

# NSX-T 管理ガイド

VMware NSX-T Data Center 1.1



vmware®

VMware Web サイトで最新の技術ドキュメントをご確認いただけます。

<https://docs.vmware.com/jp/>

VMware の Web サイトでは、最新の製品アップデートを提供しています。

本書に関するご意見、ご要望をお寄せください。フィードバック送信先：

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

ヴィエムウェア株式会社  
105-0013 東京都港区浜松町 1-30-5  
浜松町スクエア 13F  
[www.vmware.com/jp](http://www.vmware.com/jp)

Copyright © 2017 VMware, Inc. All rights reserved. 著作権および商標.

# 内容

## VMware NSX-T の管理について 6

### 1 NSX-T の概要 7

- データ プレーン 9
- 制御プレーン 9
- 管理プレーン 9
- NSX Manager 10
- NSX Controller 11
- 論理スイッチ 11
- 分散論理ルーター 11
- NSX Edge 12
- トランスポート ゾーン 13
- 主な概念 13

### 2 論理スイッチの作成と仮想マシン接続の設定 17

- BUM フレーム レプリケーション モードの理解 18
- 論理スイッチの作成 19
- レイヤー 2 ブリッジ 20
- NSX Edge アップリンク用の VLAN 論理スイッチの作成 24
- 論理スイッチへの仮想マシンの接続 26
- レイヤー 2 接続のテスト 34

### 3 論理スイッチおよび論理ポートのスイッチング プロファイルの設定 38

- QoS スwitchング プロファイルの理解 39
- ポート ミラーリング スwitchング プロファイルの理解 42
- IP アドレス検出 スwitchング プロファイルの理解 44
- SpoofGuard の理解 45
- スイッチ セキュリティの スwitchング プロファイルの理解 49
- MAC 管理 スwitchング プロファイルの理解 50
- カスタム プロファイルと論理スイッチの関連付け 51
- 論理スイッチ ポートへのカスタム プロファイルの関連付け 52

### 4 Tier-1 分散論理ルーターの設定 54

- Tier-1 分散論理ルーターの作成 55
- Tier-1 分散論理ルーターのダウンリンク ポートの追加 55
- Tier-1 分散論理ルーター上でのルートのアドバタイズの設定 57
- Tier-1 分散論理ルーターのスタティック ルートの設定 58

5	Tier-0 分散論理ルーターの設定	61
	Tier-0 分散論理ルーターの作成	62
	Tier-0 と Tier-1 の接続	63
	VLAN 論理スイッチへの Tier-0 分散論理ルーターの接続	66
	スタティック ルートの設定	69
	BGP 設定オプション	73
	Tier-0 分散論理ルーター上の BFD の設定	78
	Tier-0 分散論理ルーターのルート再配分を有効にする	78
	ECMP ルーティングの理解	81
	IP プリフィックス リストの作成	86
	ルート マップの作成	87
6	ネットワーク アドレス変換	88
	Tier-1 NAT	89
	Tier-0 NAT	95
7	ファイアウォール セクションとファイアウォール ルール	99
	ファイアウォール ルール セクションの追加	100
	ファイアウォール ルール セクションの削除	101
	セクション ルールを有効または無効にする	101
	セクション ログを有効または無効にする	101
	ファイアウォール ルールについて	102
	ファイアウォール ルールの追加	103
	ファイアウォール ルールの削除	106
	デフォルトの Distributed Firewall ルールの編集	107
	ファイアウォール ルールの順序の変更	108
	ファイアウォール ルールのフィルタ	108
	ファイアウォールからのオブジェクト除外	109
8	グループとサービスの設定	110
	IP セットの作成	110
	IP アドレス プールの作成	111
	MAC セットの作成	111
	NSGroup の作成	112
	サービスとサービス グループの設定	113
9	DHCP	115
	DHCP サーバ プロファイルの作成	115
	DHCP サーバの作成	116
	論理スイッチへの DHCP サーバの接続	117
	論理スイッチからの DHCP サーバの切り離し	117
	DHCP リレー プロファイルの作成	117

- DHCP リレー サービスの作成 117
- 分散論理ルーター ポートへの DHCP サービスの追加 118

## 10 メタデータ プロキシの設定 119

- メタデータ プロキシ サーバの追加 119
- 論理スイッチへのメタデータ プロキシ サーバの接続 120
- メタデータ プロキシ サーバの論理スイッチからの切り離し 121

## 11 運用管理 122

- ライセンス キーの追加 122
- ユーザー アカウントの管理 123
- 証明書の設定 124
- アプライアンスの設定 129
- タグの管理 130
- オブジェクトの検索 130
- リモート サーバの SSH フィンガープリントの検索 131
- NSX Manager のバックアップとリストア 132
- アプライアンスとアプライアンス クラスタの管理 143
- ロギング システム メッセージ 157
- IPFIX の設定 160
- トレースフローによるパケットのパスのトレース 162
- ポート接続情報の表示 163
- 論理スイッチ ポート アクティビティの監視 164
- ポート ミラーリング セッションの開始 164
- ファブリック ノードの監視 166
- サポート バンドルの収集 166

# VMware NSX-T の管理について

『NSX-T 管理ガイド』には、VMware NSX-T<sup>®</sup> のネットワークの設定と管理に関する情報が記載されています。論理スイッチやポートを作成する方法や、階層構造の分散論理ルーターのネットワークを設定する方法などについて説明しています。また、NAT、ファイアウォール、SpoofGuard、グループ化、DHCP の設定方法についても説明しています。

## 対象読者

この情報は、NSX-T の設定を行うユーザーを対象としています。記載されている情報は、読者に Windows または Linux のシステム管理者としての経験があり、仮想マシンテクノロジー、ネットワーク、およびセキュリティの運用に詳しいことを想定しています。

## VMware の技術ドキュメントの用語集

VMware は、新しい用語を集めた用語集を提供しています。VMware の技術ドキュメントで使用されている用語の定義については、<http://www.vmware.com/support/pubs> をご覧ください。

## NSX-T の概要

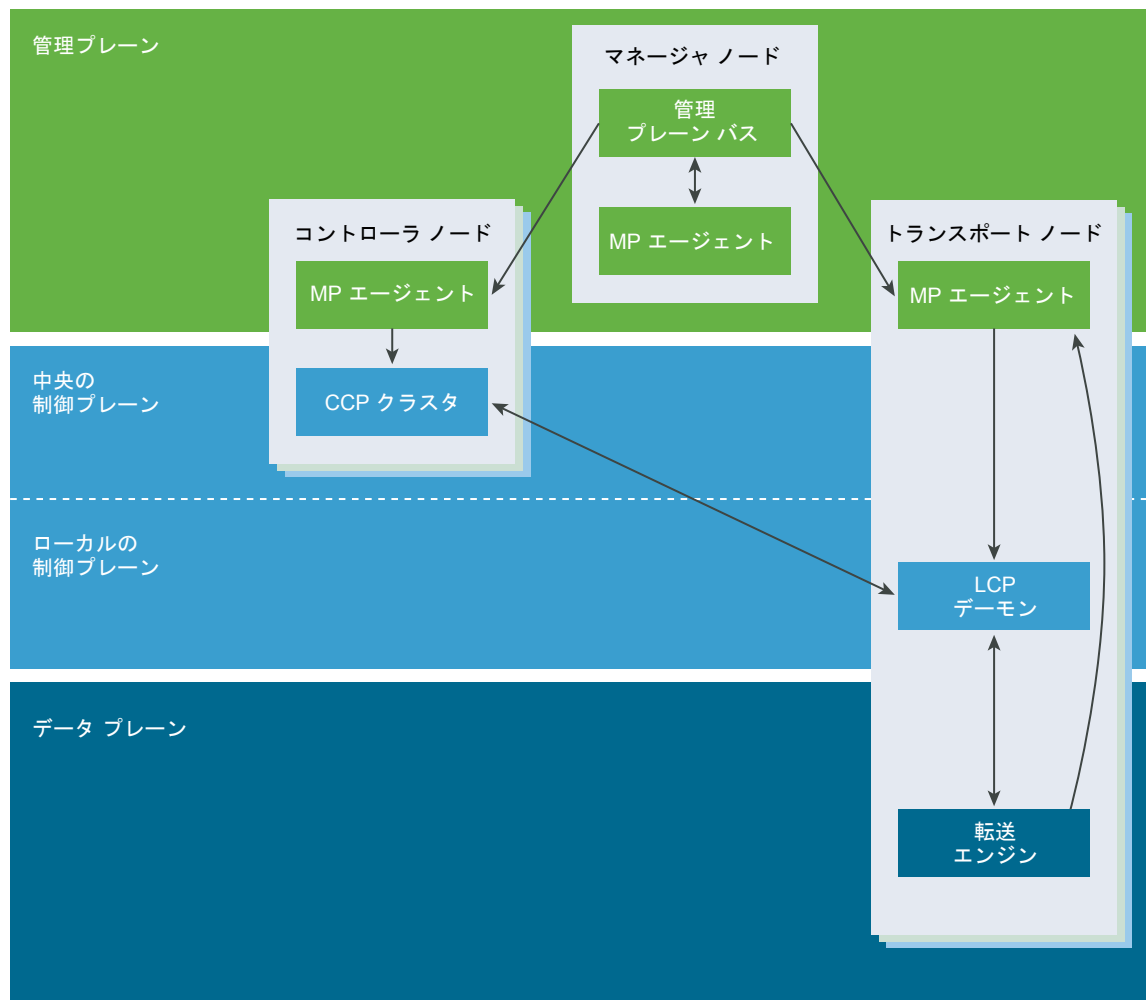
サーバ仮想化では、ソフトウェア ベースの仮想マシンの作成、削除、リストア、およびスナップショットの作成をプログラムによって行います。NSX-T のネットワーク仮想化は、ほぼ同じ方法で、ソフトウェア ベースの仮想ネットワークを作成、削除、リストア、およびスナップショットの作成を行います。

ネットワーク仮想化では、ネットワーク ハイパーバイザーと同等の機能によって、レイヤー 2 からレイヤー 7 までのネットワーク サービス（スイッチング、ルーティング、アクセス制御、ファイアウォール、QoS など）をソフトウェアで完全に再現します。プログラムでこれらのサービスを任意に組み合わせ、独自の隔離された仮想ネットワークをわずか数秒で構築できます。

NSX-T は、管理プレーン、制御プレーン、およびデータ プレーンの 3 つのプレーンを実装することで機能します。それぞれ独立し、相互に連携する 3 つのプレーンは、管理ノード、制御ノード、およびトランスポート ノードの 3 種類のノードに、プロセス、モジュール、およびエージェントのセットとして実装されます。

- すべてのノードで管理プレーン エージェントをホストします。
- NSX Manager ノードは API サービスをホストします。NSX-T インストールはそれぞれ単一の NSX Manager ノードをサポートし、NSX Manager クラスタをサポートしません。
- NSX Controller ノードは、統合制御プレーンのクラスタ デモンをホストします。
- NSX Manager および NSX Controller ノードは、同一の物理サーバ上でホストできます。

- トランスポート ノードは、ローカル制御プレーンのデーモンと転送エンジンをホストします。



この章には、次のトピックが含まれています。

- データプレーン
- 制御プレーン
- 管理プレーン
- NSX Manager
- NSX Controller
- 論理スイッチ
- 分散論理ルーター
- NSX Edge
- トランスポートゾーン
- 主な概念



## データ プレーン

制御プレーンによって入力されたテーブルに基づいて、パケットのステートレス転送/変換を行い、トポロジ情報を制御プレーンに報告して、パケット レベルの統計情報を保持します。

データ プレーンは、物理トポロジと状態、たとえば VIF の場所、トンネルの状態などの情報源です。パケットを 1 つの場所から別の場所に移動する処理を行っているのがデータ プレーンです。また、データ プレーンは、複数のリンク/トンネルの状態を管理し、フェイルオーバーを処理します。遅延やジッターの要件が非常に厳しい場合、パケット単位のパフォーマンスが重要です。データ プレーンはカーネル、ドライバ、ユーザースペース、または特定のユーザースペース プロセスに完全に含まれているとは限りません。データ プレーンは、制御プレーンによって入力されるテーブル/ルールに基づいて、完全にステートレスな転送に制約されます。

データ プレーンには、TCP ターミネーションなどの機能の状態を、ある程度まで保持するコンポーネントが存在する場合もあります。これは、MAC:IP アドレス トンネル マッピングなど、制御プレーンで管理される状態とは異なります。制御プレーンで管理される状態はパケットの転送方法に関するものであるのに対して、データ プレーンで管理される状態はペイロードの操作方法に限られます。

## 制御プレーン

管理プレーンからの構成に基づいてすべての短期的なランタイム状態を算出し、データ プレーン要素からレポートされたトポロジ情報を伝達し、ステートレス構成を転送エンジンにプッシュします。

制御プレーンは、ネットワークへのシグナル伝達と説明されることがあります。固定ユーザー構成がある場合に、データ プレーンをメンテナンスするためにメッセージを処理する際には、制御プレーンでその処理を行います。たとえば、仮想マシン (VM) の vMotion に応答するのは制御プレーンの役割ですが、仮想マシンを論理ネットワークに接続するのは管理プレーンの役割です。制御プレーンは、データ プレーン要素からのトポロジ情報のリフレクタとして機能することがよくあります (VTEP 用の MAC/トンネル マッピングなど)。その他の場合、制御プレーンはいくつかのデータ プレーン要素から受信したデータを処理して、いくつかのデータ プレーン要素を構成 (または再構成) します。たとえば、VIF ロケータを使用して、トンネルの正しいサブセットメッシュを計算し、確立します。

制御プレーンが処理するオブジェクトのセットには、VIF、論理ネットワーク、論理ポート、論理ルーター、IP アドレスなどが含まれます。

制御プレーンは、NSX-T で 2 つの部分に分けられます。中央制御プレーン (CCP) は NSX Controller クラスタ ノードで実行され、ローカル制御プレーン (LCP) は制御対象のデータ プレーンに隣接するトランスポート ノードで実行されます。中央制御プレーンは、管理プレーンからの構成に基づいていくつかの短期的なランタイム状態を算出し、データ プレーン要素からレポートされた情報を、ローカル制御プレーンを介して伝達します。ローカル制御プレーンは、ローカルリンク ステータスを監視し、データ プレーンおよび CCP から得た最新情報に基づいて最も短期的なランタイム情報を算出し、ステートレス構成を転送エンジンにプッシュします。LCP は、それをホストするデータ プレーン要素に依存します。

## 管理プレーン

管理プレーンはシステムへの単一の API エントリ ポイントで、ユーザー設定の維持とユーザー クエリの処理のほか、システム内の管理プレーン、制御プレーン、データ プレーンのすべてのノードの操作を行います。

NSX-T では、ユーザー設定のクエリ、変更、維持に関するものはすべて管理プレーンの担当となり、その設定を適切なデータ プレーン要素に広めるのは制御プレーンの担当となります。これは、一部のデータが、その存在の段階に応じて、複数のプレーンに属することを意味します。管理プレーンは、制御プレーン、また場合によってはデータ プレーンへの最近のステータスや統計情報のクエリも処理します。

管理プレーンは、設定された（論理）システムの唯一の情報源であり、ユーザーが設定を通じて管理します。変更は、RESTful API または NSX-T のユーザー インターフェイスを使用して行います。

NSX には、すべてのクラスとトランスポート ノードで実行される管理プレーン エージェント (MPA) もあります。ユースケースの例として、中央の管理ノード アドレスの認証情報、パッケージ、統計情報、ステータスなどのブートストラッピング設定があります。MPA は制御プレーンとデータ プレーンから独立して実行でき、プロセスがクラッシュするか、反応しなくなった場合は独立して再起動できますが、同じホストで実行されているため運命をともにする場合もあります。MPA はローカル アクセスとリモート アクセスが可能です。MPA はトランスポート ノード、制御ノード、管理ノードで動作してノード管理を行います。トランスポート ノードでは、データ プレーンに関連するタスクが実行される場合もあります。

管理プレーンでは次のタスクが実行されます。

- 設定のパーシステンス（適切な論理状態）
- 入力検証
- ユーザー管理：ロールの割り当て
- ポリシー管理
- バックグラウンド タスクの追跡

## NSX Manager

NSX Manager は、コントローラ、論理スイッチ、Edge Services Gateway などの、NSX-T コンポーネントの作成、設定、監視を行うためのグラフィカル ユーザー インターフェイス (GUI) と REST API を提供します。

NSX Manager は、NSX-T エコシステムの管理プレーンです。NSX Manager は、NSX-T のネットワーク集中管理コンポーネントで、集約されたシステム ビューを提供します。NSX-T で作成された仮想ネットワークに関連するワークロードの監視とトラブルシューティングの方法を提供します。後述の設定と連携が可能です。

- 論理ネットワーク コンポーネント：論理的なスイッチングとルーティング
- ネットワークと Edge サービス
- セキュリティ サービスと Distributed Firewall：Edge サービスとセキュリティ サービスは、NSX Manager の組み込みコンポーネントとして、または連携するサードパーティ ベンダーから提供されます。

NSX Manager では、組み込みサービスと外部サービスとのシームレスな連携が可能です。組み込みまたはサードパーティに関係なく、すべてのセキュリティ サービスが NSX-T の管理プレーンで展開、設定されます。管理プレーンでは、1 つの画面で複数のサービスの可用性を確認できます。また、ポリシー ベースのサービス チェーン、コンテキスト共有、サービス間イベントを容易に操作できます。これにより、セキュリティ状態の監査を簡素化し、ID ベースの制御（Active Directory やモビリティ プロファイルなど）を効率的に適用できるようになります。

NSX Manager は、コンポーネントの使用を自動化するための REST API エントリ ポイントにもなります。この柔軟なアーキテクチャにより、任意のクラウド管理プラットフォーム、セキュリティ ベンダー プラットフォーム、または自動化フレームワークを通じて、設定と監視に関するあらゆる要素を自動化できます。

NSX-T の管理プレーン エージェント (MPA) は、すべてのノード (ハイパーバイザー) に常駐する NSX Manager のコンポーネントです。MPA は、システムの適切な状態を維持し、また設定、統計、ステータス、リアルタイム データなどのフロー制御以外 (NFC) のメッセージをトランスポート ノードと管理プレーンの間でやりとりする役割を担います。

## NSX Controller

NSX Controller は、仮想ネットワークとオーバーレイ転送トンネルを制御する高度な分散状態管理システムです。

NSX Controller は、可用性に優れた仮想アプライアンスのクラスタとして展開され、NSX-T アーキテクチャ全体における仮想ネットワークをプログラムで展開する役割を担います。NSX-T の中央制御プレーン (CCP) はすべてのデータ プレーン トラフィックから論理的に分離されます。このため、制御プレーンで障害が発生しても、既存のデータ プレーンの処理に影響はありません。トラフィックはコントローラを経由しません。コントローラは、論理スイッチ、分散論理ルーター、Edge 設定など、他の NSX Controller コンポーネントに設定を提供する役割を担います。ネットワークでは、データ転送の安定性と信頼性が、重要な懸念事項です。高可用性と拡張性をさらに向上するために、NSX Controller は 3 インスタンスのクラスタで展開されます。

## 論理スイッチ

NSX Edge プラットフォームの論理スイッチング機能によって、仮想マシンと同じ柔軟性と俊敏性で、独立型の論理 L2 ネットワークを追加できます。

仮想データセンターのクラウド環境には、複数のテナントに跨るさまざまなアプリケーションが存在します。セキュリティ、障害分離、IP アドレス重複の問題回避のために、これらのアプリケーションとテナントは互いに分離させる必要があります。仮想エンドポイントと物理エンドポイントは論理セグメントに接続し、データセンター ネットワーク内の物理的な位置に関係なく、接続を確立できます。これは、ネットワーク インフラストラクチャを、NSX-T のネットワーク仮想化による論理ネットワークから (つまり、基盤ネットワークをオーバーレイ ネットワークから) 切り離すことで実現します。

論理スイッチは、レイヤー 3 の IP アドレス アクセスが可能な多数のホストにわたるレイヤー 2 スイッチ接続を表します。論理ネットワークを一部のホストに制限するか、接続についてカスタムの要件がある場合は、追加の論理スイッチを作成する必要がある可能性があります。

## 分散論理ルーター

NSX-T の分散論理ルーターは、North-South 接続を提供するため、テナントからパブリック ネットワークへのアクセスが可能です。また、同じテナント内の異なるネットワーク間の East-West 接続も提供します。

分散論理ルーターは、従来型のネットワーク ハードウェア ルーターの中で設定が可能な部分です。ハードウェアの機能を複製し、単一のルーター内に複数のルーティング ドメインを作成します。分散論理ルーターは物理ルーターで処理できるタスクの一部を実行します。また、それぞれ複数のルーティング インスタンスやルーティング テーブルを含めることができます。分散論理ルーターの使用は、ルーターの使用率を最大にする効果的な方法です。単一の物理ルーター内の複数の分散論理ルーターで、以前は複数の装置で実行していた処理を実行できるからです。

NSX-T では、2 階層の分散論理ルーター トポロジを作成できます。上位の分散論理ルーターが Tier-0、下位の分散論理ルーターが Tier-1 です。この構成では、プロバイダ管理者とテナント管理者の両者が、それぞれのサービスとポリシーを完全に制御できます。管理者が Tier-0 のルーティングとサービスを制御および設定し、テナント管理者が Tier-1 を制御および設定します。Tier-0 の north 側の端は物理ネットワークとのインターフェイスになり、ここでダイナミック ルーティング プロトコルを設定して、物理ルーターとルーティング情報を交換できます。Tier-0 の south 側の端は複数の Tier-1 ルーティング レイヤーと接続し、これらからルーティング情報を受け取ります。リソースの使用率を最適化するため、Tier-0 レイヤーは物理ネットワークから受け取るルートをすべて Tier-1 にプッシュしませんが、デフォルト情報は提供します。

Tier-1 ルーティング レイヤーの south バウンドは、テナント管理者によって定義された論理スイッチと接続し、その論理スイッチとの間の 1 ホップルーティング機能を提供します。Tier-1 に接続されたサブネットに物理ネットワークからアクセスするには、Tier-0 レイヤー方向のルート再配分を有効にする必要があります。ただし、Tier-1 レイヤーと Tier-0 レイヤーの間に標準的なルーティング プロトコル (OSPF、BGP など) はなく、すべてのルートが NSX-T の制御プレーンを経由します。2 階層のルーティング トポロジは必須ではなく、プロバイダとテナントを分離する必要がない場合は 1 階層のトポロジを作成できます。この場合、論理スイッチは Tier-0 レイヤーに直接接続し、Tier-1 レイヤーはありません。

分散論理ルーターは 2 つのオプションで構成されます。1 つの分散ルーター (DR) と、1 つまたは複数のサービス ルーター (SR) です。

DR は、この分散論理ルーターに接続している仮想マシンのハイパーバイザーに加え、分散論理ルーターがバインドされている Edge ノードにまたがります。機能的には、DR は、この分散論理ルーターに接続している論理スイッチまたは分散論理ルーター、あるいはその両方の間で 1 ホップの分散ルーティングを担います。SR は、ステートフル NAT など、現在は分散式で実装されていないサービスの提供を担います。

分散論理ルーターには DR が必ずあり、次のいずれかの条件を満たす場合は SR があります。

- 分散論理ルーターが Tier-0 ルーターの場合。ステートフル サービスが設定されていない場合を含む。
- 分散論理ルーターが、Tier-0 ルーターにリンクされた Tier-1 ルーターであり、分散型の実装がないサービス (NAT、LB、DHCP など) が設定されている場合。

NSX-T の管理プレーン (MP) が、サービス ルーターを分散ルーターに接続する構成の自動作成を担います。MP は、中継論理スイッチを作成し、VNI を割り当ててから、各 SR と DR にポートを作成し、これらの中継論理スイッチに接続して、SR と DR に IP アドレスを割り当てます。

## NSX Edge

NSX Edge は、ルーティング サービスと NSX-T 環境の外部のネットワークへの接続を提供します。

NSX Edge によって、複数のサブネットにわたっている同一ホスト上に存在する仮想マシンまたはワークロードは、従来のルーティング インターフェイスを経由することなく相互に通信できます。

NSX Edge は、NSX-T ドメインから、Tier-0 ルーターを経由して、BGP またはスタティック ルーティングで外部接続を確立するために必要です。また、Tier-0 または Tier-1 のいずれかの分散論理ルーターでネットワーク アドレス変換 (NAT) サービスが必要な場合は、NSX Edge を展開する必要があります。

NSX Edge ゲートウェイは NAT、ダイナミック ルーティングなどの一般的なゲートウェイ サービスを提供して、分離されたスタブネットワークを共有 (アップリンク) ネットワークへ接続します。NSX Edge は一般的に DMZ やマルチテナントのクラウド環境などに展開されますが、NSX Edge は各テナント用の仮想境界を構築します。

## トランスポート ゾーン

トランスポート ゾーンは、論理スイッチでアクセスできるホストを制御します。トランスポート ゾーンは 1 つ以上のホスト クラスタにまたがって設定できます。トランスポート ゾーンでは、特定のネットワークを使用できるホストと仮想マシンを指定します。

トランスポート ゾーンは、物理ネットワーク インフラストラクチャを介して相互に通信できるホストの集合を定義します。この通信は、仮想トンネル エンドポイント (VTEP) として定義されている、1 つ以上のインターフェイスを介して行われます。

2 台のトランスポート ノードが同じトランスポート ゾーンにある場合、両方のトランスポート ノードでホストされる仮想マシンは、同じトランスポート ゾーン内の NSX-T 論理スイッチを認識して、接続できます。これにより、仮想マシンがレイヤー 2/レイヤー 3 に到達できる場合は、仮想マシン同士が互いに通信できるようになります。各仮想マシンが、それぞれ別のトランスポート ゾーン内のスイッチに接続されている場合、それらの仮想マシンは互いに通信できません。トランスポート ゾーンは、レイヤー 2/レイヤー 3 接続性要件に変わるものではありませんが、接続性に制約を加えます。つまり、相互に接続するには、前提条件として同じトランスポート ゾーンに属する必要があります。この前提条件が満たされれば、相互接続は可能になりますが、自動的に通信が可能となるわけではありません。実際に接続を可能にするには、レイヤー 2 および別のサブネットの場合のレイヤー 3 ネットワークの設定と条件が正しく動作している必要があります。

ノードに 1 台以上のホストスイッチが含まれている場合、そのノードはトランスポート ノードとして機能できます。ホスト トランスポート ノードを作成し、トランスポート ゾーンに追加すると、NSX-T によってホストにホストスイッチがインストールされます。ホストが属する各トランスポート ゾーンごとに、別のホストスイッチがインストールされます。ホストスイッチは、仮想マシンを NSX-T 論理スイッチに接続するとき、および NSX-T 分散論理ルーターのアップリンクとダウンリンクを作成するときに使用されます。

## 主な概念

このドキュメントとユーザー インターフェイスで使用されている NSX-T の一般的な概念について説明します。

制御プレーン	管理プレーンからの設定に基づいてランタイム状態を算出します。制御プレーンは、データ プレーン要素からもたらされたトポロジ情報を伝達し、ステートレス設定をフォワーディング エンジンにプッシュします。
データ プレーン	制御プレーンが設定したテーブルに基づいて、パケットのステートレスな転送または変換を行います。データ プレーンはトポロジ情報を制御プレーンに報告し、パケット レベルの統計情報を保持します。
外部ネットワーク	NSX-T の管理対象ではない物理ネットワークまたは VLAN です。NSX Edge を通じて、論理ネットワークまたはオーバーレイ ネットワークを外部ネットワークにリンクできます。例として、お客様のデータセンター内の物理ネットワークや、物理環境内の VLAN などが挙げられます。
ファブリック ノード	NSX-T の管理プレーンに登録され、NSX-T モジュールがインストールされているノードです。ハイパーバイザー ホストまたは NSX Edge を NSX-T のオーバーレイの一部にするためには、NSX-T のファブリックに追加する必要があります。

ファブリック プロファイル	NSX Edge クラスタに関連付けることができる特定の設定を表します。ファブリック プロファイルには、たとえば、停止したピアを検出するためのトンネリング プロパティを含めることができます。
論理ポート出力	仮想マシンまたは論理ネットワークへのネットワーク トラフィックを出力と呼びます。トラフィックがデータセンター ネットワークを離れ、仮想領域に入るためです。
論理ポート入力	仮想マシンからデータセンター ネットワークへのネットワーク トラフィックを入力と呼びます。トラフィックが物理ネットワークに入るためです。
分散論理ルーター	NSX-T のルーティング エンティティです。
分散論理ルーター ポート	論理スイッチ ポート、または物理ネットワークへのアップリンク ポートを関連付けることができる論理ネットワーク ポートです。
論理スイッチ	<p>仮想マシン インターフェイスとゲートウェイ インターフェイスに仮想レイヤー 2 スイッチングを提供する API エンティティです。論理スイッチは、物理レイヤー 2 スイッチに対応する論理スイッチをテナント ネットワークの管理者に提供し、管理者が複数の仮想マシンを共通のブロードキャスト ドメインに接続できるようにします。論理スイッチは、物理ハイパーバイザー インフラストラクチャに依存せず、多数のハイパーバイザーに跨る論理エンティティであり、物理的な場所を問わずに仮想マシンを接続します。このため、テナント ネットワークの管理者が再設定することなく仮想マシンを移行できます。</p> <p>マルチテナントのクラウドでは、各レイヤー 2 セグメントを相互に分離した状態で、多数の論理スイッチを同じハイパーバイザー ハードウェアに並べて配置できます。論理スイッチは分散論理ルーターを使用して接続でき、分散論理ルーターは外部物理ネットワークに接続したアップリンク ポートを提供できます。</p>
論理スイッチ ポート	仮想マシン ネットワーク インターフェイスまたは分散論理ルーター インターフェイスへの接続を確立するための論理スイッチの接続ポイントです。論理スイッチ ポートは、適用されているスイッチング プロファイル、ポートの状態、リンクのステータスを報告します。
管理プレーン	システムへの単一の API エントリ ポイントで、ユーザー設定の維持とユーザー クエリの処理、システム内の管理プレーン、制御プレーン、データ プレーンのすべてのノードの操作を行います。管理プレーンは、ユーザー設定のクエリ、変更、維持も行います。
NSX Controller クラスタ	可用性に優れた仮想アプライアンスのクラスタとして展開され、NSX-T アーキテクチャ全体において、プログラムによる仮想ネットワークの展開を担います。
NSX Edge クラスタ	高可用性の監視に関わるプロトコルと同じ設定を持つ NSX Edge ノード アプライアンスの集合。
NSX Edge ノード	IP アドレス ルーティングと IP アドレス サービスの機能のための処理能力を提供することを機能的目標とするコンポーネント。

**NSX-T ホストスイッチまたは KVM Open vSwitch (OVS)**

ハイパーバイザー上で実行され、物理的なトラフィック転送を行うソフトウェアです。ホストスイッチまたは OVS はテナント ネットワークの管理者から認識できず、各論理スイッチが依存する、基盤となる転送サービスを提供します。ネットワークを仮想化するには、ネットワーク コントローラが、テナントの管理者が論理スイッチを作成、設定したときに定義した論理ブロードキャスト ドメインを形成するネットワーク フロー テーブルを使用してハイパーバイザー ホストスイッチを設定する必要があります。

各論理ブロードキャスト ドメインは、トンネル カプセル化メカニズム Geneve を使用して、仮想マシン間のトラフィックと、仮想マシンと分散論理ルーターの間のトラフィックをトンネリングすることで実装されます。ネットワーク コントローラが、データセンター全体を把握し、仮想マシンの作成、移動、削除に伴ってハイパーバイザー ホストスイッチのフロー テーブルが更新されることを確認します。

**NSX Manager**

API サービス、管理プレーン、エージェント サービスをホストするノードです。

**Open vSwitch (OVS)**

XenServer、Xen、KVM、およびその他の Linux ベースのハイパーバイザーでハイパーバイザー ホストスイッチとして機能するオープン ソース ソフトウェア スイッチです。NSX Edge のスイッチング コンポーネントは OVS に基づいています。

**オーバーレイ 論理ネットワーク**

仮想マシンで認識されるトポロジが、物理ネットワークのトポロジから切り離されるように、レイヤー 3 内のレイヤー 2 を使用して実装された論理ネットワークです。

**物理インターフェイス (pNIC)**

ハイパーバイザーがインストールされている物理サーバ上のネットワーク インターフェイスです。

**Tier-0 分散論理ルーター**

プロバイダ分散論理ルーターは、物理ネットワークへの Tier-0 分散論理ルーターとも呼ばれます。Tier-0 分散論理ルーターは最上位のルーターであり、サービス ルーターのアクティブ/アクティブ クラスタまたはアクティブ/スタンバイ クラスタとして実現できます。分散論理ルーターは BGP を実行し、物理ルーターとピアリングされます。アクティブ/スタンバイ モードでは、分散論理ルーターがステートフル サービスを提供することもできます。

**Tier-1 分散論理ルーター**

Tier-1 分散論理ルーターは、2 番目の分散論理ルーターです。north バウンド接続用に 1 台の Tier-0 分散論理ルーターと接続し、south バウンド接続用に 1 つ以上のオーバーレイ ネットワークと接続します。Tier-1 分散論理ルーターには、ステートフル サービスを提供するサービス ルーターのアクティブ/スタンバイ クラスタを使用できます。

**トランスポート ゾーン**

論理スイッチの最大範囲を定義するトランスポート ノードの集合。トランスポート ゾーンは、同じようにプロビジョニングされた一連のハイパーバイザーと、これらのハイパーバイザー上の仮想マシンを接続する論理スイッチを表します。NSX-T は、論理スイッチで有効になっている機能がわかるため、必要なサポート ソフトウェア パッケージをホストに展開できます。

## 仮想マシン インターフェイス (vNIC)

仮想ゲスト OS と標準の vSwitch または vSphere Distributed Switch の間の接続を提供する、仮想マシン上のネットワーク インターフェイスです。vNIC は論理ポートに接続できます。vNIC は、固有の ID (UUID) で識別できます。

## VTEP

仮想トンネル エンドポイントです。トンネル エンドポイントによって、ハイパーバイザー ホストを NSX-T のオーバーレイに加えることができます。NSX-T のオーバーレイは、パケット内にフレームをカプセル化し、基盤となるトランスポート ネットワーク上でパケットを送信することで、レイヤー 2 ネットワークを既存のレイヤー 3 ネットワーク ファブリック上に展開します。基盤となるトランスポート ネットワークは、別のレイヤー 2 ネットワークである場合と、レイヤー 3 の境界をまたぐ場合があります。VTEP は、カプセル化とカプセル化解除が行われる接続ポイントです。



# 論理スイッチの作成と仮想マシン接続の設定

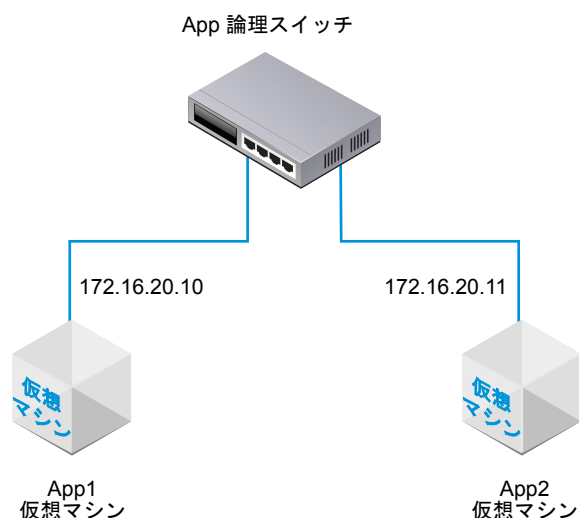
## 2

NSX-T 論理スイッチは、基盤となるハードウェアから完全に分離された仮想環境内で、切り替え機能、ブロードキャスト、不明のユニキャスト、マルチキャスト (BUM) トラフィックを再現します。

論理スイッチは、仮想マシンを接続できるネットワーク接続を提供する点で、VLAN と似ています。同じ論理スイッチに接続された仮想マシンは、ハイパーバイザー間のトンネルで互いに通信できます。各論理スイッチには、VLAN ID のような仮想ネットワーク識別子 (VNI) があります。VLAN と異なり、VNI は VLAN ID の制限を超えて拡張できます。

論理スイッチを追加する場合、構築しているトポロジについての計画を立てることが重要です。

図 2-1. 論理スイッチ トポロジ



たとえば、トポロジは 2 台の仮想マシンに接続された単一の論理スイッチを示します。2 台の仮想マシンのホストやホストクラスタは同じにすることも、別々にすることもできます。例に示す仮想マシンは同じ仮想ネットワーク上にあるため、仮想マシン上で設定された基になる IP アドレスは同じサブネットにある必要があります。

この章には、次のトピックが含まれています。

- [BUM フレーム レプリケーション モードの理解](#)
- [論理スイッチの作成](#)
- [レイヤー 2 ブリッジ](#)
- [NSX Edge アップリンク用の VLAN 論理スイッチの作成](#)

- 論理スイッチへの仮想マシンの接続
- レイヤー 2 接続のテスト

## BUM フレーム レプリケーション モードの理解

各ホスト トランスポート ノードはトンネル エンドポイントです。各トンネル エンドポイントには IP アドレスがあります。これらの IP アドレスは、トランスポート ノードの IP アドレス プールまたは DHCP の設定に応じて、同じサブネットにある場合も別のサブネットにある場合もあります。

異なるホスト上の 2 台の仮想マシンが直接通信する場合、ユニキャストでカプセル化されたトラフィックが、2 つのハイパーバイザーに関連付けられた 2 つのトンネル エンドポイントの IP アドレス間でフラッドを必要とすることなく交換されます。

ただし、レイヤー 2 ネットワークのように、仮想マシンによって送信されたトラフィックのフラッドが必要になる場合があります。これは、同じ論理スイッチに属する他のすべての仮想マシンにトラフィックを送信する必要があることを意味します。これは、レイヤー 2 ブロードキャスト、不明のユニキャスト、およびマルチキャストトラフィック (BUM トラフィック) の場合です。単一の NSX-T 論理スイッチが複数のハイパーバイザーにまたがる場合があることに注意してください。特定のハイパーバイザー上の仮想マシンによって送信された BUM トラフィックを、同じ論理スイッチに接続された他の仮想マシンをホストするリモート ハイパーバイザーにレプリケートする必要があります。このフラッドを有効にするために、NSX-T は 2 つの異なるレプリケーション モードをサポートします。

- 階層型の 2 層 (MTEP と呼ばれることもあります)
- ヘッド (ソースと呼ばれることもあります)

次の例は、階層型の 2 層レプリケーション モードを示したものです。ホスト A には、5000、5001、および 5002 の仮想ネットワーク識別子 (VNI) に接続された仮想マシンがあるとします。VNI は VLAN に似ていますが、各論理スイッチには単一の VNI が関連付けられています。そのために VNI と論理スイッチが同じ意味で使用されることがあります。ホストが VNI 上にあるという場合、ホストにはその VNI を持つ論理スイッチに接続された仮想マシンがある、という意味になります。

トンネル エンドポイント テーブルはホスト VNI 接続を示します。ホスト A は、VNI 5000 のトンネル エンドポイント テーブルを調べ、VNI 5000 上の他のホストのトンネル エンドポイント IP アドレスを決定します。

これらの VNI 接続の一部は、ホスト A のトンネル エンドポイントと同じ IP サブネット (IP セグメントとも呼ばれます) にあります。それぞれの接続に対して、ホスト A は、各 BUM フレームの個別のコピーを作成し、各ホストに直接コピーを送信します。

他のホストのトンネル エンドポイントは、別のサブネットまたは IP セグメントにあります。各セグメントに複数のトンネル エンドポイントがある場合、ホスト A は、レプリケーターとなるエンドポイントを 1 つ指名します。

レプリケーターは、ホスト A から VNI 5000 の各 BUM フレームのコピーを 1 つ受信します。このコピーには、カプセル化ヘッダーにローカルで「Replicate」というフラグが付けられます。ホスト A は、レプリケーターと同じ IP セグメントの他のホストにはコピーを送信しません。VNI 5000、およびそのレプリケーター ホストと同じ IP セグメントにある、レプリケーターが認識している各ホストの BUM フレームのコピーを作成することはレプリケーターの責任になります。

プロセスは VNI 5001 および 5002 に対してレプリケートされます。トンネル エンドポイントのリストおよび生成されるレプリケーターは、VNI によって異なる場合があります。

ヘッドエンド レプリケーションとも呼ばれるヘッド レプリケーションには、レプリケータはありません。ホスト A は、VNI 5000 にある自分が認識している各トンネル エンドポイントの各 BUM フレームのコピーを作成して送信するだけです。

すべてのホスト トンネル エンドポイントが同じサブネット上にある場合、動作に差異はないため、どのレプリケーション モードを選択しても結果は同じです。ホスト トンネル エンドポイントが異なるサブネット上にある場合、階層型の 2 層レプリケーションは複数のホスト間で負荷を分散するのに役立ちます。階層型の 2 層はデフォルトのモードです。

## 論理スイッチの作成

論理スイッチはネットワークの単一の仮想マシンまたは複数の仮想マシンに接続します。論理スイッチに接続された仮想マシンは、ハイパーバイザー間のトンネルを使用して相互に通信することができます。

### 前提条件

- トランSPORT ゾーンが設定されていることを確認します。『NSX-T インストール ガイド』を参照してください。
- ファブリック ノードが NSX-T 管理プレーン エージェント (MPA) および NSX-T ローカル制御プレーン (LCP) に正常に接続されていることを確認します。

GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state` API の呼び出しで、**state** が **success** である必要があります。『NSX-T インストール ガイド』を参照してください。

- トランSPORT ノードがトランSPORT ゾーンに追加されていることを確認します。『NSX-T インストール ガイド』を参照してください。
- ハイパーバイザーが NSX-T ファブリックに追加され、仮想マシンがこれらのハイパーバイザー上でホストされていることを確認します。
- 論理スイッチ トポロジおよび BUM フレーム レプリケーションの概念を理解します。[章 2 「論理スイッチの作成と仮想マシン接続の設定」](#) および [「BUM フレーム レプリケーション モードの理解」](#) を参照してください。
- NSX Controller クラスタが安定していることを確認します。

### 手順

- 1 ブラウザから、NSX Manager (`https://<nsx-manager-ip-address>`) にログインします。
- 2 [スイッチング (Switching)] > [スイッチ (Switches)] を選択します。
- 3 [追加 (Add)] をクリックします。
- 4 論理スイッチの名前を割り当てます。
- 5 論理スイッチのトランSPORT ゾーンを選択します。

同じトランSPORT ゾーンにある論理スイッチに接続された仮想マシンは、相互に通信することができます。

## 6 論理スイッチのレプリケーション モードを選択します。

オーバーレイ論理スイッチにはレプリケーション モード（階層型の 2 層またはヘッド）が必要ですが、VLAN ベースの論理スイッチには必要ありません。

レプリケーション モード	説明
階層型の 2 層	レプリケータは、同じ VNI 内の他のホストへの BUM トラフィックのレプリケーションを実行するホストです。 ホストはそれぞれ、各 VNI でレプリケータとなる 1 つのホスト トンネル エンドポイントを指名します。これは VNI ごとに実行されます。
ヘッド	ホストは各 BUM フレームのコピーを作成し、各 VNI に対して認識している各トンネル エンドポイントにコピーを送信します。

## 7 (オプション) [スイッチング プロファイル (Switching Profiles)] タブをクリックして、スイッチング プロファイルを選択します。

## 8 [保存 (Save)] をクリックします。

NSX Manager のユーザー インターフェイスで、新しい論理スイッチがクリック可能なリンクになります。

### 次のステップ

仮想マシンを論理スイッチに接続します。[「論理スイッチへの仮想マシンの接続」](#)を参照してください。

## レイヤー 2 ブリッジ

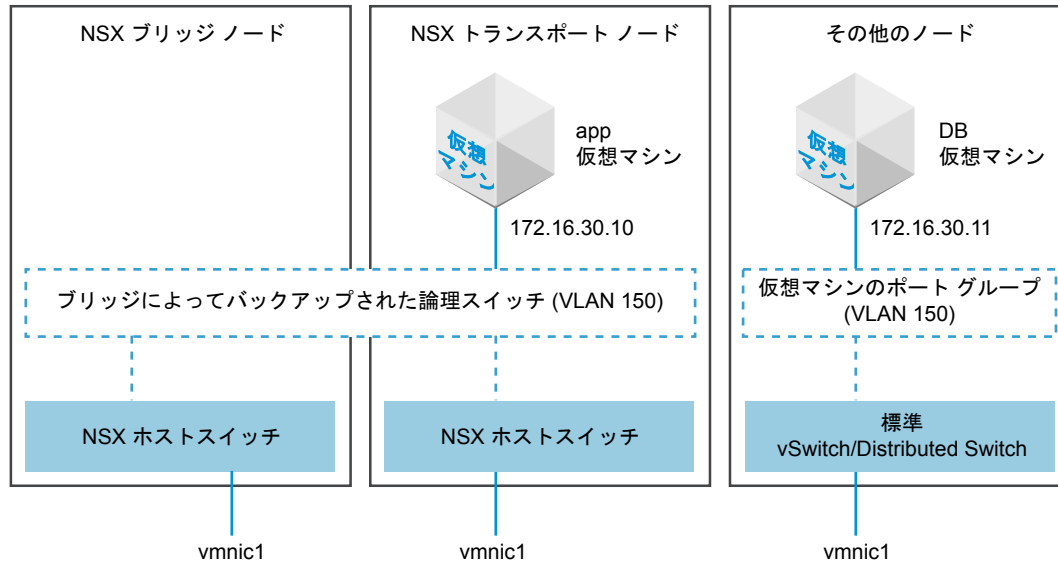
NSX-T 論理スイッチが VLAN によりバックアップされたポート グループへのレイヤー 2 接続を必要とする場合、あるいは NSX-T デプロイの外部に存在するゲートウェイなど、別のデバイスにアクセスする必要がある場合は、NSX-T レイヤー 2 ブリッジを使用することができます。これは、物理ワークロードと仮想ワークロード上でサブネットを分割する必要がある移行シナリオで特に役に立ちます。

レイヤー 2 ブリッジに含まれる NSX-T のコンセプトは、ブリッジ クラスタ、ブリッジ エンドポイントおよびブリッジ ノードです。ブリッジ クラスタはブリッジ ノードの高可用性 (HA) コレクションです。ブリッジ ノードはブリッジ機能を提供するトランスポート ノードです。仮想デプロイと物理デプロイのブリッジに使用される各論理スイッチには VLAN ID が関連付けられています。ブリッジ エンドポイントは、ブリッジ クラスタ ID および関連付けられた VLAN ID など、ブリッジの物理属性を識別します。

この NSX-T のリリースでは、レイヤー 2 ブリッジは、ブリッジ ノードとして機能する ESXi ホストによって提供されます。ブリッジ ノードはブリッジ クラスタに追加された ESXi ホストのトランスポート ノードです。

次の例では、2 つの NSX-T トランスポート ノードは同じオーバーレイ トランスポート ゾーンの一部です。これによって、NSX-T ホストスイッチ（図に示すように NSX-T vSwitch と呼ばれることもあります）を、ブリッジによってバックアップされる同じ論理スイッチに接続することができます。

図 2-2. ブリッジトポロジ



左側のトランスポート ノードはブリッジ クラスタに属し、したがってこれはブリッジ ノードです。

論理スイッチはブリッジ クラスタに接続されているので、ブリッジによってバックアップされる論理スイッチと呼ばれます。ブリッジによるバックアップを可能にするには、論理スイッチを VLAN トランスポート ゾーンではなくオーバーレイ トランスポート ゾーンに置く必要があります。

中央のトランスポート ノードはブリッジ クラスタの一部ではありません。これは標準のトランスポート ノードです。KVM または ESXi ホストの場合があります。図では、「app VM」と呼ばれるこのノード上の仮想マシンはブリッジによってバックアップされる論理スイッチに接続されています。

右側のノードは NSX-T オーバーレイの一部ではありません。これは（図に示すような）仮想マシンを備えた任意のハイパーバイザー、または物理ネットワーク ノードの場合があります。非 NSX-T ノードが ESXi ホストの場合、標準の vSwitch または vSphere 分散スイッチをポート接続に使用することができます。1 つの要件として、ポート接続に関連付けられた VLAN ID はブリッジによってバックアップされる論理スイッチの VLAN ID と一致する必要があります。また、通信はレイヤー 2 で発生するので、2 つの端末装置の IP アドレスは同じサブネットにある必要があります。

すでに述べたように、ブリッジの目的は 2 台の仮想マシン間でのレイヤー 2 通信を可能にすることです。トラフィックが 2 台の仮想マシン間で転送されるときに、トラフィックはブリッジ ノードを経由します。

## ブリッジ クラスタの作成

ブリッジ クラスタは、ブリッジ機能を提供し、高可用性 (HA) に参加するトランスポート ノードのコレクションです。一度に 1 台のトランスポート ノードのみをアクティブにすることができます。NSX-T ブリッジ ノードの複数ノード クラスタがあれば、少なくとも 1 台の NSX-T ブリッジ ノードを常に使用可能な状態にすることができます。ブリッジによってバックアップされる論理スイッチを作成するには、論理スイッチをブリッジ クラスタに関連付ける必要があります。したがって、ブリッジ ノードの数が 1 台の場合でも、ブリッジ クラスタに含める必要があります。

作成したブリッジ クラスタを後で編集し、ブリッジ ノードを追加することができます。

### 前提条件

- ブリッジ ノードとして使用するための少なくとも 1 台の NSX-T トランスポート ノードを作成します。
- ブリッジ ノードとして使用するトランスポート ノードは ESXi ホストである必要があります。ブリッジ ノードでは KVM はサポートされません。
- ブリッジ ノードにはホストされた仮想マシンが含まれないようにすることを推奨します。
- トランスポート ノードは 1 台のブリッジ クラスタにのみ追加することができます。同じトランスポート ノードを複数のブリッジ クラスタに追加することはできません。

### 手順

- 1 NSX Manager ユーザー インターフェイスで、[ファブリック (Fabric)] > [設定 (Configuration)] > [ブリッジ (Bridges)] の順に選択します。
- 2 ブリッジ クラスタの名前を指定します。
- 3 ブリッジ クラスタのトランスポート ゾーンを選択します。  
トランスポート ゾーンのタイプは、VLAN ではなくオーバーレイにする必要があります。
- 4 [使用可能 (Available)] 列からトランスポート ノードを選択し、右矢印をクリックして選択されたトランスポート ノードを [選択済み (Selected)] 列に移動します。

### 次のステップ

これで、論理スイッチをブリッジ クラスタに関連付けることができます。

## レイヤー 2 のブリッジによってバックアップされる論理スイッチの作成

仮想マシンが NSX-T オーバーレイに接続されている場合、NSX-T デプロイの外部にある他のデバイスまたは仮想マシンとの間でレイヤー 2 接続を行う方法があります。この場合、ブリッジによってバックアップされる論理スイッチを使用することができます。

トポロジのサンプルについては、[図 2-2](#) を参照してください。

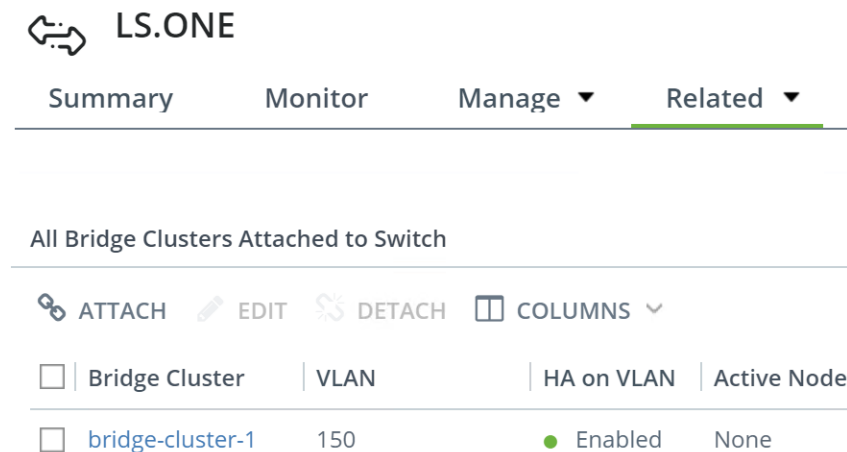
### 前提条件

- ブリッジ ノードとして機能する少なくとも 1 つの ESXi ホスト。ブリッジ ノードはブリッジ機能のみを提供する ESXi トランスポート ノードです。このトランスポート ノードをブリッジ クラスタに追加する必要があります。[「ブリッジ クラスタの作成」](#) を参照してください。
- 通常のトランスポート ノードとして機能する少なくとも 1 つの ESXi または KVM ホスト。このノードは、NSX-T デプロイの外部にあるデバイスとの接続を必要とする仮想マシンをホストします。
- NSX-T デプロイの外部にある仮想マシンまたは別の端末装置。この端末装置は、ブリッジによってバックアップされる論理スイッチの VLAN ID と一致する VLAN ポートに接続する必要があります。
- ブリッジによってバックアップされる論理スイッチとして機能するオーバーレイ トランスポート ゾーン内の 1 台の論理スイッチ。

## 手順

- 1 ブラウザから、<https://<nsx-mgr>> の NSX Manager にログインします。
- 2 [スイッチング (Switching)] > [スイッチ (Switches)] を選択します。
- 3 スイッチのリストから、オーバーレイ スイッチ（トラフィック タイプ：オーバーレイ）を選択します。
- 4 スイッチの設定ページで、[関連 (Related)] > [ブリッジ クラスタ (Bridge Clusters)] を選択します。
- 5 [接続 (ATTACH)] をクリックし、ブリッジ クラスタを選択して、VLAN ID を入力します。

次はその例です。



LS.ONE

Summary Monitor Manage ▼ Related ▼

All Bridge Clusters Attached to Switch

ATTACH EDIT DETACH COLUMNS ▼

Bridge Cluster	VLAN	HA on VLAN	Active Node
<input type="checkbox"/> bridge-cluster-1	150	● Enabled	None

- 6 仮想マシンを論理スイッチに接続します（まだ接続されていない場合）。

仮想マシンは、ブリッジ クラスタと同じトランスポートゾーンのトランスポート ノード上にある必要があります。

ブリッジの機能をテストするには、NSX-T の内部仮想マシンから NSX-T の外部にあるノードに ping を送信します。たとえば、[図 2-2](#) では、NSX-T トランスポート ノード上の App 仮想マシンと外部ノード上の DB 仮想マシンは相互に ping を送信できる必要があります。

[スイッチング (Switching)] > [スイッチ (Switches)] > [監視 (Monitor)] の順に選択し、ブリッジ スイッチ上のトラフィックを監視することができます。

GET <https://192.168.110.31/api/v1/bridge-endpoints/<endpoint-id>/statistics>

API 呼び出しを実行して、ブリッジ トラフィックを表示することができます。

```
{
  "tx_packets": {
    "total": 134416,
    "dropped": 0,
    "multicast_broadcast": 0
  },
  "rx_bytes": {
    "total": 22164,
    "multicast_broadcast": 0
  },
  "tx_bytes": {
    "total": 8610134,
```

```

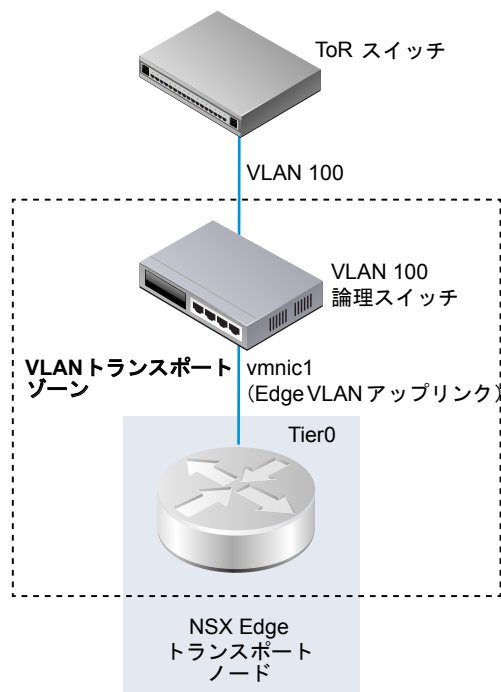
    "multicast_broadcast": 0
  },
  "rx_packets": {
    "total": 230,
    "dropped": 0,
    "multicast_broadcast": 0
  },
  "last_update_timestamp": 1454979822860,
  "endpoint_id": "ba5ba59d-22f1-4a02-b6a0-18ef0e37ef31"
}

```

## NSX Edge アップリンク用の VLAN 論理スイッチの作成

Edge アップリンクは VLAN 論理スイッチを介して接続されます。

VLAN 論理スイッチを作成する場合、構築する特定のトポロジを考慮することが重要です。たとえば、次の単純なトポロジは、VLAN トランスポートゾーン内部の単一の VLAN 論理スイッチを示します。VLAN 論理スイッチの VLAN ID は 100 です。これは、Edge の VLAN アップリンクに使用されるハイパーバイザー ホスト ポートに接続された TOR ポートの VLAN ID に一致します。



### 前提条件

- VLAN 論理スイッチを作成するには、最初に VLAN トランスポートゾーンを作成する必要があります。



- NSX-T vSwitch を NSX Edge に追加する必要があります。Edge 上で確認するには、**get host-switch** コマンドを実行します。次はその例です。

```
nsx-edge1> get host-switch

Host Switch      : c0a78378-1c20-432a-9e23-ddb34f1c80c9
Switch Name      : hs1
Transport Zone   : c46dcd72-808a-423d-b4cc-8752c33f6b2c
Transport Zone   : 73def985-d122-4b7b-ab6a-a58176dfc32d
Physical Port    : fp-eth0
Uplink Name      : uplink-1
Transport VLAN   : 4096
Default Gateway  : 192.168.150.1
Subnet Mask      : 255.255.255.0
Local VTEP Device : fp-eth0
Local VTEP IP    : 192.168.150.102
```

- NSX Controller クラスタが安定していることを確認します。
- ファブリック ノードが NSX-T 管理プレーン エージェント (MPA) および NSX-T ローカル制御プレーン (LCP) に正常に接続されていることを確認します。

GET <https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state> API の呼び出しで、**state** が **success** である必要があります。『NSX-T インストール ガイド』を参照してください。

#### 手順

- 1 ブラウザから、<https://<nsx-mgr>> の NSX Manager にログインします。
- 2 [スイッチング (Switching)] > [スイッチ (Switches)] を選択します。
- 3 [追加 (Add)] をクリックします。
- 4 論理スイッチの名前を入力します。
- 5 論理スイッチのトランスポート ゾーンを選択します。  
VLAN トランスポート ゾーンを選択すると、VLAN ID フィールドが表示されます。
- 6 VLAN ID を入力します。  
物理 TOR へのアップリンクの VLAN ID がない場合は、[VLAN] フィールドに 0 を入力します。
- 7 (オプション) [スイッチング プロファイル (Switching Profiles)] タブをクリックして、スイッチング プロファイルを選択します。

#### 次のステップ

分散論理ルーターを追加します。

## 論理スイッチへの仮想マシンの接続

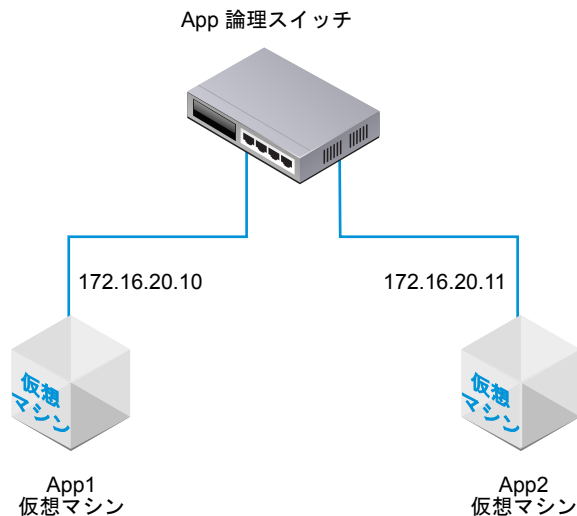
仮想マシンを論理スイッチに接続する設定は、ホストによって異なります。

論理スイッチへの接続が可能なホストは、vCenter Server で管理される ESXi ホスト、スタンドアロンの ESXi ホスト、および KVM ホストです。

### vCenter Server 上でホストされた仮想マシンの NSX-T 論理スイッチへの接続

vCenter Server で管理される ESXi ホストがある場合、Web ベースの vSphere Web Client を介してホストの仮想マシンにアクセスすることができます。その場合は、この手順に従って、仮想マシンを NSX-T 論理スイッチに接続します。

ここで示す例では、app-vm という名前の仮想マシンを app-switch という名前の論理スイッチに接続します。



インストールベースの vSphere Client アプリケーションは、NSX-T 論理スイッチへの仮想マシンの接続をサポートしません。(Web ベースの) vSphere Web Client を所有していない場合は、[「スタンドアロン ESXi にホストされている仮想マシンの NSX-T 論理スイッチへの接続」](#) を参照してください。

#### 前提条件

- 仮想マシンは、NSX-T ファブリックに追加されたハイパーバイザー上でホストされている必要があります。
- ファブリック ノードが、NSX-T 管理プレーン (MPA) と NSX-T 制御プレーン (LCP) に接続できる
- ファブリック ノードがトランスポート ゾーンに追加されている
- 論理スイッチが作成されている

## 手順

- 1 vSphere Web Client で、仮想マシン設定を編集し、仮想マシンを NSX-T 論理スイッチに接続します。

次はその例です。

1-vm_ubuntu_1404_srv_64-local-645-bfd95df0-ea28-4408-ae9a-2561750b0674 - 設定の編集			
仮想ハードウェア	仮想マシン オプション	Storage DRS ルール	vApp オプション
CPU	1		
メモリ	1024	MB	
ハード ディスク 1	16	GB	
SCSI コントローラ 0	LSI Logic パラレル		
*ネットワーク アダプタ 1	LS.ONE (nsx.LogicalSwitch)	<input checked="" type="checkbox"/>	接続中
ネットワーク アダプタ 2	lswitch301 (nsx.LogicalSwitch)	<input checked="" type="checkbox"/>	接続中
ビデオ カード	カスタム設定の指定		
VMCI デバイス			

- 2 [OK] をクリックします。

仮想マシンを論理スイッチに接続した後、論理スイッチ ポートが論理スイッチに追加されます。論理スイッチ ポートは [スイッチング] > [ポート] の NSX Manager で確認することができます。

NSX-T API で、GET `https://<nsx-mgr>/api/v1/fabric/virtual-machines` API 呼び出しを使用して NSX-T に接続された仮想マシンを表示することができます。

[スイッチング] > [ポート] の NSX-T Manager ユーザー インターフェイスで、VIF 接続 ID は API 呼び出しで見つかった ExternalID に一致します。仮想マシンの ExternalID に一致する VIF 接続 ID を探し、管理と操作の状態が Up/Up であることを確認します。

2 台の仮想マシンが同じ論理スイッチに接続され、IP アドレスが同じサブネットを設定されている場合、それらの仮想マシンは互いに ping を送信することができます。

## 次のステップ

論理ルーターを追加します。

論理スイッチ ポート上でアクティビティを監視して、問題をトラブルシューティングできます。[「論理スイッチ ポート アクティビティの監視」](#)を参照してください。

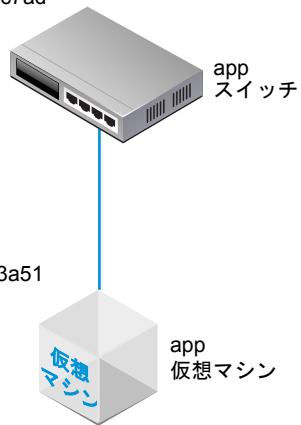
## スタンドアロン ESXi にホストされている仮想マシンの NSX-T 論理スイッチへの接続

スタンドアロン ESXi ホストを使用する場合、Web ベースの vSphere Web Client を介してホスト仮想マシンにアクセスすることはできません。その場合は、この手順に従って、仮想マシンを NSX-T 論理スイッチに接続します。

ここで示す例では、app-vm という名前の仮想マシンを app-switch という名前の論理スイッチに接続します。

スイッチの不透明ネットワーク ID :  
22b22448-38bc-419b-bea8-b51126bec7ad

仮想マシンの外部 ID :  
50066bae-0f8a-386b-e62e-b0b9c6013a51



#### 前提条件

- 仮想マシンが、NSX-T ファブリックに追加したハイパーバイザーでホストされている必要があります。
- ファブリック ノードが、NSX-T 管理プレーン (MPA) と NSX-T 制御プレーン (LCP) に接続できる
- ファブリック ノードがトランスポート ゾーンに追加されている
- 論理スイッチが作成されている
- NSX Manager API にアクセスできる
- 仮想マシンの VMX ファイルに対する書き込み権限がある

## 手順

- 1 (インストール ベースの) vSphere Client アプリケーションまたはその他の仮想マシン管理ツールを使用して、仮想マシンを編集し、VMXNET 3 イーサネット アダプタを追加します。

任意のネットワークを選択します。ネットワーク接続は後の手順で変更します。

## ハードウェアのカスタマイズ

仮想マシン ハードウェアを設定します

仮想ハードウェア	仮想マシン オプション	Storage DRS ルール
▶ CPU	1	
▶ メモリ	4096	MB
▶ 新規ハード ディスク	40	GB
▶ 新規 SCSI コントローラ	LSI Logic SAS	
▼ *新規ネットワーク	VM Network	
ステータス	<input checked="" type="checkbox"/> パワーオン時に接続	
アダプタ タイプ	VMXNET 3	
DirectPath I/O	<input type="checkbox"/> 有効化	
MAC アドレス	<input type="text"/> 自動	
▶ 新規 CD/DVD ドライブ	クライアント デバイス	<input type="checkbox"/> 接続...
▶ 新規フロッピー ドライブ	クライアント デバイス	<input type="checkbox"/> 接続...

新規デバイス:  ネットワーク

- 2 NSX-T API を使用して、GET <https://<nsx-mgr>/api/v1/fabric/virtual-machines/<VM-ID>> API 呼び出しを発行します。

結果から仮想マシンの externalId を検出します。

次はその例です。

```
GET https://<nsx-mgr>/api/v1/fabric/virtual-machines/60a5a5d5-ea2b-407e-a806-4fdc8468f735
```

```
{
  "resource_type": "VirtualMachine",
  "id": "60a5a5d5-ea2b-407e-a806-4fdc8468f735",
  "display_name": "app-vm",
  "compute_ids": [
    "instanceUuid:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "moIdOnHost:5",
    "externalId:[50066bae-0f8a-386b-e62e-b0b9c6013a51]",
    "hostLocalId:5",
  ]
}
```

```

    "locationId:564dc020-1565-e3f4-f591-ee3953eef3ff",
    "biosUuid:4206f47d-fef7-08c5-5bf7-ea26a4c6b18d"
  ],
  "external_id": "50066bae-0f8a-386b-e62e-b0b9c6013a51",
  "type": "REGULAR",
  "host_id": "cb82b0fa-a8f1-11e5-92a9-6b7d1f8661fa",
  "local_id_on_host": "5"
}

```

- 3 仮想マシンをパワーオフし、ホストから登録解除します。

ここに示すように、仮想マシン管理ツールまたは ESXi CLI を使用できます。

```

[user@host:~] [vim-cmd /vmtoolsd/getallvms]
Vmid    Name      File           Guest OS      Version  Annotation
5       app-vm    [ds2] app-vm/app-vm.vmx  ubuntuGuest  vmx-08
8       web-vm    [ds2] web-vm/web-vm.vmx  ubuntu64Guest vmx-08


[user@host:~] [vim-cmd /vmtoolsd/power.off 5]
Powering off VM:

[user@host:~] [vim-cmd /vmtoolsd/unregister 5]

```

- 4 NSX Manager のユーザー インターフェイスから論理スイッチ ID を取得します。

次はその例です。


**app-switch**

Summary
Monitor
Manage ▼
Related ▼

---

**Summary**

---

Name	app-switch
ID	27428a39-9b29-4f73-a1b8-0ffb83c7d4e3
Description	
Admin Status	● Up
Replication Mode	Hierarchical Two-Tier replication
VNI	33672
Logical Ports	0
Traffic Type	Overlay
Transport Zone	TZ.ONE
Created	7/28/2016, 11:35:51 AM by admin
Last Updated	7/28/2016, 11:35:51 AM by admin

## 5 仮想マシンの VMX ファイルを修正します。

[ethernet1.networkName = "<name>"] フィールドを削除し、次のフィールドを追加します。

- ethernet1.opaqueNetwork.id = "<logical switch's ID>"
- ethernet1.opaqueNetwork.type = "nsx.LogicalSwitch"
- ethernet1.externalId = "<VM's externalId>"
- ethernet1.connected = "TRUE"
- ethernet1.startConnected = "TRUE"

次はその例です。

### [修正前 (OLD)]

```
ethernet1.pciSlotNumber = "224"
ethernet1.virtualDev = "vmxnet3"
ethernet1.networkName = "VM Network"
ethernet1.addressType = "vpx"
ethernet1.generatedAddress = "00:50:56:86:7b:d7"
ethernet1.uptCompatibility = "true"
ethernet1.present = "TRUE"
```

### [修正後 (NEW)]

```
ethernet1.pciSlotNumber = "224"
ethernet1.virtualDev = "vmxnet3"
ethernet1.addressType = "vpx"
ethernet1.generatedAddress = "00:50:56:86:7b:d7"
ethernet1.uptCompatibility = "true"
ethernet1.present = "TRUE"
ethernet1.opaqueNetwork.id = "22b22448-38bc-419b-bea8-b51126bec7ad"
ethernet1.opaqueNetwork.type = "nsx.LogicalSwitch"
ethernet1.externalId = "50066bae-0f8a-386b-e62e-b0b9c6013a51"
ethernet1.connected = "TRUE"
ethernet1.startConnected = "TRUE"
```

- 6 NSX Manager のユーザー インターフェイスで、論理スイッチ ポートを追加し、仮想マシンの externalId を VIF 接続に使用します。

次はその例です。

New Logical Port

×

Name:\*

to-app

Description:

Logical Switch:\*

app-tier-01

▼

Admin State:\*

☒ Up

Attachment Type:\*

VIF

▼

Attachment ID:

50066bae-0f8a-386b-e62e-b0b9c6013a51

Switching Profiles Type:\*

None

▼

Switching Profiles Id:

Save

Cancel

- 7 仮想マシンを再登録し、パワーオンします。

ここに示すように、仮想マシン管理ツールまたは ESXi CLI を使用できます。

```
[user@host:~] [vim-cmd /solo/register /path/to/file.vmx]
```

For example:

```
[user@host:~] [vim-cmd solo/registervm /vmfs/volumes/355f2049-6c704347/app-vm/app-vm.vmx]
9
```

```
[user@host:~] [vim-cmd /vmvc/power.on 9]
```

Powering on VM:

NSX Manager のユーザー インターフェイスの [スイッチング (Switching)] > [ポート (Ports)] で、仮想マシンの externalId と一致する VIF 接続 ID を検出し、管理および運用ステータスが [アップ/アップ] であることを確認します。

2 台の仮想マシンが同じ論理スイッチに接続され、IP アドレスが同じサブネットで設定されている場合、それぞれが互いに ping を送信できるはずです。



## 次のステップ

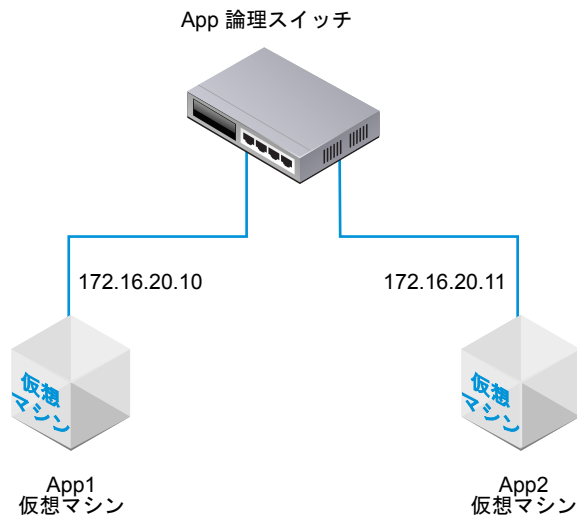
分散論理ルーターを追加します。

論理スイッチ ポート上でアクティビティを監視して、問題をトラブルシューティングできます。[「論理スイッチ ポート アクティビティの監視」](#)を参照してください。

## KVM 上でホストされた仮想マシンの NSX-T 論理スイッチへの接続

KVM ホストがある場合は、この手順を使用して NSX-T 論理スイッチに仮想マシンを接続することができます。

この手順の例では、app-switch と呼ばれる論理スイッチに app-vm と呼ばれる仮想マシンを接続する方法を説明しています。



## 前提条件

- 仮想マシンは、NSX-T ファブリックに追加したハイパーバイザーでホストされている必要があります。
- ファブリック ノードには、NSX-T 管理プレーン (MPA) および NSX-T 制御プレーン (LCP) 接続が必要です。
- ファブリック ノードはトランスポート ゾーンに追加する必要があります。
- 論理スイッチを作成する必要があります。

## 手順

- 1 KVM CLI から、`virsh dumpxml <your vm> | grep interfaceid` コマンドを実行します。

- 2 NSX Manager のユーザー インターフェイスで、論理スイッチ ポートを追加し、VIF 接続に仮想マシンのインターフェイス ID を使用します。

次はその例です。

**New Logical Port** [X]

Name: \* to-app

Description:

Logical Switch: \* app-tier-01

Admin State: \* ☒ Up

Attachment Type: \* VIF

Attachment ID: 50066bae-0f8a-386b-e62e-b0b9c6013a51

Switching Profiles Type: \* None

Switching Profiles Id:

[Save] [Cancel]

[スイッチング (Switching)] > [ポート (Ports)] の NSX Manager ユーザー インターフェイスで、VIF 接続 ID を探し、管理と操作のステータスが Up/Up であることを確認します。

2 台の仮想マシンが同じ論理スイッチに接続され、IP アドレスが同じサブネットで設定されている場合、それらの仮想マシンは互いに ping を送信することができます。

#### 次のステップ

分散論理ルーターを追加します。

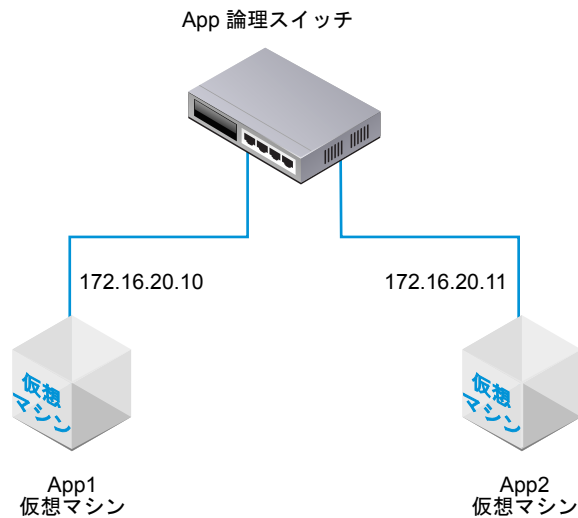
論理スイッチ ポート上でアクティビティを監視して、問題をトラブルシューティングできます。[「論理スイッチ ポート アクティビティの監視」](#)を参照してください。

## レイヤー 2 接続のテスト

論理スイッチを正しく設定して仮想マシンを論理スイッチに接続したら、接続された仮想マシンのネットワーク接続をテストすることができます。

トポロジに基づいてネットワーク環境が適切に設定されていれば、App2 仮想マシンは App1 仮想マシンに ping を送信できます。

図 2-3. 論理スイッチ トポロジ



## 手順

- 1 SSH または仮想マシン コンソールを使用して、論理スイッチに接続された仮想マシンの 1 台にログインします。

例 : App2 VM 172.16.20.11

- 2 論理スイッチに接続された 2 番目の仮想マシンに ping を送信して接続をテストします。

```
$ ping -c 2 172.16.20.10
PING 172.16.20.10 (172.16.20.10) 56(84) bytes of data.
64 bytes from 172.16.20.10: icmp_seq=1 ttl=63 time=0.982 ms
64 bytes from 172.16.20.10: icmp_seq=2 ttl=63 time=0.654 ms
64 bytes from 172.16.20.10: icmp_seq=3 ttl=63 time=0.791 ms

--- 172.16.20.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1990ms
rtt min/avg/max/mdev = 0.654/0.809/0.902/0.104 ms
```

- 3 (オプション) ping コマンドの失敗の原因となる問題を特定します。
  - a 仮想マシン ネットワーク設定が正しいことを確認します。
  - b 仮想マシン ネットワーク アダプタが正しい論理スイッチに接続されることを確認します。
  - c 論理スイッチの [管理] 状態が [UP] であることを確認します。
  - d NSX Manager から、[スイッチング] - [スイッチ] を選択します。

- e 論理スイッチをクリックし、UUID および VNI 情報をメモします。
- f NSX Controller から、次のコマンドを実行して問題をトラブルシューティングします。

コマンド	説明
<b>get logical-switch &lt;vni-or-uuid&gt; arp-table</b>	<p>指定された論理スイッチの ARP テーブルを表示します。</p> <p>出力例：</p> <pre>nsx-controller1&gt; get logical-switch 41866 arp-table VNI      IP          MAC          Connection-ID 41866    172.16.20.11 00:50:56:b1:70:5e 295422</pre>
<b>get logical-switch &lt;vni-or-uuid&gt; connection-table</b>	<p>指定された論理スイッチの接続を表示します。</p> <p>出力例：</p> <pre>nsx-controller1&gt; get logical-switch 41866 connection-table Host-IP      Port  ID 192.168.110.37 36923 295420 192.168.210.53 37883 295421 192.168.210.54 57278 295422</pre>
<b>get logical-switch &lt;vni-or-uuid&gt; mac-table</b>	<p>指定された論理スイッチの MAC テーブルを表示します。</p> <p>出力例：</p> <pre>nsx-controller1&gt; get logical-switch 41866 mac-table VNI      MAC          VTEP-IP      Connection-ID 41866    00:50:56:86:f2:b2 192.168.250.102 295421 41866    00:50:56:b1:70:5e 192.168.250.101 295422</pre>
<b>get logical-switch &lt;vni-or-uuid&gt; mac-table</b>	<p>指定された論理スイッチの統計情報を表示します。</p> <p>出力例：</p> <pre>nsx-controller1&gt; get logical-switch 41866 stats update.member 11 update.vtep 11 update.mac 4 update.mac.invalidate 0 update.arp 7 update.arp.duplicate 0 query.mac 2 query.mac.miss 0 query.arp 9 query.arp.miss 6</pre>
<b>get logical-switch &lt;vni-or-uuid&gt; mac-table</b>	<p>すべての論理スイッチの統計情報のサマリを時系列で表示します。</p> <p>出力例：</p> <pre>nsx-controller1&gt; get logical-switch 41866 stats-sample 21:00:00 21:10:00 21:20:00 21:30:00 21:40:00 update.member 0 0 0 0 0 update.vtep 0 0 0 0 0 update.mac 0 0 0 0 0 update.mac.invalidate 0 0 0 0 0 update.arp 0 0 0 0 0 update.arp.duplicate 0 0 0 0 0</pre>

コマンド	説明
	<pre>query.mac 0 0 0 0 0 query.mac.miss 0 0 0 0 0 query.arp 0 0 0 0 0 query.arp.miss 0 0 0 0 0</pre>
<b>get logical-switch &lt;vni-or-uuid&gt; vtep</b>	<p>指定された論理スイッチに関連する仮想トンネルのエンドポイントをすべて表示します。</p> <p>出力例：</p> <pre>nsx-controller1&gt; get logical-switch 41866 vtep VNI      IP          LABEL      Segment MAC      Connection-ID 41866 192.168.250.102 0x8801 192.168.250.0 00:50:56:65:f5:fc 295421 41866 192.168.250.100 0x1F801 192.168.250.0 02:50:56:00:00:00 295420 41866 192.168.250.101 0x16001 192.168.250.0 00:50:56:64:7c:28 295422</pre>

論理スイッチに接続された最初の仮想マシンが、2 番目の仮想マシンにパケットを送信することができます。

# 論理スイッチおよび論理ポートのスイッチング プロファイルの設定

## 3

スイッチング プロファイルには、論理スイッチと論理ポートを対象とした、レイヤー 2 ネットワークの設定の詳細が含まれます。NSX Manager は、いくつかのタイプのスイッチング プロファイルをサポートします。また、各プロファイル タイプ用に、1 個以上のシステム定義のデフォルト スwitchング プロファイルを維持します。

次のタイプのスイッチング プロファイルを使用できます。

- QoS (サービス品質)
- ポート監視
- IP アドレス検出
- SpoofGuard
- スwitch セキュリティ
- MAC 管理

---

**注:** デフォルトのスイッチング プロファイルを NSX Manager で編集または削除することはできません。代わりに、カスタムのスイッチング プロファイルを作成できます。

---

デフォルト スwitchング プロファイルやカスタム スwitchング プロファイルには、それぞれ固有の ID が予約されます。この ID を使用して、スイッチング プロファイルを論理スイッチまたは論理ポートと関連付けます。たとえば、デフォルトの QoS スwitchング プロファイルの ID は f313290b-eba8-4262-bd93-fab5026e9495 です。

論理スイッチまたは論理ポートは、各タイプの 1 個のスイッチング プロファイルと関連付けることができます。たとえば、2 個の異なる QoS スwitchング プロファイルを 1 個の論理スイッチまたは論理ポートと関連付けることはできません。

論理スイッチの作成中または更新中にスイッチング プロファイル タイプを関連付けなかった場合は、NSX Manager で、対応するシステム定義のデフォルト スwitchング プロファイルが関連付けられます。子論理ポートは、システム定義のデフォルト スwitchング プロファイルを親論理スイッチから継承します。

論理スイッチや論理ポートを作成または更新するときに、デフォルト スwitchング プロファイルまたはカスタム スwitchング プロファイルを関連付けできます。スイッチング プロファイルを論理スイッチと関連付けたり、関連付けを解除したりすると、次の基準に従って、子論理ポート用のスイッチング プロファイルが適用されます。

- 親論理スイッチにプロファイルが関連付けられている場合、子論理ポートはその親からスイッチング プロファイルを継承します。

- 親論理スイッチにスイッチング プロファイルが関連付けられていない場合、デフォルト スwitchング プロファイルが論理スイッチに割り当てられ、論理ポートはそのデフォルト スwitchング プロファイルを継承します。
- カスタム プロファイルを明示的に論理ポートと関連付ける場合、そのカスタム プロファイルは既存のスイッチング プロファイルをオーバーライドします。

---

**注:** カスタム スwitchング プロファイルを論理スイッチと関連付けたが、子論理スイッチ ポートのうち 1 つに対してデフォルト スwitchング プロファイルを維持する場合は、デフォルト スwitchング プロファイルのコピーを作成し、それを特定の論理ポートと関連付ける必要があります。

---

論理スイッチや論理ポートと関連付けられているカスタム スwitchング プロファイルを削除することはできません。論理スイッチや論理ポートがカスタム スwitchング プロファイルと関連付けられているかどうかを確認するには、サマリ ビューの割当先のセクションで、リストされている論理スイッチおよび論理ポートをクリックします。

この章には、次のトピックが含まれています。

- [QoS スwitchング プロファイルの理解](#)
- [ポート ミラーリング スwitchング プロファイルの理解](#)
- [IP アドレス検出スswitchング プロファイルの理解](#)
- [SpoofGuard の理解](#)
- [スイッチ セキュリティのスswitchング プロファイルの理解](#)
- [MAC 管理スswitchング プロファイルの理解](#)
- [カスタム プロファイルと論理スイッチの関連付け](#)
- [論理スイッチ ポートへのカスタム プロファイルの関連付け](#)

## QoS スwitchング プロファイルの理解

QoS は、高帯域幅を必要とする優先トラフィックに対して高品質の専用ネットワーク パフォーマンスを提供します。QoS メカニズムがこれを実現するには、ネットワークが輻輳している場合でも、優先パケットのために十分な帯域幅を割り当て、待ち時間とジッタを制御し、データ損失を低減します。このレベルのネットワーク サービスは、既存のネットワーク リソースを効率的に使用することにより提供されます。

このリリースでは、シェーピングとトラフィック マーキング、すなわち CoS と DSCP がサポートされます。レイヤー 2 の Class of Service (CoS) は、トラフィックが輻輳により論理スイッチにバッファされているときに、データ パケットの優先順位を指定することを可能にします。レイヤー 3 の Differentiated Services Code Point (DSCP) は、それらの DSCP 値に基づいてパケットを検出します。CoS は、信頼されるモードに関係なく常にデータ パケットに適用されます。

NSX-T は、仮想マシンによって、または論理スイッチ レベルで DSCP 値を変更および設定することによって適用された DSCP 設定を信頼します。いずれの場合も、DSCP 値は のカプセル化フレームの外部 IP ヘッダーに伝達されます。これによって、外部の物理ネットワークは、外部ヘッダーの DSCP 設定に基づいてトラフィックに優先順位を付けることができます。DSCP が信頼されるモードにある場合、DSCP 値は内部ヘッダーからコピーされます。信頼されないモードにある場合、DSCP 値は内部ヘッダー用に確保されません。

**注:** DSCP 設定はトンネリングされたトラフィックでのみ有効です。これらの設定は同じハイパーバイザー内のトラフィックには適用されません。

QoS スイッチング プロファイルを使用して、入力側と出力側の平均帯域幅を設定し、転送制限速度を設定することができます。ピーク時の帯域幅速度は論理スイッチで許可されるバースト トラフィックをサポートするために使用され、Northbound ネットワーク リンクでの輻輳を回避することができます。ただし、これらの設定は帯域幅を保証するものではなく、ネットワーク帯域幅の使用を制限するのに利用されます。

QoS スイッチング プロファイル設定は論理スイッチに適用され、子の論理スイッチ ポートに継承されます。

## カスタムの QoS スイッチング プロファイルの設定

DSCP 値を定義し、入力側と出力側を設定して、カスタムの QoS スイッチング プロファイルを作成することができます。

### 前提条件

- QoS スイッチング プロファイルの概念を理解します。[「QoS スイッチング プロファイルの理解」](#) を参照してください。
- 優先するネットワーク トラフィックを識別します。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[スイッチング (Switching)] - [スイッチング プロファイル (Switching Profiles)] の順に選択します。
- 3 [追加 (Add)] をクリックします。
- 4 QoS スイッチング プロファイルの詳細を完成させます。

オプション	説明
名前と説明	カスタムの QoS スイッチング プロファイルに名前を割り当てます。 オプションとして、プロファイルで変更した設定の説明を入力することができます。
タイプ	ドロップダウン メニューから [QoS] を選択します。



オプション	説明
DSCP	<p>[モード] ドロップダウン メニューから [信頼されています (Trusted)] または [信頼されていません (Untrusted)] オプションのいずれかを選択します。</p> <p>信頼されるモードを選択すると、内部ヘッダーの DSCP 値は IP/IPv6 トラフィック用の外部 IP ヘッダーに適用されます。IP/IPv6 以外のトラフィックの場合、外部 IP ヘッダーはデフォルト値を使用します。信頼されるモードは、オーバーレイベースの論理ポートでサポートされます。デフォルト値は 0 です。</p> <p>信頼されないモードは、オーバーレイベースおよび VLAN ベースの論理ポートでサポートされます。オーバーレイベースの論理ポートの場合、送信 IP ヘッダーの DSCP 値は、論理ポートの内部パケットのタイプに関係なく設定された値にセットされます。VLAN ベースの論理ポートの場合、IP/IPv6 パケットの DSCP 値は設定された値にセットされます。信頼されないモードの DSCP 値の範囲は 0 ～ 63 です。</p> <p><b>注:</b> DSCP 設定はトンネリングされたトラフィックでのみ有効です。これらの設定は同じハイパーバイザー内のトラフィックには適用されません。</p>
サービスのクラス	<p>トラフィックの優先順位レベルを設定します。</p> <p>CoS は VLAN ベースの論理ポートでサポートされます。CoS はネットワーク内の類似するトラフィック タイプをグループ化し、各タイプのトラフィックは独自のレベルのサービス優先順位を持つクラスとして扱われます。優先度の低いトラフィックは低速になるか、場合によってはドロップされ、優先度の高いトラフィックのスループットを向上させます。また、CoS はパケットがゼロの VLAN ID に対しても設定することができます。</p> <p>CoS の値の範囲は 0 ～ 7 で、0 がベスト エフォート サービスです。</p>
入力側	<p>仮想マシンから論理ネットワークへの送信ネットワーク トラフィックに対するカスタムの値をセットします。</p> <p>平均帯域幅を使用して、ネットワークの輻輳を低減することができます。ピークの帯域幅レートはバースト トラフィックをサポートするために使用され、バーストの期間はバースト サイズの設定内でセットされます。帯域幅を保証することはできません。ただし、ネットワーク帯域幅を制限するための設定を使用することができます。デフォルト値は 0 で、入力側トラフィックを無効にします。</p> <p>たとえば、論理スイッチの平均帯域幅を 30 Mbps にセットすると、ポリシーは帯域幅を制限します。20 バイトの間、バースト トラフィックを 100 Mbps に制限することができます。</p>
入力側ブロードキャスト	<p>ブロードキャストに基づいて、仮想マシンから論理ネットワークへの送信ネットワーク トラフィックに対するカスタムの値をセットします。</p> <p>デフォルト値は 0 で、入力側ブロードキャスト トラフィックを無効にします。</p> <p>たとえば、論理スイッチの平均帯域幅を 50 Kbps にセットすると、ポリシーは帯域幅を制限します。60 バイトの間、バースト トラフィックを 400 Kbps に制限することができます。</p>
出力側	<p>論理ネットワークから仮想マシンへの受信ネットワーク トラフィックに対するカスタムの値をセットします。</p> <p>デフォルト値は 0 で、出力側トラフィックを無効にします。</p>

入力側、入力側ブロードキャスト、および出力側オプションを設定しない場合、デフォルト値がプロトコル バッファとして使用されます。

## 5 [保存 (Save)] をクリックします。

カスタムの QoS スイッチング プロファイルがリンクとして表示されます。

## 次のステップ

この QoS がカスタマイズされたスイッチング プロファイルを論理スイッチに接続し、スイッチング プロファイル内で変更されたパラメータがネットワーク トラフィックに適用されるようにします。[「カスタム プロファイルと論理スイッチの関連付け」](#)を参照してください。

## ポート ミラーリング スイッチング プロファイルの理解

論理ポートのミラーリングによって、仮想マシン VIF ポートに接続された論理スイッチ ポートとの間で発生するすべてのトラフィックをレプリケートおよびリダイレクトすることができます。ミラーリングされたトラフィックは、Generic Routing Encapsulation (GRE) トンネル内でカプセル化されてからコレクタに送信されるので、ネットワーク上をリモートのターゲットまで移動する間に元のパケット情報はすべて保持されます。

通常、ポート ミラーリングは次のシナリオで使用されます。

- **トラブルシューティング**：トラフィックを分析して、侵入を検知しネットワーク上のエラーをデバッグおよび診断します。
- **コンプライアンスと監視**：分析と修正のために、監視されたトラフィックをすべてネットワーク アプライアンスに転送します。

物理ポート ミラーリングと比較して、論理ポート ミラーリングは、すべての仮想マシン ネットワーク トラフィックを確実にキャプチャします。ポート ミラーリングを物理ネットワークにのみ実装した場合、一部の仮想マシン ネットワーク トラフィックがミラーリングされない可能性があります。これは、同じホストに存在する仮想マシン間の通信は物理ネットワークを通過することがなく、ミラーリングされないために発生します。論理ポート ミラーリングでは、仮想マシンが別のホストに移行される間にも仮想マシン トラフィックのミラーリングを継続できます。

ポート ミラーリングのプロセスは、NSX-T ドメインの仮想マシン ポートと物理アプリケーションのポートの場合で類似しています。論理ネットワークに接続されたワークロードによってキャプチャされたトラフィックを転送し、このトラフィックをコレクタにミラーリングすることができます。IP アドレスは、仮想マシンがホストされるゲスト IP アドレスからアクセス可能である必要があります。このプロセスは、ゲートウェイ ノードに接続された物理アプリケーションの場合にも適用されます。

## カスタムのポート ミラーリング スイッチング プロファイルの設定

異なるターゲットとキーの値を使用してカスタムのポート ミラーリング スイッチング プロファイルを作成することができます。

### 前提条件

- ポート ミラーリング スイッチング プロファイルの概念を理解します。[「ポート ミラーリング スイッチング プロファイルの理解」](#)を参照してください。
- ネットワーク トラフィックのリダイレクト先のターゲット論理ポート ID の IP アドレスを特定します。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[スイッチング (Switching)] - [スイッチング プロファイル (Switching Profiles)] の順に選択します。

3 [追加 (Add)] をクリックします。

4 ポート ミラーリング スイッチング プロファイルの詳細を完成させます。

オプション	説明
名前と説明	カスタムのポート ミラーリング スイッチング プロファイルに名前を割り当てます。 オプションとして、このプロファイルのカスタマイズするために変更した設定の説明を入力することができます。
タイプ	ドロップダウン メニューから [ポートの監視 (Port Mirroring)] を選択します。
方向	このソースを [入力側 (Ingress)]、[出力側 (Egress)] または [双方向 (Bidirectional)] トラフィックに使用するためのオプションをドロップダウン メニューから選択します。 入力側は、仮想マシンから論理ネットワークへ向かう送信ネットワーク トラフィックです。 出力側は、論理ネットワークから仮想マシンへ向かう受信ネットワーク トラフィックです。 双方向は、仮想マシンから論理ネットワーク、および論理ネットワークから仮想マシンへの双方向のトラフィックです。デフォルトのオプションです。
パケットの切り捨て	任意。範囲は 60 ～ 65535 です。
キー	論理ポートからミラーリングされたパケットを識別するためにランダムな 32 ビット値を入力します。 このキーの値は、ミラーリングされた各パケットの GRE ヘッダー内の [キー] フィールドにコピーされます。キーの値を 0 にセットすると、デフォルトの定義が GRE ヘッダーの [キー] フィールドにコピーされます。 デフォルトの 32 ビット値は次の値で設定されます。 <ul style="list-style-type: none"> <li>■ 最初の 24 ビットは VNI 値です。VNI はカプセル化されたフレームの IP ヘッダーの一部です。</li> <li>■ 25 番目のビットは、最初の 24 ビットが有効な VNI 値かどうかを示します。1 は値が有効であることを表わし、0 は値が無効であることを表わします。</li> <li>■ 26 番目のビットは、ミラーリングされたトラフィックの方向を示します。1 は入力側方向を表わし、0 は出力側方向を表わします。</li> <li>■ 残りの 6 ビットは未使用です。</li> </ul>
ターゲット	ミラーリングセッションのコレクタのターゲット ID を入力します。 ターゲットの IP アドレスの ID には、ネットワーク内の IPv4 アドレス、または NSX-T によって管理されていないリモートの IPv4 アドレスのいずれかのみを使用できます。ターゲット IP アドレスは、カンマで区切って最大 3 つまで追加することができます。

5 [保存 (Save)] をクリックします。

カスタムのポート ミラーリング スイッチング プロファイルがリンクとして表示されます。

#### 次のステップ

カスタマイズされたポート ミラーリング スイッチング プロファイルが動作することを確認します。[「カスタムのポート ミラーリング スイッチング プロファイルの確認」](#)を参照してください。

## カスタムのポート ミラーリング スイッチング プロファイルの確認

カスタムのポート ミラーリング スイッチング プロファイルを使用する前に、カスタマイズが正常に動作するかを確認します。

## 前提条件

- カスタムのポート ミラーリング スイッチング プロファイルが設定されていることを確認します。[「カスタムのポート ミラーリング スイッチング プロファイルの設定」](#) を参照してください。
- カスタマイズされたポート ミラーリング スイッチング プロファイルが論理スイッチに接続されていることを確認します。[「カスタム プロファイルと論理スイッチの関連付け」](#) を参照してください。

## 手順

- 1 ポート ミラーリング用に設定された論理ポートに接続している、VIF を持つ 2 台の仮想マシンを見つけます。  
たとえば、VM1 10.70.1.1 と VM2 10.70.1.2 には VIF が接続され、同じ論理ネットワークにあります。

- 2 ターゲット IP アドレスで `tcpdump` コマンドを実行します。

```
sudo tcpdump -n -i eth0 dst host <destination_IP_address> and proto gre
```

たとえば、ターゲット IP アドレスは 10.24.123.196 です。

- 3 最初の仮想マシンにログインして、2 番目の仮想マシンに ping を送信し、対応する ECHO リクエストと応答がターゲット アドレスで受信されることを確認します。

たとえば、最初の仮想マシン 10.70.1.1 は、2 番目の仮想マシン 10.70.1.2 に ping を送信してポート ミラーリングを確認します。

No.	Time	Source	Destination	Protocol	Length	Info
8	0.748510	10.70.1.1	10.70.1.2	ICMP	140	Echo (ping) request id=0x650c, seq=57/14592, ttl=64
9	0.748521	10.70.1.2	10.70.1.1	ICMP	140	Echo (ping) reply id=0x650c, seq=57/14592, ttl=64
30	1.748345	10.70.1.1	10.70.1.2	ICMP	140	Echo (ping) request id=0x650c, seq=58/14848, ttl=64
31	1.748602	10.70.1.2	10.70.1.1	ICMP	140	Echo (ping) reply id=0x650c, seq=58/14848, ttl=64
59	2.748266	10.70.1.1	10.70.1.2	ICMP	140	Echo (ping) request id=0x650c, seq=59/15104, ttl=64
60	2.748515	10.70.1.2	10.70.1.1	ICMP	140	Echo (ping) reply id=0x650c, seq=59/15104, ttl=64
90	3.748306	10.70.1.1	10.70.1.2	ICMP	140	Echo (ping) request id=0x650c, seq=60/15360, ttl=64
91	3.748563	10.70.1.2	10.70.1.1	ICMP	140	Echo (ping) reply id=0x650c, seq=60/15360, ttl=64

## 次のステップ

このポート ミラーリングがカスタマイズされたスイッチング プロファイルを論理スイッチに接続し、スイッチング プロファイル内で変更されたパラメータがネットワーク トラフィックに適用されるようにします。[「カスタム プロファイルと論理スイッチの関連付け」](#) を参照してください。

## IP アドレス検出スイッチング プロファイルの理解

IP アドレス検出は、DHCP または ARP スヌーピングを使用して仮想マシンの MAC および IP アドレスを学習します。MAC アドレスと IP アドレスを学習すると、エントリは NSX Controller と共有され、ARP 抑制が有効になります。ARP 抑制は、同じ論理スイッチに接続された仮想マシン内の ARP トラフィックのフラッドを最小限に抑えます。

DHCP スヌーピングは、仮想マシンの DHCP クライアントと DHCP サーバ間で交換された DHCP パケットを検査し、仮想マシンの IP アドレスおよび MAC アドレスを学習します。

ARP スヌーピングは、仮想マシンの送信 ARP および GARP を検査し、IP アドレスと MAC アドレスを学習します。

## IP アドレス検出スイッチング プロファイルの設定

ARP スヌーピングまたは DHCP スヌーピングを有効にして、IP アドレスおよび MAC アドレスを学習するカスタムの IP アドレス検出スイッチング プロファイルを作成し、論理スイッチの IP 整合性を保持することができます。

### 前提条件

IP アドレス検出スイッチング プロファイルの概念を理解します。[「IP アドレス検出スイッチング プロファイルの理解」](#)を参照してください。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[スイッチング (Switching)] - [スイッチング プロファイル (Switching Profiles)] の順に選択します。
- 3 [追加 (Add)] をクリックします。
- 4 IP アドレス検出スイッチング プロファイルの詳細を完成させます。

オプション	説明
名前と説明	カスタムの IP アドレス検出スイッチング プロファイルに名前を割り当てます。 オプションとして、プロファイルで有効にした設定の説明を入力することができます。
タイプ	ドロップダウン メニューから [IP アドレス検出 (IP Discovering)] を選択します。
ARP スヌーピング	[ARP スヌーピング (ARP Snooping)] ボタンを切り替えて、機能を有効にします。 ARP スヌーピングは仮想マシンの送信 ARP および GARP を検査し、仮想マシンの MAC アドレスおよび IP アドレスを学習します。ARP スヌーピングは、仮想マシンが DHCP ではなく固定 IP アドレスを使用する場合に適用可能です。
DHCP スヌーピング	[DHCP スヌーピング (DHCP Snooping)] ボタンを切り替えて、機能を有効にします。 DHCP スヌーピングは、仮想マシンの DHCP クライアントと DHCP サーバ間で交換された DHCP パケットを検査し、仮想マシンの MAC アドレスおよび IP アドレスを学習します。

- 5 [保存 (Save)] をクリックします。

カスタムの IP アドレス検出スイッチング プロファイルがリンクとして表示されます。

### 次のステップ

この IP アドレス検出がカスタマイズされたスイッチング プロファイルを論理スイッチに接続し、スイッチング プロファイル内で変更されたパラメータがネットワーク トラフィックに適用されるようにします。[「カスタム プロファイルと論理スイッチの関連付け」](#)を参照してください。

## SpoofGuard の理解

SpoofGuard は、「Web スプーフィング」または「フィッシング」と呼ばれる悪意のある攻撃を防ぎます。SpoofGuard ポリシーは、なりすましであると判定されたトラフィックをブロックします。

SpoofGuard は、環境内の仮想マシンが、未承認の IP アドレスを使用してトラフィックを送信することを防ぐためのツールです。仮想マシンの IP アドレスが対応する論理ポートの IP アドレスおよび SpoofGuard のスイッチ アドレス バインドに一致しない場合、仮想マシンの vNIC からネットワークへのアクセスは完全に遮断されます。

SpoofGuard はポートまたはスイッチ レベルで設定することができます。SpoofGuard を導入環境で使用するのにはいくつかの理由があります。

- 悪意のある仮想マシンが既存の仮想マシンの IP アドレスを使用することによる成りすましを防ぐ。
- 仮想マシンの IP アドレスがユーザーの介入なしで改変されないようにする： 環境によっては、変更管理による確認なしでは、仮想マシンの IP アドレスを変更できないようにする場合があります。SpoofGuard では、仮想マシンの所有者が簡単に IP アドレスを変更できないため、妨害なしで IP アドレスを継続して使用できます。
- 分散ファイアウォール (DFW) ルールが誤って (あるいは意図的に) 回避されないようにする： DFW ルールで、ソースまたはターゲットに IP セットを使用する場合は、仮想マシンの IP アドレスがパケット ヘッダー内で偽装され、分散ファイアウォール ルールが回避される可能性があります。

NSX-T SpoofGuard の設定には次のものが含まれます。

- MAC SpoofGuard：パケットの MAC アドレスを認証します
- IP SpoofGuard：パケットの MAC アドレスおよび IP アドレスを認証します
- ダイナミック Address Resolution Protocol (ARP) 検査、すなわち ARP、Gratuitous Address Resolution Protocol (GARP) SpoofGuard、および Neighbor Discovery (ND) SpoofGuard 検証は、すべて ARP/GARP/ND ペイロードにマッピングする MAC ソース、IP ソースおよび IP-MAC ソース に対するものです。

ポート レベルでは、許可された MAC/VLAN/IP ホワイトリストは、ポートのアドレス バインド プロパティによって提供されます。仮想マシンがトラフィックを送信すると、その IP/MAC/VLAN がポートの IP/MAC/VLAN プロパティに一致しない場合、トラフィックはドロップされます。ポート レベルの SpoofGuard はトラフィック認証に対応します。つまり、トラフィックが VIF 設定に準拠することを確認します。

スイッチ レベルでは、許可された MAC/VLAN/IP ホワイトリストは、スイッチのアドレス バインド プロパティによって提供されます。これは通常、スイッチに対して許可された IP アドレス範囲/サブネットで、スイッチ レベルの SpoofGuard はトラフィック認証に対応します。

トラフィックをスイッチに送信するには、ポート レベルとスイッチ レベルの両方の SpoofGuard によって許可される必要があります。ポート レベルとスイッチ レベルの SpoofGuard を有効または無効にするには、SpoofGuard のスイッチ プロファイルを使用します。

## ポート アドレス バインドの設定

アドレス バインドは、論理ポートの IP アドレスおよび MAC アドレスを指定し、SpoofGuard でポートのホワイトリストを指定するために使用されます。

ポート アドレス バインドでは、論理ポートの IP アドレスと MAC アドレス、および適用可能な場合は VLAN を指定します。SpoofGuard を有効にすると、指定されたアドレス バインドがデータ パスで強制されます。SpoofGuard に加え、ポート アドレス バインドは DFW ルールの変換に使用されます。

### 手順

- 1 NSX Manager で、[スイッチング (Switching)] > [ポート (Ports)] の順に移動します。

- 2 アドレス バインドを適用する論理ポートをクリックします。  
論理ポートのサマリが表示されます。
- 3 [サマリ] タブで、[アドレス バインド (Address Bindings)] を拡張します。
- 4 [追加 (Add)] をクリックします。  
[アドレス バインドを追加] ダイアログ ボックスが表示されます。
- 5 アドレス バインドを適用する論理ポートの IP アドレスおよび MAC アドレスを指定します。オプションで VLAN を指定することもできます。
- 6 [保存 (Save)] をクリックします。

#### 次のステップ

[[SpoofGuard のスイッチング プロファイルの設定](#)] をするときにポート アドレス バインドを使用します。

## スイッチ アドレス バインドの設定

アドレス バインドによって、一連の IP アドレス、MAC アドレス、および VLAN をスイッチにバインドすることができます。

SpoofGuard では、アドレス バインドは許可された MAC/VLAN/IP のホワイトリストを提供します。対応する SpoofGuard を有効にすると、指定されたアドレス バインドがデータ パスで強制されます。

#### 手順

- 1 NSX Manager で、[スイッチング (Switching)] > [スイッチ (Switches)] の順に移動します。
- 2 アドレス バインドを適用する論理スイッチをクリックします。  
右側のウィンドウにスイッチのサマリが表示されます。
- 3 [サマリ] タブで、[アドレス バインド (Address Bindings)] を拡張します。
- 4 [追加 (Add)] をクリックします。  
[アドレス バインドを追加] ダイアログ ボックスが表示されます。
- 5 スイッチ アドレス バインドにスイッチの MAC アドレスと IP アドレス範囲（および適用可能な場合は VLAN）を入力します。  
IP アドレス範囲/サブネットを指定すると、データ パスはスイッチ上のすべてのポートにバインドを適用します。
- 6 [保存 (Save)] をクリックします。

#### 次のステップ

ここで、[[SpoofGuard のスイッチング プロファイルの設定](#)] を実行し、SpoofGuard ホワイトリストにアドレス バインドを追加します。

## SpoofGuard のスイッチング プロファイルの設定

SpoofGuard を設定するときに仮想マシンの IP アドレスを変更する場合、対応する設定済みのポート/スイッチ アドレス バインドが新しい IP アドレスによって更新されるまで、仮想マシンからのトラフィックがブロックされる場合があります。

ゲストを含むポート グループの SpoofGuard を有効にします。SpoofGuard を各ネットワーク アダプタに対して有効にすると、規定された MAC アドレスおよび対応する IP アドレスについてパケットを検査します。

### 前提条件

SpoofGuard を設定する前に、各論理スイッチにアドレス バインドまたはスイッチ バインドを追加します。アドレス バインドによって、IP アドレスおよび MAC アドレスをポートまたはスイッチにバインドすることができます。[「ポート アドレス バインドの設定」](#)[「スイッチ アドレス バインドの設定」](#)を参照してください。

### 手順

- 1 NSX Manager で、[スイッチング (Switching)] > [スイッチング プロファイル (Switching Profiles)] の順に移動します。
- 2 [追加 (Add)] をクリックします。  
[新規スイッチング プロファイル] ウィンドウが表示されます。
- 3 プロファイルの名前を入力し、タイプとして [SpoofGuard] を選択します。プロファイルの説明を追加することもできます。
- 4 ポート レベルの SpoofGuard を有効にするには [ポート バインド (port bindings)] を選択し、スイッチ レベルの SpoofGuard を有効にするには [スイッチ バインド (switch bindings)] を選択します。  
アドレス バインドはポートおよびスイッチの SpoofGuard に許可されるホワイトリストです。
- 5 [保存 (Save)] をクリックします。

SpoofGuard プロファイルを持つ新しいスイッチング プロファイルが作成されます。

### 次のステップ

SpoofGuard プロファイルを論理スイッチに関連付けます。[「カスタム プロファイルと論理スイッチの関連付け」](#)を参照してください。



## スイッチ セキュリティのスイッチング プロファイルの理解

スイッチ セキュリティはステートレスのレイヤー 2 およびレイヤー 3 セキュリティを提供します。具体的には、IP アドレス、MAC アドレスおよびプロトコルを、許可された一連のアドレスおよびプロトコルと照合することによって、論理スイッチへの入力方向トラフィックをチェックし、仮想マシンから送信される承認されていないパケットをドロップします。スイッチ セキュリティを使用して、ネットワーク内の仮想マシンからの悪意のある攻撃をフィルタすることにより、論理スイッチの整合性を保護することができます。

Bridge Protocol Data Unit (BPDU) フィルタ、DHCP スヌーピング、DHCP サーバ ブロック、速度制限オプションを設定することで、論理スイッチ上のスイッチ セキュリティのスイッチング プロファイルをカスタマイズすることができます。

## カスタムのスイッチ セキュリティ スイッチング プロファイルの設定

許可された BPDU リストの MAC ターゲット アドレスを使用してカスタムのスイッチ セキュリティのスイッチング プロファイルを作成し、レート制限を設定することができます。

### 前提条件

スイッチ セキュリティ スイッチング プロファイルの概念を理解します。[「スイッチ セキュリティのスイッチング プロファイルの理解」](#)を参照してください。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[スイッチング (Switching)] - [スイッチング プロファイル (Switching Profiles)] の順に選択します。
- 3 [追加 (Add)] をクリックします。
- 4 スwitch セキュリティ プロファイルの詳細を指定します。

オプション	説明
名前と説明	カスタムのスイッチ セキュリティ プロファイルに名前を割り当てます。 オプションで、プロファイルで変更した設定の説明を入力できます。
タイプ	ドロップダウン メニューから [スイッチ セキュリティ (Switch Security)] を選択します。
BPDU フィルタ	[BPDU フィルタ (BPDU filter)] ボタンを切り替えて BPDU フィルタを有効にします。 BPDU フィルタを有効にすると、BPDU ターゲットの MAC アドレスへのすべてのトラフィックがブロックされます。また、BPDU フィルタを有効にすると、論理スイッチ ポートの STP が無効になります。これらのポートが STP に参加することは想定されていないためです。
BPDU フィルタ許可リスト	BPDU ターゲットの MAC アドレスの一覧からターゲットの MAC アドレスをクリックし、承認されたターゲットへのトラフィックを許可します。

オプション	説明
DHCP フィルタ	<p>[サーバ ブロック (Server Block)] ボタンおよび [クライアント ブロック (Client Block)] ボタンを切り替えて、DHCP フィルタを有効にします。</p> <p>DHCP サーバのブロックにより、DHCP サーバから DHCP クライアントへのトラフィックがブロックされます。DHCP サーバから DHCP リレー エージェントへのトラフィックはブロックされないことに注意してください。</p> <p>DHCP クライアントのブロックでは DHCP 要求がブロックされるため、仮想マシンによる DHCP IP アドレスの取得を防止できます。</p>
非 IP トラフィックをブロック	<p>[非 IP トラフィックをブロック (Block Non-IP Traffic)] ボタンを切り替えて、IPv4、IPv6、ARP、GARP、および BPDU トラフィックのみを許可します。</p> <p>それ以外のトラフィックはブロックされます。許可される IPv4、IPv6、ARP、GARP および BPDU トラフィックは、アドレス バインドおよび SpoofGuard に設定されたその他のポリシーに基づきます。</p> <p>デフォルトではこのオプションは無効で、非 IP トラフィックは通常のトラフィックとして処理されます。</p>
レートの制限	<p>入力側または出力側のブロードキャストおよびマルチキャスト トラフィックのレートに制限を設定します。</p> <p>レートの制限は、たとえば大量のブロードキャスト トラフィックが発生した場合に論理スイッチや仮想マシンを保護するために設定します。</p> <p>接続の問題を回避するため、レートの制限の最小値は 10 pps 以上にする必要があります。</p>

## 5 [保存 (Save)] をクリックします。

カスタムのスイッチ セキュリティ プロファイルがリンクとして表示されます。

### 次のステップ

このスイッチ セキュリティがカスタマイズされたスイッチング プロファイルを論理スイッチに割り当て、スイッチング プロファイル内で変更されたパラメータがネットワーク トラフィックに適用されるようにします。[「カスタム プロファイルと論理スイッチの関連付け」](#)を参照してください。

## MAC 管理スイッチング プロファイルの理解

MAC 管理スイッチング プロファイルは、MAC アドレスの学習および MAC アドレスの変更の 2 つの機能をサポートします。

MAC アドレスの学習は、1 つの vNIC の背後に複数の MAC アドレスが設定されている環境にネットワーク接続を提供します。たとえば、ハイパーバイザーがネストされた環境において、ESXi ホスト上で ESXi 仮想マシンを実行しており、複数の仮想マシンが ESXi 仮想マシン上で実行されている場合などです。MAC アドレスの学習を使用しない場合、ESXi 仮想マシンの vNIC がスイッチ ポートに接続する際、その MAC アドレスは固定アドレスになります。ESXi 仮想マシン上で稼動する仮想マシンの場合、パケットのソース MAC アドレスが異なるため、ネットワークに接続できません。MAC アドレスの学習を使用すると、vSwitch は vNIC から送信される各パケットのソース MAC アドレスを検査し、MAC アドレスを学習して、パケットが通過するのを許可します。学習された MAC アドレスが一定期間使用されない場合は、削除されます。このエイジング プロパティは設定可能ではありません。

MAC アドレスの学習は、不明なユニキャストのフラッドもサポートします。通常、ポートが受信したパケットに不明なターゲット MAC アドレスが含まれていると、そのパケットはドロップされます。不明なユニキャストのフラッドを有効にすると、ポートは、MAC アドレスの学習およびユニキャストのフラッドを有効にしているスイッチ上のすべてのポートに、不明なユニキャストトラフィックをフラッドします。このプロパティは、MAC アドレスの学習が有効である場合にのみ、デフォルトで有効になります。

MAC 管理スイッチング プロファイルは、仮想マシンの MAC アドレスを変更もサポートします。仮想マシンが MAC アドレスの変更プロパティを有効にしたポートに接続されている場合、管理コマンドを実行して vNIC の MAC アドレスを変更し、その vNIC 上でトラフィックの送受信ができます。この機能は ESXi でのみサポートされ、KVM ではサポートされません。このプロパティはデフォルトで無効になっています。

MAC アドレスの学習および MAC アドレスの変更を有効にしてセキュリティを強化する場合は、SpoofGuard も設定します。

MAC 管理スイッチング プロファイルを作成し、スイッチまたはポートにプロファイルに関連付ける方法については、『NSX-T API ガイド』を参照してください。

---

**注:** このリリースでは、MAC 管理スイッチング プロファイル機能は NSX API を介してのみ使用できます。NSX Manager ユーザー インターフェイスからは使用できません。

---

## カスタム プロファイルと論理スイッチの関連付け

カスタム スイッチング プロファイルをネットワークに適用するには、そのプロファイルを論理スイッチに関連付ける必要があります。

カスタムのスイッチング プロファイルを論理スイッチに適用すると、既存のデフォルト スイッチング プロファイルが上書きされます。このカスタム スイッチング プロファイルは、子論理スイッチ ポートに継承されます。

---

**注:** カスタム スイッチング プロファイルを論理スイッチに関連付けたが、子論理スイッチ ポートのうち 1 つに対してデフォルト スイッチング プロファイルを維持する場合は、デフォルト スイッチング プロファイルのコピーを作成し、それを特定の論理スイッチ ポートと関連付ける必要があります。

---

### 前提条件

- 論理スイッチが設定されていることを確認します。[「論理スイッチの作成」](#)を参照してください。
- カスタムのスイッチング プロファイルが設定されていることを確認します。[章 3 「論理スイッチおよび論理ポートのスイッチング プロファイルの設定」](#)を参照してください。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[スイッチング (Switching)] - [スイッチ (Switches)] の順に選択します。
- 3 論理スイッチをダブルクリックして、カスタム スイッチング プロファイルを適用します。
- 4 [管理 (Manage)] タブをクリックします。
- 5 ドロップダウン メニューからカスタムのスイッチング プロファイルのタイプを選択します。
  - [QoS]

- [ポート ミラーリング (Port Mirroring)]
- [IP アドレス検出 (IP Discovering)]
- [SpoofGuard]
- [スイッチ セキュリティ (Switch Security)]

6 [変更 (Change.)] をクリックします。

7 ドロップダウン メニューから以前に作成されたカスタムのスイッチング プロファイルを選択します。

8 [保存 (Save)] をクリックします。

これで論理スイッチとカスタム スwitchング プロファイルが関連付けられました。

9 設定を変更した新しいカスタム スwitchング プロファイルが [管理 (Manage)] タブに表示されることを確認します。

10 (オプション) [関連 (Related)] タブをクリックし、ドロップダウン メニューから [ポート (Ports)] を選択して、子論理ポートにカスタム スwitchング プロファイルが適用されていることを確認します。

#### 次のステップ

論理スイッチから継承したスイッチング プロファイルを使用しない場合は、子論理ポートにカスタム スwitchング プロファイル適用できます。[「論理スイッチ ポートへのカスタム プロファイルの関連付け」](#)を参照してください。

## 論理スイッチ ポートへのカスタム プロファイルの関連付け

論理スイッチ ポートは、VIF、ルーターへのパッチ接続、または外部ネットワークへのレイヤー 2 ゲートウェイ接続のための論理接続ポイントを提供します。また、論理スイッチ ポートは、スイッチング プロファイル、ポート統計カウンタ、および論理リンク ステータスを公開します。

論理スイッチから継承されたスイッチング プロファイルを、子の論理スイッチ ポートのための別のカスタム スwitchング プロファイルに変更することができます。

#### 前提条件

- 論理スイッチ ポートが設定されていることを確認します。[「論理スイッチへの仮想マシンの接続」](#)を参照してください。
- カスタムのスイッチング プロファイルが設定されていることを確認します。[章 3 「論理スイッチおよび論理ポートのスイッチング プロファイルの設定」](#)を参照してください。

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [スイッチング (Switching)] - [ポート (Port)]の順に選択します。
- 3 カスタムのスイッチング プロファイルを適用する論理スイッチ ポートをダブルクリックします。
- 4 [管理 (Manage)] タブをクリックします。
- 5 ドロップダウン メニューからカスタムのスイッチング プロファイルのタイプを選択します。
  - [QoS]

- [ポート ミラーリング (Port Mirroring)]
- [IP アドレス検出 (IP Discovering)]
- [SpoofGuard]
- [スイッチ セキュリティ (Switch Security)]

6 [変更 (Change)] をクリックします。

7 ドロップダウン メニューから以前に作成されたカスタムのスイッチング プロファイルを選択します。

8 [保存 (Save)] をクリックします。

これで、論理スイッチ ポートがカスタムのスイッチング プロファイルに関係付けられます。

9 設定を変更した新しいカスタム スwitchング プロファイルが [管理 (Manage)] タブに表示されることを確認します。

#### 次のステップ

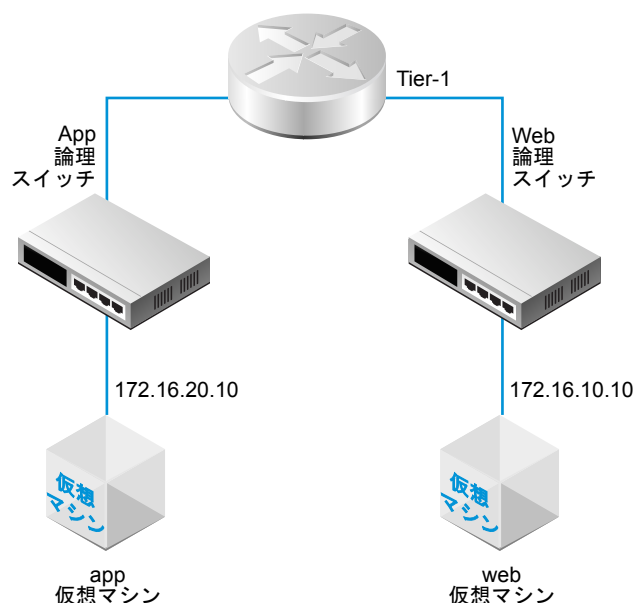
論理スイッチ ポート上でアクティビティを監視して、問題をトラブルシューティングできます。[「論理スイッチ ポート アクティビティの監視」](#)を参照してください。

## Tier-1 分散論理ルーターの設定

NSX-T 分散論理ルーターは基盤となるハードウェアから完全に分離された仮想環境でルーティング機能を再現します。Tier-1 分散論理ルーターには NSX-T 論理スイッチに接続するダウンリンク ポート、および NSX-T Tier-0 分散論理ルーターに接続するアップリンク ポートがあります。

分散論理ルーターを追加する場合、構築しているネットワーク トポロジについての計画を立てることが重要です。

図 4-1. Tier-1 分散論理ルーターのトポロジ



たとえば、この単純なトポロジは、Tier-1 分散論理ルーターに接続された 2 台の論理スイッチを示します。各論理スイッチには単一の仮想マシンが接続されています。2 台の仮想マシンのホストやホスト クラスタは同じにすることも、別々にすることもできます。分散論理ルーターで仮想マシンを分離しない場合、各仮想マシンに設定する IP アドレスには、同じサブネットを指定する必要があります。分散論理ルーターで仮想マシンを分離する場合、各仮想マシンの IP アドレスには、別のサブネットを指定する必要があります。

この章には、次のトピックが含まれています。

- Tier-1 分散論理ルーターの作成
- Tier-1 分散論理ルーターのダウンリンク ポートの追加
- Tier-1 分散論理ルーター上でのルートのアドバタイズの設定

## ■ Tier-1 分散論理ルーターのスタティック ルートの設定

# Tier-1 分散論理ルーターの作成

north バウンド物理ルーターにアクセスするには、Tier-1 ルーターが Tier-0 分散論理ルーターに接続されている必要があります。

### 前提条件

- 論理スイッチが設定されていることを確認します。[「論理スイッチの作成」](#)を参照してください。
- ネットワークアドレス変換 (NAT) 設定を実行するように、NSX Edge クラスタが展開されていることを確認します。『NSX-T インストール ガイド』を参照してください。
- Tier-1 分散論理ルーターのトポロジを理解します。[章 4 「Tier-1 分散論理ルーターの設定」](#)を参照してください。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [ルーティング (Routing)] を選択します。
- 3 [追加 (Add)] をクリックし、[Tier-1 ルーター (Tier-1 Router)] を選択します。
- 4 分散論理ルーターの名前を割り当てます。
- 5 (オプション) この Tier-1 分散論理ルーターに接続する Tier-0 分散論理ルーターを選択します。

Tier-0 分散論理ルーターが設定されていない場合は、このフィールドを空白のままにして、後でルーター設定を編集できます。

- 6 (オプション) この Tier-1 分散論理ルーターに接続する Edge クラスタを選択します。

NAT 設定に使用される Tier-1 分散論理ルーターは NSX Edge クラスタに接続される必要があります。Edge クラスタが設定されていない場合は、このフィールドを空白のままにして、後でルーター設定を編集できます。

- 7 [保存 (Save)] をクリックします。

NSX Manager のユーザー インターフェイスで、新しい分散論理ルーターがクリック可能なリンクとして表示されます。

### 次のステップ

Tier-1 分散論理ルーター用のダウンリンク ポートを作成します。[「Tier-1 分散論理ルーターのダウンリンク ポートの追加」](#)を参照してください。

# Tier-1 分散論理ルーターのダウンリンク ポートの追加

Tier-1 の分散論理ルーター上でダウンリンク ポートを作成すると、ポートは、同じサブネットにある仮想マシンのデフォルトのゲートウェイとして動作します。

### 前提条件

Tier-1 の分散論理ルーターが設定されていることを確認します。[「Tier-1 分散論理ルーターの作成」](#)を参照してください。

## 手順

- 1 Tier-1 の分散論理ルーター リンクをクリックしてポートを作成します。
- 2 [設定 (Configuration)] タブをクリックします。
- 3 [分散論理ルーター ポート] セクションの [追加 (Add)] をクリックします。
- 4 分散論理ルーター ポートの名前を割り当てます。
- 5 この接続によってスイッチ ポートを作成するのか既存のスイッチ ポートを更新するのかを選択します。  
接続が既存のスイッチ ポート用の場合は、ドロップダウン メニューからポートを選択します。
- 6 ルーター ポート IP アドレスを CIDR 表記で入力します。  
たとえば、IP アドレスを 172.16.10.1/24 のように表記します。  
また、あらかじめ設定された DHCP サービスの IP アドレスを入力することもできます。
- 7 [保存 (Save)] をクリックします。
- 8 (オプション) 手順 1 ~ 7 を繰り返して、追加の Tier-1 分散論理ルーター ポートを作成します。
- 9 Tier-1 分散論理ルーターが East-West 仮想マシン トラフィックをルーティングできることを確認します。

この例では、Tier-1 分散論理ルーターには、2 台の論理スイッチに接続するダウンリンク ポートが 2 つ あります。各論理スイッチには仮想マシンが接続されています。仮想マシンは互いに ping を送信することができます。

```
web-virtual-machine$ ping 172.16.20.10
PING 172.16.20.10 (172.16.20.10): 56(84) data bytes
64 bytes from 172.16.20.10: icmp_req=0 ttl=64 time=178 ms
^C
--- 172.16.20.10 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 178 ms/178 ms/178 ms/0.000 ms
```

```
app-virtual-machine$ ping 172.16.10.10
PING 172.16.10.10 (172.16.10.10): 56(84) data bytes
64 bytes from 172.16.10.10: icmp_req=0 ttl=64 time=178 ms
^C
--- 172.16.10.10 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 178 ms/178 ms/178 ms/0.000 ms
```

## 次のステップ

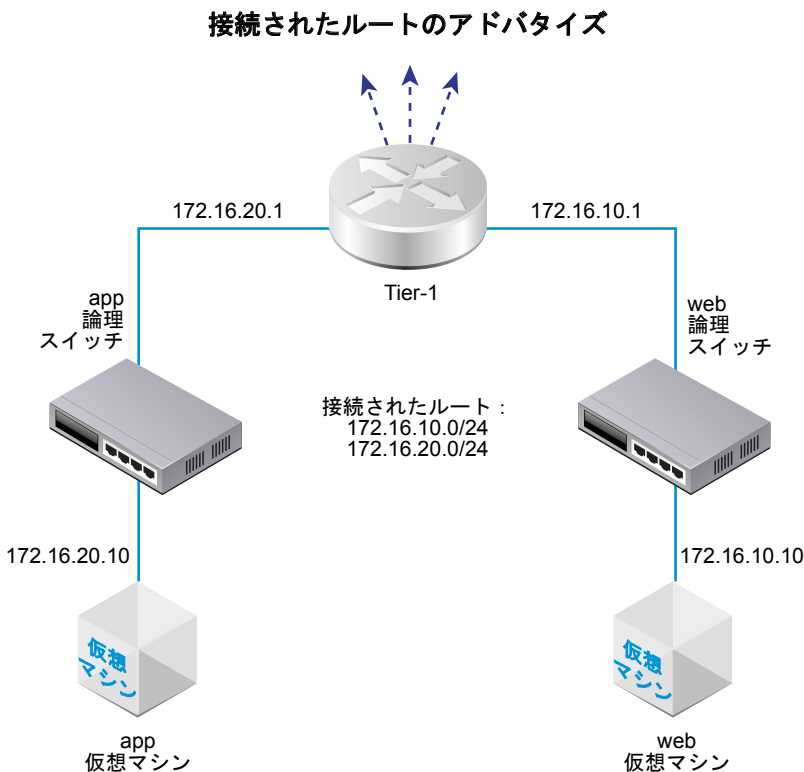
ルートのアドバタイズを有効にして、仮想マシンと外部の物理ネットワーク間、または同じ Tier-0 分散論理ルーターに接続された異なる Tier-1 分散論理ルーター間に North-South 接続を提供します。[「Tier-1 分散論理ルーター上で  
のルートのアドバタイズの設定」](#)を参照してください。



## Tier-1 分散論理ルーター上でのルートのアドバタイズの設定

異なる Tier-1 分散論理ルーターに接続している複数の論理スイッチに接続された仮想マシンにレイヤー 3 接続を提供するには、Tier-0 への Tier-1 ルートのアドバタイズを有効にする必要があります。Tier-1 と Tier-0 分散論理ルーター間のルーティング プロトコルまたはスタティック ルートを設定する必要はありません。ルートのアドバタイズを有効にすると、NSX-T は NSX-T スタティック ルートを自動的に作成します。

たとえば、他のピア ルーターを介して仮想マシンとの接続を提供するには、Tier-1 分散論理ルーターでは接続されたルートに対するルートのアドバタイズを設定する必要があります。接続されたルートをすべてアドバタイズしない場合、どのルートをアドバタイズするかを指定することができます。



### 前提条件

- 仮想マシンが論理スイッチに接続されていることを確認します。[章 2 「論理スイッチの作成と仮想マシン接続の設定」](#)を参照してください。
- Tier-1 分散論理ルーターのダウンリンク ポートが設定されていることを確認します。[Tier-1 分散論理ルーターのダウンリンク ポートの追加](#)を参照してください。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 [ルーティング (Routing)] を選択します。
- 3 Tier-1 分散論理ルーターをクリックします。

- 4 [ルーティング] ドロップダウン メニューから [ルートのアドバタイズ (Route Advertisement)] を選択します。
- 5 [編集 (Edit)] をクリックして [ステータス] ボタンが [有効] であることを確認し、ルートのアドバタイズを有効にします。
- 6 すべてのルートをアドバタイズするか選択したルートをアドバタイズするかを指定します。
  - [編集 (Edit)] をクリックし、[NSX に接続されたすべてのルートをアドバタイズ (Advertise All NSX Connected Routes)] を選択します。
  - [追加 (Add)] をクリックして、アドバタイズされるルートについての情報を入力します。ルートごとに、名前とルート プリフィックスを CIDR 形式で入力することができます。
- 7 [ステータス (Status)] 切り替えボタンをクリックして [ルートをアドバタイズ] を有効にします。

次はその例です。

The screenshot shows the NSX-T management console. On the left, a sidebar lists logical routers: 'Logical Router' (with an up arrow), 'router1\_496d3...', 'T0', and 'T1' (which is selected and highlighted in green). The main area is titled 'ROUTING' and shows the configuration for 'T1'. The 'Routing' tab is active, displaying the 'Route Advertisement' settings. The settings are as follows:

Route Advertisement	
Status	● Enabled
Advertise All NSX Connected Routes	● Yes
Advertise NAT Routes	● Yes
Advertise Static Routes	● No

- 8 [保存 (Save)] をクリックします。

#### 次のステップ

Tier-0 分散分散論理ルーター トポロジについて理解し、Tier-0 分散論理ルーターを作成します。[章 5 「Tier-0 分散論理ルーターの設定」](#) を参照してください。

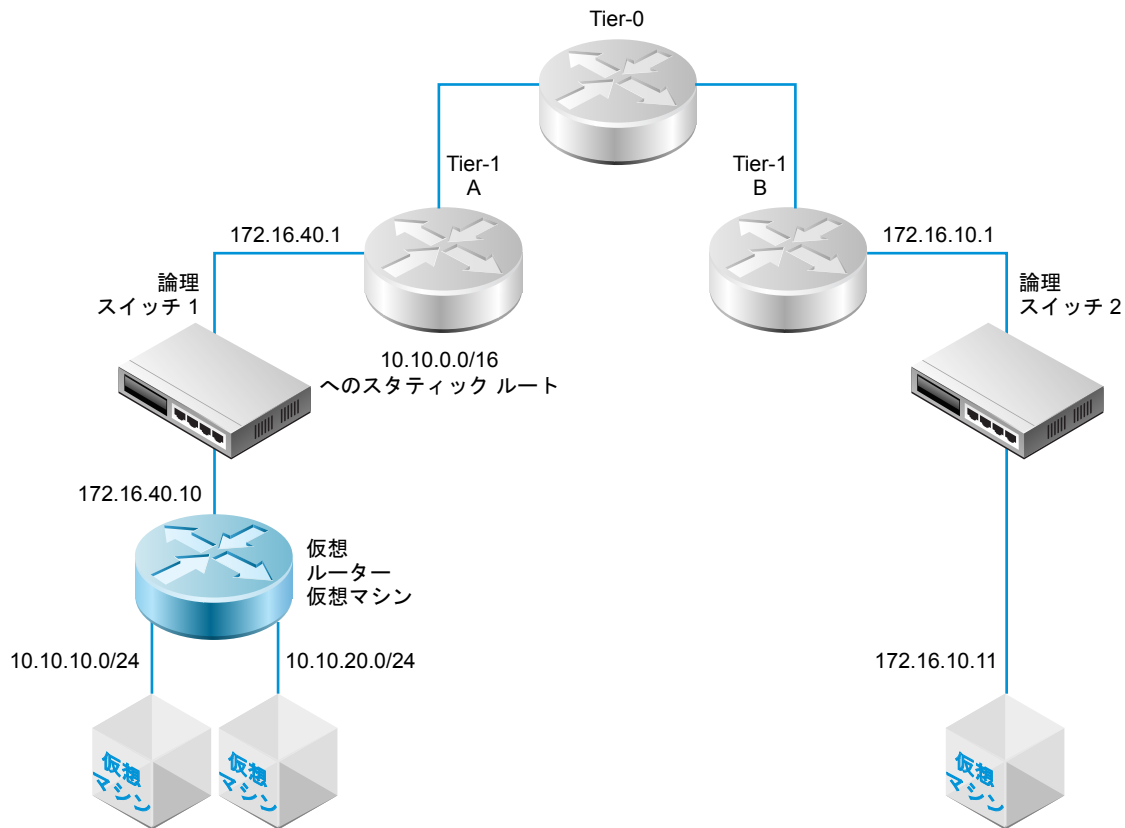
Tier-0 分散論理ルーターがすでに Tier-1 分散論理ルーターに接続されている場合は、Tier-0 ルーターが Tier-1 ルーターに接続されたルートを学習していることを確認することができます。[「Tier-0 ルーターが Tier-1 ルーターからルートを学習したことの確認」](#) を参照してください。

## Tier-1 分散論理ルーターのスタティック ルートの設定

Tier-1 分散論理ルーターのスタティック ルートを設定して、NSX-T と仮想ルーター経由でアクセス可能なネットワーク セットとの接続を可能にすることができます。

たとえば、次の図では、Tier-1 A 分散論理ルーターに NSX-T 論理スイッチへのダウンリンク ポートがあります。このダウンリンク ポート (172.16.40.1) は、仮想ルーター仮想マシンのデフォルト ゲートウェイとして機能します。仮想ルーター仮想マシンと Tier-1 A は、同じ NSX-T 論理スイッチを介して接続されています。Tier-1 分散論理ルーターのスタティック ルート 10.10.0.0/16 は、仮想ルーターを介して使用可能なネットワークを要約しています。Tier-1 A には、Tier-1 B へのスタティック ルートをアドバタイズする、ルート アドバタイズが設定されています。

図 4-2. Tier-1 分散論理ルーターのスタティック ルート トポロジ



#### 前提条件

ダウンリンク ポートが設定されていることを確認します。[\[Tier-1 分散論理ルーターのダウンリンク ポートの追加\]](#)を参照してください。

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [ルーティング (Routing)] を選択します。
- 3 Tier-1 分散論理ルーターを選択します。
- 4 [ルーティング (Routing)] タブをクリックし、ドロップダウン メニューから [スタティック ルート (Static Route)] を選択します。
- 5 [追加 (Add)] を選択します。
- 6 ネットワーク アドレスを CIDR 形式で入力します。  
たとえば、10.10.10.0/16 と入力します。
- 7 [行を挿入 (Insert Row)] をクリックし、ネクスト ホップ IP アドレスを追加します。  
たとえば、172.16.40.10 と入力します。

- 8 [保存 (Save)] をクリックします。

新しく作成したスタティック ルート ネットワーク アドレスが、行内に表示されます。

- 9 Tier-1 分散論理ルーターから、[ルーティング (Routing)] > [ルート アドバタイズ (Route Advertisement)] の順に選択します。

- 10 [編集 (Edit)] をクリックし、[スタティック ルートのアドバタイズ (Advertise Static Routes)] を選択します。

- 11 [保存 (Save)] をクリックします。

スタティック ルートが NSX-T オーバーレイ全体に伝達されます。

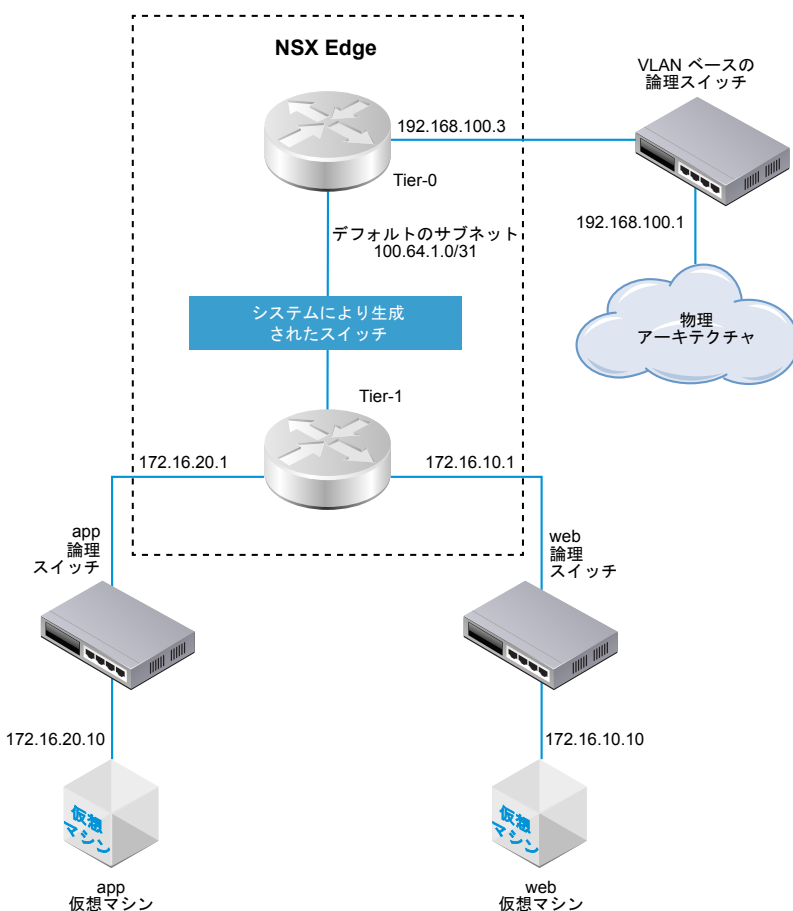
## Tier-0 分散論理ルーターの設定

NSX-T 分散論理ルーターは基盤となるハードウェアから完全に分離された仮想環境でルーティング機能を再現します。Tier-0 分散論理ルーターは、論理ネットワークと物理ネットワークの間にオン/オフ ゲートウェイ サービスを提供します。

1 つの NSX Edge クラスターが複数の Tier-0 分散論理ルーターをバックアップすることができます。Tier-0 ルーターは BGP のダイナミック ルーティング プロトコルおよび ECMP をサポートします。

Tier-0 分散論理ルーターを追加する場合、構築しているネットワーク トポロジについての計画を立てることが重要です。

図 5-1. Tier-0 分散論理ルーターのトポロジ



説明を簡単にするため、サンプルトポロジは、単一の NSX Edge ノード上でホストされた単一の Tier-0 分散論理ルーターに接続された単一の Tier-1 分散論理ルーターを示します。これは推奨されるトポロジではないことに注意してください。理想的には、分散論理ルーターの設計を十分に活用するには最低 2 つの NSX Edge ノードが必要です。

Tier-1 分散論理ルーターには Web 論理スイッチおよび App 論理スイッチがあり、それぞれの仮想マシンが接続されています。Tier-1 ルーターと Tier-0 ルーター間のルーター リンク スイッチは、Tier-0 ルーターに Tier-1 ルーターを接続すると自動的に作成されます。これで、このスイッチには「システムにより生成」というラベルが付けられます。この章には、次のトピックが含まれています。

- [Tier-0 分散論理ルーターの作成](#)
- [Tier-0 と Tier-1 の接続](#)
- [VLAN 論理スイッチへの Tier-0 分散論理ルーターの接続](#)
- [スタティック ルートの設定](#)
- [BGP 設定オプション](#)
- [Tier-0 分散論理ルーター上の BFD の設定](#)
- [Tier-0 分散論理ルーターのルート再配分を有効にする](#)
- [ECMP ルーティングの理解](#)
- [IP プリフィックス リストの作成](#)
- [ルート マップの作成](#)

## Tier-0 分散論理ルーターの作成

Tier-0 分散論理ルーターには NSX-T Tier-1 分散論理ルーターに接続するダウンリンク ポート、および外部ネットワークに接続するアップリンク ポートがあります。

### 前提条件

- 1 つ以上の NSX Edge がインストールされていることを確認します。『NSX-T インストール ガイド』を参照してください。
- NSX Controller クラスタが安定していることを確認します。
- Edge クラスタが設定されていることを確認します。『NSX-T インストール ガイド』を参照してください。
- Tier-0 分散論理ルーターのネットワーク トポロジを理解します。「[章 5 「Tier-0 分散論理ルーターの設定」](#)」を参照してください。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [ルーティング (Routing)] を選択します。
- 3 [追加] をクリックして Tier-0 分散論理ルーターを作成します。
- 4 ドロップダウン メニューから [Tier-0 ルーター] を選択します。

- 5 Tier-0 分散論理ルーターの名前を割り当てます。
- 6 この Tier-0 論理ルーターをバックアップする既存の Edge クラスタをドロップダウン メニューから選択します。
- 7 (オプション) 高可用性モードを選択します。

デフォルトでは、アクティブ/アクティブモードが使用されます。アクティブ/アクティブモードでは、トラフィックはすべてのメンバー間で負荷分散されています。アクティブ/スタンバイ モードでは、すべてのトラフィックは選ばれたアクティブ メンバーによって処理されます。アクティブ メンバーが失敗すると、新しいメンバーが選ばれてアクティブになります。

- 8 (オプション) [詳細] タブをクリックして Tier-0 内の移行サブネットのサブネットを入力します。

これは、分散ルーターへの Tier-0 サービス ルーターに接続するサブネットです。空白のままにすると、デフォルトの 169.0.0.0/28 サブネットが使用されます。

- 9 (オプション) [詳細] タブをクリックして Tier-0 と Tier-1 間の移行サブネットのサブネットを入力します。

これは、Tier-0 ルーターを、この Tier-0 ルーターに接続する任意の Tier-1 ルーターに接続するサブネットです。空白のままにすると、これらの Tier-0 と Tier-1 の接続に割り当てられるデフォルトのアドレス空間は 100.64.0.0/10 になります。Tier-0 から Tier-1 の各ピア接続には、100.64.0.0/10 アドレス空間内で /31 サブネットが提供されます。

- 10 [保存] をクリックします。

新しい Tier-0 分散論理ルーターがリンクとして表示されます。

- 11 (オプション) Tier-0 分散論理ルーター リンクをクリックしてサマリを確認します。

#### 次のステップ

Tier-1 分散論理ルーターをこの Tier-0 分散論理ルーターに接続します。

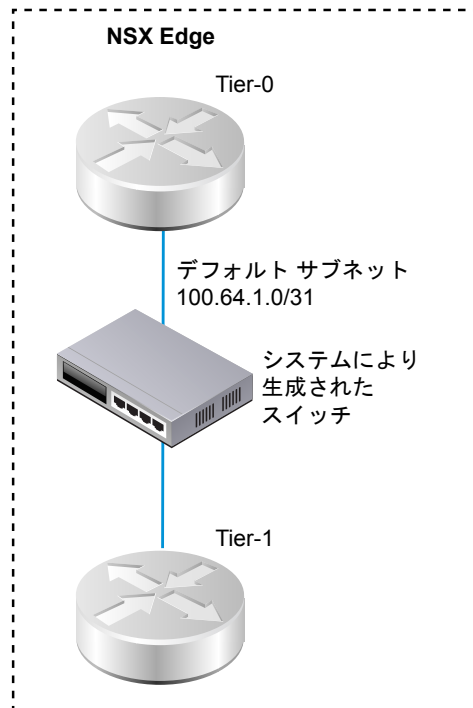
Tier-0 分散論理ルーターを VLAN 論理スイッチに接続するように設定し、外部ネットワークへのアップリンクを作成します。「[VLAN 論理スイッチへの Tier-0 分散論理ルーターの接続](#)」を参照してください。

## Tier-0 と Tier-1 の接続

Tier-0 分散論理ルーターを Tier-1 分散論理ルーターに接続し、Tier-1 分散論理ルーターが Northbound および East-West ネットワーク接続を実現できるようにします。

Tier-1 分散論理ルーターを Tier-0 分散論理ルーターに接続すると、2 つのルーター間にルーター リンク スイッチが作成されます。トポロジ内ではこのスイッチに「システム生成」というラベルが付けられます。これらの Tier-0 と Tier-1 の接続に割り当てられるデフォルトのアドレス空間は 100.64.0.0/10 です。Tier-0 から Tier-1 の各ピア接続には、100.64.0.0/10 アドレス空間内で /31 サブネットが提供されます。オプションとして、アドレス空間を Tier-0 の [サマリ] - [詳細] で設定できます。

次の図はサンプルのトポロジを示したものです。



#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [ルーティング (Routing)] を選択します。
- 3 Tier-1 分散論理ルーターを選択します。
- 4 [サマリ] タブで [編集] をクリックします。
- 5 ドロップダウン メニューから Tier-0 分散論理ルーターを選択します。
- 6 (オプション) ドロップダウン メニューから Edge クラスタを選択します。

ルーターを NAT などのサービスに使用する場合は、Tier-1 ルーターが Edge デバイスによってバックアップされる必要があります。Edge クラスタを選択しない場合、Tier-1 ルーターは NAT を実行することができません。

- 7 メンバーおよび優先メンバーを指定します。

Edge クラスタを選択し、メンバーおよび優先メンバーのフィールドを空白のままにすると、NSX-T は指定されたクラスタからバックアップ用の Edge デバイスを設定します。

- 8 [保存] をクリックします。
- 9 Tier-1 ルーターの [設定] タブをクリックして、新しいポイントツーポイントのリンク ポート IP アドレスが作成されていることを確認します。

たとえば、リンク ポートの IP アドレスは 100.64.1.1/31 のようになります。

- 10 ナビゲーション パネルから Tier-0 分散論理ルーターを選択します。



- 11 Tier-0 ルーターの [設定] タブをクリックして、新しいポイントツーポイントのリンク ポート IP アドレスが作成されていることを確認します。

たとえば、リンク ポートの IP アドレスは 100.64.1.1/31 のようになります。

#### 次のステップ

Tier-0 ルーターが Tier-1 ルーターによってアドパタイズされるルートを学習していることを確認します。

## Tier-0 ルーターが Tier-1 ルーターからルートを学習したことの確認

Tier-1 分散論理ルーターが Tier-0 分散論理ルーターにルートをアドパタイズすると、ルートは Tier-0 ルーターのルーティング テーブルに NSX-T スタティック ルートとしてリストされます。

#### 手順

- 1 NSX Edge で、**get logical-routers** コマンドを実行して Tier-0 サービス ルーターの VRF 番号を検出します。

```
nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf        : 7
type       : SERVICE_ROUTER_TIER1

Logical Router
UUID       : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf        : 8
type       : DISTRIBUTED_ROUTER
```

- 2 **vrf <number>** コマンドを実行して Tier-0 サービス ルーターのコンテキストを入力します。

```
nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>
```

- 3 Tier-0 サービス ルーター上で **get route** コマンドを実行し、期待されたルートがルーティング テーブルに表示されるのを確認します。

Tier-1 ルーターがルートをアドバタイズしているため、NSX-T スタティック ルート (ns) が Tier-0 ルーターによって学習されたことに注意してください。

```
nsx-edge1(tier0_sr)> get route
```

```
Flags: c - connected, s - static, b - BGP, ns - nsx_static
```

```
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT
```

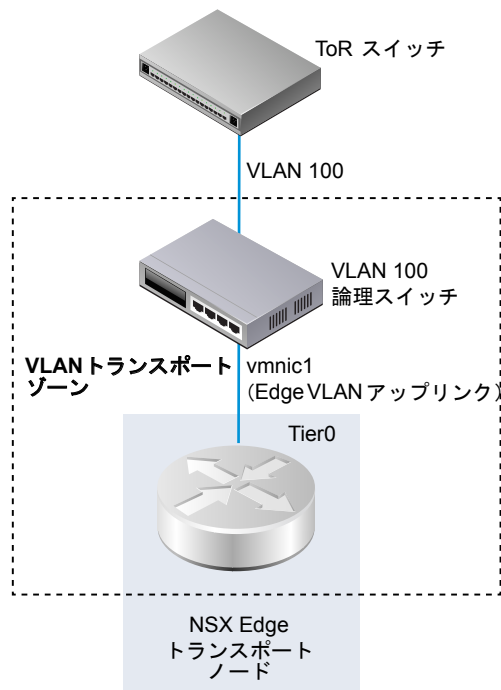
```
Total number of routes: 7
```

```
b   10.10.10.0/24      [20/0]      via 192.168.100.254
rl  100.91.176.0/31   [0/0]      via 169.254.0.1
c   169.254.0.0/28    [0/0]      via 169.254.0.2
ns  172.16.10.0/24 [3/3] via 169.254.0.1 ns 172.16.20.0/24 [3/3] via 169.254.0.1
c   192.168.100.0/24  [0/0]      via 192.168.100.2
```

## VLAN 論理スイッチへの Tier-0 分散論理ルーターの接続

Edge アップリンクを作成するには、Tier-0 ルーターを VLAN スイッチに接続します。

次の単純なトポロジは、VLAN トランスポート ゾーン内部の VLAN 論理スイッチを示します。VLAN 論理スイッチには、Edge の VLAN アップリンクのための TOR ポートの VLAN ID と一致する VLAN ID があります。



## 前提条件

VLAN 論理スイッチを作成します。[「NSX Edge アップリンク用の VLAN 論理スイッチの作成」](#)を参照してください。

Tier-0 ルーターを作成します。

## 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [ルーティング (Routing)] を選択します。
- 3 Tier-0 分散論理ルーターを選択します。
- 4 [設定 (Configuration)] タブから、新しい分散論理ルーター ポートを追加します。
- 5 uplink など、ポートの名前を入力します。
- 6 [アップリンク (Uplink)] タイプを選択します。
- 7 Edge トランスポート ノードを選択します。
- 8 VLAN 論理スイッチを選択します。
- 9 TOR スイッチに接続しているポートと同じサブネットにある IP アドレスを CIDR 形式で入力します。

次はその例です。

New Router Port

Name: \*

uplink

Description:

Type:

☒ Uplink

☐ Downlink

Transport Node: \*

TN-edgenode-02a

Logical Switch:

LS.VLAN.240

OR Create a New Switch

Logical Switch Port:

☒ Attach to new switch port

Switch Port Name:

☐ Attach to existing switch port

IP Address/mask: \*

192.168.100.3/24

Save

Cancel

Tier-0 ルーターのための新しいアップリンク ポートが追加されます。

#### 次のステップ

BGP またはスタティック ルートを設定します。

## Tier-0 分散論理ルーターおよび TOR の接続の確認

Tier-0 ルーターからのアップリンクで動作するようにルーティングするには、トップオブラック (TOR) デバイスとの接続が必要です。

#### 前提条件

- Tier-0 分散論理ルーターが VLAN 論理スイッチに接続されていることを確認します。「[\[VLAN 論理スイッチへの Tier-0 分散論理ルーターの接続\]](#)」を参照してください。

#### 手順

- 1 NSX Manager CLI にログインします。
- 2 NSX Edge で、**get logical-routers** コマンドを実行して Tier-0 サービス ルーターの VRF 番号を検出します。

```
nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf        : 7
type       : SERVICE_ROUTER_TIER1

Logical Router
UUID       : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf        : 8
type       : DISTRIBUTED_ROUTER
```

- 3 **vrf <number>** コマンドを実行して Tier-0 サービス ルーターのコンテキストを入力します。

```
nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>
```

- 4 Tier-0 サービス ルーターで **get route** コマンドを実行し、想定したルートがルーティング テーブルに表示されていることを確認します。

TOR へのルートは接続済み (c) と表示されます。

```
nsx-edge1(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

Total number of routes: 7

b   10.10.10.0/24      [20/0]      via 192.168.100.254
rl  100.91.176.0/31    [0/0]      via 169.254.0.1
c   169.254.0.0/28     [0/0]      via 169.254.0.2
ns  172.16.10.0/24     [3/3]      via 169.254.0.1
ns  172.16.20.0/24     [3/3]      via 169.254.0.1
c  192.168.100.0/24   [0/0] via 192.168.100.2
```

- 5 TOR に ping を送信します。

```
nsx-edge1(tier0_sr)> ping      192.168.100.254
PING 192.168.100.254 (192.168.100.254): 56 data bytes
64 bytes from 192.168.100.254: icmp_seq=0 ttl=64 time=2.822 ms
64 bytes from 192.168.100.254: icmp_seq=1 ttl=64 time=1.393 ms
^C
nsx-edge1>
--- 192.168.100.254 ping statistics ---
3 packets transmitted, 2 packets received, 33.3% packet loss
round-trip min/avg/max/stddev = 1.393/2.107/2.822/0.715 ms
```

Tier-0 分散論理ルーターと物理ルーターとの間でパケットが送信され、接続が確認されます。

#### 次のステップ

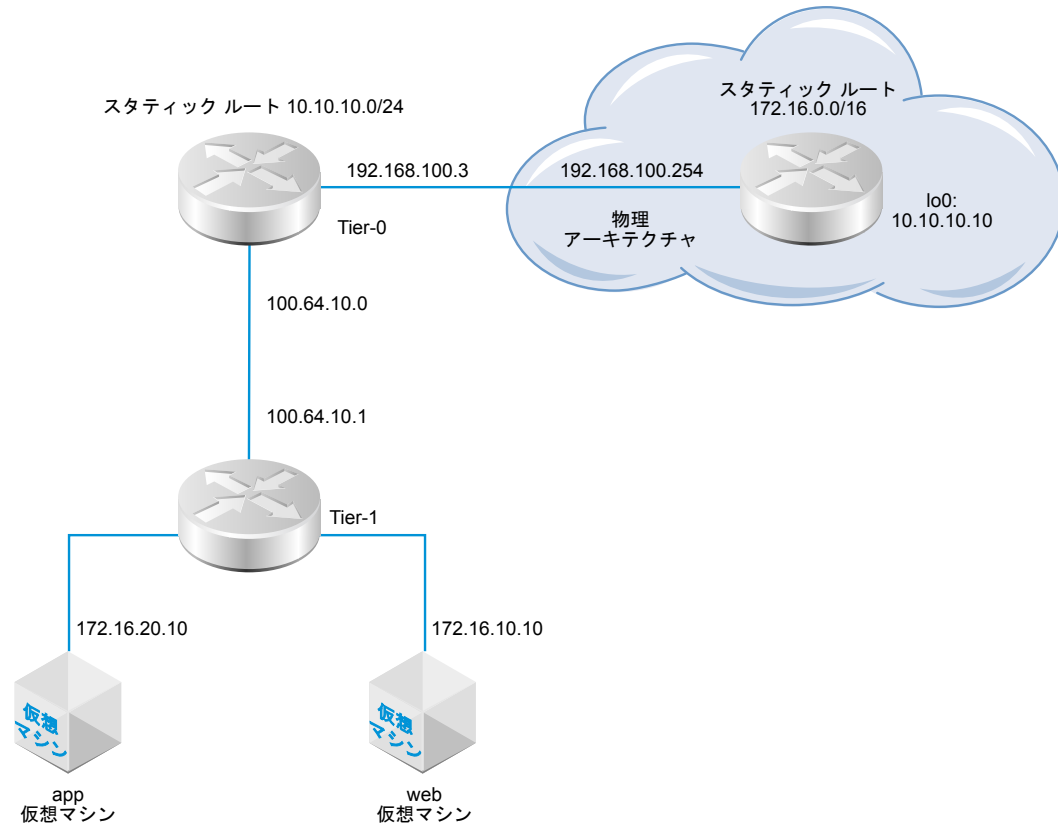
ネットワーク要件に従って、スタティック ルートまたは BGP を設定できます。[「スタティック ルートの設定」](#) または [「Tier-0 分散論理ルーター上の BGP の設定」](#) を参照してください。

## スタティック ルートの設定

Tier-0 ルーター上で外部ネットワークへのスタティック ルートを設定することができます。スタティック ルートを設定した後で Tier-0 から Tier-1 にルートをアドバタイズする必要はありません。Tier-1 ルーターには接続された Tier-0 ルーターへのデフォルトのスタティック ルートが自動的に設定されているからです。

スタティック ルート トポロジは、10.10.10.0/24 プリフィックスへのスタティック ルートを持つ Tier-0 分散論理ルーターの物理アーキテクチャを示します。テストの目的で、10.10.10.10/32 アドレスは外部ルーターのループバックインターフェイス上で設定されます。外部ルーターには、app 仮想マシンと web 仮想マシンにアクセスするための 172.16.0.0/16 プリフィックスへのスタティック ルートがあります。

図 5-2. スタティック ルート トポロジ



#### 前提条件

- 物理ルーターと Tier-0 分散論理ルーターが接続されていることを確認します。[「Tier-0 分散論理ルーターおよび TOR の接続の確認」](#)を参照してください。
- 接続されたルートを実アドバタイズするように Tier-1 ルーターが設定されていることを確認します。[「Tier-1 分散論理ルーターの作成」](#)を参照してください。

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [ルーティング (Routing)] を選択します。
- 3 Tier-0 分散論理ルーターを選択します。
- 4 [ルーティング (Routing)] タブをクリックし、ドロップダウン メニューから [スタティック ルート (Static Route)] を選択します。
- 5 [追加 (Add)] を選択します。

- 6 ネットワーク アドレスを CIDR 形式で入力します。

例 : 10.10.10.0/24

- 7 [行を挿入 (Insert Row)] をクリックしてネクストホップ IP アドレスを追加します。

例 : 192.168.100.254

- 8 [保存 (Save)] をクリックします。

新しく作成されたスタティック ルート ネットワーク アドレスが行に表示されます。

#### 次のステップ

スタティック ルートが適切に設定されていることを確認します。[「スタティック ルートの確認」](#)を参照してください。

## スタティック ルートの確認

スタティック ルートが接続されたことを確認するには CLI を使用します。また、外部ルーターが内部仮想マシンに ping を送信できることと、内部仮想マシンが外部ルーターに ping を送信できることも確認します。

#### 前提条件

スタティック ルートが設定されていることを確認します。[「スタティック ルートの設定」](#)を参照してください。

#### 手順

- 1 NSX Manager CLI にログインします。

## 2 スタティック ルートを確認します。

- a サービス ルーターの UUID 情報を取得します。

```
get logical-routers
```

```
nsx-edge1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 2
type       : TUNNEL

Logical Router
UUID       : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf        : 4
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf        : 5
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : a6ee6316-2212-4171-99cc-930c98bcad7f
vrf        : 6
type       : DISTRIBUTED_ROUTER
```

- b 出力から UUID 情報を見つけます。

```
Logical Router
UUID       : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf        : 4
type       : SERVICE_ROUTER_TIER0
```

- c スタティック ルートが動作することを確認します。

```
get logical-router d40bbfa4-3e3d-4178-8615-6f42ea335037 static
```

```
Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

s    10.10.10.0/24      [1/1]      via 192.168.100.254
rl   100.64.1.0/31     [0/0]      via 169.0.0.1
ns   172.16.10.0/24    [3/3]      via 169.0.0.1
ns   172.16.20.0/24    [3/3]      via 169.0.0.1
```



- 3 内部仮想マシンに ping を送信して、NSX-T オーバーレイを介して内部仮想マシンにアクセスできることを、外部ルーターから確認します。

- a 外部ルーターに接続します。

ping 172.16.10.10

```
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=62 time=127 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=62 time=1.96 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.966/64.793/127.620/62.827 ms
```

- b ネットワーク接続を確認します。

tracert 172.16.10.10

```
tracert to 172.16.10.10 (172.16.10.10), 30 hops max, 60 byte packets
 1  192.168.100.3 (192.168.100.3)  0.640 ms  0.575 ms  0.696 ms
 2  100.64.1.1 (100.64.1.1)  0.656 ms  0.604 ms  0.578 ms
 3  172.16.10.10 (172.16.10.10)  3.397 ms  3.703 ms  3.790 ms
```

- 4 仮想マシンから外部 IP アドレスに ping を送信します。

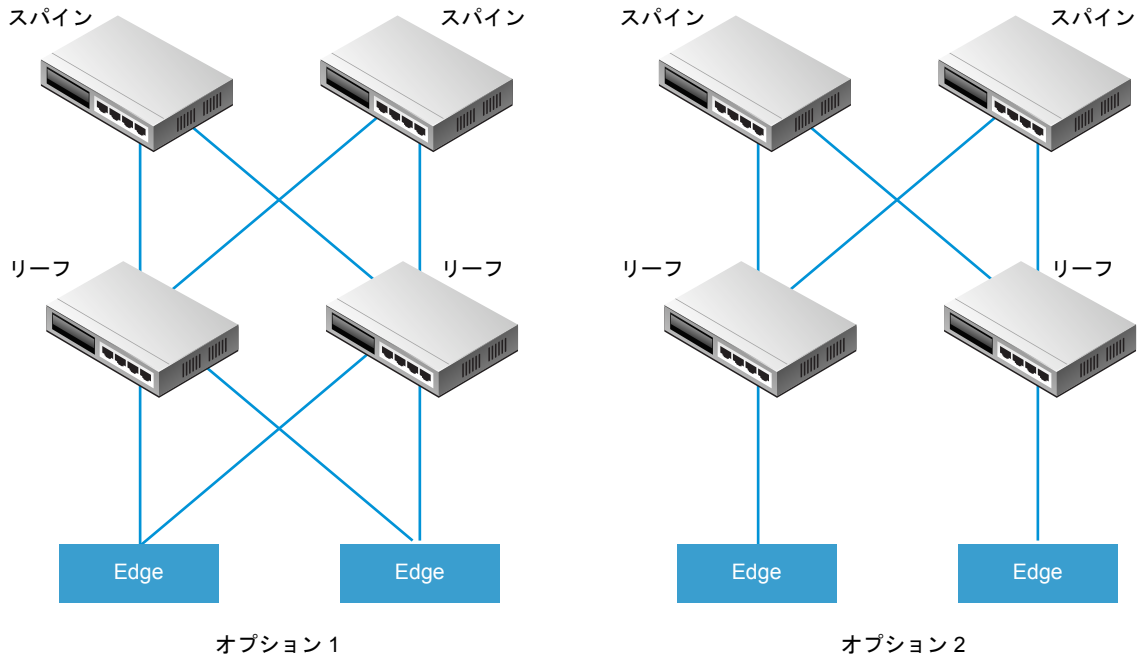
ping 10.10.10.10

```
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_req=1 ttl=62 time=119 ms
64 bytes from 10.10.10.10: icmp_req=2 ttl=62 time=1.93 ms
^C
--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.936/60.865/119.795/58.930 ms
```

## BGP 設定オプション

Tier-0 分散論理ルーターの利点を十分に活用するには、Tier-0 ルーターと外部のトップオブラック ピアの間で BGP を使用し、トポロジに冗長性と対称性を設定する必要があります。この設計によって、リンクおよびノードに障害が発生しても接続を維持することができます。

設定にはアクティブ/アクティブおよびアクティブ/スタンバイの 2 つのモードがあります。次の図は、対称設定の 2 つのオプションを示したものです。各トポロジには 2 つの NSX Edge ノードが示されています。アクティブ/アクティブ設定の場合、Tier-0 アップリンク ポートを作成するときに、各アップリンク ポートに対して最大 8 つの NSX Edge トランスポート ノードを関連付けることができます。各 NSX Edge ノードは 2 つのアップリンクを持つことができます。



オプション 1 の場合、物理的なリーフノードルーターを設定するときに、NSX Edge との間に BGP ネイバーシップが必要です。ルートの再配分には、すべての BGP ネイバーと同等の BGP メトリックを持つ同じネットワーク プリフィックスを含める必要があります。Tier-0 の分散論理ルーターの設定では、すべてのリーフノードルーターは BGP ネイバーとして設定する必要があります。

Tier-0 ルーターの BGP ネイバーの設定で、ローカル アドレス（ソース IP アドレス）を指定しない場合、BGP ネイバー設定は、Tier-0 の分散論理ルーター アップリンクに関連付けられたすべての NSX Edge ノードに送信されます。ローカル アドレスを設定する場合、その IP アドレスを所有するアップリンクを持つ NSX Edge ノードに影響します。

オプション 1 の場合、アップリンクが NSX Edge ノードの同じサブネットにある場合、ローカル アドレスは通常省略することができます。NSX Edge ノードのアップリンクが異なるサブネットにある場合は、ローカル アドレスを Tier-0 ルーターの BGP ネイバー設定で指定し、設定が関連付けられたすべての NSX Edge ノードに影響しないようにします。

オプション 2 の場合は、Tier-0 分散論理ルーター設定に Tier-0 サービス ルーターのローカル IP アドレスが含まれていることを確認します。リーフノードルーターは、ルーターが BGP ネイバーとして直接接続される NSX Edge のみを使用して設定します。

## Tier-0 分散論理ルーター上の BGP の設定

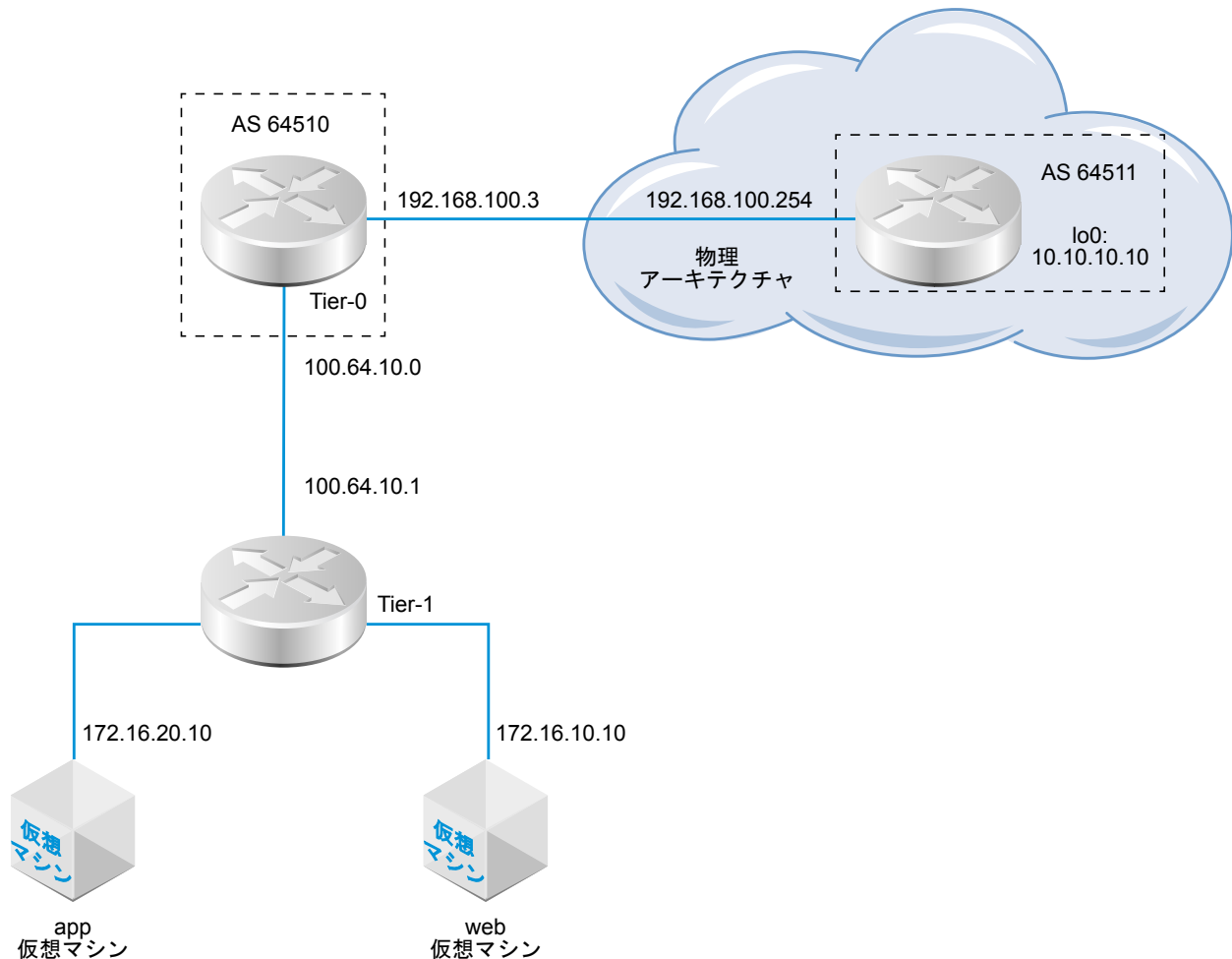
仮想マシンとその外部との間でアクセスを有効にするために、Tier-0 分散論理ルーターと物理インフラストラクチャ内のルーター間に外部 BGP (eBGP) 接続を設定することができます。

BGP を設定する場合は、Tier-0 分散論理ルーターのためのローカルの自律システム (AS) 番号を設定する必要があります。たとえば、次のトポロジはローカルの AS 番号が 64510 であることを示します。また、物理ルーターのリモート AS 番号を設定する必要もあります。この例では、リモート AS 番号は 64511 です。リモート ネイバー IP アドレスは 192.168.100.254 です。ネイバーは、Tier-0 分散論理ルーター上のアップリンクと同じ IP サブネットにある必要があります。BGP マルチホップはサポートされていません。

テストの目的で、10.10.10.10/32 アドレスは外部ルーターのループバック インターフェイス上で設定されます。

**注:** Edge ノードで BGP セッションを形成するために使用されるルーターの ID は、Tier-0 分散論理ルーターのアップリンクに設定された IP アドレスから自動的に選択されます。ルーターの ID が変更されると、Edge ノード上の BGP セッションでフラッピングが発生する場合があります。これは、ルーター ID 用に自動的に選択された IP アドレスが削除された場合や、その IP アドレスが割り当てられた分散論理ルーター ポートが削除された場合に発生する可能性があります。

図 5-3. BGP 接続トポロジ



#### 前提条件

- 接続されたルートをアドバタイズするように Tier-1 ルーターが設定されていることを確認します。[「Tier-1 分散論理ルーター上でのルートのアドバタイズの設定」](#)を参照してください。これは厳密には BGP 設定のための前提条件ではありません。しかし、2 層トポロジで Tier-1 ネットワークを BGP に再配分する計画の場合は、この手順が必要です。
- Tier-0 ルーターが設定されていることを確認します。[「Tier-0 分散論理ルーターの作成」](#)を参照してください。
- Tier-0 分散論理ルーターが Tier-1 分散論理ルーターからのルートを学習したことを確認します。[「Tier-0 ルーターが Tier-1 ルーターからルートを学習したことの確認」](#)を参照してください。

## 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [ルーティング (Routing)] を選択します。
- 3 Tier-0 分散論理ルーターを選択します。
- 4 [ルーティング (Routing)] タブをクリックし、ドロップダウン メニューから [ボーダー ゲートウェイ プロトコル (BGP)] を選択します。
- 5 [編集 (Edit)] をクリックしてローカル AS 番号を設定し、[保存 (Save)] をクリックします。  
例：64510。
- 6 [ステータス (Status)] 切り替えボタンをクリックして BGP を有効にします。  
[ステータス] ボタンには [有効] と表示される必要があります。
- 7 (オプション) ルート集約を設定し、グレースフル リスタートを有効にして、ECMP を有効にします。  
グレースフル リスタートがサポートされるのは、Tier-0 ルーターに関連付けられた Edge クラスターの Edge ノードが 1 台の場合のみです。
- 8 [保存 (Save)] をクリックします。
- 9 [ネイバー] セクションの [追加 (Add)] をクリックして BGP ネイバーを追加します。
- 10 ネイバー IP アドレスを入力します。  
例：192.168.100.254。
- 11 (オプション) ドロップダウン メニューからローカル アドレスを選択します。
- 12 リモートの AS 番号を入力します。  
例：64511
- 13 (オプション) タイマー（キープ アライブ時間とホールド ダウン時間）およびパスワードを設定します。
- 14 (オプション) アドレス ファミリーを追加して、ルート フィルタおよびルート マップを設定します。

## 次のステップ

BGP が適切に動作しているかをテストします。[「Tier-0 サービス ルーターからの BGP 接続の確認」](#) を参照してください。

## Tier-0 サービス ルーターからの BGP 接続の確認

ネイバーへの BGP 接続が確立されていることを Tier-0 サービス ルーターから確認するには CLI を使用します。

### 前提条件

BGP が設定されていることを確認します。「[Tier-0 分散論理ルーター上の BGP の設定](#)」を参照してください。

## 手順

- 1 NSX Manager CLI にログインします。

- 2 NSX Edge で、`get logical-routers` コマンドを実行して Tier-0 サービス ルーターの VRF 番号を検出します。

```
nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf        : 7
type       : SERVICE_ROUTER_TIER1

Logical Router
UUID       : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf        : 8
type       : DISTRIBUTED_ROUTER
```

- 3 `vrf <number>` コマンドを実行して Tier-0 サービス ルーターのコンテキストを入力します。

```
nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>
```

- 4 BGP の状態が **Established**, **up** であることを確認します。

`get bgp neighbor`

```
BGP neighbor: 192.168.100.254   Remote AS: 64511
BGP state: Established, up
Hold Time: 180s   Keepalive Interval: 60s
Capabilities:
    Route Refresh: advertised and received
    Address Family: IPv4 Unicast:advertised and received
    Graceful Restart: none
    Restart Remaining Time: 0
Messages: 28 received, 31 sent
Minimum time between advertisements: 30s (default)
For Address Family IPv4 Unicast:advertised and received
    Route Refresh: 0 received, 0 sent
```

```

Prefixes: 2 received, 2 sent, 2 advertised
1 Connections established, 2 dropped
Local host: 192.168.100.3, Local port: 179
Remote host: 192.168.100.254, Remote port: 33044

```

#### 次のステップ

BGP 接続を外部ルーターから確認します。「[「North-South 接続とルート再配分の確認」](#)」を参照してください。

## Tier-0 分散論理ルーター上の BFD の設定

双方向フォワーディング検出 (BFD) は転送パスの障害を検出することができるプロトコルです。

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [ルーティング (Routing)] を選択します。
- 3 Tier-0 分散論理ルーターを選択します。
- 4 [ルーティング] タブをクリックし、ドロップダウン メニューから [BFD] を選択します。
- 5 [編集] をクリックして BFD を設定します。
- 6 [ステータス] 切り替えボタンをクリックして BFD を有効にします。

オプションでグローバル BFD プロパティ [受信間隔]、[転送間隔]、[非活動時間の間隔] を変更することができます。

- 7 (オプション) [スタティック ルートのネクスト ホップの BFD ピア] の [追加] をクリックして BFD ピアを追加します。

ピア IP アドレスを指定し、管理ステータスを [有効] に設定します。オプションでグローバル BFD プロパティ [受信間隔]、[転送間隔]、[非活動時間の間隔] をオーバーライドすることができます。

## Tier-0 分散論理ルーターのルート再配分を有効にする

ルート再配分を有効にすると、Tier-0 の分散論理ルーターが指定ルートをノースバウンド ルーターと共有し始めます。

#### 前提条件

- Tier-0 と Tier-1 の分散論理ルーターが接続され、Tier-1 分散論理ルーター ネットワークをアドバタイズし、Tier-0 分散論理ルーターで再配分できることを確認します。「[「Tier-0 と Tier-1 の接続」](#)」を参照してください。
- ルート再配分から特定の IP アドレスを除外する場合は、ルート マップが設定されていることを確認します。「[「ルート マップの作成」](#)」を参照してください。

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [ルーティング (Routing)] を選択します。
- 3 Tier-0 分散論理ルーターを選択します。

- 4 [ルーティング] タブをクリックし、ドロップダウン メニューから [ルート再配分] を選択します。
- 5 [追加] をクリックしてルート再配分の条件を完了します。

オプション	説明
名前と説明	ルート再配分に名前を割り当てます。オプションで説明を入力できます。 名前の例: advertise-to-bgp-neighbor
送信元	再配分するソース ルートのチェック ボックスを選択します。 スタティック: Tier-0 スタティック ルート NSX 接続: Tier-1 接続ルート NSX スタティック: Tier-1 スタティック ルート。スタティック ルートは自動的に作成されます。 Tier-0 NAT: Tier-0 分散論理ルーターで NAT が設定されている場合に生成されるルート。 Tier-1 NAT: Tier-1 分散論理ルーターで NAT が設定されている場合に生成されるルート。
ルート マップ	(オプション) 一連の IP アドレスをルート再配分から除外するためのルート マップを割り当てます。

- 6 [保存] をクリックします。
- 7 [状態] 切り替えボタンをクリックして、ルート再配分を有効にします。  
状態ボタンが「有効」になります。

## North-South 接続とルート再配分の確認

BGP ルートが学習されていることを CLI を使用して確認します。また、NSX-T に接続された仮想マシンがアクセス可能かどうか、外部のルーターから確認できます。

### 前提条件

- BGP が設定されていることを確認します。「[Tier-0 分散論理ルーター上の BGP の設定](#)」を参照してください。
- NSX-T のスタティック ルートが再配分されるように設定していることを確認します。「[Tier-0 分散論理ルーターのルート再配分を有効にする](#)」を参照してください。

### 手順

- 1 NSX Manager CLI にログインします。
- 2 外部の BGP ネイバーから学習したルーターを確認します。

```
nsx-edge1(tier0_sr)> get route bgp

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

b    10.10.10.0/24      [20/0]      via 192.168.100.254
```

- 3 BGP ルートが学習されていること、NSX-T オーバーレイを通じて仮想マシンにアクセスできることを、外部ルーターから確認します。

- a BGP ルートを一覧表示します。

```
user@router# run show ip route bgp
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
        I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 172.16.10.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
B>* 172.16.20.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
B>* 172.16.30.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
```

- b 外部ルーターから、NSX-T に接続された仮想マシンに ping を送信します。

ping 172.16.10.10

```
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=62 time=127 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=62 time=1.96 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.966/64.793/127.620/62.827 ms
```

- c NSX-T オーバーレイを通じてパスを確認します。

tracert 172.16.10.10

```
tracert to 172.16.10.10 (172.16.10.10), 30 hops max, 60 byte packets
 1  192.168.100.3 (192.168.100.3)  0.640 ms  0.575 ms  0.696 ms
 2  100.91.176.1 (100.91.176.1)  0.656 ms  0.604 ms  0.578 ms
 3  172.16.10.10 (172.16.10.10)  3.397 ms  3.703 ms  3.790 ms
```

- 4 内部の仮想マシンから、外部の IP アドレスに ping を送信します。

ping 10.10.10.10

```
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_req=1 ttl=62 time=119 ms
64 bytes from 10.10.10.10: icmp_req=2 ttl=62 time=1.93 ms
^C
--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.936/60.865/119.795/58.930 ms
```

次のステップ

ECMP など、その他のルーティング機能を設定します。

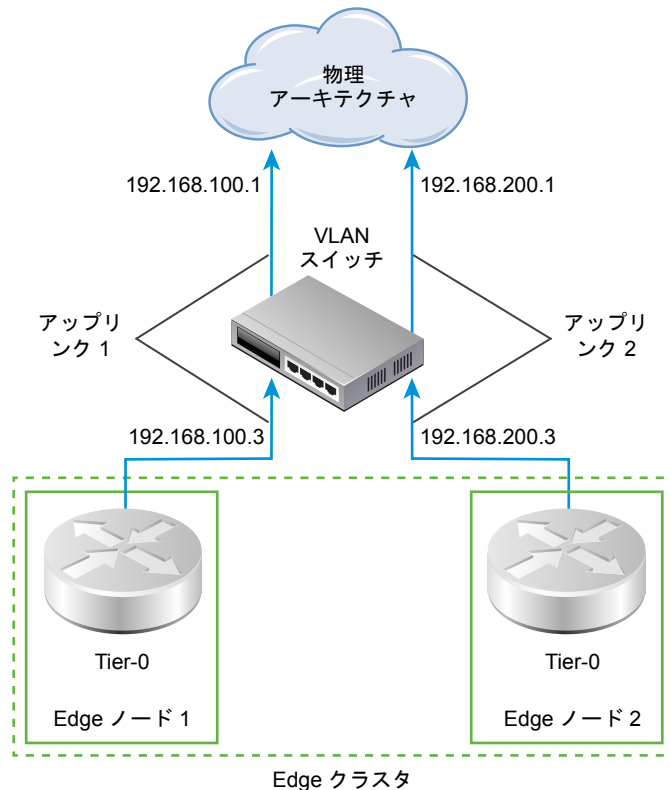


## ECMP ルーティングの理解

等価コスト マルチパス (ECMP) ルーティング プロトコルは Tier-0 分散論理ルーターにアップリンクを追加することで North および South の通信帯域幅を増やし、Edge クラスタ内の各 Edge ノードに対して設定されます。ECMP ルーティング パスはトラフィックの負荷を分散し、失敗したパスに対するフォールト トレランスを提供します。

ECMP パスは、論理スイッチに接続された仮想マシンと Tier-0 分散論理ルーターがインスタンス化される Edge ノードの間に自動的に作成されます。最大 8 つの ECMP パスがサポートされます。

図 5-4. ECMP ルーティング トポロジ



たとえば、トポロジは 1 つの Edge クラスタ内の 2 つの Tier-0 分散論理ルーターを示します。各 Tier-0 分散論理ルーターは Edge ノードにあり、これらのノードはクラスタの一部です。アップリンク ポート 192.168.100.3 および 198.168.200.3 は、物理ネットワークにアクセスするためにトランスポート ノードがどのように論理スイッチに接続するかを定義します。ECMP ルーティング パスを有効にすると、これらのパスは、論理スイッチに接続された仮想マシンと Edge クラスタの 2 つの Edge ノードを接続します。複数の ECMP ルーティング パスによってネットワークのスループットと復元性が向上します。

## 2 番目の Edge ノードのアップリンク ポートの追加

ECMP を有効にする前に、アップリンクを設定して Tier-0 の分散論理ルーター VLAN 論理スイッチに接続する必要があります。

## 前提条件

- 1つのトランスポート ゾーンと2つのトランスポート ノードが設定されていることを確認します。『NSX-T インストール ガイド』を参照してください。
- 2つの Edge ノードと1つの Edge クラスタが設定されていることを確認します。『NSX-T インストール ガイド』を参照してください。
- アップリンク用の VLAN 論理スイッチが使用可能であることを確認します。[「NSX Edge アップリンク用の VLAN 論理スイッチの作成」](#)を参照してください。
- Tier-0 分散論理ルーターが設定されていることを確認します。[「Tier-0 分散論理ルーターの作成」](#)を参照してください。

## 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [ルーティング (Routing)] を選択します。
- 3 Tier-0 分散論理ルーターを選択します。
- 4 [設定 (Configuration)] タブをクリックして、ルーター ポートを追加します。
- 5 [追加 (Add)] をクリックします。
- 6 ルーター ポートの詳細を完成させます。

オプション	説明
名前	ルーター ポートの名前を割り当てます。
説明	ポートが ECMP 設定用であることを示す追加の説明を入力します。
タイプ	デフォルトのタイプである [アップリンク (Uplink)] を受け入れます。
トランスポート ノード	ドロップダウン メニューからホストのトランスポート ノードを割り当てます。
論理スイッチ	ドロップダウン メニューから VLAN 論理スイッチを割り当てます。
論理スイッチ ポート	新しいスイッチ ポート名を割り当てます。 既存のスイッチ ポートを使用することもできます。
IP アドレス/マスク	ToR スイッチに接続しているポートと同じサブネットにある IP アドレスを入力します。

ルーター ポート設定の例。

7 [保存 (Save)] をクリックします。

新しいアップリンク ポートが Tier-0 ルーターおよび VLAN 論理スイッチに追加されます。Tier-0 分散論理ルーターは、両方の Edge ノード上で設定します。

#### 次のステップ

2 番目のネイバーの BGP 接続を作成し、ECMP ルーティングを有効にします。[\[2 番目の BGP ネイバーを追加し、ECMP ルーティングを有効にする\]](#) を参照してください。

## 2 番目の BGP ネイバーを追加し、ECMP ルーティングを有効にする

ECMP ルーティングを有効にする前に、BGP ネイバーを追加し、新しく追加したアップリンク情報を使用して設定する必要があります。

#### 前提条件

2 番目のエッジ ノードにアップリンク ポートが設定されていることを確認します。[\[2 番目の Edge ノードのアップリンク ポートの追加\]](#) を参照してください。

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [ルーティング (Routing)] を選択します。
- 3 Tier-0 分散論理ルーターを選択します。
- 4 [ルーティング (Routing)] タブをクリックし、ドロップダウン メニューから [ボーダー ゲートウェイ プロトコル (BGP)] を選択します。
- 5 [ネイバー] セクションの [追加 (Add)] をクリックして BGP ネイバーを追加します。

- 6 ネイバー IP アドレスを入力します。

例 : 192.168.200.254

- 7 ドロップダウン メニューからローカル アドレスを選択します。

例 : uplink2 192.168.200.1

- 8 リモートの AS 番号を入力します。

例 : 64511

- 9 [保存 (Save)] をクリックします。

新しく追加した BGP ネイバーが表示されます。

- 10 [BGP 設定] セクションの横にある [編集 (Edit)] をクリックします。

- 11 [等価コスト マルチパス (ECMP)] 切り替えボタンをクリックして ECMP を有効にします。

[ステータス] ボタンには [有効] と表示される必要があります。

- 12 [保存 (Save)] をクリックします。

複数の ECMP ルーティングパスが、論理スイッチに接続された仮想マシンと Edge クラスターの 2 台の Edge ノードを接続します。

#### 次のステップ

ECMP ルーティング接続が適切に動作しているかをテストします。[「ECMP ルーティング接続の確認」](#)を参照してください。

## ECMP ルーティング接続の確認

ネイバーへの ECMP ルーティング接続が確立されたことを確認するには CLI を使用します。

#### 前提条件

ECMP ルーティングが設定されていることを確認します。[「2 番目の Edge ノードのアップリンク ポートの追加」](#)および [「2 番目の BGP ネイバーを追加し、ECMP ルーティングを有効にする」](#)を参照してください。

#### 手順

- 1 NSX Manager CLI にログインします。
- 2 分散ルーターの UUID 情報を取得します。

**get logical-routers**

```
Logical Router
UUID          : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf           : 2
type          : TUNNEL

Logical Router
UUID          : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf           : 4
```

```

type      : SERVICE_ROUTER_TIER0

Logical Router
UUID      : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf       : 5
type      : DISTRIBUTED_ROUTER

Logical Router
UUID      : a6ee6316-2212-4171-99cc-930c98bcad7f
vrf       : 6
type      : DISTRIBUTED_ROUTER

```

- 出力から UUID 情報を見つけます。

```

Logical Router
UUID      : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf       : 5
type      : DISTRIBUTED_ROUTER

```

- Tier-0 分散ルーターの VRF を入力します。  
**vrf 5**
- Tier-0 分散ルーターが Edge ノードに接続されていることを確認します。  
**get forwarding**  
例 : edge-node-1 および edge-node-2。
- exit** と入力して vrf コンテキストを終了します。
- Tier-0 分散論理ルーターのためのアクティブなコントローラを開きます。
- コントローラ ノードの Tier-0 分散ルーターが接続されていることを確認します。

```
get logical-router <UUID> route
```

UUID のルート タイプは **NSX\_CONNECTED** と表示されます。

- 2 つの Edge ノードで SSH セッションを開始します。
- セッションを開始してパケットをキャプチャします。

```
set capture session 0 interface fp-eth1 dir tx
set capture session 0 expression src net <IP_Address>
```

- コントロール センターに移動して、httpdata11.bat と httpdata12.bat スクリプトをダブルクリックします。  
大量の HTTP リクエストが両方の Web 仮想マシンに送信され、Edge ノードを使用して両方のパスにトラフィックが分かれている様子がわかります。これは ECMP が動作していることを示します。

- キャプチャ セッションを終了します。

```
del capture session 0
```

- bat スクリプトを削除します。

## IP プリフィックス リストの作成

IP プリフィックス リストには、ルートのアドバタイズのアクセス権が割り当てられた単一または複数の IP アドレスが含まれています。ここにリストされた IP アドレスは順番に処理されます。IP プリフィックス リストは、BGP ネイバー フィルタまたは、受信または送信の方向を持つルート マップを介して参照されます。

たとえば、IP プリフィックス リストに IP アドレス 192.168.100.3/27 を追加し、ノースパウンド ルーターへのルートの再配分を拒否することができます。これは、192.168.100.3/24 の IP アドレスを例外として、他のすべての IP アドレスがルーターで共有されることを意味します。

また、IP アドレスに less-than-or-equal-to (le) および greater-than-or-equal-to (ge) 修飾子を追加して、ルートの再配分を許可または制限することができます。たとえば、192.168.100.3/27 ge 24 le 30 修飾子は、長さが 24 ビット以上 30 ビット以下のサブネット マスクに一致します。

---

**注:** ルートのデフォルト アクションは[拒否]です。特定のルートを拒否または許可するプリフィックス リストを作成するときに、他のすべてのルートを許可する場合は、空のネットワーク アドレスを持つ IP プリフィックスおよび[許可]アクションを作成します。

---

### 前提条件

Tier-0 分散論理ルーターが設定されていることを確認します。「[Tier-0 分散論理ルーターの作成](#)」を参照してください。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [ルーティング (Routing)] を選択します。
- 3 Tier-0 分散論理ルーターを選択します。
- 4 [ルーティング] タブをクリックし、ドロップダウン メニューから [IP プリフィックス リスト] を選択します。
- 5 [追加] を選択します。
- 6 IP プリフィックス リストの名前を割り当てます。
- 7 [行を挿入] をクリックして、ネットワーク アドレスを CIDR 形式で追加します。  
例 : 192.168.100.3/27。
- 8 ドロップダウン メニューから [拒否] または [許可] を選択します。  
要件に応じて、各 IP アドレスのアドバタイズを許可または拒否します。
- 9 (オプション) le または ge 修飾子に IP アドレスの数の範囲を設定します。  
たとえば、le 修飾子を 30 に設定し、ge 修飾子を 24 に設定します。
- 10 [保存] をクリックします。

新しく作成された IP プリフィックス リストが行に表示されます。

## ルート マップの作成

ルート マップは、IP プリフィックス リスト、BGP パス属性のシーケンス、および関連付けられたアクションで設定されます。ルーターはシーケンスをスキャンして IP アドレスの一致を検出します。一致が見つかったら、ルーターはアクションを実行し、それ以上はスキャンを実行しません。

ルート マップは BGP ネイバー レベルおよびルートの再配分で参照することができます。IP プリフィックス リストがルート マップ内で参照され、許可または拒否のルート マップアクションが適用されると、ルート マップシーケンスで指定されたアクションは、IP プリフィックス リストでの指定をオーバーライドします。

### 前提条件

IP プリフィックス リストが設定されていることを確認します。[「IP プリフィックス リストの作成」](#)を参照してください。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [ルーティング (Routing)] を選択します。
- 3 Tier-0 分散論理ルーターを選択します。
- 4 [ルーティング (Routing)] - [ルート マップ (Route Maps)]の順に選択します。
- 5 [追加 (Add)] をクリックします。
- 6 ルート マップの名前と説明（任意）を入力します。
- 7 [追加 (Add)] をクリックして、ルート マップにエントリを追加します。
- 8 1 つ以上の IP プリフィックス リストを選択します。
- 9 (オプション) BGP 属性を設定します。

BGP 属性	説明
AS パスの追加	パスに 1 つ以上の AS（自律システム）番号を追加し、パスを長くして優先されないようにします。
MED	Multi-Exit Discriminator は外部ピアに対して AS への優先パスを示します。
重み	パスの選択に影響する重みを設定します。範囲は 0 ～ 65535 です。
コミュニティ	aa:nn 形式を使用してコミュニティを指定します（例：300:500）。または、ドロップダウン メニューを使用して、次のいずれかを選択します。 <ul style="list-style-type: none"> <li>■ NO_EXPORT_SUBCONFED：EBGP ピアにアドバタイズしません。</li> <li>■ NO_ADVERTISE：どのピアにもアドバタイズしません。</li> <li>■ NO_EXPORT：BGP コンフェデレーションの外部にアドバタイズしません。</li> </ul>

- 10 [アクション] 列で、[許可 (Permit)] または [拒否 (Deny)] を選択します。

IP プリフィックス リスト内の IP アドレスのアドバタイズを許可または拒否することができます。

- 11 [保存 (Save)] をクリックします。

## ネットワーク アドレス変換

NSX-T のネットワークアドレス変換 (NAT) は、Tier-0 および Tier-1 分散論理ルーター上で設定することができます。

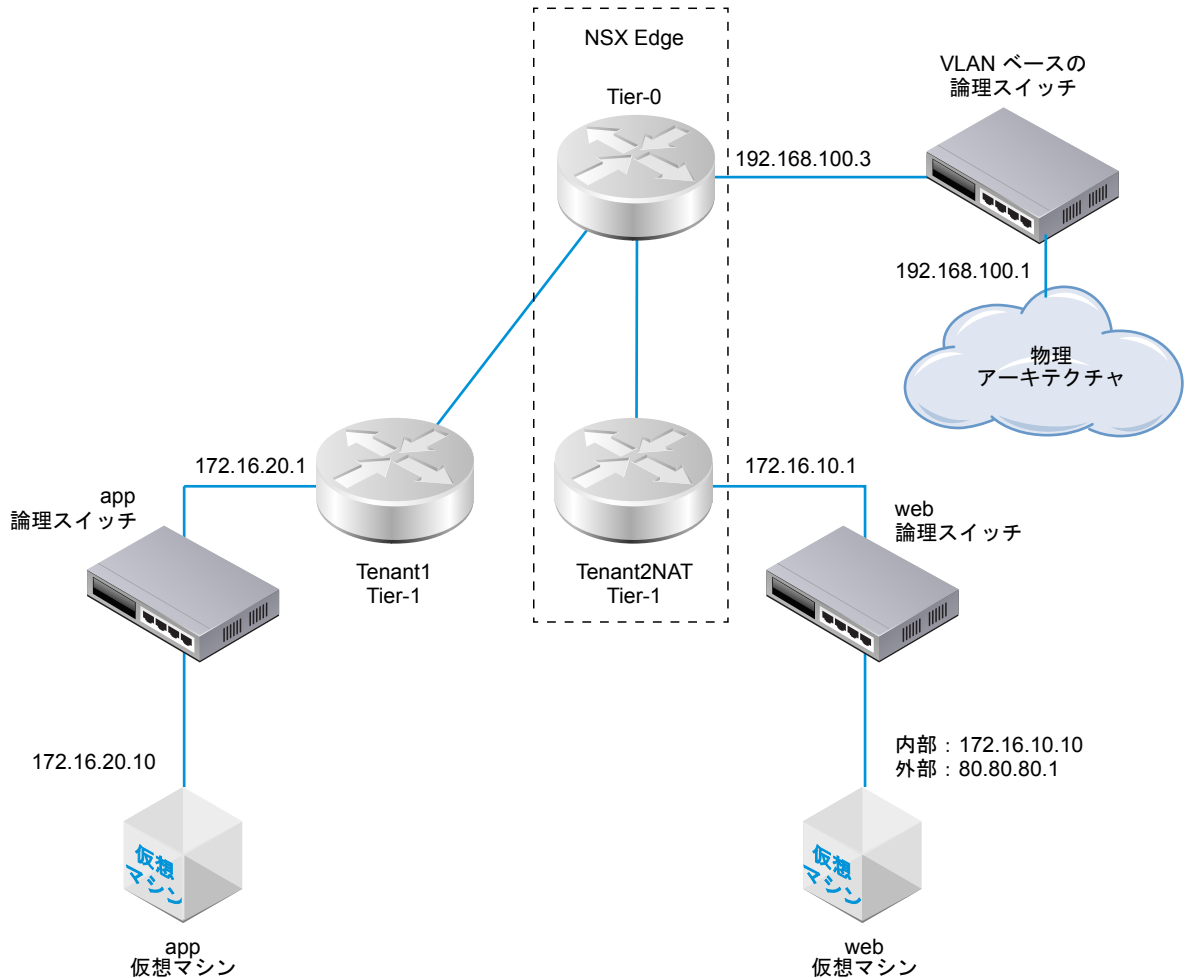
たとえば次の図は、Tenant2NAT に NAT が設定された 2 つの Tier-1 分散論理ルーターを示します。web 仮想マシンは、単に IP アドレスとして 172.16.10.10、デフォルトのゲートウェイとして 172.16.10.1 を使用するように設定されます。

NAT は、Tier-0 分散論理ルーターへの接続時に Tenant2NAT 分散論理ルーターのアップリンクで適用されます。

NAT 設定を有効にするには、Tenant2NAT は NSX Edge クラスタ上にサービス コンポーネントを持っている必要があります。したがって、Tenant2NAT は NSX Edge の内部に示されます。それに比べて、Tenant1 は Edge サービスを使用していないので NSX Edge の外部に置くことができます。



図 6-1. NAT トポロジ



この章には、次のトピックが含まれています。

- Tier-1 NAT
- Tier-0 NAT

## Tier-1 NAT

Tier-1 分散論理ルーターはソース NAT およびターゲット NAT をサポートします。

### Tier-1 ルーター上のソース NAT の設定

ソース NAT (SNAT) は、パケットの IP ヘッダー内のソース アドレスを変更します。また、TCP/UDP ヘッダー内のソース ポートを変更することもできます。典型的な使用方法として、ネットワークから離れるパケットに対してプライベート (rfc1918) アドレス/ポートをパブリック アドレス/ポートに変更します。

この例では、Web 仮想マシンからパケットを受信すると、Tenant2NAT の Tier-1 ルーターはパケットのソース ポートを 172.16.10.10 から 80.80.80.1 に変更します。パブリック ソース アドレスを持つことによって、プライベート ネットワークの外側のターゲットは元のソースに戻ることができます。

## 前提条件

- Tier-0 ルーターでは VLAN ベースの論理スイッチにアップリンクが接続されている必要があります。[\[VLAN 論理スイッチへの Tier-0 分散論理ルーターの接続\]](#) を参照してください。
- Tier-0 ルーターでは、ルーティング（スタティックまたは BGP）およびルート再配分が物理アーキテクチャへのアップリンク上で設定されている必要があります。[\[スタティック ルートの設定\]](#)、[\[Tier-0 分散論理ルーター上の BGP の設定\]](#)、および [\[Tier-0 分散論理ルーターのルート再配分を有効にする\]](#) を参照してください。
- 各 Tier-1 ルーターには、Tier-0 ルーターへのアップリンクを設定する必要があります。Tenant2NAT は Edge クラスタによってバックアップされている必要があります。[\[Tier-0 と Tier-1 の接続\]](#) を参照してください。
- Tier-1 ルーターには、ダウンリンク ポートと、ルートのアドバタイズを設定する必要があります。[\[Tier-1 分散論理ルーターのダウンリンク ポートの追加\]](#) および [\[Tier-1 分散論理ルーター上でのルートのアドバタイズの設定\]](#) を参照してください。
- 仮想マシンは正しい論理スイッチに接続する必要があります。

## 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 [ルーティング (Routing)] を選択します。
- 3 NAT を設定する Tier-1 分散論理ルーターをクリックします。
- 4 [NAT] で [追加 (Add)] をクリックします。
- 5 [アクション] には、[SNAT] を選択します。
- 6 プロトコル タイプを選択します。  
デフォルトでは、[任意のプロトコル (Any Protocol)] が選択されています。
- 7 [ソース IP] のアドレスには、仮想マシンの内部 IP アドレスを入力します。  
ソース IP を空白のままにすると、ルーターのダウンリンク ポート上のソースがすべて変換されます。この例では、ソース IP は 172.16.10.10 です。
- 8 [変換された IP] のアドレスには、仮想マシンの外部 IP アドレスを入力します。  
外部 IP アドレスまたは変換された IP アドレスを仮想マシン上で設定する必要はありません。NAT ルーターのみが変換された IP アドレスについて認識する必要があります。  
この例では、変換された IP アドレスは 80.80.80.1 です。
- 9 [ターゲット IP] のアドレスは、空白のままにしておくか、IP アドレスを入力することができます。  
ターゲット IP を空白にしておくと、NAT はローカル サブネットの外部のすべてのターゲットに適用されます。
- 10 ルールを有効にします。
- 11 (オプション) ログを有効にします。

新しいルールが NAT にリストされます。次はその例です。

Tenant2NAT

概要設定ルーティングサービス

NAT | 更新

統計情報は収集されませんでした

+ 追加 編集 削除

ID	アクション	一致					変換		適用先	統計
		プロトコル	送信元の IP アドレス	送信元ポート	宛先の IP アドレス	宛先ポート	IP アドレス	ポート		
優先順位: 1024										
1031	SNAT	任意	172.16.10.10	任意	任意	任意	80.80.80.1	任意		

### 次のステップ

NAT ルートをアドバタイズするように Tier-1 ルーターを設定します。

Tier-0 ルーターから物理アーキテクチャまで NAT ルートをアップストリームにアドバタイズするには、Tier-1 NAT ルートをアドバタイズするように Tier-0 ルーターを設定します。

## Tier-1 ルーター上での送信先 NAT の設定

送信先 NAT は、パケットの IP アドレス ヘッダー内の送信先アドレスを変更します。また、TCP/UDP ヘッダー内の送信先ポートを変更することもできます。一般的な使用目的は、受信パケットの送信先のパブリック アドレス/ポートを、ネットワーク内のプライベート IP アドレス/ポートにリダイレクトすることです。

この例ではパケットを app 仮想マシンから受信するため、Tenant2NAT Tier-1 ルーターは、パケットの送信先ポートを 172.16.10.10 から 80.80.80.1 に変更します。パブリック送信先アドレスを使用することで、プライベート ネットワーク内の送信先にプライベート ネットワーク外からアクセスできます。

### 前提条件

- Tier-0 ルーターには、VLAN ベースの論理スイッチに接続されているアップリンクが必要です。[\[VLAN 論理スイッチへの Tier-0 分散論理ルーターの接続\]](#) を参照してください。
- Tier-0 ルーターの場合は、物理アーキテクチャへのアップリンク上で、ルーティング（スタティックまたは BGP）とルート再配分が設定されている必要があります。[\[スタティック ルートの設定\]](#)、[\[Tier-0 分散論理ルーター上の BGP の設定\]](#)、および [\[Tier-0 分散論理ルーターのルート再配分を有効にする\]](#) を参照してください。
- Tier-1 ルーターそれぞれに、Tier-0 ルーターへのアップリンクが設定されている必要があります。Tenant2NAT は、Edge クラスターでバックアップされる必要があります。[\[Tier-0 と Tier-1 の接続\]](#) を参照してください。
- Tier-1 ルーターには、ダウンリンク ポートとルート アドバタイズが設定されている必要があります。[\[Tier-1 分散論理ルーターのダウンリンク ポートの追加\]](#) および [\[Tier-1 分散論理ルーター上でのルートのアドバタイズの設定\]](#) を参照してください。
- 仮想マシンが正しい論理スイッチに接続されている必要があります。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 [ルーティング (Routing)] を選択します。

3 NAT を設定する Tier-1 分散論理ルーターをクリックします。

4 NAT の下で、[追加 (Add)] をクリックします。

5 アクションとして DNAT を選択します。

6 プロトコル タイプを選択します。

デフォルトでは、[任意のプロトコル (Any Protocol)] が選択されます。

7 送信先 IP アドレスとして、仮想マシンの外部 IP アドレスを入力します。

この例の送信先 IP アドレスは 80.80.80.1 です。仮想マシンには、外部 IP アドレスを常に設定する必要はありません。NAT ルーターのみが、外部 IP アドレスを認識する必要があります。

8 変換後 IP アドレスとして、仮想マシンの内部 IP アドレスを入力します。

内部 IP アドレスは仮想マシン上で設定する必要があります。

この例では、内部/変換後 IP アドレスは 172.16.10.10 です。

9 送信元 IP アドレスは、空白のままにすることも、IP アドレスを入力することもできます。

送信元 IP アドレスを空白のままにした場合、NAT はローカル サブネット外のすべてのソースに適用されます。

10 ルールを有効にします。

11 (オプション) ログを有効にします。

新しいルールが NAT の下に表示されます。次はその例です。

Tenant2NAT

概要

設定

ルーティング

サービス

NAT

更新

統計情報は収集されませんでした

追加

編集

削除

ID	アクション	一致					変換		適用先	統計
		プロトコル	送信元の IP アドレス	送信元ポート	宛先の IP アドレス	宛先ポート	IP アドレス	ポート		
優先順位: 1024										
1029	DNAT	任意	任意	任意	80.80.80.1	任意	172.16.10.10	任意		

## 次のステップ

NAT ルートをアドバタイズするように Tier-1 ルーターを設定します。

Tier-0 ルーターから物理アーキテクチャへの NAT ルート アップストリームをアドバタイズするには、Tier-1 NAT ルートをアドバタイズするように Tier-0 ルーターを設定します。

## アップストリームの Tier-0 ルーターへの Tier-1 NAT ルートのアドバタイズ

Tier-1 NAT ルートをアドバタイズすることにより、アップストリームの Tier-0 ルーターはそれらのルートを学習することができます。

## 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 [ルーティング (Routing)] を選択します。
- 3 NAT を設定した Tier-1 分散論理ルーターをクリックします。
- 4 Tier-1 ルーターから、[ルーティング (Routing)] > [ルートのアドバタイズ (Route Advertisement)] の順に選択します。
- 5 ルートのアドバタイズのルールを編集して、NAT ルートのアドバタイズを有効にします。



## Tenant2NAT

Summary

Configuration

Routing ▼

NAT

## Route Advertisement

Status	● Enabled
Advertise All NSX Connected Routes	● Yes
Advertise NAT Routes	● Yes
Advertise Static Routes	● No

## 次のステップ

Tier-0 ルーターからアップストリームの物理アーキテクチャに Tier-1 NAT ルートをアドバタイズします。

## 物理アーキテクチャへの Tier-1 NAT ルートのアドバタイズ

Tier-0 ルーターから Tier-1 NAT ルートをアドバタイズすることにより、アップストリームの物理アーキテクチャはそれらのルートを学習することができます。

## 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 [ルーティング] を選択します。
- 3 NAT を設定した Tier-1 ルーターに接続された Tier-0 分散論理ルーターをクリックします。
- 4 Tier-0 ルーターから、[ルーティング] > [ルートの再配分] の順に選択します。
- 5 ルートのアドバタイズのルールを編集して、Tier-1 NAT ルートのアドバタイズを有効にします。

Edit Redistribution Criteria - T1

×

Name: \*

T1

Description:

Sources: \*

☐ Static
 ☒ NSX Connected
 ☒ NSX Static
 ☐ Tier-0 NAT
 

☒ Tier-1 NAT

Route Map:

×

▼

Save

Cancel

#### 次のステップ

NAT が期待したとおりに動作していることを確認します。

## Tier-1 NAT の確認

SNAT および DNAT ルールが正常に動作していることを確認します。

#### 手順

- 1 NSX Edge にログインします。
- 2 `get logical-routers` を実行して Tier-0 サービス ルーターの VRF 番号を確認します。
- 3 `vrf <number>` コマンドを実行して Tier-0 サービス ルーターのコンテキストに入ります。
- 4 `show route` コマンドを実行して、Tier-1 NAT アドレスが表示されることを確認します。

```
nsx-edge(tier0_sr)> get route
```

```
Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT
```

```
Total number of routes: 8
```

```
t1n 80.80.80.1/32      [3/3]      via 169.0.0.1
...
```

- 5 Web 仮想マシンが Web ページを提供するように設定されている場合は、http://80.80.80.1 で Web ページが開くことを確認します。
- 6 物理アーキテクチャの Tier-0 ルーターのアップストリーム ネイバーが 80.80.80.1 に ping を送信できることを確認します。
- 7 ping コマンドの実行中に DNAT ルールの統計情報の列を確認します。  
アクティブなセッション が 1 つあれば正常に動作しています。

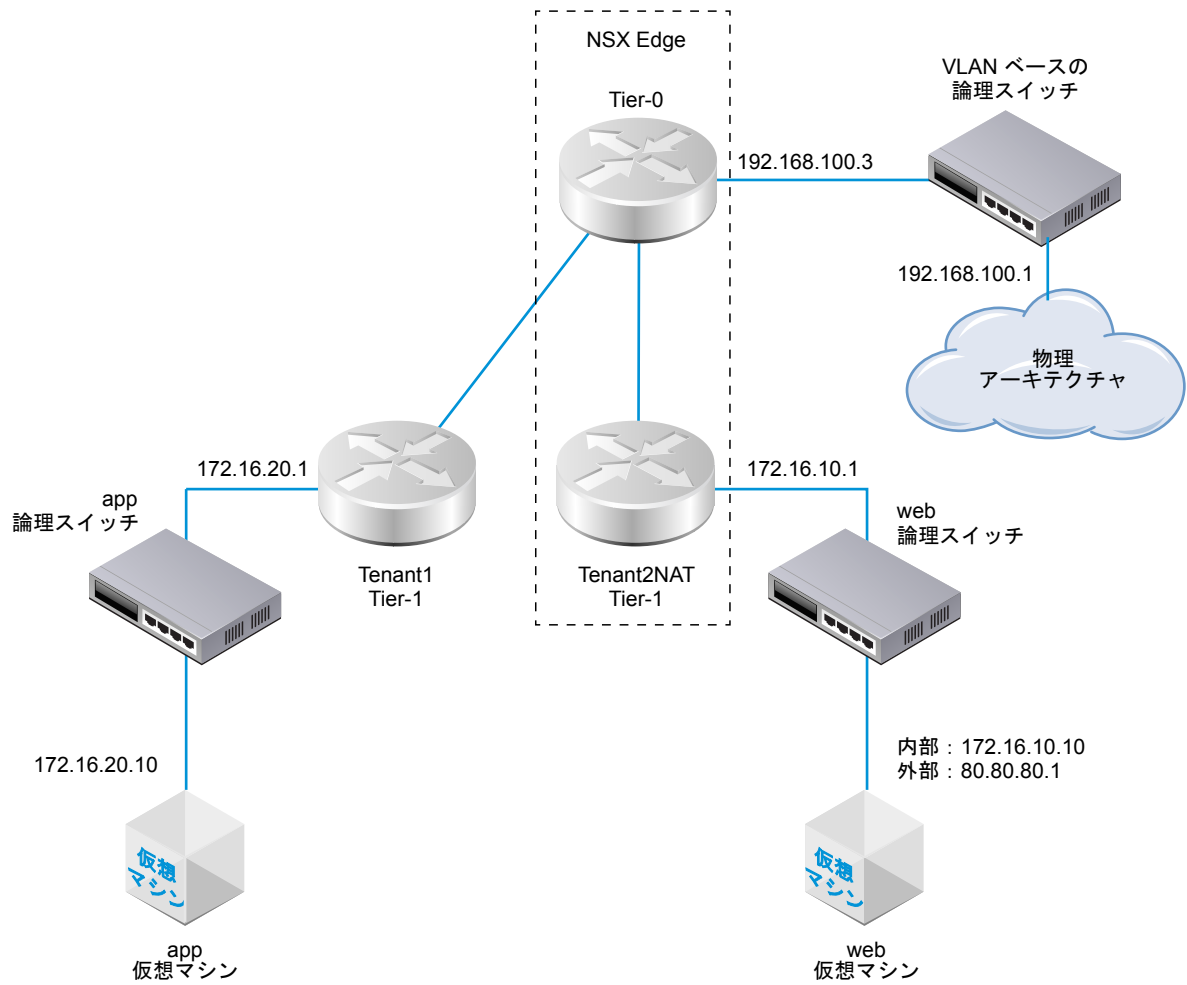
## Tier-0 NAT

Tier-0 分散論理ルーターは再帰 NAT をサポートします。

### 再帰 NAT

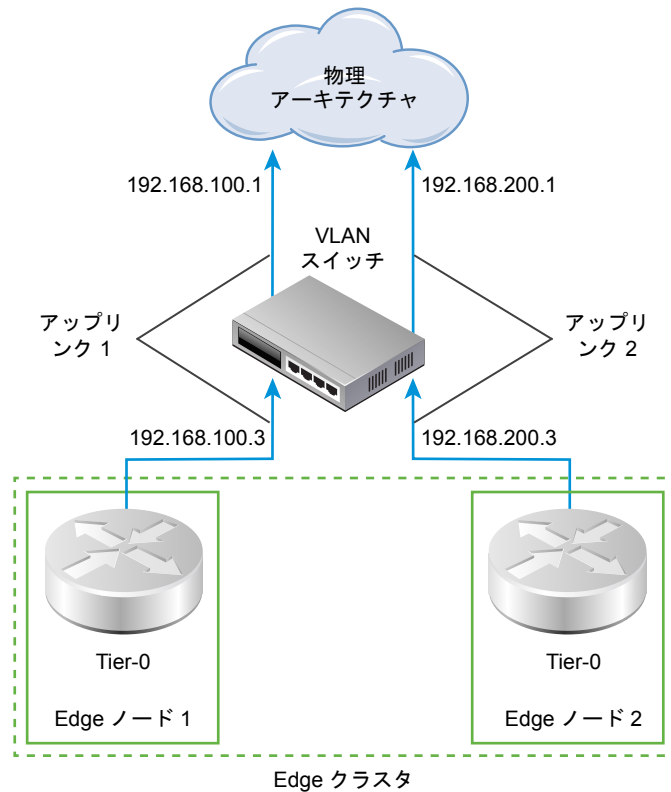
Tier-0 論理ルーターがアクティブ/アクティブ ECMP モードで実行している場合、非対称のパスが問題となる可能性がある場合にはステートフル NAT を設定することができません。アクティブ/アクティブ ECMP ルーターの場合は、再帰 NAT（ステートレス NAT と呼ばれることもあります）を使用することができます。

この例では、Web 仮想マシンからパケットを受信すると、Tenant2NAT の Tier-1 ルーターはパケットのソース ポートを 172.16.10.10 から 80.80.80.1 に変更します。パブリック ソース アドレスを持つことによって、プライベート ネットワークの外側の宛先は送信元に戻ることができます。





ただし、ここに示すように 2 つのアクティブ/アクティブ Tier-0 ルーターが含まれている場合は、再帰 NAT を設定する必要があります。



## Tier-0 分散論理ルーター上の再帰 NAT の設定

Tier-0 分散論理ルーターがアクティブ/アクティブ ECMP モードで実行している場合、非対称のパスが問題となる可能性がある場合にはステートフル NAT を設定することができません。アクティブ/アクティブ ECMP ルーターの場合は、再帰 NAT（ステートレス NAT と呼ばれることもあります）を使用することができます。

### 前提条件

- Tier-0 ルーターでは VLAN ベースの論理スイッチに 2 つのアップリンクが接続されている必要があります。[\[VLAN 論理スイッチへの Tier-0 分散論理ルーターの接続\]](#) を参照してください。
- Tier-0 ルーターでは、物理アーキテクチャへのアップリンク上に、ルーティング（スタティックまたは BGP）およびルート再配分を設定する必要があります。[\[スタティック ルートの設定\]](#)、[\[Tier-0 分散論理ルーター上の BGP の設定\]](#)、および [\[Tier-0 分散論理ルーターのルート再配分を有効にする\]](#) を参照してください。
- 各 Tier-1 ルーターには、Tier-0 ルーターへのアップリンクを設定する必要があります。Tenant2NAT は Edge クラスタによってバックアップされている必要があります。[\[Tier-0 と Tier-1 の接続\]](#) を参照してください。
- Tier-1 ルーターには、ダウンリンク ポートと、ルートのアドバタイズを設定する必要があります。[\[Tier-1 分散論理ルーターのダウンリンク ポートの追加\]](#) および [\[Tier-1 分散論理ルーター上でのルートのアドバタイズの設定\]](#) を参照してください。
- 仮想マシンは正しい論理スイッチに接続する必要があります。

## 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 [ルーティング (Routing)] を選択します。
- 3 再帰 NAT を設定する Tier-0 分散論理ルーターをクリックします。
- 4 [NAT] で [追加 (Add)] をクリックします。
- 5 [アクション] には、[再帰] を選択します。
- 6 [ソース IP アドレス] のアドレスには、仮想マシンの外部 IP アドレスを入力します。  
この例では、ソース IP は 80.80.80.1 です。
- 7 変換後 IP アドレスとして、仮想マシンの内部 IP アドレスを入力します。  
この例では、変換された IP アドレスは 172.16.10.10 です。
- 8 [ターゲット IP] のアドレスは、空白のままにしておくか、IP アドレスを入力することができます。  
ターゲット IP を空白にしておくと、NAT はローカル サブネットの外部のすべてのターゲットに適用されます。
- 9 ルールを有効にします。
- 10 (オプション) ログを有効にします。

新しいルールが NAT にリストされます。次はその例です。

PLR-1

概要設定ルーティングサービス

NAT | 更新

ルールの統計情報の合計 | 最終更新日: 9/13/2018, 2:44:27 AM

○ アクティブセッション

○ パケットの数

○ バイト データ

+ 追加

✎ 編集

🗑 削除

ID	アクション	一致					変換		適用先	統計
		プロトコル	送信元の IP アドレス	送信元ポート	宛先の IP アドレス	宛先ポート	IP アドレス	ポート		
優先順位: 1024										
1030	再帰	任意	80.80.80.1	任意	任意	任意	172.16.10.10	任意		

## 次のステップ

NAT ルートをアドバタイズするように Tier-1 ルーターを設定します。

Tier-0 ルーターから物理アーキテクチャまで NAT ルートをアップストリームにアドバタイズするには、Tier-1 NAT ルートをアドバタイズするように Tier-0 ルーターを設定します。

# ファイアウォール セクションとファイアウォール ルール

## 7

ファイアウォール セクションはファイアウォール ルールのセットをグループ化するために使用されます。

ファイアウォール セクションは1つ以上の個別のファイアウォール ルールで設定されます。各ファイアウォール ルールには、パケットを許可するかブロックするか、どのプロトコルの使用が許可されるか、どのポートの使用が許可されるか、などを決定する指示が含まれています。セクションは、個別のセクションの営業およびエンジニアリング部門の特定のルールなど、マルチテナントに使用されます。

セクションはステートフルまたはステートレスのルールの適用として定義されることができます。ステートレス ルールは従来のステートレス アクセス制御リストとして処理されます。再帰アクセス制御リストはステートレスセクションではサポートされません。単一の論理スイッチ ポートにステートレスとステートフルのルールを混在させることは推奨されません。定義されていない動作が発生する可能性があります。

ルールは、セクション内で上下に移動させることができます。トラフィックがファイアウォールを通過しようとするとき、パケット情報はセクションに示されるルールに従います。ルールは、一番上から一番下のデフォルト ルールまで順番に適用されます。パケットに一致する最初のルールには設定済みのアクションが適用され、ルールの設定済みのオプションで指定された処理が実行され、後に続くすべてのルールは無視されます（後のルールの方がより正確に一致する場合でも）。したがって、具体的なルールを全般的なルールよりも上位に配置し、無視されないようにする必要があります。デフォルトのルールは、ルール テーブルの一番下に置かれた「catchall」ルールです。他のどのルールにも一致しないパケットにはデフォルトのルールが適用されます。

この章には、次のトピックが含まれています。

- [ファイアウォール ルール セクションの追加](#)
- [ファイアウォール ルール セクションの削除](#)
- [セクション ルールを有効または無効にする](#)
- [セクション ログを有効または無効にする](#)
- [ファイアウォール ルールについて](#)
- [ファイアウォール ルールの追加](#)
- [ファイアウォール ルールの削除](#)
- [デフォルトの Distributed Firewall ルールの編集](#)
- [ファイアウォール ルールの順序の変更](#)
- [ファイアウォール ルールのフィルタ](#)

## ■ ファイアウォールからのオブジェクト除外

# ファイアウォール ルール セクションの追加

ファイアウォール ルール セクションは独立して編集および保存され、個別のファイアウォール設定をテナントに適用するために使用されます。

### 手順

- 1 ナビゲーション パネルの [ファイアウォール (Firewall)] を選択します。

[全般] タブが開かれていることを確認し、L3 ルールを追加します。[イーサネット] タブをクリックし、L2 ルールを追加します。

- 2 セクションを追加するには、最初の列でホイール (⚙️) アイコンまたはルールをクリックし、[セクションを上追加 (Add Section Above)] または [セクションを下追加 (Add Section Below)] のいずれかを選択します。

**注:** トラフィックがファイアウォールを通過しようとするとき、パケット情報は [ルール] テーブルに示されるルールに従います。ルールは、一番上から一番下のデフォルト ルールまで順番に適用されます。場合によっては、2 つ以上のルールの優先順位が、パケットの処理を決定するのに重要になります。

- 3 セクション名およびオプションの説明を入力します。

- 4 [ステートフル (Stateful)]、[偽 (False)]、または [真 (True)] のいずれかを選択します。このオプションは L3 ルールにのみ適用されます。

ステートレス ファイアウォールはネットワーク トラフィックを監視し、ソースおよびターゲットのアドレスまたは他の固定値に基づいてパケットを制限またはブロックします。ステートフル ファイアウォールはトラフィック ストリームを終端から終端まで監視することができます。ステートレス ファイアウォールは一般により高速で、トラフィックの負荷がより高い状況でより適切に動作します。ステートフル ファイアウォールは、未承認の偽装された通信を特定するのに効果的です。一度定義すると、ステートフルとステートレスを切り替えることはできません。

- 5 セクションをどこに適用するかを選択します。

**注:** あるセクションで [適用先 (Applied To)] を使用した場合、そのセクションのルールのすべての [適用先 (Applied To)] 設定が上書きされます。

論理ポート：すべての論理ポートを表示します

論理スイッチ：すべての論理スイッチを表示します

NSGroup：すべての NSGroup を表示します

- 6 利用可能なポート、スイッチ、またはグループの横にあるチェックボックスをクリックして、矢印をクリックします。

アイテムが [選択済み] 列に移動します。

- 7 [保存 (Save)] をクリックしてセクションを保存します。

新しく追加されたセクションが [ファイアウォール (Firewall)] ウィンドウに表示されます。

## 次のステップ


セクションにファイアウォール ルールを追加します。

## ファイアウォール ルール セクションの削除

使用しなくなったファイアウォール ルール セクションは削除することができます。

ファイアウォール ルール セクションを削除すると、そのセクション内のすべてのルールが削除されます。セクションを削除して、ファイアウォール テーブルの別の場所に追加し直すことはできません。セクションを追加し直す場合は、セクションを削除して、設定を発行する必要があります。その後、セクションをファイアウォール テーブルに追加して再び発行します。

### 手順

- 1 ナビゲーション パネルの [ファイアウォール (Firewall)] を選択します。
- 2 [全般] タブが開かれていることを確認し、L3 ルールを追加します。
- 3 [イーサネット] タブをクリックし、L2 ルールを追加します。
- 4 セクションを削除するには、最初の列で、削除するセクションの横にあるホイール  を右クリックします。
- 5 [削除 (Delete)] をクリックしてセクションを削除します。セクションと、セクションに含まれるすべてのルールが削除されます。

## セクション ルールを有効または無効にする

ファイアウォール ルール セクション内のルールをすべて有効または無効にすることができます。

### 手順


- 1 ナビゲーション パネルの [ファイアウォール (Firewall)] を選択します。
- 2 最初の列で、ホイール アイコンをクリックし、[セクション ルールを無効にする (Disable Section Rules)] または [セクション ルールを有効にする (Enable Section Rules)] を選択します。
- 3 [保存 (Save)] をクリックします。

## セクション ログを有効または無効にする

セクション ルールのログを有効にすると、セクション内のすべてのルールのパケットについての情報が記録されます。セクション内のルールの数にもよりますが、典型的なファイアウォール セクションは大量のログ情報を生成し、パフォーマンスに影響をおよぼす場合があります。

ログは vSphere ESXi および KVM ホストの /var/log/dfwpktlogs.log ファイルに保存されます。

### 手順

- 1 ナビゲーション パネルの [ファイアウォール (Firewall)] を選択します。
- 2 最初の列で、ホイール  アイコンをクリックします。[セクション ルールのログを無効にする (Disable Logs for Section Rules)] または [セクション ルールのログを有効にする (Enable Logs for Section Rules)] を選択します。

3 [保存 (Save)] をクリックします。

## ファイアウォール ルールについて

NSX-T は、ファイアウォール ルールを使用してネットワークとの間でのトラフィック処理を指定します。

ファイアウォールには、レイヤー 3 ルール ([全般] タブ) とレイヤー 2 ルール ([イーサネット] タブ) という複数の設定ルール セットがあります。レイヤー 2 のファイアウォール ルールは、レイヤー 3 のルールの前に処理されます。[設定] タブには除外リストが含まれています。このリストには、ファイアウォールの適用から除外される論理スイッチ、論理ポートおよびグループが含まれます。

ファイアウォール ルールは次のように適用されます。

- ルールは上から下に順番に処理されます。
- 各パケットがルール テーブルの一番上のルールに照らしてチェックされ、順にテーブルの下位のルールに照らしてチェックされます。
- テーブル内のルールのうち、トラフィック パラメータと一致する最初のルールが適用されます。

そのパケットの検索はそこで終了するため、後続のルールを適用することはできません。このため、最も詳細なポリシーをルール テーブルの一番上に配置することが推奨されます。これにより、個別のルールの前に、上位のポリシーが適用されるようになります。

デフォルトのルールは、ルール テーブルの一番下に置かれた **catchall** ルールです。他のどのルールにも一致しないパケットにはデフォルトのルールが適用されます。ホストの準備が完了すると、アクションを許可するデフォルトルールが設定されます。これによって、仮想マシン間の通信がステージングや移行段階で切断されることがなくなります。次に、ベスト プラクティスとして、アクションをブロックしてポジティブ コントロール モデル（たとえば、ファイアウォール ルールに定義されたトラフィックのみがネットワークで許可される）によってアクセス コントロールを実行するようにこのデフォルト ルールを変更します。

ファイアウォール ルール オプションにアクセスするには、[列] の横にあるドロップダウン矢印をクリックします。ファイアウォール ルールを含めるには、適切な列のチェックボックスを選択します。次のオプションを設定できます。

表 7-1. ファイアウォール ルール画面の列

カラム名	定義
名前	ファイアウォール ルールの名前。
ソース	ルールのソースは、IP アドレスか MAC アドレス、または IP アドレス以外のオブジェクトのいずれかです。定義しない場合は、すべてのソースと一致します。ソースまたはターゲットの範囲には IPv6 はサポートされません。
ID	各ルールに対してシステムが生成した一意の ID。
方向	方向ルール要素は、インターフェイス上で移動するパケットの方向に一致します。In 方向とは、トラフィックがファイアウォールを入力方向に進むことを指します。Out 方向とは、トラフィックがファイアウォールを出力方向に進むことを指します。デフォルトの方向は In Out（双方向）です。
IP プロトコル	これは L3 ルールにのみ適用されます。IPv4 および IPv6 の両方がサポートされています。デフォルト値は both です。
ターゲット	ルールの影響を受ける接続のターゲット IP アドレスまたは MAC アドレス/ネットマスク。定義しない場合は、すべてのターゲットと一致します。ソースまたはターゲットの範囲には IPv6 はサポートされません。
サービス	L3 の場合、サービスは定義済みのポート プロトコルの組み合わせになります。L2 の場合、サービスは ether-type になります。L2 と L3 のどちらの場合も、新しいサービスまたはサービス グループを手動で定義することができます。指定しない場合は、すべてのサービスと一致します。

表 7-1. ファイアウォール ルール画面の列 (続き)

カラム名	定義
アクション (必須)	ルールによって適用されるアクションには、許可、ブロック、または却下があります。
適用先	このルールを適用する範囲を定義します。定義しない場合、範囲はすべての論理ポートになります。セクションに [適用先] を追加した場合、ルールが上書きされます。
ログに記録	ログへの記録をオンまたはオフにすることができます。ログは ESX および KVM ホストの /var/log/dfwpktlogs.log ファイルに保存されます。
統計	バイト、パケット カウント、セッションを表示する読み出し専用フィールド。
メモ	ルールのコメント。

デフォルトのファイアウォール ルールは次のとおりです (列のオプションの一部が表示されます)。

図 7-1. [ファイアウォール ルール] ウィンドウ

GENERAL   ETHERNET   CONFIGURATION									
<span>UP</span> <span>DOWN</span> <span>COLUMNS</span> <span>FILTER</span> <span>OBJECTS</span>									
	Name	ID	Sources	Destinations	Services	Action	Applied To	Log	Stats
1	default - a3b004... (5) Applied To: 1	4ae3398c-6c...	default - a3b0...	default - a3b0...	Any	Allow	All	No	packets: 0 bytes: 0 sessions: 0

## ファイアウォール ルールの追加

ファイアウォールは、事前に定義したファイアウォール ルールに基づいて受信および送信ネットワークのトラフィックを監視および制御するネットワーク セキュリティ システムです。

ファイアウォール ルールは NSX Manager のスコープで追加されます。その後、[適用先] フィールドを使用して、ルールを適用するスコープを絞り込むことができます。各ルールのソースおよびターゲットのレベルに複数のオブジェクトを追加することで、追加する必要のあるファイアウォール ルールの総数を減らすことができます。

**注:** デフォルトでは、ルールは任意のソース、ターゲットおよびサービス ルール要素のデフォルトで一致し、すべてのインターフェイスおよびトラフィックの方向に一致します。ルールの影響を特定のインターフェイスまたはトラフィック方向に制限する場合は、ルール内で制限を指定する必要があります。

### 前提条件

アドレスのグループを使用するには、最初に各仮想マシンの IP アドレスおよび MAC アドレスをそれらの論理スイッチに手動で関連付けます。

### 手順

- 1 ナビゲーション パネルの [ファイアウォール (Firewall)] を選択します。

[全般] タブが開かれていることを確認し、L3 ルールを追加します。[イーサネット] タブをクリックし、L2 ルールを追加します。

- 2 ルールを追加するには、最初の列でホイール (⚙️) アイコンをクリックし、リストの一番下で [ルールを追加 (Add Rule)] を選択します。

ファイアウォール ルールを定義する新しい列が表示されます。

**注:** トラフィックがファイアウォールを通過しようとするとき、パケット情報は [ルール] テーブルに示されるルールに従います。ルールは、一番上から一番下のデフォルト ルールまで順番に適用されます。場合によっては、2 つ以上のルールの優先順位が、パケットの処理を決定するのに重要になります。

- 3 セクションの一番上に新しいルールが追加されます。セクション内の特定の場所にルールを追加する場合は、ルールを選択します。最初の列で、ホイール (⚙️) アイコンをクリックし、[ルールを上へ挿入 (Insert Rule Above)] または [ルールを下へ挿入 (Insert Rule Below)] を選択します。

ファイアウォール ルールを定義する新しい列が表示されます。

- 4 [名前 (Name)] 列の右上隅の鉛筆のアイコンをクリックします。[名前を編集] ダイアログ ボックスにルール名を入力します。

指定した名前のルールが表示されます。

- 5 新しいルールの [ソース (Sources)] セルをポイントし、鉛筆のアイコンをクリックして、ルールのソースを選択します。ソースを定義しない場合は、そのすべてと一致します。[ソースを編集 (Edit Sources)] ダイアログ ボックスが表示されます。

**注:** 新しいファイアウォールを作成する場合、[ソース]、[ターゲット]、[サービス] および [適用先] フィールドに使用するオブジェクトを、毎回選択する代わりにドラッグ アンド ドロップすることができます。これは、特に同じオブジェクトが頻繁に再使用される場合、ルール作成プロセスを高速化するのに役立ちます。

それには、[ファイアウォール ルール] ウィンドウの左側隅の **オブジェクト** をクリックし、リストからオブジェクト タイプを選択して、必要なオブジェクトを右側のフィールド、すなわちファイアウォール ルールの [ソース] にドラッグ アンド ドロップします。

表 7-2. [ソースを編集] ウィンドウ

オプション	説明
IP アドレスまたは MAC アドレス	複数の IP アドレスまたは MAC アドレスをコンマ区切りのリストで入力します。リストの長さは、最大 255 文字です。IPv4 および IPv6 形式の両方がサポートされています。
オブジェクト	<p>矢印をクリックして、オブジェクトを選択します。</p> <ol style="list-style-type: none"> <li>1 IP セット、論理ポート、論理スイッチ、または NS グループを選択します。</li> <li>2 選択したコンテナの使用可能なオブジェクトが表示されます。</li> <li>3 1 つ以上のオブジェクトを選択し、矢印をクリックします。使用可能なすべてのオブジェクトを選択するには、[使用可能] の横にあるチェックボックスをクリックし、矢印をクリックします。</li> <li>4 オブジェクトが [選択済み] 列に移動します。</li> <li>5 [OK] をクリックします。</li> </ol>



- 6 新しいルールの [ターゲット (Destinations)] セルをポイントします。ターゲットを定義しない場合は、そのすべてと一致します。[ターゲットを編集 (Edit Destinations)] ダイアログ ボックスが表示されます。

表 7-3. [ターゲットを編集] ウィンドウ

オプション	説明
IP アドレスまたは MAC アドレス	複数の IP アドレスまたは MAC アドレスをコンマ区切りのリストで入力できます。リストの長さは、最大 255 文字です。IPv4 および IPv6 形式の両方がサポートされています。
オブジェクト	<p>矢印をクリックして、オブジェクトを選択します。</p> <ol style="list-style-type: none"> <li>1 IP セット、論理ポート、論理スイッチ、または NS グループを選択することができます。</li> <li>2 選択したコンテナの使用可能なオブジェクトが表示されます。</li> <li>3 1 つ以上のオブジェクトを選択し、矢印をクリックします。使用可能なすべてのオブジェクトを選択するには、[使用可能] の横にあるチェックボックスをクリックし、矢印をクリックします。</li> <li>4 オブジェクトが [選択済み] 列に移動します。</li> <li>5 [OK] をクリックします。</li> </ol>

- 7 新しいルールの [サービス (Service)] セルをポイントします。サービスを定義しない場合は、そのすべてと一致します。

[サービスを編集 (Edit Services)] ダイアログ ボックスが表示されます。リストにはすでに多くの定義済みのサービスが表示されていますが、選択できるのはこれらのサービスだけではありません。

- 8 定義済みのサービスを選択するには、1 つ以上の使用可能なオブジェクトを選択し、矢印をクリックします。[OK] をクリックします。
- 9 新しいサービスを定義するには、[新規 (New)] をクリックします。[NSService] ダイアログ ボックスが表示されます。

オプション	説明
名前	新しいサービスの名前を指定します。
説明	新しいサービスの説明を入力します。
サービスのタイプ	<ul style="list-style-type: none"> <li>■ ALG</li> <li>■ ICMP</li> <li>■ IP</li> <li>■ L4 ポート セット</li> <li>■ IGMP</li> </ul>
プロトコル	利用可能なプロトコルの 1 つを選択します。
ソース ポート	ソース ポートを入力します。
ターゲット ポート	ターゲット ポートを入力します。
既存のサービスのグループ化	ラジオ ボタンをクリックして既存のグループ サービスを追加します。

- 10 [アクション (Action)] セルをポイントし、鉛筆のアイコンをクリックします。このパラメータは必須です。[アクションを編集] ダイアログ ボックスが表示されます。

オプション	説明
許可	指定されたソース、ターゲット、およびプロトコルを持つすべての L3 または L2 トラフィックが現在のファイアウォール コンテキストを通過することを許可します。ルールに一致し、承認されたパケットは、ファイアウォールが存在しないかのようにシステム内を移動します
ドロップ	指定されたソース、ターゲット、およびプロトコルを持つパケットをドロップします。パケットのドロップは情報が表示されず、ソース システムまたはターゲット システムへの通知なしで実行されます。パケットをドロップすると、再試行のしきい値に到達するまで、接続が再試行されます。
却下	指定されたソース、ターゲット、およびプロトコルを持つパケットを却下します。パケットの却下は、送信者に対してターゲットに到達できないというメッセージを送信するので、パケットを拒否する方法としてはより適切です。プロトコルが TCP の場合、TCP RST メッセージが送信されます。UDP、ICMP およびその他の IP 接続では、管理上禁止されたコードが含まれる ICMP メッセージが送信されます。[却下] を使用する利点の 1 つは、一度試行しただけで、接続を確立できないことが送信側のアプリケーションに通知されることです。

- 11 [適用先 (Applied To)] セルをポイントし、鉛筆のアイコンをクリックします。[適用先を編集] ダイアログ ボックスが表示されます。

ドロップダウン リストからオブジェクトのタイプを選択します。[OK] をクリックします。

- 12 [ログ (Log)] セルをポイントし、鉛筆のアイコンをクリックします。ログはデフォルトでオフになっています。[はい (Yes)] を選択してログを有効にするか、[いいえ (No)] を選択してログを無効にします。ログは ESX および KVM ホストの /var/log/dfwpktlogs.log ファイルに保存されます。ここにメモを書き込むこともできます。[はい (Yes)] を選択すると、このルールに一致するすべてのセッションがログに記録されます。ログを有効にするとパフォーマンスに影響が出る場合があります。

- 13 ルールを有効にするには、[保存 (Save)] をクリックします。

[保存 (Save)] をクリックする前に複数のルールを追加することができます。

## ファイアウォール ルールの削除

ファイアウォールは、事前に定義したファイアウォール ルールに基づいて受信および送信ネットワークのトラフィックを監視および制御するネットワーク セキュリティ システムです。カスタム定義されたルールを追加または削除することができます。

### 手順

- ナビゲーション パネルの [ファイアウォール (Firewall)] を選択します。  
[全般] タブが開かれていることを確認し、L3 ルールを追加します。[イーサネット] タブをクリックし、L2 ルールを追加します。
- 移動するルールの番号を右クリックします。  
ドロップダウン リストが表示されます。
- [削除 (Delete)] を選択します。  
ファイアウォール ルールが削除されます。

- 4 [保存 (Save)] をクリックして変更を有効にします。

ルールが削除されます。

## デフォルトの Distributed Firewall ルールの編集

どのユーザー定義ファイアウォール ルールにも一致しないトラフィックに適用されるデフォルトのファイアウォール設定を編集することができます。

デフォルトのファイアウォール設定は、どのユーザー定義ファイアウォール ルールにも一致しないトラフィックに適用されます。デフォルトの Distributed Firewall ルールは、統合ファイアウォール ユーザー インターフェイスに表示されます。デフォルトのレイヤー 3 ルールは [全般] タブに表示され、デフォルトのレイヤー 2 ルールは [イーサネット] タブに表示されます。

デフォルトの Distributed Firewall ルールでは、すべての L3 および L2 トラフィックがインフラストラクチャの準備済み全クラスタを通過します。デフォルト ルールは常に、ルール テーブルの下部に表示され、削除や追加はできません。ただし、ルールの操作要素を [許可] から [ドロップ] または [却下] (推奨されません) に変更し、そのルールのトラフィックをログ記録するかどうかを指定したりすることは可能です。

### 手順

- 1 [ファイアウォール (Firewall)] をクリックします。  
[ファイアウォール全般] 画面が表示されます。
- 2 [全般 (General)] タブが開かれていることを確認し、デフォルトの L3 ルールを編集します。[イーサネット (Ethernet)] タブをクリックし、L2 ルールを編集します。
- 3 [アクション (Action)] 列で、セクションを展開し、次のいずれかのオプションを選択します。
  - 許可：指定されたソース、ターゲット、およびプロトコルを持つすべての L3 または L2 トラフィックが、現在のファイアウォール コンテキストを通過するのを許可します。ルールに一致し、承認されたパケットは、ファイアウォールが存在しないかのようにシステム内を移動します。
  - ドロップ：指定されたソース、ターゲット、およびプロトコルを持つパケットをドロップします。パケットのドロップは情報が表示されず、ソース システムまたはターゲット システムへの通知なしで実行されます。パケットをドロップすると、再試行のしきい値に到達するまで、接続が再試行されます。
  - 却下：指定されたソース、ターゲット、およびプロトコルを持つパケットを却下します。パケットの却下は、送信者に対してターゲットに到達できないというメッセージを送信するので、パケットを拒否する方法としてはより適切です。プロトコルが TCP の場合、TCP RST メッセージが送信されます。UDP、ICMP およびその他の IP 接続では、管理上禁止されたコードが含まれる ICMP メッセージが送信されます。[却下] を使用する利点の 1 つは、一度試行しただけで、接続を確立できないことが送信側のアプリケーションに通知されることです。

---

**注：** デフォルト ルールのアクションとして [却下 (Reject)] を選択することは推奨されません。

---

- 4 [ログ (Log)] 列でセクションを展開し、[はい (Yes)] を選択してログを有効にするか、[いいえ (No)] を選択してログを無効にします。ここにメモを書き込むこともできます。[はい] を選択すると、このルールに一致するすべてのセッションがログに記録されます。ログを有効にするとパフォーマンスに影響が出る場合があります。

- 5 [保存 (Save)] をクリックして変更を確定します。

## ファイアウォール ルールの順序の変更

ルールは上から下に順番に処理されます。リスト内のルールの順序を変更することができます。

トラフィックがファイアウォールを通過しようとするとき、パケット情報は [ルール] テーブルに示されるルールに従います。ルールは、一番上から一番下のデフォルト ルールまで順番に適用されます。場合によっては、2 つ以上のルールの優先順位が、トラフィック フローを決定するのに重要になります。

テーブル内でカスタム ルールの位置を上下に移動することができます。デフォルト ルールは常にルール テーブルの下部に表示され、これを移動することはできません。

### 手順

- 1 ナビゲーション パネルの [ファイアウォール (Firewall)] を選択します。  
[全般] タブが開かれていることを確認し、L3 ルールを追加します。[イーサネット] タブをクリックし、L2 ルールを追加します。
- 2 移動するルールの番号を右クリックします。
- 3 [上に移動 (Move Up)] または [下に移動 (Move Down)] を選択します。  
ルールが上または下に 1 つ移動します。

## ファイアウォール ルールのフィルタ

さまざまな基準を使用してルール セットをフィルタできます。これにより、ルールの変更が簡略化されます。

### 手順

- 1 [ファイアウォール] ウィンドウの左上隅で、[フィルタ (Filter)] ▼ FILTER をクリックします。  
[フィルタ] ダイアログ ボックスが表示されます。
- 2 フィルタを使用して次の項目を検索できます。
  - ソース：受信ファイアウォール ルールを検索します。
  - ターゲット：送信ファイアウォール ルールを検索します。
  - 適用先：適用先の基準のルールを検索します。
  - サービス：このリストから、許可またはブロックするアプリケーションまたはサービスを選択します。リストにはすでに多くの一般的なサービスが表示されていますが、選択できるのはこれらのサービスだけではありません。[サービス] セルを使用して、まだ表示されていないサービスまたはアプリケーションを追加します。
- 3 検索する基準をクリックすると、ボックスの一番上に表示されます。
- 4 検索のタイプを選択します。
  - IP セット：このオプションは、ルールのソースまたはターゲットのいずれかの IP アドレスをすべてリストします。
  - 論理ポート：論理ポートでフィルタします。

- 論理スイッチ：論理スイッチでフィルタします。
- NSGroup：NSGroup でフィルタします。

フィルタの結果がボックスに表示されます。

## ファイアウォールからのオブジェクト除外

論理ポート、論理スイッチ、または NSGroup をファイアウォール ルールから除外できます。

ファイアウォール ルールのセクションを作成後、1 つの NSX-T アプライアンス ポートをファイアウォール ルールから除外できます。

### 手順

- 1 ナビゲーション パネルの [ファイアウォール (Firewall)] を選択します。[設定 (Configuration)] タブを選択します。  
除外リスト画面が表示されます。
- 2 ウィンドウ右上の [オブジェクト (Objects)] を選択します。
- 3 ドロップダウン リストから [論理ポート (Logical Ports)]、[論理スイッチ (Logical Switch)]、または [NSGroup] を選択します。
- 4 ファイアウォール ルールから除外する特定のポート、スイッチ、またはグループをダブルクリックします。[オブジェクト] ダイアログ ボックスを閉じるには、もう一度 [オブジェクト (Objects)] をクリックします。  
除外リストに、除外するオブジェクトの名前と種類が入力されます。
- 5 オブジェクトを除外グループから削除するには、[x] をクリックします。
- 6 [保存 (Save)] をクリックします。

## グループとサービスの設定

グループを設定してオブジェクトを分類することができます。

ファイアウォール ルールには次のグループを使用することができます。

- IP セット
- MAC セット
- サービス グループ
- IP セット、MAC セット、論理ポート、論理スイッチ、および他の NSGroup を含むことができる NSGroup

さらに、トランスポート ノードを作成するときに IP アドレス プールを作成して、IP アドレスを割り当てることができます。

この章には、次のトピックが含まれています。

- [IP セットの作成](#)
- [IP アドレス プールの作成](#)
- [MAC セットの作成](#)
- [NSGroup の作成](#)
- [サービスとサービス グループの設定](#)

### IP セットの作成

IP セットは、ファイアウォール ルール内のソースおよびターゲットとして使用することができる IP アドレスのグループです。

IP セットには、個々の IP アドレス、IP アドレス範囲およびサブネットの組み合わせを含めることができます。IPv4 または IPv6 アドレス、あるいはその両方を指定することができます。IP セットは NSGroup のメンバーである場合があります。

---

**注:** ファイアウォール ルールのソースまたはターゲットの範囲には IPv6 はサポートされません。

---

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[インベントリ (Inventory)] - [グループ (Groups)] の順に選択します。

- 3 メイン パネルの一番上で [IP セット] を選択します。
- 4 [追加] をクリックします。
- 5 名前を入力します。
- 6 (オプション) 説明を入力します。
- 7 個々のアドレスまたはアドレスの範囲を入力します。
- 8 [保存] をクリックします。

## IP アドレス プールの作成

L3 サブネットを作成するときに、IP アドレス プールを使用して IP アドレスまたはサブネットを割り当てることができます。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[インベントリ (Inventory)] - [グループ (Groups)] の順に選択します。
- 3 メイン パネルの一番上で [IP アドレス プール] を選択します。
- 4 [追加] をクリックします。
- 5 名前を入力します。
- 6 (オプション) 説明を入力します。
- 7 [追加] をクリックします。
- 8 IP アドレス範囲を入力します。  
任意のセルの右上隅にマウスを合わせ、鉛筆のアイコンをクリックして編集します。
- 9 (オプション) ゲートウェイを入力します。
- 10 CIDR IP アドレスをサフィックス付きで入力します。
- 11 (オプション) DNS サーバを入力します。
- 12 (オプション) DNS サフィックスを入力します。
- 13 [保存] をクリックします。

## MAC セットの作成

MAC セットは MAC アドレスのグループで、レイヤー 2 ファイアウォール ルールのソースまたはターゲット、および NS グループのメンバーとして使用することができます。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[インベントリ (Inventory)] - [グループ (Groups)] の順に選択します。

- 3 メイン パネルの一番上で [MAC セット] を選択します。
- 4 [追加] をクリックします。
- 5 名前を入力します。
- 6 (オプション) 説明を入力します。
- 7 MAC アドレスを入力します。
- 8 [保存] をクリックします。

## NSGroup の作成

IP セット、MAC セット、論理ポート、論理スイッチおよび他の NSGroup の組み合わせを含むように NSGroup を設定することができます。ファイアウォール ルールまた **Applied To** フィールド内のソースおよびターゲットとして、NSGroup を指定することができます。

NSGroup には次の特性があります。

- 直接メンバーを指定することができます。これには、IP セット、MAC セット、論理スイッチ、論理ポート、および NSGroup があります。
- 論理スイッチと論理ポートには、最大 5 つのメンバーシップ基準を指定することができます。基準ごとに、タグ、およびオプションとして範囲を指定します。
- NSGroup には直接メンバーと有効なメンバーがあります。有効なメンバーには、メンバーシップ基準を使用して指定するメンバー、およびこの NSGroup のメンバーに属するすべての直接メンバーおよび有効なメンバーが含まれます。たとえば、NSGroup-1 に直接メンバー LogicalSwitch-1 が含まれているとします。NSGroup-2 を追加し、メンバーとして NSGroup-1 および LogicalSwitch-2 を指定します。これで、NSGroup-2 には直接のメンバーとして NSGroup-1 および LogicalSwitch-2、有効なメンバーとして LogicalSwitch-1 が含まれるようになります。次に、NSGroup-3 を追加し、メンバーとして NSGroup-2 を指定します。これで、NSGroup-3 には直接のメンバーとして NSGroup-2、有効なメンバーとして LogicalSwitch-1 および LogicalSwitch-2 が含まれるようになります。
- NSGroup には最高で 500 の直接メンバーを含めることができます。
- NSGroup で推奨される有効なメンバーの最大数は 5000 です。この制限を超えても機能への影響はありませんが、パフォーマンスにマイナスの影響をおよぼす場合があります。NSX Manager で、NSGroup の有効なメンバーの数が 5000 の 80% を超えると、「**NSGroup xyz is about to exceed the maximum member limit.Total number in NSGroup is ...**」という警告メッセージがログ ファイルに表示され、5000 を超えると、「**NSGroup xyz has reached the maximum numbers limit.Total number in NSGroup = ...**」という警告メッセージが表示されます。NSX Controller で、NSGroup 内の変換された VIF/IP/MAC の数が 5000 を超えると、「**Container xyz has reached the maximum IP/MAC/VIF translations limit.Current translations count in Container – IPs:..., MACs:..., VIFs:...**」という警告メッセージがログ ファイルに表示されます。NSX Manager および NSX Controller は、この制限について NSGroup を一日 2 回（午前 7 時と午後 7 時）チェックします。



メンバーとして NSGroup に追加できるすべてのオブジェクト、すなわち論理スイッチ、論理ポート、IP セット、MAC セットおよび NSGroup について、それらのオブジェクトの画面に移動して、[関連 (Related)] - [NSGroup (NSGroups)] の順に選択し、そのオブジェクトを直接的または間接的にメンバーとして所有するすべての NSGroup を表示することができます。たとえば上の例で、LogicalSwitch-1 の画面に移動した後、[関連 (Related)] - [NSGroup (NSGroups)] の順に選択すると、NSGroup-1、NSGroup-2、および NSGroup-3 が表示されます。それは、これらの 3 つがすべて、直接的または間接的に LogicalSwitch-1 をメンバーとして所有しているからです。

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[インベントリ (Inventory)] - [グループ (Groups)] の順に選択します。
- 3 メイン パネルの一番上で [NSGroup (NSGroups)] を選択します。
- 4 [追加 (Add)] をクリックします。
- 5 NSGroup の名前を入力します。
- 6 (オプション) 説明を入力します。
- 7 (オプション) [メンバーシップ基準 (Membership Criteria)] をクリックして、最大 5 つの基準を指定します。

基準は論理スイッチまたは論理ポートに適用することができます。

基準は、タグ値、範囲の値、またはその両方を指定することができます。

- 8 (オプション) [メンバー (Members)] をクリックしてメンバーを選択します。

使用可能なタイプは、[IP セット (IP Set)]、[MAC セット (MAC Set)]、[論理スイッチ (Logical Switch)]、[論理ポート (Logical Port)]、および [NSGroup] です。

- 9 [保存 (Save)] をクリックします。

## サービスとサービス グループの設定

NSService を設定して、ポートやプロトコルのペアリングなど、一致するネットワーク トラフィックのパラメータを指定することができます。また、NSService を使用してファイアウォール ルールの特定のタイプのトラフィックを許可またはブロックすることもできます。

NSService には、次のようなタイプがあります。

- Ether
- IP
- IGMP
- ICMP
- ALG
- L4 ポート セット

L4 ポート セットは、ソース ポートおよびターゲット ポートの特定をサポートします。個々のポートを指定することも、最大 15 ポートまで一括で指定することもできます。

NSService は、他の NSService のグループになることもできます。グループとしての NSService には次のタイプがあります。

- レイヤー 2
- レイヤー 3 以上

NSService を作成した後でタイプを変更することはできません。いくつかの NSService は事前定義されています。それらを変更または削除することはできません。

## NSService の作成

NSService を作成して、ネットワークの一致で使用する特性を指定したり、ファイアウォール ルールでブロックまたは許可するトラフィックのタイプを定義したりすることができます。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[インベントリ (Inventory)] - [サービス (Services)] の順に選択します。
- 3 [追加 (Add)] をクリックします。
- 4 名前を入力します。
- 5 (オプション) 説明を入力します。
- 6 [プロトコルを指定 (Specify a protocol)] を選択して個々のサービスを設定するか、[既存のサービスをグループ化 (Group existing services)] を選択して NSService のグループを設定します。
- 7 個々のサービスに対して、タイプとプロトコルを選択します。  
使用可能なタイプは、[Ether]、[IP アドレス]、[IGMP]、[ICMP]、[ALG]、および [L4 ポートセット (L4 Port Set)] です。
- 8 サービス グループに対して、グループのタイプとメンバーを選択します。  
使用可能なタイプは、[レイヤー 2 (Layer 2)] および [レイヤー 3 以上 (Layer 3 and above)] です。
- 9 [保存 (Save)] をクリックします。

# DHCP

Dynamic Host Configuration Protocol (DHCP) を使用すると、IP アドレス、サブネット マスク、デフォルト ゲートウェイ、DNS 設定などのネットワーク設定をクライアントが DHCP サーバから自動的に取得できます。

DHCP リクエストを処理する DHCP サーバを作成するか、外部の DHCP サーバに DHCP トラフィックを中継する DHCP リレー サービスを作成できます。

DHCP サーバを設定する場合は、セキュリティを強化するために、UDP ポート 67 と 68 で有効な DHCP サーバ IP アドレスのトラフィックのみを許可する Distributed Firewall ルールを設定します。

---

**注:** **Logical Switch/Logical Port/NSGroup** を送信先、**Any** を送信元として、ポート 67 と 68 で DHCP パケットをドロップするように設定した Distributed Firewall ルールでは、DHCP トラフィックをブロックできません。DHCP トラフィックをブロックするには、送信元と送信先の両方を **Any** に設定します。

---

この章には、次のトピックが含まれています。

- DHCP サーバ プロファイルの作成
- DHCP サーバの作成
- 論理スイッチへの DHCP サーバの接続
- 論理スイッチからの DHCP サーバの切り離し
- DHCP リレー プロファイルの作成
- DHCP リレー サービスの作成
- 分散論理ルーター ポートへの DHCP サービスの追加

## DHCP サーバ プロファイルの作成

DHCP サーバ プロファイルは、NSX Edge クラスタまたは NSX Edge クラスタのメンバーを指定します。このプロファイルを持つ DHCP サーバは、プロファイルで指定された NSX Edge ノードに接続されている論理スイッチ上の仮想マシンからの DHCP 要求を処理します。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [DHCP] を選択します。
- 3 [サーバ プロファイル] をクリックし、[追加] をクリックします。

- 名前を入力します。オプションで説明を入力できます。
- ドロップダウン メニューから NSX Edge クラスタを選択します。
- (オプション) NSX Edge クラスタのメンバーを選択します。

最大で 2 つのメンバーを指定できます。

#### 次のステップ

DHCP サーバを作成します。「[「DHCP サーバの作成」](#)」を参照してください。

## DHCP サーバの作成

論理スイッチに接続されている仮想マシンからの DHCP 要求を処理する DHCP サーバを作成できます。

#### 手順

- ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- ナビゲーション パネルから [DHCP] を選択します。
- [サーバ] をクリックし、[追加] をクリックします。
- 名前を入力します。オプションで説明を入力できます。
- DHCP サーバの IP アドレスとサブネット マスクを CIDR 形式で入力します。  
たとえば、**192.168.1.2/24** と入力します。
- ドロップダウン メニューから DHCP プロファイルを選択します。
- (オプション) ドメイン名、デフォルト ゲートウェイ、DNS サーバ、サブネット マスクなどの共通オプションを入力します。
- (オプション) クラスレス スタティック ルート オプションを入力します。
- (オプション) 他のオプションを入力します。
- [保存] をクリックします。
- 新しく作成した DHCP サーバを選択します。
- IP アドレス プールのセクションを展開します。
- [追加] をクリックして、IP アドレス範囲、デフォルト ゲートウェイ、リース期間、警告のしきい値、エラーのしきい値、クラスレス スタティック ルート オプション、およびその他のオプションを追加します。
- 静的バインドのセクションを展開します。
- [追加] をクリックして、MAC アドレスと IP アドレスの間の静的バインド、デフォルト ゲートウェイ、ホスト名、リース期間、クラスレス スタティック ルート オプション、およびその他のオプションを追加します。

#### 次のステップ

DHCP サーバを論理スイッチに接続します。「[「論理スイッチへの DHCP サーバの接続」](#)」を参照してください。

## 論理スイッチへの DHCP サーバの接続

DHCP サーバがスイッチに接続された仮想マシンからの DHCP リクエストを処理するには、DHCP サーバを論理スイッチに接続する必要があります。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[スイッチング (Switching)] - [スイッチ (Switches)] の順に選択します。
- 3 DHCP サーバを接続する論理スイッチをクリックします。
- 4 [アクション] - [DHCP サーバを接続] をクリックします。

## 論理スイッチからの DHCP サーバの切り離し

論理スイッチから DHCP サーバを切り離して、環境を再設定することができます。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[スイッチング (Switching)] - [スイッチ (Switches)] の順に選択します。
- 3 DHCP サーバを切り離す論理スイッチをクリックします。
- 4 [アクション] - [DHCP サーバを切断] をクリックします。

## DHCP リレー プロファイルの作成

DHCP リレー プロファイルは 1 台以上の外部 DHCP サーバを指定します。DHCP リレー サービスを作成するには、DHCP リレー プロファイルを指定する必要があります。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [DHCP] を選択します。
- 3 [リレー プロファイル] をクリックし、[追加] をクリックします。
- 4 名前を入力します。オプションで説明を入力できます。
- 5 1 つ以上の外部 DHCP サーバ アドレスを入力します。

### 次のステップ

DHCP リレー サービスを作成します。「[\[DHCP リレー サービスの作成\]](#)」を参照してください。

## DHCP リレー サービスの作成

DHCP リレー サービスを作成して、NSX-T で作成されていない DHCP クライアントと DHCP サーバ間にトラフィックをリレーすることができます。

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [DHCP] を選択します。
- 3 [リレー サービス] をクリックし、[追加] をクリックします。
- 4 名前を入力します。オプションで説明を入力できます。
- 5 ドロップダウン メニューから DHCP リレー プロファイルを選択します。

#### 次のステップ

分散論理ルーター ポートに DHCP サービスを追加します。「[\[分散論理ルーター ポートへの DHCP サービスの追加\]](#)」を参照してください。

## 分散論理ルーター ポートへの DHCP サービスの追加

分散論理ルーター ポートに DHCP リレー サービスを追加すると、そのポートに接続する論理スイッチの仮想マシンは、リレー サービス内で設定された DHCP サーバと通信することができます。

#### 前提条件

- DHCP リレー サービスが設定されていることを確認します。「[\[DHCP リレー サービスの作成\]](#)」を参照してください。

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [ルーティング (Routing)] を選択します。
- 3 目的の論理スイッチに接続されたルーターを選択し、[設定] タブをクリックします。
- 4 目的の論理スイッチに接続するルーター ポートを選択し、[編集] をクリックします。
- 5 [DHCP サービス] ドロップダウン リストから DHCP リレー サービスを選択し、[保存] をクリックします。

分散論理ルーター ポートは、[DHCP サービス] 列に DHCP リレー サービスを表示します。

また、新しい分散論理ルーター ポートを追加するときに DHCP リレー サービスを選択することもできます。

## メタデータ プロキシの設定

メタデータ プロキシ サーバでは、仮想マシン インスタンスは OpenStack Nova API サーバからインスタンス固有のメタデータを取得することができます。

次の手順では、メタデータ プロキシがどのように機能するかを説明します。

- 1 仮想マシンは、あるメタデータを要求するために HTTP GET を <http://169.254.169.254:80> に送信します。
- 2 仮想マシンと同じ論理スイッチに接続されたメタデータ プロキシ サーバが要求を受信し、ヘッダーに適切な変更を加え、Nova API サーバに要求を転送します。
- 3 Nova API サーバは、Neutron サーバから仮想マシンに関する情報の要求や受信を行います。
- 4 Nova API サーバはメタデータを検索し、それをメタデータ プロキシ サーバに送信します。
- 5 メタデータ プロキシ サーバはメタデータを仮想マシンに転送します。

メタデータ プロキシ サーバは NSX Edge ノードで実行します。高可用性を実現するため、メタデータ プロキシを NSX Edge クラスタ内の 2 台以上の NSX Edge ノードで実行するように設定することができます。

この章には、次のトピックが含まれています。

- [メタデータ プロキシ サーバの追加](#)
- [論理スイッチへのメタデータ プロキシ サーバの接続](#)
- [メタデータ プロキシ サーバの論理スイッチからの切り離し](#)

### メタデータ プロキシ サーバの追加

メタデータ プロキシ サーバを追加すると、仮想マシンが OpenStack Nova API サーバからメタデータを取得できます。

#### 前提条件

Edge クラスタを作成したことを確認します。詳細については、『[NSX-T インストール ガイド](#)』を参照してください。

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 [DHCP] > [メタデータ プロキシ (Metadata Proxies)] の順に選択します。
- 3 [追加 (Add)] をクリックします。

- 4 メタデータ プロキシ サーバの名前を入力します。
- 5 (オプション) 説明を入力します。
- 6 Nova サーバの URL を入力します。
- 7 **secret** パラメータを入力します。
- 8 ドロップダウン リストから Edge クラスタを選択します。
- 9 (オプション) Edge クラスタのメンバーを選択します。

次はその例です。

## 新しいメタデータ プロキシ サーバ



名前 *	metedata-proxy-1
説明	<div></div>
Nova サーバの URL *	http://123.1.1.1
シークレット キー *	●●●●●●
Edge クラスタ *	EDGECLUSTER1 ▼
メンバー	<div>53293932-b4b0-11e8-8ae0-000c298761d2 ×</div> × ▼

キャンセル

追加

### 次のステップ

メタデータ プロキシ サーバを論理スイッチに接続します。

## 論理スイッチへのメタデータ プロキシ サーバの接続

論理スイッチに接続された仮想マシンにメタデータ プロキシ サービスを提供するには、メタデータ プロキシ サーバをスイッチに接続する必要があります。

### 前提条件

論理スイッチが作成されたことを確認します。詳細については、「[論理スイッチの作成](#)」を参照してください。



#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 [DHCP] > [メタデータ プロキシ (Metadata Proxies)] の順に選択します。
- 3 メタデータ プロキシ サーバを選択します。
- 4 メニュー オプション [アクション (Actions)] - [論理スイッチへ接続 (Attach to Logical Switch)] の順に選択します。
- 5 ドロップダウン リストから論理スイッチを選択します。

また、[スイッチング (Switching)] > [スイッチ (Switches)] に移動し、スイッチを選択し、メニュー オプション [アクション (Actions)] - [メタデータ プロキシを接続 (Attach Metadata Proxy)] の順に選択してメタデータ プロキシサーバを論理スイッチに接続することもできます。

## メタデータ プロキシ サーバの論理スイッチからの切り離し

論理スイッチに接続しているか、別のメタデータ プロキシ サーバを使用している仮想マシンへのメタデータ プロキシサービスの提供を停止するには、メタデータ プロキシ サーバを論理スイッチから切り離すことができます。

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 [DHCP] > [メタデータ プロキシ (Metadata Proxies)] の順に選択します。
- 3 メタデータ プロキシ サーバを選択します。
- 4 [操作 (Actions)] - [論理スイッチから切り離し (Detach from Logical Switch)] の順に選択します。
- 5 ドロップダウン リストから論理スイッチを選択します。

メタデータ プロキシ サーバを論理スイッチから切り離す別の方法として、[スイッチング (Switching)] > [スイッチ (Switches)] の順に選択し、スイッチを選択して、[操作 (Actions)] - [メタデータ プロキシの切り離し (Detach Metadata Proxy)] の順に選択することもできます。

## 運用管理

たとえば、ライセンスや証明書の追加、パスワードの変更など、インストールしたアプライアンスの設定の変更が必要になる場合があります。また、バックアップの実行などを含む、ルーチンのメンテナンス タスクもあります。さらに、リモート システム ログ、トレースフロー、ポート接続など、NSX-T インフラストラクチャの一部であるアプライアンスおよび NSX-T によって作成された論理ネットワークに関する情報を見つけるのに役立つツールがあります。

この章には、次のトピックが含まれています。

- [ライセンス キーの追加](#)
- [ユーザー アカウントの管理](#)
- [証明書の設定](#)
- [アプライアンスの設定](#)
- [タグの管理](#)
- [オブジェクトの検索](#)
- [リモート サーバの SSH フィンガープリントの検索](#)
- [NSX Manager のバックアップとリストア](#)
- [アプライアンスとアプライアンス クラスタの管理](#)
- [ロギング システム メッセージ](#)
- [IPFIX の設定](#)
- [トレースフローによるパケットのパスのトレース](#)
- [ポート接続情報の表示](#)
- [論理スイッチ ポート アクティビティの監視](#)
- [ポート ミラーリング セッションの開始](#)
- [ファブリック ノードの監視](#)
- [サポート バンドルの収集](#)

### ライセンス キーの追加

NSX Manager ユーザー インターフェイスを使用して、1 つまたは複数のライセンス キーを追加することができます。

次の非評価版ライセンス タイプを使用することができます。

- 標準
- 詳細
- エンタープライズ

NSX Manager をインストールすると、インストール済みの評価版ライセンスがアクティブになり、60 日間有効になります。評価版ライセンスは、エンタープライズ ライセンスの機能をすべて提供します。評価版ライセンスをインストールしたり、割り当て解除したりすることはできません。

1 つまたは複数の非評価版ライセンスをインストールすることができますが、各タイプに対してインストールできるキーの数は 1 つです。標準、拡張、またはエンタープライズ版ライセンスをインストールすると、評価版ライセンスは利用できなくなります。また、非評価版ライセンスを割り当て解除することもできます。非評価版ライセンスをすべて割り当て解除すると、評価版ライセンスが復元されます。

同じライセンス タイプの複数のキーがあり、それらのキーを組み合わせる場合は、<https://my.vmware.com> にアクセスして キーの組み合わせ 機能を使用する必要があります。NSX Manager のユーザー インターフェイスにはこの機能はありません。

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[システム (System)] - [設定 (Configuration)] - [ライセンス (License)] の順に選択します。
- 3 [追加] をクリックしてライセンス キーを入力します。
- 4 [保存] をクリックします。

## ユーザー アカウントの管理

NSX-T アプライアンスにはローカルの管理ユーザーである admin があります。ユーザーを作成または削除することはできません。

## 管理者パスワードの変更

任意の NSX-T アプライアンスで管理者ユーザーのパスワードを変更することができます。

#### 手順

- 1 NSX Manager CLI にログインします。

## 2 set user コマンドを実行します。

```
nsx> set user admin
Current password:
New password:
Confirm new password:
nsx>
```

パスワードは、次のパスワードの複雑さの要件を満たす必要があります。

- 8 文字以上の長さ
- 1 文字以上の大文字
- 1 文字以上の小文字
- 1 文字以上の数字
- 1 文字以上の特殊文字

## アカウントのロックアウト

5 回連続してログインに失敗すると、管理者アカウントは 15 分間ロックされます。

NSX Manager、NSX Controller、および NSX Edge ノードでは、5 回連続してログインに失敗すると、管理者アカウントは 15 分間ロックされます。ロックされたアカウントをリセットするには、15 分間待ってから再度ログインします。これは意図的な動作で、ログイン失敗のメッセージが「パスワードが違います」から「アカウントがロックされています」に変わるのを見た攻撃者がアカウントの存在を知るのを防いでいます。

---

**注:** これは SSH 経由、またはコンソール経由の管理者ログインに適用されます。

---

## 証明書の設定

NSX Manager で証明書署名要求 (CSR) を生成し、認証局 (CA) に送信してサーバ証明書を取得することができます。

証明書署名要求は自己署名証明書を生成する場合にも使用することができます。既存の証明書または CA 証明書を持っている場合は、それをインポートして使用することができます。また、失効した証明書を含む証明書失効リスト (CRL) をインポートすることもできます。

## 証明書署名要求ファイルの作成

証明書署名要求 (CSR) は、組織名、共通名、地域、国などの特定の情報を含む暗号化されたテキストです。証明書署名要求ファイルを認証局 (CA) に送信して、デジタル ID 証明書を申請します。

### 前提条件

- 証明書署名要求ファイルに入力する必要がある情報を収集します。サーバの FQDN、組織単位、組織、都市、州、および国を確認しておく必要があります。
- プライベート キーとパブリック キーのペアが利用可能であることを確認します。

## 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [システム (System)] - [設定 (Settings)] の順に選択します。
- 3 [証明書 (Certificates)] タブをクリックします。
- 4 ドロップダウン メニューから [証明書署名要求 (CSRs)] を選択します。
- 5 [証明書署名要求の生成 (Generate CSR)] をクリックします。
- 6 証明書署名要求ファイルの詳細を完成させます。

オプション	説明
名前	証明書の名前を割り当てます。
共通名	サーバの完全修飾ドメイン名 (FQDN) を入力します。 例 : test.vmware.com
組織名	適用されるサフィックスを持つ組織名を入力します。 例 : VMware Inc
組織単位	この証明書を扱う組織の部門を入力します。 例 : IT department
地域	組織が存在する都市を入力します。 例 : Palo Alto
状態	組織が存在する州を入力します。 例 : California
国	組織が存在する国を入力します。 例 : United States (US)
メッセージのアルゴリズム	証明書の暗号化アルゴリズムを設定します。  RSA 暗号化は、デジタル署名およびメッセージの暗号化に使用されます。したがって、暗号化トークンを作成するときは DSA より低速になりますが、このトークンを分析または検証するときは高速になります。この暗号化では、暗号化の解除は低速になり、暗号化は高速になります。  DSA 暗号化はデジタル署名に使用されます。したがって、暗号化トークンを作成するときは RSA より高速になりますが、このトークンを分析または検証するときは低速になります。この暗号化では、暗号化の解除は高速になり、暗号化は低速になります。
キーのサイズ	暗号化アルゴリズムのキーのビット サイズを設定します。  特にキーのサイズを変更する必要がなければ、デフォルト値の 2048 を使用します。多くの CA では、最小値 2048 が必要です。キーのサイズをこれよりも大きくすると、より安全になりますが、パフォーマンスに対する影響が大きくなります。
説明	後でこの証明書を識別しやすくするため、特定の詳細を入力します。

- 7 [保存 (Save)] をクリックします。  
カスタムの証明書署名要求がリンクとして表示されます。
- 8 証明書署名要求を選択して [アクション (Actions)] をクリックします。
- 9 ドロップダウン メニューから [CSR PEM をダウンロード (Download CSR PEM)] を選択します。  
記録および認証局送信のために CSR PEM ファイルを保存することができます。

10 証明書署名要求ファイルのコンテンツを使用して、認証局登録プロセスに従って認証局に証明書要求を送信します。

認証局は、証明書署名要求ファイルの情報に基づいてサーバ証明書を作成し、プライベート キーを使用して署名し、証明書を送信します。CA はまた、ルート CA 証明書も送信します。

## CA 証明書のインポート

署名された CA 証明書をインポートし、会社の臨時的 CA として使用することができます。証明書をインポートすると、自分の証明書に署名する権限が与えられます。

### 前提条件

CA 証明書が使用可能であることを検証します。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [システム (System)] - [設定 (Settings)] の順に選択します。
- 3 [証明書] タブの [インポート (Import)] をクリックします。
- 4 ドロップダウン メニューから [CA 証明書をインポート (Import CA Certificate)] を選択して、証明書の詳細を追加します。

オプション	説明
名前	CA 証明書に名前を割り当てます。
証明書の内容	コンピュータの CA 証明書ファイルを参照し、ファイルを追加します。
説明	この CA 証明書の内容のサマリを入力します。

- 5 [保存 (Save)] をクリックします。

これで、独自の証明書に署名できるようになります。

## 証明書のインポート

プライベート キーを使用して証明書をインポートし、自己署名証明書を作成することができます。

### 前提条件

証明書が使用可能であることを検証します。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [システム (System)] - [設定 (Settings)] の順に選択します。
- 3 [証明書] タブの [インポート (Import)] をクリックします。

- 4 ドロップダウン メニューから [証明書をインポート (Import Certificate)] を選択して、証明書の詳細を追加します。

オプション	説明
名前	CA 証明書に名前を割り当てます。
証明書の内容	コンピュータの証明書ファイルを参照し、ファイルを追加します。
プライベート キー	コンピュータのプライベート キー ファイルを参照し、ファイルを追加します。
パスワード	この証明書のパスワードを追加します。
説明	この証明書の内容のサマリを入力します。

- 5 [保存 (Save)] をクリックします。

これで、独自の自己署名証明書を作成できます。

## 自己署名証明書の作成

自己署名証明書の使用は信頼される証明書の使用ほど安全ではない場合があります。

自己署名証明書を使用すると、クライアント ユーザーは **Invalid Security Certificate** のような警告メッセージを受け取ります。先に進むために、クライアント ユーザーはサーバに最初に接続するときに自己署名証明書を受け入れる必要があります。クライアント ユーザーにこのオプションの選択を許可すると、他の認証方法に比べてセキュリティが低下します。

### 前提条件

証明書署名要求 (CSR) が使用可能であることを検証します。[「証明書署名要求ファイルの作成」](#) を参照してください。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [システム (System)] - [設定 (Settings)] の順に選択します。
- 3 [証明書 (Certificates)] タブをクリックします。
- 4 ドロップダウン メニューから [証明書署名要求 (CSRs)] を選択します。
- 5 既存の証明書署名要求を選択します。
- 6 [アクション (Actions)] をクリックし、ドロップダウン メニューから [証明書署名要求の自己署名証明書 (Self Sign Certificate for CSR)] を選択します。
- 7 自己署名証明書が有効な日数を入力します。  
デフォルトの期間は 10 年です。
- 8 [保存 (Save)] をクリックします。

[証明書 (Certificate)] リストに自己署名証明書が表示されます。証明書のタイプは自己署名として指定されます。

## 証明書の置き換え

たとえば有効期限が切れるために証明書を交換する必要がある場合は、API リクエストを使用して既存の証明書を置き換えることができます。

### 前提条件

NSX Manager で証明書が使用可能であることを検証します。「[自己署名証明書の作成](#)」および「[証明書のインポート](#)」を参照してください。

### 手順

- 1 ナビゲーション パネルから、[システム (System)] - [設定 (Settings)] の順に選択します。
- 2 [証明書 (Certificates)] タブをクリックし、ドロップダウン メニューから [証明書 (Certificates)] を選択します。
- 3 使用する証明書の ID をクリックし、ポップアップ ウィンドウから証明書 ID をコピーします。
- 4 **POST /api/v1/node/services/http?action=apply\_certificate&certificate\_id=<CertificateID>** API リクエストを送信して既存の証明書を置き換えます。

```
POST https://192.168.110.201/api/v1/node/services/http?
action=apply_certificate&certificate_id=e61c7537-3090-4149-b2b6-19915c20504f
```

API リクエストによって HTTP サービスが再起動し、新しい証明書を使用してサービスを開始できるようになります。POST リクエストに成功すると、応答コード **200 Accepted** を受け取ります。

## 証明書失効リストのインポート

証明書失効リスト (CRL) は、サブスクリイバとその証明書ステータスのリストです。ある潜在的ユーザーがサーバへのアクセスを試みた場合、サーバは、その特定のユーザーに関する CRL エントリに基づいてアクセスを拒否します。

リストには次の項目が含まれています。

- 失効した証明書と失効の理由
- 証明書が発行された日付
- 証明書を発行したエンティティ
- 次のリリースの予定日

### 前提条件

CRL が使用可能であることを確認します。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[システム (System)] - [設定 (Settings)] の順に選択します。



- 3 [証明書 (Certificates)] タブをクリックします。
- 4 ドロップダウン メニューから [CRL (CRLs)] を選択します。
- 5 [インポート (Import)] をクリックし、CRL の詳細を追加します。

オプション	説明
名前	CRL の名前を指定します。
証明書の内容	CRL 内の項目をすべてコピーし、このセクションに貼り付けます。 例： <pre>-----BEGIN X509 CRL----- MIIB0DCB4zANBgqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTETMMaoG A1UECBMD UUXEMRkwFwYDVQQKEwBNaw5jb20gUHR5LiBMdGQuMQswCQYDVQLEwJD UzEbmBkG A1UEAxMSU1NMZW5IGRlbW8gc2VydMvYFw0wMTAxMTUxNjI2NTdaFw0w MTAyMTQx NjI2NTdaMFwiEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEw MTAwMDBa MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZa MA0GCSqG SIb3DQEBAUAA0EAHPjQ3M93Q0j8Ufi +jZM7Y78TfAzG4jJn/E6MYBPFVQFY0/Gp UZexfjSVo5CIyyS0tYscz8o07avwBxTiMpDEQg== -----END X509 CRL---</pre>
説明	CRL の内容について簡単な説明を入力します。

- 6 [保存 (Save)] をクリックします。

インポートされた CRL がリンクとして表示されます。

## アプライアンスの設定

一部のシステム設定タスクは、コマンドラインまたは API を使用して実行する必要があります。

完全なコマンドライン インターフェイスの情報については、『NSX-T コマンドライン インターフェイス リファレンス』を参照してください。完全な API 情報については、『NSX-T API ガイド』を参照してください。

表 11-1. システム設定コマンドおよび API リクエスト。

タスク	コマンドライン (NSX Manager、NSX ControllerNSX Edge)	API リクエスト (NSX Manager のみ)
システムのタイムゾーンを設定	<code>set timezone &lt;timezone&gt;</code>	PUT <code>https://&lt;nsx-mgr&gt;/api/v1/node</code>
NTP サーバを設定	<code>set ntp-server &lt;ntp-server&gt;</code>	PUT <code>https://&lt;nsx-mgr&gt;/api/v1/node/services/ntp</code>

表 11-1. システム設定コマンドおよび API リクエスト。(続き)

タスク	コマンド ライン (NSX Manager、NSX ControllerNSX Edge)	API リクエスト (NSX Manager のみ)
DNS サーバを設定	<code>set name-servers &lt;dns-server&gt;</code>	PUT <code>https://&lt;nsx-mgr&gt;/api/v1/node/network/name-servers</code>
DNS 検索ドメインを設定	<code>set search-domains &lt;domain&gt;</code>	PUT <code>https://&lt;nsx-mgr&gt;/api/v1/node/network/search-domains</code>

## タグの管理

オブジェクトを検索しやすくするため、オブジェクトにタグを追加できます。オブジェクトのタグを指定するときに、対象範囲も指定できます。

### 手順

- 1 ブラウザから、NSX Manager (`https://<nsx-manager-ip-address>`) にログインします。
- 2 オブジェクト カテゴリに移動します。  
たとえば、[スイッチング (Switching)] - [スイッチ (Switches)] の順に選択します。
- 3 オブジェクトを選択します。
- 4 [操作 (Actions)] - [タグの管理 (Manage Tags)] の順に選択します。
- 5 タグを追加または削除します。

オプション	アクション
タグを追加する	[追加 (Add)] をクリックして、タグと、任意で対象範囲を指定します。
タグを削除する	既存のタグを選択し、[削除 (Delete)] をクリックします。

1 つの論理ポートに、最大で 15 個のタグを指定できます。その他のオブジェクトには最大で 10 個のタグを指定できます。

- 6 [保存 (Save)] をクリックします。

## オブジェクトの検索

さまざまな条件を指定してオブジェクトを検索できます。

検索に指定できる条件には、次のものがあります。

- リソース タイプ
- 名前
- 説明
- 作成時間

- 更新時間
- 作成者
- 更新者
- タグ

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 メイン ウィンドウで、画面右上にある虫眼鏡アイコンをクリックします。
- 3 正規表現の検索パターンを入力して、オブジェクトまたはオブジェクト タイプを検索します。

検索パターンでは、デフォルトでアンカーが有効になっています。つまり、文字列の先頭を表すアンカー `^` と、文字列の末尾を表すアンカー `$` があるものと想定されます。これらのアンカーを検索パターン内で使用しないでください。たとえば、「Logical」から始まるリソースを検索したい場合、**Logical.\*** という検索パターンで検索できます。「Switch」で終わるリソースを検索したい場合、**.\*Switch** という検索パターンで検索できます。

- 4 結果が表示されるウィンドウで、下部にある [...の結果を表示 (View ... results)] リンクをクリックすると、検索ペインが開いて検索を絞り込むことができます。
- 5 1 つまたは複数の条件を指定して検索を絞り込みます。

## リモート サーバの SSH フィンガープリントの検索

一部の API 要求で、リモート サーバとの間でファイルのコピーを行う場合は、要求の本文にリモート サーバの SSH フィンガープリントを指定する必要があります。SSH フィンガープリントはリモート サーバ上のホスト キーから生成されます。

SSH 経由で接続するには、NSX Manager とリモート サーバが共通のホスト キー タイプを持つ必要があります。共通のホスト キー タイプが複数ある場合は、NSX Manager の HostKeyAlgorithm 設定で優先されるタイプが使用されます。

リモート サーバのフィンガープリントを指定することで、正しいサーバに接続していることを確認し、中間者攻撃から保護することができます。リモート サーバの管理者に、サーバの SSH フィンガープリントの提供を依頼してください。または、リモート サーバに接続してフィンガープリントを入手することも可能です。ネットワークを経由するよりも、コンソール上でサーバに接続する方が安全です。

NSX Manager アプライアンスは Ubuntu 14.04 に基づき、デフォルトの HostKeyAlgorithm の順序を使用します。デフォルトでこのテーブルは NSX Manager に存在するキーを、優先度の高い順にリストします。

表 11-2. 優先順にリストされた NSX Manager ホスト キー

NSX Manager に存在するホスト キー タイプ	ホスト キー タイプのデフォルトの場所
ECDSA (256 ビット)	/etc/ssh/ssh_host_ecdsa_key.pub
ED25519	/etc/ssh/ssh_host_ed25519_key.pub
RSA	/etc/ssh/ssh_host_rsa_key.pub
DSA	/etc/ssh/ssh_host_dsa_key.pub

## 手順

- 1 リモート サーバの CLI にログインします。

ネットワークを経由するよりも、コンソールを使用してログインの方が安全です。

- 2 `/etc/ssh` ディレクトリにパブリック キー ファイルをリストします。

```
$ ls -al /etc/ssh/*pub
-rw-r--r-- 1 root root 601 Apr  8 18:10 ssh_host_dsa_key.pub
-rw-r--r-- 1 root root 93 Apr  8 18:10 ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root 393 Apr  8 18:10 ssh_host_rsa_key.pub
```

- 3 利用可能なキーを HostKeyAlgorithm の順序と比較します。

この例では、DSA、RSA、ED25519 という 3 つの SSH キーがあります。ED25519 は優先度の最も高いキーで、NSX Manager がリモート サーバに接続するときにはこのキーが使用されます。

- 4 優先されるキーのフィンガープリントを取得します。

```
$ ssh-keygen -lf /etc/ssh/ssh_host_ed25519_key.pub
256 d0:21:3e:ec:52:ff:19:a9:e7:71:b5:7f:63:23:57:f7 root@ubuntu (ED25519)
```

キーのフィンガープリントは d0:21:3e:ec:52:ff:19:a9:e7:71:b5:7f:63:23:57:f7 です。

---

**注:** バックアップとリストアの API 要求では SSH フィンガープリントからコロンを削除する必要があります。

---

## NSX Manager のバックアップとリストア

NSX Manager 仮想アプライアンスが動作が不能になった場合は、バックアップをリストアできます。NSX Manager は仮想ネットワークの最適な状態を保存します。NSX Manager アプライアンスが動作不能になると、データ プレーンに影響を受けませんが、設定の変更はできません。

2 種類のバックアップ方法を使用して、3 種類のバックアップを作成できます。

**クラスタのバックアップ**      このバックアップには、最適な仮想ネットワークの状態が含まれます。

**ノードのバックアップ**      このバックアップには、NSX Manager アプライアンスの設定が含まれます。

**インベントリのバックアップ**      このバックアップには、ESX と KVM のホストおよび Edge が含まれます。この情報はリストア中に使用され、管理プレーンの最適な状態とこれらのホスト間の相違を検出して修正します。

バックアップ方法には次の 2 つがあります。

**手動による NSX Manager ノードのバックアップおよびクラスタのバックアップ**      手動によるノードのバックアップとクラスタのバックアップは、必要に応じていつでも実行することができます。

**自動 NSX Manager ノードのバックアップ、クラスタのバックアップ、およびインベントリのバックアップ**      自動バックアップは設定したスケジュールに基づいて実行されます。自動バックアップが推奨されます。[「自動バックアップのスケジュール設定」](#)を参照してください。

バックアップを常に最新の状態に保つには、自動バックアップを設定します。クラスタのバックアップとインベントリのバックアップは定期的に実行することが重要です。

NSX-T の設定をリストアして、クラスタのバックアップにキャプチャされた状態に戻することができます。バックアップをリストアするときには、バックアップしたアプライアンスと同じ NSX Manager バージョンを実行する新しい NSX Manager アプライアンスにリストアする必要があります。

バックアップとリストアを行うには、ハイパーバイザー、NSX Manager アプライアンス、および NSX Controller アプライアンスに、固定の管理 IP アドレスを設定する必要があります。管理 IP アドレスの変更はサポートされません。DHCP を使用して、NSX Manager および NSX Controller アプライアンスの管理 IP アドレスを割り当てることは、サポートされていません。DHCP を使用してハイパーバイザーの管理 IP アドレスを割り当てる場合は、ハイパーバイザーに対して常に同じ IP アドレスを提供するように DHCP サーバが設定されている必要があります。

## NSX Manager 設定のバックアップ

NSX Manager 設定のバックアップは、NSX Manager ノードのバックアップ、クラスタのバックアップ、およびインベントリのバックアップで構成されます。

### 手順

#### 1 バックアップの保存場所の設定

NSX Manager がアクセスできるリモート SFTP サーバをバックアップの保存場所として設定します。バックアップの保存場所は、バックアップを行う前に設定する必要があります。

#### 2 自動バックアップのスケジュール設定

頻繁に行うバックアップのスケジュールを設定することで、NSX Manager が動作しなくなった場合、設定データをリストアできます。自動バックアップはデフォルトで無効になっています。自動バックアップは、特定の曜日または指定した間隔で実行するようにスケジュール設定できます。バックアップをスケジュール設定することをお勧めします。

### バックアップの保存場所の設定

NSX Manager がアクセスできるリモート SFTP サーバをバックアップの保存場所として設定します。バックアップの保存場所は、バックアップを行う前に設定する必要があります。

### 手順

#### 1 NSX Manager 仮想アプライアンスにログインします。

- 2 [システム (System)] > [ユーティリティ (Utilities)] > [バックアップ (Backup)] の順にクリックします。
- 3 バックアップの保存場所に対するアクセス資格情報を指定するには、ページの右上にある [編集 (Edit)] をクリックします。
- 4 [自動バックアップ (Automatic Backup)] 切り替えボタンをクリックして自動バックアップを有効にします。
- 5 SFTP サーバの IP アドレスまたはホスト名を入力します。
- 6 必要に応じてデフォルトのポートを編集します。
- 7 SFTP サーバへのログインに必要なユーザー名とパスワードを入力します。
- 8 [ターゲット ディレクトリ (Destination Directory)] フィールドに、バックアップの保存先の絶対ディレクトリパスを入力します。
- 9 バックアップ データの暗号化に使用するパスフレーズを入力します。  
バックアップをリストアするにはこのパスフレーズが必要です。バックアップのパスフレーズを忘れた場合、バックアップをリストアすることはできません。
- 10 バックアップを格納するサーバの SSH フィンガープリントを入力します。[「リモート サーバの SSH フィンガープリントの検索」](#) を参照してください。
- 11 [保存 (Save)] をクリックします。
- 12 ページの下にある [今すぐバックアップ (Backup Now)] をクリックして、ファイルを SFTP サーバに書き出し、問題がないかどうか確認します。

#### 次のステップ

自動バックアップのスケジュールを設定します。

### 自動バックアップのスケジュール設定

頻繁に行うバックアップのスケジュールを設定することで、NSX Manager が動作しなくなった場合、設定データをリストアできます。自動バックアップはデフォルトで無効になっています。自動バックアップは、特定の曜日または指定した間隔で実行するようにスケジュール設定できます。バックアップをスケジュール設定することをお勧めします。

#### 前提条件

- 適切なバックアップの保存場所を決定します。単一点障害から保護できる場所を選択します。たとえば、アプライアンスと同じファイル ストアにバックアップを配置しないようにします。そのファイル ストアで障害が発生した場合、アプライアンスとそのバックアップの両方に影響が生じる可能性があります。
- バックアップを格納するサーバの ssh フィンガープリントを検出します。[「リモート サーバの SSH フィンガープリントの検索」](#) を参照してください。バックアップおよびリストアの API 要求では、SSH フィンガープリントにコロンが含まれていないことが必要です。

#### 手順

- 1 NSX Manager 仮想アプライアンスにログインします。
- 2 [システム (System)] > [ユーティリティ (Utilities)] > [バックアップ (Backup)] の順にクリックします。
- 3 ページの右上隅の [編集 (Edit)] をクリックします。

- 4 [ファイル サーバ (File Server)] をクリックし、自動バックアップが有効であることを確認します。
- 5 ページの上にある [スケジュール (Schedule)] をクリックします。
- 6 ノード/クラスタのバックアップの場合、[毎週 (Weekly)] をクリックし SFTP サーバへのバックアップの日時を設定するか、[間隔 (Interval)] をクリックしバックアップの時間間隔を設定します。
- 7 インベントリ バックアップはデフォルトで 30 秒間隔で発生するように設定されているので、頻繁にバックアップが実行されます。デフォルトの設定を使用するか、必要に応じて変更します。
- 8 [保存 (Save)] をクリックします。

---

**注:** 毎週実行するスケジュールの場合、最初のバックアップは、指定した曜日と時刻に実行されます。一定の間隔で実行するスケジュールの場合、最初のバックアップは、バックアップ設定で自動バックアップを有効にした後すぐに実行されます。

---

NSX Manager は、ノードレベル、クラスタレベル、およびインベントリの 3 つのバックアップ ファイルを個別に保存します。バックアップ ファイルは、バックアップ設定で指定した SFTP サーバのディレクトリに保存されます。このディレクトリでは、ファイルはそれぞれ次のディレクトリに保存されます。

- /<ユーザー指定ディレクトリ>/cluster-node-backups (クラスタとノードのバックアップ)
- /<ユーザー指定ディレクトリ>/inventory-summary (インベントリ バックアップ)

## NSX Manager 設定のリストア

NSX Manager アプライアンスが動作不能になり、推奨されるバックアップを実行した場合は、NSX Manager アプライアンスをリストアできます。バックアップをリストアするには、バックアップを作成するときに指定したパスワードが必要です。

### 手順

#### 1 NSX Manager のバックアップをリストアする準備

NSX Manager のバックアップをリストアする前に、新しい NSX Manager アプライアンスをインストールする必要があります。新しい NSX Manager は以前の NSX Manager と同じ管理 IP アドレスを使用してデプロイする必要があります。

#### 2 クラスタのバックアップのリストア

クラスタのバックアップは、適切なネットワーク状態にリストアするために使用されます。ノードのバックアップをリストアする前に、クラスタのバックアップをリストアする必要があります。

#### 3 NSX Manager ノードのバックアップのリストア

ノードのバックアップを作成すると、アプライアンス設定をリストアして、NSX Controller クラスタを接続できるようになります。ノードのバックアップをリストアする前に、クラスタのバックアップをリストアする必要があります。選択するノードのバックアップ ファイルのタイムスタンプは、クラスタのバックアップ ファイルと同一である必要があります。

#### 4 バックアップとリストアのヘルパー スクリプトのダウンロード

NSX Manager から、バックアップとリストアのヘルパー スクリプトをダウンロードする必要があります。

## 5 クラスタのバックアップ後に加えられたファブリックへの変更の取り消し

バックアップとリストアのヘルパー スクリプトは、バックアップがリストアされた後の状態と、スクリプトによってキャプチャされた最新のファブリックの状態と比較し、バックアップをリストア後の最適な状態とファブリックの状態を一致させるように指示します。

## 6 NSX Controller クラスタのリストア

NSX Controller クラスタをリストアできない場合、またはクラスタのメンバーシップ変更により 1 つ以上のコントローラを置き換える必要がある場合は、コントローラの全クラスタをリストアする必要があります。

## NSX Manager のバックアップをリストアする準備

NSX Manager のバックアップをリストアする前に、新しい NSX Manager アプライアンスをインストールする必要があります。新しい NSX Manager は以前の NSX Manager と同じ管理 IP アドレスを使用してデプロイする必要があります。

### 前提条件

- リストアのためのノード、クラスタおよび最新のインベントリ バックアップ ファイルが利用可能であることを確認します。
- ノードおよびクラスタのバックアップ ファイルのパスフレーズを確認します。
- バックアップの作成に使用する NSX Manager のバージョンを確認し、同じバージョンの適切なインストール ファイル（OVA、OVF、または QCOW2）が使用可能であることを確認します。
- ノードのバックアップ作成に使用する NSX Manager に割り当てられた IP アドレスを確認します。
- リストア プロセスが完了するまでは、NSX Manager の設定を変更しないようにします。

### 手順

- 1 古い NSX Manager アプライアンスが実行中の場合（たとえばアップグレード処理をロールバックするためにリストアしている場合）は、アプライアンスをシャット ダウンします。
- 2 新しい NSX Manager アプライアンスをインストールします。
  - 新しい NSX Manager アプライアンスは、バックアップの作成に使用するアプライアンスと同一のバージョンにする必要があります。
  - このアプライアンスは、ノードのバックアップ作成に使用する NSX Manager の IP アドレスを使用して設定する必要があります。

これらの手順の詳細については、『NSX-T インストール ガイド』を参照してください。

### 次のステップ

クラスタ バックアップをリストアします。

## クラスタのバックアップのリストア

クラスタのバックアップは、適切なネットワーク状態にリストアするために使用されます。ノードのバックアップをリストアする前に、クラスタのバックアップをリストアする必要があります。



## 前提条件

- バックアップを格納するサーバの ssh フィンガープリントを検出します。[「リモートサーバの SSH フィンガープリントの検索」](#)を参照してください。バックアップおよびリストアの API 要求では、SSH フィンガープリントにコロンが含まれていないことが必要です。

## 手順

- 1 NSX Manager のステータスが STABLE であることを確認してから、バックアップをリストアします。

```
GET https://192.168.110.201/api/v1/cluster/status
{
  "control_cluster_status" : {
    "status" : "NO_CONTROLLERS"
  },
  "mgmt_cluster_status" : {
    "online_nodes" : [ {
      "mgmt_cluster_listen_ip_address" : "192.168.110.201",
      "uuid" : "422E901F-B167-DA0A-951F-C0278CA8A4BA"
    } ],
    "status" : "STABLE"
  }
}
```

**注:** コントロール クラスタのステータスは **NO\_CONTROLLERS** です。これは、ノード バックアップがリストアされるまで、コントロール クラスタが NSX Manager に接続されないためです。

- 2 クラスタ バックアップのリストアを行うために、API 要求 **POST /api/v1/cluster/backups?action=restore** を送信します。これにより、リモートの場所からバックアップ ファイルがコピーされ、NSX Manager アプライアンス上でリストアされます。API 要求でバックアップ ファイルおよび場所の情報を指定します。

### リストア要求のフィールド:

パスフレーズ	バックアップの作成時に指定されたパスフレーズです。このパスワードを知らない場合は、このバックアップをリストアできません。
サーバ	バックアップ ファイルが格納されるリモート サーバです。
uri	リモート サーバ上のバックアップ ファイルのパスです。
ssh_fingerprint	バックアップ ファイルが格納されるリモート サーバの SSH フィンガープリントです。 <a href="#">「リモートサーバの SSH フィンガープリントの検索」</a> を参照してください。

## リストア要求のフィールド:

<b>username</b>	バックアップ ファイルをコピーする際、リモート サーバへのログインに使用するユーザー名です。
<b>password</b>	バックアップ ファイルをコピーする際、リモート サーバにログインするときに使用するパスワードです。

クラスタ バックアップのリストア要求の例:

```
POST https://192.168.110.201/api/v1/cluster/backups?action=restore
```

```
{
  "restore_file": {
    "passphrase" : "7Taspa5anecR",
    "file_store" : "remote",
    "server" : "192.168.120.151",
    "uri" : "/vol0/backups/backup-cluster-20160314.zip",
    "protocol" : {
      "name" : "scp",
      "ssh_fingerprint" : "b508dfc65562e46e95707c25baf246f1",
      "authentication_scheme" : {
        "scheme_name" : "password",
        "username" : "admin" ,
        "password" : "4uhasWak"
      }
    }
  }
}
```

- 3 システムが再び安定した状態になるまで待機します。
- 4 自動バックアップを無効にします。
  - a NSX Manager 仮想アプライアンスにログインします。
  - b [システム (System)] > [ユーティリティ (Utilities)] > [バックアップ (Backup)] の順にクリックします。
  - c ページの右上の [編集 (Edit)] をクリックします。
  - d [自動バックアップ (Automatic Backup)] 切り替えボタンをクリックして自動バックアップを無効にします。

バックアップとリストアのヘルパー スクリプトを完了した後、自動バックアップをもう一度有効にすることができます。

## 次のステップ

ノードのバックアップがリストアされる前、および NSX Manager と NSX Controller が同期される前に、すべての NSX Controller を再起動してキャッシュされたデータを削除します。[\[NSX Controller クラスタ メンバーの再起動\]](#) を参照してください。

## NSX Manager ノードのバックアップのリストア

ノードのバックアップを作成すると、アプライアンス設定をリストアして、NSX Controller クラスタを接続できるようになります。ノードのバックアップをリストアする前に、クラスタのバックアップをリストアする必要があります。選択するノードのバックアップ ファイルのタイムスタンプは、クラスタのバックアップ ファイルと同一である必要があります。



**警告:** ノードのバックアップをリストアする前に、クラスタのバックアップをリストアする必要があります。ノードのバックアップがリストアされると、コントローラは NSX Manager と通信できるようになり、認識しているネットワーク状態を更新して NSX Manager で設定された、リストア後の適切なネットワーク状態と一致させます。クラスタのバックアップがリストアされていない場合は、適切なネットワーク状態が設定されていないため、現在認識されているネットワーク状態は破棄されます。

### 前提条件

- クラスタのバックアップを NSX Manager 上でリストアします。[「クラスタのバックアップのリストア」](#)を参照してください。
- NSX Manager のバックアップがあることを確認します。[「NSX Manager 設定のバックアップ」](#)を参照してください。
- バックアップを格納するサーバの ssh フィンガープリントを検出します。[「リモートサーバの SSH フィンガープリントの検索」](#)を参照してください。バックアップおよびリストアの API 要求では、SSH フィンガープリントにコロンの含まれていないことが必要です。

### 手順

- 1 NSX Manager のステータスが STABLE であることを確認してから、バックアップをリストアします。

```
GET https://192.168.110.201/api/v1/cluster/status
{
  "control_cluster_status" : {
    "status" : "NO_CONTROLLERS"
  },
  "mgmt_cluster_status" : {
    "online_nodes" : [ {
      "mgmt_cluster_listen_ip_address" : "192.168.110.201",
      "uuid" : "422E901F-B167-DA0A-951F-C0278CA8A4BA"
    } ],
    "status" : "STABLE"
  }
}
```

**注:** コントロール クラスタのステータスは **NO\_CONTROLLERS** です。これは、ノード バックアップがリストアされるまで、コントロール クラスタが NSX Manager に接続されないためです。

- 2 ノードのバックアップをリストアするため、API 要求 **POST /api/v1/node/backups?action=restore** を送信します。これにより、リモート場所からバックアップ ファイルがコピーされ、NSX Manager アプライアンスでリストアされます。API 要求でバックアップ ファイルおよび場所の情報を指定します。

#### リストア要求のフィールド:

パスフレーズ	バックアップの作成時に指定されたパスフレーズです。このパスワードを知らない場合は、このバックアップをリストアできません。
サーバ	バックアップ ファイルが格納されるリモート サーバです。
uri	リモート サーバ上のバックアップ ファイルのパスです。
ssh_fingerprint	バックアップ ファイルが格納されるリモート サーバの SSH フィンガープリントです。 <a href="#">「リモートサーバの SSH フィンガープリントの検索」</a> を参照してください。
username	バックアップ ファイルをコピーする際、リモート サーバへのログインに使用するユーザー名です。
password	バックアップ ファイルをコピーする際、リモート サーバにログインするときに使用するパスワードです。

ノードのバックアップのリストア要求の例:

```
POST https://192.168.110.201/api/v1/node/backups?action=restore

{
  "restore_file": {
    "passphrase" : "7Taspa5anecR",
    "file_store" : "remote",
    "server" : "192.168.120.151",
    "uri" : "/vol0/backups/backup-node-192.168.110.201-20160314.bak",
    "protocol" : {
      "name" : "scp",
      "ssh_fingerprint" : "b508dfc65562e46e95707c25baf246f1",
      "authentication_scheme" : {
        "scheme_name" : "password",
        "username" : "admin" ,
        "password" : "4uhasWak"
      }
    }
  }
}
```

#### 次のステップ

バックアップとリストアのヘルパー スクリプトをダウンロードします。

#### バックアップとリストアのヘルパー スクリプトのダウンロード

NSX Manager から、バックアップとリストアのヘルパー スクリプトをダウンロードする必要があります。

## 前提条件

- ヘルパー スクリプトの実行に使用するマシンがシステム要件を満たしていることを確認します。ヘルパー スクリプトには Python 2 および TLS 1.2 が必要です。ヘルパー スクリプトは、Ubuntu 14.04 で動作することが確認されています。

## 手順

- ◆ バックアップとリストアのヘルパー スクリプトをダウンロードします。これはコマンドラインまたは API を使用して実行できます。

- コマンドラインを使用する場合：

**copy file** コマンドを実行して、リモート サーバにスクリプトをコピーします。**url** 引数は、標準の URL 構文を使用してスクリプトのターゲットを指定します（例：  
<scp://user@server/home/path/to/destination>）。

```
nsx-manager-1> copy file backup_restore_helper.py url  
scp://backups@192.168.120.151/vol0/backups/scripts/
```

- API を使用する場合：

この API 要求を送信し、出力を backup\_restore\_helper.py ファイルに保存します。

```
GET https://nsx-manager-1/api/v1/node/file-store/backup_restore_helper.py/data
```

## 次のステップ

前回クラスタをバックアップした後、ファブリックに加えた変更を元に戻します。

## クラスタのバックアップ後に加えられたファブリックへの変更の取り消し

バックアップとリストアのヘルパー スクリプトは、バックアップがリストアされた後の状態と、スクリプトによってキャプチャされた最新のファブリックの状態と比較し、バックアップをリストア後の最適な状態とファブリックの状態を一致させるように指示します。

## 前提条件

- バックアップとリストアのヘルパー スクリプトをダウンロードしたことを確認します。
- SFTP サーバから最新のインベントリ バックアップをダウンロードしたことを確認します。

## 手順

- 1 バックアップとリストアのヘルパー スクリプトをダウンロードまたはコピーしたマシンにログインします。

- 2 バックアップとリストアのヘルパー スクリプトを実行し、**-d** オプションで、どのチェックポイント（インベントリ）ファイルを使用するかを指定します。

このとき、次の情報を指定します。

<b>-m</b>	NSX Manager IP アドレス
<b>-u</b>	NSX Manager ユーザー名
<b>-p</b>	NSX Manager パスワード
<b>-d</b>	チェックポイント（最新のインベントリ バックアップ）ファイル名

```
$ python backup_restore_helper.py -m 192.168.110.201 -u admin -p <password> -d
backups/backup_restore_checkpoint_20160318_013354.json
```

- 3 **backup\_restore\_helper.py** スクリプト出力の指示に従って、リストア後の最適な状態と一致するようにファブリックの状態を更新します。

## NSX Controller クラスタのリストア

NSX Controller クラスタをリストアできない場合、またはクラスタのメンバーシップ変更により 1 つ以上のコントローラを置き換える必要がある場合は、コントローラの全クラスタをリストアする必要があります。

コントローラのクラスタをリストアする前に、まず、管理プレーンによって認識されているメンバーシップと、コントローラ自身によって認識されている実際のメンバーシップとの間で、制御クラスタ メンバーシップが変更されているかを確認します。バックアップの後で変更が行われた場合は、メンバーシップは異なる場合があります。

- 全クラスタを回復できない場合は、[「NSX Controller クラスタの再展開」](#)を参照してください。
- 以下の手順を実行してクラスタ メンバーシップが変更されたかを確認し、変更されている場合はクラスタをリストアします。

### 前提条件

- クラスタレベルのバックアップが最新の状態であることを確認します。
- クラスタレベルのリストアを実行します。[「クラスタのバックアップのリストア」](#)を参照してください。

### 手順

- 1 NSX Manager の CLI にログインし、**get management-cluster status** コマンドを実行します。
- 2 NSX Controller の CLI にログインし、**get managers** コマンドを実行して、コントローラが Manager に登録されていることを確認します。
- 3 **get control-cluster status** コマンドを実行します。
- 4 メンバーシップの変更を確認するには、**get management-cluster status** コマンドで出力された IP アドレスと **get control-cluster status** コマンドで出力された IP アドレスを比較します。

IP アドレスがすべて同じである場合、アクションは必要ありません。異なる IP アドレスがある場合、残りの手順を実行してコントローラ クラスタ全体をリストアします。

- 5 NSX Controller の CLI にログインし、**get control-cluster status** コマンドを実行して、どれがマスター コントローラかを確認します。  
マスター コントローラは出力で、**is master: true** のように表示されます。
- 6 マスター コントローラ以外のコントローラのいずれかで、**stop service <controller>** コマンドを実行します。
- 7 マスター コントローラにログインし、**detach control-cluster <ip-address[:port]>** コマンドを実行して、前の手順の通常のコントローラの接続を解除します。
- 8 (オプション) NSX Manager で、**get management-cluster status** コマンドの出力にマスター以外のコントローラが表示される場合のみ、NSX Manager 上で **detach controller <uuid>** コマンドを実行して、このコントローラの接続を解除します。
- 9 NSX Controller の CLI にログインし、**deactivate control-cluster** コマンドを実行します。
- 10 **rm -r /opt/vmware/etc/bootstrap-config** および **rm -r /config/vmware/node-uuid** コマンドを使用して、ブートストラップ ファイルおよび uuid ファイルを削除します。
- 11 マスター以外の残りのコントローラに対して手順 6 ~ 10 を実行します。
- 12 マスター コントローラの CLI にログインし、**stop service <controller>** コマンドを実行します。
- 13 NSX Manager 上で **detach controller <uuid>** コマンドを実行し、このコントローラを解除します。
- 14 マスター コントローラの CLI にログインし、**deactivate control-cluster** コマンドを実行します。
- 15 **rm -r /opt/vmware/etc/bootstrap-config** および **rm -r /config/vmware/node-uuid** コマンドを使用して、ブートストラップ ファイルおよび uuid ファイルを削除します。
- 16 NSX Manager から **get management-cluster status** コマンドを実行します。出力にコントローラがまだ表示される場合は、**detach controller <uuid>** コマンドを実行して表示されているコントローラの接続を解除します。

#### 次のステップ

リストされた順序で以下のタスクを完了します。

- 1 ノード レベルのリストアを完了します。[「NSX Manager ノードのバックアップのリストア」](#)を参照してください。
- 2 『NSX-T インストール ガイド』を参照し、管理プレーンを使用して NSX Controller に参加します。
- 3 『NSX-T インストール ガイド』にを参照して、NSX Controller クラスタを再デプロイします。

## アプライアンスとアプライアンス クラスタの管理

NSX-T の各インストールでは、NSX Manager の 1 つのインスタンスのみを必要とし、複数のインスタンスをサポートしません。NSX Controller クラスタには 3 つのメンバーが必要です。NSX Edge クラスタには 2 つ以上のメンバーが必要です。

コントローラまたは Edge クラスタのアプライアンスが動作不能になるか、なんらかの理由で削除する必要がある場合は、新しいアプライアンスに置き換えることができます。

---

**重要:** NSX Controller または NSX Edge クラスタ メンバーシップに変更を加えた場合は、後でクラスタのバックアップを作成し、新しい設定をバックアップしておく必要があります。「[「NSX Manager のバックアップとリストア」](#)」を参照してください。

---

## NSX Manager の管理

CLI コマンドを使用して、NSX Manager のステータスをチェックすることができます。NSX Manager が動作不能で復元できない場合は、NSX Manager アプライアンスを再起動することができます。

### NSX Manager のステータスの取得

CLI コマンドを使用して NSX Manager のステータスを取得することができます。

#### 手順

- 1 NSX Manager の CLI にログインします。
- 2 `get management-cluster status` コマンドを実行します。次に例を示します。

```
nsx-manager> get management-cluster status
Number of nodes in management cluster: 1
-192.168.110.105
Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.52
- 192.168.110.53
- 192.168.110.51
Control cluster status: STABLE.
```

---

**注:** 結果に管理クラスタが表示されても、NSX Manager のインスタンスは 1 つのみです。

---

### NSX Manager の再起動

CLI コマンドを使用して NSX Manager を再起動し、重大なエラーから復元することができます。

#### 手順

- 1 NSX Manager の CLI にログインします。
- 2 `reboot` コマンドを実行します。次に例を示します。

```
nsx-manager> reboot
Are you sure you want to reboot (yes/no): y
```



## NSX Controller クラスタの管理

NSX Controller クラスタには 3 つのメンバーが必要です。トラブルシューティングの結果、NSX Controller アプライアンスの 1 つが回復不能であると判断した場合、交換のためのアプライアンスをクラスタに追加するか、必要に応じて NSX Controller クラスタを再デプロイすることができます。

NSX Controller クラスタが正常に機能するには、マジョリティを持っている必要があります。3 つのメンバーのうち 2 つがオンラインであれば、クラスタはまだマジョリティを持っています。オフラインの NSX Controller をオンラインにして 3 つのメンバーから成るクラスタを復元する必要があります。オンラインできない場合は、別の NSX Controller アプライアンスを追加して交換し、再度マジョリティを取得することができます。[「NSX Controller クラスタのメンバーの置き換え」](#)を参照してください。

3 つのメンバーのうち 1 つがオンラインの場合、クラスタにはマジョリティがなく、正常に機能しません。オフラインのメンバーをオンラインにすると、クラスタはマジョリティを再度取得します。オフラインのメンバーをどれもオンラインにできない場合は、NSX Controller クラスタを再デプロイすることができます。[「NSX Controller クラスタの再展開」](#)を参照してください。

### 前提条件

トラブルシューティングを通じて、アプライアンスがリカバリ不能であることを確認してください。たとえば、次の手順を行うことで、アプライアンスを交換せずにリカバリできる場合があります。

- アプライアンスがネットワークに接続されていることを確認します。接続されていない場合は解決します。
- アプライアンスを再起動します。

### 次のステップ

NSX Controller クラスタのステータスを取得します。[「NSX Controller クラスタのステータスの取得」](#)を参照してください。

## NSX Controller クラスタのステータスの取得

NSX Manager から NSX Controller クラスタのステータスを検索することができます。また、コマンドライン インターフェイスから各 NSX Controller のステータスをチェックすることができます。

NSX Controller クラスタおよびクラスタ メンバーのステータスを取得して、NSX Controller クラスタの問題の原因の特定に利用できます。

表 11-3. NSX Controller クラスタのステータス

	1 台以上のコントローラが NSX Manager に登録されて いますか。	NSX Controller クラスタがマジョリティ を持っていますか。	NSX Controller クラスタのメンバーのい ずれかが停止していますか。
NO_CONTROLLERS	いいえ	該当なし	該当なし
UNAVAILABLE	不明	不明	不明
STABLE	○	○	いいえ
DEGRADED	○	○	○
UNSTABLE	○	いいえ	いいえ

## 手順

- 1 NSX Manager CLI にログインします。
- 2 `get management-cluster status` コマンドを実行します。

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 3
- 192.168.110.203 (UUID 564DDA9E-8E84-E374-1F12-C69FAAE6A698) Online
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online
- 192.168.110.202 (UUID 564DC1B0-259A-9D6C-AF1F-12AEB6951882) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)

Control cluster status: STABLE
```

- 3 NSX Controller CLI にログインします。
- 4 `get control-cluster status` コマンドを実行します。

```
nsx-controller-1> get control-cluster status
uuid: 03fad907-612f-4068-8109-efdf73002038
is master: true
in majority: true


| uuid                                 | address        | status |
|--------------------------------------|----------------|--------|
| 03fad907-612f-4068-8109-efdf73002038 | 192.168.110.51 | active |
| 1228c336-3932-4b5b-b87e-9f66259cebcd | 192.168.110.52 | active |
| f5348a2e-2d59-4edc-9618-2c05ac073fd8 | 192.168.110.53 | active |


```

## NSX Controller クラスタ メンバーの再起動

NSX Controller クラスタの複数のメンバーを再起動する場合は、一度に 1 つずつメンバーを再起動する必要があります。3 つのメンバーから成るクラスタは、1 つのメンバーがオフラインになってもマジョリティを持つことができます。2 つのメンバーがオフラインになると、クラスタはマジョリティを失い、正常に機能しなくなります。

## 手順

- 1 NSX Manager の CLI にログインします。
- 2 管理およびコントロール クラスタのステータスを取得します。

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 3
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online
- 192.168.110.202 (UUID 564D0B9E-DEBD-A19E-233C-C13432CB23FB) Online
- 192.168.110.203 (UUID 564D666C-EB23-CDC1-8101-95155E9EB916) Online

Management cluster status: STABLE
```

```

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)

Control cluster status: STABLE

```

- 3 再起動が必要な NSX Controller の CLI にログインし、再起動します。

```

nsx-controller-2> reboot
Are you sure you want to reboot (yes/no): y

```

- 4 管理およびコントロールクラスタのステータスを再度取得します。コントロールクラスタのステータスが **STABLE** になってから、追加のメンバーを再起動します。

この例では、NSX Controller 192.168.110.53 が再起動中で、コントロールクラスタのステータスは **DEGRADED** です。これは、クラスタがマジョリティを持ち、ただしメンバーの 1 つが停止していることを意味します。NSX Controller クラスタのステータスの詳細については、[「NSX Controller クラスタのステータスの取得」](#) を参照してください。

```

nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 3
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online
- 192.168.110.202 (UUID 564D0B9E-DEBD-A19E-233C-C13432CB23FB) Online
- 192.168.110.203 (UUID 564D666C-EB23-CDC1-8101-95155E9EB916) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)

Control cluster status: DEGRADED

```

NSX Controller クラスタのステータスが **STABLE** になると、追加のメンバーを安全に再起動することができます。

```

nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 3
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online
- 192.168.110.202 (UUID 564D0B9E-DEBD-A19E-233C-C13432CB23FB) Online
- 192.168.110.203 (UUID 564D666C-EB23-CDC1-8101-95155E9EB916) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)

```

- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)

Control cluster status: STABLE

- 5 個々の NSX Controller アプライアンス ステータスに関する情報が必要な場合は、NSX Controller にログインし、**get control-cluster status** コマンドを実行することができます。

```
nsx-controller-1> get control-cluster status
uuid: 03fad907-612f-4068-8109-efdf73002038
is master: true
in majority: true
uuid                                address                        status
03fad907-612f-4068-8109-efdf73002038 192.168.110.51                active
1228c336-3932-4b5b-b87e-9f66259cebcd 192.168.110.52                active
f5348a2e-2d59-4edc-9618-2c05ac073fd8 192.168.110.53                not active
```

- 6 必要に応じて、手順を繰り返して追加の NSX Controller アプライアンスを再起動します。

## NSX Controller クラスタのメンバーの置き換え

NSX Controller クラスタには少なくとも 3 つのメンバーが必要です。NSX Controller アプライアンスが動作不能になり、クラスタから削除する必要がある場合は、まず新しい NSX Controller アプライアンスを追加してクラスタのメンバーの数を 4 つにする必要があります。4 番目のメンバーを追加したら、NSX Controller アプライアンスをクラスタから削除することができます。

### 前提条件

- トラブルシューティングを通じて、アプライアンスがリカバリ不能であることを確認してください。たとえば、次の手順を行うことで、アプライアンスを交換せずにリカバリできる場合があります。
  - アプライアンスがネットワークに接続されていることを確認します。接続されていない場合は解決します。
  - アプライアンスを再起動します。
- 置き換える NSX Controller のバージョンを確認し、同じバージョンの適切なインストール ファイル（OVA、OVF、または QCOW2）が使用可能であることを確認します。

### 手順

- 1 新しい NSX Controller をインストールして設定します。

これらの手順の情報と手順については、『NSX-T インストール ガイド』を参照してください。

- 新しい NSX Controller アプライアンスをインストールします。  
新しい NSX Controller のバージョンは交換する NSX Controller と同じである必要があります。
- 管理プレーンに新しい NSX Controller を参加させます。
- 制御クラスタに新しい NSX Controller を参加させます。

- 2 クラスタから削除する NSX Controller をシャット ダウンします。

- 3 別の NSX Controller にログインし、削除する NSX Controller のステータスが **not active** であることを確認します。

```
nsx-controller-1> get control-cluster status
uuid: e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b
is master: true
in majority: true


| uuid                                 | address        | status     |
|--------------------------------------|----------------|------------|
| 06996547-f50c-43c0-95c1-8bb644dea498 | 192.168.110.53 | active     |
| 471e5ac0-194b-437c-9359-564cea845333 | 192.168.110.54 | active     |
| e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b | 192.168.110.51 | active     |
| 863f9669-509f-4eba-b0ac-61a9702a242b | 192.168.110.52 | not active |


```

- 4 クラスタからコントローラを切り離します。

```
nsx-controller-1> detach control-cluster 192.168.110.52
Successfully detached node from the control cluster.
```

- 5 管理プレーンからコントローラを切り離します。

```
nsx-manager-1> detach controller 863f9669-509f-4eba-b0ac-61a9702a242b
The detach operation completed successfully
```

- 6 コントローラがアクティブで、制御クラスタが安定していることを確認します。

NSX Controller から :

```
nsx-controller-1> get control-cluster status
uuid: e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b
is master: true
in majority: true


| uuid                                 | address        | status |
|--------------------------------------|----------------|--------|
| 06996547-f50c-43c0-95c1-8bb644dea498 | 192.168.110.53 | active |
| 471e5ac0-194b-437c-9359-564cea845333 | 192.168.110.54 | active |
| e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b | 192.168.110.51 | active |


```

NSX Manager から :

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 4213216E-F93A-71B2-DA20-AFE5E714644F) Online
- 192.168.110.202 (UUID 4227F3D2-B7FE-8925-EA45-95ECD829C3E2) Online
- 192.168.110.203 (UUID 4227824A-1BDD-3A72-3EB3-8D306FEAE42D) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.51 (UUID e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b)
```

- 192.168.110.53 (UUID 06996547-f50c-43c0-95c1-8bb644dea498)
- 192.168.110.54 (UUID 471e5ac0-194b-437c-9359-564cea845333)

Control cluster status: STABLE

## NSX Controller クラスタの再展開

1 つのコントローラを置き換えても NSX Controller クラスタの問題が解決しない場合、または複数の NSX Controller アプライアンスが回復不能な場合は、クラスタ全体を再展開することができます。NSX Manager には希望の設定状態がすべて含まれ、NSX Controller クラスタを再作成するために使用することができます。

NSX Controller クラスタの復元中にデータ パス接続は中断されません。

### 前提条件

- トラブルシューティングを通じて、アプライアンスがリカバリ不能であることを確認してください。たとえば、次の手順を行うことで、アプライアンスを交換せずにリカバリできる場合があります。
  - アプライアンスがネットワークに接続されていることを確認します。接続されていない場合は解決します。
  - アプライアンスを再起動します。
- 置き換える NSX Controller のバージョンを確認し、同じバージョンの適切なインストール ファイル (OVA、OVF、または QCOW2) が使用可能であることを確認します。
- NSX Controller アプライアンスに割り当てられた IP アドレスを確認します。

### 手順

- 1 NSX Controller クラスタのすべてのコントローラをシャット ダウンします。

## 2 NSX Manager からコントローラを切り離します。

- a NSX Manager CLI にログインします。
- b `get management-cluster status` コマンドを使用してコントローラのリストを取得します。

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 422EC8D8-B43F-D206-5048-781A5AECDC6) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID c28d0ac7-3107-4548-817a-50d76db007ab)
- 192.168.110.51 (UUID 4a0916c7-2f4d-48c2-81b6-29b7b3758ef4)
- 192.168.110.52 (UUID 1a409f24-9b9a-431e-a03a-1929db74bf00)

Control cluster status: UNSTABLE
```

- c `detach controller` コマンドを使用してコントローラを切り離します。

```
nsx-manager-1> detach controller 1a409f24-9b9a-431e-a03a-1929db74bf00
The detach operation completed successfully
nsx-manager-1> detach controller 4a0916c7-2f4d-48c2-81b6-29b7b3758ef4
The detach operation completed successfully
nsx-manager-1> detach controller c28d0ac7-3107-4548-817a-50d76db007ab
The detach operation completed successfully
```

## 3 3 台の NSX Controller アプライアンスをインストールし、新しい NSX Controller クラスタを作成します。

これらの手順の詳細については、『NSX-T インストール ガイド』を参照してください。

- a 3 台の NSX Controller アプライアンスをインストールします。
  - 新しい NSX Controller アプライアンスのバージョンは交換する NSX Controller アプライアンスと同じである必要があります。
  - 新しいコントローラに古いコントローラに使用された同じ IP アドレスを割り当てます。
- b 管理プレーンに NSX Controller アプライアンスを参加させます。
- c NSX Controller アプライアンスの 1 つでコントロール クラスタを初期化します。
- d 残りの 2 つのコントローラをコントロール クラスタに参加させます。

## NSX Edge クラスタの管理

たとえば、NSX Edge が動作不能になった場合、またはハードウェアの変更が必要になった場合は、交換することができます。新しい NSX Edge をインストールし、新しいトランスポート ノードを作成した後、Edge クラスタを変更して古いトランスポート ノードを新しいトランスポート ノードに交換することができます。

**注:** Tier-1 の Edge クラスタを削除すると、Tier-1 分散ルーター (DR) インスタンスは短時間の間非稼動状態になります。

## 手順

- 1 交換する NSX Edge が動作中の場合は、それをメンテナンス モードにすることによってダウンタイムを最小限にすることができます。関連付けられた分散論理ルーター上で高可用性が有効になっている場合、メンテナンス モードにすると、分散論理ルーターは別の Edge クラスタ メンバーを使用します。この手順は、NSX Edge が動作不能状態の場合は必要ありません。

- a 失敗したファブリック ノードのファブリック ノード ID を取得します。

```
https://192.168.110.201/api/v1/fabric/nodes
...
  "resource_type": "EdgeNode",
  "id": "a0f4fa74-e77c-11e5-8701-005056aeed61",
  "display_name": "edgenode-02a",
...
```

- b 失敗した NSX Edge ノードをメンテナンス モードにします。

```
POST https://192.168.110.201/api/v1/fabric/nodes/a0f4fa74-
e77c-11e5-8701-005056aeed61?action=enter_maintenance_mode
```

- 2 新しい NSX Edge をインストールします。

これらの手順の詳細については、『NSX-T インストール ガイド』を参照してください。

- 3 **join management-plane** コマンドを使用して管理プレーンに新しい NSX Edge を参加させます。

これらの手順の詳細については、『NSX-T インストール ガイド』を参照してください。



#### 4 NSX Edge をトランスポート ノードとして設定します。

これらの手順の詳細については、『NSX-T インストール ガイド』を参照してください。

API から失敗した NSX Edge アプライアンスのトランスポート ノード設定を取得し、この情報を使用して新しいトランスポート ノードを作成することができます。

- a 新しいファブリック ノードのファブリック ノード ID を取得します。

```
https://192.168.110.201/api/v1/fabric/nodes
...
  "resource_type": "EdgeNode",
  "id": "d61c8d86-f4b8-11e5-b1b2-005056ae3c10",
  "display_name": "edgenode-03a",
...
```

- b 失敗したトランスポート ノードのトランスポート ノード ID を取得します。

```
GET https://192.168.110.201/api/v1/transport-nodes
...
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
...
}
```

- c 失敗したトランスポート ノードのトランスポート ノード設定を取得します。

```
GET https://192.168.110.201/api/v1/transport-nodes/73cb00c9-70d0-4808-abfe-a12a43251133
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
  "tags": [],
  "transport_zone_endpoints": [
    ...
  ],
  "host_switches": [
    ...
  ],
  "node_id": "a0f4fa74-e77c-11e5-8701-005056aeed61",
  "_create_time": 1457696199196,
  "_last_modified_user": "admin",
  "_last_modified_time": 1457696225606,
  "_create_user": "admin",
  "_revision": 2
}
```

- d POST /api/v1/transport-nodes を使用して新しいトランスポート ノードを作成します。

リクエストの本文で、新しいトランスポート ノードについての次の情報を提供します。

- 新しいトランスポート ノードの **description** (オプション)
- 新しいトランスポート ノードの **display\_name**
- 新しいトランスポート ノードを作成するために使用されるファブリック ノードの **node\_id**

リクエストの本文で、失敗したトランスポート ノードについての次の情報をコピーします。

- **transport\_zone\_endpoints**
- **host\_switches**
- **tags** (オプション)

```
POST https://192.168.110.201/api/v1/transport-nodes
{
  "description": "",
  "display_name": "TN-edgenode-03a",
  "tags": [
    ...
  ],
  "transport_zone_endpoints": [
    ...
  ],
  "host_switches": [
    ...
  ]
}
```

```
...  
],  
"node_id": "d61c8d86-f4b8-11e5-b1b2-005056ae3c10"  
}
```

## 5 Edge クラスタを編集して、失敗したトランスポート ノードを新しいトランスポート ノードに置き換えます。

- a 新しいトランスポート ノードおよび失敗したトランスポート ノードの ID を取得します。**id** フィールドにはトランスポート ノード ID が含まれています。

```
GET https://192.168.110.201/api/v1/transport-nodes
...
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
  ...
  {
    "resource_type": "TransportNode",
    "description": "",
    "id": "890f0e3c-aa81-46aa-843b-8ac25fe30bd3",
    "display_name": "TN-edgenode-03a",
    ...
  }
}
```

- b Edge クラスタの ID を取得します。**id** フィールドには Edge クラスタ ID が含まれています。**members** アレイから Edge クラスタのメンバーを取得します。

```
GET https://192.168.110.201/api/v1/edge-clusters
....
{
  "resource_type": "EdgeCluster",
  "description": "",
  "id": "9a302df7-0833-4237-af1f-4d826c25ad78",
  "display_name": "Edge-Cluster-1",
  ...
  "members": [
    {
      "member_index": 0,
      "transport_node_id": "73cb00c9-70d0-4808-abfe-a12a43251133"
    },
    {

```

```

        "member_index": 1,
        "transport_node_id": "e5d17b14-cdeb-4e63-b798-b23a0757463b"
    }
],

```

- c Edge クラスタを編集して、失敗したトランスポート ノードを新しいトランスポート ノードに置き換えます。**member\_index** は失敗したトランスポート ノードのインデックスに一致する必要があります。



**警告:** NSX Edge が動作中の場合、動作が中断します。これによってすべての分散論理ルーター ポートが失敗したトランスポート ノードから新しいトランスポート ノードに移動します。

この例では、トランスポート ノード TN-edgenode-01a (73cb00c9-70d0-4808-abfe-a12a43251133) が失敗し、Edge クラスタ Edge-Cluster-1 (9a302df7-0833-4237-af1f-4d826c25ad78) のトランスポート ノード TN-edgenode-03a (890f0e3c-aa81-46aa-843b-8ac25fe30bd3) に置き換えられます。

```

POST http://192.168.110.201/api/v1/edge-clusters/9a302df7-0833-4237-
af1f-4d826c25ad78?action=replace_transport_node
{
    "member_index": 0,
    "transport_node_id" : "890f0e3c-aa81-46aa-843b-8ac25fe30bd3"
}

```

- 6 (オプション) 失敗したトランスポート ノードおよび NSX Edge ノードを削除します。

## ロギング システム メッセージ

ESXi 上で実行するコンポーネント以外のすべての NSX-T コンポーネントからのログ メッセージは、RFC 5424 形式に準拠します。ログ メッセージを受信するようにリモート ログ サーバを設定することができます。

RFC 5424 の詳細については、<https://tools.ietf.org/html/rfc5424> を参照してください。

RFC 5424 は、ログ メッセージのための次の形式を定義します。

```
<facility * 8 + severity> version UTC-TZ hostname APP-NAME procid MSGID [structured-data] msg
```

NSX Manager からのログ メッセージのサンプル：

```
<187>1 2016-03-15T22:53:00.114Z nsx-manager NSX - SYSTEM [nsx@6876 comp="nsx-manager"
errorCode="MP4039" subcomp="manager"] Connection verification failed for broker
'10.160.108.196'. Marking broker unhealthy.
```

NSX-T は、通常のログ（ファシリティ local6。数値 22）および監査ログ（ファシリティ local7。数値 23）を生成します。すべての API 呼び出しは監査ログをトリガーします。

RFC 5424 は次の重要度レベルを定義します。

重要度の値	説明
0	緊急：システムが不安定な状態
1	アラート：迅速な対応が必要な状態

重要度の値	説明
2	重大：重大な状況
3	エラー：エラーが発生した状態
4	警告：警告が発生した状態
5	通知：正常ではあっても注意を要する状態
6	情報：情報メッセージ
7	デバッグ：デバッグレベルのメッセージ

重要度が緊急、アラート、重大、またはエラーのすべてのログには、ログ メッセージの構造化データの部分に固有のエラー コードがあります。エラー コードは文字列と 10 進数で構成されます。文字列は特定のモジュールを表わします。

MSGID フィールドはログ メッセージのカテゴリを示します。カテゴリのリストについては、「[ログ メッセージのカテゴリ](#)」を参照してください。

## リモート ログの設定

リモート ログ サーバにログ メッセージを送信するように NSX-T アプライアンスおよびハイパーバイザーを設定することができます。

リモート ログは NSX Manager、NSX Controller、NSX Edge アプライアンスでサポートされます。およびハイパーバイザー。

次の基準に基づいて、どのログ メッセージをログ サーバに送信するかをフィルタすることができます。

- レベル：emerg、alert、crit、err、warning、notice、info、debug
- ファシリティ：コードは RFC 5424 で定義されています。監査メッセージにはファシリティ local7 が使用され、監査以外のメッセージには local6 が使用されます。
- メッセージ ID またはカテゴリ：カテゴリと例は、「[ログ メッセージのカテゴリ](#)」にリストされています。

関連するコマンドおよび要求については、『NSX-T コマンドライン リファレンス』と『NSX-T API ガイド』を参照してください。

### 前提条件

- NSX-T アプライアンスからログを受信するようにリモート ログ サーバを設定します。
- どのようなログ メッセージをログ サーバに送信するかを決定します。

### 手順

- 1 リモート ログを設定する NSX-T アプライアンスにログインします。
- 2 次の構文で **set logging-server** コマンドを使用し、ログ サーバを設定します。複数のファシリティまたはメッセージ ID は、スペースなしのカンマ区切りのリストとして指定することができます。

```
set logging-server <hostname-or-ip-address[:port]> proto <proto> level <level> [facility <facility>] [messageid <messageid>] [certificate <filename>]
```

コマンドを複数回実行し、複数のログ サーバ設定を追加することができます。

```
nsx> set logging-server 192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
nsx> set logging-server 192.168.110.60 proto udp level info facility auth,user
```

3 (オプション) **get logging-server** コマンドを実行してログの設定を表示します。

```
nsx> get logging-servers
192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
192.168.110.60 proto udp level info facility auth,user
```

## ログ メッセージのカテゴリ

ログ メッセージはカテゴリに属します。これらのカテゴリは、どのログ メッセージをログ サーバに送信するかをフィルタするために **set logging-server** コマンドで使用することができます。

表 11-4. ログ メッセージのカテゴリ

ログ メッセージのカテゴリ	例
FABRIC	ホスト ノード ホストの準備 Edge ノード トランスポート ゾーン トランスポート ノード アップリンク プロファイル クラスタ プロファイル Edge クラスタ ブリッジ クラスタとエンドポイント
SWITCHING	論理スイッチ 論理スイッチ ポート スイッチング プロファイル スイッチ セキュリティ機能
ROUTING	分散論理ルーター 分散論理ルーター ポート 固定ルーティング 動的ルーティング NAT
FIREWALL	ファイアウォール ルール ファイアウォール ルール セクション
FIREWALL_PKTLOG	ファイアウォール接続ログ ファイアウォール パケット ログ

表 11-4. ログ メッセージのカテゴリ (続き)

ログ メッセージのカテゴリ	例
GROUPING	IP セット MAC セット NSGroup NSService NSService グループ VNI プール IP アドレス プール
DHCP	DHCP リレー
SYSTEM	アプライアンス管理 (リモート Syslog、ntp など) クラスタ管理 信頼管理 ライセンス ユーザーとロール タスク管理 インストール (NSX Manager、NSX Controller) アップグレード (NSX Manager、NSX Controller、NSX Edge およびホスト パッケージのアップグレード) 実現 タグ
MONITORING	SNMP ポート接続 トレースフロー
-	その他のすべてのログ メッセージ

## IPFIX の設定

IPFIX (Internet Protocol Flow Information Export) は、ネットワーク フロー情報の形式とエクスポートの標準です。IPFIX を有効にすると、設定済みのすべてのホスト トランスポート ノードが、ポート 4739 を使用して IPFIX メッセージを IPFIX コレクタに送信します。

ESXi の場合、NSX-T は自動的にポート 4739 を開きます。KVM でファイアウォールが有効になっていない場合、ポート 4739 が開かれます。ファイアウォールが有効になっている場合、NSX-T によってこのポートが自動的に開かれないため、ポートが開いていることを確認する必要があります。

### 前提条件

- 1 個以上の IPFIX コレクタをインストールします。
- IPFIX コレクタがハイパーバイザーにネットワーク接続できることを確認します。
- ESXi ファイアウォールを含む関連ファイアウォールで、IPFIX コレクタ ポート上のトラフィックが許可されることを確認します。



## 手順

1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。

2 ナビゲーション パネルから、[ツール (Tools)] - [IPFIX] の順に選択します。

3 まだ選択していない場合は、[コレクタ (Collectors)] タブをクリックします。

4 [コレクタの設定 (Configure Collectors)] をクリックします。

5 [追加 (Add)] をクリックし、コレクタの IP アドレスとポートを入力します。

最大で 8 個のコレクタを追加できます。

6 (オプション) 収集オプションのセクションで、[編集 (Edit)] をクリックして監視ドメイン ID を指定します。

監視ドメイン ID は、ネットワーク フローの送信元である監視ドメインを識別します。デフォルト値は 0 で、特定の監視ドメインを指定しません。

7 [IPFIX プロファイルのスイッチ (Switch IPFIX Profiles)] タブをクリックします。

8 [追加 (Add)] をクリックしてプロファイルを追加します。

設定	説明
アクティブ タイムアウト (秒)	フローをタイムアウトにするまでの時間 (秒) を指定します。フローに関連付けられているパケットを受信中の場合でも、フローはタイムアウトになります。デフォルト値は 300 です。
アイドル タイムアウト (秒)	フローと関連付けられているパケットを受信しない場合に、フローがタイムアウトするまでの時間 (秒) を指定します。これは ESXi の場合にのみ有効です。KVM の場合は、アクティブ タイムアウトの値に基づいて、すべてのフローがタイムアウトします。デフォルト値は 300 です。
最大フロー数	ブリッジにキャッシュされるフローの最大数を指定します。KVM の場合にのみ有効です。ESXi では設定できません。デフォルト値は 16384 です。
サンプリングの割合 (%)	サンプリングされるパケットの割合です (概数値)。この値を高くすると、ハイパーバイザーとコレクタのパフォーマンスに影響する場合があります。すべてのハイパーバイザーがより多くの IPFIX パケットをコレクタに送信した場合、コレクタですべてのパケットを収集できない可能性があります。この設定をデフォルト値の 0.1% にすると、パフォーマンスに与える影響が低くなります。

9 [適用先 (Applied To)] をクリックして、プロファイルを 1 個以上のオブジェクトに適用します。

オブジェクトのタイプは、論理ポートと論理スイッチです。

ESXi と KVM の IPFIX は異なる方法でトンネル パケットをサンプリングします。ESXi では、トンネル パケットは 2 つのレコードとしてサンプリングされます。

- 一部の内部パケット情報を備えた外部パケット レコード
  - SrcAddr、DstAddr、SrcPort、DstPort、およびプロトコルは外部パケットを参照します。
  - 内部パケットを記述するためのいくつかのエンタープライズ エントリを含んでいます。
- 内部パケット レコード
  - SrcAddr、DstAddr、SrcPort、DstPort、およびプロトコルは内部パケットを参照します。

KVM では、トンネル パケットは 1 つのレコードとしてサンプリングされます。

- 一部の外部トンネル情報を備えた内部パケット レコード
  - SrcAddr、DstAddr、SrcPort、DstPort、およびプロトコルは内部パケットを参照します。
  - 外部パケットを記述するためのいくつかのエンタープライズ エントリを含んでいます。

## トレースフローによるパケットのパスのトレース

トレースフローを使用して、論理ネットワーク上のある論理ポートから同じネットワーク上の別の論理ポートに移動するパケットのパスを検査します。トレースフローは、論理ポートで取り込まれたパケットのトランスポート ノードレベルのパスをトレースします。トレース パケットは論理スイッチ オーバーレイを横断しますが、論理スイッチに接続されたインターフェイスでは確認できません。すなわちパケットは、実際にはテスト パケットで意図された受信者に配信されません。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 [トレースフロー] 画面に移動します。これには次の 2 つのオプションがあります。
  - ナビゲーション パネルから [ツール (Tools)] - [トレースフロー (Traceflow)] の順に選択します。
  - ナビゲーション パネルから [スイッチング (Switching)] を選択し、[ポート (Ports)] タブをクリックして、VIF に接続されたポートを選択し、[アクション (Actions)] - [トレースフロー (Traceflow)] の順にクリックします。
- 3 トラフィック タイプを選択します。  
タイプには、ユニキャスト、マルチキャスト、ブロードキャスト があります。
- 4 トラフィック タイプに従って送信元と宛先情報を指定します。

トラフィック タイプ	送信元情報を指定	宛先情報を指定
ユニキャスト	<p>仮想マシンと仮想インターフェイスを選択します。</p> <p>VMware Tools が仮想マシンにインストールされている場合、または仮想マシンが OpenStack プラグインを使用してデプロイされている (アドレスバインドが使用される) 場合は、IP アドレスと MAC アドレスが表示されます。仮想マシンに複数の IP アドレスが設定されている場合は、ドロップダウン メニューから 1 つを選択してください。</p> <p>IP アドレスと MAC アドレスが表示されない場合は、テキスト ボックスに IP アドレスと MAC アドレスを入力します。</p> <p>これはマルチキャストとブロードキャストにも適用されます。</p>	<p>[タイプ] ドロップダウン メニューから仮想マシン名または IP-MAC のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>■ 仮想マシン名を選択した場合は、仮想マシンおよび仮想インターフェイスを選択します。IP アドレスと MAC アドレスを選択または入力します。</li> <li>■ IP-MAC を選択した場合は、トレース タイプ ([レイヤー 2] または [レイヤー 3]) を選択します。トレース タイプが [レイヤー 2] の場合は、IP アドレスと MAC アドレスを入力します。トレース タイプが [レイヤー 3] の場合は、IP アドレスを入力します。</li> </ul>
マルチキャスト	上と同じ。	IP アドレスを入力します。224.0.0.0 ~ 239.255.255.255 までのマルチキャスト アドレスである必要があります。
ブロードキャスト	上と同じ。	サブネット プリフィックス長を入力します。

- 5 (オプション) [詳細 (Advanced)] をクリックして詳細オプションを表示します。
- 6 (オプション) 左の列で、希望の値を入力するか、次のフィールドに入力します。

オプション	説明
フレーム サイズ	例：128
TTL	例：64
タイムアウト (ミリ秒)	例：10000
EtherType	例：2048
ペイロード タイプ	ドロップダウン メニューからオプションを選択します。
ペイロード データ	選択されたペイロードタイプ ([Base64]、[Hex]、[Plaintext]、[Binary]、または [Decimal]) に基づいて書式設定されたペイロード

- 7 (オプション) 左の列の [プロトコル] で、[タイプ] ドロップダウン メニューからプロトコルを選択します。
- 8 (オプション) 選択したプロトコルに基づいて、次のテーブルの関連する手順を完了します。

プロトコル	ステップ 1	ステップ 2	ステップ 3
TCP	送信元ポートを入力します。	宛先ポートを入力します。	ドロップダウン メニューから適切な TCP フラグを選択します。
UDP	送信元ポートを入力します。	宛先ポートを入力します。	該当なし
ICMP	ICMP ID を入力します。	シーケンス値を入力します。	該当なし

- 9 [トレース (Trace)] をクリックします。

接続、コンポーネントおよびレイヤーに関する情報が表示されます。出力には、監視タイプ (配信済み、ドロップ、受信、転送済み)、トランスポート ノードおよびコンポーネントをリストしたテーブルが含まれ、さらに宛先としてユニキャストと論理スイッチを選択した場合は、グラフィカルなトポロジ マップが含まれます。表示される監視記録に、フィルタとして [すべて (All)]、[配信済み (Delivered)]、[ドロップ (Dropped)] を適用することができます。ドロップされた監視記録がある場合は、デフォルトで [ドロップ (Dropped)] フィルタが適用されます。ドロップされた監視記録がない場合は、[すべて (All)] フィルタが適用されます。

## ポート接続情報の表示

ポート接続ツールを使用して、2 台の仮想マシン間の接続状態を迅速に視覚化し、トラブルシューティングを実行できます。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[ツール] - [ポート接続ツール] の順に選択します。
- 3 [ソース仮想マシン] ドロップダウン メニューから仮想マシンを選択します。
- 4 [ターゲット仮想マシン] ドロップダウン メニューから仮想マシンを選択します。

## 5 [移動] をクリックします。

ポート接続トポロジを視覚化したマップが表示されます。表示されたコンポーネントをクリックすると、そのコンポーネントの詳細を確認できます。

# 論理スイッチ ポート アクティビティの監視

論理ポート アクティビティを監視することで、たとえば輻輳するネットワークやパケットのドロップに対してトラブルシューティングを行うことができます。

## 前提条件

論理スイッチ ポートが設定されていることを確認します。[「論理スイッチへの仮想マシンの接続」](#)を参照してください。

## 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから [スイッチング (Switching)] - [ポート (Port)]の順に選択します。
- 3 監視する論理スイッチ ポートをダブルクリックします。
- 4 [監視 (Monitor)] タブをクリックします。
- 5 [追跡を開始 (Begin Tracking)] を選択します。

ポート追跡ページが開きます。

- 6 論理スイッチ ポート上で監視アクティビティを開始します。

双方向のポート トラフィックを監視して、ドロップされたパケットを特定することができます。ポートの追跡ページには、論理スイッチポートに接続されたスイッチング プロファイルもリストされます。

たとえば、ネットワークの輻輳が原因でパケットのドロップが見つかった場合、論理スイッチ ポートの QoS スイッチング プロファイルを設定して優先パケット上のデータ損失を防ぐことができます。[「QoS スイッチング プロファイルの理解」](#)を参照してください。

# ポート ミラーリング セッションの開始

トラブルシューティングおよびその他の目的でポート ミラーリング セッションを監視することができます。

この機能には次の制限があります。

- 送信元のミラー ポートを複数のミラー セッションで使用することはできません。
- 宛先ポートはミラー トラフィックのみを受け取ることができます。
- KVM では、複数の NIC を同じ OVS ポートに接続することができます。ミラーリングは OVS アップリンク ポートで発生します。これは、OVS ポートに接続されたすべての pNIC 上のトラフィックがミラーリングされることを意味します。
- ミラー セッションの送信元および宛先ポートは、同じホストの vSwitch 上にある必要があります。したがって、送信元または宛先ポートを持つ仮想マシンを vMotion によって別のホストに移行すると、そのポート上のトラフィックはミラーリングすることができなくなります。

- ESXi 上でアップリンクのミラーリングを有効にすると、VDL2 によって Geneve プロトコルが使用され、本番環境の raw TCP パケットが UDP パケットにカプセル化されます。TSO (TCP Segmentation Offload) をサポートする物理 NIC は、パケットを変更し、パケットに MUST\_TSO フラグを付けることができます。VMXNET3 または E1000 vNIC を使用するモニター仮想マシンでは、ドライバはパケットを通常の UDP パケットとして処理し、MUST\_TSO フラグに対応していないため、パケットがドロップされます。

大量のトラフィックがモニター仮想マシンにミラーリングされると、ドライバのリング バッファがいっぱいになり、パケットのドロップが発生する可能性があります。この問題を緩和するには、次のいずれかのアクションを実行します。

- 受信バッファのリング サイズを増やします。
- 仮想マシンにより多くの CPU リソースを割り当てます。
- データ プレーン デベロップメント キット (DPDK) を使用してパケット処理のパフォーマンスを改善します。

**注:** モニター仮想マシンの MTU 設定が、パケットの処理に十分な大きさであることを確認します。KVM の場合は、ハイパーバイザーの仮想 NIC デバイスの MTU 設定も確認します。カプセル化によってパケットのサイズが増えるため、パケットをカプセル化する場合は特に重要な作業です。十分な大きさでない場合、パケットがドロップされる可能性があります。これは VMXNET3 NIC を使用する ESXi 仮想マシンの場合は問題ではありませんが、ESXi および KVM 仮想マシンでその他のタイプの NIC を使用する場合は問題となる可能性があります。

**注:** KVM ホストの仮想マシンを含む L3 ポート ミラーリング セッションでは、MTU サイズを十分に増やして、カプセル化によって必要となる追加容量を処理できるようにする必要があります。ミラー トラフィックは、OVS インターフェイスおよび OVS アップリンクを通過します。OVS インターフェイスの MTU は、カプセル化とミラーリング前の元のパケットのサイズより、少なくとも 100 バイト大きく設定する必要があります。パケットがドロップされる場合は、ホストの仮想 NIC および OVS インターフェイスの MTU 設定値を大きくします。次のコマンドを使用して OVS インターフェイスの MTU を設定します。

```
ovs-vsctl -- set interface <ovs_Interface> mtu_request=<MTU>
```

**注:** 仮想マシンの論理ポートおよび仮想マシンが常駐するホストのアップリンク ポートを監視する場合、ホストが ESXi か KVM かによって動作が異なります。ESXi の場合、論理ポート ミラー パケットおよびアップリンク ミラー パケットには同じ VLAN ID のタグが付けられ、モニター仮想マシンに同じように表示されます。KVM の場合、論理ポート ミラー パケットには VLAN ID のタグが付けられず、アップリンク ミラー パケットにはタグが付けられ、モニター仮想マシンには異なって表示されます。

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[ツール (Tools)] - [ポート ミラーリング セッション (Port Mirroring Session)] の順に選択します。
- 3 セッション名を入力します。
- 4 ドロップダウン メニューからトランスポート ノードを選択します。

ポート ミラーリング セッションは同じトランスポート ノード上の NIC 間で実行される必要があります。

- 5 ドロップダウン メニューから方向を選択します。  
[双方向 (Bidirectional)]、[入力側 (Ingress)]、および [出力側 (Egress)] から選択することができます。
- 6 (オプション) パケットの切り捨て値を選択します。
- 7 [次へ (Next)] をクリックします。
- 8 送信元 PNIC を選択します。
- 9 (オプション) [カプセル化パケット (Encapsulated Packet)] スイッチを切り替え、カプセル化されたトラフィックのキャプチャを無効にします。  
このスイッチはデフォルトで有効になっています。
- 10 送信元 vNIC を選択します。
- 11 宛先を選択します。  
最大で 3 台までの仮想マシンと 3 つの vNIC を選択することができます。
- 12 [保存 (Save)] をクリックします。  
ポート ミラーリング セッションを保存した後で送信元と宛先を変更することはできません。

## ファブリック ノードの監視

NSX Manager ユーザー インターフェイスから、ホスト、Edge、Edge クラスタ、ブリッジおよびトランスポート ノードなどのファブリック ノードを監視することができます。

### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[ファブリック (Fabric)] - [ノード (Nodes)] の順に選択します。
- 3 次のいずれかのタブを選択します。
  - ホスト
  - Edge
  - Edge クラスタ
  - ブリッジ
  - トランスポート ノード

---

**注:** [ホスト] 画面でホストの [MPA 接続] ステータスが [停止] または [不明] の場合、[LCP 接続] ステータスは不正確な場合があるので無視します。

---

## サポート バンドルの収集

登録されたクラスタおよびファブリック ノード上のサポート バンドルを収集し、バンドルをマシンにダウンロードするか、ファイル サーバにアップロードすることができます。

バンドルをマシンにダウンロードすることを選択すると、マニフェスト ファイルおよび各ノードのサポート バンドルで設定される単一のアーカイブ ファイルを受け取ります。バンドルをファイル サーバにアップロードすることを選択すると、マニフェスト ファイルおよび個々のバンドルがファイル サーバに個別にアップロードされます。

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 ナビゲーション パネルから、[システム (System)] - [ユーティリティ (Utilities)] の順に選択します。
- 3 [サポート バンドル (Support Bundle)] タブをクリックします。
- 4 宛先ノードを選択します。  
利用可能なノードのタイプは、管理ノード、コントローラ ノード、Edge およびホストです。
- 5 (オプション) ログの存続期間 (日) を指定し、指定した日数を超えて存続するログを除外します。
- 6 (オプション) コア ファイルおよび監査ログを含めるか除外するかを示すスイッチを切り替えます。  
コア ファイルおよび監査ログには、パスワードまたは暗号化キーのような機密情報が含まれている場合があります。
- 7 (オプション) チェック ボックスを選択して、バンドルをファイル サーバにアップロードします。
- 8 [バンドルの収集を開始 (Start Bundle Collection)] をクリックして、サポート バンドルの収集を開始します。  
存在するログ ファイルの数に応じて、収集には各ノードごとに数分かかる場合があります。
- 9 収集プロセスのステータスを監視します。  
ステータス フィールドは、サポート バンドルの収集を完了したノードの割合を示します。
- 10 ファイル サーバにバンドルを送信するオプションを設定していない場合は、[ダウンロード (Download)] をクリックしてバンドルをダウンロードします。