



Citrix SD-WAN プラットフォーム

Machine translated content

Disclaimer

このコンテンツの正式なバージョンは英語で提供されています。Citrix ドキュメントのコンテンツの一部は、お客様の利便性のみを目的として機械翻訳されています。Citrix は機械翻訳されたコンテンツを管理していないため、誤り、不正確な情報、不適切な用語が含まれる場合があります。英語の原文から他言語への翻訳について、精度、信頼性、適合性、正確性、またはお使いの Citrix 製品またはサービスと機械翻訳されたコンテンツとの整合性に関する保証、該当するライセンス契約書またはサービス利用規約、あるいは Citrix とのその他すべての契約に基づき提供される保証、および製品またはサービスのドキュメントとの一致に関する保証は、明示的か黙示的かを問わず、かかるドキュメントの機械翻訳された範囲には適用されないものとします。機械翻訳されたコンテンツの使用に起因する損害または問題について、Citrix は責任を負わないものとします。

Contents

製品データシート	3
Platform Editions	3
WANOP	4
Citrix SD-WAN 800、1000、2000、3000 WANOP アプライアンス	4
Citrix SD-WAN WANOP 800	5
Citrix SD-WAN WANOP 1000	7
Citrix SD-WAN WANOP 2000	11
Citrix SD-WAN WANOP 3000	12
ハードウェア仕様の概要	14
Citrix SD-WAN 800、1000、2000、3000 WANOP アプライアンス	17
Windows Server 搭載の SD-WAN 1000 アプライアンス	18
Windows Server を搭載した SD-WAN 2000 アプライアンス	19
イーサネットポート名	20
サポートされる機能	21
ハードウェア仕様の概要	22
Citrix SD-WAN 4100 および 5100 WANOP アプライアンス	24
アーキテクチャ	25
SD-WAN 4100 WANOP	29
SD-WAN 5100 WANOP	31
ハードウェア仕様の概要	32
SD-WAN WANOP 4100/5100 アプライアンスの管理ポートが点灯する	33
トラブルシューティングのヒント	36
サポートされる機能	41

Standard Edition	42
ハードウェアのインストール	42
Citrix SD-WAN 110 Standard Edition アプライアンス	47
Citrix SD-WAN 210 Standard Edition アプライアンス	64
ハードウェア仕様の概要	74
Citrix SD-WAN 400 および 410 Standard Edition アプライアンス	77
Citrix SD-WAN 400 SE	78
Citrix SD-WAN 410 SE	79
ハードウェア仕様の概要	81
Citrix SD-WAN 4000、4100、および 5100 Standard Edition アプライアンス	82
Citrix SD-WAN 4000 SE	83
Citrix SD-WAN 4100 SE	84
Citrix SD-WAN 5100 SE	86
ハードウェア仕様の概要	88
Citrix SD-WAN 1000、2000、および 2100 の Standard Edition アプライアンス	89
Citrix SD-WAN 1000 SE	90
Citrix SD-WAN 2000 SE	94
Citrix SD-WAN 2100 SE	96
ハードウェア仕様の概要	98
6100 スタンダードエディションおよびプレミアムエディションアプライアンス	100
Citrix SD-WAN 1100 Standard Edition および Premium Edition	103
工場出荷時リセット	108
Premium (Enterprise) Edition	110
Citrix SD-WAN 1000、2000、および 2100 Premium (Enterprise) Edition アプライアンス	110

Citrix SD-WAN 2100 PE (EE) アプライアンス	111
SD-WAN 2000 PE (EE) アプライアンス	112
Citrix SD-WAN 1000 PE (EE) アプライアンス	113
ハードウェア仕様の概要	118
イーサネットポート名	120
アプライアンスのインストール	120
アプライアンスのラックマウント	121
アプライアンスのラックマウント	121
ケーブルの接続	121
アプライアンスのスイッチを入れる	123
初期構成	123
前提条件	124
コンピュータをイーサネットポートに接続してアプライアンスを構成する	124
シリアルコンソールを介した管理 IP アドレスの割り当て	128
SD-WAN アプライアンスの設定	130
Citrix SD-WAN 5100 Premium (Enterprise) Edition アプライアンス	130
Citrix SD-WAN 5100 PE	130
ハードウェア仕様の概要	132
VPX モデル	133
Citrix SD-WAN VPX Standard Edition	133
前提条件	135
チェックリスト	137
Citrix SD-WAN VPX-SE と VPX-WANOP	137
VPX のインストールと展開の概要	139

VPX-SE/VPXL-SE プラットフォームごとの仮想イーサネットポート	140
ESXi の VPX Standard Edition	140
クライアントをインストールする	141
SD-WAN VPX を展開する	143
管理 IP の構成	151
SD-WAN VPX への接続と展開のテスト	163
SD-WAN VPX の使用シナリオ	165
システム要件とプロビジョニング	167
XenServer への SD-WAN 仮想アプライアンスのインストール	170
XenServer 6.5 Upgrade for SD-WAN Standard Edition アプライアンス	173
VMware ESX での SD-WAN 仮想アプライアンスのインストール	174
HyperV 2012 R2 および 2016 のハイパーバイザーの SD-WAN Standard Edition 仮想アプライアンス (VPX)	179
Installing SD-WAN VPX on Microsoft Server 2008 R2	183
Installing SD-WAN VPX on the Microsoft Server 2012	185
Linux-KVM プラットフォームでの SD-WAN SE 仮想アプライアンス (VPX) のインストール	187
Google Cloud Platform に Citrix SD-WAN SE VPX をインストールする	190
Oracle クラウドインフラストラクチャ上の Citrix SD-WAN (テクニカルプレビュー)	204
SD-WAN VPX Standard Edition AMI を AWS にインストールする	206
Azure への Citrix SD-WAN VPX Standard Edition のインストール-リリースバージョン 9.3	218
Azure での Citrix SD-WAN Standard Edition インスタンスのデプロイ-リリースバージョン 10.2 以降	222
Citrix SD-WAN Standard Edition 仮想アプライアンス (VPX) の高可用性サポート	227
Azure の高可用性モードで SD-WAN Standard Edition インスタンスをデプロイ-リリースバージョン 9.3	232
Azure の高可用性モードで SD-WAN Standard Edition インスタンスをデプロイ-リリースバージョン 10.2 以降	236

Citrix ADC SDX アプライアンスに Citrix SD-WAN VPX インスタンスをデプロイする	239
クラウドウォッチサポート向け AWS の Standard Edition	243
Citrix SD-WAN VPX WANOP	244
Amazon AWS に SD-WAN WANOP エディション AMI をインストールする	244
AWS での SD-WAN WANOP エディション AMI の SNMP モニタリングの設定	251
AWS 上の SD-WAN WANOP Edition AMI インスタンスの制限および使用上のガイドライン	252
Microsoft Azure に SD-WAN WANOP VPX をデプロイする	253
一般的なハードウェアコンポーネント	258
フィールド交換可能ユニット	266
ポート	270
電源装置	271
ソリッドステートドライブ	275
ハードディスクドライブ	276
1G SFP トランシーバの取り付けと取り外し	277
10G SFP+ トランシーバの取り付けと取り外し	278
法令順守	280
台湾 BSMI RoHS ステートメント	281
ハードウェアの取り付け	282
インストールの準備	283
アプライアンスの解凍	283
現場とラックの準備	284
注意事項と警告	285
アプライアンスのラックマウント	287
ケーブルの接続	293

ポート 10/3 および 10/4 へのファイバパッチケーブルの取り付け	296
アプライアンスのスイッチを入れる	296

製品データシート

April 15, 2021

Citrix SD-WAN 製品のデータシートは、で入手できます www.citrix.co.jp。[製品] をクリックし、[ネットワーク] ボックスの一覧で [Citrix SD-WAN] を選択します。[プラットフォーム] で [SD-WAN プラットフォーム] を選択して、使用可能な SD-WAN プラットフォームの完全なリストを確認します。

Platform Editions

April 15, 2021

さまざまな Citrix SD-WAN ハードウェアプラットフォームは、さまざまな機能、通信ポート、および処理能力を提供します。すべての Citrix SD-WAN ハードウェアプラットフォームは、Citrix SD-WAN ソフトウェアをサポートしています。

重要:

NetScaler SD-WAN 製品は Citrix SD-WAN にリブランドされています。NetScaler SD-WAN という用語に関するすべての言及は、新しい製品用語 Citrix SD-WAN に適用されます。

Citrix SD-WAN Standard アプライアンスには、次のエディションがあります。

- SD-WAN スタンダードエディション 110、210、400、410
- SD-WAN スタンダードエディション 1000、1100、2000、および 2100
- SD-WAN スタンダードエディション 4000、4100、5100、および 6100

Citrix SD-WAN WANOP アプライアンスには、次のエディションが含まれます。

- SD-WAN WANOP 800、1000、2000、2100、3000
- SD-WAN WANOP 1000 WS と 2000 WS
- SD-WAN WANOP 4100 と 5100

Citrix SD-WAN Premium (Enterprise) アプライアンスには、次のエディションが含まれます。

- SD-WAN Premium (Enterprise) Edition 1000、1100、2000、2100
- SD-WAN プレミアム (エンタープライズ) エディション 5100、および 6100

パスワードの更新

10.2.6 リリース以降、アプライアンスと LOM パスワードは Citrix シリアルナンバーに設定されます。このシリアル番号は、アプライアンスの背面に表示されます。初回ログイン時にパスワードを変更します。

10.2.6 および 11.0.3 リリース以降では、SD-WAN アプライアンスのプロビジョニング時または新しい SD-WAN SE VPX の導入時に、デフォルトの管理者ユーザーアカウントパスワードを変更することが必須です。この変更は、CLI と UI の両方を使用して適用されます。

WANOP

April 15, 2021

重要:

NetScaler SD-WAN 製品は **CitrixSD-WAN** にリブランドされています。**NetScaler SD-WAN** という用語に関するすべての言及は、新しい製品用語 **Citrix SD-WAN** に適用されます。

Citrix SD-WAN WANOP アプライアンスには、次のエディションが含まれます。

- [SD-WAN WANOP 800、1000、2000、3000](#)
- [SD-WAN WANOP 1000 WS と 2000 WS](#)
- [SD-WAN WANOP 4100 と 5100](#)

Citrix SD-WAN 800、1000、2000、3000 WANOP アプライアンス

April 15, 2021

SD-WAN 800、1000、2000、3000 のアプライアンスは、データセンターや大規模なブランチオフィスで使用するための 1U アクセラレータです。

SD-WAN 2000 は、2つの加速ブリッジを備えた高速リピータ 8500 アプライアンスと考えることができます。一方、SD-WAN WANOP 3000 は、3つの加速ブリッジを備えた、より高速なリピータ 8800 と考えることができます。ただし、設定プロセスは同じではありません。ハイエンドのリピータ SDX アプライアンスと同様に、SD-WAN 2000 および WANOP 3000 アプライアンスは、XenServer ハイパーバイザーで実行される仮想マシンを高速化および管理に使用します。

- SD-WAN 800 シリーズ。中規模ブランチオフィスに適した小型 1U アプライアンス、800 シリーズは、2つの高速ブリッジを備え、最大 10 Mbps の WAN 速度をサポートします。
- SD-WAN 2000 シリーズ。大規模なブランチオフィスや小規模なデータセンターに適したフルサイズの 1U アプライアンス 2000 シリーズは、2つの高速ブリッジを備え、10 ~ 50 Mbps の WAN 速度をサポートします。
- SD-WAN 3000 シリーズ。最大規模のブランチオフィスおよび中規模のデータセンターに適したフルサイズの 1U アプライアンス、3000 シリーズは 3つの高速ブリッジを備え、50 ~ 155 Mbps の WAN 速度をサポートします。

Citrix コンプライアンス規制モデルは次のとおりです。

- SD-WAN 800 WANOP: CB 504-2

- SD-WAN 1000 WANOP: CB 504-2
- SD-WAN 2000 WANOP: NS 6xCU
- SD-WAN 3000 WANOP: NS 6xCU 6xSFP

すべての SD-WAN プラットフォームは、同様のコンポーネントを備えており、ハードウェアプラットフォームは幅広い機能、通信ポート、および処理能力を提供します。すべてのプラットフォームが SD-WAN ソフトウェアをサポートし、マルチコアプロセッサを備えています。これらのアプライアンスは同様のアーキテクチャを持ち、同じリリースバイナリを実行し、リリース 9.2 で完全にサポートされます。

Citrix SD-WAN WANOP 800

April 15, 2021

Citrix SD-WAN WANOP 800 プラットフォームには、デュアルコアプロセッサと 8 GB のメモリが搭載されています。プラットフォームの帯域幅は、それぞれ最大 6 Mbps、最大 10 Mbps です。

次の図は、SD-WAN WANOP 800 アプライアンスのフロントパネルを示しています。

図 1: Citrix SD-WAN 800、フロントパネル



- SD-WAN 800 アプライアンスの前面パネルには、電源ボタンと 5 つの LED があります。
- 電源ボタンにより、主電源 (電源への電源) のオン/オフが切り替わります。
- リセットボタンは、アプライアンスを再起動します。

LED は、アプライアンスのさまざまな部分に関する重要な情報を提供します。

- [Power Fail]: 電源装置に障害が発生したことを示します。
- 情報 LED: 次のことを示します。

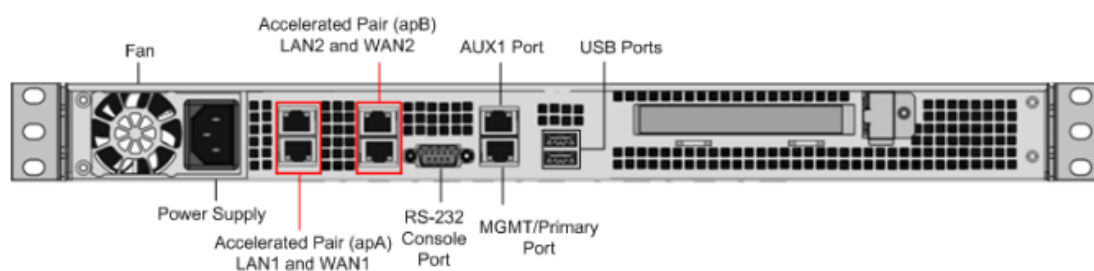
ステータス	説明
連続的にオンにして赤い	アプライアンスが過熱しています。(これは、ケーブルの輻輳が原因である可能性があります)。
赤で点滅 (1Hz)	ファンの障害。
赤で点滅 (0.25Hz)	電源障害。

ステータス	説明
青に点灯	ローカル UID がアクティブ化されました。この機能を使用して、ラックマウント環境でサーバを特定します。
青で点滅 (300 m/s)	リモート UID はオンです。この機能を使用して、リモートロケーションからサーバを識別します。

- NIC1 および NIC2: LAN1 ポートおよび WAN1 ポートでのネットワークアクティビティを示します。
- HDD: ハードディスクドライブのステータスを示します。
- [Power]: 点滅すると、電源装置に電力が供給され、正常に動作していることを示します。

次の図は、SD-WAN 800 アプライアンスの背面パネルを示しています。

図 2: Citrix SD-WAN 800 アプライアンス、背面パネル



SD-WAN 800 アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 冷却ファン
- 単一電源、定格 200 ワット、110~240 ボルト
- 加速ブリッジとして機能するイーサネットポート (apA および APB) のアクセラレーションペア。個々のポートの割り当て: LAN1 は Apa.1、WAN1 は Apa.2、LAN2 は APB.1、LAN2 は APB.2 です。
- RS-232 シリアル・コンソール・ポート
- AUX イーサネットポートと 1 つの管理ポート
- 2 つの USB ポート
- ソリッドステートドライブ (SSD) 1 つ
 - SD-WAN 800-240GB SSD

SD-WAN アプライアンスの初期設定を行うには、次のタスクを実行します。

- サイトで使用するようアプライアンスを構成します。
- Citrix ライセンスをインストールします。
- アクセラレーションを有効にします。
- トラフィックシェーピングを有効にします (インラインモードのみ)。

アプライアンスは、イーサネットポートまたはシリアルコンソールのいずれかを使用してアプライアンスをコンピュータに接続して設定できます。以下の手順では、イーサネットポートを介してアプライアンスをコンピュータに接続

してアプライアンスを構成できます。

シリアルコンソールを使用してアプライアンスをコンピューターに接続して構成する場合は、[シリアルコンソールを介した管理 IP アドレスの割り当て手順](#)を完了することで[アプライアンスのセットアップ](#)管理サービス IP アドレスを割り当てます。

Citrix SD-WAN WANOP 1000

April 15, 2021

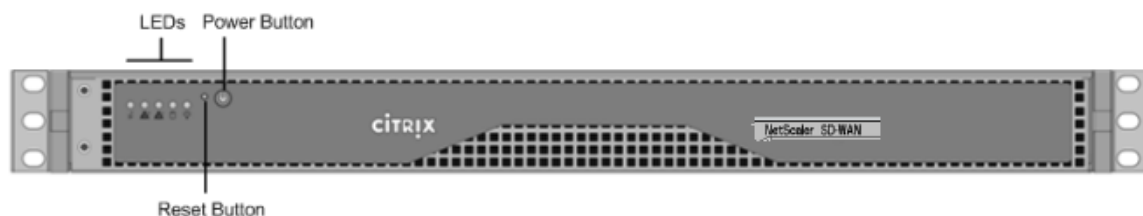
Citrix SD-WAN WANOP 1000 プラットフォームには、SD-WAN 1000-06、SD-WAN 1000-010、SD-WAN 1000-020 の 3 つのモデルがあり、帯域幅はそれぞれ 6Mbps、10Mbps、20Mbps である。各モデルは、1 つのクアッドコアプロセッサと 24 GB (GB) のメモリを搭載した 1U アプライアンスです。

次の図は、SD-WAN 1000 アプライアンスのフロントパネルを示しています。

Citrix SD-WAN WANOP 1000 アプライアンスのフロントパネルには、電源ボタンと 5 つの LED があります。

- 電源ボタンにより、主電源 (電源への電源) のオン/オフが切り替わります。
- リセットボタンは、アプライアンスを再起動します。
- LED は、アプライアンスのさまざまな部分に関する重要な情報を提供します。

図 1: Citrix SD-WAN WANOP 1000、フロントパネル

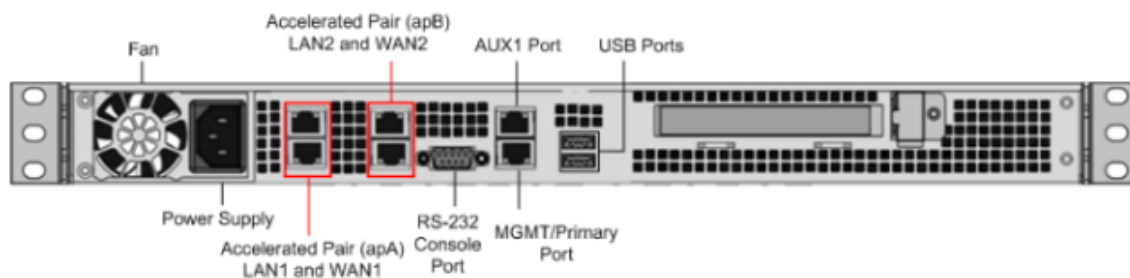


アプライアンスには次のポートがあります。

- RS232 シリアルコンソールポート。
- 銅線イーサネット (RJ45) 管理ポート。管理ポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。
- 4 つの 10/100/1000Base-T 銅線イーサネットポート。左から右に 1/1、1/2、1/3、および 1/4 の番号が付けられます。4 つのポートは 2 つの加速ペアを形成し、加速ブリッジとして機能します。ポート 1/1 および 1/2 はアクセラレーションペア A (apA)、1/3 および 1/4 はアクセラレーションペア B (APB) です。

次の図は、SD-WAN 1000 アプライアンスの背面パネルを示しています。

図 2: Citrix SD-WAN WANOP 1000 アプライアンス、背面パネル



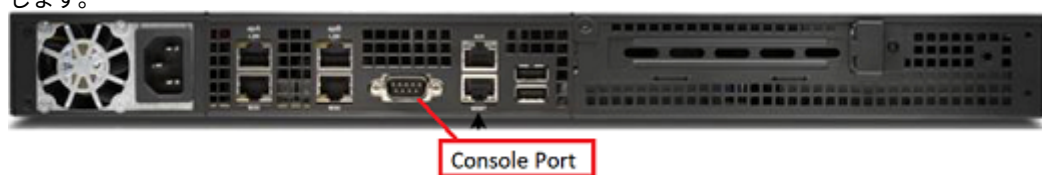
SD-WAN WANOP 1000 アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 600 GB リムーバブルソリッドステートドライブ。アプライアンスのソフトウェアとユーザーデータを格納します。
- USB ポート (将来のリリース用に予約)。
- 単一電源、定格 300 ワット、100-240 ボルト。

正常なシャットダウン後にアプライアンスの電源を入れます

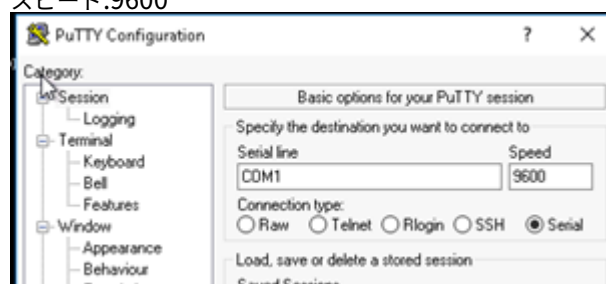
正常なシャットダウン後にアプライアンスを電源投入するには：

1. シリアル・コンソール・ケーブルを、アプライアンスの背面と管理用ラップトップのシリアル・ポートに接続します。

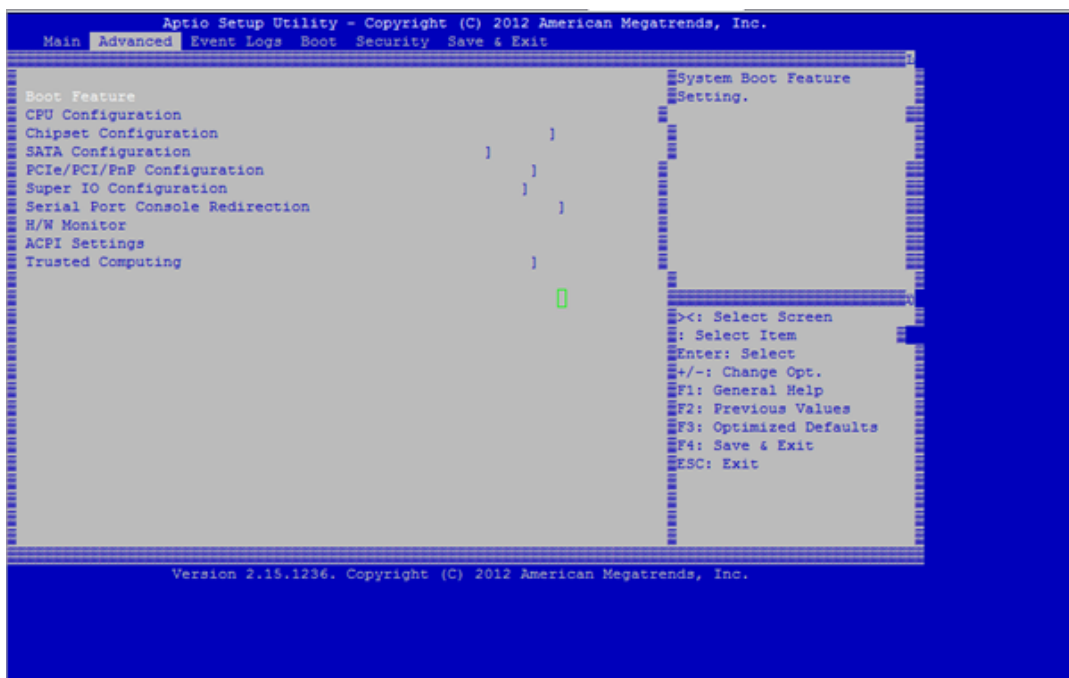


2. 管理ラップトップで、次の構成設定を使用してパテセッションを再起動します。

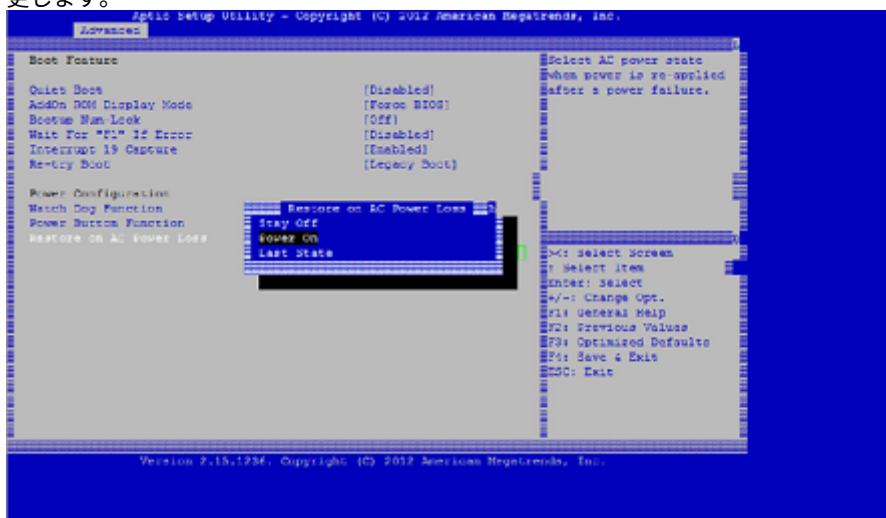
- シリアル回線:COM1
- スピード:9600



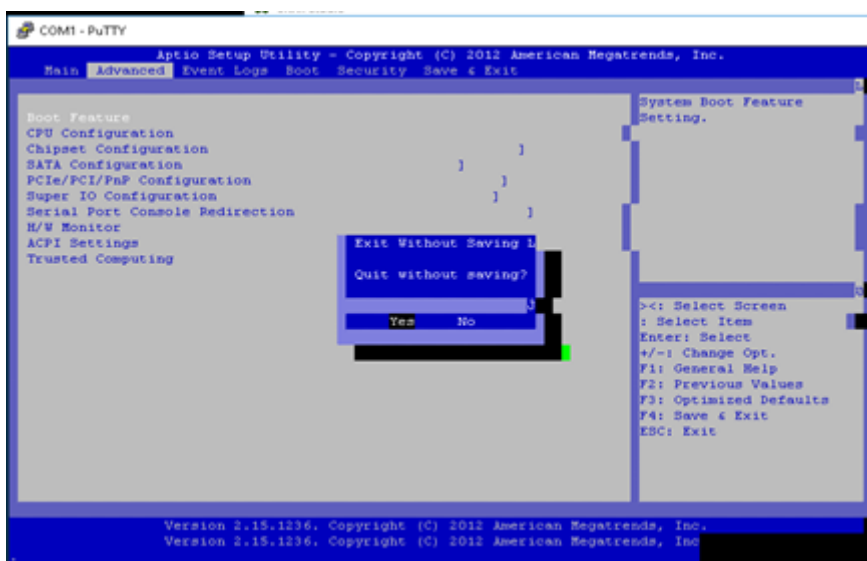
3. アプライアンスの電源を入れ、起動中に Putty セッションで次のキーを押して BIOS 設定画面に入ります。キー押し: **DEL**
4. BIOS で、
 - [詳細] タブ > [選択]
 - 起動機能 > 入力



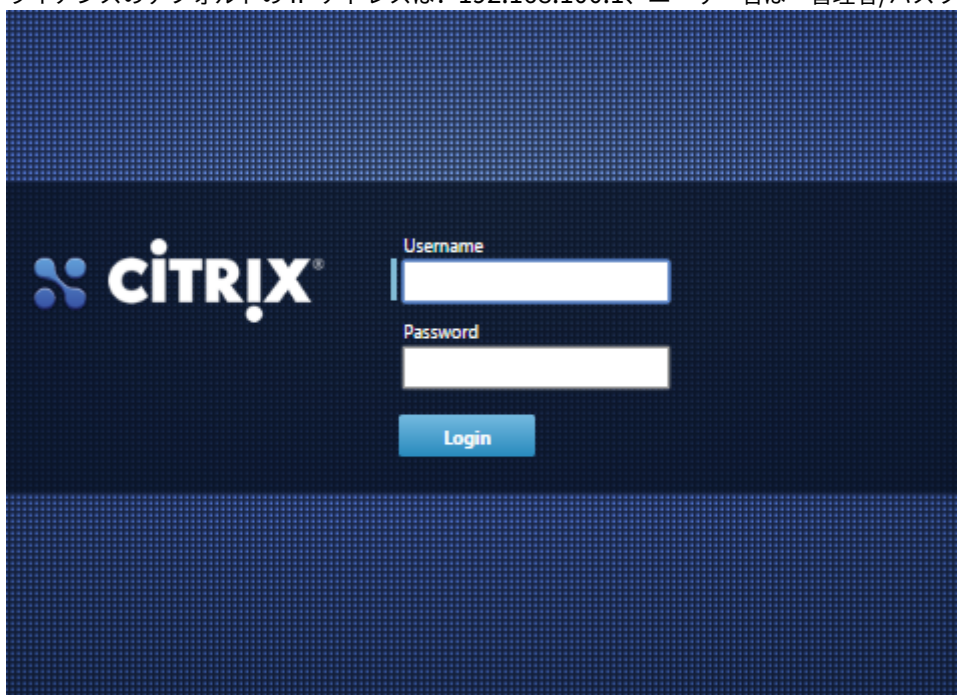
5. [起動機能] 画面で、[AC 電源切断時の復元] パラメータの値を [** 前回の状態 **] > [** 電源オン **] から変更します。



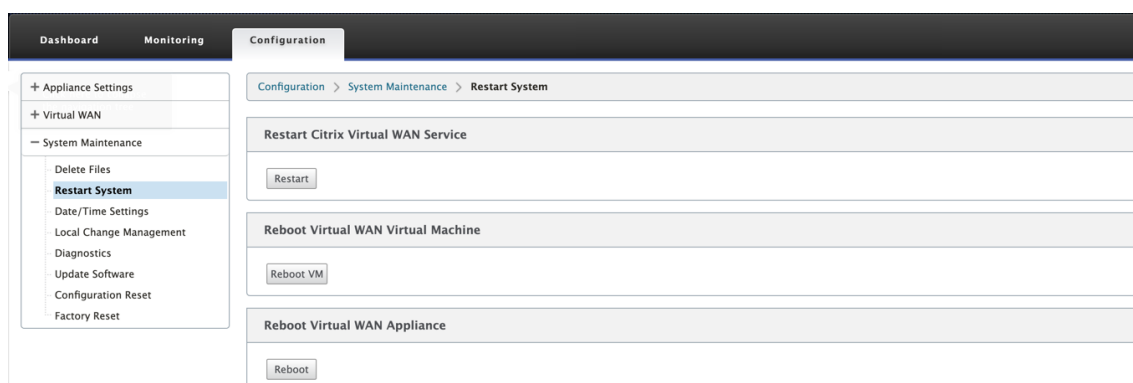
6. [保存して終了] に移動します。
- [** 変更を保存してリセット **] を選択します。
 - [はい]
- [システムの再起動を許可する] を選択します。これには約 5 分かかります。



7. アプライアンスの電源がオンになったら、アプライアンス管理インスタンス (SVM) にログインします。アプライアンスのデフォルトの IP アドレスは: 192.168.100.1、ユーザー名は「管理者/パスワード」です。



8. SD-WAN アプライアンスの GUI で、[構成] > [メンテナンス] > [アプライアンスの再起動] に移動します。アプライアンスが完全にシャットダウンできるようにします。シャットダウンプロセスが完了したら、アプライアンスに電源ライトがないことを確認します。



9. アプライアンスの電源をオンにして、BIOS 構成の変更が正常に適用されたことを確認します。これは、APC Intelligent PDU Web 管理コンソールを使用するか、シャットダウンした SD-WAN アプライアンスから電源ケーブルを物理的に引き出し、10 秒間待ってから再び差し込むことで実行できます。アプライアンスの電源は、すべてのシャットダウンシナリオから自動的に起動します。

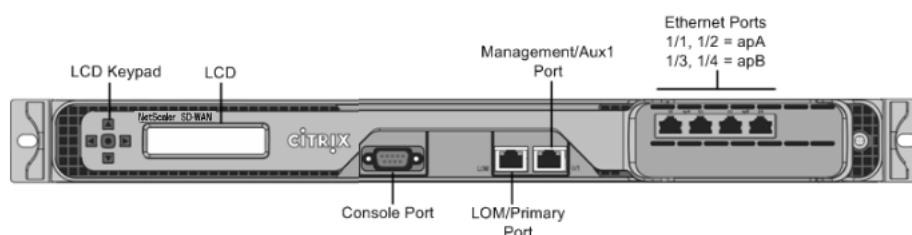
Citrix SD-WAN WANOP 2000

April 15, 2021

Citrix SD-WAN WANOP 2000 プラットフォームには、SD-WAN 2000-010、SD-WAN 2000-020、SD-WAN 2000-050 の 3 つのモデルがあり、帯域幅はそれぞれ 10Mbps、20Mbps、50Mbps である。各モデルは、1 つのクアッドコアプロセッサと 24 GB (GB) のメモリを搭載した 1U アプライアンスです。

次の図は、SD-WAN WANOP 2000 アプライアンスの前面パネルを示しています。

図 1: Citrix SD-WAN WANOP 2000、フロントパネル



アプライアンスには次のポートがあります。

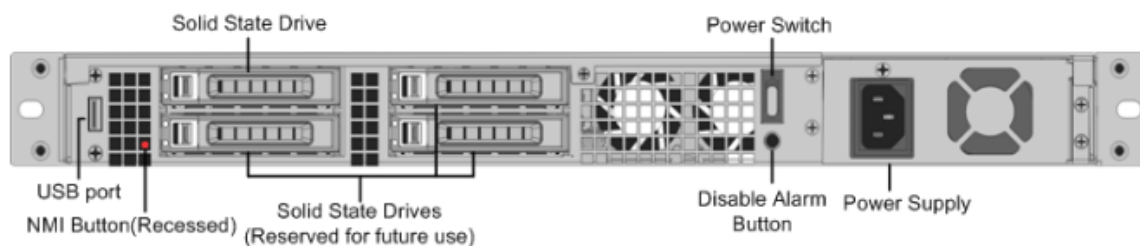
- RS232 シリアルコンソールポート。
- ライトアウト管理 (LOM) ポートと呼ばれる銅線イーサネット (RJ45) ポート。このポートを使用して、アプライアンスのソフトウェアとは無関係にアプライアンスをリモートで監視および管理できます。
- 0/1 の番号が付いた銅線イーサネット (RJ45) 管理ポート。管理ポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。

注: LOM ポートは、管理ポートとしても動作します。

- 4つの 10/100/1000Base-T 銅線イーサネットポート。左から右に 1/1、1/2、1/3、および 1/4 の番号が付けられます。4つのポートは2つの加速ペアを形成し、加速ブリッジとして機能します。ポート 1/1 および 1/2 はアクセラレーションペア A (apA)、1/3 および 1/4 はアクセラレーションペア B (APB) です。

次の図は、SD-WAN 2000 アプライアンスの背面パネルを示しています。

図 2: Citrix SD-WAN WANOP 2000 アプライアンス、背面パネル



SD-WAN 2000 アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 600 GB リムーバブルソリッドステートドライブ。アプライアンスのソフトウェアとユーザーデータを格納します。
- 電源スイッチ。アプライアンスへの電源を切ります。スイッチを 5 秒間押して、電源を切ります。
- USB ポート (将来のリリース用に予約)。
- 非マスク割り込み (NMI) ボタン。テクニカルサポートの要求に応じてコアダンプを生成するために使用する。この赤いボタンを押すには、ペン、鉛筆、またはその他の尖ったオブジェクトを使用する必要があります。このボタンは、意図しない起動を防ぐためにくぼんだ状態になっています。
- 300 ワット、100~240 ボルトの単一電源。

Citrix SD-WAN WANOP 3000

April 15, 2021

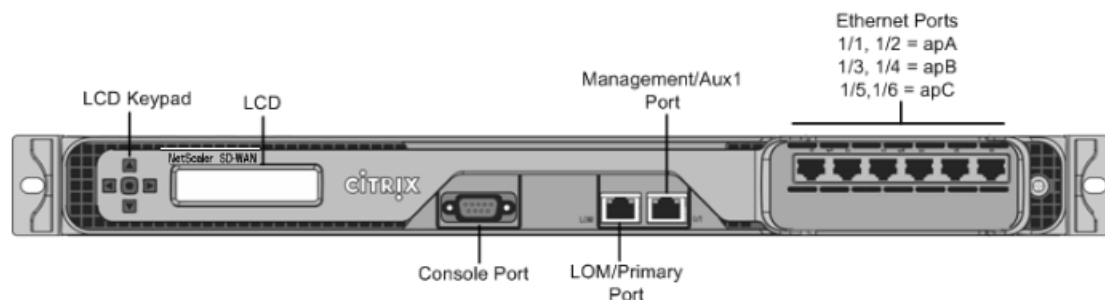
Citrix SD-WAN WANOP 3000 プラットフォームには、SD-WAN 3000-050、SD-WAN 3000-100、SD-WAN 3000-155 の 3 つのモデルがあり、帯域幅はそれぞれ 50Mbps、100Mbps、155Mbps である。各モデルは、1 つのクアッドコアプロセッサと 32 GB (GB) のメモリを搭載した 1U アプライアンスです。

Citrix SD-WAN WANOP 3000 アプライアンスは、次の 2 つのポート構成で使用できます。

- 6 つの 10/100/1000 ベース-T 銅線イーサネットポート
- 1G SX ファイバポート ×4

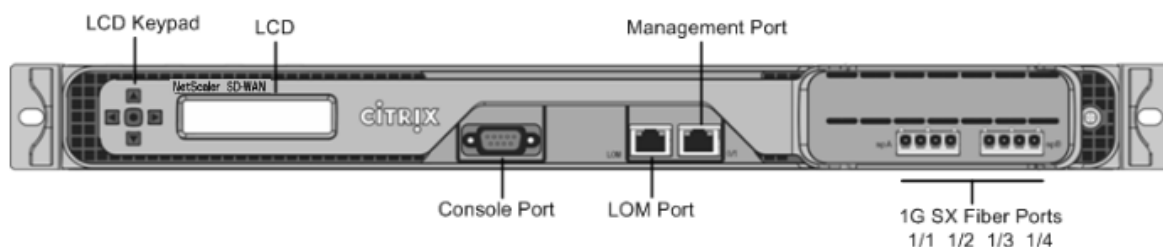
次の図は、6 つの 10/100/1000 ベース-T 銅線イーサネットポートを備えた SD-WAN 3000 の前面パネルを示しています。

図 1: Citrix SD-WAN WANOP 3000 (6×10/100/1000 ベース-T 銅線イーサネットポート)、フロントパネル



次の図は、4つの1G SXファイバポートを備えたSD-WAN 3000アプライアンスの前面パネルを示しています。

図 2: Citrix SD-WAN WANOP 3000 (4×1G SX ファイバポート)、フロントパネル



アプライアンスには次のポートがあります。

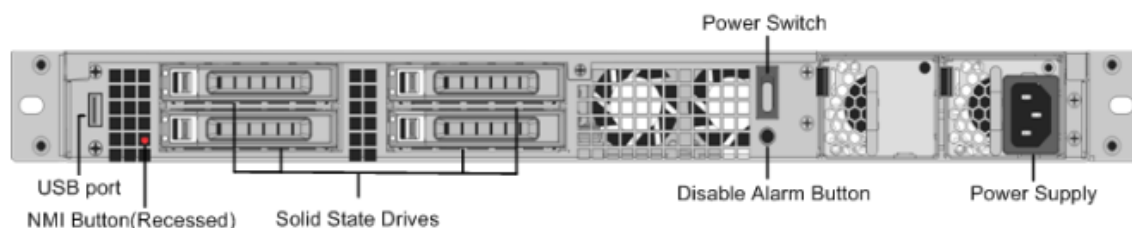
- RS232 シリアルコンソールポート。
- ライトアウト管理 (LOM) ポートと呼ばれる銅線イーサネット (RJ45) ポート。このポートを使用して、アプライアンスのソフトウェアとは無関係にアプライアンスをリモートで監視および管理できます。
- 0/1 の番号が付いた銅線イーサネット (RJ45) 管理ポート。管理ポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。

注: LOM ポートは、管理ポートとしても動作します。

- 次のいずれかの構成で、ネットワークポート:
 - SD-WAN 3000 (6×10/100/1000 ベース-T 銅線イーサネットポート) 1/1、1/2、1/3、1/4、1/5、および 1/6 の番号が左から右に 6 つの 10/100/1000 ベース-T 銅線イーサネットポート 6 つのポートは 3 つの加速ペアを形成し、加速ブリッジとして機能します。ポート 1/1 および 1/2 はアクセラレーションペア A (apA)、1/3 および 1/4 はアクセラレーションペア B (APB)、1/5 および 1/6 はアクセラレーションペア C (APC) です。
 - SD-WAN 3000 (1G SX ファイバポート×4)。1/1、1/2、1/3、1/4 の番号が付いた 4 つの 1G SX ファイバポート (左から右) 4 つのポートは 2 つの加速ペアを形成し、加速ブリッジとして機能します。ポート 1/1 および 1/2 はアクセラレーションペア A (apA)、1/3 および 1/4 はアクセラレーションペア B (APB) です。

次の図は、SD-WAN WANOP 3000 アプライアンスの背面パネルを示しています。

図 3: Citrix SD-WAN WANOP 3000 アプライアンス、背面パネル



SD-WAN WANOP 3000 アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 600 GB リムーバブルソリッドステートドライブ ×4 左上のソリッドステートドライブには、アプライアンスのソフトウェアとユーザーデータの両方が格納されます。他の 3 つはユーザーデータのみを格納します。
- 電源スイッチ。アプライアンスへの電源をオンまたはオフにします。電源を切るには、スイッチを 5 秒間押します。
- USB ポート (将来のリリース用に予約)。
- 非マスク割り込み (NMI) ボタン。テクニカルサポートの要求に応じてコアダンプを生成するために使用する。この赤いボタンを押すには、ペン、鉛筆、またはその他の尖ったオブジェクトを使用する必要があります。このボタンは、意図しない起動を防ぐためにくぼんだ状態になっています。
- アラームボタンを無効にする。これは、2 台目の電源装置を取り付けない限り機能しません。この場合、アプライアンスが 1 つの電源コンセントにのみ接続されている場合、またはいずれかの電源装置に障害が発生した場合に鳴るアラームが無効になります。
- 単一電源、定格 450 ワット、100~240 ボルト。

ハードウェア仕様の概要

April 15, 2021

次の表は、Citrix SD-WAN WANOP 800、1000、2000、および 3000 ハードウェアプラットフォームの仕様をまとめたものです。

表 1. Citrix SD-WAN WANOP 800、2000、1000、および 3000 プラットフォームの概要

プラットフォームのパフォーマンス

ハードウェア仕様	SD-WAN WANOP 800	SD-WAN WANOP 1000	SD-WAN WANOP 2000	SD-WAN WANOP 3000	
帯域幅	最大 6 Mbps	最大 10 Mbps	モデル 1000-006:6 Mbps	モデル 2000-010:10 Mbps	モデル 3000-050:50 Mbps

ハードウェア仕様	SD-WAN WANOP 800	SD-WAN WANOP 1000	SD-WAN WANOP 2000	SD-WAN WANOP 3000	
	モデル 400-002:2Mbps	モデル 800-002:2Mbps	モデル 1000-010:10 Mbps	モデル 2000-020:20 Mbps	モデル 3000-100:100 Mbps
	モデル 400-006:6 Mbps	モデル 800-006:6 Mbps	モデル 1000-020:20 Mbps	モデル 2000-050:50 Mbps	モデル 3000-155:155 Mbps
		モデル 800-010:10 Mbps			
HDX セッションの最大数	60 まで	100 まで	200	300	500
合計セッション数	500	10,000	10,000	20,000	50,000
アクセラレーションプラグイン CCU	-	-	-	750	1,000

ハードウェア仕様

ハードウェア仕様	SD-WAN WANOP 800	SD-WAN WANOP 1000	SD-WAN WANOP 2000	SD-WAN WANOP 3000	
プロセッサ	2 コア	2 コア	2 コア	4 コア	4 コア
ディスク容量の合計	160 GB SSD × 1	240GB の SSD×1		1 x 600 GB SSD	600GB の SSD×4
SSD (専用圧縮履歴)	40GB	80 ギガバイト		275 GB	1.5TB
RAM	8GB	8GB	24 ギガバイト	32GB	
ネットワークインタフェース	バイパス 10/100/1000 と 2 ペア	バイパス 10/100/1000 と 2 ペア		10/100/1000 ベース-T 銅線イーサネット x 4	10/100/1000 ベース-T 銅線イーサネット x 6
トランシーバのサポート	いいえ	いいえ	はい	はい	
電源装置	1	1	1	1	

物理的寸法

ハードウェア仕様	SD-WAN WANOP 800	SD-WAN WANOP 1000	SD-WAN WANOP 2000	SD-WAN WANOP 3000
ラックユニット	1U	1U		1U
システム幅	19 インチラック用の EIA 310-D	19 インチラック用の EIA 310-D		19 インチラック用の EIA 310-D
システムの深さ	10.5" (26.7 cm)	10.5" (26.7 cm)		25.4" (64.5 cm)
システム重量	8 ポンド (3.5kg)	8 ポンド (3.5kg)		32 ポンド (14.5kg)
配送の寸法と重量	長さ 26 インチ x 幅 18.5 インチ x 高さ 6.5 インチ、14 ポンド。	長さ 26 インチ x 幅 18.5 インチ x 高さ 6.5 インチ、14 ポンド。	長さ 32× 幅 23.5× 高さ 7.5 インチ、39 ポンド。	長さ 32× 幅 23.5× 高さ 7.5 インチ、39 ポンド。

環境と規制

ハードウェア仕様	SD-WAN WANOP 800	SD-WAN WANOP 1000	SD-WAN WANOP 2000	SD-WAN WANOP 3000
電圧	100/240 VAC、50-60 Hz	100/240 VAC、50-60 Hz		100/240 VAC、50-60 Hz
消費電力 (最大)	200W	200W		300 W
動作温度 (摂氏)	10-35	10-35		0-40
非動作時温度 (摂氏)	-40-+70	-40-+70		-40-+70
許容相対湿度	8%-90%	8%-90%		5%-95%
安全認定	CSA/EN/IEC/UL 60950-1 準拠、UL または CSA リスト (米国およびカナダ)、CE マーキング (ヨーロッパ)	CSA/EN/IEC/UL 60950-1 準拠、UL または CSA リスト (米国およびカナダ)、CE マーキング (ヨーロッパ)		CSA TUV

ハードウェア仕様	SD-WAN WANOP 800	SD-WAN WANOP 1000	SD-WAN WANOP 2000	SD-WAN WANOP 3000	
電磁界および感受性の認定	FCC (パート 15 クラス A)、EN 55022 クラス A、EN 61000-3-2/-3-3、CISPR 22 クラス A	FCC (パート 15 クラス A)、EN 55022 クラス A、EN 61000-3-2/-3-3、CISPR 22 クラス A	FCC (パート 15 クラス A)、EN 55022 クラス A、EN 61000-3-2/-3-3、CISPR 22 クラス A	FCC (Part 15 Class A)、CE、C-Tick、VCCI-A、CCC、KCC、NOM、SASO、SABS、PCT	FCC (Part 15 Class A)、CE、C-Tick、VCCI-A、CCC、KCC、NOM、SASO、SABS、PCT
環境認証	ROHS、ウィー	ROHS、ウィー	ROHS、ウィー	ROHS、ウィー	ROHS、ウィー

Citrix SD-WAN 800、1000、2000、3000 WANOP アプライアンス

April 15, 2021

SD-WAN 800、1000、2000、3000 のアプライアンスは、データセンターや大規模なブランチオフィスで使用するための 1U アクセラレータです。

SD-WAN 2000 は、2 つの加速ブリッジを備えた高速リピータ 8500 アプライアンスと考えることができます。一方、SD-WAN WANOP 3000 は、3 つの加速ブリッジを備えた、より高速なリピータ 8800 と考えることができます。ただし、設定プロセスは同じではありません。ハイエンドのリピータ SDX アプライアンスと同様に、SD-WAN 2000 および WANOP 3000 アプライアンスは、XenServer ハイパーバイザーで実行される仮想マシンを高速化および管理に使用します。

- SD-WAN 800 シリーズ。中規模ブランチオフィスに適した小型 1U アプライアンス、800 シリーズは、2 つの高速ブリッジを備え、最大 10 Mbps の WAN 速度をサポートします。
- SD-WAN 2000 シリーズ。大規模なブランチオフィスや小規模なデータセンターに適したフルサイズの 1U アプライアンス 2000 シリーズは、2 つの高速ブリッジを備え、10 ~ 50 Mbps の WAN 速度をサポートします。
- SD-WAN 3000 シリーズ。最大規模のブランチオフィスおよび中規模のデータセンターに適したフルサイズの 1U アプライアンス、3000 シリーズは 3 つの高速ブリッジを備え、50 ~ 155 Mbps の WAN 速度をサポートします。

Citrix コンプライアンス規制モデルは次のとおりです。

- SD-WAN 800 WANOP: CB 504-2
- SD-WAN 1000 WANOP: CB 504-2
- SD-WAN 2000 WANOP: NS 6xCU
- SD-WAN 3000 WANOP: NS 6xCU 6xSFP

すべての SD-WAN プラットフォームは、同様のコンポーネントを備えており、ハードウェアプラットフォームは幅

広い機能、通信ポート、および処理能力を提供します。すべてのプラットフォームが SD-WAN ソフトウェアをサポートし、マルチコアプロセッサを備えています。これらのアプライアンスは同様のアーキテクチャを持ち、同じリリースバイナリを実行し、リリース 9.2 で完全にサポートされます。

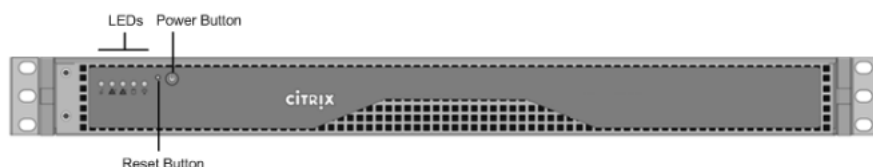
Windows Server 搭載の SD-WAN 1000 アプライアンス

April 15, 2021

Windows Server プラットフォームを搭載した Citrix SD-WAN 1000 には、クアドコアプロセッサと 32 GB のメモリが搭載されています。このプラットフォームの帯域幅は最大 20 Mbps です。

次の図は、Windows サーバを備えた SD-WAN 1000 アプライアンスのフロントパネルを示しています。

図 1: Windows Server 搭載の Citrix SD-WAN 1000、フロントパネル



Windows サーバアプライアンス搭載の SD-WAN 1000 の前面パネルには、電源ボタンと 5 つの LED があります。

電源ボタンは、アプライアンスのオン/オフを切り替えるために使用します。

リセットボタンは、アプライアンスを再起動します。

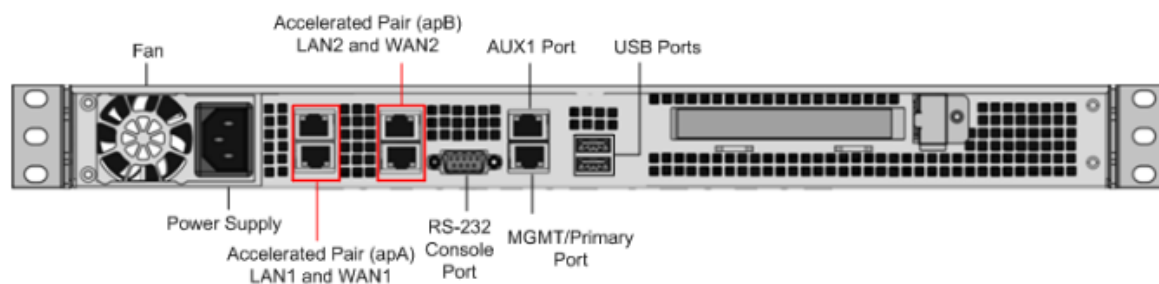
LED は、アプライアンスのさまざまな部分に関連する重要な情報を提供します。

- [Power Fail]: 電源装置に障害が発生したことを示します。
- 情報 LED — 次のことを示します。

ステータス	説明
— —	連続的に点灯し、赤 アプライアンスが過熱しています。(これは、ケーブルの輻輳が原因である可能性があります)。
赤で点滅 (1Hz)	ファンの障害、動作していないファンがないか確認。
赤で点滅 (0.25Hz)	電源障害、動作していない電源を確認します。
青に点灯	ローカル UID がアクティブになりました。この機能を使用して、ラックマウント環境でサーバを特定します。
青で点滅 (300 m/s)	リモート UID はオン。この機能を使用して、リモートロケーションからサーバを識別します。
- NIC1 および NIC2: LAN1 ポートおよび WAN1 ポートでのネットワークアクティビティを示します。
- HDD — ハードディスクドライブのステータスを示します。
- [Power]: 電源装置に電力が供給され、正常に動作していることを示します。

次の図は、Windows サーバを備えた SD-WAN 1000 アプライアンスの背面パネルを示しています。

図 2: Windows Server を搭載した Citrix SD-WAN 1000 アプライアンス、背面パネル



Windows Server 搭載の SD-WAN 1000 アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 冷却ファン
- 単一電源、定格 200 ワット、110-240 ボルト
- 加速ブリッジとして機能するイーサネットポートの加速ペア（apA および APB）
- RS-232 シリアル・コンソール・ポート
- AUX イーサネットポートと 1 つの管理ポート
- 2 つの USB ポート

Windows Server を搭載した SD-WAN 2000 アプライアンス

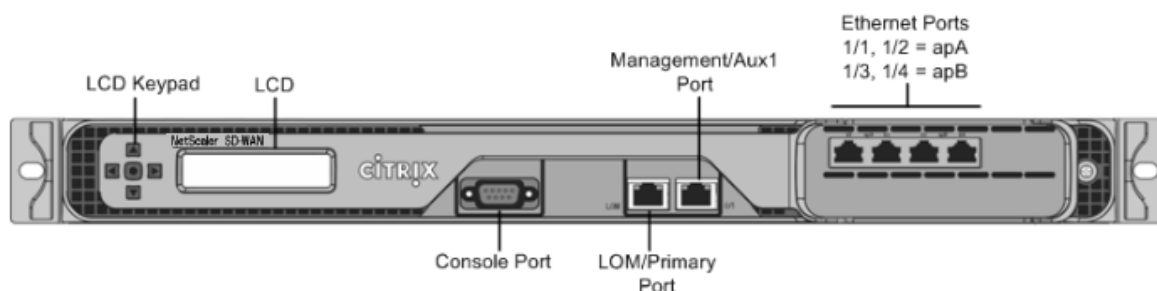
April 15, 2021

Windows Server プラットフォームを搭載した Citrix SD-WAN 2000 は、1 つのクアドコアプロセッサと 24 ギガバイト（GB）のメモリを搭載した 1U アプライアンスです。

次の図は、Windows サーバを備えた SD-WAN 2000 アプライアンスのフロントパネルを示しています。

図 1: Windows Server を搭載した Citrix SD-WAN 2000 アプライアンス、フロントパネル

注: Windows サーバに apA ポートを割り当てることはできません。ただし、AUX ポートを Windows Server に割り当てることができます。



Windows サーバを備えた SD-WAN 2000 アプライアンスには、次のポートがあります。

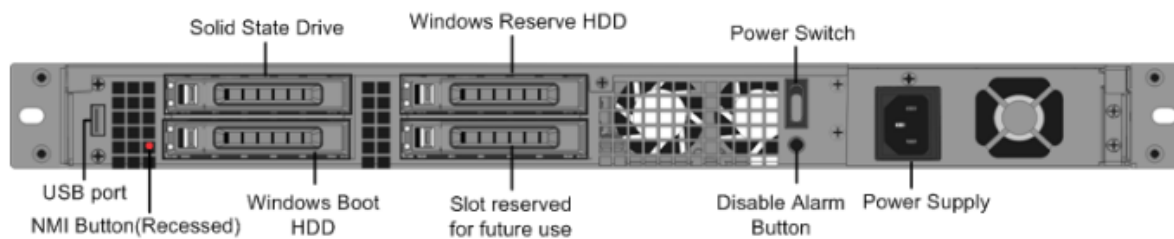
- RS232 シリアルコンソールポート。
- ライトアウト管理 (LOM) ポートと呼ばれる銅線イーサネット (RJ45) ポート。このポートを使用して、アプライアンスのソフトウェアとは無関係にアプライアンスをリモートで監視および管理できます。
- 銅線イーサネット (RJ45) 管理ポート。番号が 0/1 で、PRI (プライマリ) という名前が付いています。管理ポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。このポートは、WAN 最適化および Windows Server の初期プロビジョニングに使用できます。

注: LOM ポートは、管理ポートとしても動作します。

- 4 つの 10/100/1000Base-T 銅線イーサネットポート。左から右に 1/1、1/2、1/3、および 1/4 の番号が付けられます。4 つのポートは 2 つの加速ペアを形成し、加速ブリッジとして機能します。ポート 1/1 および 1/2 はアクセラレーションペア A (apA)、1/3 および 1/4 はアクセラレーションペア B (APB) です。

次の図は、Windows サーバを備えた SD-WAN 2000 アプライアンスの背面パネルを示しています。

図 2: Windows Server を搭載した Citrix SD-WAN 2000 アプライアンス、背面パネル



Windows サーバ搭載の SD-WAN 2000 アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 600 GB リムーバブルソリッドステートドライブ。アプライアンスのソフトウェアとユーザーデータを格納し、1 TB のハードディスクドライブを格納します。
- 電源スイッチ。アプライアンスへの電源をオンまたはオフに切り替えます。スイッチを 5 秒間押して、電源を切ります。
- USB ポート (将来のリリース用に予約)。
- 非マスク割り込み (NMI) ボタン。テクニカルサポートの要求に応じてコアダンプを生成するために使用する。この赤いボタンを押すには、ペン、鉛筆、またはその他の尖ったオブジェクトを使用する必要があります。このボタンは、意図しない起動を防ぐためにくぼんだ状態になっています。
- 300 ワット、100~240 ボルトの単一電源。

イーサネットポート名

April 15, 2021

アプライアンスを設定するときは、アプライアンスのさまざまなイーサネットポートの IP アドレスを指定する必要があります。次の表に示すように、イーサネットポートの名前は、Windows Server を使用する Citrix SD-WAN

1000 および 2000 アプライアンスのフロントパネル、Citrix SD-WAN インスタンス、および Windows サーバーでは異なる名前が付けられます。

SD-WAN 1000WS	SD-WAN 2000WS	SD-WAN インスタンス	Windows Server
管理管理 (青)	0/1 (LOM/PRI)	プライマリ	Citrix PV イーサネットアダプタ #0:0/1
AUX	0/2 (AUX)	Aux	Citrix PV イーサネットアダプタ #1:0/2
apA LAN1/WCCP (Green)	1/1	apA.1	-
apA WAN1	1/2	APA.2	-
APB LAN2	1/3	apB.1*	デスクトップアイコン nic_mapping.vbs をダブルクリックしてマッピングを表示します **
apB WAN2	1/4	apB.2*	デスクトップアイコン nic_mapping.vbs をダブルクリックしてマッピングを表示します **

* SD-WAN インスタンスでは、4 ポートモードでのみ使用できます。

** Windows サーバでは、2 ポートモードでのみ使用できます。

サポートされる機能

April 15, 2021

次の表は、Windows Server の SD-WAN 1000 および 2000 アプライアンスでサポートされるさまざまな機能の一覧です。

Windows Server シリーズアプライアンスを搭載した Citrix SD-WAN 1000 および 2000 の機能表

	Windows Server シリーズを搭載した Citrix SD-WAN 1000 シリーズ	Windows Server シリーズを搭載した Citrix SD-WAN 2000 シリーズ
自動構成	○	○
SD-WAN プラグイン	×	○

	Windows Server シリーズを搭載した Citrix SD-WAN 1000 シリーズ	Windows Server シリーズを搭載した Citrix SD-WAN 2000 シリーズ
圧縮	○	○
HTTPS 経由の RPC	○	○
SSL 圧縮	○	○
TCP アクセラレーション	○	○
トラフィックシェーピング	○	○
ビデオキャッシング	○	○
Windows ファイルシステムアクセラレーション	○	○
Windows Outlook アクセラレーション	○	○
XenApp/XenDesktop アクセラレーション	○	○
グループモード	○	○
高可用性モード	○	○
インラインモード	○	○
仮想インラインモード	○	○
WCCP モード	○	○
VLAN	○	○

ハードウェア仕様の概要

April 15, 2021

次の表は、Windows Server ハードウェアプラットフォームでの SD-WAN 1000 および 2000 の仕様をまとめたものです。

ハードウェア仕様	Windows Server 搭載の SD-WAN 1000	Windows Server 搭載の SD-WAN 2000
Windows Server のバージョン	Windows Server 2012 R2	Windows Server 2012 R2

プラットフォームのパフォーマンス

ハードウェア仕様	Windows Server 搭載の SD-WAN 1000	Windows Server 搭載の SD-WAN 2000
帯域幅	最大 20 Mbps	最大 50Mbps
HDX セッションの最大数	100 まで	300
合計セッション数	10,000	20,000
アクセラレーションプラグイン CCU	-	750

ハードウェア仕様

ハードウェア仕様	Windows Server 搭載の SD-WAN 1000	Windows Server 搭載の SD-WAN 2000
プロセッサ	4 コア	4 コア
ディスク容量の合計	1x300 GB SSD と 1 x1 TB HDD	600GB の SSD と 1X1 TB の HDD×1
SSD (専用圧縮履歴)	ディスクベース圧縮 (DBC) の場 合は 123 GB、ビデオキャッシュ の場合は 25 GB	ディスクベース圧縮 (DBC) の場 合は 225 GB、ビデオキャッシュ の場合は 50 GB
RAM	32GB	24 ギガバイト
ネットワークインタフェース	バイパス 10/100/1000 と 2 ペア、 管理ポートおよび AUX ポート用の 2 GigE ポート	10/100/1000 ベース-T 銅線イー サネット x 4、管理ポートおよび AUX ポート用 2 GigE ポート
電源装置	1	1

物理的寸法

ハードウェア仕様	Windows Server 搭載の SD-WAN 1000	Windows Server 搭載の SD-WAN 2000
ラックユニット	1U	1U
システム幅	19 インチラック用の EIA 310-D	19 インチラック用の EIA 310-D
システムの深さ	10” (25.4 cm)	25.4” (64.5 cm)
システム重量	8.5 ポンド (3.9 kg)	32 ポンド (14.5kg)

	Windows Server 搭載の SD-WAN 1000	Windows Server 搭載の SD-WAN 2000
ハードウェア仕様		
配送の寸法と重量	長さ 26 インチ x 幅 18.5 インチ x 高さ 6.5 インチ、14.5 ポンド。	長さ 32×幅 23.5×高さ 7.5 イン チ、39 ポンド。

環境と規制

	Windows Server 搭載の SD-WAN 1000	Windows Server 搭載の SD-WAN 2000
ハードウェア仕様		
電圧	100/240 VAC、50-60 Hz	100/240 VAC、50-60 Hz
消費電力 (最大)	200 W	300 W
動作温度 (摂氏)	10-35	0-40
非動作時温度 (摂氏)	-40 - +70	-40 - +70
許容相対湿度	8% ~90% 結露しないこと	5%-95%
安全認定	CSA/EN/IEC/UL 60950-1 準拠、 UL または CSA リスト (米国およ びカナダ)、CE マーキング (ヨー ロッパ)	CSA/EN/IEC/UL 60950-1 準拠、 UL または CSA リスト (米国およ びカナダ)、CE マーキング (ヨー ロッパ)
電磁界および感受性の認定	FCC (パート 15 クラス A)、CCC、 KCC、NOM、SASO、CITC、 EAC、DOC、CE、VCCI、RCM	FCC (パート 15 クラス A)、CCC、 KCC、NOM、SASO、CITC、 EAC、DOC、CE、VCCI、RCM
環境認証	ROHS、ウィー	ROHS、ウィー

Citrix SD-WAN 4100 および 5100 WANOP アプライアンス

April 15, 2021

Citrix SD-WAN 4100,5100 WANOP アプライアンスは、忙しいデータセンター向けのハイパフォーマンス WAN アクセラレータです。これらのアプライアンスは、複数の仮想アクセラレータインスタンスと NetScaler ロードバランサーの単一の仮想インスタンスを組み合わせ、単一のパッケージで複数の SD-WAN WANOP アプライアンスのパフォーマンスを提供します。

Citrix SD-WAN 4100、5100 WANOP WAN アクセラレータは、Citrix SD-WAN 製品ラインのハイエンドです。これらは、1 Gbps を超える速度で WAN リンクを使用するサイト、特に多くのブランチサイトや地域のサイトと通信するビジネデータセンターを高速化するように設計されています。

単一の SD-WAN WANOP 4100、5100 アプライアンスは、最大 2 Gbps および最大 5000 人の XenApp/XenDesktop ユーザーまでの WAN 速度をサポートできます。

さらに高いパフォーマンスを必要とするデータセンターでは、WCCP クラスタリング機能を使用して、複数の SD-WAN WANOP 4100/5100 アプライアンスを負荷分散アレイとして展開できます。

Citrix SD-WAN WANOP 4100、5100 は、ハブアンドスポーク展開のハブで推奨されます。ハブアンドスポーク展開では、リンク速度または XenApp/XenDesktop ユーザーの数が小さいアプライアンスでサポートされるよりも高い場合は、小さいアプライアンスがスポークで使用されます。

DC から DC へのレプリケーション

セカンダリデータセンターが必要な場合、SD-WAN WANOP 4000、5000 アプライアンスは、データセンターからデータセンターへのレプリケーションを最適化できます。この最適化により、レプリケーション時間が短縮され、帯域幅消費が削減されます。

NetApp Snap Mirror を使用した DC/DC レプリケーション用に SD-WAN WANOP アプライアンスを構成する方法については、<http://support.citrix.com/article/CTX137181>を参照してください。

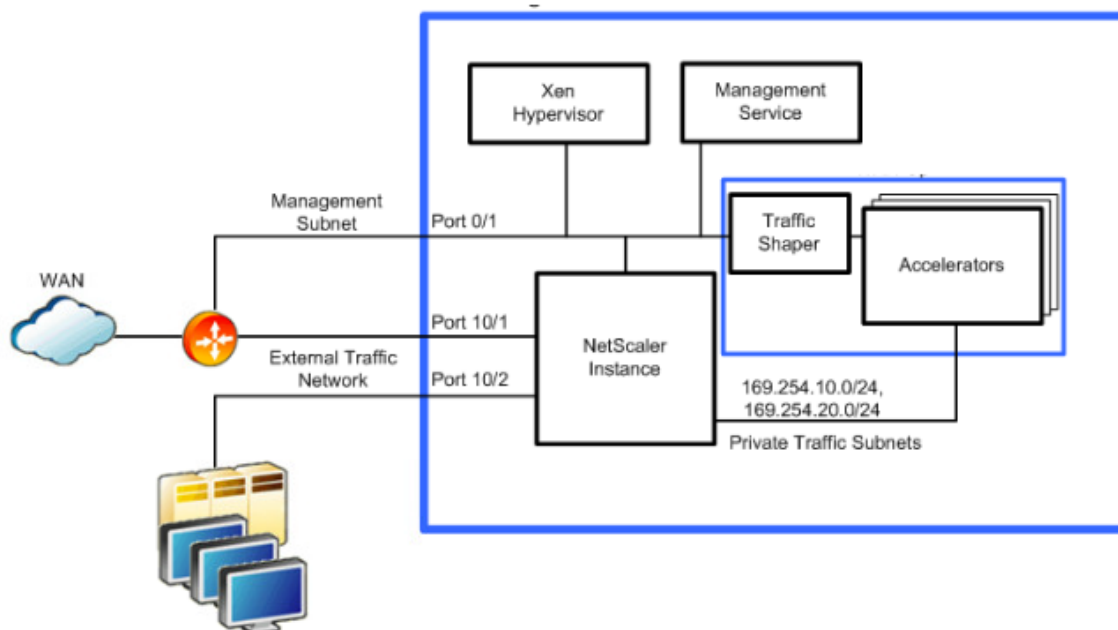
アーキテクチャ

April 15, 2021

内部的には、SD-WAN 4000/5000 アプライアンスには複数の仮想マシンが含まれています。

- Xen ハイパーバイザ
- NetScaler インスタンス
- 少なくとも 2 つのアクセラレータインスタンス
- GUI およびその他のタスクを管理する管理サーバー・インスタンス
- 内部ネットワーク

図 2: SD-WAN 4100/5100 仮想マシン、内部ネットワーク、および外部ポートの使用状況（インライン展開を参照）



NetScaler インスタンスで構成されている場合を除き、アクセラレータに出入りする WAN トラフィックはありません。アプライアンスを最初に使用すると、プロビジョニングウィザードによって、NetScaler インスタンスとアクセラレータ間の通信と負荷分散を提供する初期構成が設定されます。

管理サービスは、アプライアンスの管理構成インターフェイスであり、アプライアンスの主要な操作要素および監視要素へのアクセスを提供します。管理サービスは、SD-WAN パラメータを 1 つのアクセラレータからのものと同じように表示し、このインターフェイスを介して行われたすべての変更は、すべてのアクセラレータインスタンスに適用されます。

Xen ハイパーバイザーは、すべての仮想マシンをホストします。ハイパーバイザーはユーザーが構成できないので、Citrix からの要求以外にアクセスしないでください。

内部および外部ネットワーク

外部ネットワークインターフェイスは、トラフィックインターフェイスと管理インターフェイスの 2 つのカテゴリに分類されます。

トラフィックインターフェイス: トラフィックインターフェイスには、管理だけに使用されるポート 0/1 と 0/2 を除くすべてのネットワークインターフェイスが含まれます。アクセラレーションは、トラフィックインターフェイスだけで実行されます。

注: ARP フラッピングやその他の問題を防ぐには、トラフィックインターフェイスを管理インターフェイスから分離しておく必要があります。この分離は、物理的に、または異なる VLAN で管理インターフェイスおよびトラフィックインターフェイスパケットにタグを付けることによって実現できます。

管理サブネット: 仮想マシンは、管理サービス、NetScaler インスタンス、および XenServer に対して異なる IP アドレスを使用して、外部管理サブネットに直接接続します。

注: ARP フラッピングやその他の問題を防ぐには、トラフィックインターフェイスを管理インターフェイスから分離しておく必要があります。この分離は、物理的に、または異なる VLAN で管理インターフェイスおよびトラフィックインターフェイスパケットにタグを付けることによって実現できます。

プライベート内部トラフィックサブネット: アクセラレータのアクセラレーションポートは、内部トラフィックサブネットを使用して、ワンアームモードで内部的に NetScaler インスタンスに接続されます。インスタンスのアクセラレーションポートとアプライアンスの外部ポートの間には、直接接続はありません。アクセラレータへの高速化されたトラフィックはすべて、NetScaler インスタンスによって制御されます。

この内部サブネットはアプライアンスの外部からアクセスできないため、169.254.0.0/16 の範囲のルーティング不可能なサブネットを使用します。NetScaler インスタンスは、アクセラレータへのルーティング可能なアクセスを必要とする機能に NAT を提供します。アクセラレータの次の 2 つの機能だけが、外部から到達できる IP アドレスを必要とします。

- セキュアピアリングおよび SD-WAN プラグインに使用されるシグナリング IP アドレス。
- IP アドレス。WCCP プロトコルが使用されるときにルータとの通信に使用されます。

いずれの場合も、外部から見える IP アドレスの数は、アプライアンスのアクセラレータの数とは無関係です。

内部トラフィックサブネットには、アクセラレータごとに 2 つの IP アドレスと、NetScaler アドレスに加えて、WCCP を使用する場合は、1 つまたは 2 つの WCCP VIP アドレスが必要です。内部ネットワークはプライベートであるため、これらのタスク用のアドレス空間が豊富にあります。

プライベートトラフィックサブネットでのデータフロー-NetScaler インスタンスとアクセラレータ間のワンアーム接続では、SD-WAN 仮想インラインモードが使用されます。このモードでは、NetScaler インスタンスはパケットをアクセラレータにルーティングし、アクセラレータは NetScaler インスタンスにルーティングします。この内部トラフィックサブネット上のトラフィックフローは、(外部インターフェイス上の) 外部から認識できるモードがインライン、仮想インライン、または WCCP のいずれであるかに関係なく、同じです。

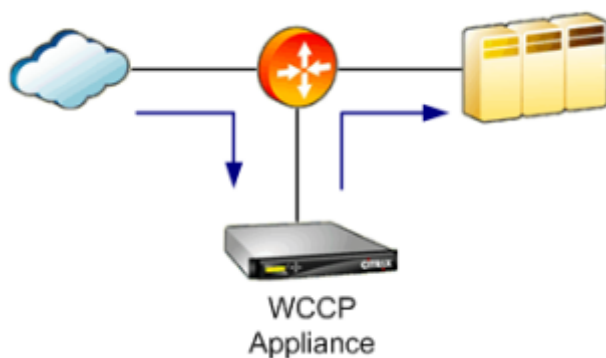
このトラフィックには、SD-WAN の「イーサネット送信者に戻る」オプションと、プロビジョニングウィザードで有効な「NetScaler MAC アドレス転送」および「サブネット IP の使用」オプションが必要です。

展開モードの概要: WCCP モード、インラインモード、および仮想インラインモードの相違点は、次のように要約できます。

- WCCP モードは、ワンアーム構成です。アクセラレータは、ルータと WCCP 制御チャネルを確立します。WCCP モードでは、1 つまたは 2 つのアクセラレータだけが、すべてのアクセラレータに代わって WCCP コントロールチャネルを管理します。データトラフィックは、すべてのアクセラレータ間で負荷分散されます。GRE カプセル化を使用すると、NetScaler インスタンスは自身とルーター間のデータストリームに対して GRE カプセル化/カプセル解除を実行し、NetScaler とアクセラレータ間のデータでカプセル解除されたレベル 2 構成を使用できます。
- インラインモードは、内部的に WCCP モードとほぼ同じ動作しますが、アプライアンスはブリッジをエミュレートするため、WCCP 制御チャネルは確立されません。一方のブリッジポートでアプライアンスに入力されるパケットは、もう一方のブリッジポートを通過します。SD-WAN 4000 および 5000 アプライアンスには、複数のインラインリンクをサポートするための複数のブリッジがあります。

- 仮想インラインモード（WCCP およびインラインモードが実現できない場合に使用される）では、アプライアンスは WCCP と同様にワンアーム設定で展開されますが、WCCP コントロールチャンネルはありません。トラフィックは、ポリシーベースルーティング（PBR）ルールを使用して、ルータからアプライアンスに送信されます。アプライアンスはトラフィックを処理し、ルータに返します。

図 3: WCCP および仮想インラインケーブル



SD-WAN 4100/5100 アプライアンスでのポート使用量の図については、「SD-WAN 4100/5100 仮想マシン、内部ネットワーク、および外部ポートの使用状況」を参照してください。トラフィックポートは加速ブリッジのセットとして配置され、管理ポートは独立しています。通常、管理ポートは 1 つだけ使用されます。

図 4: インライン配線



アクセラレーションブリッジ

SD-WAN 4100/5100 アプライアンスには、複数の高速ブリッジがあります。モデルによって、ブリッジポートの数とタイプが異なります。このようなブリッジを構成している 2 つのポートを「アクセラレーションペア」と呼びます。現在のすべてのモデルには、ネットワークバイパス機能が内蔵されています。（古い SD-WAN 4100-500 および 4100 ~1000 ユニットには、ネットワークバイパスが含まれないものがあります）。ネットワークバイパス機能（「Fail to Wire」とも呼ばれる）は、電源喪失またはソフトウェア障害（内部ウォッチドッグタイマーによって決定される）によってアプライアンスに障害が発生した場合、ポートのペアを接続します。

インライン展開。バイパス機能により、SD-WAN 4100/5100 を WAN に沿って（通常は LAN と WAN ルータ間）に配置できます。ネットワーク障害の発生は発生しません。

加速ブリッジは、1 Gbps または 10 Gbps のデータレートをサポートします。イーサネットインターフェイスおよび SFP+ インターフェイスは、モデルに応じてサポートされます。

ワンアーム展開。WCCP モードまたは仮想インラインモードを使用して、ワンアーム配置もサポートされます。このような配置では、SD-WAN 4000/5000 トラフィックポートが WAN ルータのポートに直接接続されます。ブリッジドペアのもう一方のポートは接続されていないままになります。

パフォーマンスに関する考慮事項インライン配置では、1つのポートではなく2つのポートを使用すると、インターフェイスのピークスループットが2倍になるため、ワンアーム配置よりもパフォーマンスが向上します。

SD-WAN 4100/5100 アプライアンスでは、コンプレッサーが圧縮比に比例して加速するため、ピークスループットが重要です。つまり、100:1の圧縮を達成した接続は、ネットワークパスの残りの部分が維持できる限り、非圧縮接続の100倍高速にデータを転送します。

たとえば、500 Mbps WAN リンクと 1 Gbps の LAN があるデータセンターとします。WAN と LAN の間の 2:1 の速度比が小さいため、圧縮では、リンク全体で2倍のスピードアップを実現できます。これは、1 Gbps を超える速度で LAN との間でデータを取得する方法がないためです。SD-WAN 4100/5100 配置では、ピークデータレートを10倍に増加できる 10 Gbps LAN を使用することをお勧めします。

SD-WAN 4100/5100 アプライアンスをワンアームモードで展開すると、ピーク転送レートは半分に低下します。ワンアームモードの SD-WAN 4100/5100 は、1 Gbps LAN インターフェイスでルータに接続され、WAN が両方向でフルスピードで実行されている場合、このインターフェイスは飽和状態になります。良好なパフォーマンスを得るには、SD-WAN 4100/5100 には、WAN よりもはるかに高速な LAN インターフェイスが必要です。アプライアンスがワンアームモードでルータに直接接続されている場合は、10 Gbps ルータポートを使用します。

注

10 Gbps ポートは 10 Gbps だけをサポートします。彼らは低速をネゴシエートしません。1 Gbps ネットワークには、1 Gbps ポートを使用します。

その他のポート

SD-WAN 4100/5100 アプライアンスには、少なくとも2つの非アクセラレーションポートがあります。ポート 0/1 は通常、管理に使用され、ポート 0/2 は存在しますが、通常は使用されません。ライトアウト管理 (LOM) ポートも用意されています。RS-232 ポートは管理に使用できます。

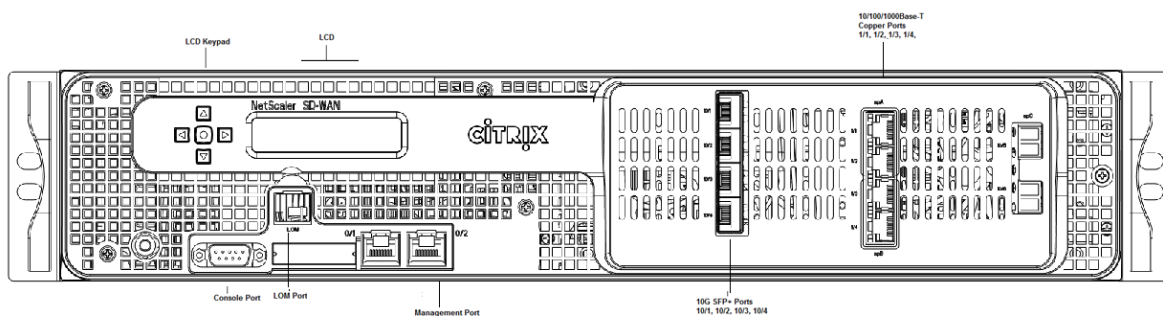
SD-WAN 4100 WANOP

April 15, 2021

Citrix SD-WAN 4100 WANOP は、2U アプライアンスです。各モデルには、合計 12 個の物理コア (ハイパースレッディング付きの 24 コア) と 48 ギガバイト (GB) のメモリ用の 6 コアのプロセッサが2つ搭載されています。Citrix SD-WAN 4100 WANOP の帯域幅は、それぞれ 310 Mbps、500 Mbps、および 1 Gbps です。

次の図は、Citrix SD-WAN 4100 アプライアンスのフロントパネルを示しています。

図 1. Citrix SD-WAN 4100、フロントパネル



Citrix SD-WAN 4100 WANOP アプライアンスには、次のポートがあります。

- 10/100Base-T 銅線イーサネットポート (RJ45)。LOM ポートとも呼ばれます。このポートを使用して、アプライアンスのソフトウェアとは無関係にアプライアンスをリモートで監視および管理できます。
- RS232 シリアルコンソールポート。
- ネットワークポート
 - 2 ポート 10/1G バイパス x
 - 4 ポート 1G バイパス
 - 4 ポート 10G/1G×1。
 - 2 ポート 10G (隠し) ×1。

次の図は、Citrix SD-WAN 4100 WANOP アプライアンスの背面パネルを示しています。

図 2: Citrix SD-WAN 4100 WANOP 背面パネル



Citrix SD-WAN 4100 WANOP アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 4 つの 800 GB リムーバブルソリッドステートドライブ。アプライアンスの圧縮履歴を保存します。
- 2 つの 1 TB リムーバブルハードディスクドライブ。
- 電源スイッチ。電源装置を取り外すかのように、アプライアンスへの電源を切ります。スイッチを 5 秒間押して、電源を切ります。
- アラームボタンを無効にします。このボタンは、アプライアンスに電源装置が 2 つある場合にのみ機能します。アプライアンスを 1 つの電源コンセントだけに接続した場合、または 1 つの電源装置が故障して修理されるまでアプライアンスの動作を続行する場合は、このボタンを押して、電源アラームの鳴りを停止します。
- 2 つの電源 (AC または DC のいずれか)。完全なホットスワップ冗長性を提供します。

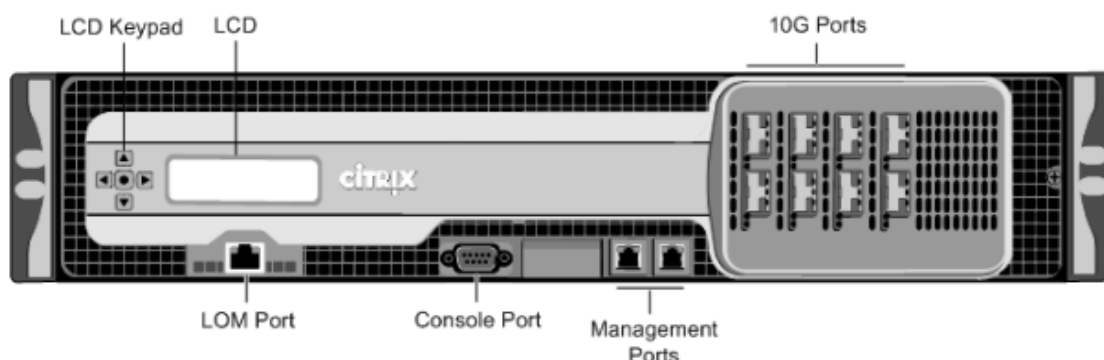
SD-WAN 5100 WANOP

April 15, 2021

Citrix SD-WAN 5100 WANOP は、2U アプライアンスです。各モデルは、2.80 GHz と 128 ギガバイト (GB) のメモリを備えた 10 コアプロセッサを備えています。Citrix SD-WAN 5100 WANOP アプライアンスの帯域幅は 2 Gbps です。

次の図は、Citrix SD-WAN 5100 WANOP アプライアンスのフロントパネルを示しています。

図 1: Citrix SD-WAN 5100 WANOP、フロントパネル



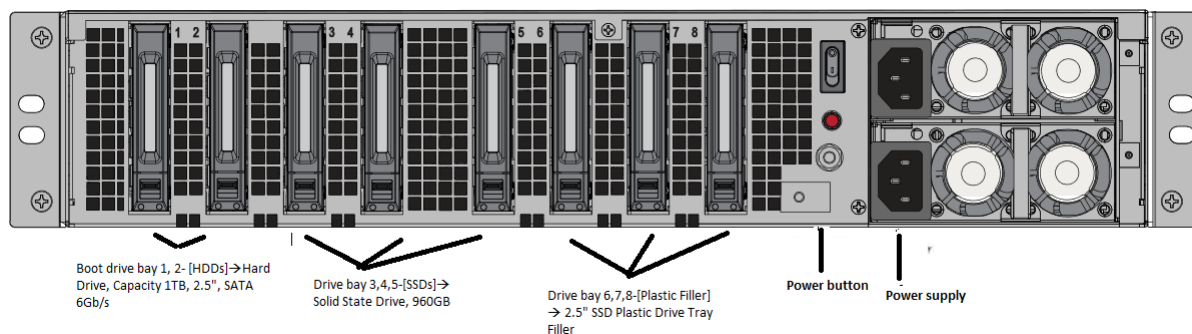
Citrix SD-WAN 5100 WANOP アプライアンスには、次のポートがあります。

- 10/100Base-T 銅線イーサネットポート (RJ45)。LOM ポートとも呼ばれます。このポートを使用して、アプライアンスのソフトウェアとは無関係にアプライアンスをリモートで監視および管理できます。
- RS232 シリアルコンソールポート。
- イーサネットポート:
 - 2 ポート 10/1G バイパス、4 ポート 10G/1G バイパス、2 ポート 10G/1G バイパス

これらのポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。

次の図は、Citrix SD-WAN 5100 WANOP アプライアンスの背面パネルを示しています。

図 2: Citrix SD-WAN 5100 WANOP、背面パネル



Citrix SD-WAN 5100 WANOP アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 6つの 800 GB リムーバブルソリッドステートドライブ。アプライアンスの圧縮履歴を保存します。
- 電源スイッチ。電源装置を取り外すかのように、アプライアンスへの電源を切ります。スイッチを 5 秒間押し、電源を切ります。
- 2つの 1 TB リムーバブルハードディスクドライブ
- アラームボタンを無効にします。このボタンは、アプライアンスに電源装置が 2 つある場合にのみ機能します。アプライアンスを 1 つの電源コンセントだけに接続した場合、または 1 つの電源装置が故障して修理されるまでアプライアンスの動作を続行する場合は、このボタンを押して、電源アラームの鳴りを停止します。
- 2つの電源 (AC または DC のいずれか)。完全なホットスワップ冗長性を提供します。各電源装置には、その状態を示す LED があります。

ハードウェア仕様の概要

April 15, 2021

次の表は、Citrix SD-WAN 4100/5100 WANOP ハードウェアプラットフォームの仕様をまとめたものです。

仕様	4100 WANOP	5100 WANOP
帯域幅	最大 1Gbps	最大 2 Gbps
規制モデル番号	2U1P1B	2U1P1D
プロセッサ	6 コア 2.60GHz×2	10 コア 2.80 GHz × 2
HDD	RAID 1 (ミラーリング) モードでの 2 TB HDD 起動ドライブ	RAID 1 (ミラーリング) モードでの 2 TB HDD 起動ドライブ
SSD	4 倍 800GB	6x800GB
メモリ	96 ギガバイト	128GB
電源装置の数	完全なホットスワップ冗長性を提供する 2 台の電源装置	完全なホットスワップ冗長性を提供する 2 台の電源装置
交流電源	100 ~240 V AC、50 Hz ~60 Hz、2 × 9.0 ~4.5A	100 ~240 V AC、50 Hz ~60 Hz、2 × 9.0 ~4.5A
直流電源	-36V 直流から-72V DC、2 × 25.5~13.0A	-36V 直流から-72V DC、2 × 25.5~13.0A
最大 AC 消費電力	633 W	822 W
最大 DC 消費電力	712 W	895 W
エアフロー (前面から背面)	65 CFM、標準	65 CFM、標準
放熱	137 W/フィート 2/フィート、標準	144 W/フィート 2/フィート、標準

仕様	4100 WANOP	5100 WANOP
パッケージ重量 (ポンド) 配送の寸法と重量	62 ポンド (28.1 キログラム)	64 ポンド (29.10 キログラム)
寸法	36.5 インチ × 24.5 インチ × 11 インチ (93cm × 63cm × 28cm)	36.5 インチ × 24.5 インチ × 11 インチ (93cm × 63cm × 28cm)
システム重量 (ポンド)	45 ポンド (20.4 kg)	47 ポンド (27kg)
ラックユニット	2U	2U
幅	EIA 310-D、IEC 60297、DIN 41494 SC48D ラック 17.25 インチ (44 cm)	EIA 310-D、IEC 60297、DIN 41494 SC48D ラック 17.25 インチ (44 cm)
奥行き	28" (71.1 cm)	28" (71.1 cm)
動作温度	32–104 F (0–40 C)	32–104 F (0–40 C)
非動作温度	14F~140F (-10C~60C)	14F~140F (-10C~60C)
湿度範囲 (結露しないこと)	5%-95% 結露しないこと	5%-95% 結露しないこと
安全認定	IEC 60950-1、第 2 版; CSA 60950-1、第 2 版; UL 60950-1、第 2 版; AS/NZS 6050-1	IEC 60950-1、第 2 版; CSA 60950-1、第 2 版; UL 60950-1、第 2 版; AS/NZS 6050-1
EMC と感受性	米国 (FCC (パート 15 クラス A))、ヨーロッパ (CE (EN55022/55024))、オーストラリア (RCM)、日本 (VCCI)、韓国 (KCC)、台湾 (BSMI)、中国 (CCC)、インド (BIS)、ロシア (EAC)、サウジアラビア (CITC)、ブラジル (アナテル)、南アフリカ (ICASA)、メキシコ (NOM)、エジプト (NTRA)、イスラエル (MoC)	米国 (FCC (パート 15 クラス A))、ヨーロッパ (CE (EN55022/55024))、オーストラリア (RCM)、日本 (VCCI)、韓国 (KCC)、台湾 (BSMI)、中国 (CCC)、インド (BIS)、ロシア (EAC)、サウジアラビア (CITC)、ブラジル (アナテル)、南アフリカ (ICASA)、メキシコ (NOM)、エジプト (NTRA)、イスラエル (MoC)
環境コンプライアンス	RoHS、リーチ、ウィー	RoHS、リーチ、ウィー

SD-WAN WANOP 4100/5100 アプライアンスの管理ポートが点灯する

April 15, 2021

SD-WAN 4100/5100 アプライアンスには、アプライアンスの前面パネルにインテリジェントプラットフォーム管理インターフェイス (IPMI) (ライトアウト管理 (LOM) と呼ばれます) ポートがあります。LOM を使用すると、SD-WAN 4100/5100 ソフトウェアとは無関係に、アプライアンスをリモートで監視および管理できます。LOM ポート経由でアプライアンスに接続することで、IP アドレスの変更、さまざまな電源操作、およびアプライアンスの健全性監視情報の取得をリモートで行うことができます。

LOM ポートを、データチャネルとは別の専用チャネルに接続することで、データネットワークがダウンしている場合でも、アプライアンスへの接続を維持できます。

Web ブラウザを使用した LOM ポートへのアクセス

Web ブラウザを使用すると、LOM ポートにリモートでログオンし、アプライアンスに関する情報を取得し、アプライアンス上でさまざまな操作を実行することができます。

Web ブラウザを使用して LOM にアクセスするには

1. Web ブラウザで、LOM ポートの IP アドレスを入力します。初期構成の場合は、ポートのデフォルトアドレスを入力します。
2. [ユーザー名] ボックスに「**nsroot**」と入力します。
3. [パスワード] ボックスに「**nsroot**」と入力します。

LOM ポートの設定

インテリジェントプラットフォーム管理インターフェイス (IPMI) (ライトアウト管理 (LOM) ポートとも呼ばれ、NetScaler ソフトウェアとは無関係に、アプライアンスをリモートで監視および管理できます。Lights-Out Management (LOM) ポートを初期構成するには、ポートのデフォルト IP アドレスに接続し、リモート監視および管理に使用するアドレスに変更します。管理者の資格情報とネットワーク設定も指定します。

メモ: LOM ポートの LED は設計上、動作しません。

NetScaler LOM ポートを構成するには

1. LOM ポートを管理ワークステーションまたはネットワークに接続します。
2. Web ブラウザで、次のように入力します <http://192.168.1.3>。

注: NetScaler LOM ポートは、IP アドレス 192.168.1.3 とサブネットマスク 255.255.0 で事前構成されています。

3. [ユーザー名] ボックスに「**nsroot**」と入力します。
4. [パスワード] ボックスに「**nsroot**」と入力します。
5. [構成] タブで、[ネットワーク] をクリックし、次のパラメーターの値を入力します。

- IP アドレス: LOM ポートの IP アドレス。
- [Subnet Mask]: LOM ポートのサブネットを定義するために使用されるサブネットマスク。
- デフォルトゲートウェイ: LOM ポートをネットワークに接続するルータの IP アドレス。

6. [保存] をクリックします。

アプライアンスの電源を入れ直します

アプライアンスの電源をリモートでオフにし、再びオンにすることができます。結果は、アプライアンスの背面パネルの電源ボタンを 2 秒未満押しした場合と同様です。

アプライアンスの電源を入れ直すには

1. Web ブラウザで、LOM ポートの IP アドレスを入力します。
2. [ユーザー名] ボックスと [パスワード] ボックスに、管理者の資格情報を入力します。
3. メニューバーで、[リモートコントロール] をクリックします。
4. [オプション] の [電源制御] をクリックし、[システムの電源を入れ直す] をクリックします。
5. [アクションを実行] をクリックします。

アクセスコンソールを使用したアプライアンスへのアクセス

LOM ポートを使用すると、リダイレクトされたコンソールにログオンして、アプライアンスにリモートからアクセスおよび管理できます。

アクセスコンソールを使用してアプライアンスにアクセスするには

1. Web ブラウザで、LOM ポートの IP アドレスを入力します。
2. [ユーザー名] ボックスと [パスワード] ボックスに、管理者の資格情報を入力します。
3. メニューバーで、[リモートコントロール] をクリックします。
4. [オプション] の [コンソールリダイレクト] をクリックします。
5. [コンソールの起動] をクリックし、[はい] をクリックします。
6. アプライアンスの管理者資格情報を入力します。

ヘルスマニタリング情報の取得

LOM ポートにログオンして、アプライアンスに関する正常性情報を表示できます。システム温度、CPU 温度、ファン、電源のステータスなど、すべてのシステムセンサー情報は、センサーの読み取り値ページに表示されます。

ヘルスマニタリング情報を取得するには

1. Web ブラウザで、LOM ポートの IP アドレスを入力します。

2. [ユーザー名] ボックスと [パスワード] ボックスに、管理者の資格情報を入力します。
3. メニューバーで、[システムの正常性] をクリックします。
4. [オプション] で、[センサーの読み取り値] をクリックします。

LOM ポートを使用した電源制御操作

LOM ポートを使用して、アプライアンスの再起動、正常なシャットダウン、強制シャットダウンの実行など、さまざまな電源制御操作をリモートで実行できます。

電源制御操作を実行するには

1. Web ブラウザーで、管理者の資格情報を使用して LOM ポートにログオンします。
2. メニューバーで、[リモートコントロール] をクリックします。
3. [オプション] の [電源制御] をクリックし、次のいずれかのオプションを選択します。
 - システムのリセット: アプライアンスを再起動します。
 - システムの電源オフ - 即時: アプライアンスをシャットダウンせずに、アプライアンスへの電源を切断します。
 - システムの電源オン: アプライアンスの電源を入れます。
 - システムの電源オフ/オン: アプライアンスの電源を切り、再び電源を入れます。
4. [アクションを実行] をクリックします。

トラブルシューティングのヒント

April 15, 2021

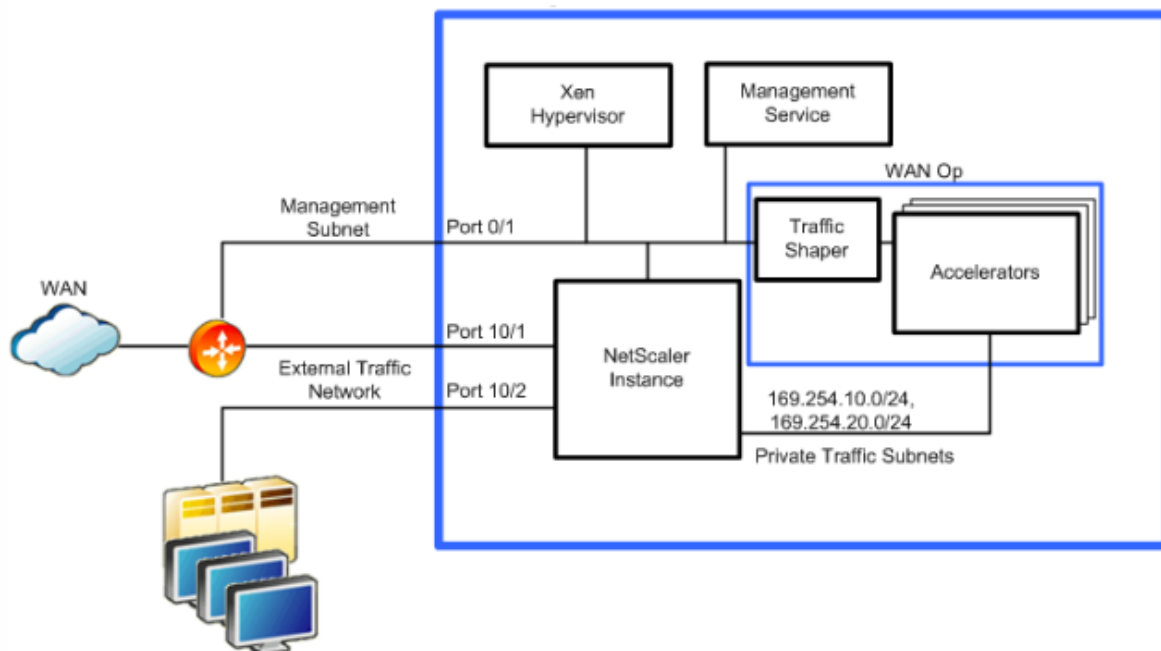
ほとんどのインストールはスムーズに完了しますが、一部のインストールでは、さらに監視とトラブルシューティングを実行する前に、アプライアンスの内部構造またはほとんど知られていない機能の使用に関する知識が必要です。これらのトラブルシューティングのヒントは、アプライアンスのより詳細な分析を可能にする情報とテクニックを提供します。

内部アドレスの理解

一部のレポートでは、SD-WAN 4100/5100 内のプライベートサブネットのアドレスが表示されるため、これらのアドレスの意味を知っておきましょう。これらのサブネットは、外部ポートに接続せずに、仮想マシンと一緒に接続します。

これらのアドレスはすべて、RFC3927 で説明されているローカルリンクサブネット 169.254.0.0/16 にあります。このアドレス空間は、システム管理、プライベートトラフィック、アクセラレータ管理サブネットという 3 つの部分的に重複するサブネットに分割されます。

SD-WAN 4100 および 5100 内の仮想マシン。システム管理サブネットは、この図には示されていません。トラフィックシェーパは、すべてのアクセラレータからのトラフィックを管理し、アクセラレータ GUI を介して制御されます。



システム管理サブネット

機能	アドレス
管理サービス	169.254.0.10/16
NetScaler インスタンス	169.254.0.11/16
XenServer	169.254.0.1/16

プライベートトラフィックサブネット

機能	アドレス
APA IP、アクセラレータ 1~8	169.254.10.21/24 - 169.254.10.28/24
APA シグナリング IP、アクセラレータ 1 ~8	169.254.10.121/24 - 169.254.10.128/24
NetScaler インスタンス	169.254.10.11/24

アクセラレータ管理サブネット

機能	アドレス
アクセラレータ統合管理 IP (すべてのアクセラレータを制御)	169.254.0.20/24
プライマリポート IP、アクセラレータ 1~8	169.254.0.21/24 - 169.254.0.28/24

アクセラレータインスタンスステータスの確認と修正

エラーメッセージは、アプライアンス内の仮想マシンのいずれかに問題があることを示している場合があります。ステータスを確認するには、[システム構成] ページに移動し、SD-WAN または NetScaler サブシステムのインスタンスビューを選択します。たとえば、SD-WAN ページなどです。

- 完全にアクティブなインスタンスには、仮想マシンの状態、インスタンスの状態、およびライセンスに関する緑色の円が表示されます。
- アプライアンスには、ライセンス数よりも多くのインスタンスが存在する可能性があります。ライセンスされていないインスタンスは無視してください。
- 残りのインスタンスの仮想マシンの状態またはインスタンス状態が緑色でない場合は、「Rediscover」アクションを使用して、これらのインスタンスを動作状態に戻します。

各インスタンスの詳細情報を取得することもできます。

- すべてのインスタンスのステータスが「SD-WAN インスタンスからのインベントリが完了しました。」
- すべてのインスタンスで、同じバージョンのソフトウェアが実行されている必要があります。
- すべてのインスタンスには、ネットマスク (255.255.255.0) とゲートウェイ (169.254.0.20) が必要です。
- 他のインスタンスよりも短い稼働時間を示すインスタンスは、前回のシステム全体の再起動後に再起動されました。

NetScaler インスタンスへのログイン

NetScaler インスタンスにログインしてステータスを確認したり、構成を実行したりすると便利な場合があります。次に示すように、ビューの [NetScaler インスタンス] ページから NetScaler インスタンスにログインできます。[IP アドレス] リンクをクリックします。

管理ポート (ポート 0/1) の IP アドレスがわかっている場合は、ブラウザから直接 NetScaler インスタンスにログインすることもできます。

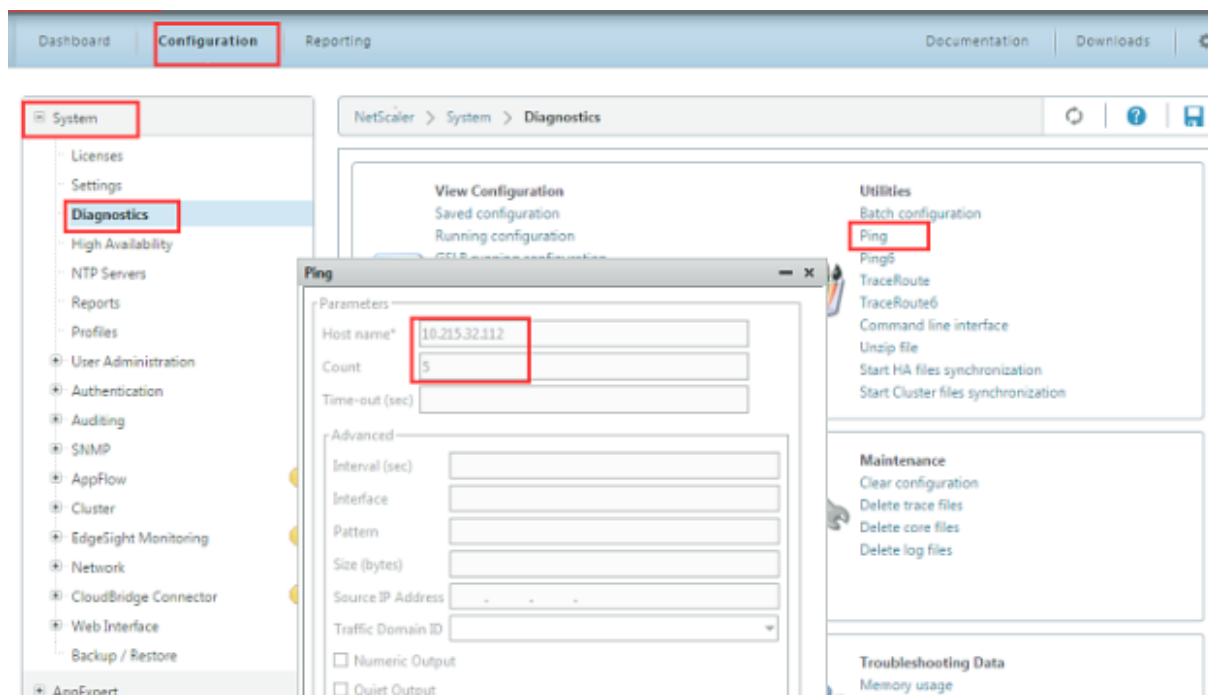
ログインすると、NetScaler GUI が表示されます。この GUI は、NetScaler VPX として識別されます。

これは、標準の NetScaler ユーザーインターフェイスです。監視機能の使用は安全です。SD-WAN 4100/5100 では、NetScaler インスタンスの構成方法に関する文書化されていない前提条件となるため、構成の変更は慎重に行う必要があります。

ping とトレーズルートを使用する

ping および traceroute ユーティリティは、他の SD-WAN 製品にあるため、アクセラレータインスタンスでは使用できません。代わりに、次の図に示すように [診断] ページを使用して、NetScaler インスタンスで同等の機能を使用できます。

これらの機能は、外部ネットワークおよびアプライアンスの内部サブネット上で機能します。



システムダッシュボードの使用

SD-WAN ダッシュボードとは異なり、[システムダッシュボード] ページは主にハードウェア監視専用です。

- [System Health] テーブルには、ステータスの概要が表示され、詳細リンクがグラフィカル形式で展開されます。
- [イベント] テーブルにはステータスの概要が表示され、関連するログエントリを表示するには [Show Events] リンクが表示されます。
- 複数のポートが Down とマークされている場合。これは、ケーブルが存在すると想定されている場合にのみエラーになります。ほとんどのアプライアンスには、いくつかの未使用のポートがあります。
- 配線に失敗すると、すべてのポートで FTW が無効になります。これは、このアプライアンスではネットワークバイパス機能が有効になっていないことを意味します。FTW イベントを調べると、実際のイベントがないことが示され、機能がおそらく無効になっていることが示されました。

警告またはエラーごとに、[詳細] リンクまたは [イベントの表示] ボタンから詳細を確認できます。

SSH 経由で別のインスタンスにログインする

一部の仮想マシンには、管理ポート（ポート 0/1）から、ssh ユーティリティ（Windows の PuTTY など）を使用し、root または nsroot としてログインし、管理パスワードを使用してログインできます。これにより、シェルプロンプトが表示されます。

SSH 経由でログオンする最も一般的な用途は、ネットワークパラメータの設定が間違っているために到達不能になったインスタンス（通常は管理サービス）の IP アドレスを復元することです。設定を変更すると、アプライアンスが不安定になったり、使用できなくなる可能性があるため、SSH の使用はお勧めしません。

以下の 2 つのインスタンスのいずれもネットワーク経由でアクセスできない場合は、RS-232 ポートを使用して XenServer インスタンスにログインできます。これにより、シェルプロンプトが表示されます。

これらの仮想マシンの 1 つにログインすると、シェルプロンプトから SSH を使用して、NetScaler インスタンスまたは適切な 169.254.x.x アドレスのアクセラレータにアクセスできます。

テキストエディタを含む、通常の UNIX/Linux コマンドを使用できます。

インスタンス	ログイン	パスワード	実際のユーザー名
管理サービス	nsroot	管理者パスワード	ルート
管理サービス	ルート	管理者パスワード	ルート
XenServer	nsroot	管理者パスワード	nsroot
XenServer	ルート	管理者パスワード	ルート

個々のアクセラレータインスタンスの監視

アクセラレータ GUI IP にログインすると、すべてのアクセラレータインスタンスを 1 つのユニットとして管理できます。変更は、すべてのアクセラレータインスタンスに自動的に反映されます。

まれに、個々のアクセラレータインスタンスのトラブルシューティングが必要になる場合があります。

インスタンスのログインは admin です。パスワードは、他のインスタンスで使用されているものと同じ管理者パスワードです。

これは、永続的な変更を行うためではなく、監視に推奨されます。インスタンスに設定したパラメーターは、後で同期プロセスによって上書きされる可能性があるためです。これを行うには、次の URL を使用します。

アクセラレータインスタンス	URL
1	<a href="https://<accelerator_ip>:4001">https://<accelerator_ip>:4001
2	<a href="https://<accelerator_ip>:4002">https://<accelerator_ip>:4002
8	<a href="https://<accelerator_ip>:4008">https://<accelerator_ip>:4008

更新バンドルの個々の要素の使用

Citrix によって配布されるアップデートバンドルは、単純な.tgz 形式（gzip で圧縮された tar アーカイブ）です。Citrix Web サイトに戻って個別にダウンロードするのではなく、アーカイブから個々のコンポーネントを抽出すると便利な場合があります。これは、管理サービス (build-svm*.tgz) またはアクセラレータリリース (orbital*.bin) で最も便利です。

アップデートバンドルは、tar/gzip または 7-zip などのアーカイブユーティリティによって管理されます。

サポートされる機能

April 15, 2021

表 1. Citrix SD-WAN 4100 および 5100 WANOP シリーズアプライアンスの機能表

機能	Citrix SD-WAN 4100 シリーズ	Citrix SD-WAN 5100 シリーズ
自動構成	×	×
SD-WAN コネクタ	○	○
SD-WAN プラグイン	○	○
圧縮	○	○
HTTPS 経由の RPC	○	○
SSL 圧縮	○	○
TCP アクセラレーション	○	○
トラフィックシェーピング	○	○
ビデオキャッシング	×	×
Windows ファイルシステムアクセラレーション	○	○
Windows Outlook アクセラレーション	○	○
XenApp/XenDesktop アクセラレーション	○	○
グループモード	×	×
高可用性モード	○	○
インラインモード	○	○
仮想インラインモード	○	○

機能	Citrix SD-WAN 4100 シリーズ	Citrix SD-WAN 5100 シリーズ
WCCP モード	○	○
VLAN	○	○

Standard Edition

April 15, 2021

重要:

NetScaler SD-WAN 製品は **CitrixSD-WAN** にリブランドされています。**NetScaler SD-WAN** という用語に関するすべての言及は、新しい製品用語 **Citrix SD-WAN** に適用されます。

Citrix SD-WAN Standard アプライアンスには、次のエディションがあります。

- [SD-WAN Standard Edition 210](#)
- [SD-WAN Standard Edition 400 および 410](#)
- [SD-WAN Standard Edition 1000、2000、および 2100](#)
- [SD-WAN Standard Edition 4000、4100、5100](#)
- [SD-WAN Standard Edition 6100](#)

ハードウェアのインストール

April 15, 2021

アプライアンスの設置場所が環境基準を満たしており、サーバラックが配置されていることを確認したら、ハードウェアを取り付ける準備が整います。アプライアンスをマウントしたら、ネットワーク、電源、および初期設定に使用できるコンソール端末に、アプライアンスを接続する準備が整いました。インストールを完了するには、アプライアンスをオンにします。インストール手順に記載されている注意事項と警告を必ず守ってください。

アプライアンスの物理的な設置手順と注意事項

- ラックを設置する前に、ラック内の各コンポーネントの配置を決定します。
- 簡単にアクセスできるように、機器をコンセントの近くに設置してください。
- 安全な動作のために十分な通気量のあるラックに機器を取り付けます。

- 閉じたラックアセンブリまたは複数ユニットラックアセンブリの場合、ラック環境の周囲動作温度は室内の周囲温度よりも大きくなる可能性があります。したがって、ラックにアプライアンスを設置する場所を決定するときは、装置の最低および最高動作温度を考慮してください。

ほとんどのアプライアンスは EIA-310-D 仕様に準拠する標準のサーバーラックに設置できます。アプライアンスを取り付ける前に、アプライアンスに付属するレールのセットを取り付ける必要があります。アプライアンスを取り付けるときに必要な工具は、プラスのドライバとマイナスのドライバだけです。

警告: アプライアンスをラック内の唯一のユニットとしてインストールする場合は、下部に取り付けます。ラックにほかのユニットも取り付ける場合は、最も重いユニットを一番下にしてください。ラックを固定する器具がある場合は、アプライアンスを取り付ける前に設置してください。

アプライアンスには、アプライアンスの高さに応じて 1 つまたは 2 つのラックユニットが必要です。

注意事項

- 静電気放電 (ESD) は、機器を損傷する可能性があります。
- アプライアンスにオブジェクトを配置しないでください。
- アプライアンスの側面にある通気孔を覆わないでください。
- アプライアンスの金属表面が加熱する可能性があります。
- アプライアンスの金属表面に触れるときは注意してください。

電気安全上の注意

取り付けまたはメンテナンスの手順では、アプライアンスの電子機器の静電気損傷を避けるために、アース用リストストラップを着用してください。導電性リストストラップを良好な接地、またはアプライアンスに接続して使用してください。背面の ESD シンボルのそばにあるコネクタに接続できます。

危害や器具の損傷から身を守るために、基本的な電氣的な安全対策に従ってください。

- 緊急電源オフ (EPO) スイッチの位置に注意して、電気事故が発生した場合にアプライアンスの電源をすばやく取り外すことができます。
- 電気ショックからの保護として、静電気放電を減らすように設計されたマットを使用しないでください。代わりに、電気絶縁体として設計されたゴムマットを使用してください。
- 電源装置コードに接地プラグが含まれており、接地されたコンセントに差し込まれていることを確認します。
- 過負荷の危険がない状態で電源がアプライアンスの最大消費電力を処理できることを確認します。
- 信頼できる地面は常に維持されなければなりません。したがって、ラックは接地する必要があります。分岐回路への直接接続以外の電源装置接続（たとえば、電源タップへの接続）には特に注意してください。

警告

バッテリーを誤った種類のバッテリーに交換すると、爆発の危険性があります。

デスクトップマウント

Citrix SD-WAN アプライアンスは、アプライアンスパッケージに同梱されているゴム脚を使用してデスクトップマウントできます。

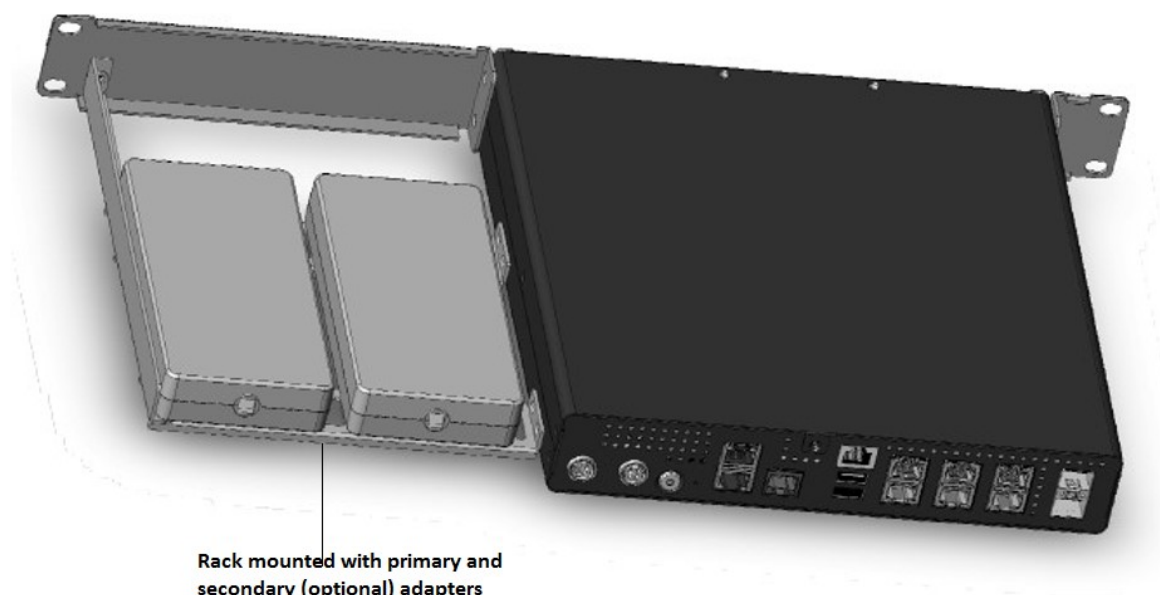
アプライアンスのラックマウント

SD-WAN アプライアンス用のラックマウントシャーシは、標準的なラックに適合し、1U のラック高さが必要です。アプライアンスは、平らな面に設置することも、付属のラックマウントブラケットとネジを使用して、標準ラックユニットに取り付けることもできます。

アプライアンスをラックに取り付けるには：

1. ラックマウントを取り付ける前に、アプライアンスが安定した面に設置されていることを確認します。
2. 付属のブラケットネジを使用して、付属のラックマウントブラケットをアプライアンスの側面に取り付けます。
 - アプライアンスを 4 支柱ラックに取り付ける場合は、ラックマウントブラケットを、アプライアンスの前面にハンドルが揃った状態で取り付けます。
 - アプライアンスを 2 支柱ラックに取り付ける場合は、ラックマウントブラケットを、アプライアンスの中央にハンドルが揃った状態で取り付けます。
3. アプライアンスをラックに配置します。十分な空気の流れができるように、デバイスの周りに十分なスペースがあることを確認してください。
4. ラックマウントブラケットの穴をラックの穴に並べて、SD-WAN 1100-SE および PE アプライアンスが水平であることを確認します。
5. 4 本のラック取り付けネジを指で締めて、アプライアンスをラックに取り付けます。
6. 適切なドライバでラックマウントネジを締めます。
7. 付属の電源ケーブルを接続します。

アプライアンスをラックマウントします。



アプライアンスを電源に接続する

アプライアンスに同梱されている電源ケーブルの数は、アプライアンスの電源装置の数によって異なります。電源ケーブルが2本付属のアプライアンスも、電源ケーブルが1本だけ接続されている場合に動作します。電源ケーブルが4本付属のアプライアンスは、電源ケーブルが2本だけ接続されている場合にも動作します。3本プラグが接地するため、アースケーブルは別途必要ない場合があります。

1. 電源ケーブルをアプライアンスの背面にある入口コンセントの1つに接続し、電源ケーブルのもう一方の端を電源コンセントに接続します。
2. アプライアンスに複数の電源装置がある場合は、この手順を繰り返します。追加の電源装置は、ホットスワップ可能な冗長電源装置です。
3. Citrix SD-WAN アプライアンスが起動します。

アプライアンスのネットワークへの接続

1. アプライアンスがコンソールポートまたはイーサネットポートを介して接続されていることを確認します。これにより、電源を入れた後にアプライアンスを構成できるようになります。
2. アプライアンスの背面パネルのオン/オフ切り替え電源スイッチを押します。

イーサネットケーブルまたは光ファイバケーブルを使用して、アプライアンスのインターフェイスを適切なスイッチのネットワークポートに接続します。同じスイッチまたはVLANに複数のネットワークポートを接続すると、ネットワークループが発生する可能性があります。

アプライアンスの設定

1. ゼロタッチ展開 (ZTD) を使用してアプライアンスを構成する場合は、docs.citrix.com サイトの次のリンクを参照してください。 [ゼロタッチ展開](#)
2. ハードウェア SD-WAN アプライアンスを構成する場合は、アプライアンスを物理的に PC に接続します。 docs.citrix.com サイトの次のリンクを参照してください。 [SD-WAN ハードウェアの設定](#)

Citrix SD-WAN アプライアンスハードウェアを設定するには、次の手順に従います。

1. シャーシをセットアップします。
 - Citrix SD-WAN アプライアンスは標準ラックに設置されています。デスクトップに設置する場合は、シャーシを平らな場所に置きます。適切な換気のために、アプライアンスの側面と背面に最低 2 インチの隙間があることを確認してください。
2. 電源を接続します。
 - 電源スイッチがオフに設定されていることを確認します。
 - 電源コードをアプライアンスと AC コンセントに差し込みます。
 - アプライアンスの前面にある電源ボタンを押します。
3. アプライアンスの管理ポートを PC に接続します。次の手順を完了する準備として、アプライアンスの管理 IP アドレスを設定する準備として、アプライアンスを PC に接続します。

注: アプライアンスを接続する前に、PC でイーサネットポートが有効になっていることを確認してください。イーサネットケーブルを使用して、SD-WAN アプライアンス管理ポートを PC のデフォルトのイーサネットポートに接続します。

ハードウェア SD-WAN アプライアンスの管理 IP アドレスを構成するには、次の手順を実行します。

注: ネットワークに追加するハードウェアアプライアンスごとに、以下のプロセスを繰り返します。

1. ハードウェア SD-WAN アプライアンスを構成する場合は、アプライアンスを物理的に PC に接続します。
 - イーサネットケーブルの一方の端をアプライアンスの管理ポートに接続し、もう一方の端を PC のデフォルトのイーサネットポートに接続します。

注: アプライアンスへの接続に使用している PC でイーサネットポートが有効になっていることを確認します。
2. アプライアンス管理 IP アドレスの設定に使用する PC の現在のイーサネットポート設定を記録します。アプライアンス管理 IP アドレスを設定する前に、PC のイーサネットポート設定を変更します。管理 IP アドレスの構成後に復元できるように、元の設定を記録します。
3. PC の IP アドレスを変更します。PC で、ネットワークインターフェイス設定を開き、PC の IP アドレスを次のように変更します:192.168.100.50
4. PC の [サブネットマスク] 設定を次のように変更します。255.255.0.0
5. PC で、ブラウザを開き、アプライアンスのデフォルトの IP アドレスを入力します。ブラウザのアドレス行に、次の IP アドレスを入力します: 192.168.100.1

注: SD-WAN アプライアンスに接続するときは、Google Chrome ブラウザを使用してください。管理 Web インターフェイスのブラウザ証明書の警告を無視します。

接続されているアプライアンスの **SD-WAN 管理 Web** インターフェイスのログイン画面が表示されます。

1. 管理者のユーザー名とパスワードを入力し、[**Login**] をクリックします。管理 Web インターフェイスにログインすると、[ダッシュボード] ページが表示されます。
 - デフォルトの管理者ユーザー名: `admin<!--NeedCopy-->`
 - デフォルトの管理者パスワード: `password<!--NeedCopy-->`

注

デフォルトのパスワードを変更します。パスワード回復には構成のリセットが必要になる場合があるため、パスワードを安全な場所に記録してください。

ポート **10/3** および **10/4** へのファイバパッチケーブルの取り付け

リリース 9.3 以降、アプライアンスでは、次の図に示すように、SD-WAN ポート 10/3 および 10/4 を付属のケーブルで接続する必要があります。

注:

10/3 および 10/4 ポートのファイバパッチケーブルは、4000 および 5000 WANOP シリーズのアプライアンスにだけ適用できます。

リリース 9.3 以降、パッチケーブルは不要になり、次の場合は省略できます。

- アプライアンスはリリース 9.3 以降の工場出荷時、または
- アプライアンスはリリース 9.3 以前の出荷時に出荷されていますが、このアプライアンスを新しいバージョンにアップグレードし、管理サービスでデフォルトのループバックを変更します ([システム] > [構成] > [システム] > [ループバック設定の構成])。

ループバックケーブルを使用する必要性をなくす場合は、ポート 10/3 および 10/4 は引き続き予約されています。これらのポートは、WAN 最適化には使用できません。

パッチケーブルを取り付けるには

1. 上の図に示すように、LC と LC ケーブルをポートに接続します。
2. ケーブルの一方の端をポート 10/3 に挿入します。
3. ケーブルのもう一方の端をポート 10/4 に挿入します。

Citrix SD-WAN 110 Standard Edition アプライアンス

April 15, 2021

Citrix SD-WAN 110 SE プラットフォームは、マイクロオフィスおよび小規模ブランチオフィス/リモートサイト/小売店、および一時的な職場に展開できるブランチサイドアプライアンスです。単一のボックスインブランチソリューションにより、ハードウェアの設置面積を削減し、ブランチ展開を容易にします。

Citrix SD-WAN 110-SE アプライアンスは、デスクトップフォームファクタアプライアンスです。このアプライアンスには、4 GB のメモリと 32 GB のストレージ (SATA-DOM ドライブ) を備えた 2 コアプロセッサが搭載されています。

Citrix コンプライアンス規制モデルは次のとおりです。

- SD-WAN 110
- SD-WAN 110-LTE-Wi-Fi
- SD-WAN 110-WiFi

詳しくは、以下を参照してください：

- [Citrix SD-WAN プラットフォームのデータシート](#)
- [Citrix SD-WAN 110 SE クイックスタートガイド：WAN インターフェイス経由の ZTD](#)
- [Citrix SD-WAN 110 LTE Wi-Fi クイックスタートガイド：LTE インターフェイス経由の ZTD](#)
- [Citrix SD-WAN 110 LTE Wi-Fi のボックス解除とインストール](#)
- [Citrix SD-WAN 110 LTE Wi-Fi コンプライアンス](#)
- [Citrix SD-WAN 110 Wi-Fi コンプライアンス](#)

注

110-SE アプライアンスは MCN として設定できません。

SD-WAN 110 SE 管理 Web インターフェイスにログインするには、次の資格情報を使用します。

- デフォルトの管理者ユーザー名: admin
- デフォルトの管理者パスワード: アプライアンスのシャーシの下部にあるアプライアンスのシリアル番号。

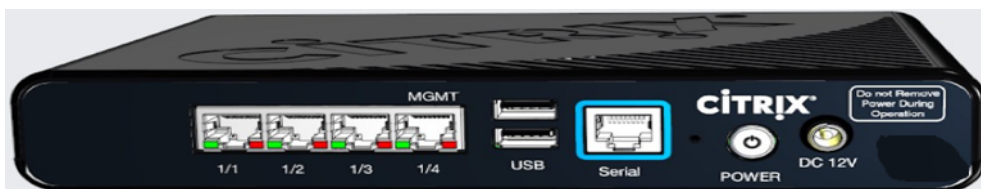
注:

初回ログイン時に、既定のパスワードを任意のパスワードに変更するように要求されます。

Citrix SD-WAN 11.1.0 は、Citrix SD-WAN 110-SE アプライアンスに必要な最小限のソフトウェアバージョンです。Citrix SD-WAN 11.3.0 は、Citrix SD-WAN 110-LTE-WiFi および Citrix SD-WAN 110-WiFi-SE モデルの Wi-Fi 機能をサポートする最小ソフトウェアバージョンです。



LED	説明
イーサネット銅線ポート LED	アクティブ/リンク: 緑
	スピード 1000: オレンジ
	スピード 100: 緑
	スピード 10: オフ
電源 LED	電源オン: 緑に点灯
	電源オフ: 青に点灯
	工場出荷時設定にリセット: 青と緑に点滅 (または) ソフトウェア電源のオフ/オン: 緑色に約 15 秒 (シャットダウン時間) 点滅し、その後青色で 25 秒 間点滅した後、緑に点灯



注:

ポート 1/1 はデフォルトの LAN ポートで、ポート 1/2 はデフォルトの WAN ポートです。ポート 1/3 は無効です。デフォルトの LAN IP オンポートは 192.168.101.1 です。また、LAN クライアントに 192.168.0.50 から 192.168.0.250 の IP アドレスプールを提供するデフォルトの DHCP サーバーも実行します。

ポートラベル	種類	説明
1/1、1/2、1/3	トラフィック	データポートは、ネットワークトラフィックを伝送するために使用されます。

ポートラベル	種類	説明
1/4	管理ポート	管理ポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。このポートは、アプライアンスの初期プロビジョニングに使用できます。 Citrix SD-WAN バージョン 11.1.1 以降では、構成ごとにポート 1/4 をデータポートまたは管理ポートとして使用できます。詳しくは、「 構成可能な管理ポートまたはデータポート 」を参照してください。
USB	USB ポート ×2	USB ポート
シリアル	RJ-45/RS-232	RS232 シリアルコンソールポート。
電源	電源ボタン	電源オフ状態：電源ボタンを押してすぐに放します：アプライアンスの電源を入れます。 電源ボタンを押して 10 秒以上押し続けます：工場出荷時にアプライアンスがリセットされます。アプライアンスは工場出荷時設定にリセットされるまで約 7 分かかります。 電源投入状態：電源ボタンを押してすぐに放します：アプライアンスを正常シャットダウンします。 電源ボタンを押して 5 秒以上押し続けます：アプライアンスを強制的にシャットダウンします。
直流 12V	直流電源	電源情報については、システム仕様を参照してください。

注:

Citrix SD-WAN 11.2.2 リリース以降、ファームウェア E8372 は、SD-WAN 110 アプライアンスでサポートされています。

Citrix SD-WAN 110-lte-wifi-se

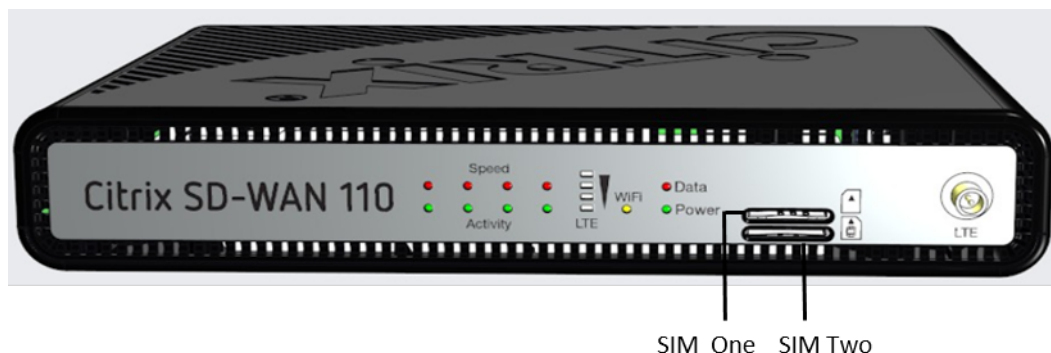
Citrix SD-WAN 110-LTe-WiFi-SE プラットフォームは、マイクロおよび小規模ブランチオフィス/リモートサイト/小売店、および一時的な職場に展開できるブランチサイドアプライアンスです。単一のボックスインブランチソリューションにより、ハードウェアの設置面積を削減し、ブランチ展開を容易にします。

Citrix SD-WAN 110-LTe-WiFi-SE アプライアンスは、デスクトップフォームファクタアプライアンスです。このアプライアンスには、4 GB のメモリと 32 GB のストレージ (SATA-DOM ドライブ) を備えた 2 コアプロセッサが搭載されています。

注

- Citrix SD-WAN 110-LTe-WiFi-SE アプライアンスは、MCN として構成できません。
- 2020 年 3 月 10 日時点で、アプライアンスは **Wi-Fi Ready** として出荷されます。Wi-Fi アクセスポイント機能は、Citrix SD-WAN ソフトウェアバージョン 11.3.0 以降で使用できます。
- Citrix SD-WAN 110-LTe-WiFi-SE アプライアンスは、SD-WAN Orchestrator を使用してアクセスポイントとして構成できます。詳しくは、「[Wi-Fi アクセスポイント](#)」を参照してください。

次の図は、110-LTe-WiFi-SE アプライアンスの前面パネルを示しています。



LED	説明
イーサネット銅線ポート LED	アクティブ/リンク: 緑
	スピード:1000 オレンジ
	スピード 100: 緑
	スピード 10: オフ
電源 LED	電源オン: 緑に点灯
	電源オフ: 青に点灯
	工場出荷時設定にリセット: 青と緑に点滅 (または)

LED	説明
	ソフトウェア電源のオフ/オン: 緑色に約 15 秒 (シャットダウン時間) 点滅し、その後青色で 25 秒間 点滅した後、緑に点灯
Wi-Fi	オフ: Wi-Fi を使用しない 緑に点滅: Wi-Fi は構成されていますが、使用されていません 緑に点灯: Wi-Fi が積極的に使用されています
LTE	消灯: 信号なし 1 バー: かわいそう 2 バー: フェア 3 バー: いいね 4 バー: 優秀
SIM カードスロット	ミニ (2FF) サイズの SIM スロット ×2。Micro (3FF) および Nano (4FF) サイズの SIM を使用するには、アダプターを使用してください。小さい SIM をアダプタにスナップします。アダプタを FRU として注文します。 注: いつでも、アクティブな SIM は 1 つだけです。アプライアンスの電源を入れ、SIM カードを挿入します。

LTE	LTE アンテナオスコネクタ
-----	----------------



注:

ポート 1/1 はデフォルトの LAN ポートで、ポート 1/2 はデフォルトの WAN ポートです。ポート 1/3 は無効です。ポート 1/1 のデフォルトの LAN IP は 192.168.101.1 です。また、LAN クライアントに 192.168.0.50 から 192.168.0.250 の IP アドレスプールを提供するデフォルトの DHCP サーバも実行されます。LTE アプライアンスの場合、LTE SIM スロットはデフォルトの WAN ポートでもあります。WAN ポートは DHCP クライアントとして構成されます。

ポートラベル	種類	説明
LTE	アンテナオスコネクタ	LTE アンテナ用コネクタ。
1/1、1/2、1/3	データポート	データポートは、ネットワークトラフィックを伝送するために使用されます。
1/4	管理ポート	管理ポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。このポートは、アプライアンスの初期プロビジョニングに使用できます。Citrix SD-WAN バージョン 11.1.1 以降では、構成ごとにポート 1/4 をデータポートまたは管理ポートとして使用できます。詳しくは、「 構成可能な管理ポートまたはデータポート 」を参照してください。
USB	USB ポート ×2	USB 2.0 ポート
シリアル	RJ-45/RS-232	RS232 シリアル・コンソール・ポート
電源	電源ボタン	電源オフ状態：電源ボタンを押してすぐに放します：アプライアンスの電源を入れます 電源ボタンを押して 10 秒以上押し続けます：工場出荷時にアプライアンスがリセットされます。アプライアンスは工場出荷時設定にリセットされるまで約 7 分かかります。 電源投入状態：電源ボタンを押してすぐに放します：アプライアンスを正常シャットダウンします。 電源ボタンを押して 5 秒以上押し続けます：アプライアンスを強制的にシャットダウンします。

ポートラベル	種類	説明
直流 12V	直流電源	電源情報については、システム仕様を参照してください。

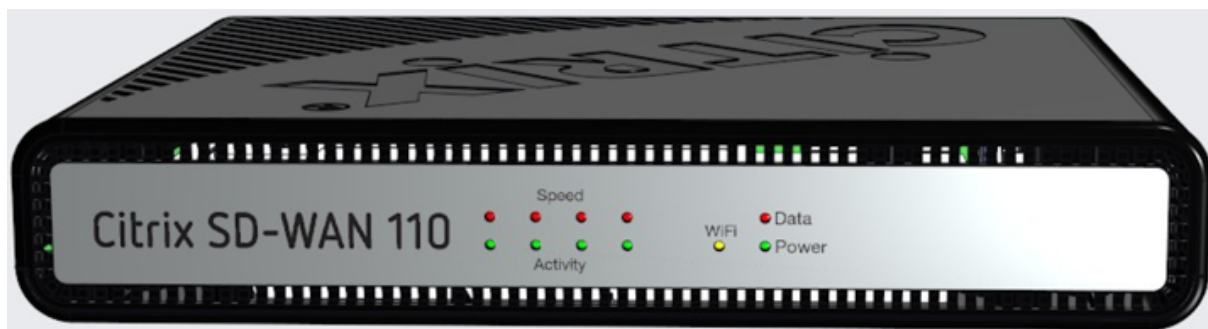
Citrix SD-WAN 110-WiFi-SE

Citrix SD-WAN 110-WiFi-SE プラットフォームは、マイクロオフィスおよび小規模ブランチオフィス/リモートサイト/小売店、および一時的な職場に展開できるブランチサイドアプライアンスです。これは、ハードウェアフットプリントを削減し、ブランチ展開を容易にする単一のボックス・イン・ブランチ・ソリューションです。

Citrix SD-WAN 110-WiFi-SE アプライアンスは、デスクトップフォームファクタアプライアンスです。このアプライアンスには、4 GB のメモリと 32 GB のストレージ（SATA-DOM ドライブ）を備えた 2 コアプロセッサが搭載されています。

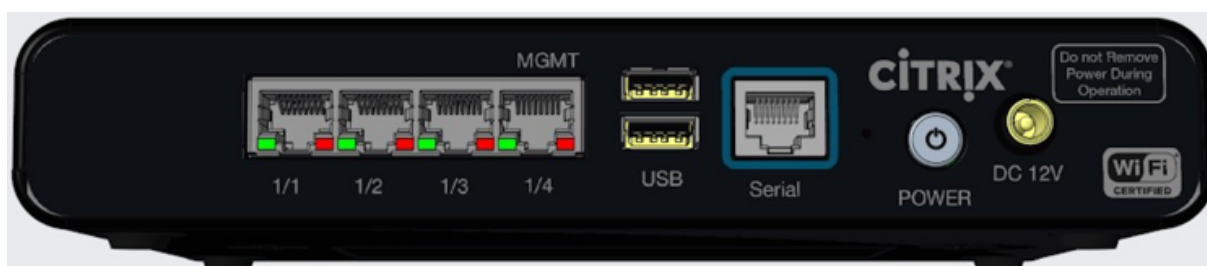
注

- Citrix SD-WAN 110-WiFi-SE アプライアンスは、MCN として構成できません。
- Citrix SD-WAN 110-WiFi-SE アプライアンスは、SD-WAN Orchestrator を使用してアクセスポイントとして構成できます。詳しくは、「[Wi-Fi アクセスポイント](#)」を参照してください。



LED	説明
イーサネット銅線ポート LED	アクティブ/リンク: 緑
	スピード:1000 オレンジ
	スピード 100: 緑
	スピード 10: オフ
電源 LED	電源オン: 緑に点灯
	電源オフ: 青に点灯
	工場出荷時設定にリセット: 青と緑に点滅 (または)

LED	説明
	ソフトウェア電源のオフ/オン: 緑色に約 15 秒 (シャットダウン時間) 点滅し、その後青色で 25 秒 間点滅した後、緑に点灯
Wi-Fi	オフ: Wi-Fi を使用しない
	緑に点滅: Wi-Fi は構成されていますが、使用されていません
	緑に点灯: Wi-Fi が積極的に使用されています



注

ポート 1/1 はデフォルトの LAN ポートで、ポート 1/2 はデフォルトの WAN ポートです。ポート 1/3 は無効です。デフォルトの LAN IP は 192.168.101.1 です。WAN ポートは DHCP クライアントとして構成されます。

ポートラベル	種類	説明
1/1、1/2、1/3	データポート	データポートは、ネットワークトラフィックを伝送するために使用されます。
1/4	管理ポート	管理ポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。このポートは、アプライアンスの初期プロビジョニングに使用できます。Citrix SD-WAN バージョン 11.1.1 以降では、構成ごとにポート 1/4 をデータポートまたは管理ポートとして使用できます。詳しくは、「 構成可能な管理ポートまたはデータポート 」を参照してください。

ポートラベル	種類	説明
USB	USB ポート×2	USB 2.0 ポート
シリアル	RJ-45/RS-232	RS232 シリアル・コンソール・ポート
電源	電源ボタン	<p>電源オフ状態：電源ボタンを押してすぐに放します：アプライアンスの電源を入れます</p> <p>電源ボタンを押して 10 秒以上押し続けます：工場出荷時にアプライアンスがリセットされます。アプライアンスは工場出荷時設定にリセットされるまで約 7 分かかります。</p> <p>電源投入状態：電源ボタンを押してすぐに放します：アプライアンスを正常シャットダウンします。</p> <p>電源ボタンを押して 5 秒以上押し続けます：アプライアンスを強制的にシャットダウンします。</p>
直流 12V	直流電源	電源情報については、システム仕様を参照してください。

SD-WAN 110 SE アプライアンスのマウント

Citrix SD-WAN 110-SE アプライアンスは、次のインストールモードでインストールできます。

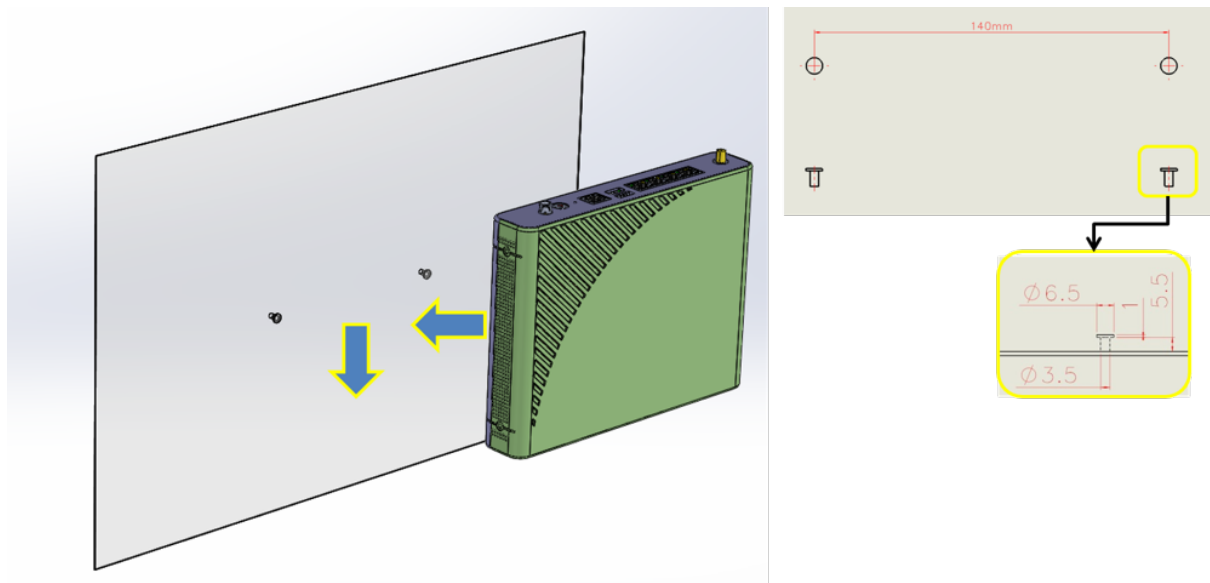
- デスクトップマウント
- ウォールマウント
- ラックマウント

デスクトップマウント

Citrix SD-WAN 110-SE アプライアンスは、アプライアンスパッケージに同梱されているゴム製の脚を使用してデスクトップマウントできます。

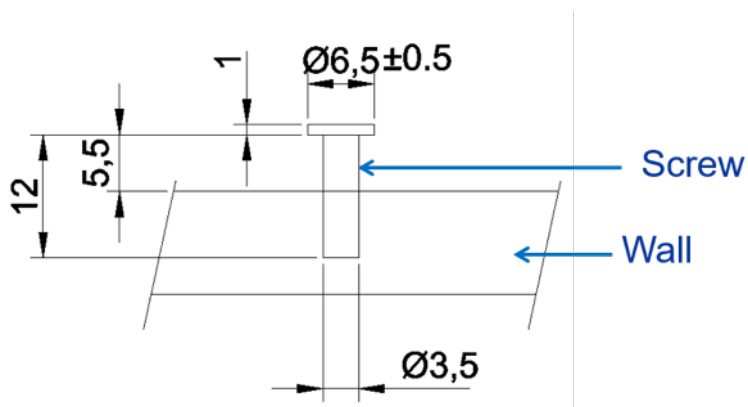
アプライアンスを壁に取り付け

Citrix SD-WAN 110-SE アプライアンスは、アプライアンスのネジスロットを壁のネジに取り付けて調整することで、壁面に取り付けることができます。



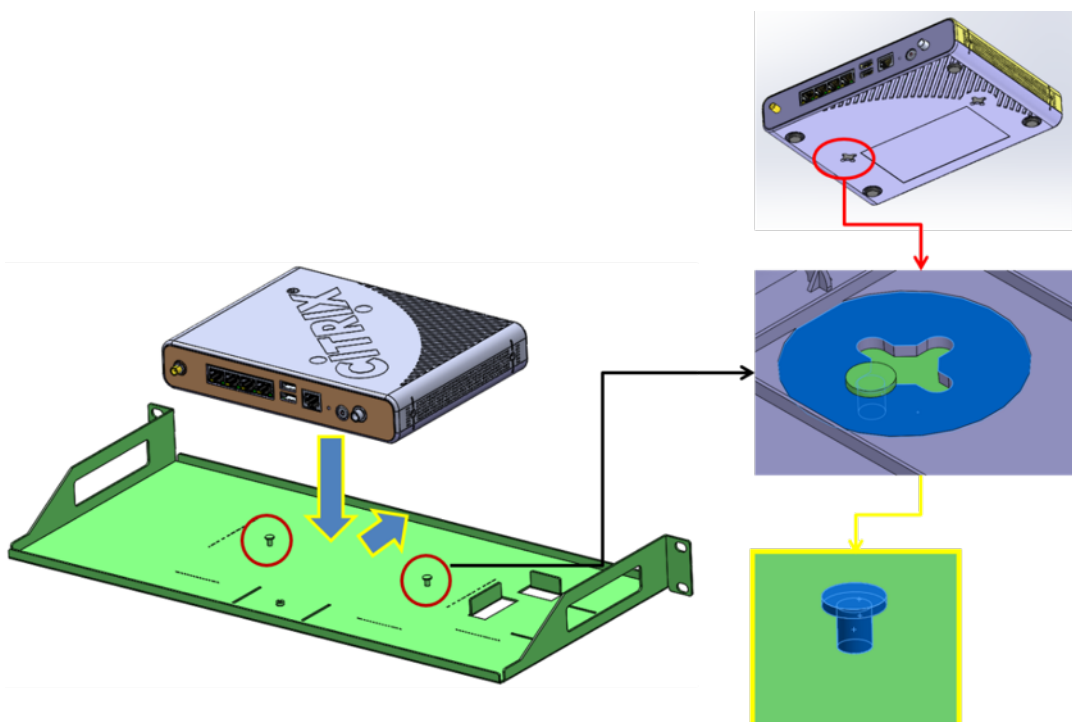
次の寸法の 2 本の壁取り付けネジを使用します。

- ネジの長さ:12 ミリメートル。
- 壁のねじ込み: 5.5 ミリメートル
- スクリューヘッド: 6.0mm~7.5mm
- ネジ本体:3.5mm

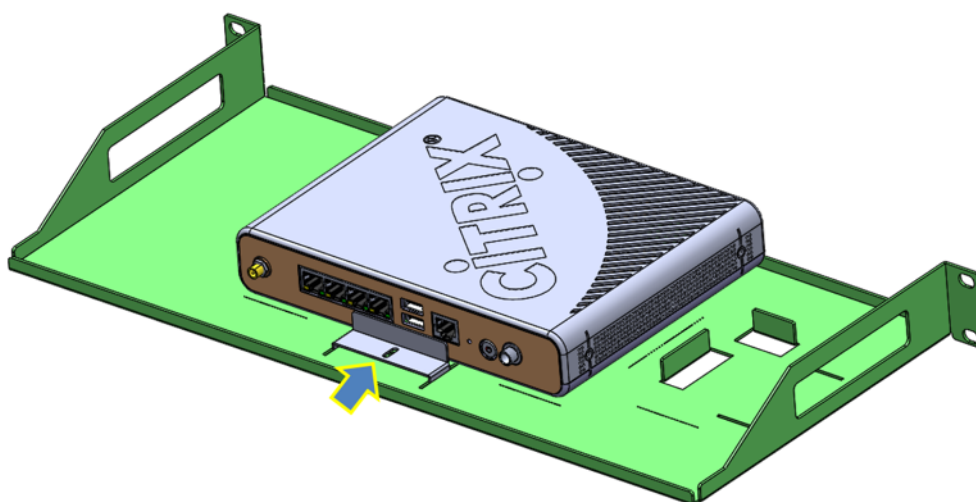


アプライアンスのラックマウント

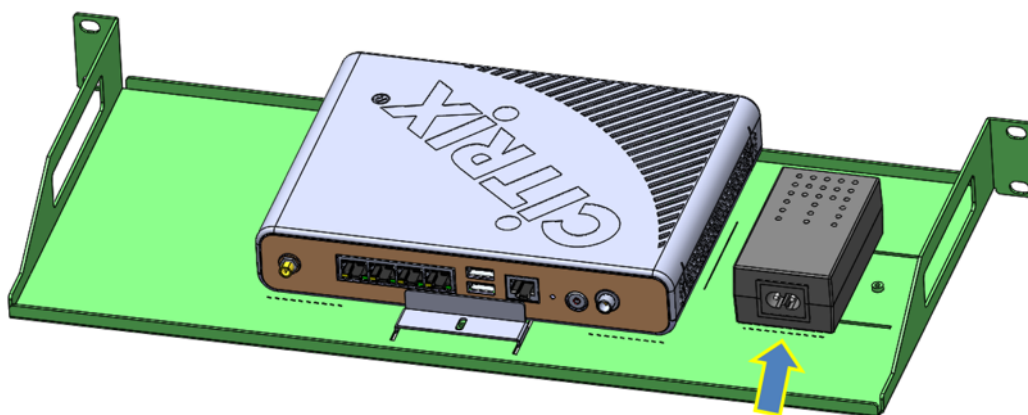
1. 付属のネジで棚をラックに固定します。
2. シャーシを取り付けます。アプライアンスのネジスロットを棚のポジショニングネジに置き、スライドさせて、所定の位置にロックします。



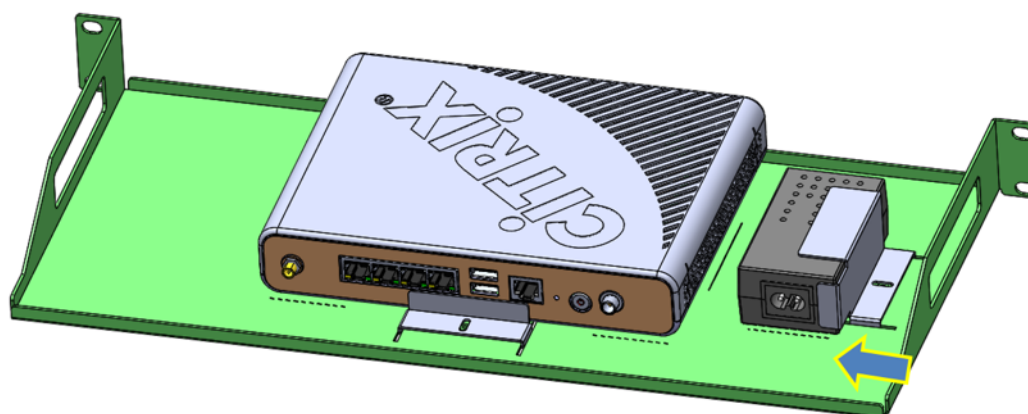
3. シャーシ固定ブラケットを取り付けて、アプライアンスを所定の位置に固定します。シャーシ固定ブラケットをスロットに置き、ネジで固定します。



4. 電源アダプタを取り付けます。アダプタスロットに電源アダプタを置きます。



5. アダプタ固定ブラケットを取り付けて、電源アダプタを固定します。アダプタ固定ブラケットをスロットに置き、ネジで固定します。



LTE アンテナの取り付け

Citrix SD-WAN 110-LTE-WiFi-SE アプライアンスを LTE モデムとして使用するには、アプライアンスにアンテナを取り付けます。アンテナは、アプライアンスパッケージに含まれています。Citrix SD-WAN 110-LTE-WiFi-SE アプライアンスには、アプライアンスの前面と背面に 2 つの SMA 同軸オスコネクタがあります。アンテナは、独立した回転 SMA メスコネクタを備えています。

注

LTE セルラー接続を向上させるため、両方の LTE アンテナが取り付けられていることを確認します。

アプライアンスにアンテナを取り付けるには：

1. アンテナ SMA 同軸コネクタ (F) をアプライアンスの SMA 同軸コネクタ (M) に置き、コネクタが締まるまでアンテナコネクタを時計回りに回します。

注

推奨トルクは 0.20-0.28 ニュートンメートル (N m) です。



2. アンテナの方向と方向を調整します。



3. 同様に、もう一方のアンテナをアプライアンスの背面の SMA 同軸コネクタ (M) に接続します。

GUI および CLI を使用した LTE 機能の設定の詳細については、[110 SE LTE アプライアンスでの LTE 機能の設定](#)を参照してください。

ハードウェア仕様の概要

仕様	110-SE、110-lte-wifi-SE、110-wifi-SE
規制モデル番号	SD-WAN 110、SD-WAN 110-LTE-WiFi、SD-WAN 110-WiFi
メモリ	4GB
不揮発性ストレージ	32GB

仕様	110-SE、110-lte-wifi-SE、110-wifi-SE
LTE	3G, 4G. Citrix SD-WAN 110-LTe-WiFi-SE アプライアンスのみ。
LAN ポート	4xGbE RJ45
USB 2.0	2
SIM スロット	X2 2FF. FRU として注文する 3FF と 4FF 用のアダプタ。Citrix SD-WAN 110-LTe-WiFi-SE アプライアンスのみ。
LTE モジュール	Quectel EG25-G. Citrix SD-WAN 110-LTe-WiFi-SE アプライアンスのみ。
電源定格	
電源装置	シングル (外部)
入力電圧/周波数範囲 (ノーマル)	100—240 VAC、50—60 Hz
入力電流	0.6 A
ワット数 (最大)	24 W
アプライアンスの評価	
入力電圧	12VDC
入力電流	2.0 A
ワット数 (標準)	10 W
ワット数 (最大)	15.5 W
熱放散	
エアフロー (前面から背面)	N/A: ファンレス
典型的な放熱	34BTU
最大熱放散	53BTU
機械	
パッケージ重量 (kg)	0.9 kg
パッケージ寸法	長さ 38.5cm× 幅 25.4cm× 高さ 9.01cm
システム重量 (kg)	0.62 kg
システム寸法	長さ 21.59cm× 幅 15.87cm× 高さ 3.81cm
環境と規制	
動作温度	0~40 度摂氏

仕様	110-SE、110-lte-wifi-SE、110-wifi-SE
湿度範囲	5~90%、結露しないこと
業界標準	GCF、PTCRB、Wi-Fi 認定™
安全認定	CB、UL
法令順守	CE、FCC、ISD (IC)、RCM、VCCI & MIC、アナテル、BTK、BSMI & NCC (台湾)、CITC、CCC、エナコム、ICASA、IFT、SRRC、WPC、DWLFM & TRA (バーレーン)、TRA (UAE)、サブテル、SDPPI、CAK、MCINET、NCC (ナイジェリア)、CRA
環境コンプライアンス	RoHS 3、WEEE、REACH

Quectel EG25-G (LTE) 用 EG25-G TX (送信) 出力電力 (dBm)

頻度	最大値 (dBm)
WCDMA B1/B2/B4/B5/B6/B8/B19	24+1/-3dB
LTE-FDD B1/B2/B3/B3/B4/B5/B7/B8/B12/B13/B13/B18/B19/B20/B25/B26/B28	23+/-2dB
LTE-TDD B38/B39/B40/B41	23+/-2dB

Quectel EG25-G (LTE) 向け EG25-G RX 受信感度 (dBm)

頻度	プライマリ (dBm)
WCDMA B1	-108.2
WCDMA B2	-109.5
WCDMA B4	-108.5
WCDMA B5	-109.2
WCDMA B6	-109
WCDMA B8	-109.5
WCDMA B19	-109
LTE-FDD B1 (10M)	-97.3
LTE-FDD B2 (10M)	-98

頻度	プライマリ (dBm)
LTE-FDD B3 (10M)	-97.5
LTE-FDD B4 (10M)	-97.8
LTE-FDD B5 (10M)	-98
LTE-FDD B7 (10M)	-97.3
LTE-FDD B8 (10M)	-98
LTE-FDD B12 (10M)	-98
LTE-FDD B13 (10M)	-98
LTE-FDD B18 (10M)	-98
LTE-FDD B19 (10M)	-98
LTE-FDD B20 (10M)	-98
LTE-FDD B25 (10M)	-98
LTE-FDD B26 (10M)	-98
LTE-FDD B28 (10M)	-98.1

Quectel EG25-G (LTE) のアンテナゲイン

| イーサロニクス LTE アンテナ 1004112-C003 |

|—|—|—|—|

| 部品番号 100412-ブロードバンド外部 LTE/セルラーアンテナ |

| 周波数 | 690—960 | 1710—2220 | 2500—2700 |

| ピークゲイン | 1.18 dBi | 4.5 dBi | 4.0 dBi |

ワイヤレス WAN (LTE) の仕様

仕様	110-SE と 110-lte-wifi-SE
モデム	クエクトル EG25-G
地理学	グローバル
LTE カテゴリ	Cat4 (理論 150Mbps DL; 50Mbps UL)
キャリア集約	いいえ
SIM スロット	2 (アクティブは 1 つのみ)
LTE バンド	B1/B2/B3/B4/B5/B7/B8/B12/B13/B18/B19/B20/B25/B26/B28/

仕様	110-SE と 110-lte-wifi-SE
出力電力	クラス 3 (23 dBm±2 dB)
理論上の速度	150 Mbps ダウンリンク/50Mbps アップリンク

無線 LAN (Wi-Fi) の仕様

|Wi-Fi 機能 ||110-wifi-SE と 110-LTE-WiFi | アンテナピークゲイン |

|----|----|----|---|

|Wi-Fi 規格 ||802.11 a/b/g/n/ac |

|周波数帯域 * || 2412 MHz, 2417 MHz, 2422 MHz, 2427 MHz, 2432 MHz, 2437 MHz, 2442 MHz, 2447 MHz, 2452 MHz, 2457 MHz, 2462 MHz, 2472 MHz| 2.6 dBi |

|| チャネル幅:20 MHz | 5180 MHz, 5200 MHz、 5220MHz、 5240MHz, 5745 MHz, 5765 MHz, 5785 MHz, 5825 MHz| 5.0 dBi |

|| チャネル幅:40 MHz | 5190MHz, 5230 MHz, 5755 MHz| 5.0 dBi || | チャネル幅:20 MHz

| 5180MHz, 5200MHz, 5220 MHz, 5240 MHz, 5240 MHz, 5755 MHz, 5765 MHz、 5785 MHz、 5805 MHz、 5825 MHz| 5.0dBi

|| | チャネル幅:80 MHz | 5210 MHz、 5775 MHz| 5.0 dBi |

|最大同時 SSID | |4|

*-国ごとにサポートされているバンドに応じて、一部の国では一部の周波数帯域/チャンネルとチャンネル幅を利用できません。デバイスの出力電力は、ホストの国/ドメインによって設定された規制制限内で動作するように構成されています。

Wi-Fi 認定™ ロゴは、Wi-Fi アライアンス® の認証マークです。

Citrix SD-WAN 210 Standard Edition アプライアンス

April 15, 2021

Citrix SD-WAN 210-SE アプライアンスは、小規模なブランチオフィスで使用するための 1U アプライアンスです。このアプライアンスには、4 GB のメモリと 64 GB のストレージを備えた 2 コアプロセッサが搭載されています。

Citrix コンプライアンス規制モデルは次のとおりです。

- SD-WAN 210-SE (非 LTE) -NS-SDW-210
- SD-WAN 210-SE LTE-NS-SDW-210-LTE-R1、NS-SDW-210-LTE-R2、NS-SDW-210-LTE-RC

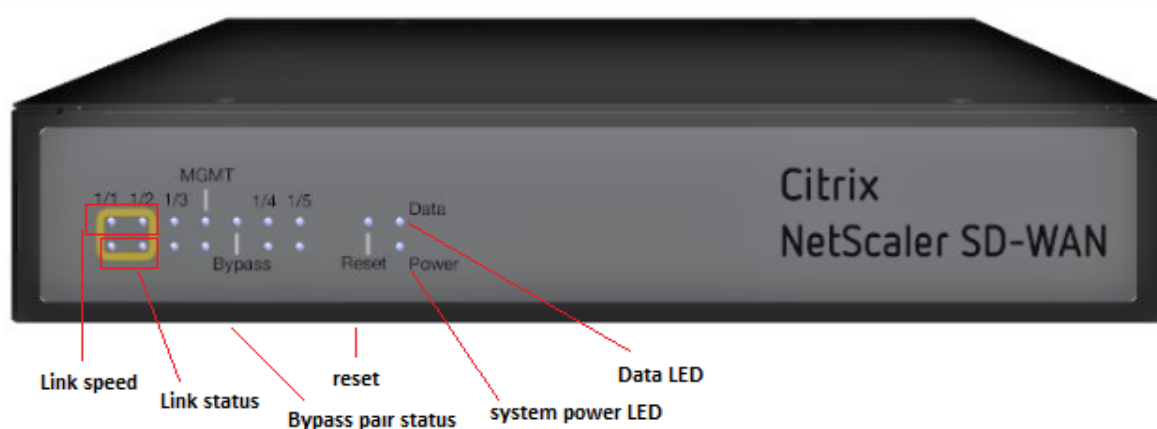
詳細については、Citrix SD-WAN プラットフォーム [データシート](#) を参照してください。

注

- Citrix SD-WAN 210-SE および Citrix SD-WAN 210-SE LTE は、SD-WAN Orchestrator が管理するネットワーク内のみ MCN として構成できます。
- 新しいユーザーインターフェイスを使用して、Citrix SD-WAN 210-SE アプライアンスを構成できます。詳しくは、「[SD-WAN アプライアンスのユーザー・インターフェイス](#)」を参照してください。Citrix SD-WAN 210-SE を MCN としてプロビジョニングすると、レガシーユーザーインターフェイスにリダイレクトされます。

次の図に、210 SE アプライアンスのフロントパネルを示します。

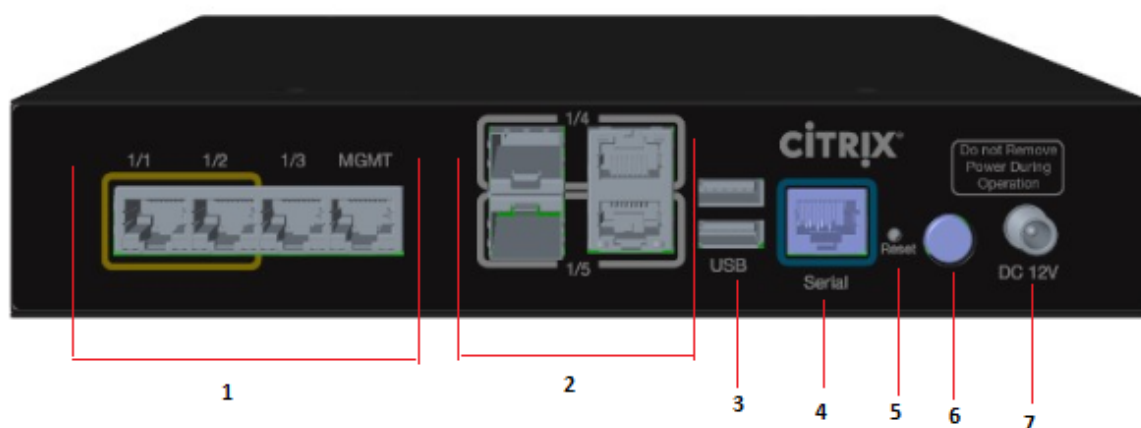
Figure 1. SD-WAN 210-SE front panel



LED	説明
イーサネット銅線ポート LED	アクティブ/リンク: 緑
	スピード 1000: オレンジ
	スピード 100: 緑
	スピード 10: オフ
SIM カードスロット	ミニ (2FF) サイズの SIM スロット×2。Micro (3FF) および Nano (4FF) サイズの SIM を使用するには、アダプターを使用してください。小さい SIM をアダプタにスナップします。アダプタを FRU として注文します。 注: いつでも、アクティブな SIM は 1 つだけです。アプライアンスの電源を入れ、SIM カードを挿入します。
LED をバイパスする	ノーマルモード: 緑
	バイパスモード: オレンジ。

LED	説明
イーサネットファイバポート	アクティブ/リンク: 緑 スピード:1000: オレンジ
電源 LED	電源オン: 緑 電源オフ: オフ

Figure 2. SD-WAN 210 SE back panel



210 SE アプライアンスの背面パネルには、次のコンポーネントが表示されます。

インターフェイス	ポートラベル	種類	説明
1	1/1 および 1/2	バイパス/FTW	配線不可能
	1/3	トラフィック	ネットワークトラフィック
	経営陣	RJ-45	銅線イーサネット (RJ45) 管理ポート。管理ポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。このポートは、仮想 WAN の初期プロビジョニングに使用できます。

インターフェイス	ポートラベル	種類	説明
2	1/4 および 1/5	SFP とイーサネット（組み合わせポート）	上下にそれぞれ SFP とイーサネットの組み合わせとして使用します。
3	USB	2	USB ポート
4	コンソール	RS-232 シリアル	RS232 シリアルコンソールポート。
5	リセットする	リセットボタン	詳細については、Citrix テクニカルサポートにお問い合わせください。
6	パワー	電源ボタン	電源ボタンを押して、アプライアンスの電源をオンまたはオフにします。スイッチを 5 秒間押して、電源を切ります。
7	電源装置	直流電源	電源アダプタ 1 つ。電力定格:40 W、電圧:12 V、電流:3.33 A。

注:

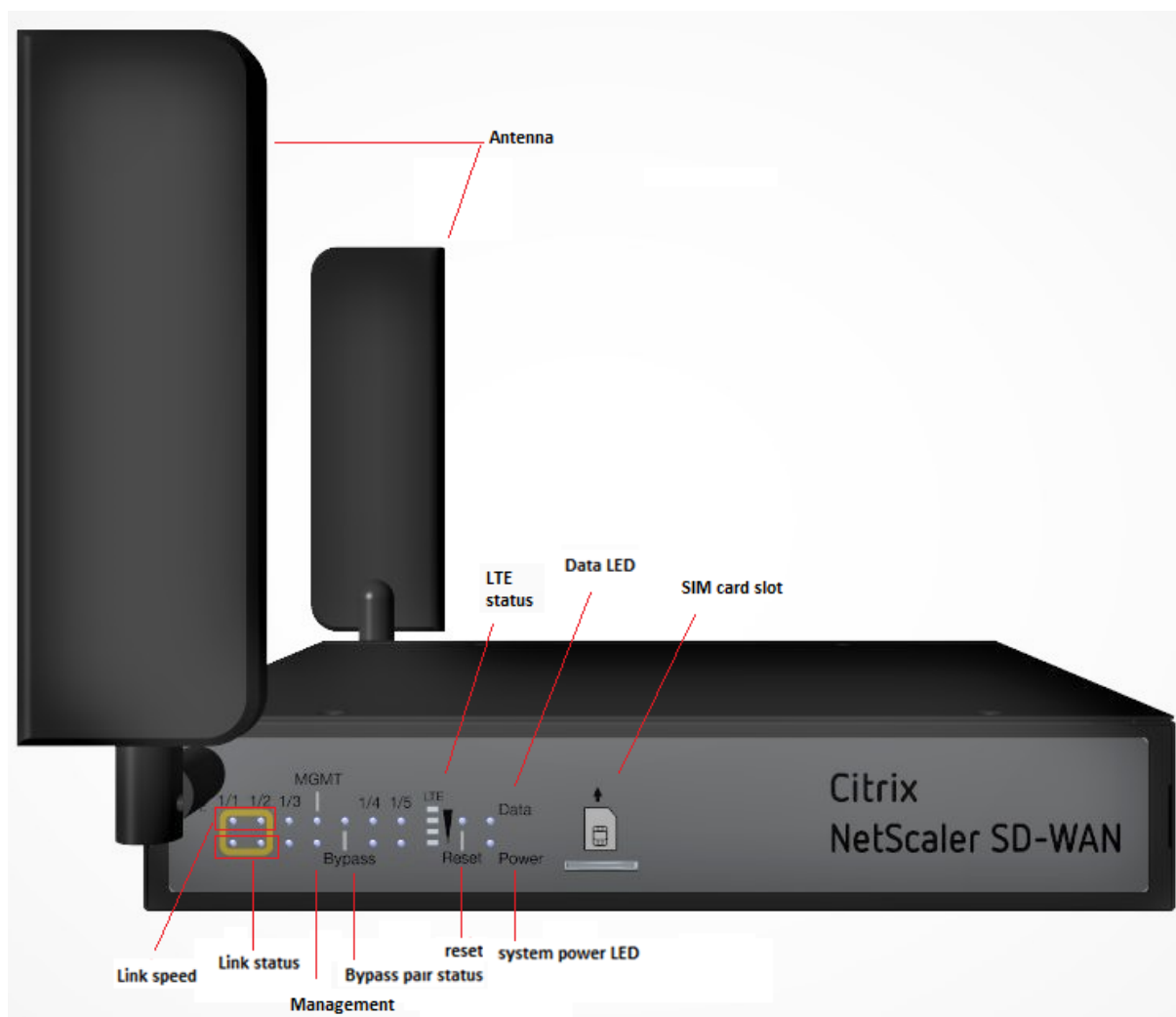
Citrix SD-WAN 11.2.2 リリース以降、ファirmware ドングル E8372 は、SD-WAN 210 アプライアンスでサポートされています。

Citrix SD-WAN 210-SE LTE

210 SE LTE アプライアンスは、1U アプライアンスです。このアプライアンスには、4 GB のメモリと 64 GB のストレージを備えた 2 コアプロセッサが搭載されています。

次の図は、210 SE LTE アプライアンスの前面パネルを示しています。

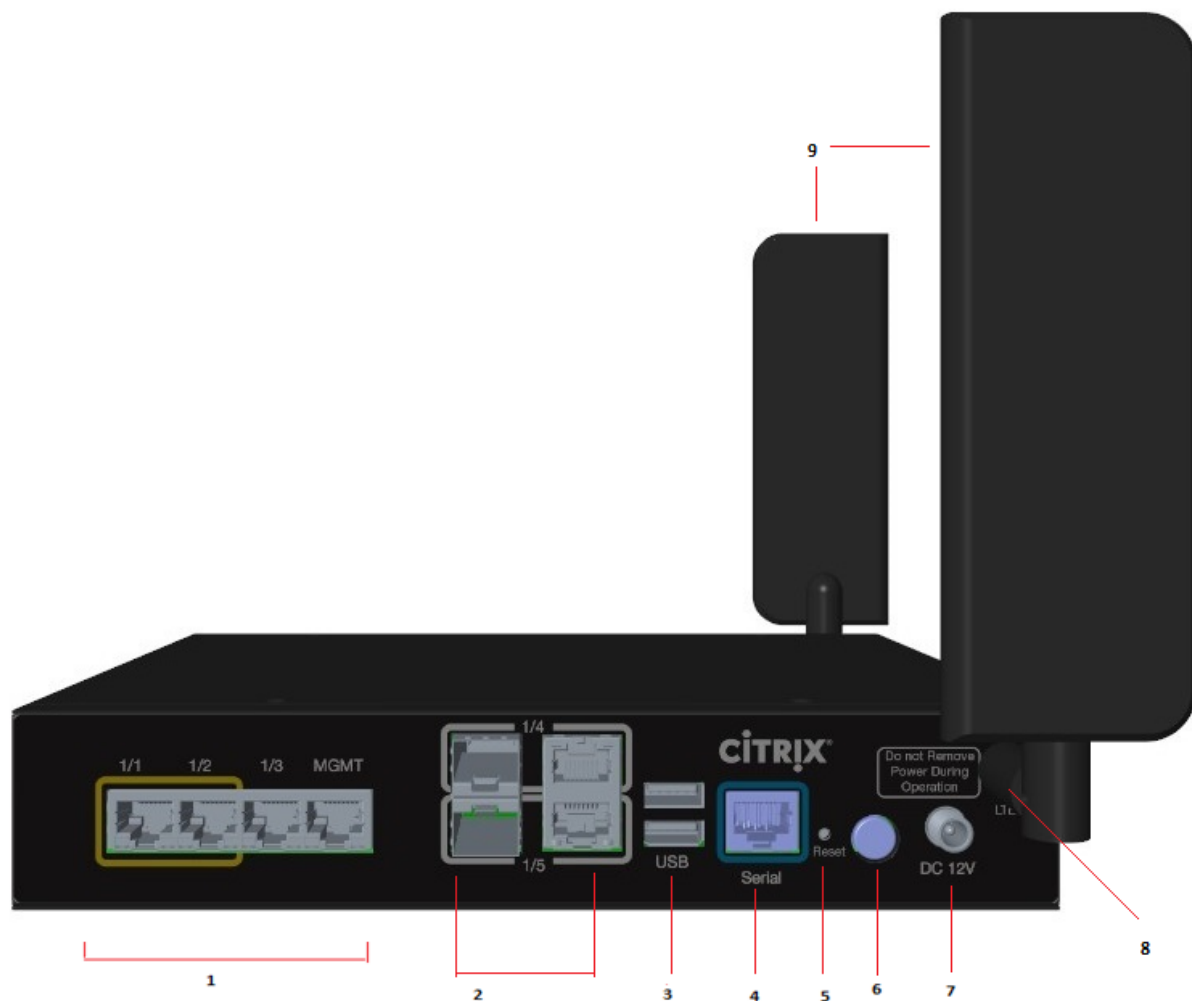
図 3. アンテナ付きの 210 SE (LTE) フロントパネル



LED	説明
イーサネット銅線ポート LED	アクティブ/リンク: 緑
	スピード:1000 オレンジ
	スピード 100: 緑
LED をバイパスする	スピード 10: オフ
	ノーマルモード: 緑 バイパスモード: オレンジ。
イーサネットファイバポート	アクティブ/リンク: 緑
	スピード:1000: オレンジ **
システム LED とデータの LED	システム: 電源オン: 緑

LED	説明
	システム: 電源オフ: オフ
	データアクセスストレージ: 青

図 4. アンテナ付きの 210 SE (LTE) バックパネル



210 SE LTE アプライアンスの背面パネルには、次のコンポーネントが表示されます。

インターフェイス	ポートラベル	種類	説明
1	1/1 および 1/2	バイパス/FTW	FTW ポート
	1/3	トラフィック	トラフィックポート

インターフェイス	ポートラベル	種類	説明
	管理	RJ-45	銅線イーサネット (RJ45) 管理ポート。管理ポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。このポートは、仮想 WAN の初期プロビジョニングに使用できます。
2	1/4 および 1/5	SFP とイーサネット (組み合わせポート)	上下にそれぞれ SFP とイーサネットの組み合わせとして使用します。
3	USB	2	USB ポート
4	コンソール	RS-232 シリアル	RS232 シリアル・コンソール・ポート
5	リセットする	リセットボタン	詳細については、Citrix テクニカルサポートにお問い合わせください。
6	パワー	電源ボタン	電源ボタンを押して、アプライアンスの電源をオンまたはオフにします。スイッチを 5 秒間押して、電源を切ります。
7	電源装置	直流電源	電源アダプタ 1 つ。電力定格:40 W、電圧:12 V、電流:3.33 A。
8	アンテナコネクタ	オスコネクタ	アンテナ用コネクタ
9	2つのアンテナ	LTE アンテナ	アプライアンスに同梱されているアンテナ。

LTE アンテナの取り付け

Citrix SD-WAN 210 SE LTE アプライアンスを LTE モデムとして使用するには、アプライアンスにアンテナを取り付けます。アンテナは、アプライアンスパッケージに含まれています。210 SE LTE アプライアンスには、アプライアンスの前面と背面に 2 つの SMA 同軸オスコネクタがあります。アンテナは、独立した回転 SMA メスコネクタを備

えています。

注

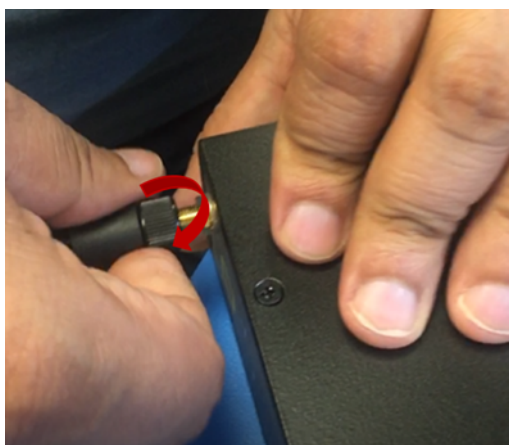
LTE セルラー接続を向上させるため、両方の LTE アンテナが取り付けられていることを確認します。

アプライアンスにアンテナを取り付けるには：

1. アンテナ SMA 同軸コネクタ (F) をアプライアンスの SMA 同軸コネクタ (M) に置き、コネクタが締まるまでアンテナコネクタを時計回りに回します。

注

推奨トルクは 1.8~2.5 ポンドのカインチです。



2. アンテナの方向と方向を調整します。



3. 同様に、もう一方のアンテナをアプライアンスの背面の SMA 同軸コネクタ (M) に接続します。

GUI および CLI を使用した LTE 機能の設定の詳細については、[210 SE LTE アプライアンスでの LTE 機能の構成](#)を

参照してください。

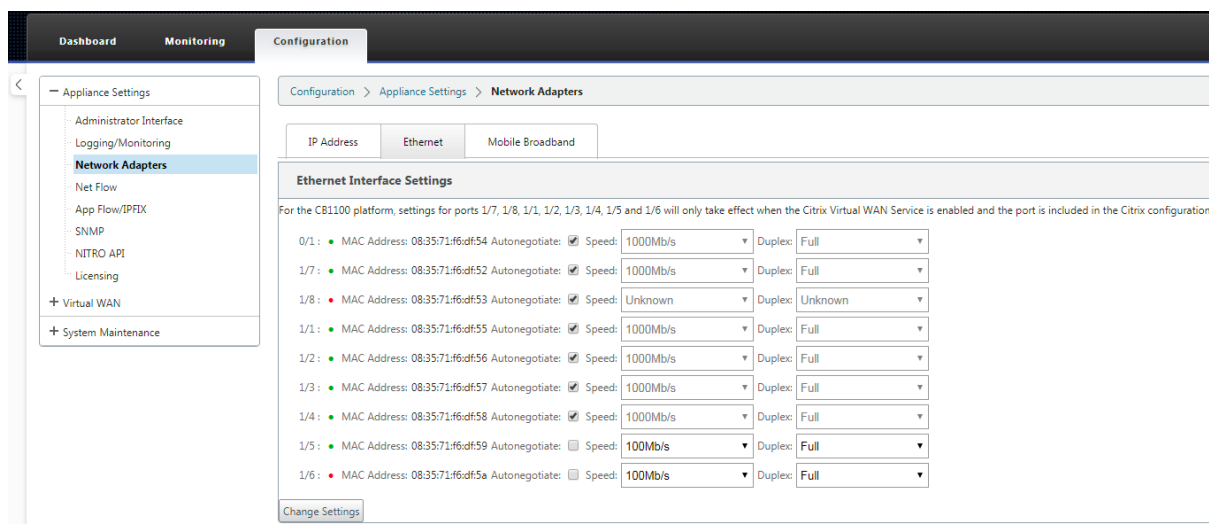
miric-E1T1 FE/GBE SFP に対する Citrix SD-WAN 210 プラットフォームのサポート

210 アプライアンスでは、SFP ポート 1/5 および 1/6 に対して、次の 2 種類の miriC SFP がサポートされています。

1. MiRiC-E1T1 FE SFPs.
2. MiRiC-E1T1 GBE SFPs.

miric-E1T1 FE SFP は、速度を 100 Mbps、デュプレックスを全二重に設定する必要があります。miric-E1T1 GBE SFP は、速度を 1 Gbps、デュプレックスを全二重に設定する必要があります。

構成するには、SD-WAN アプライアンスの GUI に移動し、**[構成] > [ネットワークアダプタ] > [イーサネット]** ページに移動します。



miriC SFP ウェブサービスにアクセスする

1. SFP トランシーバのデフォルトの管理 IP アドレスは 192.168.205.1 です。このアドレスを使用して、SFP Web サービスで関連する設定 (T1 や E1 など) を設定できます。IP アドレスは 192.168.205.1 以外に変更できません。ただし、IP アドレスの競合は避けてください。
2. 管理への SFP アクセスを有効にするには、次の手順を実行します。
 - **ssh admin@ (IP アドレス)** 経由でアプライアンスの CLI にログインします
 - 実行: `sfp_access`
 - 1/5 でアクセスを有効にするには、次のコマンドのいずれかを実行します。
 - `enable 1/5 # GBE トランシーバのために動作しすでに設定されている場合のみ。`
 - `enable 1/5 100 # -FE トランシーバでのみ動作します`
 - `enable 1/5 1000 # -GBE トランシーバでのみ動作します`

- 1/5 100 172.217.43.2 #-FE トランシーバの場合、172.217.43.0/24 でユーザがデフォルトの IP を IP に変更すると仮定します
- 有効 1/5 1000 172.217.43.2 #-GBE トランシーバの場合、ユーザがデフォルトの IP を 172.217.43.0/24 の IP に変更したと想定しています。

注:

1/5 で管理アクセスを有効にすると、1/6 の管理アクセスは自動的に無効になり、逆に無効になります。

- 管理へのアクセスを無効にする手順は、次のとおりです。
 - SSH 管理者 @ (IP アドレス) 経由でアプライアンスの CLI にログインします
 - 実行:sfp_access
 - 実行: 無効にする
- ステータスを表示する手順は、次のとおりです。
 - SSH 管理者 @ (IP アドレス) 経由でアプライアンスの CLI にログインします
 - 実行:sfp_access
 - 実行: ステータス
- 設定が完了したら、管理アクセスを無効にしてください。
- アプライアンスが再起動されると、管理アクセスは自動的に無効になります。
- 仮想サービスが再起動されると、管理アクセスは、有効または無効の操作が完了するまで構成されたままになります。
- アプライアンスを無効にすると、SFP への管理アクセスは失われます。
- アプライアンスが再び有効になると、管理アクセスは回復されます。

3. SFP トランシーバの E1 または T1 タイプを設定するには、次の手順を実行します。

- クライアントマシンは、アプライアンス管理サブネットと同じ IP サブネットに存在する必要があります。
- クライアントマシンには、アプライアンス管理 IP をゲートウェイとする SFP トランシーバ IP アドレス 192.168.205.0/24 のサブネットへのルートが必要です。
- ブラウザを開き、[SFP トランシーバの管理](#)
- デフォルトのユーザー名:su
- デフォルトのパスワード:1234
- インターフェイスタイプ (E1 または T1) を設定するには、**[設定] > [物理ポート]** に移動し、ドロップダウンメニューから **[E1]** または **[T1]** を選択し、**[保存]** ボタンをクリックします。

ハードウェア仕様の概要

April 15, 2021

仕様	210-SE と 210-SE LTE
規制モデル番号	NS-SDW-210, NS-SDW-210-LTE-R1, NS-SDW-210-LTE-R2
プロセッサ	Intel C3338
メモリ	4GB DR4 PC4-2400 SODIMM
電源アダプタの数	1
AC 電源 (アダプタ) 電圧、周波数および電流	115–230 V 50–60 Hz 1.5A
最大 AC 消費電力	18.9 W
最大 DC 消費電力	13.2 W
エアフロー (前面から背面)	ファンレス
放熱	45.0384 BTU
パッケージ重量 (ポンド)	5 ポンド
システム重量 (ポンド)	2.9 lb
幅	175 mm
高さ	42 mm
奥行き	232 mm
動作温度	0–40°C
湿度範囲 (結露しないこと)	5% から 90% RH
安全認定	UL
規制認定	FCC、CE
環境コンプライアンス	RoHS/REACH/PFOS/CoM/WEEE
安全認定	C UL 米国上場しました
LTE アドバンスドモジュール (CAT6)	Sierra Wireless™ EM7455、Sierra Wireless™ EM7430、Taoglas TG.30.8113 (理論的 300 Mbps DL、デュアルキャリアアグリゲーション、50 Mbps UL)
LTE アドバンスドバンド (CAT6)	1, 2, 3, 4, 5, 7, 8, 12, 13, 20, 25, 26, 29, 30, 41; 1, 3, 5, 7, 8, 18, 19, 21, 28, 38, 39, 40, 41

仕様	210-SE と 210-SE LTE
法令順守	FCC, IC, CE, ICASA, ENACOM, IFETEL, ANATEL, RCM, BIS
業界認定	PTCRB、GCF

シエラワイヤレス™ EM7455、シエラワイヤレス™ EM7430 の RX 受信感度 (dBm)

LTE バンド	AirPrime EM7455 (SD-WAN-210-LTE-R1)	LTE バンド	AirPrime EM7430 (SD-WAN-210-LTE-R2)
バンド 1	-97.5	バンド 1	-97.5
バンド 2	-97.0	バンド 3	-97.1
バンド 3	-97.0	バンド 5	-99.3
バンド 4	-97.5	バンド 7	-96.4
バンド 5	-98.5	バンド 8	-99.3
バンド 7	-96.5	バンド 18	-98.9
バンド 8	-99.0	バンド 19	-99.3
バンド 12	-97.5	バンド 21	-98.2
バンド 13	-97.0	バンド 28	-97.3
バンド 20	-98.5	バンド 38	-97.2
バンド 25	-97.0	バンド 39	-98.4
バンド 26	-98.5	バンド 40	-96.0
バンド 29	-	バンド 41	-97.0
バンド 30	-95.5		
バンド 41	-97.5		

UMTS バンド	AirPrime EM7455 (SD-WAN-210-LTE-R1)	UMTS バンド	AirPrime EM7430 (SD-WAN-210-LTE-R2)
バンド 1	-110.5	バンド 1	-110.1
バンド 2	-110.0	バンド 5	-111.4
バンド 3	-109.5	バンド 6	-112.0

UMTS バンド	AirPrime EM7455 (SD-WAN-210-LTE-R1)	UMTS バンド	AirPrime EM7430 (SD-WAN-210-LTE-R2)
バンド 4	-110.0	バンド 8	-112.0
バンド 5	-111.0	バンド 9	-110.2
バンド 8	-111.5	バンド 19	-111.7

Sierra Wireless™ EM7455、Sierra Wireless™ EM7430 用の TX (送信) 出力電力 (dBm)

LTE バンド	AirPrime EM7455 (SD-WAN-210-LTE-R1)	LTE バンド	AirPrime EM7430 (SD-WAN-210-LTE-R2)
バンド 1、2、3、4、5、 8、12、13、20、25、26	+23 dBm +/-1 dB	バンド 1、3、5、8、18、 19、21、28、29	+23 dBm +/-1 dB
バンド 7、30、41	+22 dBm +/-1 dB	バンド 7、38、40、41	+22 dBm +/-1 dB

UMTS バンド	AirPrime EM7455 (SD-WAN-210-LTE-R1)	UMTS バンド	AirPrime EM7430 (SD-WAN-210-LTE-R2)
バンド 1 (IMT 2100 12.2kbps)	+23 dBm +/-1 dB、注: コネクタ化 (クラス 3)	バンド 1 (IMT 2100 12.2kbps)	+23 dBm +/-1 dB、注: コネクタ化 (クラス 3)
バンド 2 (UMTS 1900 12.2 kbps)	+23 dBm +/-1 dB、注: コネクタ化 (クラス 3)	バンド 5 (UMTS 850 12.2 kbps)	+23 dBm +/-1 dB、注: コネクタ化 (クラス 3)
バンド 3 (UMTS 1800 12.2 kbps)	+23 dBm +/-1 dB、注: コネクタ化 (クラス 3)	バンド 6 (UMTS 850 12.2 kbps)	+23 dBm +/-1 dB、注: コネクタ化 (クラス 3)
バンド 4 (UMTS 1700/2100 12.2kbps)	+23 dBm +/-1 dB、注: コネクタ化 (クラス 3)	バンド 8 (UMTS 900 12.2 kbps)	+23 dBm +/-1 dB、注: コネクタ化 (クラス 3)
バンド 5 (UMTS 850 12.2 kbps)	+23 dBm +/-1 dB、注: コネクタ化 (クラス 3)	バンド 9 (UMTS 1700 12.2 kbps)	+23 dBm +/-1 dB、注: コネクタ化 (クラス 3)
バンド 8 (UMTS 900 12.2 kbps)	+23 dBm +/-1 dB、注: コネクタ化 (クラス 3)	バンド 19 (UMTS 850 12.2 kbps)	+23 dBm +/-1 dB、注: コネクタ化 (クラス 3)

タオグラのアンテナゲイン (dB)

仕様	詳細
パーツ No.	TG.30.8113

仕様	詳細
製品名	Apex ヒンジ付き TG.30 超広帯域 4G LTE アンテナ
周波数範囲	698 MHz ~960 MHz、1575.42 MHz、1710 MHz ~2700 MHz (標準 70% + 効率、3 dBi+ ピークゲイン)
その他の機能	ダイポール回転ターミナルアンテナ
	SMA (M) コネクタ付きヒンジ式 90° 終端
	RoHS 準拠

Citrix SD-WAN 400 および 410 Standard Edition アプライアンス

April 15, 2021

Citrix SD-WAN 400 SE と 410 SE は、小規模なブランチオフィスで使用するための 1U アプライアンスです。SD-WAN 410 SE シリーズは、仮想 WAN 機能を備えた次世代の SD-WAN Standard Edition アプライアンスです。

- SD-WAN 400 シリーズ: 小規模のブランチオフィスに適した小型で手頃な価格の 1U アプライアンス。SD-WAN 400 SE シリーズには、2つの高速ブリッジがあり、最大 50 Mbps の WAN 速度をサポートします。
- SD-WAN 410 シリーズ: 小規模ブランチオフィスに適した小型で手頃な価格の 1U アプライアンス。SD-WAN 410 SE シリーズは、最大 150 Mbps の WAN 速度をサポートします。

400-SE プラットフォームはハイパーバイザーベースで、410-SE はベアメタルアプライアンスです。

特定のシリーズでは、すべてのモデルが同じハードウェアを使用し、異なるライセンスオプションを使用して異なる WAN 速度定格を取得できます。たとえば、SD-WAN 410 SE モデル (410-20、410-50、410 ~100、および 410 ~150) は同じハードウェアを使用し、アプライアンスは 20 Mbps、50 Mbps、100 Mbps、または 150 Mbps のアプライアンスのいずれかとしてライセンスを取得できます。

ライセンスされた帯域幅は送信方向にのみ適用されるため、送信方向で 20 Mbps の定格の SD-WAN 410 SE-20 は、16 Mbps/8 Mbps ダウンロード/アップロード帯域幅の仮想パス (固定/ダイナミック) に適しています。

WAN 帯域幅機能の違いに加えて、CPU パワー、インストールされている RAM、およびインストールされているディスク容量が異なるシリーズもあります。

すべてのモデルは、スピードと信頼性を向上させるため、従来のハードドライブの代わりにソリッドステートドライブを使用しています。

SD-WAN 400-SE と 410-SE の Citrix コンプライアンス規制モデルは次のとおりです。

- SD-WAN 400-SE: CB 504-2
- SD-WAN 410-SE: 512-2

詳細については、Citrix 製品プラットフォーム [データシート](#) を参照してください。

Citrix SD-WAN 400 SE

April 15, 2021

SD-WAN 400 SE プラットフォームは、デュアルコアプロセッサと 8 GB のメモリを備えています。このプラットフォームの帯域幅は最大 50 Mbps です。

次の図は、SD-WAN 400 SE アプライアンスのフロントパネルを示しています。

図 1.SD-WAN 400 SE、フロントパネル



- SD-WAN 400 SE アプライアンスの前面パネルには、電源ボタンと 5 つの LED があります。
- 電源ボタンにより、主電源 (電源への電源) のオン/オフが切り替わります。
- リセットボタンは、アプライアンスを再起動します。

LED は、アプライアンスのさまざまな部分に関する重要な情報を提供します。

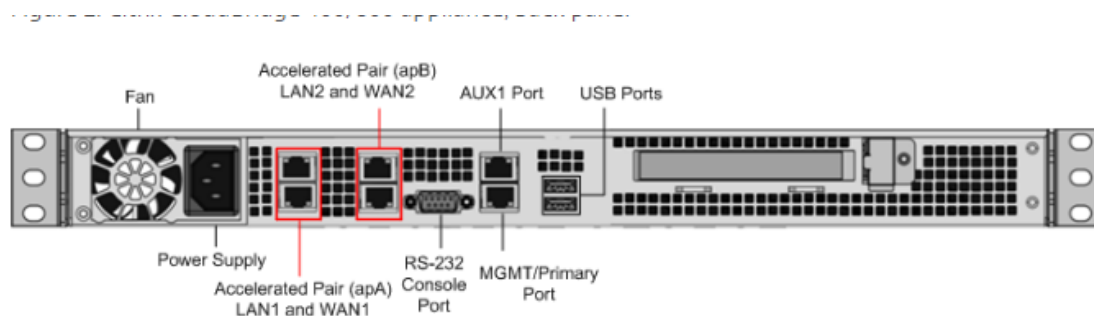
- [Power Fail]: 電源装置に障害が発生したことを示します。
- 情報 LED: 次のことを示します。

ステータス	説明
連続的にオンにして赤い	アプライアンスが過熱しています。
ゆっくり点滅-毎秒 1 点滅	ファンの障害。
高速点滅-毎秒 4 点滅	電源障害。
青に点灯	ローカル UID がアクティブ化されました。この機能を使用して、ラックマウント環境でサーバを特定します。
高速点滅-毎秒 3~4 点滅	リモート UID はオンです。この機能を使用して、リモートロケーションからサーバを識別します。

- NIC1 および NIC2: LAN1 ポートおよび WAN1 ポートでのネットワークアクティビティを示します。
- HDD: ハードディスクドライブのステータスを示します。
- [Power]: 点滅すると、電源装置に電力が供給され、正常に動作していることを示します。

次の図は、SD-WAN 400 SE アプライアンスの背面パネルを示しています。

図 2: SD-WAN 400 SE アプライアンス、背面パネル



SD-WAN 400 SE アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 冷却ファン
- 単一電源、定格 200 ワット、110~240 ボルト
- 加速ブリッジとして機能するイーサネットポート (apA および APB) のアクセラレーションペア。個々のポートの割り当て:LAN1 は Apa.1、WAN1 は Apa.2、LAN2 は APB.1、LAN2 は APB.2 です。
- RS-232 シリアル・コンソール・ポート
- AUX イーサネットポートと 1 つの管理ポート
- 2 つの USB ポート
- ソリッドステートドライブ (SSD) 1 つ
- SD-WAN 400-160GB SSD

Citrix SD-WAN 410 SE

April 15, 2021

SD-WAN 410 SE プラットフォームは、デュアルコアプロセッサと 8 GB のメモリを備えています。このプラットフォームの帯域幅は最大 150Mbps です。

次の図は、SD-WAN 410 SE アプライアンスのフロントパネルを示しています。



電源ボタンにより、主電源 (電源への電源) のオン/オフが切り替わります。スイッチを 2 秒間押しして電源を切ります。

リセットボタンは、アプライアンスを再起動します。

- apA、APB、および APC-LAN および WAN ポートでのネットワークアクティビティを示します。
- バイパスポート: バイパスポートの 3 番目のペアのペアのステータスを示します。
- 電源: 点滅すると、アプライアンスが工場出荷時の状態にリセットされていることを示します。

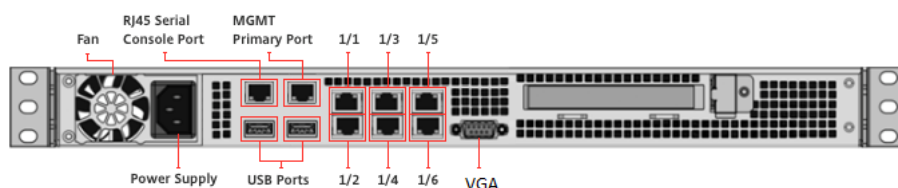
LED は、アプライアンスのさまざまな部分に関する重要な情報を提供します。

- 電源インジケータ: 電源装置に障害が発生したことを示します。
- 情報 LED: 次のことを示します。

ステータス	説明
オレンジ色に連続して点けてる	データポートがバイパスモード (FTW)
連続的にオン、赤。	アプライアンスが過熱しています。(これは、ケーブルの輻輳が原因である可能性があります)。
ゆっくり点滅-毎秒 1 点滅	ファンの障害。
高速点滅-毎秒 4 点滅	電源障害。
青に点灯	ローカル UID がアクティブ化されました。この機能を使用して、ラックマウント環境でサーバを特定します。
高速点滅-毎秒 3~4 点滅	リモート UID はオンです。この機能を使用して、リモートロケーションからサーバを識別します。
緑に点灯	アプライアンスは動作中です。

注

FTW とバイパスという用語は相互交換可能です。バイパスポートは FTW ポートです。



上の図は、SD-WAN 410 SE アプライアンスの背面パネルを示しています。

SD-WAN 410 SE アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 冷却ファン-このプラットフォームは、通常、周囲空気温度で取り付けられたデスクトップブランチでの使用を目的としています。
- 単一電源、定格 200 ワット、110~240 ボルト。電源装置には、電源装置のステータスを示す LED があります ([hardware-common-components-con1.html](#)を参照)。
- 1 つの RJ45 管理ポート。
- RJ45 コンソールポート 1 つ。

- 6X1 GigE Copper (1000BASE-TX)。
- VGA ポート。
- 2 つの USB ポート。

レールの取り付け、ハードウェアのラック取り付け、およびケーブルの接続については、「[ハードウェアのインストール](#)」を参照してください。

アプライアンスの初期設定の実行については、「[初期構成](#)」を参照してください。

SD-WAN 410 のポートラベリング

すべてのデータポートは、オペレーティングシステムによって列挙された順序でラベルが付けられます。ポートは、LAN ポートには奇数のポート番号を使用し、WAN ポートには偶数のポート番号を使用します。1/1 は最初の LAN ポートに、1/2 は最初の WAN ポートに、1/3、2 番目の LAN ポートには 1/3、2 番目の WAN ポートには 1/4、3 番目の LAN ポートには 1/5、3 番目の WAN ポートには 1/6 が使用されます。

ハードウェア仕様の概要

April 15, 2021

次の表は、SD-WAN 400 SE および 410 SE ハードウェアプラットフォームの仕様をまとめたものです。

Citrix SD-WAN 400 および 410 プラットフォーム仕様の概要

ハードウェア仕様

機能 SD-WAN 400 SE SD-WAN 410 SE
--- --- ---
プロセッサ 2 コア 4 コア
ディスク容量の合計 160 GB SSD × 1 64 GB SATADOM
SSD および圧縮履歴 (SSD) の合計数 40GB 60 GB (圧縮履歴 (SSD)-なし)
RAM 8GB 8GB
ネットワーク・インタフェース (Fail-to-Wire、ノンフェイル・トゥ・ワイヤ、管理) バイパス 10/100/1000 と 2 ペア 1000 ベース-TX、N/A、1 x 1000Base-TX
トランシーバのサポート いいえ いいえ。FTW ポートには、トランシーバがあらかじめ取り付けられています。
電源 1 1

物理的寸法

機能	SD-WAN 400 SE	SD-WAN 410 SE
ラックユニット	1U	1RU (1.75 インチ/4.45cm)
システムの深さ	10.5" (26.7 cm)	14" (35 cm)
システム重量	8 ポンド (3.87kg)	8.5 ポンド (3.87kg)
配送の寸法と重量	26 インチ × 6.5 インチ × 18.5 インチ (66.1×16.6×47.0cm)、13.5 ポンド (6.14kg)	26 インチ × 6.5 インチ × 18.5 インチ (66.1×16.6×47.0cm)、13.5 ポンド (6.14kg)

環境と規制

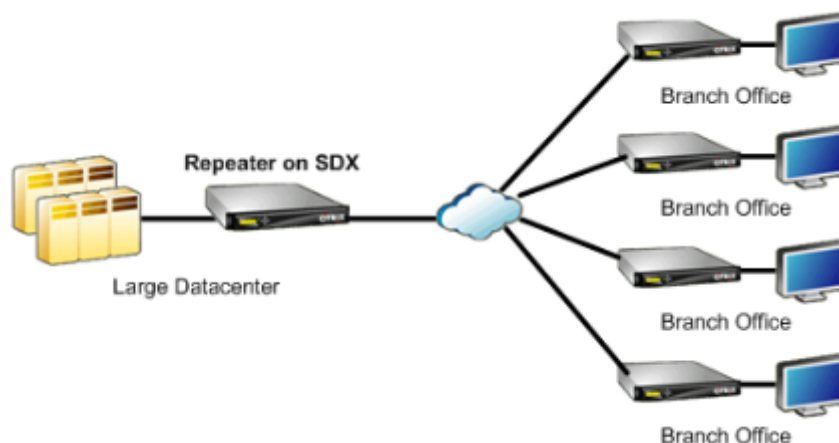
機能	SD-WAN 400 SE	SD-WAN 410 SE
ワット数	200 W	200 W
電圧	100–240 VAC、50–60 Hz	100–240 VAC、50–60 Hz
動作温度	32–104°F (0–40℉)	32–104°F (0–40℉)
動作高度	0–4921 ft (0–1500M)	0–4921 ft (0–1500M)
保管温度	14–140°F (-10–60℉)	14–140°F (-10–60℉)
許容相対湿度	8%–90%	動作時:20% ~80% (結露しないこと)
安全認定	CSA/EN/IEC/UL 60950-1 準拠、UL、または CSA リスト (米国およびカナダ)、CE マーキング (ヨーロッパ)	CSA/EN/IEC/UL 60950-1 準拠、UL、または CSA リスト (米国およびカナダ)、CE マーキング (ヨーロッパ)
電磁界および感受性の認定	FCC (パート 15 クラス A)、CCC、KCC、NOM、CITC、EAC、DOC、CE、VCCI、RCM	FCC (パート 15 クラス A)、CCC、KCC、NOM、CITC、EAC、DOC、CE、VCCI、RCM
環境認証	ROHS、ウィー	RoHS、WEEE、REACH (オプション)

Citrix SD-WAN 4000、4100、および 5100 Standard Edition アプライアンス

April 15, 2021

Citrix SD-WAN スタンダードエディション 4000、4100、5100 アプライアンスは、忙しいデータセンター向けのハ

パフォーマンスアプライアンスです。これらの Platform Edition は、1 Gbps を超える速度の Virtual WAN リンク用に設計されています。特に、多くの支店サイトや地域サイトと通信するビジネスデータセンター向けです。これらのアプライアンスは、ハブアンドスポーク展開のハブで推奨されます。ハブアンドスポークでは、リンク速度または XenApp/XenDesktop ユーザー数が小さいアプライアンスでサポートされるよりも高い場合は、小さいアプライアンスがスポークで使用されます。



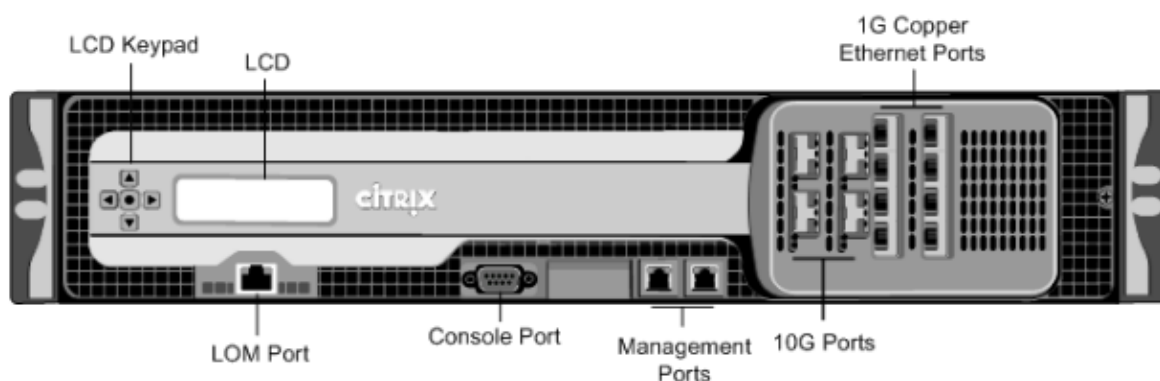
Citrix SD-WAN 4000 SE

April 15, 2021

SD-WAN 4000 は、2U アプライアンスです。各モデルには、合計 12 個の物理コア (ハイパースレッディング付きの 24 コア) と 48 GB (GB) のメモリ用の 6 コアのプロセッサが 2 つ搭載されています。SD-WAN 4000 SE の帯域幅は、それぞれ 300 Mbps、500 Mbps、1 Gbps、および 2 Gbps です。

次の図は、SD-WAN 4000 SE アプライアンスの前面パネルを示しています。

図 1.SD-WAN 4000 SE、フロントパネル



Citrix SD-WAN 4000 SE アプライアンスには、次のポートがあります。

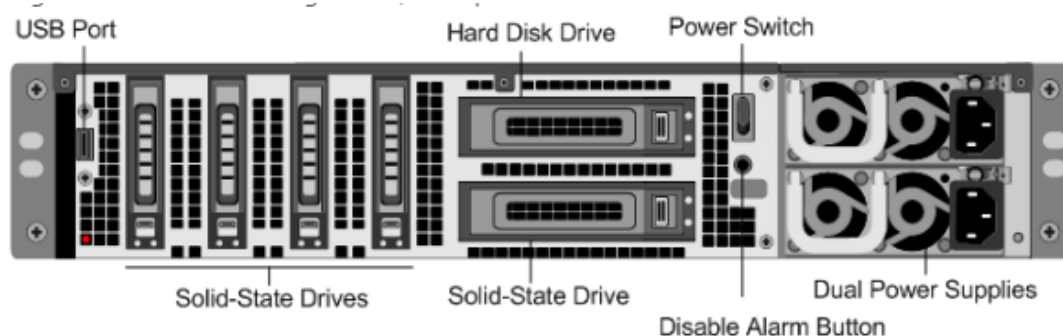
- 10/100Base-T 銅線イーサネットポート (RJ45)。LOM ポートとも呼ばれます。このポートを使用して、アプライアンスのソフトウェアとは無関係にアプライアンスをリモートで監視および管理できます。

メモ: LOM ポートの LED は設計上動作していません。

- RS232 シリアルコンソールポート。
- 2つの 10/100/1000Base-T 銅線イーサネット管理ポート (RJ45)。これらのポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。
- ネットワークポート
 - SD-WAN 4000 SE (FTW カードなし)。8 個の 1G SFP ポートと 4 つの 10G SFP+ ポート。
 - SD-WAN 4000 SE (FTW カード付き)。8 個の 1G 銅線イーサネットポートと 4 つの 10G ポート。

次の図は、SD-WAN 4000 SE アプライアンスの背面パネルを示しています。

図 2: SD-WAN 4000 SE、背面パネル



4000 SE アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 600 GB リムーバブルソリッドステートドライブ ×4 ハードディスクドライブの下にある 256 GB のソリッドステートドライブには、アプライアンスのソフトウェアが格納されます。4000-SE の新しいエディションには、800 GB リムーバブル SSD と 240 GB の SSD があります。
- USB ポート (将来のリリース用に予約)。
- 1 TB リムーバブルハードディスクドライブ。
- 電源スイッチ。電源装置を取り外すかのように、アプライアンスへの電源を切ります。スイッチを 5 秒間押して、電源を切ります。
- アラームボタンを無効にします。アプライアンスを 1 つの電源コンセントだけに接続した場合、または 1 つの電源装置が故障して修理されるまでアプライアンスの動作を続行する場合は、このボタンを押して、電源アラームの鳴りを停止します。
- デュアル電源 (AC または DC)、各定格は 850 ワット、100 ~240 ボルトです。

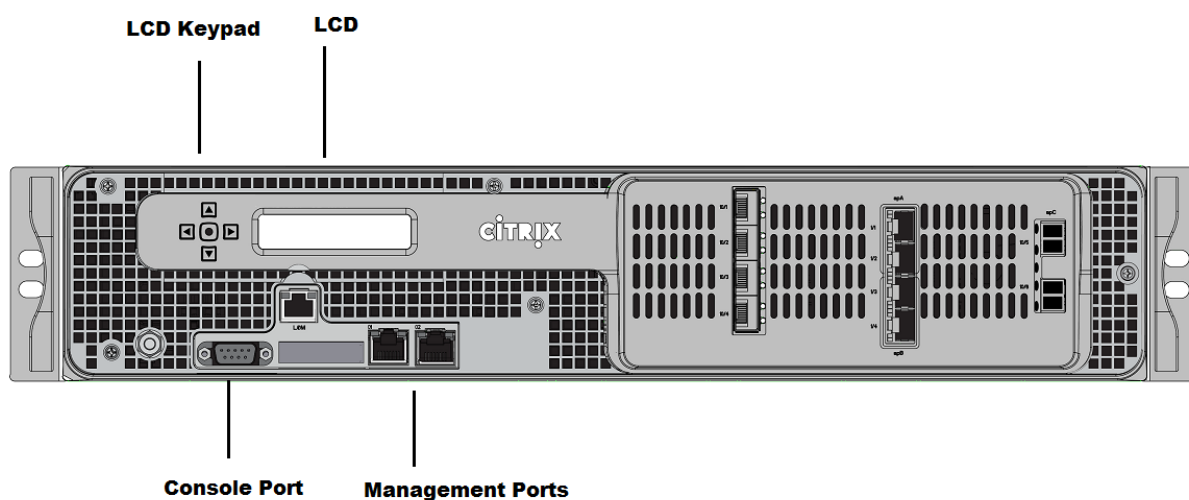
Citrix SD-WAN 4100 SE

April 15, 2021

Citrix SD-WAN 4100 は、2U アプライアンスです。各モデルには 2 つの 6 コアプロセッサが搭載されており、合計 12 個の物理コア (ハイパースレッディング付き 24 コア) と 96 GB (GB) のメモリを搭載しています。SD-WAN 4100 SE の仮想 WAN 帯域幅は 4 Gbps および 6 Gbps です。

次の図は、SD-WAN 4100 SE アプライアンスの前面パネルを示しています。

図 1: SD-WAN 4100 SE、フロントパネル



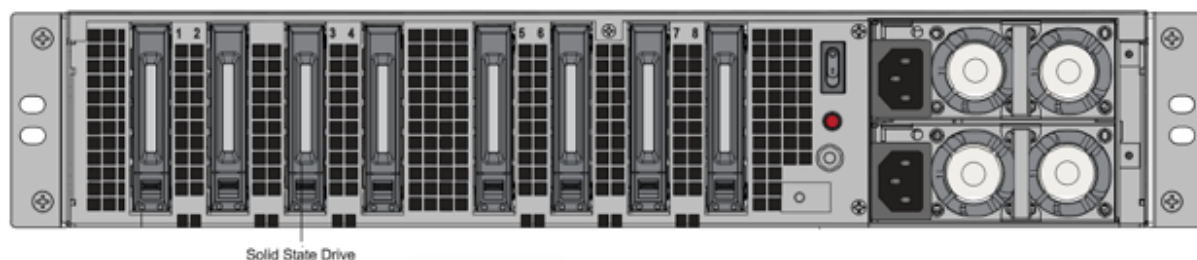
SD-WAN 4100 SE アプライアンスには、次のポートがあります。

- 10/100Base-T 銅線イーサネットポート (RJ45)。LOM ポートとも呼ばれます。このポートを使用して、アプライアンスのソフトウェアとは無関係にアプライアンスをリモートで監視および管理できます。LOM ポートの LED は設計上動作していません。
- RS232 シリアルコンソールポート。
- 2 つの 10/1000Base-T 銅線イーサネット管理ポート (RJ45) これらのポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。
- 2 ポート 10G FTW
- 4 ポート 10G/1G SFP+
- 4 ポート 10/100/1000 FTW RJ 45

次の図は、SD-WAN 4100 SE アプライアンスの背面パネルを示しています。

図 2: SD-WAN 4100 SE、背面パネル

SD-WAN 4100 SE アプライアンスの背面パネルには、次のコンポーネントが表示されます。



- RAID 1 で 1 TB HDD × 2。
- 電源スイッチ。電源装置を取り外す場合と同様に、アプライアンスへの電源を切ります。スイッチを 5 秒間押し、電源を切ります。
- アラームボタンを無効にします。アプライアンスを 1 つの電源コンセントだけに接続した場合、または 1 つの電源装置が故障して修理されるまでアプライアンスの動作を続行する場合は、このボタンを押して、電源アラームの鳴りを停止します。
- デュアル電源 (AC または DC)、それぞれ最大電力は 850 ワット、100~240 ボルトです。

Citrix SD-WAN 5100 SE

April 15, 2021

SD-WAN 5100 SE は、2U アプライアンスです。各モデルには、合計 20 個の物理コア (ハイパースレッディング付き 40 コア) と 128 GB (GB) のメモリ用の 2 つの 10 コアプロセッサが搭載されています。最新のパフォーマンスと帯域幅容量の詳細については、より定期的に更新される最新のデータシートを参照してください。 [citrix.com](https://www.citrix.com); [データシート](#)。

SD-WAN 5100 SE アプライアンスのフロントパネルには、次のポートがあります。

- 10/100Base-T 銅線イーサネットポート (RJ45)。ライトアウト管理 (LOM) ポートとも呼ばれます。このポートを使用して、アプライアンスのソフトウェアとは無関係にアプライアンスをリモートで監視および管理できます。
- RS232 シリアルコンソールポート。
- 2 つの 10/100/1000Base-T 銅線イーサネット管理ポート (RJ45)。これらのポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。
- 8 つの 10G ポート: バイパス付き LC ファイバポート ×4、SFP+ ポート (バイパスなし) ×4。
- 2 つの USB ポート (将来のリリース用に予約)

SD-WAN 5100 SE アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 2 X 1 TB リムーバブルハードディスクドライブ。
- 電源スイッチ。電源装置を取り外すかのように、アプライアンスへの電源を切ります。スイッチを 5 秒間押し、電源を切ります。
- PS アラームボタンを無効にします。このボタンは、アプライアンスに電源装置が 2 つある場合にのみ機能します。このボタンを押して、アプライアンスを 1 つの電源コンセントにのみ差し込んだ場合、または 1 つの電源装置が故障して修理されるまでアプライアンスを操作し続ける場合に、電源アラームが鳴るのをミュートします。
- ホットスワップ対応冗長デュアル電源装置。

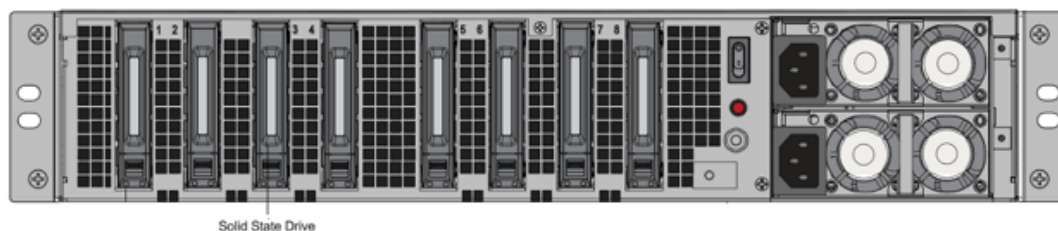


5100 SE アプライアンスを 5100 PE アプライアンスにアップグレードする

ソリッドステートドライブ (SSD) を挿入する

1. 標準エディションアプライアンスに必要な SSD を挿入します。SSD を挿入する方法については、[ソリッドステートドライブ \(フィールド交換可能ユニット\)](#) を参照してください。

a) 5100 SE アプライアンスには、800 GB 以上の SSD が必要です。SSD を 3 番目のベイに挿入します。



2. SD-WAN Web 管理インターフェイスを使用してアプライアンスを再起動します。
3. アプライアンスにインストールされているソフトウェアリリースバージョンが SD-WAN リリースバージョン 10.0 であることを確認します。ここに記載されている手順に従います。[新しいアプライアンスのアップグレード](#)。
4. Premium (Enterprise) Edition プラットフォームライセンスをインストールします。ライセンス情報については、Citrix SD-WAN 製品のダウンロードサイトを参照してください。
5. [シングルステップアップグレード](#)を使用してネットワークをソフトウェアリリースバージョン 10.0 以降にアップグレードします。

注: Citrix SD-WAN 5100-SE はベアメタルプラットフォームです。admin/password を使用してアプライアンスコンソールに直接ログインし、シェルプロンプトにログインできます。

シリアル・コンソールを使用した管理 IP アドレスの構成

1. アプライアンスのシリアルコンソールにアクセスします。
2. **root/nsroot** 認証情報を使用してログインします。
3. **ssh 管理者 @169.254.0.60 -l** 管理コマンドを入力します。
4. パスワード: パスワードを入力します。
5. **management_ip** コマンドを入力します。
6. 設定インターフェイス **192.168.100.1 255.255.255.0 192.168.100.254** コマンドを入力します。

7. 適用コマンドを入力します。

ハードウェア仕様の概要

April 15, 2021

次の表は、Citrix SD-WAN 4000、4100、および 5100 SE ハードウェアプラットフォームの仕様をまとめたものです。

仕様	SD-WAN 4000 SE	SD-WAN 4100 SE	SD-WAN 5100 SE
規制モデル番号	4x10GE SFP+ 8xSFP	2U1P1B	2U1P1D
プロセッサ	6 コア ×2	6 コア ×2	10 コア 2 個
メモリ	96 ギガバイト	96 ギガバイト	128GB
電源装置の数	デュアル電源装置	デュアル電源装置	デュアル電源装置
AC 電源、入力電圧、周波数および電流	交流 100-240V、47-63 ヘルツ	交流 100-240 V、47—63 ヘルツ; 7.0-3.5A	交流 100-240 V、47—63 Hz; 9.0-4.5 A
最大 AC 消費電力	650 W	850 W	850 W
パッケージ重量	69 ポンド	69 ポンド	69 ポンド
配送寸法	高さ 36.5 フィート × 幅 24.5 フィート × 高さ 11 フィート	高さ 36.5 フィート × 幅 24.5 フィート × 高さ 11 フィート	高さ 36.5 フィート × 幅 24.5 フィート × 高さ 11 フィート
システム重量	60 ポンド	60 ポンド	60 ポンド
ラックユニット	2RU	2RU	2RU
ラックオプション-幅	EIA 310-D、IEC 60297、DIN 41494 SC48D ラック幅、マウントブラケット付き	EIA 310-D、IEC 60297、DIN 41494 SC48D ラック幅、マウントブラケット付き	EIA 310-D、IEC 60297、DIN 41494 SC48D ラック幅、マウントブラケット付き
奥行き	28" (72 cm)	28" (72 cm)	28" (72 cm)
動作温度	32—104 F (0—40 C)	32—104 F (0—40 C)	32—104 F (0—40 C)
湿度 (結露しないこと)	20% - 80%	20% - 80%	20% - 80%
安全認定	CSA	CSA	CSA

仕様	SD-WAN 4000 SE	SD-WAN 4100 SE	SD-WAN 5100 SE
EMC と感受性	米国 (FCC)、ヨーロッパ (CE)、日本 (VCCI)、オーストラリア (RCM)、中国 (CCC)、韓国 (KCC)、インド (BIS)、メキシコ (NOM)、サウジアラビア (CITC)、南アフリカ (ICASA)、ロシア (EAC)、台湾 (BSMI)、ブラジル (Anatel)、イスラエル (MoC)	米国 (FCC)、ヨーロッパ (CE)、日本 (VCCI)、オーストラリア (RCM)、中国 (CCC)、韓国 (KCC)、インド (BIS)、メキシコ (NOM)、サウジアラビア (CITC)、南アフリカ (ICASA)、ロシア (EAC)、台湾 (BSMI)、ブラジル (Anatel)、イスラエル (MoC)	米国 (FCC)、ヨーロッパ (CE)、日本 (VCCI)、オーストラリア (RCM)、中国 (CCC)、韓国 (KCC)、インド (BIS)、メキシコ (NOM)、サウジアラビア (CITC)、南アフリカ (ICASA)、ロシア (EAC)、台湾 (BSMI)、ブラジル (Anatel)、イスラエル (MoC)
環境コンプライアンス	ROHS, WEEE	ROHS, WEEE	ROHS, WEEE

Citrix SD-WAN 1000、2000、および 2100 の Standard Edition アプライアンス

April 15, 2021

SD-WAN スタンダードエディション 1000、2000、および 2100 アプライアンスは、SD-WAN アプライアンスの仮想インスタンスを組み合わせています。



SD-WAN Standard Edition 1000、2000、および 2100 アプライアンスは、複数の仮想マシンをサポートする Citrix ブランチアーキテクチャに基づいています。すべてのブランチアプライアンスには、SD-WAN Standard Edition インスタンスと管理サービスインスタンスが含まれます。

SD-WAN インスタンスは通常、インラインモードで使用され、SD-WAN インスタンスは WAN ルータと LAN 間で割り付けられます。SD-WAN インスタンスは、仮想インラインモードでデプロイすることもできます。

アプライアンスには 2 つのモードがあります。2 ポートモードと 4 ポートモード。ポート 1/3 と 1/4 の使用方法を決定します。

Citrix SD-WAN 1000 SE

April 15, 2021

プラットフォームを搭載した SD-WAN 1000-SE は、クアドコアプロセッサと 32 GB のメモリを備えています。このプラットフォームの帯域幅は最大 100 Mbps です。

次の図は、SD-WAN 1000-SE アプライアンスのフロントパネルを示しています。

図 1: Citrix SD-WAN 1000-SE フロントパネル



SD-WAN 1000-SE アプライアンスの前面パネルには、電源ボタンと 5 つの LED があります。電源ボタンは、アプライアンスのオン/オフを切り替えるために使用します。リセットボタンは、アプライアンスを再起動します。

LED は、アプライアンスのさまざまな部分に関連する重要な情報を提供します。

- [Power Fail]: 電源装置に障害が発生したことを示します。
- 情報 LED: 次のことを示します。

ステータス	説明
連続的にオンとレッド	アプライアンスが過熱しています。(これは、ケーブルの輻輳が原因である可能性があります)。
赤で点滅 (1Hz)	ファンの障害。ファンが動作しないかどうかを確認します。
赤で点滅 (0.25Hz)	電源障害、動作していない電源装置を確認します。
青に点灯	ローカル UID がアクティブ化されました。この機能を使用して、ラックマウント環境でサーバを特定します。
青で点滅 (300 m/s)	リモート UID はオンです。この機能を使用して、リモートロケーションからサーバを識別します。

- NIC1 および NIC2: LAN1 ポートおよび WAN1 ポートでのネットワークアクティビティを示します。
- HDD — ハードディスクドライブのステータスを示します。
- [Power]: 電源装置に電力が供給され、正常に動作していることを示します。

次の図は、SD-WAN 1000-SE アプライアンスの背面パネルを示しています。

図 2: Citrix SD-WAN 1000-SE アプライアンス、背面パネル



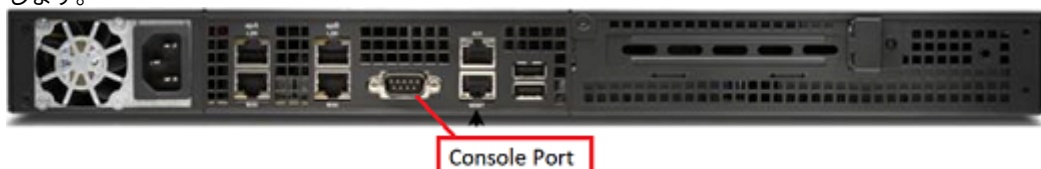
SD-WAN 1000-SE アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 冷却ファン。
- 単一電源、定格 200 ワット、110～240 ボルト。
- イーサネットポートのアクセラレーションペア (apA および APB)
- RS-232 シリアルコンソールポート。
- AUX イーサネットポートと 1 つの管理ポート。
- 2 つの USB ポート。

正常なシャットダウン後にアプライアンスを電源投入する

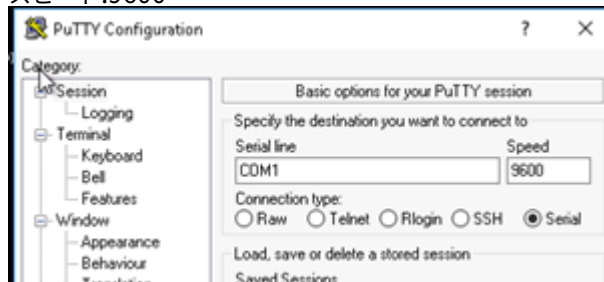
正常なシャットダウン後にアプライアンスを電源投入するには:

1. シリアル・コンソール・ケーブルを、アプライアンスの背面と管理用ラップトップのシリアル・ポートに接続します。

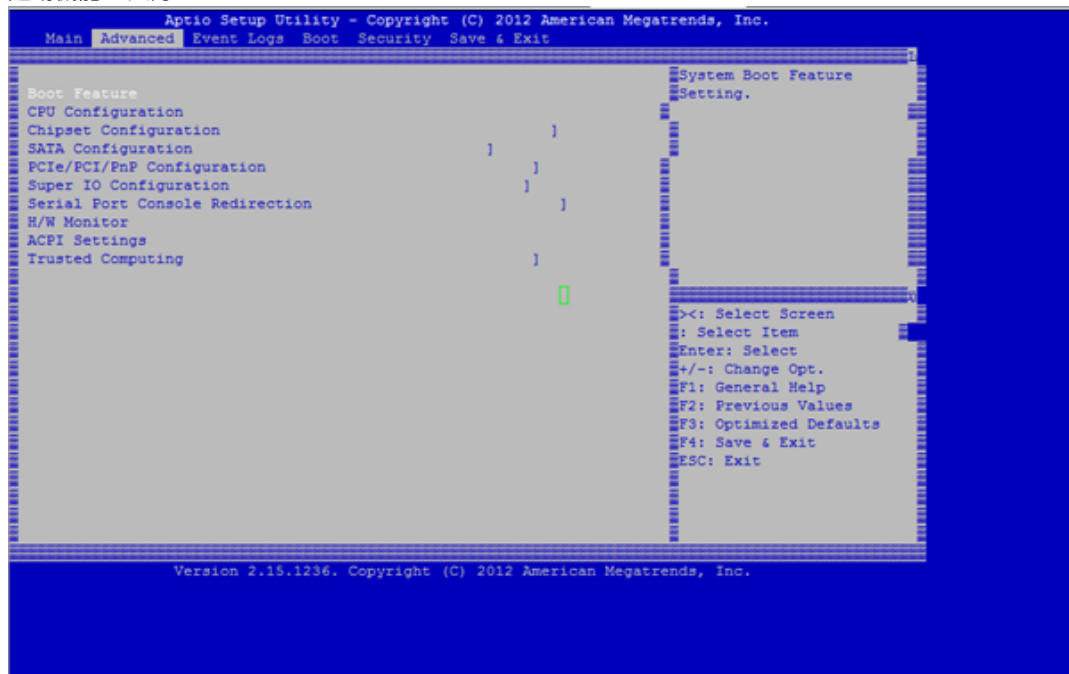


2. 管理ラップトップで、次の構成設定を使用してパテセッションを再起動します。
 - シリアル回線:COM1

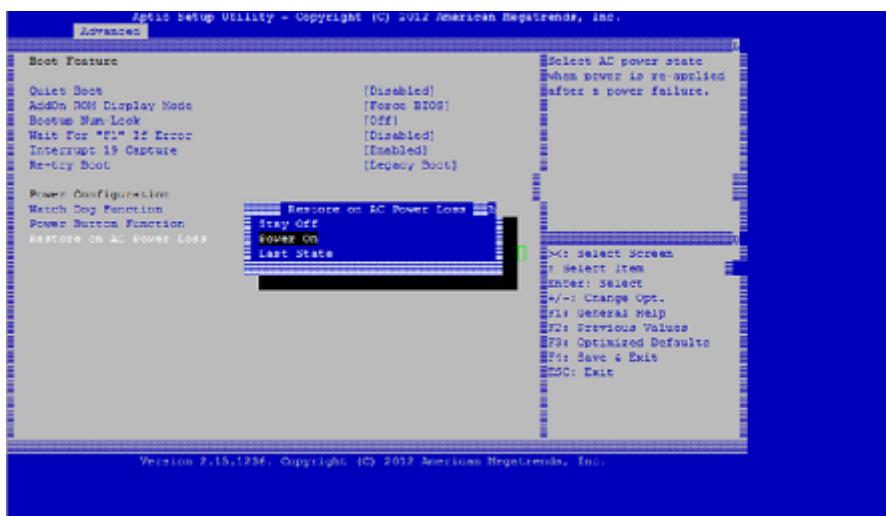
- スピード:9600



3. アプライアンスの電源を入れ、起動中に Putty セッションで次のキーを押して BIOS 設定画面に入ります。キー押し: **DEL**
4. BIOS で、
 - a) [詳細] タブ > [選択]
 - b) 起動機能 > 入力



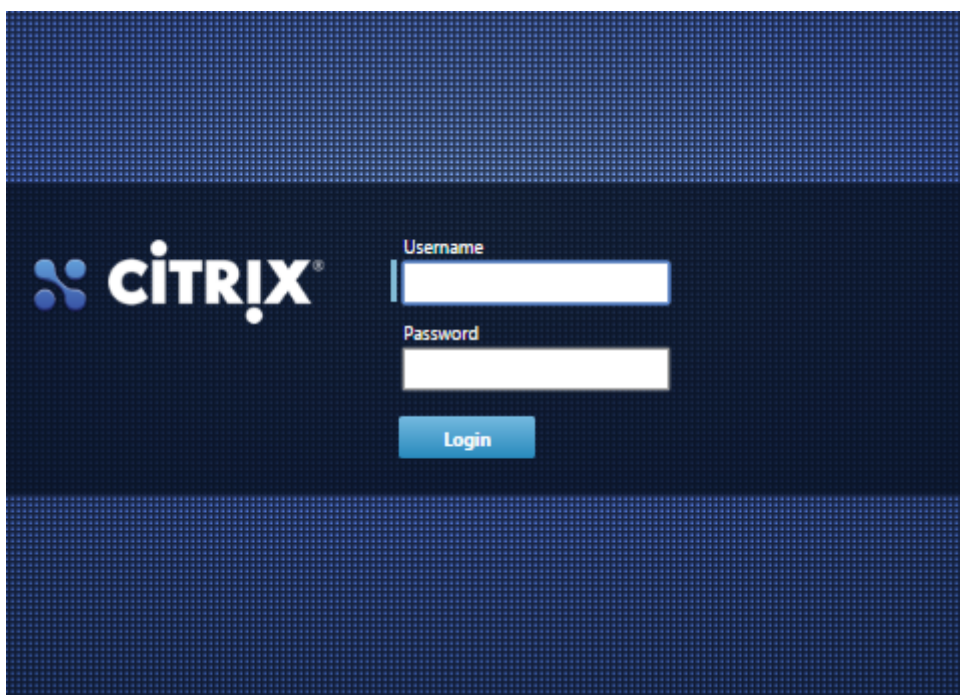
5. [起動機能] 画面で、[AC 電源切断時の復元] パラメータの値を [前回の状態] > [電源オン] から変更します。



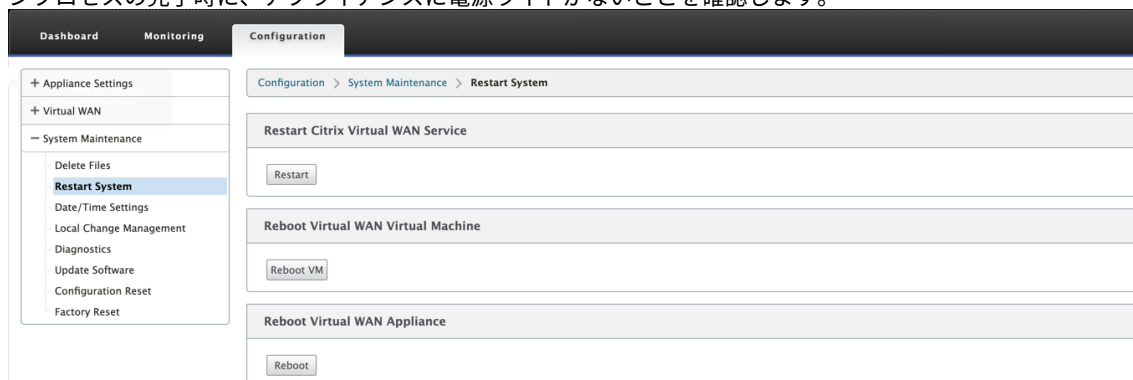
6. [保存して終了] に移動します。
 - a) [**** 変更を保存してリセット ****] を選択します。
 - b) [はい]
- [システムの再起動を許可する] を選択します。これには約 5 分かかります。



7. アプライアンスの電源がオンになったら、アプライアンス管理インスタンス (SVM) にログインします。アプライアンスのデフォルトの IP アドレスは: 192.168.100.1、ユーザー名は「管理者/パスワード」です。



8. SD-WAN アプライアンスの GUI で、[構成] > [システムメンテナンス] > [** システムの再起動 **] に移動し、[再起動] をクリックします。アプライアンスが完全にシャットダウンできるようにします。シャットダウンプロセスの完了時に、アプライアンスに電源ライトがないことを確認します。



9. アプライアンスの電源をオンにして、BIOS 構成の変更が正常に適用されたことを確認します。これは、APC インテリジェント・PDU Web 管理コンソールを使用するか、シャットダウンした SD-WAN アプライアンスから電源ケーブルを物理的に引き出し、10 秒間待ってから再び差し込むことで実行できます。アプライアンスの電源は、すべてのシャットダウンシナリオから自動的に起動します。

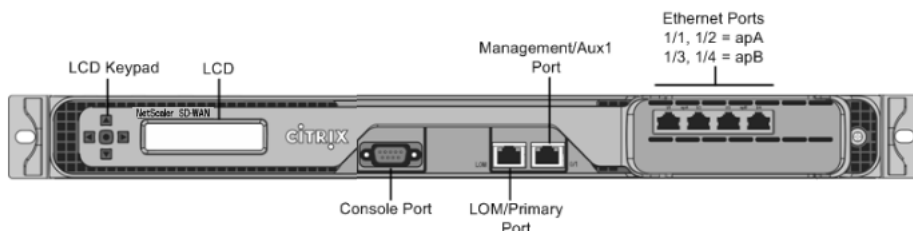
Citrix SD-WAN 2000 SE

April 15, 2021

Citrix SD-WAN 2000-SE プラットフォームは、1 つのクアドコアプロセッサと 24 ギガバイト (GB) のメモリを搭載した 1U アプライアンスです。

次の図は、SD-WAN 2000-SE アプライアンスのフロントパネルを示しています。

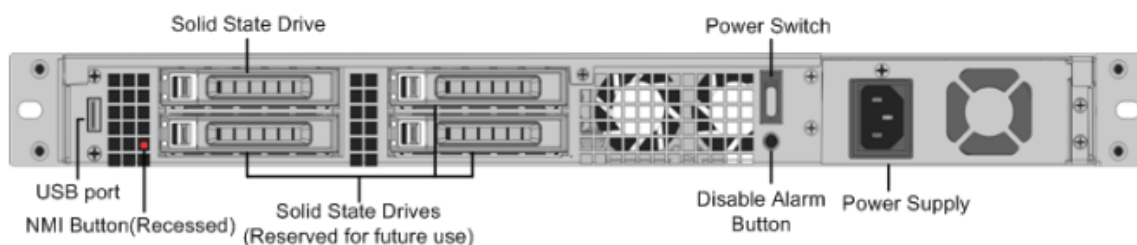
図 1: Citrix SD-WAN 2000-SE アプライアンス、フロントパネル



SD-WAN 2000-SE アプライアンスには、次のポートがあります。

- RS232 シリアルコンソールポート。
- ライトアウト管理 (LOM) ポートと呼ばれる銅線イーサネット (RJ45) ポート。このポートを使用して、アプライアンスのソフトウェアとは無関係にアプライアンスをリモートで監視および管理できます。
- 銅線イーサネット (RJ45) 管理ポート。番号が 0/1 で、PRI (プライマリ) という名前が付いています。管理ポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。このポートは、仮想 WAN の初期プロビジョニングに使用できます。LOM ポートは、管理ポートとしても動作します。
- 4 つの 10/100/1000Base-T 銅線イーサネットポート。左から右に 1/1、1/2、1/3、および 1/4 の番号が付けられます。4 つのポートは 2 つの加速ペアを形成し、加速ブリッジとして機能します。ポート 1/1 および 1/2 はアクセラレーションペア A (apA)、1/3 および 1/4 はアクセラレーションペア B (apB) です。

図 2: Citrix SD-WAN 2000-SE アプライアンス、背面パネル



SD-WAN 2000-SE アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 600 GB リムーバブルソリッドステートドライブ。アプライアンスのソフトウェアとユーザーデータを格納し、1 TB のハードディスクドライブを格納します。
- 電源スイッチ。スイッチを 5 秒間押して、電源を切ります。
- USB ポート (将来のリリース用に予約)。
- 非マスク割り込み (NMI) ボタン。テクニカルサポートの要求に応じてコアダンプを生成するために使用する。この赤いボタンを押すには、ペン、鉛筆、またはその他の尖ったオブジェクトを使用する必要があります。このボタンは、意図しない起動を防ぐためにくぼんだ状態になっています。
- 単一電源、定格 300 ワット、100-240 ボルト。

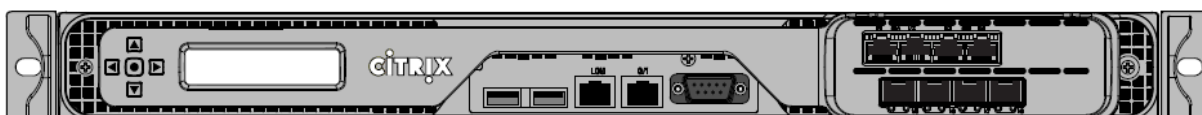
Citrix SD-WAN 2100 SE

April 15, 2021

Citrix SD-WAN 2100-SE プラットフォームは、8 コアプロセッサと 32 GB (GB) のメモリを搭載した 1U アプライアンスです。

次の図は、SD-WAN 2100-SE アプライアンスの前面パネルを示しています。

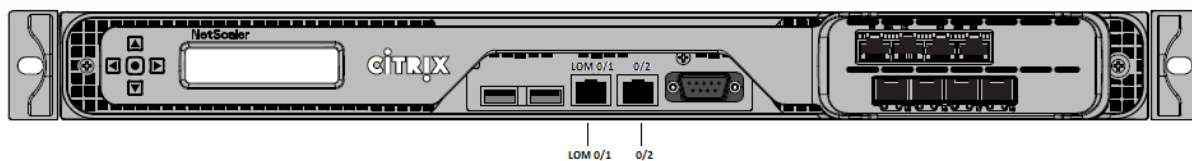
図 1: Citrix SD-WAN 2100-SE アプライアンス、フロントパネル



SD-WAN 2100-SE アプライアンスには、次のポートがあります。

- RS232 シリアルコンソールポート。
- 10/100/1000 Base-T 銅線イーサネット管理ポート (RJ45) は LOM というライトアウト管理 (LOM) ポートと呼ばれ、管理ポートは 0/1 とラベル付けされています。これらのポートを使用して、アプライアンスのソフトウェアとは無関係にアプライアンスをリモートで監視および管理できます。
- USB ポート。
- 1000 ベース TX 銅線イーサネットポート 4 個。
- 4 つの 1GE SFP ポート。

ポート・ラベル-古い 2100-SE フロント・ベゼル	説明
LOM	管理ポートが点灯します
0/1	管理ポート



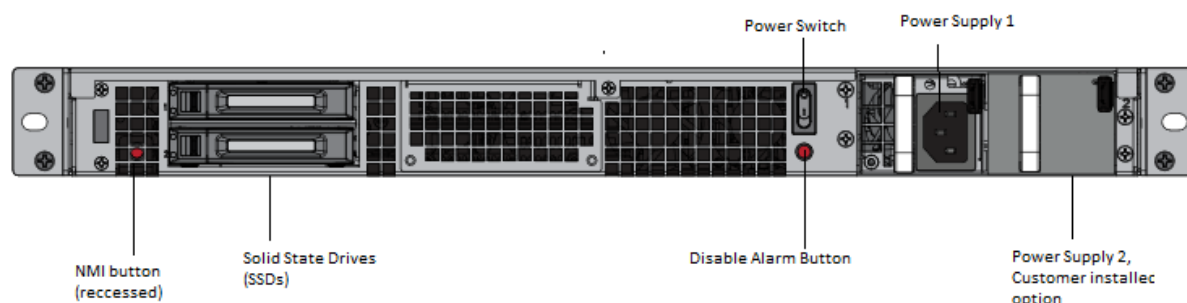
ポート・ラベル-新しい 2100-SE フロント・ベゼル	説明
LOM 0/1	管理用ポートと管理ポートが点灯します
0/2	将来使用するために予約されている管理ポート (Management)

- ライトアウト管理 (LOM) ポートと呼ばれる銅線イーサネット (RJ45) ポート。ライトアウト管理 (0/1) とラベ

ル付けされています。このポートを使用して、アプライアンスのソフトウェアとは無関係にアプライアンスをリモートで監視および管理できます。

- 0/2 というラベルが付いた銅線イーサネット (RJ45) 管理ポート。この管理ポートは、システム管理機能には使用できません。このポートは、将来の使用のために予約されています。

図 2: Citrix SD-WAN 2100-SE アプライアンス、背面パネル



SD-WAN 2100-SE アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 240 GB リムーバブルソリッドステートドライブ、ブランクスロット 1
- 電源スイッチ。アプライアンスへの電源をオンまたはオフに切り替えます。スイッチを 5 秒間押し、電源を切ります。
- 非マスク割り込み (NMI) ボタン。テクニカルサポートの要求に応じてコアダンプを生成するために使用する。ペン、鉛筆、またはその他の尖った物を使用して、意図しない起動を防ぐために必要な赤いボタンを押します。
- 単一電源、定格 450 ワット、100~240 ボルト。

2100 SE アプライアンスを 2100 PE アプライアンスに変換する

重要

PE 機能を使用するには、2100 アプライアンスで SD-WAN リリース 9.3 以降のソフトウェアバージョンが必要です。SD-WAN リリース 9.3 以降のソフトウェアリリースバージョンは 2100 PE をサポートします。

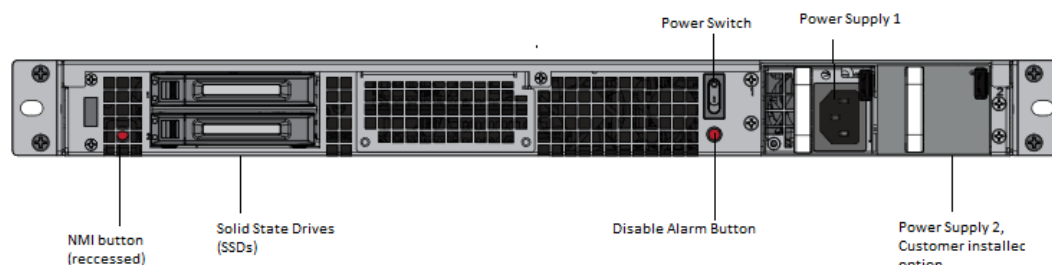
- 2100 SE は SSD (240 GB) とブランクキャリアが 1 つだけ出荷されます。
- PE アプライアンスにアップグレードする場合は、キットを注文できます。キットには、追加の SSD (480 GB) と PE 用の適切なライセンスが含まれています。
- キットを受け取ったら、新しい 480 GB ドライブを空のスロットに取り付けます (元の SSD はそのままにします)。SD-WAN リリース 10.0 にアップグレードし、新しい PE ライセンスを適用します。

注

[USB イメージ再作成ユーティリティ](#)を使用して、2100 SE アプライアンスを 2100 PE アプライアンスに変換することもできます。

ソリッドステートドライブ (SSD) を挿入する

1. 標準エディションアプライアンスに必要な SSD を挿入します。SSD を挿入する方法については、[ソリッドステートドライブ \(フィールド交換可能ユニット\)](#) を参照してください。
 - a) 2100 SE アプライアンスには 480 GB 以上の SSD が必要です。



2. SD-WAN Web 管理インターフェイスを使用してアプライアンスを再起動します。
3. アプライアンスにインストールされているソフトウェアリリースバージョンが SD-WAN リリースバージョン 10.0 であることを確認します。ここに記載されている手順に従います。[新しいアプライアンスのアップグレード](#)。
4. エンタープライズエディションプラットフォームライセンスをインストールします。ライセンス情報については、Citrix SD-WAN 製品のダウンロードを参照してください。
5. [シングルステップアップグレード](#)を使用してネットワークをソフトウェアリリースバージョン 10.0 以降にアップグレードします。

シリアル・コンソールを使用した管理 IP アドレスの構成

1. アプライアンスのシリアルコンソールにアクセスします。
2. **root/nsroot** 認証情報を使用してログインします。
3. **ssh 管理者 @169.254.0.60 -l 管理者** コマンドを入力します。
4. パスワード: パスワードを入力します。
5. **management_ip** コマンドを入力します。
6. 設定インターフェイス **192.168.100.1 255.255.255.0 192.168.100.254** コマンドを入力します。
7. 適用コマンドを入力します。

ハードウェア仕様の概要

April 15, 2021

次の表は、SD-WAN 1000-SE、2000-SE、および 2100-SE ハードウェアプラットフォームの仕様をまとめたものです。

仕様	SD-WAN 1000-SE	SD-WAN 2000-SE	SD-WAN 2100-SE
帯域幅	最大 100Mbps まで	300Mbps まで	最大 2 Gbps
セッション合計、最大仮想パス (静的/ダイナミック)	10,000	20,000	256/32
プロセッサ	4 コア	4 コア	8 コア 2.1 GHz
合計ディスク容量	1X480 GB SSD	1X800GB SSD	1X240GB SSD
RAM	16GB	24 ギガバイト	32GB
ネットワークインタフェース	バイパス 10/100/1000 と 2 ペア、管理ポートおよび AUX ポート用の 2 GigE ポート	バイパス 10/100/1000 と 2 ペア	1G のバイパス付き 2 ペア、1GE SFP×4、管理ポートおよび AUX ポート用の GigE ポート×2
電源装置	1	1	モジュール×1、オプションの FRU
ラックユニット	1U	1U	1U
システム幅	19 インチ (482.6 mm) ラック用の EIA 310-D	19 インチラック用の EIA 310-D	19 インチラック用の EIA 310-D
システムの深さ	10" (25.4 cm)	23.5" (60 cm)	24" (61 cm)
システム重量	8.5 ポンド (3.9 kg)	32 ポンド (14.5kg)	32 ポンド (14.5kg)
配送の寸法と重量	長さ 26 インチ x 幅 18.5 インチ x 高さ 6.5 インチ、14.5 ポンド。	長さ 32×幅 23.5×高さ 7.5 インチ、39 ポンド。	長さ 33 インチ x 幅 24 インチ x 高さ 8 インチ、40 ポンド。
電圧	100/240 VAC、50–60 Hz	100/240 VAC、50–60 Hz	100/240 VAC、50–60 Hz
消費電力 (最大)	200 W	300 W	450 W
動作温度 (摂氏)	10–35	0–40	0–40
非動作時温度 (摂氏)	-40~+70	-40~+70	-10C~+60C
許容相対湿度	8% ~90% 結露しないこと	5% ~95% 結露しないこと	20% ~80% 結露しないこと
安全認定	CSA/EN/IEC/UL 60950-1 準拠、UL、または CSA リスト (米国およびカナダ)、CE マーキング (ヨーロッパ)	CSA/EN/IEC/UL 60950-1 準拠、UL、または CSA リスト (米国およびカナダ)、CE マーキング (ヨーロッパ)	CSA/EN/IEC/UL 60950-1 準拠、UL、または CSA リスト (米国およびカナダ)、CE マーキング (ヨーロッパ)

仕様	SD-WAN 1000-SE	SD-WAN 2000-SE	SD-WAN 2100-SE
電磁界および感受性の認定	FCC クラス A、EN 55022 クラス A、EN 61000-3-2/-3-3、CISPR 22 クラス A	FCC (Part 15 Class A)、CE、C-Tick、VCCI-A、CCC、KCC、NOM、SASO、SABS、PCT	FCC (パート 15 クラス A)、CCC、KCC、NOM、CITC、EAC、DOC、CE、VCCI、RCM
環境認証	ROHS、ウィー	ROHS、ウィー	ROHS、ウィー

6100 スタンダードエディションおよびプレミアムエディションアプライアンス

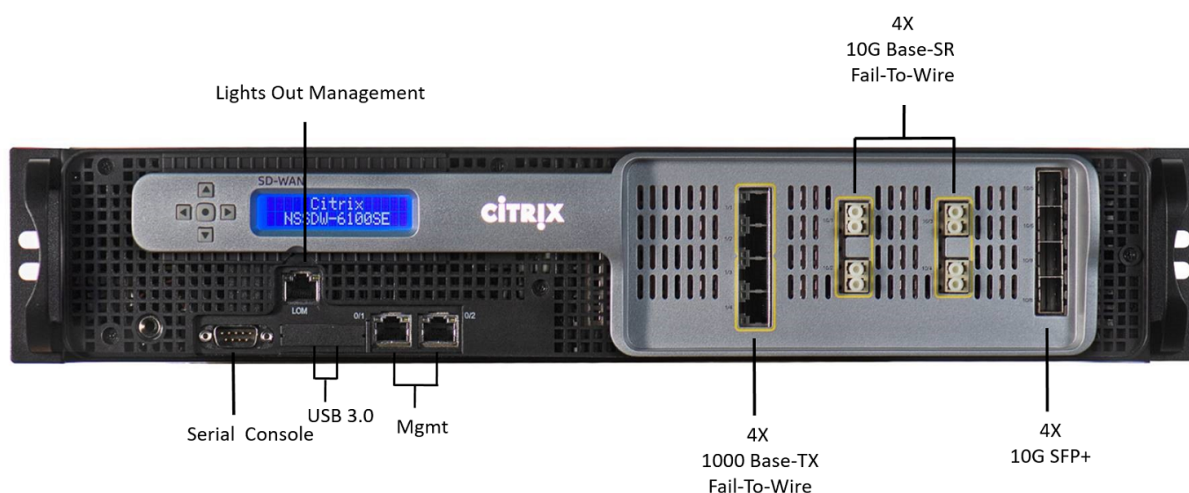
April 15, 2021

Citrix SD-WAN 6100 スタンダードエディション (SE) /プレミアムエディション (PE) は、2U アプライアンスです。各モデルには、合計 28 個の物理コア (ハイパースレッディングが有効になっている) と 256 GB のメモリが搭載されています。最新のパフォーマンスおよび帯域幅容量の詳細については、[Citrix SD-WAN のデータシート](#)を参照してください。

6100 アプライアンスエディションでは、次の Citrix SD-WAN ソフトウェアバージョンがサポートされています。

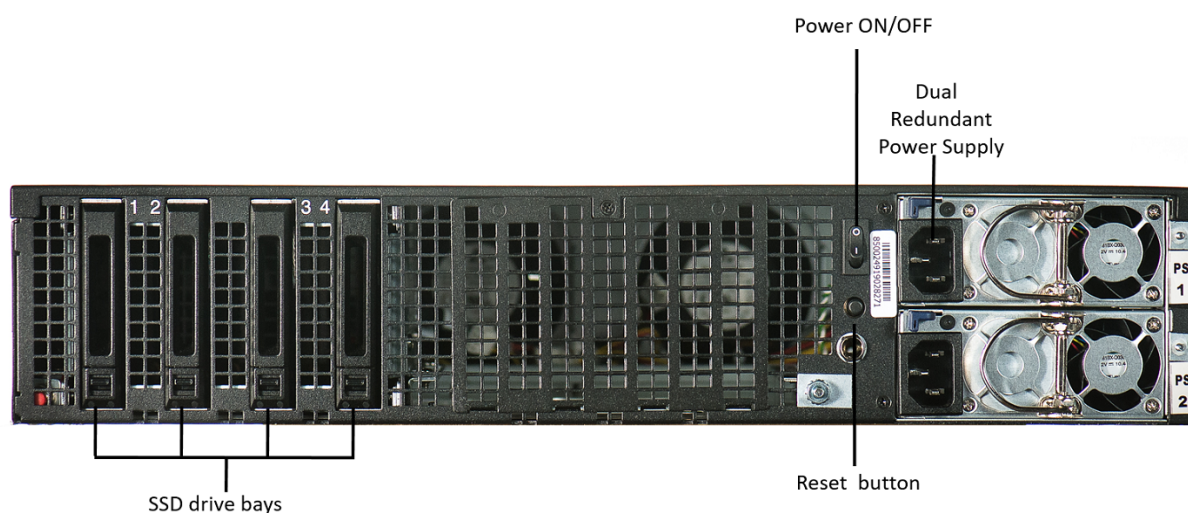
- Citrix SD-WAN 6100 SE — Citrix SD-WAN 10.2.3 以上。
- Citrix SD-WAN 6100 PE-Citrix SD-WAN 10.2.7 イメージとともに出荷され、ソフトウェアを Citrix SD-WAN 11.2.1 以上にアップグレードして、PE 機能を有効にします。

Citrix SD-WAN 6100 SE/PE アプライアンスのフロントパネルには、次のポートがあります。



ポート	説明
0/1, 0/2	10/100/1000 ベース-T 銅線イーサネット管理ポート (RJ45)
1/1, 1/2, 1/3, 1/4	1000 ベース TX フェイル・トゥ・ワイヤ
10/1, 10/2, 10/3, 10/4	10G ベース SR フェイル・トゥ・ワイヤ
10/5, 10/6, 10/7, 10/8	10G SFP+

Citrix SD-WAN 6100 SE/PE アプライアンスの背面パネルには、次のコンポーネントが表示されます。



Citrix SD-WAN 6100 SE の場合 [SSD コンフィギュレーション]

- ドライブベイ 3- 2.5 インチブートドライブ SSD、容量 480 GB
- ドライブベイ 1、2、4-2.5 インチ SSD プラスチックドライブトレイ「フィラー-ダミー」

Citrix SD-WAN 6100 PE の場合 [SSD コンフィギュレーション]

- ドライブベイ 3-2.5 インチブートドライブ SSD、容量 480 GB
- ドライブベイ 1、2、4-2.5」960 GB SSD。

電源スイッチとバックエンドボタンの機能:

- 電源スイッチ。電源装置を取り外すかのように、アプライアンスへの電源を切ります。スイッチを 5 秒間押し、電源を切ります。
- PS アラームを無効にするボタンは、アプライアンスに 2 つの電源装置がある場合にのみ機能します。
電源アラームをミュートするには、このボタンを押します。
 - アプライアンスを 1 つの電源コンセントにのみ接続した場合。
 - 1 つの電源装置が故障していて、修理されるまでアプライアンスの動作を続行する場合。
- ホットスワップ対応デュアル冗長電源 (100 ~240 VAC 標準 1,000 W、48 V DC オプション)

Citrix SD-WAN 6100 SE アプライアンスを **Citrix SD-WAN 6100 PE** アプライアンスに変換します

- Citrix SD-WAN SE アプライアンスに必要な SSD を挿入します。
 - ドライブベイ 3 2.5 インチブートドライブ SSD を 480 GB の容量で挿入します。
 - ドライブベイ 1、2、4-2.5 インチ 960 GB SSD を挿入します。
SSD を挿入する方法については、「」を参照してください [ソリッドステートドライブ](#)。
- SD-WAN Web 管理インターフェイスを使用してアプライアンスを再起動します。
- アプライアンスにインストールされているソフトウェアリリースバージョンが Citrix SD-WAN 11.2.1 以上であることを確認します。アプライアンスで 11.2.1 より前のバージョンが実行されている場合は、ソフトウェアを 11.2.1 にアップグレードし、ローカルの変更管理を実行します。アップグレード手順については、を参照してください [アップグレードパス](#)。
- プレミアムエディションプラットフォームライセンスをインストールします。ライセンス情報については、を参照してください [Citrix SD-WAN 製品のダウンロード](#)。

ハードウェア仕様の概要

次の表は、Citrix SD-WAN 6100 SE ハードウェアプラットフォームの仕様をまとめたものです。

仕様	Citrix SD-WAN 6100 SE/PE
コンプライアンス規制モデル番号	2U1P1A
プロセッサ	2 x 14 コア・プロセッサ (インテル E5-2680 v4 14 コア、2.4 GHz)
メモリ	256 GB 2,400 MHz、8 x 32 GB RDIMM
電源装置の数	2 (1,000 W、デュアル冗長ホットスワップ可能)
AC 電源、入力電圧、周波数、電流	100~240 V AC、50~60 Hz、5.5-2.8A
DC 入力電圧および電流	-36V 直流から-72V 直流、15.4-7.7A
典型的な AC 消費電力	357 W
最大 AC 消費電力	480 W
典型的な放熱	1251 BTU/時間
最大熱放散	1218 BTU/時間
典型的な風量 (前面から背面)	65 CFM
最大風量 (前面から背面)	125CFM
高度範囲	最大 5,000 m (最大 16,000 フィート)
ソリッドステートドライブ (SSD)	1x480GB および 3x960GB SSD (1.2GB DBC、PE にも適用)

仕様	Citrix SD-WAN 6100 SE/PE
パッケージ重量	69 (ポンド) (31.3 Kg)
配送寸法	長さ 36.5 フィート×幅 24.5 フィート×高さ 11 フィート (94×63×28cm)
システム重量 (ポンド)	60 (ポンド) (27.2 Kg)
ラック高さ	2U
ラック幅	19 (インチ) ラック用 EIA 310-D
ラックの奥行き	28 インチ (71.1cm)
動作温度	0–45°C (32–113°F)
湿度 (結露しないこと)	5% - 95%
安全認定	IEC 60950-1、第 2 版 CSA 60950-1、第 2 版 UL 60950-1、第 2 版 S/NZS 60950-1
EMC と感受性	米国 (FCC (第 15 クラス A))、ヨーロッパ (CE (EN55032/55024))、オーストラリア (RCM)、日本 (VCCI)、韓国 (KCC)、台湾 (BSMI)、中国 (CCC)、インド (BIS)、ロシア (CUTR)、ロシア (EAC)、サウジアラビア (CITC)、ブラジル (アナテル)、南アフリカ (ICASA)、メキシコ (NOM)、エジプト (NTRA)、イスラエル (MoC)
環境コンプライアンス	ローズ、ウィー、リーチ

Citrix SD-WAN 1100 Standard Edition および Premium Edition

April 15, 2021

Citrix SD-WAN 1100 の標準エディションおよびプレミアムエディションアプライアンスは、デスクトップフォームファクタアプライアンスです。各モデルは、24 GB のメモリと 480 GB のストレージ (SSD ドライブ) を備えた 8 コアプロセッサを備えています。

次の図は、1100 SE および PE アプライアンスの前面パネルを示しています。

図 1: Citrix SD-WAN 1100 SE および PE、フロントパネル

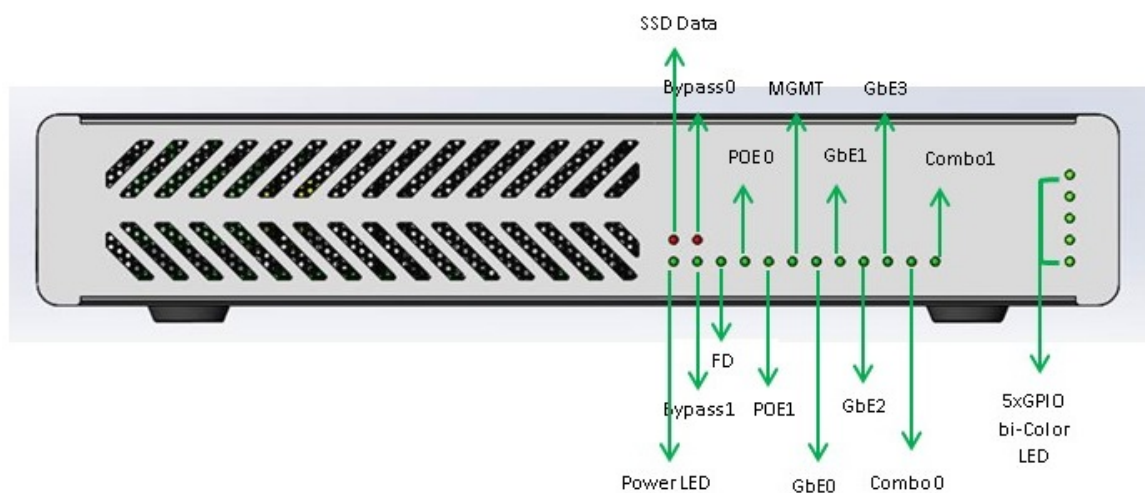


表 1. LED 電源インジケータ

LED カラー	LED が示す状態
イーサネットポート	アクティブ/リンク: 緑、速度-1000 オレンジ、速度-100: 緑、速度-10: オフ
LED をバイパスする	通常モード: 緑、バイパスモード: オレンジ。
SFP ポート LED	アクティブ/リンク: グリーン, スピード-1000: オレンジ
電源 LED	電源オン: 緑、電源オフ: オフ

アプライアンスには次のポートがあります。

- シリアルコンソールポート。
- 10/100/1000 ベース-T 銅線イーサネット管理ポート (RJ45) 1 個。管理ポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。
- 2つのCOMポート (1/5 と 1/6)。一度に RJ45 または SFP ポートを使用できます。
- 480 GB のソリッドステートドライブ。Citrix SD-WAN ソフトウェアとユーザーデータを格納するために使用されます。
- 電源スイッチ。電源装置を取り外すかのように、アプライアンスへの電源を切ります。スイッチを 5 秒間押し、電源を切ります。
- 2つのパワーオーバーイーサネット (POE) ポート (1/7 および 1/8)。
- FTW ポートの 2 セット、(1/1、1/2)、および (1/3、1/4)。
- USB ポート。
- 単一電源装置。冗長性のための 2 番目の電源 (オプション)、それぞれ定格 150 W

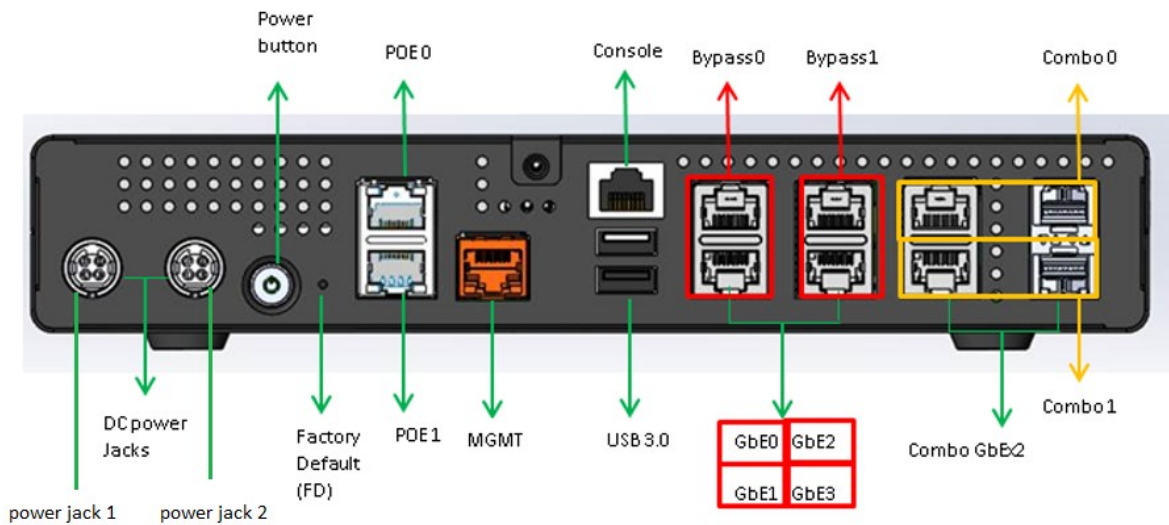
アクセサリ FRU:

- ラックマウントキット
- 追加の電源アダプタと電源コード — DC ジャック 2 に接続
- SFP トランシーバおよびケーブル

Citrix SD-WAN 1100 SE および PE 背面パネル:



Citrix SD-WAN 1100 SE および PE の背面パネルには、次のラベルが付いています。



レールの取り付け、ハードウェアのラック取り付け、およびケーブルの接続については、[ハードウェアのインストール](#)を参照してください。

ポート	対応スピード
1/1-1/4	100/1000
1/5-1/6	RJ45:1000のみ、SFP: 100 (特定の SFP) /1000
1/7-1/8	100/1000

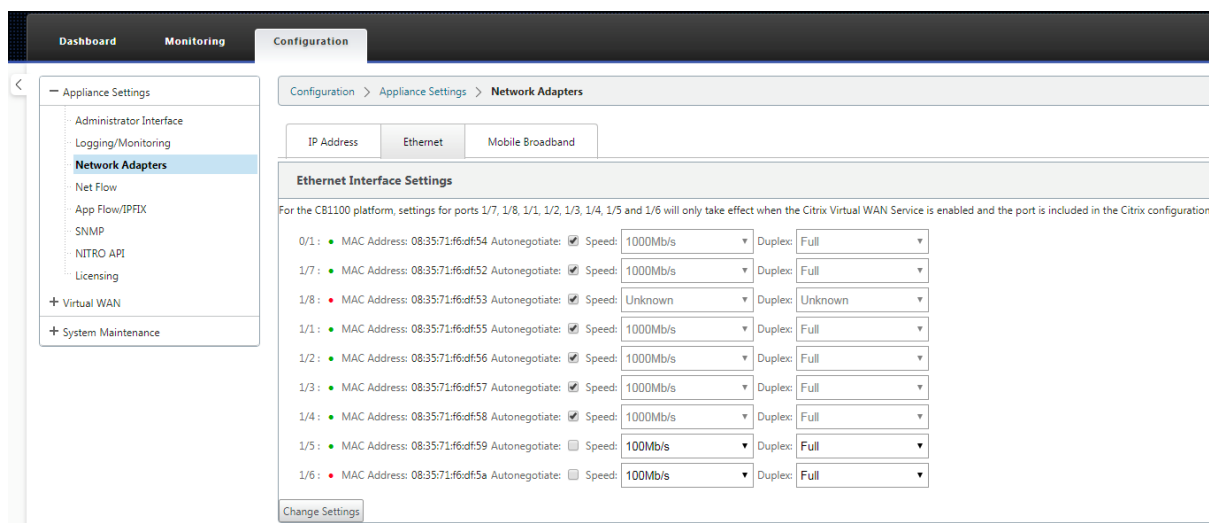
MiRiC-E1T1 FE/GBE SFP 用のシトリックス SD-WAN 1100 プラットフォームのサポート

1100 アプライアンスでは、SFP ポート 1/5 および 1/6 に対して、次の 2 種類の miriC SFP がサポートされています。

1. MiRiC-E1T1 FE SFPs.
2. MiRiC-E1T1 GBE SFPs.

miric-E1T1 FE SFP は、速度を 100 Mbps、デュプレックスを全二重に設定する必要があります。miric-E1T1 GBE SFP は、速度を 1 Gbps、デュプレックスを全二重に設定する必要があります。

構成するには、SD-WAN アプライアンスの GUI に移動し、**[構成] > [ネットワークアダプタ] > [イーサネット]** ページに移動します。



miriC SFP ウェブサービスにアクセスする

- SFP トランシーバのデフォルトの管理 IP アドレスは 192.168.205.1 です。このアドレスを使用して、SFP Web サービスに関連する設定 (T1 や E1 など) を設定できます。IP アドレスは 192.168.205.1 以外に変更できません。ただし、IP アドレスの競合は避けてください。
- 管理への SFP アクセスを有効にするには、次の手順を実行します。
 - ssh admin@ (IP アドレス) 経由でアプライアンスの CLI にログインします
 - 実行:sfp_access
 - 1/5 でアクセスを有効にするには、次のいずれかのコマンドを実行します。
 - enable 1/5 # GBE トランシーバのために動作しすでに設定されている場合のみ。
 - enable 1/5 100 # -FE トランシーバでのみ動作します
 - enable 1/5 1000 # -GBE トランシーバでのみ動作します
 - 1/5 100 172.217.43.2 #-FE トランシーバの場合、172.217.43.0/24 でユーザがデフォルトの IP を IP に変更すると仮定します
 - 有効 1/5 1000 172.217.43.2 #-GBE トランシーバの場合、ユーザがデフォルトの IP を 172.217.43.0/24 の IP に変更したと想定しています。

注:

1/5 で管理アクセスを有効にすると、1/6 の管理アクセスが自動的に無効になります。逆も同様です。

- 管理へのアクセスを無効にする手順は、次のとおりです。
 - SSH 管理者 @ (IP アドレス) 経由でアプライアンスの CLI にログインします
 - 実行:sfp_access
 - 実行: 無効にする

- ステータスを表示する手順は、次のとおりです。
 - SSH 管理者 @ (IP アドレス) 経由でアプライアンスの CLI にログインします
 - 実行:sfp_access
 - 実行: ステータス
- 設定が完了したら、管理アクセスを無効にしてください。
- アプライアンスが再起動されると、管理アクセスは自動的に無効になります。
- 仮想サービスが再起動されると、管理アクセスは、有効または無効の操作が完了するまで構成されたままになります。
- アプライアンスを無効にすると、SFP への管理アクセスは失われます。
- アプライアンスが再び有効になると、管理アクセスは回復されます。

3. SFP トランシーバの E1 または T1 タイプを設定するには、次の手順を実行します。

- クライアントマシンは、アプライアンス管理サブネットと同じ IP サブネットに存在する必要があります。
- クライアントマシンには、アプライアンス管理 IP をゲートウェイとする SFP トランシーバ IP アドレス 192.168.205.0/24 のサブネットへのルートが必要です。
- ブラウザを開き、[SFP トランシーバの管理](#)
- デフォルトのユーザー名:su
- デフォルトのパスワード:1234
- インターフェイスタイプ (E1 または T1) を設定するには、**[設定] > [物理ポート]** に移動し、ドロップダウンメニューから **[E1]** または **[T1]** を選択し、**[保存]** ボタンをクリックします。

工場出荷時リセット

April 15, 2021

ボタンを押して工場出荷時設定にリセット

Citrix SD-WAN 210、410、および 1100 アプライアンスの工場出荷時のデフォルト設定を復元するには、ボタンを押してリセットします。



Citrix SD-WAN 410 アプライアンスで工場出荷時設定にリセットするには:

1. 電源ボタンを使用してアプライアンスの電源を切ります。

注

アプライアンスの電源はオンになっているが、オフ状態であることを確認します。

2. クリップを使用して、NMI リセットボタンを 5 秒以上、または電源 LED が点滅し始めるまで押し続けます。
3. 電源 LED が点滅している状態で、電源ボタンを押して放し、工場出荷時の状態にリセットします。

Citrix SD-WAN 210 および 1100 アプライアンスで工場出荷時のリセットを実行するには:

1. 電源ボタンを使用してアプライアンスの電源を切ります。

注

アプライアンスの電源はオンになっているが、オフ状態であることを確認します。

2. クリップを使用して NMI ボタンを押して放すと、電源 LED が点滅し始めます。
3. 3 秒以内に電源ボタンを押して放し、工場出荷時のリセットプロセスを開始します。

ヒント

- NMI リセットボタンを偶数押すと、リセットアクションがキャンセルされ、アプライアンスが通常再起動します。
- リセットボタンを奇数回押すと、工場出荷時設定にリセットされます。
- 電源 LED が点滅すると、アプライアンスがリセット中であることが示されます。

アプライアンスが再起動し、CLI が表示されます。アプライアンスは、起動プロセスの抽出、コピー、初期化時に 4 ～ 5 回再起動することがあります。ログインプロンプトで、CLI または Web 管理インターフェイスを使用してアプライアンスの設定を開始できます。

内蔵 USB 経由で工場出荷時リセット

Citrix SD-WAN 210、410、1100、2100、4100、5100、6100 アプライアンスの出荷時のデフォルト設定を復元するには、内蔵 USB 経由でリセットを実行します。これらのアプライアンスには、工場出荷時のデフォルト設定を保存する内蔵 USB ドライブがあります。

内蔵 USB 経由でアプライアンスをリセットするには:

1. Citrix SD-WAN アプライアンスのシリアルコンソールにコンピュータを接続します。
2. アプライアンスを再起動します。
3. 画面上でカーソルが移動しているときにアプライアンスが起動している間に、次の手順に従います。
 - a) Esc キーを押したままにします。
 - b) [Shift] キーを押したままにします。
 - c) 数字 1 キーを押す (SHIFT +1 =!) すべてのキーを放します。
 - d) カーソルの移動を停止するまで、手順 a、b、c を繰り返します。
4. ブートメニューに表示される内部 USB オプションを選択します。

注

内部 USB 名は、プラットフォームによって異なる場合があります。ブートメニューにも UEFI と同様のオプションがあり、それを無視して UEFI のないものを選択してください。

Premium (Enterprise) Edition

April 15, 2021

重要:

** エンタープライズエディションアプライアンスはプレミアムにリブランドされています。エンタープライズという用語に関するすべての言及は **、新製品用語「プレミアム」に適用されます。

また、**NetScaler SD-WAN** 製品は **CitrixSD-WAN** にリブランドされます。**NetScaler SD-WAN** という用語に関するすべての言及は、新しい製品用語 **Citrix SD-WAN** に適用されます。

Citrix SD-WAN Premium

(Enterprise) アプライアンスには、次のエディションが含まれます。

- [SD-WAN Premium \(Enterprise\) エディション 1000、2000、および 2100](#)

Citrix SD-WAN 1000、2000、および 2100 Premium (Enterprise) Edition アプライアンス

April 15, 2021

SD-WAN Premium (Enterprise) Edition 1000、2000、および 2,100 のアプライアンスは、WAN 最適化の仮想インスタンスとアプライアンスにインストールされた仮想 WAN 機能を組み合わせています。仮想 WAN と WAN の最適化機能の組み合わせを提供します。

SD-WAN 1000 PE、2000 PE、および 2100 アプライアンスは、複数の仮想マシンをサポートする Citrix ブランチアーキテクチャに基づいています。すべてのブランチアプライアンスには、SD-WAN インスタンス、管理サービスインスタンス、Xenserver ハイパーバイザーが含まれます。

SD-WAN インスタンスは通常、インラインモードで使用されます。SD-WAN インスタンスは WAN ルータと LAN 間でやり取りされるため、WAN トラフィックは高速ブリッジを通過します。SD-WAN インスタンスは、単一のアクセラレーションブリッジポートを使用して、仮想インラインモードでデプロイすることもできます。

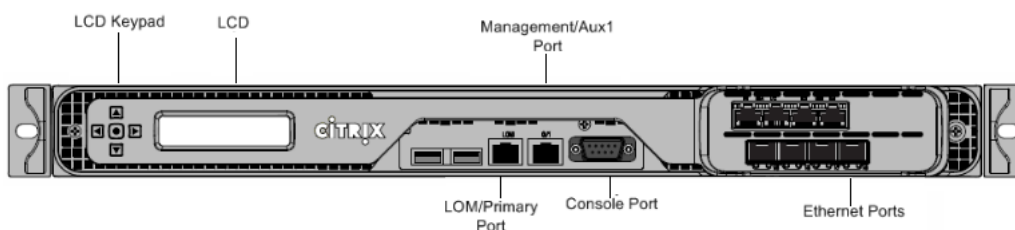
高速ブリッジと Windows **LAN** ポートに加えて、管理ポートはすべての仮想マシン（インスタンス）とハイパーバイザーに接続します。

アプライアンスには、2 ポートモードと 4 ポートモードの 2 つのモードがあり、ポート 1/3 と 1/4 の使用方法が決まります。

Citrix SD-WAN 2100 PE (EE) アプライアンス

April 15, 2021

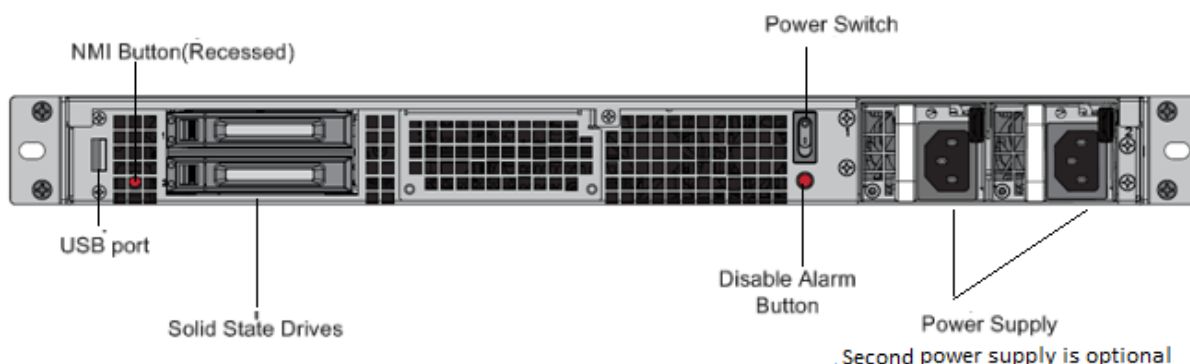
Citrix SD-WAN 2100 PE (EE) アプライアンスは、1U アプライアンスです。このアプライアンスには、2.1 GHz と 32 GB のメモリを持つ 8 コアプロセッサが搭載されています。



SD-WAN 2100 PE (EE) アプライアンスのフロントパネルには、次のポートがあります。

- RS232 シリアルコンソールポート。
- ライトアウト管理 (LOM) ポートと呼ばれる銅線イーサネット (RJ45) ポート。このポートは、仮想 WAN の初期プロビジョニングに使用できます。このポートを使用して、アプライアンスのソフトウェアとは無関係にアプライアンスをリモートで監視および管理できます。
- 2 つの USB ポート。
- 4 つの 1000Base-TX 銅線イーサネットポート (フェールツーワイヤ)。
- 4 つの 1GE SFP ポート。

Citrix SD-WAN 2100 PE (EE) 背面パネル



2100 PE (EE) アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- アプライアンスのソフトウェアとユーザーデータを格納する 240 GB および 480 GB リムーバブルソリッドステートドライブ
- 電源スイッチ。アプライアンスへの電源をオンまたはオフに切り替えます。スイッチを 5 秒間押し、電源を切ります。

- 単一電源、定格 450 ワット、100~240 ボルト。各電源装置には、次に説明するように、そのステータスを示す LED があります。2 台目の電源装置は、追加のアクセサリ（オプションのフィールド交換可能ユニット (FRU)）として利用できます。

2100 PE には 2 つのディスクがあり、ドライブ Bay1 は 240 GB SSD (ブートディスク)、ドライブ Bay2 は 480 GB SSD を保持します。古いブートディスクを新しい 240 GB SSD ブートディスクに置き換える場合は、Bay1 で新しい 240 GB SSD を接続し、480 GB SSD を差し込む前に 240 GB と 480 GB SSD の両方を取り外す必要があります。これは、BIOS がブート順序シーケンスを通常の状態に更新し、240 GB SSD (ブートディスク) から起動するために必要です。

重要

PE 機能を使用するには、2100 PE アプライアンスに SD-WAN リリース 10.0 が必要で、PE ライセンスをインストールします。

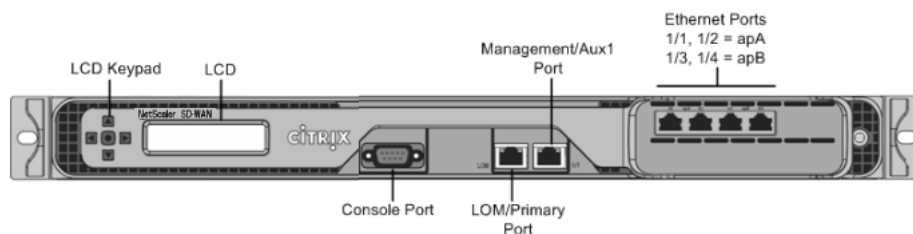
SD-WAN 2000 PE (EE) アプライアンス

April 15, 2021

Citrix SD-WAN 2000 PE (EE) プラットフォームは、1 つのクアドコアプロセッサと 24 ギガバイト (GB) のメモリを搭載した 1U アプライアンスです。

次の図は、SD-WAN 2000 PE (EE) アプライアンスの前面パネルを示しています。

図 1: Citrix SD-WAN 2000 PE (EE) アプライアンス、フロントパネル



SD-WAN 2000 PE (EE) アプライアンスには、次のポートがあります。

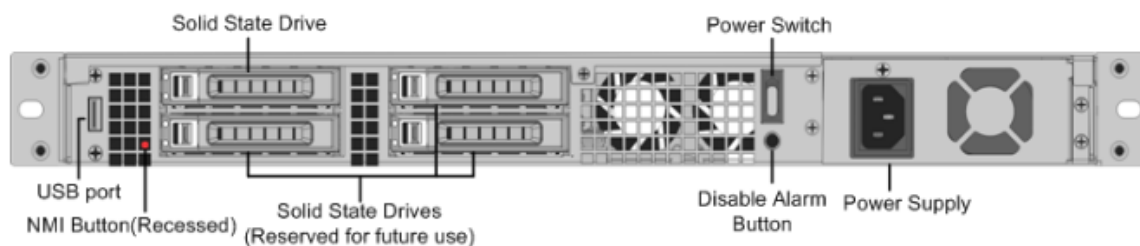
- RS232 シリアルコンソールポート。
- ライトアウト管理 (LOM) ポートと呼ばれる銅線イーサネット (RJ45) ポート。このポートを使用して、アプライアンスのソフトウェアとは無関係にアプライアンスをリモートで監視および管理できます。
- 銅線イーサネット (RJ45) 管理ポート。番号が 0/1 で、PRI (プライマリ) という名前が付いています。管理ポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。このポートは、WAN 最適化および Windows Server の初期プロビジョニングに使用できます。

注: LOM ポートは、管理ポートとしても動作します。

- 4つの 10/100/1000Base-T 銅線イーサネットポート。左から右に 1/1、1/2、1/3、および 1/4 の番号が付けられます。4つのポートは2つの加速ペアを形成し、加速ブリッジとして機能します。ポート 1/1 および 1/2 はアクセラレーションペア A (apA)、1/3 および 1/4 はアクセラレーションペア B (APB) です。

次の図は、SD-WAN 2000 PE アプライアンスの背面パネルを示しています。

図 2: Citrix SD-WAN 2000 PE アプライアンス、背面パネル



SD-WAN 2000 PE アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 600 GB リムーバブルソリッドステートドライブ。アプライアンスのソフトウェアとユーザーデータを格納し、1 TB のハードディスクドライブを格納します。
- 電源スイッチ。アプライアンスへの電源をオンまたはオフに切り替えます。スイッチを 5 秒間押し、電源を切ります。
- USB ポート (将来のリリース用に予約)。
- 非マスク割り込み (NMI) ボタン。テクニカルサポートの要求に応じてコアダンプを生成するために使用する。ペン、鉛筆、またはその他の尖ったオブジェクトを使用して、この赤いボタンを押します。このボタンは、意図しない起動を防ぐためにくぼんだ状態になっています。
- 300 ワット、100~240 ボルトの単一電源。

Citrix SD-WAN 1000 PE (EE) アプライアンス

April 15, 2021

SD-WAN 1000 PE (EE) プラットフォームには、クアッドコアプロセッサと 32 GB のメモリが搭載されています。このプラットフォームの帯域幅は最大 100 Mbps です。

次の図は、SD-WAN 1000 PE (EE) アプライアンスの前面パネルを示しています。

図 1: Citrix SD-WAN 1000 PE (EE)、フロントパネル



- SD-WAN 1000 PE (EE) アプライアンスの前面パネルには、電源ボタンと 5 つの LED があります。
- 電源ボタンは、アプライアンスのオン/オフを切り替えるために使用します。
- リセットボタンは、アプライアンスを再起動します。

LED は、アプライアンスのさまざまな部分に関連する重要な情報を提供します。

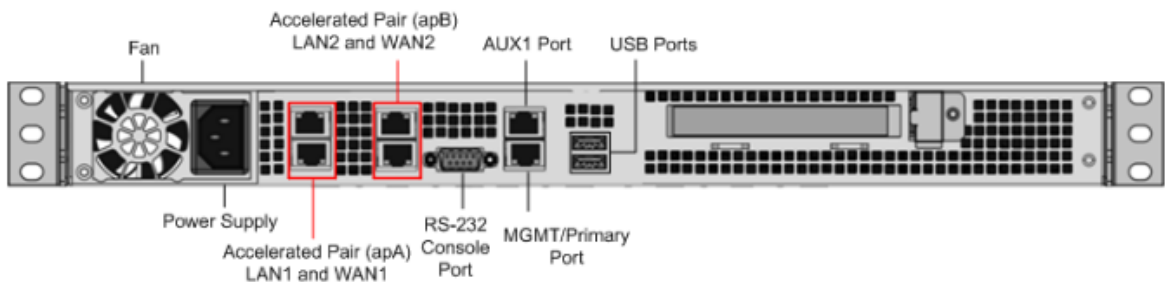
- [Power Fail]: 電源装置に障害が発生したことを示します。
- 情報 LED: 次のことを示します。

ステータス	説明
連続的にオンとレッド	アプライアンスが過熱しています。
ゆっくり点滅-毎秒 1 点滅	ファンの障害。ファンが動作しないかどうかを確認します。
高速点滅-毎秒 4 点滅	電源障害、動作していない電源装置を確認します。
青に点灯	ローカル UID がアクティブ化されました。この機能を使用して、ラックマウント環境でサーバを特定します。
高速点滅-毎秒 3~4 点滅	リモート UID はオンです。この機能を使用して、リモートロケーションからサーバを識別します。

- NIC1 および NIC2: LAN1 ポートおよび WAN1 ポートでのネットワークアクティビティを示します。
- HDD — ハードディスクドライブのステータスを示します。
- [Power]: 電源装置に電力が供給され、正常に動作していることを示します。

次の図は、SD-WAN 1000 EE アプライアンスの背面パネルを示しています。

図 2: Citrix SD-WAN 1000 PE (EE) アプライアンス、背面パネル

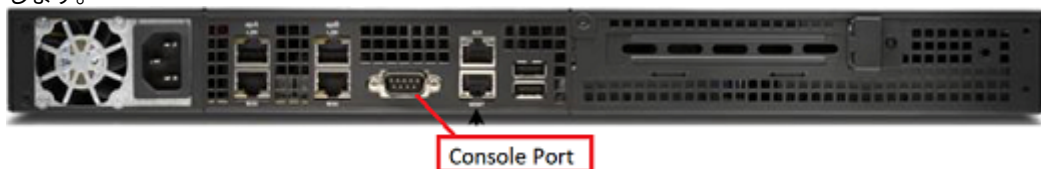


SD-WAN 1000 PE (EE) アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 冷却ファン
- 単一電源、定格 200 ワット、110~240 ボルト
- 加速ブリッジとして機能するイーサネットポートの加速ペア (apA および APB)
- RS-232 シリアル・コンソール・ポート
- AUX イーサネットポートと 1 つの管理ポート
- 2 つの USB ポート

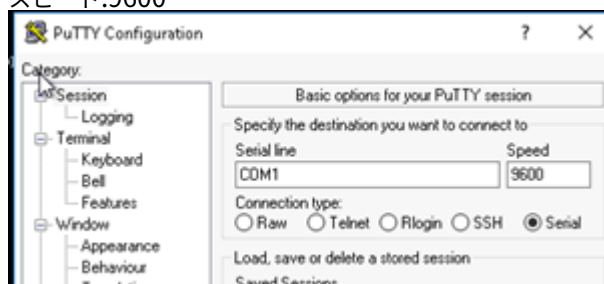
正常なシャットダウン後にアプライアンスの電源を入れます

1. シリアル・コンソール・ケーブルを、アプライアンスの背面と管理用ラップトップのシリアル・ポートに接続します。



2. 管理ラップトップで、次の構成設定を使用してパテセッションを再起動します。

- シリアル回線:COM1
- スピード:9600

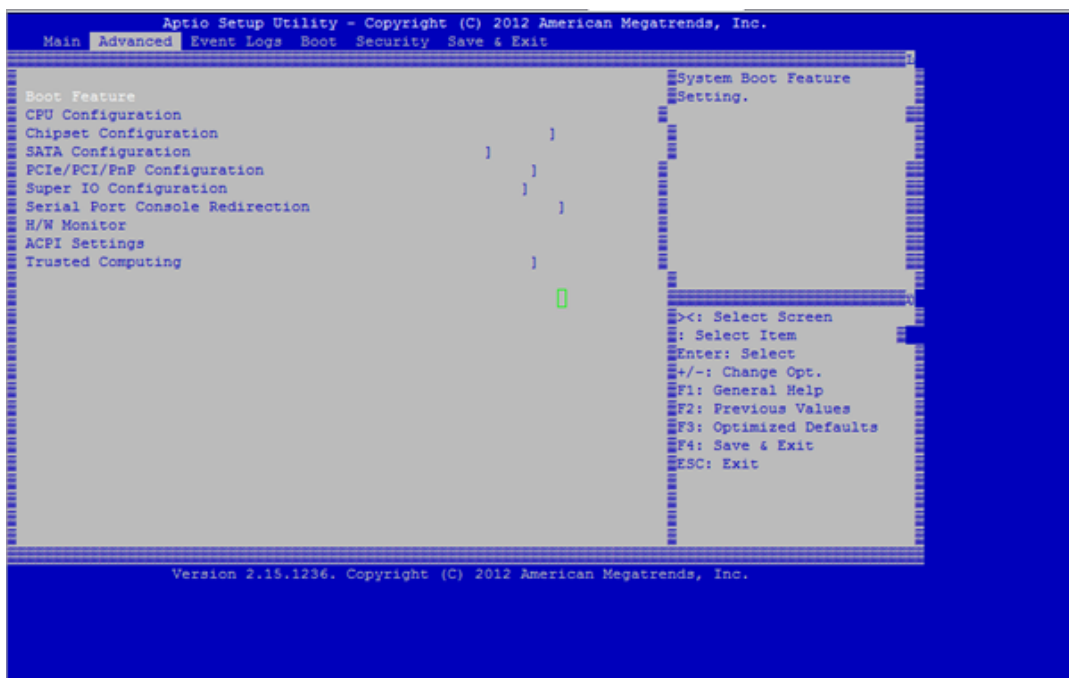


3. アプライアンスの電源を入れ、起動中に Putty セッションで次のキーを押して **BIOS** 設定画面に入ります。

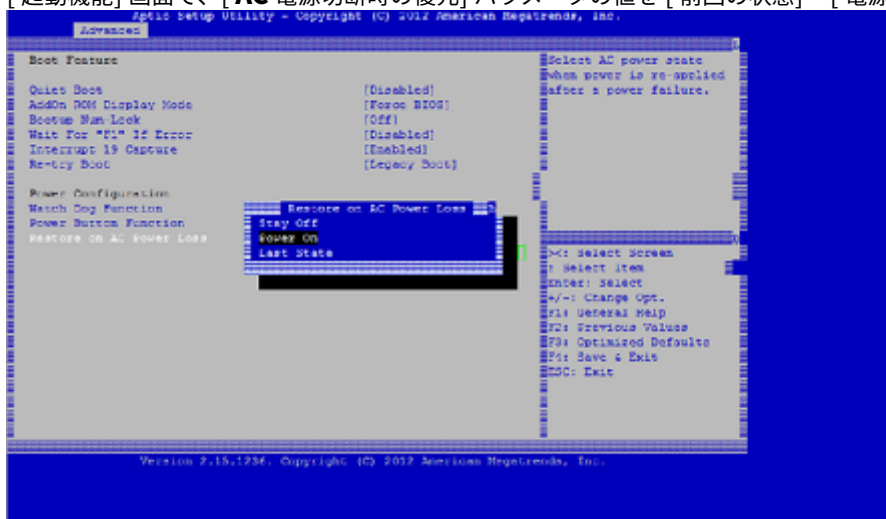
キー押し: **DEL**

4. BIOS で、

- [詳細] タブ > [選択
- 起動機能 > 入力



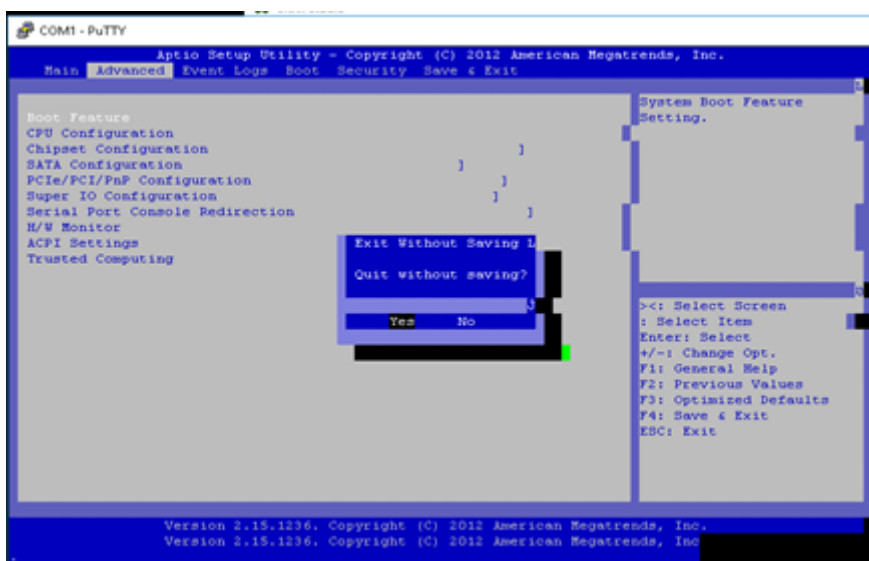
5. [起動機能]画面で、[AC電源切断時の復元]パラメータの値を[前回の状態]>[電源オン]から変更します。



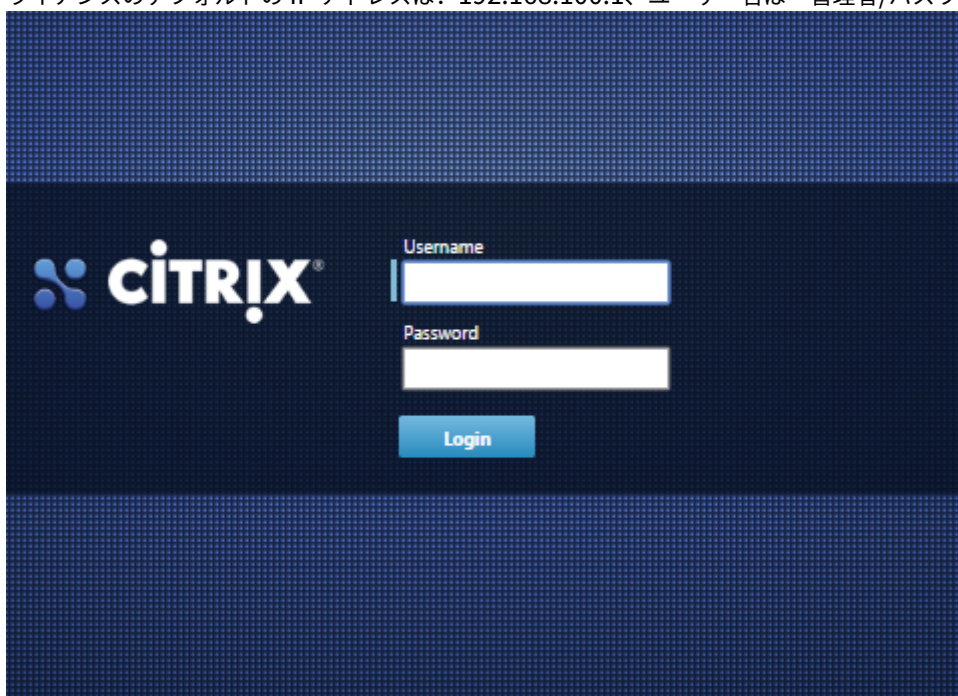
6. [保存して終了]に移動します。

- [** 変更を保存してリセット **]を選択します。
- [はい]

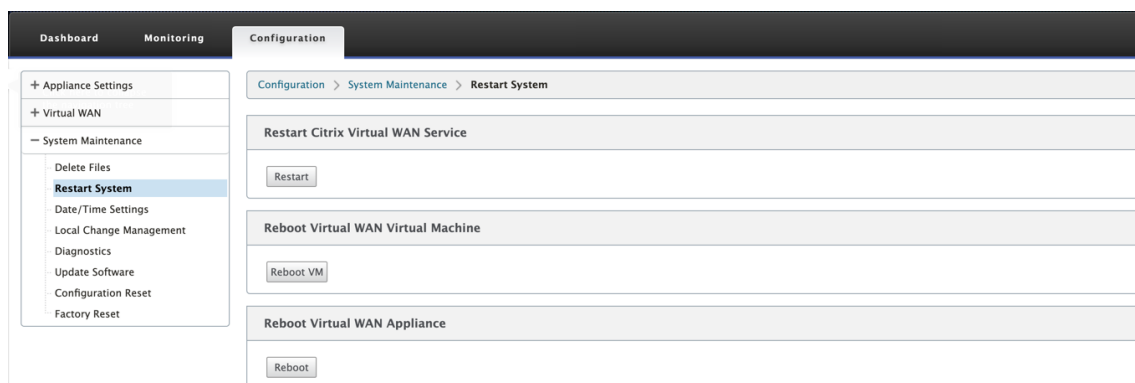
[システムの再起動を許可する]を選択します。これには約5分かかります。



7. アプライアンスの電源がオンになったら、アプライアンス管理インスタンス (SVM) にログインします。アプライアンスのデフォルトの IP アドレスは: 192.168.100.1、ユーザー名は「管理者/パスワード」です。



8. SD-WAN アプライアンスの GUI で、[構成] > [メンテナンス] > [アプライアンスの再起動] に移動します。アプライアンスが完全にシャットダウンできるようにします。シャットダウンプロセスが完了したら、アプライアンスに電源ライトがないことを確認します。



9. アプライアンスの電源をオンにして、BIOS 構成の変更が正常に適用されたことを確認します。これは、APC インテリジェント・PDU Web 管理コンソールを使用するか、シャットダウン SD-WAN アプライアンスから電源ケーブルを物理的に引き出し、10 秒間待ってから再び差し込むことで実行できます。アプライアンスの電源は、すべてのシャットダウンシナリオから自動的に起動します。

ハードウェア仕様の概要

April 15, 2021

次の表は、SD-WAN 1000 PE、2000 PE、および 2100 PE プラットフォームの仕様をまとめたものです。

仕様	SD-WAN 1000 PE	SD-WAN 2000 PE	SD-WAN 2100 PE
帯域幅	最大 100Mbps まで	最大 250Mbps	最大 1Gbps
規制モデル番号	NS 6xCU	NS 6xCU	1U1P1A
プロセッサ	4 コア	4 コア	8 コア、2.1GHz
ソリッドステートドライブ (SSD)	ディスクベース圧縮 (DBC) の場合は 123 GB、ビデオキャッシュの場合は 25 GB	ディスクベース圧縮 (DBC) の場合は 225 GB、ビデオキャッシュの場合は 50 GB	1X240GB と 1X480 GB
メモリ	32GB	24 ギガバイト	32GB
電源装置の数	電源装置 ×1	電源装置 ×1	電源装置 ×1、オプションの FRU × 1
AC 電源の入力電圧、周波数、電流	100 V AC から 240 V AC、50 ~60 Hz、1.7 ~3.4 A	100 V AC から 240 V AC、50 ~60 Hz、1.7 ~3.4 A	100 V AC から 240 V AC、50 ~60 Hz、1.7 ~3.4 A
直流電源入力電圧および電流	-40~-70V DC、4.8~8.6A	-40~-70V DC、4.8~8.6A	-40~-72V DC、4.8~8.6A
最大 AC 消費電力	200 W	300 W	450 W

仕様	SD-WAN 1000 PE	SD-WAN 2000 PE	SD-WAN 2100 PE
エアフロー（前面から背面）	22.1 CFM、フル:76.2 CFM	22.1 CFM、フル:76.2 CFM	22.1 CFM、フル:76.2 CFM
パッケージ重量 (ポンド) 配送の寸法と重量	長さ 26 インチ x 幅 18.5 インチ x 高さ 6.5 インチ、14.5 ポンド。	長さ 32 x 幅 23.5 x 高さ 7.5 インチ、39 ポンド。	長さ 33 インチ x 幅 24 インチ x 高さ 8 インチ、40 ポンド。
システム重量 (ポンド)	8.5 ポンド (3.9 キログラム)	32 ポンド (14.5 キログラム)	32 ポンド (14.5 キログラム)
ラックユニット	1U	1U	1U
幅	EIA 310-D, 19"	EIA 310-D, 19"	EIA 310-D, 19"
奥行き	10" 25.4 cm	25.4" (64.5 cm)	28" (71.1 cm)
動作温度	10–35 C	0–40 C	32–104 F (0–40 C)
非動作温度	-40~+70C	-40~+70C	14F~140F (-10C~60C)
湿度範囲（結露しないこと）	8%-90%	5%-95%	20%-80%
安全認定	CSA/EN/IEC/UL 60950-1 準拠、UL、または CSA リスト (米国およびカナダ)、CE マーキング (ヨーロッパ)	CSA/EN/IEC/UL 60950-1 準拠、UL、または CSA リスト (米国およびカナダ)、CE マーキング (ヨーロッパ)	IEC 60950-1、第 2 版、CSA 60950-1、第 2 版、UL 60950-1、第 2 版、AS/NZS 6050-1
EMC と感受性	FCC (パート 15 クラス A)、CCC、KCC、NOM、SASO、CITC、EAC、DOC、CE、VCCI、RCM	FCC (パート 15 クラス A)、CCC、KCC、NOM、SASO、CITC、EAC、DOC、CE、VCCI、RCM	米国 (FCC (パート 15 クラス A))、ヨーロッパ (CE (EN55032/ CISPR32))、オーストラリア (RCM)、日本 (VCCI)、韓国 (KCC)、台湾 (BSMI)、中国 (CCC)、インド (BIS)、ロシア (EAC)、サウジアラビア (CITC)、ブラジル (アナテル)、南アフリカ (ICASA)、メキシコ (NOM)、エジプト (NTRA)、イスラエル (MoC)

仕様	SD-WAN 1000 PE	SD-WAN 2000 PE	SD-WAN 2100 PE
環境認証	ROHS、ウィー	ROHS、ウィー	ROHS、ウィー

イーサネットポート名

April 15, 2021

アプライアンスの構成時に、アプライアンスのさまざまなイーサネットポートの IP アドレスを指定します。次の表に示すように、SD-WAN インスタンス内の SD-WAN 1000 PE および 2000 PE アプライアンスの前面パネルでは、イーサネットポートのラベルが異なります。

フロントパネル	SD-WAN インスタンス	
SD-WAN 1000 PE	SD-WAN 2000 PE	
管理管理 (青)	0/1 (LOM/PRI)	プライマリ
AUX	0/2 (AUX)	Aux
apA LAN1/WCCP (Green)	1/1	apA.1
apA WAN1	1/2	APA.2
APB LAN2	1/3	apB.1*
apB WAN2	1/4	apB.2*

SD-WAN インスタンスは、4 ポートモードでのみ使用できます。

アプライアンスのインストール

April 15, 2021

アプライアンスの設置場所が環境基準を満たしており、指示に従ってサーバラックが配置されていることを確認したら、ハードウェアを取り付ける準備が整います。アプライアンスをマウントしたら、ネットワーク、電源、および初期設定に使用するコンソール端末に、アプライアンスを接続する準備が整いました。Ethernet ポートを使用してアプライアンスをコンピュータに接続して、初期設定を行うこともできます。SD-WAN 1000 PE アプライアンスでは、このポートは MGMT (管理) ポートとラベル付けされ、SD-WAN 2000 PE では PRI (プライマリ) ポートというラベルが付けられます。インストールを完了するには、アプライアンスのスイッチをオンにします。インストール手順に記載されている注意事項と警告を必ず守ってください。

アプライアンスのラックマウント

April 15, 2021

SD-WAN 1000 PE (EE) または 2000 PE (EE) アプライアンスには、ラックユニットが 1 つ必要です。どちらもラックマウントデバイスで、2 支柱リレーラックまたは 4 ポスト EIA-310 サーバラックに取り付けることができます。ラックがアプライアンスと互換性があることを確認します。

アプライアンスのラックマウント

April 15, 2021

SD-WAN 1000 PE (EE) または 2000 PE (EE) アプライアンスには、ラックユニットが 1 つ必要です。どちらもラックマウントデバイスで、2 支柱リレーラックまたは 4 ポスト EIA-310 サーバラックに取り付けることができます。ラックがアプライアンスと互換性があることを確認します。

ケーブルの接続

April 15, 2021

アプライアンスがラックにしっかり取り付けられている場合は、使用するポートを決定します。これで、ケーブルを接続する準備が整いました。Ethernet ケーブルとオプションのコンソールケーブルを最初に接続します。最後に電源ケーブルを接続します。

警告: アプライアンスの取り付けまたは修理を行う前に、電源やワイヤに接触している可能性のあるジュエリーやその他の金属部品をすべて取り外してください。電気の通じている電源または配線とアースの両方に触れると、金属物が急速に加熱し、火傷を負ったり、衣服に火が付いたり、金属物が溶けて露出している端子がショートしたりする可能性があります。

ポート

単一のアクセラレーションブリッジを使用する一般的なインストールでは、4 つのイーサネットポート（プライマリポートと apA）と 6 つの IP アドレス（プライマリポートのサブネットに 4 つ、ApA のサブネットに 2 つ）を使用します。

アプライアンスには、マザーボードポートが 2 つと 2 つの加速ブリッジがあります。

- マザーボードポートは、SD-WAN 1000 アプライアンスでは MGMT（管理）ポートと AUX1（補助）ポート、SD-WAN 2000 アプライアンスでは PRI（プライマリ）および AUX（補助）のラベルが付けられます。初期設

定には、SD-WAN 1000 アプライアンスの MGMT ポートと SD-WAN 2000 アプライアンスの PRI ポートを使用します。

- 高速ブリッジポートは、SD-WAN 1000 アプライアンスの背面パネルと SD-WAN 2000 アプライアンスの前面パネルでは、apA および APB を使用できます。SD-WAN 1000 アプライアンスでは、これらのポートは、それぞれ「LAN1」と「WAN1」、および「LAN2」と「WAN2」というラベルが付けられます。ただし、SD-WAN 2000 アプライアンスでは、これらのポートはそれぞれ 1/1 と 1/2、および 1/3 と 1/4 とラベル付けされます。

イーサネットケーブルの接続

Ethernet ケーブルはアプライアンスをネットワークに接続します。必要なケーブルの種類は、ネットワークへの接続に使用するポートの種類によって決まります。10/100/1000BASE-T ポートには、標準 RJ-45 コネクタを備えたカテゴリ 5e またはカテゴリ 6 イーサネットケーブルを使用します。

イーサネットケーブルを **10/100/1000BASE-T** ポートに接続するには

1. イーサネットケーブルの一端にある RJ-45 コネクタを適切なポートに挿入します。**SD-WAN 1000** アプライアンスでは、これらのポートは背面パネルで使用でき、LAN および WAN リンク用の apa ブリッジポートの場合は、それぞれ LAN1 および WAN1 とラベル付けされています。**SD-WAN 2000** アプライアンスでは、ポートはフロントパネルで使用できます。SD-WAN 2000 のポートには、apa ブリッジポートの 1/1 および 1/2 というラベルが付けられます。LAN に 1/1、WAN リンクに 1/2 を使用できます。
2. もう一方の端の RJ-45 コネクタを、ルーターやスイッチなどのターゲットデバイスに挿入します。
3. 接続が確立されて、黄色の LED が点灯することを確認します。

コンソールケーブルの接続

コンソールケーブルを使用して、アプライアンスをコンピューターまたは端末に接続します。このコンピューターまたは端末からアプライアンスを設定できます。コンソールケーブルを接続する前に、コンピューターまたは端末を、VT100 端末エミュレーション、9600 ボー、8 データビット、1 ストップビット、および「NONE」に設定されたフロー制御をサポートするように設定します。次に、コンソールケーブルの一方の端をアプライアンスの RS232 シリアルポートに、もう一方の端をコンピューターまたは端末に接続します。

コンソールケーブルをコンピューターまたは端末に接続するには

1. ケーブルの端にある DB-9 コネクタをコンソールポートに挿入します。**SD-WAN 1000** アプライアンスでは、ポートは背面パネルにあります。**SD-WAN 2000** アプライアンスでは、ポートはフロントパネルにあります。

注：RJ-45 コンバータ付きのケーブルを使用するには、付属のオプションのコンバータをコンソールポートに挿入し、ケーブルを接続します。

2. ケーブルのもう一方の端にある RJ-45 コネクタをコンピューターまたは端末のシリアルポートに挿入します。

電源ケーブルの接続

SD-WAN アプライアンスには 1 つの電源装置があります。3 極プラグはアースを兼ねているので、別途アースケーブルを用意する必要はありません。電源コードを取り付けて、アプライアンスに電力を供給します。電源ケーブルのもう一方の端を、標準 110V/220V 電源コンセントに接続します。

アプライアンスのスイッチを入れる

April 15, 2021

アプライアンスをラックに取り付け、ケーブルを接続したら、電源ケーブルが正しく接続されていることを確認します。接続を確認したら、アプライアンスをオンにできます。

アプライアンスをオンにするには

1. アプライアンスがコンソールポートまたはイーサネットポートを介して接続されていることを確認します。これにより、電源を入れた後にアプライアンスを構成できます。
2. アプライアンスのオン/オフ切り替え電源スイッチを押します。
3. SD-WAN **2000** アプライアンスで、フロントパネルの LCD がバックライトされており、開始メッセージが表示されることを確認します

注意: 緊急電源オフ (EPO) スwitchの位置に注意してください。これにより、電気事故が発生した場合、アプライアンスの電源をすばやく取り外すことができます。

初期構成

April 15, 2021

接続を確認したら、SD-WAN 1000 および 2000 アプライアンスをネットワーク上に展開する準備が整いました。

Citrix から出荷されたアプライアンスには、デフォルトの IP アドレスが構成されています。アプライアンスをネットワークに展開するには、アプライアンスに適切な IP アドレスを構成して、ネットワークトラフィックを高速化する必要があります。

初期設定を実行するには、次の手順に従います。

- 初期構成の前提条件を特定します。
- 初期構成手順に必要なさまざまな値を記録します。
- アプライアンスをイーサネットポートに接続して構成します。
- Windows 用の構成をさらに実行します。
- シリアルコンソールから管理 IP アドレスを割り当てます。

- 初期設定の問題のトラブルシューティングを行います。

デフォルトでは、初期構成はアプライアンスをインラインモードで展開します。

前提条件

April 15, 2021

アプライアンスの構成を開始する前に、次の前提条件が満たされていることを確認してください。

- アプライアンスへの物理的なアクセス権を持っている必要があります。
- ワークシートに、アプライアンスの構成に使用するすべての IP アドレスおよびその他の値を記録します。できれば、構成プロセスを開始する前に、ワークシートを印刷してください。
- Citrix からの SD-WAN ライセンスキーをメールで送信する必要があります。リモートライセンスを使用している場合は、ライセンスサーバーの IP アドレスが必要です。
- WAN の送信速度と受信速度。

コンピュータをイーサネットポートに接続してアプライアンスを構成する

April 15, 2021

SD-WAN アプライアンスの初期設定を行うには、次のタスクを実行します。

- サイトで使用するようアプライアンスを構成します。
- Citrix ライセンスをインストールします。
- アクセラレーションを有効にします。
- トラフィックシェーピングを有効にします（インラインモードのみ）。

インライン展開では、ほとんどのアクセラレーション機能がデフォルトで有効になっており、追加の構成を必要としないため、この構成で十分な場合があります。

アプライアンスをコンピュータに接続するアプライアンスは、イーサネットポートまたはシリアルコンソールを使用して設定できます。以下の手順では、イーサネットポートを介してアプライアンスをコンピュータに接続してアプライアンスを構成できます。

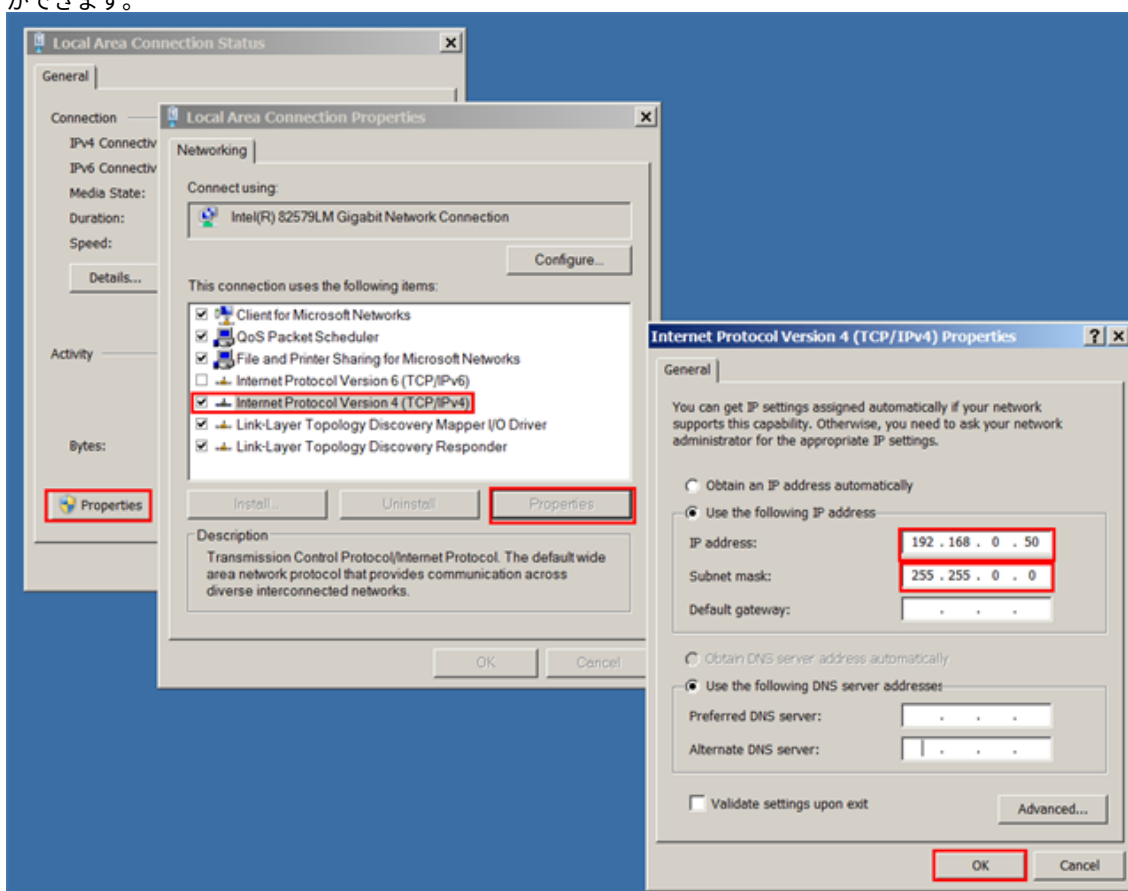
注: SD-WAN 1000 アプライアンスでは、MGMT というラベルの付いたイーサネットポートを使用します。ただし、SD-WAN 2000 アプライアンスでは、PRI または LOM というラベルの付いたイーサネットポートを使用します。

シリアル・コンソールを使用してアプライアンスをコンピュータに接続して構成する場合は、「シリアル・コンソールによる管理 IP アドレスの割り当て」手順を完了して、ワークシートから管理サービス IP アドレスを割り当てます。次に、次の手順の手順 4～25 を実行します。

注: アプライアンスに物理的にアクセスできることを確認してください。

コンピュータを **SD-WAN** アプライアンスのイーサネットポート **0/1** に接続してアプライアンスを設定するには

1. コンピュータ（またはイーサネットポートを備えた他のブラウザ搭載デバイス）のイーサネットポートアドレスを 192.168.100.1 に設定します。ネットワークマスクは 255.255.0.0 です。Windows デバイスでは、これは、以下に示すように、LAN 接続のインターネットプロトコルバージョン 4 のプロパティを変更することによって行われます。ゲートウェイフィールドと DNS サーバーのフィールドを空白のままにしておくことができます。



2. イーサネットケーブルを使用して、このコンピュータを SD-WAN 1000 アプライアンスの MGMT とラベル付けされたポート、または SD-WAN 2000 アプライアンスの PRI とラベル付けされたポートに接続します。
3. アプライアンスの電源を入れます。コンピュータの Web ブラウザを使用して、デフォルトの管理サービス IP アドレス <http://192.168.100.1> を使用してアプライアンスにアクセスします。
4. ログインページで、次のデフォルトの認証情報を使用してアプライアンスにログオンします。
5. 始めましょクリックして設定ウィザードを起動します。
6. 次の例に示すように、「プラットフォーム構成」ページで、ワークシートからそれぞれの値を入力します。

The screenshot shows a configuration wizard with the following sections:

- Network Configuration:**
 - XenServer IP Address*: 10 . 102 . 76 . 96
 - Management Service IP Address*: 10 . 102 . 76 . 97
 - Netmask*: 255 . 255 . 255 . 0
 - Gateway*: 10 . 102 . 76 . 1
 - DNS*: 10 . 140 . 50 . 6
- CloudBridge Configuration:**
 - IP Address*: 10 . 102 . 76 . 98
 - Use System Netmask and Gateway
 - Netmask*: 255 . 255 . 255 . 0
 - Gateway*: 10 . 102 . 76 . 1
- System Settings:**
 - NTP Server*: pool.ntp.org
 - Time Zone*: UTC-0700 PDT America/Los_Ang
- Admin Password:**
 - Change Password

Buttons: Done, Cancel

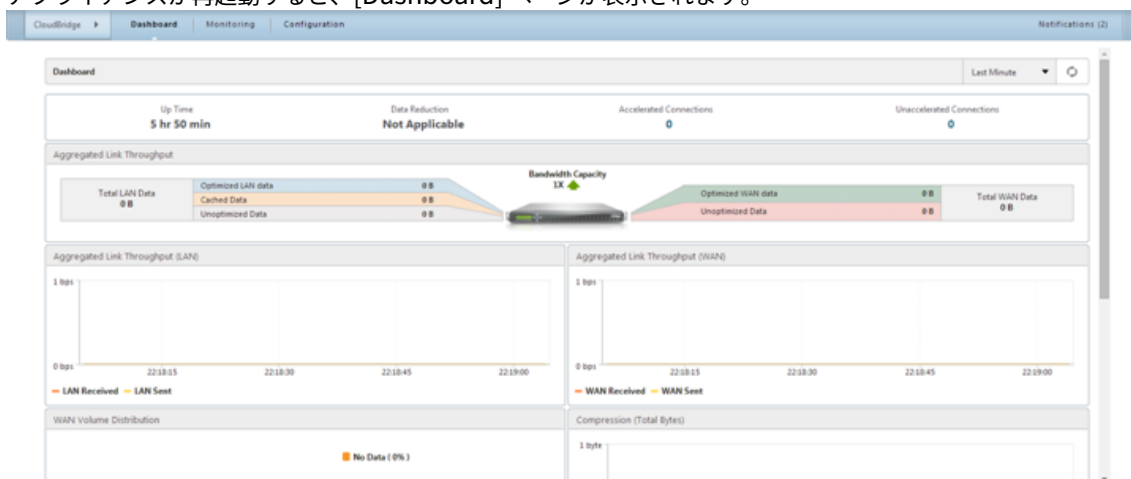
注: SD-WAN 構成で、ネットワーク構成と同じネットワークマスクとゲートウェイを使用する場合は、
[システムネットマスクとゲートウェイを使用] オプションを選択します。

7. [完了] をクリックします。インストール中...メッセージを示す画面が表示されます。このプロセスには、ネットワーク速度にもよりますが、約 2~5 分かかります。

注: アプライアンスをシリアル・コンソール・ポート経由でコンピュータに接続して構成する場合は、手順 8 から手順 14 を省略してください。

8. 新しい管理 IP へのリダイレクトメッセージが表示されます。
9. **[OK]** をクリックします。
10. コンピューターをイーサネットポートから取り外し、ポートを管理ネットワークに接続します。
11. コンピューターの IP アドレスを以前の設定にリセットします。
12. 管理ネットワーク上のコンピュータから、新しい管理サービス IP アドレス (https://<Management_IP_Address>など) を Web ブラウザに入力して、アプライアンスにログオンします。
13. 構成を続行するには、証明書を受け入れて続行します。続行するオプションは、使用している Web ブラウザーによって異なります。
14. アプライアンスにログオンします。
15. 構成ウィザードが再び起動します。このウィザードでは、既に指定した値のいくつかは既定で表示されます。ワークシートに記録した残りの値を指定します。
16. [システムサービス] セクションで、必要に応じて値を更新します。
17. [ライセンス] セクションで、適切なライセンスの種類を選択します。ローカルライセンスまたはリモートライセンスサーバーを選択して、アプライアンスにライセンスを適用できます。

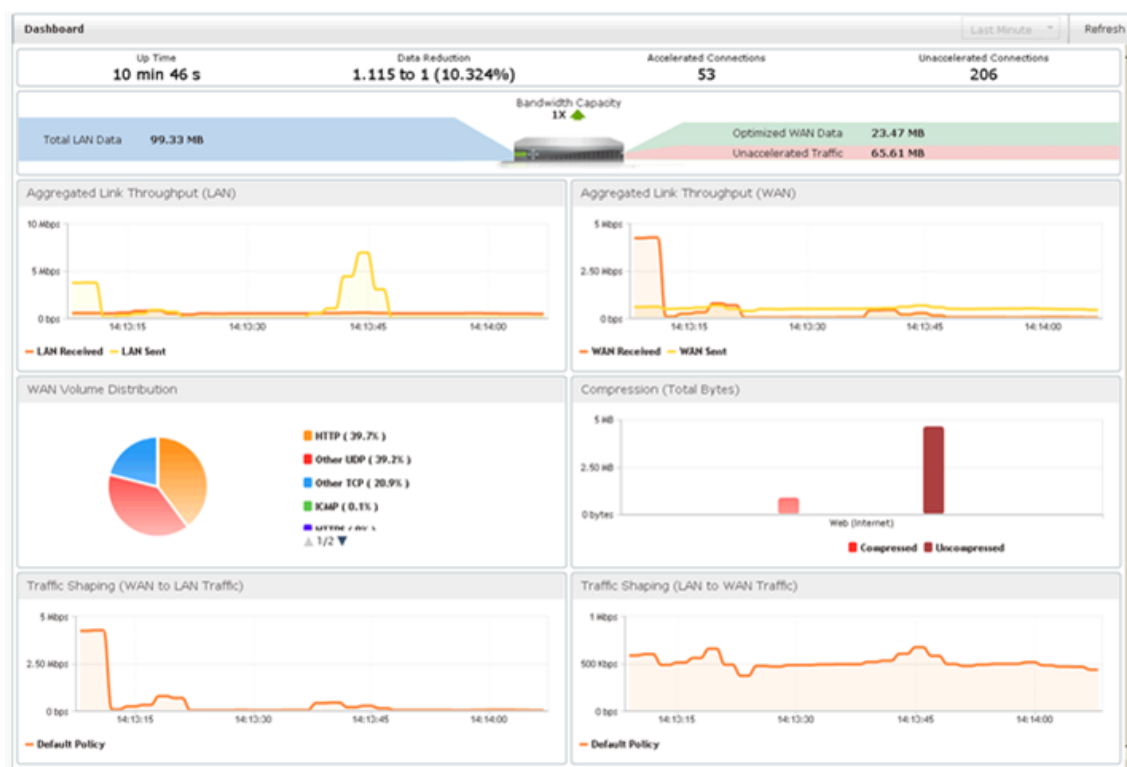
- a) ローカルライセンスを選択する場合は、アプライアンスのホスト ID を使用してライセンスを生成する必要があります。アプライアンスのローカルライセンスを生成するには、<http://support.citrix.com/article/ctx131110>を参照してください。ライセンスを適用するには、構成ウィザードを完了した後、[SD-WAN] > [構成] > [アプライアンスの設定] > [ライセンス] ページに移動します。
 - b) リモートライセンスサーバーを選択する場合は、リモートアプライアンスモデルを選択し、ライセンスサーバーの IP アドレスを [ライセンスサーバーアドレス] フィールドに入力する必要があります。
18. [WAN リンク定義] セクションで、各フィールドに WAN リンクの受信速度と送信速度を指定します。ネットワークの輻輳を避けるために、WAN 帯域幅よりも 10%低い値に設定することをお勧めします。
 19. デフォルトでは、WAN 側のアダプタ設定はアプライアンス上で構成されています。デフォルトの設定をそのまま適用してください。
 20. [インストール] をクリックします。インストールプロセスが完了すると、アプライアンスは再起動します。
 21. アプライアンスが再起動すると、[Dashboard] ページが表示されます。



22. ネットワークトラフィックを加速するようにアプライアンスを構成するには、[**Configuration**] タブを開きます。

注: アプライアンスに適切なライセンスがすでに適用されていることを確認してください。
23. [アプライアンスの設定] ノードの [ネットワークアダプタ] ページで、使用するアクセラレーションブリッジ (apa および APB) に IP アドレス、サブネットマスク、ゲートウェイを確認し、必要に応じて割り当てます。これらの変更を適用すると、アプライアンスが再起動されます。

注: アプライアンスで WCCP モード、仮想インラインモード、またはビデオキャッシュ機能を設定する場合のみ、Apa および APB アダプタに IP アドレスを割り当てる必要があります。
24. 初期設定が完了しました。トラフィックがアプライアンスを通過するようになりました。[ダッシュボード] ページには、このトラフィックが表示されます。



25. 仮想インラインモード、ビデオキャッシング、セキュアピアリング、高可用性、暗号化された CIFS/MAPI アクセラレーション、AppFlow 監視、SNMP 監視など、一部のモードと機能を使用する場合は、アプライアンス上でさらに構成する必要があります。

注:

- インラインインストールでは、アプライアンスを LAN と WAN ルータの間に配置します。たとえば、Windows サーバを備えた SD-WAN 1000 アプライアンスのポート LAN1 と WAN1、または Windows Server を使用する SD-WAN 2000 アプライアンスのポート 1/1 と 1/2 など、アクセラレーションされたブリッジポートの両方を使用して、APA アクセラレーションブリッジポート用にアプライアンスを配置します。
- WCCP および仮想インラインインストールは、単一のアクセラレーションブリッジポートを WAN ルータに接続します。
- 仮想インラインインストールでは、WAN トラフィックをアプライアンスに転送するようにルータを設定する必要があります。「[ルーター構成](#)」を参照してください。
- WCCP のインストールには、ルータとアプライアンスの設定が必要です。「[WCCP モード](#)」を参照してください。

シリアルコンソールを介した管理 IP アドレスの割り当て

April 15, 2021

コンピュータの設定を変更したくない場合は、シリアルヌルモデムケーブルを使用してアプライアンスをコンピュータに接続することで、初期構成を実行できます。アプライアンスに物理的にアクセスできることを確認します。

シリアルコンソールからアプライアンスを構成するには

1. シリアルヌルモデムケーブルをアプライアンスのコンソールポートに接続します。
2. ケーブルのもう一方の端を、Microsoft ハイパーターミナルなどのターミナルエミュレータを実行しているコンピュータのシリアル COM ポートに接続します。設定 9600、N、8、1、p。
3. ハイパーターミナルの出力で、**Enter** キーを押します。端末画面にログオンプロンプトが表示されます。

注意: 使用している端末プログラムによっては、**Enter** キーを 2~3 回押す必要がある場合があります。
4. ログオンプロンプトで、次のデフォルトの資格情報を使用してアプライアンスにログオンします。
 - ユーザー名: nsroot
 - パスワード: nsroot。
5. **\$** プロンプトで次のコマンドを実行して、アプライアンスのシェルプロンプトに切り替えます。\$ ssh 169.254.0.10
6. [はい]を入力して、管理サービスへの接続を続行します。
7. 次のデフォルトの認証情報を使用して、アプライアンスのシェルプロンプトにログオンします。
 - パスワード: nsroot。
8. ログオンプロンプトで、次のコマンドを実行して、管理サービスの初期ネットワークアドレスの構成メニューを開きます。## networkconfig
9. **1** と入力し、**Enter** キーを押してオプション **1** を選択し、管理サービスの新しい管理 IP アドレスを指定します。
10. **2** を入力し、**Enter** キーを押してオプション **2** を選択し、XenServer サーバーの新しい管理 IP アドレスを指定します。
11. **3** を入力し、**Enter** キーを押してオプション **3** を選択し、管理サービスの IP アドレスのネットワークマスクを指定します。
12. **4** を入力し、**Enter** キーを押してオプション **4** を選択し、管理サービスの IP アドレスのデフォルトゲートウェイを指定します。
13. **8** と入力し、**Enter** キーを押して設定を保存し、終了します。
14. SD-WAN アプライアンスにアクセスするには、管理ネットワーク上のコンピュータの Web ブラウザで、アプライアンスの新しい管理サービス IP アドレス (https://<Management_Service_IP_Address> など) を入力します。
15. 構成を続行するには、証明書を受け入れて続行します。続行するオプションは、使用している Web ブラウザによって異なります。

16. コンピュータをイーサネットポートに接続してアプライアンスを構成する手順の手順 4～25 を実行して、構成プロセスを完了します。

SD-WAN アプライアンスの設定

April 15, 2021

SD-WAN アプライアンスハードウェアをセットアップするには、[アプライアンスハードウェアのセットアップ](#)に記載されている手順を参照してください。

Citrix SD-WAN 5100 Premium (Enterprise) Edition アプライアンス

April 15, 2021

Citrix SD-WAN Premium (Enterprise) Edition 5100 アプライアンスは、混雑しているデータセンター向けの高性能アプライアンスです。

このアプライアンスは、多くの支店や地域のサイトと通信するビジネスイ状態のデータセンターで、1 Gbps を超える速度で仮想 WAN リンクを操作するように設計されています。

ハブアンドスポーク展開のハブでは、SD-WAN 5100 PE (EE) を推奨します。ハブアンドスポーク展開では、リンク速度または XenApp/XenDesktop ユーザー数が小さいアプライアンスでサポートできるよりも高い場合は、小さいアプライアンスがスポークで使用されます。

Citrix SD-WAN 5100 PE

April 15, 2021

SD-WAN 5100 PE は、2U アプライアンスです。各モデルには、合計 20 個の物理コア (ハイパースレッディング付き 40 コア) と 128 GB (GB) のメモリ用の 2 つの 10 コアプロセッサが搭載されています。最新のパフォーマンスと帯域幅容量の詳細については、より定期的に更新される最新のデータシートを参照してください。[citrix.com](#); [データシート](#)。

SD-WAN 5100 PE アプライアンスのフロントパネルには、次のポートがあります。

- 10/100Base-T 銅線イーサネットポート (RJ45)。ライトアウト管理 (LOM) ポートとも呼ばれます。このポートを使用して、アプライアンスのソフトウェアとは無関係にアプライアンスをリモートで監視および管理できます。
- RS232 シリアルコンソールポート。

- 2つの 10/100/1000Base-T 銅線イーサネット管理ポート (RJ45)。これらのポートは、システム管理機能のためにアプライアンスに直接接続するために使用されます。
- 8個の 10G ポート-バイパス付き LC ファイバポート ×4、SFP+ ポート (バイパスなし) 4 個。
- 2つの USB ポート (将来のリリース用に予約)

SD-WAN 5100 PE アプライアンスの背面パネルには、次のコンポーネントが表示されます。

- 2 X 1 TB リムーバブルハードディスクドライブ。
- 960 GB 以上の SSD が必要です。SSD を 3 番目、4 番目、5 番目のドライブベイに挿入します。
- 起動ドライブベイ 1、2 [HDD]-ハードドライブ、容量 1 TB、2.5 インチ、SATA 6 Gb/秒。
- ドライブベイ 3、4、5[SSD]-ソリッドステートドライブ、960 GB。
- ドライブベイ [プラスチックフィルタ] 6,7,8-2.5 インチ SSD プラスチックドライブトレイフィルタ。
- 電源スイッチ。電源装置を取り外すかのように、アプライアンスへの電源を切ります。スイッチを 5 秒間押し、電源を切ります。
- PS アラームボタンを無効にします。このボタンは、アプライアンスに電源装置が 2 つある場合にのみ機能します。このボタンを押して、アプライアンスを 1 つの電源コンセントにのみ差し込んだ場合、または 1 つの電源装置が故障して修理されるまでアプライアンスを操作し続ける場合に、電源アラームが鳴るのをミュートします。
- ホットスワップ対応デュアル冗長電源 (100~240VAC 標準、-48VDC オプション)

5100 アプライアンスに使用される電源は、1000 W ごとに 2 つの電源装置です。

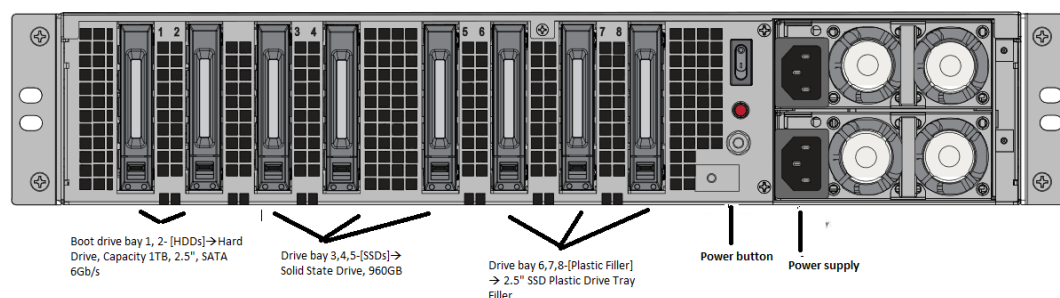
Standard Edition から Premium Edition へのアップグレードでは、ベイ 3、4、5 に搭載された SSD の 3 つである 960G SSD が使用されます。



5100 SE アプライアンスを 5100 PE アプライアンスにアップグレードする

ソリッドステートドライブ (SSD) を挿入する

1. 標準エディションアプライアンスに必要な SSD を挿入します。SSD を挿入する方法については、[ソリッドステートドライブ](#) (フィールド交換可能ユニット) を参照してください。
 - a) 5100 SE アプライアンスには、960 GB 以上の SSD が必要です。SSD を 3 番目、4 番目、5 番目のドライブベイに挿入します。



2. SD-WAN Web 管理インターフェイスを使用してアプライアンスを再起動します。
3. アプライアンスにインストールされているソフトウェアリリースバージョンが SD-WAN リリースバージョン 10.0 であることを確認します。ここに記載されている手順に従います。[新しいアプライアンスのアップグレード](#)。
4. Premium (Enterprise) Edition プラットフォームライセンスをインストールします。ライセンス情報については、Citrix SD-WAN 製品のダウンロードサイトを参照してください。
5. [シングルステップアップグレード](#)を使用してネットワークをソフトウェアリリースバージョン 10.0 以降にアップグレードします。

ハードウェア仕様の概要

April 15, 2021

次の表は、Citrix SD-WAN 5100 PE ハードウェアプラットフォームの仕様をまとめたものです。

仕様	SD-WAN 5100 PE
規制モデル番号	2U1P1D
プロセッサ	10 コア 2 個
メモリ	128GB
電源装置の数	1 (冗長性のためのオプションの第 2 電源装置)
AC 電源、入力電圧、周波数および電流	交流 100-240 V、47–63 Hz; 9.0-4.5 A
最大 AC 消費電力	850 W
パッケージ重量	69 ポンド
配送寸法	高さ 36.5 フィート × 幅 24.5 フィート × 高さ 11 フィート
システム重量	60 ポンド
ラックユニット	2RU

仕様	SD-WAN 5100 PE
ラックオプション-幅	EIA 310-D、IEC 60297、DIN 41494 SC48D ラック幅、マウントブラケット付き
奥行き	28” (72 cm)
動作温度	32–104 F (0–40 C)
湿度 (結露しないこと)	20% - 80%
安全認定	CSA
EMC と感受性	米国 (FCC)、ヨーロッパ (CE)、日本 (VCCI)、オーストラリア (RCM)、中国 (CCC)、韓国 (KCC)、インド (BIS)、メキシコ (NOM)、サウジアラビア (CITC)、南アフリカ (ICASA)、ロシア (EAC)、台湾 (BSMI)、ブラジル (Anatel)、イスラエル (MoC)
環境コンプライアンス	ROHS, WEEE

VPX モデル

April 15, 2021

重要:

NetScaler SD-WAN 製品は **CitrixSD-WAN** にリブランドされています。 **NetScaler SD-WAN** という用語に関するすべての言及は、新しい製品用語 **Citrix SD-WAN** に適用されます。

Citrix SD-WAN VPX (仮想) アプライアンスには、次のエディションが含まれます。

- [SD-WAN VPX-SE](#)
- [SD-WAN VPX-WANOP](#)
- [SD-WAN VPX-L](#)

Citrix SD-WAN VPX Standard Edition

April 15, 2021

Citrix SD-WAN スタンダードエディションは、Citrix XenServer、VMware ESX または ESXi、Microsoft Hyper-V、および Amazon AWS 仮想化プラットフォーム上でホストできる仮想 Citrix SD-WAN アプライアンスです。SD-WAN VPX アプライアンスは、物理スタンダードエディションまたは WANOP アプライアンスのほとんどの機能をサポートしています。

SD-WAN SE Edition VPX は仮想マシンであるため、必要な場所にハードウェアを選択したり、サーバ、VPN ユニット、その他のアプライアンス（サーバ、VPN ユニット、その他のアプライアンス）と組み合わせて、ニーズにぴったりに合ったユニットを作成できます。

SD-WAN スタンダードエディション VPX ソフトウェアは次のバージョンで提供されています。

- XenServer 6.5 SP1 で実行されている Xen 仮想マシンです。
- ESX/ESXi 5.5、6.0、および 6.5 で実行される VMware vSphere 仮想マシン。

新しくインストールされた SD-WAN SE VPX 仮想マシンが起動して実行されている場合は、物理 SD-WAN SE アプライアンスの構成と同様に、同じ構成画面を使用して構成します。

WANOP VPX と物理 SD-WAN WANOP アプライアンスの違い

SD-WAN WANOP VPX 仮想アプライアンスは、SD-WAN リピータ 8500 シリーズ・アプライアンスと似ています。これには、

SD-WAN プラグインのサポートと最大 45 Mbps のリンクが含まれます。主な違いは次のとおりです。

- Amazon EC2 インスタンスを除き、リモートライセンスサーバーを介したライセンスは、小売ライセンスでは必須です。ローカルライセンスは、評価ライセンスや VPX Express ライセンスなど、小売以外のライセンスで利用できます。Amazon EC2 インスタンスの場合は、Citrix ライセンスを使用するか、必要な帯域幅制限（2、10、20 Mbps、45 Mbps）の組み込みライセンスを使用する製品を選択できます。
- SD-WAN VPX は、リモートライセンスサーバーから SD-WAN プラグインライセンスを取得します（Amazon Web Services 用の SD-WAN VPX は例外で、プラグインをサポートしていません）。複数の仮想アプライアンスに接続するプラグインは、すべての仮想アプライアンスが同じライセンスサーバーを使用している限り、アプライアンスごとに 1 つのライセンスではなく、1 つのプラグインライセンスのみを使用します。
- SD-WAN LCD フロントパネルディスプレイはサポートされていません。
- **RS-232** シリアルコマンドインターフェイスはサポートされていません。
- 複数のアクセラレーションブリッジはサポートされていません。
- イーサネットバイパスカードはサポートされていません。
- グループモードはサポートされていません。
- SD-WAN 高可用性モードはサポートされていません。（XenServer の高可用性と vSphere の高可用性がサポートされています）。
- 1 つのポートのみをサポートする Amazon Web Services インスタンスを除き、3 つのポート（APA.1、APA.2、プライマリ）がサポートされています。

SD-WAN VPX-SE のインストールと配置の手順については、次を参照してください。

- VMware ESXi への VPX-SE のインストール：「[ESXi での SD-WAN VPX-SE のインストールとデプロイ](#)」を参照してください。
- XenServer への SD-WAN VPX-SE のインストール — SD-WAN 仮想 WAN（スタンダードエディション）VPX（SD-WAN VPX-SE）と SD-WAN WAN 最適化アプライアンス（WANOP VPX）をインストールする手順は似ています。ただし、[SD-WAN VPX-VW と WAN OP VPX インストールの違い](#)で説明されているように、いくつかの重要な違いがあります。

前提条件

April 15, 2021

このセクションでは、Citrix SD-WAN 仮想アプライアンス (SD-WAN VPX-SE) のハードウェア要件とソフトウェアの要件の概要を説明し、プラットフォームの依存関係を定義します。

メモ

- 10.2.6 および 11.0.3 リリース以降では、SD-WAN アプライアンスのプロビジョニング時または新しい SD-WAN SE VPX の導入時に、デフォルトの管理者ユーザーアカウントパスワードを変更することが必須です。この変更は、CLI と UI の両方を使用して適用されます。
- システムメンテナンスアカウント (CBVWSSH) は、開発およびデバッグ用に存在し、外部ログイン権限はありません。このアカウントには、通常の管理ユーザーの CLI セッションからのみアクセスできます。

10.2.6 リリースでは、デフォルトのパスワードは SD-WAN アプライアンスのシリアル番号であり、初回ログイン時に変更する必要があります。LOM アクセスも無効になります。

ハードウェア要件

ホスティングプラットフォームの SD-WAN VPX-SE ハードウェア要件は次のとおりです。

- 仮想 CPU: 4 コア、2.7 GHz (または同等) プロセッサ以上。
- メモリ: 4 GB RAM
- 管理インターフェイス: 1 (デフォルト)

ディスクスペースの要件

仮想パス数	MCN/RCN	プランチ
128 未満	120 GB	40 GB (デフォルト)
128 以上です	240 ギガバイト	120 GB

ソフトウェア要件

ここでは、SD-WAN VPX-SE のソフトウェア要件と、SD-WAN VPX-SE ソフトウェアの取得およびダウンロードに関する基本情報について説明します。

オペレーティングシステムの要件

SD-WAN VPX-SE 仮想アプライアンスは、次のサーバプラットフォームをサポートします。

- XenServer ハイパーバイザー 6.5 SP1
- VMware ハイパーバイザー ESXi サーバ (バージョン 5.5.0 以降)
- Microsoft Azure
- AWS
- Linux-KVM

ブラウザの要件

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。

SD-WAN VPX-SE 管理 Web インターフェイスは、次のブラウザをサポートしています。

- Google Chrome 49.0.2623112 m+
- Mozilla Firefox 43.0.4+
- Microsoft Internet Explorer 11.0.9600.18163+

インストールファイルのダウンロード

インストールを開始する前に、SD-WAN VPX-SE をホストする ESXi サーバへの接続に使用するローカル PC に SD-WAN VPX-SE OVF テンプレート (.ova ファイル) をダウンロードまたはコピーする必要があります。

注

SD-WAN VPX-VW では、リモートライセンスがサポートされます。SD-WAN ソフトウェアのライセンス取得とダウンロードの詳細については、[ライセンス](#)および[SD-WAN ソフトウェアパッケージの取得](#)を参照してください。

SD-WAN VPX-SE インストールファイルをダウンロードするには、次の URL にアクセスしてください。

<http://www.citrix.com/downloads.html>

ソフトウェアのダウンロード手順は、このサイトに記載されています。

次のように、適切なファイルをダウンロードします。

- XenServer に SD-WAN VPX-SE をインストールするには、cb-vw-vpx-<version> .xva
- VMware ESXi サーバに SD-WAN VPX-SE をインストールするには、cb-vw-vpx-<version> _vmware.ova というファイルをダウンロードします。<version> は現在の SD-WAN SE バージョン番号です。

次のセクションでは、SD-WAN VPX-SE 仮想アプライアンスのインストールおよび設定手順の概要を示します。

インターフェイス仕様

SD-WAN VPX-SE インターフェイスの仕様は次のとおりです。

- SD-WAN VPX-SE は、最大 5 つのインターフェイスをサポートします。
- 最初のインターフェイスは、仮想アプライアンスの管理 IP アドレスとして使用するために予約されています。

- SD-WAN VPX-SE 仮想アプライアンスの新しい仮想マシンをパワーアップする前に、LAN および WAN に複数のインターフェイス（それぞれ 1 つ）を設定して割り当てる必要があります。
- SD-WAN VPX-SE の場合、デフォルトでは、データインターフェイス（eth1 および eth2 など）のブリッジは作成されません。

サポートされているトポロジ展開

ハードウェア SD-WAN アプライアンスでサポートされている展開は、SD-WAN VPX-SE でもサポートされます。SD-WAN VPX-SE は、1 アームおよびインライン展開の両方をサポートします。WCCP はサポートされていません。

チェックリスト

April 15, 2021

次の情報を収集します。

- SD-WAN VPX-SE 仮想マシン (VM) をホストする ESXi サーバの IP アドレスをメモします。
- SD-WAN VPX-SE 仮想マシンに割り当てる一意の名前を選択します。
- SD-WAN VPX-SE 仮想マシンに割り当てるメモリの量を決定します。
- 仮想マシンの仮想ディスクに割り当てるディスク容量を決定します（デフォルトのディスク容量要件は 39.1 GB）。
- DHCP を使用していない場合は、SD-WAN VPX-SE の静的な管理 IP アドレスとして割り当てる IP アドレスを書き留めます。（デフォルトでは、SD-WAN VPX-SE は DHCP を使用します）。
- SD-WAN VPX-SE が外部ネットワークとの通信に使用するゲートウェイ IP アドレスを決定します。
 - SD-WAN VPX-SE が存在するネットワークのサブネットマスクをメモします。

Citrix SD-WAN VPX-SE と VPX-WANOP

April 15, 2021

このセクションでは、SD-WAN ネットワークに配置するための SD-WAN VPX (VPX-SE) のインストールと、WAN 最適化用の SD-WAN VPX との基本的な違いについて説明します。

SD-WAN VPX-SE 仮想アプライアンスと SD-WAN WANOP VPX をインストールおよび構成する場合の主な違いは、次のとおりです。

- Citrix SD-WAN ダウンロードサイト (<http://www.citrix.com/downloads.html>) から次のインストールファイルをダウンロードします。

注

リモートライセンスは SD-WAN VPX-SE でサポートされます。

- XenServer に SD-WAN VPX-SE をインストールするには、次のファイルをダウンロードします。`*cb-vw-vpx-<version>.xva*`
- VMware ESXi サーバに SD-WAN VPX-SE をインストールするには、次のファイルをダウンロードします。`*cb-vw-vpx-<version>_vmware.ova*`

<version> 現在の SD-WAN ** バージョン番号はどこにありますかです。

注

SD-WAN ソフトウェアのライセンス取得とダウンロードの詳細については、[ライセンス](#)および[SD-WAN ソフトウェアパッケージの取得](#)を参照してください。

- SD-WAN VPX-SE 仮想アプライアンスは、次のサーバプラットフォームをサポートします。
 - XenServer ハイパーバイザー 6.5 SP1
 - VMware ハイパーバイザー ESXi サーバ (バージョン 5.5.0 以降)
- SD-WAN VPX-SE は、インライン展開と PBR 配置の両方をサポートしますが、VPX-SE では WCCP 配置はサポートされません。
- SD-WAN VPX-SE 仮想アプライアンスの仮想マシンは、XenServer または VMware ESXi Server プラットフォームのいずれかに手動でインストールする必要があります。現在、この手順にはインストールウィザードはありません。
- 仮想マシンの最小構成要件は次のとおりです。
 - 仮想 **CPU: 4**
 - メモリ: 4 GB RAM
 - 仮想データストア: 40 GB ディスク
 - 管理インターフェイス: 1 (デフォルト)
- SD-WAN VPX-SE インターフェイスの仕様は次のとおりです。
 - SD-WAN VPX-SE は、最大 5 つのインターフェイスをサポートします。
 - 最初のインターフェイスは、仮想アプライアンスの管理 IP アドレスとして使用するために予約されています。
 - SD-WAN VPX-SE 仮想アプライアンスの新しい仮想マシンをパワーアップする前に、LAN および WAN に追加インターフェイス (それぞれ 1 つ) を設定して割り当てる必要があります。
 - VPX-SE の場合、デフォルトでは、データインターフェイス (eth1 および eth2 など) のブリッジは作成されません。
- DHCP を使用していない場合は、SD-WAN VPX-SE 仮想アプライアンスの静的な管理 IP アドレスを設定する必要があります。

注

DHCP は、SD-WAN VPX-SE 管理 IP アドレスに対してデフォルトで有効になっています。

SD-WAN VPX-SE 仮想アプライアンスの静的管理 IP アドレスを設定するには、次の手順を実行します。

1. SD-WAN VPX-SE 仮想マシン (VM) を作成した vSphere クライアントまたは XenServer クライアントを開きます。
2. 新しい SD-WAN VPX-SE 用の vSphere または XenServer コンソールを開き、仮想マシンの管理者アカウントにログインします。
 - デフォルトの管理者ユーザー名: **admin**
 - デフォルトの管理者パスワード: パスワード
3. コンソール CLI プロンプトで、次のコマンドラインを入力します。

```
pre codeblock management_ip set_management_ip set interface <ip> <subnetmask> <gateway> <!--NeedCopy-->
```

ここで

- <ip> は SD-WAN VPX-SE 仮想アプライアンスの管理 IP アドレスです。*
- <subnetmask>* は、SD-WAN VPX-SE 仮想アプライアンスが存在するネットワークを定義するために使用されるサブネットマスクです。
- * は、VPX-SE 仮想アプライアンスが外部ネットワークとの通信に使用する SD-WAN のゲートウェイ IP アドレスです。

4. SD-WAN VPX-SE 仮想アプライアンス仮想マシンを再起動します。

注

「[アプライアンスの管理 IP アドレスの設定](#)」の項も参照してください。

VPX のインストールと展開の概要

April 15, 2021

この項では、

SD-WAN VPX-SE 仮想アプライアンスのインストールと展開に関する手順の概要について説明します。

SD-WAN VPX-SE は、次のプラットフォームにインストールできます。

- **VMware ESXi** : 手順については、[ESX での SD-WAN VPX-SE のインストールとデプロイ](#)を参照してください。
- **XenServer** : SD-WAN VPX (VPX-SE) と SD-WAN (WAN 最適化) VPX のインストール手順は非常に似ています。XenServer に SD-WAN WANOP VPX をインストールする手順については、Citrix ドキュメントポータル (<http://docs.citrix.com/>) の [Citrix CloudBridge 7.4 製品ドキュメント](#) というドキュメントの「[CloudBridge VPX](#)」を参照してください。「[SD-WAN VPX-SE インストールと WANOP VPX インストールの違い](#)」も参照してください。

ESXi で SD-WAN VPX-VW を展開する手順の概要

次のリストは、VMware ESXi サーバに SD-WAN VPX-SE を展開する手順と手順をまとめたものです。

1. SD-WAN VPX-SE のインストールおよび構成情報を収集します。手順については、[SD-WAN VPX-SE のインストールと構成のチェックリスト](#)を参照してください。
2. VMware vSphere クライアントをインストールします。手順については、「[VMware vSphere クライアントのインストール](#)」を参照してください。
3. SD-WAN VPX-SE OVF テンプレートをインストールしてデプロイします。手順については、「[SD-WAN VPX-SE OVF テンプレートのインストールとデプロイ](#)」を参照してください。
4. SD-WAN VPX-SE 管理 IP アドレスを設定します。手順については、[SD-WAN VPX-SE の管理 IP アドレスの設定](#)を参照してください。
5. SD-WAN VPX-SE に接続し、展開をテストします。手順については、「[SD-WAN VPX-SE への接続と展開のテスト](#)」を参照してください。

VPX-SE/VPXL-SE プラットフォームごとの仮想イーサネットポート

April 15, 2021

SD-WAN 9.3 リリースでは、VPX-SE/VPXL-SE プラットフォームは 4 つの仮想イーサネットインターフェイスだけをサポートします。これにより、複数の VLAN が同じインターフェイスにマッピングされている場合（デバッグ可能）、展開の問題が発生します。SD-WAN 10.0 では、サーバー間の VPX-SE 高可用性展開用のポートの追加サポートが追加されました。このサポートにより、お客様は、高可用性インターフェイスを実ポートに 1 対 1 でマッピングし、仮想アプライアンスを分離し、両方の仮想アプライアンスがアクティブになるハイパーバイザの設定ミスを回避できます。すべてのハイパーバイザが、最大構成をサポートするために必要な 9 つの仮想ポートをサポートしているわけではありません。SD-WAN アプライアンスに構成されているポートの数が、利用可能よりも多い場合、SD-WAN は、ハイパーバイザーポートよりも多くの SD-WAN ポートを持つ現在の構成をサポートします。

ESXi の VPX Standard Edition

April 15, 2021

この章では、SD-WAN VPX-SE のインストール、設定、および配置の手順について説明します。これには、SD-WAN VPX-SE 仮想マシンの作成および展開に使用する VMware vSphere Client のインストールに関する基本的な手順が含まれます。

注

VMware vSphere クライアントの操作の詳細は、vSphere ソフトウェアの新しいリリースで変更される場合があります。vSphere Client のインストールと操作に関する最も完全かつ最新の手順については、VMware

のマニュアルを参照してください。この章の手順では、ESXi プラットフォームに SD-WAN VPX-SE 仮想マシンをインストールする場合のみ、最も基本的で基本的なガイドラインを提供することを目的としています。

次に、SD-WAN VPX-SE をインストールおよび展開する最上位の手順をまとめます。これらの手順は、リストされた順序で実行してください。

1. VMware vSphere クライアントをインストールします。
2. SD-WAN VPX-SE OVF テンプレートをインストールしてデプロイします。
3. SD-WAN VPX-SE 管理 IP アドレスを設定します。
4. 展開を接続してテストします。

クライアントをインストールする

April 15, 2021

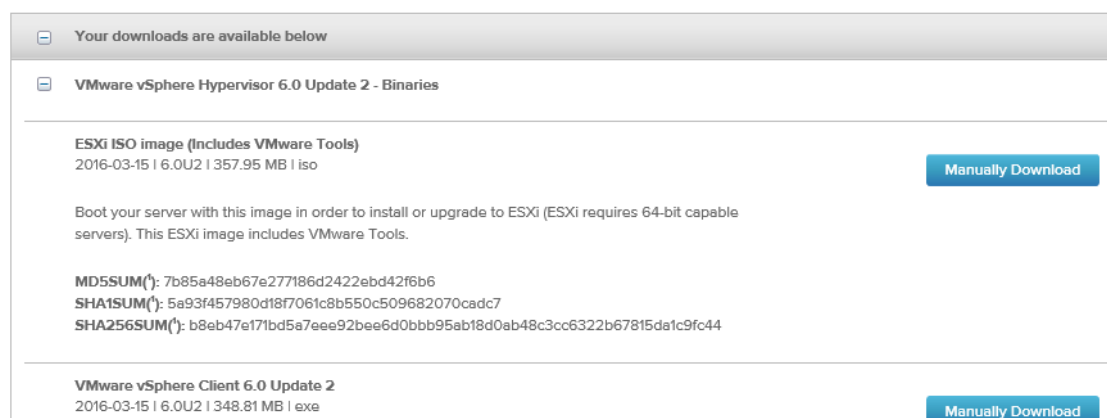
このセクションでは、SD-WAN VPX-SE 仮想マシンの作成および展開に使用する VMware vSphere クライアントをダウンロードしてインストールするための基本的な手順について説明します。

注

詳細については、VMware vSphere クライアントのマニュアルを参照してください。SD-WAN は、vshPere クライアントバージョン 5.5 以降で展開できます。

1. ブラウザーを開き、次の場所で vSphere Client および VPX-SE Virtual Machine (VM) インスタンスをホストする ESXi サーバーに移動します: <https://my.vmware.com/group/vmware/evalcenter?p=free-esxi6> **VMware ESXi** のダウンロードページは次を表示します。

Download Packages



The screenshot shows a web interface for downloading VMware packages. It features a header "Your downloads are available below" and a main section titled "VMware vSphere Hypervisor 6.0 Update 2 - Binaries". Under this section, there are two items:

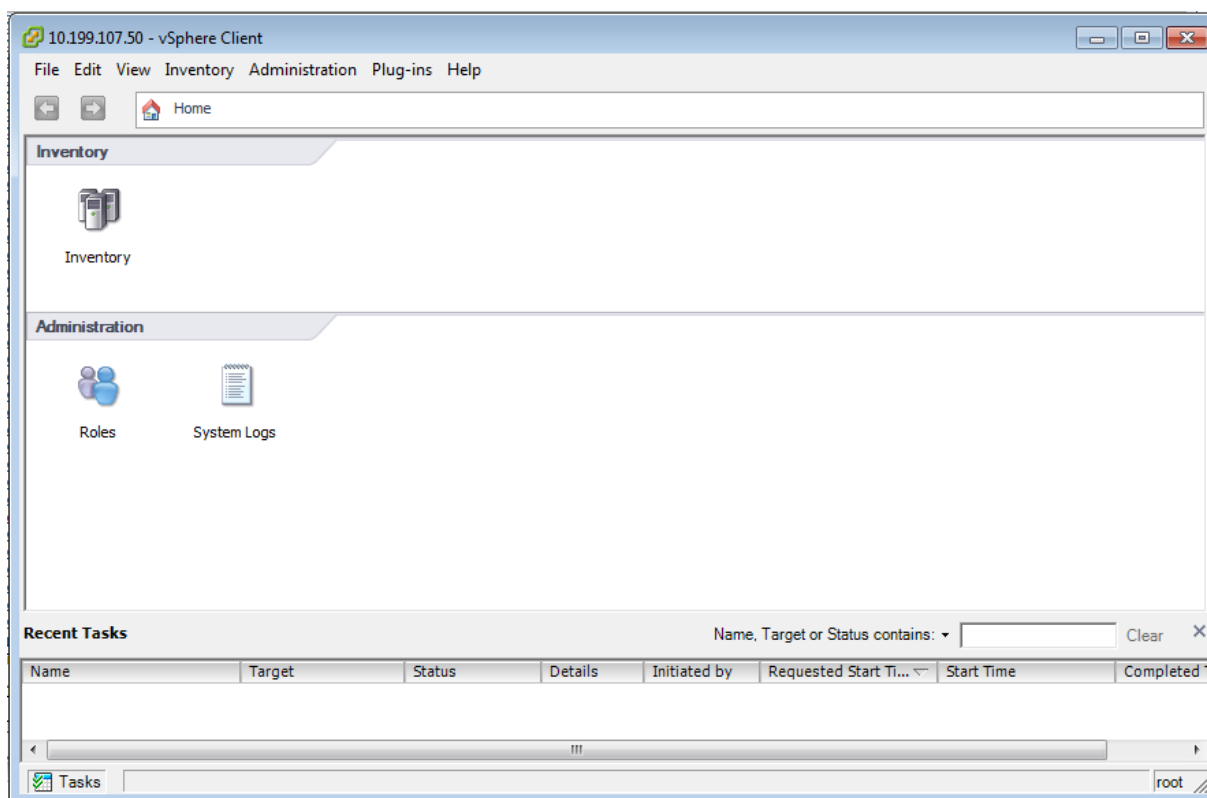
- ESXi ISO image (Includes VMware Tools)**: 2016-03-15 | 6.0U2 | 357.95 MB | iso. A "Manually Download" button is visible to the right. Below the title, there is a note: "Boot your server with this image in order to install or upgrade to ESXi (ESXi requires 64-bit capable servers). This ESXi image includes VMware Tools." Below this note are three lines of hashes: MD5SUM(*): 7b85a48eb67e277186d2422ebd42f6b6, SHA1SUM(*): 5a93f457980d18f7061c8b550c509682070cad7, and SHA256SUM(*): b8eb47e171bd5a7eee92bee6d0bb95ab18d0ab48c3cc6322b67815da1c9fc44.
- VMware vSphere Client 6.0 Update 2**: 2016-03-15 | 6.0U2 | 348.81 MB | exe. A "Manually Download" button is visible to the right.

2. **vSphere Client** のインストールファイルをダウンロードするには、[vSphere クライアントのダウンロード] リンクをクリックします。
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** クライアントのログインページが表示され、ESXi サーバのログイン資格情報の入力を求められます。



5. **ESXi** サーバのログイン資格情報を入力します。以下のコマンドを実行します。
- **IP アドレス/名前:** SD-WAN VPX-SE VM インスタンスをホストする ESXi サーバの **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:** サーバ管理者アカウント名を入力します。デフォルトは [root] です。
 - **パスワード:** この管理者アカウントに関連付けられているパスワードを入力します。
6. [ログイン] をクリックします。**vSphere** クライアントのメインページが表示されます。



次の段階は、SD-WAN VPX-SE OVF テンプレートをインストールしてデプロイし、仮想マシンをセットアップすることです。ここでは、これらの手順について説明します。

SD-WAN VPX を展開する

April 15, 2021

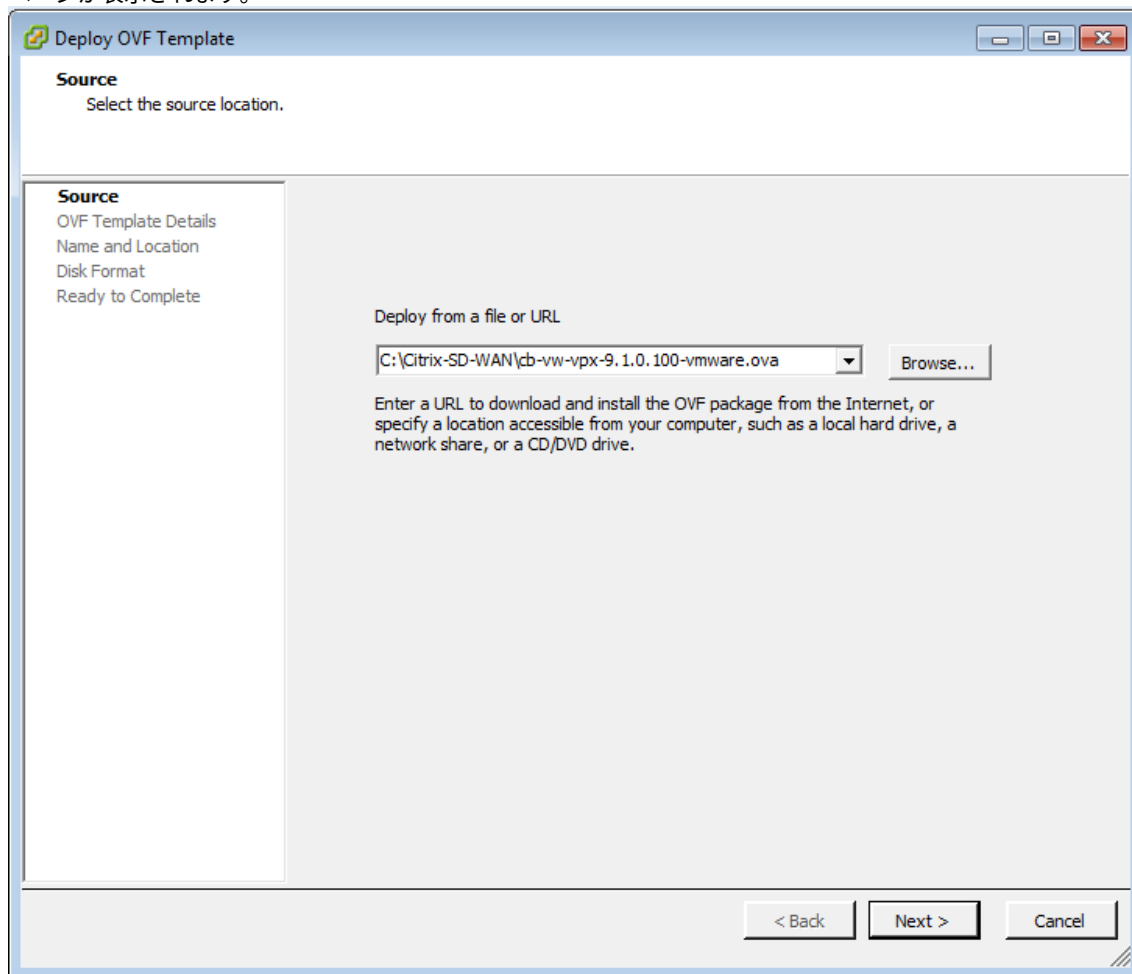
このセクションでは、SD-WAN VPX OVF テンプレートのインストールと SD-WAN VPX 仮想マシンの作成手順について説明します。

1. SD-WAN VPX OVF テンプレートファイル (.ova ファイル) をローカル PC にダウンロードしていない場合は、ダウンロードします。SD-WAN VPX OVF テンプレートをダウンロードするか、SD-WAN VPX をホストする ESXi サーバへの接続に使用するローカル PC にコピーします。OVF テンプレートファイルのファイル名には、`cb-vw-vpx-vx-vx-vvx-version_number-vmware.ova` という命名規則が使用されます。
 - バージョン番号は、SD-WAN VPX リリースのバージョン番号です。
 - .ova は、これが OVF テンプレートファイルであることを示すファイル名のサフィックスです。

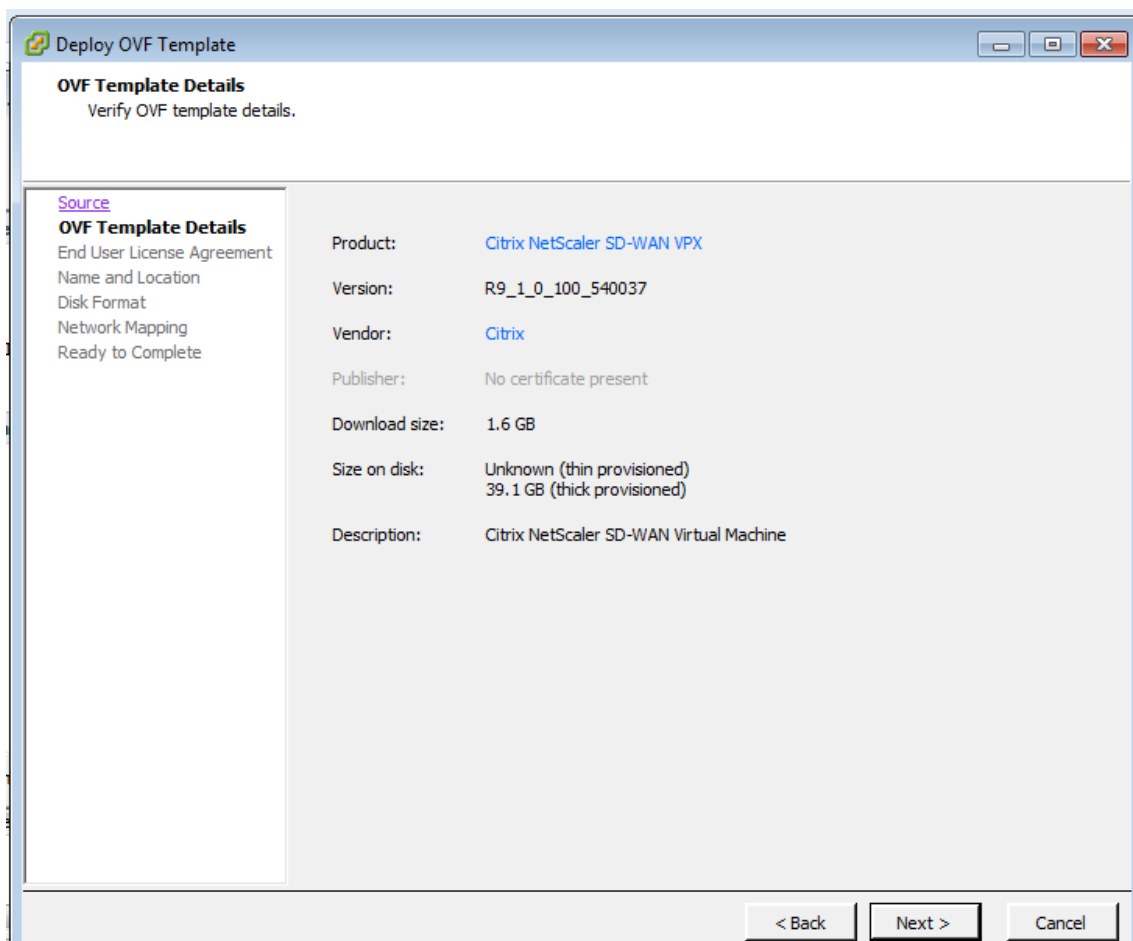
注

詳しくは、以下を参照してください：[ソフトウェアパッケージのダウンロード](#)。

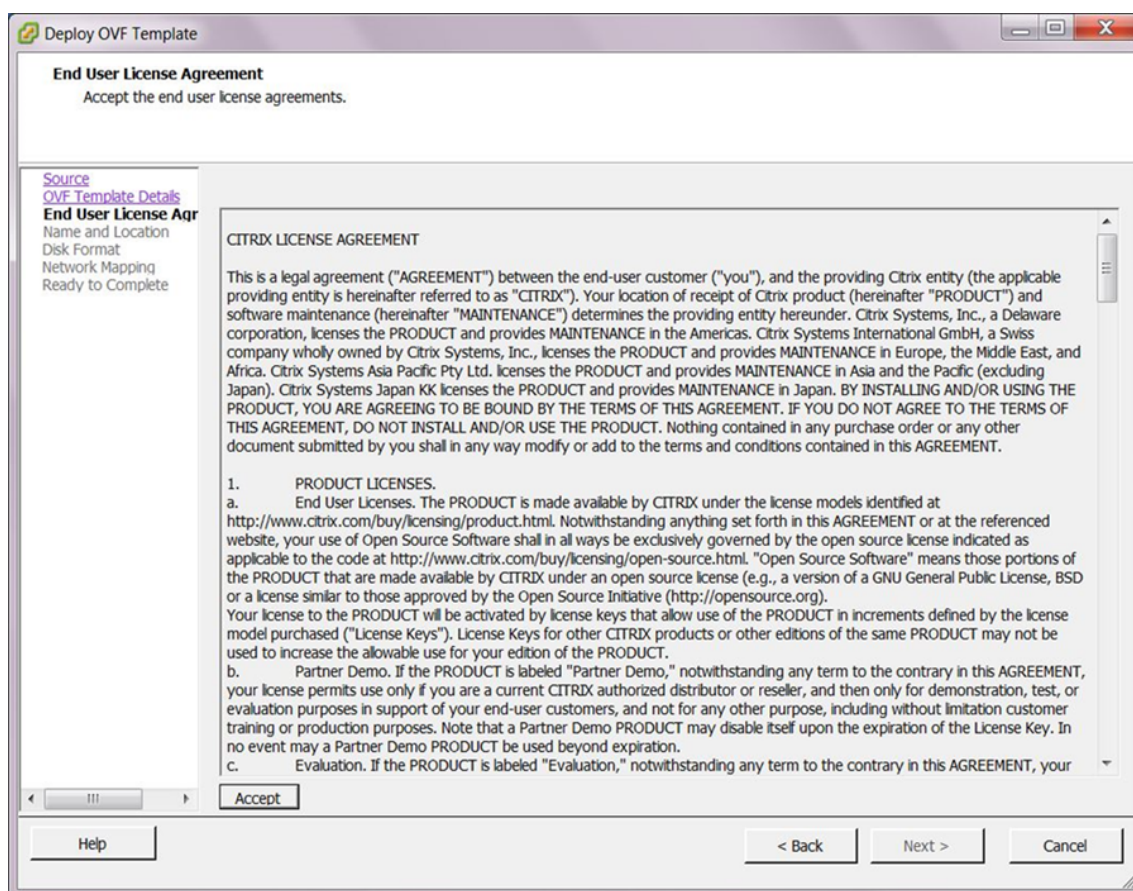
2. vSphere Client で続行し、[ファイル] をクリックし、[**OVF** テンプレートの展開...] を選択します。をドロップダウンメニューから選択します。[**OVF** テンプレートのデプロイ] ウィザードの最初のページ、[ソース] ページが表示されます。



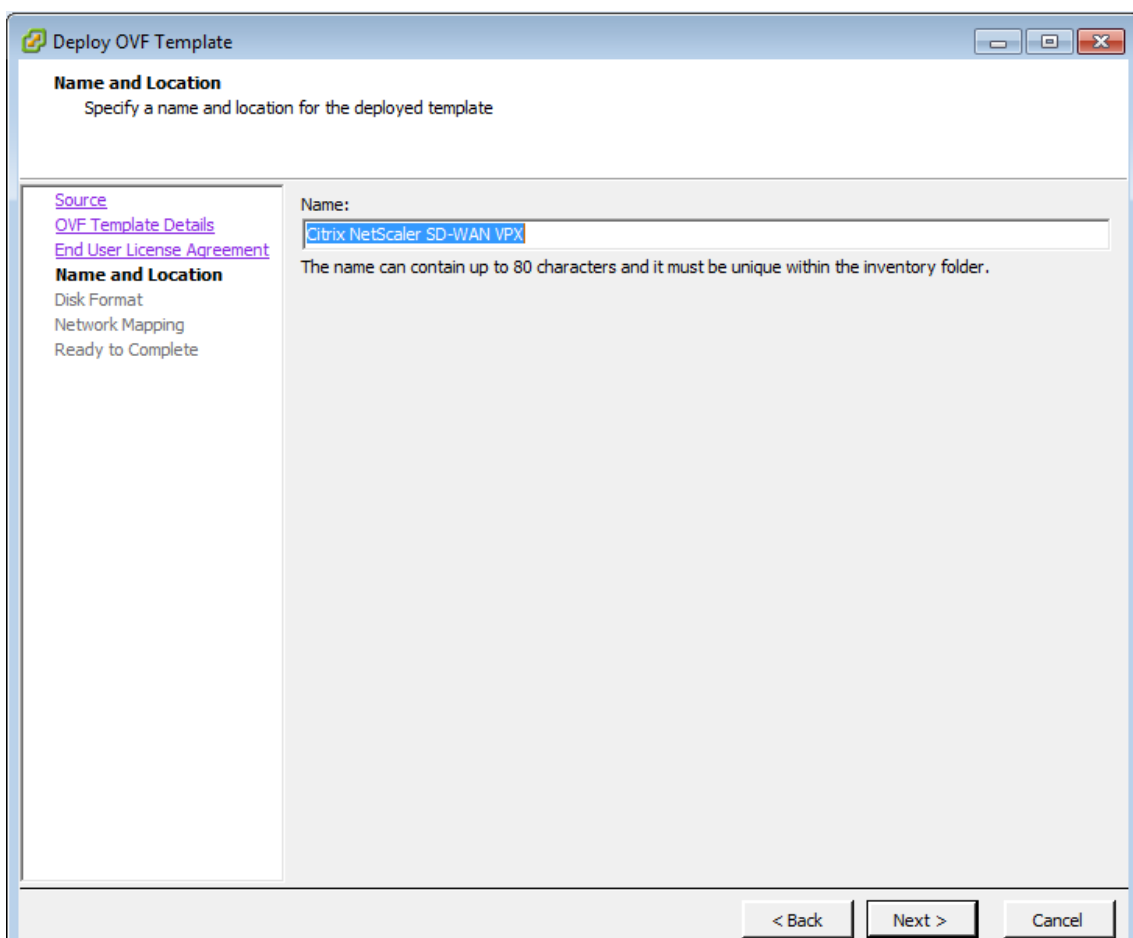
3. インストールする CB VPX-VW OVF テンプレート (.ova ファイル) を選択します。以前にローカル PC にダウンロードした .ova ファイルの場所を参照し、選択します。
4. [次へ] をクリックします。これにより、選択した .ova ファイルがインポートされ、[**OVF** テンプレートの詳細] ページが表示されます。



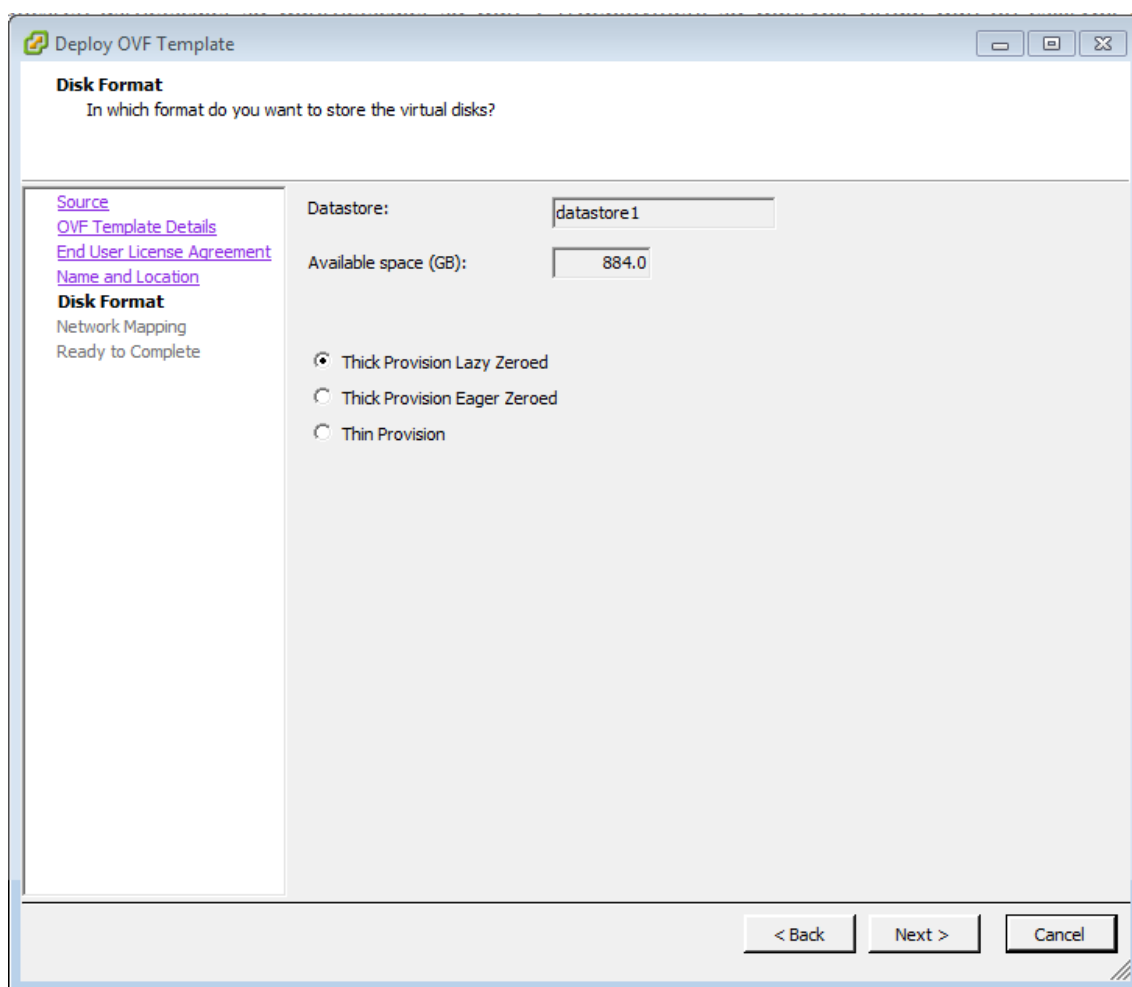
5. このページには、インポートした OVF テンプレートに関する基本情報が表示されます。
6. [次へ] をクリックします。これは、エンドユーザー使用許諾契約ページに進みます。



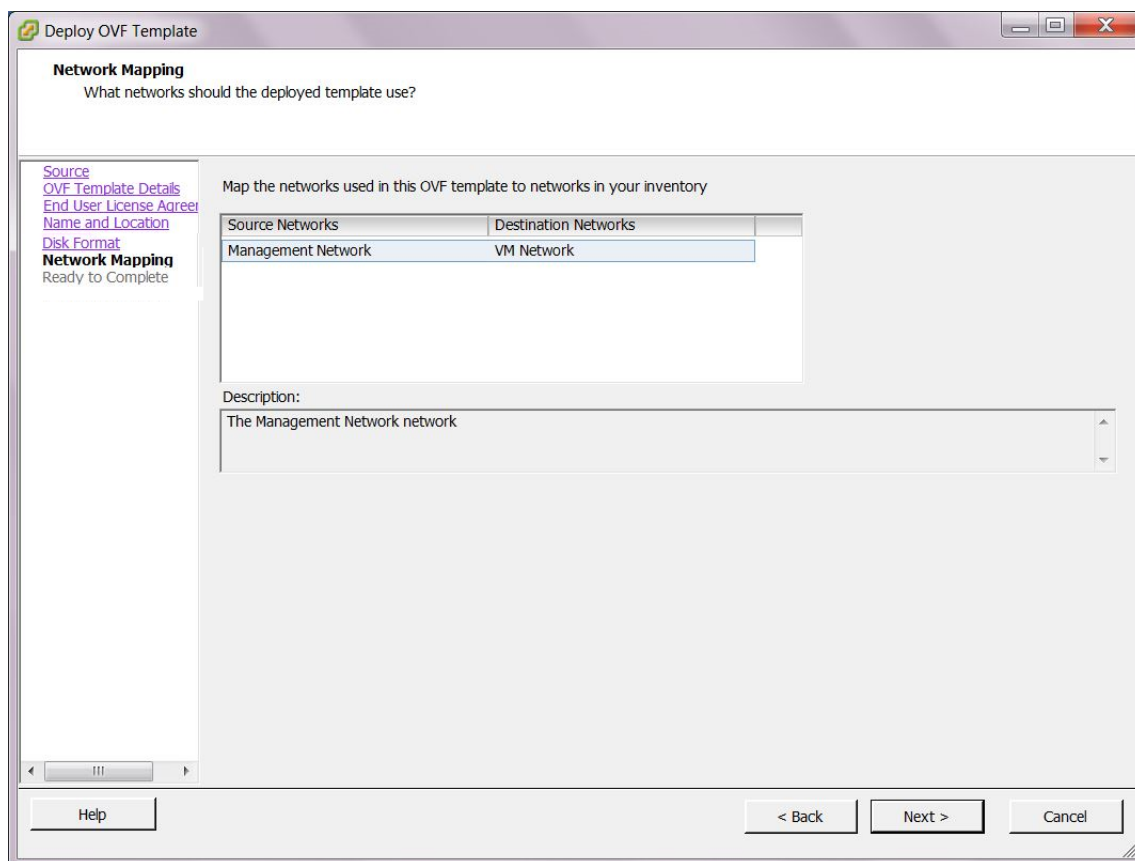
7. [同意する] をクリックし、[次へ] をクリックします。これは、[名前と場所] ページに進みます。



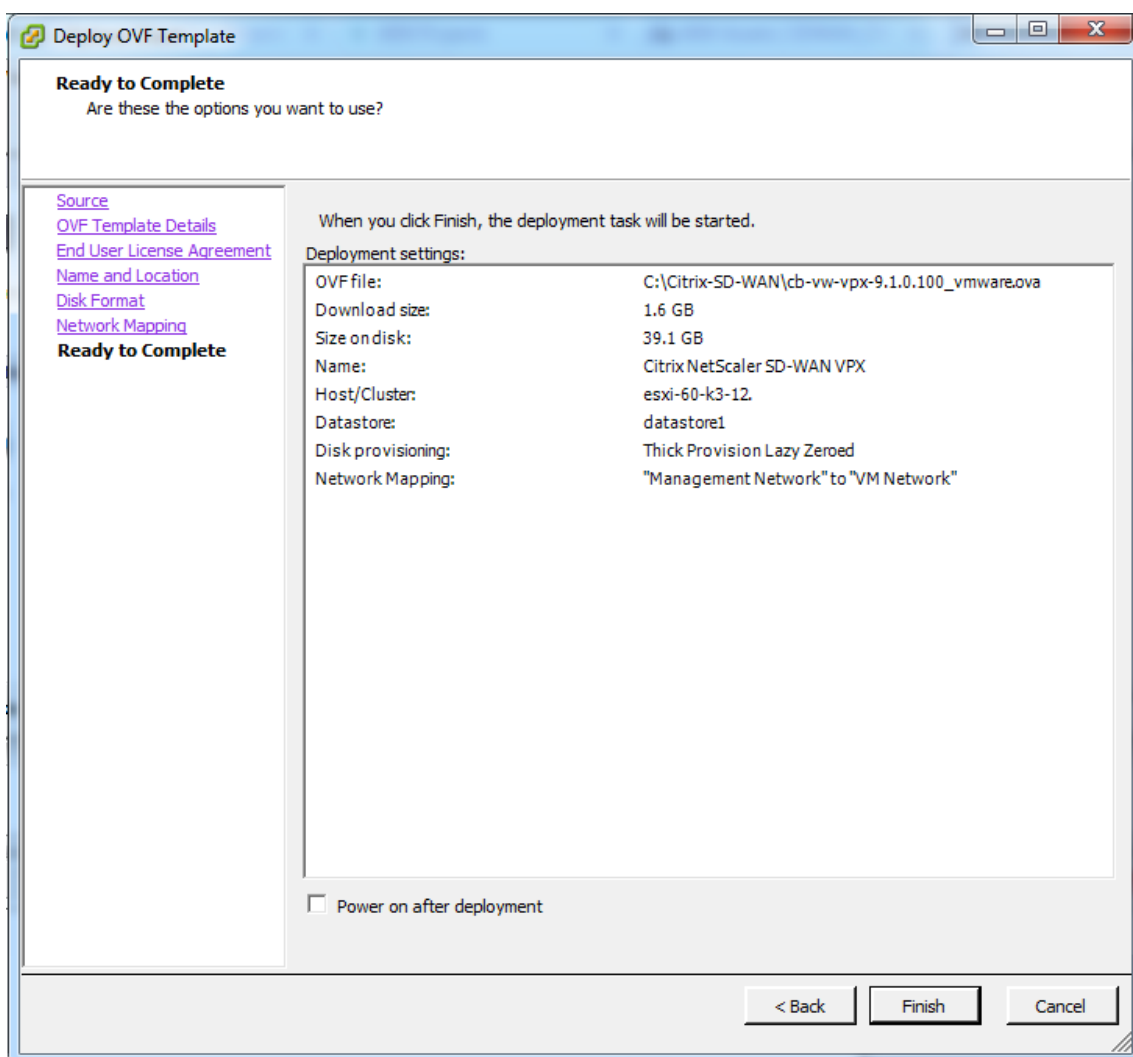
8. 新しい仮想マシンの一意の名前を入力します（またはデフォルトをそのまま使用します）。この名前は、現在の **Inventory** フォルダー内で固有でなければならず、長さは最大 80 文字です。
9. [次へ] をクリックします。[ディスクフォーマット] ページが表示されます。SD-WAN VPX-VW 仮想マシンには、39.1 GB のディスク領域が必要です。



10. デフォルトの設定をそのまま使用し、[次へ]をクリックします。[ネットワークマッピング]ページに進みます。



11. デフォルト (**VM** ネットワーク) をそのまま使用し、[次へ] をクリックします。[完了の準備完了] ページに進みます。

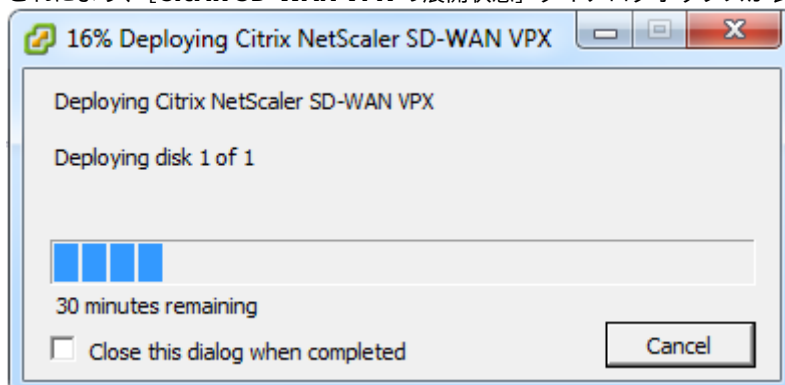


12. [完了] をクリックして仮想マシンを作成します。

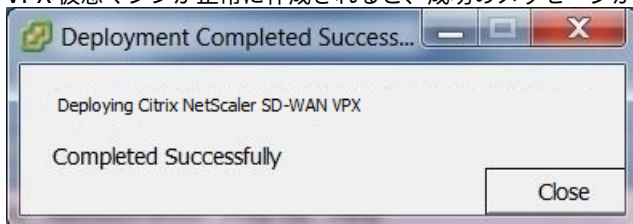
注

サーバへのディスクイメージの解凍には、数分かかる場合があります。

これにより、**[Citrix SD-WAN VPX の展開状態]** ダイアログボックスが表示されます。



サーバー上に存在する条件によっては、展開が完了するまで数分から数時間かかる場合があります。SD-WAN VPX 仮想マシンが正常に作成されると、成功のメッセージが表示されます。



13. [閉じる] をクリックします。これにより、**OVF** テンプレートのデプロイウィザードが閉じ、vSphere Client のメインウィンドウに戻ります。この vSphere Client を使用して最初に作成した仮想マシンである場合は、vSphere Client ホームページが表示されます。以前に 1 つ以上の仮想マシンを作成した場合は、[インベントリ] ページが表示されます。

次の段階は、SD-WAN VPX 管理 IP アドレスを構成することです。ここでは、この手順の手順について説明します。

管理 IP の構成

April 15, 2021

SD-WAN VPX 仮想マシンに管理 IP アドレスを割り当てるには、次の 2 つの方法があります。

- 自動: デフォルトでは、すべての SD-WAN VPX 仮想アプライアンスは、動的ホスト制御プロトコル (DHCP) を使用して管理 IP アドレスを自動的に取得します。DHCP を使用するには、DHCP サーバが SD-WAN に存在し、利用可能である必要があります。IPv6 アドレスを自動的に取得するために、アプライアンスは DHCP またはステートレスアドレス自動構成 (SLAAC) を使用できます。取得した管理 IP アドレスを特定する方法については、を参照してください [VPX に割り当てられた DHCP の管理 IP アドレスの表示](#)。
- 手動: DHCP または SLAAC を使用していない場合は、SD-WAN VPX 仮想アプライアンスの静的管理 IP アドレスを手動で割り当てる必要があります。手順については、「[VPX の静的管理 IP アドレスの手動構成](#)」を参照してください。

VPX の静的管理 IP アドレスの手動構成

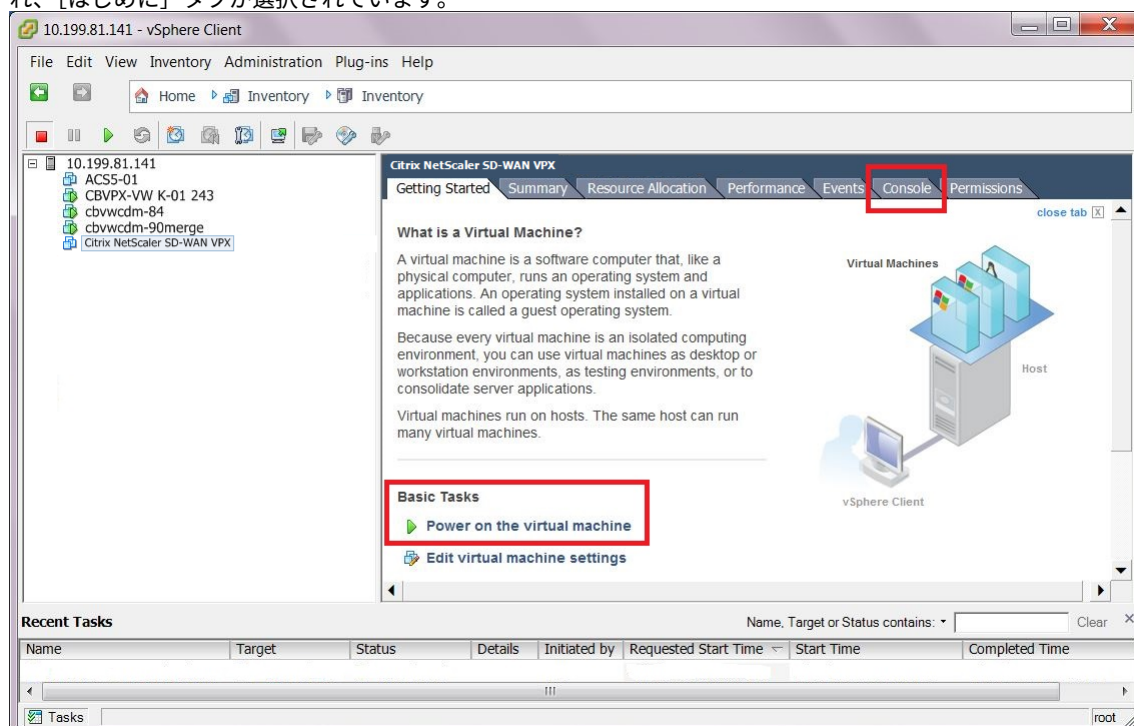
DHCP または SLAAC を使用していない場合は、SD-WAN VPX 仮想アプライアンス仮想マシンの静的管理 IP アドレスを手動で構成する必要があります。構成するには、vSphere Client で作成した仮想マシンのコンソールを使用します。

注

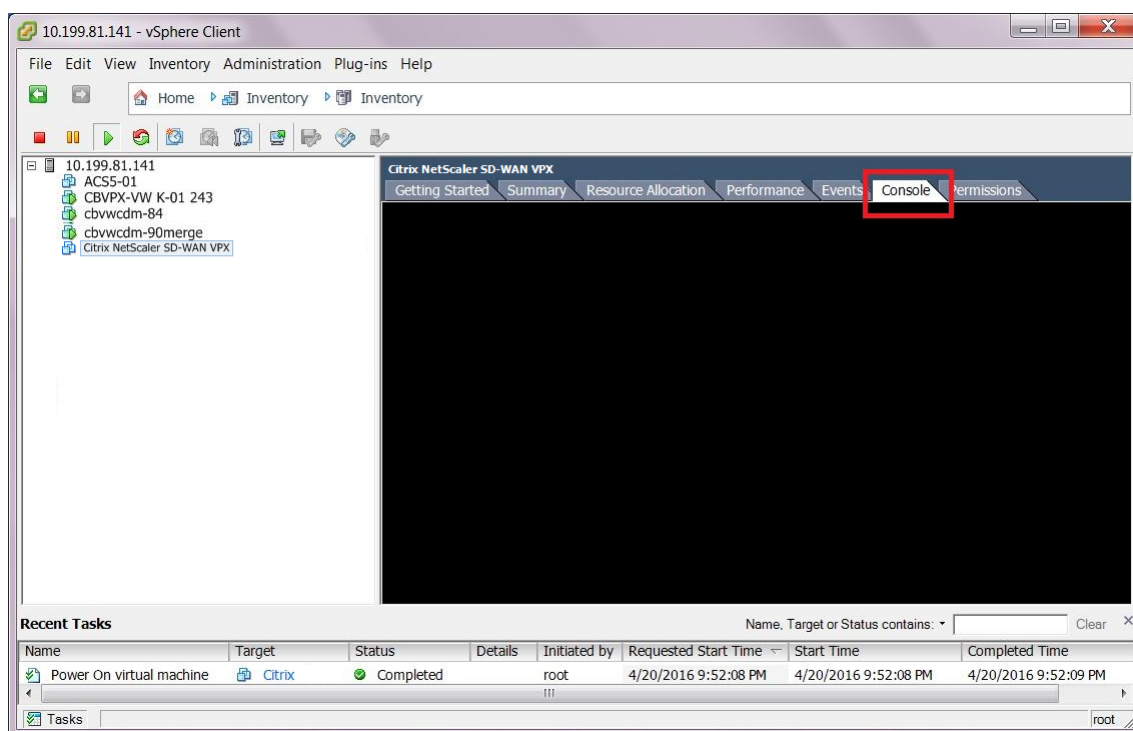
DHCP は、SD-WAN VPX 管理 IP アドレスに対してデフォルトで有効になっています。

1. vSphere クライアントの [インベントリ] ページで、[インベントリ] ツリー (左ウィンドウ) で新しい SD-WAN VPX 仮想マシンを選択します。これにより、新しい仮想マシンの [インベントリ] ページが表示さ

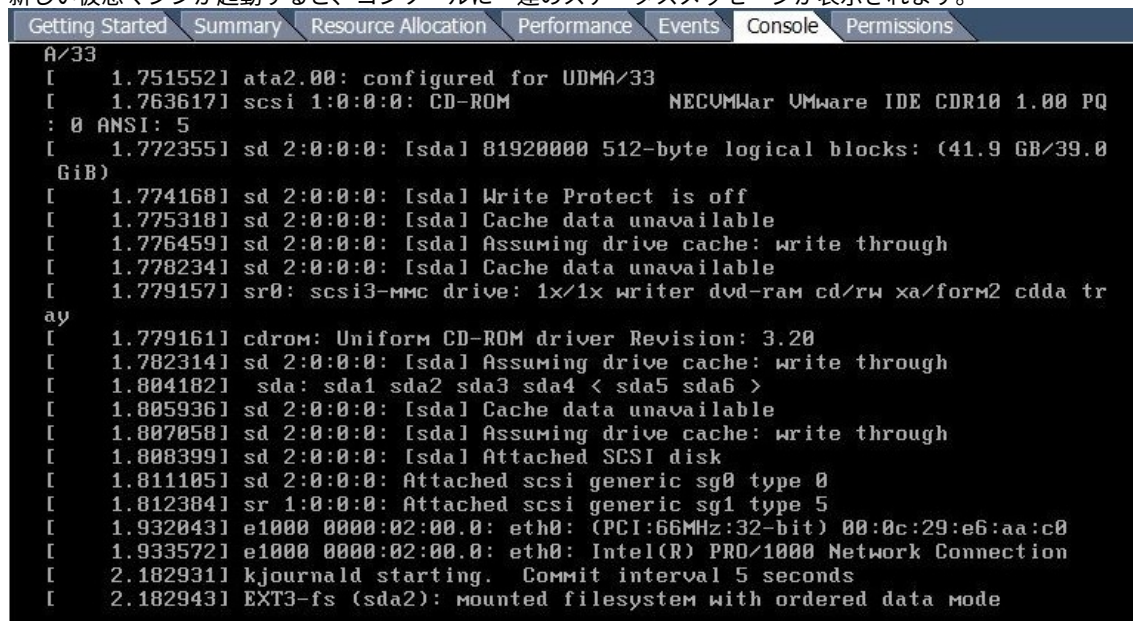
れ、[はじめに] タブが選択されています。

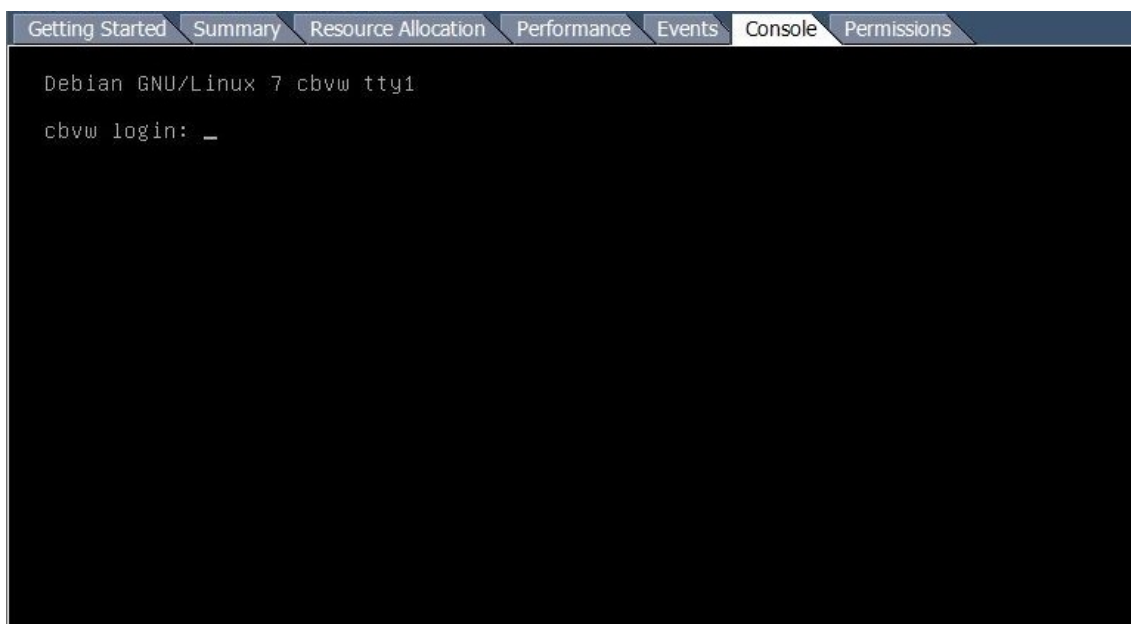


2. 新しい仮想マシンをパワーオンします。[はじめに] タブページの [基本タスク] セクションで、仮想マシンをパワーオン (緑色の再生ボタン) をクリックして、新しい SD-WAN VPX-SE 仮想マシンをパワーオンします。
3. 「インベントリ」 ページのタブバーで「コンソール」タブを選択します。[コンソール] タブは、メインページ領域の上部にある [インベントリ] ページのタブバーにあります。このタブを選択すると、仮想マシンの CLI コンソールが表示され、アクセスできるようになります。



新しい仮想マシンが起動すると、コンソールに一連のステータスメッセージが表示されます。





起動プロセスが完了すると、コンソールログインプロンプトが表示されます。

4. コンソール領域内の任意の場所をクリックして、コンソールモードを開始します。これにより、マウスカーソルの制御が仮想マシンコンソールに切り替わり、コンソールモードが有効になります。

注

コンソールのカーソルの制御を解除するには、**Ctrl** キーと **Alt** キーを同時に押します。

5. VM コンソールにログインします。新しい SD-WAN VPX-SE 仮想マシンのデフォルトのログインクレデンシャルは次のとおりです。

- ログイン: 管理者
- パスワード: パスワード

コンソールの [ようこそ] 画面が表示されます。

```
Last login: Tue Dec  1 14:30:29 on ttys000

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
[BANLSREEJITHS:~ sridhara]$ ssh admin@10.1.1.56
[admin@10.1.1.56's password:
```

6. コンソールプロンプトで、次のコマンドラインを入力します。

- IPv4 アドレスを構成するには、次の手順を実行します。

```
management_ip
```

コンソールで *management_ip* CLI に切り替わり、*set_management_ip* プロンプトが表示されます。

Console to Citrix acquired

```
MCN_DC-MCN_DC-VPX>management_ip
]
Which would you like to do?
  "set interface <ip address> <subnet mask> <gateway>" - Stage New Settings
  s for IP Address, Subnet Mask, and Gateway IP Address
  "address" - Stage New IP Address
  "mask" - Stage New Subnet Mask
  "gateway" - Stage New Gateway IP Address
  "clear" - Clear Settings
  "disable" - disable IPv4 address on the interface
  "apply" - Apply Staged Settings
  "cancel" - Cancel Staged Settings
  "main_menu" - Return to the Main Menu
]
set_management_ip>
```

- IPv6 アドレスを構成するには、次の手順を実行します。

management_ipv6

これにより、コンソールで *management_ipv6* CLI に切り替わり、*set_management_ipv6* プロンプトが表示されます。

```
[BANLSREEJITHS:~ sri $ ssh admin@10.10.10.56
]
[admin@10.10.10.56's password:
]
Console to Citrix acquired

[MCN_DC-MCN_DC-VPX>management_ipv6
set_management_ipv6>Configuring IPv6: Enter "SLAAC" or "DHCP" or "static". Enter
"disable" to
disable. Enter "main_menu" to return to the main menu.
]
set_management_ipv6>
```

7. 仮想マシンのインターフェイス設定を構成します。*set_management_ip* プロンプトで、次のコマンドラインを入力します。

- IPv4 アドレスの場合:

set interface <ip address> <subnet mask> <gateway>

場所:

- <IP address> は、SD-WAN VPX-SE 仮想アプライアンスの管理 IP アドレスです。
- <subnetmask> CB VPX-VW 仮想アプライアンスが常駐するネットワークを定義するために使用されるサブネットマスクです。
- は、SD-WAN VPX-SE 仮想アプライアンスが外部ネットワークとの通信に使用するゲートウェイ IP アドレスです。

これは段階的になりますが、インターフェイス設定は適用されません。


```
Console to Citrix acquired
```

```
[WARNING] RADIUS server is unreachable. This may cause slowness in the CLI.
```

```
[MCN_DC-MCN_DC-VPX>management_ip
```

```
Which would you like to do?
```

```
"set interface <ip address> <subnet mask> <gateway>" - Stage New Setting
s for IP Address, Subnet Mask, and Gateway IP Address
"address" - Stage New IP Address
"mask" - Stage New Subnet Mask
"gateway" - Stage New Gateway IP Address
"clear" - Clear Settings
"disable" - disable IPv4 address on the interface
"apply" - Apply Staged Settings
"cancel" - Cancel Staged Settings
"main_menu" - Return to the Main Menu
```

```
set_management_ip>set interface 10. 255.255.255.0 10. 1
```

- IPv6 アドレスの場合:

```
set interface <IPv6 address> <prefix>
```

各項目の意味は次の通りです:

- <IPv6 address> は、SD-WAN VPX-SE 仮想アプライアンスの管理 IP アドレスです。
- は <prefix>、アドレス空間またはネットワークのブロックを表します。

次のいずれかを入力します。

- **SLAAC**: ネットワーク上の各デバイスに IPv6 アドレスを自動的に割り当てる SLAAC を有効にします。SLAAC は、IPv6 クライアントが独自のアドレスを生成できるようにします。

```
Console to Citrix acquired

[WARNING] RADIUS server is unreachable. This may cause slowness in the CLI.

MCN_DC-MCN_DC-VPX>
[WARNING] RADIUS server is unreachable. This may cause slowness in the CLI.

[MCN_DC-MCN_DC-VPX>management_ipv6
set_management_ipv6>Configuring IPv6: Enter "SLAAC" or "DHCP" or "static". Enter "disable" to
disable. Enter "main_menu" to return to the main menu.

set_management_ipv6>SLAAC

set_management_ipv6_slaac>Please enter "enable" to enable slaac. To disable, please go to management_ipv6
menu. Enter "main_menu" to return to the main menu.

set_management_ipv6_slaac>enable

Management interface settings have been enabled for V6. Applying settings to take effect.
Applied changes, duplicate address detection is in progress!! Please wait.

No conflicts detected!! The IPv6 address is applied to tn-mgt0!!

set_management_ipv6_slaac>
```

- **[DHCP]**: IP アドレスを自動的に割り当てる DHCP を有効にします。必要に応じて、ステートフルまたはステートレスを選択します。

```

Console to Citrix acquired

[WARNING] RADIUS server is unreachable. This may cause slowness in the CLI.

[MCN_DC-MCN_DC-VPX>management_ipv6
set_management_ipv6>Configuring IPv6: Enter "SLAAC" or "DHCP" or "static". Enter "disable" to
disable. Enter "main_menu" to return to the main menu.

set_management_ipv6>DHCP

set_management_ipv6_dhcp>Please enter "enable" to enable DHCPv6. To disable, please go to
management_ipv6 menu. Enter "main_menu" to return to the main menu.

set_management_ipv6_dhcp>enable
set_management_ipv6_dhcp>Which mode of DHCP do you like to enable? Please select "stateful" or
["stateless". Enter "main_menu" to return to the main menu.

set_management_ipv6_dhcp>stateful
Management interface settings have been enabled for V6. Applying settings to take effect.

set_management_ipv6_dhcp>

=====
Console to Citrix acquired

[WARNING] RADIUS server is unreachable. This may cause slowness in the CLI.

[MCN_DC-MCN_DC-VPX>management_ipv6
set_management_ipv6>Configuring IPv6: Enter "SLAAC" or "DHCP" or "static". Enter "disable" to
disable. Enter "main_menu" to return to the main menu.

set_management_ipv6>DHCP

set_management_ipv6_dhcp>Please enter "enable" to enable DHCPv6. To disable, please go to
management_ipv6 menu. Enter "main_menu" to return to the main menu.

set_management_ipv6_dhcp>enable
set_management_ipv6_dhcp>Which mode of DHCP do you like to enable? Please select "stateful" or
["stateless". Enter "main_menu" to return to the main menu.

set_management_ipv6_dhcp>stateless
Management interface settings have been enabled for V6. Applying settings to take effect.

set_management_ipv6_dhcp>

```

- 静的: IP アドレスを手動で入力します。

```

=====
Console to Citrix acquired

[MCN_DC-MCN_DC-VPX>management_ipv6
set_management_ipv6>Configuring IPv6: Enter "SLAAC" or "DHCP" or "static". Enter "disable" to
disable. Enter "main_menu" to return to the main menu.

set_management_ipv6>static

IPv6 Address:          (Not configured)
IP Prefix:             (Not configured)

Which would you like to do?
  "set interface <ip address> <IPv6 prefix>" - Stage New Settings for IP Address and prefix
  "main_menu" - Return to the Main Menu

set_management_ipv6_static>set interface fd73:.....::4 64
The following management interface settings have been staged
IP Address:           fd73:2039:5849:26::4
IP Prefix:            64

Which would you like to do?
  "apply" - Apply Staged Settings
  "cancel" - Cancel Staged Settings
  "main_menu" - Return to the Main Menu

set_management_ipv6_static>

```

8. VM インターフェイスの段階的な設定を適用します。以下を実行します:

- `set_management_ip` プロンプト (IPv4 の場合) または `set_management_ipv6` プロンプト (IPv6

の場合) で次のコマンドを入力します。 **apply**

- b) 適用操作を確認するプロンプトが表示されたら、**Y**と入力します。

これにより、仮想マシンの段階的なインターフェイス設定が適用され、結果が表示されます。

```

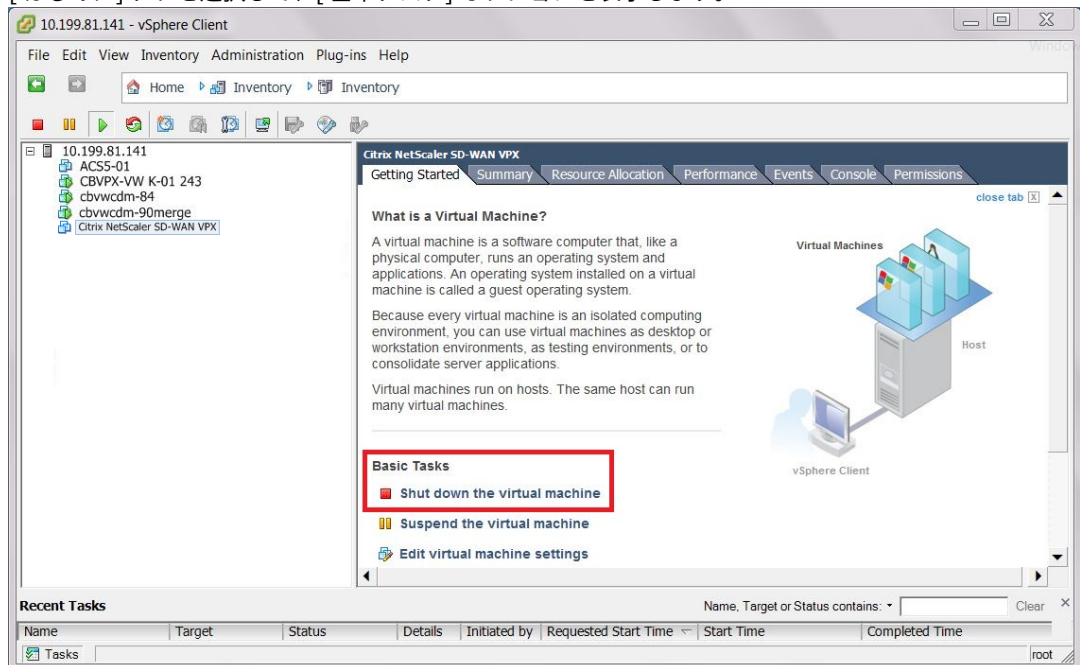
Getting Started Summary Resource Allocation Performance Events Console Permissions
Are you sure you want to change your Management Interface IP settings?
You may lose connectivity to the appliance. <y/n>?
y
IP Address:          10.199.81.237
Subnet Mask:        255.255.255.128
Gateway IP Address: 10.199.81.254

Which would you like to do?
"set interface <ip address> <subnet mask> <gateway>" - Stage New Setting
s for IP Address, Subnet Mask, and Gateway IP Address
"address" - Stage New IP Address
"mask" - Stage New Subnet Mask
"gateway" - Stage New Gateway IP Address
"clear" - Clear Settings
"apply" - Apply Staged Settings
"cancel" - Cancel Staged Settings
"main_menu" - Return to the Main Menu

set_management_ip>_
  
```

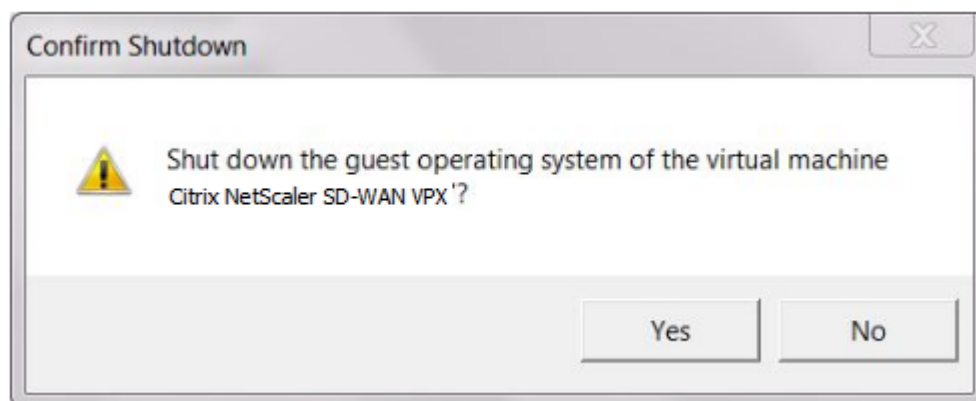
9. **exit** と入力し、プロンプトで **Return** キーを押して **management_ip** CLI を終了します。
10. コンソールを終了します。 **exit** と入力し、コンソールプロンプトで **Return** キーを押し、**Ctrl+Alt** キーを押して、カーソルの制御を取り戻します。
11. 仮想マシンをシャットダウンして再起動します。以下を実行します:

- a) [はじめに] タブを選択して、[基本タスク] オプションを表示します。

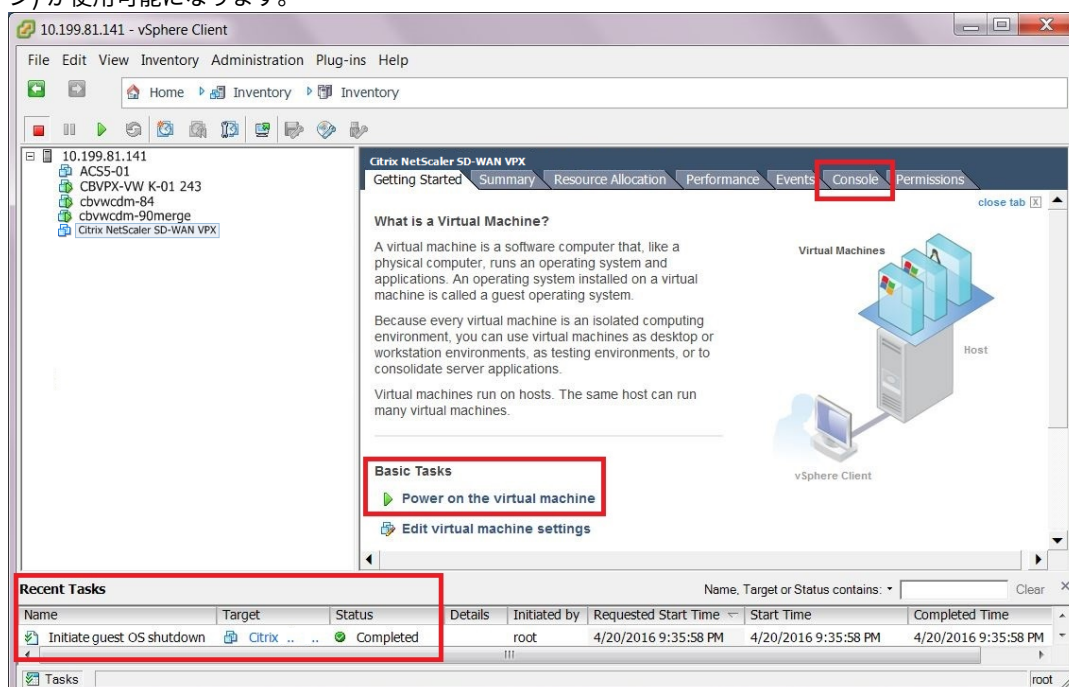


- b) [基本タスク] セクションで、[仮想マシンのシャットダウン] (赤いボックスアイコン) をクリックします。

仮想マシンのゲスト OS をシャットダウンするかどうかを確認するメッセージが表示されます。



- c) [はい] をクリックして確定します。これにより、ゲスト OS がシャットダウンされ、VM の電源がオフになります。シャットダウンが完了すると、仮想マシンをパワーオンするオプション (緑色の再生ボタン) が使用可能になります。



12. 仮想マシンを再起動します。仮想マシンをパワーオンする (緑色の右矢印) をクリックして、仮想マシンを再起動します。起動プロセスの進行状況は、仮想マシンの [コンソール] タブページで確認できます。

Getting Started	Summary	Resource Allocation	Performance	Events	Console	Permissions
[2.319376]	EXT3-fs (sda2):	mounted filesystem with ordered data mode			
[3.349616]	udev[348]:	starting version 175			
[3.475648]	input: Power Button	as /devices/LNXSYSTM:00/LNXPWRBN:00/input/input1			
[3.478001]	ACPI: Power Button	[PWRB]			
[3.530475]	input: PC Speaker	as /devices/platform/pcspkr/input/input2			
[3.674449]	alg: No test for __gcm-aes-aesni	(__driver-gcm-aes-aesni)			
[3.710378]	udev[380]:	renamed network interface eth0 to tn-mgt0			
[3.886738]	input: ImPS/2 Generic Wheel Mouse	as /devices/platform/i8042/serio1/input/input3			
[4.757848]	Adding 249964k swap	on /dev/sda5. Priority:-1 extents:1 across:249964k			
[11.662431]	EXT3-fs (sda2):	using internal journal			
[21.165250]	kjournald	starting. Commit interval 5 seconds			
[21.165607]	EXT3-fs (sda1):	using internal journal			
[21.165618]	EXT3-fs (sda1):	mounted filesystem with ordered data mode			
[21.197837]	kjournald	starting. Commit interval 5 seconds			
[21.198237]	EXT3-fs (sda6):	using internal journal			
[21.198246]	EXT3-fs (sda6):	mounted filesystem with ordered data mode			
[21.707241]	kjournald	starting. Commit interval 5 seconds			
[21.707683]	EXT3-fs (sda3):	using internal journal			
[21.707693]	EXT3-fs (sda3):	mounted filesystem with ordered data mode			
[24.553644]	e1000: tn-mgt0 NIC	Link is Up 1000 Mbps Full Duplex, Flow Control: None			

起動プロセスが完了すると、ログインプロンプトが表示されます。

Getting Started	Summary	Resource Allocation	Performance	Events	Console	Permissions
					Debian GNU/Linux 7 cbvw tty1	
					cbvw login: _	

これで、最後の段階SD-WAN VPX-SE への接続と展開のテストに進むことができます。

VPX に割り当てられた DHCP の管理 IP アドレスの表示

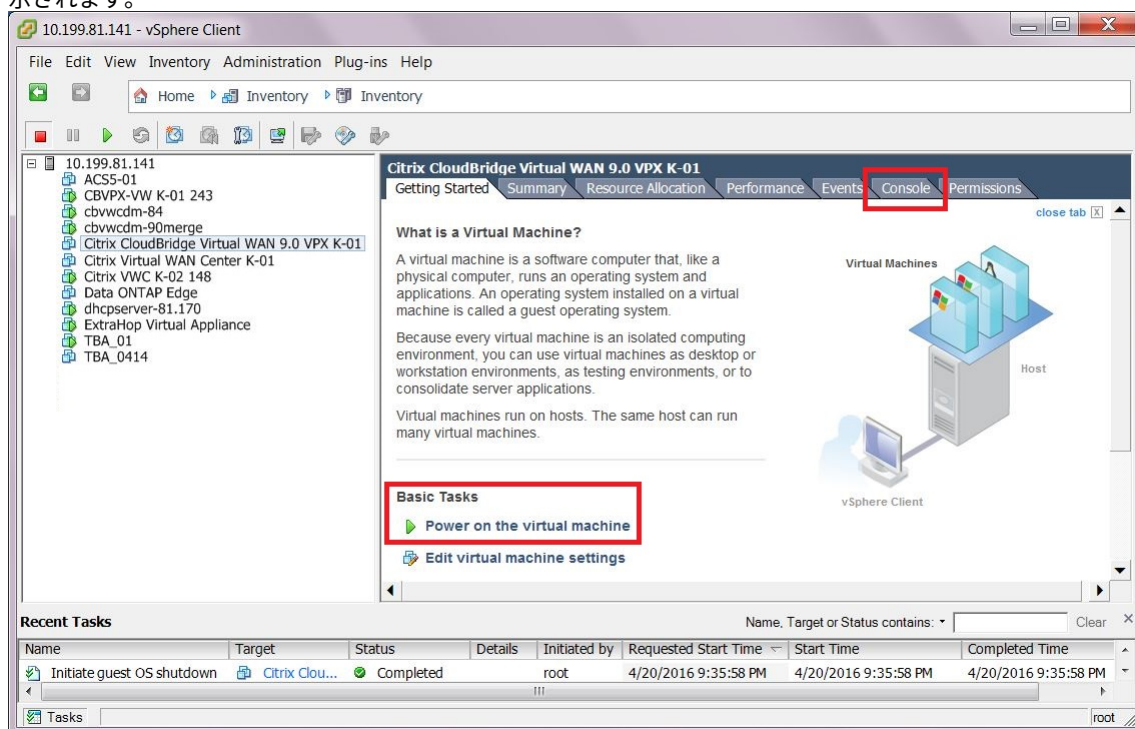
このセクションでは、新しい SD-WAN VPX-SE 仮想アプライアンス仮想マシンの DHCP 割り当ての管理 IP アドレスを表示および記録する手順について説明します。

注

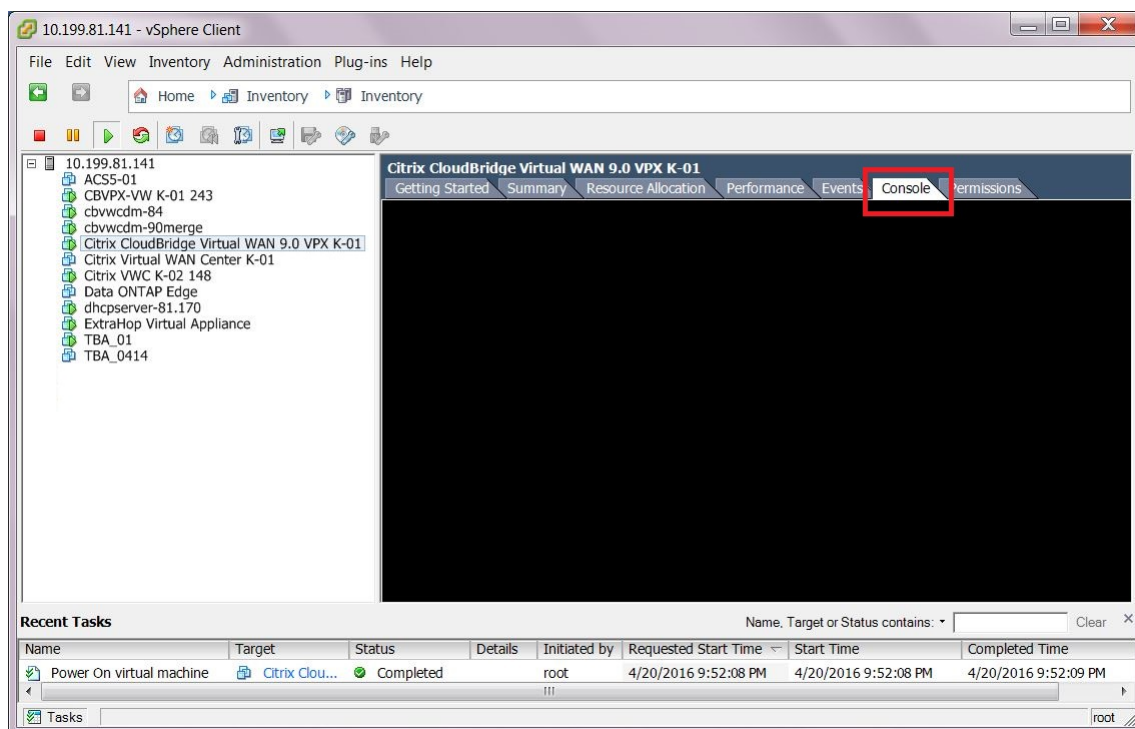
デフォルトでは、すべての SD-WAN VPX-SE 仮想アプライアンスは DHCP を使用します。DHCP を使用していない場合、または仮想アプライアンスに静的 IP アドレスを割り当てている場合は、この手順を省略できます。DHCP を使用している場合は、この手順を完了する前に、DHCP サーバが SD-WAN に存在し、使用可能になっている必要があります。

仮想アプライアンスの DHCP によって割り当てられた管理 IP アドレスを表示するには、次の手順を実行します。

1. [vSphere クライアントインベントリ] ページで、[インベントリ] ツリー（左ウィンドウ）で新しい SD-WAN VPX-SE 仮想マシンを選択します。これにより、SD-WAN VPX-SE 仮想マシンの [インベントリ] ページが表示されます。



2. まだ実行していない場合は、新しい仮想マシンをパワーオンします。[基本タスク] セクションで、[再生] アイコン（緑色の矢印）をクリックして、新しい SD-WAN VPX-SE 仮想マシンをパワーオンします。
3. 「インベントリ」ページのタブバーで「コンソール」タブを選択します。[コンソール] タブは、メインページ領域の上部にある [インベントリ] ページのタブバーにあります。このタブを選択すると、仮想マシンの CLI コンソールが表示され、アクセスできるようになります。

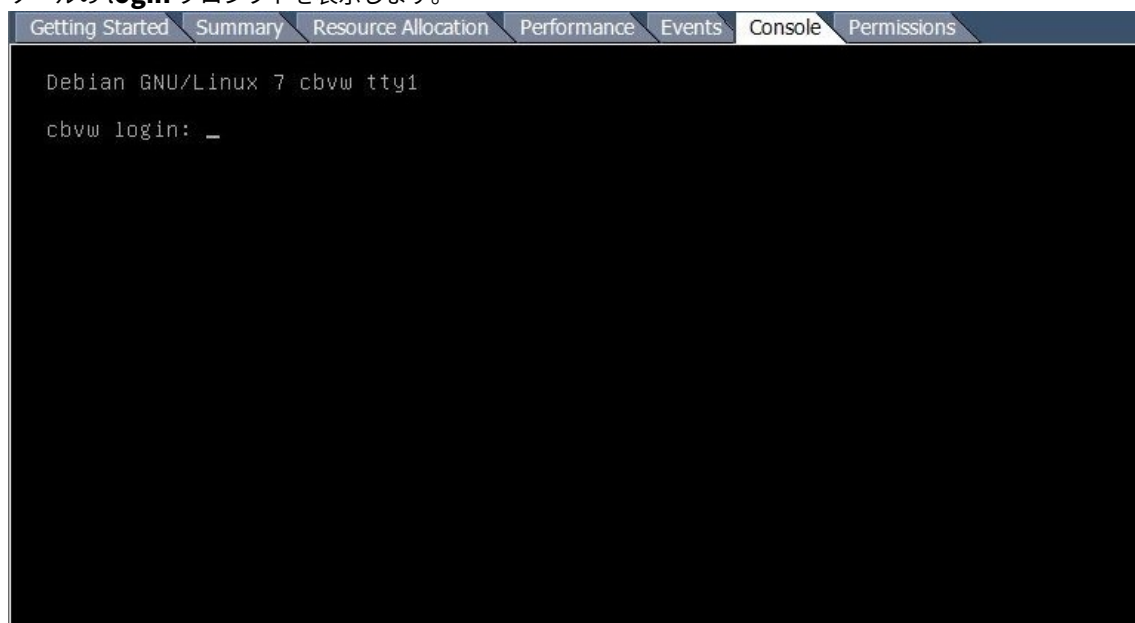


4. コンソール領域内の任意の場所をクリックして、コンソールモードを開始します。これにより、マウスカーソルの制御が仮想マシンコンソールに切り替わり、コンソールモードが有効になります。

注

コンソールのカーソルの制御を解除するには、**Ctrl** キーと **Alt** キーを同時に押します。

5. **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。**Enter** を 1 回または 2 回押して、コンソールの **login** プロンプトを表示します。



6. VM コンソールにログインします。新しい SD-WAN VPX-SE 仮想マシンのデフォルトのログインクレデンシャルは次のとおりです。

- ログイン: 管理者
- パスワード: パスワード

これにより、ホスト **IP** アドレスを含むコンソールへようこそ ****(Welcome)** メッセージが表示されます。
Last login: Tue Dec 1 17:15:16 on ttys000

```
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
[BANLSREE:~ sri $ ssh admin@10.3.56
admin@10.3.56's password:
```

```
=====
Operating System 5.1 on CBVPXv1
Host IPV4 = 10.3.56
Host IPv6 = fd73:1b35:1000::bcf1
```

```
=====
Console to Citrix acquired
```

```
[WARNING] RADIUS server is unreachable. This may cause slowness in the CLI.
```

```
MCN_DC-MCN_DC-VPX>
```

7. SD-WAN VPX-SE 仮想マシンの管理 IP アドレスを記録します。

注

DHCP サーバが SD-WAN に存在し、使用可能である必要があります。そうしないと、この手順を完了できません。

コンソールにログインすると、[*Last login*] 情報とホスト IP アドレスが Welcome メッセージに表示されます。この IP アドレスは、この新しい SD-WAN VPX-SE 仮想マシンの管理 IP アドレスです。

これで、SD-WAN VPX-SE 仮想マシンの展開は完了です。最後の段階は、新しい SD-WAN VPX-SE に接続し、展開をテストすることです。手順は次のセクションで説明します。

SD-WAN VPX への接続と展開のテスト

April 15, 2021

次のステップでは、新しい SD-WAN VPX-SE 仮想アプライアンスに接続し、展開が正常に行われたことを確認します。

展開をテストするには、次の手順を実行します。

1. 接続された PC で、ブラウザを開き、SD-WAN VPX-SE 仮想アプライアンスの管理 IP アドレスを入力します。ネットワークに接続された任意の PC（たとえば、vSphere Client で SD-WAN VPX-SE 仮想マシンを展開するために使用したローカル PC など）を使用できます。SD-WAN VPX-SE の管理 IP アドレスを正常に割り当てると、管理 Web インターフェイスのログインページが表示されます。

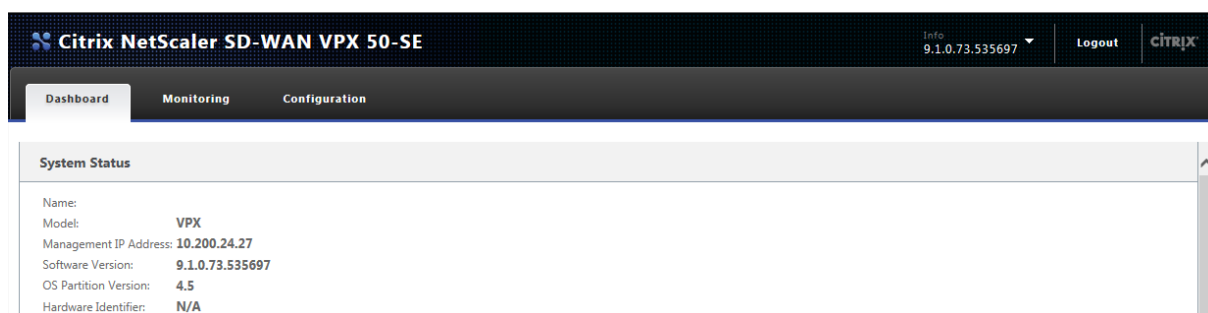


2. 管理者のユーザー名とパスワードを入力し、[ログイン] をクリックします。
 - デフォルトの管理者ユーザー名: *admin*
 - デフォルトの管理者パスワード: パスワード

注

デフォルトのパスワードはできるだけ早く変更することをお勧めします。パスワード回復には設定のリセットが必要になる場合があるため、必ず安全な場所にパスワードを記録してください。

管理 Web インターフェイスにログインすると、[ダッシュボード] ページが表示されます。



アプライアンスの管理 Web Interface に初めてログインすると、ダッシュボードにアラートアイコン（金色のデルタ）と、Virtual WAN サービスが無効であり、ライセンスがインストールされていないことを示すアラートメッセージが表示されます。現時点では、このアラートは無視できます。このアラートは、ライセンスをインストールし、アプライアンスの構成および展開プロセスを完了すると、自動的に解決されます。

これで、SD-WAN VPX-SE 仮想アプライアンスの初期インストールと展開が完了しました。ただし、SD-WAN ネットワークに追加する前に、仮想アプライアンスのセットアッププロセスを完了するための残りの手順がいくつかあります。次の手順を完了する手順については、「[初期設定](#)」のセクションに進んでください。

SD-WAN VPX の使用シナリオ

April 15, 2021

VPX を展開して、ブランチオフィスとの間で送受信されるトラフィックを、特定のサーバー、またはクラウドで高速化できます。データセンターでは、各サーバーに個別の VPX インスタンスを割り当てることにより、柔軟で強力な構成を作成できます。または、任意の場所で、同じサーバー内の異なるタイプまたはレベルのアクセラレーションサービスに対して、複数の VPX インスタンスを 1 つのサーバーに割り当てることができます。

VPN 経由で接続する従業員の場合、VPX は接続を高速化できます。

物理アプライアンスと同様に、最も一般的な設定タイプがインラインモードですが、WCCP モードと仮想インラインモードを使用すると、効果的な展開を実現できます。

VPX の使用シナリオ

VPX を展開して、ブランチオフィスとの間のトラフィックや、特定のサーバーとの間で送受信されるトラフィックを高速化できます。データセンターでは、各サーバーに個別の VPX インスタンスを割り当てることにより、柔軟で強力な構成を作成できます。または、任意の場所で、同じサーバー内の異なるタイプまたはレベルのアクセラレーションサービスに対して、複数の VPX インスタンスを 1 つのサーバーに割り当てることができます。

VPN 経由で接続する従業員の場合、VPX は接続を高速化できます。

物理アプライアンスと同様に、最も一般的な設定タイプがインラインモードですが、WCCP モードは効果的なフェールオーバーメカニズムを提供できます。

ブランチオフィス・アクセラレーター

VPX イメージは、SD-WAN/SD-WAN アプライアンスのように任意のサーバーにインストールし、展開できます。VPX は、SD-WAN/SD-WAN アプライアンスのすべての機能を備えているだけでなく、仮想化によってもたらされる利点もあります。グループモードおよび高可用性モードはサポートされていません。

図 1.VPX のユースケース #1: ブランチオフィスアクセラレーター

ブランチオフィス・サーバの高速化

仮想サーバーを単純なブランチオフィスアクセラレータ構成に追加すると、次の図に示すように、高速ブランチオフィスサーバーを使用できます。WAN へのパスが仮想 SD-WAN/SD-WAN を通過するように、仮想マシンをホストす

るアプライアンス内の仮想ネットワークを割り当てると、すべての WAN トラフィックが自動的に高速化されます。たとえば、ネットワークファイルシステムへのアクセスを必要とするすべての Web トラフィック、バックアップ、リモートアプリケーション、データベースクエリ、およびオペレーションが高速化されます。

仮想環境では、オペレーティングシステムや選択した機能など、必要な機能をサーバユニットに追加できます。この設定により、ブランチオフィスのすべてのシステムからのすべての WAN トラフィックが高速になります。また、同じマシンに複数の仮想サーバをデプロイして、ブランチオフィスのラックを複数の仮想マシンを実行する単一のユニットに統合することもできます。

図 2: VPX ユースケース #2: 高速ブランチオフィス・サーバ

データセンターサーバの高速化

データセンター内のすべてのサーバに VPX VM をインストールすると、サーバ自体の高速化によってサーバ数を最小限に抑えながら、サーバ容量の追加に応じて完全に拡張できるソリューションが作成されます。高速化されたサーバの数個を超えると、MultipleVPX VM によって提供される集約アクセラレーションは、単一のアプライアンスで提供できるものを超えます。

VPX は、XenApp、XenDesktop、Citrix マーチャンダイジングサーバー、ネットワークファイルシステム、データベース、Web サーバーなど、あらゆる種類のネットワークアプリケーションを高速化します。

図 3: VPX ユースケース #3: 加速されたデータセンターサーバー

VPN アクセラレータ

VPX で任意の VPN をインストールすることで、VPN が加速されます。

注: 他の構成とは異なり、VPN 仮想マシンは WAN 側にあり、VPX 仮想アプライアンスは LAN 側にあります。これは、VPN トラフィックを圧縮およびアプリケーションアクセラレーションのために復号化するためです。

図 4: VPX ユースケース #4: VPN アクセラレータ

同じサーバー上に複数の VPX インスタンス

同じサーバー上に複数の VPX 仮想マシンを配置することで、同じユニット内に異なるタイプまたはレベルのアクセラレーションサービスを作成できます。1 つの VPX インスタンスは、重要なアプリケーション専用の場合もあれば、個々のリモート・サイトや顧客専用の各インスタンスもあります。VLAN スイッチを使用して、トラフィックを適切な VPX インスタンスに転送します。

図 5: VPX ユースケース #5: 専用アクセラレーションリソース用の複数のインスタンス

WCCP および仮想インライン展開

WCCP および仮想インラインモードは、ポートを 1 つだけ使用するワンアーム配置に適しています。Amazon AWS バージョンの VPX は 1 つのポートのみを使用するため、常にワンアームモードでデプロイされます。

図 6. VPX ユースケース #6: WCCP または仮想インライン展開

イーサネットバイパスカードが望ましい場合、WCCP にはヘルスチェックが組み込まれているため、インラインモードではなく WCCP を使用すると効果的なフォールトトレランスが提供されます。ルータは、応答しない WCCP デバイスを介してトラフィックを転送する代わりに、エンドポイントに直接トラフィックを送信します。

ブランチオフィスアクセラレータ SD-WAN/SD-WAN VPX は、任意のサーバーにインストールし、他の SD-WAN/SD-WAN アプライアンスと同様に展開できます。VPX は、SD-WAN/SD-WAN アプライアンスと同じ機能に加えて、仮想化によって提供される追加機能を備えています。グループモードおよび高可用性モードはサポートされていません。

SD-WAN VPX の機能

VPX は、CitrixCommand Center リリース 4.0 以降をサポートしています。SD-WAN は、SD-WAN/SD-WAN VPX Express ライセンスもサポートします。このライセンスでは、最大 512 kbps の高速送信レート、10 の高速接続、および 5 つの SD-WAN/SD-WAN プラグインをサポートします。

- XenServer 用 VPX の特別な機能は次のとおりです。
 - XenServer 基本機能のサポート
 - XenMotion ライブマイグレーション
 - XenServer の高可用性
 - ワークロードバランス
 - パフォーマンス監視とアラート
- VMware vSphere の VPX の特長は、次のとおりです。
 - VMware vCenter サーバ (リモート管理)。
 - VMware vSphere ハイアベイラビリティ (高可用性)。
 - VMware vSphere vMotion (同じプロセッサを搭載した別のサーバに SD-WAN VPX を移行)
 - VMware ゲストのカスタマイズ (異なるインスタンスごとのパラメータで VPX を複製)

システム要件とプロビジョニング

April 15, 2021

SD-WAN VPX は XenServer 5.5 以降、VMware vSphere ESX/ESXi 4.1 以降、64 ビット Windows Server 2008 R2 SP1 では Hyper-V、Amazon AWS で動作します。SD-WAN VPX は、2GB から 8GB の RAM および 100 GB から 500 GB のディスク容量までの 4 つの構成をサポートします。4 GB RAM/250 GB の中間のディスク構成は、リピータ 8500 シリーズ・アプライアンスに似ています。

サポートされている構成

次の表に、サポートされているすべての SD-WAN 仮想マシン構成を示します。(Amazon AWS の設定は事前に選択されており、異なっています)。

種類	VCPU	RAM	ディスク	WAN の最大速度	最大高速接続数	SD-WAN/SD-WAN プラグインの最大数
2 GB の本番構成	2	2GB	100GB	2 Mbps	1,000	50
4 GB の本番構成。	2	4GB	250 ギガバイト	10 mbps	10,000	250
4 GB の本番構成。(45Mbps ライセンス付き)	2	4GB	250 ギガバイト	45 メガビット/秒	15,000	400
8 GB の本番構成	4	8GB	500GB	45 メガビット/秒	25,000	500

その他の構成 (実稼働ネットワーク用ではない)

種類	VCPU	RAM	ディスク	WAN の最大速度	最大高速接続数	SD-WAN/SD-WAN プラグインの最大数
VPX エクスプレス	2	1GB	60GB	512kbps	10	5
最小評価構成。	2	1GB	60GB	2 Mbps	1,000	5

最小リソース要件

SD-WAN VPX 仮想マシンには、本番環境に対して次の最小ハードウェア要件があります。

- 2GB の RAM
- 100 GB ディスク (ローカルディスクは最高のパフォーマンスを提供)
- 2 つの仮想 NIC (イーサネットポート)。ただし、1 つの仮想 NIC のみを必要とする Amazon AWS を除く

- 2つの仮想 CPU
- 現代の CPU (Intel Nehalem またはそれより新しいまたは AMD ファミリーの 10 時間以降、どちらも 2008 年に導入されました)。エミュレートされた x86 TSC (タイムスタンプカウンタ) 機能の使用により、古い CPU はパフォーマンスが低下する可能性があります。C1 より高いクロック状態を使用せず、古いプロセッサの BIOS で SpeedStep/PowerNow モードが無効になっている場合、TSC エミュレーションは使用されず、システムは通常で動作します。

VPX をホストするサーバーには、VPX VM に必要なものよりも大きい RAM、CPU、ディスクリソースが必要です。(VPX は、VMware ハードウェアのオーバーコミットをサポートしていません)。明らかに、サーバには、仮想アプライアンスに加えて、ハイパーバイザーを実行するのに十分なリソースが必要です。ただし、VPX VM の Ethernet ポートの 1 つが同じサーバー上の別の仮想マシンに接続されている場合は、仮想イーサネットポートと同じ数の物理イーサネットポートを持つことは必須ではありません。イーサネットオプションには、次のものがあります。

- VPX VM の 2 つの仮想ポートを 2 つの物理ポートにマッピングし、その操作はスタンドアロンの SD-WAN と同じになります。
- VPX VM の仮想ポートの 1 つを物理ポートに、もう一方を同じサーバ上の 1 つ以上の仮想マシンを含む仮想ネットワークにマッピングすることで、高速化されたサーバが作成されます。
- VPX VM の各仮想ポートを仮想ネットワークにマッピングし、同じサーバー上の 2 つの VM セット間で VPX 仮想マシンをチェーン化します。

次の図は、同じサーバー上の別の仮想マシンで終了するトラフィックのワンアーム展開における VPX 仮想マシンを示しています。この場合、必要な物理ポートは 1 つだけですが、両方の仮想ポートが使用されます。

使用可能なリソースの最大数

単一の VPX 仮想マシンが効果的に使用できるリソースの最大量は次のとおりです。

- 4 つの仮想 CPU
- 8 GB のラム
- 500 GB ディスク
- 4 つの仮想 NIC (リリース 9.x)
- 8 つの仮想 NIC (リリース 10.x)

VPX 仮想マシンに割り当てられていないサーバリソースは、同じサーバー上の他の仮想マシンでも使用できますが、リソースのオーバーコミットを避けるように注意してください。

ディスクと RAM

RAM とディスク領域の量が増加している間、追加のリソースは主に圧縮サブシステムに割り当てられます。メモリを増やすと、より多くの接続とアクセラレーションパートナーがサポートされます。

SD-WAN 圧縮システムは、ディスクサブシステムに大きな要求を行います。一般に、ローカルディスクストレージはネットワークディスクストレージよりも優れており、LAN とネットワークディスクの両方でリソース競合が減少します。

ディスクリソースまたはメモリリソースとリンク速度との関係は間接的です。メモリとディスクサイズは、リンク (bps) よりも多くのパケットが送信される速度には影響しません。メモリとディスク領域を増やすと、パターンマッチングに使用できる圧縮履歴の量が増加するため、圧縮のパフォーマンスが向上します。

仮想 NIC

Amazon AWS を除き、2 つの仮想ネットワークインターフェイスが必要です。これらはブリッジされ、アクセラレーションとブラウザベースのユーザーインターフェイスの両方に使用されます。これらのインターフェイスは、異なる仮想ネットワークに接続する必要があります。ワンアーム操作の場合、2 番目のインタフェースはスタブであり、VPX VM にのみ接続できます。

3 番目の仮想ネットワーク・インタフェースは、VPX VM への独立したインタフェースを提供します。これは、物理アプライアンス上のプライマリ・ポートに相当します。ブラウザベースのインターフェイスには使用できますが、アクセラレーションには使用できません。

その他の仮想マシン

- VPX に割り当てられたリソースを超えるサーバリソースは、同じサーバ上の他の仮想マシンで使用できます。
- 他の VM によるリソース使用量は、VPX のパフォーマンスに影響します。アクセラレーションにより、CPU、メモリ、ディスク、ネットワークが集中的に利用されます。

仮想ネットワークルーティングは、サーバ上の他の仮想マシンを VPX 仮想マシンに接続するために使用できますが、このような VM を接続する最も簡単な方法は、サーバの LAN 側の Ethernet ポートに仮想マシンを接続することです。WAN バインドされたパケットは、VPX VM のブリッジを通過し、VPX をホストするサーバの内部または外部から発信された場合、自動的に高速化されます。

図 2: ローカル仮想マシンからの外部トラフィックとトラフィックを加速するインライン展開

XenServer への SD-WAN 仮想アプライアンスのインストール

April 15, 2021

Citrix XenServer に NetScaler SD-WAN 仮想アプライアンスをインストールするには、まず十分なシステムリソースを持つマシンに XenServer をインストールする必要があります。SD-WAN VPX のインストールを実行するには、Citrix XenCenter を使用します。XenCenter は、ネットワーク経由で XenServer ホストに接続できるリモートマシンにインストールする必要があります。

仮想アプライアンスのインストールを開始する前に、次の操作を行います。

- 最小要件を満たすハードウェアに、サポートされているバージョンの XenServer® をインストールします。サポートされている XenServer のバージョンについては、SD-WAN リリースノートを参照してください。
- 最小システム要件を満たす管理用のワークステーションに XenCenter® をインストールします。

- VPX ライセンスファイルを入手します。

前提条件が満たされたら、仮想アプライアンスをインポートして構成する準備が整いました。

XenCenter を使用して SD-WAN 仮想アプライアンスを XenServer にインポートするには

1. ワークステーションで XenCenter を起動します。
2. [サーバー] メニューの [追加] を選択します。
3. [新しいサーバーの追加] ダイアログボックスの [ホスト名] ボックスに、接続先の XenServer サーバーの IP アドレスまたは DNS 名を入力します。
4. [ユーザー名] および [パスワード] ボックスに、管理者の資格情報を入力し、[接続] をクリックします。ナビゲーションペインに、緑の丸印の付いた XenServer 名が表示されます。これは、XenServer に接続済みであることを示します。
5. ナビゲーションペインで、SD-WAN VPX をインストールする XenServer サーバーの名前をクリックします。
6. [VM] メニューの [Import] を選択します。
7. [インポート] ダイアログボックスの [インポートファイル] で、SD-WAN VPX.xVA イメージファイルを保存した場所を参照します。[エクスポートされた仮想マシン] オプションが選択されていることを確認し、[次へ] をクリックします。
8. 仮想アプライアンスをインストールする **XenServer** サーバーを選択し、[次へ] をクリックします。
9. 仮想アプライアンスを保存するローカルストレージリポジトリを選択して [Import] をクリックし、インポート処理を開始します。
10. 必要に応じて、仮想ネットワークインターフェイスを追加、変更、または削除します。仮想ネットワークインターフェイス、インターフェイス 0、インターフェイス 1 を 2 つの異なる仮想アダプタ (この画面では Networks) に接続します。これら 2 つのインターフェイスは、仮想アプライアンスのアクセラレーションブリッジとして使用されます。仮想ネットワークインターフェイス 2 が存在する場合は、それを割り当てて、管理インターフェイス (プライマリポートに相当) として使用できます。完了したら [Next] をクリックします。
11. [インポート後に仮想マシンを起動する] チェックボックスをオフにします。
12. [完了] をクリックして、インポート処理を完了します。インポート処理の状態を参照するには、[Log] タブをクリックします。XenCenter インターフェイスのサーバーリストの下に、新しく作成された仮想マシンが表示されます。

重要

両方の仮想アダプタを同じネットワークに接続しないでください。これにより、転送ループが作成され、ネットワークの停止を引き起こす可能性があります。また、SD-WAN VPX に関連付けられている 2 つの物理イーサネットポートを、同じイーサネットスイッチに接続しないでください。

仮想 SD-WAN アプライアンスを設定するには

1. XenCenter で、SD-WAN VPX 仮想マシンのアイコンを選択します。次に、[ストレージ] タブで [プロパティ] を選択し、[プロパティ] ダイアログボックスで、ディスク割り当てを目的のレベルに調整します。

注:

- SD-WAN VPX 仮想マシンのディスク割り当てを変更すると、圧縮履歴のサイズが変更され、再初期化されます。蓄積された履歴はすべて失われます。
- SD-WAN VPX の実行中は、リソース割り当てを変更しないでください。
- [強制シャットダウン] または [強制再起動] コマンドは使用しないでください。彼らは動作しない可能性があり、問題を引き起こす可能性があります。代わりに、[シャットダウン] および [再起動] コマンドを使用します。

2. [**SD-WAN VPX**] アイコンを右クリックし、[プロパティ] オプションを選択します。[CPU とメモリ] で、サポートされている構成に対応する vCPU の数と VM メモリの量を選択します。
3. [**SD-WAN VPX** のプロパティ] ダイアログボックスで、[スタートアップオプション] をクリックし、[サーバー起動時に自動起動] チェックボックスをオンにします。(OS 起動パラメータは使用されません)。
4. 基本的なネットワークパラメータを設定します。実行しているリリースに応じて、次のいずれかの操作を行います。
 - a) 仮想マシンが起動したら、仮想マシンコンソールに移動し、コマンドラインインタープリタにログインし、次の例を参考にアクセラレーションブリッジの IP パラメータを設定します。

```
pre codeblock Login: admin Password: password admin> set adapter  
apa -ip 172.16.0.213 -netmask 255.255.255.0 -gateway 172.16.0.1  
admin> restart <!--NeedCopy-->
```
 - b) SD-WAN VPX 仮想マシンを初めて起動すると、展開ウィザードが自動的に実行されます。ウィザードに従って、IP パラメータを設定します。
5. SD-WAN VPX が再起動したら、Apa に割り当てた IP アドレスでブラウザベースの UI (デフォルトの資格情報: 管理者およびパスワード) にログオンします。
6. [コマンド] メニューから、[クイックインストール] を選択します。
7. [クイックインストール] ページで、物理 SD-WAN アプライアンスの場合と同様に、クイックインストールを実行します。
8. 構成を完了します。

メモ

- 10.2.6 および 11.0.3 リリース以降では、SD-WAN アプライアンスのプロビジョニング時または新しい SD-WAN SE VPX の導入時に、デフォルトの管理者ユーザーアカウントパスワードを変更することが必須です。この変更は、CLI と UI の両方を使用して適用されます。
- システムメンテナンスアカウント (CBVWSSH) は、開発およびデバッグ用に存在し、外部ログイン権限はありません。このアカウントには、通常の管理ユーザーの CLI セッションからのみアクセスできます。

XenServer 6.5 Upgrade for SD-WAN Standard Edition アプライアンス

April 15, 2021

重要

XenServer バージョン 6.5 にアップグレードするには、アプライアンスで SD-WAN ソフトウェアリリース 9.0.x 以降が実行されている必要があります。

注

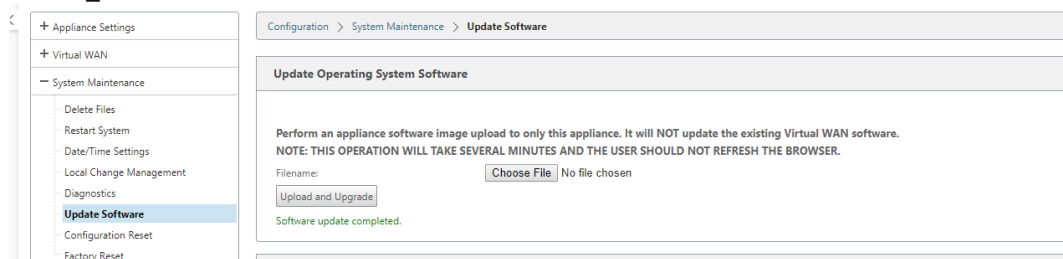
アップグレードの問題を回避するために、アプライアンスがリリース 9.0.x より前のソフトウェアバージョンで実行されている場合は、アップグレードを試みないでください。

XenServer 6.5 にアップグレードする方法

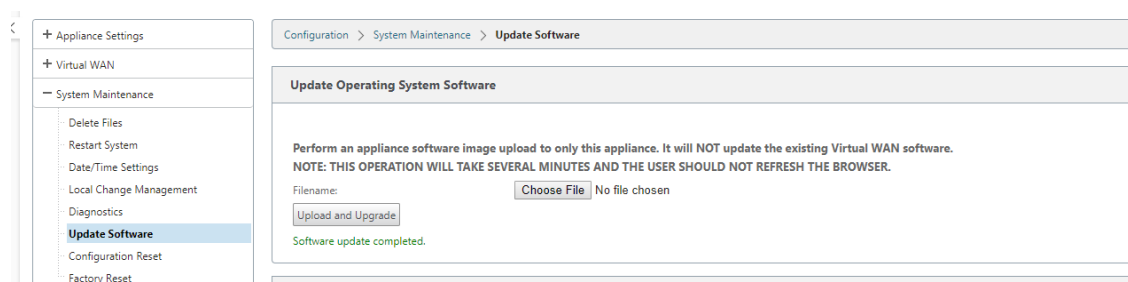
SD-WAN Standard Edition アプライアンスで XenServer 6.5 にアップグレードするには、アプライアンスでソフトウェアリリース 9.0.x 以降が実行されていることを確認します。アプライアンスが古いソフトウェアリリースバージョンを実行している場合は、最初に最新のソフトウェアリリースバージョンにアップグレードしてください。

1. 変更管理手順を使用して、SD-WAN Standard Edition ソフトウェアをアップグレードします。変更管理の手順を参照してください。

- a) SD-WAN SE GUI で、[構成] > [システムメンテナンス] > [ソフトウェアの更新] の順に選択します。cb-vw-.tar.gz <Platform_Model> <Build_No> ファイルをダウンロードします。次に、ns-sdw-vw-.upg <Build_No> ファイルをダウンロードして、オペレーティングシステムのソフトウェアを更新します。



- b) シングルステップアップグレードワークフローに従って、SD-WAN ソフトウェアをアップグレードします。
2. Citrix XenServer 6.5 にアップグレードする前に、手順 1 で説明した手順 a または b を実行します。
 3. SD-WAN GUI で [ソフトウェアの更新] に移動します。
 4. ダウンロードしたファイルの場所を選択して、ダウンロードサーバーからダウンロードした Citrix **XenServer6.5** バンドルをオペレーティングシステムソフトウェアにアップロードします。



5. [アップロードしてアップグレード] をクリックします。アップグレードが完了するまで約 20 分待ちます。アップグレードが正常に完了すると、アプライアンスが再起動します。

VMware ESX での SD-WAN 仮想アプライアンスのインストール

April 15, 2021

警告

仮想マシンネットワークでのみ無差別モードを有効にしてください。仮想スイッチの設定では、無差別モードを有効にしないでください。

注

VMware vSphere クライアントの操作の詳細は、vSphere ソフトウェアの新しいリリースで変更される場合があります。vSphere Client のインストールと操作に関する最も完全かつ最新の手順については、VMware のマニュアルも参照してください。この章の手順では、ESXi プラットフォームに SD-WAN VPX-SE 仮想アプライアンスをインストールする場合のみ、最も基本的で基本的なガイドラインを提供することを目的としています。

次に、SD-WAN VPX-SE をインストールおよび展開する最上位の手順をまとめます。これらの手順は、リストされた順序で実行してください。

1. VMware vSphere クライアントをインストールします。
2. SD-WAN VPX-SE OVF テンプレートをインストールしてデプロイします。
3. SD-WAN VPX-SE 管理 IP アドレスを設定します。
4. 展開を接続してテストします。

この章では、SD-WAN VPX-SE のインストール、設定、および配置の手順について説明します。これには、SD-WAN VPX-SE 仮想マシンの作成および展開に使用する VMware vSphere Client のインストールに関する基本的な手順が含まれます。

仮想アプライアンスのインストールを開始する前に、次の操作を行います。

- 最小要件を満たすハードウェアに VMware ESX バージョン 5.5 または ESXi 6.0 以降をインストールします。
- 最小システム要件を満たす管理ワークステーションに VMware vSphere クライアントをインストールします。

- SD-WAN VPX-SE セットアップファイルをダウンロードします。
- SD-WAN VPX-SE ライセンスファイルを取得します。

また、SD-WAN VPX-SE 仮想アプライアンスをインストールする前に、VPX 仮想アプライアンスに割り当てる予定のすべてのインターフェイスに一意の形式でラベルを付けます。大規模な展開では、これらのインターフェイスを固有の形式でラベル付けすると、Windows 仮想マシンや Linux 仮想マシンなどのように、他の仮想マシンで使用される他のインターフェイス間でインターフェイスをすばやく識別できます。このようなラベル付けは、異なるタイプの仮想マシンがインターフェイスを共有する場合に特に重要です。

SD-WAN VPX-SE には、デフォルト以外のネットワークオプションが必要です。とりわけ、アクセラレーションブリッジ用に 2 つの新しい仮想スイッチ (vswitch0 および vswitch1) を作成し、2 つの異なる仮想スイッチに割り当てる必要があります。

VMware vSphere クライアントのインストール

このセクションでは、SD-WAN VPX-SE 仮想マシンの作成および展開に使用する 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について説明します。

注

詳細については、VMware vSphere クライアントのマニュアルも参照してください。

1. ブラウザを開き、vSphere Client および SD-WAN VPX-SE 仮想マシン (VM) インスタンスをホストする ESXi サーバに移動します。 **VMware ESXi** へようこそ] ページが表示されます。
2. **vSphere Client** のインストールファイルをダウンロードするには、[vSphere クライアントのダウンロード] リンクを選択します。
3. vSphere Client をインストールします。ダウンロードした vSphere Client インストーラファイルを実行し、プロンプトが表示された場合はデフォルトの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** クライアントのログイン画面が表示され、ESXi サーバのログイン資格情報の入力を求められます。
5. ESXi サーバのログイン資格情報を入力します。次のように入力します：
 - **[IP アドレス/名前]:** SD-WAN VPX-SE VM インスタンスをホストする ESXi サーバの 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] を選択します。 **vSphere** クライアントのメインページが表示されます。

次の段階は、SD-WAN VPX-SE OVF テンプレートをインストールしてデプロイし、仮想マシンをセットアップすることです。ここでは、これらの手順について説明します。

SD-WAN VPX-SE OVF テンプレートのインストールとデプロイ

この項では、SD-WAN VPX-SE OVF テンプレートのインストールと SD-WAN VPX-SE 仮想マシンの作成手順について説明します。

1. まだダウンロードしていない場合は、SD-WAN VPX-SE 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。SD-WAN VPX-SE をホストする ESXi サーバへの接続に使用するローカル PC に、SD-WAN VPX-SE OVF テンプレートをダウンロードまたはコピーします。OVF テンプレートファイルには、**cb-vwc-version_number-vmware.ova** という命名規則を使用したファイル名があります:
`version_number` は SD-WAN VPX-SE リリースのバージョン番号です。
.ova は、これが OVF テンプレートファイルであることを示すファイル名のサフィックスです。

注

詳細については、[ソフトウェアパッケージのダウンロード](#) セクションを参照してください。

2. vSphere Client で続行し、[ファイル]、[OVF テンプレートの展開...] の順に選択します。をドロップダウンメニューから選択します。[OVF テンプレートのデプロイ] ウィザードの最初のページ、[ソース] ページが表示されます。
3. インストールする SD-WAN VPX-SE OVF テンプレート (.ova ファイル) を選択します。以前にローカル PC にダウンロードした .ova ファイルの場所を参照し、選択します。
4. [次へ] を選択します。これにより、選択した .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. 次のページには、インポートした OVF テンプレートに関する基本情報がいくつか表示されます。
6. [次へ] を選択します。これは、**EULA** ページに進みます。
7. [受け入れ] を選択し、[次へ] を選択します。これは、[名前と場所] ページに進みます。
8. 新しい仮想マシンの一意の名前を入力します (またはデフォルトをそのまま使用します)。名前は、現在のイベントリフォルダ内で一意である必要があります。80 文字以内で指定できます **。 **
9. [次へ] を選択します。これは、[ストレージ] ページに進みます。
10. 仮想マシンに十分な領域があるデータストアを選択します。SD-WAN VPX-SE 仮想マシンには、39.1 GB のディスク領域が必要です。
11. [次へ] を選択します。[ディスクフォーマット] ページが表示されます。
12. デフォルトの設定をそのまま使用し、[Next] を選択します。[ネットワークマッピング] ページに進みます。
13. デフォルト (**VM** ネットワーク) をそのまま使用し、[次へ] を選択します。[完了の準備完了] ページに進みます。
14. [完了] を選択して、仮想マシンを作成します。[NetScaler SD-WAN VPX-SE の展開状態] ダイアログボックスが表示されます。サーバー上に存在する条件によっては、展開が完了するまで数分から数時間かかる場合があります。SD-WAN VPX-SE 仮想マシンが正常に作成されると、成功メッセージが表示されます。

15. [閉じる]を選択します。これにより、**OVF** テンプレートのデプロイウィザードが閉じ、vSphere Client のメインウィンドウに戻ります。この vSphere Client を使用して最初に作成した仮想マシンの場合は、vSphere Client ホームページが表示されます。以前に 1 つ以上の仮想マシンを作成した場合は、[インベントリ] ページが表示されます。

次のステップでは、SD-WAN VPX-SE 管理 IP アドレスを設定します。ここでは、この手順の手順について説明します。

SD-WAN VPX-SE の管理 IP アドレスの設定

SD-WAN VPX-SE 仮想マシンに管理 IP アドレスを割り当てるには、次の 2 つの方法があります。

- DHCP を使用していない場合: SD-WAN VPX-SE 仮想アプライアンスの静的な管理 IP アドレスを手動で割り当てる必要があります。
- DHCP を使用している場合: デフォルトでは、すべての SD-WAN-VW 仮想アプライアンスは DHCP を使用して管理 IP アドレスを取得します。DHCP を使用するには、DHCP サーバーが仮想 WAN に存在し、利用可能である必要があります。

詳しくは、「[管理 IP の設定](#)」を参照してください。

VPX の静的管理 IP アドレスの手動構成

DHCP を使用していない場合、または SD-WAN VPX-SE 仮想アプライアンス仮想マシンの静的な管理 IP アドレスを設定する場合は、手動で行う必要があります。これを行うには、vSphere Client で作成した仮想マシンのコンソールを使用します。

「[SD-WAN 仮想 WAN アプライアンスの設定](#)」も参照してください。

管理 IP アドレスを手動で設定するには、次の手順を実行します。

注

DHCP は、SD-WAN VPX-SE 管理 IP アドレスに対してデフォルトで有効になっています。

1. [vSphere クライアントインベントリ] ページで、[インベントリ] ツリー (左ウィンドウ) で新しい SD-WAN VPX-SE 仮想マシンを選択します。新しい仮想マシンの [インベントリ] ページが表示され、[はじめに] タブが選択されています。
2. 新しい仮想マシンをパワーオンします。[はじめに] タブページの [基本タスク] セクションで、[仮想マシンをパワーオン] (緑色のマウスボタン) を選択して、新しい SD-WAN VPX-SE 仮想マシンをパワーオンします。
3. 「インベントリ」ページのタブバーの「コンソール」タブをクリックします。[コンソール] タブは、メインページ領域の上部にある [インベントリ] ページのタブバーにあります。このタブを選択すると、仮想マシンの CLI コンソールにアクセスできるようになります。新しい仮想マシンが起動するため、コンソールには一連のステータスメッセージが表示されます。起動プロセスが完了すると、コンソールログインプロンプトが表示されます。

4. コンソール領域内の任意の場所を選択して、コンソールモードを入力します。これにより、ポインティングデバイスのカーソルの制御が VM コンソールよりも大きくなり、コンソールモードが有効になります。
5. VM コンソールにログインします。新しい SD-WAN VPX-SE 仮想マシン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: 管理者パスワード
: パスワードコンソールの
**[** ようこそ] 画面が表示されます。
6. コンソールプロンプトで次のコマンドを入力します。management_ip コンソールで management_ip CLI に切り替わり、set_management_ip プロンプトが表示されます。
7. 仮想マシンのインターフェイス設定を構成します。set_management_ip プロンプトで次のコマンドラインを入力します。
set interface <ipaddress> <subnetmask> <gateway><!--NeedCopy-->
 - <ip> は、SD-WAN VPX-SE 仮想アプライアンスの管理 IP アドレスです。
 - <subnetmask> は、SD-WAN VPX-SE 仮想アプライアンスが常駐するネットワークを定義するために使用されるサブネットマスクです。
 - <gateway> は、SD-WAN VPX-SE 仮想アプライアンスが外部ネットワークとの通信に使用するゲートウェイ IP アドレスです。
このステージでは、インターフェイス設定は適用されません。
8. VM インターフェイスの段階的な設定を適用します。以下を実行します:
 - a) set_management_ip プロンプトで次のコマンドを入力します。
適用
 - b) 適用操作を確認するメッセージが表示されたら、「Y」と入力します。これにより、仮想マシンの段階的なインターフェイス設定が適用され、結果が表示されます。
9. exit と入力し、プロンプトで **Return** キーを押して management_ip CLI を終了します。
10. コンソールを終了します。コンソールプロンプトで「exit」と入力し、**Return** キーを押し、**Ctrl+Alt** キーを押して、カーソルの制御を取り戻します。
11. 仮想マシンをシャットダウンして起動します。以下を実行します:
 - a) [はじめに] タブを選択して、[基本タスク] オプションを表示します。
 - b) [基本タスク] セクションで、[仮想マシンをシャットダウンする] (赤いチェックボックスアイコン) を選択します。仮想マシンのゲスト OS を終了するかどうかを確認するメッセージが表示されます。
 - c) [はい] を選択して確定します。これにより、ゲスト OS がシャットダウンされ、VM の電源がオフになります。シャットダウンが完了すると、[仮想マシンのパワーオン] オプション (緑色の再生マウスボタン) が使用可能になります。
12. 仮想マシンを起動します。仮想マシンをパワーオンする (緑色の右矢印) を選択して、仮想マシンを起動します。起動プロセスの進行状況は、仮想マシンの [コンソール] タブページで確認できます。

起動プロセスが完了すると、ログインプロンプトが表示されます。これで、最後の段階「SD-WAN VPX-SE への接続」および「展開のテスト」に進むことができます。

メモ

- 10.2.6 および 11.0.3 リリース以降では、SD-WAN アプライアンスのプロビジョニング時または新しい SD-WAN SE VPX の導入時に、デフォルトの管理者ユーザーアカウントパスワードを変更することが必須です。この変更は、CLI と UI の両方を使用して適用されます。
- システムメンテナンスアカウント (CBVWSSH) は、開発およびデバッグ用に存在し、外部ログイン権限はありません。このアカウントには、通常の管理ユーザーの CLI セッションからのみアクセスできます。

HyperV 2012 R2 および 2016 のハイパーバイザーの SD-WAN Standard Edition 仮想アプライアンス (VPX)

April 15, 2021

HyperV 2012 R2 および 2016 のハイパーバイザーに SD-WAN VPX-SE をインストールするには:

1. **HyperV** マネージャをインストールします。詳細については、のドキュメントを参照してください [Microsoft.com](https://www.microsoft.com)。
2. **My Citrix** からダウンロードした **SD-WAN** ディストリビューションを解凍します。
3. **Hyper-V** マネージャーを起動します。

仮想マシンを作成する方法は 2 つあります。

- 方法 **1**: 仮想マシンをインポートする
 1. ナビゲーションウィンドウの [**Hyper-V** マネージャー] で、**SD-WAN VPX** をインストールするサーバーを選択します。
 2. [操作] メニューの [仮想マシンのインポート] をクリックします。
 3. [仮想マシンのインポート] ダイアログボックスの [場所] ボックスで、SD-WAN VPX ファイルを含むフォルダへのパスを指定します。

注:

圧縮ファイルを受け取った場合は、フォルダーへのパスを指定する前に、フォルダーにファイルを展開することを確認します。

4. [インポート] をクリックします。
5. 作成した仮想アプライアンスが [仮想マシン] の下に表示されていることを確認します。
6. 仮想マシンを右クリックし、[設定] をクリックします。

7. [設定] ウィンドウのナビゲーションペインの [ハードウェア] で、一覧の最初のネットワークアダプタを選択します。
8. [ネットワーク] ドロップダウンメニューで、[Apa1 ネットワーク] を選択します。これは Apa1 の LAN インターフェイスです。
9. [**MAC** アドレススプーフィングを有効にする] ボックスが選択されていることを確認します。そうでない場合は、それを選択して変更を適用します。
10. [設定] ウィンドウのナビゲーションペインの [ハードウェア] で、一覧の 2 番目のネットワークアダプタを選択します。手順 10 と手順 11 を繰り返し、アダプタを Apa2 ネットワークに割り当てます。これは Apa2 の WAN インターフェイスです。重要: 両方のネットワークアダプタに同じネットワークを構成しないでください。設定が正しくないと、パケットループが作成され、ネットワークがダウンする可能性があります。
11. 必要に応じて、仮想ハードディスクのサイズを変更します。
 - 「設定」ウィンドウのナビゲーションウィンドウの「IDE コントローラ 0」で、「ハードドライブ」を選択します。
 - [編集] をクリックします。
 - 仮想ハードディスクの編集ウィザードの手順に従って、ウィザードの [展開] オプションを使用して、割り当てをサポートされているサイズの 1 つに増やします。
12. 必要に応じて、メモリサイズを変更します。
 - [設定] ウィンドウのナビゲーションウィンドウの [ハードウェア] で、[メモリ] を選択します。
 - サポートされているサイズの 1 つにメモリを調整して、RAM 領域を割り当てます。
 - [OK] をクリックします。
13. 必要に応じて、管理ポートを定義します。
 - 仮想マシンを右クリックし、[設定] をクリックします。
 - [設定] ウィンドウのナビゲーションペインの [ハードウェア] で、[** ハードウェアの追加 **] を選択します。
 - デバイスの一覧から [ネットワークアダプタ] を選択し、[追加] をクリックします。
 - 新しい仮想ネットワークに「プライマリネットワーク 3」という名前を付けます。
 - * [**MAC** アドレスのスプーフィングを有効にする] チェックボックスがオンになっていることを確認します。
 - * [OK] をクリックして変更を適用します。
14. **SD-WAN VPX** 仮想マシンを右クリックし、[接続] を選択します。
15. [ファイル] メニューの [操作] をクリックし、[開始] をクリックして仮想マシンを起動します。
16. SD-WAN VPX 仮想マシンを初めて起動すると、展開ウィザードが自動的に起動します。このウィザードでは、展開モードに関する質問が表示されます。[**Web UI** を使用して設定] を選択します。次の画面で、apa インターフェイスの **IP** アドレス、ネットマスク、ゲートウェイを入力し、[**Finish**] をクリックします。

17. SD-WAN VPX が再起動したら、ブラウザベースの UI (ユーザー名:admin、パスワード: パスワード: パスワード) に、apa に割り当てた IP アドレスにログオンします。次に例を示します。
<https://172.16.0.213>
18. [**HyperV** マネージャ] ウィンドウで、[仮想スイッチマネージャ] に移動し、管理、LAN、および WAN の順にインターフェースを構成します。
19. **hyperv.tgz** ファイルをダウンロードし、解凍します。
20. 抽出した VHD を使用して仮想マシンをインポートし、それに応じて CPU とメモリの数を割り当てます。インターフェースを順序 (管理、LAN、および WAN) に追加します。LAN および WAN インターフェースで Mac スプーフィングを有効にします。[設定] > [インターフェース] > [高度な機能] の順に選択します。

• 方法 2: 新しい仮想マシンウィザード

注:

Hyper-V 仮想マシンをオーケストレータに接続する必要がある場合は、方法 2 を選択します。

1. SD-WAN Hyper-V セットアップファイルを開き、[仮想ハードディスク] フォルダを選択します。
2. ハードディスクイメージをコピーし、Hyper-V セットアップファイルの外部に新しく作成したフォルダに貼り付けます。
3. **Hyper-V** マネージャーを開き、**Hyper-V ID** を選択し、右クリックして [新規] > [仮想マシン] を選択します。
4. 仮想マシンウィザードが開き、[次へ] をクリックします。
5. 名前を指定し、仮想マシンの場所を指定することもできます。仮想マシンを保存する別の場所を指定する場合は、このチェックボックスをオンにします。[次へ] をクリックします。
6. 仮想マシンの世代を選択し、[次へ] をクリックします。
7. 仮想マシンに割り当てるメモリの量を指定し、[次へ] をクリックします。
8. ドロップダウンリストから接続を選択し、[**Next**] をクリックします。ここで選択している接続は、管理ポート用です。
9. VHD を接続するには、[既存の仮想ハードディスクを使用する] ラジオボタンを選択し、展開された zip ファイルから VHD ファイルを参照して選択し、[次へ] をクリックします。仮想ハードディスクは、以下の場所にあります。
> ctx-sdw-se-vmx > 仮想ハードディスク <extracted_zip_file location>
10. [概要] ページの詳細を確認し、[完了] をクリックして仮想マシンの作成を完了します。

デフォルトでは、仮想マシンはオフ状態になっています。これまでに作成した仮想マシンには 1 つのインターフェースと 1 つのコアしかありません。SD-WAN が機能するには、コア数を増やし、2 つのインターフェースを追加する必要があります。以下の手順を実行します。

1. 作成した仮想アプライアンスが [仮想マシン] の下に表示されていることを確認します。
2. 仮想マシンを右クリックし、[設定] をクリックします。
3. [設定] ウィンドウのナビゲーションペインの [ハードウェア] で、一覧の最初のネットワークアダプタを選択します。
4. [ネットワーク] ドロップダウンメニューで、[Apa1 ネットワーク] を選択します。これは Apa1 の LAN インターフェイスです。
5. [MAC アドレススプーフィングを有効にする] ボックスが選択されていることを確認します。そうでない場合は、それを選択して変更を適用します。
6. [設定] ウィンドウのナビゲーションペインの [ハードウェア] で、一覧の 2 番目のネットワークアダプタを選択します。手順 10 と手順 11 を繰り返し、アダプタを Apa2 ネットワークに割り当てます。これは Apa2 の WAN インターフェイスです。重要: 両方のネットワークアダプタに同じネットワークを構成しないでください。設定が正しくないと、パケットループが作成され、ネットワークがダウンする可能性があります。
7. 仮想 CPU コアの数を増やします。
 - [設定] ウィンドウのナビゲーションペインで、[プロセッサ] を選択します。
 - 仮想プロセッサの数を少なくとも 4 に増やします。
 - [Apply] をクリックします。
8. 必要に応じて、仮想ハードディスクのサイズを変更します。
 - 「設定」ウィンドウのナビゲーションウィンドウの「IDE コントローラ 0」で、「ハードドライブ」を選択します。
 - [編集] をクリックします。
 - 仮想ハードディスクの編集ウィザードの手順に従って、ウィザードの [展開] オプションを使用して、割り当てをサポートされているサイズの 1 つに増やします。
9. 必要に応じて、メモリサイズを変更します。
 - [設定] ウィンドウのナビゲーションウィンドウの [ハードウェア] で、[メモリ] を選択します。
 - サポートされているサイズの 1 つにメモリを調整して、RAM 領域を割り当てます。
 - [OK] をクリックします。
10. 右クリックして [開始] を選択します。状態が [Running] に変更されると、仮想マシンを使用できるようになります。

インターフェイスの追加

インターフェイス (LAN および WAN) での Mac スプーフィングの有効化

仮想マシンが起動したら、空き IP アドレスを割り当てます。仮想マシンは、IP アドレスを割り当てた後にアクセスできます。

注

ダウンロードされた qcow イメージは、デフォルトのフォルダ /var/lib/libvirt/images の下に存在する必要があります。このイメージをダウンロードして **KVM** の別のフォルダで使用すると、ディスクサイズの拡張が行われるときに問題が発生する可能性があります。

HyperV 2012 R2 および 2016 での SD-WAN VPX-SE の展開に関する制限事項

- VLAN タグ付きトランク配置はサポートされていません。

Installing SD-WAN VPX on Microsoft Server 2008 R2

April 15, 2021

インストール手順の実行

Microsoft Server 2008 R2 で HYPER-V の役割を有効にし、VPX ファイルを抽出した後、HYPER-V マネージャーを使用して SD-WAN VPX をインストールできます。仮想マシンをインポートしたら、Hyper-V によって作成された仮想ネットワークに関連付けて、仮想 NIC を構成する必要があります。

注: 仮想アプライアンスの実行中は、設定を変更できません。仮想アプライアンスをシャットダウンしてから変更を行います。

HYPER-V マネージャーを使用して、**Microsoft Server 2008 R2** に **SD-WAN VPX** をインストールするには

1. My Citrix からダウンロードした SD-WAN ディストリビューションを解凍します。
2. **Hyper-V** マネージャーを起動します。
3. ナビゲーションウィンドウの [**Hyper-V** マネージャー] で、SD-WAN VPX をインストールするサーバーを選択します。
4. [操作] メニューの [仮想スイッチマネージャ] をクリックします。
5. [仮想マシンのインポート] ダイアログボックスの [場所] で、ブランチ VPX SD-WAN ファイルを含むフォルダへのパスを指定します。

注: 圧縮ファイルを受け取った場合は、フォルダーへのパスを指定する前に、フォルダーにファイルを展開してください。

6. [インポート] をクリックします。
7. インポートした仮想アプライアンスが [仮想マシン] の下に表示されていることを確認します。
8. インポートした仮想マシンを右クリックし、[設定] をクリックします。

9. [設定] ウィンドウのナビゲーションペインの [ハードウェア] で、一覧の最初のネットワークアダプタを選択します。
10. [ネットワーク] ドロップダウンメニューで、[apa ネットワーク 1] を選択します。これは Apa1 の LAN インターフェイスです。
11. [**MAC** アドレスのスプーフィングを有効にする] ボックスが選択されていることを確認します。そうでない場合は、それを選択して変更を適用します。
12. [設定] ウィンドウのナビゲーションペインの [ハードウェア] で、一覧の 2 番目のネットワークアダプタを選択します。手順 10 と手順 11 を繰り返し、アダプタを Apa ネットワーク 2 に割り当てます。これは Apa2 の WAN インターフェイスです。

重要: 両方のネットワークアダプタに同じネットワークを構成しないでください。設定が正しくないと、パケットループが作成され、ネットワークがダウンする可能性があります。
13. 必要に応じて、仮想ハードディスクのサイズを変更します。
 - 「設定」 ウィンドウのナビゲーションウィンドウの「IDE コントローラ 0」で、「ハードドライブ」を選択します。
 - [編集] をクリックします。
 - 仮想ハードディスクの編集ウィザードの手順に従って、ウィザードの [展開] オプションを使用して、割り当てをサポートされているサイズの 1 つに増やします。
14. 必要に応じて、メモリサイズを変更します。
 - [設定] ウィンドウのナビゲーションウィンドウの [ハードウェア] で、[メモリ] を選択します。
 - サポートされているサイズの 1 つにメモリを調整して、RAM 領域を割り当てます。
 - [OK] をクリックします。
15. 必要に応じて、管理ポートを定義します。
 - 仮想マシンを右クリックし、[設定] をクリックします。
 - [設定] ウィンドウのナビゲーションペインの [ハードウェア] で、[** ハードウェアの追加 **] を選択します。
 - デバイスの一覧から [ネットワークアダプタ] を選択し、[追加] をクリックします。
 - 新しい仮想ネットワークに「プライマリネットワーク 3」という名前を付けます。
 - [**MAC** アドレスのスプーフィングを有効にする] チェックボックスがオンになっていることを確認します。
 - [OK] をクリックして変更を適用します。
16. ブランチリピータ **VPX** 仮想マシンを右クリックし、[接続] を選択します。
17. [ファイル] メニューの [操作] をクリックし、[開始] をクリックして仮想マシンを起動します。
18. SD-WAN VPX 仮想マシンを初めて起動すると、展開ウィザードが自動的に起動します。このウィザードでは、展開モード (インライン、WCCP、または PBR (仮想インライン)、または Web UI を使用してセットアップする) に関する質問をします。[**Web UI** を使用して設定] を選択します。次の画面で、apA インターフェイスの **IP**、ネットマスク、ゲートウェイを入力し、[**Finish**] をクリックします。

19. SD-WAN VPX が再起動したら、ブラウザベースの UI (ユーザー名:admin、パスワード: パスワード: パスワード) に、apa に割り当てた IP アドレスにログオンします。次に例を示します。<https://172.16.0.213>

その他の構成

構成手順の詳細については、物理 SD-WAN および SD-WAN アプライアンスのドキュメントを参照してください。

旧リリースへのアップグレード

物理 SD-WAN アプライアンスに組み込まれているソフトウェアアップグレードメカニズムは、SD-WAN VPX でもサポートされています。または、目的のリリースを実行する新しい仮想マシンをインストールすることもできます。

Installing SD-WAN VPX on the Microsoft Server 2012

April 15, 2021

インストール手順の実行

Microsoft サーバーで Hyper-V の役割を有効にし、VPX ファイルを抽出した後、HYPER-V マネージャーを使用して SD-WAN VPX をインストールできます。仮想マシンをインポートしたら、Hyper-V によって作成された仮想ネットワークに関連付けて、仮想 NIC を構成する必要があります。

注: 仮想アプライアンスの実行中は、設定を変更できません。仮想アプライアンスをシャットダウンしてから変更を行います。

Hyper-V Manager を使用して、**Microsoft Server 2012** に **SD-WAN VPX** をインストールするには

1. My Citrix からダウンロードした SD-WAN ディストリビューションを解凍します。
2. Hyper-V マネージャーを起動します。
3. ナビゲーションウィンドウの [**Hyper-V** マネージャー] で、SD-WAN VPX をインストールするサーバーを選択します。
4. [操作] メニューの [**** 仮想マシンのインポート**] をクリックします。
5. [仮想マシンのインポート] ダイアログボックスの [場所] ボックスで、SD-WAN VPX ファイルを含むフォルダへのパスを指定します。

注: 圧縮ファイルを受け取った場合は、フォルダーへのパスを指定する前に、フォルダーにファイルを展開してください。

6. [インポート] をクリックします。

7. インポートした仮想アプライアンスが [仮想マシン] の下に表示されていることを確認します。
8. インポートした仮想マシンを右クリックし、[設定] をクリックします。
9. [設定] ウィンドウのナビゲーションペインの [ハードウェア] で、一覧の最初のネットワークアダプタを選択します。
10. [ネットワーク] ドロップダウンメニューで、[Apa1 ネットワーク] を選択します。これは Apa1 の LAN インターフェイスです。
11. [**MAC** アドレススプーフィングを有効にする] ボックスが選択されていることを確認します。そうでない場合は、それを選択して変更を適用します。
12. [設定] ウィンドウのナビゲーションペインの [ハードウェア] で、一覧の 2 番目のネットワークアダプタを選択します。手順 10 と手順 11 を繰り返し、アダプタを Apa2 ネットワークに割り当てます。これは Apa2 の WAN インターフェイスです。

重要: 両方のネットワークアダプタに同じネットワークを構成しないでください。設定が正しくないと、パケットループが作成され、ネットワークがダウンする可能性があります。
13. 必要に応じて、仮想ハードディスクのサイズを変更します。
 - 「設定」ウィンドウのナビゲーションウィンドウの「IDE コントローラ 0」で、「ハードドライブ」を選択します。
 - [編集] をクリックします。
 - 仮想ハードディスクの編集ウィザードの手順に従って、ウィザードの [展開] オプションを使用して、割り当てをサポートされているサイズの 1 つに増やします。
14. 必要に応じて、メモリサイズを変更します。
 - [設定] ウィンドウのナビゲーションウィンドウの [ハードウェア] で、[メモリ] を選択します。
 - サポートされているサイズの 1 つにメモリを調整して、RAM 領域を割り当てます。
 - [OK] をクリックします。
15. 必要に応じて、管理ポートを定義します。
 - 仮想マシンを右クリックし、[設定] をクリックします。
 - [設定] ウィンドウのナビゲーションペインの [ハードウェア] で、[** ハードウェアの追加 **] を選択します。
 - デバイスの一覧から [ネットワークアダプタ] を選択し、[追加] をクリックします。
 - 新しい仮想ネットワークに「プライマリネットワーク 3」という名前を付けます。
 - [**MAC** アドレスのスプーフィングを有効にする] チェックボックスがオンになっていることを確認します。
 - [OK] をクリックして変更を適用します。
16. **SD-WAN VPX** 仮想マシンを右クリックし、[接続] を選択します。
17. [ファイル] メニューの [操作] をクリックし、[開始] をクリックして仮想マシンを起動します。

18. SD-WAN VPX 仮想マシンを初めて起動すると、展開ウィザードが自動的に起動します。このウィザードでは、展開モードに関する質問が表示されます。[**Web UI** を使用して設定] を選択します。次の画面で、apa インターフェイスの **IP** アドレス、ネットマスク、ゲートウェイを入力し、[**Finish**] をクリックします。
19. SD-WAN VPX が再起動したら、ブラウザベースの UI (ユーザー名:admin、パスワード:パスワード:パスワード) に、apa に割り当てた IP アドレスにログオンします。次に例を示します。<https://172.16.0.213>

追加の構成

構成手順の詳細については、物理 SD-WAN/SD-WAN アプライアンスのドキュメントを参照してください。

以前のリリースにダウングレードする

物理 SD-WAN/SD-WAN アプライアンスに組み込まれているソフトウェアアップグレードメカニズムは、SD-WAN/SD-WAN VPX でサポートされています。または、目的のリリースを実行する新しい仮想マシンをインストールすることもできます。

Linux-KVM プラットフォームでの **SD-WAN SE** 仮想アプライアンス (VPX) のインストール

April 15, 2021

1. Linux-KVM プラットフォーム用の SDWAN VPX-SE を設定するには、次の手順を実行します。
 - グラフィカル仮想マシンマネージャー (仮想マネージャー) アプリケーションを使用します。または
 - virsh プログラム Linux-KVM コマンドラインを使用します。
2. KVM Module および QEMU のような仮想化ツールを使って、適切なハードウェアにホスト Linux オペレーティングシステムをインストールする必要があります。ハイパーバイザー上で展開できる仮想マシン (VM) の数はアプリケーション要件および選択されたハードウェアにより異なります。
3. .qcow2 ファイルは、プロビジョニングされた NetScaler VPX インスタンスごとに一意である必要があります。これは、仮想マシンに接続されている仮想ハードディスク (VHD) です。

必須要件:

- 仮想化をサポートするベアメタルアプライアンスに Ubuntu 16.04 をインストールします。ベアメタルアプライアンスが仮想化をサポートしているかどうかを確認する手順を次に示します。
- AMD-V および Intel VT-X プロセッサに含まれているハードウェア仮想化機能を備えた 64 ビット x86 プロセッサ。
 - Linux ホストの CPU が仮想化をサポートしているかどうかをテストするには、ホスト Linux シェルプロンプトで次のコマンドを入力します。この出力は 0 より大きくする必要があります。

```
egrep -c '(vmx|svm)'/proc/cpuinfo
```


- 手順 2 の代わりに、「CPU チェッカー」(sudo apt-get インストール CPU チェッカー) と呼ばれるパッケージ/ツールをインストールし `kvm-ok`、次のコマンドを入力します。、出力は「KVM アクセラレーションを使用できます」でなければなりません。
- ホストハイパーバイザーで、`cat /proc/cpuinfo | grep flags` コマンドを実行し、次の CPU フラグがあるかどうかを確認します `popcnt`, `sse`, `sse2`, `pni`, `ssse3`, `sse4_1`, and `sse4_2`。
- 最小ハードウェア要件: SDWAN (ゲスト OS) には 4 つの vCPU、4 GB RAM、40 GB (VHD) が必要です。これを満たすことができるこれらの仕様を持つホストが必要です。
- ソフトウェア要件: Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-78-ジェネリック x86_64)

`qemu-kvm`、`libvirt-bin`、`virt-manager`: `sudo apt-get` インストール `qemu-kvm` `libvirt-bin` `virt-manager` ブリッジユーティリティをインストールします。このコマンドを実行して、必要なパッケージ/ソフトウェアをすべて取得します。

仮想マシンマネージャー (VMM) を使用して **SD-WAN VPX** アプライアンスをプロビジョニングします。

1. 仮想マシンマネージャーを開きます。[アプリケーション] > [システムツール] > [仮想マシンマネージャ] の順に選択し、[認証] ウィンドウでログオン資格情報を入力します。
2. VMM が開いたら、VMM が QEMU 仮想化に接続されていないことを示す QEMU/KVM が表示される必要があります。SD-WAN VPX-SE プロビジョニングの NIC 順序は、管理、LAN、および **WAN** の順でなければなりません。
3. [新しい仮想マシン] を選択します。
[新しい VMM の追加](#)
4. **VHD** を選択します。1 つのマシンで使用している VHD は共有できません。仮想マシンごとに固有の VHD が必要です。画像を参照し、ダウンロード先のパスを選択します。
5. RAM を 4,096 MB、CPU を 4 として提供します。
6. 必要に応じて仮想マシンに名前を付けて、[インストール] の前に [構成のカスタマイズ] を選択します。デフォルトでは、1 つの NIC が仮想マシンに選択されるように、ネットワーク選択オプションが表示されます。この設定では、**enp4s0f0** はホストマシンの管理ネットワークです。この NIC を使用する場合は、管理アクセス用にゲストとホスト間で同じ NIC を共有します。ソースモードは、仮想マシン間で共有されるため、ブリッジモードになります。
7. [完了] をクリックした後、[インストール前に設定をカスタマイズ] を選択して、さらに構成を行います。割り当てられている NIC の場合、この例では「enp4s0f0: macVTap」で、デバイスモデルを「**virtio**」として選択します。通信でサポートされているモデル。
8. 左下隅にある [ハードウェアの追加] で、LAN および WAN 用の NIC をさらに追加します。良好なパフォーマンスを得るには、パススルーとしてソースモードを使用することをお勧めします (下位 NIC を使用できるのは、1 つの仮想マシンのみであるため、仮想マシン間で共有することはできません)。LAN および WAN インターフェイスの場合は「パススルー」モードを使用し、デバイスモデルは「virtio」である必要があります。

9. インストールプロセスを開始するには、[インストールを開始] を選択すると、アプライアンスのコンソールが表示されます。
10. **management_ip** コマンドを使用して IP アドレスを設定します。

Linux-KVM ハイパーバイザープラットフォームインスタンスで SD-WAN アプライアンスを同じホスト上にデプロイする方法

同じホストに高可用性モードで SD-WAN アプライアンスを展開するには、SD-WAN VPX アプライアンス間で物理インターフェイスを共有する必要があります。たとえば、プライマリ仮想マシンの WANLink-1 には物理ハイパーバイザ (ホスト) の eth3 が使用されます。そのため、プライミアプライアンスが非アクティブになった場合、セカンダリアプライアンスは共有 MAC に対する ARP 要求に応答できるように、同じインターフェイスをセカンダリアプライアンスに使用する必要があります。

同じホスト上にある仮想マシン間で物理 NIC を共有する場合、KVM ネットワークに応じて使用できるソースモードは **MACVTAP Bridge** または Linux Bridge** です。

Linux ブリッジの使い方

- ホスト (KVM ハイパーバイザーレベル) で `brctl` を使用してブリッジを作成します。
- (`brctl` コマンドを使用して) 作成したブリッジに、必要な物理 NIC を関連付けます。
- ハイパーバイザーレベルで作成されたこれらのブリッジは、SD-WAN 仮想マシンに関連付ける必要があります。
- プライマリ仮想マシンとセカンダリ仮想マシンは、作成された Linux ブリッジに関連付けられます。

Linux ブリッジを作成して仮想マシンに関連付けるには、次の手順に従います。

- ブリッジの追加、`brctl addbr ha-brwan1`
 - 物理 NIC をブリッジに関連付けます `ha-brwan1`。 `brctl addif ha-brwan1 eth3`
 - ブリッジ「`ha-brwan1`」を SD-WAN-SE (仮想 WAN) に関連付ける (物理およびセカンダリの両方)
1. ネットワークインターフェイスを追加する場合は、[共有デバイス名の指定] として [ネットワークソース] を選択します。
 2. [ブリッジ名] で、作成したブリッジの名前を入力します。
 3. デバイスモデルは常に「`virtio`」でなければなりません。

LAN および WAN インターフェイスのブリッジを作成します。次のスナップショットは、仮想マシンマネージャーを使用して SDWAN-SE にインターフェイスを関連付ける方法を示しています。

注

これらの手順は、プライマリとセカンダリの両方の高可用性ノードが同じ KVM ハイパーバイザー/ホスト上に存在する場合にのみ実行する必要があります。高可用性ノードが異なるハイパーバイザーに存在する場合は、

MACVTAP: パススルーソースモードを使用できます。

MacVTap ブリッジモードタイプでの制限

MacVTap ブリッジモードタイプとして仮想マシンに関連付けられたインターフェイスでは、共有 MAC 通信に問題があります。SD-WAN 仮想 WAN は共有 MAC (AA: AA: 00:00: XX) を使用します。MacVTap ブリッジモードを使用すると、共有 Mac では ARP 解決は行われません。したがって、MacVTap ブリッジは推奨されません。

メモ

- 10.2.6 および 11.0.3 リリース以降では、SD-WAN アプライアンスのプロビジョニング時または新しい SD-WAN SE VPX の導入時に、デフォルトの管理者ユーザーアカウントパスワードを変更することが必須です。この変更は、CLI と UI の両方を使用して適用されます。
- システムメンテナンスアカウント (CBVWSSH) は、開発およびデバッグ用に存在し、外部ログイン権限はありません。このアカウントには、通常の管理ユーザーの CLI セッションからのみアクセスできます。

Google Cloud Platform に Citrix SD-WAN SE VPX をインストールする

April 15, 2021

GCP に Citrix SD-WAN SE VPX を展開すると、組織は GCP 上でホストされているブランチとアプリケーション間で、直接かつ安全性の高い接続を確立できます。これにより、データセンター経由のクラウドバインドトラフィックをバックホールする必要がなくなります。GCP で Citrix SD-WAN を使用する主な利点は次のとおりです。

- すべてのブランチサイトから GCP への直接接続を作成します。
- GCP への常時接続を確認します。
- セキュアな境界をクラウドに拡張します。
- シンプルで管理しやすいブランチネットワークへと進化します。

GCP 用 Citrix SD-WAN スタンダードエディションは、複数のネットワークリンクを単一のセキュアな論理仮想パスに論理的に結合します。このソリューションにより、組織は異なるサービスプロバイダーからのさまざまな接続を使用して、復元性の高い仮想 WAN パスを取得できます。これらの仮想パスはオーバーレイとして機能し、複数のリンクにわたって帯域幅容量をシームレスに集約し、メンバーリンクの一部がダウンしたり低下したりしても、一貫したユーザーエクスペリエンスを提供します。これは、Citrix SD-WAN のパケット単位の負荷分散および監視機能によって有効になります。

導入手順の概要

1. インスタンスをデプロイするリージョンを選択し、異なるサブネットに 3 つの VPC を作成します。

NIC	割り当て済みネットワーク
NIC 0 (デフォルト)	管理サブネット
NIC 1	LAN サブネット
NIC 2	WAN サブネット

注

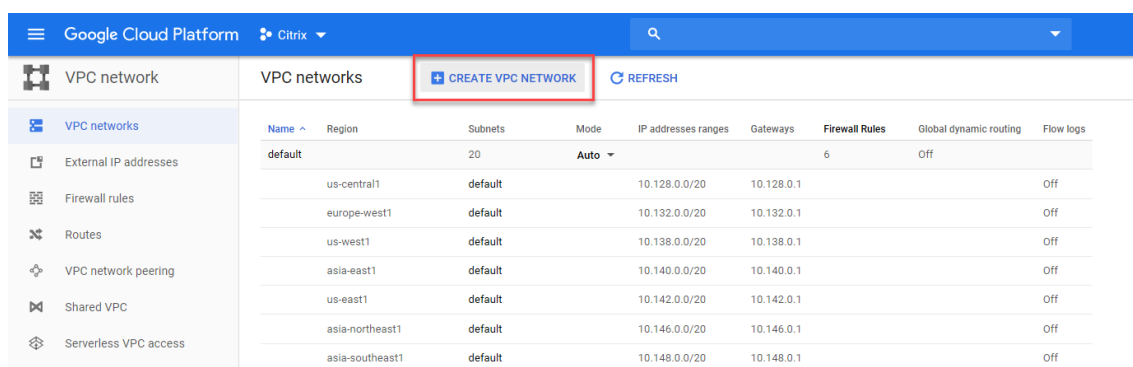
新しい管理サブネットを作成する場合は、ファイアウォールルールでポート 443 を許可します。

2. Citrix SD-WAN SE インスタンスを作成し、インターフェイスを VPC に関連付けます。
3. WAN サブネット VPC でファイアウォールルールを作成し、UDP ポート 4980 での入力を有効にします。これは、Citrix SD-WAN インスタンスによって仮想パスを作成するために使用されます。
4. LAN サブネット VPC 上にルートを作成して、LAN から生成されたすべてのトラフィックをインターセプトします。
5. 管理 IP アドレスを使用して、Citrix SD-WAN SE VPX にアクセスします。

VPC ネットワークを作成する

管理サブネット、LAN サブネット、および WAN サブネットに関連付けられる VPC ネットワークを作成します。イメージの作成時には、デフォルトのインターフェイスが使用可能ですが、これを管理インターフェイスとして使用できます。LAN と WAN サブネット用の 2 つの VPC ネットワークを作成します。

1. VPC ネットワークを作成するには、GCP コンソールで [VPC ネットワーク] > [VPC ネットワーク] > [VPC ネットワークを作成] に移動します。



2. 名前、説明、リージョンサブネット IP アドレスを指定し、LAN VPC ネットワークを作成します。

VPC network

- VPC networks
- External IP addresses
- Firewall rules
- Routes
- VPC network peering
- Shared VPC
- Serverless VPC access

Create a VPC network

Name

Description (Optional)

Subnets

Subnets allow you to create your own private cloud topology within Google Cloud. Click 'Automatic' to create a subnet in each region, or click 'Custom' to manually define the subnets. [Learn more](#)

Subnet creation mode

Custom Automatic

New subnet

Name

[Add a description](#)

Region

IP address range

[Create secondary IP range](#)

Private Google access

On
 Off

Flow logs

Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Stackdriver. [Learn more](#)

On
 Off

Dynamic routing mode

Regional
Cloud Routers will learn routes only in the region in which they were created

Global
Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router

DNS server policy (Optional)

3. 同様に、WAN VPC ネットワークを作成します。

Google Cloud Platform SD-WAN on GCP proofing

Create a VPC network

Name [?]
Name is permanent
sdwan-wan-vpc

Description (Optional)
SDWAN WAN VPC

Subnets
Subnets allow you to create your own private cloud topology within Google Cloud. Click 'Automatic' to create a subnet in each region, or click 'Custom' to manually define the subnets. [Learn more](#)

Subnet creation mode
Custom Automatic

New subnet

Name [?]
Name is permanent
sdwan-wan-subnet

[Add a description](#)

Region [?]
us-east1

IP address range [?]
192.168.20.0/24

[Create secondary IP range](#)

Private Google access [?]
 On
 Off

Flow logs
Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Stackdriver. [Learn more](#)
 On
 Off

Done Cancel

注

3つのVPCネットワークはすべて同じリージョンに存在する必要があります。

4. WANリンクパブリックIPを作成します。

Google Cloud Platform SD-WAN on GCP proofing

← Reserve a static address

Name ?
Name is permanent

Description (Optional)

Network Service Tier ?

Premium (current project-level tier, [change](#)) ?

Standard ?

IP version

IPv4

IPv6

Type

Regional

Global (to be used with Global forwarding rules. [Learn more](#))

Region ?
Region is permanent

Attached to ?
Some of the instances may be disabled due to the 'External IPs for VM instances' organisation policy. [Learn more](#)

Warning: Static IP addresses not attached to an instance or load balancer are billed at an hourly rate. [Pricing details.](#)

Equivalent [REST](#) or [command line](#)

5. インスタンスの作成後に、WAN パブリック IP を WAN サブネットに関連付けます。

Network interface

Network
testsdwan-wan-site

Subnetwork
test-wan-site

Internal IP
172.19.10.7

Internal IP type
Ephemeral

⌵ Show alias IP ranges

External IP ?
sdwan-wan-public-ip (35.229.70.175)

Network Service Tier ?
Premium

Done Cancel

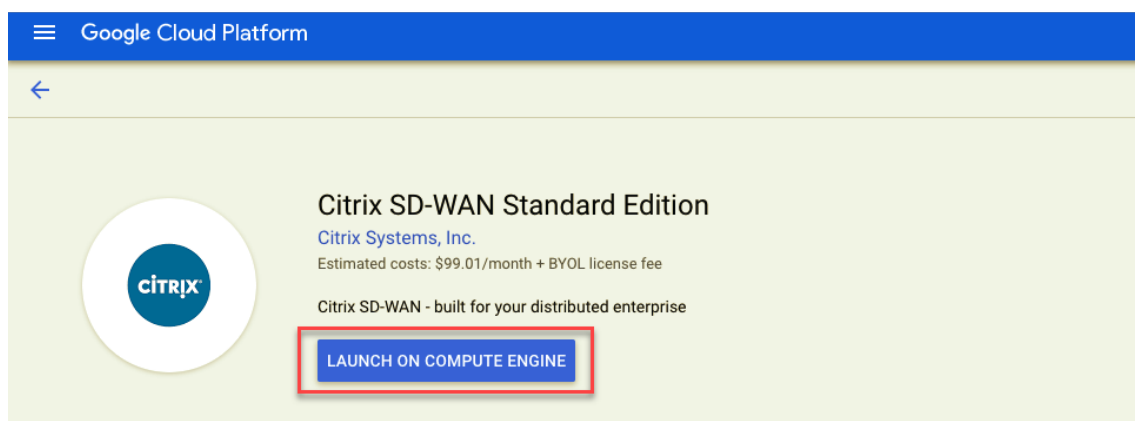
+ Add item

Citrix SD-WAN SE VPX インスタンスの作成

1. GCP Marketplace で **Citrix SD-WAN Standard Edition** を検索して開き、[コンピュートエンジンで起動] をクリックします。


The screenshot shows the Google Cloud Marketplace interface. At the top, there is a blue header with the Google Cloud Platform logo, a 'Select a project' dropdown, and a search icon. Below the header, a search bar contains the text 'citri'. The main content area displays search results for 'citri' in the Marketplace. On the left, there is a sidebar with filter options under 'Filter by', including 'TYPE' (Kubernetes apps (2), APIs & services (1), Virtual machines (2)), 'CATEGORY' (Analytics (1), Monitoring (2), Networking (4), Security (2)), and 'PRICE' (Free (3), BYOL (2)). The search results are listed as follows:

- Citrix Ingress Controller**
Citrix Systems, Inc. • Kubernetes apps
Kubernetes Ingress Controller for Citrix ADC
- Citrix ADC VPX - Customer Licensed**
Citrix Systems, Inc. • Virtual machines
Citrix ADC: Load Balancer, SSL VPN, WAF & SSO
- Citrix SD-WAN Standard Edition** (highlighted with a red box)
Citrix Systems, Inc. • Virtual machines
Citrix SD-WAN - built for your distributed enterprise
- Citrix ADC CPX**
Citrix Systems, Inc. • Kubernetes apps
High-performance, low-footprint, edge & service proxy for K8s
- BindPlane**
Blue Medora • APIs & services
Full-stack operations data collection for Stackdriver



Google Cloud Platform

←



Citrix SD-WAN Standard Edition

Citrix Systems, Inc.

Estimated costs: \$99.01/month + BYOL license fee

Citrix SD-WAN - built for your distributed enterprise

[LAUNCH ON COMPUTE ENGINE](#)

Runs on
Google Compute Engine

Type
[Virtual machines](#)
Single VM
BYOL

Last updated
8/7/19, 12:07 PM

Category
[Networking](#)
[Security](#)

Version
11.0

Overview

Citrix SD-WAN is a next-generation WAN Edge solution delivering flexible, automated, and secure connectivity and performance for cloud and virtual applications to ensure an always-on workspace experience. Quickly add new sites with zero-touch deployment and centrally monitor connections between remote sites and the cloud. SD-WAN provides an unparalleled experience for mission- and business-critical applications delivered from any location with comprehensive security that protects users, applications, and data across the branch, network, and cloud. Version 11.0 includes: Optimization of Office 365 traffic API integration with Zscaler API integration with GPCS Support for PPPoE and SD-WAN as a DNS forwarder Exporting of flow records to 3rd-party collectors using IPFIX Virtual Path QoS report shows how the entire virtual tunnel is performing Optimize the Microsoft Office 365 experience: Citrix SD-WAN ensures reliable connectivity to the nearest Office 365 front doors directly from branch locations. Citrix SD-WAN leverages APIs containing published Office 365 endpoint URLs and IP addresses to learn the closest front door locations to the users. This, in conjunction with the built-in stateful firewall, provides the ability to do local breakout of trusted, latency-sensitive Office 365 traffic over local ISPs for all your branches. For Office 365 customers who also use Microsoft Azure, you can push Office 365 policies and firewall rules to Citrix SD-WAN directly from Azure Virtual WAN using the Microsoft REST API. The SD-WAN appliances in the branches leverage them to optimize these preferences to route Office 365 traffic to the nearest Office 365 cloud front door. Key Benefits Provides the best digital workspace experience – whether Citrix, Microsoft Office 365, or any other SaaS. Offers advanced capabilities such as bi-directional QoS and link resiliency with failover in milliseconds.

[Learn more](#) 

About Citrix Systems, Inc.

Citrix

2. 必須の vCPU とメモリがデフォルトで選択されます。**GCP** リージョンを選択します。

注

GCP リージョンは、VPC ネットワークのリージョンと同じである必要があります。

Deployment name
citrix-sd-wan-standard-edition-3

Instance name ?
sdwan-instance

Machine type ?
4 vCPUs 15 GB memory Customise

Zone ?
us-east1-c

GCP Region ?
us-east1

Existing network1
Show Existing network1 options

Existing network2
Show Existing network2 options

Existing network3
Show Existing network3 options

Existing network4
Show Existing network4 options

Deploy


3. [既存のネットワーク **1**] リストから [デフォルト] を選択します。これは管理インターフェイスです。同様に、[既存のネットワーク **2**] と [既存のネットワーク **3**] で、それぞれ LAN サブネットと WAN サブネットを選択します。3つのネットワークすべてで **UseExNet** が選択されていることを確認し、[**Deploy**] をクリックします。

注


新しい管理サブネットを作成する場合は、ファイアウォールルールでポート 443 を許可します。

[Less](#)

Existing network2

Network 

sd-wan-lan


Subnetwork 

lan-subnet (192.168.10.0/24)


click on it to use useExNet2

[Less](#)

Existing network3

Network 

sd-wan-wan

Subnetwork 

wan-subnet (192.168.20.0/24)

click on it to use useExNet3

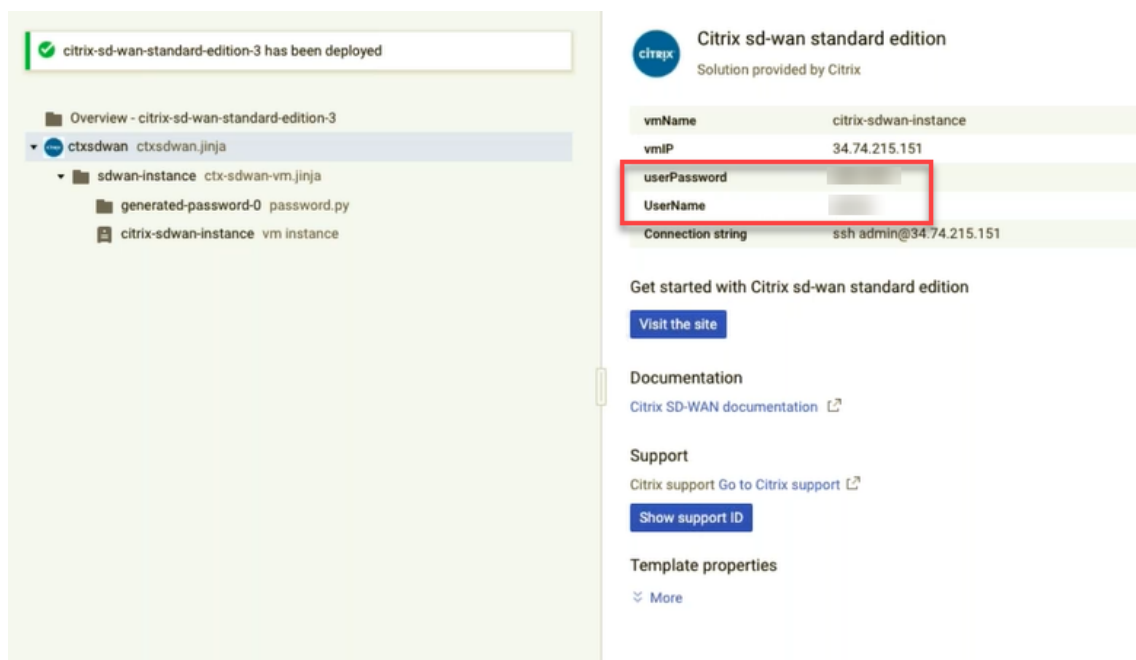
[Less](#)

Existing network4

[Show Existing network4 options](#)

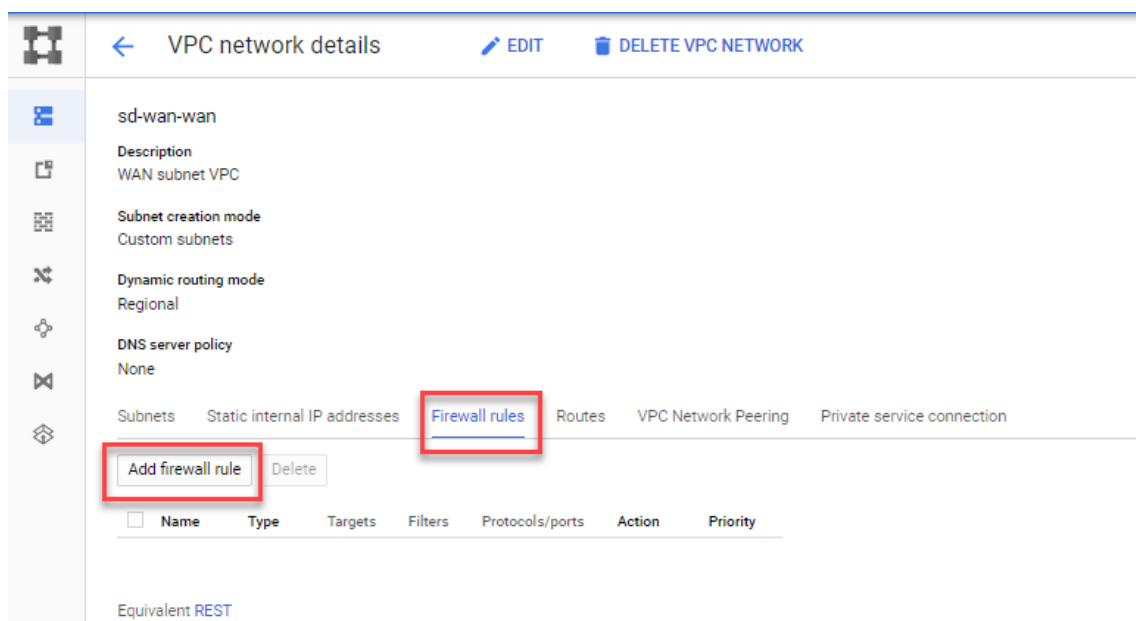
Deploy

4. SD-WAN SE VPX インスタンスがデプロイされた後。GCP によって提供されたデフォルトのユーザー名とパスワードを使用して SD-WAN SE VPX にログインします。



WAN サブネット VPC でファイアウォールルールを作成する

1. [**VPC ネットワーク**] > [**VPC ネットワーク**] > [**WAN サブネット VPC**] に移動します。[ファイアウォールルール] タブで、[ファイアウォールルールの追加] をクリックします。



2. UDP ポート 4980 のすべてのインスタンスへの入力を許可します。このポートは、オーバーレイネットワークを作成するために SD-WAN インスタンスによって使用されます。

← Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Name ⓘ
server-firewall1

Description (Optional)

Logs
Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. [Learn more](#)

On
 Off

Network ⓘ
sd-wan-wan

Priority ⓘ
Priority can be 0–65535 [Check priority of other firewall rules](#)
1000

Direction of traffic ⓘ
 Ingress
 Egress

Action on match ⓘ
 Allow
 Deny

Targets ⓘ
All instances in the network

Source filter ⓘ
IP ranges

Source IP ranges ⓘ
0.0.0.0/0

Second source filter ⓘ
None

Protocols and ports ⓘ
 Allow all
 Specified protocols and ports

top :

udp :

Other protocols

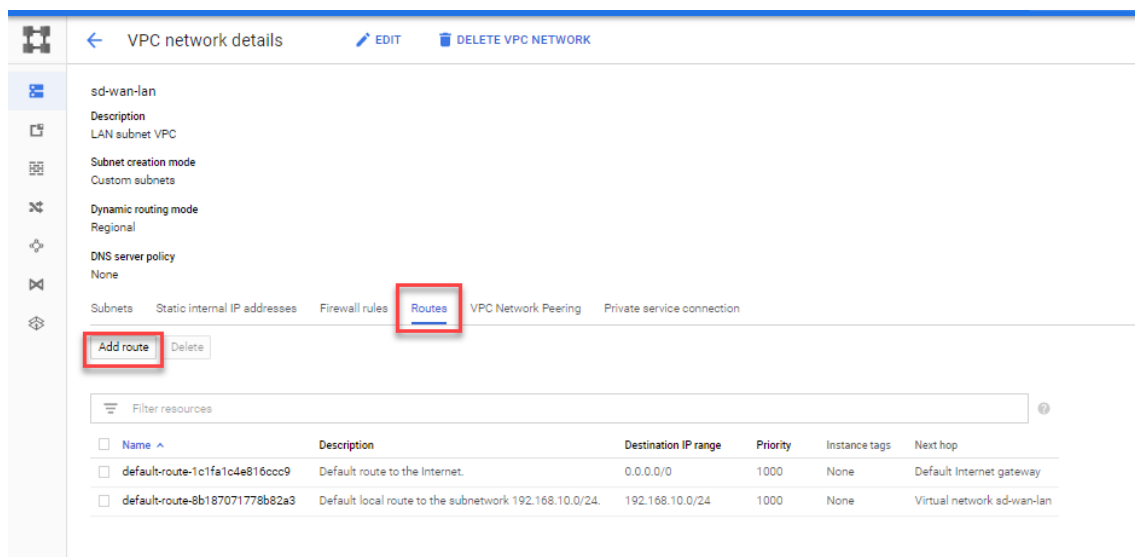
Disable rule

Equivalent [REST](#) or [command line](#)

LAN サブネット VPC でルートを作成する

LAN サブネット VPC 上にルートを作成して、LAN から生成されたすべてのトラフィックをインターセプトします。

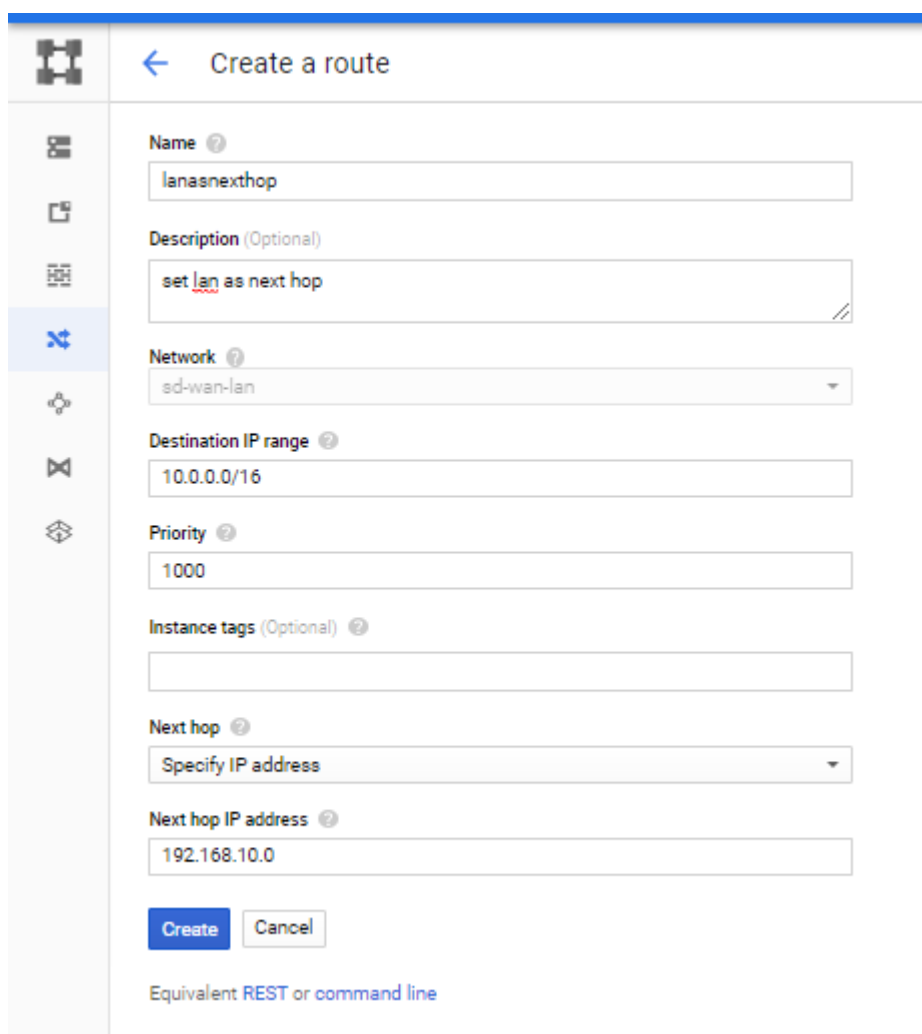
1. [VPC ネットワーク] > [VPC ネットワーク] > [LAN サブネット VPC] に移動します。[ルート] タブで、[ルートの追加] をクリックします。



The screenshot shows the 'VPC network details' page for 'sd-wan-lan'. The 'Routes' tab is selected and highlighted with a red box. Below the tab, there is an 'Add route' button, also highlighted with a red box. The table below shows the existing routes:

Name	Description	Destination IP range	Priority	Instance tags	Next hop
default-route-1c1fa1c4e816ccc9	Default route to the Internet.	0.0.0.0/0	1000	None	Default Internet gateway
default-route-8b187071778b82a3	Default local route to the subnetwork 192.168.10.0/24.	192.168.10.0/24	1000	None	Virtual network sd-wan-lan

2. 宛先 IP 範囲、もう一方の端の LAN ネットワークを入力します。[ネクストホップ] フィールドで、[IP アドレスの指定] を選択し、[ネクストホップ IP アドレス] に SD-WAN LAN インターフェイス IP を指定します。



← Create a route

Name ⓘ
lanasnexthop

Description (Optional)
set lan as next hop

Network ⓘ
sd-wan-lan

Destination IP range ⓘ
10.0.0/16

Priority ⓘ
1000

Instance tags (Optional) ⓘ

Next hop ⓘ
Specify IP address

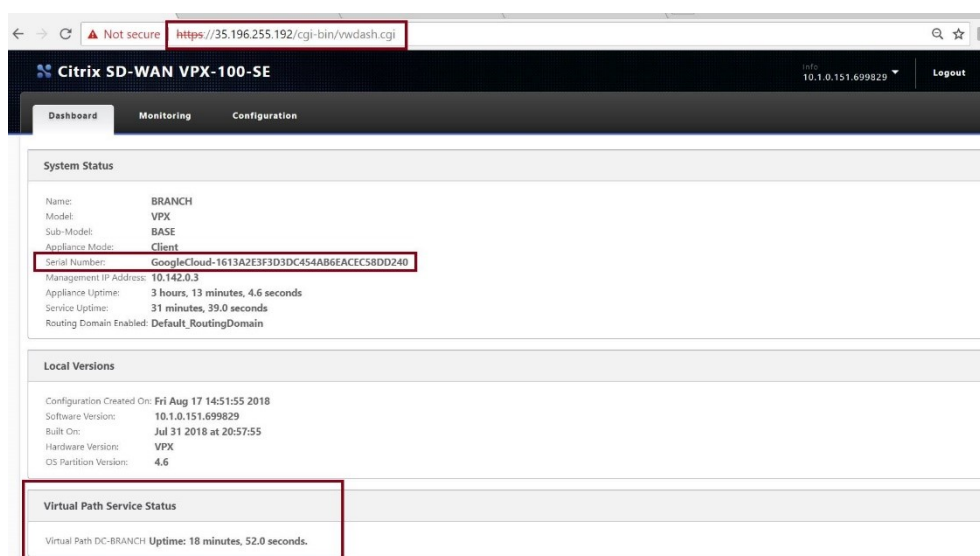
Next hop IP address ⓘ
192.168.10.0

Create Cancel

Equivalent REST or command line

SD-WAN SE VPX インスタンスへのアクセス

管理インターフェイスの IP アドレスを使用して、SD-WAN SE VPX インスタンスの GUI にアクセスします。GCP によって提供されるデフォルトのユーザー名とパスワードを使用して SD-WAN SE VPX にログインします。



メモ

- 10.2.6 および 11.0.3 リリース以降では、SD-WAN アプライアンスのプロビジョニング時または新しい SD-WAN SE VPX の導入時に、デフォルトの管理者ユーザーアカウントパスワードを変更することが必須です。この変更は、CLI と UI の両方を使用して適用されます。
- システムメンテナンスアカウント（CBVWSSH）は、開発およびデバッグ用に存在し、外部ログイン権限はありません。このアカウントには、通常の管理ユーザーの CLI セッションからのみアクセスできます。

Oracle クラウドインフラストラクチャ上の Citrix SD-WAN（テクニカルレビュー）

April 15, 2021

メモ

11.0.2 以降のテクニカルレビュービルドとして Oracle クラウドで Citrix SD-WAN が利用できるようになりました

あなたは、オンプレミス SD-WAN インスタンスとそれを接続し、したがって、Oracle クラウド内のリソースにアクセスするために、Oracle クラウドで SD-WAN インスタンスを使用することができます。

次のワークフローでは、SD-WAN インスタンスをプロビジョニングし、管理、LAN、および WAN 用の 3 つのサブネットワークを作成できます。

1. [オラクル・クラウド](#)にログインし、SD-WAN アプライアンスを導入するリージョンを選択します。資格情報を入力すると、以下の画面が表示されます。クラウドテナント ID を入力して開始してください。
2. 正常にログインできたら、[ネットワーク] > [仮想クラウドインスタンス]に移動します。この手順は、仮想ネットワークを作成するために必要です。この手順では、新しい仮想ネットワークをセットアップすることを前

提としています。既存の仮想ネットワークがある場合は、既存の仮想ネットワークを使用することもできます。そうでない場合は、ネットワークに適切な名前を指定します。次の 2 つのオプションがあります。

- 仮想ネットワークのみを作成します。デフォルトでは、インターネットへのアクセスは許可されません。この例では、このオプションを選択します。基本的に、これは LAN 環境です。
 - 仮想クラウドネットワークと関連リソースを作成する — このオプションはデフォルトでインターネットへのアクセスを許可し、トラフィックを許可/ブロックするには ACL を作成する必要があります。
3. 次の手順では、SD-WAN アプライアンスをホストするサブネットを作成します。ここでも、サブネットが使用可能な既存の仮想ネットワークを使用している場合は、その仮想ネットワークも使用できます。
 4. 上記の手順では、サブネットを作成し、たとえばこのサブネットにパブリック IP アドレスを許可しています。SD-WAN アプライアンスは、SD-WAN ブランチアプライアンスまたは MCN を使用して仮想パスを形成する必要があるため、パブリック IP は必須です。
 5. **SD-WAN** イメージの可用性: OCI オブジェクトストレージを使用して、SD-WAN イメージを専用のオブジェクトストレージバケットにアップロードします。SD-WAN イメージは、リリースバージョン 11.0.2 の downloads.citrix.com にあります。KVM イメージ、つまり 11.0.2.29_kvm.qcow2.gz を使用する必要があります。見つかったら、[オブジェクトストレージ] > [オブジェクトストレージ] の順に選択してオブジェクトストレージバケットを作成し、そのバケットに名前を割り当てます。
 6. 標準バケットまたはアーカイブバケットを選択できます。一度ティアを選択すると変更できなくなることに注意してください。また、Oracle で管理されたキーを使用するか、独自のキーを使用して、このバケットを暗号化することもできます。
 7. 次の手順では、オブジェクトストレージに qcow イメージをインポートしてカスタムイメージを作成し、それに名前を割り当てます。これを行うには、[計算] > [カスタムイメージ] に移動します。
 8. [import import image] をクリックして、イメージをオブジェクトストレージにインポートし、イメージがアップロードされるまで待ちます。アップロードしたら、画像に名前を割り当てます。これで、SD-WAN イメージのベースが形成され、同じイメージを使用して複数の SD-WAN インスタンスを作成できます。
 9. 次に、カスタムイメージに基づいて VM インスタンスを作成する必要があります。そのためには、[コンピュータ] > [インスタンス] に移動し、[インスタンスを作成] をクリックします。
 10. 前の手順で作成したカスタムイメージ (この場合は sdwan-PV) を選択します。

VM シェイプを適切なサイズと数の vNIC に変更します (この例では vm.standard2.4 を使用しました): 仮想マシンには 3 つ以上の vNIC があるだけでなく、他の仮想マシンを使用できます。
 11. VM サイズを選択したら、インスタンスをプロビジョニングする仮想ネットワークを選択します。この場合、仮想クラウドネットワークは dconoci と呼ばれます。

インスタンスを作成したら、管理パブリック IP アドレスを使用して SD-WAN 管理 GUI にログインできます。
 12. ログインすると、使用可能なネットワークアダプタは 1 つだけです。
 13. OSI ポータルに戻り、VM インスタンスで vNIC を作成します。SD-WAN インスタンスが機能するには、少なくとも 3 つのネットワークアダプタ/NIC が必要となるため、vNIC を作成します。さらに 2 つの NIC を作成

し、それらを VM に接続します。

14. 追加の vNIC をすべて作成したら、OCI ポータルからそれらを表示できます。
15. SD-WAN 管理 GUI にログインすると、仮想マシンを再起動すると、[ネットワークアダプタ] にすべての追加の vNIC が表示されます。
16. **SD-WAN MCN** およびクライアント設定: 標準の SD-WAN 設定手順に従って、2 つの SD-WAN インスタンス間に仮想パスを作成できます。

メモ

- 10.2.6 および 11.0.3 リリース以降では、SD-WAN アプライアンスのプロビジョニング時または新しい SD-WAN SE VPX の導入時に、デフォルトの管理者ユーザーアカウントパスワードを変更することが必須です。この変更は、CLI と UI の両方を使用して適用されます。
- システムメンテナンスアカウント (CBVWSSH) は、開発およびデバッグ用に存在し、外部ログイン権限はありません。このアカウントには、通常の管理ユーザーの CLI セッションからのみアクセスできます。

SD-WAN VPX Standard Edition AMI を AWS にインストールする

April 15, 2021

Citrix SD-WAN SE アプライアンスは、単一の仮想パスに複数のネットワークパスを結合します。仮想パスは監視されるため、重要なアプリケーション・パスは常に最適なパスを介してルーティングされます。このソリューションにより、お客様はアプリケーションをクラウドにデプロイし、複数のサービスプロバイダネットワークを活用して、エンドユーザーにアプリケーションをシームレスに配信できます。

Amazon Web Services (AWS) で SD-WAN SE-VPX を作成するには、他のインスタンスの作成と同じプロセスで、いくつかのインスタンスパラメータをデフォルト以外の設定に設定します。

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

AWS VPC に SD-WAN 仮想アプライアンスをインストールするには、AWS アカウントが必要です。AWS アカウントは、<http://aws.amazon.com/>で作成できます。SD-WAN は、AWS Marketplace で Amazon Machine Image (AMI) として利用できます。

注: Amazon は AWS ページに頻繁に変更を加えているため、以下の手順は最新ではない場合があります。

AWS で SD-WAN 仮想アプライアンス (AMI) をインスタンス化するには:

1. Web ブラウザで、<http://aws.amazon.com/>と入力します。
2. [**My Account** /コンソール] をクリックし、[**My Account**] をクリックして、**Amazon Web Services** サインインページを開きます。
3. 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。

Citrix SD-WAN SE アプライアンスは、次の AWS サービスインスタンスを提供します。

- VPC ダッシュボード — EC2 インスタンスなどの AWS オブジェクトによって移入された AWS クラウドの分離された部分
 - AWS で VPC を作成することで有効になります。次の設定手順を参照してください。
- 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
 - NetScaler SD-WAN AMI を作成することで有効になります。設定手順については、以下を参照してください。
 - CIDR — 継続的な IP アドレス範囲で構成されるクラスレスドメイン間ルーティングブロック。VPC を指定するために使用されます (16 リージョンを超えることはできません)。

SD-WAN ウェブインターフェイス

- Citrix (旧 NetScaler SD-WAN) の SD-WAN AMI を構成する

AWS で SD-WAN SE-VPX AMI をデプロイするための要件と制限を次に示します。

最小要件

- **AWS EC2** インスタンスタイプ: c4.2xlarge、c4.4xlarge、c5.xlarge、c5.2xlarge、c5.4xlarge、c5.4xlarge、c5.4xLarge、m5.4xLarge、m5.4xLarge
- 仮想 **CPU**: 8
- **RAM**: 15 ギガバイト
- ストレージ: 160 GB
- ネットワークインターフェイス: 最低 2 つ (管理が 1 つ、LAN/WAN に 1 つ)
- **BYOL** — 自分のライセンスとサブスクリプションの登録

11.3 リリース以降、Citrix SD-WAN は、M5 および C5 インスタンスのサポートを導入しました。香港やパリなどの新しい AWS リージョンは、M5 および C5 インスタンスのみをサポートします。

M5 および C5 インスタンスは、ハードウェアパフォーマンスが向上しており、要求の厳しいワークロード向けに設計されています。M5 および C5 インスタンスは、コアごとに M4 インスタンスよりも優れたコストパフォーマンスを提供します。

注:

M5 および C5 インスタンスは、11.3 以降のバージョンの新規プロビジョニングからのみサポートされます。M5 および C5 インスタンスを使用し続けるには、11.3 バージョンからダウングレードできません。M5 および C5 インスタンスは 11.3 より前のバージョンのファームウェアではサポートされていません。

制限事項

- AWS はインターフェイスのブリッジングを許可していないため、Fail-to-Wire はインターフェイスグループを設定するためのオプションではありません。
- 10.2.4/11.2.1 バージョンでプロビジョニングされたインスタンスでは、AMI はインスタンスタイプを M5/C5 に変更できません。

Citrix (旧 NetScaler SD-WAN) の SD-WAN (AWS)

指定されたアベイラビリティゾーンで AWS リージョンをデプロイする。仮想プライベートクラウド (VPC) インフラストラクチャ内では、SD-WAN Standard Edition AMI (Amazon マシンイメージ) が VPC ゲートウェイとしてデプロイされます。

- VPC プライベートには VPC ゲートウェイへのルートがあります。
- SD-WAN インスタンスには、直接接続用の AWS VGW (VPN ゲートウェイ) へのルートと、インターネット接続用の IGW (インターネットゲートウェイ) への別のルートがあります。
- 複数の WAN パスを同時に利用する異なるトランスポートモードを適用する、データセンター、ブランチ、クラウド間の接続。
- OSPF および BGP による自動ルート学習
- リンク障害の発生時にセキュリティの再ネゴシエーションが不要な複数のパスにまたがる 1 つの IPSec トンネル。

AWS では、SD-WAN AMI インターフェイスごとにサブネットと IP アドレスを定義する必要があります。使用されるインターフェイスの数は、デプロイメントの使用例によって異なります。VPX の LAN 側 (同じリージョン内) にあるアプリケーション・リソースに確実にアクセスすることが目的である場合、VPX は、eth0 の管理用、eth1 上の LAN 用、および eth2 上の WAN 用の 3 つのイーサネットインタフェースを使用して VPX を構成できます。

また、VPX を経由するトラフィックを他のリージョンまたはパブリックインターネットにヘアピン接続することが目的である場合、VPX は、2 つのイーサネットインタフェース (eth0 の管理用、もう 1 つは eth1 上の LAN/WAN 用) で構成できます。

AWS の SD-WAN SE AMI の概要

1. VPC ダッシュボードを使用して AWS で VPC を作成する

Amazon 仮想プライベートクラウドの使用を開始するには、VPC を作成する必要があります。VPC は AWS アカウント専用の仮想ネットワークです。

- ネットワーク内のデバイスを識別するために、CIDR ブロック/サブネットを定義し、VPC に割り当てます。たとえば、WAN、LAN、および管理サブネットを含むネットワークダイアグラムの例では、VPC に 192.168.100.0/22 が選択されています。192.168.100.0 – 192.168.103.255)-192.168.100.0/22
- VPC のインターネットゲートウェイを定義する – クラウド環境外と通信するため
- 定義された各サブネットのルーティングの定義-サブネットとインターネット間の通信用

- ネットワーク ACL (アクセスコントロールリスト) の定義-セキュリティ上の目的でサブネットとの間のトラフィックの流入/流出を制御する
- セキュリティグループの定義-ネットワークデバイスの各インスタンスとの間のトラフィックの流入/流出を制御します。

Citrix SD-WAN AMI を作成します。

- 詳細については、[EBS のベストプラクティス](#) およびを参照してください。 [Amazon EBS 暗号化に関する知っておくべきベストプラクティス](#)
- セキュリティグループを定義するには、ポリシーが次のようになっている必要があります。
 - アウトバウンド: すべてのトラフィックを許可する
 - インバウンド:
 - 管理 IP にアクセスするすべての IP アドレス/サブネットからの SSH。
 - AWS VPC (プライベート IP) からのすべてのトラフィック
 - Prem またはクラウドでホストされている Citrix SD-WAN ピアアプライアンスの WAN 側のパブリック IP からのすべてのトラフィック。
- EC2 インスタンスのネットワークインターフェイスを定義する
- EC2 インスタンスの Elastic IP アドレスの作成
- EC2 インスタンスとネットワークインターフェイスのセキュリティを定義する

SD-WAN Web インターフェイスに接続します。

- ライセンス
- ローカル変更管理を使用して識別をインストールする

AWS で VPC を作成する-仮想プライベートクラウド (VPC)

VPC を作成するには:

1. AWS マネジメントコンソールのツールバーから、[サービス] > [**VPC**] (ネットワーキングとコンテンツ配信) を選択します。
2. **VPC** を選択し、[**Create VPC**] ボタンをクリックします。
3. ネットワークダイアグラムに従って、名前タグ、CIDR ブロックを追加し、Tenancy = default、[はい、作成] をクリックします。

VPC のインターネットゲートウェイを定義する

VPC のインターネットゲートウェイを定義するには:

1. AWS マネジメントコンソールから、[インターネットゲートウェイ] > [インターネットゲートウェイの作成] を選択します。0.0.0.0/0 ルートに一致するインターネットゲートウェイトラフィックは、ルートテーブルで

設定できます。また、追加の構成のために SD-WAN AMI ウェブインターフェイスへの外部アクセスにも必要です。

2. IGW に Name タグを付けて、[はい、作成] をクリックします。
3. 新しく作成した IGW を選択し、[**Attach to VPC**] をクリックします。
4. 以前に作成した VPC を選択し、[**Yes, Attach**] をクリックします。

管理、**LAN**、および **WAN** を区別するために **VPC** のサブネットを定義します

VPC のサブネットを定義するには:

1. AWS マネジメントコンソールで、[サブネット] > [サブネットの作成] の順に選択し、管理、LAN、および WAN サブネットを作成します。定義済みのサブネットを使用して、SD-WAN 設定で定義された LAN、WAN、管理サブネットを区別します。
2. VPX の管理サブネットに固有の詳細を入力し、[**Yes, Create**] ボタンを使用して作成します。
 - 名前タグ: 異なるサブネットを識別するための名前 (管理、LAN、または WAN)
 - VPC: <the VPC previously created>
 - アベイラビリティゾーン:<set at discretion>
 - CIDR ブロック: 定義済みの名前 (管理、LAN、または WAN) に固有のサブネット。以前に定義された CIDR の小さいサブセットです。
3. Mgmt、LAN、および WAN ネットワークのサブネットを作成するまで、このプロセスを繰り返します。

管理サブネットのルートテーブルの定義

ルートテーブルを定義する手順は、次のとおりです。

1. AWS マネジメントコンソールで、[ルートテーブル] > [ルートテーブルの作成] を選択して、管理、LAN、および WAN サブネットのルートテーブルを作成します。
2. 管理サブネットの詳細を入力します
 - 名前タグ: 異なるサブネットを識別するための名前 (管理、LAN、または WAN)
 - VPC: 以前に作成された VPC
3. 新しく作成したルートテーブルがハイライト表示された状態で、[**Subnet Association**] > [**Edit**] を選択します。
4. 目的のサブネットとの関連付けを作成し、[**Save**] をクリックします。
5. 新しく作成したルートテーブルがハイライト表示された状態で、[ルート] > [編集] を選択します。
6. [**Add another route**] ボタン (管理サブネットおよび WAN サブネットにのみ必要) をクリックし、[保存] をクリックします。

- 目的地:0.0.0.0/0
- 対象: インターネットゲートウェイ (以前に定義された igw-xxxxxxx)

注

AWS は EC2 インスタンスにグローバルルートテーブルを提供しますが、NetScaler SD-WAN AMI はローカルルートテーブルを使用して、ユーザーが仮想パスへのトラフィック転送を制御できるようにします。

WAN サブネットのルートテーブルの定義

ルートテーブルを定義する手順は、次のとおりです。

1. AWS マネジメントコンソールで、[ルートテーブル] > [ルートテーブルの作成] を選択して、管理、LAN、および WAN サブネットのルートテーブルを作成します。
2. WAN サブネットの詳細を入力します。
 - 名前タグ: 異なるサブネットを識別するための名前 (管理、LAN、または WAN)
 - VPC: 以前に作成された VPC
3. 新しく作成したルートテーブルがハイライト表示された状態で、[**Subnet Association**] > [**Edit**] を選択します。
4. 目的のサブネットとの関連付けを作成し、[**Save**] をクリックします。
5. 新しく作成したルートテーブルがハイライト表示された状態で、[ルート] > [編集] を選択します。
6. [**Add another route**] ボタン (管理サブネットおよび WAN サブネットにのみ必要) をクリックし、[保存] をクリックします。
 - 目的地:0.0.0.0/0
 - ターゲット:<The Internet Gateway> (以前に定義された igw-xxxxxxx)

LAN サブネットのルートテーブルの定義

LAN サブネットのルートテーブルを定義するには、次の手順を実行します。

1. AWS マネジメントコンソールで、[ルートテーブル] > [ルートテーブルの作成] を選択して、管理、LAN、および WAN サブネットのルートテーブルを作成します。
2. LAN サブネットの詳細を入力します。
 - 名前タグ: 異なるサブネットを識別するための名前 (管理、LAN、または WAN)
 - VPC: 以前に作成された VPC
3. 新しく作成したルートテーブルがハイライト表示された状態で、[**Subnet Association**] > [**Edit**] を選択します。
4. 目的のサブネットとの関連付けを作成し、[**Save**] をクリックします。

注

SD-WAN を介して LAN 側のトラフィックをルーティングするには、SD-WAN LAN ルートテーブルで、ターゲット宛先を SD-WAN LAN インターフェイス ID として関連付けます。任意の宛先のターゲットをインターフェイス ID に設定できるのは、インスタンスを作成し、そのインスタンスにネットワークインターフェイスをアタッチした後だけです。

SD-WAN SE AMI の作成

EC2 インスタンスを作成するには:

1. AWS マネジメントコンソールのツールバーから、[サービス] > [**EC2 (コンピュート)**] を選択します。
2. **EC2** ダッシュボードツールバーを選択し、[インスタンス] > [**** インスタンスの起動 ****] を選択します。
3. [**AWS Marketplace**] タブを使用して SD-WAN Amazon Machine Image (AMI) を検索するか、[**マイ AMI**] タブを使用して所有または共有の SD-WAN AMI を探し、**Citrix NetScaler SD-WAN** スタンドアードエディションを見つけて [選択] をクリックします。
4. [続行] で選択を確定します。
5. [インスタンスタイプの選択] 画面で、準備中に識別された **EC2** インスタンスタイプを選択し、[次へ: インスタンスの詳細の設定] を選択します。
6. インスタンスの詳細を入力します (指定されていないものは未設定/デフォルトのままにしておく必要があります)。
 - インスタンス数:1
 - ネットワーク: 以前に作成した VPC を選択 >
 - サブネット: 以前に定義した管理サブネットを選択
 - パブリック IP の自動割り当て: 有効
 - [ネットワークインターフェイス] > [プライマリ IP]: 定義済みの管理 IP を入力します。
7. [次へ: ストレージの追加] をクリックします。

注

EC2 インスタンスを Mgmt サブネットに関連付けて、最初の EC2 インターフェイス (eth0) を SD-WAN 管理インターフェイスに関連付けます。eth0 が SD-WAN 管理インターフェイスに関連付けられていない場合、リポート後接続が失われます。1。

8. ルートストレージについて次の情報を入力します。
 - ボリュームタイプ: 汎用 (SSD) GP2
9. 次に、[次へ: タグインスタンス] を選択します。
10. デフォルトの Name Tag に値を指定して、EC2 インスタンスに名前を付けます。必要に応じて、他の必要なタグを作成します。

11. 次に、[**次へ: セキュリティグループの構成**] を選択します。
12. 既存のセキュリティグループを選択するか、セキュリティグループを作成します。
 - 生成されるデフォルトのセキュリティグループには HTTP、HTTPS、SSH が含まれます。
[**Add Rule**] ボタンをクリックして、さらに 2 つを追加します。
 - ソース付きすべての ICMP: カスタム 0.0.0.0/0
 - ポート範囲:4980、ソース: カスタム UDP ルール <known IP addresses from partner SD-WAN>
13. [**** 確認して起動 ****] を選択します。
14. 確認を完了したら、[**Launch**] を選択します。
15. [**Key Pair**] ポップアップで、既存のキーペアを選択するか、新しいキーペアを作成し、[**Launch Instance**] を選択します。

重要

新しいキーペアが作成された場合は、必ずダウンロードして安全な場所に保管してください。

16. Citrix SD-WAN SE AMI を正常に起動する必要があります。

注

セキュリティグループは、EC2 インスタンスのトラフィックを制御する一連のファイアウォールルールです。インバウンドルールとアウトバウンドルールは、EC2 起動中および起動後に編集できます。各 EC2 インスタンスには、セキュリティグループが割り当てられている必要があります。また、各ネットワークインターフェイスには、セキュリティグループが割り当てられている必要があります。複数のセキュリティグループを使用して、個別のルールセットを個々のインターフェイスに適用できます。AWS によって追加されたデフォルトのセキュリティグループでは、VPC 内のトラフィックのみが許可されます。

NetScaler SD-WAN AMI とそのインターフェイスに割り当てられたセキュリティグループでは、SSH、ICMP、HTTP、および HTTPS を受け入れる必要があります。WAN インターフェイスに割り当てられたセキュリティグループも、ポート 4980 で UDP を受け入れる必要があります（仮想パスサポートの場合）。セキュリティグループ設定情報の詳細については、AWS のヘルプを参照してください。

重要

新しいアカウントからプロビジョニングした場合は 2 時間待ってから再試行してください

17. **AWS** コンソール:**EC2** ダッシュボードに戻ります。
18. ツールバーの [ネットワークとセキュリティ] で [**** ネットワークインターフェイス ****] を選択し、[**管理**] インターフェイスをハイライトし、[**名前**] タグを編集して、インターフェイスに便利な名前を付けます。
19. 次に、[**ネットワークインターフェイスの作成**] をクリックして LAN インターフェイスを作成します。
 - 説明: <a user-defined description for the interface>
 - サブネット:<the subnet previously defined for the interface>
 - プライベート IP: <the private IP for the interface previously defined during preparation>
 - セキュリティグループ:<the appropriate security group for the interface>

20. を繰り返して [ネットワークインターフェイスの作成] をクリックして、WAN インターフェイスを作成します。
21. 新しい各インターフェイスの Name タグを編集し、便利な名前を付けます。
22. ** 管理インタフェースを強調表示し **、[アクション] > [ソース/宛先を変更] を選択します。オンにすると、ソース/宛先が無効になります。チェックボックスをオンにし、[保存] を選択します。
23. LAN および WAN インターフェイスについても繰り返します。
24. この時点で、すべてのネットワークインターフェイス（管理、**LAN**、**WAN**）には、名前、プライマリプライベート IP が設定され、送信元/宛先に対して無効になります。属性をチェックしてください。管理だけだネットワークインターフェイスには、パブリック IP が関連付けられています。

重要

ソース/宛先を無効にします。[Check] 属性を使用すると、インターフェイスが EC2 インスタンス宛ではないネットワークトラフィックを処理できません。NetScaler SD-WAN AMI は、ネットワークトラフィックの移動間として機能するため、ソース/宛先です。正しく動作するには、チェック属性を無効にする必要があります。

これらのネットワークインターフェイスに定義されたプライベート IP は、最終的には SD-WAN 設定の IP アドレスと一致する必要があります。このサイトノードの SD-WAN 構成で、そのインターフェイスが複数の WAN リンク IP に関連付けられている場合は、WAN ネットワークインターフェイスに対して複数のプライベート IP を定義する必要があります。これは、必要に応じて WAN インターフェイスのセカンダリプライベート IP を定義することで実現できます。

25. **EC2** ダッシュボードツールバーから、[インスタンス] を選択します。
26. 新しく作成したインスタンスを強調表示し、[アクション] > [ネットワーク] > [ネットワークインターフェイスのアタッチ] の順に選択します。
27. 最初に LAN ネットワークインターフェイスを接続し、次に WAN ネットワークインターフェイスを SD-WAN SE AMI に接続します。

注

管理、LAN、および WAN をこの順序でアタッチすると、SD-WAN AMI の eth0、eth1、eth2 に接続されます。これは、プロビジョニングされた AMI のマッピングと一致し、AMI の再起動時にインターフェイスが正しく再割り当てされないようにします。

28. **EC2** ダッシュボードツールバーから、[**Elastic IP (EIP)**] を選択し、[新しいアドレスを割り当て] をクリックします。
29. [**Allocate**] をクリックして新しい IP アドレスを割り当てて、[新しいアドレス] 要求が成功したら [**Close**] をクリックします。
30. 新しい EIP を強調表示し、[アクション] > [アドレスの関連付け] を選択して、EIP を Mgmt に関連付けます。インターフェイスを右クリックし、[関連付け] をクリックします。

- リソースタイプ:<network interface>
- ネットワークインタフェース: 以前に作成された >
- プライベート IP: <previously defined private IP for Mgmt>

31. このプロセスを繰り返して、別の新しい EIP を WAN インターフェイスに関連付けます。

SD-WAN SE AMI の設定-SD-WAN ウェブ管理インターフェイス

SD-WAN SE AMI を設定するには、次の手順を実行します。

1. この時点で、ウェブブラウザを使用して SD-WAN SE AMI の管理インターフェイスに接続できる必要があります。
ます。
2. 管理に関連付けられた **Elastic IP (EIP)** を入力します。インターフェイス。セキュリティ証明書が認識されない場合は、セキュリティ例外を作成できます。
3. 次の認証情報を使用して SD-WAN SE AMI にログインします。
 - ユーザー名: *admin*
 - パスワード: <aws-instance-id> (例; i-00ab111abc2222abcAbc22abcabcAbc22Abc

注

管理の場合インターフェイスに到達できません。次の点を確認してください。

- 1 - EIP が Mgmt. インターフェイスに正しく関連付けられていることを確認します。

- EIP が ping に応答することを確認する
- 管理インターフェイスのルートテーブルにインターネットゲートウェイルート (0.0.0.0/0) が含まれていることを確認します
- 管理インターフェイスセキュリティグループが HTTP/HTTP/ICMP/SSH を許可するように設定されていることを確認してください。

リリース 9.1 SD-WAN AMI 以降、ユーザーは *ssh admin@<mgmt>* を使用して SD-WAN AMI コンソールにログインすることもできます。EIP>。EC2 インスタンスのキーペアがユーザーの SSH キーチェーンに追加されていることを前提としています。

4. SD-WAN SE 独自のライセンス (**BYOL**) **AMI** の場合、ソフトウェアライセンスをインストールする必要があります。
 - SD-WAN Web インターフェイスで、[構成] > [アプライアンスの設定] > [ライセンス] に移動します。
 - [ライセンス設定: このアプライアンスのライセンスのアップロード] から、[ファイルの選択] を選択し、**SD-WAN SE AWS** ライセンスを参照して開き、[アップロードとインストール] をクリックします。
 - アップロードに成功すると、ライセンスステータスは状態: ライセンス済みと表示されます
5. 新しい AMI に適切なデータ/時刻を設定します。

- SD-WAN Web インターフェイスで、[構成] > [システムメンテナンス] > [日付/時刻の設定] に移動します。
- **NTP**、日付/時刻設定、またはタイムゾーンを使用して正しい日付と時刻を設定する **

注

SD-WAN SE AMI 仮想 WAN サービスは、アプライアンスパッケージ (ソフトウェア + 構成) が AMI にインストールされるまで無効のままになります。

SD-WAN SE AMI を SD-WAN 環境に追加する

SD-WAN 環境に SD-WAN AMI を追加するには、次の手順を実行します。

1. **SD-WAN** 環境の **SD-WAN** センターまたはマスターコントロールノードに移動します **。
2. ** 構成エディタを使用して新しいサイトノードを追加します **。
 - サイトの追加: モデル VPX、モード: クライアント
 - インターフェイスグループ: AWSLAN = eth1、awSwan = eth2 (信頼できない)
 - 仮想 IP アドレス: 192.168.100.5 = AWSLAN、192.168.101.5 = AWSLAN 仮想 IP アドレスが設定されている AWSWAN の場合、SD-WAN は、LAN サブネット 192.168.100.5/24 を SD-WAN 環境へのローカルルートとしてアドバタイズします ([接続] > [AWSNode] > [ルート] を参照)。
WAN リンク:
 - アクセスタイプパブリックインターネット AWSBR-WAN、クライアントノードの場合はパブリック IP を自動検出するか、MCN ノードの場合は WAN リンクの EIC を設定します。アクセスインターフェイス: AWSan 192.168.101.5 ゲートウェイ 192.168.101.1 (#.#.#.1 は通常 AWS リザーブドゲートウェイです)。
3. 設定エディタで、[接続] > [DC] > [仮想パス] > [**DC-AWS**] > [パス] でパスの関連付けを確認します。

注

仮想パスは、管理インターフェイスに直接接続するのではなく、AMI WAN インターフェイス全体で使用され、ソフトウェアおよび設定の更新を SD-WAN AMI にプッシュします。

プライベート IP アドレスは、設定エディタのすべての WAN リンク IP の EC2 WAN ネットワークインターフェイスで定義する必要があります。これは、必要に応じて、ネットワークインターフェイスに 1 つ以上のセカンダリプライベート IP を定義することで実現できます。

重要

AWS EC2 ダッシュボードで割り当てられたマッピングを呼び出して、管理を eth0、LAN を eth1、WAN を eth2 として割り当てます。

Amazon は、各サブネット CIDR ブロック内の最初の 4 つの IP アドレスと最後の IP アドレスを再サービスし、インスタンスに割り当てることはできません。たとえば、CIDR ブロック 192.168.100.0/24 のサブネットでは、次の 5 つの IP アドレスが予約されています。

1 - 192.168.100.0: ネットワークアドレス

- 192.168.100.1: VPC ルーター用に AWS によって予約された
- 192.168.100.2: DNS サーバー用に AWS によって予約された
- 192.168.100.3: 将来の使用のために AWS によって予約済み
- 192.168.100.255: VPC でサポートされていないネットワークブロードキャストアドレス

4. 新しく作成した SD-WAN 構成を保存してエクスポートし、変更管理受信トレイにエクスポートします。
5. MCN 変更管理に移動して変更管理プロセスを実行し、最新の設定を SD-WAN 環境にプッシュし、新しく追加された AWS ノードとそれに関連付けられたサブネット（仮想インターフェイス）を既存のすべての SD-WAN ノードに通知します。既存の SD-WAN 環境で使用されている現在のソフトウェアと一致する変更準備段階で、VPX 固有のソフトウェアパッケージを必ずアップロードしてください。
6. [**Change Management**] ページから、アクティブリンクを使用して、新しい AWS ノード用に特別に生成されたパッケージをダウンロードします。
7. 管理インターフェイスに割り当てられた EIP を使用して、SD-WAN SE AMI の管理インターフェイスに戻ります。
8. [構成] > [システムメンテナンス] > [ローカル変更管理] に移動します。
9. [**Choose File**] をクリックして、最近ダウンロードしたアクティブな AWS ソフトウェア/設定パッケージを参照してアップロードします。
10. ローカル変更管理が正常に終了した後、Web インターフェイスは、**Virtual WAN** サービスを無効にした状態で、インストールされている最新のソフトウェアで自動更新する必要があります。
11. [SD-WAN SE AMI] セクションで、[設定] > [仮想 WAN 有効/無効/パージフローの順に移動し、[有効] ボタンを使用してサービスを有効にします。
12. WAN インターフェイスでの接続に成功すると、SD-WAN は、[モニタリング] > [統計] > [パス] ページに [良好なパス状態] を報告します。

トラブルシューティング

SD-WAN アクセスインターフェイス設定では、正しいプライベート Web ゲートウェイ (IWG) IP を使用する必要があります。

- 設定エディターで誤った IWG を使用して AWS サイト（仮想 IP アドレスと正しいゲートウェイ）の WAN リンクを定義すると、仮想パスの確立に失敗します。
- IWG が正しく設定されていないかどうかを確認する簡単な方法は、**SD-WAN ARP** テーブルをチェックすることです。

パケットキャプチャツールに組み込まれた SD-WAN は、適切なパケットフローを確認するのに役立ちます

1. SD-WMA AMI の [設定] > [システムメンテナンス] > [診断] ページに移動します。

2. [パケットキャプチャ] タブを選択し、次の設定を行い、[キャプチャ] をクリックします。
 - インターフェイス: WAN インターフェイスに関連付けられた eth2 でキャプチャします。
3. Web ページのキャプチャ出力には、WAN VIP /プライベート IP を送信元として SD-WAN SE AMI から出る UDP プロブパケット、MCN に使用されるスタティックパブリック IP の宛先、MCN スタティックパブリック IP の送信元とローカル VIP/ の宛先を含む UDP プロブパケットが示されている必要があります。プライベート IP (IWG が NAT したもの)

注

これは、通常、VPC に割り当てられた CIDR ブロックの外部に IP アドレスが作成された場合に発生します。

メモ

- 10.2.6 および 11.0.3 リリース以降では、SD-WAN アプライアンスのプロビジョニング時または新しい SD-WAN SE VPX の導入時に、デフォルトの管理者ユーザーアカウントパスワードを変更することが必須です。この変更は、CLI と UI の両方を使用して適用されます。
- システムメンテナンスアカウント (CBVWSSH) は、開発およびデバッグ用に存在し、外部ログイン権限はありません。このアカウントには、通常の管理ユーザーの CLI セッションからのみアクセスできます。

Azure への Citrix SD-WAN VPX Standard Edition のインストール-リリースバージョン 9.3

April 15, 2021

Azure 用 Citrix SD-WAN スタンダードエディションは、複数のネットワークリンクを 1 つの安全な論理仮想パスに論理的に結合します。このソリューションにより、組織は、ブロードバンド、MPLS、4G/LTE、Satellite、ポイントツーポイントリンクなど、さまざまなサービスプロバイダーからの接続を使用して、高い復元性の仮想 WAN パスを取得できます。Azure 用 SD-WAN 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への直接セキュアな接続を確立でき、データセンター経由のクラウドバインドトラフィックをバックホールする必要がなくなります。Azure で SD-WAN を使用する利点のいくつかを次に示します。

- すべての場所から Azure への直接接続を作成します。
- Azure への常時接続を確実にします。
- セキュアな境界をクラウドに拡張します。
- シンプルで管理が容易なブランチネットワークへと進化します。

トポロジ-Azure の SD-WAN

Citrix SD-WAN Standard Edition は、Azure のゲートウェイデプロイモードでのみデプロイできます。Azure の SD-WAN の WAN 側インターフェイスには、パブリック IP アドレス (静的/動的) を割り当てる必要があります。

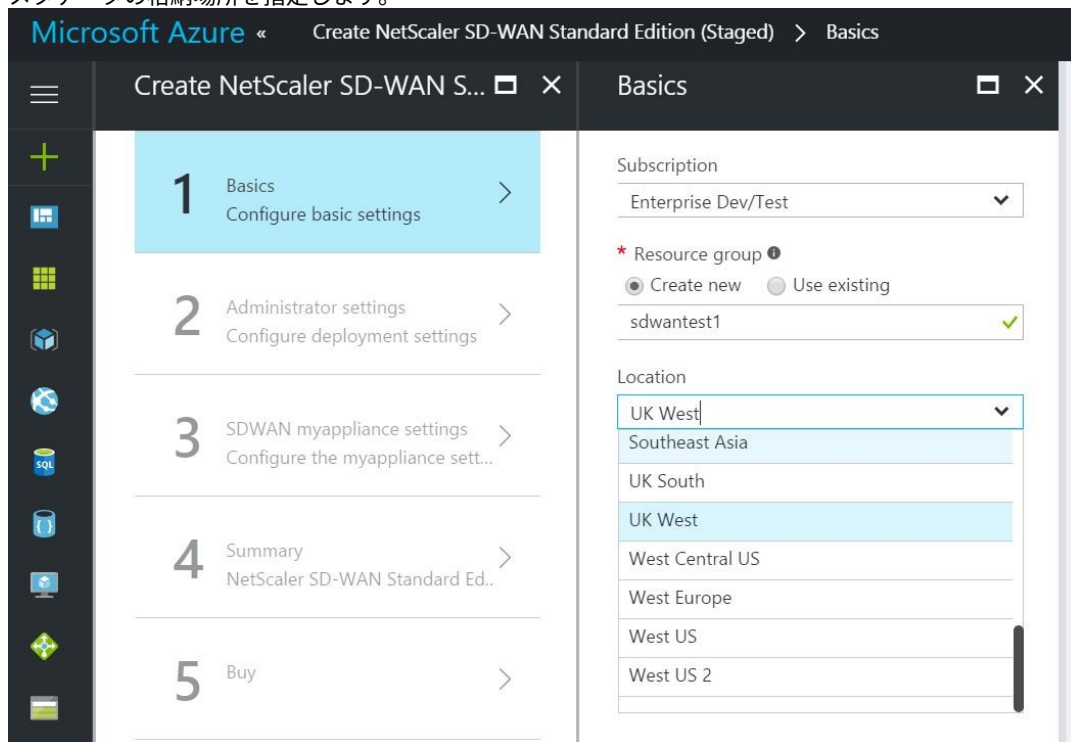
使用例

Azure VM は指定されたリージョン内にデプロイされ、MPLS、インターネット、または 4G/LTE を介して複数のブランチロケーションに接続できます。仮想ネットワーク (VNET) インフラストラクチャ内で、SD-WAN スタンダードエディション VHD (仮想ハードドライブ) がゲートウェイモードで展開されます。VNET には Azure ゲートウェイへのルートがあります。SD-WAN インスタンスには、インターネット接続用の Azure Gateway へのルートがあります。データセンター、支店、クラウド間の接続は、複数の WAN パスを同時に利用するさまざまな転送方法を使用することによって実現されます。

Microsoft Azure で Citrix SD-WAN Standard Edition を展開するには

1. Web ブラウザで、<https://portal.azure.com/>と入力します。マイクロソフトの Azure アカウントにログインします。SD-WAN Standard Edition を検索してください。
2. 検索結果ウィンドウで、次の解決策を選択します。
3. 説明を確認し、選択したソリューションが正しいことを確認したら、[作成] をクリックします。
4. [作成] をクリックすると、Azure での仮想マシンの作成に必要な詳細の入力を求めるウィザードが表示されます。最初の段階で、ソリューションをデプロイするリソースグループを選択します。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。リソースグループを定義する際に考慮すべき重要な点は、次のとおりです。
 - グループ内のすべてのリソースは、ライフサイクルを共有する必要があります。それらをまとめて展開、更新、および削除します。
 - データベースサーバーなどの 1 つのリソースが別のデプロイサイクルに存在する必要がある場合は、別のリソースグループに属することができます。
 - 各リソースは、1 つのリソースグループにのみ存在することができます。
 - リソースは、いつでも別のリソースグループに追加または削除できます。
 - リソースを 1 つのリソースグループから別のリソースグループに移動できます
 - リソースグループには、異なるリージョンに存在するリソースを含めることができます。
 - リソースグループを使用して、管理アクションのアクセス制御の範囲を設定できます。
 - リソースは、他のリソースグループのリソースと対話できます。この相互作用は、2 つのリソースが関連しているがライフサイクルを共有しない場合に一般的です (データベースに接続している Web アプリなど)。次の図で、[新規作成] を選択します。

[場所] で、ソリューションをデプロイするリージョンを選択します。リソースグループを作成するときは、そのリソースグループの場所を指定する必要があります。リソースグループには、作成するリソースに関するメタデータが格納されます。したがって、リソースグループの場所を指定するときは、そのメタデータの格納場所を指定します。



5. 仮想マシンの名前を指定します。ユーザ名と強力なパスワードを選択します。パスワードは大文字、特殊文字で構成され、9文字以上である必要があります。[OK] をクリックします。
6. イメージを実行するインスタンスを選択します。現在、Standard_D3_V2 と Standard_D4_V2 がサポートされている。入力によって集約された 200 Mbps を実現する場合は、インスタンスタイプとして **Standard_D4_V2** を選択します。
7. イメージを選択したら、ストレージアカウントを選択します。既存のストレージアカウントをお持ちの場合は、そのアカウントを選択できます。この手順では、次の図に示すようにストレージアカウントを作成します。ストレージアカウントは、オペレーティングシステムの一時ディスクおよびより多くのデータディスクの VHD を格納します。
8. 仮想マシンのパブリック IP を選択します。これは、ソリューションの WAN 側インターフェイスに割り当てられます。静的 IP またはダイナミック IP のいずれかを選択できます。ただし、静的 IP を選択することをお勧めします。ここでアプライアンスに割り当てられたパブリック IP は Azure によって提供され、SD-WAN VM の仮想 IP となり、マスターコントロールノードとの通信に使用されます。
9. IP アドレスを割り当てたら、DNS ラベルを割り当てます。この DNS ラベルは、SD-WAN 仮想マシンを一意

に識別できる必要があります。

10. 新しい仮想ネットワーク (VNET) を作成するか、既存の VNET を使用します。この手順では、SD-WAN VM のインターフェイスに割り当てるサブネットを選択するため、これは展開にとって最も重要な手順です。
11. これで、仮想マシン内の各インターフェイスに必要なサブネットを割り当てることができます。サブネットの割り当て順序は、それぞれ WAN、LAN、および管理です。必要に応じてを選択し、「**OK**」をクリックします。

NIC	割り当て済みネットワーク
NIC 0 (デフォルト)	管理サブネット
NIC 1	LAN サブネット
NIC 2	WAN サブネット

12. すべての構成の詳細を確認し、「**OK**」をクリックします。
13. 前の手順で提供したすべての構成が検証され、適用されます。正しく設定した場合は、次のように検証がメッセージを通過したことがわかります。「**OK**」をクリックします。
14. 検証に合格したら、「**購入**」をクリックして画像を購入し、作成します。
15. 購入後、展開が開始され、通知セクションでステータスを確認できます。
16. デプロイを作成するリソースグループに移動すると、展開の詳細を確認できます。
17. デプロイが成功したら、設定した資格情報を使用して、パブリック IP を使用して GUI にアクセスしてみてください。
18. アップデートソフトウェアオプションを選択して、VPX アプライアンスの最新 9.2.147 ソフトウェアイメージを適用して、ソフトウェアを最新のイメージにアップグレードします。これは 1 回限りの操作であり、イメージを初めて起動するときに必要です。
19. ソフトウェアの更新後は、パブリック IP を使用して仮想パスの設定に使用されるため、パブリック IP を使用して GUI にアクセスすることはできません。ソリューションを管理するための GUI にアクセスするには、同じ **vnet** に **Windows** 仮想マシンを作成し、アプライアンスに割り当てられた管理 IP に接続します。管理 IP は、最後の NIC (次の図に示すように `sdwanrg42-nic2`) に割り当てられます。アプライアンス

スの GUI には、次のように、この NIC に割り当てられた管理 IP (10.14.2.4) を介して接続する必要があります。

20. GUI にログインすると、Azure 上の SD-WAN が BYOL (自分のライセンスを持参) モデルで動作するため、仮想サービスが無効になっていることがわかります。ライセンスをすでにお持ちの場合は、[ライセンス] タブからライセンスを適用するか、<http://store.citrix.com> に移動して新しいライセンスを注文してください。
21. ライセンスの適用後、アプライアンスに構成を適用し、他のブランチと同じように使用できます。アプライアンスの設定の詳細については、以下を参照してください。[SD-WAN ライセンス](#)

制限事項-Microsoft Azure VM

- Azure で VM を作成し、起動した後、インターフェイスを追加または削除することはできません。仮想マシンプロファイル (RAM/HD/CPU) を変更できます。
- Azure クラウドには MAC アドレススプーフィングの概念はありません。SE-VPX の LAN サブネットとクライアント/サーバ・ホストの LAN サブネットは異なる必要があります。これには、2 つの場所でより多くのルーティング設定を行う必要があります。
- WAN からクライアント/サーバ LAN サブネットに送信されるすべての仮想 WAN データトラフィックを指示するルートが仮想 WAN 設定ファイルに追加されます。

Microsoft Azure は、デプロイのためのゲートウェイモードのみをサポートしています。詳細については、次の記事を参照してください

[VPN ゲートウェイ](#)

Azure での Citrix SD-WAN Standard Edition インスタンスのデプロイ-リリースバージョン 10.2 以降

April 15, 2021

Azure 用 Citrix SD-WAN スタンダードエディションは、複数のネットワークリンクを 1 つの安全な論理仮想パスに論理的に結合します。このソリューションにより、組織は、ブロードバンド、MPLS、4G/LTE、Satellite、ポイントツーポイントリンクなど、さまざまなサービスプロバイダーからの接続を使用して、高い復元性の仮想 WAN パスを取得できます。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。Azure で Citrix SD-WAN を使用する利点には、次のようなものがあります。

- すべての場所から Azure への直接接続を作成します。
- Azure への常時接続を確実にします。
- セキュアな境界をクラウドに拡張します。
- シンプルで管理が容易なブランチネットワークへと進化します。

注:

以前は、128 の仮想パスが Azure でサポートされていました。11.2 リリース以降では、Azure の SD-WAN SE で 256 個のバーチャルパーツがサポートされています。

トポロジ-Azure の SD-WAN

Citrix SD-WAN Standard Edition は、Azure のゲートウェイデプロイモードでのみデプロイできます。パブリック IP アドレス (静的/動的) は SD-WAN の WAN 側インターフェイスに割り当てられ、Azure の管理インターフェイスにアクセスするための管理インターフェイスに 1 つのパブリック IP が割り当てられます。

使用例

Azure VM は指定されたリージョン内にデプロイされ、MPLS、インターネット、または 4G/LTE を介して複数のブランチロケーションに接続できます。仮想ネットワーク (VNET) インフラストラクチャ内で、SD-WAN スタンダードエディション仮想マシンはゲートウェイモードで展開されます。VNET には Azure ゲートウェイへのルートがあります。SD-WAN インスタンスには、インターネット接続用の Azure Gateway へのルートがあります。

データセンター、支店、クラウド間の接続は、複数の WAN パスを同時に利用するさまざまな転送方法を使用することによって実現されます。

Microsoft Azure で Citrix SD-WAN Standard Edition を展開するには

1. Web ブラウザで、<https://portal.azure.com/>と入力します。マイクロソフトの Azure アカウントにログインします。「Citrix SD-WAN Standard Edition」を検索します。
2. 検索結果ウィンドウで、次の解決策を選択します。説明を確認し、選択したソリューションが正しいことを確認したら、[作成] をクリックします。
3. [作成] をクリックすると、Azure での仮想マシンの作成に必要な詳細の入力を求めるウィザードが表示されます。最初の段階で、ソリューションをデプロイするリソースグループを選択します。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。リソースグループを定義する際に考慮すべき重要な点は、次のとおりです。
 - データベースサーバーなどの 1 つのリソースが別のデプロイサイクルに存在する必要がある場合は、別のリソースグループに属することができます。
 - 各リソースは、1 つのリソースグループにのみ存在することができます。
 - リソースは、いつでも別のリソースグループに追加または削除できます。
 - リソースを 1 つのリソースグループから別のリソースグループに移動できます
 - リソースグループには、異なるリージョンに存在するリソースを含めることができます。
 - リソースグループを使用して、管理アクションのアクセス制御の範囲を設定できます。

- リソースは、他のリソースグループのリソースと対話できます。この相互作用は、2つのリソースが関連しているがライフサイクルを共有しない場合に一般的です (データベースに接続している Web アプリなど)。

次の図で、[新規作成] を選択します。

[場所] で、ソリューションをデプロイするリージョンを選択します。リソースグループを作成するときは、そのリソースグループの場所を指定する必要があります。リソースグループには、作成するリソースに関するメタデータが格納されます。したがって、リソースグループの場所を指定するときは、そのメタデータの格納場所を指定します。

注

Azure では、新しいリソースグループまたは空のリソースグループ内にリソースを作成することが義務付けられています。空でないリソースグループに SD-WAN インスタンスをデプロイすることはできません。

4. 仮想マシンの名前を指定します。ユーザ名と強力なパスワードを選択します。パスワードは大文字、特殊文字で構成され、9文字以上である必要があります。[OK] をクリックします。このパスワードは、インスタンスの管理インターフェイスにログインするために必要です。

注

予約名であるため、*admin* というユーザー名を使用してインスタンスをプロビジョニングすることはできません。ただし、インスタンスのプロビジョニング後に管理者アクセスを取得するには、インスタンスのプロビジョニング中に作成されたユーザー名およびパスワードとして *admin* を使用します。インスタンスのプロビジョニング中に作成されたユーザー名を使用すると、読み取り専用アクセス権が付与されます。

5. イメージを実行するインスタンスを選択します。以下に示すように、要件に応じてインスタンスタイプを選択します。
 - インスタンスタイプ D3_V2 では、最大単一方向スループット 200 Mbps、最大仮想パス/ブランチが 16 個あります。
 - インスタンスタイプ D4_V2: 最大単一方向スループット 500 Mbps、最大仮想パス/ブランチ数は 16 です。
 - インスタンスタイプ F8 標準で、1 Gbps の最大単一方向スループット、最大仮想パス/ブランチは 64 個です。
 - インスタンスタイプ F16 標準、最大 128 仮想パス/ブランチで 1 Gbps の最大単一方向スループットを実現します。
6. Citrix SD-WAN 11.0.3 リリースでは、デフォルトで 120GB の OS ディスクサイズが割り当てられます。必要に応じて、ディスクサイズを 40 GB ~999 GB の値に変更できます。
7. 新しい仮想ネットワーク (VNET) を作成するか、既存の VNET を使用します。このステップでは、SD-WAN VPX VM のインターフェイスに割り当てるサブネットを選択するため、展開にとって最も重要なステップです。
8. 仮想マシン内の各インターフェイスに必要なサブネットを割り当てることができます。サブネットの割り当て

順序は、それぞれ [管理]、[LAN]、[WAN]、および [AUX] です。必要に応じてを選択し、「OK」をクリックします。次の図では、サブネットを各インターフェイスに割り当てています。

NIC	割り当て済みネットワーク
NIC 0 (デフォルト)	管理サブネット
NIC 1	LAN サブネット
NIC 2	WAN サブネット

9. [レビュー + 作成] をクリックし、検証に合格していることを確認します。
展開が開始され、[通知] セクションでステータスを確認できます。
10. デプロイを作成するリソースグループに移動すると、展開の詳細を確認できます。
11. プロビジョニング後、管理インターフェイスのパブリック IP アドレスが自動的に作成されます。パブリック IP アドレスを使用して、SD-WAN GUI にアクセスします。
12. インスタンスへの管理者アクセスを取得するには、最初のステップで作成したユーザー名およびパスワードとして *admin* を使用します。
13. GUI にログインした後、Azure 上の SD-WAN は BYOL (自分のライセンスを持参) モデルで動作するため、仮想サービスが無効になっていることに注意してください。ライセンスをすでに持っている場合は、[ライセンス] タブでライセンスを適用するか、[Citrix ストア](#) に移動して新しいライセンスを注文します。
14. ライセンスの適用後、アプライアンスに構成を適用し、他のブランチと同じように使用できます。アプライアンスの設定の詳細については、以下を参照してください。[SD-WAN ライセンス](#)

Azure MCN のインターネットブレイクアウト

Azure MCN のインターネットブレイクアウトを構成するには:

1. MCN アプライアンスで、WAN リンク用に構成されたパブリック IP を使用して、WAN インターフェイスに DHCP IP を設定します。
2. MCN でインターネットサービスを構成します。
3. 内部サービスをインターネットとして、アウトバウンドダイナミックポート制限付き NAT を追加します。
4. MCN にファイアウォールポリシーを追加して、ポート番号 500 で Azure ロードバランサーの正常性プローブを許可します。
5. ポート番号 80 の TCP 用の Azure 外部ロードバランサーに、直接サーバーリターンを無効にした状態で別の負荷分散ルールを追加します。

The screenshot shows a configuration window for a service. The settings are as follows:

- Protocol:** TCP UDP
- Port *:** 80 (with a green checkmark)
- Backend port * ①:** 80 (with a green checkmark)
- Backend pool ①:** sdwan-ext-backendpool (2 virtual machines) (with a dropdown arrow)
- Health probe ①:** sdwan-ext-tcprobe (TCP:500) (with a dropdown arrow)
- Session persistence ①:** None (with a dropdown arrow)
- Idle timeout (minutes) ①:** A slider set to 4 minutes.
- TCP reset:** Disabled Enabled
- Floating IP (direct server return) ①:** Disabled Enabled
- Create implicit outbound rules ①:** Yes No

At the bottom of the configuration area is a blue button labeled "OK".

- インターネットへのブレイクアウトが必要なエンドクライアントマシンで、ルートネクストホップ IP アドレスを内部ロードバランサーのプライベート IP アドレスに設定します。ロードバランサーの IP は、MCN で LAN VIP として設定されます。

制限事項-Microsoft Azure VM

- Azure で VM を作成し、起動した後、インターフェイスを追加または削除することはできません。仮想マシンプロファイル (RAM/HD/CPU) を変更できます。
- WAN からクライアント/サーバ LAN サブネットに送信されるすべての仮想 WAN データトラフィックを指示するルートが仮想 WAN 設定ファイルに追加されます。

Microsoft Azure は、デプロイのためのゲートウェイモードのみをサポートしています。ゲートウェイモードの詳細については、[「ゲートウェイモード」](#)

Citrix SD-WAN Standard Edition 仮想アプライアンス (VPX) の高可用性サポート

April 15, 2021

以下の手順では、AWS クラウドで高可用性モードで SD-WAN 仮想 (VPX) アプライアンスをデプロイする方法について説明します。

SD-WAN VPX 高可用性アプライアンスを AWS クラウドにデプロイする際に考慮すべきポイント。

1. AWS は GARP (汎用属性登録プロトコル)、VLAN、または L2 関連機能 (無差別モードやブリッジングなど) をサポートしていません。これは、異なる顧客に属する 2 つの VM を、同じホスト共有の NIC 上でスケジューリングできるためです。
2. L2 では、スイッチアプライアンスを設定する必要があり、これらは AWS ユーザーには公開されません。
3. SD-WAN アプライアンスの高可用性モデルは、GARP に依存します。フェイルオーバーが発生すると、新しいプライマリアプライアンスは VIP アドレスに対して GARPS を送信します。
4. AWS は、高可用性フェイルオーバーの新しいアプローチを採用しています。ENI (エラスティックネットワークインターフェイス) の新しい概念が導入されました。ENI は、IP アドレス、MAC アドレス、セキュリティグループ、およびポートルールなどの属性を持つネットワークインターフェイスの略エンティティです。
5. ENI をアクティブまたは非アクティブインスタンスから別のアクティブまたは非アクティブインスタンスに移動できます。
6. インスタンスは、インターフェイスのホットプラグを処理できる必要があります。
7. 各インスタンスタイプには、関連付けられている ENI の数と ENI ごとの IP 数に制限があります。
8. 高可用性フェイルオーバーのための AWS 設計では、インスタンスは外部サーバーと通信して Query API AWS サーバーを呼び出します。
9. AWS サーバーは従来の HTTP サーバーです。インスタンスから Query API サーバーにリクエストが送信され、インスタンス/サブネット/VPC または AWS の他の属性に関する情報を取得または投稿します。
10. クラウドプラットフォームの設定では、共有ベース MAC アドレスの設定は無視され、重要ではありません。

クラウドテンプレートを使用して高可用性モードで **Citrix SD-WAN** 標準エディション **VPX** を展開する

詳細については、[EBS のベストプラクティス](#) および [Amazon EBS 暗号化に関する知っておくべきベストプラクティス](#)

- セキュリティグループを定義するには、ポリシーが次のようになっている必要があります。
 - アウトバウンド: すべてのトラフィックを許可する
 - インバウンド:
 - 管理 IP にアクセスするすべての IP アドレス/サブネットからの SSH。
 - AWS VPC (プライベート IP) からのすべてのトラフィック
 - Prem またはクラウドでホストされている Citrix SD-WAN ピアアプライアンスの WAN 側のパブリック IP からのすべてのトラフィック。

11.3 リリース以降、Citrix SD-WAN は、M5 および C5 インスタンスのサポートを導入しました。香港

やパリなどの新しい AWS リージョンは、M5 および C5 インスタンスのみをサポートします。

M5 および C5 インスタンスは、ハードウェアパフォーマンスが向上しており、要求の厳しいワークロード向けに設計されています。M5 および C5 インスタンスは、コアごとに M4 インスタンスよりも優れたコストパフォーマンスを提供します。

メモ

- M5 および C5 インスタンスは、11.3 以降のバージョンの新規プロビジョニングからのみサポートされます。M5 および C5 インスタンスを使用し続けるには、11.3 バージョンからダウングレードできません。M5 および C5 インスタンスは 11.3 より前のバージョンのファームウェアではサポートされていません。
- 10.2.4/11.2.1 バージョンでプロビジョニングされたインスタンスでは、AMI はインスタンスタイプを M5/C5 に変更できません。

クラウドテンプレートを使用して高可用性モードで **SD-WAN Standard Edition VPX** をデプロイする

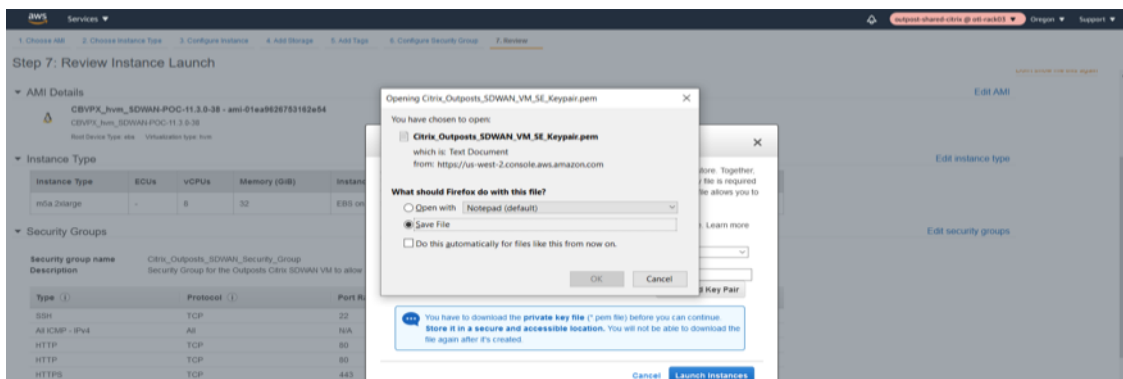
SD-WAN 高可用性ソリューションテンプレートは AWS マーケットプレイスで公開されています。**CloudFormation** テンプレートをサブスクライブし、使用して HA セットアップをデプロイできます。

前提条件

CloudFormation テンプレートを起動する前に、管理、LAN、および WAN ネットワーク用に VPC、サブネット、ルートテーブルを作成しておく必要があります。サブネットおよびルートテーブルを作成および定義するには（作成されていない場合）、[SD-WAN VPX Standard Edition AMI を AWS にインストールする](#) トピックを参照してください。

クラウドテンプレートを使用して高可用性モードで SD-WAN Standard Edition VPX を展開するには：

1. [AWS マーケットプレイス](#) に移動し、[価格設定] タブをクリックします。ドロップダウン・リストからリージョンを選択し、「履行オプション」を「高可用性モード」配布として指定します。[続行] をクリックして購読します。
2. [設定に進む] をクリックします。
3. ドロップダウンリストから、[**CloudFormation** テンプレート] と [高可用性モードデプロイ] として [フルフィルメントオプション] を指定します。[地域] を選択し、[続行] をクリックして起動してください。
4. ソフトウェアの起動ウィンドウで [**CloudFormation** の起動] として [アクション] を選択し、[起動] をクリックします。



5. [スタックの作成] ウィンドウで、**CloudFormation** の実行中に、定義済みの **S3** テンプレート **URL** が表示されます。[次へ] をクリックします。
6. [詳細の指定] ** セクションでスタック名を指定します **。
7. 仮想プライベートネットワーク構成を構成します。次のパラメータの詳細を入力します。

- **VPC ID:** 仮想プライベートクラウド ID を指定します。
- リモート **SSH CIDR IP:** EC2 インスタンス (ポート 22) に SSH できる IP アドレス範囲を指定します。

注:

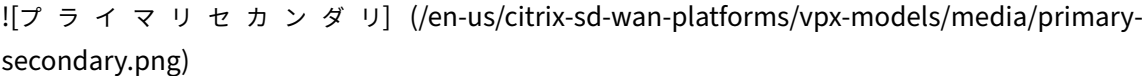
既知の IP アドレスから SSH のみを許可することをお勧めします。

- リモート **HTTP CIDR IP:** EC2 インスタンス (port80) に HTTP できる IP アドレス範囲を指定します。
 - リモート **HTTPS CIDR IP:** EC2 インスタンス (ポート 443) に HTTPS できる IP アドレス範囲を指定します。
 - キーペア: インスタンスへの SSH アクセスを有効にするには、既存の EC2 KeyPair の名前を指定します。
8. 作成したインスタンスにアタッチする必要があるネットワークインターフェイスを設定します。プライマリ IP はハイアベイラビリティペアのプライマリインスタンス用であり、セカンダリ IP はハイアベイラビリティペアのセカンダリインスタンス用に設定されていることに注意してください。
 9. ** インスタントタイプやテナントタイプなどの他のパラメータを設定し **、[次へ] をクリックします。

メモ

検証が失敗した場合、AWS はユーザーに通知し、エラーが解決されるまで続行できません。

10. タグを設定します。これらのタグは、ユーザーが構成できる AWS 固有のオプションです。
11. IAM ロールを設定することはお勧めしません。これは、カスタマイズされた IAM ロールによってすでに作成されています。このロールは、クラウドフォーメーションテンプレートを使用して行われます。
12. [次へ] をクリックした後、テンプレートを確認し、**Cloud Formation** テンプレートによって作成されたカスタム IAM ロールを確認します。「作成」に進みます。

- 作成した新しいスタックが [クラウドフォーメーションスタック] ページに表示されます。テンプレートのアップロードが成功したら、テンプレートのステータスを監視します。
- クラウドフォーメーションテンプレートによって作成されたすべてのリソースのイベントを監視します。障害が発生した場合、AWS によってイベントの詳細な説明が生成され、問題のデバッグに役立ちます。イベントは次のように表示されます。
- スタックの作成に成功すると、テンプレートのステータスは **Create_Complete** として表示されます。
- AWS コンソールから [サービス] > [EC2] > [インスタンス] に移動します。作成された 2 つのインスタンス **sdwanPrimary** と **sdwanSecondary** インスタンスが、インスタンスに関連付けられた Elastic IP を使用して起動および実行されていることがわかります。
 ([プライマリセカンダリ] (/en-us/citrix-sd-wan-platforms/vpx-models/media/primary-secondary.png))
- sdwanPrimary** インスタンスを選択します。インスタンス、セキュリティグループ、Elastic IP、IAM ロール、および 4 つのネットワークインターフェイスに正しく割り当てられているすべてのリソースがわかります。高可用性機能を作成できませんでした。期待どおりに動作しない可能性があります。
- 同様に、**sdwanSecondary** インスタンスを選択し、上記のリソースを確認します。

LAN および WAN リンク用のセカンダリフローティング IP

高可用性を機能させるには、LAN および WAN リンク用のセカンダリフローティング IP が必要です。スタックが作成されたら、アクティブな EC2 インスタンスの LAN および WAN インターフェイスに新しいセカンダリプライベート IP を割り当てます。これらのセカンダリ構成 IP は、VPX で仮想 IP アドレスを構成するときに使用されます。

セカンダリ LAN IP をアクティブインスタンスに接続するには、次の手順を実行します。

注:

HA ソリューションを導入したら、セカンダリ・フローティング IP をプライマリ・インスタンスにのみ割り当てる必要があります。

- [サービス] > [EC2] > [インスタンス] に移動します。
- [サービス] > [EC2] > [ネットワークインターフェイス] に移動し、プライマリインスタンスの LAN/WAN Elastic Network Interface (ENI) を選択します。
- 新しいセカンダリ IP を割り当てます。
- [Yes, Update] をクリックします。
- 同様に、WAN インターフェイスのセカンダリプライベート IP も作成します。

WAN リンク上のパブリック IP

外部の世界と通信するために WAN リンク上で必要なパブリック IP。Elastic IP を WAN ENI インターフェイスに関連付けるには、次の手順を実行します。

1. [住所] > [新しい住所の割り当て] に移動します。
2. 作成された Elastic IP を選択し、[アクション] > [アドレスの関連付け] をクリックし、作成したセカンダリプライベート WAN IP にパブリックを関連付けます。
3. 次のように、最終的なインターフェイスと IP が想定されていることを確認します。
 - プライマリ・インスタンス:
 - セカンダリインスタンス:

これでインスタンスのプロビジョニングが完了しました。SD-WAN 高可用性アプライアンスの設定は、スタンドアロンアプライアンスの設定とほとんど似ています。相違点を以下に挙げます。

- LAN および WAN 仮想 IP インターフェイスの作成時に、作成したセカンダリプライベート IP を指定します。また、高可用性仮想 IP インターフェイスの場合は、高可用性ネットワークでダミー IP を指定します。
- ハイアベイラビリティをイネーブルにし、アクティブインスタンスとセカンダリインスタンスのハイアベイラビリティインターフェイス IP を指定します。

高可用性ステータスを確認できます。

AWS で実行されている SD-WAN インスタンスに対して高可用性フェールオーバーを設定する方法

3 つ以上の ENI を持つ 1 つのハイアベイラビリティピアと、同数の ENS を持つ 1 つのハイアベイラビリティピアと 1 つのハイアベイラビリティピアを設定します。どちらのピアでも、最初の ENI は管理専用です。1 つの高可用性ピアがすべてのトラフィック ENA を所有します。フェイルオーバー中、トラフィック ENI は障害が発生したインスタンスから新しいプライマリ・インスタンスに移動します。

たとえば、2 つのトラフィックの ENI を移動するには、最大で 20 秒以上かかることがあります。AWS には API レスポンスに SLA がないため、高可用性フェールオーバー時間用の SLA を持つことはできません。

注

AWS の設計には、アタッチとデタッチに応答する AWS サーバーに依存するインスタンスの制限があります。フェールオーバー時間は予測できません。

構成の手順

1. REST API を使用して関連付けられた ENI の数および関連付けられた ENI の詳細に関する情報について、高可用性ピアインスタンスに関する情報を取得します。
2. 障害が発生したインスタンスの状態を検出します。
3. REST API を使用して失敗したインスタンスから ENS の Detach を呼び出します。
4. 関連付けられているすべての ENIs がデタッチされていることを確認します。

5. ENI を現在のプライマリ・インスタンスにアタッチします。
6. すべての ENI が接続されていることを確認します。
7. 上層をトリガーして、新しい ENS が所定の位置にあることを検出します。

単一の **AWS** 仮想プライベートクラウド (**VPC**) サブネット、またはパブリック **WAN** リンク **IP** アドレスを持つリージョン間で **SD-WAN VPX-SE** を設定する方法

AWS VPC では、アクティブな SD-WAN インスタンスに対して、同じ VPC で実行されている別の高利用可能な SD-WAN インスタンスがリリースされます。

1. アクティブな SD-WAN アプライアンスとスタンバイ SD-WAN アプライアンスの間で設定されたリンクは同じです。
2. AWS の場合、SD-WAN アプライアンス間で通信するための RACP プロトコル用のサブネットと専用リンクを作成できます。
3. SD-WAN GUI で、次の項目を設定します。
 - インターフェイスグループを作成します。「高可用性リンク」という名前を付けます。高可用性に使用するインターフェイスを追加します。
 - インターフェイスグループの仮想 IP アドレスを作成します。
 - 高可用性ノードで、高可用性を有効にし、RACP プロトコルが通信に使用する制御仮想 IP を追加します。AWS でネットワークインターフェイスを作成する際に、IP アドレスが設定された IP アドレスと同じであることを確認します。
 - 変更管理を実行し、スタンバイ SD-WAN アプライアンスのアクティブな構成をダウンロードします。
 - スタンバイ側の SD-WAN アプライアンスでローカル変更管理を使用して設定を適用すると、アクティブ側とスタンバイ側の SD-WAN 高可用性アプライアンス間でハートビートが交換されます。
 - フェイルオーバーが発生すると、SD-WAN アプライアンスがスタンバイモードからアクティブモードに移行したり、逆に構成が失われることはありません。

注

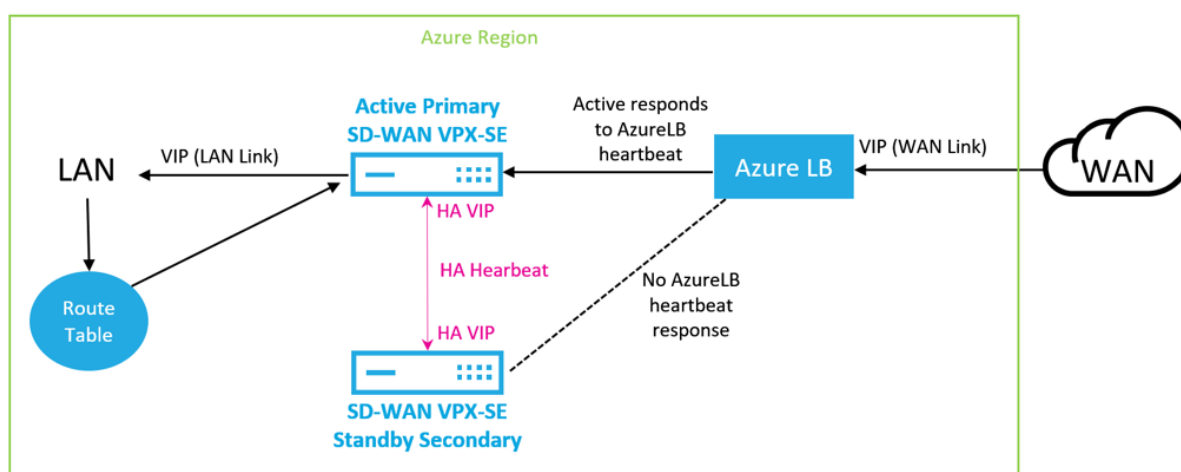
1. AWS は、Elastic Load Balancing や Auto Scaling などの機能を備えた高可用性モードをサポートしています。ここでは、SD-WAN アプライアンス内の設定を同期することが課題となります。この展開では、効率的な高可用性を実現するために、既存の RACP プロトコルを適用します。
2. MCN アプライアンスとブランチサイトアプライアンスの両方をクラウド環境で使用することができます。

Azure の高可用性モードで **SD-WAN Standard Edition** インスタンスをデプロイ-リリースバージョン **9.3**

April 15, 2021

Citrix SD-WAN Azure ソリューションは、単一インスタンスとして、または高可用性 (HA) 用のクラスターペアとして、エッジゲートウェイモードで SD-WAN を展開します。高可用性展開では、Azure ロードバランサー (ALB) が Citrix SD-WAN アプライアンスの WAN インターフェイス間のフェイルオーバーを制御します。Citrix SD-WAN アプライアンス自体は、Azure ルートテーブル (RT) を更新して、Citrix SD-WAN アプライアンスの LAN 側でのフェイルオーバーを制御します。高可用性の Citrix **SD-WAN Azure** ソリューションは、**sdwanhalb** という名前の **ALB (Azure ロードバランサー)** と **sdwan** RouteTable という名前の **RT (ルートテーブル)** を自動的に作成します。

次の図は、Citrix SD-WAN Azure の高可用性の展開を示しています。



以下のセクションでは、Microsoft Azure で Citrix SD-WAN ソリューションをデプロイし、SD-WAN GUI で HA を構成するためのワークフローについて説明します。

1. アプリケーション登録の作成-HA 展開用のアプリケーション ID、アプリケーションキー、およびディレクトリ ID (オブジェクト ID) を取得します。
2. Citrix SD-WAN を展開します。
3. Citrix SD-WAN アプライアンスを構成します。

Azure での SD-WAN スタンダードエディションの展開は、エッジモードまたはゲートウェイモードの展開で展開する必要があります。この展開では、SD-WAN インスタンスが LAN 環境のゲートウェイとして機能します。詳しくは、「[ゲートウェイモード](#)」を参照してください。

Citrix の SD-WAN 用の Azure での作成とアプリケーションの登録方法

アプリケーションキーは、ローカル LAN ルーティングテーブルの更新に使用されます。

アプリケーションを登録するには、次の手順に従います。

1. **Azure Active Directory** にログインし、[アプリの登録] を選択します。

2. [+新規アプリケーション登録] をクリックします。アプリケーションの名前を指定します。[アプリケーションの種類] で [Web アプリケーション/API] を選択し、[ホームページ] フィールドに任意の HTTP アドレスを入力します。SD-WAN のアプリケーション ID とオブジェクト ID を文書化します。[設定] をクリックします。
3. 新しく作成したアプリ登録で、[設定]>[キー] を選択します。次に、キーの説明を作成し、[有効期限なし] を選択します。値を文書化した後に新しいキーを保存し、Citrix SD-WAN の展開に進みます。

Citrix SD-WAN を展開する方法

Citrix SD-WAN を高可用性で展開するには：

展開には、Azure VNET が必要です。展開中に VNET を作成するか、Citrix SD-WAN 用の既存の VNET を選択します。

以下は、このトピックで使用されている VNET のサブネットのスクリーンショットです。

1. Azure リソースを作成します。SD-WAN を検索し、WAN Standard Edition リリース 9.3 を選択します。
2. 基本設定ページを構成し、リソースグループ名を指定します。
3. 仮想マシンに名前を付けて、[** 高可用性展開モードで有効] を選択し、ユーザー名とパスワードを作成します。**
4. **SDWAN** 設定を構成します。[サブネット] セクションの [管理] サブネットには SD-WAN 管理 IP が含まれています。Aux サブネットには HA IP が含まれています。WAN VIP は、sdwanhalb ALB の背後に利用可能である間、LAN VIP は SDWanharoute Azure RT を更新します。
5. Citrix SD-WAN が更新したルートを構成し、リモート SD-WAN ネットワークを送信先として定義し、アプリケーション ID、ディレクトリ (オブジェクト) ID、およびアプリケーションキー値を入力します。Citrix SD-WAN は、ルートテーブル名フィールドで定義されている名前で始まるすべてのルートステートメントを制御します (このドキュメントの SeavNetSDWGW)。
6. 手順 5 で、設定を検証し、SD-WAN HA ペアを作成します。Citrix SD-WAN アプライアンスの構成に進みます。

Azure でシトリックスの SD-WAN HA を構成する方法

1. SD-WAN インターフェイスに割り当てられた IP アドレスを確認します。[仮想マシン]>[SDWSA] (または必要に応じて)>[ネットワーク] に移動し、各 Azure ネットワークインターフェイスの IP を確認します。
 - この展開では、管理用の SDWSE インターフェイス 0 は 10.100.254.4/13.67.93.144 です。
 - SDWSA インターフェイス 1 LAN VIP は 10.100.1.4 です。

- SDWSEA インターフェイス 2 WAN VIP は 10.100.0.4 です。
 - SDWSEA インターフェイス 3 HA トラッキング IP (VIP ではない) は 10.100.253.4 です。
 - セカンダリ Citrix SD-WAN アプライアンスについても手順を繰り返します。
2. SD-WAN ALB パブリック IP を確認します。[ロードバランサー]>[**sdwanhalb**]に移動します。デプロイ中に作成されたリソースグループに基づいて、適切な ALB を選択します。この環境では、SD-WAN WAN リンクパブリック IP アドレス。
 3. Web ブラウザーを使用して管理 IP に接続します。
 - 管理者/パスワードでログインします。管理者パスワードを変更するには、左側のナビゲーション・バーで [構成] タブを選択し、[アプライアンスの設定] > [管理者インタフェース] を選択し、現在の管理者パスワードと新しいパスワードを入力し、[パスワードの変更] ボタンをクリックします。ログアウトするように求められます。
 4. SD-WAN MCN アプライアンスまたは SD-WAN センターに進み、SD-WAN HA サイトを設定します。サポートされているリリースバージョンは 10.0.6 です。このトピックでは、SDWSWEA および SDWSEASec アプライアンスは MCN アプライアンスです。
 5. SDWANSEA および SDWanSec インターフェイスグループの設定は、次のように提供されます。Edge ゲートウェイモードごとにインターフェイスがブロックされなかったことに注意してください。ALB からの接続を受け入れるには、WAN インターフェイスを [信頼済み] に設定する必要があります。
 6. 仮想 IP 構成は次のように提供されます。HA VIP は、インターフェイス 3 に割り当てられた IP アドレスではないことに注意してください。Citrix SD-WAN アプライアンスに割り当てられた IP ではなく、適切なサブネットワークで使用可能な IP アドレスを使用します。アイデンティティ IP は、各サブネット内の 1 つの VIP のみであることに注意してください。
 7. SDWANSEA WANSEA WAN リンクの設定は以下の通りです。パブリック IP アドレスをメモします。SD-WAN ライセンスによって、帯域幅の設定が決まります。
 8. アクセスインターフェイスの設定は次のとおりです。10.100.0.1 IP は、Azure 予約 IP です。
 9. 高可用性設定は次のとおりです。
 10. SDWSEA-LAN Azure 予約 IP をゲートウェイとして使用する SDWSEA-LAN サブネットより多くとの間でルーティングする場合は、SD-WAN が、VNET のエクスポートルートを追加します。
 11. Azure ルートテーブルで、SDWSEA アプライアンスが制御するルートは SeavNetSDWGW で始まる必要があります。この図は、SDWANSEA 展開における WAN サイトを示しています。
 - SDWSEA アプライアンスがアクティブなときのルートテーブル。
 - SDWSEASec アプライアンスがアクティブなときのルートテーブル。

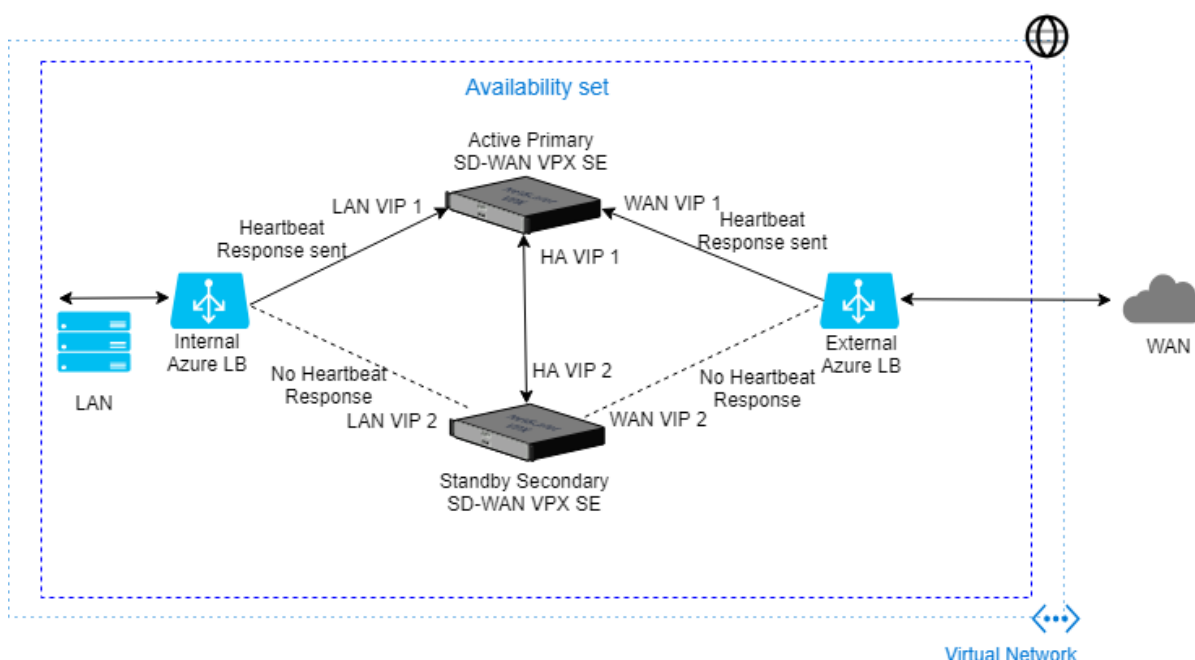
Azure の高可用性モードで **SD-WAN Standard Edition** インスタンスをデプロイ-リリースバージョン **10.2** 以降

April 15, 2021

Citrix SD-WAN Azure ソリューションは、単一インスタンスとして、または高可用性 (HA) 用のクラスターペアとして、エッジゲートウェイモードで Citrix SD-WAN を展開します。高可用性展開では、Azure ロードバランサー (ALB) が Citrix SD-WAN アプライアンスの WAN インターフェイス間のフェイルオーバーを制御します。

LAN 側で Azure ロードバランサー (ALB) を使用して、SD-WAN アプライアンスの LAN 側のフェイルオーバーを制御できます。高可用性の Citrix SD-WAN Azure ソリューションでは、2 つの別々の ALB (LAN および WAN 上に 1 つ) が作成されます。

次の図は、Citrix SD-WAN Azure の高可用性の展開を示しています。



Azure での SD-WAN スタンダードエディションの展開は、エッジモードまたはゲートウェイモードの展開で展開する必要があります。この展開では、SD-WAN インスタンスが LAN 環境のゲートウェイとして機能します。詳しくは、「[ゲートウェイモード](#)」を参照してください。

Citrix SD-WAN を展開する方法

Citrix SD-WAN Standard Edition (SE) インスタンスを作成するには:

1. Azure Marketplace で **Citrix SD-WAN** を検索し、[**Citrix SD-WAN** スタンダードエディション **10.2.X**] を選択します。
2. [作成] ボタンをクリックして、**Citrix SD-WAN SE 10.2.X** インスタンスを作成します。

3. [基本設定] ページを構成し、** リソースグループ名に適切な場所を指定します **。

注:

インスタンスを作成するには、新しいリソースグループを作成するか、リソースグループを空にして再利用する必要があります。

4. 仮想マシンに名前を付けて、[** 高可用性展開モードで有効] を選択し、ユーザー名とパスワードを作成します。 **

注:

admin は、プロビジョニング時に付与されたパスワードと同じパスワードで、プロビジョニングされたインスタンスのユーザー名として使用し、管理者アクセスを取得します。前述のスクリーンショットでは、プロビジョニングされたユーザーはゲスト権限を持っています。

5. 要件に基づいて仮想マシンのサイズを選択します。
6. Citrix SD-WAN 11.0.3 リリースでは、デフォルトで 120GB の OS ディスクサイズが割り当てられます。必要に応じて、ディスクサイズを 40 GB ~999 GB の値に変更できます。
7. 指定した場所に既存の VNet を使用するか、新しいを作成します。
8. **Vnet** を作成したら、管理、**LAN**、**WAN**、および AUC の自動設定されたサブネットを確認し、[**OK**] をクリックします。
9. インスタンスを作成する前に、設定を検証します。
10. [作成] をクリックします。

Azure でシトリックスの **SD-WAN HA** を構成する方法

1. SD-WAN インターフェイスに割り当てられた IP アドレスを確認します。[仮想マシン] > [**SDWSA**] (または必要に応じて) > [ネットワーク] に移動し、各 Azure ネットワークインターフェイスの IP を確認します。
 - この展開では、管理用の SDWSE インターフェイス 0 は 10.100.254.4/13.67.93.144 です。
 - SDWSA インターフェイス 1 LAN VIP は 10.100.1.4 です。
 - SDWSEA インターフェイス 2 WAN VIP は 10.100.0.4 です。
 - SDWSEA インターフェイス 3 HA トラッキング IP (VIP ではない) は 10.100.253.4 です。
 - セカンダリ Citrix SD-WAN アプライアンスについても手順を繰り返します。
2. SD-WAN ALB パブリック IP を確認します。[ロードバランサー] > [**sdwanha-外部**] に移動します。デプロイ中に作成されたリソースグループに基づいて、適切な ALB を選択します。

次のように 2 つのロードバランサーが表示されます。

- 外部: 外部 LB には、WAN リンク設定で設定するパブリック IP が含まれます。
- 内部: 内部 LB にはプライベート IP が含まれています。LAN 側のトラフィックはすべて、内部 LB に送られます。したがって、内部 LB IP をネクストホップとしてルートテーブルを設定できます。

3. SD-WAN MCN アプライアンスまたは SD-WAN センターに進み、SD-WAN HA サイトを設定します。このトピックでは、SDWSWEA および SDWSEASec アプライアンスは MCN アプライアンスです。

注:

Azure では、SD-WAN オーケストレータを使用して Citrix SD-WAN HA を構成することもできます。

4. SDWANSEA および SDWanSec インターフェイスグループの設定は、次のように提供されます。仮想インターフェイスごとに 1 つのイーサネット/物理インターフェイスだけが使用されるため、バイパスモードは fail-to-block に設定されます。ALB からの接続を受け入れるには、WAN インターフェイスを [信頼済み] に設定する必要があります。

5. 仮想 IP 構成は次のように提供されます。HA VIP は、インターフェイス 3 に割り当てられた IP アドレスではないことに注意してください。Citrix SD-WAN アプライアンスに割り当てられた IP ではなく、適切なサブネット (AUX インターフェイスに割り当てられたサブネット) で使用可能な IP アドレスを使用します。アイデンティティ IP は、各サブネット内の 1 つの VIP のみであることに注意してください。

LAN と WAN 仮想インターフェイスの両方に、2 つの仮想 IP が割り当てられます。一方の IP はプライマリ **SD-WAN** 仮想マシンに属し、もう 1 つの IP は LAN と WAN の両方でセカンダリ **SD-WAN** 仮想マシンに属します。アイデンティティではプライマリ IP だけがイネーブルになります。

6. SDWANSEA WANSEA WAN リンクの設定は以下の通りです。注: **WAN** リンクのパブリック IP アドレス設定の一部として、外部ロードバランサーのパブリック IP アドレスを構成します。SD-WAN ライセンスによって、帯域幅設定が決まります。

7. アクセスインターフェイスの設定は次のとおりです。10.100.0.1 IP は、Azure 予約 IP です。

8. 高可用性設定は次のとおりです。この HA 設定の一部としてのプライマリ IP アドレスとセカンダリ IP アドレスは、プライマリ仮想マシンとセカンダリ仮想マシンの両方の AUX インターフェイス IP アドレスを使用して構成する必要があります。

9. [Apply] をクリックします。

10. LAN トラフィックが SD-WAN を通過するようにするには、次のホップが Azure 内部ロードバランサー IP をポイントするルートを持つ Azure 上のルートテーブルを追加します。そして、作成したルートテーブルに LAN サブネットを関連付けます。

すべてのトラフィックを SD-WAN 経由でルーティングする必要がある場合は、ネクストホップが内部ロードバランサー IP を指しているデフォルトルートを作成します。

Citrix ADC SDX アプライアンスに Citrix SD-WAN VPX インスタンスをデプロイする

April 15, 2021

Citrix SD-WAN テクノロジーは、ソフトウェア定義ネットワーク (SDN) の概念を WAN 接続に適用します。このテクノロジーは、ネットワークハードウェアからトラフィック管理とモニタリングを抽象化し、個々のアプリケーションに適用します。その結果、パフォーマンスが向上し、地理的に分散した場所での高品質なユーザーエクスペリエンス、広域ネットワークとクラウドアクセスネットワークの導入が簡素化されます。詳しくは、「[Citrix SD-WAN](#)」を参照してください。

リリース 12.1 49.xx から、Citrix ADC SDX 14XXX および SDX 115XX アプライアンスに Citrix SD-WAN VPX インスタンスを展開できます。詳しくは、次のドキュメントを参照してください。

- [Citrix ADC SDX 14020、SDX 14030、SDX 14040、SDX 14060、SDX 14060、SDX 14080、SDX 14100](#)
- [Citrix ADC SDX 11515、SDX 11520、SDX 11530、SDX 11540、SDX 11540、SDX 11542](#)

注

SD-WAN VPX Standard Edition のみがサポートされます。詳しくは、「[SD-WAN VPX エディション](#)」を参照してください。

SDX アプライアンスへの Citrix SD-WAN VPX インスタンスの展開には、次のタスクが含まれます。

- ハードウェアの取り付け: SDX ハードウェアが正しく取り付けられていることを確認します。詳しくは、「[ハードウェアのインストール](#)」を参照してください。
- SDX 管理サービスの設定および設定詳しくは、「[管理サービスユーザーインターフェイスの使用開始](#)」および「[管理サービスの構成](#)」を参照してください。
- SDX アプライアンスでの SD-WAN VPX インスタンスのプロビジョニング詳しくは、「[Citrix ADC SDX での Citrix SD-WAN VPX インスタンスのプロビジョニング](#)」を参照してください。
- SD-WAN VPX インスタンスの構成詳しくは、[構成](#)および[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](#)のドキュメントを参照してください。

前提条件

次のライセンスがあることを確認してください。

- Citrix SD-WAN VPX ライセンス
- Citrix ADC SDX プラットフォームライセンス

Citrix SD-WAN VPX の要件

SDX プラットフォーム上の Citrix SD-WAN VPX は、サイトと MCN の両方として機能できます。MCN は、1 Gb/秒の双方向スループットと 64 サイトを処理できます。

MCN およびサイトでサポートされるスループット

- 250 MB/秒~1 Gb/秒の双方向スループット
- MCN は 64 サイトをサポート

サポートされるスループットのハードウェア要件

サイト

- 4 CPU から 16 CPU
- 4 GB から 16 GB RAM
- 60 GB ~250 GB のディスクストレージ
- 最低 4 つの NIC: 1 つは管理用、残りは 3 つはデータパス用

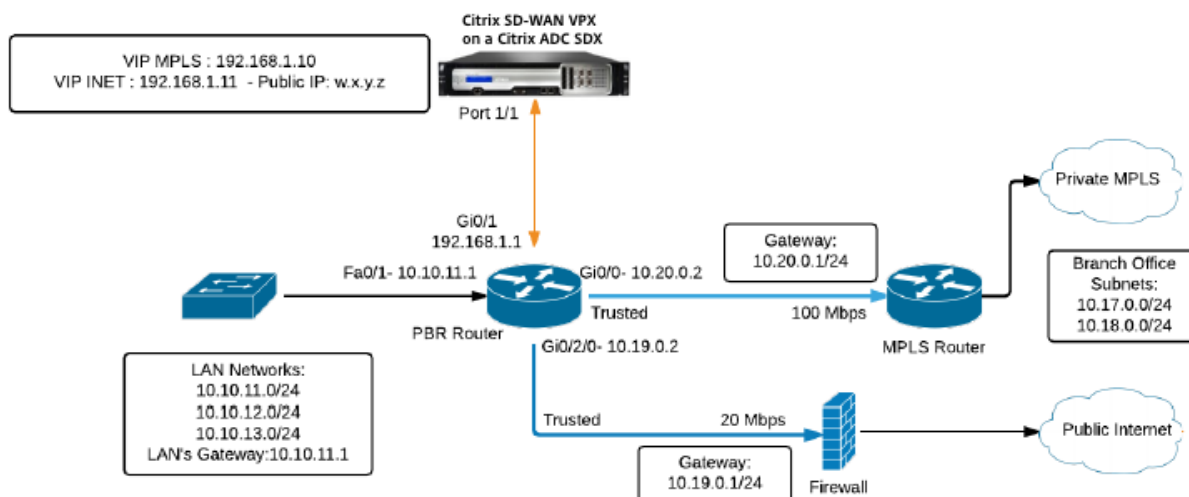
マスターコントロールノード (MCN)

- 4,8、16 CPU
- 16 ギガバイトの RAM
- 250 GB ディスクストレージ
- 最低 4 つの NIC: 1 つは管理用、残りの 3 つはデータパス用、データパス専用の NIC

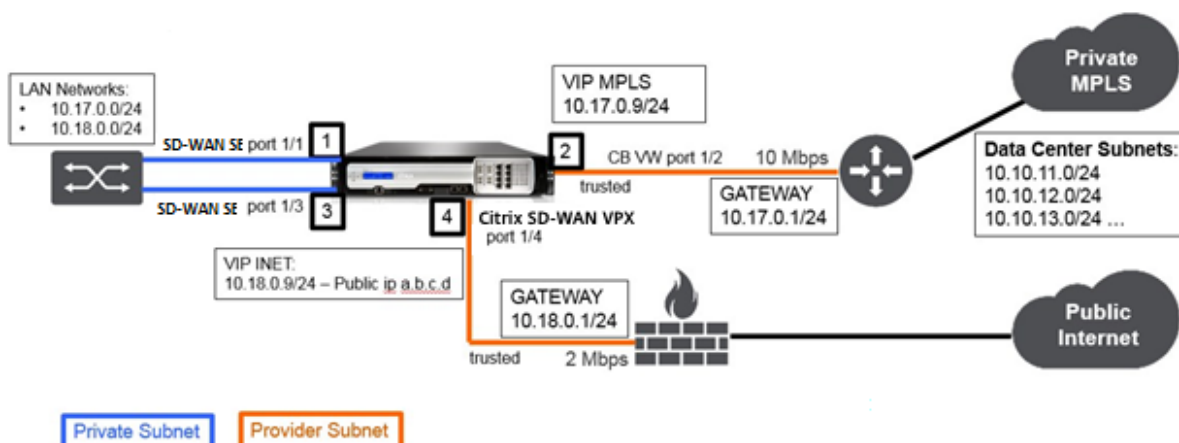
データセンタートポロジ

Citrix SD-WAN VPX アプライアンスは、ポリシーベースルート (PBR) モードまたはインラインモードで Citrix ADC SDX に展開できます。これら 2 つのサポートされているモードのトポロジについては、シナリオ 1 および 2 を参照してください。詳しくは、「[PBR モードでの SD-WAN の展開 \(仮想インラインモード\)](#)」を参照してください。

シナリオ 1. データセンタートポロジ:PBR モードまたは仮想インラインモード



シナリオ 2. ブランチトポロジ: インラインモード

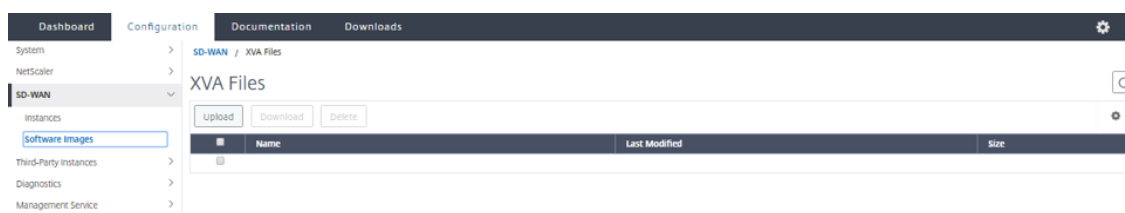


Citrix ADC SDX での Citrix SD-WAN VPX インスタンスのプロビジョニング

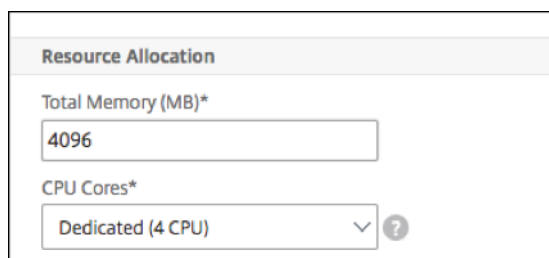
Citrix SD-WAN VPX アプライアンスをプロビジョニングする前に、[ダウンロード](#) Citrix 製品サイトから SD-WAN VPX イメージをダウンロードします。

Citrix SD-WAN VPX アプライアンスをプロビジョニングするには、次の手順に従います。

1. Citrix ADC SDX アプライアンスにログオンします。
2. [構成] > [SD-WAN] > [インスタンス] に移動します。
3. ソフトウェアイメージ > **SD-WAN XVA** ファイルをアップロードしてアップロードを選択します。



4. [インスタンス] > [追加] を選択します。[SD-WAN インスタンスのプロビジョニング] ページが表示されます。
5. [SD-WAN インスタンスのプロビジョニング] ページで、次のように入力します。
 - 名前
 - IP アドレス
 - ネットマスク
 - ゲートウェイアドレス
 - XVA ファイルをアップロードする
 - [リソースの割り当て] で、リソースを割り当てます。

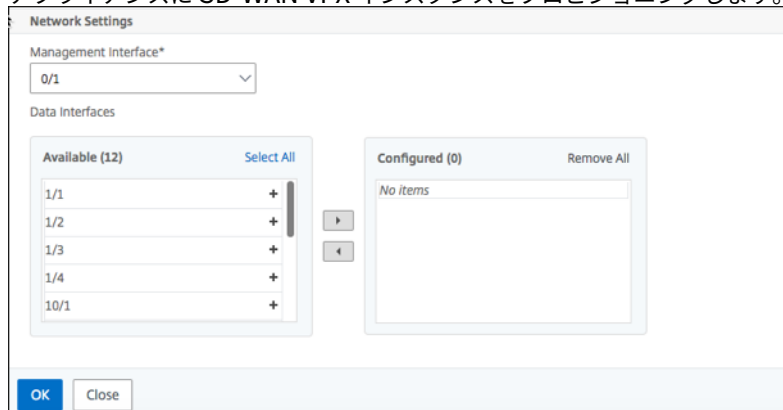


Resource Allocation

Total Memory (MB)*
4096

CPU Cores*
Dedicated (4 CPU)

- 「ネットワーク設定」で、管理インターフェースをプロビジョニングし、「OK」を選択して作成し、SDX アプライアンスに SD-WAN VPX インスタンスをプロビジョニングします。



Network Settings

Management Interface*
0/1

Data Interfaces

Available (12) Select All

1/1	+
1/2	+
1/3	+
1/4	+
10/1	+

Configured (0) Remove All

No items

OK Close

注

SDX 管理サービスは、インタフェース名の昇順で VPX インスタンスにインタフェースをバインドします。たとえば、1/4、および 1/1 を追加すると、管理サービスはそれらを 1/1、1/4 として配置します。新しいインタフェースを追加すると、既存のシーケンスが保持され、新しいシーケンスが作成されます。たとえば、インタフェース 1/2、10/1、1/3 を追加します。新しいシーケンスは、1/1、1/4; 1/2、1/3、10/1 になります。

- 「インスタンス」ページの下に、**SD-WAN VPX** インスタンスが表示されます。ここに例があります。



Instances

Add Delete Start Shut Down Reboot Rediscover

<input type="checkbox"/>	Name	IP Address
<input type="checkbox"/>	SDWAN1	10.102.103.211

インスタンスを編集するには、[設定] > [SD-WAN] > [インスタンス] に移動します。インスタンスを選択してクリックします。編集が完了したら、「OK」をクリックして変更を保存します。

Citrix SD-WAN VPX インスタンスの構成

SDX アプライアンスで SD-WAN インスタンスを作成したら、次の 2 つのタスクを実行して SD-WAN インスタンスを設定します。

1. MCN アプライアンスとサイトアプライアンスの両方に設定を適用します。
2. 仮想パスを設定し、トラフィックを送信します。

詳しくは、次のトピックを参照してください：

- [構成](#)
- [MCN サイトとクライアントサイト間の仮想パスサービスの構成](#)

関連情報

Citrix SD-WAN アプライアンスの使用を開始する方法については、「[Citrix SD-WAN](#)」を参照してください。

Citrix ADC SDX アプライアンスの詳細については、[Citrix ADC SDX](#)を参照してください。

クラウドウォッチサポート向け **AWS** の **Standard Edition**

April 15, 2021

AWS の Citrix SD-WAN Standard Edition では、AWS インフラストラクチャで実行されている SD-WAN インスタンスを監視するための基本的な CloudWatch がサポートされるようになりました。CloudWatch アラームは、モニタリングしているリソースに通知を送信するか、自動的に変更を加えます。基本モニタリングでは、事前選択された 7 つのメトリックスを 5 分間隔で、3 つのステータスチェックメトリックスを 1 分間隔で SD-WAN インスタンスで使用できます。SD-WAN イメージについて、次のメトリックスを表示できます。

- CPU 使用率-インスタンスに現在使用されている割り当て済みコンピューティングユニットの割合。このメトリックは、選択したインスタンスでアプリケーションを実行するために必要な処理能力を識別します。
- ディスクの読み取り操作-指定された期間に使用可能なすべてのインスタンスボリュームからの読み取り操作。
- ディスク書き込みオペレーション — 指定した期間内にインスタンスで使用可能なすべてのインスタンスストアボリュームの書き込み操作。
- DiskReadBytes — 実行中のインスタンスで使用可能なすべてのインスタンスストアボリュームに書き込まれたバイト数
- ネットワーク — このメトリックスは、単一インスタンスの着信トラフィックの量を識別します。
- Network Out-このメトリックは、単一インスタンスの発信トラフィックの量を識別します。
- Networkpacketsout — インスタンスによってすべてのネットワークインターフェイスから送信されたパケット数。これは基本的なモニタリングでのみ使用できます。

Citrix SD-WAN VPX WANOP

April 15, 2021

Citrix SD-WAN WANOP VPX は、Citrix XenServer、VMware ESX または ESXi、Microsoft Hyper-V、および Amazon AWS 仮想化プラットフォーム上でホストできる仮想 Citrix SD-WAN アプライアンスです。SD-WAN WANOP VPX アプライアンスは、物理 SD-WAN WANOP アプライアンスのほとんどの機能をサポートします。

SD-WAN WANOP Edition VPX は仮想マシンであるため、選択したハードウェアを必要な場所に配置し、他の仮想マシン、サーバー、VPN ユニット、または他のアプライアンスと組み合わせて、ニーズに正確に一致するユニットを作成できます。

Citrix SD-WAN WANOP VPX ソフトウェアは、次のもので使用できます。

- XenServer 5.5 以降で実行されている Xen 仮想マシンです。
- ESX/ESXi 4.1 ~6.0 で実行される VMware vSphere 仮想マシン。
- 64 ビット Windows 2008 R2 SP1-2012 の下の Hyper-V 仮想マシン。
- Amazon AWS インスタンス。
- Microsoft Azure インスタンス。

注:

XenServer と VMware vSphere は VLAN トランキングをサポートしますが、Hyper-V ではサポートされていません。

XenServer、VMware ESX、Microsoft Hyper-V、Amazon AWS での SD-WAN WANOP VPX の設定については、[CloudBridge 7.4 PDF](#)の 691 ~749 ページを参照してください。

新しくインストールした SD-WAN WANOP VPX 仮想マシンが起動して実行されている場合は、物理 SD-WAN WANOP アプライアンスを構成する場合と同様に構成できます。詳しくは、[Citrix SD-WAN WANOP](#)のドキュメントを参照してください。

Amazon AWS に SD-WAN WANOP エディション AMI をインストールする

April 15, 2021

Amazon AWS 用の Citrix SD-WAN VPX は、Amazon クラウドに高速サポートを提供します。

注: 7.1.0 ソフトウェアリリースの時点では、Amazon AWS 用の SD-WAN (現 SD-WAN) WANOP-VPX のサポート対象の最新リリースは 7.0.1 です。他のアプライアンスでは、このバージョンをリリース 7.1.0 とともに使用します。

次の 5 つのバリエーションがサポートされており、そのうちの 4 つはハードワイヤードライセンスを使用し、そのうちの 1 つは通常の SD-WAN ライセンスを使用します。

- 2Mbps

- 10Mbps
- 20Mbps
- 45 Mbps
- 「自分のライセンスを持参」では、標準の Citrix ライセンスを使用して、ライセンスされた帯域幅を決定します。

ハードワイヤードライセンスに加えて、Amazon AWS 用 SD-WAN WANOP-VPX の主な違いは、管理とアクセラレーションの両方で 1 つのポートしかサポートできないことです。これは、アプライアンスをインラインモードで使用できないことを意味します。

Amazon AWS で SD-WAN WANOP-VPX を作成するには、他のインスタンスの作成と同じプロセスで、いくつかのインスタンスパラメータをデフォルト以外の設定に設定します。

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

AWS VPC に SD-WAN 仮想アプライアンスをインストールするには、AWS アカウントが必要です。AWS アカウントは、<http://aws.amazon.com/>で作成できます。SD-WAN は、AWS Marketplace で Amazon Machine Image (AMI) として利用できます。

注: Amazon は AWS ページに頻繁に小さな変更を加えているため、次の手順は正確ではない場合があります。

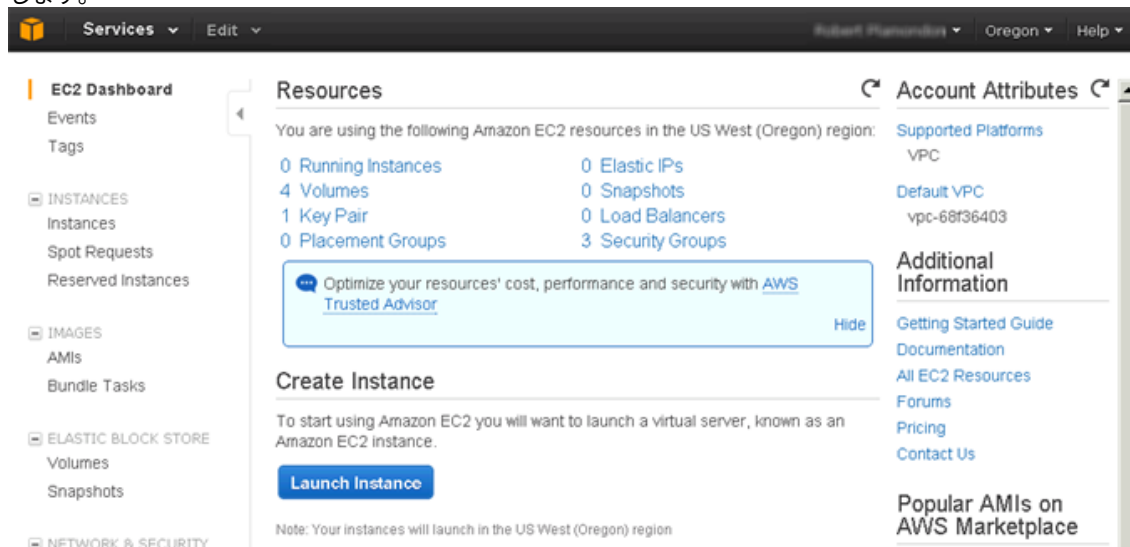
AWS で SD-WAN 仮想アプライアンス (AMI) をインスタンス化するには

1. Web ブラウザで、<http://aws.amazon.com/>と入力します。
2. [**My Account** /コンソール] をクリックし、[**My Account**] をクリックして、**Amazon Web Services** サインインページを開きます。
3. Amazon 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

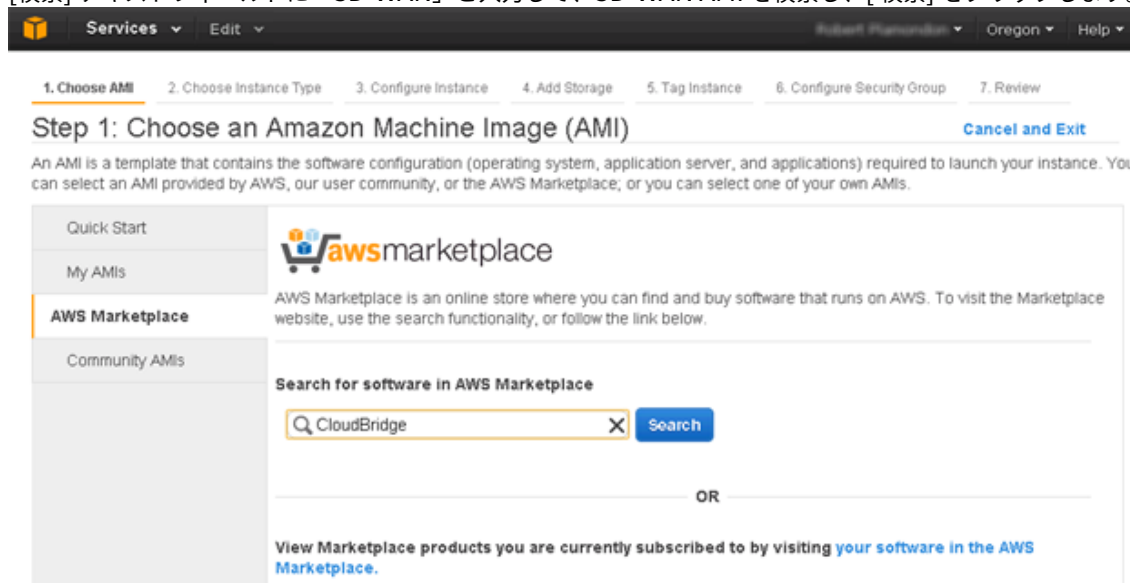


ジに移動します。

4. [コンピューティングとネットワーク] セクションで [EC2] をクリックし、[インスタンスの起動] をクリックします。



5. [新しいインスタンスの作成] ダイアログボックスで、[AWS Marketplace] を選択し、[続行] をクリックして [インスタンスリクエストウィザード] を開きます。
6. [インスタンスリクエストウィザード] ダイアログボックスで、[AWS Marketplace] タブをクリックします。
7. [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、Citrix SD-WAN サービスを 1 つ選択します [Citrix SD-WAN Citrix SD-WAN ページで、[続行] をクリックします。

8. [EC2 コンソールで起動] タブで、[** 条件に同意する] ボタン（存在する場合）をクリックし、Citrix SD-WAN AMI を起動するリージョンの [EC2 コンソールで起動] をクリックします。**

Launch on EC2:

Citrix CloudBridge VPX, Customer Licensed

Launch with EC2 Console
Info for EC2 Console or API Launches

Accept Terms

Once subscribed you will be able to launch via EC2 Console or APIs

Usage Instructions

NOTE: The CloudBridge AMI must be launched into an AWS VPC. AWS Marketplace 1-click Launch does not support launching instances into a VPC - please launch the Branch Repeater AMI using the EC2 Console or API.

To launch CloudBridge AMI
 1) Ensure you have an AWS VPC with the proper subnets already... [Show more](#)

Click "Accept Terms" to gain access to this software

Once you accept these terms, you will have access to this software in any supported region. You can then launch the AMIs listed below directly from the EC2 console, EC2 APIs, or with other AWS management tools.

Select a Version

7.0, released 08/13/2013

AMI IDs

Region	ID	
US East (Virginia)	ami-813c76e8	<input type="button" value="Launch with EC2 Console"/>
US West (Oregon)	ami-3278e702	<input type="button" value="Launch with EC2 Console"/>
US West (Northern California)	ami-82ae9bc7	<input type="button" value="Launch with EC2 Console"/>
EU West (Ireland)	ami-0a65817d	<input type="button" value="Launch with EC2 Console"/>
Asia Pacific (Singapore)	ami-18d2994a	<input type="button" value="Launch with EC2 Console"/>
Asia Pacific (Sydney)	ami-d3a33ee9	<input type="button" value="Launch with EC2 Console"/>
Asia Pacific (Tokyo)	ami-099c0308	<input type="button" value="Launch with EC2 Console"/>
South America (Sao Paulo)	ami-1b963106	<input type="button" value="Launch with EC2 Console"/>

Security Group

The vendor recommends using the following security group policies. You will be able to select these settings or configure your own when launching this software.

Connection Method	Protocol	Port Range	Source (IP or Group)
	tcp	1 - 65535	0.0.0.0/0
	udp	1 - 65535	0.0.0.0/0

Release Notes

Pricing Details

For region:

Bring Your Own License (BYOL)
Available for customers with current licenses purchased via other channels.

Hourly Fees (includes Windows 2008 R2 2008R2 x64)
Total hourly fees will vary by instance type and EC2 region.

EC2 Instance Type	Software	EC2	Total
Standard Large (m1.large)	\$0.00/hr	\$0.364/hr	\$0.364/hr

EBS Storage Fees
\$0.10 / GB / Month for Standard EBS Storage

Assumes On-Demand EC2 pricing; prices for [Reserved](#) and [Spot](#) instances will be lower. [See pricing details.](#)

This software is built on a version of EC2 that includes Windows 2008 R2 2008R2 x64.

Data transfer fees not included.

[Learn about instance types](#)

9. [インスタンスリクエストウィザード] ページの [インスタンス数] テキストボックスに「1」と入力し、[インスタンスタイプ] ドロップダウンリストから [Large (m1.large、7.5GIB)] を選択します。

Request Instances Wizard Cancel X

CHOOSE AN AMI **INSTANCE DETAILS** CREATE KEY PAIR CONFIGURE FIREWALL REVIEW

Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances.

Number of Instances: **Instance Type:**

Launch as an EBS-Optimized instance (additional charges apply):

This AMI requires a subscription and may incur additional charges not listed below. Click [here](#) for details.

Launch Instances

EC2 Instances let you pay for compute capacity by the hour with no long term commitments. This transforms what are commonly large fixed costs into much smaller variable costs.

Launch into:

Subnet: * denotes default subnet

Request Spot Instances

[Back](#) [Continue](#)

10. [**Subnet**] ドロップダウンリストから、プライベートネットワークサブネットを選択し、[**Continue**] をクリックします。
11. 次のページの [**Advanced Instance Options**] セクションで、[] を選択して、[**Continue**] をクリックします。

注: SD-WAN AMI は、複数のネットワークインターフェイスではサポートされていません。したがって、[ネットワークインターフェイスの数] フィールドの値は 1 に設定されます。

Request Instances Wizard Cancel

CHOOSE AN AMI **INSTANCE DETAILS** CREATE KEY PAIR CONFIGURE FIREWALL REVIEW

Number of Instances: 1 Availability Zone: No Preference

Advanced Instance Options

You can choose to enable CloudWatch Detailed Monitoring or enter data that will be available from your instances once they launch.

Monitoring: Enable CloudWatch detailed monitoring for this instance (additional charges will apply)

User Data: as text as file

(Use shift+enter to insert a newline)

base64 encoded

Termination Protection: Prevention against accidental termination.

IAM Role: None

Public IP: Automatically assign Public IP

Shutdown Behavior: Stop

Tenancy: Default

[< Back](#) **Continue**

12. [インスタンスのリクエストウィザード] ページで、[値] テキストボックスに EC2 インスタンスの名前を入力し、[**Continue**] をクリックします。

Request Instances Wizard Cancel

CHOOSE AN AMI **INSTANCE DETAILS** CREATE KEY PAIR CONFIGURE FIREWALL REVIEW

Add tags to your instance to simplify the administration of your EC2 infrastructure. A form of metadata, tags consist of a case-sensitive key/value pair, are stored in the cloud and are private to your account. You can create user-friendly names that help you organize, search, and browse your resources. For example, you could define a tag with key = Name and value = Webserver. You can add up to 10 unique keys to each instance along with an optional value for each key. For more information, go to [Tagging Your Amazon EC2 Resources](#) in the *EC2 User Guide*.

Key (127 characters maximum)	Value (255 characters maximum)	Remove

[Add another Tag.](#) (Maximum of 10)

[< Back](#) **Continue**

- [インスタンスのリクエストウィザード] ページで、3 つの Key ペアオプションのいずれかを選択し、[続行] をクリックします。

Request Instances Wizard Cancel

Public/private key pairs allow you to securely connect to your instance after it launches. For Windows Server instances, a Key Pair is required to set and deliver a secure encrypted password. For Linux server instances, a key pair allows you to SSH into your instance.
To create a key pair, enter a name and click **Create & Download Your Key Pair**. You will be prompted to save the private key to your computer. Note: You only need to generate a key pair once - not each time you want to deploy an Amazon EC2 instance.

Choose from your existing Key Pairs

Your existing Key Pairs*:

Create a new Key Pair

Proceed without a Key Pair

[Back](#) [Continue](#)

13. EC2 インスタンス設定の詳細を確認し、[**Launch**] をクリックして EC2 インスタンスを起動します。

Request Instances Wizard Cancel

Please review the information below, then click **Launch**.

This AMI requires a subscription and may incur additional charges not listed below. Click [here](#) for details.

AMI: Windows AMI ID ami-3278e702 (x86_64) [Edit AMI](#)

Number of Instances: 1

VPC ID: No Preference

VPC Subnet: No Preference

Availability Zone: No Preference

Instance Type: M1 Large (m1.large)

Instance Class: On Demand [Edit Instance Details](#)

EBS-Optimized: No

Monitoring: Disabled **Termination Protection:** Disabled

Tenancy: Default

Kernel ID: Use Default **Shutdown Behavior:** Stop

RAM Disk ID: Use Default

Network Interfaces: 1

Primary IP Addresses: 1 auto-assigned

Assign Public IP Address: Yes

User Data:

IAM Role: [Edit Advanced Details](#)

[Back](#) [Launch](#)

14. [閉じる] をクリックして、[インスタンス起動ウィザード] ダイアログボックスを閉じます。新しい EC2 インスタンスは正常に起動されました。

Launch Instance Wizard Cancel X

Your instances are now launching.
Instance ID(s): i-66f0ca52

Note: Your instances may take a few minutes to launch, depending on the software you are running.
Note: Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

You can perform the following tasks while your instances are launching:

- > **Create Status Check Alarms**
- > **Create EBS Volumes** (Additional charges may apply.)
- > **View your instances on the Instances page**
Note: To view the VPC ID and Subnet ID columns on the Instances page click the **Show/Hide** button and check the corresponding boxes.

Close

AWS での SD-WAN WANOP エディション AMI の SNMP モニタリングの設定

April 15, 2021

AWS の SD-WAN AMI で SNMP モニタリングを有効にする必要があります。また、SD-WAN AMI インスタンスに NSIP を追加して、ペアリングされた NetScaler VPX または SD-WAN コネクタへの SNMP 監視アクセス権を付与する必要があります。

SD-WAN グラフィカルユーザーインターフェイスを使用して **SD-WAN** コネクタ AMI で **SNMP** モニタリングを構成するには

1. ナビゲーションウィンドウで、[構成] を展開し、[ログ/監視] をクリックします。
2. 詳細ペインで、[SNMP] タブをクリックします。
3. [システム情報] セクションの [SNMP ステータス] 行で、[有効] をクリックします。このアクションにより、SD-WAN AMI インスタンスで SNMP モニタリングが有効になります。
4. [アクセス構成] セクションで、次のパラメータを設定して、**SD-WAN VPX** アプライアンスへの **SNMP** 監視アクセスを追加します。
 - コミュニティストリング (文字列 public に設定)
 - 管理ステーション IP (AWS 上の SD-WAN VPX の NSIP に設定)

Log Options | Log Extraction | Log Statistics | Log Removal | Alert Options | Syslog Server | **SNMP**

Logging/Monitoring: SNMP


System Information

SNMP Status: **NORMAL**

Name:	BR-VPX-198
Location:	<input type="text" value="public"/>
Contact:	<input type="text" value="public"/>
Enable SNMP Authorization Failure Traps:	<input type="checkbox"/>
<input type="button" value="Update"/>	

Access Configuration

ID	Community String	Management Station IP	IP Bit Mask	
1	public	10.16.3.10	32	<input type="button" value="Delete"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="32"/>	<input type="button" value="Add"/>

 SNMP management table is used to specify the SNMP management stations that would like to manage this appliance. Current support is read only.

5. [追加] をクリックします。

AWS 上の SD-WAN WANOP Edition AMI インスタンスの制限および使用上のガイドライン

April 15, 2021

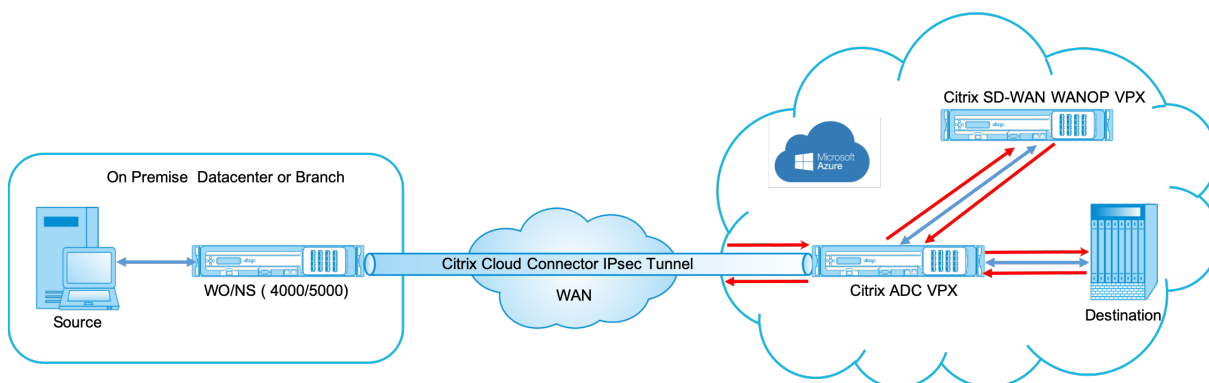
- SD-WAN AMI インスタンスの高可用性セットアップはサポートされていません。
- グループモードの SD-WAN AMI インスタンスはサポートされていません。
- SD-WAN プラグインはサポートされていません。
- タグ付き VLAN は、AWS の本質的な制限のためにサポートされていません。
- トラフィックシェーピングはサポートされていません。
- AWS では、m1.large SD-WAN AMI インスタンスのみを作成できます。
- SD-WAN 管理ユーザーインターフェイスを使用した IP アドレス、ゲートウェイ、サブネットの割り当てはサポートされていません。
- AWS の SD-WAN AMI インスタンスでは、コンソールアクセスは使用できません。
- SD-WAN インスタンスの設定中は、デフォルト値が 250 GB のディスクサイズを変更することはできません。容量の大きいディスクでは、使用可能なディスクベース圧縮 (DBC) キャッシュサイズは増加しません。

Microsoft Azure に SD-WAN WANOP VPX をデプロイする

April 15, 2021

Citrix SD-WAN WANOP エディションが Azure Marketplace で利用できるようになりました。これにより、エンタープライズデータセンター/ブランチと Azure クラウド間で WAN を最適化できます。L2 モードのサポートはクラウドインフラストラクチャでは利用できないため、Citrix SD-WAN WANOP をスタンドアロン VPX として Azure Cloud にデプロイすることはできません。ただし、Citrix クラウドインフラストラクチャに Citrix SD-WAN WANOP VPX を Citrix ADC VPX と一緒にデプロイできます。Citrix ADC VPX はクラウドコネクタを使用して IPsec トンネルを作成しますが、SD-WAN WANOP VPX は接続を高速化し、LAN に似たパフォーマンスをアプリケーションに提供します。

Azure クラウドトポロジでの Citrix SD-WAN WANOP



トポロジ図は、データセンターまたはブランチプレミスに導入された SD-WAN 4000 または 5000 アプライアンスを示しています。SD-WAN WANOP および SD-WAN SE アプライアンスは、2 ボックスモードで展開することも、両方を VPX にすることもできます。Azure クラウド VNET では、SD-WAN WANOP VPX は、Citrix ADC VPX とともにワンアーム（PBR）モードで展開されます。

展開の概要

SD-WAN WANOP を Microsoft Azure に展開するには：

1. Citrix ADC VPX インスタンスを Azure クラウドにデプロイします。詳しくは、「[Microsoft Azure で Citrix ADC VPX インスタンスを展開する](#)」を参照してください。4 つの異なるサブネットに 4 つのネットワークインターフェイスを構成し、すべてのネットワークインターフェイスで IP 転送を有効にします。4 つのネットワークインターフェイスは次のように使用されます。
 - 管理インターフェイス
 - WAN 側インターフェイス、IPsec トンネル用
 - サーバーに接続するための LAN 側インターフェイス
 - Azure クラウド上の Citrix SD-WAN WANOP VPX と通信するための WANOP 通信インターフェイス。

2. Citrix SD-WAN WANOP VPX を Azure クラウドにデプロイします。詳細については、以下の展開手順を参照してください。

注意: WANOP インターフェースで IP 転送を有効にします。

3. Citrix ADC WAN インターフェイスのパブリック IP アドレスを使用して、オンプレミスアプライアンスと Azure クラウド上の Citrix ADC VPX 間の IPsec トンネルを構成します。IP トンネルの設定の詳細については、[IP トンネル](#)を参照してください。
4. パケットを Citrix SD-WAN WANOP VPX にリダイレクトするように Citrix ADC VPX を構成します。WANOP 通信インターフェイスのプライベート IP アドレスを使用して、負荷分散仮想サーバーを作成します。詳しくは、「[負荷分散仮想サーバーの作成](#)」を参照してください。
5. Azure で次のルートテーブルを構成します。
 - Citrix ADC VPX 上の WANOP 向きインターフェイスのルートテーブル ルートテーブルエントリには、それぞれクライアントサブネットとサーバーのサブネットとして送信元アドレスと宛先アドレスを指定する必要があります。Citrix ADC VPX の WANOP 側インターフェイス IP アドレスがネクストホップです。
 - Citrix SD-WAN WANOP インターフェイスのルートテーブルルートテーブルエントリには、それぞれクライアントサブネットとサーバーのサブネットとしてソースアドレスと宛先アドレスが必要です。Citrix SD-WAN WANOP インターフェイスの IP アドレスはネクストホップです。

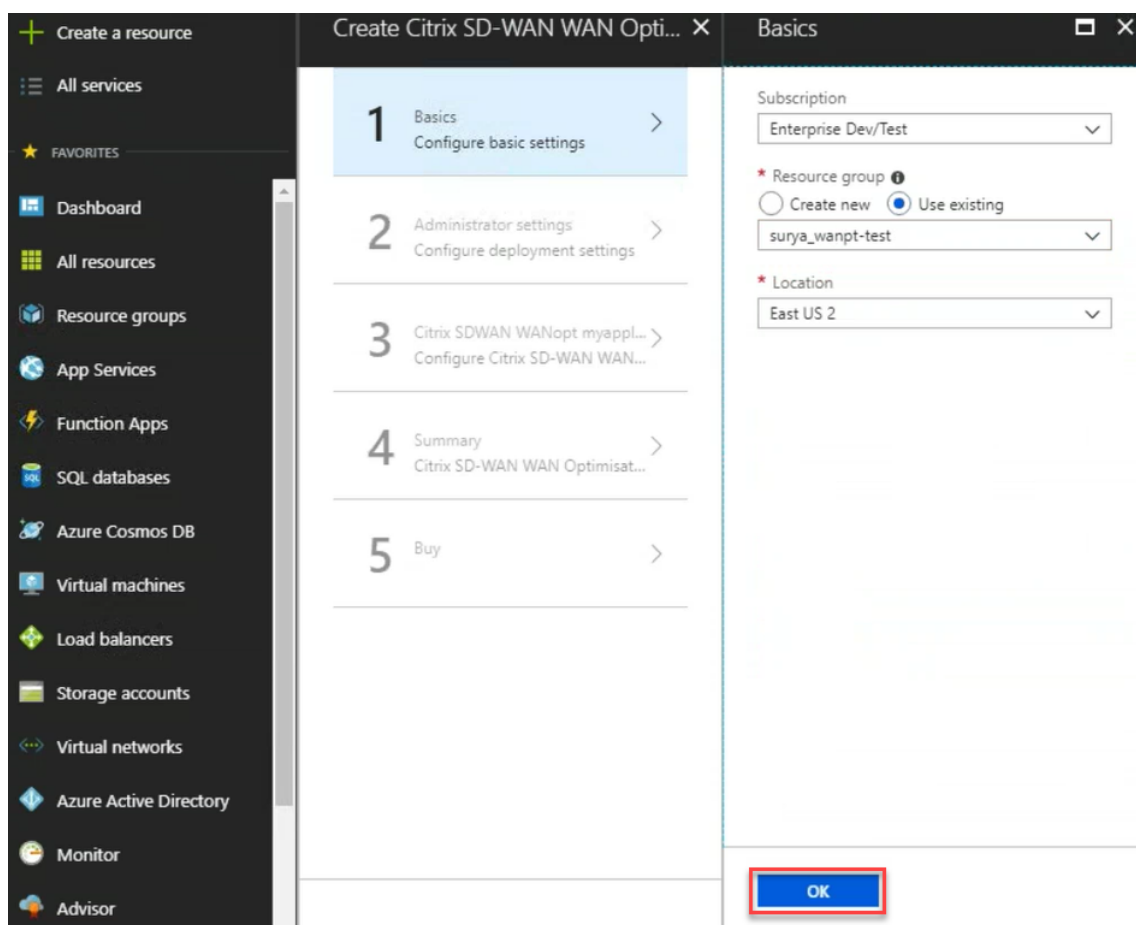
上記の例では、送信元がクラウドの宛先上のアプリケーションにアクセスしようとする、パケットは確立された IPsec トンネルを通過します。Azure クラウド VNET 側で、Citrix ADC VPX はパケットを受信し、復号化して、Citrix SD-WAN WANOP VPX に転送します。Citrix SD-WAN WANOP VPX は、パケットを処理して最適化し、Citrix ADC VPX に送り返します。Citrix ADC VPX はパケットを宛先に送信します。リターンパスでは、Citrix ADC VPX がパケットを Citrix SD-WAN WANOP VPX に転送して最適化します。最適化されたパケットは、確立された IPsec トンネルを介して送信元に返送されます。

Microsoft Azure に Citrix SD-WAN OP VPX をデプロイする

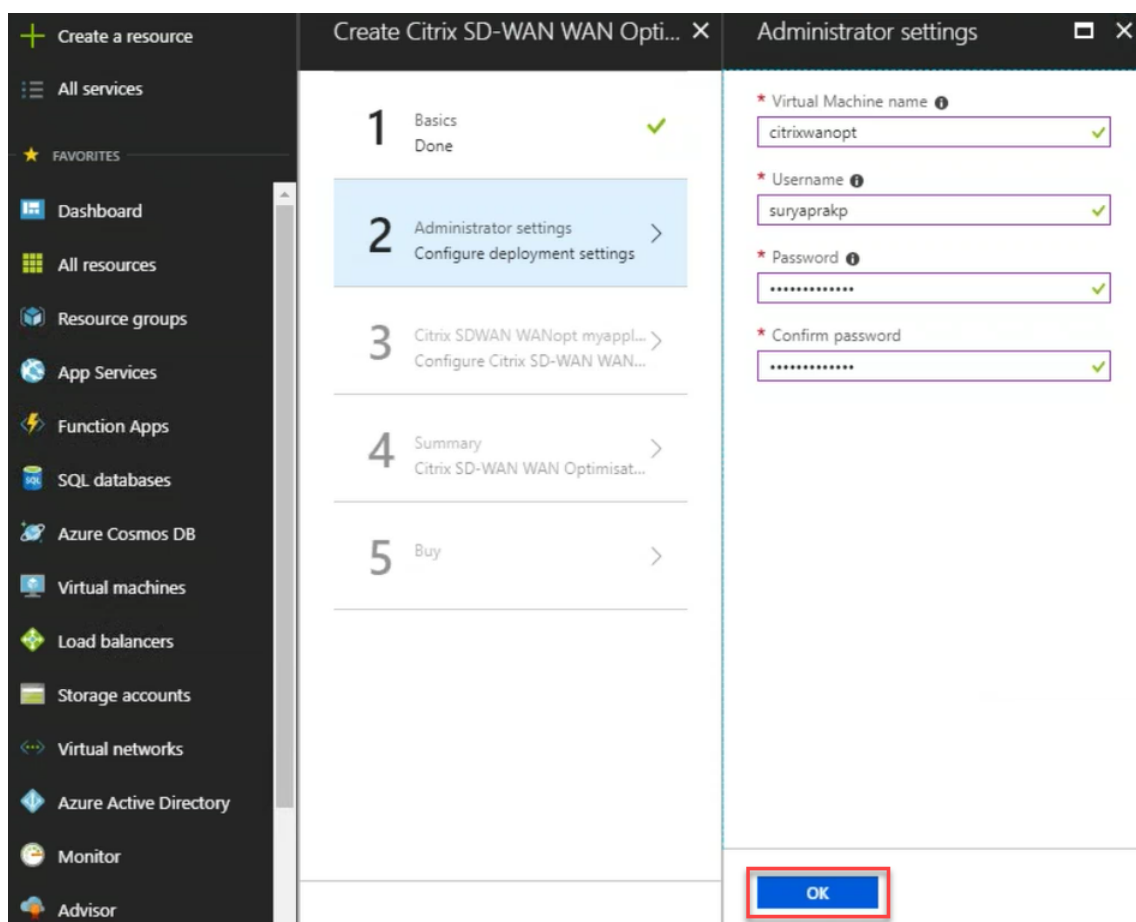
Citrix SD-WAN WANOP VPX を Microsoft Azure に展開するには:

1. Microsoft Azure で、[ホーム]>市場>ネットワークに移動し、**Citrix SD-WAN WANOP** を検索してインストールします。
2. Citrix SD-WAN WAN OP ページで、ドロップダウンリストから [リソースマネージャー] を選択し、[作成] をクリックします。[**Citrix SD-WANWAN** 最適化の作成] 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。

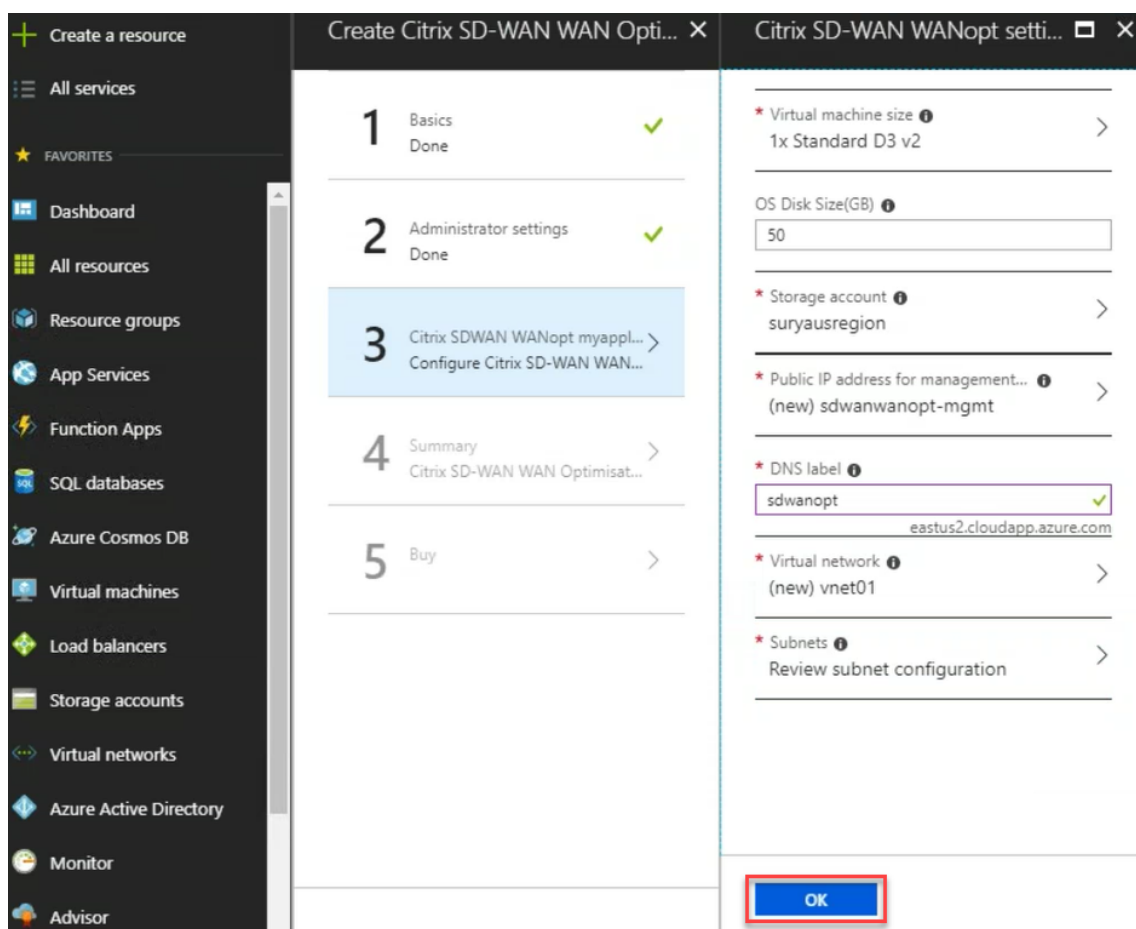
注: リソースグループの作成を選択できます。リソースグループは、Azure ソリューションの関連リソースを保持するコンテナです。リソースグループには、ソリューションのすべてのリソースを含めることも、グループとして管理するリソースのみを含めることもできます。



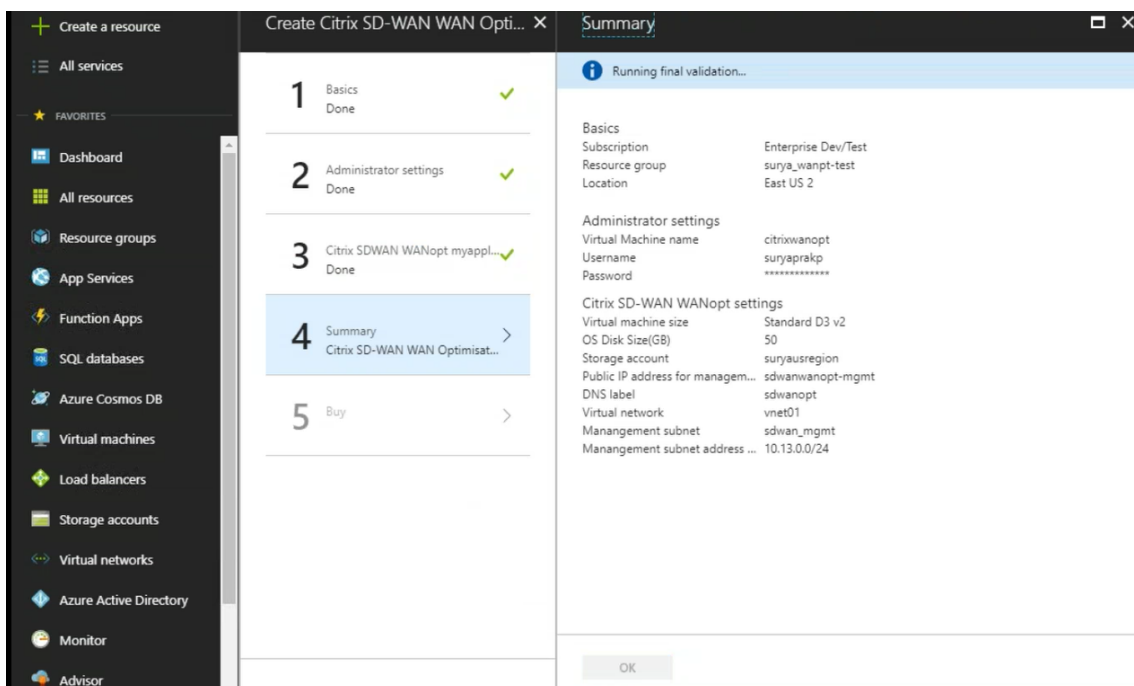
4. [管理者] セクションで、Citrix SD-WAN WANOP 仮想マシンの名前と資格情報を入力します。[OK] をクリックします。



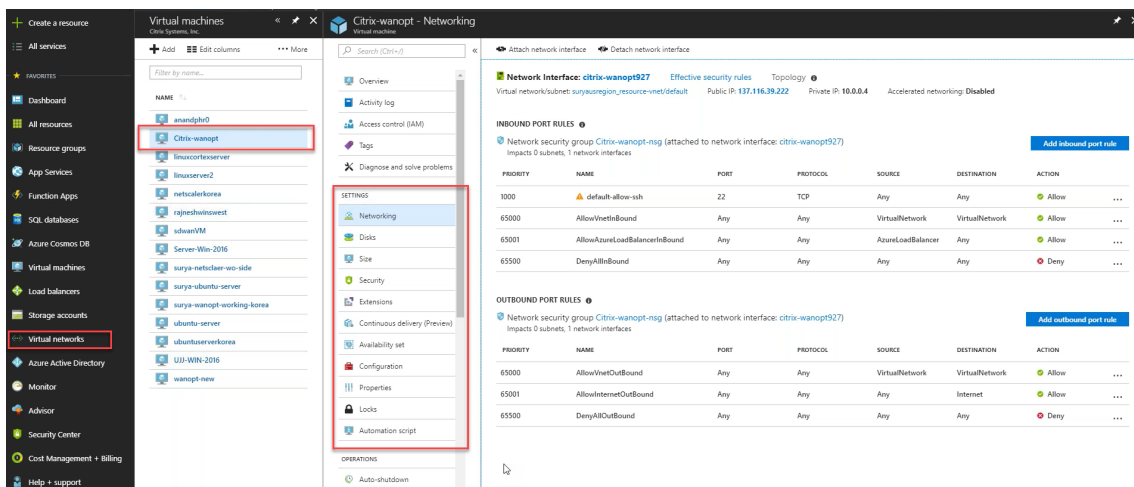
5. [**Citrix SD-WAN WANOP 設定**] セクションで、要件に応じて Citrix SD-WAN WANOP VPX の設定を構成します。[**OK**] をクリックします。



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. 導入が成功したら、仮想ネットワークに移動して Citrix SD-WAN WANOP VPX を表示します。設定オプションを使用して、仮想マシンのパラメーターをさらに構成できます。



一般的なハードウェアコンポーネント

April 15, 2021

各プラットフォームには、フロントパネルと背面パネルのハードウェアコンポーネントがあります。フロントパネルには、LCD ディスプレイとシリアルコンソールポートがあります。ポートの数、タイプ、および場所は、銅線イーサネット、銅線およびファイバ 1G SFP、および 10GSFP+ のトランシーバのハードウェアプラットフォームによって異なります。背面パネルからは、ファンとフィールド交換可能ユニット（電源、ソリッドステートドライブ、ハード

ディスクドライブ) にアクセスできます。

LCD ディスプレイと LED ステータスインジケータ

各アプライアンスの前面にある LCD ディスプレイには、アプライアンスの現在の動作ステータスに関するメッセージが表示されます。これらのメッセージは、アプライアンスが正常に起動し、正常に動作しているかどうかを伝えます。アプライアンスが正常に動作していない場合は、LCD にトラブルシューティングメッセージが表示されます。

LCD には、リアルタイムの統計情報、診断情報、およびアクティブなアラートが表示されます。LCD の寸法により、表示はそれぞれ 16 文字の 2 行に制限され、表示される情報が一連の画面に流れます。各画面には、特定の機能に関する情報が表示されます。

LCD には LED バックライトがあります。通常、バックライトは着実に光ります。アクティブなアラートがある場合、そのアラートは急速に点滅します。アラート情報が LCD 画面サイズを超えると、各表示画面の先頭でバックライトが点滅します。アプライアンスがシャットダウンすると、バックライトは 1 分間点灯したままになり、その後自動的に消灯します。

システムステータス LED は、アプライアンスの全体的なステータスを示します。次の表に、システムステータス LED のインジケータを示します。

システムステータス LED

LED カラー	LED が示す状態
オフ	電源無し
緑	アプライアンスに電力が供給されています。
赤	アプライアンスがエラーを検出しました。

ポート LED は、リンクが確立され、トラフィックがポートを通過しているかどうかを示します。次の表に、各ポートの LED インジケータを示します。ポートタイプごとに 2 つの LED インジケータがあります。

注: このセクションはすべてのアプライアンスに適用されます。

LED ポートステータスインジケータ

ポートタイプ	LED の位置	LED 機能	LED カラー	LED が示す状態
イーサネット (RJ45)	左	速度	無効	接続なし、または 10 メガビット/秒 (Mbps) のトラフィ ックレート。
			緑	トラフィックの速 度は 100Mbps。
			黄	1 ギガビット/秒の トラフィックレー ト。
	右	リンク/アクティビ ティ	無効	リンクなし。
			緑に点灯	リンクは確立され ますが、ポートを通 過するトラフィッ クはありません。
			緑で点滅	トラフィックはポ ートを通過してい ます。
マネジメント (RJ45)	左	速度	無効	接続なし、または 10 メガビット/秒 (Mbps) のトラフィ ックレート。
			緑	トラフィックの速 度は 100Mbps。
			黄	1 ギガビット/秒の トラフィックレー ト。
	右	リンク/アクティビ ティ	無効	リンクなし。
			黄色に点灯	リンクは確立され ますが、ポートを通 過するトラフィッ クはありません。

ポートタイプ	LED の位置	LED 機能	LED カラー	LED が示す状態
			黄色で点滅	トラフィックはポートを通過しています。

各電源装置の 2 色の LED インジケータは、電源装置の状態を示します。各アプライアンスの AC 電源の LED は、他のアプライアンスの LED とは異なります。

表 2。LED 電源インジケータ

電源タイプ	LED カラー	LED が示す状態
AC	オフ	電源装置に電力が供給されていません。
	赤に点滅	この電源装置に電力が供給されていません。
	緑に点滅	電源装置はスタンバイモードです。
	緑	電源は機能している。
直流	赤	電源装置の障害。
	オフ	電源装置に電力が供給されていません。
	赤に点滅	この電源装置に電力が供給されていません。
	青で点滅	電源装置はスタンバイモードです。
	青	電源は機能している。
	赤	電源装置の障害。

ポート

ポートは、アプライアンスを外部デバイスに接続するために使用されます。Citrix SD-WAN アプライアンスは、RS232 シリアルポート、10/100/1000Base-T 銅線イーサネットポート、1 ギガビットの銅線およびファイバ 1G SFP ポート、10 ギガビットファイバ SFP+、および 10G Base-T ポートをサポートします。すべての Citrix SD-WAN アプライアンスには、これらのポートの一部またはすべての組み合わせがあります。アプライアンスで使用可能なポートの種類と数の詳細については、そのプラットフォームについて説明しているセクションを参照してください。

RS232 シリアルポート

RS232 シリアル・コンソール・ポートは、アプライアンスとコンピュータ間の接続を提供し、初期構成またはトラブルシューティングのためにアプライアンスに直接アクセスできるようにします。

すべてのハードウェアプラットフォームには、コンピュータとアプライアンスの接続に使用する適切なシリアル・ケーブルが付属しています。コンピュータをアプライアンスに接続する方法については、「[ハードウェアのインストール](#)」を参照してください。

銅線イーサネットポート

アプライアンスの多くのモデルにインストールされている銅線イーサネットポートは、標準の RJ45 ポートです。

アプライアンスにインストールできる銅線イーサネットポートには、次の 2 種類があります。

- 10/100BASE-T ポート

10/100BASE-T ポートの最大伝送速度は 100 メガビット/秒 (Mbps) です。

ほとんどのプラットフォームには、少なくとも 1 つの 10/100BASE-T ポートがあります。

- 10/100/1000BASE-T ポート

10/100/1000BASE-T ポートの最大伝送速度は 1 ギガビット/秒で、他のタイプの銅線イーサネットポートの 10 倍高速です。

ほとんどのプラットフォームには、少なくとも 1 つの 10/100/1000Base-T ポートがあります。

これらのポートのいずれかをネットワークに接続するには、標準イーサネットケーブルの一方の端をポートに接続し、もう一方の端を適切なネットワークコネクタに接続します。

管理ポート

管理ポートは標準の銅線イーサネットポート (RJ45) で、システム管理機能のためにアプライアンスへの直接アクセスに使用されます。

1G SFP および 10G SFP+ ポート

1G SFP ポートは、1 Gbps の速度で動作できます。銅線イーサネットポートとして動作するための銅線 1G SFP トランシーバ、または光ファイバポートとして動作するためのファイバ 1G SFP トランシーバのいずれかを受け入れます。

10G SFP+ および Base-T 10G は高速ポートです。ポートに接続するには、光ファイバケーブルが必要です。光ファイバケーブルのもう一方の端が 1G SFP ポートに接続されている場合、10G SFP+ ポートは、1G SFP ポートの速度に合わせて自動的にネゴシエートします。

ポートの互換性:

一部のアプライアンスでは、10G スロットは銅線 1G トランシーバをサポートしており、10 Gbps スロットでは最大 1 Gbps で動作できます。

注意:

- 一部のプラットフォームには、銅線トランシーバをサポートしない 10G スロットがあります。サポートの詳細については、アカウント担当者にお問い合わせください。
- ファイバ 1G トランシーバを 10G スロットに挿入することはできません。
- 10G トランシーバを 1G スロットに挿入することはできません。

次の表に、Citrix SD-WAN プラグ可能なメディア（1G SFP および 10G SFP+ トランシーバ）の最大距離仕様を示します。

10G SFP+ モジュールはデュアルスピードに対応しており、モデルの接続先ピアスイッチに応じて、1 Gbps と 10 Gbps の両方をサポートします。

ほとんどのテーブルには、次の列があります。

- 摘要: 部品の価格表の摘要。
- 送信波長: 公称伝送波長。
- ケーブル/ファイバーの種類: ファイバー特性は達成可能な最大伝送距離に影響します。これは、マルチモードファイバ（MMF）上の 10G で、さまざまな分散コンポーネントが支配的になる場合に特に当てはまります。詳しくは、「<http://www.thefoa.org/tech/ref/basic/fiber.html>」を参照してください。
- 標準リーチ: 最大送信距離。
- 製品: 一部のシャーシは、異なるメディアオプションで利用できます。該当するデータシートを使用して、特定のシャーシタイプがメディアをサポートしていることを確認します。

1G プラグ可能なメディア

次の表に、1G トランシーバの最大距離仕様を示します。

銅 1G SFP 距離仕様

説明: 1G SFP イーサネット銅 (100 m)-4 パック

送信機の波長 (nm): 適用不可

ケーブルタイプ: カテゴリ 5 (猫 5) 銅ケーブル。

典型的なリーチ (メートル) : 100m

適用可能なプラットフォーム:

- SD-WAN 1100 SE と PE

短いリーチファイバ 1G SFP 距離仕様

説明: 1 G SFP イーサネット SX (300 m)-4 パック

送信波長 (nm): 850 nm (公称)

ファイバーの種類: 50/125um MMF、2000MHZ-km (OM3)

典型的なリーチ (メートル): 550m

ファイバーの種類: 50/125um MMF、500mHZ-km (OM2)

典型的なリーチ (m): 550m

ファイバーの種類: 50/125um MMF、400MHZ-km

典型的なリーチ (m): 550m

ファイバーの種類: 62.5/125um MMF、200mHZ-km (OM1)

典型的なリーチ (m): 300m

ファイバーの種類: 62.5/125um MMF、160MHZ-km

典型的なリーチ (m): 300m

適用可能なプラットフォーム:

- SD-WAN 1100 SE と PE

短いリーチファイバ **1G SFP** 距離仕様

説明: 1G SFP イーサネットショートレンジ (300 m) -シングル

送信波長 (nm): 850 nm (公称)

ファイバーの種類: 50/125um MMF、2000MHZ-km (OM3)

典型的なリーチ (メートル): 550m

ファイバーの種類: 50/125um MMF、500mHZ-km (OM2)

典型的なリーチ (m): 550m

ファイバーの種類: 50/125um MMF、400MHZ-km

典型的なリーチ (m): 550m

ファイバーの種類: 62.5/125um MMF、200mHZ-km (OM1)

典型的なリーチ (m): 275m

ファイバーの種類: 62.5/125um MMF、160MHZ-km

典型的なリーチ (m): 220m

適用可能なプラットフォーム:

- SD-WAN 1100 SE と PE

長いリーチファイバ **1G SFP** 距離仕様

説明: 1G SFP イーサネット LX-シングル

送信機の波長 (nm): 1310 nm (公称)

ファイバーの種類: 9/125um SMF

典型的なリーチ (メートル): 10 km

適用可能なプラットフォーム:

- SD-WAN 1100 SE と PE

長いリーチファイバ **1G SFP** 距離仕様

概要: 1G SFP イーサネット長範囲 (10 km) -シングル

送信機の波長 (nm): 1310 nm (公称)

ファイバーの種類: 9/125um SMF

典型的なリーチ (メートル): 10 km

適用可能なプラットフォーム:

- SD-WAN 1100 SE と PE

10 GE プラグ可能なメディア

次の表に、10G トランシーバの最大距離仕様を示します。

ショートリーチファイバ **10G SFP+** 距離仕様

説明	トランスミッタ波長 (nm)	ファイバーの種類	典型的なリーチ (m)
10G SFP+, イーサネット短距離 (300 m) -シングル	850 nm (公称)	50/125um MMF、 2000mHZ-km (OM3)	300 m
		50/125um MMF、 500MHZ-km (OM2)	82 m
		50/125um MMF、 400MHZ-km	66 m
		62.5/125um MMF、 200mHZ-km (OM1)	33 m
		62.5/125um MMF、 160MHZ-km	26 m

長リーチファイバ **10G SFP+** 距離仕様

概要: 10G SFP+ イーサネット長範囲 (10 km) -シングル

送信機の波長 (nm): 1310 nm (公称)

ファイバーの種類: 9/125um SMF

典型的なリーチ (メートル): 10 km

Citrix 直接接続 (DAC) 銅線 **TwinaX 10G SFP+** パッシブケーブル

説明: 1m DAC SFP+ ケーブルで最大 1m の距離まで対応

説明: 3m DAC SFP+ ケーブルで最大 3m の距離まで対応

説明: 5m DAC SFP+ ケーブル。最大 5m の距離まで対応。

フィールド交換可能ユニット

April 15, 2021

Citrix SD-WAN フィールド交換可能ユニット (FRU) は、アプライアンスから迅速かつ簡単に取り外し、ユーザーサイトのユーザーまたは技術者が交換できるコンポーネントです。Citrix SD-WAN アプライアンス用の FRU には、DC または AC 電源、ソリッドステートまたはハードディスク・ドライブ、および DAC (直接接続ケーブル) が含まれます。

注: ソリッドステートドライブまたはハードディスクドライブには構成情報が保存されるため、ユニットを交換した後にバックアップから復元する必要があります。

電源装置

2つの電源装置を含むアプライアンスの場合、2台目の電源はオプションですが、推奨されます。一部のアプライアンスでは、4つの電源装置を搭載でき、適切に動作するためには、最低でも2つの電源装置が必要です。ベストプラクティスとして、冗長性を確保するために、すべての電源装置を接続します。

アプライアンスの出荷には、アプライアンスの電源装置に差し込む標準電源コードと、ラックまたは壁面の電源コンセントに接続するための NEMA 5-15 プラグがもう一方の端に取り付けられています。

電源ファンが動作していないと思われる場合は、プラットフォームの説明を参照してください。一部のプラットフォームでは、ファンは回転せず、実際のファンは必要なときにのみ回転します。

各電源装置の2色のLEDインジケータは、電源装置の状態を示します。

電源装置の交換に関する電気的安全上の注意

通常の使用中は、アプライアンスがアースに直接物理的に接続されていることを確認します。アプライアンスを取り付けまたは修理するときは、必ずアース回路を最初に接続し、最後に切断してください。

電源コードが差し込まれているときは、電源装置に触れないでください。電源コードが差し込まれている限り、電源スイッチがオフになっていても、電源装置に回線電圧が供給されます。

AC 電源を交換してください

ほとんどの Citrix SD-WAN プラットフォームでは、2つの電源装置に対応できます。プラットフォームによっては、4つの電源装置に対応できるものもあります。すべての Citrix SD-WAN アプライアンスは、4つの電源に対応できるアプライアンスを除き、1つの電源装置で正常に機能します。これらのアプライアンスは、正常に動作するために2つの電源装置が必要です。他の電源はバックアップとして機能します。すべての電源装置が同じタイプ（AC または DC）である必要があります。

注：アプライアンスに電源装置が1つしかない場合は、電源装置を交換する前にアプライアンスをシャットダウンする必要があります。アプライアンスに電源装置が2つある場合、もう一方の電源装置が動作していれば、アプライアンスをシャットダウンせずに一方の電源装置を交換できます。また、アプライアンスに4つの電源装置がある場合は、他の2つの電源装置であれば、アプライアンスをシャットダウンせずに1つまたは2つの電源装置を交換できます。消耗品は機能しています。

Citrix SD-WAN アプライアンスに AC 電源装置を取り付けまたは交換するには：

1. 半円形のハンドルを電源装置に対して垂直に揃えます。蝶ネジを緩め、レバーをハンドルの方向に押し、既存の PSU を引き出します。
2. 新しい電源を箱から慎重に取り外します。
3. アプライアンスの背面で、電源装置を電源スロットに合わせます。
4. 電源装置をスロットに挿入し、電源装置が所定の位置に固定されるまで半円形のハンドルを押しします。
5. 電源を電源に接続します。すべての電源装置を接続する場合は、個別の電源コードを電源装置に接続し、それらを別々のコンセントに接続します。

注：Citrix SD-WAN アプライアンスは、1つの電源装置に障害が発生した場合、または2つの電源装置が取り付けられているアプライアンスに1本の電源ケーブルのみを接続すると、高ピッチの警告を発します。アラームを消音するには、アプライアンスの背面パネルにある小さな赤いボタンを押します。アラームを無効にするボタンは、アプライアンスに電源装置が2つある場合にのみ機能します。

DC 電源を交換してください

ほとんどの Citrix SD-WAN プラットフォームでは、2つの電源装置に対応できます。プラットフォームによっては、4つの電源装置に対応できるものもあります。すべての Citrix SD-WAN アプライアンスは、4つの電源に対応できるアプライアンスを除き、1つの電源装置で正常に機能します。これらのアプライアンスは、正常に動作するために2つの電源装置が必要です。他の電源はバックアップとして機能します。すべての電源装置が同じタイプ（AC または DC）である必要があります。

注: アプライアンスに電源装置が 1 つしかない場合は、電源装置を交換する前にアプライアンスをシャットダウンする必要があります。アプライアンスに電源装置が 2 つある場合、もう一方の電源装置が動作していれば、アプライアンスをシャットダウンせずに一方の電源装置を交換できます。また、アプライアンスに 4 つの電源装置がある場合は、他の 2 つの電源装置であれば、アプライアンスをシャットダウンせずに 1 つまたは 2 つの電源装置を交換できます。消耗品は機能しています。

Citrix SD-WAN アプライアンスに DC 電源装置を取り付けまたは交換するには:

1. 蝶ネジを緩め、レバーをハンドルの方向に押し、既存の PSU を引き出します。
2. 新しい電源を箱から慎重に取り外します。
3. アプライアンスの背面で、電源装置を電源スロットに合わせます。
4. レバーをハンドルの方向に押しながら、電源装置をスロットに挿入します。しっかり圧力をかけ、電源装置をスロットにしっかりと挿入します。
5. 電源装置がスロットに完全に挿入されたら、レバーを放します。
6. 電源を電源に接続します。すべての電源装置を接続する場合は、個別の電源コードを電源装置に接続し、それらを別々のコンセントに接続します。

ソリッドステートドライブ

ソリッドステートドライブ (SSD) は、ソリッドステートフラッシュメモリにデータを格納する高性能デバイスです。MPX ソリッドステートドライブには、ブートルoader構成ファイル、構成ファイル (ns.conf)、ライセンス、および一部のモデルでは、Citrix SD-WAN ソフトウェアとユーザーデータが含まれます。

すべてのプラットフォームで、Citrix SD-WAN ソフトウェアが SSD に格納されます。SSD は /flash としてマウントされます。

交換用ソリッドステートドライブ (SSD) には、Citrix SD-WAN ソフトウェアのプリインストールバージョンと汎用構成ファイル (conf) が含まれていますが、SSL 関連の証明書とキー、カスタム起動設定は含まれていません。構成ファイルとカスタマイズした設定は、お客様のサイトのバックアップストレージの場所から交換用ドライブに復元する必要があります (使用可能な場合)。

ソリッドステートドライブを交換するには:

1. Citrix SD-WAN コマンドプロンプトで、シェルプロンプトを終了します。種類:

```
shell
```
2. シェルプロンプトで次のコマンドを入力して、Citrix SD-WAN アプライアンスをシャットダウンします。

```
今すぐシャットダウン -p
```
3. アプライアンスの背面パネルにある SSD を探します。プラットフォームに応じて、ドライブカバーの安全ラッチを右または下に押し、ドライブハンドルを引き出して外します。障害のあるドライブを引き出します。
4. 交換用 SSD がプラットフォームに適したタイプであることを確認します。

5. 新しい SSD を取り上げ、ドライブハンドルを左または上に完全に開き、可能な限りドライブをスロットに挿入します。ドライブを装着するには、ハンドルをアプライアンスの背面と同じ位置で閉じ、ドライブがスロットにしっかりとロックされるようにします。

重要: ドライブを挿入するときは、ドライブが水平に挿入されている場合は上部に、ドライブが垂直に挿入されている場合は右側に Citrix 製品のラベルが表示されていることを確認します。

1. Citrix SD-WAN アプライアンスをオンにします。アプライアンスが起動すると、以前の作業構成はなくなります。したがって、アプライアンスは、デフォルトの IP アドレス 192.168.10.1 またはコンソールポートを介してのみ到達可能です。
2. 「初期構成」の説明に従って、アプライアンスの初期構成を実行します。Web ブラウザを使用してデフォルトの IP アドレスにログオンするか、コンソールケーブルを使用してシリアルコンソールに接続して初期設定を実行します。
3. プラットフォームライセンスおよびユニバーサルライセンスを含むオプション機能ライセンスを Citrix SD-WAN アプライアンスにアップロードします。
4. 正しい Citrix SD-WAN ソフトウェアのバージョンが読み込まれたら、作業構成を復元できます。

ハードディスクドライブ

ハードディスクドライブ (HDD) は、ログやその他のデータファイルを格納します。HDD に保存されるファイルには、newslog ファイル、dmesg ファイル、メッセージファイル、およびコア/クラッシュファイルが含まれます。HDD には、Citrix SD-WAN プラットフォームに応じて、さまざまな容量があります。ハードドライブは、実行時に必要なファイルを格納するために使用されます。HDD は /var としてマウントされます。

ハードディスクドライブを交換してください

ハードディスクドライブ (HDD) は、ログファイルとその他のユーザーファイルを格納します。新しいログファイルの収集は、新しい HDD で起動すると開始されます。

ハードディスクドライブをインストールするには、次の手順に従います。

1. Citrix SD-WAN コマンドプロンプトで、シェルプロンプトを終了します。種類:

```
shell
```

2. シェルプロンプトで次のいずれかのコマンドを入力して、Citrix SD-WAN アプライアンスをシャットダウンします。

```
今すぐシャットダウン -p
```

3. アプライアンスの背面パネルにあるハードディスクドライブの位置を確認します。
4. 交換用ハードディスクドライブが、Citrix SD-WAN プラットフォームに適したタイプであることを確認します。
5. プラットフォームに応じて、ドライブカバーの安全ラッチを右または下に押し、ドライブハンドルを引き出し、外し、ハードディスクドライブを取り外します。障害のあるドライブを引き出します。

- 新しいディスクドライブを取り上げ、ドライブハンドルを左側に完全に開き、新しいドライブをできるだけスロットに挿入します。ドライブを装着するには、ハンドルをアプライアンスの背面と同じ高さに関じ、ハードドライブがスロットにしっかりとロックされるようにします。

重要: ドライブを挿入するときは、Citrix 製品のラベルが先頭にあることを確認してください。

- Citrix SD-WAN アプライアンスをオンにします。アプライアンスは Citrix SD-WAN ソフトウェアを起動し、構成ファイルを読み取ります。

注

SD-WAN スタンダードエディション 400 および 410 アプライアンスには、フィールド交換可能なユニットはありません。フィールド交換可能な SSD および電源装置は不要です。

SD-WAN WANOP/SE 4000 および WANOP 5000 フィールド交換可能ユニット (FRU) は、アプライアンスから迅速かつ容易に取り外し、ユーザーまたはユーザーのサイトで技術者が交換できるコンポーネントです。SD-WAN WANOP/SE 4000 および WANOP 5000 アプライアンスの FRU には、DC または AC 電源、およびソリッドステートドライブとハードディスクドライブを含めることができます。

ポート

April 15, 2021

注

一部の Citrix SD-WAN アプライアンスは、SFP トランシーバを必要としません。

ポートは、アプライアンスを外部デバイスに接続するために使用されます。Citrix SD-WAN アプライアンスは、RS232 シリアルポート、10/100/1000Base-T 銅線イーサネットポート、ファイバ 1G SFP ポート、および 10 ギガビットファイバ SFP+ ポートをサポートします。すべての SD-WAN アプライアンスには、これらのポートの一部またはすべての組み合わせがあります。アプライアンスで使用可能なポートの種類と数の詳細については、そのプラットフォームについて説明しているセクションを参照してください。

RS232 シリアルポート

RS232 シリアル・コンソール・ポートは、アプライアンスとコンピュータ間の接続を提供し、初期構成またはトラブルシューティングのためにアプライアンスに直接アクセスできるようにします。

すべてのハードウェアプラットフォームには、コンピュータとアプライアンスの接続に使用する適切なシリアル・ケーブルが付属しています。コンピュータをアプライアンスに接続する方法については、「[ハードウェアのインストール](#)」を参照してください。

銅線イーサネットポート

アプライアンスの多くのモデルに搭載されている銅線イーサネットポートは、標準の RJ45 ポートです。

アプライアンスにインストールできる銅線イーサネットポートには、次の 2 種類があります。

- 10/100BASE-T ポート。10/100BASE-T ポートの最大伝送速度は 100 メガビット/秒 (Mbps) です。ほとんどのプラットフォームには、少なくとも 1 つの 10/100BASE-T ポートがあります。
- 10/100/1000BASE-T ポート。10/100/1000BASE-T ポートの最大伝送速度は 1 ギガビット/秒で、他のタイプの銅線イーサネットポートの 10 倍高速です。ほとんどのプラットフォームには、少なくとも 1 つの 10/100/1000Base-T ポートがあります。

これらのポートのいずれかをネットワークに接続するには、標準イーサネットケーブルの一方の端をポートに接続し、もう一方の端を適切なネットワークコネクタに接続します。

管理ポート

管理ポートは標準の銅線イーサネットポート (RJ45) で、システム管理機能のためにアプライアンスへの直接アクセスに使用されます。

1G SFP および 10G SFP+ ポート

- 1G SFP ポートは、1 Gbps の速度で動作できます。銅線イーサネットポートとして動作する場合は、銅線 1G SFP トランシーバ、または光ファイバポートとして動作するためのファイバ 1G SFP トランシーバのいずれかを受け付けます。
- 10G SFP+ ポートは、最大 10 Gbps の速度で動作できる高速ポートです。10G SFP+ ポートに接続するには、光ファイバケーブルが必要です。光ファイバケーブルのもう一方の端が 1G SFP ポートに接続されている場合、10G SFP+ ポートは、1G SFP ポートの速度に合わせて自動的にネゴシエートします。

注

SD-WAN 410-SE アプライアンスは WAN 最適化デバイスとして使用できます。最初のポートペアには、apa というラベルが付いています。

マザーボードのポートには、ポート Eth0 の MGMT というラベルが付けられています。

電源装置

April 15, 2021

Citrix SD-WAN アプライアンスは、1 つの電源で構成されています。SD-WAN 3000 WANOP アプライアンスの場合は、2 台目の電源装置を注文できます。

Citrix SD-WAN 4000、5000 WANOP/SE、4100、および 5100 SE アプライアンスは、デュアル電源で構成されますが、1 つの電源装置でのみ動作できます。2 番目の電源はバックアップとして機能します。

SD-WAN Standard Edition 410 アプライアンスの場合は、シャーシ電源スイッチが 1 台提供されます。デスクトップフォームファクタが選択されている場合、デバイスには内部電源の代わりに外部電源ブリックがあります。

表 1. LED 電源インジケータ

電源タイプ	LED カラー	LED が示す状態
AC	オフ	電源装置に電力が供給されていません。
	赤に点滅	この電源装置に電力が供給されていません。
	緑に点滅	電源装置はスタンバイモードです。
	緑	電源は機能している。
直流	赤	電源装置の障害。
	オフ	電源装置に電力が供給されていません。
	赤に点滅	この電源装置に電力が供給されていません。
	青で点滅	電源装置はスタンバイモードです。
	青	電源は機能している。
	赤	電源装置の障害。

電源装置の交換に関する電気的安全上の注意

- 通常の使用中は、アプライアンスがアースに直接物理的に接続されていることを確認します。アプライアンスを取り付けまたは修理するときは、必ずアース回路を最初に接続し、最後に切断してください。
- 修理やアップグレードを行う前に、必ずアプライアンスを取り外してください。
- 電源コードが差し込まれているときは、電源装置に触れないでください。電源コードが差し込まれている限り、電源スイッチがオフになっていても、電源装置に回線電圧が供給されます。

AC 電源装置の交換

AC 電源装置を別の AC 電源装置と交換してください。すべての電源装置が同じタイプ (AC または DC) である必要があります。

注: もう一方の電源装置が動作していれば、アプライアンスをシャットダウンせずに、一方の電源装置を交換できます。

Citrix SD-WAN 4000/5000 アプライアンスに AC 電源装置を取り付けまたは交換するには

1. 半円形のハンドルを電源装置に対して垂直に揃えます。次の図に示すように、蝶ネジを緩めてレバーをハンドルの方向に押し、既存の PSU を引き出します。

図 1: 既存の AC 電源装置の取り外し

[ローカライズされた画像](#)

2. 新しい電源を箱から慎重に取り外します。
3. アプライアンスの背面で、電源装置を電源スロットに合わせます。
4. 電源装置をスロットに挿入し、電源装置が所定の位置に固定されるまで半円形のハンドルを押しします。

図 2: 交換用 AC 電源の挿入



5. 電源を電源に接続します。すべての電源装置を接続する場合は、個別の電源コードを電源装置に接続し、それらを別々のコンセントに接続します。

注: SD-WAN 4000/5000 アプライアンスは、1つの電源装置に障害が発生した場合、または2つの電源装置が取り付けられているアプライアンスに1つの電源ケーブルだけを接続すると、高ピッチの警告を發します。アラームを消音するには、アプライアンスの背面パネルにある小さな赤いボタンを押します。アラームを無効にするボタンは、アプライアンスに電源装置が2つある場合にのみ機能します。

DC 電源装置の交換

DC 電源装置を別の DC 電源装置と交換してください。すべての電源装置が同じタイプ (AC または DC) である必要があります。

注: もう一方の電源装置が動作していれば、アプライアンスをシャットダウンせずに、一方の電源装置を交換できます。

Citrix SD-WAN 4000/5000 アプライアンスで DC 電源装置を取り付けまたは交換するには

1. 次の図に示すように、蝶ネジを緩めてレバーをハンドルの方向に押し、既存の PSU を引き出します。

図 3: 既存の DC 電源装置の取り外し



2. 新しい電源を箱から慎重に取り外します。
3. アプライアンスの背面で、電源装置を電源スロットに合わせます。
4. レバーをハンドルの方向に押しながら、電源装置をスロットに挿入します。しっかり圧力をかけ、電源装置をスロットにしっかりと挿入します。

図 4: 交換用 DC 電源装置の挿入



5. 電源装置をスロットに挿入したら、レバーを放します。
6. 電源を電源に接続します。すべての電源装置を接続する場合は、個別の電源コードを電源装置に接続し、それらを別々のコンセントに接続します。

注: SD-WAN 4000/5000 アプライアンスは、1つの電源装置に障害が発生した場合、または2つの電源装置が取り付けられているアプライアンスに1つの電源ケーブルだけを接続すると、高ピッチの警告を發します。アラームを消音するには、アプライアンスの背面パネルにある小さな赤いボタンを押します。アラームを無効にするボタンは、アプライアンスに電源装置が2つある場合にのみ機能します。

SD-WAN 2000 アプライアンスは、1つの電源装置だけに対応できますが、フィールド交換はできません。SD-WAN 3000 アプライアンスには電源装置が1つしかありませんが、2台目の電源装置を注文して設置できます。

SD-WAN 3000 アプライアンスに AC 電源装置を取り付けまたは交換するには

1. 既存の電源装置を交換する場合は、半円形のハンドルを電源装置に垂直になるように合わせ、蝶ネジを緩め、レバーをハンドルに向かって押し、既存の電源装置を引き出します。
2. 新しい電源を箱から慎重に取り外します。
3. アプライアンスの背面で、電源装置を電源スロットに合わせます。
4. 電源装置をスロットに挿入し、電源装置が所定の位置に固定されるまで半円形のハンドルを押します。
5. 電源を電源に接続します。

注

もう一方の電源装置が動作していれば、アプライアンスをシャットダウンせずに 1 つの電源装置を交換できます。

ソリッドステートドライブ

April 15, 2021

ソリッドステートドライブ (SSD) は、ソリッドステートフラッシュメモリにデータを格納する高性能デバイスです。

ソリッドステートドライブを交換してください

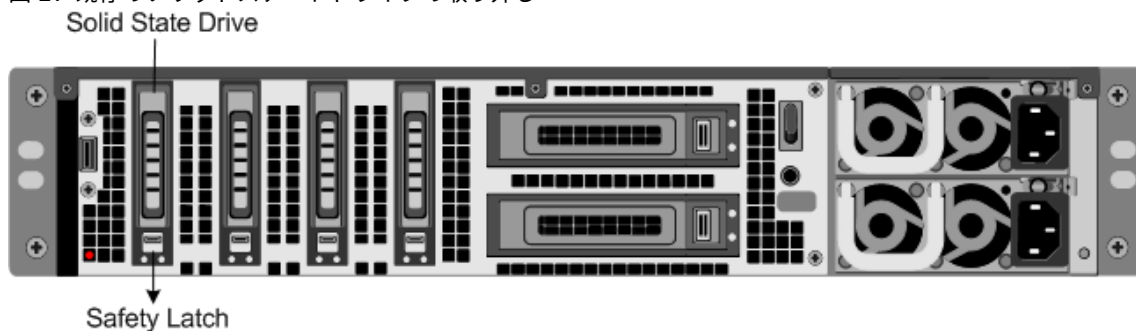
SD-WAN 4000/5000 ソフトウェアは、ソリッドステートドライブ (SSD) に格納されています。

Citrix SD-WAN 410 アプライアンスの場合、オンボード SATA ディスクコントローラが少なくとも 2 つのデバイスをサポートする必要があります。SataV3 (6 Gbps) のサポートが利用可能です。

ソリッドステートドライブを交換するには

1. アプライアンスをシャットダウンします。
2. アプライアンスの背面パネルにある SSD を探します。プラットフォームに応じて、ドライブカバーの安全ラッチを右または下に押し、ドライブハンドルを引き出して外します。障害のあるドライブを引き出します。

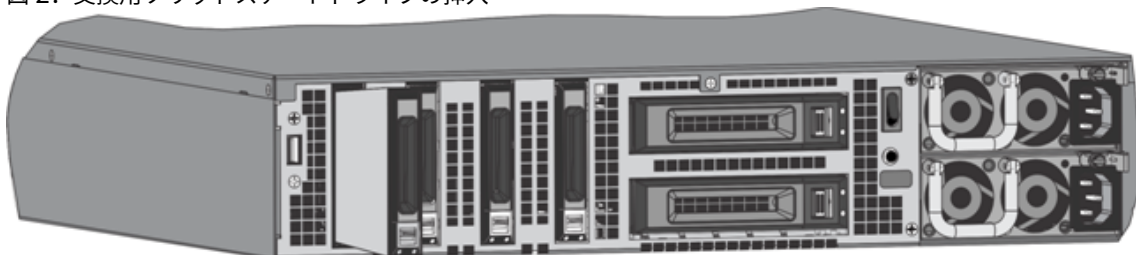
図 1: 既存のソリッドステートドライブの取り外し



3. 交換用 SSD がプラットフォームに適したタイプであることを確認します。
4. 新しい SSD を取り上げ、ドライブハンドルを左または上に完全に開き、可能な限りドライブをスロットに挿入します。ドライブを装着するには、ハンドルをアプライアンスの背面と同じ位置で閉じ、ドライブがスロットにしっかりとロックされるようにします。

重要: ドライブを挿入するときは、ドライブが水平に挿入されている場合は上部に、ドライブが垂直に挿入されている場合は右側に Citrix 製品のラベルが表示されていることを確認します。

図 2: 交換用ソリッドステートドライブの挿入



5. アプライアンスの電源を入れます。
6. Web ブラウザを使用してデフォルトの IP アドレスにログオンするか、コンソールケーブルを使用してシリアルコンソールに接続して初期設定を実行します。

ハードディスクドライブ

April 15, 2021

Citrix SD-WAN 仮想マシンは、ハードディスクドライブ上でホストされます。

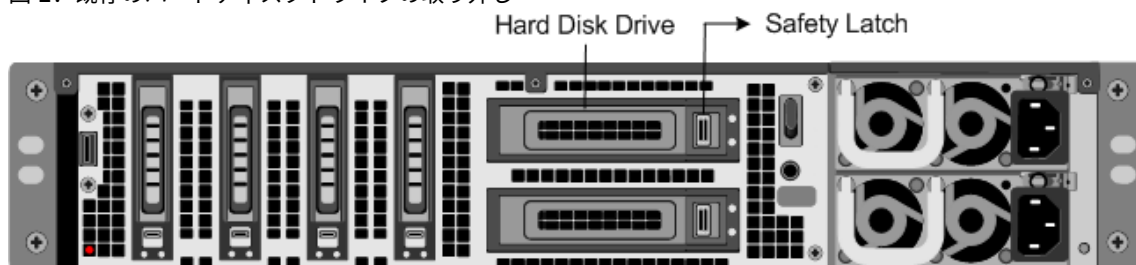
ハードディスクドライブを交換してください

交換用ハードディスクドライブが SD-WAN 4000/5000 プラットフォームに適したタイプであることを確認します。

ハードディスクドライブをインストールするには

1. アプライアンスをシャットダウンします。
2. アプライアンスの背面パネルにあるハードディスクドライブの位置を確認します。
3. プラットフォームに応じて、ドライブカバーの安全ラッチを右または下に押し、ドライブハンドルを引き出して外し、ハードディスクドライブを取り外します。障害のあるドライブを引き出します。

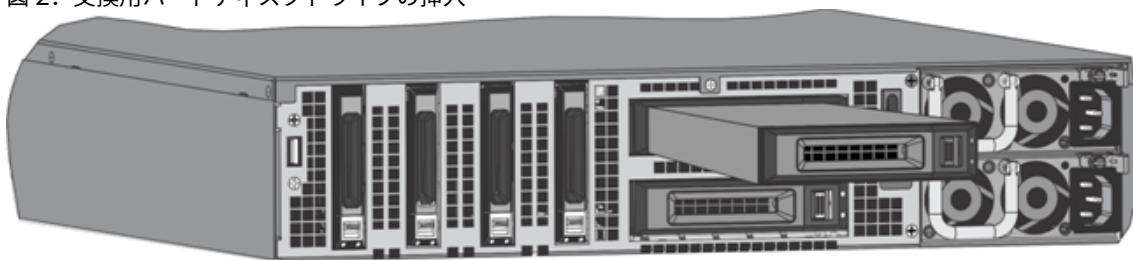
図 1: 既存のハードディスクドライブの取り外し



4. 新しいディスクドライブを取り上げ、ドライブハンドルを左側に完全に開き、新しいドライブをできるだけスロットに挿入します。ドライブを装着するには、ハンドルをアプライアンスの背面と同じ高さに閉じ、ハードドライブがスロットにしっかりとロックされるようにします。

重要: ドライブを挿入するときは、Citrix 製品のラベルが先頭にあることを確認してください。

図 2: 交換用ハードディスクドライブの挿入



5. アプライアンスの電源を入れます。

1G SFP トランシーバの取り付けと取り外し

April 15, 2021

注: 一部の SD-WAN 4000/5000 アプライアンスは SFP トランシーバを必要としません。

SFP (Small Form-Factor Pluggable) は、最速 1 ギガビット/秒で通信し、銅線タイプでもファイバータイプでも使用できるコンパクトなトランシーバーです。1G SFP 銅線トランシーバーを装着すると、1G SFP ポートが 1000BASE-T ポートに変換されます。1G SFP ファイバートランシーバーを装着すると、1G SFP ポートが 1000BASE-X ポートに変換されます。1G SFP トランシーバーを装着した 1G SFP ポートでは、オートネゴシエーションがデフォルトで有効になります。ポートとネットワーク間のリンクが確立されると、ケーブルの両端で速度とモードが一致します。

アプライアンスの前面パネルにある 1G SFP ポートに、1G SFP トランシーバーを挿入します。トランシーバーの取り付けと取り外しを頻繁に行うと、トランシーバーの寿命が短くなります。1G SFP トランシーバーまたはアプライアンスを損傷しないように、取り外しは正しい手順で行ってください。

警告: SD-WAN 4000/5000 アプライアンスは、Citrix システムズ以外のベンダーからの 1G SFP トランシーバをサポートしていません。サードパーティ製 1G SFP トランシーバを SD-WAN 4000/5000 アプライアンスにインストールしようとする、保証が無効になります。ケーブルを装着した状態でトランシーバーを取り付けないでください。これを行うと、ケーブル、コネクタ、またはトランシーバーの光インターフェイスが損傷する可能性があります。

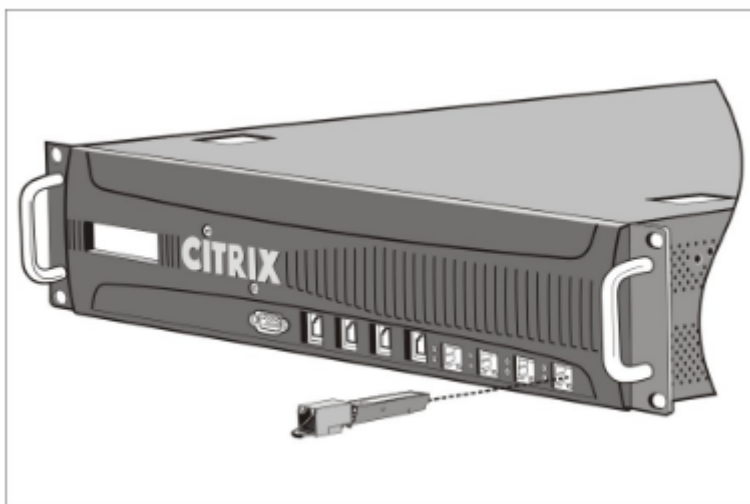
1G SFP トランシーバーを取り付けるには

1. 1G SFP トランシーバーを慎重に箱から取り出します。

危険: 光ファイバートランシーバやケーブルを直接調べないでください。レーザービームが放射されて目が傷つくおそれがあります。

2. 次の図に示すように、1G SFP トランシーバーと、アプライアンスの前面パネルにある 1G SFP トランシーバーポートの前面の位置を合わせます。

3. 親指と人差し指で 1G SFP トランシーバーを持ち、1G SFP トランシーバーポートに挿入し、トランシーバーを定位置にはめ込むようにカチッという音がするまで押し込みます。
4. トランシーバーをロックします。
5. LED が緑色で 2 回点滅するのを確認します。これは、トランシーバーが正常に機能していることを示します。
6. 光ファイバー 1G SFP トランシーバーを使用している場合は、ケーブルを挿入できる状態になるまでは、トランシーバーおよびケーブルに取り付けられている埃除けキャップを外さないでください。



注

次の図は、実際のアプライアンスと異なる可能性があります。

1G SFP トランシーバーを取り外すには

1. 1G SFP トランシーバーからケーブルを外します。光ファイバーケーブルを使用している場合は、ケーブルをしまう前にケーブルに埃除けキャップを取り付けてください。
危険: 光ファイバートランシーバやケーブルを直接調べないでください。レーザービームが放射されて目が傷つくおそれがあります。
2. 1G SFP トランシーバーのロックを解除します。
3. 親指と人差し指で 1G SFP トランシーバーを持ち、ポートからゆっくりと引き抜きます。
4. 光ファイバー 1G SFP トランシーバーを取り外す場合は、トランシーバーをしまう前に埃除けキャップを取り付けてください。
5. 1G SFP トランシーバーを元箱または代わりの容器に入れます。

10G SFP+ トランシーバの取り付けと取り外し

April 15, 2021

警告

ケーブルを装着した状態でトランシーバーを取り付けしないでください。これを行うと、ケーブル、コネクタ、またはトランシーバーの光インターフェイスが損傷する可能性があります。

注

SD-WAN 4100/5100 アプライアンスの中には、SFP+ トランシーバを必要としないものがあります。

10 ギガビット小型フォームファクタプラグ (SFP+) は、最大 10 ギガビット/秒の速度で動作できるコンパクトな光トランシーバです。自動ネゴシエーションは、10G SFP+ トランシーバを挿入する 10G SFP+ ポートでデフォルトで有効になっています。ポートとネットワーク間のリンクが確立されると、ケーブルの両端でモードが一致し、10G SFP+ トランシーバの場合、速度も自動ネゴシエーションされます。

10G SFP+ トランシーバをアプライアンスの前面パネルの 10G SFP+ ポートに挿入します。トランシーバーの取り付けと取り外しを頻繁に行うと、トランシーバーの寿命が短くなります。トランシーバーまたはアプライアンスの損傷を防ぐため、注意深く取り外し手順に従ってください。

重要

SD-WAN 4100/5100 アプライアンスは、Citrix システムズ以外のベンダーが提供する 10G SFP+ トランシーバをサポートしていません。サードパーティ製 10G SFP+ トランシーバを SD-WAN 4100/5100 アプライアンスにインストールしようとすると、保証が無効になります。

10G SFP+ トランシーバを取り付けるには

1. 10G SFP+ トランシーバをボックスから慎重に取り外します。
2. 10G SFP+ トランシーバをアプライアンスの前面パネルの 10G SFP+ トランシーバポートの前面に合わせます。
3. 10G SFP+ トランシーバを親指と人差し指の間に持ち、10G SFP+ トランシーバポートに挿入し、トランシーバが所定の位置にスナップする音がするまで押し込みます。
4. ロックヒンジを下の位置に移動します。
5. LED が緑色で 2 回点滅するのを確認します。これは、トランシーバーが正常に機能していることを示します。
6. ケーブルを挿入できる状態になるまでは、トランシーバーおよびケーブルに取り付けられている埃除けキャップを外さないでください。

警告

光ファイバーのトランシーバーおよびケーブルを直接のぞき込まないでください。レーザービームが放射されて目が傷つくおそれがあります。

10G SFP+ トランシーバを取り外すには

1. 10G SFP+ トランシーバからケーブルを取り外します。取り外す前にケーブルに埃除けキャップを取り付けてください。
2. 10G SFP+ トランシーバをロック解除するには、ロックヒンジを UP の位置に移動します。

3. 10G SFP+ トランシーバを親指と人差し指の間に持ち、ゆっくりとポートから引き出します。
4. 取り外す前にトランシーバーに埃除けキャップを取り付けてください。
5. 10G SFP+ トランシーバを元のボックスまたは別の適切な容器に入れます。

法令順守

April 15, 2021

サプライヤーの適合宣言書

このページに記載されている FCC コンプライアンスステートメントは、すべての Citrix SD-WAN ハードウェアモデルに適用されます。

責任者 — 米国の連絡先情報:

```
1 Citrix Systems, Inc.  
2 4988 Great America Parkway  
3 Santa Clara, CA  
4 95054 USA  
5  
6 compliance.prime@citrix.com  
7 <!--NeedCopy-->
```

このデバイスは、FCC ルールのパート 15 に準拠しています。操作には、次の 2 つの条件が適用されます。

1. このデバイスは有害な干渉を引き起こさない可能性があります。
2. このデバイスは、望ましくない動作を引き起こす可能性のある干渉を含む、受信した干渉を受け入れなければなりません。

注

この機器は、FCC 規則のパート 15 に従って、クラス A のデジタルデバイスの制限に準拠していることがテストされ、確認されています。これらの制限は、機器が商業環境で運用されている場合に、有害な干渉に対して合理的な保護を提供するように設計されています。この装置は、無線周波数エネルギーを生成、使用、および放射することができます。取扱説明書に従って取り付け使用しない場合、この機器は無線通信に有害な干渉を引き起こす可能性があります。住宅街でこの機器を操作すると、有害な干渉を引き起こす可能性があります。ユーザーは、自己負担で干渉を修正する必要があります。

Citrix SD-WAN 110-LTe-Wi-Fi-SE コンプライアンス

Citrix SD-WAN 110-LTe-WiFi-SE 準拠および適合宣言の詳細については、次のリンクを参照してください。

- [Citrix SD-WAN 110-LTe-Wi-Fi-SE コンプライアンス](#)
- [EU 適合宣言書](#)

Citrix SD-WAN 110-WiFi-SE コンプライアンス

Citrix SD-WAN 110-WiFi-SE 準拠および適合宣言の詳細については、次のリンクを参照してください。

- [Citrix SD-WAN 110-WiFi-SE コンプライアンス](#)
- [EU 適合宣言書](#)

台湾 BSMI RoHS ステートメント

April 15, 2021

次の表は、Citrix SD-WAN ハードウェアアプライアンスの制限物質の存在状態の宣言です。

限用物質含有状況標示聲明書

Declaration of the Presence Condition of Restricted Substances

設備名稱：網路負載均衡設備(服務器)						
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr ⁶⁺)	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
金屬外殼	○	○	○	○	○	○
印刷電路板	○	○	○	○	○	○
電源供應器	○	○	○	○	○	○
風扇	○	○	○	○	○	○
外殼前面板	○	○	○	○	○	○
配件(電源線、傳輸線)	○	○	○	○	○	○
備考1. "超出0.1 wt %" 及 "超出0.01 wt %" 係指限用物質之百分比含量超出百分比含量基準值。 Note 1: "Exceeding 0.1 wt %" and "exceeding 0.01 wt %" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.						
備考2. "○" 係指該項限用物質之百分比含量未超出百分比含量基準值。 Note 2: "○" indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.						
備考3. "—" 係指該項限用物質為排除項目。 Note 3: The "-" indicates that the restricted substance corresponds to the exemption.						

限用物質含有状況標示証明書

Declaration of the Presence Condition of Restricted Substances

設備名稱： 網路負載均衡設備						
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr ⁶⁺)	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
金屬外殼	○	○	○	○	○	○
印刷電路板	○	○	○	○	○	○
電源供應器	○	○	○	○	○	○
風扇	○	○	○	○	○	○
外殼前面板	○	○	○	○	○	○
配件(電源線、傳輸線)	○	○	○	○	○	○
備考1. "超出0.1 wt %" 及 "超出0.01 wt %" 係指限用物質之百分比含量超出百分比含量基準值。 Note 1 : "Exceeding 0.1 wt %" and "exceeding 0.01 wt %" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.						
備考2. "○" 係指該項限用物質之百分比含量未超出百分比含量基準值。 Note 2 : "○" indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.						
備考3. "—" 係指該項限用物質為排除項目。 Note 3 : The "-" indicates that the restricted substance corresponds to the exemption.						

ハードウェアの取り付け

April 15, 2021

アプライアンスの設置場所が環境基準を満たしており、指示に従ってサーバラックが配置されていることを確認したら、ハードウェアを取り付ける準備が整います。アプライアンスをマウントしたら、ネットワーク、電源、および初期設定に使用するコンソール端末に、アプライアンスを接続する準備が整いました。インストールを完了するには、アプライアンスをオンにします。インストール手順に記載されている注意事項と警告を必ず守ってください。

特定のシリーズでは、すべてのモデルが同じハードウェアを使用し、異なるライセンスオプションを使用して異なる WAN 速度定格を取得できます。たとえば、両方の SD-WAN 400 モデル (400-002 および 400-006) で同じハードウェアを使用し、特定のライセンスを 2 Mbps アプライアンスまたは 6 Mbps アプライアンスのいずれかにライセンスを付与できますが、SD-WAN 400 を SD-WAN 800、1000、2000、または 3000 にアップグレードすることはできません。同じことが他のシリーズにも当てはまります。

ライセンスされた帯域幅は送信方向にのみ適用されるため、12 Mbps/2 Mbps のダウンロード/アップロード帯域幅を持つ ADSL リンクには、送信方向で 2 Mbps の定格の SD-WAN 400-002 が適しています。

Windows Server がインストールされた SD-WAN 1000 アプライアンスでは、このポートは MGMT (管理) ポートとラベル付けされ、Windows Server がインストールされている SD-WAN 2000 アプライアンスでは、ポートは PRI (プライマリ) ポートとラベル付けされます。インストールを完了するには、アプライアンスのスイッチをオンに

します。インストール手順に記載されている注意事項と警告を必ず守ってください。

WAN 帯域幅機能の違いに加えて、CPU パワー、インストールされている RAM、およびインストールされているディスク容量が異なるシリーズもあります。

すべてのモデルは、スピードと信頼性を向上させるため、従来のハードドライブの代わりにソリッドステートドライブを使用しています。

インストールの準備

April 15, 2021

新しいアプライアンスを設置する前に、アプライアンスを慎重に開梱し、すべての部品が納入されたことを確認してください。アプライアンスが期待どおりに供給されたことを確認したら、アプライアンスの設置場所が温度と電力要件を満たしていること、およびサーバキャビネットまたは床から天井までのキャビネットが床に固定され、十分な通気量があることを確認します。

アプライアンスの設置、メンテナンス、または交換は、トレーニングを受けた資格のある担当者のみが行う必要があります。また、すべての注意事項と警告に従うように努める必要があります。

アプライアンスの解凍

April 15, 2021

広いスペースのある頑丈なテーブルの上で新しいアプライアンスを含むボックスを開梱し、内容を確認します。

Citrix SD-WAN 4100、5100、または 6100 を注文した場合は、次の一覧を使用して、ボックスに含める必要があるすべてのものを受け取ったことを確認します。

- 注文したアプライアンス
- RJ-45 to DB-9 アダプター 1 個
- 6 フィートの RJ-45/DB-9 ケーブル 1 本
- 電源ケーブル 2 本
- 標準 4 ポストレールキット 1 つ

新しいアプライアンスのボックスに含まれている項目に加えて、インストールと初期構成プロセスを完了するには、次の項目が必要です。

- ネットワークに接続する追加のイーサネットポートごとに Ethernet ケーブル
- ネットワークに接続するイーサネットポートごとに、ネットワークスイッチまたはハブの 1 つの使用可能なイーサネットポート
- 管理用のワークステーションとして使用するコンピューター

注

受け取ったキットがラックに合わない場合は、Citrix 製品の販売担当者に連絡し、適切なキットを注文してください。

現場とラックの準備

April 15, 2021

SD-WAN 4100/5100 アプライアンスには、特定のサイトおよびラック要件があります。適切な環境制御と電力密度が利用可能であることを確認する必要があります。ラックは、アースにボルトで固定され、十分な通気量があり、十分な電源とネットワーク接続が必要です。設置場所とラックの準備は、設置プロセスの重要な段階であり、円滑な設置を実現します。

サイトの要件

アプライアンスは、次の機能を備えたサーバールームまたはサーバキャビネットに設置する必要があります。

環境制御

エアコン、好ましくは専用のコンピュータールームエアコン (CRAC)、2100 メートル/ 7000 フィートまでの高度で 27 度 C/80.6°F 以下の温度でキャビネットまたはサーバールームを維持することができ、より高い高度では 18 度 C/64.4 度 F、湿度レベルを超えない湿度 45 パーセント、そしてほこりのない環境。

電力密度

CRAC に必要な電力に加えて、ラックユニットあたり 4,000 ワット以上を処理できる配線。

ラックの要件

アプライアンスを設置するラックは、次の条件を満たす必要があります。

ラックの特性

ラックは、専用設計のサーバキャビネットに統合するか、床から天井までのタイプで、安定性を確保するために、上部と下部の両方にボルトで固定する必要があります。キャビネットがある場合は、安定性と十分な通気のために、耐荷重壁に垂直に設置する必要があります。サーバールームがある場合は、十分な通気を確保するために、ラックは 1 メートル/3 フィート以上の間隔に配置された列に設置する必要があります。ラックでは、IT 担当者が各サーバの前面と背面、およびすべての電源とネットワーク接続に自由にアクセスできるようにする必要があります。

電源接続

ユニットごとに最低 2 つの標準電源コンセント。

ネットワーク接続

少なくとも、ラックユニットあたりのイーサネット接続。

スペース要件

SD-WAN 4100/5100 アプライアンス用の 2 つの空のラックユニット。

以下のレールキットは別途注文できます。

- 23~33 インチのラックにフィットするコンパクトな 4 支柱レールキット。
- 2 支柱レールキット、2 支柱ラックに適合します。

注意事項と警告

April 15, 2021

警告

取り付けまたはメンテナンスの手順では、アプライアンスの電子機器の静電気損傷を避けるために、アース用リストストラップを着用してください。導電性リストストラップを良好な接地、またはアプライアンスに接続して使用してください。背面の ESD シンボルのそばにあるコネクタに接続できます。

電気安全上の注意

危害や器具の損傷から身を守るために、基本的な電気的安全対策に従ってください。

- 緊急電源オフ（EPO）スイッチの位置に注意して、電気事故が発生した場合にアプライアンスの電源をすばやく取り外すことができます。
- アプライアンスの取り付けまたは修理を行う前に、電源やワイヤに接触する可能性のあるジュエリーやその他の金属オブジェクトをすべて取り外してください。ライブ電源またはワイヤとアースの両方に触れると、金属物体が急速に加熱し、火傷を引き起こしたり、衣服に火をつけたり、金属オブジェクトを露出した端子に溶け出したりすることがあります。
- 電源サージや電圧スパイクからアプライアンスを保護し、電源障害が発生した場合でも、アプライアンスの動作を維持するには、安定化無停電電源装置（UPS）を使用します。
- アプライアンスを他のサーバーや電子機器の上に積み重ねないでください。
- すべてのアプライアンスは、TN アースを使用する電源システムに設置されています。TT または IT アースを使用する電源システムにデバイスを設置しないでください。

- 通常の使用中は、アプライアンスが地球に直接物理的に接続されていることを確認します。アプライアンスを設置または修理するときは、必ずアース回路が最初に接続され、最後に切断されていることを確認してください。
- アプライアンスが接続されている電源システムのすべての通電導体に、120 VAC、15 A 米国（240 VAC、16 A 国際）以下のヒューズまたは回路ブレーカが使用されていることを確認します。
- 高電圧部品を扱うときは、単独では動作しないでください。
- コンポーネントの取り外しまたは取り付けを行う前に、必ずアプライアンスを電源から外してください。電源を切断するときは、まずアプライアンスをシャットダウンしてから、アプライアンスに接続されているすべての電源装置の電源コードを取り外します。電源コードが差し込まれている限り、電源スイッチがオフの場合でも、電源モジュールに回線電圧が存在する可能性があります。
- 電気ショックからの保護として、静電気放電を減らすように設計されたマットを使用しないでください。代わりに、電気絶縁体として設計されたゴムマットを使用してください。
- 電源がアプライアンスの最大消費電力を処理できることを確認してください。過負荷の危険はありません。修理やアップグレードを行う前に、必ずアプライアンスを取り外してください。
- サーバキャビネットやサーバールームラックに配線を過負荷にしないでください。
- 雷雨や予想される雷雨の際は、雷の危険性がなくなるまで、ハードウェアの修理やアップグレードは避けてください。
- 古い家電製品または部品を廃棄する場合は、電子廃棄物の処分に関する地方法および国の法律に従ってください。
- 爆発を防ぐため、期限切れのバッテリーを同じモデルまたはメーカーが推奨する代替品に交換し、製造元の指示に従ってバッテリー交換を行ってください。
- 電源装置のカバーや、次のラベルが付いた密閉されたパーツは絶対に取り外さないでください。

Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no user-serviceable parts inside these components. If you suspect a problem with one of these parts, contact Citrix Technical Support.

アプライアンスの注意事項

- レールを取り付ける前に、ラック内の各コンポーネントの配置を決定します。
- 最初に最も重いアプライアンスをラックの下部に取り付けて、次に上に作業します。ラックの負荷を均等に分配します。不均衡なラックは危険です。
- 電源装置とハードドライブに触れる前に冷却してください。
- 簡単にアクセスできるように、機器をコンセントの近くに設置してください。
- 安全な動作のために十分な通気量のあるラックに機器を取り付けます。
- 閉じたラックアセンブリまたは複数ユニットラックアセンブリの場合、ラック環境の周囲動作温度は室内の周囲温度よりも大きくなる場合があります。したがって、ラックにアプライアンスを設置する場所を決定するときは、装置の最低および最高動作温度を考慮してください。

ラックの注意事項

- ラックの底部のレベリングジャックが床まで完全に伸ばされ、ラックの全重量がそれらの上に置かれていることを確認してください。
- シングルラック設置の場合は、スタビライザーをラックに取り付けます。
- 複数ラックを設置する場合は、ラックを一緒に (取り付け) します。
- コンポーネントをラックから延長する前に、必ずラックが安定していることを確認してください。
- 一度に拡張するコンポーネントを 1 つだけです。2 つ以上を同時に延長すると、ラックが不安定になる可能性があります。
- アプライアンスの前面パネルの左右にあるハンドルは、アプライアンスをラックから引き出すためだけに使用してください。ラックへのアプライアンスの取り付けには、これらのハンドルを使用しないでください。代わりに後述するラックレールハードウェアを使用してください。

アプライアンスのラックマウント

April 15, 2021

SD-WAN 400、800、1000、2000、または 3000 のアプライアンスには、1 つのラックユニットが必要です。これらのアプライアンスは、2 ポストリレーラックまたは 4 ポスト EIA-310 サーバーラックに取り付けることができるラックマウントデバイスです。ラックがアプライアンスと互換性があることを確認します。

アプライアンスをマウントするには、次の手順に従って、まずレールを取り付けてからアプライアンスをラックに取り付ける必要があります。

1. レールアセンブリからインナーレールを外します。
2. インナーレールをアプライアンスに取り付けます。
3. ラックレールをラックに取り付けます。
4. アプライアンスをラックに取り付けます。

レールアセンブリからインナーレールを取り外すには

1. レールアセンブリを平らな面に置きます。
2. アセンブリの前面に向かってインナーレールを引き出します。
3. 内側のレールがレールアセンブリからずっと外れるまで、ロッキングタブを押し込みます。
4. 手順 1.~3. を繰り返してもう 1 つのインナーレールも取り外します。

インナーレールをアプライアンスに取り付けるには

1. アプライアンスの右側にあるイヤブラケットの後ろの右側のインナーレールを配置します。
2. レールの穴とアプライアンスの側面の対応する穴の位置を合わせます。
3. 付属のネジでレールをアプライアンスに取り付けます。
4. 手順 1 ~ 3 を繰り返して、アプライアンスの左側に左側のインナーレールを取り付けます。

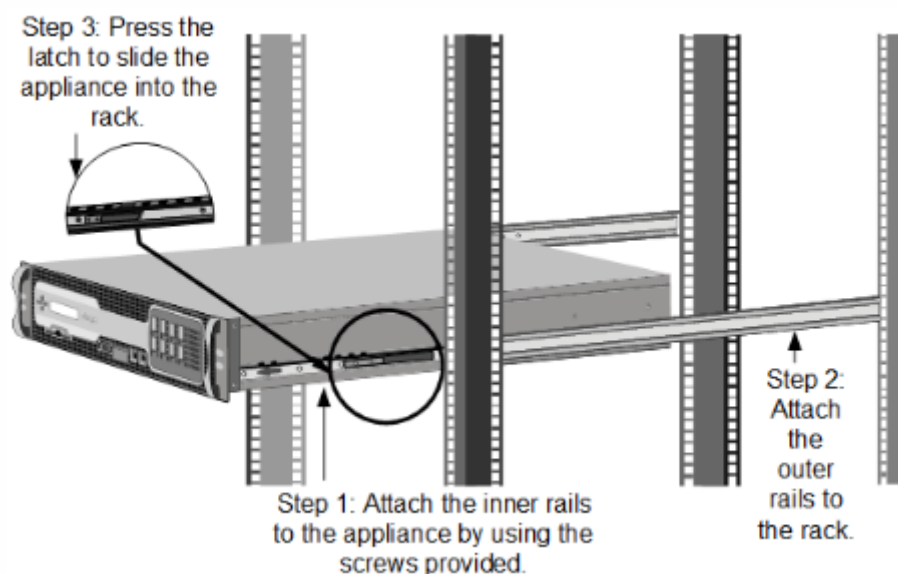
ラックレールを取り付けるには

1. スライド式レールガイドを内側に向いたまま、ラック内の目的の位置にラックレールを配置します。
2. レールをラックにスナップします。両方のラックレールの高さが同じで、レールガイドが内側を向いていることを確認します。

ラックにアプライアンスを取り付けるには

1. アプライアンスに取り付けたインナーレールとラックレールの位置を合わせます。
2. アプライアンスをラックレールにスライドさせ、両側でも圧力を維持し、アプライアンスをラックレールまで押し込みます 1. アプライアンスをラックから完全に引き出して、アプライアンスが所定の位置にロックされていることを確認します。

図 1: アプライアンスのラックマウント

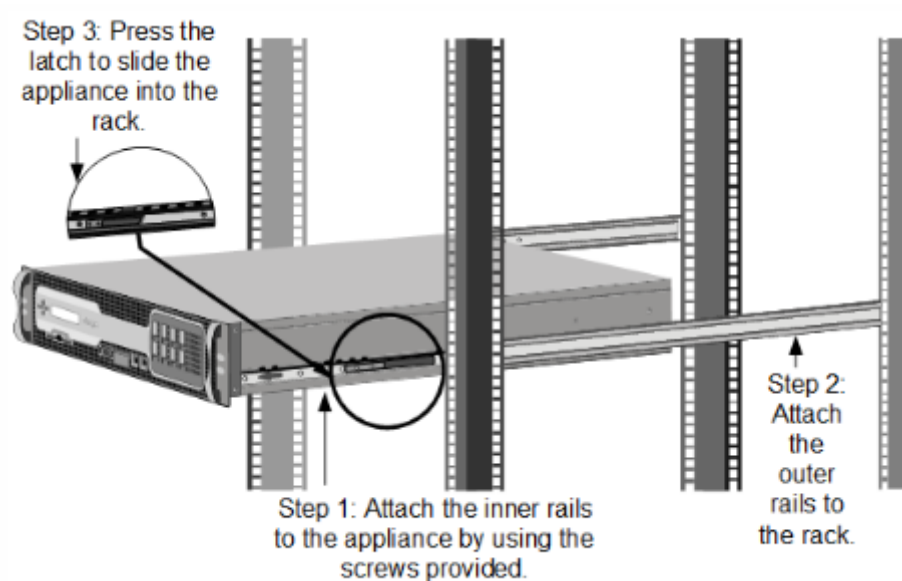


注

上の図は、実際のアプライアンスを表していない可能性があります。

Windows サーバを搭載した SD-WAN 1000 または 2000 アプライアンスには、ラックユニットが 1 つ必要です。どちらもラックマウントデバイスで、2 支柱リレーラックまたは 4 ポスト EIA-310 サーバラックに取り付けることができます。ラックがアプライアンスと互換性があることを確認します。

図 2: アプライアンスのラックマウント



SD-WAN アプライアンスをマウントするには、次の手順に従って、まずレールを取り付けてからアプライアンスをラックに取り付ける必要があります。

1. レールアセンブリからインナーレールを外します。
2. インナーレールをアプライアンスに取り付けます。
 - ラックレールをラックに取り付けます。
 - アプライアンスをラックに取り付けます。

レールアセンブリから内側のレールを取り外す手順は、次のとおりです。

1. レールアセンブリを平らな面に置きます。
2. アセンブリの前面に向かってインナーレールを引き出します。
3. 内側のレールがレールアセンブリからずっと外れるまで、ロックングタブを押し込みます。
4. 手順 1.~3. を繰り返してもう 1 つのインナーレールも取り外します。

アプライアンスにインナーレールを取り付けるには:

1. アプライアンスの右側にあるイヤブラケットの後ろの右側のインナーレールを配置します。
2. レールの穴とアプライアンスの側面の対応する穴の位置を合わせます。
3. 付属のネジでレールをアプライアンスに取り付けます。
4. 手順 1~3 を繰り返して、アプライアンスの左側に左側のインナーレールを取り付けます。

ラックレールを取り付ける手順は、次のとおりです。

1. スライド式レールガイドを内側に向いたまま、ラック内の目的の位置にラックレールを配置します。
2. レールをラックにスナップします。

注: 両方のラックレールの高さが同じで、レールガイドが内側を向いていることを確認してください。

図 3: ラックアセンブリ

アプライアンスをラックに取り付けるには:

1. アプライアンスに取り付けたインナーレールとラックレールの位置を合わせます。
2. アプライアンスをラックレールにスライドさせ、両側の圧力を維持し、所定の位置にロックされるまでアプライアンスをラックレールに押し込みます。
3. アプライアンスをラックから完全に引き出して、アプライアンスが所定の位置にロックされていることを確認します。

注: 次の図に示す図は、実際のアプライアンスを表していない場合があります。

Citrix SD-WAN 4000/5000 アプライアンスには、2つのラックユニットが必要です。

各アプライアンスには取り付けレールキットが付属しており、キットには2組のレールアセンブリ（アプライアンスの左側と右側に1本ずつ）とレールを取り付けるためのネジが含まれます。アセンブリはインナーレールとラックレールで構成されます。付属のレールキットの長さは28インチです（延長した場合は38インチ）。23インチ（延長33インチ）のレールキットを注文するには、Citrixの営業担当者にお問い合わせください。

注: 角穴ラックと丸穴ラックの両方に同じレールキットが使用されます。ネジ付き丸穴ラックの具体的な手順については、図4を参照してください。

アプライアンスを取り付けるには、最初にレールを設置した後、アプライアンスをラックに取り付けます。

アプライアンスを取り付けるには、以下の作業を行います。

- レールアセンブリからインナーレールを外します。
- インナーレールをアプライアンスに取り付けます。
- ラックレールをラックに取り付けます。
- アプライアンスをラックに取り付けます。

レールアセンブリからインナーレールを取り外すには

1. レールアセンブリを平らな面に置きます。
2. アセンブリの前面に向かってインナーレールを引き出します。
3. インナーレールがレールアセンブリから完全に出るまで、ラッチを押し下げます。
4. 手順1.~3.を繰り返してもう1つのインナーレールも取り外します。

インナーレールをアプライアンスに取り付けるには

1. 右のインナーレールを、アプライアンスの右側のハンドルの後側に配置します。
2. レールの穴とアプライアンスの側面の対応する穴の位置を合わせます。
3. 次の図に示すように、付属のネジでレールをアプライアンスに取り付けます。各側面に5本ずつ取り付けます。
4. 手順1.~3.を繰り返して、左のインナーレールをアプライアンスのもう一方の側に取り付けます。

図1: インナーレールの取り付け



ラックレールをラックに取り付けるには

1. 丸穴のネジ式ラックを使用している場合は、手順 3. に進みます。
2. 次の図のように、四角ナットの固定器具をラック前面の支柱と背面の支柱に取り付けます。ネジを挿入する前に、角ナットをアプライアンスの正しい穴に合わせてください。3つの穴は等間隔に並んでいません。

図 2: ラック前面の支柱への固定器具の取り付け

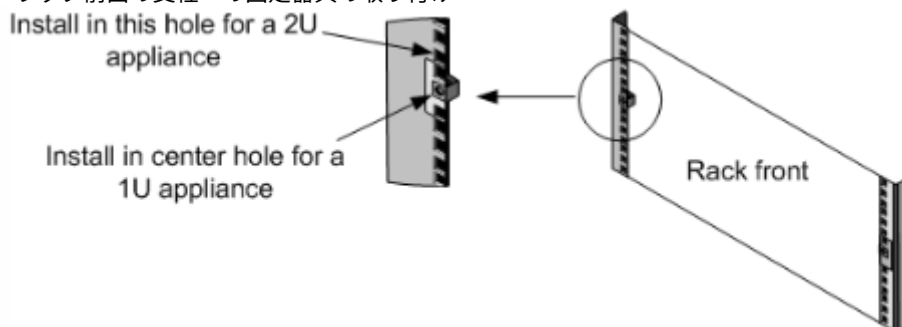
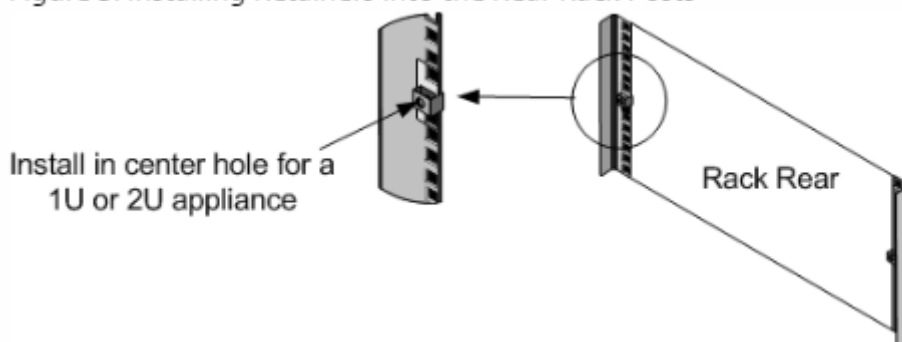
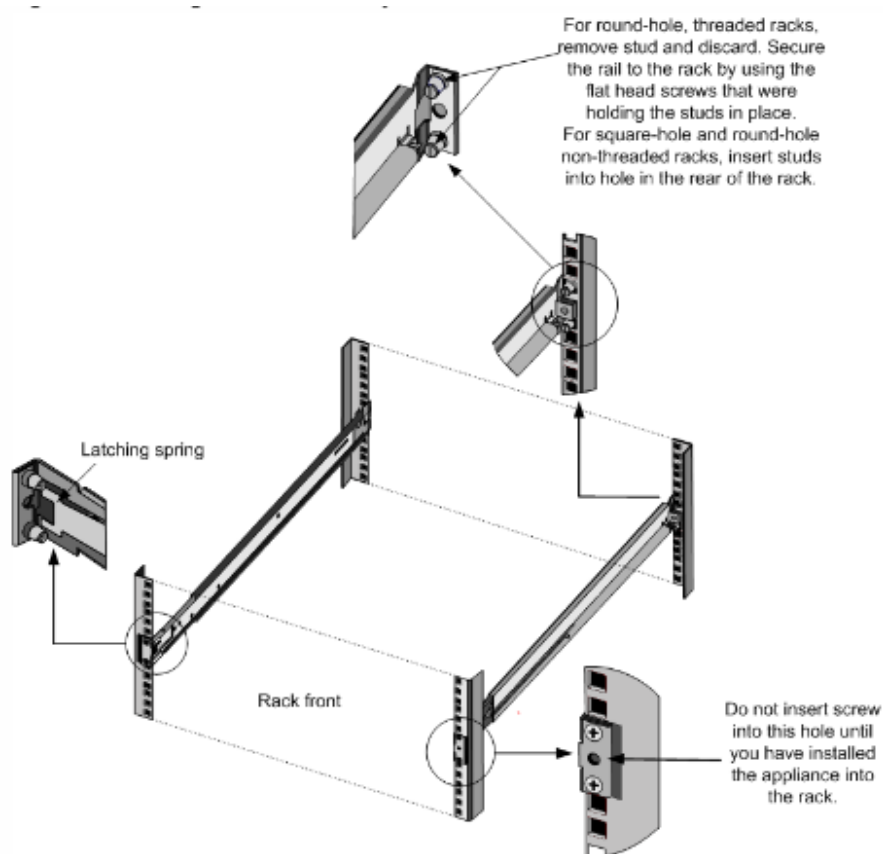


Figure 3. Installing Retainers into the Rear Rack Posts



3. 次の図のように、調整可能なレールアセンブリをラックに取り付けます。後ろのレールフランジをネジでラックに固定します。ネジでレールを適切な位置に固定すると、ラッチのバネを取り外すこともできます。

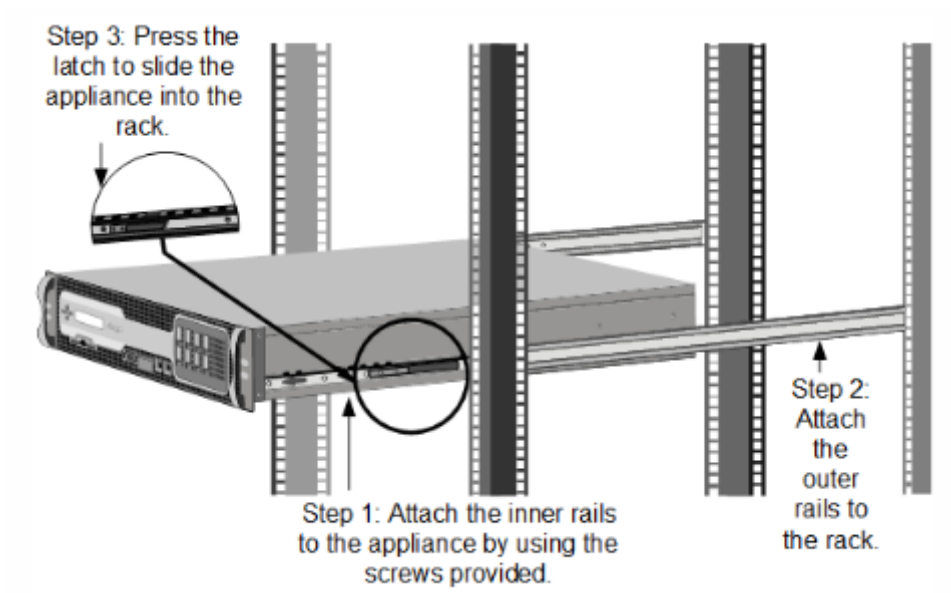
図 4: ラックの組み立て



ラックにアプライアンスを取り付けるには

1. アプライアンスに取り付けたインナーレールとラックレールの位置を合わせます。
2. 両側に均等に力を加えながら、アプライアンスをラックレールに挿入します。
3. アプライアンスをラックから完全に引き出して、アプライアンスが所定の位置にロックされていることを確認します。

図 5: アプライアンスのラックへの取り付け



ケーブルの接続

April 15, 2021

アプライアンスがラックにしっかり取り付けられている場合は、使用するポートを決定します。これで、ケーブルを接続する準備が整いました。Ethernet ケーブルとオプションのコンソールケーブルを最初に接続します。最後に電源ケーブルを接続します。

警告: アプライアンスの取り付けまたは修理を行う前に、電源やワイヤに接触している可能性のあるジュエリーやその他の金属部品をすべて取り外してください。電気の通じている電源または配線とアースの両方に触れると、金属物が急速に加熱し、火傷を負ったり、衣服に火が付いたり、金属物が溶けて露出している端子がショートしたりする可能性があります。

ポート

単一のアクセラレーションブリッジを使用する一般的なインストールでは、4つのイーサネットポート（プライマリポートと apA）と6つの IP アドレス（プライマリポートのサブネットに4つ、ApA のサブネットに2つ）を使用します。

アプライアンスには、マザーボードポートが2つと2つ（SD-WAN 400/800 および SD-WAN 1000/2000）または3つの（SD-WAN 3000）加速ブリッジがあります。

- マザーボードのポートは、Windows Server の SD-WAN1000 アプライアンスでは MGMT（管理）ポートと AUX1（補助）ポートとラベル付けされ、Windows Server がインストールされた SD-WAN 2000 アプライアンスでは PRI（プライマリ）および AUX（補助）ポートとラベル付けされます。

- 初期設定には、Windows Server 搭載の SD-WAN 1000 アプライアンスで MGMT ポートと、Windows Server 搭載の SD-WAN 2000 アプライアンスで Windows Server の PRI ポートを使用します。
- SD-WAN 400/800/1000 および 2000 アプライアンスには、それぞれ 2 組の加速ブリッジポートがあります。3000 アプライアンスには、加速ブリッジポートのペアが 3 つあります。アプライアンスでは、ポート 1/1 と 1/2 はアクセラレーションペア A (apA) ブリッジポート、ポート 1/3 と 1/4 は APB ポート、ポート 1/5 と 1/6 は APC ブリッジポートです。
- 高速ブリッジポートは、Apa と APB は、Windows Server の SD-WAN 1000 アプライアンスの背面パネル、Windows Server では SD-WAN 2000 アプライアンスの前面パネルで使用できます。Windows Server が搭載された SD-WAN 1000WS アプライアンスでは、これらのポートは、それぞれ LAN1 と WAN1、および LAN2 と WAN2 というラベルが付けられます。ただし、Windows Server がインストールされている SD-WAN 2000WS アプライアンスでは、これらのポートは、それぞれ 1/1 と 1/2、および 1/3 と 1/4 とラベル付けされます。

イーサネットケーブルの接続

Ethernet ケーブルはアプライアンスをネットワークに接続します。必要なケーブルの種類は、ネットワークへの接続に使用するポートの種類によって決まります。10/100/1000BASE-T ポートには、標準 RJ-45 コネクタを備えたカテゴリ 5e またはカテゴリ 6 イーサネットケーブルを使用します。

イーサネットケーブルを 10/100/1000BASE-T ポートに接続するには:

1. イーサネットケーブルの一端にある RJ-45 コネクタをアプライアンスの適切なポートに挿入します。
2. もう一方の端の RJ-45 コネクタを、ルーターやスイッチなどのターゲットデバイスに挿入します。
3. 接続が確立されて、黄色の LED が点灯することを確認します。

コンソールケーブルの接続

コンソールケーブルを使用して、アプライアンスをコンピューターまたは端末に接続します。このコンピューターまたは端末からアプライアンスを設定できます。コンソールケーブルを接続する前に、コンピューターまたは端末を、VT100 端末エミュレーション、9600 ボー、8 データビット、1 ストップビット、および「NONE」に設定されたフロー制御をサポートするように設定します。次に、コンソールケーブルの一方の端をアプライアンスの RS232 シリアルポートに、もう一方の端をコンピューターまたは端末に接続します。

Figure 1. Inserting an Ethernet cable



Connecting the Console Cable

コンソールケーブルをコンピュータまたは端末に接続するには:

1. ケーブルの端にある DB-9 コネクタをコンソールポートに挿入します。Windows サーバを備えた SD-WAN **1000** アプライアンスでは、ポートは背面パネルにあります。Windows サーバを備えた SD-WAN **2000** アプライアンスでは、ポートはフロントパネルにあります。

注: RJ-45 コンバータ付きのケーブルを使用するには、付属のオプションのコンバータをコンソールポートに挿入し、ケーブルを接続します。

2. ケーブルのもう一方の端にある RJ-45 コネクタをコンピュータまたは端末のシリアルポートに挿入します。

電源ケーブルを接続します

SD-WAN アプライアンスには、2 台目の電源装置を取り付けた場合を除き、電源装置が 1 つあります。3 極プラグはアースを兼ねているので、別途アースケーブルを用意する必要はありません。電源コードを取り付けて、アプライアンスに電力を供給します。電源ケーブルのもう一方の端を、標準 110V/220V 電源コンセントに接続します。

1. 電源ケーブルの一端を、アプライアンスの背面パネルの電源装置の横にあるコンセントに接続します。
2. 電源ケーブルのもう一方の端を、標準 110V/220V 電源コンセントに接続します。

SD-WAN 4000/5000 アプライアンスには 2 つの電源装置があり、一方はバックアップとして機能します。3 極プラグはアースを兼ねているので、別途アースケーブルを用意する必要はありません。一方または両方の電源コードを取り付けて、アプライアンスの電源を入れます。

注

1 つの電源装置に障害が発生した場合、または 1 つの電源ケーブルだけをアプライアンスに接続すると、アプラ

イアンスは高ピッチの警告を発します。アラームを消音するには、アプライアンスの背面パネルにある小さな赤いボタンを押します。

ポート **10/3** および **10/4** へのファイバパッチケーブルの取り付け

April 15, 2021

リリース 9.3 以降、アプライアンスでは、次の図に示すように、SD-WAN ポート 10/3 および 10/4 を付属のケーブルで接続する必要があります。

注:

10/3 および 10/4 ポートのファイバパッチケーブルは、4000 および 5000 WANOP シリーズのアプライアンスにだけ適用できます。

リリース 9.3 以降、パッチケーブルは不要になり、次の場合は省略できます。

- アプライアンスはリリース 9.3 以降の工場出荷時、または
- アプライアンスはリリース 9.3 以前の出荷時に出荷されていますが、このアプライアンスを新しいバージョンにアップグレードし、管理サービスでデフォルトのループバックを変更します ([システム] > [構成] > [システム] > [ループバック設定の構成])。

ループバックケーブルを使用する必要性をなくす場合は、ポート 10/3 および 10/4 は引き続き予約されています。これらのポートは、WAN 最適化には使用できません。

パッチケーブルを取り付けるには

1. 上の図に示すように、LC と LC ケーブルをポートに接続します。
2. ケーブルの一方の端をポート 10/3 に挿入します。
3. ケーブルのもう一方の端をポート 10/4 に挿入します。

アプライアンスのスイッチを入れる

April 15, 2021

アプライアンスをラックに取り付け、ケーブルを接続したら、電源ケーブルが正しく接続されていることを確認します。2 台目の電源装置を取り付けた場合は、第 2 のケーブルが 1 番目の電源装置とは異なる回路のコンセントに接続されていることを確認します。接続を確認したら、アプライアンスをオンにできます。

アプライアンスをオンにするには

1. アプライアンスがコンソールポートまたはイーサネットポートを介して接続されていることを確認します。これにより、電源を入れた後にアプライアンスを構成できるようになります。

2. アプライアンスの背面パネルのオン/オフ切り替え電源スイッチを押します。

警告

緊急電源オフ（EPO）スイッチの位置に注意して、電気事故が発生した場合にアプライアンスの電源をすばやく取り外すことができます。

**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2021 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).