ıılııılıı cısco

Cisco NX-OS および Cisco® Application Centric Infrastructure(Cisco ACI™)モー ドでの Cisco Nexus 9000 シリーズ スイッ チへの Microsoft Azure Stack HCI 接続 目次

はじめに	5
前提条件	5
用語	5
エグゼクティブサマリー	6
本書の目的	7
テクノロジーの概要	7
Cisco ACI について	7
Cisco ACI アーキテクチャ	8
ファブリックをベースにした Cisco Nexus 9000 NX-OS	9
ソリューション設計	
物理アーキテクチャ	10
論理アーキテクチャ	11
ファブリックとメリットに基づいた Cisco Nexus 9000 シリーズ スイッチ	16
Azure Stack HCI 接続向け Cisco ACI 設計	17
Azure Stack HCI 接続用 Cisco ACI	17
Azure Stack HCI ACI テナントモデルの概要	19
Azure Stack HCI 接続のための Cisco NX-OS ペースのファブリック設計	19
Azure Stack HCI 接続用 Cisco NX-OS ベースのファブリック	20
ソリューションの導入	21
Azure Stack HCI の Cisco ACI 構成	21
Azure Stack HCI サーバーに接続されたリーフ インターフェイスの構成	21
QoS の構成	
EPG の構成	40
Azure Stack HCI 用の Cisco NX-OS ベースのファブリック構成	47
QoS の設定	48
LLDP の設定	52
Azure Stack HCI のネットワークの構成	53
Azure Stack HCI サーバーの外部接続の構築	59
付録	60
Azure Stack HCI での Microsoft ソフトウェア定義型ネットワーキング (SDN)の設計例	60
Microsoft Azure SDN コンポーネント	60
論理アーキテクチャ	61
PA ネットワークと SLB MUX VM の接続	62
Azure Stack HCI VNET 接続 (論理ネットワークおよびゲートウェイ VM 接続)	64
ソリューションの導入	66

PA ネットワークおよび SLB 接続の Cisco ACI 構成	72
Azure Stack HCI VNET およびゲートウェイ VM 接続用の Cisco ACI 構成	84
詳細情報	92
更新履歴	

注: このドキュメントには、複数の依存関係を持つ資料とデータが含まれています。情報は必要に情報カテゴリて更新される可能性があり、予告なく変更される場合があります。

このドキュメントには特権/機密情報が含まれており、法的権限の情報カテゴリとなる場合があります。意図さ れた以外の者がこの資料にアクセスすることは許可されていません。お客様が意図された受信者ではない場合 (またはかかる人物への情報の配信の責任者でない場合)、お客様は、この情報(またはその内容の一部)を使 用、複製、配布、または他者に譲渡することはできませアクション。それを実行します。このような場合は、こ の情報を破棄し、Ciscoにただちに通知する必要があります。この資料をエラーて受け取った場合は、ただちに 当社に通知し、コンピュータから資料を削除してください。お客様またはお客様の雇用主がこのメッセージに同 意しない場合は、ただちに当社に通知してください。当社は、本資料の使用によって生じたいかなる損失または 損害についても責任を負いません。

はじめに

このドキュメントでは、 Cisco NX-OS および Cisco[®] Application Centric Infrastructure (Cisco ACI[™])を使用した Cisco Nexus 9000 シリーズ スイッチベースのネットワークにおける Microsoft Azure Stack ハイパー コンバージド インフラストラクチャ (HCI) のネットワーク設計に関する考慮事項について説明します。

前提条件

このドキュメントは、Cisco ACI および Cisco NX-OS VXLAN テクノロジーの基本的な知識があることを前提 としています。

詳細は、Cisco.com にある Cisco ACI のホワイトペーパー(<u>https://www.cisco.com/c/ja_jp/solutions/data-</u> <u>center-virtualization/application-centric-infrastructure/white-paper-listing.html</u>) を参照してください。

Cisco NX-OS ベースの VXLAN ファブリックの詳細については、Cisco.com (<u>https://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/white-paper-</u> listing.html)のホワイトペーパーを参照してください。ホワイトペーパーリスト.html

用語

- Cisco ACI 関連の用語 BD:ブリッジドメイン
 EPG:エンドポイントグループ
 L3Out: レイヤ3外部または、外部ルーティングネットワーク
 L3Out EPG: L3Out のサブネットベース EPG
 VRF: Virtual Routing and Forwarding (仮想ルーティングおよびフォワーディング) ボーダー リーフ: L3Out が展開されている ACI リーフ
- Cisco NX-OS 関連の用語

NDFC : Nexus Dashboard Fabric Controller

VXLAN : Virtual Extensible LAN

VNI: 仮想ネットワーク識別子(VLAN と VNI 間の1対1の相関関係)

DAG: 分散型エニーキャスト ゲートウェイ

リーフ:これは仮想トンネルエンドポイント(VTEP)として機能し、カプセル化とカプセル化解除を実行 します。エンドホストは VXLAN ファブリックのリーフに接続されます。

スパイン: VXLAN ファブリック内のリーフ間のアンダーレイ レイヤ3 接続を提供します。

ボーダーリーフ(Border Leaf): リーフと同様の機能を実行します。さらに、ボーダーリーフは VXLAN ファブリックを外部ネットワークに接続し、VXLAN ファブリックのエッジに配置されます。

外部接続: VXLAN ファブリックの外部に L3 接続を提供します。

• Microsoft Azure Stack HCI 関連の用語

RDMA: リモート ダイレクト メモリ アクセス

RoCE : RDMA over Converged Ethernet

SET: スイッチ組み込み Teaming

SMB: サーバー メッセージ ブロック

ストレージスペース ダイレクト: Microsoft Azure Stack HCl および Windows Server の機能の 1 つで、 内部ストレージを備えたサーバーをソフトウェア定義型記憶域ソリューションにクラスタ化できます。記憶 域スペースダイレクトは、SMB3 (SMB ダイレクトおよびイーサネットの SMB マルチチャネルを含む)を 使用してサーバー間の通信を行います。

SMB ダイレクト: Windows Server には、RDMA 機能を持つネットワークアダプタの使用をサポートする SMB ダイレクトと呼ばれる機能が含まれています。RDMA 機能を備えたネットワーク アダプタは、CPU 使用率を損なうことなく、低遅延でフルスピードで機能できます。SMB ダイレクトには、サーバー上に RDMA 機能を備えたネットワーク アダプタと、ネットワーク上に RDMA over Converged Ethernet (RoCEv2) が必要です。

エグゼクティブサマリー

Cisco ACI リリース 6.0(3e) および NX-OS 10.3(2)F 以降、 Nexus 9000 シリーズ スイッチは Microsoft <u>Azure Stack HCI 要件</u>をサポートします。このドキュメントでは、Cisco ACI または Cisco NX-OS モードの Cisco Nexus 9000 シリーズ スイッチを使用した Microsoft Azure Stack HCI ネットワーク設計について詳しく 説明します。



図 1.

Cisco ACI モードの Nexus 9000 シリーズ スイッチを使用したトポロジの例

注: Cisco Application Policy Infrastructure Controller (APIC) は、リーフ スイッチに直接接続することも、 スパイン スイッチを介してレイヤ 3 ネットワークで接続することもできます。



図 2.

Cisco NX-OS モードの Nexus 9000 シリーズ スイッチのトポロジ例

本書の目的

Microsoft Azure Stack HCI をインストールする場合は、 Microsoft Azure Stack Azure Stack HCI サーバーから Cisco Nexus 9000 トップオブラック (ToR) スイッチへの直接接続と、他の必要なタスクの中でも特にデータ センターへのユーザー補助が可能であることを確認する必要があります。

このドキュメントでは、Microsoft Azure Stack HCI サーバーをデータ センター内の既存の Cisco Nexus 9000 シリーズ スイッチベースのネットワークに接続するための情報、教育、およびガイダンスを提供します。この ドキュメントには、ソリューションの内部テストに基づいた基本情報と推奨される設定が記載されています。こ のドキュメントでは、Cisco ACI または NX-OS ベースのインフラストラクチャのインストールと設定について は説明していません。また、Microsoft Azure Stack HCI のセットアップについても詳しく説明していません。

このドキュメントでは、 Microsoft Azure Stack HCI サーバーとして Cisco UCS C240 M6/M7 サーバーを使用 します。Cisco UCS の設定と設計に関する考慮事項については、cisco.com

(<u>https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/ucs_mas_hci_m7.html</u>) で Cisco Validated Design (CVD) を参照してください。

Microsoft Azure Stack HCI 内部ネットワークは、このソリューションでは Cisco APIC や NDFC などのシスコ コントローラを使用して管理されません。Azure Stack HCI システムは、 Nexus 9000 シリーズ スイッチベー スのネットワークに接続されます。これは、Azure Stack HCI 仮想マシン (VM) がデータセンター内の他の VM、 外部ネットワーク、およびその他の内部ネットワーク サービスに接続できるようにするゲートウェイとして機 能します。

テクノロジーの概要

このセクションでは、ソリューションで使用されるテクノロジーについて説明します。これらはこのドキュメントで説明します。

Cisco ACI について

Cisco ACI は、ネットワークの俊敏性とプログラマビリティを通じて業務効率を実現するという SDN の当初の ビジョンから進化したものです。Cisco ACI は、管理の自動化、プログラムによるポリシー、ダイナミック ワ ークロードのプロビジョニングにおいて、業界をリードするイノベーションを実現します。Cisco ACI ファブリ ックではこれらを、ハードウェア、ポリシーベースの制御システム、ソフトウェアを組み合わせて緊密に結びつ けることで実現し、他のアーキテクチャにはないメリットを提供します。

Cisco ACI は、データ センター ネットワークの運用化にポリシーベースのシステム アプローチを採用していま す。ポリシーは、アプリケーションのニーズ(到達可能性、サービスへのアクセス、およびセキュリティ ポリ シー)を中心にしています。Cisco ACI は、今日のダイナミック アプリケーションに対応する復元力のあるフ ァブリックを提供します。

Cisco ACI アーキテクチャ

Cisco ACI ファブリックはリーフ/スパイン型アーキテクチャであり、各リーフは高速 40/100/400 Gbps イー サネット リンクを使用してすべてのスパインに接続し、スパイン スイッチまたはリーフ スイッチ間の直接接続 はありません。ACI ファブリックは、すべてのリーフが VXLAN トンネル エンドポイント (VTEP) である VXLAN オーバーレイ ネットワークを備えたルーテッド ファブリックです。Cisco ACI は、このルーテッド フ ァブリック インフラストラクチャ全体でレイヤ 2 (L2) とレイヤ 3 (L3) の両方の転送を提供します。

次は、ACI ファブリック トポロジです。

Cisco APIC: Cisco Application Policy Infrastructure Controller(APIC)では、Cisco ACI ファブリックの自動化と管理を一元的に行うことができます。Cisco APIC は、すべてのファブリック情報への集中アクセスを提供し、スケールとパフォーマンスに合わせてアプリケーション ライフサイクルを最適化し、物理リソースと仮想リソース全体にわたる柔軟なアプリケーション プロビジョニングをサポートする、集中型のクラスタ コントローラです。Cisco APIC は、XML と JSON を通じてノースバウンド API を公開し、API を使用してファブリックを管理するコマンドライン インターフェイス (CLI) と GUI の両方を提供します。

リーフスイッチ: ACI リーフは、サーバー、ストレージデバイス、およびその他のアクセス層コンポーネント に物理接続を提供し、 ACI ポリシーを適用します。リーフ スイッチは、既存の企業またはサービス プロバイダ ー インフラストラクチャへの接続も提供します。リーフ スイッチには、接続用に 1G から最大 400G のイーサ ネット ポートまでのオプションがあります。

スパインスイッチ: ACI では、スパインスイッチはマッピング データベース機能とリーフスイッチ間の接続 を提供します。スパインスイッチには、ACI 対応回線カードを搭載したモジュラ型の Cisco Nexus 9500 シリ ーズ、または Cisco Nexus 9332D-GX2B などの固定フォームファクタスイッチを使用できます。スパインス イッチは、リーフスイッチへの高密度 40/100/400 ギガビットイーサネット接続を提供します。



図 3. Cisco ACI ファブリック コンポーネント

ファブリックをベースにした Cisco Nexus 9000 NX-OS

Cisco NX-OS ベースのファブリックは、Nexus 9000 シリーズ スイッチを使用してデータセンターを構築す るためのもう 1 つのオプションです。これらのスイッチは 独立した デバイスとして機能し、独自のコントロー ルプレーンとデータプレーンを備えています。NX-OS を実行する Nexus 9000 シリーズ スイッチは、VXLAN、 L3 ルーテッド、または従来の(2 階層または 3 階層) LAN など、さまざまなデータ センター ファブリック オプションを提供します。

このドキュメントでは、 Azure Stack HCI を VXLAN ファブリックに接続することにのみ焦点を当てています。 ただし、NX-OS ベースの L3 ルーテッドまたは従来の LAN ファブリックも使用できます。

Cisco NX-OS ベースの VXLAN ファブリック コンポーネントは次のとおりです。

NDFC: Cisco Nexus Dashboard Fabric Controller (NDFC) は、データ センター ファブリックを構築および 管理するためのオーケストレーションおよび自動化ツールです。Cisco NDFC は、LAN または SAN モードで 使用できます。LAN モードでは、NDFC は、VXLAN、VXLAN マルチサイト、L3 ルーテッド ファブリック、お よびメディア用の従来の LAN および IP ファブリックを作成するためのさまざまなファブリック テンプレート をサポートします。Cisco NDFC は、次の Day 0 から Day 2 の動作を提供します。

- 0日目:デバイスのブートストラップ(POAP) サポートとファブリックの事前プロビジョニング。
- 1 日目:新しいグリーンフィールドファブリックの自動化、ブラウンフィールドファブリックのサポート、ネットワークと VRF の導入、L4 ~ L7 サービスの挿入。
- 2日目: イメージ管理、RMA ワークフロー、変更管理とロールバック、デバイスの正常性性とインター フェイスのモニタリング。

Cisco NDFC はオプションです。VXLAN ファブリックは、従来の CLI を使用して管理することもできます。ただし、Cisco NDFC には独自の利点があります。前述のように、Cisco NDFC は、人的エラーの可能性を排除することで、あらゆるタイプのデータ センター ファブリックの完全自動化サポートを提供します。

Nexus 9000 シリーズ スイッチ: Nexus 9000 スイッチは、ハイブリッド クラウド ネットワーキング基盤の データセンタースイッチです。Cisco Nexus 9000 シリーズは、モジュラ型および固定型のフォームファクタを 提供し、1 ~ 800 Gig のラインレート転送を実現します。

VXLAN EVPN ファブリック: VXLAN EVPN は、大規模なデータ センター ファブリックを構築するための事実 上の標準規格であり、ホストのシームレスなモビリティ、テナントの分離、L2 セグメントの大規模な名前空間、 およびすべての ECMP パスにわたるトラフィック エントロピーを提供します。

スパイン スイッチ: VXLAN ファブリックでは、スパイン スイッチは、高速リンクを使用してすべてのリーフ スイッチ間の接続を提供します。スパインは、エンドホストの接続には使用されません。

リーフスイッチ: リーフスイッチは VTEP として機能し、VXLAN ヘッダーのカプセル化とカプセル化解除化 解除を行います。エンドホストはリーフスイッチで終端されます。



図 4. Cisco NX-OS ベースのファブリック コンポーネント

ソリューション設計

ソリューションを実装する前に、 Microsoft Azure Stack HCI の論理的なアーキテクチャと、基盤となる物理ア ーキテクチャにマッピングする方法を理解することが重要です。このセクションでは、 Microsoft Azure Stack HCI、および Cisco ACI または Cisco NX-OS モードのいずれかを使用した Nexus 9000 シリーズ スイッチ ベ ースのネットワークの論理的な接続と物理接続について説明します。

物理アーキテクチャ

各 Cisco UCS C240 M6/M7 サーバは、デュアル 100 Gb 接続を使用して、 Cisco Nexus 9000 トップオブラ ック(ToR) スイッチ のペアに接続されます。この例では、 Cisco Nexus 9000 シリーズ スイッチ ベースのデ ータセンターネットワークは、すべての Azure Stack HCI ネットワーク トラフィック(ホストオペレーティン グ システム、クラスタ通信、コンピューティング、およびストレージ トラフィックの管理)を伝送します。異 なるネットワークを使用することもできます。

Cisco UCS Cシリーズ上の **Cisco** 統合管理コントローラ (**CIMC**) などの物理サーバー管理は、サーバーの専 用管理ポートを 1GbE リンクを使用して OOB 管理スイッチに接続するアウトオブバンド (OOB) 管理ネット ワークを介して促進されます。

次の図は、物理アーキテクチャ設計の概要を示しています。



図 5.

物理アーキテクチャ(Cisco ACI または NX-OS モード)

Cisco NX-OS モードの場合、スパイン リーフトポロジの使用は一般的な設計オプションですが必須ではありま せんが、Cisco ACI モードではスパイン リーフトポロジが必要です。Microsoft Azure Stack HCI サーバを ToR スイッチのペアに接続するためにダウンストリーム vPC は使用されませんが、vPC ピアリンクの使用が推奨さ れます。 注: ACI ベースのファブリックと NX-OS ベースのファブリックの唯一の違いは vPC ピアリンクであるため、 このドキュメントでは vPC ピアリンクのトポロジ図を使用します。この vPC ピアリンクは、 ACI ファブリッ クに存在しません。

物理的接続に関する検討事項には、次のものがあります。

- Microsoft では、リモート ダイレクト メモリアクセス(RDMA)を使用した 10+ ギガビットイーサネットネットワークを推奨しています。
 UCS C240 M6/M7 ベースの Azure Stack HCI の場合、NVIDIA ConnectX-6X デュアル ポート 100 ギガビット イーサネット NIC カードが必要です。(Cisco VIC は現在オプションではありません)。
 Microsoft では、すべてのサーバ ノードを同じように設定する必要があります。
 クラスタあたり最大 16 台の Azure Stack HCI サーバー。
- Microsoft Azure Stack HCI サーバインターフェイスは、仮想ポート チャネル (vPC) ではなく、個別の リンクを使用して ToR スイッチのペアに接続されます。
- ToR スイッチのペアは、 Azure Stack HCI 接続専用である必要はありません。
- ToR スイッチは、9216 の MTU サイズに設定されます。ネットワーク上で送信されるパケットの MTU サイズは、エンドポイントによって制御されます。

論理アーキテクチャ

Azure Stack HCI のネットワークインフラストラクチャは、複数の論理的なネットワークで構成されています。

- テナント(コンピューティング)ネットワーク:テナントネットワークは、テナントリモート対応マシン へのアクセスを提供する1つ以上のVLANを伝送するVLANトランクです。各VLANは、物理サーバ上 で実行されているToRスイッチおよびSETスイッチでプロビジョニングされます。各テナントVLANに は、IPサブネットが割り当てられている必要があります。
- 管理 ネットワーク(ネイティブ VLAN が優先されますが、タグ付き VLAN もサポートされます):管理 ネットワークは、親パーティションにネットワークトラフィックを伝送する VLAN です。この管理ネッ トワークは、ホストオペレーティング システムにアクセスするために使用されます。管理ネットワーク への接続は、親パーティションの管理(Mgmt) vNICによって提供されます。管理 vNIC の許容度障害性 は、SET スイッチによって提供されます。必要に応じて、帯域幅制限を管理に割り当てることができます。
- ストレージネットワーク:ストレージネットワークは、記憶域スペースダイレクト、ストレージレプリケーション、およびライブ移行ネットワークトラフィックに使用される RoCEv2 ネットワークトラフィックを伝送します。ストレージネットワークには、ストレージAとストレージBのセグメントがあり、それぞれに独自の IP サブネットがあります。この設計により、East-West RDMA が ToR スイッチに分離されます。
 このドキュメントでは、ストレージネットワークはクラスタ通信の優先経路としても使用されます。

(ストレージAとストレージBの両方のセグメントが使用できない場合は、管理ネットワークがクラス タ通信に使用されます)。

次の図は、テナントと管理ネットワーク(図 6) とストレージネットワーク(図 7) を示しています。テナント および管理ネットワークの場合、ToR はゲートウェイ機能を提供します。

Azure Stack HCI で実行されているサーバーのデフォルト ゲートウェイは、ToR によって提供されるエニーキャスト ゲートウェイです。



Note: vPC peer-link doesn't exist for ACI fabric.

図 6.

Azure Stack HCI 論理アーキテクチャ(テナントおよび管理ネットワーク)

テナント ネットワークや管理ネットワークとは異なり、ストレージ ネットワークには ToR のペアを接続するために 個別の VLAN が必要です。たとえば、VLAN 10 はリーフ 1(ストレージ A セグメント)の接続に使用され、VLAN 20 はリーフ 2(ストレージ B セグメント)の接続に使用されます。



Note: vPC peer-link doesn't exist for ACI fabric.

図 7. Azure Stack HCI 論理アーキテクチャ(ストレージ ネットワーク) ストレージネットワークの設計に関する考慮事項は次のとおりです。

- ストレージ ネットワークは、ToR スイッチのゲートウェイが必要ないレイヤ 2 通信にのみ使用されます。
- ストレージネットワークは、ストレージスペースダイレクト、ストレージレプリケーション、および ライブ移行ネットワークトラフィックに使用される RoCEv2トラフィックを伝送します。このドキュメ ントでは、クラスタ通信の優先経路としても使用されます。
- RoCE では、ネットワークをロスレスにするために Data Center ブリッジング (DCB) が必要です (DCB は iWARP のオプションです)。 DCB を使用する場合は、PFC および ETS 構成をネットワーク に実装する必要があります。
- ストレージネットワークは、このドキュメントではクラスタ通信の優先経路としても使用されるため、 ストレージトラフィックとクラスタ通信トラフィックには異なる QoS 設定が必要です。たとえば、Cos 4 はストレージトラフィック用で、Cos 7 はクラスタ通信トラフィック用です。

次の表に、 Microsoft が提供する QoS の推奨事項を示します。

ークの場合は2%

ストレージ トラフィック クラスタ通信トラフィック デフォルト(テナントおよび 管理ネットワーク) ストレージ スペース ダイレクト クラスタ ヒートビートの帯域幅 テナント ネットワークなどの 目的 他のすべてのトラフィック 予約 に使用されるロスレス RDMA 通 信の帯域幅予約 用。 フロー制御(PFC対 非対応 はい いいえ 応) トラフィック クラス 7 3または4 0 (デフォルト) 帯域予約 **25GbE** 以上の RDMA ネットワ 50 % デフォルト(ホスト構成は不 ークの場合は1% 要) **10GbE** 以下の RDMA ネットワ

表 1. Azure Stack HCI ネットワーク QoS の推奨事項

注: このドキュメントでは、ストレージネットワークがクラスタ通信の優先経路としても使用されています が、クラスタ通信は、優先経路と呼ばれる使用可能なネットワークを使用できます。この経路は、Microsoftネ ットワーク ATC を介して設定されたクラスタネットワークで定義されているメトリック ロールに基づいて選 択されます。(Microsoft ネットワーク ATC は、Azure Stack HCl サーバーでネットワーク展開をホストする ためのインテント ベースのアプローチ(管理、コンピューティング、またはストレージ)を提供します。詳細 については、Microsoft ネットワーク ATC のドキュメント を参照してください)。この例では、ストレージ A、 ストレージ B、および管理の 3 つのクラスタ ネットワークが存在します。

PS C:\Users\Administrator.MIHIGUCH> Get	t-Clus	terNetwo	ork
Name	State	Metric	Role
mgmt_compute_storage(Management)	Up	68800	ClusterAndClient
mgmt compute storage(Storage VLAN1601)	Up	19200	Cluster
mgmt_compute_storage(Storage_VLAN1602)	Up	19201	Cluster

図 8.

Azure Stack HCI クラスタ ネットワーク。Azure Stack HCI サーバの内部には、次のネットワーク コンポーネント があります。

- SET スイッチ:これは、チーミング機能が組み込まれた仮想スイッチです。SET スイッチは、SMB マル チチャネルを使用しないネットワークトラフィックにチーミング機能を提供します。SMB ダイレクト (RDMA)トラフィックは、SET スイッチのチーミング機能ではなく、SMB マルチチャネル*を使用し て、帯域幅と冗長性のために使用可能なネットワーク接続を活用します。
- ゲストパーティション:テナントリモート対応マシンは、Hyper-Vホストのゲストパーティションで 実行されます。各仮想マシンは他の仮想マシンから分離して実行され、ホストの物理ハードウェアに直通 窓口することはできません。仮想仮想マシンの合成 NIC をホストの SET スイッチに接続することで、テ ナント仮想マシンにネットワーク接続が提供されます。
- 親パーティション:親パーティションは、仮想化管理スタックを実行し、物理サーバハードウェアにアクセスホストオペレーティングシステムです。次の例に示すように、親パーティションには1つの管理 vNIC と2つのストレージ vNIC があります。必要に応じて、バックアップ操作用の専用 vNIC をオプションで追加できます。

* SMB マルチチャネルは、SMA 3.0 プロトコルの一部であり、ネットワーク パフォーマンスとファイル サーバーの可用性を向上させます。SMB マルチチャネルを使 用すると、ファイル サーバーは複数のネットワーク接続を同時に使用できます。

次の図は、Azure Stack HCI サーバ内の論理的なネットワーク図を示しています。この例では、ストレージAとストレージBは親パーティション専用ですが、管理ネットワークは親パーティションとゲストパーティションのVMの両方で使用できます。デフォルトでは、[管理オペレーティングシステムがこのネットワークアダプタを共有することを許可する]オプションは、SET スイッチの vNIC で有効になっています。この例では、管理 vNIC(黄色)で有効になっていますが、ストレージ vNIC(緑と紫)では無効になっています。



Note: vPC peer-link doesn't exist for ACI fabric.

図 9. Azure Stack HCI 論理アーキテクチャ(SET スイッチ、ゲスト、および親パーティション)

VM リモート対応 NIC の MAC アドレスは動的に割り当てられ、SET スイッチは送信元 MAC アドレスに基づいて使 用可能なアップリンク(サーバ上の物理 NIC)の1 つを選択します。この動作により、負荷バランシングと許容度障 害性が提供されます。次の図は、リモート対応 NIC MAC -A を備えた仮想マシン A からのトラフィックがアップリ ンクとして物理 NIC1 を使用し、リモート対応 NIC MAC -B を備えた仮想マシン B からのトラフィックが物理 NIC2 をアップリンクとして使用する例を示しています。物理 NIC1 を使用する経路が使用できない場合、すべてのトラフ ィックは他の経路を通過します。



図 10.

MAC アドレスに基づくロード バランシング動作。

この動作の結果、ストレージトラフィックではない一部の East-West ネットワークトラフィックは、スパイン (ACI の場合)または vPC ピアリンク (NX-OS の場合)を通過します。



図 11.

トラフィック フローの例

ネットワークは、必要なトラフィックを許可する必要があります。Azure Stack HCl のファイアウォール要件に ついては、<u>https://learn.microsoft.com/en-us/azure-stack/hci/concepts/firewall-requirements</u>を参照して ください<u>。</u>

ファブリックとメリットに基づいた Cisco Nexus 9000 シリーズ スイッチ

次の表に、 Nexus 9000 シリーズ スイッチベースのデータセンターファブリックの主な機能と利点を示します。

機能	利点	ACI/NX-OS
1 か所で管理	コントローラ(APIC または NDFC)を使用 すると、設定管理とポリシー定義の単一ポ イントが提供され、ファブリックの運用面 が簡素化されます。	ACI : APIC NX-OS : NDFC
エニーキャストゲートウェイ	ファブリックは、Azure Stack HCI サーバ ーおよびその他の物理/リモート対応サーバ ー上の VM のエニーキャスト ゲートウェイ として動作します。 レイヤ 3 ゲートウェイ機能は、コアまたは 集約スイッチではなく、ToR スイッチによ って提供されます。	両方
VXLAN	VXLAN を使用すると、物理リーフの場所に 関係なく、サーバー間のシームレスなレイ ヤ2およびレイヤ3接続が提供されます。 また、マルチテナント機能も提供します。	両方
マルチポッド/マルチサイト	マルチポッド/マルチサイトファブリック は、データセンター全体の物理場所に関係 なく、エンドポイント間のシームレスなレ イヤ 2 およびレイヤ 3 接続を提供します。	ACI : マルチポッド、マルチサイト、および リモートリーフ NX-OS : マルチサイト
サービス チェーニング	サービス チェーン機能を使用すると、ファ イアウォールや負荷バランサなどの L4 〜 L7 サービス デバイスへの回数変更可能トラ フィック リダイレクションが可能になりま す。	ACI : サービス グラフ PBR NX-OS : ePBR

図 12

Cisco ACI の接続オプションとポリシードメインの進化



- Single Fabric with End-to-End Encapsulation
- Single Overlay domain

- Multiple Fabrics with Integrated DCI
- Integrated DCI Scaling within and between Fabrics
- Multiple Overlay domains
- End-to-End automation support by NDFC

図 13.

ファブリックとメリットに基づいた Cisco Nexus 9000 シリーズ スイッチ

Azure Stack HCI 接続向け Cisco ACI 設計

このセクションでは、 Azure Stack HCI が EPG とブリッジドメインを使用して Cisco ACI に接続する方法について説明します。

この設計は、スパイン スイッチと APIC が展開され、リーフ スイッチのペアを介して接続された Cisco ACI フ ァブリックがお客様にすでに導入されていることを前提としています。

Azure Stack HCI 接続用 Cisco ACI

次の図は、Cisco ACI ファブリックを通過する Azure Stack HCI トラフィックの基本的なトラフィック フロー を示しています。この設計では、Cisco ACI ファブリックには、 APIC クラスタによって制御されるリーフノー ドと 2 つのスパインノードのペアが 2 つあります。ボーダー リーフ スイッチのペアには、L3Out が構成され ています。これにより、外部ルータのペア、つまりインターネットおよび企業ネットワークへの接続が提供され ます。リーフ ノードの別のペアは、 Azure Stack HCI サーバーと他のサーバーに接続されています。



図 14.

Cisco ACI ファブリックをビアた Azure Stack HCI トラフィックフロー

この設計では、各リーフスイッチは 100GbE リンクを使用して Azure Stack HCI サーバーに接続されます。 ACI リーフ スイッチと各 Azure Stack HCI サーバ間の 2 つのリンクは、ポートチャネルまたは vPC ではなく、 個別の接続です。

次の図は、ACI インターフェイス構成例と、ドメインおよび VLAN プールの構成を示しています。ToR スイッ チのペアで異なるインターフェイスを使用することは可能ですが、このドキュメントでは同じインターフェイス を使用します。 node-101 (ethernet1/11 および 1/12) と node-102 (ethernet1/11 および 1/12)。次の 図で、ACI インターフェイス構成例について説明します。



図 15. Azure Stack HCI サーバーの ACI リーフ インターフェイス構成

Azure Stack HCI ACI テナントモデルの概要

図 16 は、Azure Stack HCI テナントを強調表示することで、設計に展開されたさまざまな ACI テナント要素 間の高レベルの関係の例を示しています。この例では、Azure Stack HCI テナント(HCI_tenant1)には、仮想 ルーティングおよび転送(VRF)、ブリッジドメイン(BD)、およびテナントネットワークのエンドポイン トグループ(EPG)が含まれており、共通テナントには外部接続(L3Out)とストレージおよび管理ネットワ ーク用 EPG が含まれています。

Azure Stack HCI テナント ネットワークが他のデータセンター ネットワークと通信し、外部ネットワークにア クセスできるようにするには、テナント HCI1_tenant1 の EPG と同じテナントの他の EPG と共通テナントの 外部 EPG (L3Out EPG) の間に契約が存在する必要があります。ストレージ ネットワーク A と B の EPG の場 合、ストレージ トラフィックはそのセグメント (BD) 内にあるため、別の EPG とのコントラクトを構成する 必要はありません。



図 16.

Azure Stack HCI の ACI テナントの概要

一般的な ACI 構成に加えて、 Azure Stack HCI ネットワークには次の構成が必要です。

- Azure Stack HCI サーバーに接続されているインターフェイスで必要な LLDP TLV を有効にします。
- ストレージおよびクラスタ通信の QoS 構成

Cisco ACI および NDFC ファブリックの構成の詳細については、「ソリューションの展開」を参照してください。

Azure Stack HCI 接続のための Cisco NX-OS ベースのファブリック設計

このセクションでは、 Azure Stack HCI が NX-OS モードで Cisco Nexus 9000 シリーズ スイッチに接続する 方法について説明します。 Cisco Nexus 9000 NX-OS ベースの VXLAN または従来の従来の LAN ファブリックを使用して、AWS パスの 拡充 HCI 環境に接続できます。VXLAN は、スパイン スイッチとリーフ スイッチ間の L3 リンクを介した ECMP ベースのマルチパスを活用し、従来の従来の LAN ファブリックは、STP を実行する L2 リンク(アクセ ス デバイスと集約デバイス間)を使用します。VXLAN は、従来の従来の LAN よりも優れているため、データ センター ファブリックの構築で人気が高まり、採用が進んでいます。

VXLAN は、リーフ(VTEP とも呼ばれる)を使用してエンドホストを接続し、VXLAN トンネルの発信と終了を 実行する CLOS アーキテクチャを使用します。スパイン スイッチは、リーフ スイッチ間のレイヤ 3 接続を提 供します。

これらのファブリックは両方とも、Cisco NDFC で構築および管理できます。これにより、以前に使用されていた CLI ベースのアプローチとは異なり、より迅速でエラーのない展開が可能になります。Cisco NDFC は、あらゆる種類のデータセンター ファブリック展開に対応するさまざまなファブリック テンプレートをサポートしています。AWS パスの拡充 HCI では、Data CenterVLXAN EVPN および Enhanced Classic LAN ファブリックテンプレートを使用する必要があります。このドキュメントでは、AWS パスの拡充 HCI を VXLAN ファブリックに接続する手順とワークフローについて説明します。

Azure Stack HCI 接続用 Cisco NX-OS ベースのファブリック

次の図は、NX-OS ベースの VXLAN ファブリックを通過する Azure Stack HCI トラフィックの基本的なトラフィック フローを示しています。



図 17.

Cisco NX-OS ベースの VXLAN ファブリックを介した Azure Stack HCI トラフィック フロー

この設計では、vPC のリーフ スイッチのペアは、100 ギガビットイーサネットリンクを使用して Azure Stack HCI サーバーに接続されます。リーフ スイッチと各 Azure Stack HCI サーバ間の 2 つのリンクは、ポート チャネルまたは vPC ではなく、個別の接続です。

ソリューションの導入

このセクションでは、環境で使用する Cisco ACI および Cisco NDFC ファブリックを設定する詳細な手順について説明します。また、既存の Cisco ACI または Cisco NDFC ファブリックに新しいコンポーネントを追加する方法についても説明します。

注: このドキュメントの手順に従って Cisco ACI または Cisco NDFC の設定が完了したら、 Azure Stack HCI クラスタをインストールできます。Azure Stack HCI を登録する前に、 Azure Stack HCI ノードまたは Azure Stack HCI クラスタを展開する同じネットワーク内の他のコンピュータで 接続検証ツール (Invoke-AzStackHciConnectivityValidation) を使用できます。この検証ツールは、 Azure Stack HCI クラスタ を AWS パスの拡充に登録するために必要なネットワーク接続を確認します。

注: このドキュメントでは、Cisco ACI または Cisco NDFC ファブリックの展開と、 Azure Stack HCI の自動インストールについては説明しません。

次の表に、既存のセットアップで使用されているハードウェアとソフトウェアのバージョンを示します。

レイヤ	デバイス	ソフトウェアのバージョン	説明
Cisco ACI	Cisco APIC	6.0 (3e)	ACI コントローラ
	Cisco Nexus スイッチ(ACI モー ド)	16.0(3e)	ACI スパイン スイッチおよび リーフ スイッチ
Cisco NX-OS	Cisco NDFC	12.1.3b	NDFC
	Cisco Nexus スイッチ(NX-OS モード)	10.2(3F)	ToR スイッチ
Cisco Azure Stack HCI		2022H2	Azure Stack HCI リリース (Azure Stack HCI の一部で あるすべてのデバイスのソフ トウェアの個々のリリースを 含む)

表 3. ハードウェアとソフトウェアのバージョン

Azure Stack HCI の Cisco ACI 構成

このセクションでは、ACIファブリックと APIC がお客様の環境にすでに存在することを前提として、Azure Stack HCI サーバー用の Cisco ACI を設定する方法について説明します。このドキュメントでは、最初の ACI ファブリックをオンラインにするために必要な設定については説明しません。

Azure Stack HCI サーバー用に Cisco ACI を設定するための設定手順は次のとおりです。

- Azure Stack HCI サーバーに接続されたリーフ インターフェイスの構成
- QoS の設定
- EPG の設定

Azure Stack HCI サーバーに接続されたリーフ インターフェイスの構成

このセクションでは以下の手順について説明します。

- Azure Stack HCI 物理ドメインの VLAN プールの作成
- Azure Stack HCI の物理ドメインの構成
- Azure Stack HCI 物理ドメインの接続可能なアクセス エンティティ プロファイルの作成
- Azure Stack HCI に必要な TLV を有効にする LLDP ポリシーを作成する
- Azure Stack HCI に必要な TLV を有効にするためのインターフェイス プライオリティ フロー制御ポリシ 一の作成
- Azure Stack HCI サーバーに接続されたインターフェイスのインターフェイス ポリシー グループの作成
- Azure Stack HCI サーバーに接続されているリーフ インターフェイスにインターフェイス ポリシー グル ープへの関連付け

図 18 と表 4 に、このセクションで使用するトポロジ、インターフェイス、および物理ドメイン構成パラメータの概要を示します。この接続では、 ACI リーフ スイッチと Azure Stack HCI サーバー間で 4 つの 100 GbE インターフェイスを使用します。



図 18.

Azure Stack HCI サーバーのインターフェイスと物理ドメインの構成

表 4. Azure Stack HCI サーバーのインターフェイスと物理ドメインの構成

インターフェ イス	インターフェイ ス ポリシー グ ループ	LLDP インター フェイス ポリシ ー	インターフェ イス PFC ポリ シー	AAEP 名	ドメイン名	ドメイン のタイプ	VLAN Pool
Leaf1 および Leaf2 イーサ ネット 1/11- 12	個別 HCI	HCI_LLDP (DCBXP : IEEE 802.1)	PFC 自動	HCI_AAEP	HCI_phys	物理	HCI_VLAN_pool (VLAN 1600 ~ 1699)

表 5 および 6 に、このセクションで使用される共通およびユーザー テナント構成パラメータの概要を示します。 ACI リーフ スイッチは、L2 専用のストレージ ネットワークを除き、 Azure Stack HCI ネットワークへのゲー トウェイとして機能します。参考のためにコントラクト名が記載されていますが、共通テナントの共有 L3Out 構成とコントラクトの構成手順については、このドキュメントでは説明しません。



図 19.

テナント構成例

表 5. Azure Stack HCI common テナントの構成例

プロパティ	名前
テナント	共通
テナント VRF	common_VRF
ブリッジドメイン	common_VRF のストレージ A(サブネットなし) common_VRF のストレージ B(サブネットなし) common_VRF での管理(10.1.1.254/24)
リーフ ノードとインターフェイス	ノード 101 および 102 イーサネット 1/11 および 1/12
EPG	BD 管理での EPG 管理(VLAN 1600) BD ストレージ A の EPG ストレージ A(VLAN 1601) BD ストレージ B 内の EPG ストレージ B(VLAN 1602)
外部 EPG (L3 Out)	common テナントの Shared_L3Out
コントラクト	common テナントによって提供される Allow-Shared-L3Out

表 6. Azure Stack HCI テナントの構成例

プロパティ	名前
テナント	HCI_tenant1
テナント VRF	VRF1

プロパティ	名前
ブリッジ ドメイン	VRF1 Ø BD1 (192.168.1.254/24)
リーフ ノードとインターフェイス	ノード 101 および 102 イーサネット 1/11 および 1/12
EPG	BD1 の Web EPG(VLAN 1611) BD1 のアプリケーション EPG(VLAN 1612)
コントラクト	common テナントによって提供される Allow-Shared-L3Out テナントで定義された Web アプリ コントラクト

Azure Stack HCI 物理ドメインの VLAN プールの作成

このセクションでは、 Azure Stack HCI への接続を有効にするための VLAN プールを作成します。

Azure Stack HCI サーバーを ACI リーフ スイッチに接続するように VLAN プールを設定するには、次の手順を 実行します。

- 一番上のナビゲーションメニューから、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] を選択します。
- 2. 左側のナビゲーション ウィンドウで、【プール (Pools)】> [VLAN] の順に選択します。
- 3. 右クリックし、[IP プールの作成(Create IP Pool)]を選択します。
- 4. [プールの作成(Create Pool)] ポップアップウィンドウで、名前(HCI_VLAN_pool など)を指定し、
 [割り当てモード(Allocation Mode)]で[静的割り当て(Static Allocation)]を選択します。
- 5. カプセル化ブロックの場合は、右側の [+] ボタンを使用して VLAN を VLAN プールに追加します。 [範 囲の作成(Create Ranges)] ポップアップ ウィンドウで、リーフ スイッチから Azure Stack HCI サ ーバーに構成する必要がある VLAN を構成します。残りのパラメータはそのままにします。

-ali CH	ulu sco	APIC									
Sy	stem	Tenants	Fabric	Virtual N	letworking	Admin	Operations	Apps	Integrations		
		itory Fal	bric Policies	Access Polk	ies						
Polic	cies			000	Pools - VL	AN					
•	Quick S										
	Interfac	e Configuratio									
	Switche	Configuration 6			Create	MI AND					
> =	Module				Create	VLAN PO	001				0
> 🖿	Interfac					Description:	ACL_VLAN_pool				
	Policies					benergener. (April Contract				
6	Pools	rana External				location Mode:	Dynamic Allocat	ion Sta	tic Allocation		
×						Encap Blocks:					□ +
	Crea	ate Rang	jes						8	vlode Role	
			Type: VLAN								
		Descrip	ption: optio	nal							
						- Indexed	_				
		~	rige: VLAN	Teger Valu	e VLAN	integer Value					
		Allocation N	lode: Or	amic Attocation	Inherit allock	lode from parent	Static Alloca	rtion			
			Role: Ext	emal or On the wi	re encapsulations	Internal)				
										Cancel	Submit
								Cance	ОК	[600-699]	

- 6. [OK] をクリックします。
- 7. 【送信 (Submit)】をクリックします。

Azure Stack HCI の物理ドメインの構成

物理ドメイン タイプを作成するには、 Azure Stack HCI サーバーに接続し、次の手順を実行します。

- 1. 一番上のナビゲーション メニューから、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] を選択します。
- 一番上のナビゲーション メニューから、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] を選択します。
- 3. 左のナビゲーション ウィンドウで、[Physical and External Domains (物理と外部ドメイン)]を展開 し、[Physical Domains (物理ドメイン)] をクリックします。
- 4. [物理ドメイン (Physical Domains)]を右クリックし、適切な[物理ドメインの作成 (Create Physical Domain)]を選択します。
- 5. 【物理ドメインの作成(Create Physical Domain)】 ポップアップ ウィンドウで、ドメインの名前 (HCI_phys など)を指定します。VLAN プールの場合は、ドロップダウン リストから以前に作成し た VLAN プール(HCI_VLAN_pool など)を選択します。

alialia cisco	APIC										
System	Tenants	Fabric	Virtual N	etworking	Admin	Operations	Apps	Integrations			
Inve	ntory Fat	oric Policies	Access Polici	es							
Policies			\bigcirc	Physical Do	mains						
C Quick S	Start ce Configuratio			Create P	hysical	Domain					۲
Switch	Configuration es			Associated Er	Attachable atity Profile:	select a value		~			
> interfac				Securit	VLAN Pool: I y Domains:	HCI_VLAN_pool(sta	itic)	₽	(t t	
 Policies Physica Evte 	s al and External arnal Bridged D	Domains				Select 1	Name	Des	scription		
> 🖬 Fibr	e Channel Dom Domains	ains									_
> 🖿 Phy	sical Domains										
> 🖿 Pools									Cancel		Submit

6. [送信 (Submit)] をクリックします。

Azure Stack HCI 物理ドメインの接続可能なアクセス エンティティ プロファイルの作成 接続可能なアクセス エンティティ プロファイル (Attachable Access Entity Profile (AAEP)) を作成するに は、次の手順を実行します。

- 1. 一番上のナビゲーション メニューから、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] を選択します。
- ナビゲーションペインで、【ポリシー (Policies)】>【グローバル (Global)】>【接続可能なアクセス エンティティ プロファイル (Attachable Access Entity Profile)】の順に選択します。
- 3. 右クリックして、**[接続可能なアクセス エンティティ プロファイル**(Create Attachable Access Entity Profile)]を作成します。
- 【接続可能なアクセス エンティティ プロファイル(Create Attachable Access Entity Profile)】 ポッ プアップ ウィンドウで、名前(HCI_AAEP など)を指定し、【インフラストラクチャ VLAN の有効化 (Enable Infrastructure VLAN)】と【インターフェイスへの関連付け(Association to Interfaces)】 をオフにします。
- 5. [ドメイン (Domains)]については、ウィンドウの右側にある [+] をクリックし、[ドメインプロファ イル (Domain Profile)]の下のドロップダウン リストから以前に作成したドメインを選択します。
- 6. [Update] をクリックします。
- 7. 次に示すように、選択したドメインと関連する VLAN プールが表示されます。
- 8. [次へ(Next)]をクリックします。上記の手順4で[インターフェイスへの関連付け(Association to Interfaces)]がオフになっているため、このプロファイルは現時点ではどのインターフェイスにも関

連付けられていません。次のセクションでインターフェイスを設定すると、それらを関連付けることが できます。

cisco APIC				
System Tenants Fabric Virtual	Networking Admin	Operations Apps Integrations		
Inventory Fabric Policies Access Pol	icies			
Policies	Create Attachab	le Access Entity Profile		\bigotimes
	ereate / teaenas			
Interface Configuration	STEP 1 > Profile			I. Profile
Switch Configuration	Name:	HCI_AAEP		
> 🚞 Switches	Description:	optional		
> 🖿 Modules				
> 🖿 Interfaces	Enable Infrastructure VLAN:			
Policies	Association to Interfaces: Domains (VMM, Physical or			
> Switch	External) To Be Associated To Interfaces:	Domain Profile	Encapsulation	<u> </u>
		Physical Domain - HCl_phys	from:vlan-1600 to:vlan-1699	
> TP User Profile				
> 🚞 DHCP Relay				
> 🔚 Attachable Access Entity Profiles				
Fror Disabled Recovery Policy				
KCP Instance Policy default	EPG DEPLOYMENT (All Se	elected EPGs will be deployed on all the interfaces associat	ed.)	
				☆ +
> Troubleshooting	Application EPGs		Encap Primary Encap	Mode
> 🖿 Physical and External Domains				
> 🚞 Pools				
			Previous	el Finish

9. [完了 (Finish)] をクリックします。

Azure Stack HCI に必要な TLV を有効にする LLDP ポリシーを作成する

Azure Stack HCI に必要な TLV を有効にする LLDP ポリシーを作成するには、次の手順を実行します。

- 1. 一番上のナビゲーション メニューから、[ファブリック (Fabric)] > [ファブリック ポリシー (Fabric Policies)] を選択します。
- 左側のナビゲーション ウィンドウで、[ポリシー (Policies)]>[グローバル (Global)]>[デフォルト での LLDP ポリシー (LLDP policy by default)]を選択します。
- 3. 次のオプションの TLV を確認します。
 - i. DCBX (ストレージ ネットワーク用)
 - **ii.** ポートリンク集約
 - ⅲ. ポート最大のフレームサイズ
 - iv. ポート VLAN 名

注: Azure Stack HCI にも必要なポート VLAN は、LLDP ポリシーの設定に関係なく常に有効になっています。

cisco	APIC	(MinakoS	ite)					
System	Tenants	Fabric	Virtua	l Networking	Admin	Opera	tions A	Apps
Inve	ntory Fabr	ic Policies	Access Po	licies				
Policies		(\odot	LLDP Policy	/ - default			
C Quick St	tart			-				
> 🚞 Pods								
> 🚞 Switche	s							
> 🚞 Modules				Properties				
> 🚞 Interface	es			Hol	d Time (sec):	120		$\hat{}$
✓				Initial Dela	y Time (sec):	2		$\widehat{}$
> 🚞 Pod				Transmit Free	quency (sec):	30		$\hat{}$
> 🚞 Swite	ch			Optional	TLV Selector:			
> 🚞 Interf	face					DCBX		
🗸 🚞 Globa	al					🗹 Port Link A 🗹 Port Maxin	aggregation num Frame S	ize
> 🚞 DI	NS Profiles					🗹 Port Vlan M	lame	
> 🚞 Fa	abric L2 MTU							
Е м	lulticast Tree P	olicy default						
.	LDP Policy def	ault						
F Fa	abric Wildcard	Rogue Excepti	on					

4. [送信 (Submit)]をクリックします。

LLDP インターフェイス ポリシーの作成

Azure Stack HCI に必要な TLV を有効にする LLDP ポリシーを作成するには、次の手順を実行します。

- 1. 一番上のナビゲーション メニューから、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] を選択します。
- 2. 左側のナビゲーション ウィンドウで、【ポリシー(Policies)】>【インターフェイス(Interfaces)】> 【LLDP インターフェイス(LLDP Interfaces)】を選択します。
- 3. 右クリックして [LLDP インターフェイス ポリシーを作成 (Create CDP Interface Policy)] を選択し ます。
- **4.** [[LLDP インターフェイス ポリシーを作成 (Create CDP Interface Policy)] ポップアップウィンドウ で、名前を指定します (例: HCI_LLDP)。
- 5. [送信状態(Transmit State)]で[有効(Enable)]を選択します。
- 6. [DCBXP バージョン (DCBXP Version)]に [IEEE 802.1] を選択します。

cisco	APIC									
System	Tenants	Fabric	Virtual N	letworking	Admin	Operations	Apps	Integrations		
Inve	ntory Fab	ric Policies	Access Polic	ies						
Policies			00	Interfac	e - LLDP Inte	rface				
Quick S	tart e Configuration									
Switch	Configuration			 Name 		labe	÷I		Receiv	e State
> 🚞 Switche	es			Creat	te LLDP In	terface Pol	licy			\otimes
> 🚞 Module					Name:	HCI_LLDP	-			
> 🚞 Interfac					Description:	optional				
∼ 🖿 Policies										
> 🚞 Swit					Alias:					
V 🖬 Inter	face				Receive State:	Disabled E	nabled			
> 🖬 8	02.1x Port Auth	entication			Transmit State	Disabled F	nabled			
	OP Interface				fransmit state.					
	ata Plane Polic	ina		\triangle	Warning: Chan	ging the DCBX ve	ersion may	prevent the port p	parameters	s from
	WDM		4		converging. In	ie link may need	to be reset	for the change to	таке еттес	εt.
> 🖬 F	ïbre Channel In	terface								
> 🚍 F	ïrewall				DCBXP Version:		302.1			
> 🚞 L	2 Interface							Cancel	Sub	mit
> 🖬 L	ink Flap									
> 🖬 L	ink Level									
> 🖬 L	ink Level Flow	Control								
	LDP Interface									

7. [送信 (Submit)]をクリックします。

インターフェイス優先順位フロー制御ポリシーの作成

リーフ ダウンリンクで PFC を有効にするインターフェイスポリシーグループを作成するには、次の手順を実行 します。

- 一番上のナビゲーションメニューから、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] を選択します。
- 左側のナビゲーション ウィンドウで、[ポリシー (Policies)]>[インターフェイス (Interface)]> [優先フロー制御 (Priority Flow Control)]を選択します。
- 3. 右クリックして、**[優先フロー制御ポリシーの作成(Create Priority Flow Control Policy)]**を選択し ます。
- [優先フロー制御ポリシーの作成(Create Priority Flow Control Policy)] ポップアップウィンドウで、 名前(PFC-Auto など)を指定し、[自動(Auto)]を選択します。(DCBX プロトコルをビア PFC 構成状態を含めるには、[自動(Auto)]に設定する必要があります)。

5. [送信 (Submit)] をクリックします。

Azure Stack HCI サーバーに接続されたインターフェイスのインターフェイス ポリシー グループの 作成

ACI ファブリックの外部の外部ゲートウェイに接続するためのインターフェイス ポリシー グループを作成する には、次の手順を実行します。

- 1. 一番上のナビゲーション メニューから、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] を選択します。
- 左側のナビゲーション ウィンドウで、【インターフェイス(Interfaces)】>【リーフ インターフェイス (Leaf Interfaces)】>【ポリシー グループ(Policy Groups)】>【リーフ アクセス ポート(Leaf Access Port)】を選択します。
- 3. 右クリックして、**[リーフ アクセス ポート ポリシー グループの作成**(Create Leaf Access Port Policy Group)]を選択します。
- 4. [リーフ アクセス ポート ポリシー グループの作成(Create Leaf Access Port Policy Group)] ポップ アップ ウィンドウで、名前(Individual-HCI など)と、各フィールドのドロップダウン リストから該 当するインターフェイス ポリシーを指定します。
- [接続エンティティプロファイル (Attached Entity Profile)]、[LLDP ポリシー (LLDP Policy)]、および[プライオリティ フロー制御 (Priority Flow Control)]フィールドで、以前に作成した AAEP、 LLDP ポリシー、およびプライオリティ フロー制御ポリシー (HCI_AAEP、HCI_LLDP、PFC-auto など)を選択します。

alialia A	PIC		Create Leaf Acces	ss Port Policy Gr	roup				\bigotimes
cisco		_	Name:	Individual-HCI					
System Ter	nants Fabric	Virtual	Description:	optional					
Inventory	Fabric Policies	Access Poli							
Policies			Attached Entity Profile:	HCI_AAEP	~ 🖉	Link Level Policy: se	elect a value	\sim	
Policies		\mathbb{O}	CDP Policy:	select a value		LLDP Policy: H	CI_LLDP	 	
🕩 Quick Start			View Advanced Settings 🗸						
E Interface Con	figuration								
\Xi Switch Config	guration		802.1x Port Authenticati	on: select a value	~	MCP	: select a value	~	
> 🚞 Switches			Transceiver poli	cy: select a value	\sim	Monitoring Policy	: select a value	~	
> 🚞 Modules			CoPP Poli	cy: select a value	\sim	PoE Interface	: select a value	\sim	
✓			DWD	M: select a value	\sim	Port Security	select a value	\sim	
🗸 🚞 Leaf Interf	aces		Egress Data Plane Polici	ng: select a value	\sim	Priority Flow Control	: PFC-Auto	~ 🕑	
> 🚞 Profiles			Fibre Channel Interfa	ce: select a value	\sim	Slow Drain	: select a value	\sim	
🗸 🚞 Policy (Groups		Ingress Data Plane Polici	ng: select a value	\sim	Storm Control Interface	: select a value	\sim	
> 🖬 Leaf	f Access Port		L2 Interfa	ce: select a value	\sim	STP Interface Policy	select a value	\sim	
> 🖬 PC I	nterface		Link Flap Poli	cy: select a value	\sim	SyncE Interface Policy	: select a value	\sim	
> 🖿 VPC	Interface		Link Level Flow Control Poli	cy: select a value	\sim				
> 🗖 PC/\	VPC Override		MACs	ec: select a value	~				
> 🚞 Leaf	f Breakout Port Group)							
> 🚞 FC II	nterface		NetFlow Monitor Policies:						+
> 🚞 FC F	PC Interface			NetFlow IP Filter Type		NetFlow Mon	itor Policy		
> 🚞 Overrid							,		
> 🚞 Spine Inter	rfaces								
> 🚞 Policies									
> 🚞 Physical and B	External Domains								
> 🖿 Pools									
							Cance	l Sub	omit

6. [送信 (Submit)] をクリックします。

Azure Stack HCI サーバーに接続されたリーフィンターフェイスへのインターフェイス ポリシー グループの関連付け

Azure Stack HCI サーバーに接続されたリーフィンターフェイスを設定するには、次の手順を実行します。

- 1. 一番上のナビゲーション メニューから、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] を選択します。
- 2. 左側のナビゲーションペインから[インターフェイス構成 (Interface Configuration)]を選択します。.
- 3. 右側のペインで、**[アクション (Actions)]**を右クリックし、**【インターフェイスの構成 (Configure Interfaces)**]を選択します。

cisco APIC		admin 🔍 🗩 🏰 🍪 🕐 🗳
System Tenants Fabric	Virtual Networking Admin Operations Apps Integrations	
Inventory Fabric Policie	Access Policies	
Policies	\odot	
Quick Start	Interface Configuration	Ø
Interface Configuration	-	_
 Switch Configuration Switches 	▲ Some of the interfaces are still configured using Selectors and Profiles. We can help you migrate them.	
> 🚞 Modules		
> 🚔 Interfaces > 🚞 Policies	Filter by attributes	Actions 🔿 🔅
Physical and External Domains Englis	P + Node + Interface + Port Type Admin State Port Mode Policy Group Interface Desc	Configure Interfaces
		Convert Interfaces

4. 【インターフェイスの構成(Configure interfaces)]ウィンドウで、次のオプションを選択します。

i. ノードタイプ: リーフ

- **ii.** ポートタイプ: アクセス
- ₩. インターフェイス タイプ: **イーサネット**
- iv. インターフェイス集約タイプ(Interface Aggregation Type):個別(Individual)
- 5. [ノードの選択 (Select Nodes)] をクリックします。[ノードの選択 (Select Nodes)] ポップアップ ウ ィンドウで、Azure Stack HCI サーバーに接続するリーフ ノード (たとえば、ノード 101-102) を選 択し、[OK] をクリックします。
- 6. Azure Stack HCI サーバーに接続するリーフィンターフェイスを指定します(たとえば、1/11-12)。

Configure Interfaces	
General	
Node Type Leaf Spine	
Port Type Access Fabric	
Interface Type Ethernet Fibre Channel	
Interface Aggregation Type	
Node* 🛈	
101-102	Select Node
Interfaces For All Switches * 🛈	

[リーフアクセスポートポリシーグループの作成(Create Leaf Access Port Policy Group)] をクリックします。[リーフアクセスポートポリシーグループの選択(Select Leaf Access Port Policy Group)] ポップアップウィンドウで、リストから以前に作成したリーフアクセスポートポリシーグループ(Individual-HCI など)を選択し、[選択(Select)] をクリックします。

d	Configure interfaces			
	General			
	Node Type Leaf Spine			
	Port Type Access Fabric			
	Interface Type Ethernet Fibre Channel			
	Interface Aggregation Type Individual PC vPC			
	Node* 🛈			
	101-102	Select Node		
	Interfaces For All Switches * 🕢	٦		
	Leaf Access Port Policy Group * Individual-HCIX			
	Configuration Status			
	ID • Name	Interfaces	Configuration Status	

8. [保存 (Save)]をクリックします。

Pod1-Leaf1

Pod1-Leaf2

QoS の構成

101

102

次の表に、 Microsoft によるホスト ネットワーク QoS の推奨事項をまとめます。詳細については、 Microsoft のドキュメント (<u>https://learn.microsoft.com/en-us/azure-stack/hci/concepts/host-network-requirements</u>) を参照してください。

Configuration will be updated

Configuration will be updated

1/11-12

1/11-12

表 7. Azure Stack HCI ホストネットワーク QoS の推奨事項

	クラスタ通信トラフィック	ストレージ トラフィック	デフォルト(テナントおよび 管理ネットワーク)
目的	クラスタ ヒートビートの帯域幅予 約	ストレージ スペース ダイレク トのロスレス RDMA 通信の帯 域幅予約	テナント ネットワークなどの 他のすべてのトラフィック 用。
フロー制御 (PFC 対応)	非対応	はい	いいえ
帯域予約	25GbE 以上の RDMA ネットワーク の場合は 1% 10GbE 以下の RDMA ネットワーク の場合は 2%	50 %	デフォルト(ホスト構成は不 要)

推奨事項に基づいて、このドキュメントでは例として次の ACI QoS 設定を使用します。これは、 <u>Microsoft</u> <u>Azure Stack HCI 用 Cisco UCS C240 M6 ソリューションで</u>使用される帯域幅予約および優先順位設定と同じ です。

 RDMA (ストレージ) トラフィックのレベル 1 (トラフィックには Azure Stack HCI によってマークさ れた Cos 4 が付属) / 前

/ 1

Cancel Save And Continue Save

- o PFC が有効になっている
- o 帯域幅予約:50%
- o ETS (ACIの重み付けラウンドロビン)
- クラスタ通信用のレベル2(トラフィックには Azure Stack HCI によってマークされた Cos 5 が付属 しています)
 - o PFC が有効になっていません
 - o 帯域幅予約:1%
 - o ETS (ACI の重み付けラウンドロビン)
- VM トラフィックと管理トラフィック(その他のトラフィック)の場合は Level3(デフォルト)
 - o PFC が有効になっていません
 - o 帯域幅予約:49%
 - o ETS (ACI の重み付けラウンドロビン)

次の図で、QoS 構成例について説明します。



QoS config on ACI fabrics

- Level1: For Storage EPGs Cos 4. 50%. PFC is enabled for Cos 4.
- Level2: For Storage EPGs Cos 5. 1%.
- Level3(default): default configuration for other EPGs. 49%

QoS config on AzureStack HCI

- Storage: 50% (Priority 4 = Cos 4)
- Cluster: 1% (Priority 5 = Cos 5)
- Others: 49%

(Cluster traffic is also carried over Storage networks: Storage A and Storage B)

図 20.

Azure Stack HCI の ACI QoS 構成

Cisco ACI ファブリックは、ユーザー構成可能な 6 つの QoS レベル (レベル 1 ~ 6) と、ファブリック制御ト ラフィック、 SPAN、およびトレースルート トラフィック用に予約済みれた 2 つのレベルをサポートします。

表 8. Cisco ACI QoS レベル

サービスクラス	DCBX で使用される QoS グ ループ(ETS 構成および ETS 推奨)*	トラフィック タイプ	VXLAN ヘッダーでの Doc1p(CoS)マーキ ング	DEI ビット**
0	0	レベル3(デフォルト)	0	0

サービスクラス	DCBX で使用される QoS グ ループ(ETS 構成および ETS 推奨)*	トラフィック タイプ	VXLAN ヘッダーでの Doc1p(CoS)マーキ ング	DEI ビット**
1	1	レベル 2	1	0
2	2	レベル 1	2	0
4	7	レベノレ 6	2	1
5	6	レベル 5	3	1
6	5	レベル 4	5	1
3	3	APIC コントローラ	3	0
9	アドバタイズなし	SPAN	4	0
8 (SUP)	4	制御	5	0
8 (SUP)	4	トレースルート	6	0
7	アドバタイズなし	コピー サービス	7	0

* IEEE DCBX PFC 構成 LLDP TLV では、優先順位値は、どの PFC レベル(1 ~ 6)が有効になっているかに関係なく、関連付けられた CoS 値です。ここで示す構成例は、次のとおりです。

**ドロップ適性インジケータ(DEI)ビットは、トラフィック輻輳中にドロップ可能なフレームを示す1ビット フィールドです。CoS 値 (3ビット)+ DEI 値(1ビット)は、QoS クラスを表します。

QoS クラスの構成

Cisco ACI QoS クラスを構成するには、次の手順を実行します。

- 1. 一番上のナビゲーション メニューから、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] を選択します。
- 2. 左側のナビゲーション ウィンドウで、[ポリシー (Policies)]>[グローバル (Global)]>[QoS クラ ス (QoS Class)]の順に展開し、いずれかのレベルを選択します。 (たとえば、ストレージ トラフ ィックの場合は level1)。
- 3. [スケジューリング アルゴリズム (Scheduling algorithm)] フィールドで、ドロップダウンリストか ら [重み付けラウンドロビン (Weighted round robin)] を選択します。これはデフォルトの設定で す。
- **4.** [帯域幅割り当て(%単位) (Bandwidth allocation (in %))]フィールドで、数値を指定します。(た とえば、ストレージトラフィックの場合は **50**)。
- 5. クラスで PFC が必要ない場合は、[PFC 管理状態(PFC Admin State)] フィールドをオフのままにします。
- 6. クラスで PFC が必要な場合、
 - a. [PFC 管理状態 (PFC Admin State)] フィールド
 - b. [No Drop-Cos] フィールドで、[Cos] 値を選択します(たとえば、ストレージ トラフィックの 場合は Cos 4)。

c. [範囲 (Scope)] オプションで、[ファブリック全体 PFC (Fabric-wide PFC)] を選択します。 (トラフィックが同じリーフ内にある場合、IntraTor PFC も問題ありません)

System	Tenants	Fabric	Virtual N	letworking	Admin	Operations	Apps	Integration	IS
Inve	ntory Fa	abric Policies	Access Poli	cies					
Policies		(06	QOS Class	Policy - Lev	vel1			0
C Quick S	tart e Configuratio	on						Policy	History
Switch (Configuration								0 +
> 🚞 Switche	s			Properties					
> 🖿 Module:	s				QoS Class	: Level1			
⇒ Interfac	es				Admin State:	Enabled	×		
🗸 🚞 Policies					MTU	9216	\bigcirc		
> 🚞 Swit	ch			M	linimum buffers	: 0	\Diamond		
> 🚞 Inter	face			Conge	stion Algorithm	: Tail drop	Weighted rar	ndom early deteo	ction
🗸 🚞 Glob	al			Queue	control method	: Dynamic			
> 🚞 P	TP User Profil	le	4	Sched	luling algorithm:	Weighted rour	nd robin \smallsetminus		
> 🖿 D	HCP Relay			Bandwidth	allocated (in %)	50	\Diamond		
> 🖿 A	ttachable Acc	ess Entity Profi	les	P	FC Admin State				
E E	rror Disabled I	Recovery Policy	/		No-Drop-CoS	cos 4	\sim		
= N	ICP Instance F	Policy default				When PFC Admin	State is unchecked	d, this field value wil	l be set to emp
v 🖿 q	OS Class				Scope	Fabric-wide	PFC Intra	Tor PFC	
Ē	Level1								
Ē	Level2								
F	Level3 (Defa	ault)							
F	Level4								
F	Level5					Show U	Isage I	Reset	Submit
Ē	Level6								

- 7. [送信 (Submit)] をクリックします。
 - この QoS 構成と LLDP IEEE DCBX 構成では、次の値が LLDP に設定されます。
 - IEEE ETS 構成および IEEE ETS 推奨
 - o Prio 4 の PGID: 2 (Cos 4 が選択され、レベル 1 が QoS グループ 2 であるため)
 - PGID 2 の帯域幅: 50 (レベル 1 は QoS グループ 2)
 - トラフィック クラス 2 の TSA: 拡張伝送選択(レベル 1 は QoS グループ 2)
 - IEEE プライオリティ フロー制御の構成
 - o プライオリティ 4 の PFC: 有効(Cos 4 が選択され、PFC が有効になっているため)


デフォルトでは、すべての「PGID for Pri 0」~「PGID for Pri 7」は 0 に設定され、すべての「PFC for Priority 0」~「PFC for Priority 7」は無効に設定されます。PFC が有効になっている場合、特定の優先 順位の値(Cos 値)が更新されます。(上記の例では「PGID for Pri 4: 2」および「PFC for Priority 4」)。

- クラスタ通信トラフィックのレベルに対してステップ2~7を繰り返します。たとえば、帯域幅予約が 1%のクラスタ通信トラフィックの level2 は次のようになります。
- QOS クラス : Level2
- スケジューリング アルゴリズム:重み付けラウンド ロビン (デフォルト設定)
- 帯域幅割り当て(%単位):1
- **PFC** 管理状態 オフ

この QoS 構成と LLDP IEEE DCBX 構成では、次の値が LLDP に設定されます。プライオリティ 0 ~ 3 および 5 ~ 7 の PGID と PFC に変更はありません。

- IEEE ETS 構成および IEEE ETS 推奨
 - a. PGID 1 の帯域幅: 1 (level2 は表 8 に基づく QoS グループ 1 であるため)
 - b. トラフィック クラス1のTSA: 拡張伝送選択
- 他のトラフィックのレベルに対してステップ2~7を繰り返します。たとえば、帯域幅予約が49%の VMトラフィックの level3 (デフォルト) は次のようになります。
- QoS クラス: level3 (デフォルト)
- スケジューリング アルゴリズム:重み付けラウンド ロビン (デフォルト構成)
- 帯域幅割り当て(%単位):49
- **PFC** 管理状態 オフ

この QoS 構成と LLDP IEEE DCBX 構成では、次の値が LLDP に設定されます。プライオリティ $0 \sim 3$ および $5 \sim 7$ の PGID と PFC に変更はありません。

- IEEE ETS 構成および IEEE ETS 推奨
 - a. PGID 0 の帯域幅: 10 (level3 は表 8 に基づく QoS グループ 0 であるため)
 - b. トラフィック クラス 0 の TSA: 拡張伝送選択



カスタム QoS ポリシーの構成

ACIには、次の図に示す複数の QoS 分類オプションがあります。



図 21. ACI QoS 構成の優先順位

このドキュメントでは、テナントおよび管理ネットワークの EPG で QoS クラス設定を使用し(デフォルトの レベル 3)、ストレージおよびクラスタ通信ネットワークの EPG でカスタム QoS ポリシー設定を使用します (Cos 4 のストレージの場合は level1、Cos 5 のクラスタ通信の場合は level2)。



図 22.

ACI QoS および EPG の構成例

ポリシーを構成するには、次の手順を実行します。

- 1. APIC の上部ナビゲーションメニューから、[テナント(Tenants)]、[共通(common)]の順に選択 します(または、EPGを設定する既存のテナントを選択します)。
- 2. 左側のナビゲーション ウィンドウから展開して、【ポリシー(Policies)】>【プロトコル(Protocol)】 > [カスタム QoS(Custom QoS)】を選択します。
- 3. 右クリックして [カスタム QoS ポリシーの作成 (Create Custom QoS)]を選択し、[カスタム QoS ポリシーの作成 (Create Custom QoS Policy)] ポップアップ ウィンドウを開きます。
- 4. [名前 (Name)] フィールドで、名前を指定します(例: Storage_and_Cluster)。
- 5. [Dot1P Classifiers] フィールドで、[+] をクリックし、以下を構成します。
 - a. 優先順位(この例では、ストレージトラフィックのドロップダウンリストから level2 を選択 します)
 - **b.** Dot1P 範囲(Dot1P Range From and To)(この例では、ストレージトラフィックに **4** を指定します)
- 6. [Update] をクリックします。
- クラスタ通信トラフィックに対してステップ5~6を繰り返します。(この例では、クラスタ通信トラフィックの場合は level1、5 です)。

APIC (172.31.184.201)	Create Custom	QOS Policy					8
cisco	Name:	Storage_and_Cluster					
System Tenants Fabric Virtual N ALL TENANTS Add Tenant Tenant Search: rea	Description:	optional					
This object was created by the Nexus Das	DSCP to priority map:						+
common Daa		Priority	DSCP Range From	DSCP Range To	DSCP Target	Target CoS	
C G G							
> Networking	Dot1P Classifiers:					1	+
E Contracta		Priority	Dot1P Range From	Dot1P Range To	DSCP Target	Target CoS	
E Policies		Level2	4	4	Unspecified	Unspecified	
V E Instant		Level1	5	5	Unspecified	Unspecified	
> 🚍 8FD							
) 🚍 BFD Multikop							
) 🔛 ND RA Prefix							
) 🚍 BGP							
Connectivity Instrumentation Policy							
- 🔚 Custom QoS							
P default Create Custom QoS Policy					Cancel	Submit	
🔅 🛅 Data Plane Policing					Cancer	Jucente	

8. [送信 (Submit)] をクリックします。

このカスタム QoS ポリシーは、次のステップ(EPG の構成)で参照されます。

EPG の構成

このセクションでは、次の EPG が作成されます。

- VM のテナント EPG
- 管理ネットワークの管理 EPG
- ストレージ ネットワークのストレージ EPG
- コントラクトの設定
- コンシューマーおよびプロバイダー EPG のコントラクトへの追加

テナント EPG の設定

Azure Stack HCI VM のテナント EPG を構成するには、次の手順を実行します。

- 1. APIC の上部のナビゲーション メニューから、[テナント(Tenants)]>[テナントの追加(Add Tenant)]を選択します。
- 2. [テナントの作成(Create Tenant)]ダイアログボックスで、名前(HCl_tenant1 など)を指定します。
- 3. [VRF 名 (VRF Name)] フィールドに、VRF 名を入力します (VRF1 など)。
- **4.** [ブリッジドメインの作成 (Create A Bridge Domain)]をオンにし、[次へ (Next)]をクリックします。

	Create VRF	Ø
cisco AFIG (1/2.51.104.	STEP 1- VRF	1. VRF 2. Bridge Domain
System Tenants Fabric	Name: VRF(
ALL TENIANTE L. Add Toront L. Toront	Allas:	
ALL TENANTS Add Tenant Tenant	Description: optional	
HCI_tenant1	Annotations: 🚳 Click to add a new annotation	
> 🕩 Quick Start	Policy Control Enforcement Preference: Enforced Unenforced	
∨ III HCI_tenant1	Policy Control Enforcement Direction: Egress Ingress Mixed policy	
E Application Profiles	BD Enforcement Status:	
✓ ➡ Networking	Endpoint Ketention Molecy: Select a Value This policy only applies to remote L3 entries	
🔚 Bridge Domains	Monitoring Policy: select a value	
VRFs	DNS Labels: enter names separated by	
> 🖬 L2Outs Create VRF	Transit Route Tag Policy: select a value	
> 🚞 L3Outs	IP Data-plane Learning: Disabled Enabled	
	Create A Bridge Domain: 🗹	
	Configure BGP Policies:	
	Configure OSPF Policies:	
	Compare croso, Policies: [1]	
		Previous Cancel Next

5. [名前 (Name)]フィールドで、名前 (BD1 など)を指定し、[完了 (Finish)]をクリックします。

Create VRF						\bigotimes
TEP 2 > Bridge Domain				1. VRF	2. Bridge	Domain
Name:	BD1					
Alias:						
Description:	optional					
Туре:	fc regular					
Forwarding:	Optimize 🗸					
IP Data-plane Learning:	Yes No					
Limit Local IP Learning To BD/EPG Subnet(s):						
Config BD MAC Address:						
MAC Address:	00:22:BD:F8:19:FF					
			_			
			Pre	vious	Cancel	Finish
6 ブリッジ ドメインに	エニーキャス	ト ゲートウェイ	IP アドレスを	作成する	5には. 「 N	lavigation

- ブリッジ ドメインにエニーキャスト ゲートウェイ IP アドレスを作成するには、[Navigation]ペインで、 [ネットワーキング (Networking)]>[ブリッジドメイン (Bridge Domains)]で作成したブリッジ ドメイン (BD1)を展開します。
- 7. [サブネット(Subnets)]を右クリックし、[サブネットの作成(Create Subnet)]を選択します。

8. 【ゲートウェイ IP(Gateway IP)】 フィールドで、エニーキャスト ゲートウェイの IP アドレス(この 例では 192.168.1.254/24)を設定し、【送信(送信)】 をクリックします。

ADIC (172 31 184 201)	Create Subnet	\otimes
cisco AFIO (1) 2.0 1.104.201)	Gateway IP: 192.168.1.254/24	
System Tenants Fabric Virtu	address/mask Treat as virtual IP address:	
ALL TENANTS Add Tenant Tenant Search:	Make this IP address primary:	
HCI_tenant1	Scope: Advertised Externally	
> C Quick Start	Description: optional	
✓		
Application Profiles	Subnet Control: No Default SVI Gateway	
🗸 🚞 Networking	IP Data-plane Learning: Disabled Enabled	
💛 🚞 Bridge Domains	ir bata-plate Learning.	
∨ (1)) вD1	L3 Out for Route Profile: select a value	
> 🖬 DHCP Relay Labels	ND RA Prefix Policy: select a value	
> 🚞 ND Proxy Subnets	Policy Tags: 🕀 Click to add a new tag	
> 🖬 Subnets		
VRFs Create Subnet		
> 🐽 VRF1		
	C	ancel Submit

- アプリケーション プロファイルを作成するには、左側のナビゲーション ウィンドウで [アプリケーショ ンプロファイル (Application Profiles)]を右クリックし、[アプリケーションプロファイルの作成 (Create Application Profile)]を選択します。
- 10.[名前(Name)] フィールドで、名前(AP1 など)を指定し、[送信(送信)] をクリックします。
- 11.EPG を作成するには、左側のナビゲーション ウィンドウから、作成したアプリケーション プロファイ ルを展開し、[アプリケーション EPG (Application EPGs)]を右クリックして、[アプリケーション EPG の作成 (Create Application EPG)]を選択します。
- 12.[名前 (Name)]フィールドで、名前 (Web など)を指定します。
- 13.[QoS クラス (QoS class)] フィールドで、ドロップダウン リストから [レベル (Level)]を選択しま す。(たとえば、VM トラフィックの場合は Level3 (デフォルト) 。これはデフォルト構成)。
- **14.[ブリッジ ドメイン (Bridge Domain)]** フィールドで、ドロップダウン リストから作成した BD (この 例では BD1) を選択します。
- 15.[リーフ/パスで静的にリンク(Statically Link with Leaves/Paths)] チェックボックスをオンにして、
 [次へ(Next)] をクリックします。

APIC (172.31.184.201)	Create Application El	PG	0
	STEP 1 - Identity		1. Identity 2. Leaves/Paths
System Tenants Fabric Virtual Net	Name	Web	Contraction and Contraction of Contr
ALL TENANTS Add Tenant Tenant Search: name	Allas		
	Description:	optional	
HCI_tenant1			
Ch Quilde Start	Annotations	CFck to add a new annotation	
	Contract Exception Tag:		
V HCI_tenant1	QoS class:	Level3 (Default)	
💛 🚞 Application Profiles	Custom QoS	select a value	
~ 🚯 ар1	Data-Plane Policer:	select a value	
Application EPGs	Intra EPG Isolation:	Enforced Unenforced	
> uSeg EPGs Create Application EPG	Preferred Group Member:	Exclude Include	
> 🧮 Endpoint Security Groups	Flood in Encapsulation	Disabled Enabled	
	Bridge Domain:	P01 🗸	
	Monitoring Policy:	select a value 🛛	
Bridge Domains	FHS Trust Control Policy.	select a value [~]	
∨ ()) вD1	EPO Admin State	Admin Up Admin Shut	
> 🚞 DHCP Relay Labels	Associate to VM Domain Profiles:		
> 🥅 ND Proxy Subnets	Statically Link with Leaves/Paths.	2	
Subnets	EPG Contract Master:		- = +
- 100 160 1 05 4/04		Application EPGs	
VRFs			
> 🚹 VRF1			
			Cancel Next

注: テナント EPG の QoS クラスは Level3(デフォルト)であり、デフォルトでは PFC は有効になりません。

- **16.**[物理ドメイン (Physical Domain)]フィールドのドロップダウンリストから、作成した物理ドメイン (この例では **HCI_phys**)を選択します。
- **17.[パス (Paths)**]フィールドで、[+]をクリックし、パスを選択してポート カプセル化を構成します。 (この例では、Web の場合は Pod-1/Node-101/eth1/11 および vlan-1611)。
- 18.手順 17 を繰り返して、クラスタの Azure Stack HCI サーバーに接続されているすべてのインターフェ イスを追加します。(この例では、Web の場合、Node-101/eth1/11-12 および Node-102/eth1/11-12 と vlan-1611)。

19.他のテナント EPG(たとえば、vlan-1612の EPG アプリ)に対して手順 11~18 を繰り返します。

管理 EPG を構成します。

Azure Stack HCI ストレージネットワーキングを構成するには、次の手順を実行します。

- 1. APIC の上部のナビゲーション メニューから、[テナント(Tenants)]>[共通(common)]の順に選 択します(または、管理 EPG を設定する既存のテナントを選択します)。
- 左側のナビゲーション ウィンドウで、[ネットワーク (Networking)]>[ブリッジドメイン (Bridge Domains)]を選択します。
- 3. 右クリックして、【ブリッジドメインの作成(Create Bridge Domain)】を選択します。
- **4. [名前 (Name)**] フィールドで、名前 (**Mgmt** など)を指定し、VRF 名 (この例では **common-VRF**) を選択します。
- 5. [次へ (Next)] をクリックします。
- 6. [Subnets] フィールドで、[+] をクリックします。

- 7. [ゲートウェイ IP (Gateway IP)] フィールドで、IP (たとえば、10.1.1.254/24) を指定します。
- 8. [OK] をクリックします。
- EPG を作成するには、左側のナビゲーション ウィンドウから [アプリケーションプロファイル (Application Profiles)]を展開し、既存のアプリケーション プロファイルを選択します(または新 しいアプリケーション プロファイルを作成します)。
- **10.**[アプリケーション EPG (Application EPGs)]を右クリックし、[アプリケーション EPG の作成 (Create Application EPG)]を選択します。
- 11.[名前 (Name)] フィールドで、名前 (Mgmt など) を指定します。
- 12.[QoS クラス(QoS class)] フィールドで、ドロップダウン リストから [レベル(Level)]を選択しま す。(たとえば、管理トラフィックの場合は Level3(Default))。
- **13.[ブリッジ ドメイン (Bridge Domain)]** フィールドのドロップダウン リストから、作成した BD (この 例では Mgmt) を選択します。
- **14.[リーフ/パスで静的にリンク(Statically Link with Leaves/Paths)]** チェックボックスをオンにして、 [次へ(Next)] をクリックします。
- **15.[物理ドメイン (Physical Domain)**] フィールドのドロップダウンリストから、作成した物理ドメイン (この例では **HCI_phys**)を選択します。
- 16.[パス (Paths)] フィールドで、[+] をクリックしてパスを選択し、Port Encap を構成します(この例では、Mgmt の Pod-1/Node-101/eth1/11 および vlan-1600)。ネイティブ VLAN(タグなし)が管理ネットワークに使用されている場合は、[モード(Mode)] フィールドで [トランク(ネイティブ)(Trunk (Native))]を選択します。
- **17.**クラスタの他の Azure Stack HCI サーバ インターフェイスに対して手順 16 を繰り返します。(この例 では、 Node-101/eth1/11-12 および Node-102/eth1/11-12 、 vlan-1600 for Mgmt)。

ストレージ EPG の構成

Azure Stack HCI ストレージネットワーキングを構成するには、次の手順を実行します。

- 1. APIC の上部ナビゲーション メニューから、【テナント(Tenants)】、【共通(common)】の順に選択 します(または、ストレージ EPG を構成する既存のテナントを選択します)。
- 左側のナビゲーション ウィンドウで、[ネットワーク (Networking)]>[ブリッジドメイン (Bridge Domains)]を選択します。
- 3. 右クリックして、【ブリッジドメインの作成(Create Bridge Domain)】を選択します。
- 4. [名前(Name)] フィールドで、名前(Storage-A など)を指定し、VRF 名(この例では common-VRF)を選択します。
- 5. [転送 (Forwarding)] ドロップダウン リストから [カスタム (Custom)] を選択します。
- 6. [L2 未知のユニキャスト(L2 Unknown Unicast)] ドロップダウン リストで、[フラッド(Flood)] を選択します。
- 7. [次へ (Next)]をクリックします。
- 8. [ユニキャストルーティング (Unicast Routing)] チェックボックスをオフにしてユニキャストルーティングを無効化にし、[次へ (Next)] をクリックします。

- **9.** [完了(Finish)] をクリックします。
- 10.EPG を作成するには、左側のナビゲーション ウィンドウから **[アプリケーションプロファイル** (Application Profiles)]を展開し、既存のアプリケーション プロファイルを選択します(または新 しいアプリケーション プロファイルを作成します)。
- 11.[アプリケーション EPG (Application EPGs)]を右クリックし、[アプリケーション EPG の作成 (Create Application EPG)]を選択します。
- 12.[名前 (Name)]フィールドで、名前を指定します(例: Storage-A)。
- **13.[カスタム QoS(Custom QoS)]** フィールドのドロップダウン リストから、作成したカスタム QoS ポリシー(この例では、 **Storage_and_Cluster**)を選択します。
- **14.[ブリッジ ドメイン (Bridge Domain)]**フィールドのドロップダウン リストから、作成した BD (この 例では **Storage-A**)を選択します。
- 15.[リーフ/パスで静的にリンク(Statically Link with Leaves/Paths)] チェックボックスをオンにして、 [次へ (Next)] をクリックします。

Create Application E	PG
STEP 1 > Identity	1. Identity 2. Leaves/Paths
Name:	Storage-A
Alias:	
Description:	optional
Annotations:	Click to add a new annotation
Contract Exception Tag:	
QoS class:	Level3 (Default)
Custom QoS:	Storage_and_Cluster 🗸 🕼
Data-Plane Policer:	select a value
Intra EPG Isolation:	Enforced Unenforced
Preferred Group Member:	Exclude Include
Flood in Encapsulation:	Disabled Enabled
Bridge Domain:	Storage-A 🗸 🔀
Monitoring Policy:	select a value
FHS Trust Control Policy:	select a value
EPG Admin State:	Admin Up Admin Shut
Associate to VM Domain Profiles:	
Statically Link with Leaves/Paths:	
EPG Contract Master:	1
	Application EPGs
	Previous Cancel Next

- 16.[物理ドメイン (Physical Domain)]フィールドのドロップダウンリストから、作成した物理ドメイン (この例では HCl_phys)を選択します。
- **17.[パス (Paths)]** フィールドで、[+] をクリックしてパスを選択し、Port Encap を構成します(この例 では、 **Storage-A の Pod-1/Node-101/eth1/11** および **vlan-107**)。
- **18**.クラスタの他の Azure Stack HCI サーバー(この例では、 ストレージ A の Pod-1/Node-102/eth1/11 および vlan-107)に対して手順 17 を繰り返します。

19.2番目の ストレージ EPG (たとえば、作成したカスタム QoS Storage_and_Cluster、 物理ドメイン HCl_phys および パス Pod-1/Node-101/eth1/12 および Pod-1/ Node-102/eth1/12 (vlan-207) を使用したストレージ-B および EPG ストレージ-B)。

コントラクトの構成

コントラストを構成する手順は、次のとおりです。

- 1. APIC の上部ナビゲーションメニューから、【テナント(Tenants)】を選択し、プロバイダーEPG が存 在するテナントを選択します。たとえば、Web EPG とアプリケーション EPG 間のコントラクトには テナント HCI_tenant1 を選択します。
- 2. 左側のナビゲーション ウィンドウで、展開して [コントラクト (Contracts)] を選択します。
- 3. 右クリックして、[コントラクトの作成(Create Contract)]を選択します。
- 4. [名前 (Name)] フィールドで、名前 (Web-to-App など) を指定します。
- 5. [範囲(Scope)] タブで、ドロップダウン リストから [範囲(Scope)] を選択します。テナント間コ ントラクトの場合は、[グローバル(Global)] を選択します)。
- 6. 【情報カテゴリ(Subjects)】 フィールドで、+ をクリックし、コントラクトの情報カテゴリ名を指定 します。(たとえば、Subject1と入力します。)
- 7. [フィルタ(Filter)] フィールドで、[+] をクリックし、既存のフィルタ処理を選択します(またはドロ ップダウン リストから新しいフィルタ処理を作成します)。
- 8. 別のフィルタ処理がある場合は、【更新(Update)】をクリックし、手順7を繰り返します。
- 9. [OK] をクリックします。

ADIC (172 21194	Create Contrac	t	\otimes
CISCO APIC (172.31.104	Name:	Web-to-App	
System Tenants Eabric	Alias:		
System renance rabite	Scope:	VRF	\checkmark
ALL TENANTS Add Tenant Tenant	QoS Class:	Unspecified	~
HCI tenant1	Target DSCP:	Unspecified	~
	Description:	optional	
Ouick Start			
✓	Annotations:	Click to add a new annotation	
> E Application Profiles	Subjects:		
> En Networking		Name Description	
		Subject1	
Create Contract			
Standarc Create Taboo Contract			
> 📩 Taboos			
> 🛅 Imported Create Filter			
			Cancel Submit

10.[送信 (Submit)] をクリックします。

11.別のコントラクトがある場合は、ステップ1~10を繰り返します。

コントラクトへのコンシューマ/プロバイダー EPG の追加

コントラクトに EPG を追加するには、次の手順に従います。

- 1. APIC の上部ナビゲーション メニューから、[テナント(Tenants)]を選択し、EPG が存在するテナントを選択します。たとえば、Web EPG とアプリケーション EPG 間のコントラクトにはテナント HCI_tenant1 を選択します。
- 左側のナビゲーション ウィンドウで、[アプリケーション プロファイル (Application Profiles)]を展開し、EPG が常駐する[アプリケーション プロファイル (Application Profile)]を展開します。
- 3. [アプリケーション EPG (Application EPGs)]を展開し、EPG を展開します。 (Web など)。
- (Contracts)]を右クリックし、EPG がプロバイダーであるかコンシューマであるかに応じて、[提供されたコントラクトの追加(Add Provided Contract)]または[消費されるコントラクトの追加(Add Consumed Contract)]を選択します。(この例では、Web EPG はコントラクトのコンシューマです)。
- 5. [コントラクト (Contract)] フィールドのドロップダウンリストから、作成したコントラクト (この例 では [Web-to-App]) を選択します。

APIC (172.31.184.201)	Add Consumed Contract 🛛 😵
System Tenants Fabric Virtual Networki ALL TENANTS Add Tenant Tenant Search: name or des	Contract: Web-to-App V C Type at least 4 characters to select contracts QoS: Unspecified V
HCI_tenant1 (È) (Cont > O Quick Start ✓ 開 HCI_tenant1	Contract Label:
 ✓ ➡ Application Profiles ✓ ➡ Application EPGs > ♣ App 	e Cancel Submit
 See Web Domains (VMs and Bare-Metals) EPG Members Static Ports 	
Static Leans Static Leans Fibre Channel (Paths) Contracts Static Endp Add Taboo Contract Subnets Add Provided Contract	
L4-L7 Virtu: Add Consumed Contract L4-L7 IP Ad Add Consumed Contract Interface L9-L7 IP Ad Add Consumed Contract Interface L9-L7 Up Ad Add Intra-EPG Contract D Endnoint Security Groups	

- 6. [送信 (Submit)]をクリックします。
- 7. 他の EPG に対してステップ 1~6 を繰り返します。

Azure Stack HCI 用の Cisco NX-OS ベースのファブリック構成

このセクションでは、Cisco NDFC によって管理される VXLAN ファブリックがお客様の環境にすでに存在する ことを前提として、 Azure Stack HCI サーバー用の Cisco NX-OS ベースの VXLAN ファブリックを設定する方 法について説明します。このドキュメントでは、最初の VXLAN ファブリックを使用するために必要な設定につ いては説明しません。IGP ベースのアンダーレイと iBGP ベースのオーバーレイ (BGP EVPN) を構築するには、 Data CenterVXLAN EVPN ファブリックテンプレートを使用する必要があります。 このドキュメントでは、NX-OS ベースの従来の従来の LAN ファブリックについては説明しませんが、従来の クラシックな LAN ファブリックでも同じワークフローに従うことができます。NDFC には、NX-OS ベースの 従来の従来の LAN ファブリックを構築するための Enhanced Classic LAN (ECL) ファブリック テンプレー トが付属しています。

全体的な構成は、次のように分類できます。

- QoS の設定
- LLDP 構成
- Azure Stack HCI サーバーに接続されたリーフ インターフェイスの構成
- ネットワークと VRF の構成
- 外部接続の構成

QoS の設定

AWS パスの拡充 Atack HCI ホストの QoS 要件は、 ACI ベースのファブリックと NX-OS ベースのファブリッ クの両方で同じです。詳細については、 <u>表 7 Azure Stack HCI ホスト ネットワーク QoS の推奨事項</u>を参照し てください。

次に示すように、 Azure Stack HCI サーバーに接続されているスイッチにのみ、必要な QoS 構成が必要です。

Azure Stack HCI サーバーによって設定された CoS マーキングに基づいて、入力インターフェイスで RDMA お よびクラスタ通信トラフィックを分類するクラスマップを作成します。

class-map type qos match-all RDMA
 match cos 4
class-map type qos match-all CLUSTER-COMM
 match cos 5

トラフィックが(サーバーによって設定された **CoS** 値に基づいて)分類されたら、それぞれの **QoS** グループ にマッピングする必要があります。

policy-map type qos AzS_HCI_QoS class RDMA set qos-group 4 class CLUSTER-COMM set qos-group 5

ネットワーク QoS クラスを定義し、 QoS グループに基づいてトラフィックを照合します。

class-map type network-qos RDMA_CL_Map_NetQos
 match qos-group 4
 class-map type network-qos Cluster-Comm_CL_Map_NetQos
 match qos-group 5

RDMA トラフィックの PFC を有効にし、ジャンボ MTU を設定するネットワーク QoS ポリシーを作成します。

policy-map type network-qos QOS_NETWORK
 class type network-qos RDMA_CL_Map_NetQos
 pause pfc-cos 4
 mtu 9216
 class type network-qos Cluster-Comm_CL_Map_NetQos
 mtu 9216
 class type network-qos class-default
 mtu 9216

RDMA トラフィックの ECN と他のクラスの帯域幅割り当てを有効にするためのキューイングポリシーの構成:

```
policy-map type queuing QOS EGRESS PORT
  class type queuing c-out-8g-g-default
    bandwidth remaining percent 49
  class type queuing c-out-8q-q1
   bandwidth remaining percent 0
  class type queuing c-out-8q-q2
   bandwidth remaining percent 0
  class type queuing c-out-8q-q3
   bandwidth remaining percent 0
  class type queuing c-out-8q-q4
    bandwidth remaining percent 50
    random-detect minimum-threshold 300 kbytes maximum-threshold 300 kbytes drop-probability 100
weight 0 ecn
  class type queuing c-out-8q-q5
   bandwidth percent 1
  class type queuing c-out-8q-q6
   bandwidth remaining percent 0
  class type queuing c-out-8q-q7
   bandwidth remaining percent 0
```

キューイングおよびネットワーク QoS ポリシーをシステム QoS に適用します。

system qos service-policy type queuing output QOS_EGRESS_PORT service-policy type network-qos QOS_NETWORK 上記の QoS 設定は、 Azure Stack HCI サーバーの接続に使用されるリーフ スイッチでのみ必要です。同じク ラスタのすべての Azure Stack HCI サーバーが同じリーフの vPC ペアに接続されている限り、ファブリック全 体の QoS 構成の要件はありません。

NDFC を使用して QoS ポリシーを設定する手順は次のとおりです。

ステップ1: 両方のリーフ スイッチ (Azure Stack HCI に接続)を選択し、 switch_freefrom ポリシーテン プレートを使用してグループ ポリシーを作成し、すべての QoS 関連の構成(上記)を [スイッチ フリーフォー ム構成 (Switch Freeform Config)] ボックスに貼り付けます。

ポリシーを作成するには、[ファブリックの **詳細ビュー(Fabric Details View)] > [ポリシー(Policies)]**タ ブに移動します。

reate Policy		? – \times
Switch List: icenf1 icenf2 > Priority*		
500 (2) 1-2000 Descenting		
Unstructure OoS configuration for Azure HCI Cluster Select Template* switch_freeform > Group		
Switch Freeform Config* class-map type stylence-gos RDMA_CL_Map_MetQos class-map type stylence-comm_CL_Map_MetQos match og:spop 4 class-map type stylence-comm_CL_Map_MetQos match og:spop 4 class-map type stylence-come_come_come_come_come_come_come_come_	Additional switch config. Notel Al configs should shirtly match there and angut, with regret to care, leading access and analysis, why manufactors all yield unspected affs using deploy.	
	(Close Previous Save

[保存 (Save)]をクリックすると、**[ポリシー (Policy)**]タブに戻ります。[ポリシー (Policy)]タブ ページ から、作成したポリシーを選択し、**[アクション (Actions)]**ドロップダウンから**[プッシュ (Push)]**ボタン をクリックして、生成された設定をリーフ スイッチに展開するします。

ステップ2: リーフスイッチのピアリンク(Azure HCI に接続)に QoS ポリシーを適用します。

これは、ピアリンクを通過する可能性のあるすべてのトラフィックに QoS を適用するために必要です。

ファブリックの[概要(Overview)]>[インターフェイス(Interfaces)]タブで、リーフ1とリーフ2のピア リンク ポート チャネル インターフェイスを選択し、[アクション(Actions)]ドロップダウンから[編集 (Edit)]をクリックします。

Fab	ic Ov	verview - Azur	e-HCI													Actions	• 🔿	?	_	\times
Over	view	Switches	Links	Interfaces	Interface Group	s Policie:	s Networks	VRFs	Services	Event Analytics	History	Resources	Virtual	Infrastructure						
	nterfac	ce contains 500 ;	×													Edit	Clear All) [Actions	^
	D	evice Name		Interface		Admin Status	Oper. Status	Reason		Policies		Overlay Ne	twork	Sync Status	Interface Group	Por Cha	Create Ir Create S	iterfai ubinte	erface	
	- 1	eaf-1		Port-chann	el500	↑ Up	↑ Up	ok		int_vpc_peer_link_p	D	NA		In-Sync			Edit			
	2 L	eaf-2		Port-chann	el500	↑ Vp	↑ Up	ok		int_vpc_peer_link_p	D	NA		In-Sync			Normaliz Multi-Att	e ach		

Edit interface(s)		
1 of 2 Selected Interface(s) : Interface Leaf-1 : Port-channel500 Policy* Int_ypc_peer_link_po > Policy Options		
VPC Peer-Link Port-Channel Member Interfaces Ethernet1/39,Ethernet1/40	A lot of member interfaces [in.g. e10, e110, e110/-9]	
vPC Peer-link Trunk Allowed Vlans Select an Option	vPC Peer-Ink Allowed Vian list (empty-all or none)	
Native Vlan	VLAN ID to set as the interface native vian	
Port Channel Description	Add description to the port-channel (Max Size 254)	
Members Description	Add description, if members don't have any (same for all members, Max Size 254)	
Port Channel Admin State*	Admin state of the port-channel	
Freeform Config service-policy type gos input <u>AxS_HCI_</u> QoS		
		Additional CLI for the interface

Leaf-1の[保存 (Save)] ボタンをクリックします。

[次へ(Next)] ボタンをクリックし、リーフ 2 の vPC ピアリンクに対して同じ手順を繰り返します。 保留中の設定を確認し、 展開するします。



ステップ3: AWS パスの拡充 HCI への接続に使用されるリーフスイッチインターフェイスに QoS ポリシーを 適用します。

Cisco NDFC では、インターフェイス グループを使用してインターフェイスをグループ化できます。同一の設定を必要とするすべてのインターフェイスは、インターフェイス グループを使用してグループ化でき、必要なすべての設定はインターフェイス グループにのみ適用されます。

Azure Stack HCI サーバに接続するリーフ1インターフェイスとリーフ2インターフェイスには同じQoS設定が必要ですが、RDMAトラフィック用に異なるVLAN(ストレージAのリーフ1とストレージBのリーフ2)を伝送するため、2つの個別のインターフェイスグループは必須です。

Fa	bric (Overview - Azure-HCI										Actions	• 0 (? —	\times
Ov	ervie	w Switches Links	Interfaces	Interface Groups	Policies	Networks	VRFs Servi	es Event Analytics Histor	ry Resources Virtua	I Infrastructure					
	Desc	ription contains AzS \times										Edit	Clear All	Actions	^
		Device Name	Interface	Ac	dmin tatus	Oper. Status	Reason	Policies	Overlay Network	Sync Status	Interface Group	Port Channel ID	Create Inte	interface	
		Leaf-1	Ethernet1/11	1	N Up	🕹 Down	XCVR not inserted	int_trunk_host	NA	In-Sync			Edit		
	~	Leaf-1	Ethernet1/12	1	► Up	U Down	XCVR not inserted	int_trunk_host	NA	In-Sync			Normalize Multi-Attac	:h	
		Leaf-2	Ethernet1/11	1	► Up	U Down	XCVR not inserted	int_trunk_host	NA	In-Sync			Multi-Deta	ch	
		Leaf-2	Ethernet1/12	1	▶ Up	🔶 Down	XCVR not inserted	int_trunk_host	NA	In-Sync			Deploy		
													No Shutdo	wn	
										Ad	id to Interface Group		More		>
										Re	move from interface G	iroup			_

ポート Eth1/11-12 は、次の設定で Leaf-1_Azure_HCI_Server_ports インターフェイス グループに追加されます。

- インターフェイス タイプの設定:イーサネット
- $\# U \gg -:$ int_ethernet_trunk_host
- BPDU ガードの有効化: True
- ポートタイプ高速の有効化:はい
- MTU Jumbo (9216 バイト)
- ネイティブ VLAN: Mgmt VLAN に設定可能(オプション)
- Freefrom Config: QoS およびキューイング ポリシーを適用する service-policy CLI コマンドと、イン ターフェイスへのポリシー フロー制御を有効にする CLI コマンドを提供します。

ate interface Group interior Name* Kare-HOI interior Nome* Kare-HOI interior Nome* interio		
Variance Var	ate Interface Group	
Static Name* Static Name* Lef-1_Abura_HOL_Server.ports Prof - Channel (PC) (PC) (AV) Prof - Channel (PC) (PC) (AV) Port - Channel (PC) (PC) (PC) Port - Channel (PC) (PC) (PC) (PC) (PC) (PC) (PC) (PC)		
table Channe* tarter HOI ter face Viges ter face Viges ter face Viges ter face Viges ter face Viges ter face Viges ter f		
and and were Hod Starse Hod of the part of	Jahrie Namat	
Autor Hui And Procession Names Left-LAzure, HOL, Server, ports Port-Channel OVC NY Port Port-Channel VC NY Port Port Port-Channel VC NY Port Port Port-Channel VC NY Port	abric Name	
Indiration Stream Indiration Stream <td>core-nor</td> <td></td>	core-nor	
Laf-Journ. HCl. Server.ports Internet Port-Channel VPC ANY Port-Channel VPC ANY Port-Channel VPC ANY <td>nterface Group Name*</td> <td></td>	nterface Group Name*	
Port-Channel VPC Norder Port-Channel VPC Port-Channel Port-Channel </td <td>Leaf-1_Azure_HCI_Server_ports</td> <td></td>	Leaf-1_Azure_HCI_Server_ports	
Port-Channel VPC ANV Port-Channel VPC ANV Policy Policy <td>nterface Type*</td> <td></td>	nterface Type*	
bolicy rt_shared_trunk_host ; bolicy rt_shared_trunk_host ; bolicy Options	Ethernet Port-Channel vPC ANY	
bildy mt_bland_trunk_host > Protect Protect Enable BPDU Guard* Ture Defer Four Ports* Shared granting-free toptoguest tree: watched twentings* Fenable RPDU Type Fest* Fenable RPDT Fenable RPDT Fenable RPDT Fenable RPDT Fenable RPDT Fenat Fenable RPDT Syme Rest Fenable RPDT Fenat Fenable RPDT Syme Rest Fenable RPDT Fenable RPDT Syme Rest Fenable RPDT Fenable RPDT Syme Rest Fenable RPDT Fenat Fenable RPDT Syme Rest Fenable RPDT Fenat Fenable RPDT Syme Rest Fenable RPDT Fenable RPD		
Construction Participated structure, books Participated structure, books Construction Construction <td< td=""><td>Indian</td><td></td></td<>	Indian	
Policy Options Enable DPDI Guard* true true true Deable spacetay-tree toptagued tree: teaster, teast theat in to default setting* Deable spacetay-tree toptagued tree: teaster, teast theat in to default setting* Deable spacetay-tree toptagued tree: teaster, teast theat in to default setting* Deable spacetay-tree toptagued tree: teaster, teast theat in to default setting* Deable spacetay-tree toptagued tree: teaster, teast theat in to default setting* Deable spacetay-tree toptagued tree: teaster, teast theat in to default setting* Deable spacetay-tree toptagued tree: teaster, teast theat in to default setting* Deable spacetay-tree toptagued tree: teaster, teast theat in to default setting* Deable spacetay-tree toptagued tree: teaster, teast theat in the default setting* Points Nuto Nuto NECOTIATE* on Native Van Inable VAN Native Van Inable VAN tor tere teather Resters, configer the interface to a VPC option port to be segued at by the secontary poer in VPC talkes Freeform Config Instruction Topic type tope type toptage type teasts type toptage type tages t	nt shared truck best N	
Parliery Options Enable BPOU Guard* Tue To Par Ports* Second graph for tex ports Enable BPOU Guard* In Enable BPOU Guard* Tue In Enable BPOU Type Fast* Second graph for tex ports Enable BPOUT Type Fast* Restor graph for tex ports Second graph for tex ports Auto Number Options Multiper for tex ports Second graph for tex ports Auto Number Options Multiper for tex ports Second graph for tex ports Second graph for tex ports Second graph for tex ports Auto Number Options Auto tex its second for speed Auto Nums* none Native Vian Second graph for tex ports Second graph for		
Enable BPDU Guard* Index spendsy-dex tpalaguant tract water, based that is, not feture to befault wetting* Ide for Fax Ports* Stered group for fax ports Enable Port Type Fast* Ration spanding-rise optig port betwee Ide for Fax Ports* Ration spanding-rise optig port betwee Impo MTU* Jumbo MTU trans instructor Speeps* Auto Auto Auto Biguitier node for speed Turuk Allowed Vlans* Auto Biguitier node for speed Native Vlan Set sative VLAN to the meritance Enable VC Orphan Port Set sative VLAN to the meritance Freeform Config Iteration to a set of option port to be supported by the secondary poer in vPC takens	Policy Options	
Enable EPDU Guard* Instead grant price to plaquet it trees wately; take of the alter wately; it was of water it to default wettage? Id For Fax Ports* Second grant for for poros Enable Port Type Fast* Reade grant for for poros MUT* Muther the interface Jumbo Muther the interface SPEED* Auto NEOOTUATE* on Auto Register mode for speed Turk Allowed Vlans* Auto Neof values (bote interface) Native Vlan Section grant for the the interface Enable VPC Orphan Port Section grant for the interface Freeform Config Hersteric os a vPC orphan port is be segned by the secondary poer in VPC failures Freeform Config Hersteric os a vPC orphan port is be segned ab y the secondary poer in VPC failures		
Enable DPDI Guard* Deale spanning-tree backguard tree: based thatder, no default witting* Ideale spanning-tree backguard tree: based thatder, no default witting* Service grapping for the pens Enable Port Type Fast* Enable open to the value MTU* Faster spanning-race dogs per to the value MTU* MTU* Jumbo MTU to the interface SPEED* Auto To NEGOTIATE* on Auto Reguiteer node for speed Trank Allowed Vlans* Auto Reguiteer node for speed Native Vlan sin subset values: bone!, wit, or vian trages ise: 1-200,500-2000,3000 Native Vlan sin subset values: bone!, wit, or vian trages ise: 1-200,500-2000,3000 Native Vlan sin subset values: bone!, wit, or vian trages ise: 1-200,500-2000,3000 Native Vlan sin subset values: bone!, wit, or vian trages ise: 1-200,500-2000,3000 Native Vlan sin subset values: bone!, wit, or vian trages ise: 1-200,500-2000,3000 Native Vlan sin subset values: bone!, wit, or vian trages ise: 1-200,500-2000,3000 Freeform Config resteeds, configure the interface as a with orghan port to be supported by the secondary poer in wPC failures Freeform Config resteeds, configure the interface as a with orghan port to be suppended by the seco		
It rue Deside sparstig-stee topliques to true to the data settings' Is for Face Ports* Second group for fee ports Enable Port Type Fact* Raster group for fee ports Finable Port Type Fact* Raster group for fee ports Finable Port Type Fact* Raster group for fee ports Finable Port Type Fact* Raster group for fee ports Finable Port Type Fact* Raster group for fee ports Jumbo Mill the rue interface Sprepo* Interface Speed Auto Interface Speed Auto Auto Negotive mode for speed Tunk Allowed Vlans* Auto Negotive mode for speed Native Vlan Set estate Quark for the interface Enable VIC Orphan Port Set estate Quark for the interface Freeform Config Restee quark to the interface set VIC Orphan port to be supported by the secondary poer in VIC Salares Freeform Config Restee quark to the interface set VIC Orphan port to be supported by the secondary poer in VIC Salares Freeform Config Restee quark to the interface set VIC Orphan port to be supported by the secondary poer in VIC Salares	Enable BPDU Guard*	
In De for Fas Ports* stever gresp for fee pers Enable Port Type Fast* Ration reparries-race orige port tetrever NTU* Imbo Mill de rise tetreface Imbo Mill de rise tetreface SPEED* Interdoce Spored Auto Interdoce Spored Auto Interdoce Spored Auto Auto Registriker mode for speed Trunk Allowed Vlans* Allowed values: hone, 'Mill or the interface Trunk Allowed Vlans* Allowed values: hone, 'Mill or the interface Enable v/PC Orphan Port ist autow VLAK for the interface Freeform Config Istebed, configure the interface as a v/O orphan port to be supported by the secondary per in v/O talues	true ~	Enable spanning-tree bpduguant true: verable) takeo bisable, noo'return to default settings'
Image: sevent group for fee ports Enable Port Type Fast* MU* Immediate Port Type Fast* Mute Enable Port Type Fast* Mute Immediate Port Type Fast*	IG for Fex Ports*	
Enable Pert Type Fast* Ratia sparsing-near sign pert ketware MTU* MTU* Jumbo MTU the the interfaces SPEED* Interfaces Speed AUTO NEGOTIATE* Auto Registries mode for speed Trunk Allowed Vlans* Auto Registries mode for speed Native Vlan Sit states vLaN for rise metrices Enable VPC Orphan Port sit states vLaN for the metrices Freeform Config restates configer the interface as a VPC option port to be segmended by the secontary peer in VPC failures		Shared group for fee ports
Impose Extent repartings - tase adapt part televiser NTU* Impose Jumbo Mitu ter me interface SPEED* Interface Speed Auto interface Speed Auto Auto Hegistice mode for speed Trunk Allowed Vlans* Auto Hegistice mode for speed Trunk Allowed Vlans* Allowed values: fored; wit, or view meganise: 1-200,000-2000,30000 Native Vlan Set astive VLAN for the interface Enable VPC Orphan Port Interface as a VPC option port to be segrended by the secondary peer in VPC Salues Freeform Config Interface as a VPC option port to be segrended by the secondary peer in VPC Salues	Enable Port Type Fast*	
MTU* MTU for the interfaces SPEED* Interfaces Speed Auto Interfaces Speed Auto Interfaces Speed Auto Auto Registrate mode for speed Turuk Allowed Vlans* Abseed values: hone/, sit, or kin mays sec. 1200,000-2000,3000 Native Vlan Set astitue VLAN for the Interface Enable VPC Orphan Port Interfaces as VPC orphan port is be segnerated by the secondary peer in VPC takenes Freedom Config Interfaces as VPC orphan port is be segnerated by the secondary peer in VPC takenes		Enable spanning-tree edge part behavior
Jumbo MIU for the Hearface SPEED* Auto Auto isterbox Rpeed AUTO NEGOTIATE* auto Biguitalier node for speed Om Auto Biguitalier node for speed Trunk, Allowed Vlans* Aldowed values: hore/, Wi, or vian morest lex: 1-200,600-2000,30000 Native Vlan set astive VLAN for the Interface Enable VPC Orphan Port reasbed, configure the Interface as a VPC orphan port to be septended by the secondary peer in VPC failures Freeform Config priority-flow-control mode on service-pointy type oggs input Acts, <u>HIGL Qoos</u>	MTU•	
SPEED* Auto Prestors Speed Auto Prestors Speed Auto Prestors Speed Prestors Config	jumbo ~	MTU for the interface
SPEED* Interface Speed Auto Interface Speed AUTO NEGOTIATE* Auto Registuer mode for speed rnink Allowed Vlans* Auto Registuer mode for speed none Allowed values: 'hote', 'wit, or vian mages lex: 1-200.000-2000.30000 Native Vlan Sit solve VLAN for the Interface Enable VPC Orphan Port If enables, configure the Interface as a VPC orphan port to be segrended by the secondary peer in VPC fallares Freeform Config If enables, LEQL QOSS		
Auto Interfaces Speed AUTO NEGOTIATE* Auto Registities node for speed On Auto Registities node for speed Trunk Allowed Vlans* Auto Negotities node for speed Native Vlan Set native VLAN for the interface Enable VPC Orphan Port If enables, configure the interface as a VPC orphan port to be suspended by the secontary pear in VPC takens Freedrom Config If enables, contrigure the interface as a VPC orphan port to be suspended by the secontary pear in VPC takens	SPEED*	
AUTO NEGOTIATE*	Auto	Interface Speed
On Adds Registrike mode for speed Trunk Allowed Vlans* Innex none Allowed values: hore," will, or rien ranges let: 1-200.600-2000.30000 Native Vlan Set aslike VLAN her the Histrikos Enable VPC Orphan Port If enables, configere the interface as a VPC orphan port to be sessended by the secondary peer in VPC failures Freeform Config If enables, configere the interface	AUTO NEGOTIATE*	
Trunk Allowed Vlans* Allowed values: hote/, Wi, or van noges iec 1-200.000-2000.0000 Native Vlan Set sative VLAN for the interface Enable VPC Orphan Port If enables, configure the interface as a VPC option port to be suspended by the secondary peer in VPC Salues Freeform Config Interface as a VPC option port to be suspended by the secondary peer in VPC Salues	on v	Auto Negotiate mode for speed
Trunk Allowed Vilans* Allowed vilues: hore(; sif, or vian ranges lest 1-200.000-2000.0000) Native Vian Sit statue VLAN for the interface Enable VPC Orphan Port If enabled, configure the interface as a VPC orphan port to be sustained by the secondary peer in VPC failures Freeform Config priority-flow-control mode on service-policy type gas input A <u>255-HCI Qoo5</u>		
none Allowed values: hose," wit, or view interfaces Native Vian Set native VLAN for the interface Enable VPC Orphan Port If enabled, configure the interface as a VPC orphan port to be suspended by the secondary peer in VPC failures Freedom Config priority-flow-control mode on service-policy type gogs input A <u>ZS_HICL QoS</u>	Trunk Allowed Vlans*	
Native Vlan Set native VLAN for the Interface Enable VPC Orphan Port If enables, configure the Interface as a VPC orphan port to be septended by the secondary peer in VPC failures Freeform Config If enables, configure the Interface as a VPC orphan port to be septended by the secondary peer in VPC failures priority-flow-control mode on service-policy type gas input Arcs, HGL Qoos If enables are control mode on service-policy type gas input Arcs, HGL Qoos	none	Allowed values: 'hone', 'ail', or vian ranges (ex: 1-200,500-2000,3000)
Set subve VLAN for the Histhean Enable VPC Orphan Port If enables, configure the Histhean as a VPC orphan port to be suspended by the secondary peer in VPC failures Freeform Config priority-flow-control mode on service-policy type gags input Ags, <u>HIGL Qos</u>	Native Vlan	
Enable VPC Orphan Port It enables, configure the interface as a VPC orphan port to be segrended by the secondary peer in VPC failures Freeform Config priority-flow-control mode on service-policy type gas input A <u>25_HCL Qo5</u>		Set native VLAN for the Interface
Enable VPC Orphan Port Hendbed, configure the Interface as a VPC orphan port to be exadended by the secondary poer in VPC failures Freeform Config priority-flow-control mode on service-policy type gos input A <u>25, HGL Ros</u>	L	
If instance, configue the interface as a WC arginan port to be suspended by the secondary pair in VPC failures Freedom Config priority-flow-control mode on service-policy type gas input A <u>ZS_HEL_QoS</u>	Enable vPC Orphan Port	
Freeform Config priority-flow-control mode on service-policy type ggs input Az5_HGL QoS		It enabled, contrigure the interface as a VPC orphan port to be suspended by the secondary peer in VPC failures
priority-flow-control mode on service-policy type gos input A <u>zS_HCL RoS</u>	Freeform Config	
service-policy type gos input AXS_HCL_QoS	priority-flow-control mode on	
service-policy type queuing output OOS EGRESS PORT	service-policy type gos input AZS_HCI_QoS service-policy type queuing output QOS_FORESS_PORT	

上記の手順を繰り返して、Leaf-2 ポート Eth1/11-12 を Leaf-2_Azure_HCI_Server_ports インターフェイス グループに追加します。

F	abric Overview - Azure-HCI											Actio	ins 🔪 🔿 🧍	? — ×
0	verview Switches Links	Interfaces Interface G	roups Polici	es Network	s VRFs Service	s Event Analytics History	Resources Virtua	I Infrastructure						
ſ	Description contains AzS \times											E	dit Clear All	Actions v
	Device Name	Interface	Admin Status	Oper. Status	Reason	Policies	Overlay Network	Sync Status	Interface Group	Port Channel ID	vPC ld	Speed	мти	Mode
lſ	Leaf-1	Ethernet1/11	↑ Up	🕹 Down	XCVR not inserted	int_shared_trunk_host	NA	In-Sync	Leaf-1_Azure_HCI_Server_ports			25Gb	9216	trunk
	Leaf-1	Ethernet1/12	↑ Up	U Down	XCVR not inserted	int_shared_trunk_host	NA	In-Sync	Leaf-1_Azure_HCI_Server_ports	J		25Gb	9216	trunk
ſ	Leaf-2	Ethernet1/11	↑ Up	🕹 Down	XCVR not inserted	int_shared_trunk_host	NA	In-Sync	Leaf-2_Azure_HCI_Server_ports			25Gb	9216	trunk
	Leaf-2	Ethernet1/12	↑ Up	🕹 Down	XCVR not inserted	int_shared_trunk_host	NA	In-Sync	Leaf-2_Azure_HCI_Server_ports	J		25Gb	9216	trunk

これで、PFC が有効になり、リーフ1とリーフ2のそれぞれのインターフェイスに QoS およびキューイング ポリシーが適用されました。次のセクションでは、 Azure Stack HCI に必要なネットワーク(VLAN)を作成し ます。

LLDP の設定

Cisco NDFC は、VXLAN ファブリック内のすべてのデバイスで LLDP 機能を有効にし、すべてのデバイスのす べてのインターフェイスで LLDP を有効にします。ただし、LLDP は、従来の従来の LAN ファブリックの Cisco NDFC では有効になりません。従来の従来の LAN ファブリックの場合、LLDP をサポートするには、 _lldp ポリシー機能をリーフ スイッチに関連付ける必要があります。

Azure Stack HCI のネットワークの構成

Azure Stack HCI のネットワーク要件は次のとおりです。

- リーフにエニーキャストゲートウェイが設定された2つのレイヤ3ネットワーク
- ストレージ用の2つのレイヤ2ネットワーク(リーフごとに1つ)



図 23.

Azure Stack HCI 向け Cisco NX-OS ベースのネットワーク

VXLAN ファブリックでは、すべてのレイヤ3ネットワークを VRF にマッピングして、2 つのテナント間を分離する必要があります。テナントに関連するすべてのネットワークは、それぞれのテナント VRF にマッピング されます。レイヤ2ネットワークを VRF にマッピングする必要はありません。

VRF を作成するには、**[ファブリックの詳細表示(Fabric Details View)]**>**[VRF]**>**[アクション(Actions)]** に移動し、**[VRF の作成(Create VRF)]**を選択し、次のパラメータを指定します。

- VRF 名: Azure_Tenant_VRF_50000
- VRF 識別子: VRF の VNI を提供します。
- VLAN 識別子: VRF に VLAN を提供
- VRF VLAN 名: VLAN の名前を指定します(オプション)。

reate VRF	
VRF Name*	
Azure_Tenant_VRF_50000	
VRF ID*	
50000	
2000 Propose VLAN	
VRF Template*	
Default_VRF_Universal >	
,	
VRF Extension Template*	
Default VRF Extension Universal N	
General Parameters Advanced Route Target	
VRF VLAN Name	
Azure_Tenant_VRF_Vlan If > 32 chars, enable	e 'system vlan long-name' for i
VRF Interface Description	
VRF Description	

VRF が作成されると、ネットワークを作成できます。ネットワークを作成するには、[ファブリックの詳細ビュー (Fabric Details View)]>>[ネットワーク (ネットワーク)]>>[アクション (Actions)]を選択し、[ネットワークの作成 (Create Network)]を選択します。

次のパラメータを使用して、 AWS パスの拡充 HCI Stack リソースの管理に使用されるレイヤ 3 ネットワーク を作成しましょう。

- ネットワーク名: Azure_Mgmt_Network_30000
- VRF 名: Azure_Tenant_VRF_50000 を指定します
- ネットワーク 識別子: 30000
- VLAN 識別子 : 2300
- IPv4 ゲートウェイ/ネットマスク: 172.16.10.1/24
- VLAN 名: Azure_Mgmt Vlan
- L3 インターフェイスの MTU : 9216 バイト

eate Network	
Network Name*	
Azure_Mgmt_Network_30000	
Layer 2 Only	
VRE Name*	
Azure_Tenant_VRF_50000 X V Create	VRF
Network ID*	
30000	
VLAN ID	
2300 Propo	DSE VLAN
Network Templete	
Default Network Universal >	
Network Extension Template*	
Generate Multicast IP. Please click only to generate a New	Multicast Group address and override the default value!
, , , , , , , , , , , , , , , , , , , ,	
General Parameters Advanced	
IPv4 Gateway/NetMask	
172.16.10.1/24	example 192.0.2.724
172.16.10.1/24	example 192.0.2.7/24
I72.16.10.1/24	example 192.0.2.1/24 example 2001.db6=1/64.2001.db6=1/64
172.16.10.1/24	example 192.0.2.1/24 example 2001:db8:1/64.2001:db8:1/64
I72.16.10.1/24 IPv6 Gateway/Prefix List VLAN Name Azure_Mgmt_Vlan	example 192.0.2.3724 example 2001xb8=1/64,2001xb8=1/64 If > 32 chers, enable 'system vian long-name' for NX-OS, disable VTPv1 and VTPv2 or switch to VTPv2
I72.16.10.1/24 IPv6 Gateway/Prefix List VLAN Name Azure_Mgmt_Vlan	example 192.0.2.3/24 example 2001xdb8+1/84,2001xdb8+1/84 If > 32 chers, enable 'system vian long-name' for NX-OS, disable VTPv1 and VTPv2 or switch to VTPv2
172.16.10.1/24 IPv6 Gateway/Prefix List VLAN Name Azure_Mgmt_Vlan Interface Description	example 192.0.2.3/24 example 2001xdb8+1/84,2001xdb8+1/84 If > 32 chers, enable 'system vian long-name' for NX+OB, disable VTPv1 and VTPv2 or switch to VTPv2
172.16.10.1/24 IPv6 Gateway/Prefix List VLAN Name Azure_Mgmt_Vlan Interface Description	example 192.0.2.3/24 example 2001xdb8+1/64,2001xdb8+1/64 If > 32 chara, enable 'system vian long-name' for NK+OB, disable VTPv1 and VTPv2 or switch to VTPv2
172.16.10.1/24 IPv6 Gateway/Prefix List VLAN Name Azure_Mgmt_Vlan Interface Description MTU for L3 interface	example 192.0.2.3/24 example 2001.do8:1/84.2001.do8:1/84 If > 32 chars, enable 'system vian long-name' for NK-OS, disable VTPv1 and VTPv2 or switch to VTPv2

AWS パスの拡充 HCI スタック テナントに使用される 2 番目のレイヤ 3 ネットワークを作成しましょう。

- ネットワーク名: Tenant_Network_30001
- VRF 名: Azure_Tenant_VRF_50000
- ネットワーク識別子: 30001
- VLAN 識別子: 2301
- IPv4 ゲートウェイ/ネットマスク: 172.16.20.1/24
- VLAN 名: Tenant_Network_Vlan
- L3 インターフェイスの MTU : 9216 バイト

ate Network	
Network Name*	
Tenant_Network_30001	
Layer 2 Only	
/RF Name*	
Azure_Tenant_VRF_50000 X V	Create VRF
Network ID*	
30001	
VLAN ID	
2301	Propose VLAN
Matwork Extension Template*	
Cenerate Multicast IP Please click only to generat	te a New Multicast Group address and override the default value!
Default_Network_Extension_Universal > Generate Multicest IP Please click only to generate General Parameters Advanced	te a New Multicast Group address and override the default value!
Ceneral Parameters Advanced IPv4 Gateway/NetMask 172.16.20.1/24	te a New Multicast Group address and override the default value!
Ceneral Parameters Advanced Ceneral Parameters Advanced IPv4 Gateway/NetMask 172.16.20.1/24 IPv6 Gateway/Ref/	te a New Multicast Group address and override the default value!
Ceneral Parameters Advanced Pv4 Gateway/NetMask 172.16.20.1/24 IPv6 Gateway/Prefix List	example 2001:tb8:1/84,2001:db9:1V84
Ceneral Parameters Advanced General Parameters Advanced IPv4 Gateway/NetMask 172.16.20.1/24 IPv6 Gateway/Prefix List	example 192.0.2.1/24
Ceneral Parameters Advanced General Parameters Advanced IPv4 Gateway/NetMask 172.16.20.1/24 IPv6 Gateway/Prefix List VLAN Name Tanant. Network. Vian	te a New Multicast Group address and override the default value! example 192.0.2.1/24 example 2001:tb8:1/64,2001:db9::V64 If > 32 chars, enable 'system vian long-name' for NV-OS, disable VTPv1 and VTPv2 or switch to VTPv3 for IOS
Ceneral Parameters Advanced General Parameters Advanced IPv4 Gateway/NetMask 172.16.20.1/24 IPv6 Gateway/Prefix List VLAN Name Tenant_Network_Vlan	te a New Multicast Group address and override the default value! example 192.0.2.1/24 example 2001:db8::1/64,2001:db9::1/64 If > 32 chars, enable 'system vian long-name' for N0-05, disable VTPv1 and VTPv2 or switch to VTPv3 for IO5 /
Ceneral Parameters Advanced General Parameters Advanced IPv4 Gateway/NetMask I72.16.20.1/24 IPv6 Gateway/Prefix List VLAN Name Tenant_Network_Vlan Interface Description	te a New Multicast Group address and override the default value! esample 192.0.2.1/24 esample 2001:db8:1/64,2001:db9:1/64 If > 32 chars, enable "system vian long-name" for NK-OS, disable VTPv1 and VTPv2 or switch to VTPv3 for IOS 3
Ceneral Parameters General Parameters General Parameters Advanced IPv4 Gateway/NetMask I72.16.20.1/24 IPv6 Gateway/Prefix List VLAN Name Tenant_Network_Vlan Interface Description	te a New Multicast Group address and override the default value! esample 192.0.2.1/24 esample 2001:db8:1/64.2001:db9::V64 If > 32 chars, enable 'system vian long-name' for N0C-05, disable VTPv1 and VTPv2 or switch to VTPv3 for IO5 3
Cenerate Automatic Extension_Universal > Cenerate Multicest IP Please click only to generat Generate Multicest IP Please click only to generat Feneral Parameters Advanced IPv4 Gateway/NetMask 172.16.20.1/24 IPv6 Gateway/Prefix List VLAN Name Tenant_Network_Vlan Interface Description MTU for L3 Interface	te a New Multicast Group address and override the default value! esample 192.0.2.1/24 esample 2001:tb&::1/64.2001:db0::V64 if > 32 chars, enable 'system vian long-name' for N0COS, disable VTPv1 and VTPv2 or switch to VTPv3 for 105 V

次に、ストレージのレイヤ2ネットワークを作成します。L3ネットワークとは異なり、L2ネットワークには SVI がなく、VRF へのマッピングは必要ありません。L2ネットワークを作成するには、[レイヤ2のみ (Layer 2 Only)]チェックボックスをオンにします。

次のパラメータを使用して、ストレージAのL2ネットワークを作成します。

- ネットワーク名: Storage-A_30100
- ネットワーク識別子: 30100
- VLAN 識別子: 2400
- VLAN 名: Storage-A_Vlan

Network Name*			
Storage-A_Network_3010	00		
Layer 2 Only			
VRF Name*			
NA	\sim		
Network ID*			
30100	0		
VLAN ID			
2400	0	Propose VLA	и
			_
Network Template*			
Default Network Universal			
	1		
Network Extension Templa	te*		
Network Extension Templa	te*		
Network Extension Templat Default_Network_Extension Generate Multicast IP Plet	te* _Universal > ase click only to generat	e a New Multic	ast Group address and override the default value!
Network Extension Templat Default_Network_Extension Generate Multicast IP	te* _Universal > ase click only to generat	e a New Multic	ast Group address and override the default value!
Network Extension Templa Default_Network_Extension Generate Multicast IP Plea	te" _Universal > ase click only to generat	e a New Multic	ast Group address and override the default value!
Network Extension Templal Default_Network_Extension Generate Multicest IP Plea General Parameters	te* LUniversal > ase click only to generat	e a New Multic	ast Group address and override the default value!
Network Extension Templal Default_Network_Extension Generate Multicast IP Plea General Parameters A IPv4 Gatewav/NetMask	te" Universal > ase click only to generat	e a New Multic	ast Group address and override the default value!
Network Extension Templal Default_Network_Extension Generate Multicast IP Plea General Parameters A IPv4 Gateway/NetMask	te" _Universal > ase click only to generat	e a New Multic	ast Group address and override the default value!
Network Extension Templal Default_Network_Extension Generate Multicast IP Plet General Parameters IPv4 Gateway/NetMask	te" _Universal > ase click only to generat	e a New Multic	ast Group address and override the default value!
Network Extension Templal Default_Network_Extension Generate Multicast IP Plet General Parameters IPv4 Gateway/NetMask	te" _Universal > ase click only to generat	e a New Multic	ast Group address and override the default value!
Network Extension Templal Default_Network_Extension Generate Multicast IP Plex General Parameters IPv4 Gateway/NetMask IPv6 Gateway/Prefix List	te" _Universal > ase click only to generat	e a New Multic	ast Group address and override the default value! example 192.0.2.1/24 example 2001.ab8 :1(94,2001.ab8 :1(94
Network Extension Templal Default_Network_Extension Generate Multicast IP Plei General Parameters IPv4 Gateway/NetMask IPv6 Gateway/Prefix List	te" _Universal > ase click only to generat	e a New Multic	ast Group address and override the default value! example 192.0.2.1/24 example 2001.abd=1/64,2001.ab9=1/64
Network Extension Templal Default_Network_Extension Generate Multicast IP Plex General Parameters IPv4 Gateway/NetMask IPv6 Gateway/Prefix List VLAN Name	te" _Universal > ase click only to generat	e a New Multic	ast Group address and override the default value! example 192.0.2.1/24 example 2001.cb8=1/64,2001.cb8=1/64
Network Extension Templal Default_Network_Extension Generate Multicast IP Plex General Parameters IPv4 Gateway/NetMask IPv6 Gateway/Prefix List VLAN Name Storage-A_Vian	te" _Universal > ase click only to generat	e a New Multic	ast Group address and override the default value! example 192.0.2.1/24 example 2001.ab8 -1/84,2001.ab8 -1/84 If > 32 chars, enable 'system vian long-name' for NE-OS, disable VTPv1 and VTPv2 or switch to
Network Extension Templal Default_Network_Extension Generate Multicast IP Plex General Parameters IPv6 Gateway/NetMask IPv6 Gateway/Prefix List VLAN Name Storage-A_Vian Interface Description	te" _Universal > ase click only to generat	e a New Multic	ast Group address and override the default value! example 192.0.2.1/24 example 2001.std=tte4.2001.std=1194 If > 32 chars, enable "system vian long-name" for NIC-OS, disable VTPv1 and VTPv2 or switch to
Network Extension Templal Default_Network_Extension Generate Multilaast IP Plex General Parameters A IPv4 Gateway/NetMask IPv6 Gateway/Prefix List VLAN Name Storage-A_VIan Interface Description	te" _Universal > ase click only to generat	e a New Multic	ast Group address and override the default value! example 192.0.2.1/24 example 2001.cl/d::t/04.2001.cl/d=1/04 If > 32 chars, enable 'system vian long-neme' for NIC-OS, disable VTPv1 and VTPv2 or switch to
Network Extension Templal Default_Network_Extension Generate Multileast IP Plex Generate Multileast IP IPv4 Gateway/NetMask IPv6 Gateway/Prefix List VLAN Name Storage-A_Vlan Interface Description	te"Universal > ase click only to generat Advanced	e a New Multic	ast Group address and override the default value! example 192.0.2.1/24 example 2001 sb3::t/64,2001.sb9:1/64 If > 32 chars, enable system vian long-nemer for N2COS, disable VTPv1 and VTPv2 or switch to

次のパラメータを使用して、ストレージ BのL2 ネットワークを作成します。

- ネットワーク名: Storage-B_30101
- ネットワーク識別子: 30101
- VLAN 識別子 : 2401
- VLAN 名: Storage-B_Vlan

Network Name*			
Storage-B_Netwo	k_30101		
aver 2 Only			
VRF Name*			
NA	\sim		
Network ID*			
30101	0		
2401	0	Propose VLA	
Network Template*			
Default Notwork Lie			
oeradic_network_on	iversal >		
Vetwork Extension 1	iversal >		
Network Extension 7	iversal > iemplate*		
Network Extension T Default_Network_Ext	iversal > iemplate* tension_Universal > Please click only to genera	te a New Multic	ast Group address and override the default value!
Network Extension 1 Default_Network_Ext Generate Multicast II	iversal > iemplate* iension_Universal > Please click only to genera	te a New Multic	ast Group address and override the default value!
Network Extension 1 Default_Network_Ext Generate Multicest II	iversal > iemplate* tension_Universal > Please click only to genera	te a New Multic	ast Group address and override the default value!
Network Extension 1 Default_Network_Ext Generate Multicest II General Parameter	iversal > iemplate* tension_Universal > Please click only to genera ars Advanced	te a New Multic	ast Group address and override the default value!
Network Extension 1 Default_Network_Ext Generate Multicast II General Parameter IPv4 Gateway/Net	iversal > iemplate* tension_Universal > Please click only to genera arsAdvanced Mask	te a New Multic	ast Group address and override the default value!
Ceneral Network Extension 1 Default_Network_Ext Generato Multicast II General Parameter IPv4 Gateway/Net	iversal > iemplate* tension_Universal > Please click only to genera ars Advanced Mask	te a New Multic	example 192.0.2.1/24
Ceneral Cettersion 1 Default_Network_Ex Generate Multicest II General Parameter IPv4 Gateway/Net	iversal > iemplate* tension_Universal > Please click only to genera tension_Advanced Mask five Liet	te a New Multic	ast Group address and override the default value! example 192.0.2.1/24
General Parameter General Parameter IPv4 Gateway/Pre	iversal > iemplate* tension_Universal > Please click only to genera ers Advanced Mask fix List	te a New Multic	example 192.0.2.1/24
Ceneral Creterion 1 Default_Network_Ex Ceneral Multicast II General Parameter IPv4 Gateway/Net	iversal > iemplate* tension_Universal > Please click only to genera Pressectick only to genera Mask fix List	te a New Multic	ast Group address and override the default value! example 192.0.2.1/24 example 2001-eb8=1/64,2001.do9=1/64
Ceneral Central (Network Extension 1 Default_Network_Ex Ceneral Multicast I IPv4 Gateway/Net IPv6 Gateway/Pre	iversal > iemplate* tension_Universal > Please click only to genera tension_Advanced Mask fix List	te a New Multic	ast Group address and override the default value! example 192.0.2.1/24 example 2001.eb8=1/64,2001.do8=1/64
Ceneral Parameter Ceneral Parameter Ceneral Parameter IPv4 Gateway/Ner IPv6 Gateway/Pre VLAN Name Storage-B_Vlan	iversal > iemplate* tension_Universal > Please click only to genera tension_Advanced Mask fix List	te a New Multic	example 192.0.2.1/24 example 192.0.2.1/24 example 2001.dtB=1/64,2001.dt9=1/64 If > 32 chars, enable 'system vian long-name' for NK-OS, disable VTPv1 and VTPv2 or switch to 1
Ceneral Parameter Ceneral Parameter Ceneral Parameter IPv4 Gateway/Net IPv6 Gateway/Pre VLAN Name Storage-B_Vlan Interface Descript	iversal > iemplate* tension_Universal > Please click only to genera tension_Advanced Mask fix List ion	te a New Multic	example 192.0.2.1/24 example 192.0.2.1/24 example 2001.db8=1/64,2001.db9=1/64 If > 32 chars, enable 'system vian long-name' for NK-OS, disable VTPv1 and VTPv2 or switch to 1
Ceneral Cretwork Con Default_Network_Ex Ceneral Parameter IPv4 Gateway/Net IPv4 Gateway/Pre VLAN Name Storage-B_Vlan Interface Descript	iversal > iemplate* tension_Universal > Please click only to genera tension_Advanced Mask fix List ion	te a New Multic	example 192.0.2.1/24 example 192.0.2.1/24 example 2001.db8=1/64,2001.db9=1/64 If > 32 chars, enable 'system vian long-name' for NK-OS, disable VTPv1 and VTPv2 or switch to V
Ceneral Creterion 1 Default_Network_Ex Ceneral Paramete IPv4 Gateway/Net IPv4 Gateway/Net VLAN Name Storage-B_Vlan Interface Descript MTULfor_L3_interfi	iversal > iemplate* iemplate* iension_Universal > Please click only to genera iense Advanced Mask fix List ion	te a New Multic	example 192.0.2.1/24 example 2001.db8::1/64,2001.db9::1/64 #> 32 chars, enable 'system vian long-name' for NK-OS, disable VTPv1 and VTPv2 or switch to V

ファブリックの[ネットワーク (Networks)]タブからすべてのネットワークを確認できます。

Fabric	Overview - Azure-HCI						
Overvi	ew Switches Links Interfac	ces Interface Groups Policies	s Networks VRFs Se	ervices Event Analytics History	Resources Virtual Infrastructure		
R	Iter by attributes						
	Network Name	Network ID	÷ VRF Name	IPv4 Gateway/Prefix	IPv6 Gateway/Prefix	Network Status	VLAN ID
	Azure_Mgmt_Network_30000	30000	Azure_Tenant_VRF_50000	172.16.10.1/24		NA NA	2300
	Tenant_Network_30001	30001	Azure_Tenant_VRF_50000	172.16.20.1/24		NA	2301
	Storage-A_Network_30100	30100	NA			NA NA	2400
	Storage-B_Network_30101	30101	NA			NA	2401

次に、ネットワークをインターフェイスに接続し、接続するネットワークを選択して、【アクション

(Actions)]→[インターフェイス グループにアタッチ(Attach to Interface Group)] をクリックします。 Azure_Mgmt とテナント ネットワークを両方のリーフに接続していますが、ストレージ ネットワークはそれぞれのスイッチに接続しています。

c Overview - Azure-HCI						Actions - 🔿 ? -
iew Switches Links Interfaces InterfaceGroups Polic	ies Networks \	/RFs Services Event Anal	ytics History Resources Virtu	al Infrastructure		
Iter by attributes						Acti
Network Name	Network ID	VRF Name	IPv4 Gateway/Prefix IPv6 Gates	way/Prefix Network Status	VLAN ID	Interface Oroup
Azure_Mgmt_Network_30000	Network ID 30000	VRF Name Azure_Tenant_VRF_50000	IPv6 Gateway/Prefix IPv6 Gatew 172.16.10.0/24	way/Prefix Network Status	2300	Interface Oroup Leaf-1_Azure_HCI_Server_ports_Leaf-2_Azure_HCI_Server_ports
Network Name Azure_Mgmt_Network_30000 Tenant_Network_30001	Network ID 30000 30001	VRF Name Azure_Tenant_VRF_50000 Azure_Tenant_VRF_50000	IPv4 Gateway/Prefix IPv6 Gateway/Prefix 172:16:10:3/24 172:16:20:1/24	vay/Prefix Network Status	2300 2301	Interface Group Leaf-1_Azure_HCL_Server_ports_Leaf-2_Azure_HCL_Server_ports Leaf-1_Azure_HCL_Server_ports_Leaf-2_Azure_HCL_Server_ports
Network Name Azure_Mgmt_Network_30000 Tenant_Network_30001 Storage-A_Network_30100	Network ID 30000 30001 30100	VRF Name Azure_Tenant_VRF_50000 Azure_Tenant_VRF_50000 NA	IPv4 Gateway/Prefix IPv6 Gateway/ 172.16.10.1/24 172.16.20.1/24	way/Prefix Network Status	2300 2301 2400	Interface Group Leaf-LAzure_HOLServer.ports.Leaf-2_Azure_HOLServer.ports Leaf-LAzure_HOLServer.ports.Leaf-2_Azure_HOLServer.ports Leaf-LAzure_HOLServer.ports

すべてのネットワークが接続されたら、ネットワークを選択し、**[アクション(Actions)] > [NDFC の展開** (Deploy for NDFC)]をクリックして設定を生成し、デバイスにプッシュします。

Azure Stack HCI サーバーの外部接続の構築

VXLAN ファブリックの外部にあるネットワークは外部と呼ばれ、そのようなネットワークへの接続を提供する ために VRF_Lite (MPLS オプション A) が使用されます。Cisco NDFC は、VXLAN または従来の従来の LAN ファブリックから外部ネットワークへの接続を拡張するための完全な自動化をサポートします。

IPv4/IPv6 ハンドオフを実行する VXLAN デバイスはボーダーデバイスと呼ばれ、このロールは Cisco NDFC で もサポートされています。テナント VRF が境界デバイスに展開されると、外部ネットワークに向けてさらに拡 張できます。

VXLAN ファブリックの外部接続を設定するには、ファブリックテンプレートの[リソース(Resources)]タブで、次の NDFC 設定が必要です。

VRF Lite Deployment*	
Back2Back&ToExternal	VRF Lite Inter-Fabric Connection Deployment Options. If 'Back2Back&ToExternal' is selected, VRF Lite IFCs are auto created between border devices of two Easy Fabrics, and between border devices in Easy Fabric and edge routers in
	External Fabric. The IP address is taken from the 'VRF Lite Subnet IP Range' pool.
Auto Deploy for Peer	Whether to auto generate VRF LITE sub-interface and BGP peering configuration on managed neighbor devices. If set, auto created VRF Life IFC links with nave 'Auto Deploy for Peer' enabled.
Auto Deploy Default VRF	Whether to auto generate Default VRF interface and BGP peering configuration on VRF LITE IFC auto deployment. If set, auto created VRF Lite IFC links will have 'Auto Deploy Default VRF' enabled.
Auto Deploy Default VRF for Peer	Whether to auto generate Default VRF interface and BGP peering configuration on managed neighbor devices. If set, auto created VRF Lite IFC links will have 'Auto Deploy Default VRF for Peer' enabled.
Redistribute BGP Route-map Name	Route Map used to redistribute BGP routes to IGP in default vrf in auto created VRF Lite IFC links
VRF Lite Subnet IP Range*	Address range to assign P2P Interfabric Connections
VKF-Lite Subnet Mask*	(Mor.8, Max:31)

必要に応じて、VRF Lite IP サブネット範囲とサブネットマスク(必要な場合)を変更します。

開始する前に、境界デバイスに VRF が展開されていることを確認します。そうでない場合は、VRF を境界デバイスに接続します。

VRF_Lite 拡張機能を設定するには、必要な VRF を選択し、VXLAN ファブリックから VRF 詳細ビューに移動し ます。[VRF アタッチメント (VRF Attachments)] タブで、ボーダーデバイスを選択し、[アクション (Actions)] ドロップダウンから[編集(編集)] をクリックします。

F Overview - Azure_Tenant_VRF_50000								E	actions +	Refresh
erview VRF Attachments Networks										
Dise by smillenes										Autio
VRF Name VRF ID	VLAN ID	Switch	Statue	Attachment	Switch Role	Fabric Name	Loopback ID	Loopback IPV4 Address	Loopba	History
Azure_Tenant_VR 50000	2000	Leaf-2	DEPLOYED	Attached	leaf	Azure-HCI				Edit
Azure_Tenant_VR 50000	2000	Leaf-1	DEPLOYED	Attached	leaf	Azure-HCI				Preview
Azure_Tenant_VR 50000	2000	Leaf-5	DEPLOYED	Attached	border	Azure-HCI				Import
Azure_Tenant_VR 50000	2000	Leaf-6	O DEPLOYED	Attached	border	Azure-HCI				Export
										Quick Attach
										Quick Detac

各ボーダーデバイスについて、**[拡張(Extend)]**の下のドロップダウンから VRF_LITE を選択し、**[すべて添付(Attach-All)]**ボタンをクリックします。**[アクション(Action)]**の下にある**[終了(Exit)]**リンクをクリックすると、追加のパラメータを指定できます。

Edit VRF Attachment - Azure_Tenant_VRF_50000														? — ×
1 of 2 : Azure_Tenant_V	RF_50000 - Leaf-5(F	D027280T	'NL)											
1 of 2 : Azure_Tenanty LeadAgroCozzerta) Detain C Attach VLA# 2000 Extensi With JIKE CL Predom Curring Edit 3 All config activations and your Longstant Prid. Address Longstant Prid. Address	RF_50000 - Leaf-S(F	DO27280T	NL)											
Import EVPN Route Target														
Export EVPN Route Target														
Extension Filter by attributes													Attach-All Detach-All	
Action Attached	Source Type Switch	IF_NAME	Dest. Switch	Dest. Interface	DOT1Q_ID	IP_MASK	IP_TAG	NEIGHBO	NEIGHBO	IPV6_MA	IPVG_NEL_	мти	ENABLE_I AUTO_)	
Edit Attached	Leaf-5 VRF_LITE	Ethernet1/39	ToR	Ethernet1/37	2	10.33.0.2/30		10.33.0.1	65000			9216	false true	
														Cancel Save & Edit Next

同じ手順と追加のボーダーデバイスを繰り返し、【保存(Save)】をクリックします。

[VRF アタッチメント (VRF Attachment)]タブに戻り、設定をデバイスに展開するには、[アクション (Actions)](上部)ドロップダウンから[展開(Deploy)]をクリックします。

_										
ŀ	VRF Overview - Azure_Tenant_VRF_50000									cliere - Refresh — X
<	Overview VRF Attachments Networks									
	Filter by attributes									Actiens ~
L	VRF Name VRF ID	VLAN ID	Switch	Status	Allachment	Switch Role	Fabric Name	Loopback ID	Loopback IPV4 Address	Loopback IPV8 Address
L	Azure_Tenant_VR 50000	2000	Leaf-S	PENDING	Attached	border	Azure-HCI			
L	Azure_Tenant_VR 50000	2000	Leaf-6	PENDING	Attached	border	Azure-HCI			
L	Arure_Tenant_VR 50000	2000	Leaf-2	DEPLOYED	Attached	leaf	Azure-HCI			
L	Azure,Tenant,VR 50000	2000	Leaf-1	DEPLOYED	Attached	losf	Azure-HOI			
1										

Cisco NDFC は、VXLAN ファブリックの境界デバイスに必要な設定をプッシュします。

外部ネットワークも NDFC によって管理されている場合は、Cisco NDFC が VRF_Lite 拡張の相手側として使用されているデバイスに設定をプッシュするために、外部ファブリックでも 再計算と展開 を実行します。

これにより、外部通信を行うために、VXLAN ネットワークを外部にアドバタイズでき、その逆も可能です。

付録

Azure Stack HCI での Microsoft ソフトウェア定義型ネットワーキング (SDN) の設計例

VLAN ベースのテナントネットワークに加えて、 Azure Stack HCI には、サーバ側の VXLAN 終端を含む Microsoft SDN を使用したネットワーク設計オプションがあります。このセクションでは、 Azure Stack HCI での Microsoft SDN 向けの Cisco ACI および Nexus 9000 の設計例を示します。このセクションでは、 Azure Stack HCI 側で必要な構成については説明しません。Cisco Nexus スイッチへの Microsoft AWS パスの拡充 HCI 接続の物理アーキテクチャは、「物理アーキテクチャ」セクションで説明したものと同じです。

Microsoft Azure SDN コンポーネント

Microsoft Azure SDN では、ソフトウェア ロード バランサ、ファイアウォール、サイト間 IPsec-VPN、サイト 間 GRE トンネルなどの追加機能が導入されています。ソフトウェア ロード バランサとファイアウォールは、 Azure Stack HCI クラスタでホストされているリモート対応マシンに負荷バランシングおよびファイアウォール サービスを提供します。サイト間 IPsec VPN およびサイト間 GRE トンネルにより、 Azure Stack HCI クラス タでホストされているリモート対応マシンと Azure Stack HCI の外部の外部ネットワーク間の接続が可能にな ります。

次の VM は、 Azure Stack HCI の Microsoft Azure SDN の主要コンポーネントです。

- ネットワーク コントローラ VM:ネットワーク コントローラ VM は、Azure Stack HCI 内で仮想ネットワーク インフラストラクチャを作成および管理するための一元化されたポイントを提供します。ネットワーク コントローラ VM は、Azure Stack HCI SDN のコントロールプレーンとして機能し、実際のデータトラフィックを伝送しません。Microsoft では、冗長性のために少なくとも3つのネットワークコントローラ VM を使用することを推奨しています。
- ソフトウェア ロード バランサ VM: ソフトウェア ロード バランサ (SLB) VM は、North-South およ び East-West TCP/UDP トラフィックにレイヤ 4 ロード バランシング サービスを提供します。ソフト ウェア ロード バランサ VM は、Azure Stack HCI クラスタで負荷バランシング サービスを提供するた めに、Azure Stack HCI サーバーにインストールされます。Microsoft では、SLB VM の代わりに、ソ フトウェア ロード バランサ マルチプレクサ VM または SLB MUX VM という用語を使用しています。 以降、このドキュメントでは SLB MUX VM を使用してソフトウェア ロード バランサ VM について説 明します。Azure Stack HCI クラスタごとに少なくとも 1 つの SLB MUX VM が必要であり、スケール に基づいて数を増やすことができます。ソフトウェア ロード バランサの詳細については、このドキュ メントの後半で説明します。
- ゲートウェイ VM: ゲートウェイ VM は、Azure Stack HCI 内の Microsoft Azure SDN リモート対応ネットワーク(VNET) と Azure Stack Azure Stack HCI 外の外部ネットワーク間にレイヤ 3 接続を作成します。IPsec VPN や GRE トンネルなどの機能は、ゲートウェイ VM によって処理されます。 Microsoft では、Azure Stack HCI クラスタごとに少なくとも 2 つのゲートウェイ VM を使用することを推奨しています。この数はスケールに基づいて増やすことができます。

注: ネットワークコントローラ VM、SLB MUX VM、およびゲートウェイ VM の展開に関する公式の拡張性 ガイドラインについては、 Microsoft にお問い合わせください。

論理アーキテクチャ

このドキュメントで前述した <u>管理ネットワーク</u>と <u>ストレージ ネットワーク</u>とは別に、 Azure Stack HCI 内の Microsoft Azure SDN では、次のネットワークが使用されます。

- HNV PA ネットワーク(Hyper-V ネットワーク仮想化プロバイダー アドレス ネットワーク)
- 論理ネットワーク

HNV PA ネットワーク

Hyper-V ネットワーク仮想化 (HNV) プロバイダー アドレス (PA) ネットワークは、Azure Stack HCI 内の Microsoft Azure でマルチテナントが必要な場合に展開されます。PA ネットワークは、VXLAN カプセル化を使 用してマルチテナントを実現します。PA ネットワーク アドレスは、Nexus スイッチの VTEP IP アドレスに似 ています。これは、Azure Stack HCI クラスタ内の East-West VM 通信のアンダーレイ物理ネットワークとし て機能します。PA ネットワークでは、物理ネットワーク上に VLAN を割り当てる必要があります。これは、ク ラスタのすべてのサーバーのデータ インターフェイスでトランクとして渡されます。

Azure Stack HCI クラスタの各サーバには 2 つの PA ネットワーク IP アドレスがあり、各 SLB MUX VM とゲートウェイ VM には PA ネットワークから 1 つの IP アドレスがあります。したがって、16 ノードクラスタの 場合、スケールに基づいて複数の SLB MUX VM とゲートウェイ VM が必要になるため、/26 以上のサブネット が必要になる場合があります。

論理ネットワーク

論理ネットワークは、 Azure Stack HCI サーバーと Cisco ACI リーフ スイッチなどの top-of-rack (ToR; トッ プオブラック) オブラック スイッチ間のネットワーク セグメントです。各論理ネットワークは、VLAN 識別子 とアドレス プレフィックスを必要とする論理サブネットで構成されます。VLAN 識別子は、 Azure Stack HCI クラスタで一意である必要があります。アドレス プレフィックスには、Azure Stack HCI クラスタ用に 1 つ、 各 top-of-rack (ToR; トップオブラック) オブラックスイッチの各 VLAN インターフェイス用に 1 つ、トップ オブラック スイッチのペアで共有されるリモート対応 IP アドレス用に 1 つ top-of-rack (ToR; トップオブラ ック) スイッチなど、少なくとも 4 つの IP アドレスが必要です。論理ネットワークは、 Azure Stack HCI VNET と top-of-rack (ToR; トップオブラック) オブラック スイッチの間でトラフィックを伝送する物理経路 として機能します。VNET は Azure Stack HCI の仮想ネットワークであり、NX-OS モードの Cisco ACI および Nexus 9000 の VRF に相当します。

PA ネットワークと SLB MUX VM の接続

このセクションでは、 PA ネットワークと SLB MUX VM を Cisco ACI および Cisco NX-OS ベースのファブリ ックに接続する方法について説明します。

ソフトウェア ロード バランサ (SLB)

Cisco ACI および Cisco NX-OS ベースのファブリックで PA ネットワーク接続を設計する前に重要な考慮事項 は、ソフトウェア ロード バランサの機能とその接続要件を理解することです。これは、SLB MUX VM が Microsoft Azure SDN のインストールに必須であるためです。SLB MUX VM は、 Azure Stack HCI の VNET 内 のロードバランスされた VM のプールへのパブリック アクセスと、VNET 内のネットワーク トラフィックの負 荷分散に使用できます。

このドキュメントでは、 Azure Stack HCI クラスタに展開された 3 つの SLB MUX VM の例を使用します。各 SLB MUX VM には、 PA ネットワークからの一意の IP アドレスが 1 つあります。SLB MUX VM は、 Azure Stack HCI クラスタの一部である Azure Stack HCI サーバーのいずれかでホストできます。

SLB MUX VM では、外部ネットワークの到達可能性のために、外部ルータ(この場合は Cisco ACI リーフ スイ ッチ)の IP を使用して eBGP ピアリングを設定する必要があります。

SLB MUX VM の展開には、2 つの追加の IP プール(パブリック VIP プールとプライベート VIP プール)が必要です。パブリック VIP プールとプライベート VIP プールは、仮想 IP を割り当てるために SLB MUX VM に割り当てられます。これらの仮想 IP は、負荷バランシング機能を必要とする Azure Stack HCI クラスタ内でホストされているアプリケーションまたはサービスによって使用されます。これらの IP プールは、SLB MUX VM の上にプロビジョニングされます。

注: SLB MUX VM は、これらの IP プールから自身に割り当てられる IP アドレスを使用しません。SLB MUX VM は、PA ネットワークから割り当てられた IP アドレスを使用します。

- パブリック VIP プール: Azure Stack HCI クラスタの外部でルーティング可能な IP サブネットプレフィックスを使用する必要があります(必ずしもインターネットルーティング可能なパブリック IP である必要はありません)。これらは、サイト間 VPN のフロントエンド VIP を含む、VNET 内の VM にアクセスするために外部クライアントが使用するフロントエンド IP アドレスです。パブリック VIP は、Azure Stack HCI クラスタの外部から負荷されたアプリケーションまたはサービスに到達するために使用されます。
- プライベート VIP プール:この IP サブネット プレフィックスは、Azure Stack HCI クラスタの外部で ルーティング可能である必要はありません。これらの VIP は、Azure Stack HCI クラスタの VNET の 一部である内部クライアントによってアクセスされることを目的としています。プライベート VIP は、 負荷分散されたアプリケーションまたはサービスが Azure Stack HCI クラスタの外部からの到達可能性 を必要としない場合に使用されます。

PA ネットワークおよび SLB 接続のための Cisco ACI 設計

SLB MUX VM は PA ネットワークの一部であり、他のネットワークと通信するためにリーフ スイッチとの eBGP ピアリングが必要です。したがって、L3Out は、 Azure Stack HCI 内で設定された PA ネットワーク VLAN 識別子と同じ encap VLAN を使用して設定する必要があります。 次の図は、Cisco ACI リーフ スイッチを使用した SLB MUX の eBGP ピアリングの論理的な設計例を示しています。



Tenant: common

図 24.

PA ネットワークでの SLB MUX および ACI の eBGP ピアリング

上の図は、 Azure Stack HCI アンダーレイ接続の設計で展開された Cisco ACI テナント要素間の高レベルの関係の例も示しています。この例では、Cisco ACI common テナントには、ストレージおよび管理ネットワーク 用の Common_VRF EPG と呼ばれる VRF が含まれています。

このテナントには、特定のクラスタの PA ネットワーク接続専用の Cluster_01_PA_L3Out という名前の L3Out も含まれています。 eBGP は L3Out で構成されたルーティング プロトコルになりますが、L3Out で使 用される encap vlan は、 Azure Stack HCI クラスタの PA ネットワーク VLAN として構成された同じ VLAN になります。

この例では、クラスタごとに 3 つの SLB MUX VM が展開されているため、各 Cisco ACI リーフには 3 つの eBGP ピアがあります。したがって、Azure Stack HCI クラスタと Cisco ACI リーフ スイッチのペアの間に、 合計 6 つの eBGP ピアリングが確立されます。この例では、10.2.1.0/24 は IP サブネット、401 は PA ネット ワークに割り当てられた VLAN 識別子です。Cisco ACI リーフスイッチで設定された SVI インターフェイスは、 リーフ 01 とリーフ 02 に対してそれぞれ 10.2.1.2/24 と 10.2.1.3/24 になります。3 つの SLB MUX VM の IP アドレスは、それぞれ 10.2.1.4/24、10.2.1.5/24、および 10.2.1.6/24 です。ループバック IP アドレスまたは 直接接続されていない IP アドレスを使用した eBGP ピアリングはサポートされていません。したがって、 eBGP ピアリングは、Cisco ACI リーフ スイッチの L3Out SVI インターフェイスで形成されます。

注: 各 Azure Stack HCI クラスタには、ストレージ用の専用 EPG、管理用の専用 EPG、および PA ネット ワーク用の専用 L3Out とその外部 EPG が 1 つ必要です。

Azure Stack HCI VNET 接続 (論理ネットワークおよびゲートウェイ VM 接続)

VNET は、 Azure Stack HCI の仮想ネットワークです。アドレス プレフィックスで作成されます。ワークロード VM への IP 割り当てのために、VNET アドレス プレフィックスから複数の小さなサブネットを作成できます。

サブネットの1つはゲートウェイサブネットとして使用されます。ゲートウェイサブネットは、Azure Stack HCI VNET の外部と通信するために必要です。このサブネットの IP アドレスは、ゲートウェイ VM に自動的に プロビジョニングされます。このサブネットは、/28、/29、または /30 プレフィックスを使用して設定できま す。/28 または /29 サブネットプレフィックスは、IPsec または GRE トンネルが必要な場合は常にサブネット からの追加の IP アドレスがゲートウェイ VM にプロビジョニングされるため、ゲートウェイサブネットで IPsec または GRE トンネルが必要な場合に必要です。このドキュメントでは、IPsec または GRE トンネルにつ いては説明しません。

Azure Stack HCI VNET 接続向け Cisco ACI 設計

ゲートウェイ VM は、ACI リーフ スイッチのペアで設定されたループバック IP アドレスを使用して 2 つの eBGP ピアリングを確立します。ループバック IP アドレスに到達可能性にするために、 Azure Stack HCI VNET にスタティック ルートが必要です。スタティック ルートのネクスト ホップ IP アドレスは、論理ネット ワークの Cisco ACI リーフ スイッチのペアで設定されたリモート対応 IP アドレスです。

注: eBGP ピアリングに使用されるスタティック ルートのネクスト ホップ IP アドレスは、Azure Stack HCI の L3 ピア IP と呼ばれ、 Azure Stack HCI で構成された仮想 IP アドレスは、Cisco ACI のセカンダリ IPv4 アドレスと呼ばれます。

L3Out は、Azure Stack HCI クラスタの VNET への接続用に Cisco ACI ファブリックで構成されます。Cisco ACI リーフ スイッチは、ゲートウェイ VM に割り当てられた IP アドレスで 2 つの eBGP ピアリング (各 ACI リーフスイッチから 1 つ)を確立します。この IP アドレスは、Azure Stack HCI の [ゲートウェイ接続 (Gateway connections)] セクションの BGP ルータ IP アドレスで確認できます。ゲートウェイ VM の IP アドレスに到達可能性にするために、Cisco ACI リーフ スイッチでスタティック ルートが設定されています。このスタティック ルートのネクスト ホップは、Azure Stack HCI クラスタで構成された論理ネットワークからの

IP アドレスです。

次の図は、 Azure Stack HCI VNET 接続を使用した Cisco ACI L3Out の例を示しています。



図 25.

Cisco ACI リーフ スイッチを使用した Azura ゲートウェイ VM の EBGP ピアリング

この設計例には、 ACI リーフ スイッチのペアに接続された 3 ノードの Azure Stack HCI クラスタがあり、 Azure Stack HCI に次のネットワーク構成が含まれています。

- VNET01 という名前の VNET が、アドレス プレフィックス 192.168.1.0/24 で Azure Stack HCI に作 成されます。ゲートウェイ サブネットは 192.168.1.0/29 です。
- Azure Stack HCI の論理ネットワークは、IP サブネット 10.10.1.0/29 と VLAN 識別子 501 を使用します。10.10.1.6/29 は、Cisco ACI リーフ スイッチへのゲートウェイ接続に使用されます。この例では、 eBGP マルチホップが使用され、65201 はゲートウェイ VM の BGP ASN です。
- スタティック ルート(10.10.10.10/32 および 10.10.1.1 をビアた 10.10.10.20/32)は、ACI リーフ スイッチのペアのループバック IP アドレスに到達するように設定されます。IP アドレス 10.10.1.1 は、 両方の ACI リーフ スイッチの VLAN インターフェイスでリモート対応 IP アドレス(セカンダリ IPv4 アドレス)として設定されます。
- VNET01 の一部でもある Web およびアプリ VM は、宛先 IP アドレスが VNET_01 の外部にある場合、 常にゲートウェイ VM にトラフィックを送信します。

Azure Stack HCI との接続を確立するために、Cisco ACI ファブリックには次の構成が含まれています。

- Azure Stack HCI の VNET_01 に対応する、HCI1_tenant1 という名前の ACI テナントと VRF1 という 名前の VRF が作成されます。
- VNET01_L3Out という名前の L3Out は、VNET01 のゲートウェイ VM との eBGP ピアリング用に作成 されます。

- Leaf01 にはループバック IP 10.10.10/32 があり、Leaf02 にはループバック IP 10.10.10.20/32 があります。
- L3Out 内の論理インターフェイス プロファイルは、VLAN インターフェイスで構成されます。
 VLAN インターフェイスにはサブネット 10.10.1.0/29 から IP アドレスが割り当てられ、カプ セル化 VLAN 識別子は 501 (Azure Stack HCI 論理ネットワークで定義されているものと同じ) です。
- スタティック ルート(192.168.1.0/29)は、L3Out 内の論理ノードプロファイルでゲートウェイ VM(192.168.1.2)に到達するように設定されており、ネクストホップは10.10.1.6です。
- o eBGP ピアリングを構築するには、値が2以上のeBGP マルチホップが必要です。
- EXT_L3Out という名前の別の L3Out は、Cisco ACI ファブリック外部の通信に使用されます。

ソリューションの導入

このセクションでは、SDN を有効にした Cisco ACI および Azure Stack HCI を設定する詳細な手順について説 明します。ACI ファブリックと APIC がお客様の環境にすでに存在することを前提としています。このドキュメ ントでは、最初の ACI ファブリックをオンラインにするために必要な設定については説明しません。

<u>表3</u>は、このソリューションで使用されるハードウェアとソフトウェアをリストします。

次の図と表 9 に、このセクションで使用するトポロジ、インターフェイス、および L3 ドメイン設定パラメータの概要を示します。この接続では、 ACI リーフ スイッチと Azure Stack HCI サーバー間で 6 つの 100 GbE インターフェイスを使用します。



図 26.

SDN を使用した Azure Stack HCI サーバーのインターフェイスと L3 ドメインの設定

表9. Azure Stack HCI サーバーのインターフェイスと L3 ドメインの構成

インターフェ イス	インターフェ イス ポリシー グループ	LLDP インター フェイス ポリシ ー	インターフェイ ス PFC ポリシ ー	AAEP 名	ドメイン名	ドメイン のタイプ	VLAN Pool
Leaf1 および Leaf2 イーサ ネット 1/11- 13	個別-HCI	HCI_LLDP (DCBXP : IEEE 802.1)	PFC 自動	HCI_AAEP	HCI_EXT_L3DOM	L3	$\begin{array}{l} \mbox{HCI_VLAN_pool} \\ (\mbox{VLAN 400} \sim \\ \mbox{600}) \end{array}$

Azure Stack HCI サーバーのインターフェイスと L3 ドメインの構成

表 10 および 11 に、このセクションで使用する ACI common およびユーザー テナントの構成パラメータを示 します。ACI リーフ スイッチは、L2 専用のストレージ ネットワークを除き、 Azure Stack HCI ネットワーク へのゲートウェイとして機能します。参考のためにコントラクト名が記載されていますが、このドキュメントで は、共通テナントの共有 L3Out 構成とコントラクトの構成手順については説明しません。



図 27.

Microsoft SDN を使用した Azure Stack HCI の ACI テナントの概要

表 10. SLB MUX 接続の ACI 共通テナント設定例

プロパティ	名前
テナント	共通の
テナント VRF	common_VRF
ブリッジドメイン	common_VRF のストレージA(サブネットなし)

プロパティ	名前
	common_VRF のストレージ B(サブネットなし) common_VRF での管理(10.1.1.254/24)
リーフ ノードとインターフェイス	ノード 101 および 102 ethernet1/11、1/12 および 1/13
EPG	BD 管理での EPG 管理 BD ストレージ A 内の EPG ストレージ A BD ストレージ B 内の EPG ストレージ B
コントラクト	Contract_1_to-external
L3Out	common テナントの Cluster_01_PA_L3Out (BGP)
論理ノードプロファイル	Cluster_01_PA_101_NP(ノード-101) - ルータ識別子:1.1.1.1 Cluster_01_PA_102_NP(ノード 102) ルータ識別子:2.2.2.2
論理インターフェイス プロファイル	Cluster_01_PA_101_IFP (eth1/11, eth1/12, $\pm \pm \sigma$ eth1/13) - $4\nu \beta - 7 \pm 4 \pi \beta \gamma \gamma$: SVI - $2\pi \beta - 7 \pi \gamma \eta$ IP : 10.2.1.2/24 - $2\pi \mu \nu \beta \eta$ IP : 10.2.1.1/24 - Encap : 401 - BGP $\ell^{*} \tau$: 10.2.1.4, 10.2.1.5, 10.2.1.6 - Remote AS: 65002 Cluster_01_PA_102_IFP (eth1/11, eth1/12, $\pm \delta \tau \sigma$ eth1/13) - $4\nu \beta - 7 \pm 4 \pi \beta \gamma \gamma$: SVI - $2\pi \beta - 7 \pi \eta$ IP : 10.2.1.2/24 - $2\pi \mu \nu \beta \eta$ IP : 10.2.1.2/24 - $2\pi \mu \nu \beta \eta$ IP : 10.2.1.1/24 - Encap : 401 - BGP $\ell^{*} \tau$: 10.2.1.4, 10.2.1.5, 10.2.1.6 Remote AS: 65002
外部 EPG	Cluster_01_PA_EXT_EPG
	エクスポート ルート コントロール サブネット (0.0.0.0)

表 11. ゲートウェイ VM 接続の ACI ユーザー テナント設定例

プロパティ	名前
テナント	HCI1_tenant1
テナント VRF	VRF1
リーフ ノードとインターフェイス	ノード 101 および 102 ethernet1/11、1/12 および 1/13
コントラクト	Contract_2_to-external
L3Out	HCI1_tenant1 @ VNET01_L3Out (BGP)
論理ノードプロファイル	VNET01_101_NP (ノード 101)

プロパティ	名前
	 ループバック IP: 10.10.10.10 ルータ識別子: 1.1.1.1 スタティック ルート: 192.168.1.0/29、ネクストホップ: 10.10.1.6 BGP ピア: 192.168.1.2、送信元インターフェイス: ループバック Remote AS: 65201 VNET02_102_NP (ノード 102) ループバック IP: 10.10.10.20 ルータ識別子: 2.2.2.2 スタティック ルート: 192.168.1.0/29、ネクストホップ: 10.10.1.6 BGP ピア: 192.168.1.2、送信元インターフェイス:
	Remote AS: 65201
論理インターフェイス プロファイル	 VNET01_101_IFP (eth1/11、1/12、および 1/13) インターフェイス タイプ: SVI プライマリ IP: 10.10.1.2/29 セカンダリ IP: 10.10.1.1/29 VLAN Encap: 501 VNET01_102_IFP (eth1/11、1/12、および 1/13) インターフェイス タイプ: SVI プライマリ IP: 10.10.1.3/29 セカンダリ IP: 10.10.1.1/29 VLAN カプセル化: 501
外部 EPG	VNET01_EXT_EPG - エクスポート ルート コントロール サブネット (0.0.0.0) 外部 EPG の外部サブネット (192.168.1.0/24)

Azure Stack HCI L3 ドメインの VLAN プールの作成

このセクションでは、 Azure Stack HCI への接続を有効にするための VLAN プールを作成します。

Azure Stack HCI サーバーを ACI リーフ スイッチに接続するように VLAN プールを構成するには、次の手順を実行 します。

- 1. 一番上のナビゲーション メニューから、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] を選択します。
- 2. 左側のナビゲーション ウィンドウで、【プール (Pools)】、【VLAN (VLAN)】の順に選択します。
- 3. 右クリックし、[IP プールの作成(Create IP Pool)]を選択します。
- 4. [プールの作成(Create Pool)] ポップアップウィンドウで、名前(HCI_VLAN_pool など)を指定し、
 [割り当てモード(Allocation Mode)]で【静的割り当て(Static Allocation)]を選択します。

- 5. カプセル化ブロックの場合は、右側の [+] ボタンを使用して VLAN を VLAN プールに追加します。[範 囲の作成(Create Ranges)] ポップアップウィンドウで、リーフ スイッチから Azure Stack HCI サー バーに設定する必要がある VLAN を設定します。残りのパラメータはそのままにします。
- 6. [OK] をクリックします。
- 7. [送信 (Submit)] をクリックします。

cise	(). CO	APIC									
Syst	tem	Tenants	Fabric	Virtual Networking	Adm	nin Oper	rations Ap	os Integration	IS		
	Invent	ory Fat	ric Policies	Access Policies	_						
Policie	es			ĐĘ	\bigcirc	Pools - VI	LAN				
	Quick Sta Interface	ırt Configuratior									
> 🖬 🖇	Switches					Creat	e VLAN Po	lool			28
	Modules Interface:						Name:	HCI_VLAN_POOL			
> 🖿 F							Description:	optional			
	Physical a	and External [omains						_		
							Allocation Mode:	Dynamic Allocation	Static Allocation	on	
	Croc	ato Don	200				Encap Blocks:		00	Allegation Made	The H
> 6 > 6 > 6	Ciea	Desc Allocation	Type: VLA ription: Opt Range: VLA Mode: C Role: E	N 400 - [integer Value -] ynamic Allocation Inherit xternal or On the wire encapsu	VLAN ~ allocMode lations	600 Into alue from parent Internal	Static Allocati	m			Role
								Cancel	ОК	Cat [4007] (Static A [4014] (Static A	ncel Submit

Azure Stack HCI の L3 ドメインの構成

L3 ドメインタイプを作成し、 Azure Stack HCI サーバーに接続するには、次の手順を実行します。

- 一番上のナビゲーション メニューから、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] を選択します。
- 2. 左のナビゲーション ウィンドウで、[Physical and External Domains (物理と外部ドメイン)]>[L3 ドメイン (L3 ドメイン)]を選択します。
- 3. [L3 ドメイン (L3 Domains)]を右クリックし、[L3 ドメインの作成 (Create L3 Domain)]を選択し ます。
- [Create L3 Domain] ポップアップウィンドウで、ドメインの名前を指定します(例: HCI_EXT_L3DOM)。VLAN プールの場合は、ドロップダウン リストから以前に作成した VLAN プー ル(HCI_VLAN_pool など)を選択します。

cisco APIC							
System Tenants Fabric	Virtual Networking Ad	min Operations	Apps	Integrations			
Inventory Fabric Policies	Access Policies						
Policies		L3 Domains					
Quick Start		Create L3 Dom	ain				\otimes
Interface Configuration Switch Configuration		Name:	HCI_EXT_L	.3DOM			1.
> E Switches		Associated Attachable Entity Profile:	select a va	lue	\sim		t
> 🚍 Modules		VLAN Pool:	HCI_VLAN	_POOL(static)	~ 🗗		_
> 💼 Interfaces		Security Domains:				0 -	+
Physical and External Domains			Select	Name		Description	
> 🚞 External Bridged Domains							
> Fibre Channel Domains							
L3 Domains Demains							
	4						
						Cancel	Submit

5. [送信 (Submit)]をクリックします。

Azure Stack HCI L3 ドメインの接続可能なアクセス エンティティ プロファイルの作成

接続可能なアクセス エンティティ プロファイル (Attachable Access Entity Profile (AAEP)) を作成するに は、次の手順を実行します。

- 1. 一番上のナビゲーション メニューから、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] を選択します。
- ナビゲーションペインで、[ポリシー (Policies)] > [グローバル (Global)]> [接続可能なアクセス エンティティ プロファイル (Attachable Access Entity Profile)]の順に選択します。
- 3. 右クリックして、**[接続可能なアクセス エンティティ プロファイル (Create Attachable Access** Entity Profile)]を作成します。
- 【接続可能なアクセス エンティティ プロファイル (Create Attachable Access Entity Profile)】ポッ プアップ ウィンドウで、名前 (HCI_AAEP など)を指定し、【インフラストラクチャ VLAN の有効化 (Enable Infrastructure VLAN)】と【インターフェイスへの関連付け(Association to Interfaces)】 をオフにします。
- 5. [ドメイン (Domains)]については、ウィンドウの右側にある[+]をクリックし、[ドメイン プロファ イル (Domain Profile)]の下のドロップダウン リストから以前に作成したドメインを選択します。
- 6. [Update] をクリックします。
- 7. 次に示すように、選択したドメインと関連する VLAN プールが表示されます。
- [次へ (Next)]をクリックします。上記のステップ4で[インターフェイスへの関連付け (Association to Interfaces)]がオフになっているため、このプロファイルは現時点ではどのインターフェイスにも 関連付けられていません。次のセクションでインターフェイスを設定すると、それらを関連付けること ができます。

cisco APIC					
System Tenants Fabric	Virtual Networking A	Create Attachable	e Access Entity Profile		08
Inventory Fabric Policies	Access Policies	STEP 1 > Profile		1. Profile	2. Association To Interfaces
Policies	$\bigcirc \bigcirc \bigcirc \bigcirc$	Name:	HCI_AAEP		
Over Quick Start		Description:	optional		
F Interface Configuration					
> 🚞 Switches		Enable Infrastructure VLAN:			
> 🚞 Modules		Domains (VMM, Physical or External) To Be Associated			會 +
> 🚍 Interfaces		To Interfaces:	Domain Profile	Encapsulation	
∼ 🚍 Policies			Physical Domain - HCI_phys	from:vlan-1600 to:v	lan-1699
> 🚞 Switch			L3 External Domain - HCI_EXT_L3DOM	from:vlan-400 to:vla	in-600
> 🚞 Interface					
🗸 🚞 Global					
> 🥅 PTP User Profile					
> 🚞 DHCP Relay					
🗸 🚞 Attachable Access Entity Profiles		EPG DEPLOYMENT (AI See	acted EPGs will be deployed on all the interfaces associated.)		
🗧 default		Application EDCo		Eason Drim	T Mada
RW_AEP		Application EPGs		спсар Рпп	lary Encap Wode
Error Disabled Recovery Policy					
MCP Instance Policy default					
> 🥅 QOS Class					
> 🚞 Monitoring					
> 🚞 Troubleshooting					
> Physical and External Domains		-			
> 🚞 Pools					
					Cancel Next

9. [終了 (Finish)] をクリックします。

Azure Stack HCI の VLAN ベースのテナントネットワークと Microsoft SDN ベースのネットワークに共通する 次の設定を実行します。

- <u>LLDP ポリシーの作成</u>
- LLDP インターフェイス ポリシーの作成
- インターフェイス優先順位フロー制御ポリシーの作成
- <u>Azure Stack HCl サーバーに接続されたインターフェイスのインターフェイス ポリシー グループの作</u> <u>成</u>
- Azure Stack HCl サーバーに接続されたインターフェイスのインターフェイス ポリシー グループの関 連付け
- <u>QoS</u>の設定

管理 VLAN、ストレージ VLAN、および PA VLAN は、SDN を使用した Azure Stack HCI の VLAN ベースのネ ットワークです。次のサブセクションでは、PA ネットワーク展開の L3Out 構成例について説明します。管理 VLAN に対応する管理 EPG とストレージ VLAN に対応するストレージ EPG の展開については、このドキュメ ントの「EPG の構成」セクションを参照してください。

PA ネットワークおよび SLB 接続の Cisco ACI 構成

このセクションでは、Cisco ACI で L3Out を構成して PA ネットワークと SLB MUX VM の接続を有効にする方 法について説明します。L3Out を作成するには、次の手順を実行します。

1. APIC の上部のナビゲーションメニューから、[テナント(Tenants)]>[common]の順に選択します (または、PA L3Out を構成する既存のテナントを選択します)。
- 左側のナビゲーション ウィンドウで、[ネットワーク (Networking)]>[L3Outs (L3Outs)]の順に 選択します。
- 3. 右クリックし、[L3Out の作成(Create L3Out)]を選択します。
- 【名前(Name)】フィールドで、名前を指定し(例: Cluster_01_PA_L3Out)、VRF 名(この例では Common_VRF)を選択し、ドロップダウンリストから以前に作成した L3 ドメイン を選択します(この例では、HCI_EXT_L3DOM)。
- 5. [BGP] チェックボックスをオンにし、[次へ (Next)] をクリックします。

cisco APIC	ad
System Tenants Fabric Virt	Create L3Out
ALL TENANTS Add Tenant Tenant Sea	1. Identity 2. Nodes And Interfaces 3. Protocols 4. External EPG
common	
Coulds Start Common Co	Protocol- Proto
Security	Name: Cluster_O1_PA_L3Out

[デフォルトを使用(Use Defaults)]チェックボックスをオフにして、[ノードプロファイル名(Node Profile Name)]フィールド(この例では Cluster_01_PA_101_NP)と[インターフェイス プロファイル名(Interface Profile Name)]フィールド(この例では Cluster_01_PA_101_IFP)に名前を手動で指定します。

			1. Identity	2. Nodes And Interfaces	3. Protocols	4. External EPG
Use Defaults:						
Node Profile Name: Cl	uster_01_PA_101_NP					
terface Types						
Layer 3:	Interface Sub-Interface	SVI Floating SVI				
Layer 2:	Port Virtual Port Channe	I Direct Port Channel				
lodes						
loues						
Node ID	Router IE	Loopback A	ddress			
LEAF1 (Node-101)	∨ 1.1.1.1			+ Hide Interfaces		
		Leave empty to any Loopback	o not configure			
Interface	Interface Profile Name	Encap	MTU (bytes)	IP Address		
eth1/11 ~	Cluster_01_PA_101_IFP	VLAN \checkmark 401	9216	10.2.1.2/24	+	
Ex: eth1/1 or topology/pod- 1/paths-101/pathep-[eth1/23]		Integer Value	9	address/mask		
Interface	Interface Profile Name	Encap	MTU (bytes)	IP Address		
eth1/12	Cluster_01_PA_101_IFP	VLAN V 401	9216	10.2.1.2/24	+	
Ex: eth1/1 or topology/pod- 1/paths-101/pathep-[eth1/23]		Integer Value	e	address/mask		
Interface	Interface Profile Name	Encan	MTU (bytes)	ID Address		
eth1/13	Cluster 01 PA 101 IFP	VLAN V 401	9216	10.2.1.2/24	+	
Ex: eth1/1 or topology/pod- 1/paths-101/pathep-[eth1/23]		Integer Value	0210	address/mask		

- 7. [インターフェイス タイプ (Interface Types)] セクションで、 レイヤ 3 の場合は [SVI] 、 レイヤ 2 の場合は [ポート (Port)] を選択します。
- 8. [ノード (Nodes)]セクションで、最初のリーフスイッチに関連するすべての詳細を入力します(この 例では、ノード識別子は Node-101、ルータ識別子は 1.1.1.1、[ループバック アドレス (Loopback Address)]フィールドは空白のままにします)。
- 2番目の行の[+]をクリックして、同じノードにインターフェイスを追加します(この例では、1つの リーフスイッチ、eth1/11、1/12、および1/13の3つのインターフェイスに接続している3つのサ ーバーがあります)。
- ドロップダウン リストから、サーバーに接続するインターフェイスを選択し、【インターフェイス プロファイル名(Interface Profile Name)】、【Encap】、【Encap 値(Encap value)】、【MTU】、および 【IP アドレス】を指定します。Azure Stack HCI サーバーは最大 MTU サイズを 9174 として使用するため、TOR スイッチで構成される MTU は 9174 以上である必要があります(この例では、インターフェイス プロファイル名は Cluster_01_PA_101_IFP、Encap は VLAN、Encap 値は 401、MTU は 9216 です。 IP アドレスは 10.2.1.2/24 です)。
- 11. すべてのインターフェイスに同じ値を入力し、[次へ (Next)]をクリックします。2番目のリーフの同等の構成は後で追加されますが、このウィザードを使用して追加することもできます。
- 12. このページで BGP 関連情報を入力せずに [次へ (Next)] をクリックします。

1. Identity 2. Nodes And Interface 3. Prodocol 4. External EPG Productions BGP Loopback Policies Node Profile: Cluster_01_PA_101_NP Interface Policies Interface Policies Node ID: 101 Interface Peer Address EBGP Multihop TTL Remote ASN Interface Policies	Create L30	ut					8
Protocol Associations BGP Loopback Policies Node Profile: Cluster_01_PA_101_NP Hide Policy Hide Policy TIL Remote ASN TO THEFace Policies Node ID: 101 Hide Policy Hide Po				1. Identity	2. Nodes And Interfaces	3. Protocols	4. External EPG
BGP Loopback Policies Node Profile: Cluster_01_PA_101_NP Image: Node Peer Address EBGP Multihop TTL Remote ASN 101 Image: Node ID: 101 Image: Peer Address EBGP Multihop TTL Remote ASN Interface Peer Address EBGP Multihop TTL Remote ASN Interface Peer Address EBGP Multihop TTL Remote ASN Interface Interface Peer Address EBGP Multihop TTL Remote ASN Interface Interface Interface Interface Interface Remote ASN Interface Interface <th>Protocol Assoc</th> <th>iations</th> <th></th> <th></th> <th></th> <th></th> <th></th>	Protocol Assoc	iations					
Loopback Policies Node Profile: Cluster_01_PA_101_NP Inde Policy Hide Policy Hide Policy Interface Policies Node ID: 101 Hide Policy Hide Policy Hide Policy Hide Policy Interface Policies Interface EBGP Multihop TTL Remote ASN Interface Interface EBGP Multihop TTL Remote ASN I/12 I/12 </td <td>BGP</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	BGP						
Node Profile: Cluster_O1_PA_101_NP Nodes Peer Address EBGP Multihop TTL Remote ASN Interface Policies Node ID: 101 Interface Peer Address EBGP Multihop TTL Remote ASN Interface Peer Address EBGP Multihop TTL Remote ASN 1/12 Interface Interface <t< th=""><th>Loopback </th><th>Policies</th><th></th><th></th><th></th><th></th><th></th></t<>	Loopback	Policies					
Nodes Peer Address EBGP Multihop TTL Remote ASN Interface Policies	Node Prof	ile: Cluster_01_PA_101_NP					
Interface Policies Node ID: 101 Hide Policy Hide Policy Hide Policy 1/11 1/12 101 101	Nodes	Peer Address	EBGP Multihop TTL	Remote ASN	Hide Pol	licy 🗌	
Interface Policies Node ID: 101 Hide Policy _ Interface Peer Address EBGP Multihop TTL Remote ASN 1/11 Image: Comparison of the policy in the policy i	101						
Node ID: 101 Hide Policy _ Interface Peer Address EBGP Multihop TTL Remote ASN 1/11	Interface P	Policies					
Hide Policy Hide P	Node ID: 1	101					
Interface Peer Address EbbP Multihip FTL Remote ASN 1/11 Image: Second and the second and	Interface	Deer Address	EDCD Multihen TTI	Domoto ACN	Hide Pol	licy 🗌	
	1/11	Peer Address					
	1/12				\Diamond		
1/13	1/13				\Diamond		
						Previous	Cancel Nevt
Previous						Hevious	Carrier Next

13. この時点では変更を加えずに、**[外部 EPG (External EPG)**] ページで**[完了 (Finish)**] をクリックします。外部 EPG は後の段階で作成されます。

Create L3Out

	\otimes
entity 2. Nodes And Interfaces 3. Prot	ocols 4. External EPG

External EPG

The L3Out Network or External EPG is used for traffic classification, contract associations, and route control policies. Classification is matching external networks to this EPG for applying contracts. Route control policies are used for filtering dynamic routes exchanged between the ACI fabric and external devices, and leaked into other VRFs in the fabric.

Name:		
Provided Contract:	select a value	\sim
Consumed Contract:	select a value	\sim
Default EPG for all external networks:	✓	

Previous Cancel Finish	Previous	Cancel	Finish
------------------------	----------	--------	--------

(

14. APIC の上部ナビゲーションメニューから、[テナント(Tenants)]>[common]>[ネットワーキング (Networking)]>[L3Outs]>[L3Out Name](この例では、Cluster_01_PA_L3Out)>[Logical Node Profiles](この例では、Cluster_01_PA_101_NP)、[論理インターフェイス プロファイル (Logical Interface Profiles)](この例では、Cluster_01_PA_101_IFP)>[SVI]の順に選択します。

common (*) (*)	0	Logical Interface Profile - Cluste	er_01_PA_101_IFP							Q
> O Quick Start									Policy	Faults History
V 🛄 common										
> 🧮 Application Profiles						General	Routed Sub-Interfa	ces Routed	Interfaces	SVI Floating SVI
V Networking										0 +
> 🚞 Bridge Domains										0 _
> 🖿 VRFs										11 +
> 🚞 L2Outs		 Path 	Side A IP	Side B IP	Secondary IP Address	IP Address	MAC Address	MTU (bytes)	Encap	Encap Scope
V 🚞 L3Outs		Port-1/Norte-101/otb1/11				10.21.2/24	00-22-PD-E0-10-EE	0.216	vian-401	Local
✓		Pou-lindue-lonjeaniji i				10.2.1.2/24	00-22-00-F0-10-FF	8210	Vian-401	Local
Logical Node Profiles		Pod-1/Node-101/eth1/12				10.2.1.2/24	00:22:BD:F8:19:FF	9216	vian-401	Local
Cluster_01_PA_101_NP	l It	Pod-1/Node-101/eth1/13				10.2.1.2/24	00:22:BD:F8:19:FF	9216	vlan-401	Local
> 🧮 Configured Nodes										
Logical Interface Profiles										
Cluster_01_PA_101_IFP										
> 🚞 External EPGs										
> The Route map for import and export route control										
> 🚹 L3DOM_F5_01										
> 🐽 L3out-osp_shared										
> 合 default										
> 🚞 SR-MPLS VRF L3Outs										
> 🚞 Dot1Q Tunnels								Show	leage D	
> 🚍 Contracts									53896 N	

15. 最初のインターフェイスをダブルクリックし、[+] をクリックして IPV4 セカンダリ アドレスを追加します。これはリモート対応 IP アドレスとして機能し、両方のリーフ スイッチで共通です(この例では、eth1/11 をダブルクリックし、セカンダリ IP アドレスとして 10.2.1.1/24 を入力します)。

SVI							
					Policy	Faults	History
8 👽 🛆 🕔						Õ	<u>+</u> %+
Properties							
Path:	topology/pod-	1/paths-101/pathe	p-[eth1/11]				
Path Description:	optional						
Encon:		401					
Encap.	VLAN V	401 nteger Value					
Encap Scope:	VRF L	.ocal					
Auto State:	disabled	enabled					- 1
Mode:	Trunk (Nati	ve) Trunk	Access (Untagged))			- 1
IPv4 Primary / IPv6 Preferred Address:	10.2.1.2/24 address/mask						- 1
IPv6 DAD:	disabled	enabled					- 1
IPv4 Secondary / IPv6 Additional Addresses:			1 +				
	 Address 	IPv6 DAD	Enable for DHCP Relay				
	10.2.1.1/24	enabled	Disabled				
Link-Local Address:							
				Show I		ose	

- 16. 下にスクロールして [+] をクリックし、BGP ピア接続プロファイルを追加します。BGP ピア アドレス は、SLB MUX VM の IP アドレスになります。
- **17.** すべての値をデフォルトのままにして、[ピア] [アドレス (Address)] と [Remote AS (Remote AS)] を入力し、[送信 (Submit)] をクリックします (この例では、ピアアドレスは 10.2.1.4 で、 Remote AS は 65002 です)。

\times
11
11
t

18. ステップ **16** とステップ **17** を繰り返して複数の BGP ピアを追加し、**[閉じる(Close)]** をクリックします(この例では **10.2.1.5** と **10.2.1.6**)。

SVI $\square \otimes$ Policy Faults History 0 ± %-Properties Link-Local Address: :: MAC Address: 00:22:BD:F8:19:FF MTU (bytes): 9216 Target DSCP: Unspecified External Bridge Group Profile: select an option BGP Peer Connectivity Profiles: 俞 +Peer IP Address Peer Controls 10.2.1.4 10.2.1.5 10.2.1.6 Rogue Exception MAC Group: select an option Exclude all MACs from Rogue EP Control:

19. 残りのインターフェイス(この例では、**eth1/12** と **eth1/13**)に対してステップ **15** ~ **18** を繰り返します。

common (*)	30	Logical Interface Profile - Cluste	er_01_PA_101_IFP							Q
✓									Policy	Faults History
✓										•
🗸 🚞 Logical Node Profiles						General	Routed Sub-Interfac	es Rout	ed Interfaces	SVI Floating SVI
✓										¢ +
> 🧮 Configured Nodes										
🗸 🚞 Logical Interface Profiles										₩ +
Cluster_01_PA_101_IFP		 Path 	Side A IP	Side B IP	Address	IP Address	MAC Address	MIU (bytes) Encap	Encap Scope
BGP Peer 10.2.1.4- Node-101/1/11		Pod-1/Node-101/eth1/11			10.2.1.1/24	10.2.1.2/24	00:22:BD:F8:19:FF	9216	vlan-401	Local
BGP Peer 10.2.1.4- Node-101/1/12		Pod-1/Node-101/eth1/12			10.2.1.1/24	10.2.1.2/24	00:22:8D:F8:19:FF	9216	vlan-401	Local
BGP Peer 10.2.1.4- Node-101/1/13		Ded 1/Nede 101/eth/1/12			10.2.11/24	10 21 2/24	00-22-00-59-10-55	0.216	vian_401	Local
BGP Peer 10.2.1.5- Node-101/1/11		Pou-invoue-ioneuninis			10.2.1.1/24	10.2.1.2724	00-22-00-10-10-11	5210	viair-401	Local
BGP Peer 10.2.1.5- Node-101/1/12										
BGP Peer 10.2.1.5- Node-101/1/13										
BGP Peer 10.2.1.6- Node-101/1/11										
F BGP Peer 10.2.1.6- Node-101/1/12										
BGP Peer 10.2.1.6- Node-101/1/13										
> External EPGs										
> Route map for import and export route control										
>L3DOM_F5_01	- PI									
> 🚹 L3out-osp_shared								_		
> 🚹 default								Sho	w Usage	
> 🚞 SR-MPLS VRF L3Outs										

- 20. すべての BGP 接続プロファイル が、[論理インターフェイスプロファイル (Logical Interface Profile)]の下のリーフ側に表示されることに注意してください(この例では、インターフェイスごと に 3 つの BGP ピアを考慮した 9 つの BGP 接続プロファイルがあります)。
- 21. [テナント(Tenants)] > [共通(common)] > [ネットワーキング(Networking)] > [ネットワーク (Networking)] > [L3Outs (L3Outs)] > [L3Out 名(L3Out Name)] (この例では、 Cluster_01_PA_L3Out) > [論理ノードプロファイル(Logical Node Profiles)]の順に選択します。
- **22.** 右クリックし、【ノードプロファイルの作成(Create Node Provile)】を選択します。これにより、2 番目のリーフ スイッチのノード プロファイルが作成されます。
- **23. [名前 (Name)**]を指定し、[+] をクリックして ノード の詳細を追加します (この例では、名前は Cluster_01_PA_102_NP になります)。

78 / 92 ページ シスコ社外秘

Create Node Pi	rofile				\bigotimes
Name:	Cluster_01_PA_102_NP				
Description:	optional				
Target DSCP:	Unspecified V				
BGP Timers:	select a value				
Nodes:					+
	Node ID	Router ID	Static Routes		
BGP Peer Connectivity Profiles:					+
	Peer IP Address	Peer Controls			
			Cancel	lubmit	

24. ノード識別子 と ルータ識別子を指定します。[ループバック アドレスとしてルーター識別子を使用する (Use Router ID as Loopback Address)] チェックボックスをオフにして、[OK] をクリックします。 この例では、ノード識別子は **102**、ルータ識別子は **2.2.2.2** です。

Select Node					\times
Node ID	: LEAF2 (Node-102)	\sim			
Router ID	: 2.2.2.2				
Use Router ID as Loopback Address	:				
Loopback Addresses:					+
	IP				•
Static Routes:					+
	IP Address	Description	Next Hop IP	Track Policy	
				,	

- 25. [ノード プロファイル (Node Profile)] ページで [送信 (Submit)] をクリックします。
- 26. [テナント(Tenants)] > [共通(common)] > [ネットワーキング(Networking)] > [L3Outs (L3Outs)] > [L3Out 名(L3Out Name)](この例では、Cluster_01_PA_L3Out)、>[論理ノード プロファイル(Logical Node Profiles)](この例では、Cluster_01_PA_102_NP)、[論理 インター フェイス プロファイル(Logical Interface Profiles)]の順に選択します。
- 27. 右クリックし、【インターフェイス プロファイルの作成(Create Interface Profile)】を選択します。
- **28. [名前 (Name)**]を指定し、[SVI] タブを選択します(この例では、名前は Cluster_01_PA_102_IFP です)。

Create Interface Profile

STFD	1>	Id	entity	
SIEP	-	ıu	CIILLI	ł

STEP 1 > Identity					1. Identity
Name:	Cluster_01_PA_102_IFP				
Description:	optional				
		Routed Sub-Interfaces	Routed Interfaces	SVI	Floating SVI
SVI Interfaces					1 +
Path	IP Address	MAC Address	MTU (bytes)	

Config Protocol Profiles: Config Advance Protocol:

29. + をクリックして、SVI インターフェイスを作成します。

 \otimes

Select SVI

Path Type:	Port Direc	et Port Channe	I Virtual Port	Channel)		
Node: LE	EAF2 (Node-102)	~					
ex:	topology/pod-1/node	-1					
Path: et: ex:	topology/pod-1/path	s-101/pathep-[eth	→ n1/23]				
Description:	optional						
Encap:	VLAN 🗸 401						
Encap Scope: (VRF Loca	er Value					
Auto State:	disabled	enabled					
Mode: (Trunk (Native)	Trunk	Access (Untagg	ed)			
IPv4 Primary / IPv6 Preferred Address:	10.2.1.3/24						
Link-Local Address:							
IPv4 Secondary / IPv6 Additional Addresses:				+			
	Address	IPv6 DAD	Enable for DHCP Relay				
	10.2.1.1/24	enabled	Disabled				
MAC Address:	00:22:BD:F8:19:FF	-					
MTU (bytes):	9216						
Target DSCP:	Unspecified	\sim					
External Bridge Group Profile:	select an option	\sim					
BGP Peer Connectivity Profiles:						1	+
	Peer IP Address		Peer Controls				
	10.2.1.4						
	10.2.1.5						
	10.2.1.6						
Rogue Exception MAC Group:	select an option	\sim					

- 30. [パスタイプ (Path Type)]をセレクトし、[Node]、[Path]、[Encap VLAN ID]、[IPV4 Primary Address]、[IPV4 Secondary Addresses]、[MTU]、および [BGP ピア接続プロファイル (BGP Peer Connectivity Profiles)]を指定し、ページの下部にある [OK] をクリックします (この例では、パス タイプ (Path type) はポート (Port)、ノードは 102、パスは eth1/11、Encap VLAN ID は 401、IPV4 プライマリ アドレスは 10.2.1.3/24、IPV4 セカンダリ アドレスは 10.2.1.1/24、MTU は 9216 バ イト、BGP ピア IP は 10.2.1.4 です。.1.5 および 10.2.1.6、BGP AS 番号は 65002)です。
- **31.** 残りのインターフェイスに対してステップ **29** とステップ **30** を繰り返し、[完了(Finish)] をクリッ クします(この例では、インターフェイス eth1/12 と eth1/13)。

 (\mathbf{X})

common (*) (=) (©)	Logical Interface Profile - Clus	ter_01_PA_102_IFP							0
V 🖿 L3Outs								Della	•
✓								Policy	Faults History
Logical Node Profiles					General	Routed Sub-Interfac	es Routed	Interfaces	SVI Floating SVI
Cluster_01_PA_101_NP									
Cluster_01_PA_102_NP									0 +
> 🧮 Configured Nodes									☆ +
V 🖿 Logical Interface Profiles	 Path 	Side A IP	Side B IP	Secondary IP Address	IP Address	MAC Address	MTU (bytes)	Encap	Encap Scope
Cluster_01_PA_102_IFP	Pod-1/Node-102/eth1/11			10.2.1.1/24	10.2.1.3/24	00:22:BD:F8:19:FF	9216	vlan-401	Local
BGP Peer 10.2.1.4- Node-102/1/11	Pod-1/Node-102/eth1/12			10.2.1.1/24	10.2.1.3/24	00:22:BD:F8:19:FF	9216	vlan-401	Local
BGP Peer 10.2.1.4- Node-102/1/13	Pod-1/Node-102/eth1/13			10.2.1.1/24	10.2.1.3/24	00:22:BD:F8:19:FF	9216	vlan-401	Local
BGP Peer 10.2.1.5- Node-102/1/11									
BGP Peer 10.2.1.5- Node-102/1/12									
BGP Peer 10.2.1.5- Node-102/1/13									
BGP Peer 10.2.1.6- Node-102/1/11									
BGP Peer 10.2.1.6- Node-102/1/12									
BGP Peer 10.2.1.6- Node-102/1/13									
> 🧮 External EPGs									
> Route map for import and export route control									
> 🚹 L3DOM_F5_01									
> 1 L3out-osp_shared							Show	Lisage	
> 🐽 default							C SHOW	oluştı	

- 32. APIC の上部のナビゲーション メニューから、[テナント(Tenants)]>[共通(common)]>[ネット ワーキング(Networking)]>[L3Outs(L3Outs)]>[L3Out 名(この例では、 Cluster_01_PA_L3Out)]>[外部 EPG(External EPGs)]の順に選択します。
- **33**. 右クリックし、**[外部 EPG の作成(Create External EPG)]**を選択します。 名前 (この例では **Cluster_01_PA_EXT_EPG**)を指定します。
- **34. [+]** をクリックし、ACI リーフによってアドバタイズされる(または受信される) サブネット をこの L3Out をビアて SLB MUX VM に追加します(この例では、IP サブネット 0.0.0.0/0 が ACI リーフによ ってアドバタイズされるため、エクスポート ルート制御サブネットとしてマークされます))。

common	090	External EPG - Clu	uster_01_P	A_EXT_EPG	3									Q
> Application Profiles									Policy	Operational	Health	Faulte	Histor	~
Networking Rridge Domains									Policy	operational	Treatur	Taults	1113101	y
							General	Contracts	Inherit	ted Contracts	Subject Lab	els EF	G Labe	ls
												Ó		(e_
/ = 120uts												0	- /	
Cluster 01 PA 1 20ut		Properties rarger DSCP.	unspecifiea											
V D Logical Node Profiles		Configuration Status: a	pplied											
> E Cluster_01_PA_101_NP		Configuration Issues:												
Cluster_01_PA_102_NP		Preferred Group Member:	Exclude	Include										1
🗸 🚞 External EPGs		Intra Ext-EPG Isolation:	Enforced											
Cluster_01_PA_EXT_EPG		Subnets:										Ĩ	1 + 1	
Route map for import and export route	e control		 IP Address 		Scope	Name		Aggregate		Route Control Profile	Route	Summarizati	on	
> 🛧 L3DOM_F5_01											Policy			
> 👚 L3out-osp_shared			0.0.0.0/0		Export Route Control Subnet									
> 合 default			172.16.1.0/23		External Subnets for the External EPG	Public_VIP_F	Pool							
> 🚞 SR-MPLS VRF L3Outs														
> 🚞 Dot1Q Tunnels														
> 🚞 Contracts														
> 🚞 Policies										External EPG	Cluster 01 PA	EVT EPG		
> 🚞 Services										External EPG	- crastel_01_P/	CENTERO		
E Security										Show Usag	Res			
DIR Address Deals														

パブリック VIP プールなどの SLB MUX VM によってアドバタイズされるサブネットは、外部 EPG の [サブネ ット (Subnet)] セクションに追加し、外部 EPG の外部サブネットとしてマークできます (この例では、IP サ ブネット 172.16.1.0/23 はパブリック VIP として設定されます)。 SLB MUX VM のプール。そのため、Cisco ACI リーフで 外部サブネットとしてマークされます)。

前のセクションで説明したように<u>コントラクトを構成</u>します。L3Out 外部 EPG と他の L3Out 外部 EPG または ACI ファブリックの EPG 部分との間のトラフィックを許可するには、コントラクトが必要です。

コントラクトは、次の経路から **外部 EPG** に追加できます。[テナント(Tenants)]>[共通(common)]> [ネットワーキング(Networking)]>[L3Outs(L3Outs)]>[L3Out 名(L3Outs Name)](この例では、 Cluster_01_PA_L3Out)>[外部 EPG(External EPGs)]>[外部 EPG 名(External EPG Name)(この例で は、Cluster_01_EXT_EPG)]>[ポリシー(Policy)]、[コントラクト(Contracts)]>[提供されたコントラ クトの追加、または消費されるコントラクトの追加) (Add Provided Contract or Add Consumed Contract)]の順に選択します。

Azure Stack HCI VNET およびゲートウェイ VM 接続用の Cisco ACI 構成

前のセクションでは、Azure Stack HCI アンダーレイ ネットワークを構築するための EPG と L3Out の展開に ついて説明しました。このセクションでは、Azure Stack HCI に展開されたお客様のワークロードをサポート するように Cisco ACI を構成する方法について説明します。この例では、Cisco ACI テナント、VRF、および AWS パスの拡充 HCI VNET に接続する L3Out が構成されています。構成手順は次のとおりです。

- 1. APIC の上部のナビゲーションメニューから、[テナント(Tenants)]>[テナントの追加(Add Tenant)]の順に選択します。
- 2. [テナントの作成(Create Tenant)]ダイアログボックスで、名前(HCI1_tenant1 など)を指定します。
- 3. **[VRF 名 (VRF Name)**] フィールドに VRF 名を入力し、**[完了 (Finish)**] をクリックします(例: **VRF1**)。

cisco APIC (LAB3-S2)		
System Tenants Fabric Virtual Ne	tworking Admin Operation	ons Apps Integrations
ALL TENANTS Add Tenant Tenant Search: nam	e or descr common HC	Cl1_tenant1 mgmt infra
HCI1_tenant1	Create VRF	8
> C► Quick Start </th <th>STEP 1> VRF</th> <th>1. VRF</th>	STEP 1> VRF	1. VRF
> 🖬 Application Profiles	Name:	c VRF1 e
✓	Alias:	e e
> 🚞 Bridge Domains	Description:	: optional
VRFs		
> 🖿 L2Outs	Annotations:	: 🕀 Click to add a new annotation
> 🖿 L3Outs	Policy Control Enforcement Preference:	Enforced Unenforced
> 🚞 SR-MPLS VRF L3Outs > 🚞 Dot1Q Tunnels	Policy Control Enforcement Direction:	c Egress Ingress Mixed policy
> 💳 Contracts	BD Enforcement Status:	
> 🧮 Policies	Endpoint Retention Policy:	This notice only applies to remote
> 🖿 Services	Monitoring Policy:	L3 entries
	Divis Labels.	enter names separated by comma
	Transit Route Tag Policy:	C select a value
	IP Data-plane Learning:	; Disabled Enabled
	Create A Bridge Domain:	
	Configure BGP Policies:	
	Configure OSPF Policies:	
	Configure EIGRP Policies:	
		Previous Cancel Finish

- **4.** 左側のナビゲーション ウィンドウで、**[ネットワーク (Networking)]>[L3Outs (L3Outs)]**の順に 選択します。
- 5. 右クリックし、[L3Out の作成(Create L3Out)]を選択します。
- 6. [名前 (Name)] フィールドで、名前 (例: VNET01_L3Out) を指定し、VRF 名 (この例では VRF1) を選択し、ドロップダウンリストから以前に作成した L3 ドメイン (この例では HCI_EXT_L3DOM) を選択します。
- 7. [BGP] チェックボックスをオンにし、[次へ (Next)]をクリックします。

CISCO APIC (LAB3-S2)	pra	tnika (
System Tenants Fabric V	Create L3Out	\times
ALL TENANTS Add Tenant Tenant Sea	1. Identity 2. Nodes And Interfaces 3. Protocols 4. External EPG	
HCI1_tenant1		
Outick Start Outick Outi	Protocol Protocol	đ
	Previous Cancel Next	

8. 【デフォルトを使用(Use 活用 Defaults)】 チェックボックスをオフにして、【ノード プロファイル名 (Node Profile Name)】 フィールドに名前を手動で指定します(この例で は VNET01_NP) <u>。</u>

cisco APIC (LAB3-S2)								pratnika
System Tenants Fabric V	Create L3Out							8
ALL TENANTS Add Tenant Tenant Sea				1	. Identity	2. Nodes And Interf	aces 3. Protocols	4. External EPG
HCI1_tenant1								
 Oulck Start HCI1_tenant1 Application Profiles Networking Bridge Domains VRFs L2Outs L3Outs SR-MPLS VRF L3Outs Dot1Q Tunnels 	Use Defaults: VNE Node Profile Name: VNE Layer 3: Layer 3: Layer 2: P Nodes Node iD LEAF1 (Node-101)	rol_tol_NP erface Sub-Interface rt Virtual Port Channel Router ID VIIII VIIII	SVI Floa Direct Port C	ting SVI thannel	55	+ Hide Interfaces		
> 🔤 Contracts				any Loopback				
> E Services	Interface eth1/11 Ex: eth1/1 or topology/pod- 1/pather-101/pather-[eth1/23]	Interface Profile Name VNET01_101_IFP	Encap VLAN	501 Integer Value	MTU (bytes) 9216	IP Address 10.10.1.2/29 address/mask	•	
	Interface eth1/12 Ex: eth1/1 or topology/pod- 1/paths-101/pathep-[eth1/23]	Interface Profile Name VNET01_101_IFP	Encap VLAN	501 Integer Value	MTU (bytes) 9216	IP Address 10.10.1.2/29 address/mask		
	Interface eth1/13 Ex: eth1/1 or topology/pod- 1/paths-101/pathep-[eth1/23]	Interface Profile Name VNET01_101_IFP	Encap VLAN ~	501 Integer Value	MTU (bytes) 9216	IP Address 10.10.1.2/29 address/mask	•	
							Previous	Cancel Next

- 9. [インターフェイス タイプ (Interface Types)] セクションで、レイヤ 3 の場合は [SVI] 、レイヤ 2 の場合は [ポート (Port)] を選択します。
- [ノード (Nodes)] セクションで、最初のリーフ スイッチに関連するすべての詳細を入力します(この例では、ノード識別子は Node-101、ルータ識別子は 1.1.1.1、ループバックアドレスは 10.10.10.10)。

- **11.2**番目の行の + をクリックして、同じノードにインターフェイスを追加します(この例では、1 つのリ ーフスイッチ、eth1/11、1/12、および 1/13 の 3 つのインターフェイスに接続している 3 つのサー バーがあります)。
- ドロップダウン リストから、サーバーに接続するインターフェイスを選択し、【インターフェイス プロファイル名 (Interface Profile Name)】、[Encap]、[Encap 値 (Encap value)】、[MTU (MTU)】、および [IP アドレス (IP address)】を指定します。Azure Stack HCI サーバーは最大 MTU サイズを9174 として使用するため、TOR スイッチで設定される MTU は 9174 と同じかそれ以上である必要があります (この例では、値は VNET01_101_IFP、VLAN、501、9216、および 10.10.1.2/29 です)。
- 13. 最初のノードに属するすべてのインターフェイスに同じ値を入力します。
- 14. 最初の行の [+] をクリックしてノードを追加し、2 番目のリーフスイッチに関するすべての詳細を入力 します(この例では、ノード識別子は102、ルータ識別子は2.2.2.2、ループバックアドレスは 10.10.10.20)。
- 15. + をクリックして、2 番目のノードの下にインターフェイスを追加します(この例では、 Azure Stack HCI サーバーに接続する 2 番目のリーフに 3 つのインターフェイス eth1/11、eth1/12、および eth1/13 があります)。
- ドロップダウンリストから、サーバーに接続するインターフェイスを選択し、【インターフェイス プロファイル名 (Interface Profile Name)】、[Encap]、[Encap 値]、[MTU]、および [IP アドレス] を指定します(この例では、値は VNET01_102_IFP、VLAN、501、9216、および 10.10.1.3/29)。

Node ID LEAF2 (Node-102)	Router IE 2.2.2.2		Loopback Address 10.10.10.20 Leave empty to not co any Loopback	onfigure	+ Hide Interfaces		
Interface eth1/11 Ex: eth1/1 or topology/pod- 1/paths-101/pathep-[eth1/23]	Interface Profile Name VNET01_102_IFP	Encap VLAN	S01 Integer Value	MTU (bytes) 9216	IP Address 10.10.1.3/29 address/mask	•	
Interface eth1/12	Interface Profile Name VNET01_102_IFP	Encap VLAN	✓ 501 Integer Value	MTU (bytes) 9216	IP Address 10.10.1.3/29 address/mask	۲	
nterface eth1/13 ix: eth1/1 or topology/pod- /paths-101/pathep-[eth1/23]	Interface Profile Name VNET01_102_IFP	Encap VLAN	501 Integer Value	MTU (bytes) 9216	IP Address 10.10.1.3/29 address/mask	÷	

- **17.**[次へ (Next)]をクリックします。
- 18. [ループバック ポリシー(Loopback Policies)] セクションに BGP 関連情報を入力し、[インターフェ イス ポリシー(Interface Policies)] セクションを空白のままにします。
- **19. ピアアドレス**を入力します。これは、VNET 内のゲートウェイ サブネットからゲートウェイ VM にアドレス です (この例では、**192.168.1.2)**。
- EBGP マルチホップ TTL を入力します。eBGP ピアは直接接続されていないため、この値は1より大きくする必要があります(ピアリングは直接接続された IP アドレス間ではないため、1より大きくする必要があります。この例では、4として設定されています。)
- **21. Remote ASN** を入力します。これは、 Azure Stack HCI VNET で設定された BGP ASN 値になります (この例では、 **65201 として設定されます**)。

22. [次へ(Next)] をクリックします。

APIC (LAB3-S	52)							pra
System Tenants Fabric	Create L3Ou	t						8
ALL TENANTS Add Tenant Te				1. Ide	ntity 2. Nodes	And Interfaces	3. Protocols	4. External EPG
HCI1_tenant1	Protocol Associa	ations						1
> 🕩 Quick Start	BGP							
✓	Loopback Pr	olicies						
> 🚞 Application Profiles	Loopbuokt							
✓	Node Profile	: VNET01_NP						
> 🚞 Bridge Domains						Hide Policy 🗌		
> 🖿 VRFs	Nodes	Peer Address	EBGP Multihop TTL	Remote AS	N			
> 🖿 L2Outs	101,102	192.168.1.2	4	65201	\Diamond			
🖿 L3Outs								
> 🚞 SR-MPLS VRF L3Outs	Interface Po	licies						
> 🚞 Dot1Q Tunnels	Node ID: 10	1						
> 🧮 Contracts	11000010-10					Llide Delieu		
> 🧰 Policies	Interface	Peer Address	EBGP Multihop TTL	Remote A	SN	Filde Policy		
> 🧰 Services	1/11							
E Security								
	1/12				\Diamond			
	1/13				<u>^</u>			
	Node ID: 10	2						
	100010-10	da.				Hide Policy		
	Interface	Peer Address	EBGP Multihop TTL	Remote A	SN	The Policy		
	1/11				\Diamond			
							Draviaua	
							Can	Next

23. [名前 (Name)] フィールドに、外部 EPG の名前 (この例では VNET01_EXT_EPG) を入力します。

24. + をクリックして、この L3Out をビアてアドバタイズまたは受信するサブネットを追加します。VNET の eBGP がトップオブラックスイッチとピアリングした後、ゲートウェイ VM は VNET サブネット全体 をトップオブラックスイッチにアドバタイズするします(この例では、 192.168.1.0/24 は ACI リーフ スイッチによって受信される VNET サブネットであるため、外部 EPG の外部サブネットとしてマーク されています。ACI リーフ スイッチは、Azure Stack HCI VNET が Azure Stack HCI 外部の外部ネット ワークに到達するための唯一の出口パスであるため、0.0.0.0/0 が Azure Stack HCI VNET にアドバタ イズされ、エクスポート ルート制御サブネットとしてマークされます。

CISCO APIC (LAB3-S	52)						prat
System Tenants Fabric	Create L3Out						8
ALL TENANTS Add Tenant Te				1. Identity	2. Nodes And Interfaces	3. Protocols	4. External EPG
HCI1_tenant1	External EPG						
> C Quick Start HCI1_tenant1 > Application Profiles	The L3Out Network or EPG for applying contr in the fabric.	External EPG is used fracts. Route control pol	or traffic classification, co icies are used for filtering	ontract association dynamic routes e	ns, and route control policies. C exchanged between the ACI fat	Classification is matchin pric and external device	g external networks to this s, and leaked into other VRFs
🗸 🖿 Networking		Name: VNET01_EXT_EP	G				
> 🚞 Bridge Domains	Provided (Contract: select a value					
> 🖿 VRFs	Consumed (Contract: select a value					
> 🖿 L2Outs	Default EPG for all external n	etworks: 🔲					
L3Outs	Subnets						
> 🔤 SR-MPLS VRF L3Outs							m +
> Dot1Q Tunnels	IP Address	Scope	Name	Age	gregate Rout	te Control Profile	Route Summarization
> Contracts	192.168.1.0/24	External Subnets for th	e Exter				1 0103
> Policies	0.0.0/0	Export Route Control S	ubnet				
> Services							
Security							
						Previous	Cancel Finish

- **25.** [終了 (Finish)]をクリックします。コントラクトは、トラフィック フローに基づいて後の段階で追加 できます。
- 26. [テナント(Tenants)] > [HCl1_tenant1] > [ネットワーキング(Networking)] > [L3Outs] > [L3Out Name] (この例では VNET01_L3Out) > [Logical Node Profiles] (この例では VNET01_NP) > [Logical Interface Profiles] > [Interface Profile Name] (この例では VNET01_101_IFP) > [Policy] > [SVI] の順に選択します。

HCI1_tenant1	001	Logical Interface Profile - VNET	01_101_IFP							0
> C Quick Start									Dollow	Coulto Mistory
✓ ₩ HCI1_tenant1									Policy	Faults History
> 🚞 Application Profiles						General	Routed Sub-Interfa	ces Routed	Interfaces	SVI Floating SVI
V 🖿 Networking										A +
> 🧮 Bridge Domains										0 -
> 🖿 VRFs										☆ +
> 🚞 L2Outs		 Path 	Side A IP	Side B IP	Secondary IP Address	IP Address	MAC Address	MTU (bytes)	Encap	Encap Scope
V 🚞 L3Outs		Pod-1/Node-101/eth1/11				10.10.1.2/29	00:22:BD:F8:19:FF	9216	vlan-501	Local
✓		Ped-1/blade-101/atb1/12				10.10.1.2/20	00:22:8D:58:10:55	0216	ulan E01	Local
Logical Node Profiles						10.10.1.2/28	00-22-BD-P6-19-PP	9210	vian-501	Local
VNET01_NP		Pod-1/Node-101/eth1/13				10.10.1.2/29	00:22:8D:F8:19:FF	9216	vlan-501	Local
BGP Peer 192.168.1.2										
> Configured Nodes										
Logical Interface Profiles										
VNET01_101_JFP										
> VNET01_102_IFP										
> External EPGs										
> Route map for import and export route	control									
> SR-MPLS VRF L3Outs										
> Dot1Q Tunnels										
Contracts										
> Policies										
> Services										
Security								Show	Usage	

- 27. 最初のインターフェイス(この場合はインターフェイス eth1/11)をダブルクリックします。
- 28. 下にスクロールして + をクリックし、IPV4 セカンダリ/IPv6 追加 アドレス (この場合は 10.10.1.1/29) を追加します。

Policy Faults History 0 ± %-Properties Path: topology/pod-1/paths-101/pathep-[eth1/11] Path Description: Description: optional 501 Encap: VLAN Encap Scope: VRF Auto State: enabled Mode: Trunk (Native) Access (Untagged) IPv4 Primary / IPv6 Preferred Address: 10.10.1.2/29 IPv6 DAD: disabled enabled IPv4 Secondary / IPv6 Additional Addresses: +Enable for IPv6 DAD Address DHCP Relay 10.10.1.1/29 enabled Disabled Link-Local Address: :: MAC Address Show Usage Close

- 29. ページの一番下にある [閉じる] をクリックします。
- 30. 他のインターフェイス(この例では、eth1/12とeth1/13)に対してステップ 27~29を繰り返しま す。

System Tenants Fabric Virtual Networking	Admin Operations Apps	Integrations							
ALL TENANTS Add Tenant Tenant Search: name or descr	common HCl1_tenant1 user1	tn-hshahane test	BR012						
HCl1_tenant1	Logical Interface Profile - VNET	01_101_IFP							0
> C+ Quick Start									U III
✓								Policy	Faults History
> 🖿 Application Profiles					General	Routed Sub-Interface	es Routed In	nterfaces	SVI Floating SVI
V 🚍 Networking	0000								<u> </u>
> 🧮 Bridge Domains									0 -
> 🖿 VRFs									亩 +
> 🛅 L2Outs	▲ Path	Side A IP	Side B IP	Secondary IP Address	IP Address	MAC Address	MTU (bytes)	Encap	Encap Scope
~ El L3Outs	Pod-1/Node-101/eth1/11			10.10.1.1/29	10.10.1.2/29	00:22:8D:F8:19:FF	9216	vlan-501	Local
VNET01_L3Out	Pod-1/Node-101/eth1/12			10 10 11/29	10 10 1 2/29	00:22:8D:E8:19:EE	9216	vlan-501	Local
Logical Node Profiles				1010111/20	1010112/20	00.00.00.00.00.00.00	0010		Lood
VNETO1_NP	Pod-1/Node-101/etn1/13			10.10.1.1/29	10.10.1.2/29	00:22-BD:F8:19:FF	9210	vian-501	Local
BGP Peer 192:168.1.2									
> Configured Nodes									
Logical Interface Profiles									
Victor_loz_irv									
P Route map for import and export route control									
SP-MDI S VDE I 30ute									
Dot10 Tunnels									
> Contracts									
> Policies									
> E Services									
Security									
							Show Us	sage	

31. [テナント(Tenants)] > [HCl1_tenant1] > [ネットワーキング(Networking)] > [L3Outs] > [L3Out Name] (この例では VNET01_L3Out) > [論理ノードプロファイル (Logical Node Profiles)] (この 例では VNET01_NP) > [論理インターフェイス プロファイル (Logical Interface Profiles)]>[イン ターフェイス プロファイル名 (Interface Profile Name)](この例では VNET01_102_IFP)>[ポリシ - (**Policy**)] > [SVI] の順に選択します。

32. Node-102 に対してステップ 27 ~ 30 を繰り返します。(この例では、 eth1/11、 eth1/12、 eth1/ 13、10.10.1.3 が ノード-102 のプライマリ IP アドレスです)。

System Tenants Fabric Virtual Networking	Admin Operations Apps	Integrations							
ALL TENANTS Add Tenant Tenant Search: name or descr	common HCI1_tenant1 user1	tn-hshahane tes	tBR012						
HCI1_tenant1	Logical Interface Profile - VNET	01_102_IFP							0
> C+ Quick Start								Dellas	Coulta Illatari
✓								Policy	Faults History
> Application Profiles					General	Routed Sub-Interfa	ces Route	d Interfaces	SVI Floating SVI
V 🧮 Networking									<u> </u>
> 🧮 Bridge Domains									0 -
> 🧮 VRFs									亩 +
> 🚞 L2Outs	 Path 	Side A IP	Side B IP	Secondary IP Address	IP Address	MAC Address	MTU (bytes)	Encap	Encap Scope
V 🖬 L3Outs	Pod-1/Node-102/eth1/11			10.10.1.1/29	10.10.1.3/29	00:22:BD:F8:19:FF	9216	vlan-501	Local
VNET01_L3Out	Part-1/Node-102/ath1/12			10.10.11/29	10.10.1.3/29	00:22-BD-E8-19-EE	9216	vian-501	Local
V 🔚 Logical Node Profiles				10.10.1.1/2.0	10.10.1.0/2.0	00/02/00/07/07/	0010	vian 501	Local
VNETO1_NP	Pod-1/Node-102/eth1/13			10.10.1.1/29	10.10.1.3/29	00:22:8D:F8:19:FF	9210	vian-501	Local
BGP Peer 192.168.1.2									
> Configured Nodes									
Cogical Internace Profiles									
Control EDCa									
Route map for import and export route control									
> SR-MPLS VRF L3Outs									
> Dot10 Tunnels									
> Contracts									
> 🔤 Policies									
> 🔤 Services									
E Security									
							Shou	v Usage	

33. [テナント(Tenants)]、[HCI1_tenant1]、[ネットワーキング(Networking)]、[L3Outs]、[L3Out Name] (この例では、VNET01_L3Out) > [論理 ノードプロファイル (Logical Node Profiles)] (この例では、VNET01_NP)、[構成ノード (Configured Nodes)]>[ノードパス (Node path)] (この例では、topology/pod-1/node-101) に移動します。。

34. + をクリックして、【静的ルート(Static Route)】を追加します。

System Tenants Fabric Virtual Networking	Admin Operations Apps	Integrations					
ALL TENANTS Add Tenant Tenant Search: name or descr	common HCI1_tenant1 u	user1 tn-hshahane test	BR012				
HCI1_tenant1	Node Association						0
C Quick Start					Dellas	Faulta	
✓					Policy	Faults	History
> 🖿 Application Profiles	8 🗸 🛆 🕐					Ō	<u>+</u> ***
V 🖬 Networking	Properties						
> 🚍 Bridge Domains	Node ID:	topology/pod-1/node-101					
> 🖿 VRFs	Router ID:	1.1.1.1					
> 📥 L2Outs	Use Router ID as Loopback Address:	This setting will be ignored if loopback as	dresses are defined in the table below.				
V 🖿 L3Outs	Loopback Addresses:						+ 1
VNET01_L3Out		▲ IP					
Logical Node Profiles		10.10.10.10					
VIETO1_NP							_
BGP Peer 192.168.1.2	*						
Configured Nodes							
v topology/pod-1/node-101	Static Routes:						+
ARP for VRF-HCI1_tenant1:VRF1		 IP Address 	Description	Track Policy	Next Hop IP		
BGP for VRF-HCI1_tenant1:VRF1				No items have been found.			
> = ND for VRF- HCI1_tenant1:VRF1				Select Actions to create a new item.			
> = topology/pod-1/node-102							
> Logical Interface Profiles							
External EPGs							
VNET01_EXT_EPG							
Route map for import and export route control		Page 0 0f0		Objects Per Page: 15		No Ohier	ets Found
SR-MPLS VHF L3OUIS							
> Dotto tunneis					Show Usage Re		
> Contracts							

- 35. [プレフィックス (Prefix)] フィールドに ゲートウェイ サブネットを追加します (この例では、 192.168.1.0/29 がゲートウェイサブネットです。ゲートウェイ サブネットは VNET サブネットの一部 であることに注意してください)。
- **36.** + をクリックして、 Azure Stack HCI VNET の 論理 IP アドレス を [次のホップのアドレス (Next Hop Addresses)] フィールドに追加します (この例では 10.10.1.6)。

Create Static R	oute			×
Prefix:	192.168.1.0/29			
Description:	optional			
Fallback Preference:	1	\Diamond		
Nexthop Type:	Static Route			
Route Control:	BFD			
Track Policy:	select an option	\sim		
Next Hop Addresses:				+
	Next Hop IP	Preference		
	10.10.1.6	0		
	If there is no next hop address added, will be automatically created.	a NULL interface		
		Cancel Sub	mit	

- 37. 【送信 (Submit)】 をクリックします。
- 38. [テナント(Tenants)]、[HCI1_tenant1]、[ネットワーキング(Networking)]、[L3Outs]、[L3Out Name] (この例では、VNET01_L3Out) > [論理 ノードプロファイル(Logical Node Profiles)] (この例では、VNET01_NP)、[構成ノード(Configured Nodes)] > [ノードパス(Node path)] (この例では、topology/pod-1/node-102) に移動します。
- 39. 手順 34 ~ 37 を繰り返して、2 番目のノードにスタティックルートを追加します。
- **40. 外部 EPG** は、手順 **23** に示すように、ウィザードを使用して作成ビアます。次のパスから作成すること もできます - テナント > HCl1_tenant1 > ネットワーキング > L3Outs > L3Out 名 (この例では、 VNET01_L3Out (> 外部 EPG > 外部 EPG 名 (この例では、VNET01_EXT_EPG)。

HCI1_tenant1	External EPG - VI	NET01_EXT_EPG						Q
> C+ Quick Start						Policy Operational	Health Faulte I	History
✓					-	rolicy operational	ribuiti ruuto r	liator y
> 🧮 Application Profiles				General	Contracts	Inherited Contracts	Subject Labels EPG	Labels
V Networking							<u> </u>	to_
> 🛅 Bridge Domains							0 -	~ ^*
> 🖿 VRFs	Properties pcTag:	32770						
> 🖿 L2Outs	Contract Exception Tag:							
V 🖿 L3Outs	Configured VRF Name:	VRF1						
VNET01_L3Out	Resolved VRF:	uni/tn-HCI1_tenant1/ctx-VF	RF1					
> 🚞 Logical Node Profiles	QoS Class:	Unspecified						
🗸 🚞 External EPGs	Target DSCP:	Unspecified						
VNET01_EXT_EPG	Configuration Status:	applied						
The second se	Configuration Issues:							
> 🚞 SR-MPLS VRF L3Outs	Preferred Group Member:	Exclude Include)					
> 🧮 Dot1Q Tunnels	Intra Ext-EPG Isolation:	Enforced Unenfor	ced					
> 🚞 Contracts	Subnets:		_					+
> 🚍 Policies		 IP Address 	Scope	Name	Aggregate	Route Control Profi	e Route Summarization	
> 🔤 Services							Policy	
Security		0.0.0.0/0	Export Route Control Subnet					
		192.168.1.0/24	External Subnets for the External EPG					
						Show Usage	Reset Su	

前のセクションで説明したように<u>コントラクトの構成</u>します。コントラクトは、L3Out 外部 EPG と他の L3Out 外部 EPG または ACI ファブリックの一部である EPG 間のトラフィックを許可するために必要です。

コントラクトは、次の経路から **外部 EPG** に追加できます。[テナント (**Tenants**)]>[HCl1_tenant1]>[ネッ トワーキング (Networking)]>[L3Outs (L3Outs)]>[L3Out Name (L3Out Name)] (この例では、 VNET01_L3Out)、[外部 EPG (External EPGs)]、[外部 EPG 名 (External EPG Name)] (この例では VNET01_EXT_EPG) > [ポリシー (Policy)]、[コントラクト (Contracts)]>[提供されたコントラクトの追 加 (Add Provided Contract)] または[消費された契約の追加 (Add Consumed Contract)]の順に選択し ます。

HCI1_tenant1	\bigcirc	External EPG	- VNET01_EXT_EPG	;						0
O Quick Start								Policy One	rational Har	Ith Faulte History
V III HCI1_tenant1								Policy Ope	rational rice	ini Paulos Plistoly
> 🚞 Application Profiles							General Contract	s Inherited Co	ntracts Sub	ject Labels EPG Labels
V 🖿 Networking								_		A 4 86
> 🧮 Bridge Domains		V Floatiny		Terrent Aller	Our track Trace	Providend 4	0-0.01	01-1-	l shal	
> 🖿 VRFs		Name	 Tenant 	Tenant Allas	Contract Type	Consumed	QOS Class	State	Label	Add Provided Contract
> 🖿 L2Outs						No items have been fou	nd.			Add Consumed Contract
✓						Select Actions to create a ne	w item.			Add Consumed Contract Interface
✓										Taboo Contract
> 🚞 Logical Node Profiles										Add Intra Ext-EPG Contract
— External EPGs										Delete
VNET01_EXT_EPG	•									
> Route map for import and export route co	ontrol									
> 🔤 SR-MPLS VRF L3Outs										
> 🛅 Dot1Q Tunnels										
> 🚞 Contracts										
> 📰 Policies										
> 🚍 Services										
E Security										

詳細情報

http://www.cisco.com/jp/go/aci

更新履歴

リビジョン	カバレッジ	日付(Date)
初版	 Microsoft Azure Stack HCI 22H2 Cisco ACI Release 6.0(3e) Cisco NX-OS Release 12.1.3b 	12/19/2023
Azure Stack HCl で Microsoft ソフ トウェア定義型ネットワーキング (SDN)を使用した設計例の付録を 追加	Microsoft Azure Stack HCI 22H2Cisco ACI Release 6.0(3e)	07/12/2024

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。