



## 概要

---

- [ハイブリッドクラウド接続のコンポーネントを理解する \(1 ページ\)](#)
- [ハイブリッドクラウド接続を構築 \(3 ページ\)](#)
- [用語 \(6 ページ\)](#)
- [前提条件 \(9 ページ\)](#)
- [注意事項と制約事項 \(9 ページ\)](#)
- [関連資料 \(10 ページ\)](#)

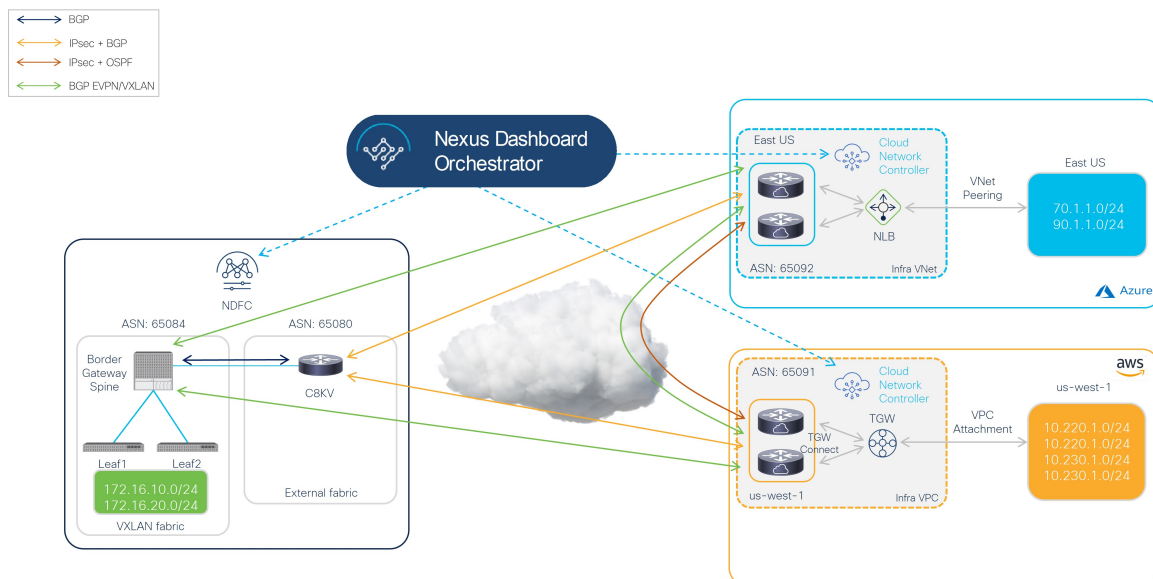
## ハイブリッドクラウド接続のコンポーネントを理解する

このドキュメントでは、Cisco Nexus ダッシュボード ファブリック コントローラ (NDFC) によって管理される Cisco Nexus 9000 NX-OS ベースのファブリックと Cisco クラウドネットワーク コントローラ (CNC) によって管理されるパブリッククラウドサイトを備えた、Cisco Nexus ダッシュボード オーケストレータ (NDO) によって強化された Cisco ハイブリッドクラウド ネットワーキング ソリューションの導入手順について説明します。

Cisco Nexus Dashboard Orchestrator (NDO) ベースのハイブリッドクラウドソリューションは、オンプレミス ネットワークとクラウド ネットワーク間のシームレスな接続を提供します。このソリューションは、NDFC を使用してオンプレミスの VXLAN ベースのファブリックとオンプレミスの Cisco Catalyst 8000V を管理しますが、クラウド サイト (AWS または Microsoft Azure) は Cisco Cloud Network Controller (CNC) によって管理されます。NDO は、オンプレミス サイトとクラウド サイト間、および 2 つ以上のクラウド サイト間の接続を調整するために使用されます。VXLAN は、サイト間にオーバーレイ トンネルを構築するために使用されます。

次の図は、これらのコンポーネントを使用したハイブリッドクラウド接続のトポロジ例を示しています。詳細については、「[サポートされるトポロジ](#)」を参照してください。

図 1:



このトポロジ例では、NDFCが管理するオンプレミスサイトにAWSおよびAzureクラウドサイトへの安全な接続が設定されています。そこではインフラ VPC/VNet の上の Cisco Catalyst 8000Vは、オンプレミスデータセンターから来るそしてオンプレミスデータセンターへ向かう全てのトラフィックのクラウドゲートウェイの役割があります。

ボーダーゲートウェイ (BGWs) でもある、様々なオンプレミス VXLAN EVPN サイトのシームレス Layer-2/Layer-3 DCI 拡張をサポートするオンプレミスサイト上で、パブリッククラウドへ Layer-3 拡張もサポートします。

クラウド内の BGW と Cisco Catalyst 8000V 間のコントロールプレーンには BGP-EVPN が使用され、データプレーンには VXLAN が使用されます。

前の図に示すように、Cisco Hybrid クラウドネットワークングソリューションは次のコンポーネントで構成されています。

- Cisco Nexus ダッシュボード オーケストレータ (NDO) :** NDO は、セントラルポリシーコントローラとして働き、様々なNDFCインスタンスに管理されている複数のオンプレミスファブリックに渡ってポリシーを管理します。そして、各クラウドサイトは、自分のCiscoクラウドネットワークコントローラに抽象化されます。NDOはNexusダッシュボード上のサービスとして実行されます。Nexusダッシュボードは、VMware ESXi、Linux KVM、Amazon Web Services、またはMicrosoft Azure で実行される物理アプライアンスまたは仮想マシンのクラスタとして展開できます。以前にバージョン間サポートが導入されているため、NDOは、異なるソフトウェアバージョンを実行しているCiscoクラウドネットワークコントローラを管理できます。
- [Cisco Nexus ダッシュボード ファブリック コントローラ (NDFC) ]:** NDFC は、LAN、VXLAN、SAN、および Cisco IP Fabric for Media (IPFM) ファブリックを構築するためのネットワーク自動化およびオーケストレーションツールです。NDFCは、物理クラスタまたは仮想クラスタのいずれかである Nexus ダッシュボード クラスタ上でサービスとして実行されます。ハイブリッドクラウドネットワークングソリューションの場合、

NDFCはオンプレミスのVXLANファブリックとオンプレミスのCisco Cloud Router (Catalyst 8000V) を管理します。

- **オンプレミス VXLAN ファブリック** : オンプレミス VXLAN ファブリックは、NDFC によって管理される Nexus 90000/3000 スイッチで構築されています。ファブリックには、オンプレミス サイトとクラウド サイト間の VXLAN マルチサイト オーバーレイ トンネルの開始と終了を担当する 1 つ以上のボーダー ゲートウェイ (BGW) デバイスが必要です。NDFC には、VXLAN ファブリックを作成するための事前に作成されたテンプレートがあります。このドキュメントでは、VXLAN ファブリックに External\_Fabric テンプレートを使用しています。
- **オンプレミスの Cisco Cloud Router (CCR)** : CCR は、オンプレミスの VXLAN ファブリックとクラウド サイト間の到達可能性を提供するために使用されます。CCR は、パブリックインターネットまたはプライベート接続 (AWS Direct Connect や Azure ExpressRoute など) を使用してクラウド サイトへの接続を提供します。オンプレミスの CCR は、事前に構築された External\_Fabric テンプレートを使用して NDFC によって管理され、コア ルーター ロールを割り当てる必要があります。

Cisco Catalyst 8000V は、Cisco ハイブリッドクラウド ネットワーキング ソリューションのオンプレミス CCR として使用されます。

- **Cisco クラウド ネットワーク コントローラ (CNC)** : Cisco クラウド ネットワーク コントローラは、サポートされているパブリッククラウド上で仮想インスタンスとして実行され、パブリッククラウド内の自動接続、ポリシー変換、およびワークロードのさらなる可視性を提供します。Cisco クラウド ネットワーク コントローラは、NDO から受け取ったすべてのポリシーを変換し、それらをクラウドネイティブの構造、AWS の VPC やセキュリティグループや Microsoft Azure の VNet などにプログラムします。Cisco Cloud Network Controller は、AWS Marketplace や Azure Marketplace などのパブリッククラウドマーケットプレイスを通じて展開されます。
- **Cisco Catalyst 8000V** : Cisco Catalyst 8000V は、パブリック クラウド プラットフォームの重要なコンポーネントです。Cisco Catalyst 8000V は、オンプレミスサイトおよびパブリッククラウドプラットフォームへのサイト間通信に使用されます。さらに、Cisco Catalyst 8000V は、オンプレミスのクラウド接続と、さまざまなクラウドプロバイダー間の接続 (たとえば、Azure から AWS) に使用されます。

## ハイブリッドクラウド接続を構築

このセクションでは、ハイブリッドクラウド接続を構築するために使用されるプロセスについて説明します。

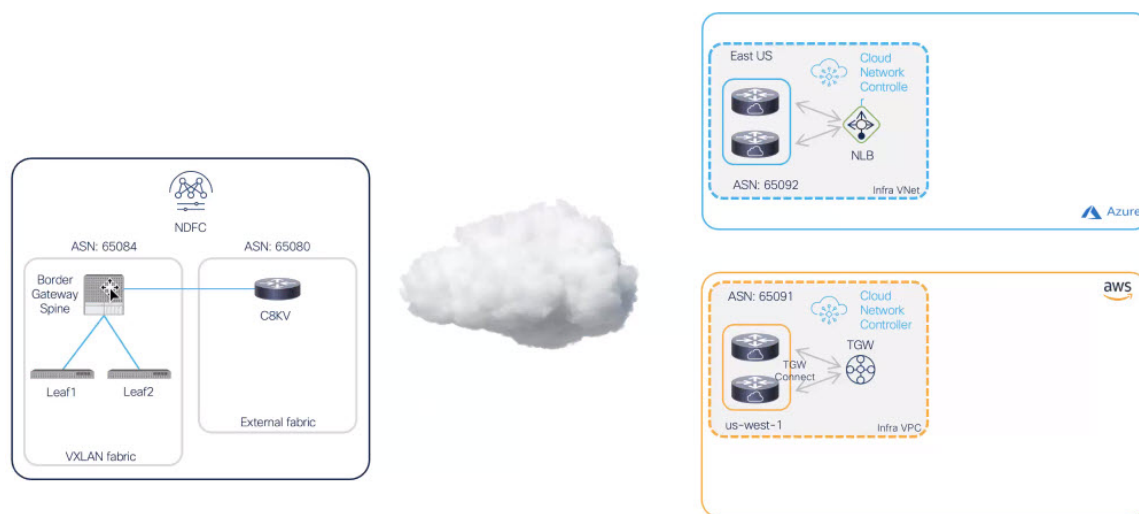
- [開始点 \(4 ページ\)](#)
- [アンダーレイ レイヤーの構築 \(4 ページ\)](#)
- [オーバーレイの構築 \(5 ページ\)](#)

## 開始点

次の図は、ハイブリッドクラウド接続の開始点を示しています。ここでは、[ハイブリッドクラウド接続のコンポーネントを理解する \(1 ページ\)](#) で説明されているさまざまな部分があります：

- Nexus ダッシュボードファブリック コントローラ (NDFC) のファブリック：
  - オンプレミスの VXLAN ファブリック
  - 外部ファブリック
- クラウドネットワーク コントローラによって管理されるクラウドサイト (AWS および Azure)

図 2:

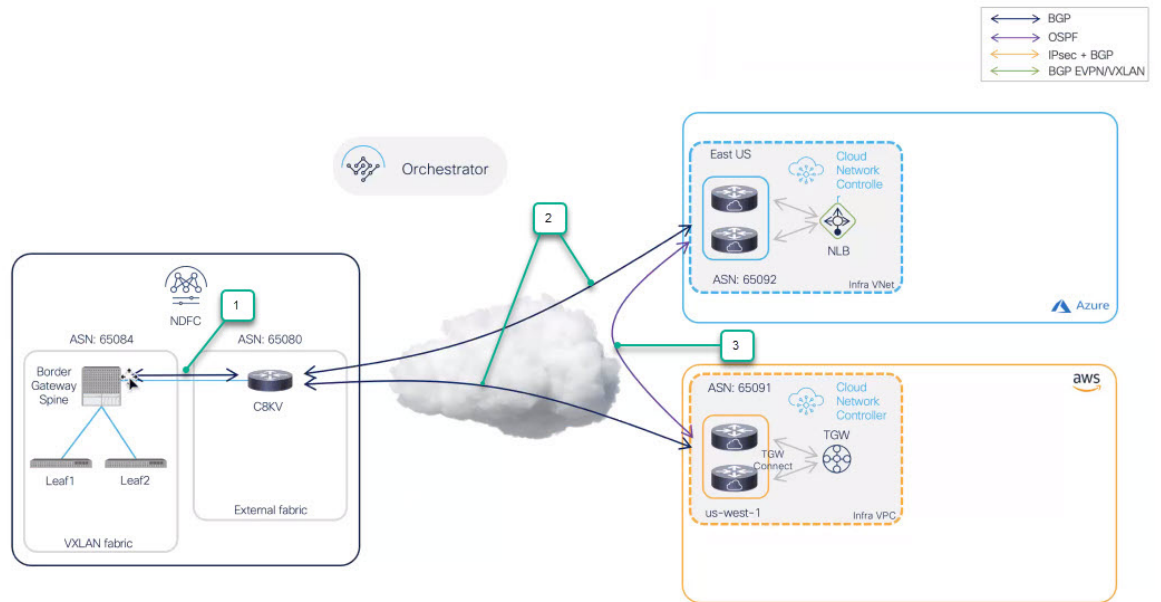


## アンダーレイ レイヤーの構築

次に、後でアンダーレイがどのように構築されるかを示します。

1. まず、VXLANファブリックのボーダーゲートウェイスパインスイッチと外部ファブリックの Cisco Catalyst 8000V の間に BGP 接続が確立されます。
2. 次に、BGP ピアリングを使用して、外部ファブリックのオンプレミス Cisco Catalyst 8000V とクラウドサイトの各クラウドルータ間のアンダーレイ接続を確立します。
3. 最後に、OSPF はクラウドサイト間でクラウド間アンダーレイ接続に使用されます。

図 3:

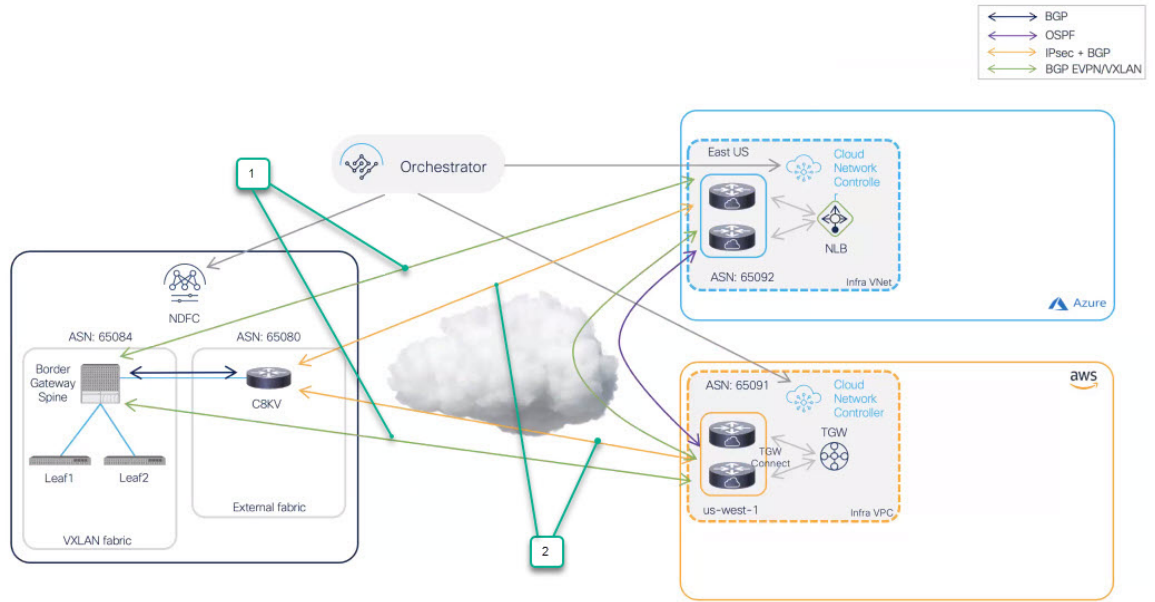


### オーバーレイの構築

最後に、前の手順で確立されたアンダーレイ接続の上に VXLAN マルチサイトオーバーレイを確立する方法を示します：

1. VXLAN マルチサイトが確立されます。これは、VXLAN ファブリックのボーダー ゲートウェイ スパイン スイッチから始まり、クラウドサイトの Cisco Catalyst 8000V で終了します。
2. 接続タイプとしてパブリック インターネットを選択した場合、IPsec と OSPF を使用して NDFC VXLAN ファブリック サイトとクラウドサイトの間を接続します。

図 4:



# 用語

このマニュアルでは、次の用語を使用します。

用語	略語	定義
ボーダーゲートウェイ	BGW	NDFC 簡単ファブリック (VXLAN EVPN ファブリックなど) でサポートされているスイッチロールの1つ。BGWは、オンプレミスファブリック間のレイヤー2/レイヤー3 DCI 接続と、パブリッククラウドサイトへのレイヤー3 接続 (ハイブリッドクラウド接続など) を拡張するために使用されます。

用語	略語	定義
コア ルータ		NDFC 外部ファブリックでサポートされる役割の1つ。 コア ルータは、一方の側でVXLAN EVPN ファブリックと、もう一方の側でクラウドサイトの Catalyst 8000V とのレイヤ 3 接続 (アンダーレイ) を確立するために使用されます。
直接接続		AWS クラウドで使用されます。AWS 直接接続は、ネットワークを AWS に直接リンクして、一貫した低遅延のパフォーマンスを提供するクラウドサービスです。
ExpressRoute		Azure クラウドで使用されます。Azure ExpressRoute を使用して、Azure データセンターとオンプレミスまたはコロケーション環境のインフラストラクチャとの間にプライベート接続を作成できます。
サイト間ネットワーク	ISN	オンプレミスの VXLAN ファブリック間、およびパブリッククラウド (「アンダーレイ」とも呼ばれる) と、オンプレミスの VXLAN ファブリックをインターコネクトするために使用されるレイヤー 3 インフラストラクチャ。そのため、ISN には、インターネットまたは直接接続および ExpressRoute 専用回線を含めることもできます。

用語	略語	定義
IP セキュリティ ルータ	IPSec ルータ	<p>オンプレミス サイトとクラウド サイト Cisco クラウド ネットワーク コントローラの間で IPSec 接続を確立するには、インターネット プロトコル セキュリティ (IPsec) 対応の ルータが必要です。</p>
ルーティング サーバ	RS	<p>コントロールプレーンノードは、オンプレミスの BGW デバイス間の EVPN 隣接関係 (アジャセンシー) の確立を容易にするために使用され、それらすべての間にフルメッシュ ピアリングを作成する必要性を軽減します。ルート サーバは BGP プロトコルを実行し、2 つ以上の BGP ピア間でルートを渡すために使用されます。</p> <p>ルート サーバ機能は、iBGP セッションに従来使用されていた「ルートルフレクタ」機能に相当する eBGP です。必要な BGP ピアリングの数を減らすのに役立ちます。</p>
仮想ネットワーク	VNet	<p>Azure クラウドで使用されます。Azure Virtual Network (VNet) は、Azure のプライベート ネットワークの基本的な構成要素です。VNet を使用すると、Azure 仮想マシン (VM) などのさまざまな種類の Azure 情報技術が、相互、インターネット、およびオンプレミス ネットワークと安全に通信できます。</p> <p>クラウド ネットワーク コントローラに関連して、クラウド ネットワーク コントローラの VRF は Azure の VNet にマッピングされます。</p>



用語	略語	定義
仮想プライベートクラウド	VPC	<p>AWS クラウドで使用されます。Amazon 仮想 プライベートクラウド (VPC) は、お客様が定義する仮想ネットワークで AWS の情報技術を起動できるようにします。この仮想ネットワークは、お客様自身のデータセンターで運用されている可能性がある従来型のネットワークとよく似ているだけでなく、AWS の拡張可能なインフラストラクチャを活用するというメリットがあります。</p> <p>クラウドネットワーク コントローラに関連して、クラウドネットワーク コントローラの VRF は AWS の VPC にマッピングされます。</p>

## 前提条件

次のソフトウェア バージョンが必要です。

- Cisco Nexus ダッシュボード (ND) バージョン 2.3.1c 以降 (物理または仮想クラスター)
- Cisco Nexus ダッシュボード ファブリック コントローラ (NDFC) バージョン 12.1.2e 以降
- Cisco Nexus ダッシュボード オーケストレータ (NDO) バージョン 4.1 (1) 以降
- AWS サイトおよび Microsoft Azure サイト用の Cisco クラウド ネットワーク コントローラ (CNC) バージョン 25.1 (1e) 以降

## 注意事項と制約事項

以下は、ハイブリッドクラウド接続ソリューションを展開するときに理解する必要がある特定のガイドラインと制限事項です。

- 現在、各 Cisco クラウド ネットワーク コントローラは、AWS および Azure クラウドで最大 16 のリージョンを管理できます。16 を超えるリージョンを管理する場合は、追加の Cisco クラウド ネットワーク コントローラを展開する必要があります。詳細については、[AWS インストールガイドの Cisco クラウド ネットワーク コントローラ](#)または[Azure インス](#)

ルガイドの [Cisco クラウド ネットワーク コントローラ](#)、リリース 25.1 (x) 以降の「サイト、リージョン、および CCR の数の制限について」セクションを参照してください。

## 関連資料

Cisco ハイブリッドクラウド ネットワーキング ソリューションを構成するコンポーネントのドキュメントは、次の場所にあります：

- [Cisco Nexus ダッシュボード オーケストレータ \(NDO\) ドキュメント](#)
- [Cisco Nexus ダッシュボード ファブリック コントローラ \(NDFC\) ソリューション](#)
- [Cisco クラウド ネットワーク コントローラ \(CNC\) ドキュメント](#)
- [Cisco キャタリスト 8000V ドキュメント](#)
- [Amazon Web Services \(AWS\) ドキュメント](#)
- [Microsoft Azure ドキュメント](#)

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。