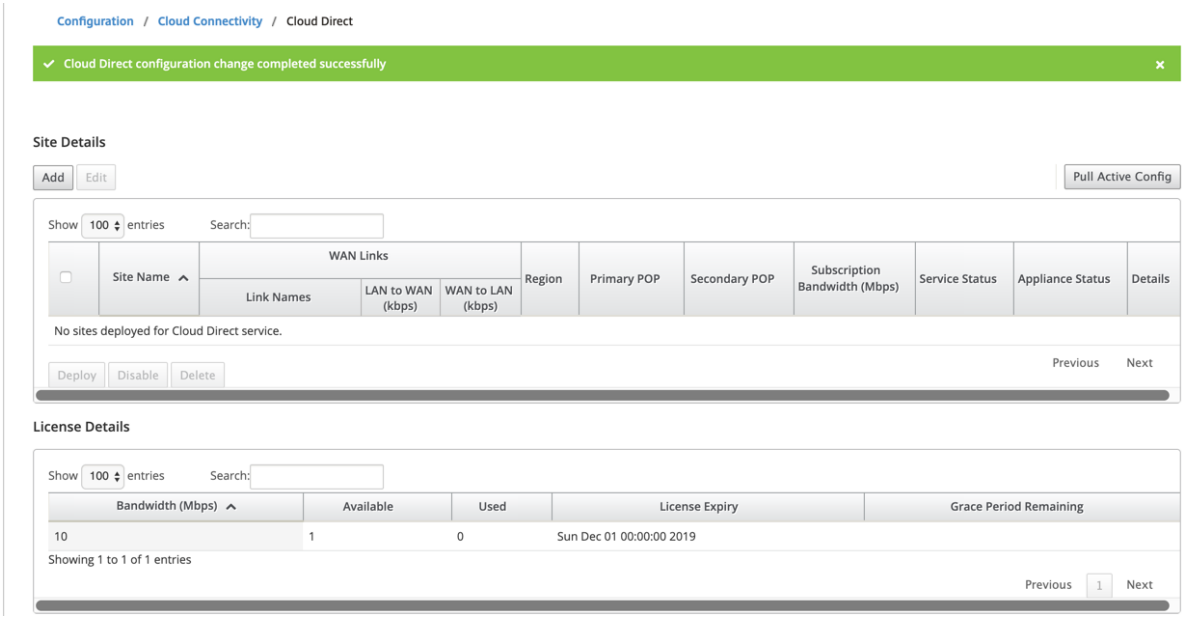
展開されたサイトを 無効 にするには、[無効] をクリックします。サイトを無効にすると、Cloud Direct サービスを使用してインターネットトラフィックを誘導できなくなります。アプライアンスで設定されている場合、すべてのトラフィックはインターネットサービスを介してリダイレクトされます。



サイトの削除

Cloud Direct 接続が不要になったサイトを削除することを選択できます。サイトを削除するには、サイトを選択して [削除] をクリックします。サイトを削除する確認メッセージが表示されます。
すべての Cloud Direct サービス構成は、変更管理プロセスを通じて削除されます。

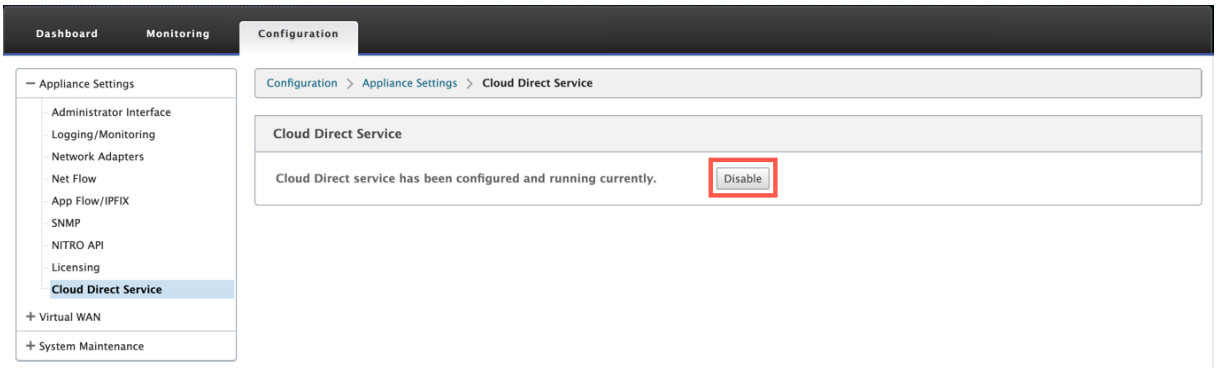




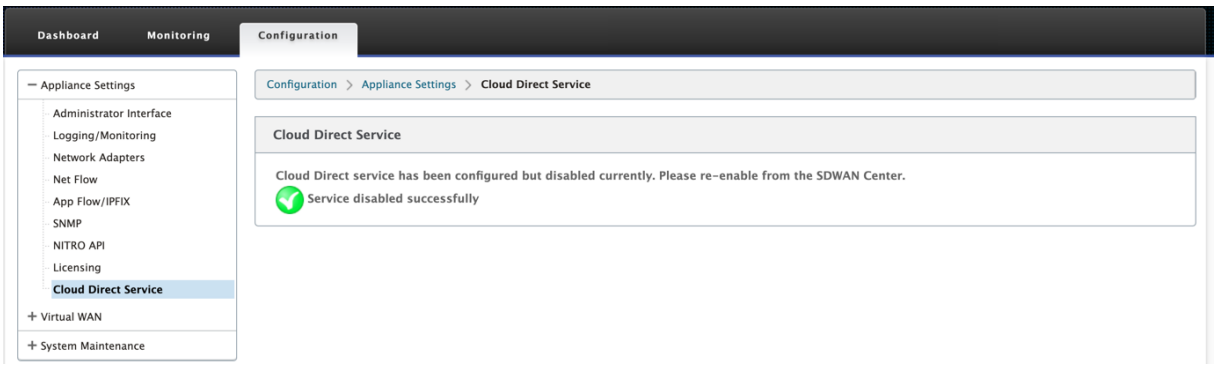
Citrix SD-WAN 上の Cloud Direct Service ステータス

ローカル SD-WAN アプライアンスで Cloud Direct サービスのステータスを確認できます。

Citrix SD-WAN GUI に移動し、**Configuration**> アプライアンス設定を 展開し **Cloud Direct Service** を選択します。



Cloud Direct サービスを無効にするには、[無効にする] オプションをクリックします。



トラブルシューティング

Cloud Direct サービスの展開時に SD-WAN Center で発生する可能性のある最も一般的なエラーメッセージは次のとおりです。

Error/status メッセージは SDW-AN センターの [設定] に > クラウド接続 > **Cloud Direct** に表示されます。

‘**Cloud Direct License error! {bandwidth} Mbps** 帯域幅‘の追加ライセンスをアップロードしてください

- 構成 > ライセンス > ファイル管理 オプションに移動して、SD-WAN Center に有効な Cloud Direct ライセンスをアップロードしてから、この機能の導入を続行してください

‘**Cloud Direct configuration HA due to Citrix Cloud Workspace login issue**’

- 構成に > クラウド接続 オプションに移動して、SD-WAN Center で Citrix Cloud Workspace ログインの認証情報を再入力します。

‘**Cloud Direct configuration processing error!** 地点：**{site_name}(IP: {mgmt_ip})** 到達できないか、**Cloud Direct** サポートがありません」

- SD-WAN アプライアンス（HA 展開の場合）が管理ポートで到達可能かどうかを確認します。

‘**Cloud Direct configuration HA Config Check error for site: {site_name}**’

- 展開されているサイトに対応する HA ペアの両方のアプライアンスの接続を確認します。

「両方の **HA** ペアアプライアンスは、**Cloud Direct** 構成を実行するために到達可能である必要があります」

- HA ペアの SD-WAN アプライアンスに Cloud Direct サービスを展開する場合、セカンダリアプライアンスとプライマリアプライアンスの両方が管理ポートで到達可能である必要があります。

‘**Cloud Direct configuration processing error!** 地点：**{site_name}(IP: {mgmt_ip}) SSO** ログインの問題があります‘

- SD-WAN アプライアンスが up/running 管理ポートで到達可能。このエラーは、SD-WAN Center が SD-WAN アプライアンスへのシングルサインオンを実行できない場合に表示されます。

‘**Internal error encountered during Cloud Direct configuration processing**’

- これは、構成チェックまたは残りの処理の実行中に複数のエラー条件が原因で発生する可能性があります。ユーザーはログを確認して、操作を再度実行する必要がある場合があります。

‘**Cloud Direct configuration processing canceled! MCN is not ready for change management**’

- Check if MCN is accessible and up and running and that its change management state is “network_staging.”

‘**Cloud Direct configuration processing error!** 地点：**{site_name}(IP: {mgmt_ip}) Cloud Direct** はサポートされていません。**Cloud Direct** サポートを利用するには、シングルステップアップグレードを実行してください‘

- **MCN** > 変更管理を介して SD-WAN アプライアンスでシングルステップソフトウェアアップグレードを実行します。この手順の後で、このサイトの Cloud Direct サービスのデプロイを再試行してください。

‘**Cloud Direct configuration processing error! SD WAN change management operation failed**’

- 変更管理操作はどういうわけか成功しませんでした。詳細については、SD-WAN Center ログを確認してください。

‘**Cloud Direct configuration processing error! Enabling service at site: {site_name} failed**’

- SD-WAN アプライアンスで Cloud Direct サービスを有効にできません。特定のアプライアンスの接続、または HA ペアの接続、またはシングルサインオンを実行する際の問題を確認します。詳細については、SD-WAN Center とアプライアンスのログを確認してください。

‘**Cloud Direct configuration processing error! Disabling service at site: {site_name} failed**’

- SD-WAN アプライアンスで Cloud Direct サービスを無効にできません。特定のアプライアンスまたは HA ペアのアプライアンスの接続、またはシングルサインオンを実行するときの問題を確認します。詳細については、SD-WAN Center とアプライアンスのログを確認してください。

‘**Cloud Direct configuration processing error! Config image push to site: {site_name} failed**’

- REST api 経由でアプライアンスにサービス固有のイメージをアップロードできないか、HA ペアの両方のアプライアンスにアクセスできません。

‘**Cloud Direct Service encountered an error during configuration processing. Audit errors found in the SD WAN config!**’

- SD-WAN 構成をコンパイルしようとしたときに検出された監査エラー。詳細については、SD-WAN Center ログを確認してください。

‘**Cloud Direct configuration processing error! Create Site failed for Site: {site_name}**’

- 対応する SD-WAN アプライアンスのサイトを作成しようとしたときのサービス側エラー。詳細については、SD-WAN Center のログを確認してください。

‘**Cloud Direct configuration processing error! Update Site failed for Site: {site_name}**’

- 対応する SD-WAN アプライアンスのサイト関連の設定を変更しようとしたときのサービス側エラー。詳細については、SD-WAN Center のログを確認してください。

ログに表示されるエラーメッセージ **(SDWAN_common.log)**

Cloud Direct サービスが SD-WAN アプライアンスにデプロイされているが、期待どおりに機能しない可能性があるいくつかのシナリオを次に示します。詳細については SDWAN_common.log を使用してローカル SD-WAN アプライアンスのログをダウンロードして確認できます。

シナリオ **1**

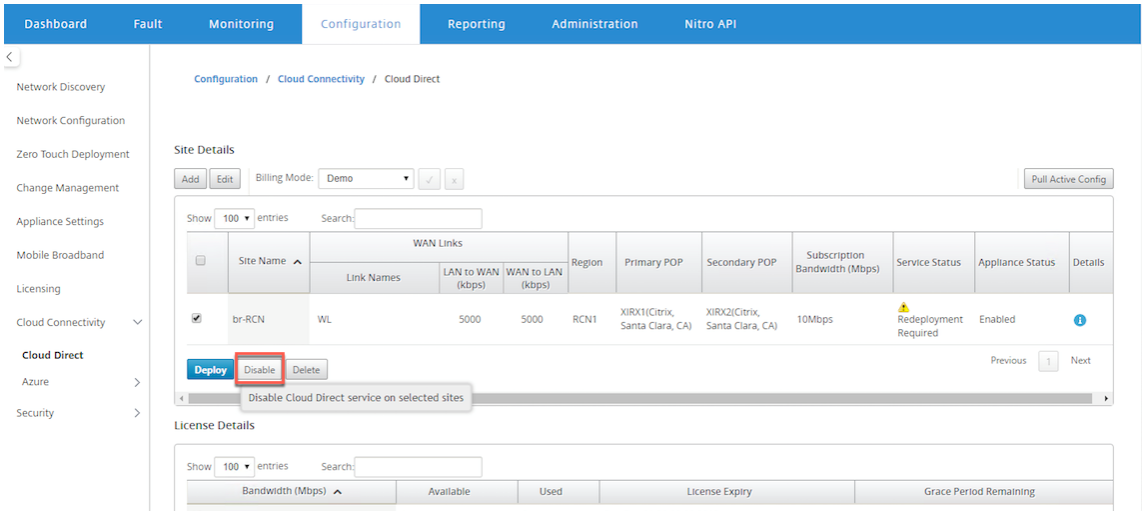
“**Detected Cloud Direct VM is not responding …Disabling Cloud Direct Service now!**”“**Cloud Direct service has been disabled.**” ローカル SD-WAN アプライアンスで実行されている基本的な KVM が期待どおりに機能していません。その場合、Cloud Direct サービス機能はアプライアンスで無効になります。

シナリオ **2**

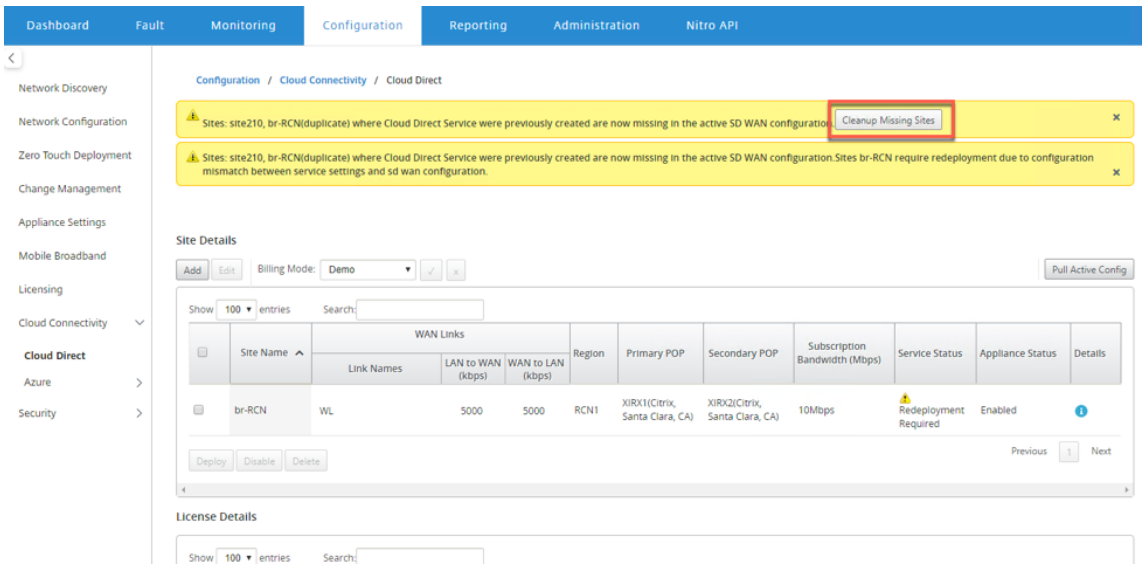
“**No tunneled packets seen for past 5 mins …Disabling Cloud Direct Service now!**” “**Cloud Direct service has been disabled.**” SD-WAN アプライアンスと Cloud Direct サービスで使用中のトンネルエンドポイントの間に確立されたトンネルはありません。これは、WAN リンクの設定ミス、設定された WAN リンクを介したインターネット接続の欠如、互換性がないか無効であることが原因である可能性があります data/config アプライアンスにプッシュされた画像、または WAN リンク経由で受信したときに UDP トンネルパケットをドロップする可能性のあるファイアウォールルール。その場合、Cloud Direct サービス機能はアプライアンスで無効になります。

異なる Cloud Direct 構成を使用して MCN の構成をアクティブ化すると（例：Cloud Direct の NAT 構成が変更される）、トラフィックが永続的に中断される可能性があります。このブロックを克服するには、次のいずれかの手順に従って、アプライアンスに存在するさまざまなルートを選択します。

1. SD-WAN Center GUI で、設定 > クラウド接続 > **Cloud Direct** に移動します。Cloud Direct アプライアンスを選択し、[無効にする] オプションをクリックしてクラウドダイレクトサービスを無効にします。



2. 構成 > クラウド接続 > **Cloud Direct** に移動してアクティブ構成をプルし、クリーンアップ通知を取得します。影響を受ける Cloud Direct アプライアンスに表示される [不足しているサイト のクリーンアップ] 通知ボタンをクリックできます。この操作により、アプライアンスで実行されている Cloud Direct サービスが無効になります。



3. 影響を受けるアプライアンスに Cloud Direct サービスを使用するには、SD-WAN Center に Cloud Direct サービスを再展開します。

Citrix SD-WAN Center を使用して Citrix SD-WAN と Zscaler を統合する

April 13, 2021

Citrix SD-WAN と Zscaler は、インターネットでホストされているアプリケーションとリソースに安全なローカルブレイクアウトを提供することにより、企業がクラウド移行のために WAN を変革するのを支援します。SD-WAN などの新しい WAN インフラストラクチャテクノロジーは、ネットワークの俊敏性と拡張性を高め、コストと複雑さを軽減して、分散組織でのユーザーエクスペリエンスを向上させます。

SD-WAN ソリューションは、クラウド宛てのトラフィックがローカルでインターネットに発信できるようにすることで、ルーティングを簡素化します。SD-WAN は、アプリケーションステアリング機能を使用して、トラフィックをインターネットにルーティングする（中央 DC 環境を削除する）柔軟性を提供します。ただし、ネットワークをインターネットに公開すると、重大なセキュリティリスクが発生します。クラウドサービスを通じてローカルのブレイクアウトを保護するための集中型のアプローチにより、ブランチのセキュリティインフラストラクチャを維持するためのオーバーヘッドが排除されます。すべてのトラフィックは、ブランチネットワークの Citrix SD-WAN を使用して、Zscaler（クラウドベースのセキュリティプラットフォーム）に確実かつ安全にルーティングされます。コストのかかるインフラストラクチャを排除し、脅威や脆弱性からネットワークを保護できます。

Citrix SD-WAN

Citrix SD-WAN は、ブランチからのインターネットアクセスを直接許可または拒否できるポリシーを作成するための組み込みのステートフルファイアウォールを使用して、ローカルのブランチからインターネットへのブレイクアウトを安全に有効にすることで、企業がクラウドに移行するのに役立ちます。Citrix SD-WAN は、個別の SaaS アプリケーションを含む、4,000 を超えるアプリケーションの統合データベースの組み合わせによってアプリケーションを識別し、ディープパケットインスペクションテクノロジーを使用して、アプリケーションをリアルタイムで検出および分類します。このアプリケーションの知識を使用して、ブランチからインターネット、クラウド、または SaaS にトラフィックを誘導します。

Zscaler

Zscaler は、オンプレミスのハードウェア、アプライアンス、ソフトウェアを必要とせずに優れたセキュリティを提供する、最先端のクラウドベースのセキュリティプラットフォームです。Zscaler はインターネットの周囲に境界を配置しているため、企業はすべてのオフィスの周囲にセキュリティの境界を配置する必要はありません。Zscaler Cloud Security Platform は、世界中の 100 以上のデータセンターで一連のセキュリティチェックの投稿として機能します。インターネットトラフィックを Zscaler にリダイレクトすることで、企業は店舗、支店、および遠隔地を即座に保護できます。Zscaler はユーザーとインターネットを接続し、トラフィックが暗号化されていても圧縮されていてもすべてのバイトを検査するので、ユーザーは安全であり、企業ネットワークに侵入する前にすべての隠れた脅威が識別されます。

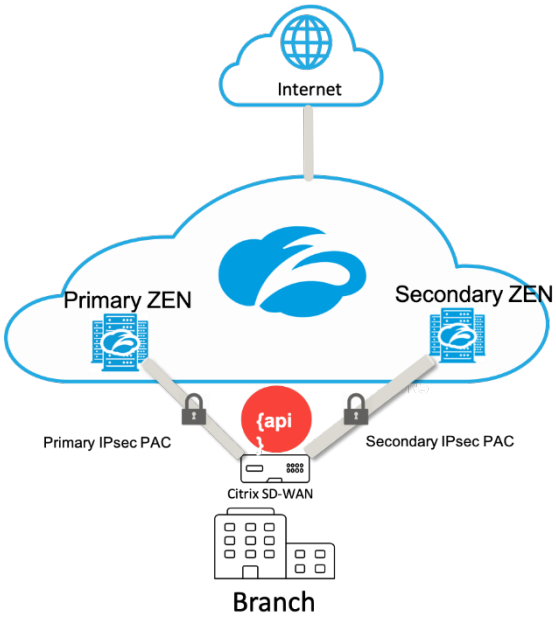
Citrix SD-WAN を使用すると、ブランチから直接インターネットにブレイクアウトできるポリシーを作成できます。Zscaler の Cloud Security Platform は、ユーザーが接続する場所の近くのクラウドサービスでインターネットに向かうトラフィックをすべて検査することで、IT のセキュリティを確保します。

Zscaler 実施ノード（**ZEN**）

Citrix SD-WAN は、Zscaler API をサポートし、Zscaler のクラウドネットワークで Citrix SD-WAN と Zscaler Enforcement Node（ZEN）間の IPsec トンネルの作成を自動化します。ZEN は、すべての機能を備えたインラインインターネットセキュリティゲートウェイであり、すべてのインターネットトラフィックをマルウェアについて双方向に検査し、セキュリティおよびコンプライアンスポリシーを適用します。

Zscaler API は、各ブランチに最も近い 2 つのデータセンターの場所を提供し、SD-WAN がトラフィックを効果的に誘導できるようにします。組織は Zscaler が自動的に WAN の IP アドレスで ZEN の外観は、Citrix SD-WAN 上で設定されたリンクまたは手動で **ZENs** を選択することができたことにより、ブランチに最も近い ZEN を選択できるようにすることができます。

> メモ
>
> トンネルが稼働している場合、両方のルートは常にアクティブモードになります。いずれかのトンネルがダウンすると、対応するルートに到達できなくなり、他のルートはアップのままになります。



長所

Citrix SD-WAN と Zscaler を統合するメリットは次のとおりです。

- 分散型エンタープライズでの SaaS とクラウドのより迅速な採用。

  - セキュリティをクラウドサービスとして一元化すると、各ブランチにセキュリティを配置する必要がなくなります。
  - インターネット宛てのトラフィックをバックホールする必要がなくなり、ブランチでローカルインターネットのブレイクアウトが可能になります。

- Secure Web Gateway への自動接続による IT 管理の簡素化。
  - API サポートにより、Zscaler への安全なトンネルの構成が自動化されます
- SaaS トラフィックのバックホールによるレイテンシを削減することにより、ユーザーエクスペリエンスが向上しました。
  - セキュリティの目的でハブアンドスポークモデルの依存関係を排除
- 支店でのコストのかかるセキュリティスタックの排除
  - ブランチでファイアウォールを展開して管理する必要があるオーバーヘッドを削減します。
- インターネットに向かうトラフィックが常に安全であることの保証。
  - セキュリティポリシーは、ユーザーを物理的な場所に関連付けません。
  - サンドボックス化、SSL、URL フィルタリング、高度な脅威保護などを含むすべてのポートとプロトコルの検査を提供し、ゼロデイ攻撃から保護します。

サポートされている機能

SD-WAN アプライアンスを使用した Zscaler の展開では、次の機能がサポートされています。

- ユーザー定義のインターネットトラフィックを Zscaler に転送することにより、直接インターネットのブレイクアウトを可能にします。
- 顧客サイトごとに Zscaler を使用した直接インターネットアクセス（DIA）。
  - 一部のサイトでは、DIA にオンプレミスのセキュリティ機器を提供し、Zscaler を使用しない場合があります。
  - 一部のサイトでは、インターネットアクセス用に別の顧客サイトへのトラフィックのバックホールを選択する場合があります。
- 仮想ルーティングと転送の展開。
- インターネットサービスの一部としての 1 つの WAN リンク。

Zscaler はクラウドサービスです。サービスとして設定し、基になる WAN リンクを定義する必要があります。

- データセンターとブランチサイトで信頼できるパブリックインターネット wan リンクを構成します。
- イントラネットサービスの IPsec トンネルを自動構成します。

Citrix SD-WAN Center のワークフローでの **Zscaler** の導入

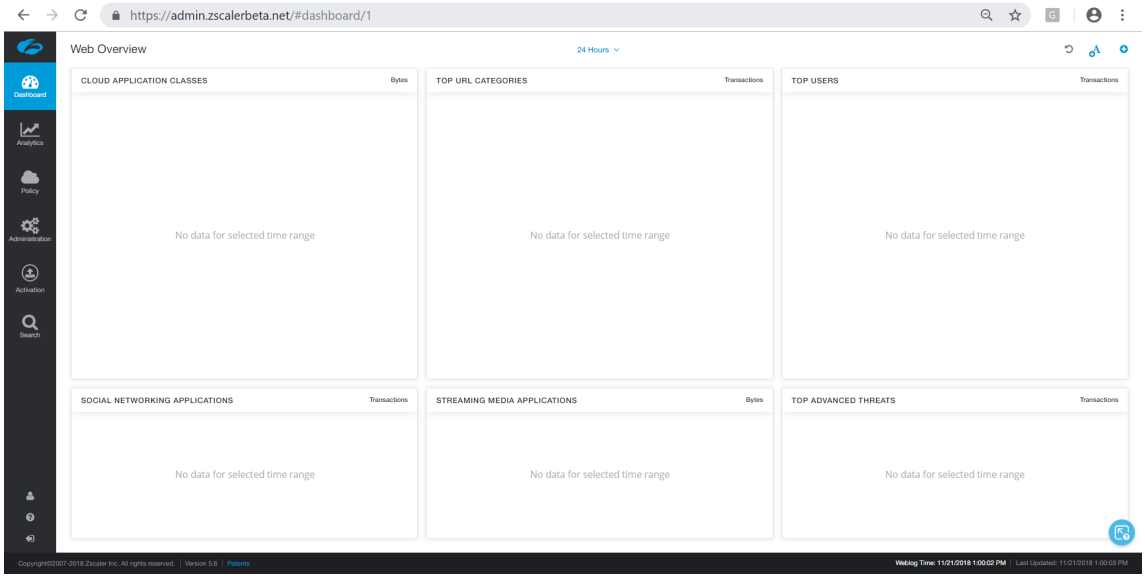
以下は、SD-WAN Center に Zscaler を展開するワークフローを定義する高レベルの手順です。

1. SD-WAN Center への Zscaler サブスクリプションを構成します（1 回限り）。Zscaler サイトにログインして、サブスクリプション情報を取得します。
2. Citrix SD-WAN Center GUI で デプロイ を選択します。
    - インターネット wan-link と事前構成されたアプリケーションオブジェクトを使用して、サイトの構成を展開します。
    - 接続を確立します。
    - Get/Update IPsec ステータスの。

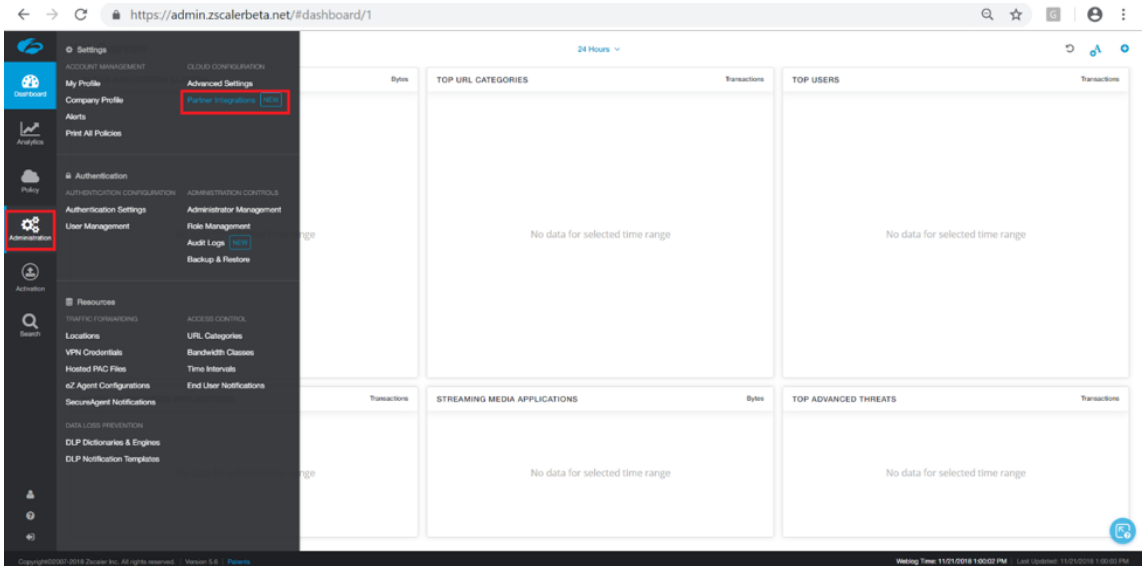
Zscaler サブスクリプション

SD-WAN Center で Zscaler を構成する前に、Zscaler ポータルにログインする必要があります。

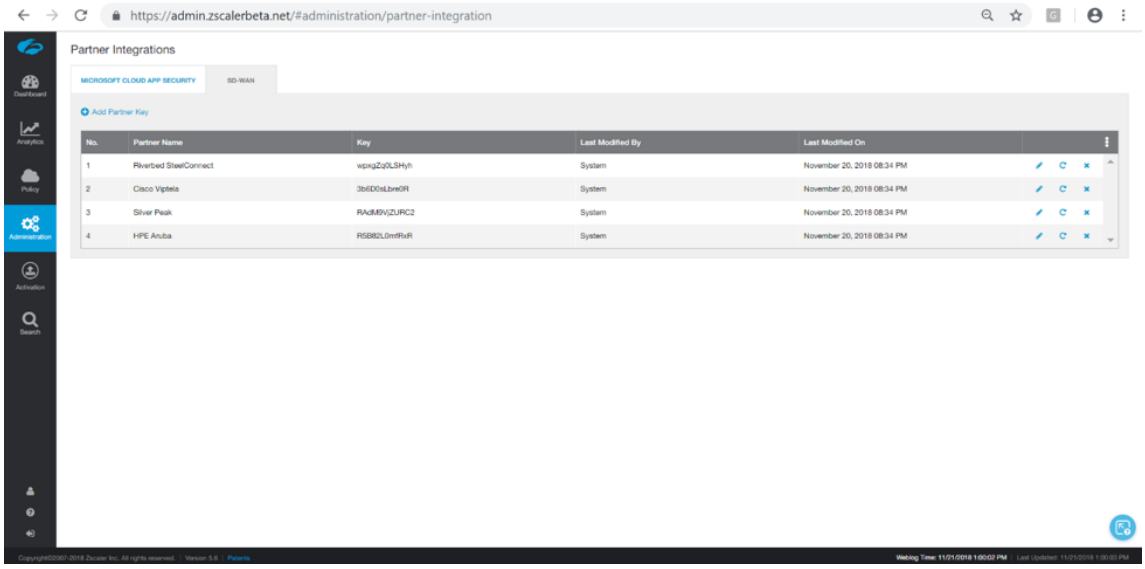
1. Zscaler サイトにログインして、サブスクリプション情報を取得します。[ダッシュボード] ページが開きます。

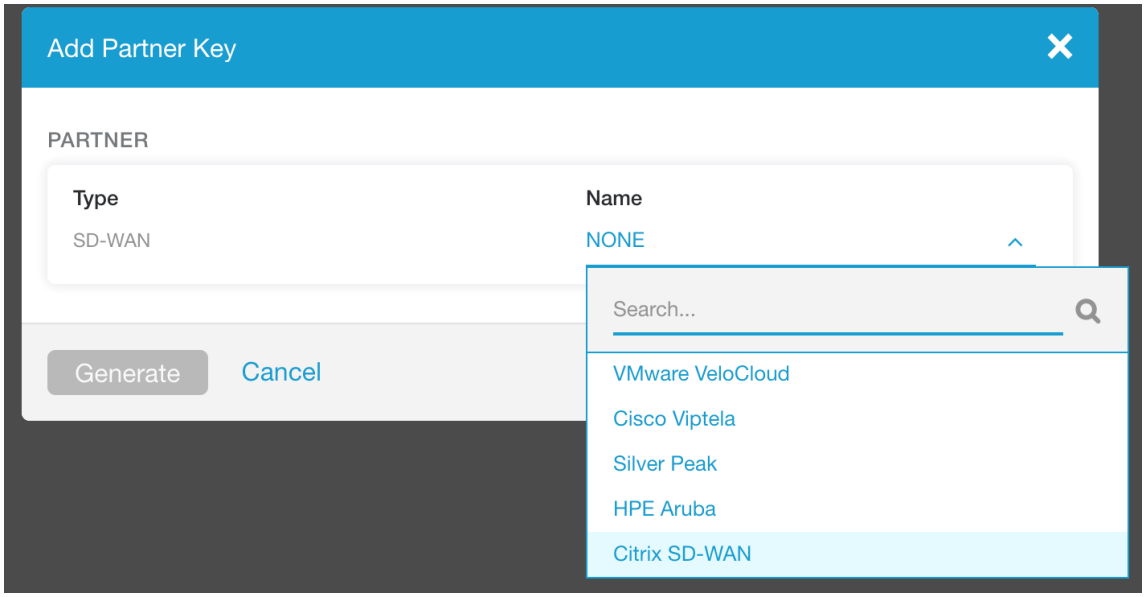


2. [管理**]>** パートナー統合をクリックします。



3. [パートナー統合] ページで [**SD-WAN]** を選択します。[パートナーキーを追加] をクリックします。

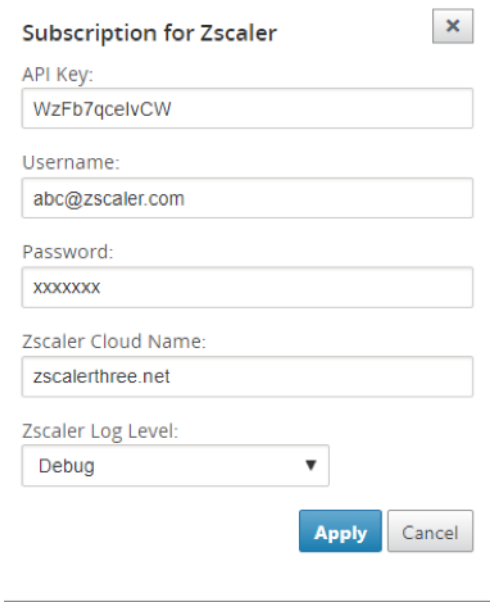




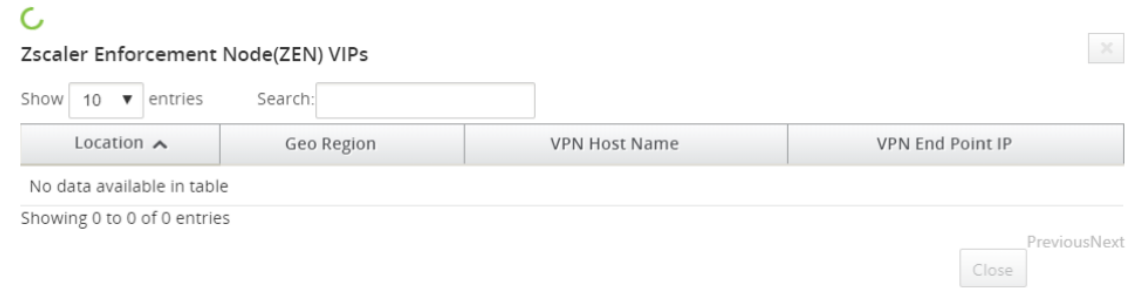
4. パートナーキーに **Citrix SDWAN** を選択し、[**Generate**] をクリックします。キーを保管します。

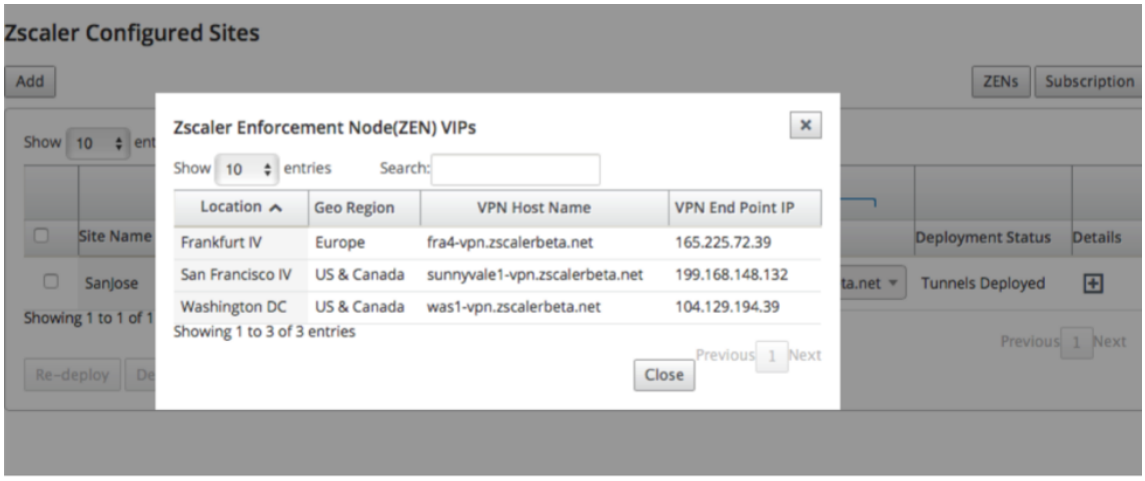
Citrix SD-WAN Center で **Zscaler** を構成する

1. Citrix SD-WAN Center GUI で、設定 **>** セキュリティページに移動します。**Zscaler Configured Sites** ページが開きます。
2. サブスクリプションをクリックします。前の手順で作成した Zscaler API（パートナーキー）を入力します。Zscaler の ユーザー名 と パスワードを入力します。**Zscaler Cloud Name**、**Zscaler Log Level** を選択し、**Apply** をクリックします。

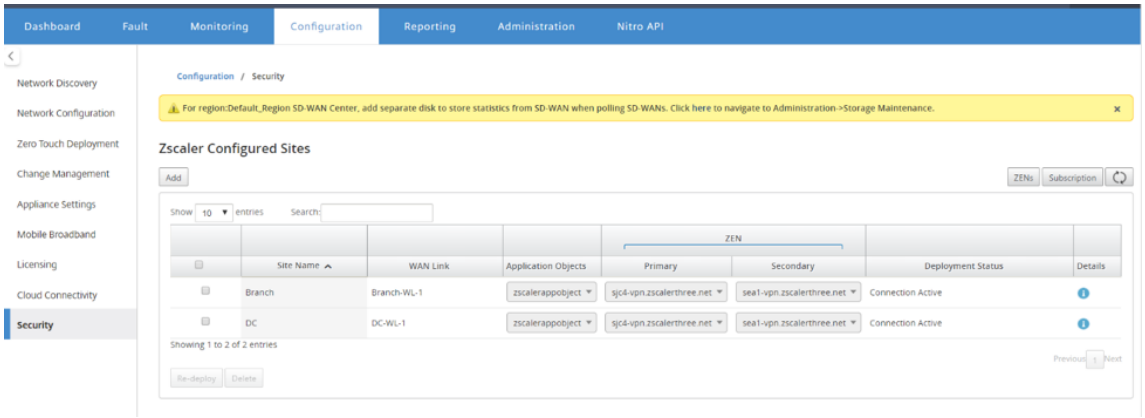


3. Zens は、この Zscaler クラウドサブスクリプションで使用可能な VPN エンドポイントのリストを提供します。

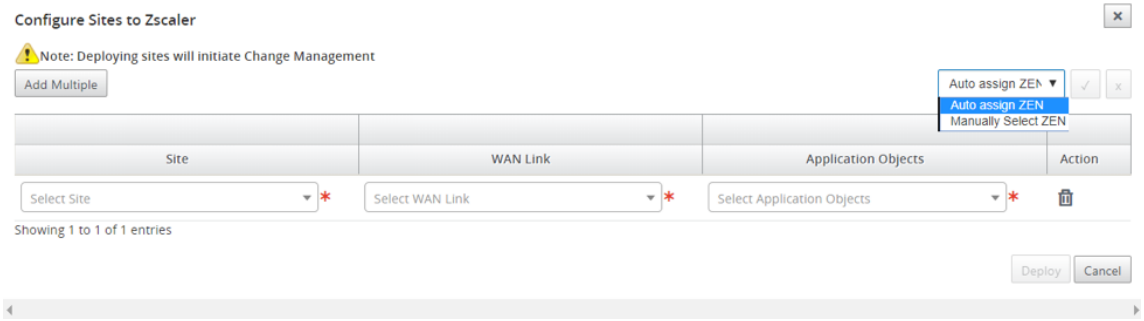




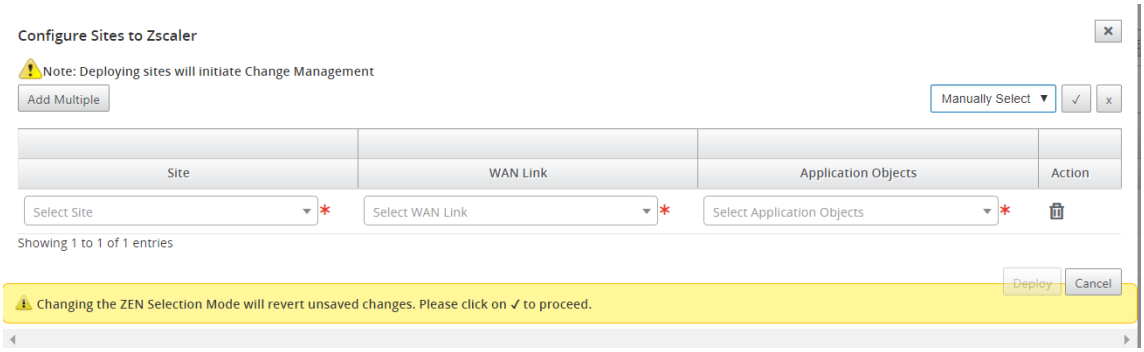
4. Zscaler サブスクリプションと ZEN の詳細を入力したら、Zscaler へのサイトの追加を開始できます。[追加] をクリックします。



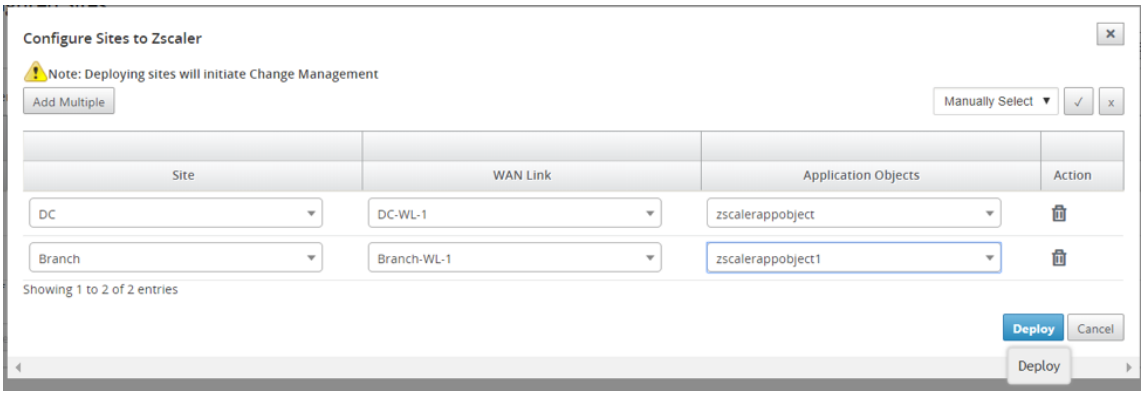
5. [**Zscaler** へのサイト の構成] ダイアログボックスで、サイト、**WAN** リンク、および アプリケーションオブジェクトを追加します。デフォルトでは、[**ZEN** の自動割り当て] オプションが選択されています。

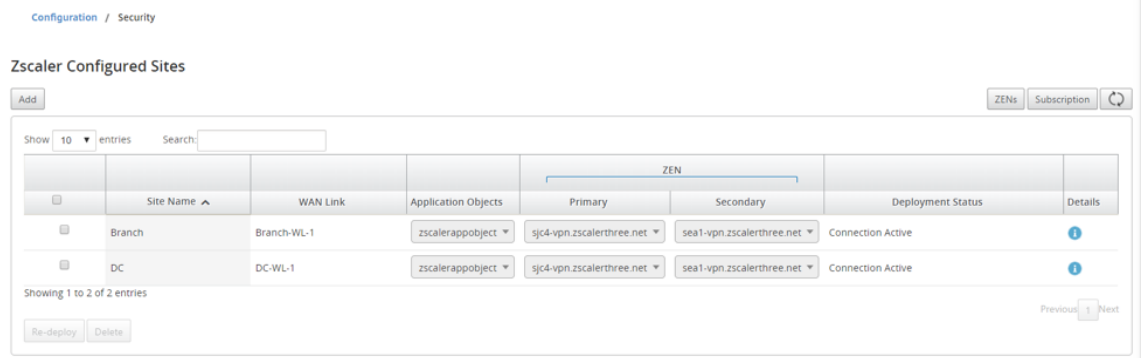


ZEN を手動で選択できます。ただし、保存されていない変更が失われたことを通知する次のメッセージが表示されます。



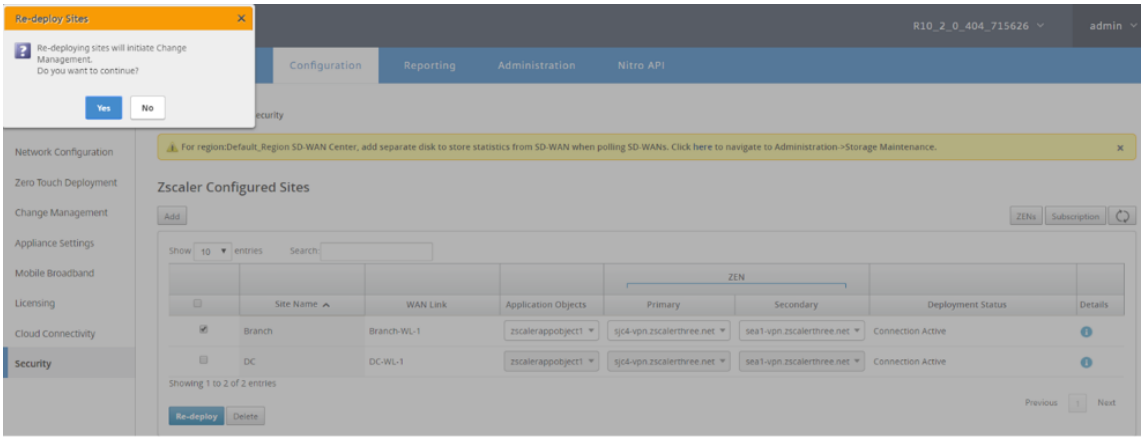
6. 必要なサイトを選択して、[展開] をクリックします。あなたは 追加の複数を選択することにより、複数のサイトを追加することを選択することができます。選択したサイトが展開され、構成ページが表示されます。



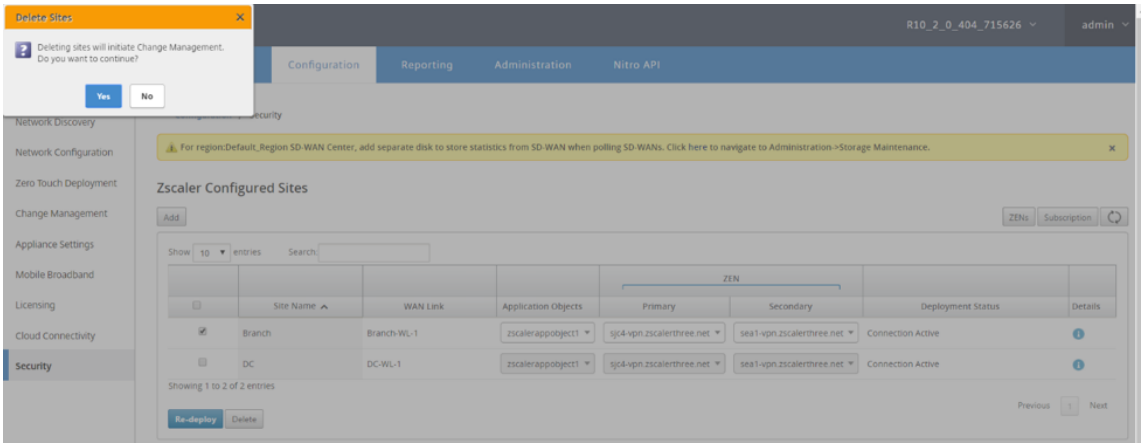


プライマリとセカンダリの ZEN IP アドレスが入力され、展開ステータスが **Connection Active** であることを確認します。

7. 構成済みサイトの VPN エンドポイントまたはアプリケーションオブジェクトを変更する場合は、[再展開] をクリックします。SD-WAN Center で構成されたサイトに変更を加えると、ブランチサイトと DC サイトで構成されたアプライアンスで変更管理 プロセスがトリガーされます。

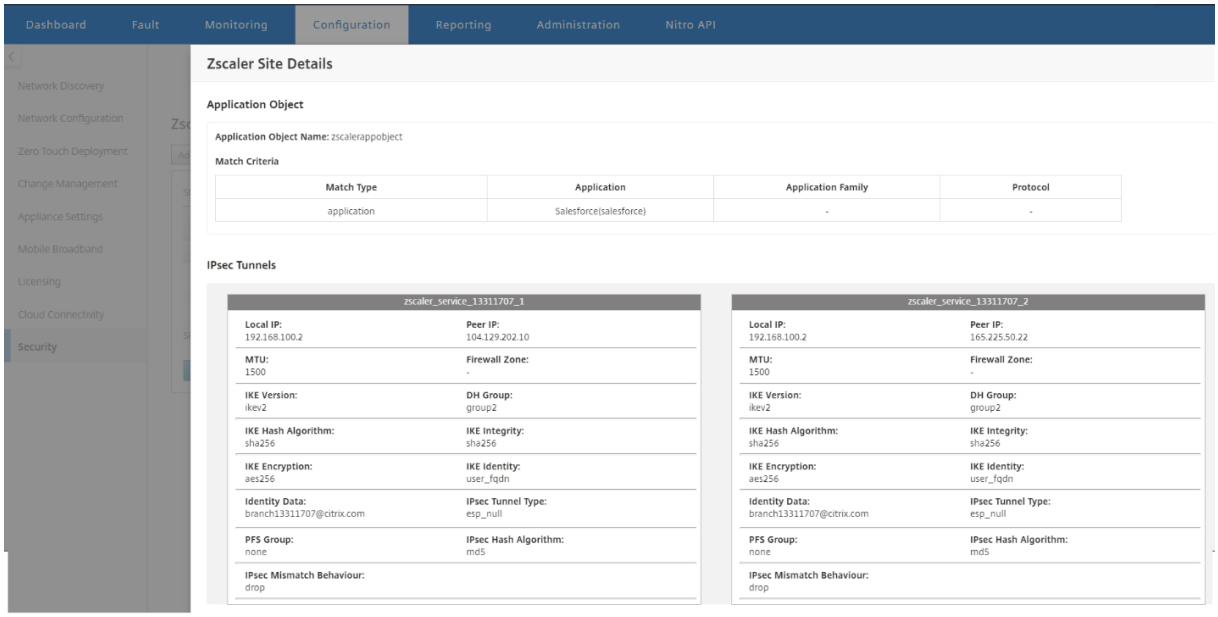


サイトを削除すると、変更管理プロセスもトリガーされます。



監視とトラブルシューティング

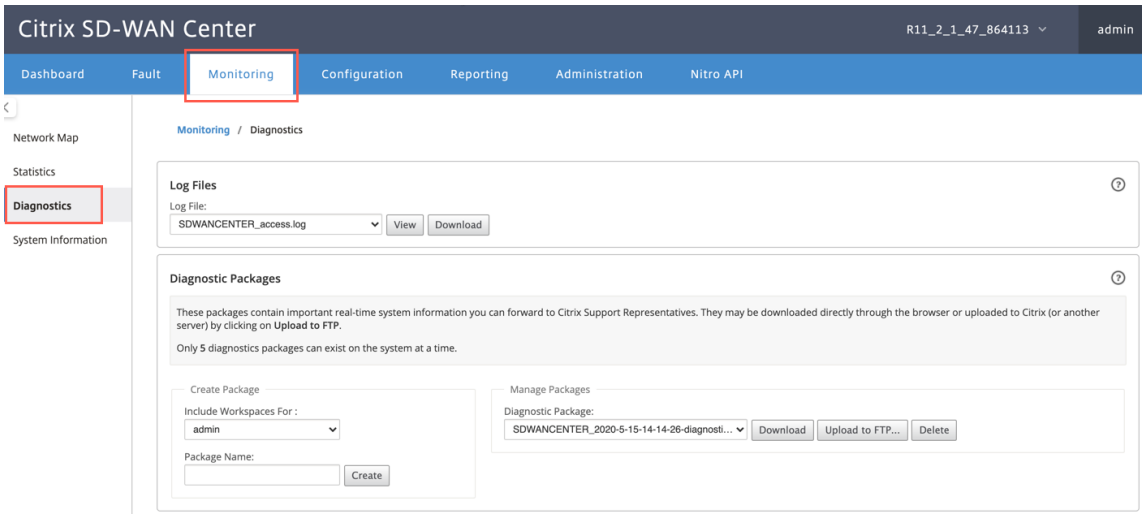
構成済みサイトを選択して、アプリケーションオブジェクトおよび Primary/Secondary IP アドレス。「詳細」アイコンをクリックして、構成済みサイトに関する完全な情報を表示できます。



Citrix SD-WAN Center での問題のトラブルシューティングに使用できる Zscaler ログを表示およびダウンロードできます。

Zscaler ログファイルを表示するには:

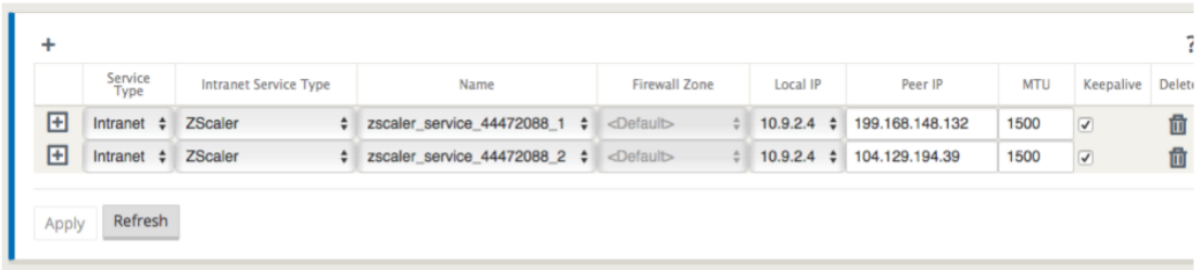
1. Citrix SD-WAN Center Web インターフェイスで、[監視] > 診断タブをクリックします。



2. **[**ログファイル**]** ドロップダウンリストから、表示する Zscaler ログファイルを選択します。表示をクリックします。
3. コンピュータにログファイルをダウンロードする場合は、[ダウンロード] をクリックします。

IPsec トンネル構成

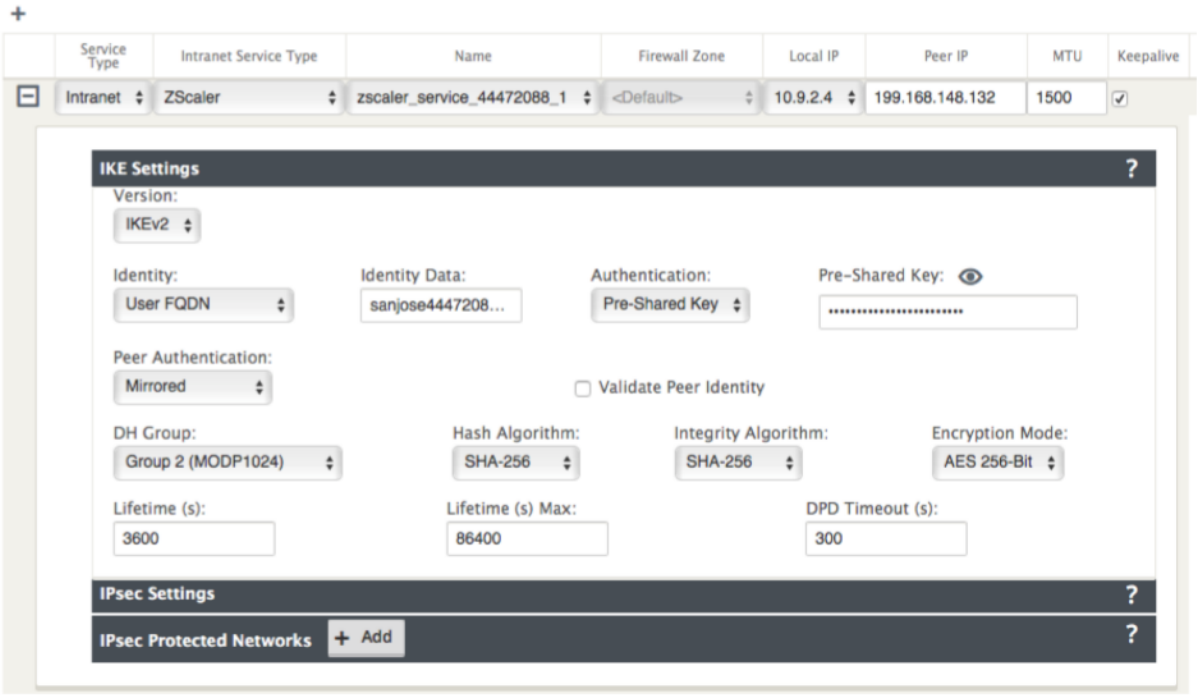
SD-WAN Center GUI の詳細ページには、プライマリおよびセカンダリエンドポイントへの IPsec トンネル構成に関する情報が表示されます。ピア IP は Zscaler から取得されます。SD-WAN アプライアンス GUI 構成エディターで IPsec トンネル構成を確認します。



IKE 設定

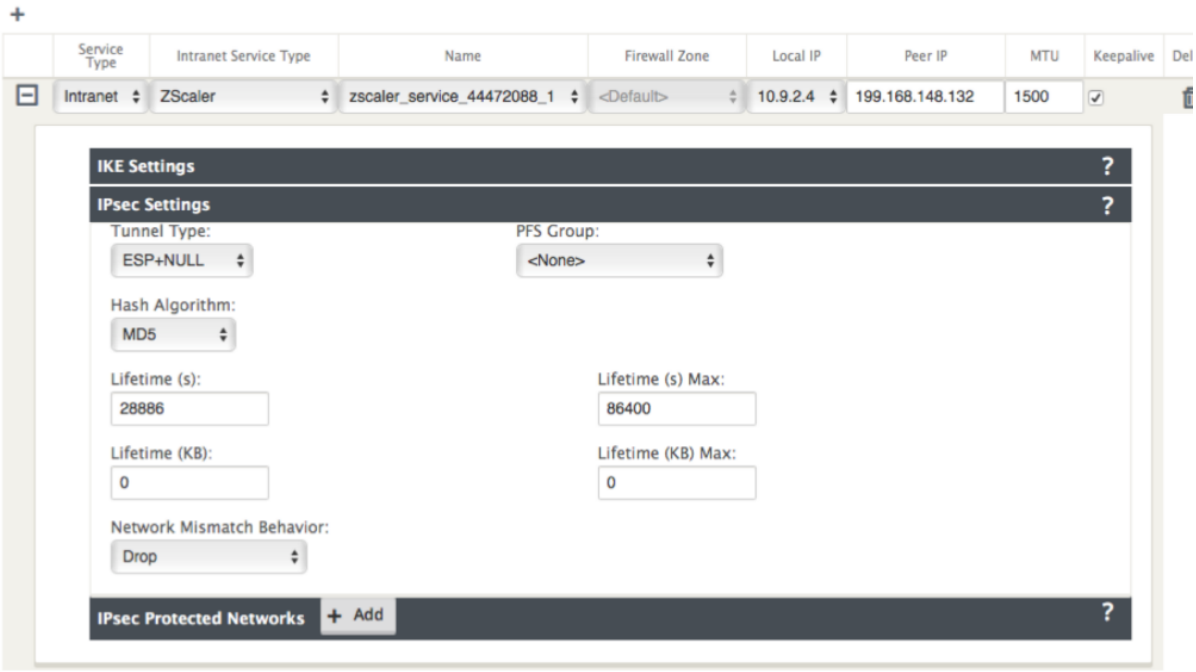
以下 IKE/IPSec 設定は、SD-WAN アプライアンスの IPsec トンネル構成用に選択されます。IPsec トンネル-IKE 設定の構成の詳細については、SD-WAN とサードパーティデバイス間の IPsec トンネルを構成する方法トピックを参照してください。

- IKE バージョン-IKEv2
- IKE ID –ユーザー FQDN
- ハッシュアルゴリズム-SHA-256
- 整合性アルゴリズム–SHA-256
- 暗号化モード–AES 256 ビット
- IPsec –トンネルモード
- IPsec 暗号化–Null



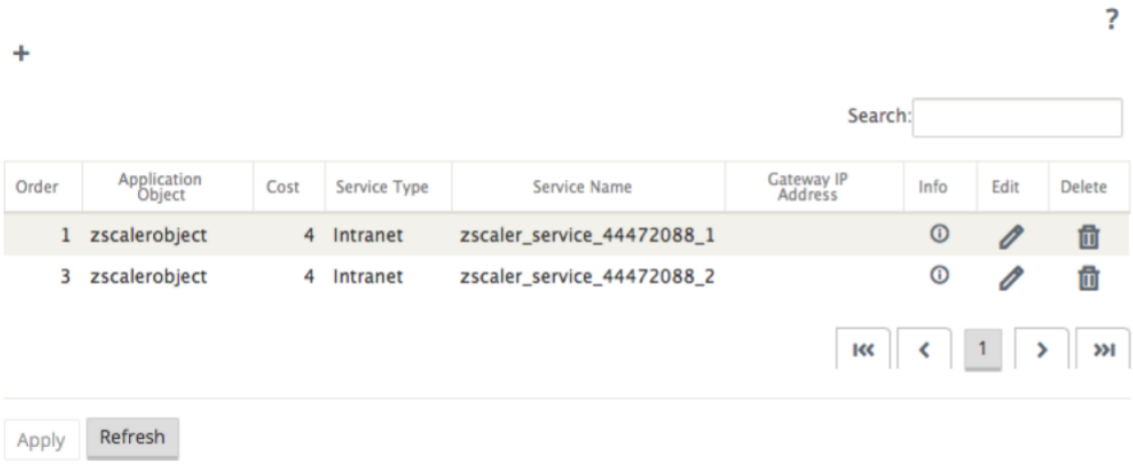
IPsec 設定

IPsec トンネル設定の構成の詳細については、SD-WAN とサードパーティデバイス間の IPsec トンネルを構成する方法 トピックを参照してください。



アプリケーションオブジェクト

アプリケーションオブジェクトが構成されていることを確認します。アプリケーションルートの構成の詳細については、アプリケーション分類 トピックを参照してください。



> 注
>
> GRE トンネル構成は、自動ワークフローの一部としてサポートされていません。ただし、手動構成は引き続き許可されます。詳しくは、「GRE トンネルと IPsec トンネルを使用した Zscaler 統合」を参照してください。

監視

April 13, 2021

Citrix SD-WAN Center ダッシュボードでは、SD-WAN ネットワークの統計情報とグラフを 1 つのペインに表示できます。詳しくは、「ダッシュボード」を参照してください。

Citrix SD-WAN Center で SD-WAN ネットワーク イベント および レポート を表示することもできます。

関連記事の監視:

診断パッケージ

イベント通知

ログ ファイル

メモリダンプ

ポーリング間隔

統計

システム情報

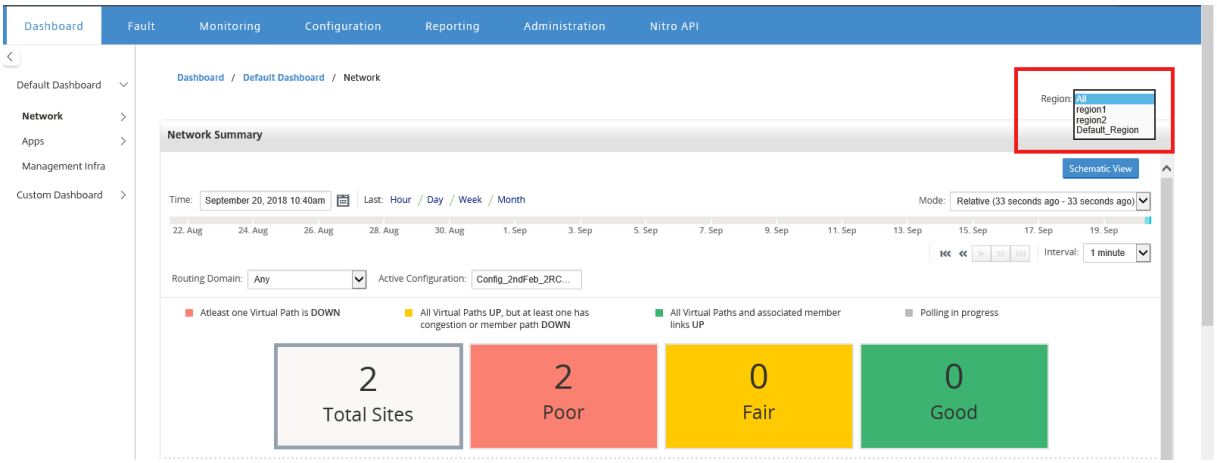
ダッシュボード

February 18, 2022

Citrix SD-WAN Center ダッシュボードには、一般的な統計のサブセットが一目で表示されます。単一リージョン展開の場合、統計は Citrix SD-WAN Center で検出された MCN から取得されます。マルチリージョン展開の場合、統計情報は、選択された時間間隔ですべてのリージョン Citrix SD-WAN Center コレクターから取得されます。次の統計を表示できます。

- ネットワークの概要
- ネットワーク QoE
- トップサイト
- Inventory
- イベントとアラーム
- 上位のアプリ
- HDX QoE
- 管理インフラ

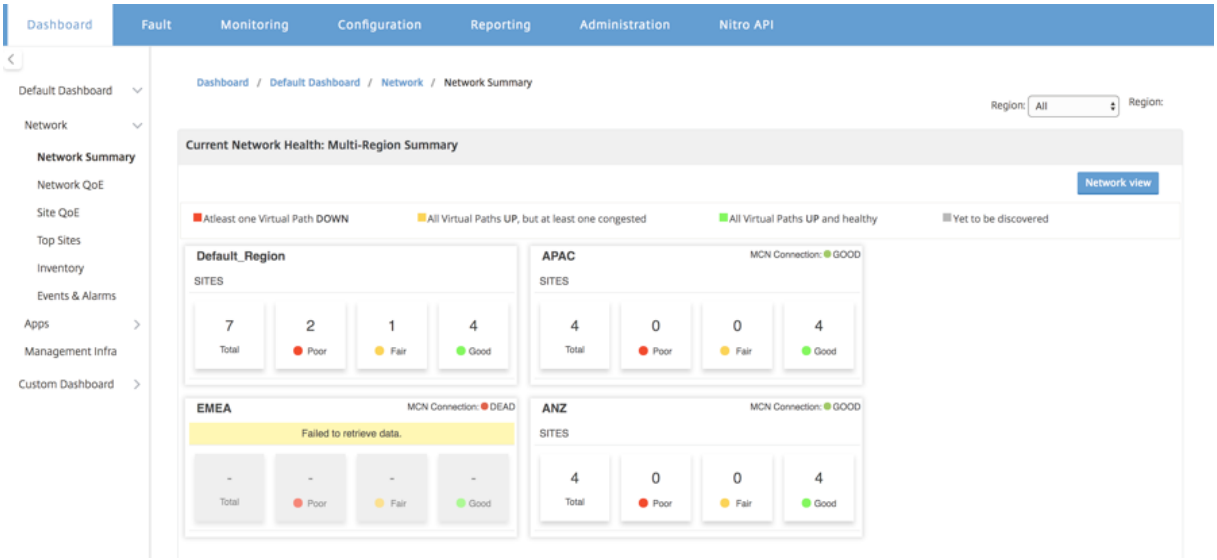
単一リージョンのデプロイの場合、デフォルトのリージョン統計がダッシュボードに表示されます。マルチリージョン展開の場合、マルチリージョンダッシュボードまたはリージョナルダッシュボードの表示を選択できます。マルチリージョンダッシュボードを表示するには、[リージョン] メニューで [すべて] を選択します。ただし、300 を超えるサイトが構成されている場合、マルチリージョンの概要ダッシュボードは表示できません。



各地域タイルで MCN 接続ステータスを表示できます。MCN 接続ステータスは、RCN と MCN 間の仮想パスのヘルスステータスです。

> 注
>
> マルチリージョン展開の場合、デフォルトのリージョン統計には、MCN によって管理されるすべてのサイトの統計が含まれます。RCN には MCN への仮想パスがあるため、RCN 統計も含まれる場合があります。

> [地域] ドロップダウンメニューは、Citrix SD-WAN Center コレクターでは使用できません。



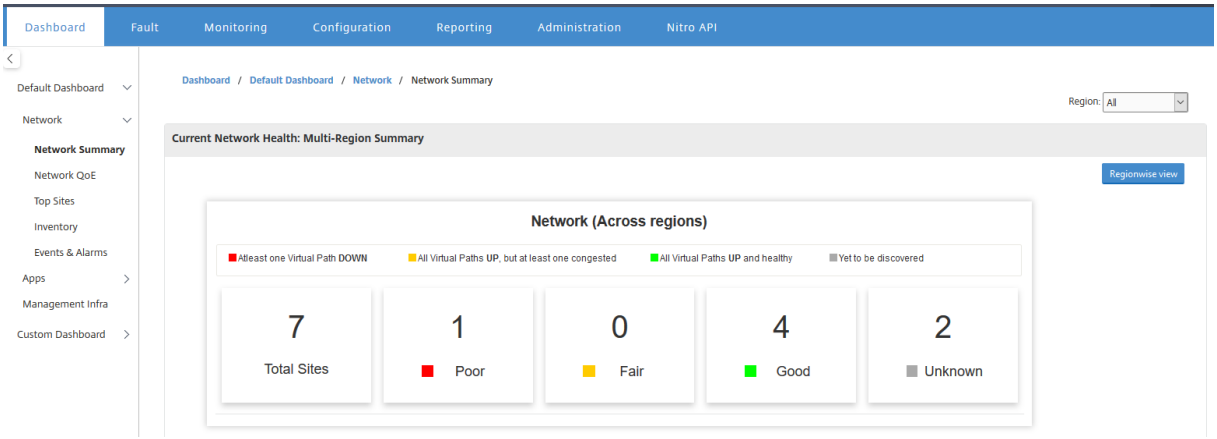
Citrix SD-WAN Center ダッシュボードは、設定されたポーリング間隔に基づいて更新されます。デフォルトのポーリング間隔は 5 分です。詳細については、「ポーリング間隔」を参照してください。

ネットワークの概要

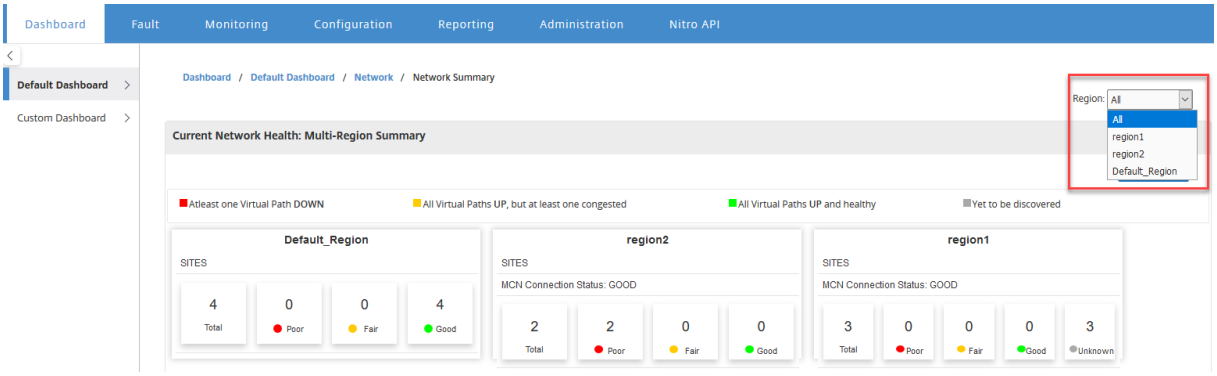
マルチリージョンのデプロイの場合、ネットワークの概要 ウィジェットは、さまざまなリージョンすべてのネットワーク状態の概要を提供します。ネットワーク内のすべての地域の地域カードが、次の情報とともに表示されます。

- リージョン内のサイトの総数。
- Poor 状態のサイトの数。少なくとも 1 つの仮想パスがダウンしている場合、サイトは貧弱な状態です。
- Fair 状態のサイトの数。サイト内のすべての仮想パスが UP であるが、少なくとも 1 つのパスに輻輳の問題があるか、メンバーパスが DOWN である場合、サイトは Fair 状態です。
- 良好な状態のサイトの数。すべての仮想パスと関連するメンバーパスが UP の場合、サイトは良好な状態です。
- 不明状態のサイトの数。ポーリングの進行中、サイトは不明な状態です。

マルチリージョンネットワークの概要を表示するには、ダッシュボード > デフォルトのダッシュボード > 通信網 > **[Network Summary**] をクリックし、[**Region**] ドロップダウンメニューで [**All**] を選択します。



デフォルトでは、画面は ネットワークビューに表示されます。地域別ビューをクリックすると、マルチリージョンネットワークの概要の現在のネットワーク状態を確認できます。各地域タイルで MCN 接続のステータスを確認することもできます。



地域カードをクリックして、地域ダッシュボードにドリルダウンします。

個々のリージョンの場合、ネットワークの概要 ウィジェットは、選択したリージョンのネットワークヘルスの概要を提供します。

地域ネットワークの概要を表示するには、ダッシュボード > デフォルトのダッシュボード > 通信網 > ネットワークの概要 と 地域の選択 ドロップダウンメニューで、地域を選択します。

地域別ネットワークの概要は、タイルビューまたはスケマティックビューで表示できます。

タイムラインコントロールを使用して、選択した期間のネットワークステータスの概要を表示できます。また、時間範囲にわたってネットワークステータスを再生または一時停止することもできます。

モードは、時間を相対的または絶対的な概念として見るのに役立ちます。

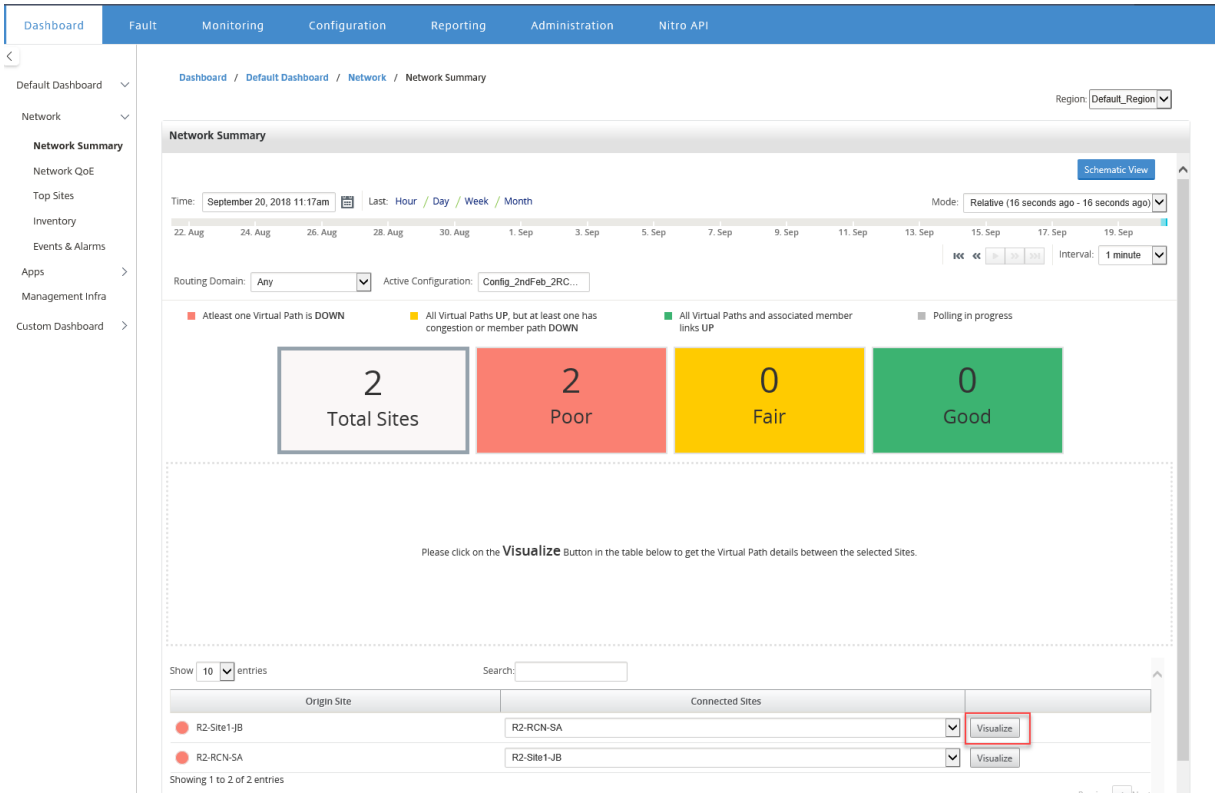
タイムラインとモードについて詳しくは、「タイムラインのコントロール」を参照してください。

タイルビュー

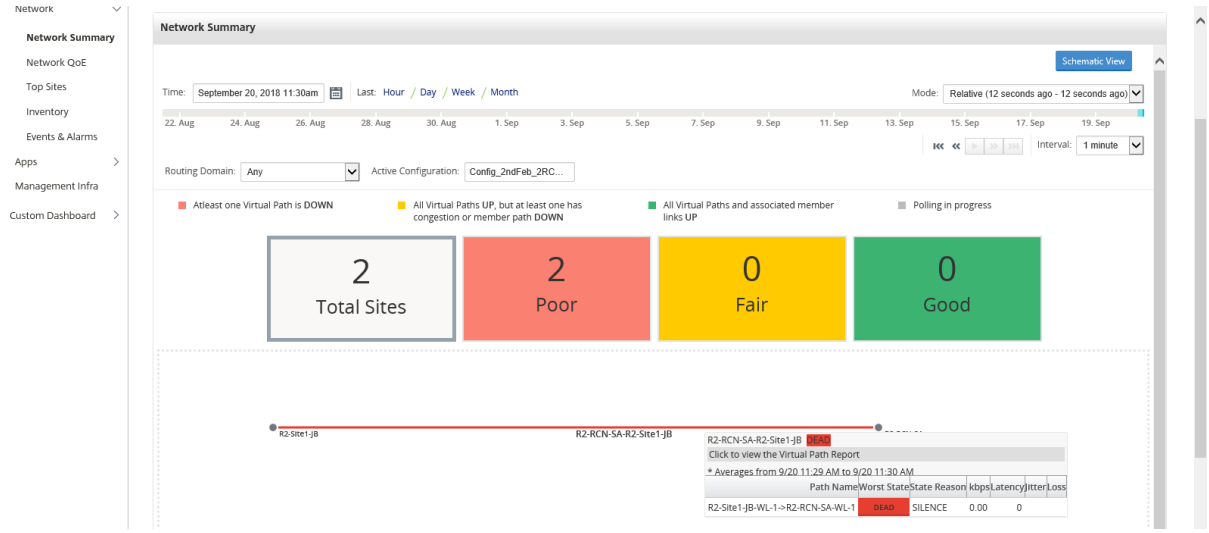
タイルビューは次の情報を提供します。

- リージョン内のサイトの総数。
- Poor 状態のサイトの数。少なくとも 1 つの仮想パスがダウンしている場合、サイトは貧弱な状態です。
- Fair 状態のサイトの数。サイト内のすべての仮想パスが UP であるが、少なくとも 1 つのパスに輻輳の問題があるか、メンバーパスが DOWN である場合、サイトは Fair 状態です。
- 良好な状態のサイトの数。すべての仮想パスと関連するメンバーパスが UP の場合、サイトは良好な状態です。
- 不明状態のサイトの数。ポーリングの進行中、サイトは不明な状態です。

2 つのサイト間のパスをグラフィカルに表示するには、パスを選択して [視覚化] をクリックします。



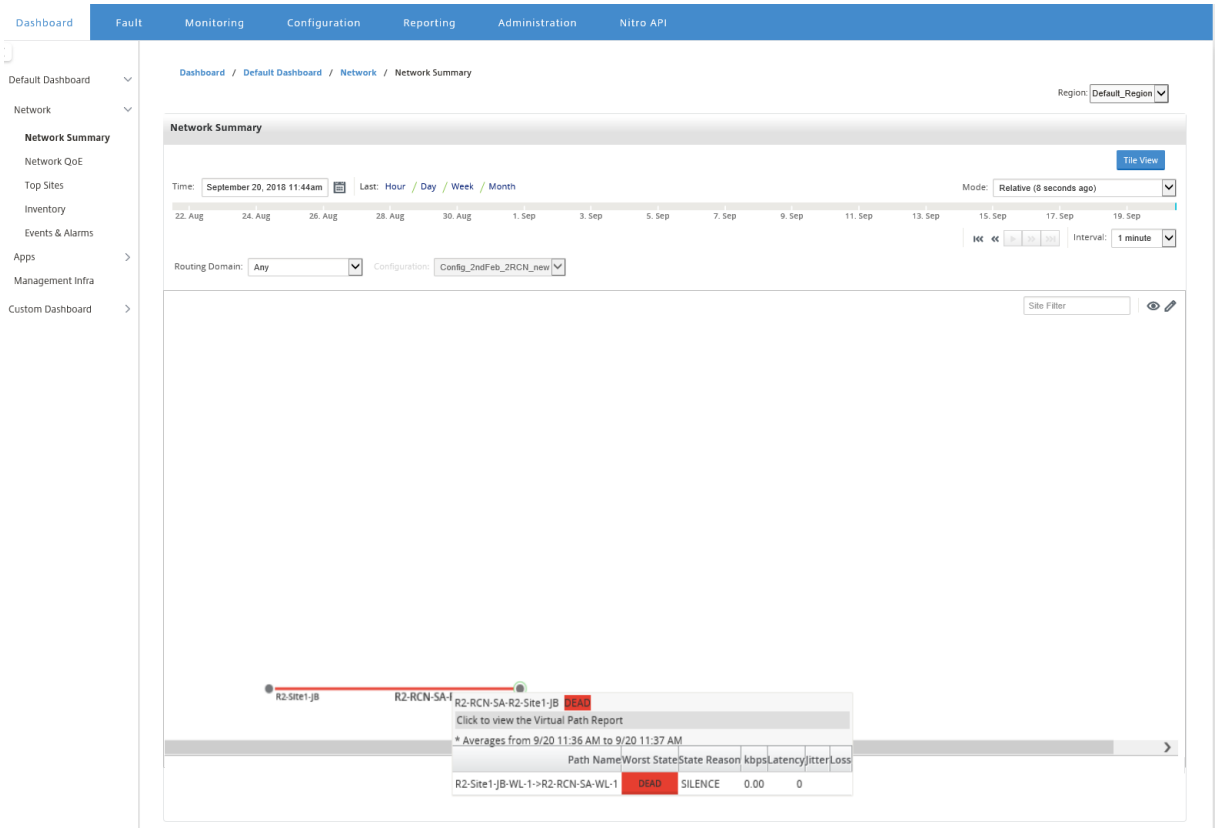
マウスカーソルをサイトまたはパスの上に置くと、詳細が表示されます。サイトをクリックして、レポートオプションを表示および選択します。



概略図

概略図は、SD-WAN ネットワークのグラフィック表示を提供します。このセクションに表示される情報は、選択した構成とルーティングドメインに応じて更新されます。ここでネットワークマップを表示するには、マスターコントローラーノード（MCN）からネットワーク構成とネットワークマップをインポートする必要があります。詳細については、「MCN 構成のインポート」を参照してください。

マウスカーソルをサイトまたはパスの上に置くと、詳細が表示されます。サイトをクリックして、レポートオプションを表示します。

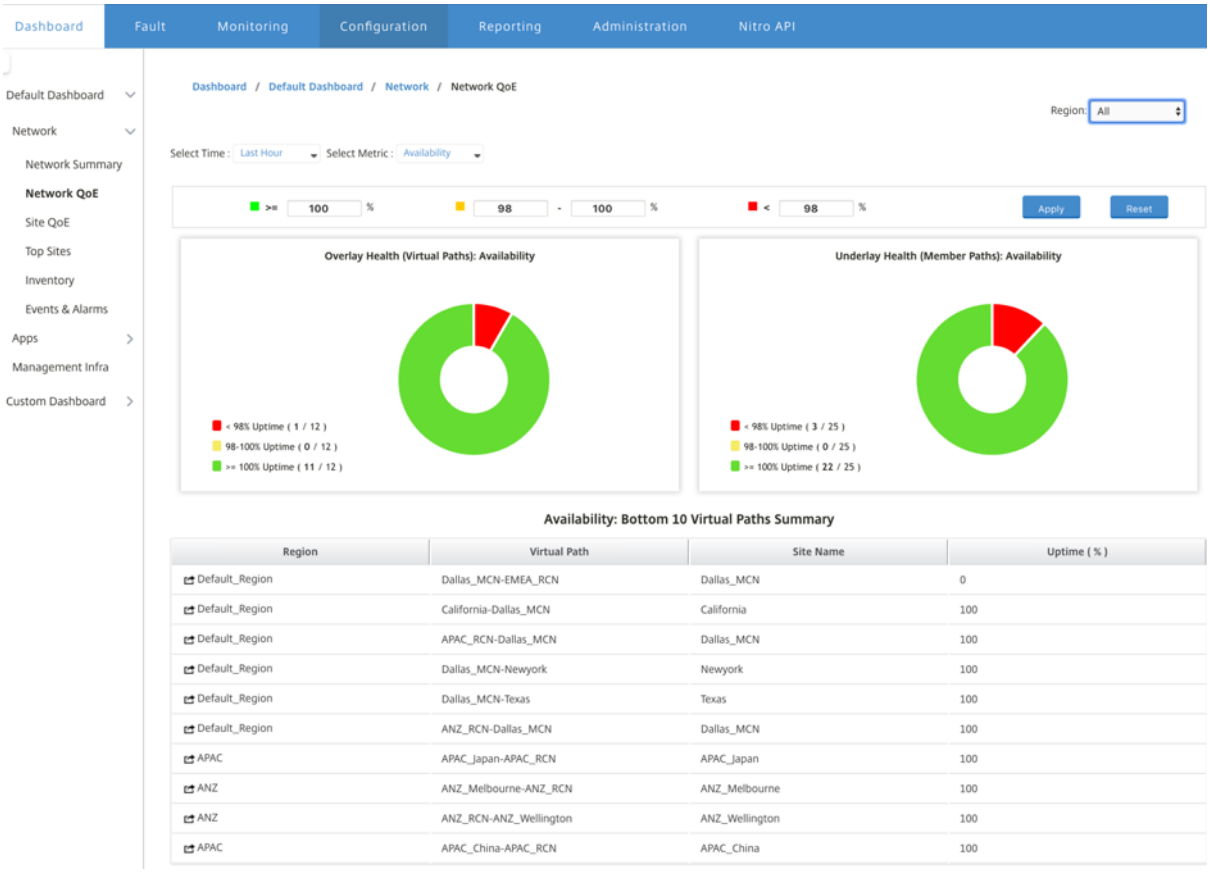


ネットワーク **QoE**

ネットワーク **QoE** ウィジェットは、仮想パスの可用性、損失、待ち時間、およびジッターパラメーターをグラフィカルに表示します。オーバーレイ仮想パスとアンダーレイメンバーパスの両方の統計情報を提供します。

マルチリージョンデプロイメントの場合、選択したメトリックに応じて、下位 10 の仮想パスのリストを表示できます。仮想パスデータは、選択した時間間隔ですべてのリージョナルコレクタから収集されます。最も注意が必要な仮想パスの帯域幅、ジッター、損失、および輻輳の詳細を表示できます。

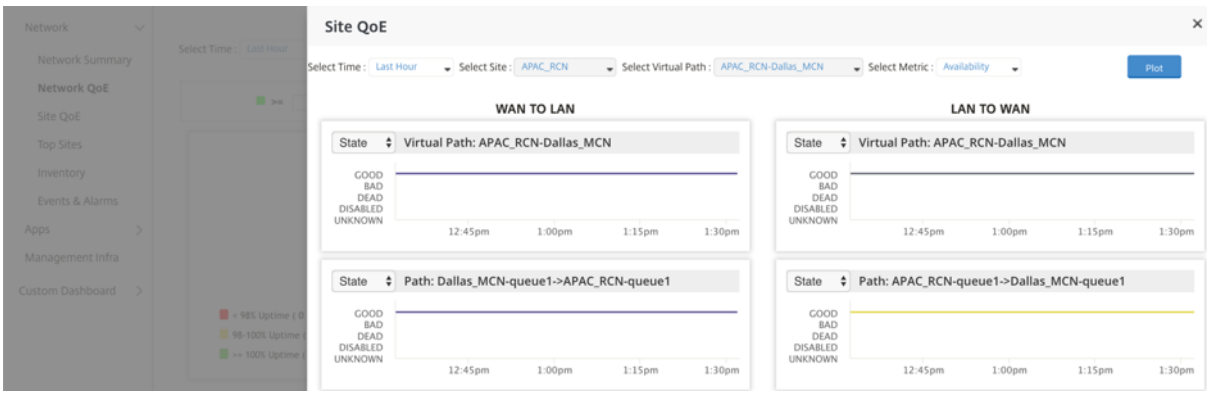
マルチリージョン仮想パスヘルスを表示するには、ダッシュボード > デフォルトのダッシュボード > 通信網 > ネットワーク **QoE** に移動し [地域] ドロップダウンメニューで [すべて] を選択します。



個々のリージョンについて、選択したメトリックに応じて、下位 10 の仮想パスのリストを表示できます。統計は、選択した時間間隔で収集されます。最も注意が必要な仮想パスの帯域幅、ジッター、損失、および輻輳の詳細を表示できます。

選択した時間間隔で、選択したメトリック（可用性、損失、ジッター、待ち時間）のオーバーレイパスとアンダーレイパスを比較できます。また、メトリックのカスタムしきい値を設定し、[適用] をクリックして保存することもできます。デフォルトのしきい値を保存するには、[リセット] をクリックします。

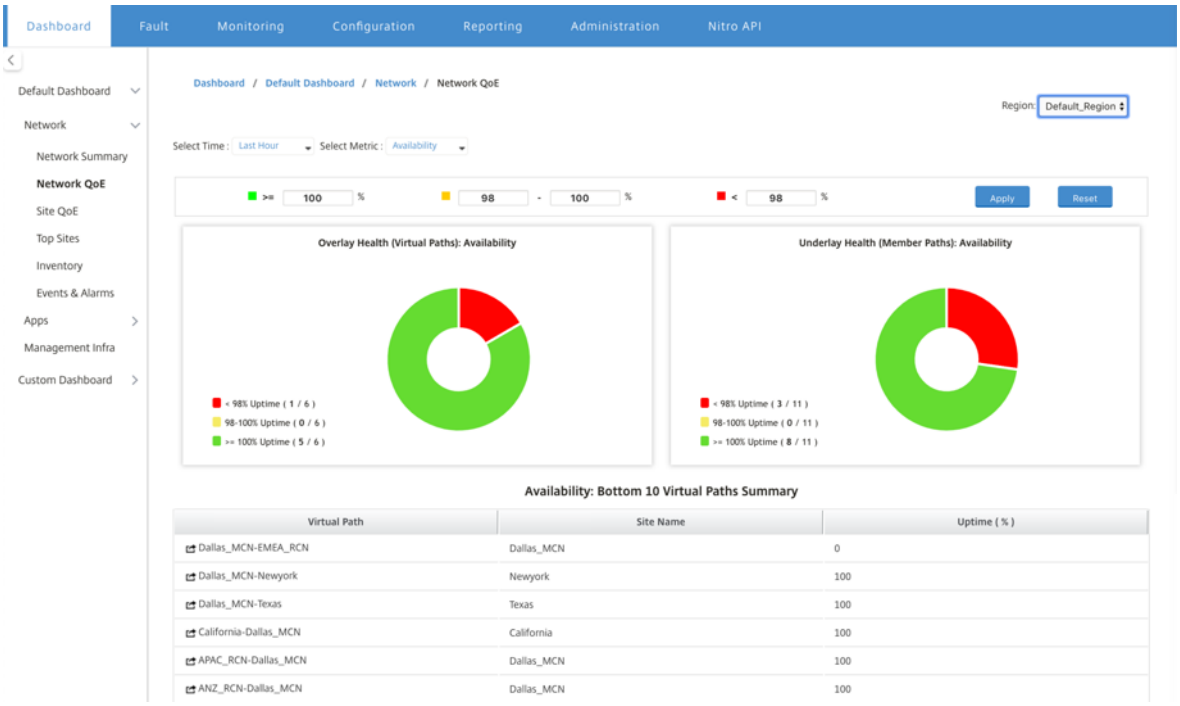
ユーザーは、各行の左側にある ドリルダウン ボタンを使用して、テーブル内の任意の仮想パスにドリルダウンすることもできます。サイト **QoE** が表示され、コンジットとその基になるメンバーパスの詳細な比較が示されます。



スライダーでは、クリックした行に応じてサイト名と仮想パスがデフォルトで選択され、無効になります。ただし、

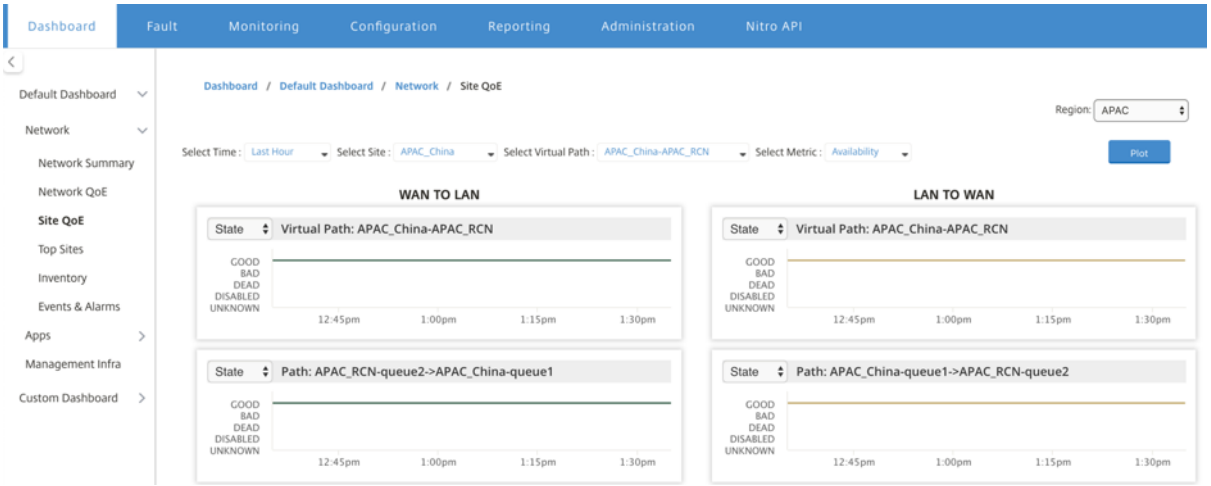
ユーザーは別の時間範囲とメトリックを 選択し、[プロット] オプションをクリックして新しいグラフをプロットできます。

地域の仮想パスヘルス統計を表示するには、ダッシュボード > デフォルトのダッシュボード > 通信網 > ネットワークの **QoE** に移動し地域の選択 ドロップダウンメニューでは、地域を選択します。



サイト **QoE**

Site QoE をツールとして使用して、仮想パスとその基礎となるメンバーパスを比較できます。このサイトとメトリックからサイトと仮想パスを選択する必要があります。**[プロット]** をクリックします。



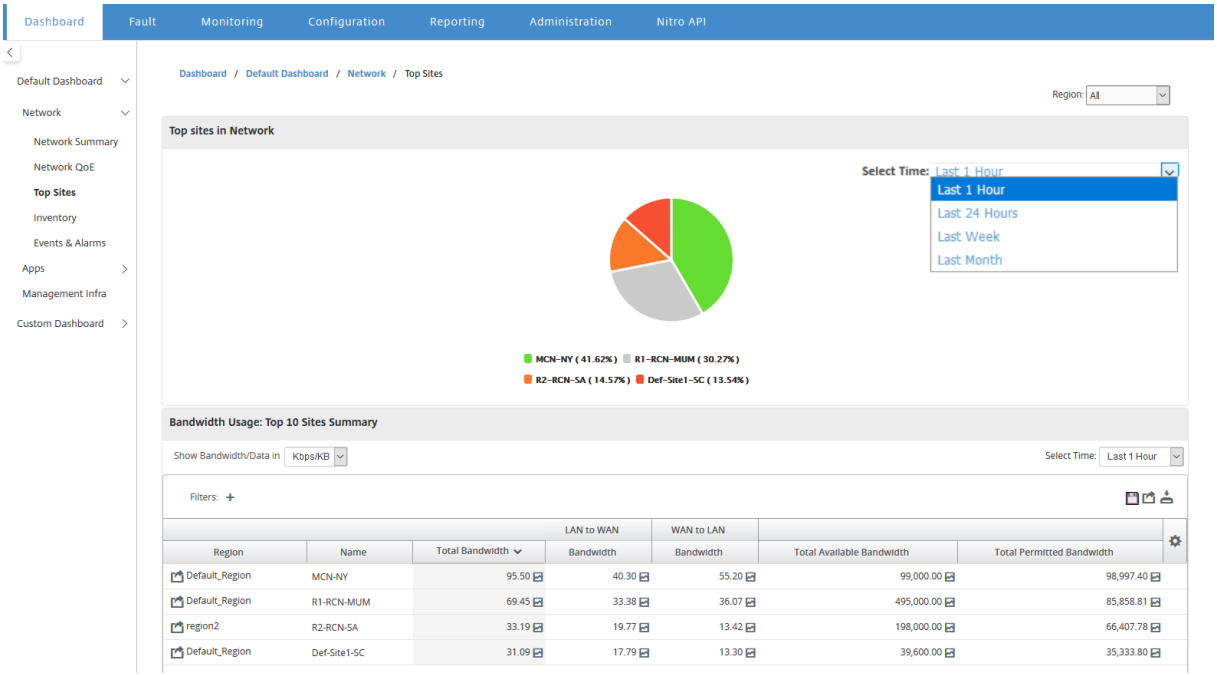
最初のセクションでは、**WAN** から **LAN** への 方向と LAN から WAN への方向の両方で仮想パスの統計をプロットし

ます。以下のセクションでは、基礎となるすべてのメンバーパスグラフをプロットします。これらは両方とも、リージョンレベルとネットワークレベルの両方に存在します。

トップサイト

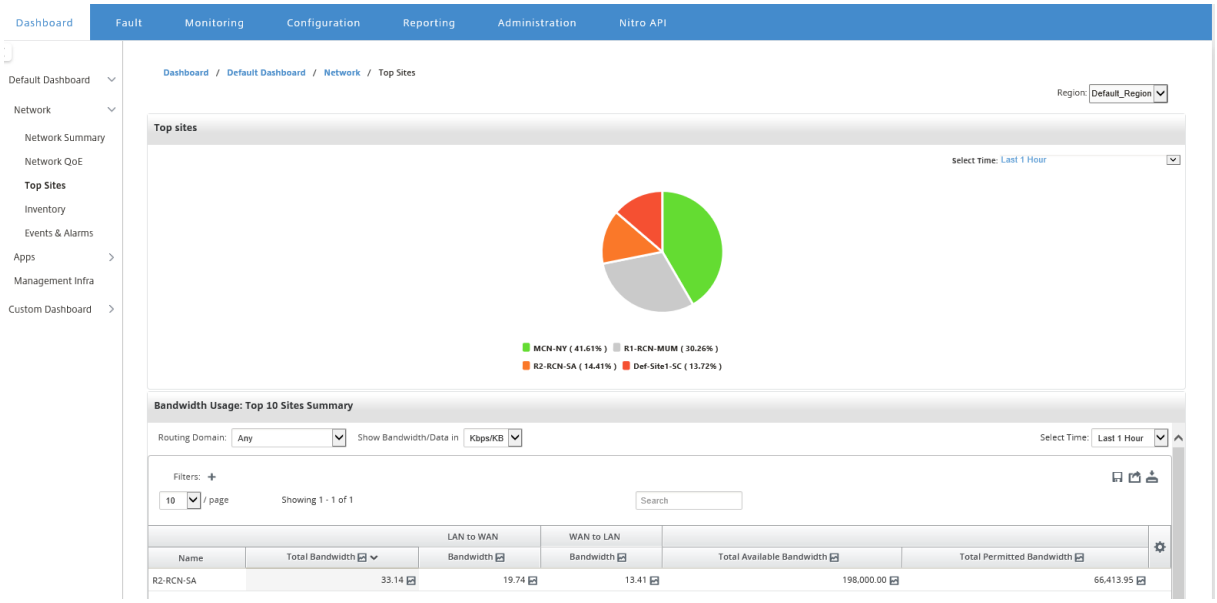
マルチリージョン展開の場合、トップサイト ウィジェットは、選択された時間間隔で帯域幅使用量が最も高い、すべてのリージョンの上位 10 サイトをリストします。

すべての地域で上位のサイトを表示するには、ダッシュボード > デフォルトのダッシュボード > 通信網 > トップサイトに移動し、[地域] ドロップダウンメニューで [すべて] を選択します。



詳細なレポートと統計を表示するには、サイトまたはメトリックをクリックします。

個々のリージョンの場合、トップサイトウィジェットには、リージョン内のすべてのサイトの帯域幅使用統計が表示されます。統計は、選択した時間間隔で収集されます。ルーティングドメインに基づいてサイトをフィルタリングできます。



Inventory

インベントリマネージャは 30 分ごとに、Citrix SD-WAN Center で検出されたすべての Citrix SD-WAN アプライアンスからハードウェア情報を収集します。

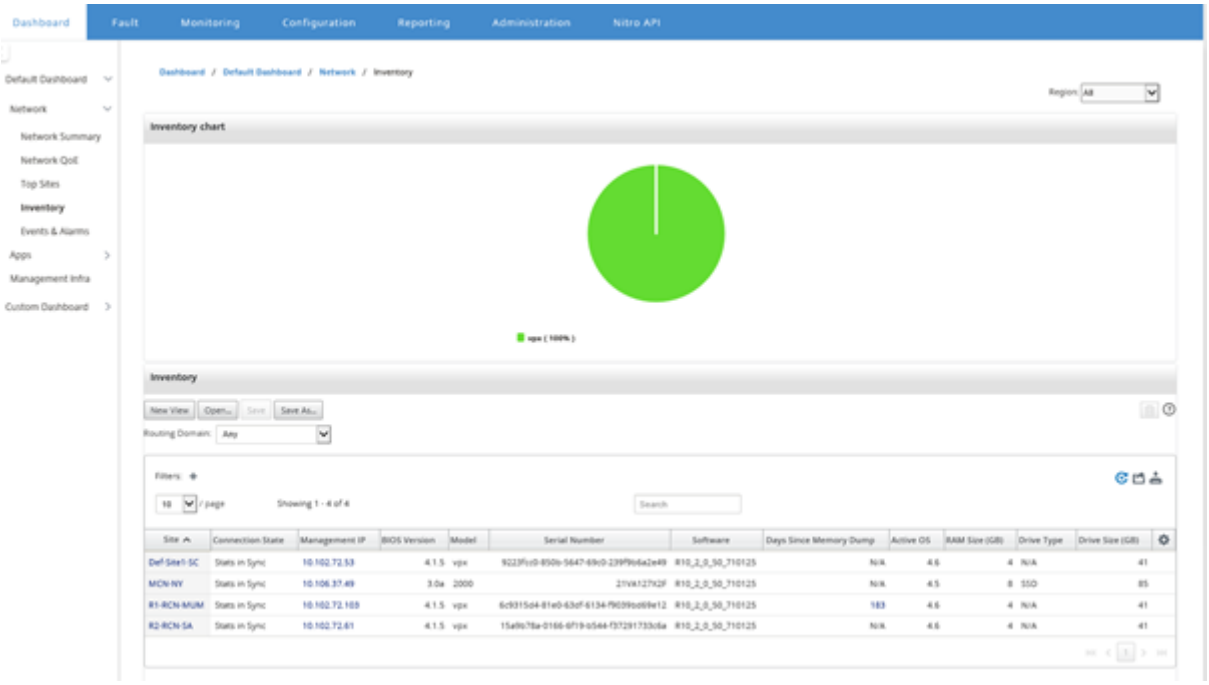
マルチリージョンのインベントリ統計を表示するには、ダッシュボード > デフォルトのダッシュボード > 通信網 > インベントリに移動し [地域] ドロップダウンメニューで選択します。

特定領域の表示の在庫統計に、地域ドロップ ダウンメニューで地域を選択します。

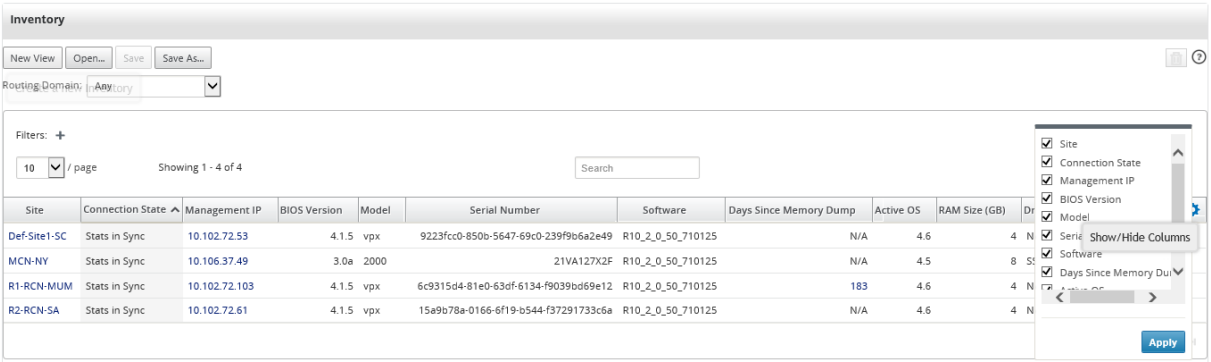
次のインベントリ統計を表示できます。

- 地点: MCN で実行されている構成で見つかったサイトの名前。アプライアンスがセカンダリ MCN の場合、名前の横に「(セカンダリ)」と表示されます。名前をクリックすると、アプライアンスの Web コンソールにアクセスできます。
- 接続状態: アプライアンスへの接続状態。接続に到達できない場合、または認証されていない場合は、赤いアイコンが表示されます。
- 管理 **IP**: アプライアンスの管理 IP アドレス。IP アドレスをクリックして、アプライアンスの Web コンソールにアクセスできます。
- **BIOS** バージョン: アプライアンスの BIOS バージョン。
- 型番: アプライアンスのハードウェアモデル。
- シリアルナンバー: アプライアンスのシリアル番号。
- ソフトウェア; SD-WAN ソフトウェアのバージョン番号。
- メモリダンプからの日数: 最後のシステムエラーメモリダンプからの時間。アプライアンスが過去 4 日間にメモリをダンプした場合、時間の横にエラーアイコンが表示されます。メモリダンプが 5〜10 日前に発生した場合、警告アイコンが表示されます。N/A 利用可能なダンプがない場合に表示されます。時間をクリックすると、SD-WAN のログページが開きます。

- アクティブ **OS**: 現在アプライアンスで実行されている OS。
- **RAM** サイズ（**GB**）：現在アプライアンスにインストールされている RAM の容量（GB）。
- ドライブタイプ: アプライアンスにインストールされているデータストレージドライブのタイプ。値は SSD（ソリッドステートドライブ）または HDD（ハードディスクドライブ）です。
- ドライブサイズ（**GB**）：現在アプライアンスにインストールされているデータストレージドライブのサイズ（GB）。



> 注
>
> を使用して、在庫統計表の列を配置できます。Show/Hide 列 オプション。



イベントとアラーム

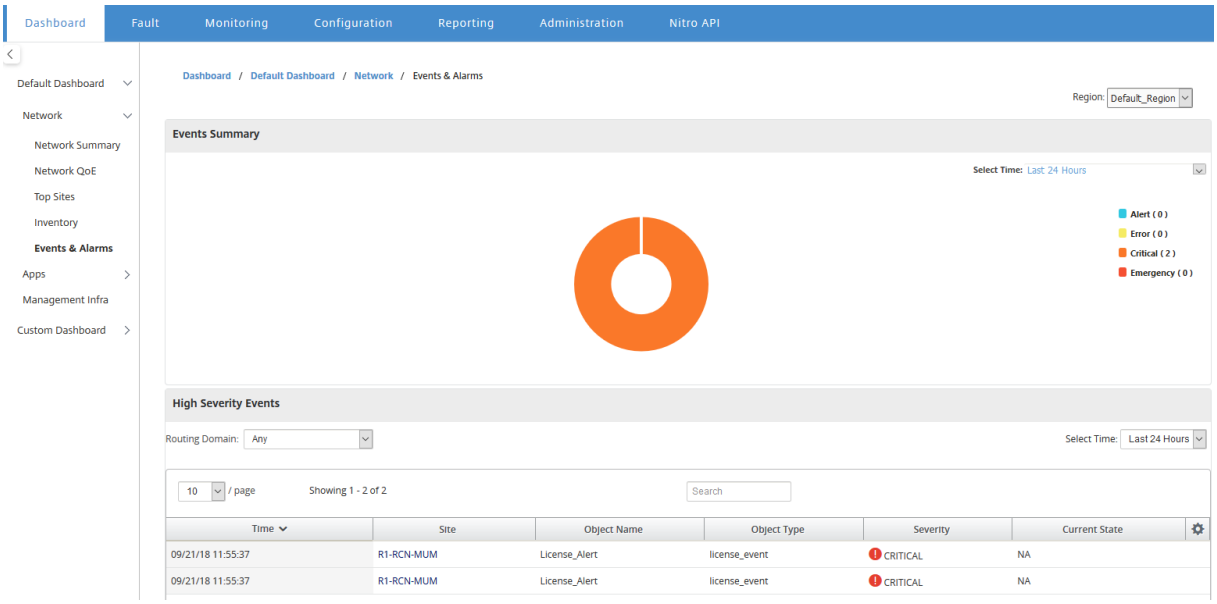
マルチリージョン展開の場合、ネットワーク内のすべてのリージョンのイベントとアラームを表示できます。この情報は、選択した時間間隔で収集されます。マルチリージョンのイベントと統計を表示するには、ダッシュボード > デ

フォルトのダッシュボード > 通信網 > イベント **&** アラームに移動し、[地域] ドロップダウンメニューで [すべて] を選択します。

個々の地域のすべてのイベントとアラームを表示することもできます。この情報は、選択した時間間隔で収集されます。イベントとアラーム統計を表示するには、ダッシュボード > デフォルトのダッシュボード > 通信網 > イベント **&** アラーム に移動し 地域の選択ドロップダウンメニューでは、地域を選択します。

[イベントの概要] セクションには、イベントのタイプと数の概要がグラフィカルに表示されます。グラフをクリックすると、**Fault** ページにイベントが表示されます。また、各カテゴリのイベント数も表示されます。アラームトリガーは、個々の SD-WAN アプライアンスで設定できます。詳細については、「イベント通知」を参照してください。

重大度 の高いイベントセクションには、重大度の高いイベントのリストが表示されます。ルーティングドメインに基づいてイベントをフィルタリングできます。このセクションに表示される情報は、[障害] タブから収集されます。詳細については、「イベント」を参照してください。

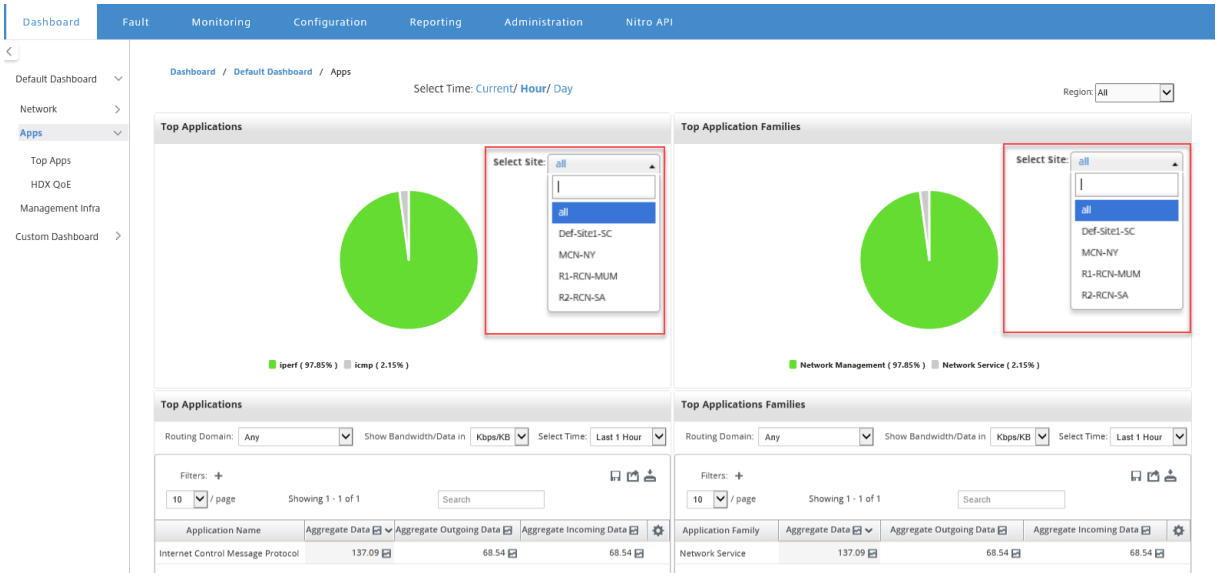


アプリ

上位のアプリ

ディープパケットインスペクション（DPI）により、SD-WAN アプライアンスは通過するトラフィックを解析し、アプリケーションとアプリケーションファミリーのタイプを識別できます。マルチリージョンのデプロイでは、ネットワーク内のすべてのリージョンで上位のアプリケーションと上位のアプリケーションファミリーを表示できます。この情報は、選択した時間間隔で収集されます。

ネットワーク内のすべてのリージョンの上位アプリケーション統計を表示するには、ダッシュボード > デフォルトのダッシュボード > アプリ **>** 上位のアプリ、に移動し [地域] ドロップダウンメニューで [すべて] を選択します。

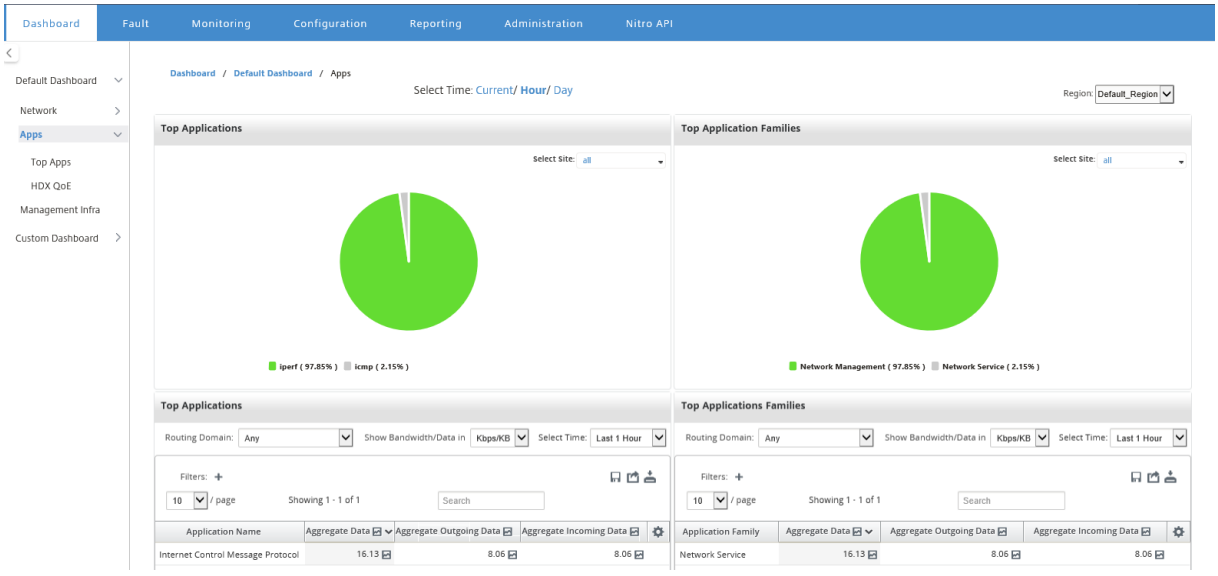


トップアプリケーション と トップアプリケーションファミリの両方のサイト選択の検索可能なドロップダウンリストを表示できます。

特定の地域の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を表示することもできます。

地域のアプリケーション統計を表示するには、ダッシュボード > デフォルトのダッシュボード > アプリ **>** トップアプリ に移動し 地域ドロップダウンメニューで ** 地域を選択。**

サイトと時間間隔は、過去 24 時間、過去 1 時間、または現在として選択できます。



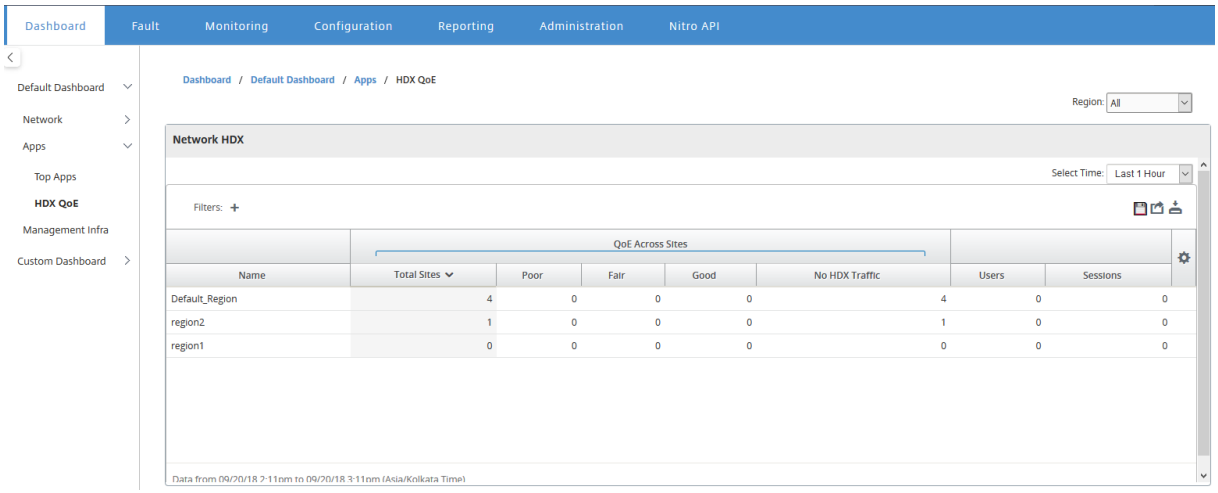
HDX QoE

Quality of Experience（QoE）は、ICA の Quality of Experience を理解するのに役立つ計算されたインデックスです。このインデックスは、WAN からサイトに移動するすべての ICA アプリケーショントラフィックに対して計

算されます。パケットドロップ、ジッター、および遅延の統計は、QoE 計算で使用されます。QoE は、[0, 100], 数値が大きいほど、ユーザーエクスペリエンスは向上します。ジッタ、遅延、およびパケットドロップの統計情報は、パケット処理中にデータパスで追跡されます。

ネットワーク全体のサイトは、HDX トラフィックの QoE に基づいて、高、中、低、または HDX トラフィックなしに分類されます。詳しくは、「HDX QoE」を参照してください。

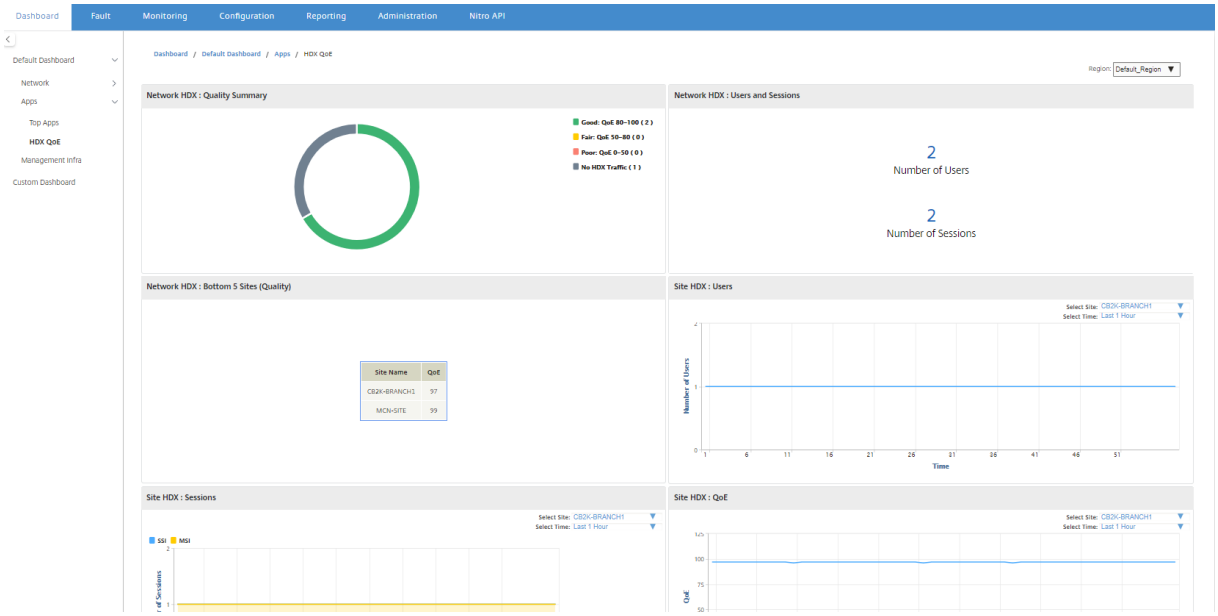
ネットワーク内のすべてのリージョンのサイトの HDX QoE を表示するには、ダッシュボード > デフォルトのダッシュボード > アプリ **> HDX QoE**、に移動し地域] ドロップダウンメニューで [すべて] を選択します。



個々のリージョンの次の HDX QoE メトリックを表示できます。

- ネットワーク HDX：品質の概要
- ネットワーク HDX：ユーザーとセッション
- ネットワーク HDX：下位 5 サイト（品質）
- サイト HDX：ユーザー
- サイト HDX：セッション
- サイト HDX：体験の質

HDX QoE 統計を表示するには、ダッシュボード > デフォルトのダッシュボード > アプリ **> HDX** の **QoE** に移動し地域の選択ドロップダウンメニューでは、地域を選択します。

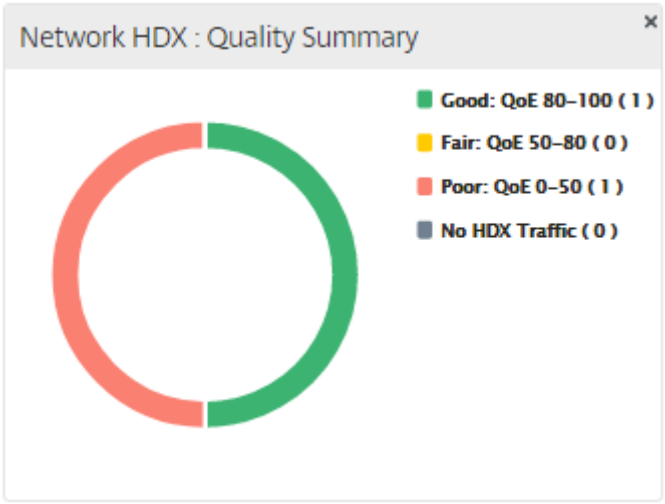


> 注
>
> 各サイトの統計は個別にポーリングされるため、異なるサイトの HDX ダッシュボードデータと HDX レポートが同期していないように見える場合があります。
>
> HDX ダッシュボードウィジェットでは、HDX トラフィックのないサイトが表示される場合がありますが、HDX セッションとユーザーの数がゼロ以外である場合があります。これは、そのポーリング期間中、HDX セッションがアイドル状態のままで、オープン状態のままである場合に発生します。

ネットワーク **HDX**：品質の概要

HDX トラフィックは、次の品質カテゴリに分類されます。

品質	QoE 範囲
高	80–100
標準	50–80
低	0–50
HDX トラフィックなし	-

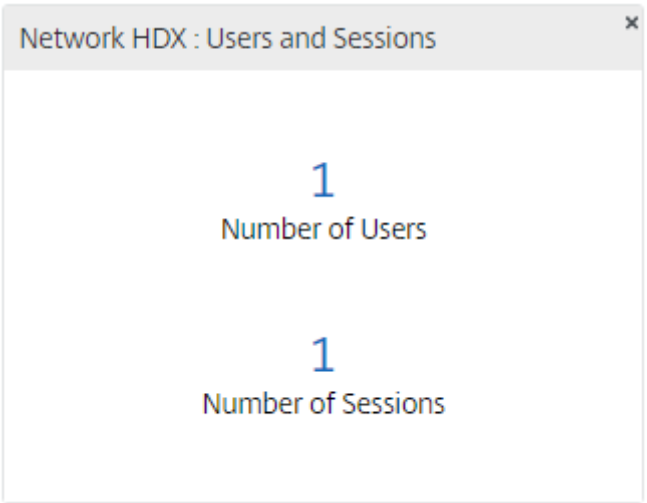


グラフをクリックすると、サイトごとの HDX レポートを表示できます。詳細については、「HDX レポートを表示する方法」を参照してください。

ネットワーク **HDX**: ユーザーとセッション

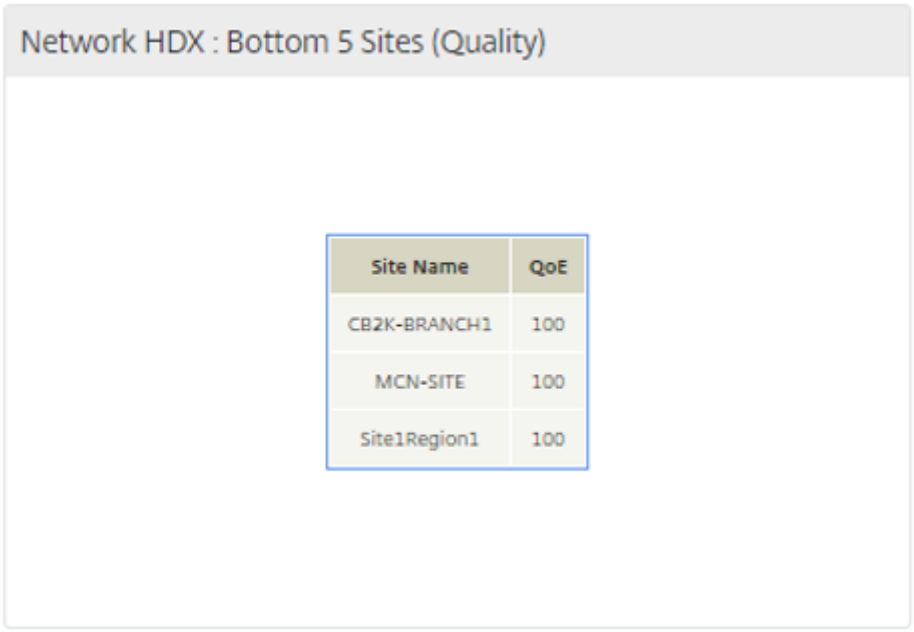
このウィジェットは、アクティブな HDX ユーザーとセッションの数に関する情報を提供します。セッション数は、アクティブなシングルセッション ICA（SSI）およびマルチセッション ICA（MSI）セッションの総数です。

> 注
>
> 現在のリリースでは、ユーザー数は明確なユーザー名に基づいていません。つまり、2 人の異なるマシンで 1 人のユーザーが開始した 2 つのセッションは、2 人のユーザーとしてカウントされます。



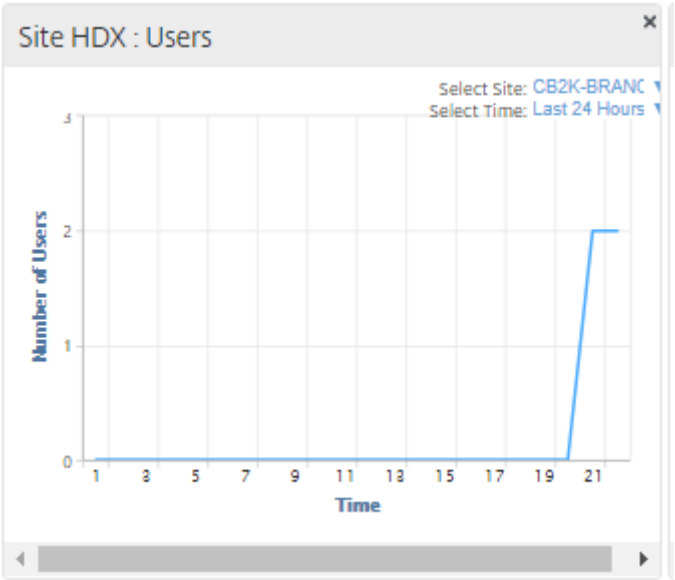
ネットワーク **HDX**：下位 **5** サイト（品質）

このウィジェットは、QoE スコアが最も低い上位 5 つのサイトのリストを提供します。これにより、エンドユーザーエクスペリエンスの取り組みが向上します。



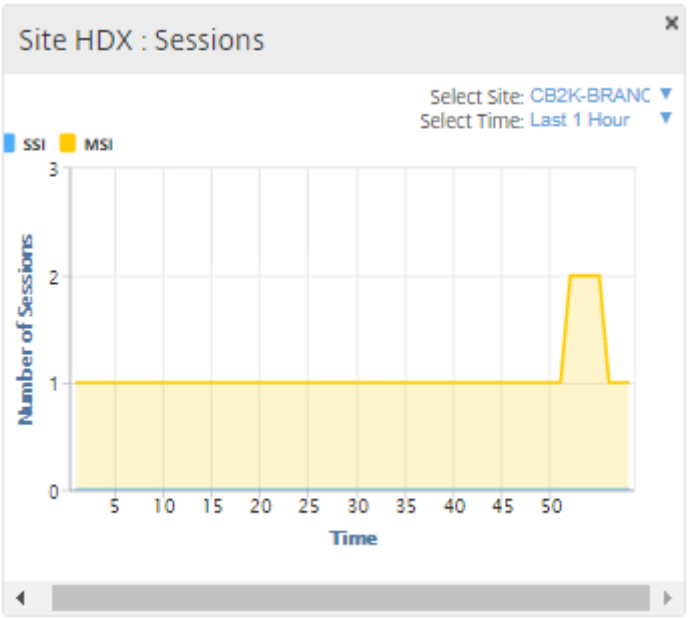
サイト **HDX**：ユーザー

このウィジェットは、選択した時間間隔で特定のサイトでアクティブだったユーザーの数をグラフィカルに表示します。サイトと時間間隔を、過去 24 時間、過去 1 時間、または過去 5 分間から選択できます。



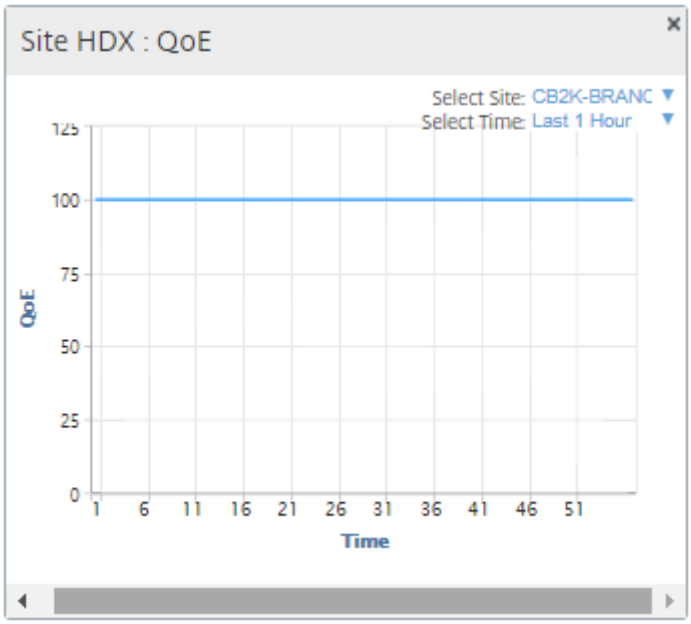
サイト **HDX**：セッション

このウィジェットは、選択した時間間隔で特定のサイトでアクティブになっている MSI および SSI セッションの数をグラフィカルに表示します。サイトと時間間隔を、過去 24 時間、過去 1 時間、または過去 5 分間から選択できます。



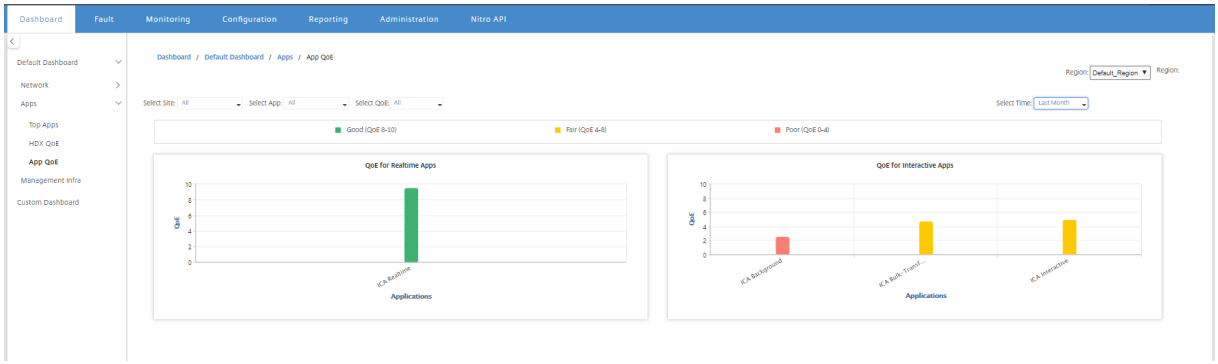
Site HDX：体験の質

このウィジェットは、選択された時間間隔における特定のサイトでの全体的な QoE のグラフィカル表現を提供します。サイトと時間間隔を、過去 24 時間、過去 1 時間、または過去 5 分間から選択できます。



アプリケーション **QoE**

アプリケーション QoE は、アプリケーションのエクスペリエンス品質の尺度です。Application QoE スコアの範囲は 0〜10 です。10 は優れた品質を表し、0 は低品質を表します。詳細については、「アプリケーション QoE」を参照してください。リアルタイムおよびインタラクティブトラフィックのアプリケーション QoE スコアを表示できます。

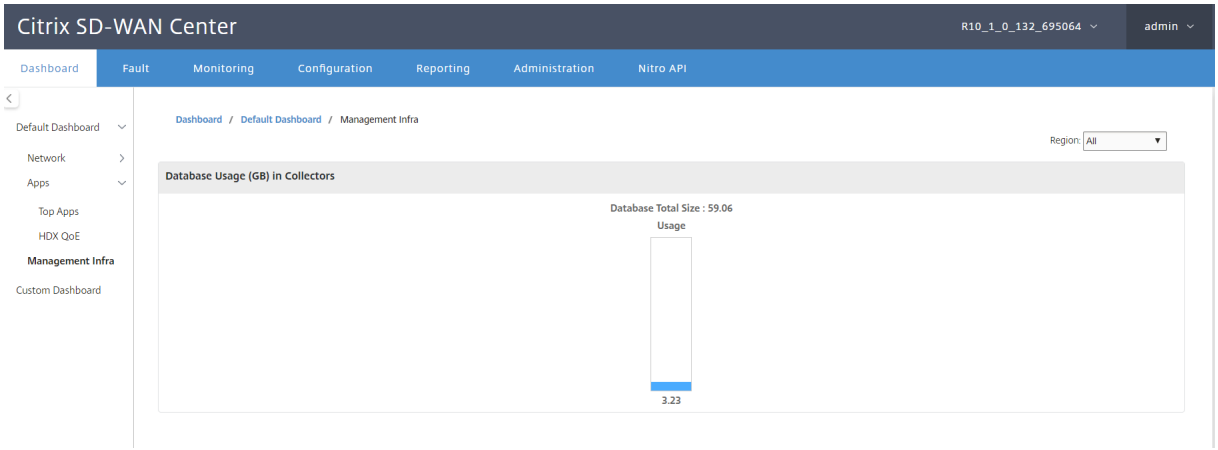


アプリケーションの QoE 統計は、サイト、アプリケーション、または QoE タイプでフィルタリングできます。

インフラ管理

[管理インフラ] ページでは、Citrix SD-WAN Center データベースの使用状況とストレージ統計を表示できます。

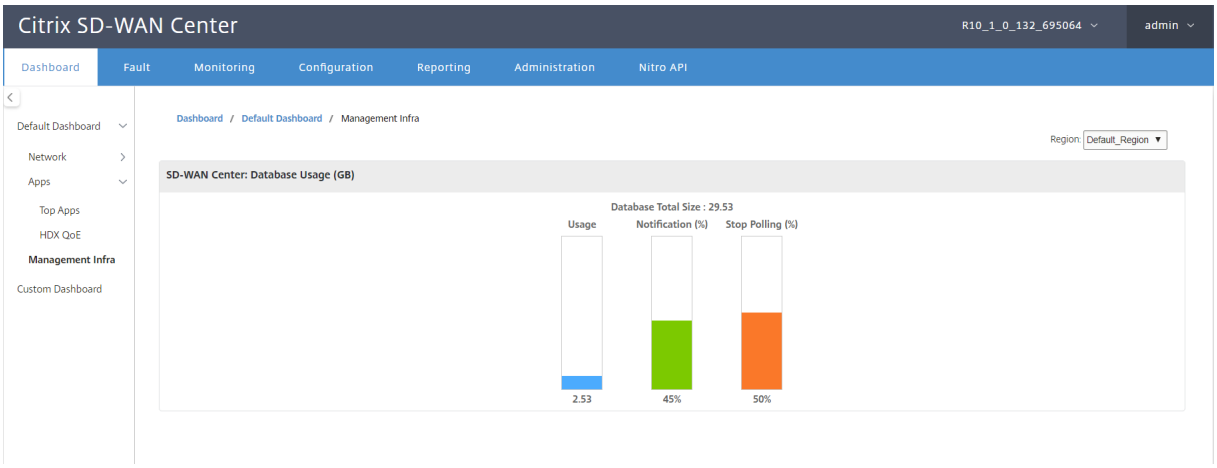
マルチリージョン展開の場合、ネットワーク内のすべてのコレクターのデータベース使用状況を表示できます。マルチリージョンデータベースの統計情報を表示するには、ダッシュボード > デフォルトのダッシュボード > **[**管理インフラ] に移動し [地域] ドロップダウンメニューで [すべて] を選択します。



特定の地域の Citrix SD-WAN Center データベース統計を表示するには、ダッシュボード > デフォルトのダッシュボード > 管理インフラ、に移動し地域**]** ドロップダウンメニューでは、地域を選択します。

[データベースの使用状況**]** セクションには、データベースリソースの使用状況のグラフィカルな概要と、通知の送信またはデータの収集の停止に関するしきい値が表示されます。グラフをクリックすると、[データベースのメンテナンス] ページに詳細が表示されます。

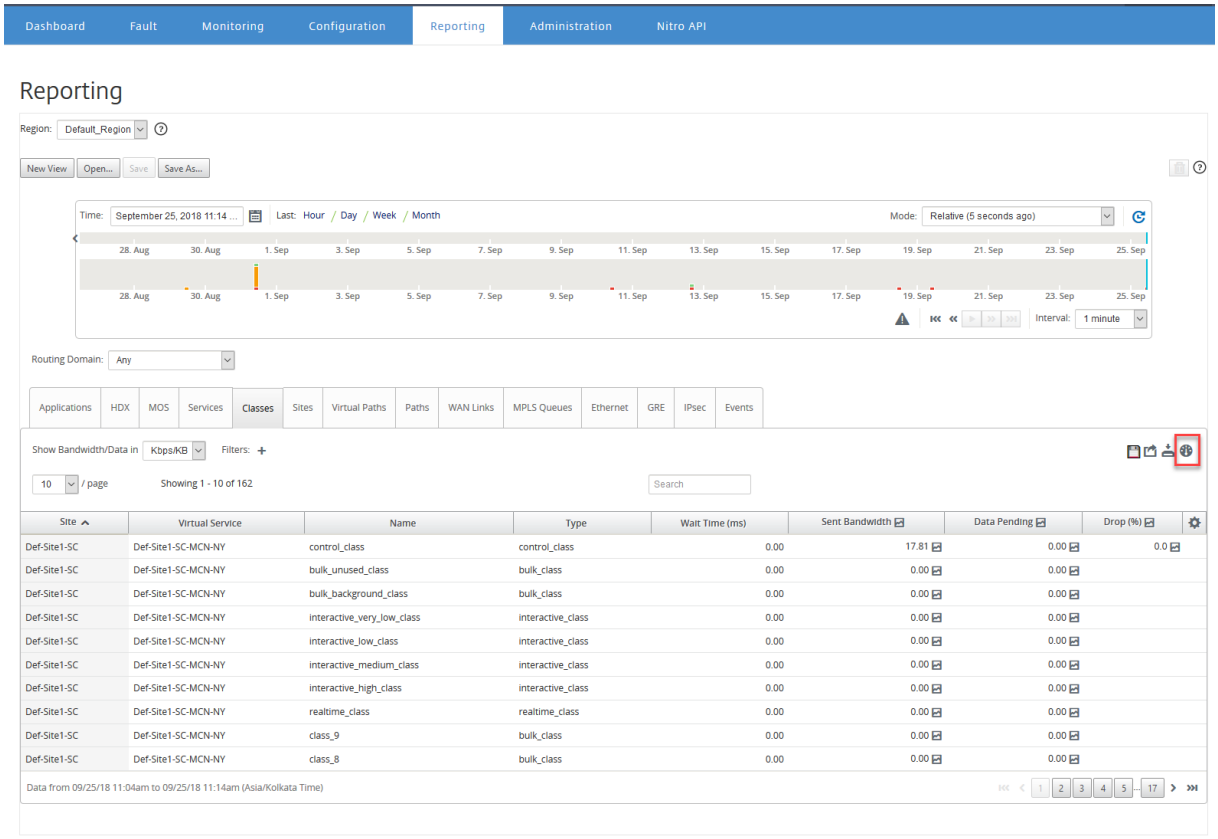
- 使用法: 現在使用されているデータベース容量（GB）。
- 通知: データベース使用通知を生成するためのしきい値。しきい値は、データベースの最大サイズの割合です。電子メールアラートが設定されている場合、データベースのサイズがこのしきい値を超えると、電子メール通知が送信されます。詳しくは、「イベント通知」を参照してください。
- ポーリングを停止: 統計ポーリングを停止するためのしきい値。しきい値は、データベースの最大サイズの割合です。データベースのサイズがこのしきい値を超えると、ポーリングが停止します。詳細については、「データベースの管理」を参照してください。



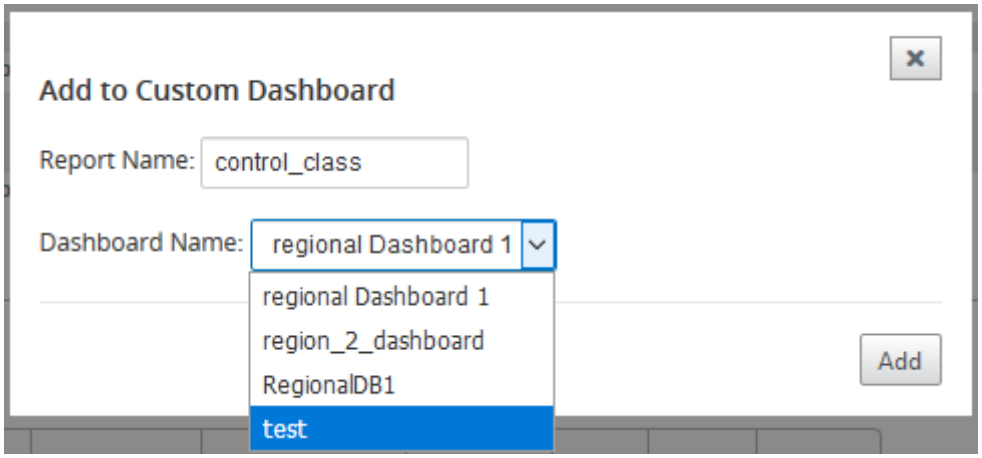
カスタムダッシュボード

Citrix SD-WAN Center のダッシュボードをカスタマイズして、分析のニーズに基づいてダッシュボードに表示する統計を選択できます。地域の詳細または全体的な概要のカスタムダッシュボードを作成します。既存のレポートをカスタマイズすることもできます。

> 注
>
> [レポート] ページの [ダッシュボードに追加] オプションを使用して、レポートをウィジェットとしてカスタムダッシュボードに固定できるようになりました。



レポート名を入力し、カスタムダッシュボードを選択します。



地域の詳細のカスタムダッシュボードでは、次の地域レベルのウィジェットから選択できます。

- サイト概要
- 仮想パス
- 地域イベント
- リージョンアラームの概要
- 在庫マネージャー（地域ごと）
- 地域ごとの上位サイト

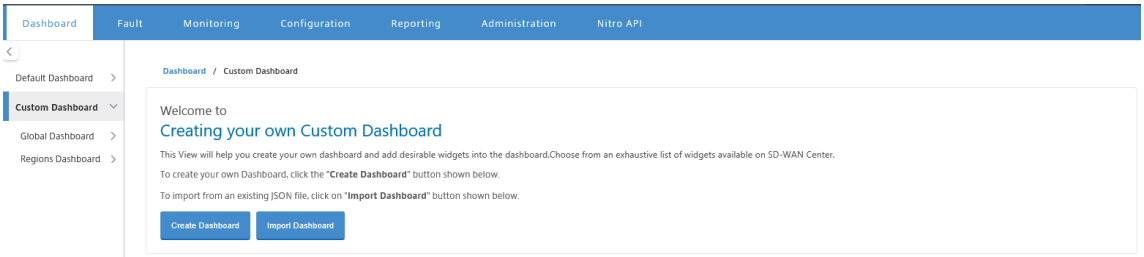
- パス
- MPLS キュー
- イーサネット
- LAN GRE トンネル
- IPsec トンネル
- サービス概要
- クラス
- サイトイベント
- 地域ごとの上位アプリケーション
- 地域ごとの上位アプリケーションファミリ
- サイト HDX：ユーザー
- サイト HDX：セッション
- サイト HDX：QoE
- MOS アプリケーション
- データベースの使用

グローバルサマリーカスタムダッシュボードの場合、次のネットワークレベルのウィジェットから選択できます。

- マルチリージョンの概要
- ネットワークの仮想パスヘルス
- イベント
- アラームの概要
- 在庫マネージャー
- ネットワークのトップサイト
- ネットワーク HDX
- コレクターでのデータベースの使用
- 上位のアプリケーション
- トップアプリケーションファミリ

カスタムダッシュボードを作成するには：

1. ダッシュボードに移動 > カスタムダッシュボード をクリックし、[ダッシュボードの作成] をクリックします。



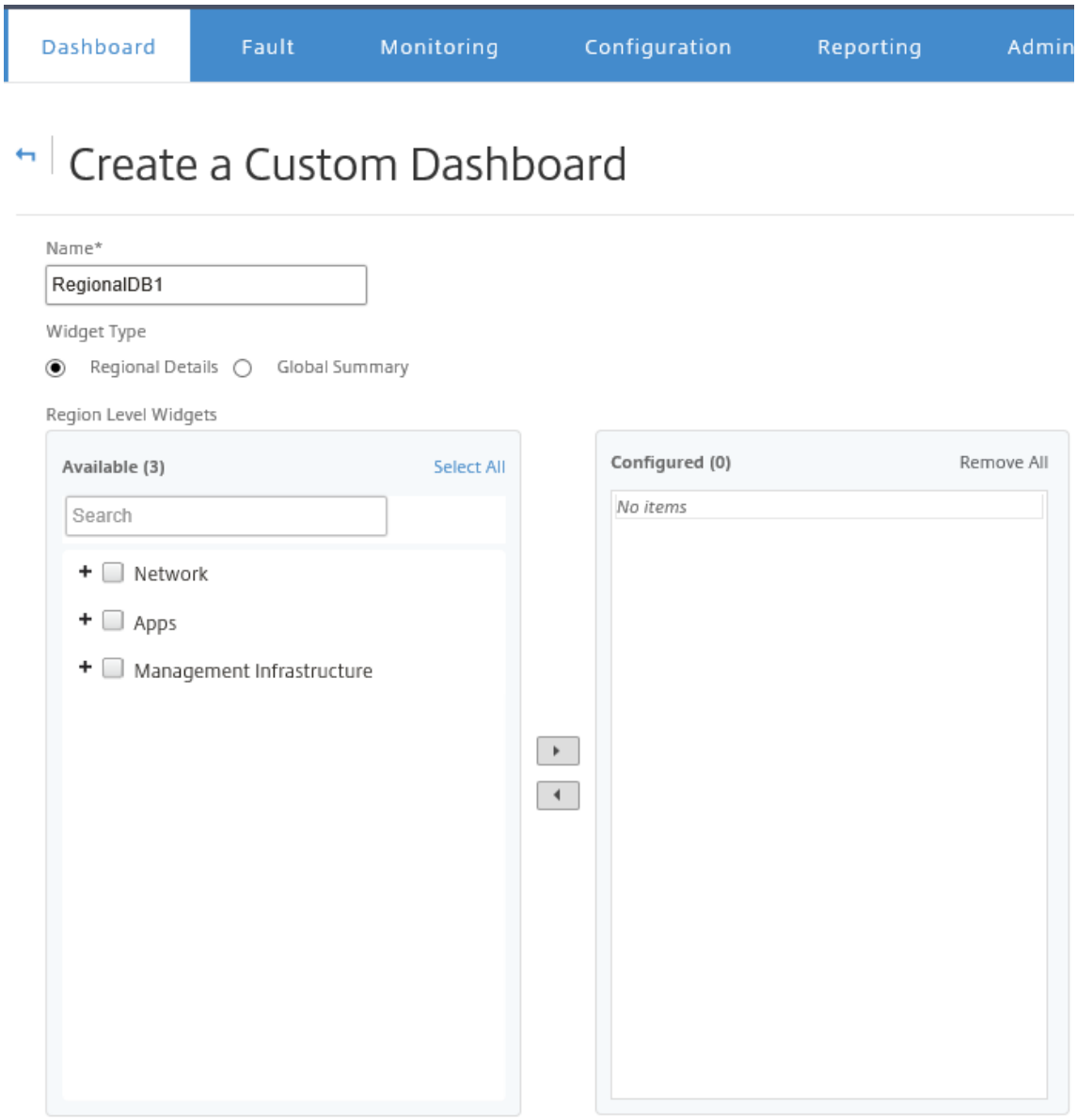
> 注
>
> [ダッシュボードのインポート] をクリックして、JSON 形式で既存のダッシュボードをインポートする

> こともできます。

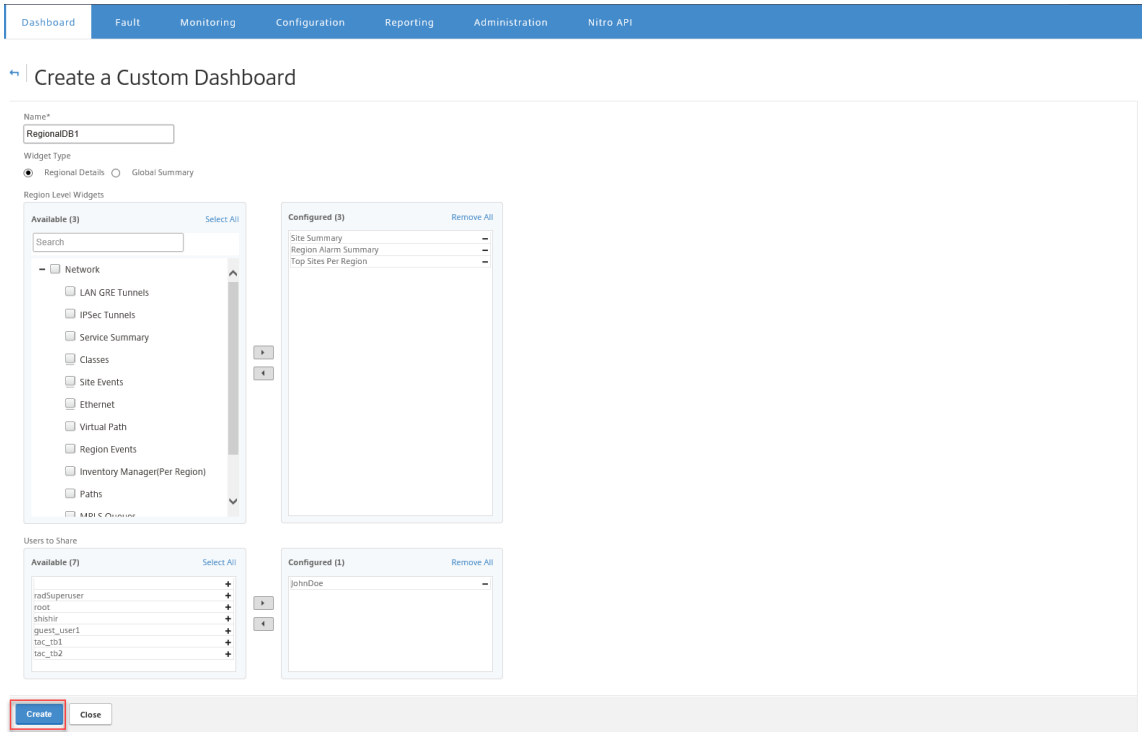
2. [名前] フィールドに、カスタムダッシュボードの名前を入力します。
3. ウィジェットのタイプを選択します。グローバル レベルを選択してネットワークレベルのウィジェットを表示し、地域の詳細 を選択して地域レベルのウィジェットを表示します。

4.「追加」をクリックして、必要なウィジェットを選択します。

ウィジェットは、ネットワーク、アプリ、管理インフラストラクチャの 3 つのレベルに分類されます。



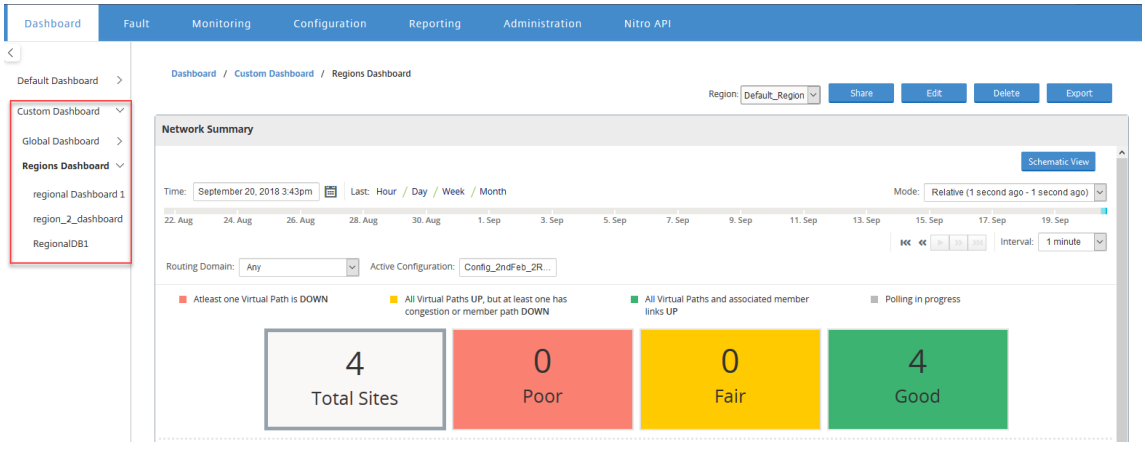
> 注
>
> 単一リージョンのデプロイメントでは、リージョンレベルのウィジェット のみを使用できます。



カスタムダッシュボードを複数のユーザーと共有することもできます。ユーザーについて詳しくは、「ユーザーアカウント」を参照してください。

5. [**Create**] をクリックします。新しく作成されたカスタムダッシュボードが [カスタムダッシュボード] に表示され ます。

> ヒント
>
> カスタムダッシュボードを編集または削除できます。



診断パッケージ

April 13, 2021

診断パッケージは、すべてのシステムログファイル、システム情報、および Citrix SD-WAN サポートチームがシステムの問題を診断して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。

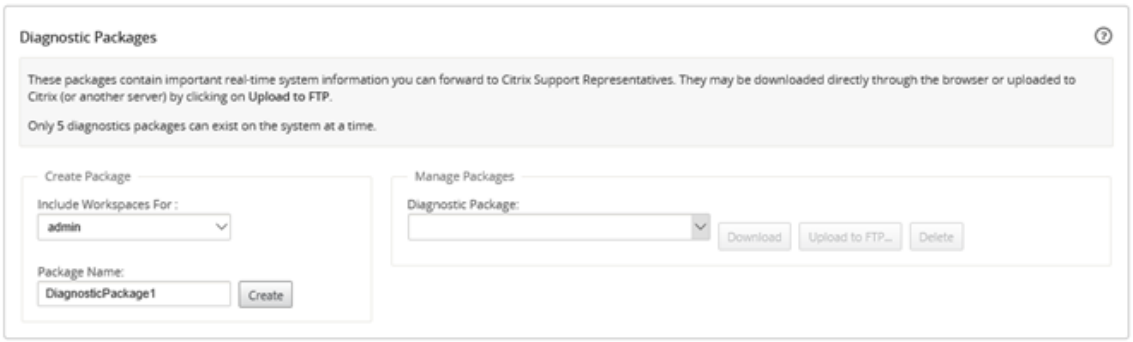
パッケージを作成したら、パッケージをコンピューターにダウンロードして診断パッケージを Citrix カスタマーサポートに郵送するか、Citrix カスタマーサポートサーバー（または別のサーバー）に直接アップロードできます。

> 注
>
> Citrix SD-WAN Center は、一度に最大 5 つの診断パッケージを保存できます。

診断パッケージを作成するには:

1. Citrix SD-WAN Center の Web インターフェイスで、[監視] タブをクリックし、[診断] をクリックします。
2. [診断パッケージ] セクションの [パッケージの 作成] で、[次のワークスペースを含める] ドロップダウンリストから、診断にワークスペースをコピーするユーザーを選択します。

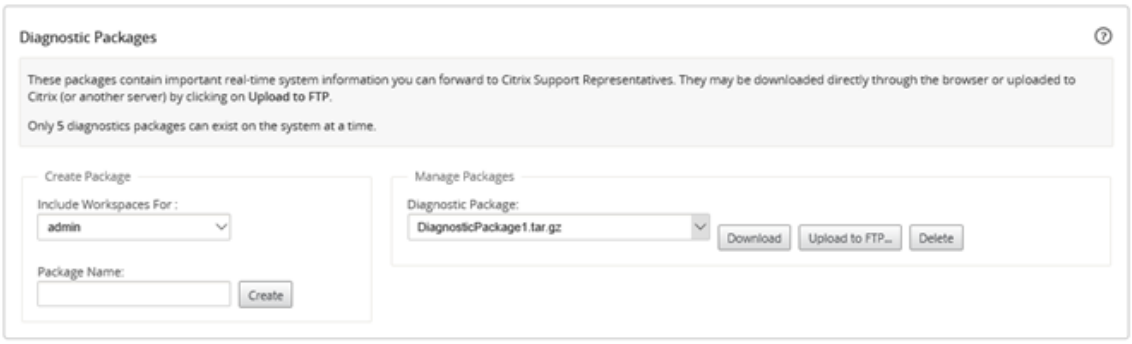
   > 注
   >
   > 診断パッケージには、選択したユーザーが最後に変更した 5 つの構成が含まれます。

3. [パッケージ名] フィールドに、診断パッケージの名前を入力します。
4. ［作成］ をクリックします。これにより、システム診断が実行され、診断パッケージが生成されます。

診断パッケージをダウンロードするには:

1. [診断パッケージ] セクションの [パッケージの管理] で、[診断パッケージ] ドロップダウンリストから、ダウンロードするパッケージを選択します。



2. [**Download**] をクリックします。診断パッケージがローカルコンピューターにダウンロードされます。

診断パッケージを FTP サーバーにアップロードするには:

1. **[**診断パッケージ**]** セクションの [パッケージの管理] で、[診断パッケージ**]** ドロップダウンリストから、アップロードするパッケージを選択します。
2. [**FTP** にアップロード**]** をクリックします。[**FTP** サーバーにアップロード] ダイアログボックスが開き、FTP 認証情報を指定して、パッケージを Citrix カスタマーサポートの FTP サーバーまたは別の FTP ホストにアップロードします。

3. [顧客名**]** フィールドに、Citrix SD-WAN サポートが診断パッケージを識別するのに役立つ名前を入力します。この名前のディレクトリが Citrix FTP サーバー上に作成され、ファイルがその場所にアップロードされます。
4. 「**FTP** ホスト」フィールドに、FTP サーバーの IP アドレスまたはホスト名（DNS が構成されている場合）を入力します。
5. ユーザー名フィールド に、FTP サーバへのログインに使用するユーザー名を入力します。
6. 「パスワード」フィールドに、ユーザー名に関連付けられているパスワードを入力します。

7. ［アップロード］をクリックします。

> 注
>
> 最大許容パッケージの制限を超えないように、定期的に古い診断パッケージを削除することをお勧めします。既存の診断パッケージを削除するには、[診断パッケージ] ドロップダウンリストから診断パッケージを選択し、[削除] をクリックします。

イベント

April 13, 2021

Citrix SD-WAN Center は、ネットワークで検出されたすべてのアプライアンスからイベント情報を収集します。このイベント情報は、イベントビューア ページでフィルタリングおよび表示できます。

イベントの詳細には、次の情報が含まれます。

- 時間：イベントが生成された時間。
- サイト：イベントが発生したサイトの名前。
- アプライアンス **ID**：イベントの発生元のアプライアンスがプライマリ（**0**）かセカンダリ（**1**）のアプライアンスかを示します。

  > 注
  >
  > アプライアンス ID 列はデフォルトで非表示になっています。列を表示するには、Show/Hide（歯車のアイコン）をクリックし、ドロップダウンメニューから [アプライアンス **ID**] チェックボックスを選択します **

- オブジェクト名：イベントを生成するオブジェクトの名前。
- オブジェクトタイプ：イベントを生成するオブジェクトのタイプ。
- 重大度：イベントの重大度レベル。
- 以前の状態：イベント発生前のオブジェクトの状態。該当しない場合、状態は 不明 としてリストされます。
- 現在の状態：イベント発生時のオブジェクトの状態。
- 説明：イベントの説明テキスト。

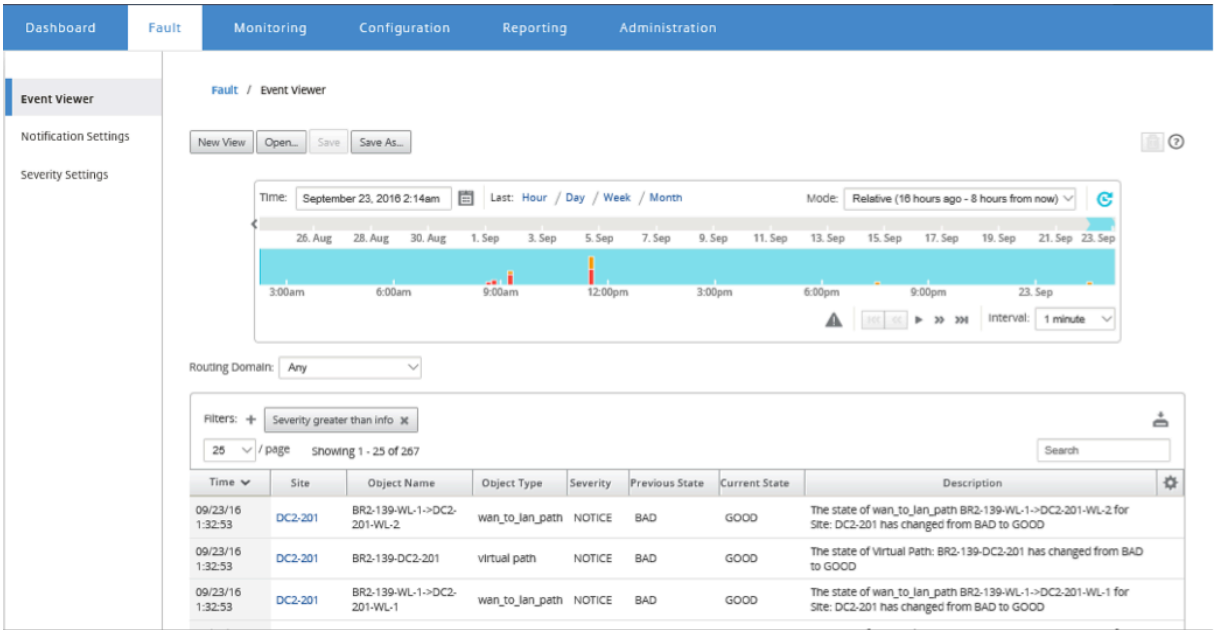
イベントを表示する

イベントビューアページからイベントを表示し、フィルタリングしてダウンロードできます。

イベントビューアページにアクセスします。

Citrix SD-WAN Center の Web インターフェイスで、[障害] タブをクリックします。

デフォルトでイベントビューアページが表示されます。



タイムラインコントロールを使用して、特定の期間のレポートを選択して表示できます。詳細については、「タイムラインコントロール」を参照してください。

> 注
>
> 過去 30 日間のイベントデータを表示できます。この期間を過ぎたデータは、SD-WAN Center コレクターとそれぞれのリージョナルコレクターから自動的に削除されます。

レポートビューを作成、保存、開くこともできます。詳細については、「ビューを管理する」を参照してください。

フィルターの使用

イベントテーブルの結果を絞り込むためのカスタムフィルターを作成できます。

フィルターを作成して適用するには:

1. クリック + [フィルター] セクションのラベルの右側にあるアイコン。**
2. ドロップダウンメニューからカテゴリを選択します。

   使用可能なオプションは次のとおりです。

   - サイズ
   - オブジェクト名
   - オブジェクトの種類

- 重大度
- 以前の状態
- 現在の状態

3. 中央のドロップダウンメニューから演算子を選択します。

   使用できるオプションは、次のとおりです。

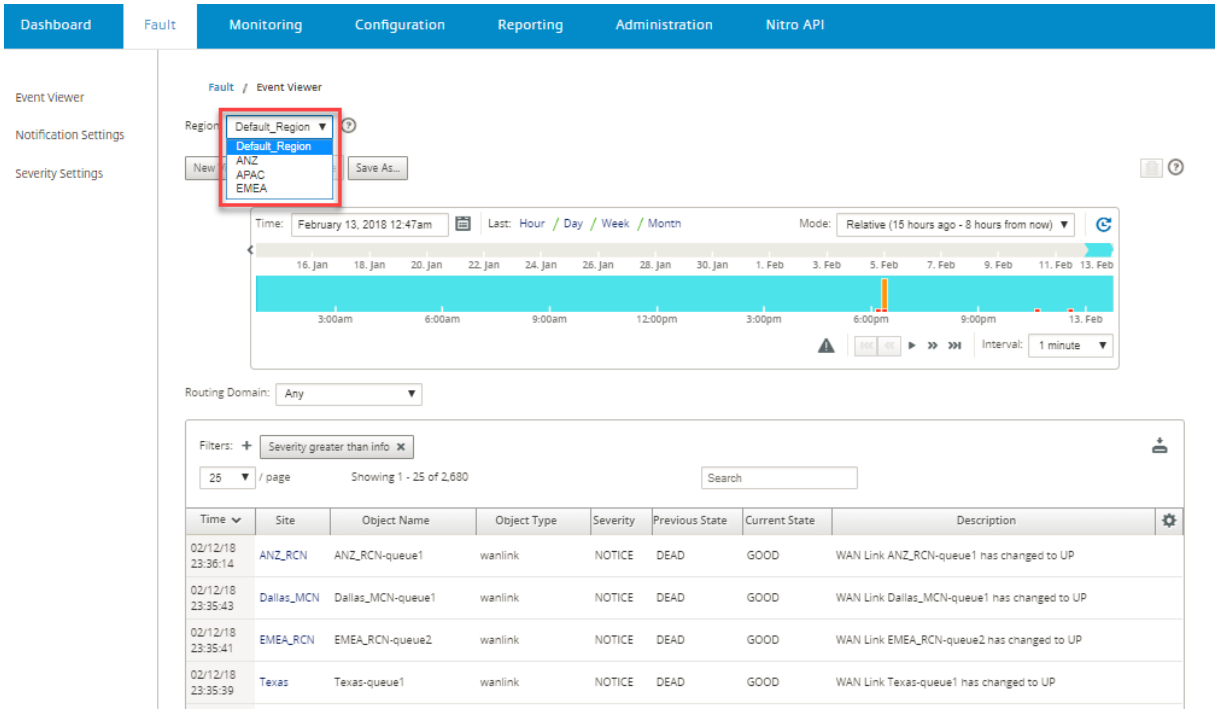
   - is
   - ≠
   - の一つであります
   - 以下を含む
   - 以下を含まない
   - 未満
   - 以下
   - 上回る
   - 次のもの以上

4. フィルターを区切る文字列または値を入力します。

> 注
>
> このフィールドでは大文字と小文字が区別されます。

> 注
>
> 複数のフィルターを作成して適用できます。
> マルチリージョンネットワークの場合、特定のリージョンを選択してイベントを表示できます。

イベントデータは、それぞれのリージョンのコレクターからフェッチされます。



> 注
>
> 単一リージョンネットワーク展開では、[リージョン] ドロップダウンリストは使用できません。

イベントテーブルを CSV ファイルとしてダウンロードするには:

イベントテーブルの右上隅にある [ダウンロード] アイコンをクリックします。

イベント統計の詳細については、「イベントレポート」を参照してください。

さまざまなイベントタイプの外部イベント通知を電子メール、SNMP トラップ、または syslog メッセージとして送信するように Citrix SD-WAN Center を構成できます。詳しくは、「イベント通知」を参照してください。

イベント通知

April 13, 2021

さまざまなイベントタイプのイベント通知を電子メール、SNMP トラップ、または syslog メッセージとして送信するように Citrix SD-WAN Center を構成できます。電子メール、SNMP、および syslog 通知設定を構成したら、さまざまなイベントタイプの重大度を選択し、イベント通知を送信するモード（電子メール、SNMP、syslog）を選択できます。通知は、イベントタイプに指定された重大度レベル以上のイベントに対して生成されます。

使用可能な重大度レベルは、重大度の降順で次のとおりです。

- 緊急

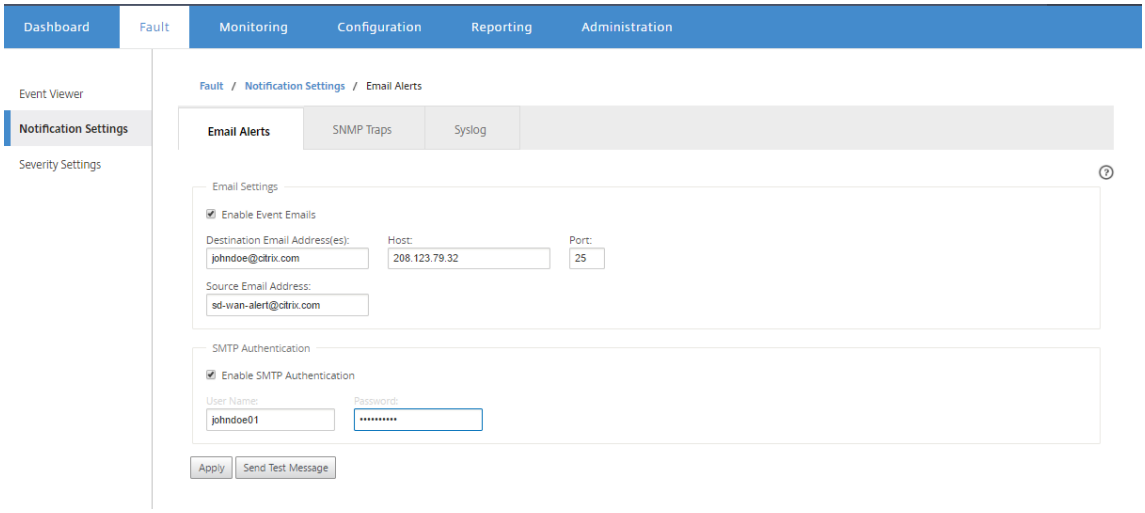
- アラート
- 重大
- エラー
- 警告
- 通知
- 情報
- デバッグ

> ヒント
>
> 通知設定を構成して、ネットワーク内の Citrix SD-WAN Center と個々の Citrix SD-WAN アプライアンスの両方で、電子メール、SNMP トラップ、または Syslog メッセージでイベントアラートを受信できます。
>
> ただし、Citrix SD-WAN Center で通知を有効にすると、Citrix SD-WAN ネットワーク全体（つまり、MCN とすべてのサイト）のイベント通知を受信できます。一方、Citrix SD-WAN アプライアンスで通知を有効にすると、個々のアプライアンスからのみ通知を受信できます。
>
> ネットワーク内の他の Citrix SD-WAN アプライアンスからの冗長な通知を回避するために、Citrix SD-WAN Center でのみ通知を有効にすることをお勧めします。

メール通知設定の構成

電子メール通知設定を構成するには：

1. Citrix SD-WAN Center の Web 管理インターフェイスで、[障害]> 通知設定 > メールアラートに移動します。



2. [イベントメールを有効にする] を選択します。
3. **Destination Email Address（es）]** フィールドに、アラート通知の送信先の電子メールアドレスを入力します。

> 注
>
> セミコロンで区切って複数のメールアドレスを入力できます。

4. [ホスト] フィールドに、外部 SMTP サーバーの IP アドレスまたはホスト名を入力して、電子メールメッセージをインターネットにリレーします。
5. [ポート] フィールドに、SMTP 接続に使用するポート番号を入力します。The default port is 25.
6. [送信 元メールアドレス] フィールドに、メールアラートの送信元のメールアドレスを入力します。
7. [**SMTP** 認証を有効にする] を選択します。
8. 「ユーザー名」フィールドに、認証に使用する SMTP サーバーのユーザー名を入力します。
9. 「パスワード」フィールドに、認証に使用される SMTP サーバーのユーザー名に関連付けられているパスワードを入力します。

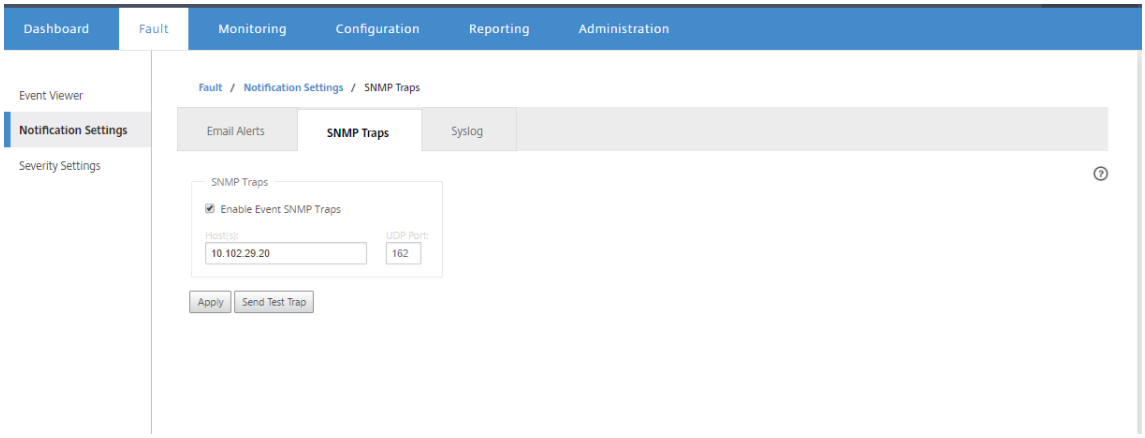
   > 注
   >
   > [テストメッセージの送信] を クリックして、サンプルの電子メールアラートを構成済みの受信者に送信します。

10. [**Apply**] をクリックします。

SNMP トラップ通知設定の構成

SNMP トラップ通知設定を構成するには:

1. Citrix SD-WAN Center の Web 管理インターフェイスで、[障害]> 通知設定 >**SNMP** トラップに移動します。
2. 「イベント **SNMP** トラップを有効にする」を選択します。



3. [**Host**（**s**）] フィールドに、外部 SNMP システムの IP アドレスまたはホスト名を入力します。このホストはイベントを SNMP トラップとして受信します。

> 注
>
> 複数の IP アドレスまたはホスト名をセミコロンで区切って入力できます。

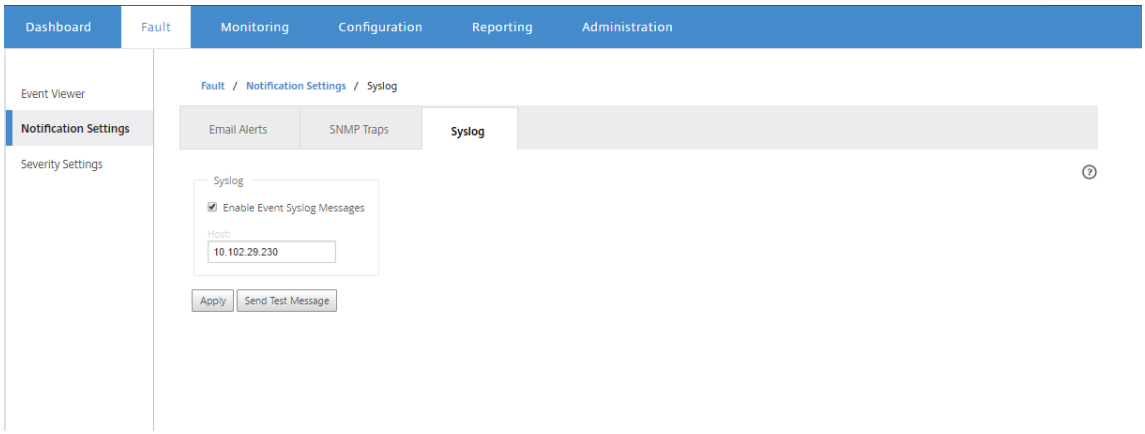
4. [**UDP** ポート] フィールドに、SNMP トラップの送信に使用する UDP ポートを入力します。デフォルトでは、UDP ポートは 162 に設定されています。
5. [適用] をクリックして、SNMP トラップ通知設定を適用します。

> 注
>
> または、[テストトラップの送信] をクリックして、システムが構成済みの宛先に SNMP トラップを送信できるかどうかを確認します。

Syslog 通知設定の構成

Syslog 通知設定を構成するには:

1. Citrix SD-WAN Center の Web 管理インターフェイスで、[障害]> 通知設定 >**Syslog** に移動します。
2. [イベント **Syslog** メッセージを有効にする] を選択します。



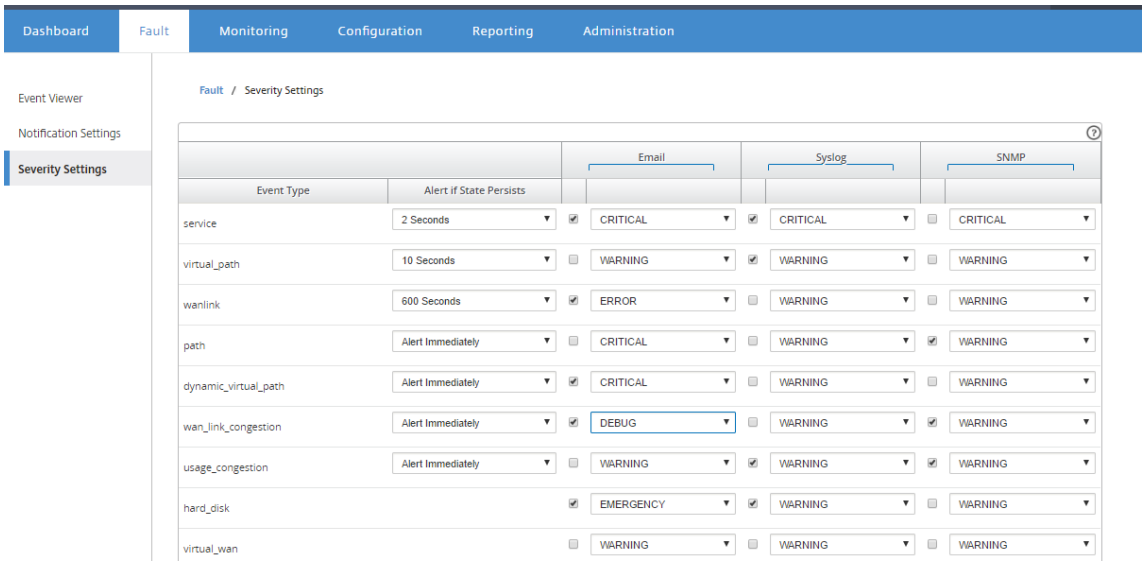
3. [ホスト] フィールドに、イベントを syslog メッセージとして受信するために使用される外部 syslog サーバーの IP アドレスまたはホスト名を入力します。
4. [適用] をクリックして、syslog 通知設定を適用します。

> 注
>
> または、「テストメッセージの送信」をクリックして、システムが構成済みのホストに syslog メッセージを送信できるかどうかを確認します。

イベント通知の構成

イベント通知を構成するには:

1. Citrix SD-WAN Center の Web 管理インターフェイスで、[障害] に移動します > 重要度の設定。
2. [状態が持続する 場合 のアラート] フィールドで、イベントがまだ持続する場合に通知が送信されるまでの期間を選択します。



3. イベントタイプごとに通知オプションを選択し、重大度を選択します。

> 注
>
> 電子メール、Syslog、SNMP 通知オプションは、それぞれの通知設定を構成した後にのみ有効になります。

4. [**Apply**] をクリックします。

アラームの設定

Citrix SD-WAN Center でアラームを設定して、個別のアプライアンスにプッシュすることもできます。

Citrix SD-WAN Center でアラームを設定するには、設定 > アプライアンスの設定 > 通知設定 > アラーム設定に移動し **+** をクリック。

次のフィールドの値を選択または入力します。

- イベントタイプ: Citrix SD-WAN アプライアンスは、ネットワーク内の特定のサブシステムまたはオブジェクトのアラームをトリガーできます。これらはイベントタイプと呼ばれます。使用可

能なイベントタイプは、SERVICE、VIRTUAL_PATH、WANLINK、PATH、DYNAMIC_VIRTUAL_PATH、WAN_LINK_CONGESTION、USAGE_CONGESTION、FAN、POWER_SUPPLY、PROXY_ARP、ETHERNET、DISCOVERED_MTU、GRE_TUNNEL、IPSEC_TUNNEL です。

- トリガー状態：イベントタイプのアラームをトリガーするイベント状態。使用可能なトリガー状態オプションは、選択したイベントタイプによって異なります。
- トリガー期間: 秒単位の期間。これにより、アプライアンスがアラームをトリガーする速度が決まります。即時アラートを受信するには「0」を入力するか、15～7200 秒の値を入力します。トリガー期間中に同じオブジェクトで追加のイベントが発生した場合、アラームはトリガーされません。追加のアラームは、イベントがトリガー期間よりも長く持続する場合にのみトリガーされます。
- **Clear State**：アラームがトリガーされた後に、イベントタイプのアラームをクリアするイベント状態。使用可能な Clear State オプションは、選択したトリガー状態によって異なります。
- クリア期間：秒単位の期間。これは、アラームをクリアするまでの待機時間を決定します。アラームをすぐにクリアするには「0」を入力するか、15～7200 秒の値を入力します。指定された時間内に同じオブジェクトで別のクリア状態イベントが発生した場合、アラームはクリアされません。
- 重症度: アラームの緊急度を決定するユーザー定義フィールド。重大度は、アラームがトリガーまたはクリアされたときに送信されるアラートと、トリガーされたアラームの概要に表示されます。
- **E** メール: イベントタイプのアラームトリガーとクリアアラートは電子メールで送信されます。
- **Syslog**: イベントタイプのアラームトリガーとクリアアラートは、Syslog を介して送信されます。
- **SNMP**: イベントタイプのアラームトリガーとクリアアラートは、SNMP トラップ経由で送信されます。

メモリダンプ

April 13, 2021

プロセスがクラッシュすると、メモリダンプが生成されます。現在システム上にあるすべてのメモリダンプを 1 つのパッケージにまとめてダウンロードし、Citrix サポートチームによる調査のために FTP サーバーにアップロードできます。ただし、個々のメモリダンプは削除できます。

メモリダンプをダウンロードするには：

1. Citrix SD-WAN Center の Web インターフェイスで、[監視] タブをクリックし、[診断] をクリックします。
2. [メモリダンプ] セクションの [メモリダンプパッケージ] ドロップダウンリストから、メモリダンプパッケージを選択します。

3. [すべてダウンロード] をクリックします。ローカルコンピューターにメモリダンプパッケージを保存します。

メモリダンプパッケージを FTP サーバーにアップロードするには:

1. [メモリダンプ] セクションの [メモリダンプパッケージ] ドロップダウンリストから、メモリダンプパッケージを選択します。
2. [**FTP** サーバーにアップロード] をクリックします。これにより、すべてを **FTP** にアップロード ダイアログボックスが開き、FTP 認証情報を指定して、パッケージを Citrix カスタマーサポートの FTP サーバーまたは別の FTP ホストにアップロードできます。

3. [顧客名] フィールドに、Citrix SD-WAN サポートが診断パッケージを識別するのに役立つ名前を入力します。

   この名前のディレクトリが Citrix FTP サーバー上に作成され、ファイルがその場所にアップロードされます。
4. 「**FTP** ホスト」フィールドに、FTP サーバーの IP アドレスまたはホスト名（DNS が構成されている場合）を入力します。
5. ユーザー名フィールド に、FTP サーバへのログインに使用するユーザー名を入力します。
6. 「パスワード」フィールドに、ユーザー名に関連付けられているパスワードを入力します。
7. ［アップロード］をクリックします。

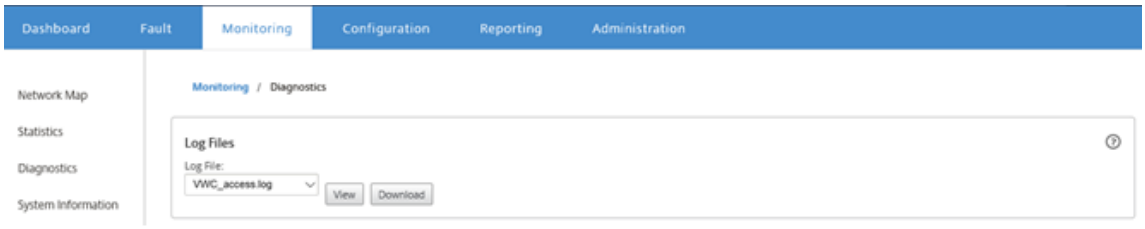
ログファイル

April 9, 2021

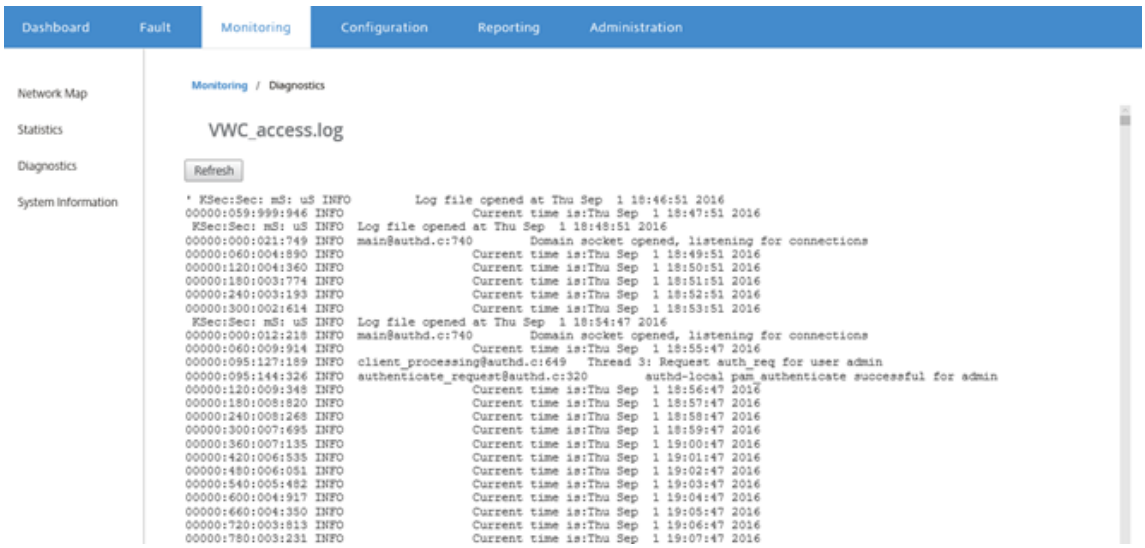
ログファイルは、Web コンソール、ユーザーインターフェイスの例外、内部クラッシュなどに関連する情報を収集します。これらのログは、Citrix SD-WAN Center の問題のトラブルシューティングに使用できます。

ログファイルを表示するには:

1. Citrix SD-WAN Center の Web インターフェイスで、[監視] タブをクリックします。
2. [診断] をクリックします。
3. [ログファイル] ドロップダウンリストから、表示するログファイルを選択します。



4. 表示をクリックします。ログファイルの内容が表示されます。



5. コンピュータにログファイルをダウンロードする場合は、[ダウンロード] をクリックします。

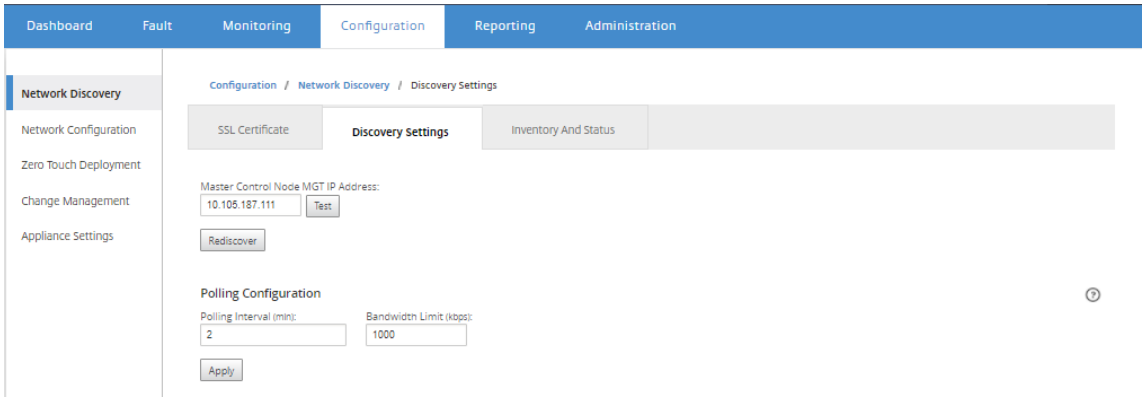
ポーリング間隔

April 13, 2021

ポーリングとは、検出されたアプライアンスから統計を収集するプロセスを指します。アプライアンスを検出した後、ポーリング操作の間隔と帯域幅制限を構成できます。アプライアンスの検出については、「単一リージョンネットワークの展開」または「マルチリージョンネットワークの導入」を参照してください。

ポーリング構成を実行するには:

1. Citrix SD-WAN Center の Web インターフェイスで、設定 > ネットワーク発見 > 検出設定に移動します。



2.「ポーリング間隔」フィールドに、ポーリング頻度を分単位で入力します。範囲は 2～60 分です。デフォルト値は 5 分です。

3. [帯域幅制限] フィールドに、ポーリング帯域幅制限を kbps で入力します。MCN は、アプライアンスから Citrix SD-WAN Center にポーリング統計を転送するときに、帯域幅を指定された値に制限します。範囲は 100 Kbp～1 Gbps です。デフォルト値は 1 Mbps です。

4. [**Apply**] をクリックします。

統計

April 13, 2021

Citrix SD-WAN Center によって収集された統計をグラフとして表示できます。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ているため、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。SD-WAN ネットワーク内のすべてのサイトについて、次のネットワークパラメータのグラフを表示できます。

- 帯域幅
- QoS
- 仮想パス
- インターネットサービス
- イントラネットサービス
- パススルーサービス
- WAN リンク
- イーサネットインターフェース
- GRE トンネル
- IPsec トンネル
- アプリケーション

- アプリケーションファミリ

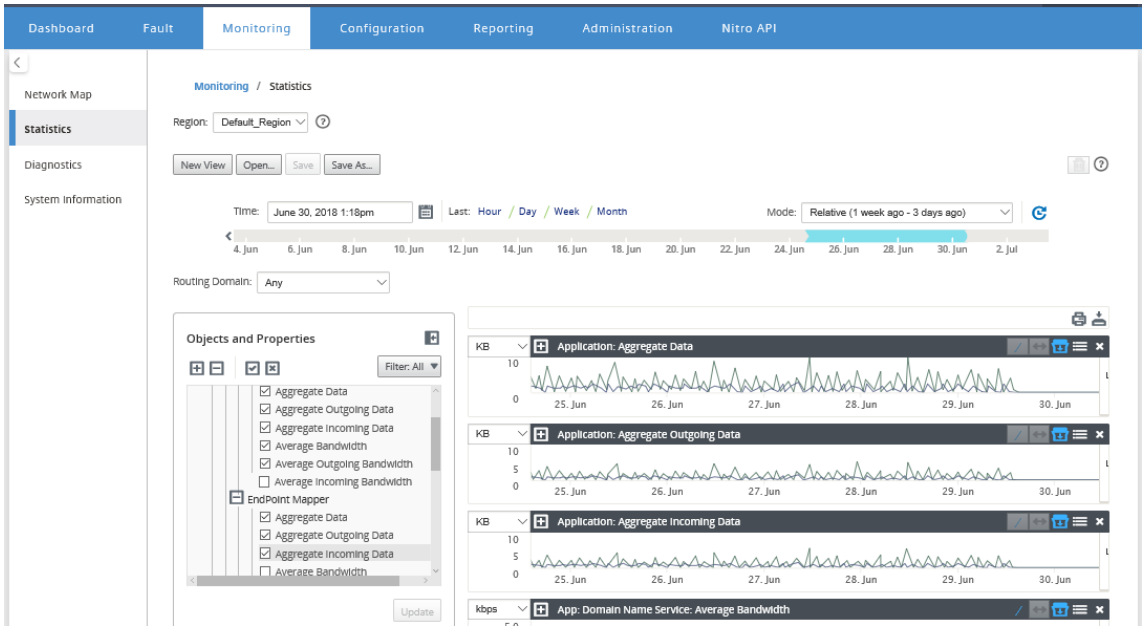
> ヒント
>
> 要件に従ってビューを作成し、保存して、既存のビューを開くことができます。

統計グラフを表示するには:

1. Citrix SD-WAN Center Web UI で、監視 > 統計に移動します。
2. リージョンとルーティングドメインを選択します。
3. オブジェクトとプロパティの 階層ツリーから、目的のプロパティを見つけて選択します。

   > ヒント
   >
   > [フィルター] ドロップダウンメニューと [プリセット] メニュー を使用して、プロパティの検索と選択のプロセスを簡略化することもできます。

4. [更新] をクリックして、選択したプロパティのグラフを表示します。

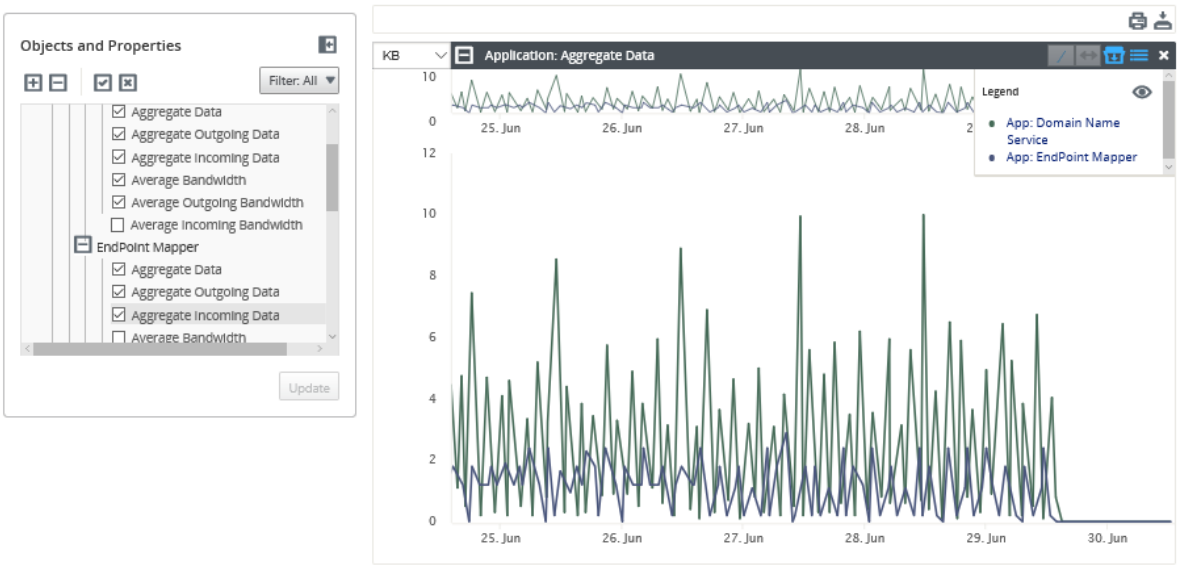


   > ヒント
   >
   > プロパティの選択を解除し、[更新] をクリックして、そのプロパティのグラフを [グラフの表示] 領域から削除します。

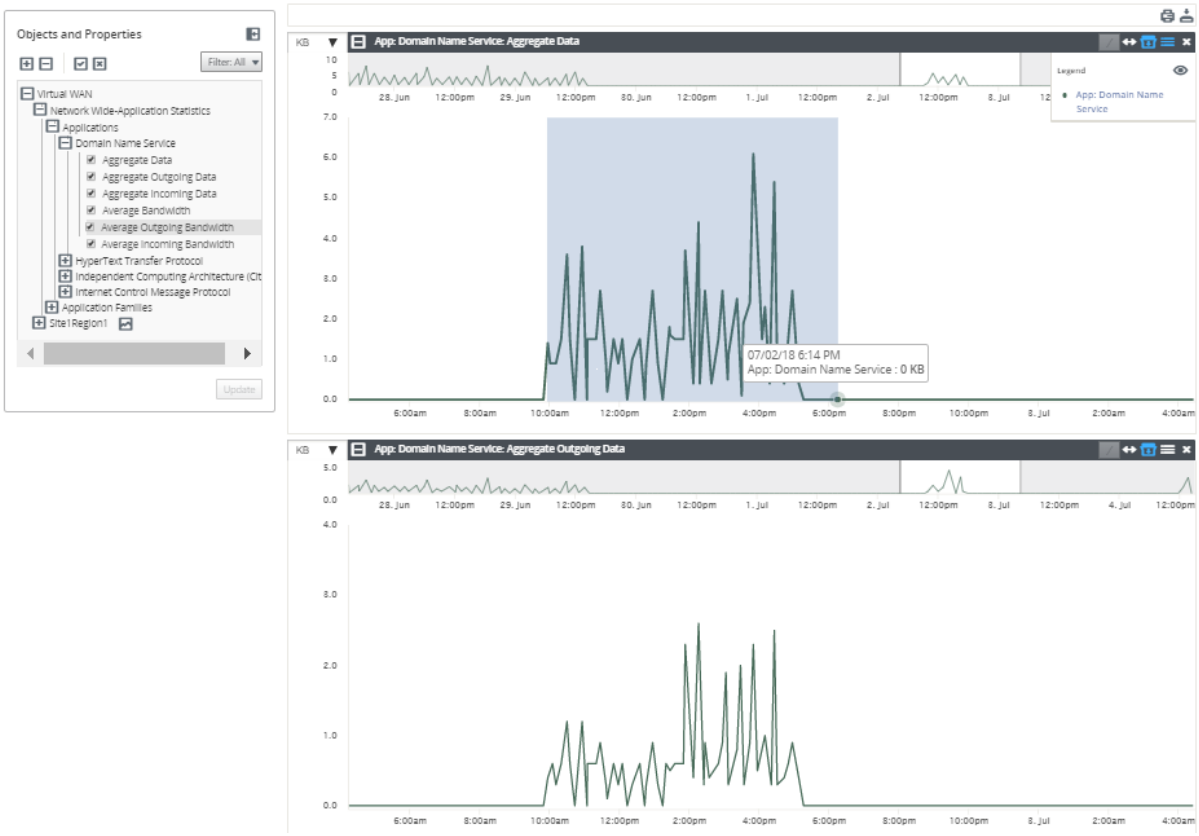
5. 現在のビューの期間を選択します。詳しくは、「タイムラインコントロール」を参照してください。

   グラフは、選択したプロパティに基づいて表示されます。

> ヒント
>
> 複数のプロパティを選択した場合、グラフは トレンドビュー モードで表示され、垂直方向のスペースを節約します。グラフの見出しをクリックして、完全に展開されたグラフの表示と非表示を切り替えます。グラフのトレンドビューと凡例を表示または非表示にすることもできます。

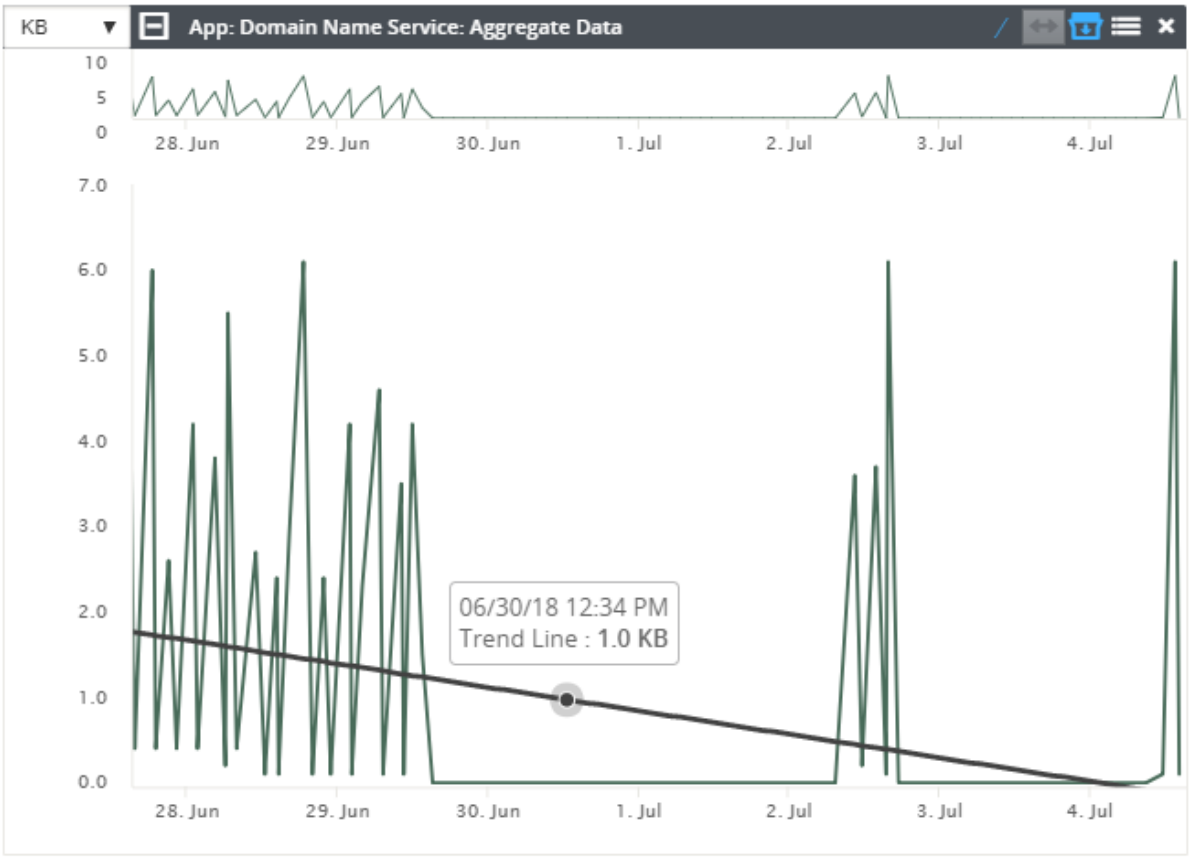


> ヒント
>
> グラフをズームするには、グラフのプロットエリアをクリックしてドラッグします。1 つのグラフをズームすると、すべてのグラフが選択した時間にズームされ、一貫したビューが維持されます。リセットアイコン（⇔）をクリックしてズームをリセットします。



ヒント

をクリックして、トレンドラインを表示または非表示にできます。(/) アイコン。



> 注
>
> グラフを印刷するか、グラフセットを CSV ファイルとしてダウンロードできます。

システム情報

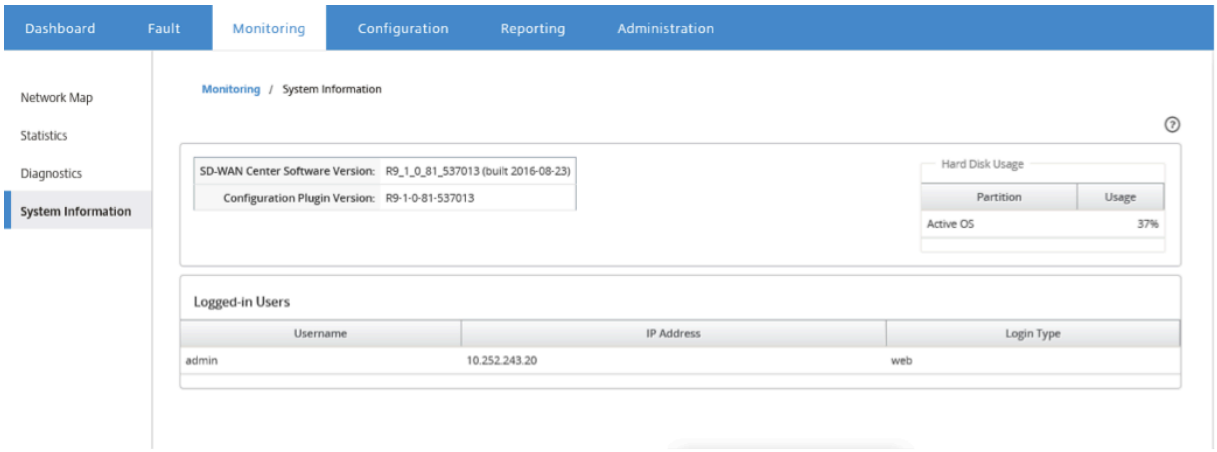
April 9, 2021

システム情報ページには、次の情報が表示されます。

- **Citrix SD-WAN Center** のソフトウェアバージョン: この仮想マシンに現在インストールされ、実行されている Citrix SD-WAN Center ソフトウェアのバージョン。
- 設定プラグインのバージョン: この Citrix SD-WAN Center 仮想マシンに現在インストールされ、実行されている構成エディタープラグインのバージョン。
- ハードディスクの使用: オペレーティングシステムとデータパーティションによって使用されるハードディスク領域の量。
- ログインしているユーザー: この Citrix SD-WAN Center 仮想マシンに現在ログインしている各ユーザーのユーザー名、IP アドレス、およびログオンタイプ。

システム情報を表示するには:

Citrix SD-WAN Center の Web インターフェイスで、[監視] タブをクリックし、[システム情報] をクリックします。



レポート

April 13, 2021

Citrix SD-WAN Center は、次のレポートを提供します。

- アプリケーション: 上位アプリケーション、サイト、およびアプリケーションファミリの着信トラフィック、発信トラフィック、および合計トラフィックに関する詳細を表示します。
- **HDX**: すべてのサイトの詳細な HDX データを表示します。
- サイト: 仮想 WAN 内のすべてのサイトのサイトレベルの統計を表示します。サイトの行が展開され、サイトでフィルタリングされた サービス テーブルが表示されます。
- サービス: 仮想 WAN 内のすべてのサイトのサービスタイプ（仮想パス、インターネット、イントラネット、パススルー）ごとに要約統計を表示します。サービスの行が展開され、サービスタイプの個々のサービスが表示されます。
- 仮想パス: SD-WAN 内のすべての仮想パスの仮想パスレベルの統計を表示します。仮想パスの行が展開され、仮想パス内に含まれるパスが表示されます。

> 注
>
> 仮想パスデータは両方のエンドポイントの観点から記録されるため、各仮想パスには、統計を記録したサイトによって識別される 2 つの行がある場合があります。

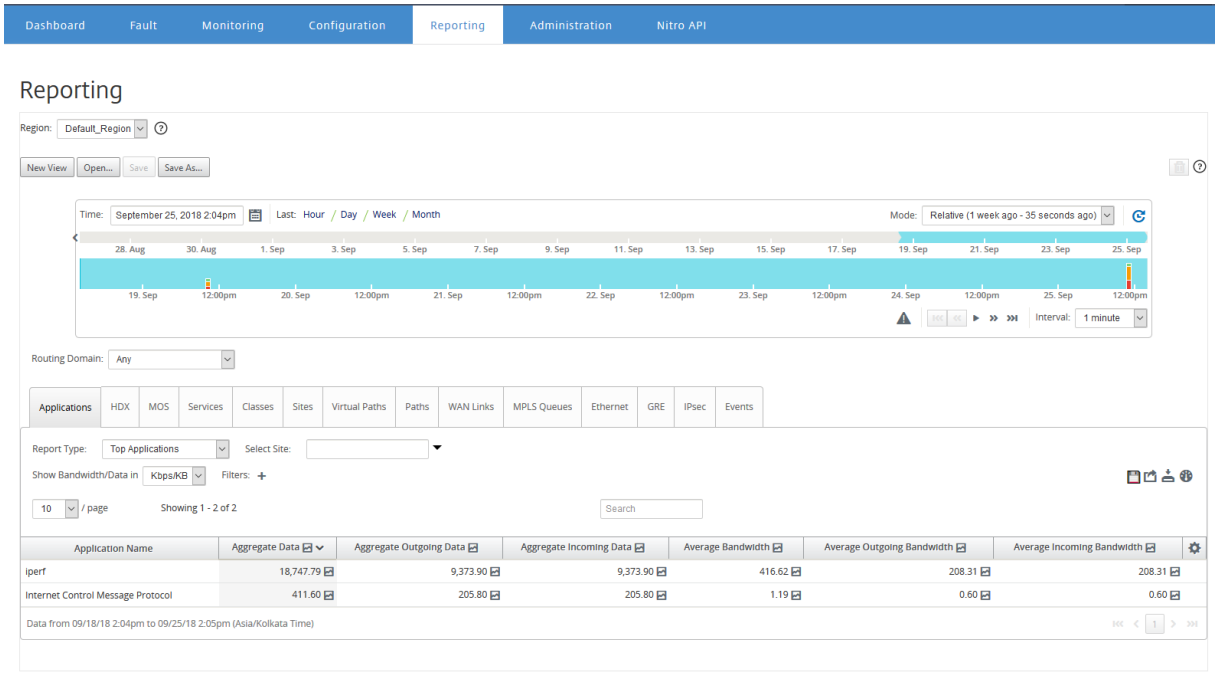
- パス: 仮想 WAN 内のすべてのパスのパスレベル統計を表示します。
- **WAN** リンク: 仮想 WAN の各サイトにあるすべての WAN リンクの WAN リンクレベル統計を表示します。WAN リンクの行が展開され、その WAN リンクの各サービスタイプの使用状況の概要が表示されます。次に、

各サービスタイプの行が展開され、そのタイプの各サービスの使用状況が表示されます。WAN リンクがプライベート MPLS リンクの場合、WAN リンクの MPLS キューを示す 2 番目のテーブルが表示されます。

- **MPLS** キュー： MPLS キューの行が展開され、そのキューの各サービスタイプの使用状況の概要が表示されます。次に、各サービスタイプの行が展開され、そのタイプの各サービスの使用状況が表示されます。
- クラス：仮想 WAN 内の各仮想パスのすべてのクラスのクラスレベル統計を表示します。
- **MOS** スコア: The 平均オピニオンスコア（MOS）は、アプリケーションがエンドユーザーに提供するエクスペリエンスの品質の数値測定を提供します。

- イーサネットインターフェイス：仮想 WAN 内の各サイトのすべてのインターフェイスのイーサネットインターフェイスレベルの統計情報を表示します。
- **GRE** トンネル： WAN の各サイトにあるすべての LAN GRE トンネルの統計を表示します。
- **IPsec** トンネル： WAN の各サイトにあるすべての IP セキュリティトンネルの統計を表示します。
- イベント：仮想 WAN の各サイトで発生するイベントの要約数を表示します。イベントの 行が展開され、そのサイトのオブジェクトタイプごとの集計カウントが表示されます。次に、各オブジェクトタイプが展開され、そのタイプの各オブジェクトの要約カウントが表示されます。

Citrix SD-WAN Center Web インターフェイスの [レポート] タブで、すべてのレポートまたは選択したレポートを表示できます。レポートをダウンロードすることもできます。

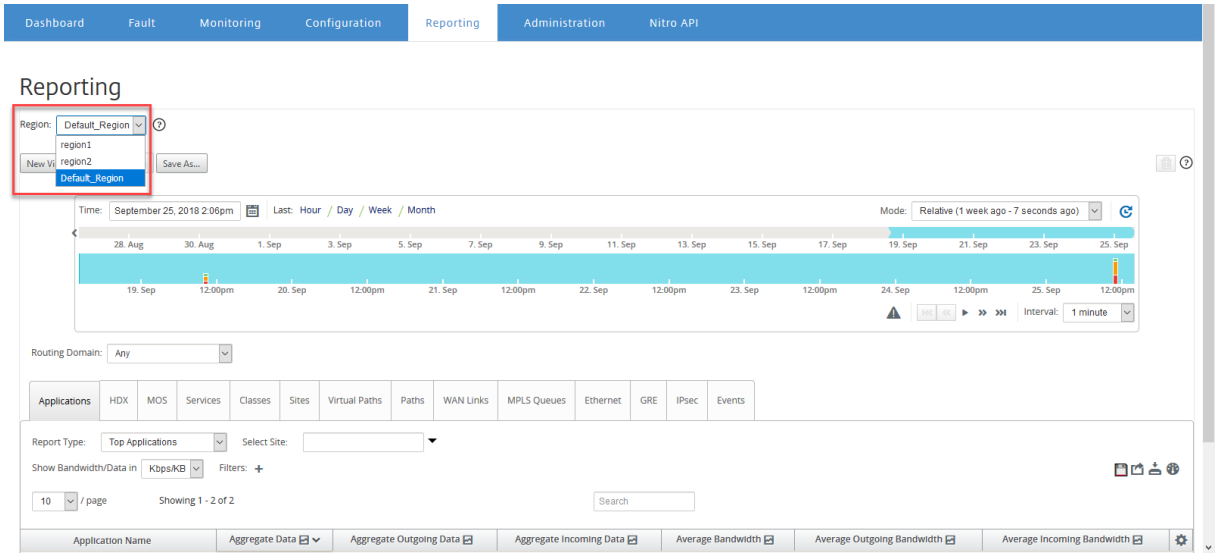


タイムラインコントロールを使用して、特定の時間枠のレポートを選択して表示できます。詳細については、「タイムラインコントロール」を参照してください。

レポートビューを作成、保存、開くこともできます。詳細については、「ビューを管理する」を参照してください。

マルチリージョンネットワークの場合、特定のリージョンを選択して統計レポートを表示できます。

レポートデータは、それぞれのリージョンのコレクターからフェッチされます。



> 注
>
> 単一リージョンネットワーク展開では、[リージョン] ドロップダウンリストは使用できません。

さまざまなレポートの表示の詳細については、以下のトピックを参照してください。

アプリケーションレポート

帯域幅レポート

クラスレポート

イーサネットインターフェイスレポート

イベントレポート

GRE トンネルレポート

HDX レポート

IPsec トンネルレポート

リンクパフォーマンスレポート

アプリケーションの MOS

MPLS キューレポート

アプリケーションレポート

April 13, 2021

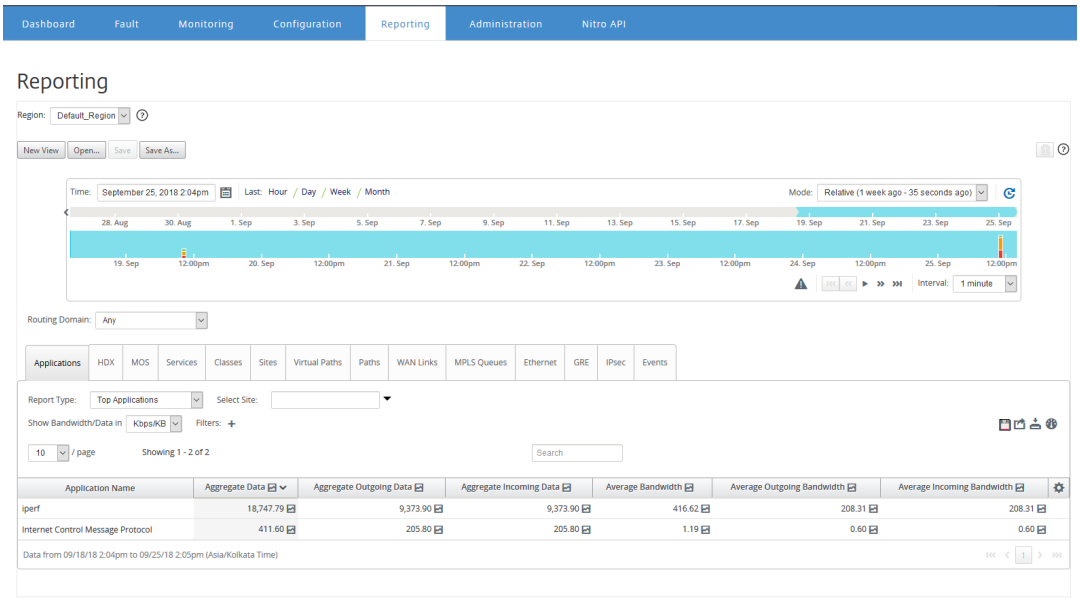
ディープパケットインスペクション（DPI）により、SD-WAN アプライアンスは通過するトラフィックを解析し、アプリケーションとアプリケーションファミリーのタイプを識別できます。Citrix SD-WAN アプライアンスは、すべてのアプリケーションの着信および発信トラフィックのバイト数と帯域幅を記録します。SD-WAN Center は、定義されたポーリング間隔で SD-WAN アプライアンスをポーリングし、このデータを取得して、ダッシュボードおよびレポートとして表示します。

上位のアプリケーション、上位のサイト、および上位のアプリケーションファミリレポートを表示できます。これらのレポートは、合計、着信、発信のデータと帯域幅に関する詳細を提供します。

Citrix SD-WAN Center でアプリケーションレポートを表示するには:

1. Citrix SD-WAN Center Web UI で、レポート > アプリケーションに移動します。
2. タイムラインコントロールで、時間間隔を選択します。詳しくは、「タイムラインコントロール」を参照してください。
3. データを表示する単位を選択します。レポートデータの表示は、Kbps、Mbps、または Gbps の単位で選択できます。
4. [レポートタイプ] ドロップダウンリストから、次のレポートタイプのいずれかを選択します。

    - 上位のアプリケーション: 選択した時間間隔でネットワークで使用された上位のアプリケーション。上位のアプリケーションをサイト名でフィルタリングできます。デフォルトでは、すべてのサイトの上位アプリケーションが表示されます。
    - トップアプリケーションファミリ: ネットワークで使用されている上位のアプリケーションファミリ。上位のアプリケーションファミリをサイト名でフィルタリングできます。デフォルトでは、すべてのサイトのトップアプリケーションファミリが表示されます。
    - トップサイト: 選択した期間の上位サイトのトラフィック。トップサイトをアプリケーションまたはアプリケーションファミリ名でフィルタリングできます。



レポートタイプごとに、次のデータを表示できます。

- 集約された受信データ: WAN からサイトに着信するアプリケーションデータ。
- 集計された送信データ: サイトから WAN に送信されるアプリケーションデータ。
- 集計データ: Sum 着信および発信トラフィックの。
- 平均着信帯域幅: 着信アプリケーショントラフィックの帯域幅。
- 平均送信帯域幅: 発信アプリケーショントラフィックの帯域幅。
- 平均帯域幅: 着信および発信アプリケーショントラフィックによって消費される合計帯域幅。

> ヒント
>
> すべての値について、グラフアイコンの上にマウスカーソルを合わせるとミニグラフが表示され、クリックすると別のウィンドウでグラフビューが開きます。詳しくは、「統計」を参照してください。

アプリケーション **QoE** レポート

April 13, 2021

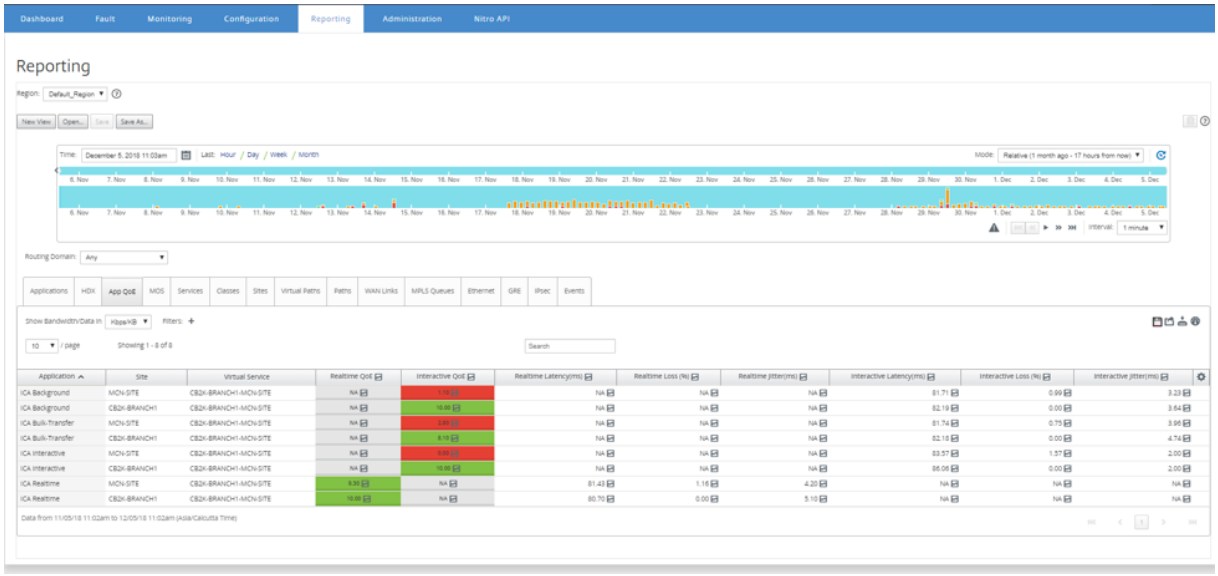
アプリケーション **QoE** は、アプリケーションのエクスペリエンス品質の尺度です。Application QoE スコアの範囲は 0〜10 です。10 は優れた品質を表し、0 は低品質を表します。詳細については、「アプリケーションの **QoE**」セクションを参照してください。

アプリケーション QoE レポートを表示するには:

Citrix SD-WAN Center で、レポート **>** アプリの **QoE** に移動し、タイムラインコントロールで期間を選択します。

タイムラインコントロールを使用して、特定の期間のレポートを選択して表示できます。詳細については、「タイムラインコントロール」を参照してください。

レポートビューを作成、保存、および開くこともできます。詳細については、「ビューを管理する」を参照してください。



次のメトリックを表示できます。

- 応用: 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名。
- 地点: サイトの名前。
- 仮想サービス: 使用される仮想パスサービス。
- リアルタイム **QoE**: リアルタイムトラフィックの QoE スコア。
- インタラクティブ **QoE**: インタラクティブトラフィックの QoE スコア。
- リアルタイムレイテンシ: リアルタイムトラフィックのミリ秒単位の遅延。
- リアルタイムの損失: リアルタイムトラフィックの損失率。
- リアルタイムジッター: リアルタイムトラフィックのミリ秒単位で観測されたジッター。
- インタラクティブな遅延: インタラクティブトラフィックのレイテンシ（ミリ秒）。
- インタラクティブな損失: インタラクティブトラフィックの損失率。
- インタラクティブジッタ: インタラクティブトラフィックのミリ秒単位で観察されたジッター。

> ヒント
>
> すべての値について、グラフアイコンの上にマウスカーソルを合わせるとミニグラフが表示され、クリックすると別のウィンドウでグラフビューが開きます。

詳しくは、「統計」を参照してください。

帯域幅レポート

April 13, 2021

Citrix SD-WAN Center は、SD-WAN ネットワークのさまざまなサイトからポーリングされた帯域幅統計データの中央ビューを提供します。

Citrix SD-WAN 構成では、仮想パスを通過するトラフィックは、リアルタイム、インタラクティブ、またはバルククラスタイプに属するものとして分類されます。クラスは事前定義されていますが、これらのクラスをカスタマイズしてルールを適用できます。詳しくは、「Classe のカスタマイズ」および「IP アドレスとポート番号によるルール」を参照してください。

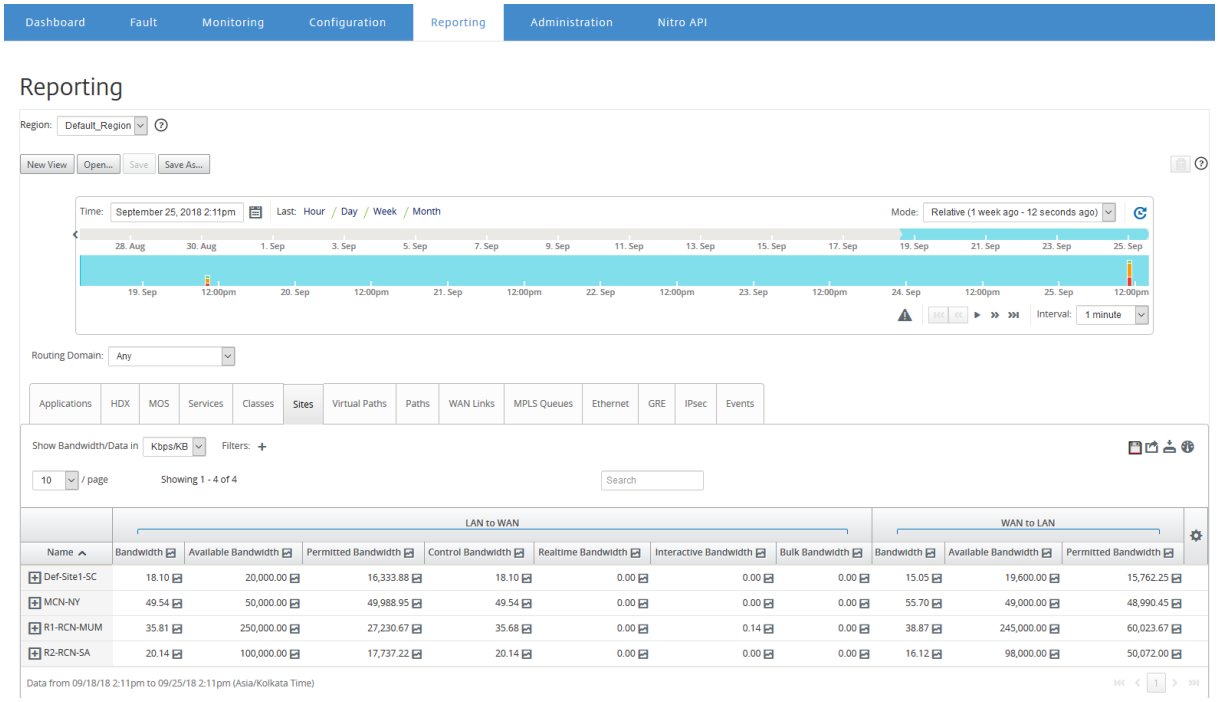
Citrix SD-WAN Center を使用すると、基本的な帯域幅統計とともに、各サイト、パス、または WAN リンクレベルでこれらのクラスタイプに属するアプリケーションによって消費される帯域幅を表示できます。

帯域幅統計を表示するには:

Citrix SD-WAN Center で、レポート に移動します > サイト、およびタイムラインコントロールで期間を選択します。

タイムラインコントロールを使用して、特定の時間枠のレポートを選択して表示できます。詳細については、「タイムラインコントロール」を参照してください。

レポートビューを作成、保存、開くこともできます。詳細については、「ビューを管理する」を参照してください。



次のメトリックを表示できます。

- 帯域幅: すべてのパケットタイプによって消費される合計帯域幅。帯域幅 = 帯域幅の制御 + リアルタイム帯域幅 + インタラクティブな帯域幅 + バルク帯域幅。たとえば、上記のスクリーンショットの SITE2 の帯域幅 = 1120.99+166.61+117.21+810.78+26.40
- 利用可能な帯域幅: サイトのすべての WAN リンクに割り当てられる合計帯域幅。

- 帯域幅の制御: 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。
- 許容帯域幅: 情報の送信に使用できる帯域幅。
- リアルタイム帯域幅: Citrix 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）。
- インタラクティブな帯域幅: Citrix 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: Citrix 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、ほとんど人間の介入を必要とせず、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。

クラスレポート

April 13, 2021

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、さまざまな帯域幅制限をさまざまなクラスに適用できます。クラスは、次の 3 つの基本タイプのいずれかになります。

- リアルタイムクラス: 特定の帯域幅制限までの迅速なサービスを要求するトラフィックフローを処理します。総スループットよりも低レイテンシが推奨されます。
- インタラクティブなクラス: 損失と遅延の影響を受けやすいトラフィックフローを提供します。インタラクティブクラスは、リアルタイムよりも優先度は低くなりますが、バルクトラフィックよりも絶対的に優先されます。
- 一括クラス: 高帯域幅を必要とし、損失の影響を受けやすいトラフィックフローを提供します。バルククラスの優先度は最も低くなります。

クラスごとに異なる帯域幅要件を指定すると、仮想パススケジューラが、同じタイプの複数のクラスからの競合する帯域幅要求を調停できます。スケジューラーは、階層的公平サービス曲線（HFSC）アルゴリズムを使用して、クラス間の公平性を実現します。

カスタムモニタの作成の詳細については、「クラスのカスタマイズ」を参照してください。

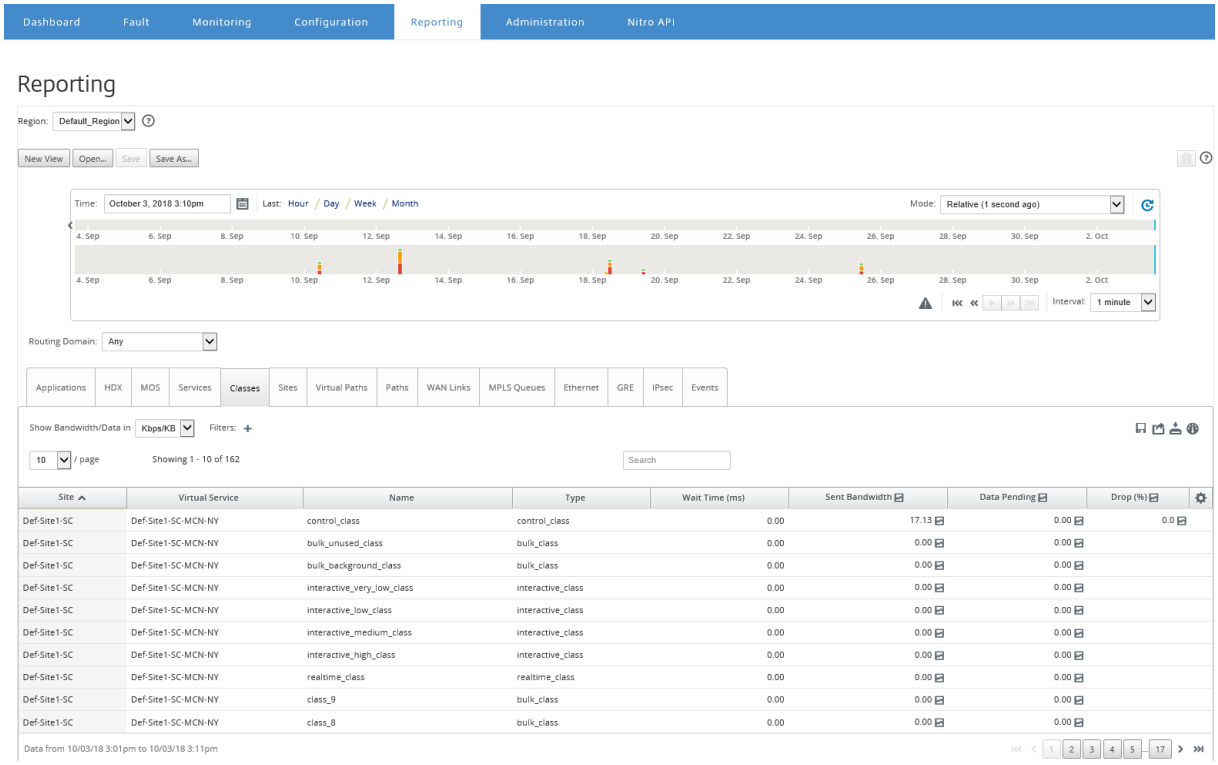
クラス統計を表示するには:

Citrix SD-WAN Center で、レポート > クラス に移動し、およびタイムラインコントロールで期間を選択します。

タイムラインコントロールを使用して、特定の期間のレポートを選択して表示できます。詳細については、「タイムラインコントロール」を参照してください。

> 注
>
> 過去 30 日間のクラスデータを表示できます。この期間を過ぎたデータは、SD-WAN Center コレクターとそれぞれのリージョナルコレクターから自動的に削除されます。

レポートビューを作成、保存、開くこともできます。詳細については、「ビューを管理する」を参照してください。



次のメトリックを表示できます。

- 名前: クラス名
- タイプ: クラスタイプ。Releatime、インタラクティブ、または一括。
- 待ち時間: パケットの送信間隔（ミリ秒）。
- 送信された帯域幅: 送信帯域幅
- 送信されたデータ: 送信されたデータ（Kbps）。
- 送信されたパケット: 送信されたパケットの数。
- データ保留中: 送信するデータ（Kbps）。
- 保留中のパケット: 送信するパケットの数。
- ドロップ: 削除されたデータの割合。
- ドロップされたデータ: ドロップされたデータ（Kbps）。
- ドロップされたパケット: ネットワークの輻輳のためにドロップされたパケットの数。
- データカバレッジ: データが利用可能な選択された期間の割合。

> 注
>
> 設定アイコンをクリックして、表示するメトリックを選択します。

イーサネットインターフェイスレポート

April 13, 2021

Citrix SD-WAN Center は、SD-WAN ネットワーク上のさまざまな Citrix SD-WAN アプライアンス上のすべてのイーサネットインターフェイスを一元的に表示します。これは、トラブルシューティング中に、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、各ポートで送受信された帯域幅、またはパケットの詳細を表示することもできます。特定の期間中にこれらのインターフェースで発生したエラーの数を表示することもできます。

イーサネットインターフェイスは、SD-WAN ネットワークのセットアップ中に各 Citrix SD-WAN アプライアンスで設定されます。

MCN サイトのインターフェイスグループの構成については、「MCN を構成する」を参照してください。

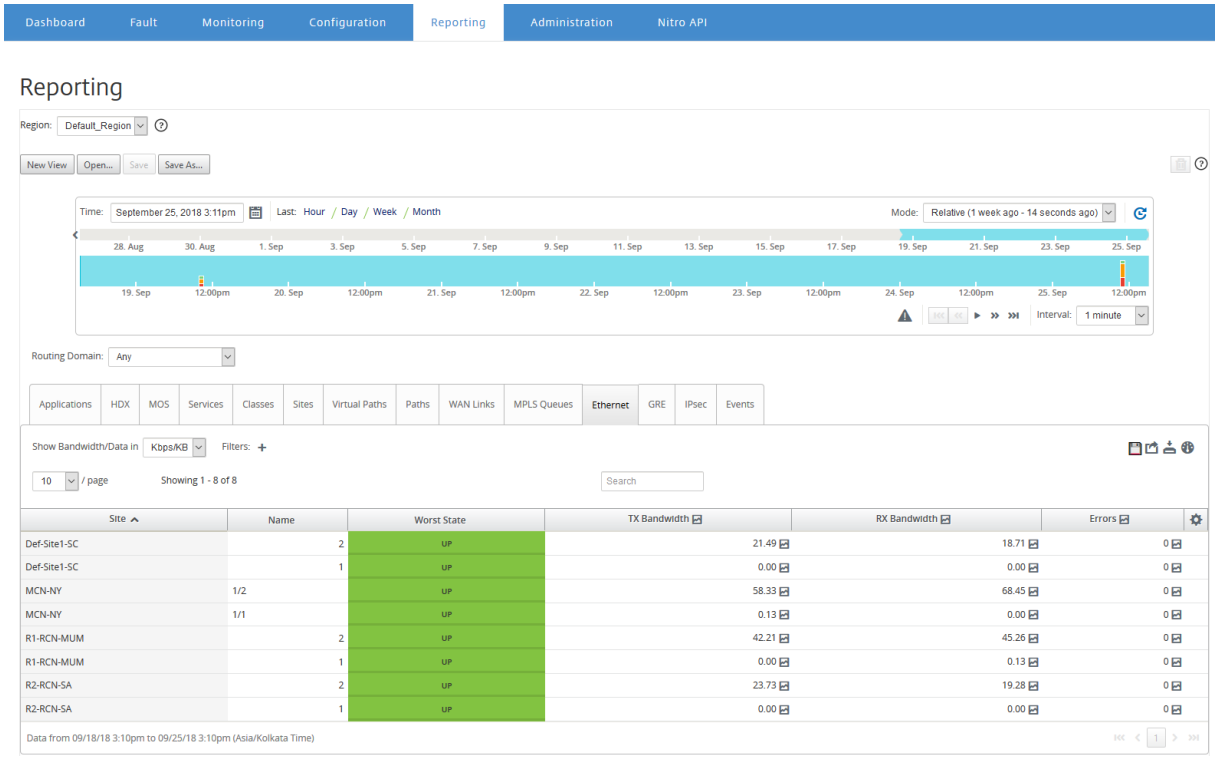
Web Interface サイトの構成については、「ブランチノードの構成」を参照してください。

イーサネットインターフェイスの統計情報を表示するには:

Citrix SD-WAN Center で、レポート > イーサネットに移動し、およびタイムラインコントロールで期間を選択します。

タイムラインコントロールを使用して、特定の時間枠のレポートを選択して表示できます。詳細については、「タイムラインコントロール」を参照してください。

レポートビューを作成、保存、開くこともできます。詳細については、「ビューを管理する」を参照してください。



次のメトリックを表示できます。

- 名前: イーサネットインターフェイスの名前。
- 最悪の状態: 選択した期間中に観測された最悪の状態。
- **TX** 帯域幅: 送信される帯域幅。
- **RX** 帯域幅: 受信した帯域幅。
- **TX** パケット: 送信されたパケットの数。
- **RX** パケット: 受信したパケットの数。
- エラー: 選択した期間中に観察されたエラーの数。
- データカバレッジ: データが利用可能な、選択した期間の割合。

> 注
>
> 設定アイコンをクリックして、表示するメトリックを選択します。

イベントレポート

April 13, 2021

SD-WAN ネットワークの各サイトで発生するさまざまなイベントの数を表示できます。

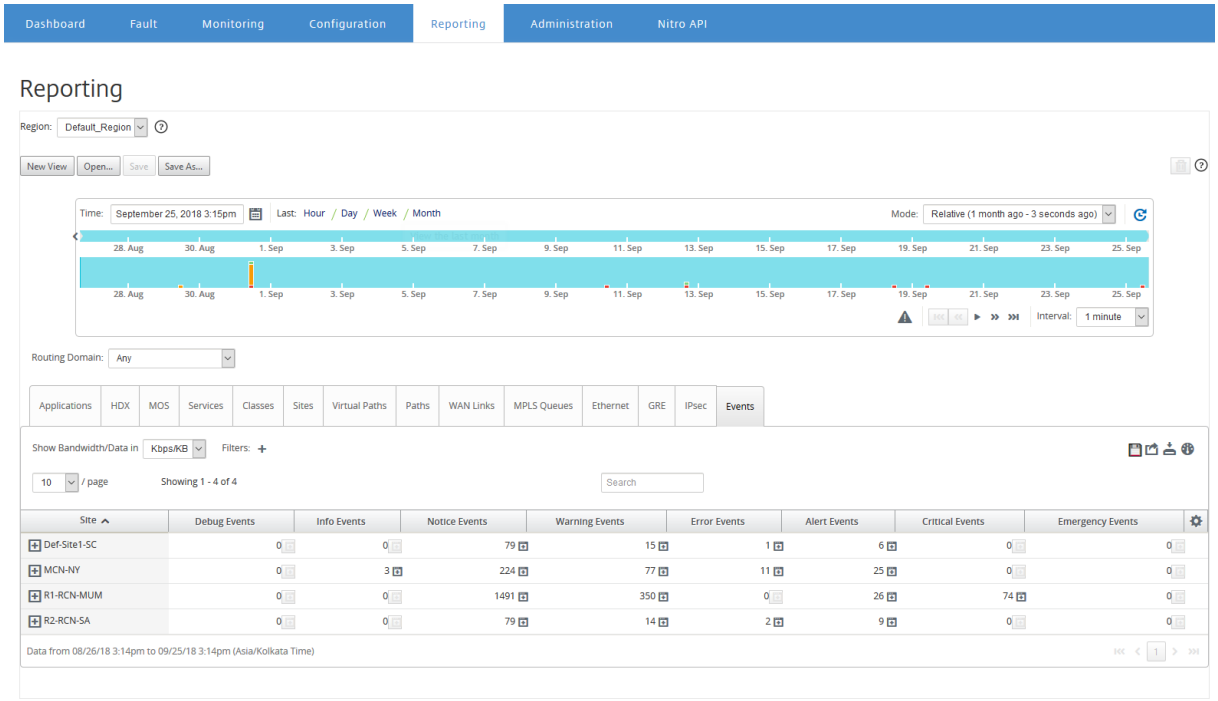
イベント統計の詳細については、「イベント」を参照してください。

イベント統計を表示するには:

Citrix SD-WAN Center で、レポート > イベントに移動し、およびタイムラインコントロールで期間を選択します。

タイムラインコントロールを使用して、特定の時間枠のレポートを選択して表示できます。詳細については、「タイムラインコントロール」を参照してください。

レポートビューを作成、保存、開くこともできます。詳細については、「ビューを管理する」を参照してください。



次のメトリックを表示できます。

- 情報イベント: 選択した期間中に発生した情報イベントの数。これらは低レベルのイベントです。
- お知らせイベント: 選択した期間中に発生した通知イベントの数。これらは、管理者が知っておくべきイベントです。
- 警告イベント: 選択した期間中に発生した警告イベントの数。これらは、近い将来の対応が必要なイベントです。
- エラーイベント: 選択した期間中に発生したエラーイベントの数。これらは、ある種のエラーを示すイベントです。
- アラートイベント: 選択した期間中に発生したアラートイベントの数。これらは、アクションを必要とする可能性があるイベントです。
- 重要なイベント: 選択した期間中に発生した重大なイベントの数。これらは差し迫った危機を示すイベントです。
- 緊急イベント: 選択した期間中に発生した緊急イベントの数。これらは、緊急の危機を示すイベントです（たとえば、電源の障害、ファンの障害、ハードディスクのしきい値の超過、サービスの無効化など）。
- デバッグイベント: 選択した期間中に発生したデバッグイベントの数。Citrix SD-WAN アプライアンスでテス

トメールまたはテスト Syslog オプションを使用すると、デバッグイベントが生成されます。

> 注
>
> 設定アイコンをクリックして、表示するメトリックを選択します。

次の表に、イベントが報告されるオブジェクトの状態変化の例をいくつか示します。

Event	Object Type	Previous State	Current State
NOTICE	LAN to WAN path	BAD	GOOD
		GOOD	BAD
	WAN to LAN path	BAD	GOOD
		GOOD	BAD
	Dynamic virtual path	BAD	GOOD
		GOOD	BAD
WARNING	Virtual path	GOOD	BAD
	WAN link congestion	UNCONGESTED	CONGESTED
		CONGESTED	UNCONGESTED
	Usage congestion	UNCONGESTED	CONGESTED
		CONGESTED	UNCONGESTED
	LAN to WAN path	GOOD	DEAD
		BAD	DEAD
	WAN to LAN path	GOOD	DEAD
		BAD	DEAD
ALERT	Virtual path	BAD	DEAD
		DEAD	BAD
ERROR	WAN-link	GOOD	DEAD
	Ethernet	GOOD	UNDEFINED
		UNDEFINED	DEAD
INFO	Proxy-arp	UNDEFINED	ACTIVE
		UNDEFINED	STANDBY

さまざまなイベントタイプの外部イベント通知を電子メール、SNMP トラップ、または syslog メッセージとして送信するように Citrix SD-WAN Center を構成できます。詳しくは、「イベント通知」を参照してください。

GRE トンネルレポート

February 18, 2022

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 トンネルの構成の詳細については、「GRE トンネル」を参照してください。

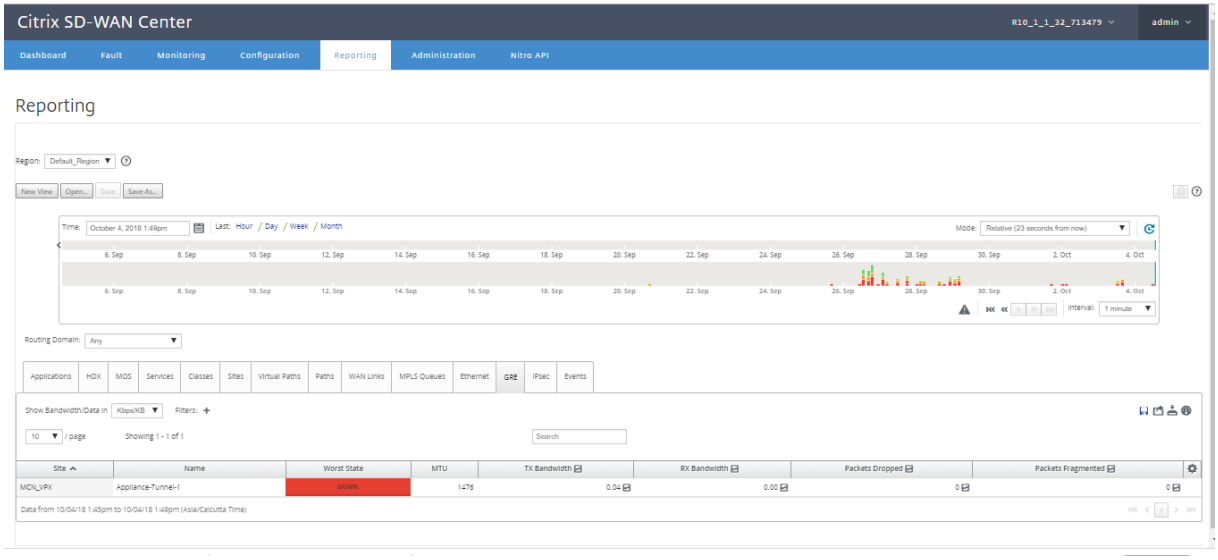
Citrix SD-WAN Center では、Citrix SD-WAN ネットワークで構成されているすべての GRE トンネルの状態を表示できます。

GRE トンネル統計を表示するには:

Citrix SD-WAN Center で、レポート > **GRE** に移動し、およびタイムラインコントロールで期間を選択します。

タイムラインコントロールを使用して、特定の時間枠のレポートを選択して表示できます。詳細については、「タイムラインコントロール」を参照してください。

レポートビューを作成、保存、開くこともできます。詳細については、「ビューを管理する」を参照してください。



次のメトリックを表示できます。

- 最悪の状態: 選択した期間中に観測された最悪の状態。
- **MTU**: 最大転送単位—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。
- **TX** 帯域幅: 送信される帯域幅。
- **RX** 帯域幅: 受信した帯域幅。
- **TX** パケット: 送信されたパケットの数。
- **RX** パケット: 受信したパケットの数。
- ドロップされたパケット: ネットワークの輻輳のためにドロップされたパケットの数。

- 断片化されたパケット: 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。
- データカバレッジ: データが利用可能な、選択した期間の割合。

> 注
>
> 設定アイコンをクリックして、表示するメトリックを選択します。

HDX レポート

April 13, 2021

ドロップダウンリストから次のレポートタイプのいずれかを選択します。

- HDX サイト統計
- HDX サマリー（利用可能なセッションと利用できない HDX 情報チャネルの両方に適用可能）
- HDX ユーザーセッション（HDX 情報チャネルで利用可能なセッションのみに適用）
- HDX アプリ（HDX 情報チャネルで利用可能なセッションのみに適用）

HDX サイト統計

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。各サイトのデータは 2 つのビューで表示されます。

[**Summary**] ビュー

概要ビューには、サイトの次のデータが表示されます。

- **QoE** インデックス -エクスペリエンスの品質（QoE）は 0〜100 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。
- ユーザー–サイトのアクティブユーザーの数。
- **TCP** フロー -TCP プロトコルを使用するサイト上のアクティブな HDX セッションの数。
- **UDP** フロー–UDP プロトコルを使用するサイト上のアクティブな HDX セッションの数。
- セッション–小規模統合（SSI）と中規模統合（MSI）の両方のセッションを含む、サイト上のアクティブな HDX セッションの総数。

詳細図

個々のサイトをクリックして、QoE に影響するすべての変数の詳細を表示できます。行の各ペアは、特定の仮想パスのローカル側とリモート側で計算されたデータの QoE 係数を示します。

QoE に影響する遅延、ジッター、およびパケットドロップ変数は、Citrix SD-WAN アプライアンスが測定している有効な数値です。たとえば、ネットワーク内のパケットドロップの割合が大きくなる可能性があります。CitrixSD-WAN が独自のプロトコルを介してパケットドロップを修正するため、アプリケーションで見られる効果的なパケット損失ははるかに少なくなり、HDX アプリケーションの QoE が向上します。

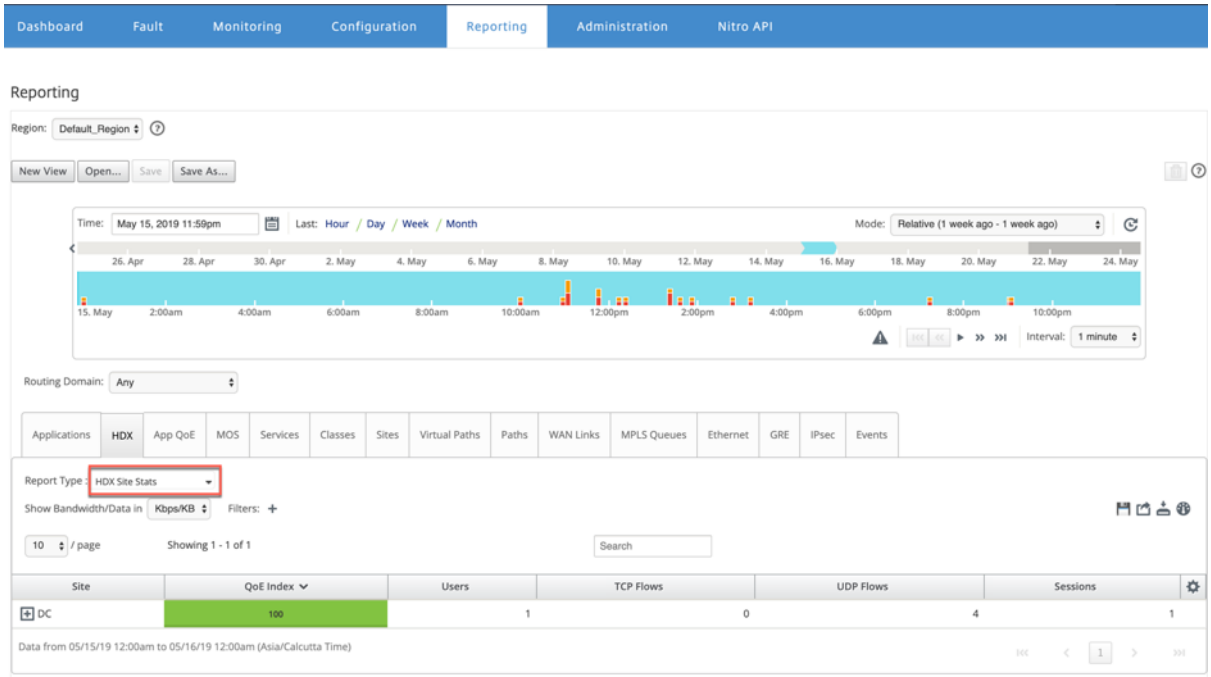
同様に、パケットの複製による遅延の改善により、HDX アプリケーションの QoE も改善されます。つまり、Citrix SD-WAN は、QoE に影響する要素を改善することにより、HDX トラフィックの QoE を改善します。詳しくは、「HDX QoE」を参照してください。

HDX レポートを表示するには:

Citrix SD-WAN Center で、レポート > **HDX** に移動し、およびタイムラインコントロールで期間を選択します。

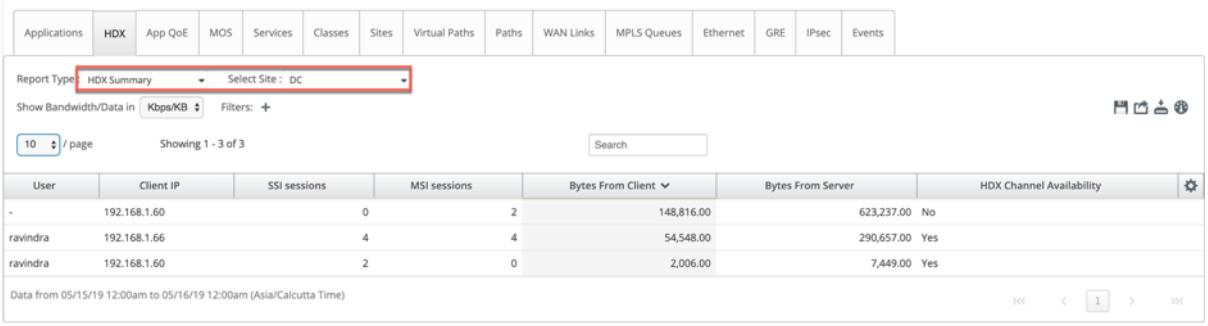
タイムラインコントロールを使用して、特定の時間枠のレポートを選択して表示できます。詳細については、「タイムラインコントロール」を参照してください。

レポートビューを作成、保存、および開くこともできます。詳細については、「ビューを管理する」を参照してください。



HDX の概要

ドロップダウンリストから **HDX** サマリー レポートとサイトを選択します。HDX サマリーレポートには、選択した期間中にログインした各ユーザーのレポートが表示されます。

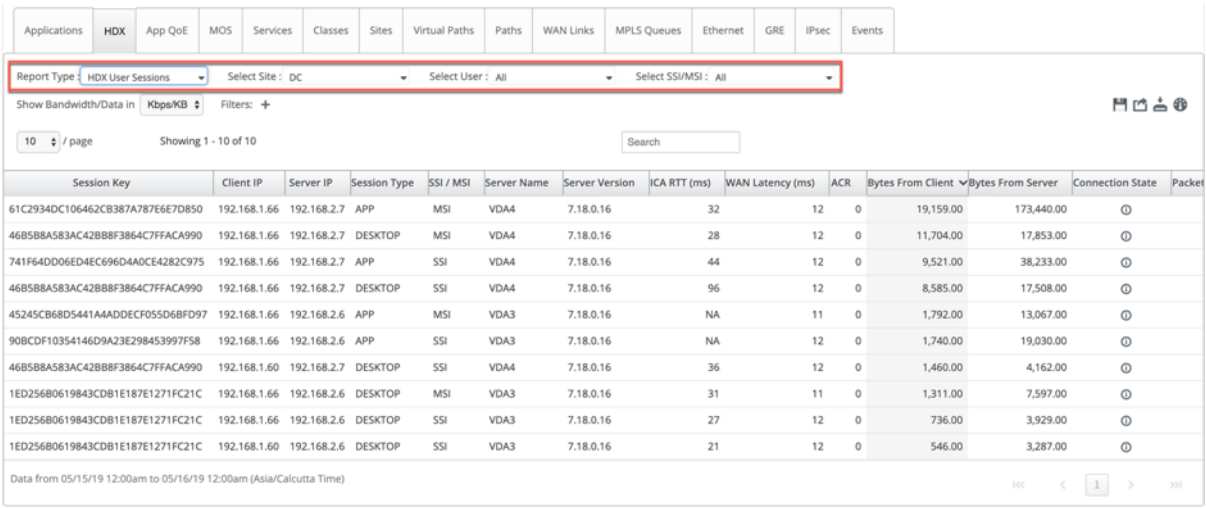


HDX 要約レポートでは、以下のパラメーターを表示できます。

- ユーザー: ユーザーの名前。
- クライアント **IP**: クライアントの IP アドレス。
- **SSI** セッション: アクティブなシングルストリーム ICA（SSI）セッションの数。
- **MSI** セッション: アクティブなマルチストリーム ICA（MSI）セッションの数。
- クライアントからのバイト: クライアントからのバイト単位のサイズ。
- サーバーからのバイト数: サーバーからのバイト単位のサイズ。
- **HDX** チャネルの可用性: HDX 情報チャネルの可用性ステータスを提供します Yes/No 。** チャネルが利用できない場合、ユーザー名はハイフン（-）として表示されます。

HDX ユーザーセッション

HDX ユーザーセッションレポートでは、各ユーザーが使用するすべてのセッションの詳細を確認できます。ドロップダウンリストからサイト、ユーザー、SSI または MSI を選択します。デフォルトでは、ユーザー の選択と 選択 SSI/MSI フィールドには **ALL** と表示されます。



検索を使用するか、Filter:+ 要件に応じて必要なセッション情報を見つけるオプション。**

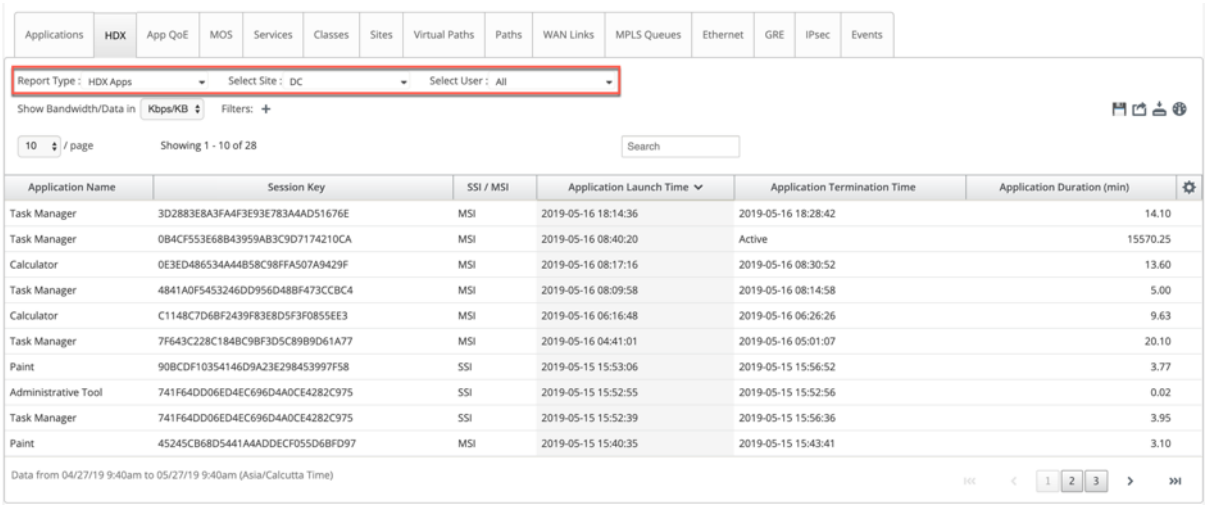
- セッションキー: セッションキーは、ICA セッションの一意の ID を表します。
- クライアント **IP**: 各セッションのクライアント IP アドレス。

- サーバー **IP**: 各セッションのサーバー IP アドレス。
- セッションタイプ: セッションのタイプ（デスクトップ、アプリ）。
- SSI/MSI : SSI セッションか MSI セッションかを示します。**
- サーバー名: サーバーの名前を表示します。
- サーバーのバージョン: サーバーのバージョンを表示します。
- **ICA RTT**（ミリ秒）: ICA ラウンドトリップ時間（RTT）をミリ秒単位で表示します。これは、クライアントとサーバー間のエンドツーエンドの往復時間です。
- **WAN** レイテンシ: WAN を介した遅延、つまり仮想パスを介した 2 つの SD-WAN 間の遅延。この待ち時間には、クライアント側またはサーバー側のネットワーク待ち時間は含まれません。
- **ACR**: 自動クライアント再接続カウントを表示します。
- クライアントからのバイト: クライアントからのバイト単位のサイズ。
- サーバーからのバイト数: サーバーからのバイト単位のサイズ。
- 接続状態: マウスをポイントすると、接続状態が表示されます。
  - MSI の場合、4 つの接続があります。これらの接続は L4 レベルです (TCP/UDP 状態)。
  - SSI の場合、接続は 1 つだけです。

- クライアントからのパケット: クライアントからのパケット数。
- サーバーからのパケット: サーバーからのパケット数。

HDX アプリ

特定のユーザーまたはすべてのユーザーが使用しているすべてのアプリケーションを表示できます。サイト と ユーザー を選択して、アプリケーションの詳細を表示します。



- アプリケーション名: HDX アプリケーションの名前を提供します。
- セッションキー: 特定のアプリケーションに使用される一意のセッションキーを提供します。
- SSI/MSI : SSI セッションか MSI セッションかを示します。**
- アプリケーションの起動時間: アプリケーションの起動時間と日付を提供します。
- アプリケーション終了時間: アプリケーションの終了時刻と日付を提供します。アプリケーションがアクティブな場合、終了時間の代わりにアクティブと表示されます。
- アプリケーション期間（分）: アプリケーションの継続時間を分単位で提供します。

> 注
>
> - アプライアンスで HDX セッション情報が利用できない場合など、意図しないエラーが発生した場合、**HDX** ユーザーレポート が有効になっていても、HDX ユーザーベースのレポートは表示されません。レポートのユーザー名、サーバー名、サーバーバージョン、ICA RTT などの一部のフィールドは **NA** と表示される場合があります。
> - **HDX** アプリ レポートのアプリケーション終了時間は、SD-WAN が Xen から アプリケーション終了時間を受信した場合にのみ表示されます Application/Xen デスクトップサーバー。それ以外の場合、一部のアプリケーションは閉じられていてもアクティブであると報告されます。

IPsec トンネルレポート

April 13, 2021

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）と認証ヘッダー（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 アプライアンスでの IPSec トンネルの構成の詳細については、「IPsec トンネルの終了」を参照してください。

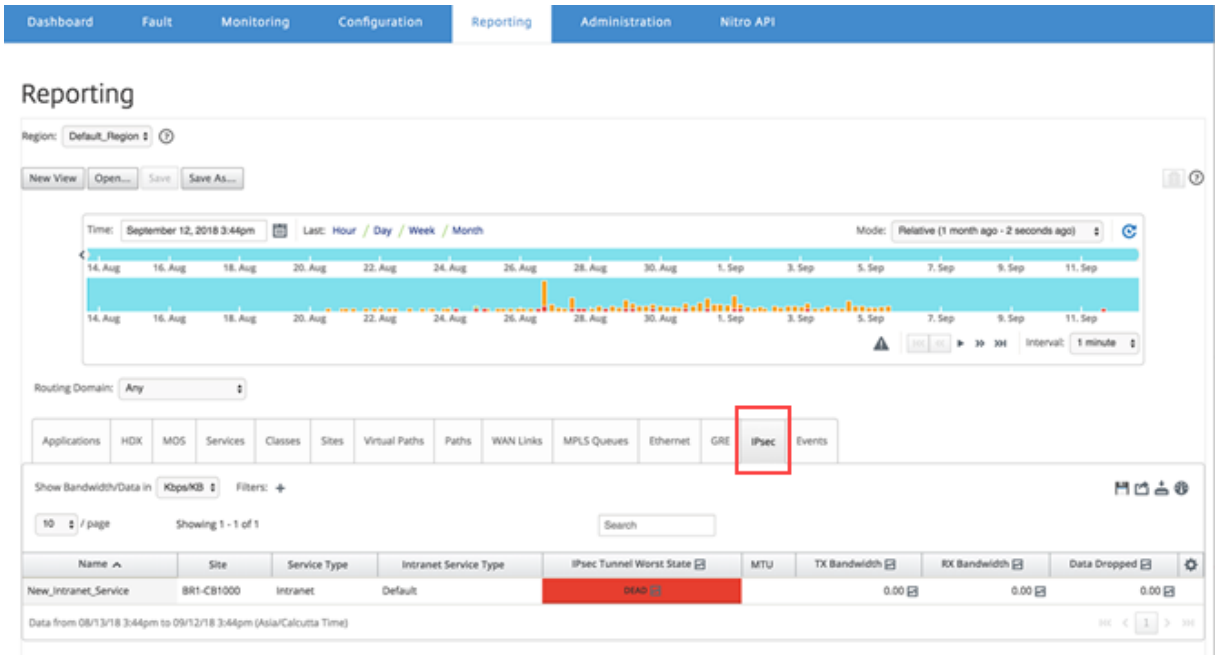
Citrix SD-WAN Center では、Citrix SD-WAN ネットワークで構成されているすべての IPsec トンネルの状態を表示できます。

IPsec トンネル統計を表示するには:

Citrix SD-WAN Center で、レポート > **IPsec** トンネルに移動し、およびタイムラインコントロールで期間を選択します。

タイムラインコントロールを使用して、特定の時間枠のレポートを選択して表示できます。詳細については、「タイムラインコントロール」を参照してください。

レポートビューを作成、保存、および開くこともできます。詳細については、「ビューを管理する」を参照してください。



次のメトリックを表示できます。

- 名前: アプリケーション名。
- 地点: サイトの名前。
- サービスの種類: サービスのタイプ。
- イントラネットサービスの種類: IPsec トンネルに関連付けられているイントラネットサービスのタイプ。以下は、イントラネットサービスのタイプです。
  - デフォルト
  - Microsoft Azure 仮想 WAN
  - Zscaler
  - Citrix SaaS Gateway

- **IPsec** の最悪の状態: 選択した期間中に観測された最悪の状態。
- **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。
- **TX** 帯域幅: 送信される帯域幅。
- **RX** 帯域幅: 受信した帯域幅。
- **TX** パケット: 送信されたパケットの数。
- **RX** パケット: 受信したパケットの数。
- ドロップされたデータ: ドロップされたデータ（Kbps）。
- ドロップされたパケット: ドロップされたパケットの数。

> 注
>
> 設定アイコンをクリックして、表示するメトリックを選択します。

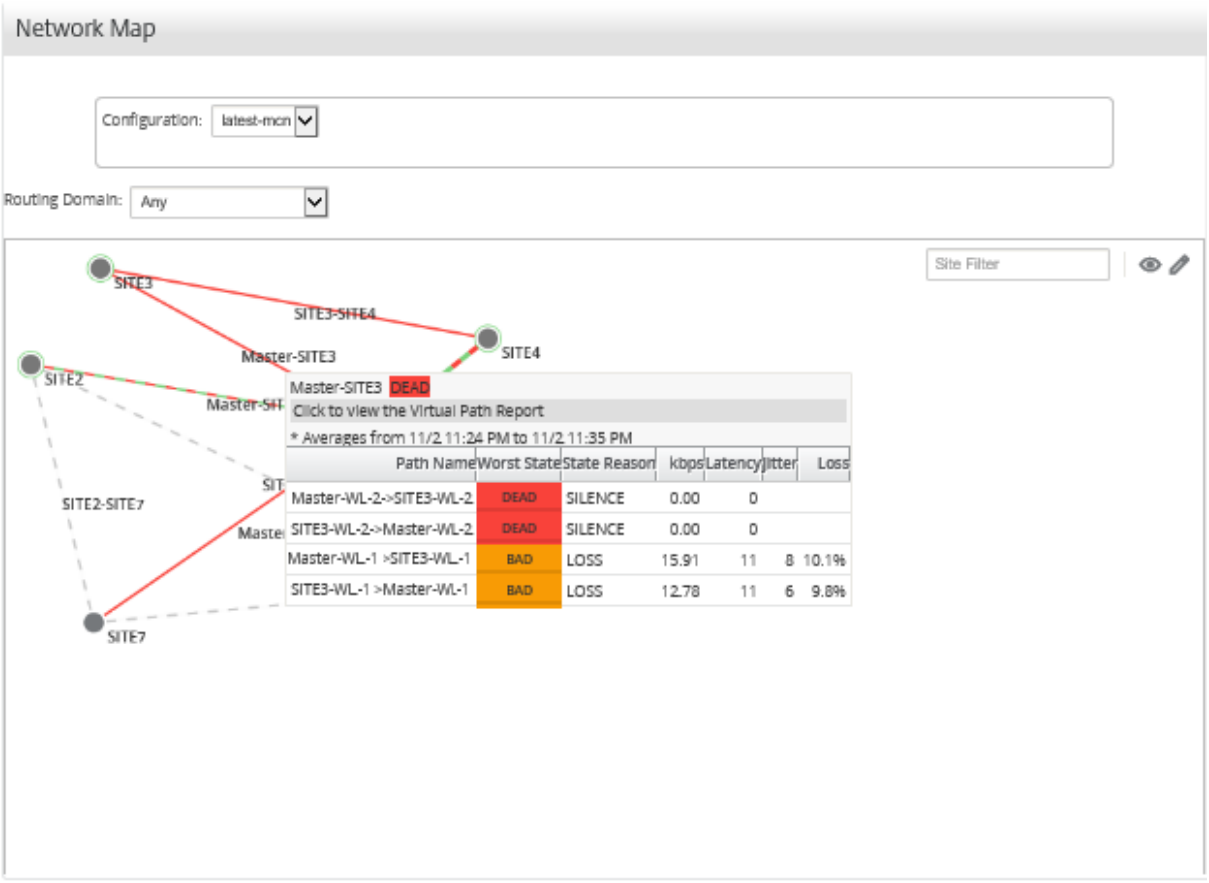
リンクパフォーマンスレポート

April 13, 2021

Citrix SD-WAN Center は、サイト、サービス、仮想パス、または WAN リンクレベルでパフォーマンス統計を表示できます。

組織 ABC に 4 つの支社があるネットワークを考えます。SITE3 で電圧低下が報告されています。つまり、従業員はイントラネットページを表示できないことがあります。根本的なリンクのパフォーマンスが原因であると思われます。

ダッシュボードのネットワークマップでサイトとデータセンター間のパスにマウスカーソルを合わせると、リンク統計の概要が表示されます。



上記のスクリーンショットは、SITE 3 とマスターコントローラーノード（MCN）の間に 2 つの WAN リンク（WL-1 と WL-2）があり、最新の 10 分間の統計を示しています。

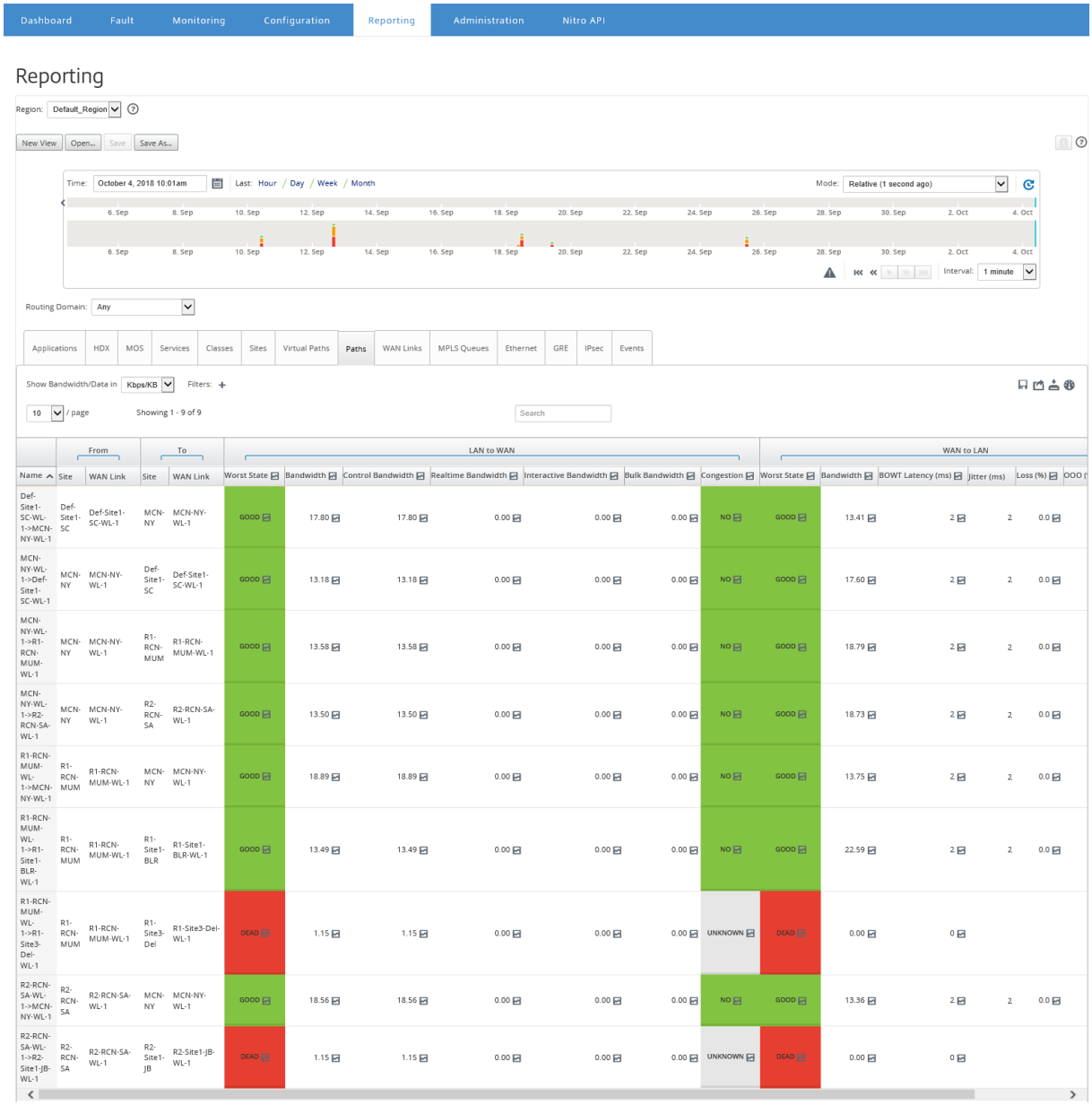
仮想パス Master-WL2->SITE3-WL2 および SITE3-WL2 ->Master-WL2 機能しておらず、代替パス Master-WL1->SITE3-WL1 および SITE3-WL1 ->Master-WL1 状態が悪く、送信データのかなりの部分が失われています。これが、SITE3 での電圧低下問題の推定原因です。

または、[レポート]> パスに移動して、リンク統計を表示できます。

タイムラインコントロールで期間を選択します。

タイムラインコントロールを使用して、特定の時間枠のレポートを選択して表示できます。詳細については、「タイムラインコントロール」を参照してください。

レポートビューを作成、保存、開くこともできます。詳細については、「ビューを管理する」を参照してください。



次のメトリックを表示できます。

- 名前: パス名。
- （サイトおよび **WAN** リンク）から: ソースサイトと WAN リンク。
- 宛先（サイトおよび **WAN** リンク）: 宛先サイトと WAN リンク。
- **LAN** から **WAN**
  - 仕事の状態:
  - 帯域幅: すべてのパケットタイプによって消費される合計帯域幅。帯域幅 = 制御帯域幅 + リアルタイムの帯域幅 + インタラクティブな帯域幅 + バルク帯域幅。
  - 帯域幅の制御: 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。

  - リアルタイムの帯域幅: 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）。
  - インタラクティブな帯域幅: 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が消費する帯域幅。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、ほとんど人間の介入を必要とせず、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。
  - 混雑: トラフィックの増加または WAN 内のパケットフローの予期しない遅延による輻輳。

- **WAN** から **LAN**:

  - 最悪の状態: 期間中に観測された最悪の WAN から LAN への状態。
  - 帯域幅:
  - **BOWT** レイテンシ（**ms**）: パケットが 1 つのポイントから別のポイントに移動するのにかかる最適な一方向時間（BOWT）（ミリ秒単位）。
  - ジッター（**ms**）: 受信パケットの遅延の変動（ミリ秒単位）。
  - 損失 (%) : 失われたパケットの割合。
  - **OOO**(%) : 正しい順序または順不同（OOO）ではないパケットのパーセンテージ。
  - 混雑: トラフィックの増加または WAN 内のパケットフローの予期しない遅延による輻輳。

[設定] アイコンをクリックし、レポートに表示するパラメーターを選択します。

アプリケーションの **MOS**

February 18, 2022

平均オピニオンスコア（MOS）は、アプリケーションがエンドユーザーに提供するエクスペリエンスの品質の数値測定を提供します。主に VoIP アプリケーションに使用されます。Citrix SD-WAN では、MOS は、VoIP コールであるかのようにトラフィックを判断することにより、非 VoIP アプリケーションの品質を評価するためにも使用されます。

Citrix SD-WAN Center は、仮想パスを通過するトラフィックの MOS を計算して表示します。すべての Citrix SD-WAN アプライアンスの各アプリケーションの **Estimate MOS** オプションを有効にして、これらのアプリケーションの MOS スコアを Citrix SD-WAN Center に表示します。

Citrix SD-WAN でアプリケーションの MOS を有効にする方法の詳細については、「ルールグループを追加して MOS を有効にする」を参照してください。

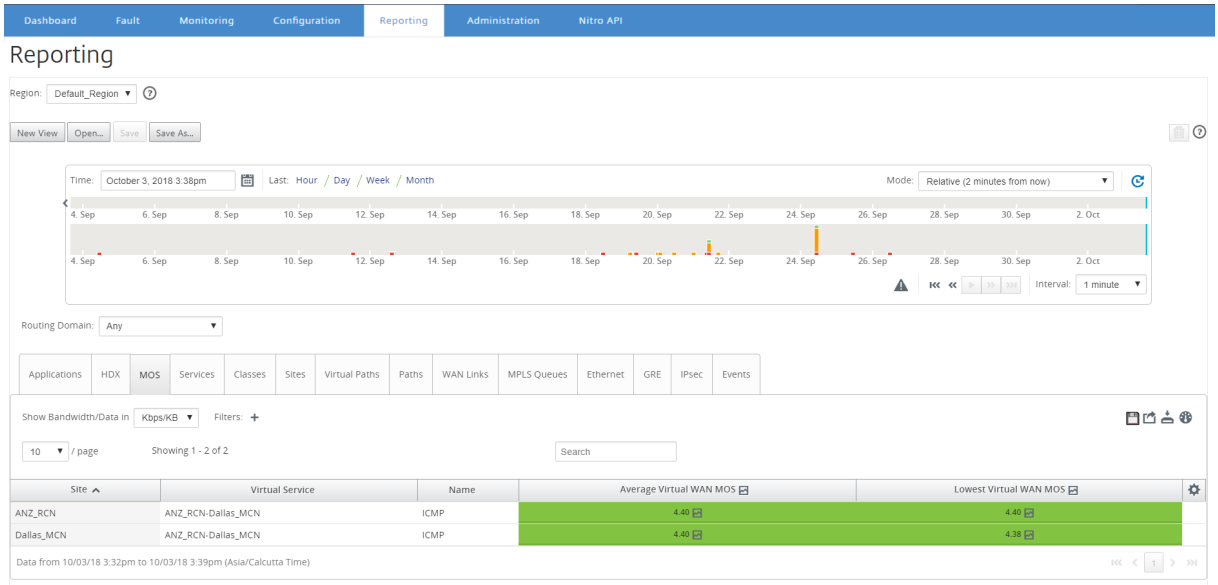
> 注
>
> アプリケーションの MOS を見積もり、Citrix SD-WAN Center に表示するには、[ルール] の [パフォーマンスの追跡] オプションを有効にします。規則の詳細については、「IP アドレスとポート番号によるルール」を参照してください。

アプリケーションの **MOS** を表示するには:

Citrix SD-WAN Center で、レポート > アプリケーションに移動、およびタイムラインコントロールで期間を選択します。

タイムラインコントロールを使用して、特定の時間枠のレポートを選択して表示できます。詳細については、「タイムラインコントロール」を参照してください。

レポートビューを作成、保存、開くこともできます。詳細については、「ビューを管理する」を参照してください。



次のメトリックを表示できます。

- 名前: アプリケーションの名前。
- 平均仮想 **WAN MOS**: 選択した期間にわたって計算された平均品質スコア。
- 最も低い仮想 **WAN MOS**: 選択した期間内に計算された最低品質スコア。

スコアは次のように評価されます。

- 5 –ユーザーは非常に満足しています。
- 4 –ユーザーは満足しています。
- 3 –ユーザーは不満です。
- 2 –ユーザーは非常に不満です。
- 1 –推奨されません。

MPLS キューレポート

April 13, 2021

MPLS キューは、標準の DiffServ コードポイント（DSCP）タグによって制御されるサービスキューを提供します。タグは、仮想 WAN 上の 2 つのサイト間のサービス品質を制御します。

MPLS キューを使用すると、MPLS プロバイダーは DSCP マーキングに基づいてトラフィックを識別できるため、プロバイダーはサービスクラスを適用できます。

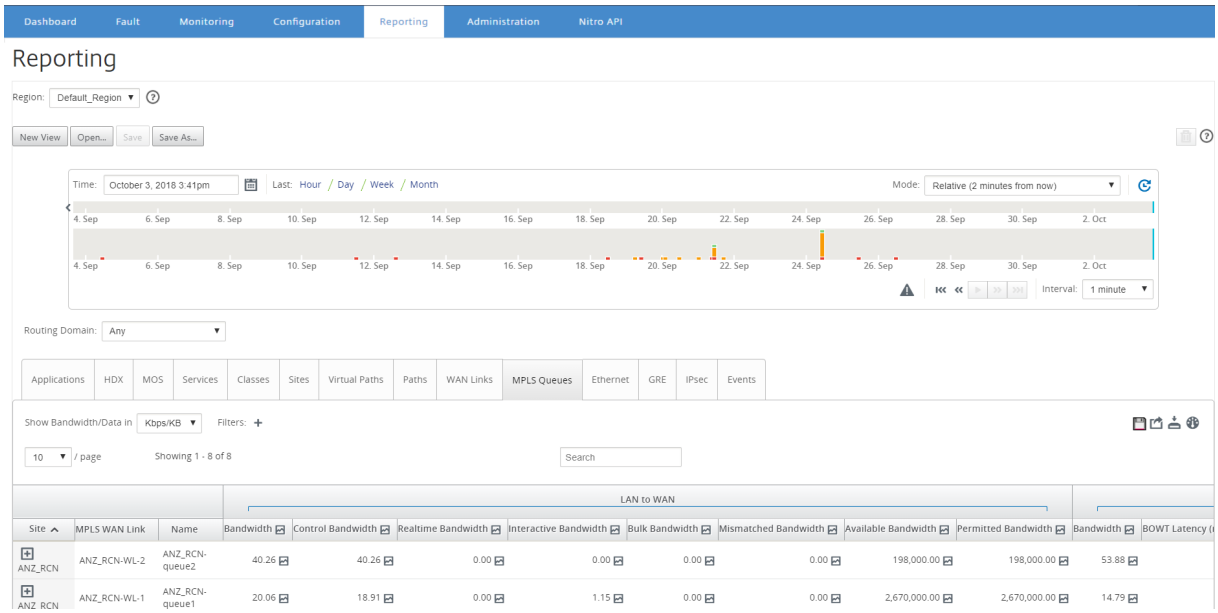
Citrix SD-WAN アプライアンスでのプライベート MPLS WAN リンクの構成の詳細については、「MPLS キュー」を参照してください。

MPLS キュー統計を表示するには:

Citrix SD-WAN Center で、レポート > **MPLS** キュー に移動、およびタイムラインコントロールで期間を選択します。

タイムラインコントロールを使用して、特定の時間枠のレポートを選択して表示できます。詳細については、「タイムラインコントロール」を参照してください。

レポートビューを作成、保存、開くこともできます。詳細については、「ビューを管理する」を参照してください。



次のメトリックを表示できます。

- **MPLS WAN** リンク: MPLS キューがメンバーである MPLS WAN リンクの名前。
- 名前: DSCP タグ名。
- 帯域幅: すべてのパケットタイプによって消費される合計帯域幅。帯域幅 = 帯域幅の制御 + リアルタイム帯域幅 + インタラクティブな帯域幅 + バルク帯域幅。

- 帯域幅の制御: 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: Citrix 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悪いものです（たとえば、VoIP、Skype for Business）。
- インタラクティブな帯域幅: Citrix 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: Citrix 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、ほとんど人間の介入を必要とせず、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。
- 帯域幅の不一致: Frames 定義された DSCP タグと一致しないものは、不一致の帯域幅用に指定されたデフォルトのキューにマッピングされます。
- 利用可能な帯域幅: サイトのすべての WAN リンクに割り当てられた帯域幅の合計。
- 許容帯域幅: 情報の送信に使用できる帯域幅。
- **BOWT** レイテンシ: パケットがあるポイントから別のポイントに移動するのにかかる最適な一方向時間（ミリ秒単位）。
- ジッタ: 受信パケットの遅延の変動（ミリ秒単位）。
- 失われたパケット: 失われたパケットの数。
- 損失: 失われたパケットの割合。
- **OOO**: 正しい順序になっていないパケットの割合。
- 混雑: トラフィックの増加または WAN 内のパケットフローの予期しない遅延による輻輳。

> 注
>
> 設定アイコンをクリックして、表示するメトリックを選択します。

管理

April 13, 2021

次の管理オプションを使用して、Citrix SD-WAN Center VPX を管理および維持できます。

日付と時刻を構成する

HTTPS 証明書

MCN 設定をインポートする

データベースを管理する

Mangae ビュー

ソフトウェアの更新

タイムラインコントロール

ユーザーアカウント

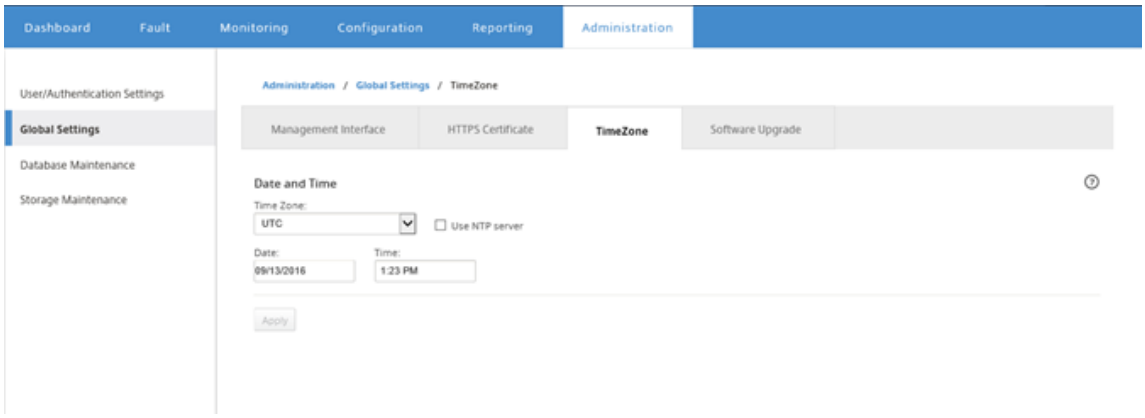
日付と時刻を構成する

April 9, 2021

手動または NTP サーバーを使用して、Citrix SD-WAN Center 管理システムの日付と時刻を変更できます。[**NTP** サーバー の使用] 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。

日付と時刻を手動で設定するには:

1. Citrix SD-WAN Center の Web インターフェイスで、[管理] タブをクリックします。
2. [グローバル設定**]** をクリックし、[タイムゾーン] をクリックします。



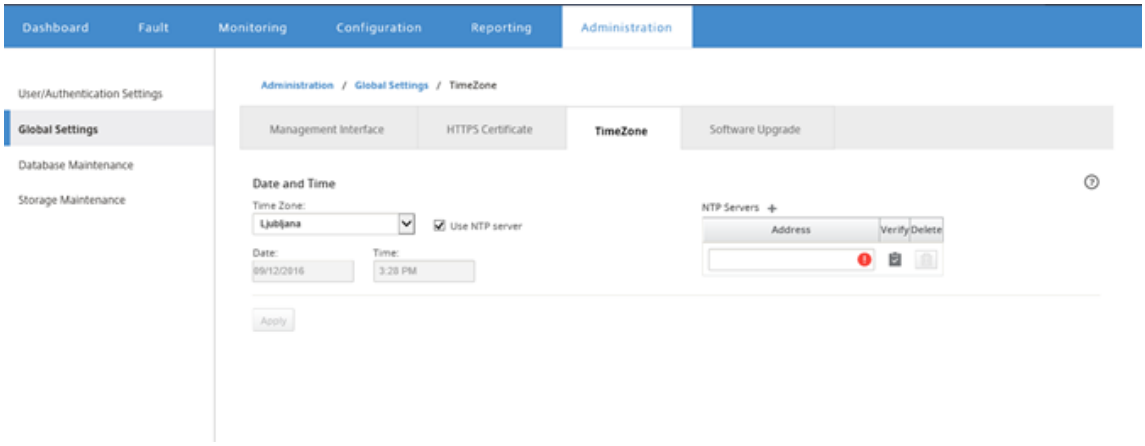
3.「タイムゾーン」フィールドで、現在のタイムゾーンの 都市 を選択します。または、タイムゾーンの現在の日付と時刻を入力します。
4. [**Apply**] をクリックします。

Citrix SD-WAN Center のクロックを外部 NTP サーバーと同期できます。

NTP サーバーを使用して日付と時刻を設定するには:

1. Citrix SD-WAN Center の Web インターフェイスで、[管理] タブをクリックします。
2. [グローバル設定**]** をクリックし、[タイムゾーン] をクリックします。
3. [**NTP** サーバーの使用**]** を選択します。

   これにより、日付と時刻のフィールドが無効になり、NTP サーバーテーブルが表示されます。



4. 新しい NTP サーバーを追加するには、+ NTP サーバーの横にあるアイコン。**
5. **Address** フィールド に、NTP サーバーのための **IP** アドレス を入力する。

   最大 3 つの NTP サーバーを指定できますが、少なくとも 1 つ指定する必要があります。これらのサーバーがバックアップ NTP サーバーとして機能する場合、一方のサーバーがダウンすると、Citrix SD-WAN Center がもう一方の 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、まだ行っていない限り、DNS サーバーも構成する必要があります。テーブルからサーバーエントリを削除するには、エントリの [削除] 列にある [削除] アイコンをクリックします。
6. 設定を適用する前に、[確認] をクリックしてサーバーにアクセスできることを確認します。
7. [**Apply**] をクリックします。

HTTPS 証明書

April 9, 2021

Citrix SD-WAN Center 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。

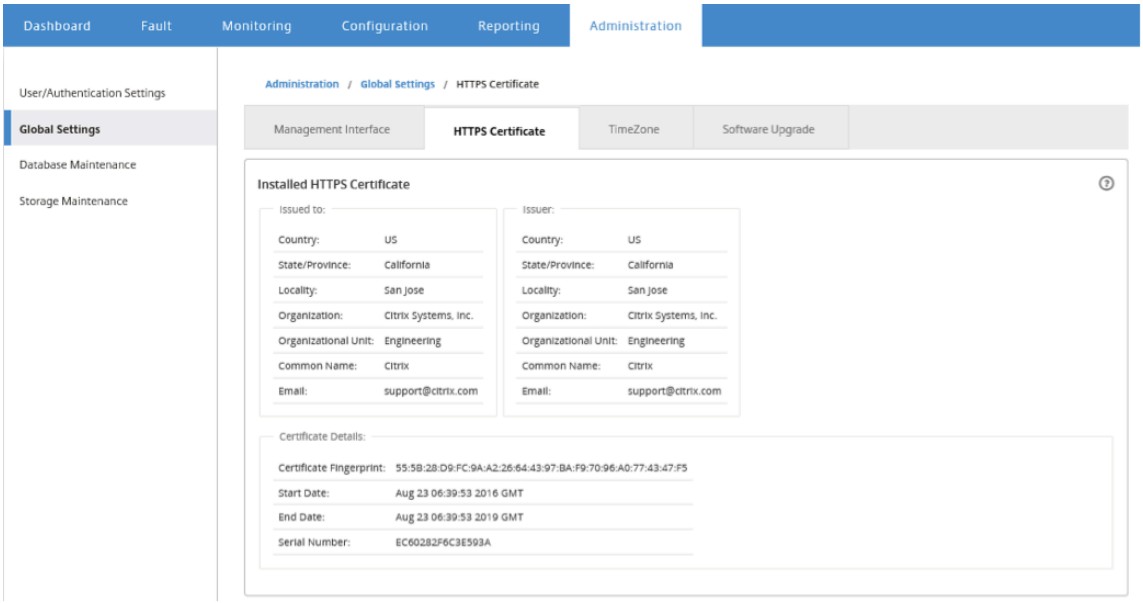
インストールされている **HTTPS** 証明書の詳細を表示する

Citrix 現在の証明書を評価するには、証明書の詳細を表示できます。

Citrix SD-WAN Center にすでにインストールされている HTTPS 証明書の詳細を表示するには:

1. Citrix SD-WAN Center の Web インターフェイスで、[管理] タブをクリックします。
2. [グローバル設定] をクリックし、[**HTTPS** 証明書] をクリックします。

   HTTPS 証明書の詳細が [インストールされた **HTTPS** 証明書] セクションに表示されます。

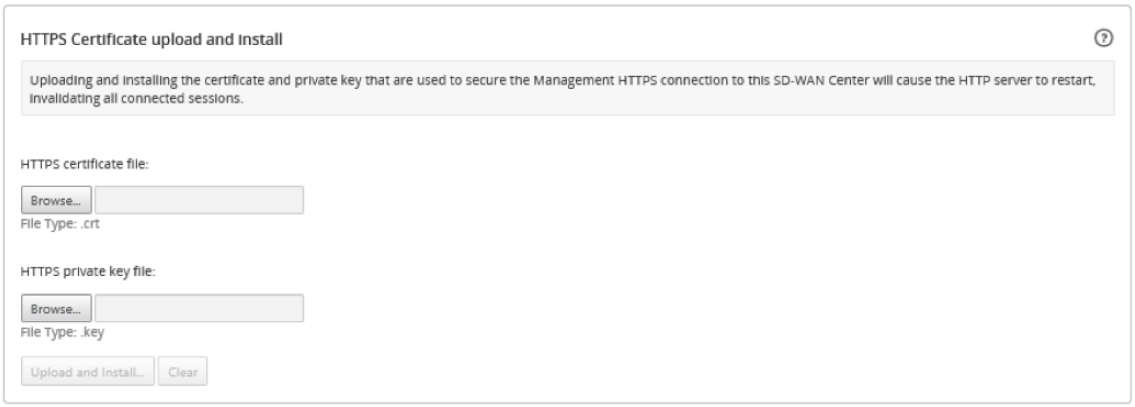


HTTPS 証明書をアップロードしてインストールする

HTTPS 証明書をインストールすると、操作が完了するまで Citrix SD-WAN Center がメンテナンスモードになります。操作が完了すると、Web サーバーが再起動され、接続されているすべてのセッションが無効になります。Web サーバーの再起動時にサーバーへの接続が失われた場合、メンテナンスモード画面が前のページを自動的に再読み込みし、ブラウザーからセキュリティ通知を表示します。画面が再読み込みされない場合は、[続行] をクリックして前のページを再読み込みします。

HTTPS 証明書をアップロードしてインストールするには:

1. Citrix SD-WAN Center の Web インターフェイスで、[管理] タブをクリックします。
2. [グローバル設定] をクリックし、[**HTTPS** 証明書] をクリックします。
3. [**HTTPS** 証明書のアップロードとインストール] セクションの [**HTTPS** 証明書ファイル] フィールドで、[参照] をクリックして HTTPS 証明書を選択します。
4. [**HTTPS** 秘密鍵ファイル] フィールドで、[参照] をクリックして HTTPS 秘密鍵ファイルを選択します。
5. [アップロードしてインストール] をクリックします。



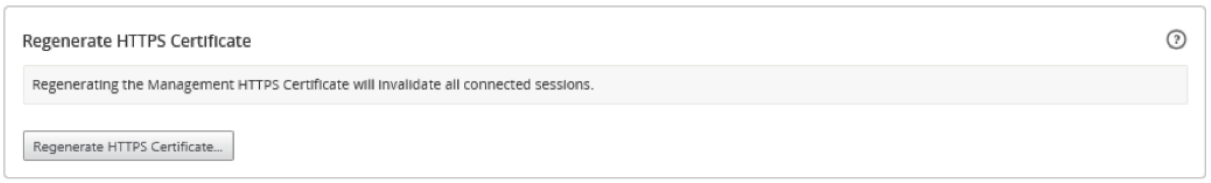
HTTPS 証明書を再生成する

Citrix SD-WAN Center への管理 HTTPS 接続を保護する自己署名証明書を再生成できます。HTTPS 証明書を再生成すると、操作が完了するまで Citrix SD-WAN Center がメンテナンスモードになります。操作が完了すると、Web サーバーが再起動され、接続されているすべてのセッションが無効になります。

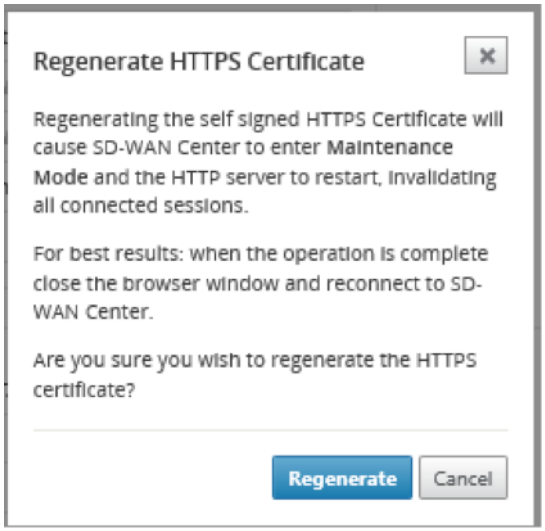
Web サーバーの再起動時にサーバーへの接続が失われた場合、メンテナンスモード画面が前のページを自動的に再読み込みし、ブラウザーからセキュリティ通知を表示します。画面が表示されない場合は、[続行] をクリックして前のページを再読み込みします。

HTTPS 証明書を再生成するには:

1. Citrix SD-WAN Center の Web インターフェイスで、[管理] タブをクリックします。
2. [グローバル設定**]** をクリックし、[**HTTPS** 証明書] をクリックします。
3. 再生成 **HTTPS** 証明書の セクションでは、再生成 **HTTPS** 証明書] をクリックします。



HTTPS 証明書の再生成メッセージが表示されます。再生成] をクリックします。



MCN 設定をインポートする

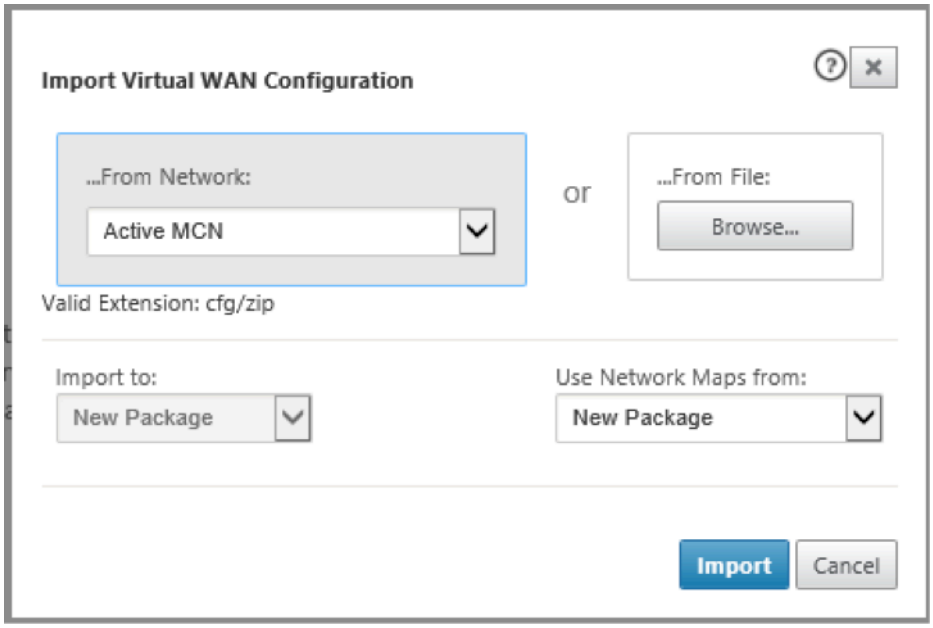
April 13, 2021

Citrix SD-WAN Center がセットアップされ、マスターコントロールノード（MCN）と Citrix SD-WAN Center の間に接続が確立されると、MCN 構成を Citrix SD-WAN Center にインポートして、ネットワークマップを表示できます。

インポート機能は、オープンまたは新規の Citrix SD-WAN マスター構成に構成をインポートします。インポート機能を使用するときに Citrix SD-WAN マスター構成が開いている場合、その構成とそのマップは新しい Citrix SD-WAN マスター構成によって上書きされます。Citrix SD-WAN マスター構成が開いていない場合、無題のパッケージが作成されます。

MCN 構成を Citrix SD-WAN Center にインポートするには:

1. Citrix SD-WAN Center の Web インターフェイスで、[構成] タブをクリックします。
2. [**Network Configuration**] をクリックしてから、[**Import**] をクリックします。



3. **From Network** フィールドで、次のオプションのいずれかを選択します。

   - アクティブな **MCN**: アクティブな MCN に接続し、現在の設定をダウンロードします。
   - その他の: 別の MCN の IP アドレスに接続し、現在の構成をダウンロードします。構成をインポートする前に、この Citrix SD-WAN Center のセキュリティ証明書を MCN にインストールする必要がある場合があります。

   詳細については、「Citrix SD-WAN Center 証明書をインストールする」を参照してください。

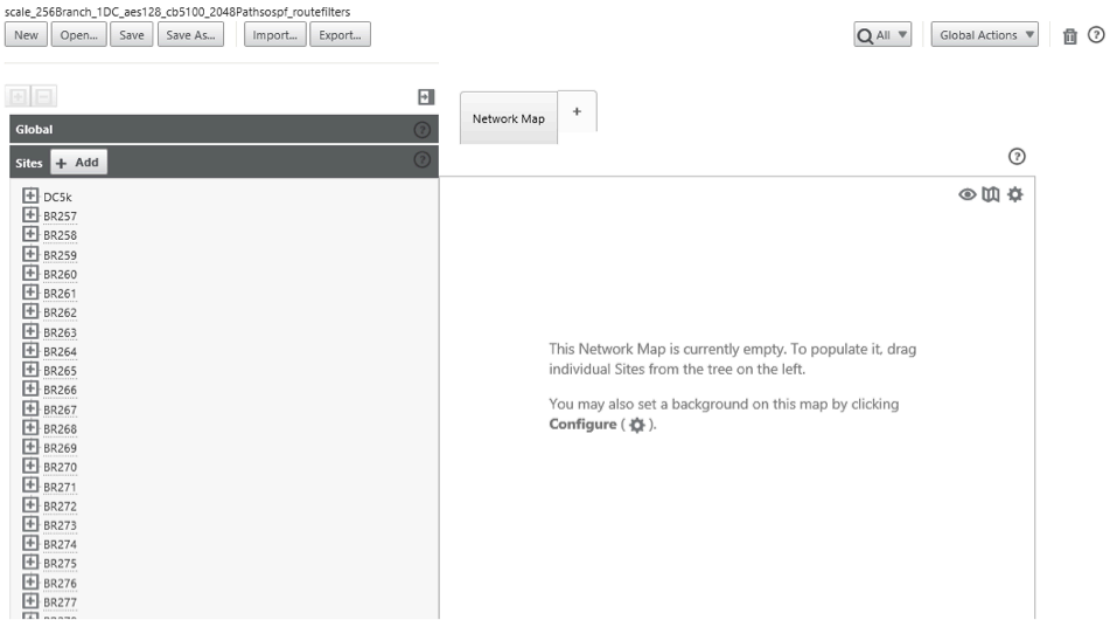
4. または、**[**ファイルから] セクションで [参照] をクリックして、コンピューターからアップロードする構成を選択します。

5. [インポート 先] フィールドで [現在のパッケージ**]** を選択して、選択したファイルの内容を現在開いているパッケージにインポートします。

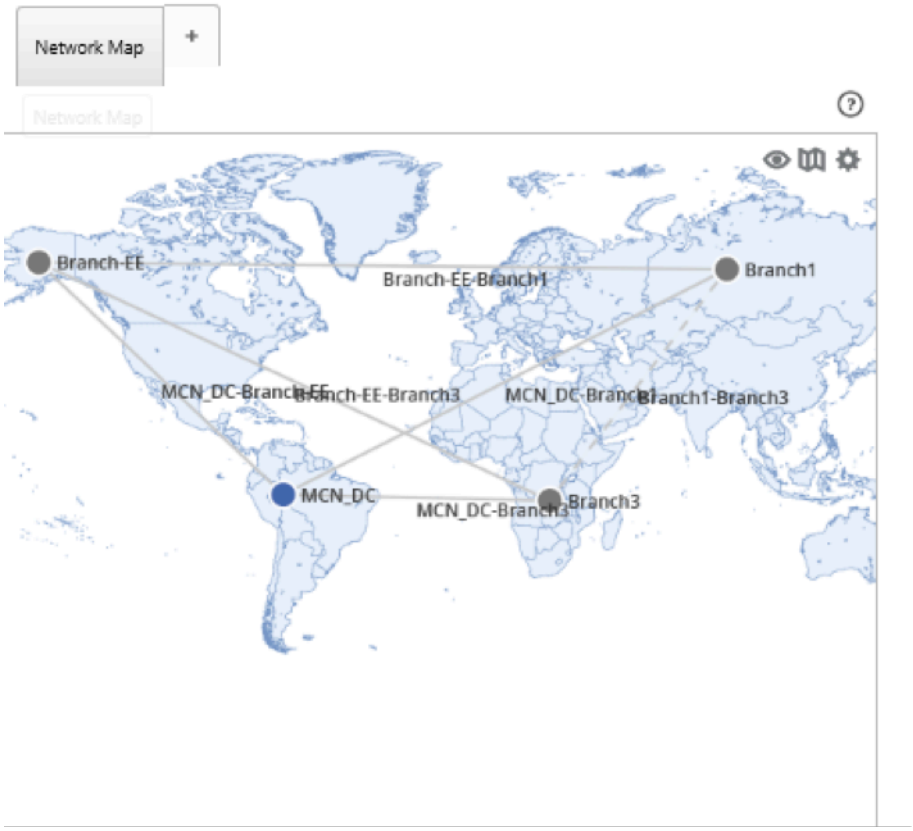
6. [**Use Network Maps from]** フィールドで、次のいずれかのオプションを選択します。

   - 現在のパッケージ: インポート後、現在保存されているネットワークマップのセットを保持します。
   - 新しいパッケージ: インポートされたパッケージのネットワークマップを使用し、現在のマップセットを破棄します。
   - 両方のパッケージ: 現在保存されているマップに加えて、インポートされたマップを使用します。

7. ［インポート］をクリックします。構成がインポートされます。



8. [ネットワークマップ] セクション。設定アイコンをクリックし、[自動入力] を選択して、構成内の各サイトをマップに自動的に追加して配置します。



データベースを管理する

April 13, 2021

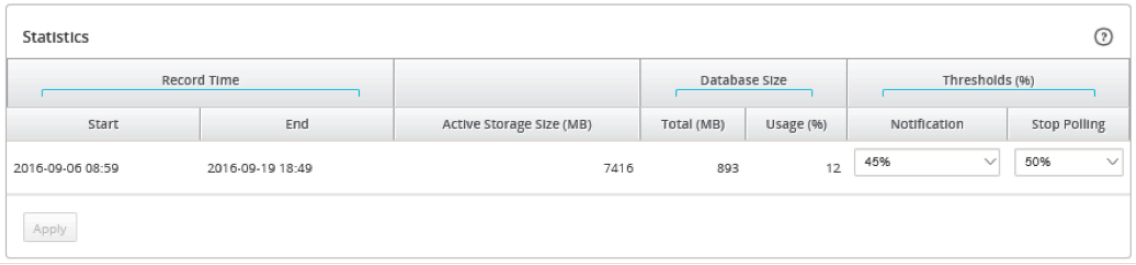
データベースを監視および管理して、ネットワーク上で検出されたすべてのアプライアンスからのポーリングデータを格納するのに十分なディスク領域があることを確認できます。

データベース統計の表示

統計 テーブルには、使用可能なデータベース統計が表示され、通知とポーリングのデータベースディスク使用量しきい値を指定するための入力フィールドが含まれています。

データベース統計を表示するには:

1. Citrix SD-WAN Center Web UI で、[管理] タブをクリックします。
2. [データベースのメンテナンス] をクリックします。[統計] セクションに次の情報が表示されます。
    - レコード時間: データベース内の最も古いレコードと最新のレコードの日付とタイムスタンプを表示します。この列には、次の情報が含まれています。
        - 開始: データベース内の最も古いレコードの日付とタイムスタンプを表示します。
        - 終わり: データベース内の最新のレコードの日付とタイムスタンプを表示します。
    - アクティブストレージサイズ（**MB**）: 現在アクティブなストレージのディスク容量を表示します。
    - データベースサイズ（**MB**）: 現在のデータベースサイズと使用情報を表示します。この列には、次の情報が含まれています。
        - 合計（**MB**）: データベースの合計サイズを MB で表示します。
        - 使用法 (%): 現在アクティブなストレージのディスク領域におけるデータベースのディスク使用率を表示します。



通知とポーリングのしきい値を設定するには:

1. 「通知」フィールドに、データベース使用通知を生成するためのしきい値として使用するデータベースサイズまたはアクティブストレージサイズの割合を入力します。データベースの使用がこのしきい値を超えると、電子メール通知が送信されます。

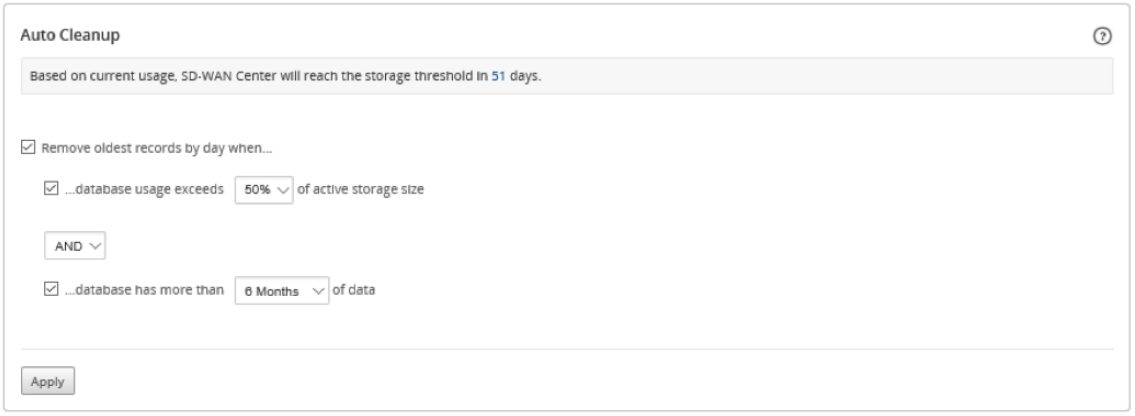
2. [ポーリング の停止] フィールドに、統計のポーリングを停止するデータベースのディスク使用量のしきい値（パーセント）を入力します。ドロップダウンメニューから **10**%～**50**%の値を選択します。デフォルトは **50**% です。
3. [**Apply**] をクリックします。

自動クリーンアップの構成

データベースのディスク使用量を管理するために、しきい値を指定できます。しきい値を超えると、古いレコードがデータベースから削除されます。

データベースのクリーンアップを有効にし、しきい値を構成するには:

1. Citrix SD-WAN Center Web UI で、[管理] タブをクリックします。
2. [データベースのメンテナンス] をクリックします。
3. [自動クリーンアップ] セクションで、[次の ときに最も古いレコードを削除…] チェックボックスをオンにして、データベースのクリーンアップを有効にします。



有効にすると、データベースが自動的にチェックされます 2:00 毎日午前。このチェックは、指定されたしきい値に達したか超えた場合に、データベースのクリーンアップを開始します。デフォルトでは、これは有効になっていません。

以前は、SD-WAN Center データベースの自動クリーンアップのデフォルト設定は次のとおりでした。

- 次の場合、最も古いレコードを日ごとに削除します。
  - …データベースの使用量がアクティブストレージサイズの 50%を超えています
  - 演算子は AND として選択する必要があります
  - …データベースには 6 か月以上のデータがあります

11.1.1 リリース以降では、SD-WAN Center データベースの自動クリーンアップのデフォルト設定が次のように変更されました。

- 次の場合、最も古いレコードを日ごとに削除します。

- …データベースの使用量がアクティブストレージサイズの 50%を超えています
- 演算子は OR として選択する必要があります
- …データベースには 1 か月以上のデータがあります

> 注意
>
> 設定の変更は、11.1.1 リリースにアップグレードされた、すでにプロビジョニングされている SD-WAN Center システムには影響しません。新たにプロビジョニングされた 11.1.1 リリース以降の SD-WAN Center システムにのみ適用されます。

4. 選択 …データベース使用量が超過 (%) アクティブなストレージサイズのドロップダウンメニューからパーセンテージを選択して、データベースのクリーンアップのしきい値を指定します。オプションは、**10**%～**50**% の増分で 5% 。**
5. **AND** または **OR** を選択し、ドロップダウンメニューから […データベースの使用率が次を超えています…] と […データベースが次を超えています…] の間の演算子を選択して、このルールの適用方法を演算子に指定します。11.1.1 リリース以降のデフォルトは **OR** です。
6. 選択 …データベースには [# [months] データの 月] をクリックし、ドロップダウンメニューから月数を選択して、データベースにデータを保持するデータベースクリーンアップの期間のしきい値を指定します。オプションは、**1** か月 ごとに 1 か月から **12** か 月です。
7. [**Apply**] をクリックします。

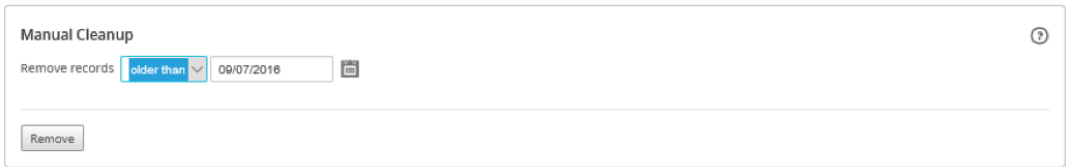
手動クリーンアップの構成

指定した基準に基づいて、統計およびイベントレコードをデータベースから手動で削除できます。

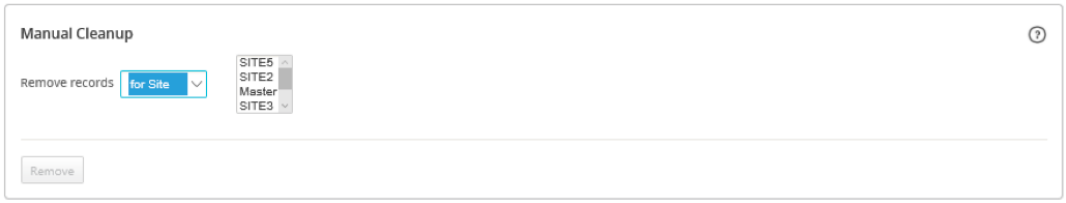
手動でデータベースをクリーンアップするには:

1. Citrix SD-WAN Center の Web インターフェイスで、[管理] タブをクリックします。
2. [データベースのメンテナンス] をクリックします。
3. [手動クリーンアップ] セクションで、 [レコード の削除] ドロップダウンメニューからフィルターを選択します。フィルタオプションは次のとおりです。

   - 古い: 指定した日付より前に収集されたレコードを削除します。このフィルターを選択すると、日付フィールドとカレンダー選択ボタンが表示されます。カレンダーボタンをクリックして日付を選択します。指定した日付より古いすべてのレコードが削除されます。



- サイトの場合：指定した日付より前に収集されたレコードを削除します。このフィルターを選択すると、日付フィールドとカレンダー選択ボタンが表示されます。カレンダーボタンをクリックして日付を選択します。指定した日付より古いすべてのレコードが削除されます。



4. [削除] をクリックします。

ビューを管理する

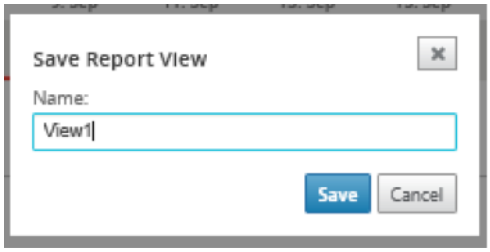
April 9, 2021

[Fault、Reporting、Network Map and Statistics] ページでは、それぞれのビューを作成、表示、変更、および削除できます。

> 注
>
> 手順で使用されているスクリーンショットは、ビューのタイプによって実際のユーザーインターフェイスと異なる場合があります。

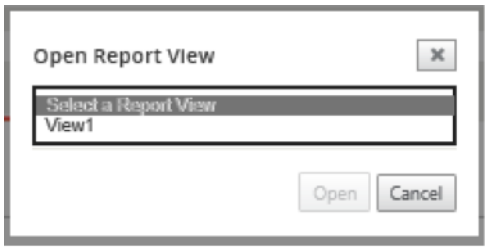
新しいビューを作成するには：

1. [新しいビュー] をクリックすると、名前のない新しいビューが作成され、時間指定が現在の時間にリセットされます。
2. フィルターを作成して適用するか、必要な変更を行います。
3. [名前を付けて保存] をクリックします。
4. [ビュー の保存] ダイアログボックスで、ビューの名前を入力します。
5. [保存] をクリックします。



既存のビューを開いて変更するには：

1. ［開く］をクリックします。
2. **[**ビューを開く**]** ダイアログボックスで、ドロップダウンリストからレポートビューを選択します。
3. ［開く］をクリックします。イベントビューが開きます。
4. 必要に応じて、必要な変更を加えます。
5. ［保存］をクリックします。



ビューを削除するには、ビューを開いて削除アイコンをクリックします。

ソフトウェアの更新

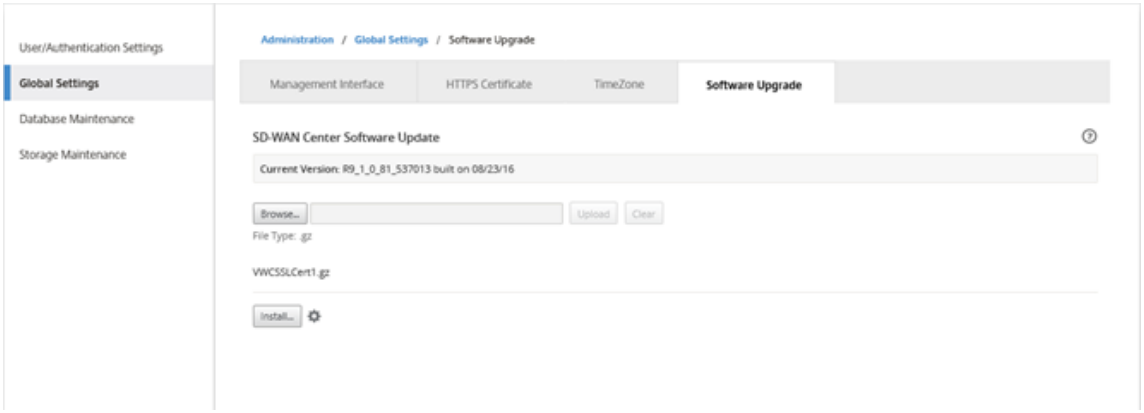
April 9, 2021

ソフトウェアアップグレードオプションを使用して、Citrix SD-WAN Center 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。ソフトウェアのアップグレードプロセスにより、Citrix SD-WAN Center がメンテナンスモードになります。データベースの移行が必要な場合、このプロセスには数時間かかることがあります。この間、統計データは仮想 WAN から収集されず、すべての Citrix SD-WAN Center 機能は使用できなくなります。

> 重要
>
> メンテナンス時間中にアップグレードを実行することをお勧めします。
>
> 注
>
> 適切な Citrix SD-WAN Center 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 SD-WAN Center ソフトウェアの新しいバージョンをアップロードしてインストールするには

1. Citrix SD-WAN Center の Web インターフェイスで、[管理] タブをクリックします。
2. [グローバル設定**]** をクリックし、[ソフトウェアアップグレード] をクリックします。



3. [参照] をクリックしてファイルブラウザを開き、アップロードするソフトウェアパッケージを選択します。
4. [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 Center 仮想マシンにアップロードします。
5. 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。
6. 確認を求められたら、[インストール] をクリックします。
7. 表示されるダイアログボックスで、[使用許諾契約書に同意し ます] チェックボックスをオンにし、[インストール] をクリックします。

タイムラインコントロール

April 9, 2021

[Fault、Reporting、Network Map and Statistics] ページの上部にあるタイムラインには、現在のビューの時間枠を制限するためのコントロールがあります。現在のデータベースから最大 30 日間のデータの時間枠を表示できます。

> 注
>
> 選択した期間に基づいて、現在の Citrix SD-WAN ネットワーク構成に関係なく、履歴データを表示できます。

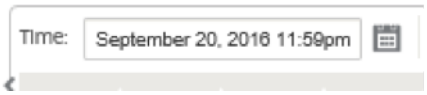
Time

次の要素を使用して、現在のビューの時間枠を指定できます。

- 時間 - 時間 フィールドに日付と時刻を入力して、グラフの結果を特定の日付と時刻に絞り込みます。形式は次のいずれかです。
  - ***Month Day, Year Hour:Minutes*** [**am** / **pm**] For example: September 7, 2015 2:00pm.
  - ***MM/DD/YYYY HH:MM*** [**am** / **pm**] For example: 09/07/2015 8:36am.

  - ***M/D/YY H:MM*** [**am** / **pm**] For example: 9/7/15 10:14pm

- カレンダー -（カレンダーアイコン）[時間] フィールドの右側にあるカレンダーアイコンをクリックし、日付を選択して、表示結果をその日付に制限します。



- タイムライン - タイムライン上の別のポイントをクリックしてドラッグし、少なくとも 30 分のタイムフレームを選選択します。

- 最後の時間 / 日 / 週間 / 月 -オプション（時間、日、週、または 月）をクリックして、表示結果をその時間枠に制限します。

モード

タイムラインモードは、タイムラインがタイムフレームの選択を解釈する方法と、自動更新が現在のビューとダッシュボードに反映される方法を決定します。**Relative** （選択された時間フレーム）と **Absolute** （選択された時間フレーム）の 2 つのモードオプションがあり、選択された時間フレームは **Time** フィールドで指定された時間フレームです。

タイムラインモードを変更するには、タイムラインの右上隅にある [モード] ドロップダウンメニューから [相対] または [絶対] を選択します。

相対モード

相対 モードを選択した場合、時間ラインは、時間に指定された時間フレームを現在を基準とした 時間 として扱います。ビューを保存して後で開く場合、ビューに表示される情報は、ビューが開かれた時間に関連しています。自動更新を有効にしており、統計の更新が検出された場合、データベースに記録されている最新の時刻を基準にしてビューが更新されます。

現在指定されている時間枠は、[相対] メニューオプションの一部として括弧内に表示されます。たとえば、時間枠として [最終：日] を選択した場合、[相対] オプションは [相対（1 日前-今から 1 分）] として表示されます。

絶対モード

あなたは 絶対モード を選択した場合は、タイムラインの扱い時間枠は 時間のために指定しました: 絶対（静的）時点として。ビューを保存して後で開いた場合や、自動更新を有効にした場合でも、ビューは常に選択した時間を表しま

す。現在指定されている時間枠は、次の形式を使用して、[絶対] メニューオプションの一部として括弧内に表示されます。

絶対（start_date start_time - end_date end_time ）**

たとえば、時間枠として「**Last**：**Day** 」を選択した場合、現在の日付と時刻は 9/7 4:43 PM、絶対 オプションは 絶対として表示されます (9/6 4:43 PM- 9/7 4:43 PM)。

ユーザーアカウント

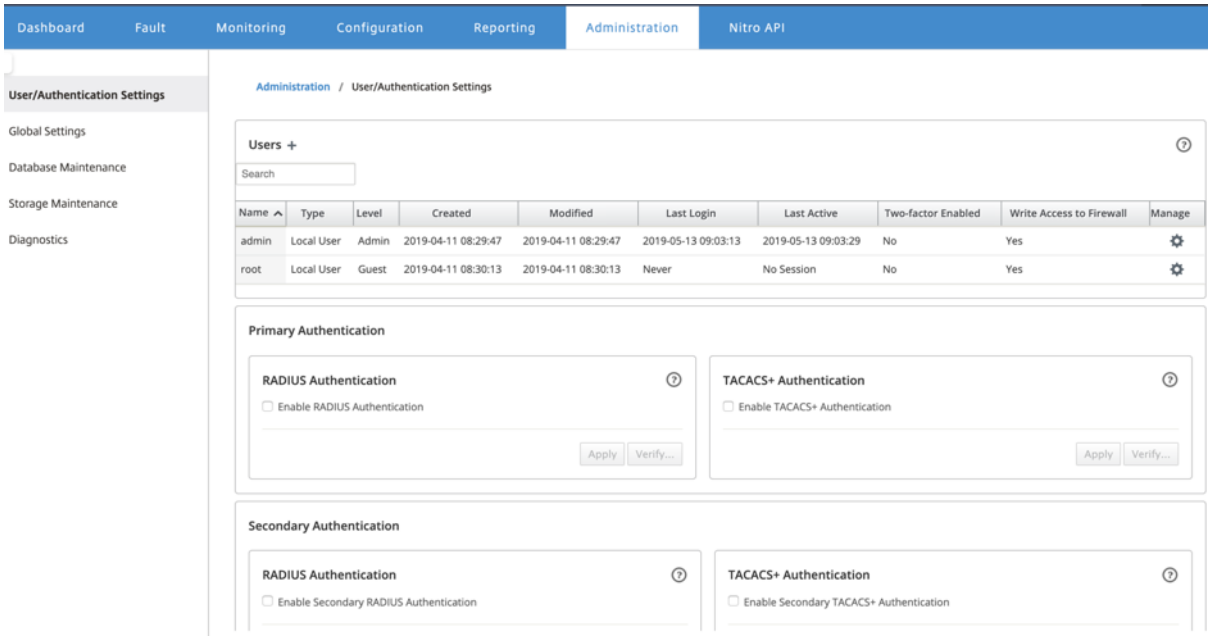
April 13, 2021

Citrix SD-WAN Center 仮想マシンに少なくとも 1 回ログインしたすべてのローカルおよびリモートユーザーアカウントのリストを表示できます。リモートユーザーアカウントは、RADIUS または TACACS + 認証サーバーを介して認証されます。新しいローカルユーザーアカウントを Citrix SD-WAN Center に追加することもできます。

> 注
>
> ユーザーアカウントがリモート認証サーバーで使用可能であるが、Citrix SD-WAN Center へのログオンに使用されていない場合、ユーザー リストに表示されません。

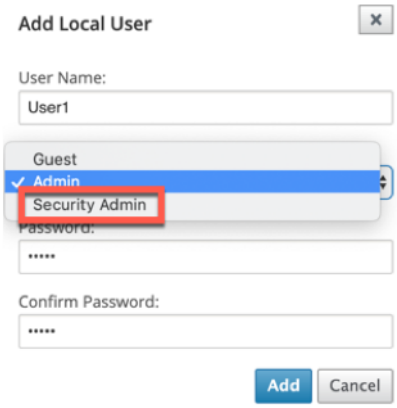
SD-WAN Center Web インターフェイスでユーザーアカウントを表示するには、**[管理] > User/Authentication** 設定に移動します。

ユーザーアカウントのリストが [ユーザー] セクションに表示されます

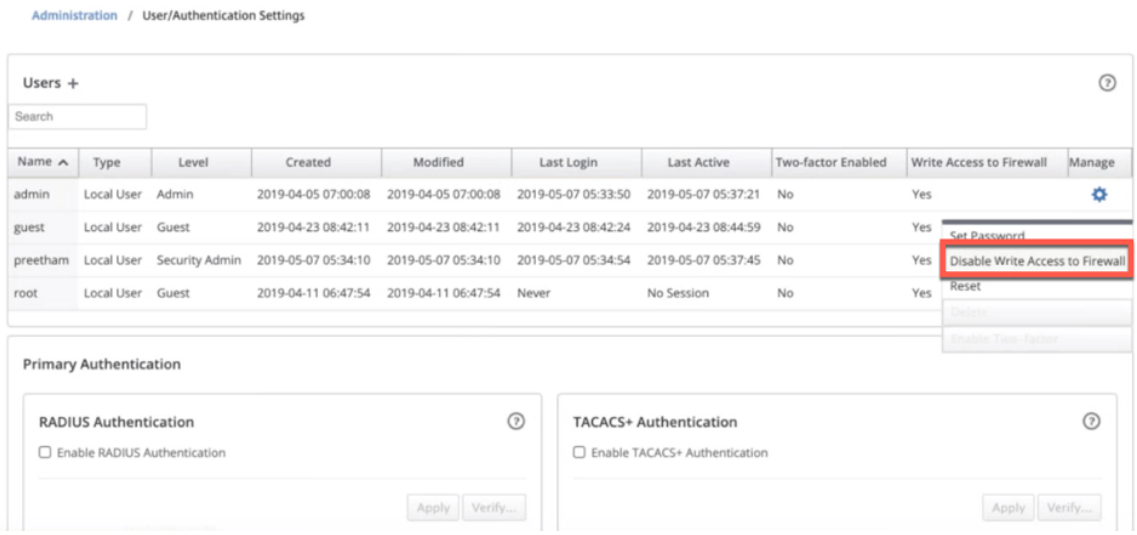


次の情報が表示されます。

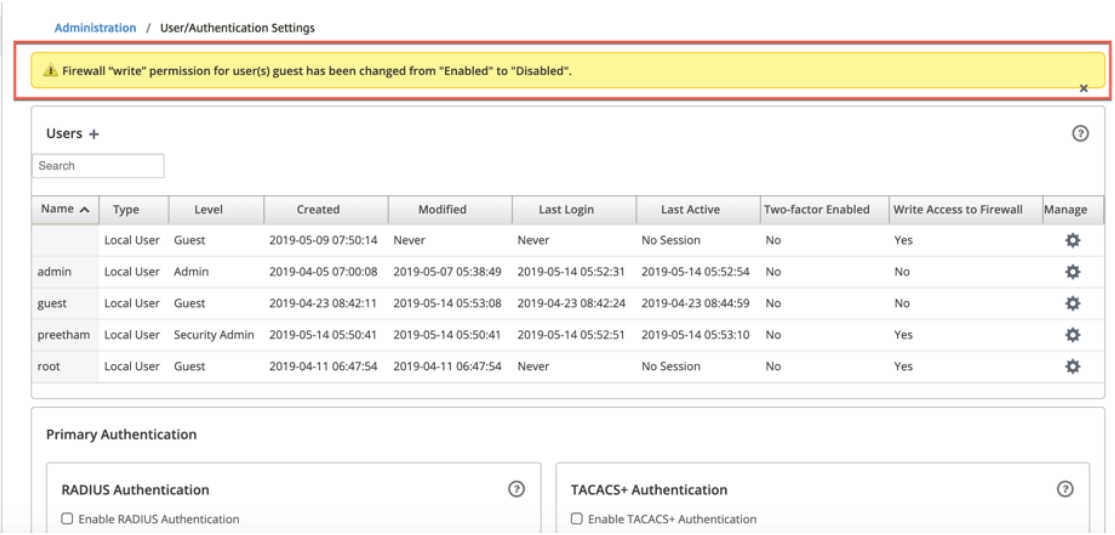
- 名前：ユーザー名。
- タイプ: ユーザーアカウントのタイプ。次のいずれかになります。
  - ローカル：SD-WAN Center インターフェイスを使用してローカルで作成および管理されるユーザーアカウント。
  - 半径: RADIUS サーバーによって認証されたリモートユーザーアカウント。
  - **TACACS +**: TACACS + サーバーによって認証されたリモートユーザーアカウント。
- レベル：アカウントの特権には次の 3 つのレベルがあります。
  - 管理者: 管理者アカウントには管理者権限があります。すべてのセクションへの読み取り/書き込みアクセス権があります。
  - ゲスト: ゲストアカウントは、ダッシュボード、レポート、モニタリング ページへのアクセス権を持つ読み取り専用アカウントです。
  - セキュリティ管理者: セキュリティ管理者 は、ファイアウォールとセキュリティに関連する **Config Editor** の設定に対してのみ読み取り/書き込みアクセス権を持ち、残りのセクションへの読み取り専用アクセス権を持ちます。



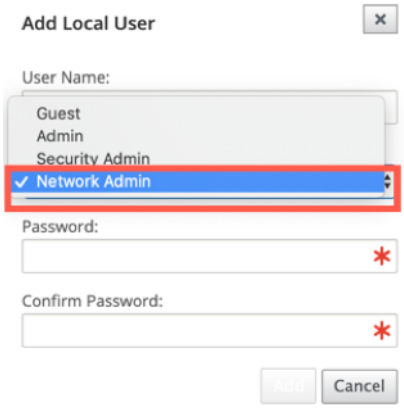
> メモ
>
> * 管理者とセキュリティ管理者のみが、セキュリティ機能の構成を変更または変更できます。
> * セキュリティ管理者は、スーパー管理者を除くすべてのユーザーアカウントのファイアウォールへの書き込みアクセスを有効または無効にできます。



セキュリティ管理者が特定のユーザーのファイアウォール書き込み権限を変更すると、すべてのユーザーに通知バーが表示されます。この通知はユーザーごとに表示されるので、ログインしている各ユーザーは、警告を削除して通知を承認する必要があります。



- ネットワーク管理者: ネットワーク管理者 は、すべてのセクションに対する読み取り/書き込み権限を持っており、構成エディターのファイアウォールとセキュリティ関連の設定を除いて、ブランチを完全にプロビジョニングできます。



ホストされているファイアウォールノードは、ネットワーク管理者が利用できません。この場合、ネットワーク管理者は新しい構成をインポートする必要があります。ネットワークとセキュリティの両方の設定は、スーパー管理者（Admin）によって維持されます。

ネットワーク管理者とセキュリティ管理者は、構成を変更したり、ネットワークに展開したりできます。

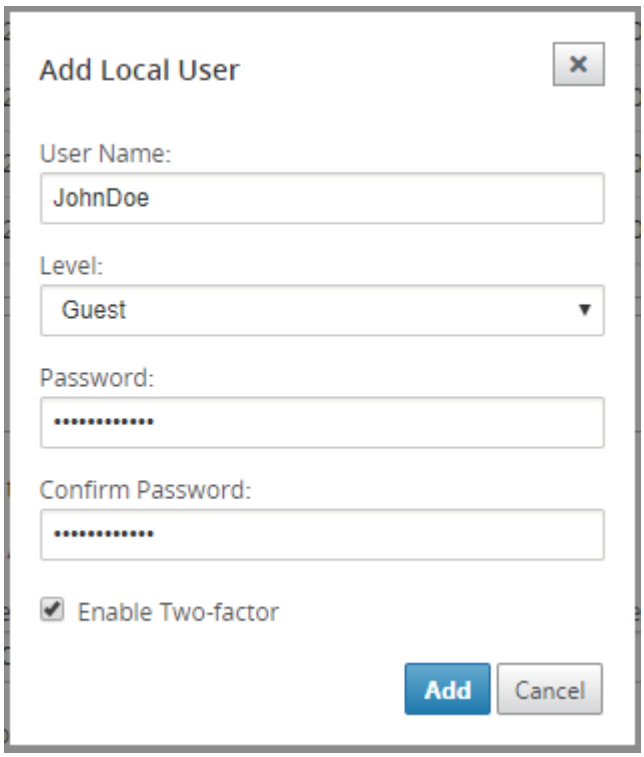
> 注
>
> ネットワーク管理者およびセキュリティ管理者は、ユーザーアカウントを追加または削除できません。編集できるのは自分のアカウントのパスワードのみです。

- 作成した: ローカルユーザーアカウントの場合、ユーザーアカウントが作成された日付。リモートユーザーアカウントの場合、最初のログインセッションの日付。
- 修正: ローカルユーザーアカウントの場合、パスワードが最後に変更された日付。リモートユーザーの場合、最初のログインセッションの日付。
- 前回のログイン: ユーザーが最後に正常にログインした日付。ツールチップに、ログインに使用されたデバイスの IP アドレスが表示されます。
- 最後にログインした時: サーバーに対して最後のリクエストが行われた日付。ツールチップに、ログインに使用されたデバイスの IP アドレスが表示されます。
- 管理：歯車アイコンをクリックして、次の オプションを含むメニューを表示します。
  - パスワードを設定してください: ローカルユーザーアカウントのパスワードを変更します。root パスワードを変更するには、現在の root パスワードが必要です。リモートユーザーアカウントの パスワードは変更できません。
  - リセット: このユーザーアカウントのワークスペースと設定を削除します。
  - 削除する: SD-WAN Center からローカルユーザーアカウント、ワークスペース、および設定を削除します。リモートアカウントと管理者アカウントは削除できません。
  - 二要素認証：ローカルおよびリモートユーザーアカウントの二要素認証を有効にします。詳しくは、「二要素認証」を参照してください。
- ファイアウォールへの書き込みアクセス: ファイアウォールへの書き込みアクセスが有効または無効であることを示します。

Citrix SD-WAN Center に新しいローカルユーザーアカウントを追加するには:

> 注
>
> Citrix SD-WAN Center でローカルに作成されたユーザーアカウントには、ネットワーク構成パッケージを編集して MCN にエクスポートする権限がありません。

1. 追加アイコンをクリックします + ユーザーの横。[ローカルユーザーの追加] ダイアログボックスが表示されます。



2. 次のパラメーターの値を入力します。

   - ユーザー名: ローカルユーザーアカウントのユーザー名。
   - レベル: アカウント特権。ゲストユーザーアカウントは、ダッシュボード、レポート、統計情報の表示に限定された読み取り専用 アカウントです。ゲスト ユーザーアカウントには、ネットワーク 構成パッケージを編集して MCN にエクスポートする権限がありません。
   - パスワード: ユーザーアカウントのパスワード。
   - パスワードを認証する: 確認のためにパスワードを再入力します。

3. ローカルユーザーアカウントの二要素認証を有効にするには、「二要素 を有効にする」を選択します。

   > 注
   >
   > [**2** 要素を有効に する] オプションは、セカンダリ認証サーバーが構成されている場合にのみ表示されます。
   >
   > RADIUS または TACAS + 認証のいずれかのセカンダリ認証サーバーを構成します。ユーザーアカウントがセカンダリ認証サーバーで構成されていることを確認します。詳しくは、「二次認証」を参照してく

> ださい。

4. [追加] をクリックします。新しいユーザーアカウントが作成され、アカウント情報が [ユーザー] テーブルに追加されます。

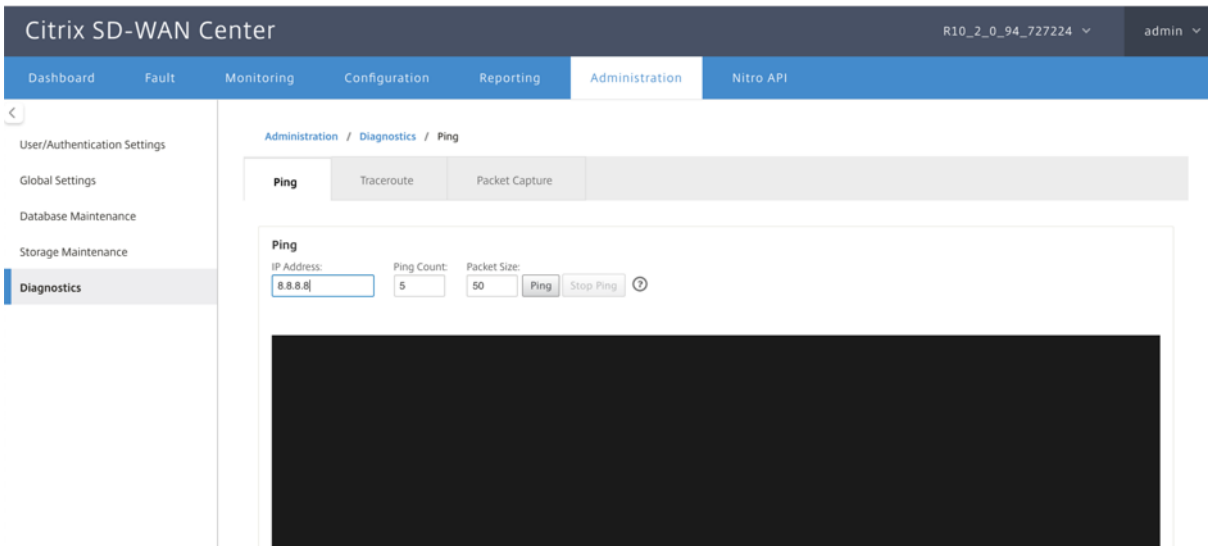
> 注
>
> Citrix SD-WAN Center は、最大 600 人のローカルユーザーを持つことができます。

診断

April 9, 2021

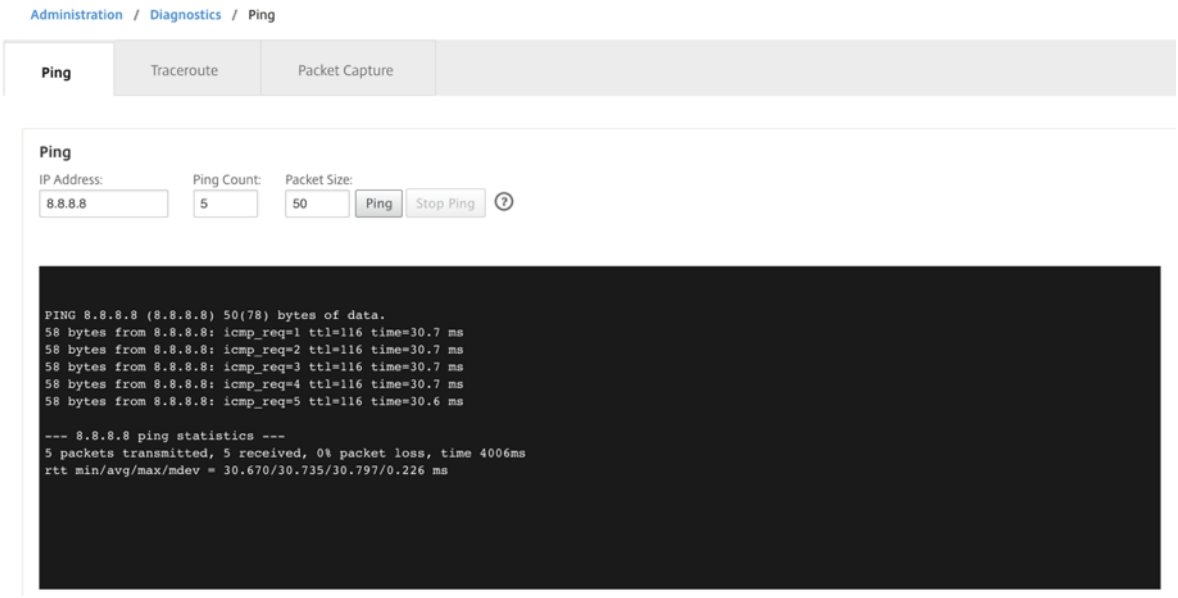
Citrix SD-WAN Center 診断 ユーティリティは、Citrix SD-WAN Center アプライアンスの接続問題をテストおよび調査するための Ping、Traceroute、およびパケットキャプチャ機能を提供します。**Citrix SD-WAN Center** ダッシュボード の診断オプションは、データ収集を制御します。

診断ツールを使用するには、管理 **>** 診断 に移動します。



Ping

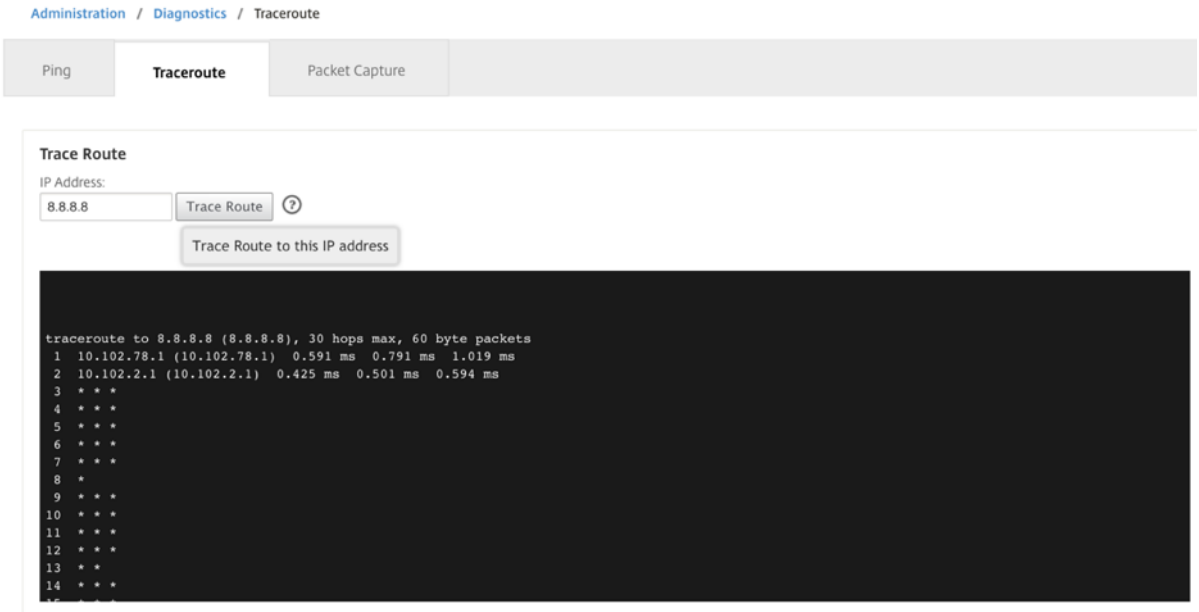
Ping オプションを使用して、SD-WAN Center ネットワークの任意の管理 IP アドレスに ping できます。



有効な IP アドレスを、ping カウントの数（ping 要求を送信する回数）およびパケットサイズ（データバイト数）とともに提供します。現在進行中の ping 検索を停止する 停止の **Ping** を クリックしてください。

Traceroute

Traceroute オプションを使用して、IP アドレスに確実に到達できるようにします。ルートを表示し、パケットの通過遅延を測定することにより、ネットワーク内の任意の管理 IP アドレスをトレースルートできます。

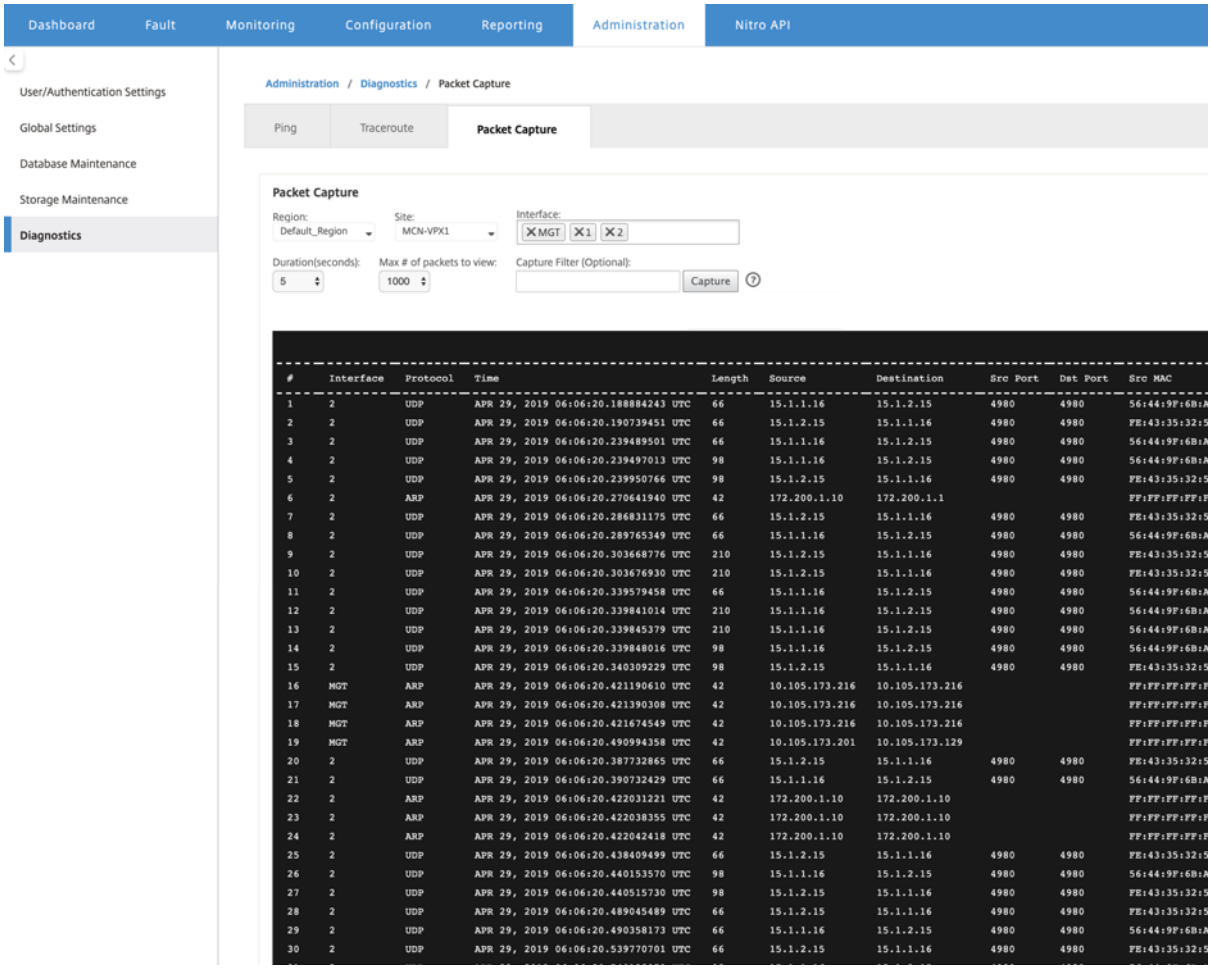


ルートをトレースするには、有効な管理 IP アドレスを入力してください。[経路をトレース] をクリックします。

> 注:
>
> traceroute の結果には、最大 30 ホップが表示されます。

Packet capture

パケットキャプチャ オプションを使用して、選択したサイトに存在する選択したアクティブなインターフェースを通過するデータパケットをインターセプトします。



パケットキャプチャ操作に次の入力を提供します。

- 地域 -ドロップダウンリストから、SD-WAN Center によって管理される地域を選択します。
- サイト -選択した地域で利用可能なサイト。ドロップダウンリストからサイトを選択します。
- インターフェース -アクティブなインターフェースは、選択したサイトでのパケットキャプチャに使用できます。ドロップダウンリストからインターフェイスを選択するか、インターフェイスを追加します。少なくとも 1 つのインターフェイスを選択して、パケットキャプチャをトリガーします。

> 注:
>
> すべてのインターフェイスで同時にパケットキャプチャを実行する機能は、トラブルシューティングタスクのスピードアップに役立ちます。

- 期間（秒）–データをキャプチャする必要のある期間（秒単位）。
- マックス # パケットキャプチャ結果のビューへのパケットの最大限界- ビューへのパケット。
- キャプチャフィルター（オプション） -オプションの [キャプチャフィルター] フィールドは、キャプチャするパケットを決定するために使用されるフィルター文字列を受け入れます。パケットはフィルター文字列と比較され、比較結果が true の場合、パケットがキャプチャされます。フィルターが空の場合、すべてのパケットがキャプチャされます。詳しくは、「キャプチャフィルター」を参照してください。

  このキャプチャフィルターの例を以下に示します。

  - **Ether proto\ARP** -ARP パケットのみをキャプチャします
  - **Ether proto\IP**-IPv4 パケットのみをキャプチャします
  - **VLAN 100** -100
    の VLAN パケットのみをキャプチャします - ホスト **10.40.10.20-** アドレス 10.40.10.20 のホストとの間の IPv4 パケットのみをキャプチャします
  - **Net 10.40.10.0 Mask 255.255.255.0** -IPv4 パケットのみをキャプチャします 10.40.10.0/24 サブネット
  - **IP** プロト \ TCP -キャプチャのみ IPv4/TCP パケット
  - ポート **80-**ポート **80** との間の IP パケットのみをキャプチャします
  - ポート範囲 **20**～**30-**ポート **20**～**30** との間の IP パケットのみをキャプチャします
  - ホスト **10.40.10.20** およびポート **80** と **TCP-**ホスト **10.40.10.20** の **TCP** ポート **80** との間の IP パケットのみをキャプチャします

> 注:
>
> キャプチャファイルの最大サイズ制限は最大 575 MB です。パケットキャプチャファイルがこのサイズに達すると、パケットキャプチャは停止します。

[キャプチャ] をクリックして、パケットキャプチャ結果を表示します。